Citrix NetScaler 10 Essentials and Networking

Citrix Course CNS-205-1I

Citrix NetScaler 10 Essentials and Networking

Citrix Course CNS-205-1I
Exercise Workbook
October 2012
Version 1.0

Table of Contents

Notices

Citrix Systems, Inc. (Citrix) makes no representations or warranties with respect to the content or use of this publication. Citrix specifically disclaims any expressed or implied warranties, merchantability, or fitness for any particular purpose. Citrix reserves the right to make any changes in specifications and other information contained in this publication without prior notice and without obligation to notify any person or entity of such revisions or changes.

Citrix Systems, Inc.

851 West Cypress Creek Road

Fort Lauderdale, FL 33309 USA

http://www.citrix.com

The following marks are service marks, trademarks or registered trademarks of their respective owners in the United States and other countries.

Mark	Owner
Active Directory®, Microsoft®, Microsoft Internet Explorer®, .NET™, SQL Server®, Windows®, Win32™	Microsoft Corporation
ActivePerl®	ActiveState Software, Inc.
American Express®	American Express Company
Apache™	The Apache Software Foundation
Citrix®, Citrix Access Gateway™, Citrix Application Firewall™, Citrix Authorized Learning Center™, Citrix Certified Administrator™, Citrix Certified Enterprise Engineer™, Citrix Certified Integration Architect™, ICA®, NetScaler®, MyCitrix™	Citrix Systems, Inc.
Diners Club®	Diners Club International Ltd.
Discover®	Discover Financial Services

Mark	Owner
Firefox®	Mozilla Corporation
FreeBSD®	FreeBSD Foundation
Google™	Google, Inc.
Intel®, Pentium®	Intel Corporation
Java®	Oracle Corporation
JCB®	JCB International Co., Ltd.
Linux®	Linus Torvalds
LiveHTTPHeaders®	Mozdev Community Organization, Inc.
MasterCard®	MasterCard Worldwide
Pearson VUE®	Pearson Education, Inc.
PuTTy®	Simon Tatham
Secure Shell®, SSH®	SSH Communications Security Corp.
UNIX®	The Open Group
Visa®	Visa, Inc.
WinSCP®	Martin Prikryl, GNU General Public License, Free Software Foundation, Inc.

Credits

Instructional Designers:	Larry Barrios, Jeremy Boehl, Karen Bridgewater, Dustin Clark, Orlando Martinez, Christopher Rudolph
Product Specialists:	Brian Bustin, Andrew Garfield, George Komoto
Graphic Artist:	Joshua Jack
Manager:	Erin Smith
Editors:	Ben Goodman, Kathryn Morris
Translation Coordinator:	Yashica Burgess
Subject Matter Experts:	Gregg Anderson, Simon Barnes, Terry Chou, Colin Christy, Mahasweta Dey, Abhishek Gautam, Bino Gopal, Dave Gunn, David Jimenez, Henrik Johansson, Curtis Kegler, Henny Louwers, Archana Maheshwari, Sandeep Mehta, Mike Nelson, Ronan O'Brien, Senthil Periasamy, Craig Pickford, Marissa Schmidt, Muthukumar Shunmugiah, Mark Simmons, Erin Smith, John Smith, Jessy Strebel, Richard Todd, Lena Yarovaya, Sharin Yeoh, Tony Zhang

Lab Overview

This book contains exercises to accompany the NetScaler 10 Essentials content. This section provides an overview of the hosted lab content environment used with the lab exercises in this course.

NetScaler Configuration

For this course, each student has been provided with a hosted client workstation and an assigned group of NetScaler systems. The NetScaler systems have one interface connected to a front-end environment facing the hosted client and a back-end environment facing the back-end resources.

The assigned NetScaler systems are provided in an initial state with an assigned NetScaler IP (NSIP) on the front-end (public) network. Students will configure an assigned Subnet IP (SNIP) on the back-end (private) network. The NetScaler systems are configured with USNIP mode and, therefore, a Mapped IP (MIP) address is not required.

Lab Approach

Each exercise presented here begins with an introduction to the exercise, followed by detailed step-by-step instructions. The introduction is comprised of the following sections:

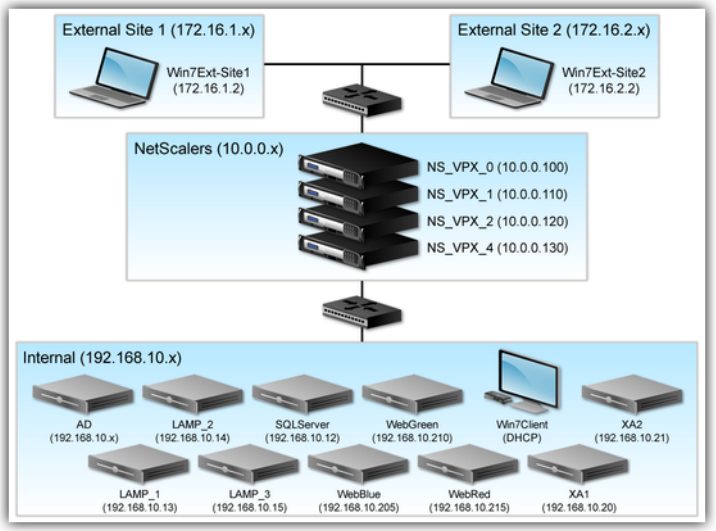
- Scenario: describes the end goal
- Before You Begin: lists the exercise dependencies

Lab Exercise Addresses

Below is a list of the IP, VIP, and SNIP addresses:

Name	Address
Virtual Machines	
NS_VPX_0	10.0.0.100
NS_VPX_1	10.0.0.110
NS_VPX_2	10.0.0.120
NS_VPX_3	10.0.0.130
NS_VPX_4 (clone)	10.0.0.100
Web_Blue	192.168.10.205
Web_Green	192.168.10.210
Web_Red	192.168.10.215
Win7Client	192.168.10.103
Virtual IP Addresses	
VIP 1	10.0.0.80
VIP 2	10.0.0.81
VIP 3	10.0.0.82
SNIP 1	10.0.0.90

Lab Environment Infrastructure



The lab network environment was created with real-world networks as a reference, but was simplified for the sake of learning. This lab environment should not be reproduced in a production network.

Module 1

Exercises for Getting Started

Exercise 1-1: Performing an Initial Configuration

Overview

This exercise will demonstrate how to complete an initial configuration on a NetScaler system, including how to set the date and time using a network time protocol server.

Before You Begin

To begin this lab, ensure that the following virtual machines are started:

- AD.training.lab
- NS_VPX_0
- Router-Vyatta
- Win7Client

Estimated time to complete this exercise: 5 minutes

Exercise 1-1: Step by Step (Configuration Utility)

This exercise provides step-by-step instructions for completing "Exercise 1-1: Performing an Initial Configuration" using the configuration utility.

Performing an Initial Configuration

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Log on to the NetScaler system from the configuration utility using the nsroot credentials.
   a. Open **XenCenter** from the hosted desktop.
   b. Select the Win7Client virtual machine, click the **Console** tab, and log on using the CitrixAdmin/Password1 credentials.
   c. Launch a **Firefox** browser window from the Win7Client desktop.
   d. Type `http://10.0.0.100` in the address bar and press **Enter**.
   e. Type `nsroot` in the User Name field, and type `nsroot` in the Password field, then click **Login**.
   f. Click **Close** when the Setup Wizard opens.

The Setup Wizard will be addressed in the next module.

2. Configure the NetScaler to your local time zone.
   a. Expand the **System** node and select **Settings**.
   b. Click **Change time zone** in the Settings pane.

      The Time Zone Selector window appears.
   c. Deselect **Use UTC Time Zone** and then choose the correct time zone from the drop-down menu and click **OK**.
   d. Click **Save** in the upper-right corner of the configuration utility window to save the NetScaler configuration, then click **Yes** to confirm saving the running configuration, and then click **OK** when the save has finished.
3. Add a network time protocol (NTP) server to the NetScaler using 192.168.10.11 as the server address.
   a. Expand the **System** node and select **NTP Servers**.
   b. Click **Add** in the NTP Servers pane.

      The Create NTP Server window appears.
   c. Type `192.168.10.11` in the NTP server field, select **Set as preferred NTP server**, click **Create** and then click **Close**.

      The Create NTP Server window closes.
   d. Click **Save** in the upper-right corner of the configuration utility window to save the NetScaler configuration, then click **Yes** to confirm saving the running configuration, and then click **OK** when the save has finished.

Exercise 1-1: Step by Step (Command-Line Interface)

This exercise provides step-by-step instructions for completing "Exercise 1-1: Performing an Initial Configuration" using the command-line interface.

Performing an Initial Configuration

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Connect to the NetScaler system from the command-line interface using PuTTY and open the NS_VPX_0 saved session. Log on using the nsroot credentials.
   a. Open **XenCenter** from the hosted desktop.
   b. Select the Win7Client virtual machine, click the **Console** tab, and log on using the CitrixAdmin/Password1 credentials.
   c. Launch the **PuTTY** command-line interface application from your desktop.

This lab environment uses PuTTY as the SSH client. Other SSH clients may be used to connect to the command-line interface, but their configuration and operation are not covered in this course.

d. Select **NS_VPX_0** from the saved sessions pane and click **Open**.

e. Type `nsroot` at the "login as:" prompt and press **Enter**. Then enter `nsroot` again in the password prompt and press **Enter**.

2. Configure the NetScaler to your local time zone.

a. Configure the time zone by entering the following command:

```
config ns
```

The Review Configuration Parameters menu appears.

b. Type `4` and press **Enter** to set the time zone.

The Time Zone Selector menu appears.

c. Use the Up Arrow and Down Arrow keys to browse to the appropriate region and press **Enter**.

d. Browse to your local time zone and press **Enter**.

e. Press **Enter** to confirm your selection.

f. Type `6` and press **Enter** to apply the changes and to exit the Review Configuration Parameters menu.

3. Set up a network time protocol (NTP) server on the NetScaler using 192.168.10.11 as a server and save the NetScaler configuration.

a. Add a NTP server to the NetScaler:

```
add ntp server 192.168.10.11
```

b. Save the NetScaler running configuration by entering the following command:

```
save ns config
```

Shorter forms of this command are also accepted.

```
save config
```

```
save ns c
```

```
save c
```

Exercise 1-2: Performing Basic Administration

Overview

This exercise will demonstrate how to complete basic administration tasks, such as enabling and disabling features, adding NetScaler administration accounts, compare the running and saved configurations, and perform a backup of the NetScaler system.

Before You Begin

To begin this lab, ensure that the following virtual machines are started:

- AD.training.lab
- NS_VPX_0
- Router-Vyatta
- Win7Client

Estimated time to complete this exercise: 25 minutes

Exercise 1-2: Step by Step (Configuration Utility)

This exercise provides step-by-step instructions for completing "Exercise 1-2: Performing Basic Administration" using the configuration utility.

Enabling and Disabling Features

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Enable SSL Offloading, HTTP Compression, Load Balancing, Content Switching, and Content Filter features.
   a. Expand the **System** node and select **Settings**.
   b. Click **Configure basic features** in the Settings node.
      The Configure Basic Features dialog box opens.
   c. Select the following features:
      - SSL Offloading
      - HTTP Compression
      - Load Balancing

- Content Switching
- Content Filter

d. Click **OK** to enable or disable the features.

Creating a New Administrator Account

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Create a new administrator account called "testuser" with read-only permissions.
   a. Expand the **System** node and select **Users**.
   b. Click **Add** in the System Users pane.

A dialog box may appear stating: "There might be some changes in configuration. Do you want to refresh the configuration?" You can click "Yes" when these dialog boxes appear throughout the course.

   The Create System User dialog box opens.
   c. Type `testuser` in the User Name field, then type `Password1` in the Password field and re-type `Password1` in the Confirm Password field.
   d. Select **read-only** in the Command Policies pane under Active, click **Create** and then click **Close**.

      The Create System User dialog box closes.
   e. Click **Save**, click **Yes**, and then click **OK** to save the current configuration. Click **Logout** to log off from of the current session.
2. Test the new administrator account by attempting to enable a feature.
   a. Log on to the configuration utility with the testuser/Password1 credentials that you just created.
   b. Click **Close** to close the Setup Wizard, when it appears.
   c. Expand the **System** node and select **Settings**.
   d. Click **Configure basic features** in the Settings node.

      The Configure Basic Features dialog box opens.
   e. Select a feature to enable and click **OK**.
   f. Verify that the chosen feature cannot be enabled with read-only access and click **OK**, and then click **Close**.
   g. Click **Logout** to log off from the current session.

Viewing the Running and Saved Configurations

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Review the current saved NetScaler configuration.
   a. Expand the **System** node and select **Diagnostics**.
   b. Click **Saved configuration** in the Diagnostics pane.

      The Saved Configuration dialog box is displayed.
   c. Review the configuration data and click **Close**.

      The Saved Configuration dialog box closes.
2. Review the current running NetScaler configuration.
   a. Click **Running configuration** in the Diagnostics pane and review the configuration data in the Running Configuration dialog box.

      The Running Configuration dialog box is displayed.
   b. Click **Close**.

      The Running Configuration dialog box closes.
   c. Click **Saved v/s running** in the Diagnostics pane.

      The Information dialog box is displayed.

      This dialog box shows that the settings between the saved configuration and the running configuration are identical.
   d. Click **OK**.

Performing a Configuration Backup

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Generate a support file to be used as a backup.
   a. Expand the **System** node and select **Diagnostics**.
   b. Click **Generate support file** in the Technical Support Tools section.

      The Tech Support script box opens.
   c. Click **Run**.

      The NetScaler will generate a backup of the entire configuration except for SSL certificates.
   d. Click **Close** when the script has finished.

This step may take up to two minutes for the script to complete.

2. Copy the newly created backup of the NetScaler configuration to your desktop using WinSCP.
   a. Launch **WinSCP** on your Win7Client desktop.
   b. Double-click the **NS_VPX_0** in the saved sessions pane.
   c. Type `nsroot` in the User name field, and press **Enter**; then type `nsroot` in the password field and press **Enter** again.
   d. In the right pane, double-click the folder icon at the top to navigate up one level from /root.
   e. Navigate to **var** > **tmp** > **support** and drag the **support.tgz** file from the right pane to the left pane.

      The Copy dialog box opens.
   f. Click **Copy** and then close the WinSCP application. Click **OK** to confirm the termination of the WinSCP session.

Exercise 1-2: Step by Step (Command-Line Interface)

This exercise provides step-by-step instructions for completing "Exercise 1-2: Performing Basic Administration" using the command-line interface.

Enabling and Disabling Features

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Enable the SSL Offloading, Compression Control, Load Balancing, Content Switching, and Content Filtering features.
   a. View the NetScaler features by entering the following command:

      ```
      show ns feature
      ```
   b. Enable the NetScaler features by entering the following command:

      ```
      enable ns feature SSL CMP LB CS CF
      ```

      This command enables SSL Offload, Compression, Load Balancing, Content Switching, and Content Filtering.

Creating a New Administrator Account

Use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Create a new system account with read-only permissions on the NetScaler system:

a. Create a new system user by entering the following command:

```
add system user testuser Password1
```

b. View the available command policies by entering the following command:

```
show system cmdPolicy
```

These command policies can be used to control the permissions allowed for delegated administration.

c. Configure the testuser with read-only permissions and a priority of 1 by entering the following command:

```
bind system user testuser read-only 1
```

d. Save the configuration by entering the following command:

```
save ns config
```

e. Log off from the current session by entering the following command:

```
logout
```

2. Verify the testuser permissions on the NetScaler system by trying to enable a feature.
   a. Open **PuTTY** from the Win7Client desktop and select the **NS_VPX_0** saved session.
   b. Type `testuser` at the "Login as:" prompt and press **Enter**. Then type `Password1` at the Password prompt and press **Enter**.
   c. Attempt to enable the Rewrite feature by entering the following command:

```
enable ns feature rewrite
```

   d. Verify that the command is not authorized when issued by a user with read-only access.

      You will receive an error because the testuser account has read-only permissions.

   e. Log off from the current session by entering the following command:

```
logout
```

Viewing the Running and Saved Configurations

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Log on to the command-line interface for NS_VPX_0 using PuTTY and log on using the nsroot credentials.
2. View the current running configuration.
   a. View the running configuration.

      ```
      show ns runningconfig
      ```

   b. View a summary of the current NetScaler configuration.

      ```
      show ns config
      ```

3. View the current saved configuration.
   a. View the saved configuration.

      ```
      show ns.conf
      ```

This is the current saved configuration. Any changes not saved in this file will be discarded at restart.

Performing a Configuration Backup

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Create a support file for the NetScaler.
   a. Create a backup of the NetScaler configuration by entering the following command:

      ```
      sh techsupport -scope node
      ```

      A backup directory named support.tgz is created in the /var/tmp/support directory.
2. Copy the newly created NetScaler support file to a local folder on your computer using the WinSCP utility.
   a. Launch **WinSCP** on your Win7Client desktop.
   b. Select **NS_VPX_0** in the saved sessions pane and click **Login**.
   c. Type `nsroot` in the User name field, and press **Enter**, then type `nsroot` in the password field and press **Enter** again.
   d. In the right pane, double-click the uppermost folder icon to navigate up one level from /root.
   e. Navigate to **var** > **tmp** > **support** and drag the **support.tgz** file from the right pane to the left pane.

      The Copy dialog box opens.

f. Click **Copy** and then close the WinSCP application, click **OK** to confirm the termination of the WinSCP session.

Exercise 1-3: Installing a NetScaler License

Overview

This exercise demonstrates how to install an upgrade license on a NetScaler.

Before You Begin

To begin this lab, ensure that the following virtual machines are started:

- AD.training.lab
- NS_VPX_0
- Router-Vyatta
- Win7Client

Estimated time to complete this exercise: 10 minutes

Exercise 1-3: Step by Step (Configuration Utility)

This exercise provides step-by-step instructions for completing "Exercise 1-3: Installing a NetScaler License" using the configuration utility.

Installing a License

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Examine the current license for the NetScaler appliance.
   a. Navigate to **System > Licenses** in the configuration utility.
   b. Examine the Model ID field and note the license for the NetScaler appliance.

The default licensed model ID is 1000.

2. Install an upgraded license on the NetScaler using the license provided on the Win7Client desktop.
   a. Expand the **System** node and select **Licenses**.
   b. Click **Manage Licenses** in the Licenses pane.
      The Manage Licenses window opens.

c. Click **Add**, browse to the Win7Client desktop, open the NetScaler License folder, and select the **NS_VPX_0-VPX_3000.lic** file.

d. Click **OK**, then select **Do a warm reboot** and **Save configuration**, then click **Yes**.

e. Close the Firefox browser window.

3. Verify that the NetScaler license has been upgraded.

a. Open a new Firefox browser window.

b. Browse to `http://10.0.0.100`.

c. Log on to the NetScaler using the nsroot credentials. Close the Setup Wizard when it appears.

d. Navigate to **System** > **Licenses** in the configuration utility.

e. Examine the Model ID field and note the upgraded license for the NetScaler appliance.

The Model ID should now read 3000.

Exercise 1-3: Step by Step (Command-Line Interface)

This exercise provides step-by-step instructions for completing "Exercise 1-3: Installing a License" using the command-line interface.

Installing a License

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Examine the current license on a NetScaler.

a. View the current NetScaler license.

```
show license | grep Model
```

2. Install an upgraded license on a NetScaler.

a. On the Win7Client desktop, double-click the **WinSCP** icon, then select **NS_VPX_0** and click **Login**.

b. Enter the `nsroot` in the Username field and click **OK**, then enter `nsroot` in the Password field and click **OK**.

c. Double-click the **uppermost folder** in the left pane, double-click **Desktop**, and then double-click the **NetScaler License** folder.

d. In the right pane of the WinSCP window, double-click the **uppermost folder** twice, double-click **nsconfig**, and then double-click **license**.

e. Click and drag the **NS_VPX_0-VPX_3000.lic** from the left pane to the right pane. Click **Copy** when the Copy window appears.

The license is copied to the NetScaler file system.

f. Close the WinSCP window.

3. Restart the NetScaler system to complete the license upgrade.

   a. Switch to the open PuTTY session on NS_VPX_0 and restart the NetScaler by entering the following command:

```
reboot -warm
```

```
y
```

   The NetScaler is restarted.

   b. Open a new PuTTY session for NS_VPX_0 and enter the following command to view the upgraded license:

```
show license | grep Model
```

   The NetScaler model shows as 3000.

Module 2

Exercises for Basic Networking

Exercise 2-1: Configuring Basic Networking

Overview

This exercise will demonstrate how to add a Subnet IP address to a NetScaler system.

Before You Begin

To begin this lab, ensure that the following virtual machines are started:

- AD.training.lab
- NS_VPX_0
- Win7Client

Estimated time to complete this exercise: 5 minutes

Exercise 2-1: Step by Step (Configuration Utility)

This exercise provides step-by-step instructions for completing "Exercise 2-1: Configuring Basic Networking" using the configuration utility.

Adding a Subnet IP to the NetScaler

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Add 10.0.0.90 as a Subnet IP address to the NetScaler.
   a. Expand the **Network** node and select **IPs**.
   b. Click **Add** at the bottom of the screen in the IPs pane.
   c. Type `10.0.0.90` in the IP address field and type `255.255.255.0` in the Netmask field.
   d. Verify that the following features are selected:
      - Subnet IP
      - Enable Management Access control to support the below listed applications

      Leave all other default settings.
   e. Click **Create**, then click **Close**.

Exercise 2-1: Step by Step (Command-Line Interface)

This exercise provides step-by-step instructions for completing "Exercise 2-1: Configuring Basic Networking" using the command-line interface.

Configuring the NetScaler Interface

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Add a Subnet IP address of 10.0.0.90 with a network mask of 255.255.255.0 to the NetScaler with Management Access enabled.
   a. Add a SNIP address to the NetScaler system by entering the following command:

```
add ns ip 10.0.0.90 255.255.255.0 -type SNIP
-mgmtAccess ENABLED
```

2. Enable Use Subnet IP mode.
   a. Enable USNIP mode by entering the following command:

```
enable ns mode USNIP
```

Module 3

Exercises for Basic Load Balancing

Exercise 3-1: Configuring Load Balancing

Overview

This exercise will demonstrate how to add servers, services, and a load balancing virtual server to a NetScaler, then configure all of those items to work together for load balancing.

Before You Begin

To begin this lab, ensure that the following virtual machines are started:

- AD.training.lab
- NS_VPX_0
- Router-Vyatta
- WebBlue
- WebGreen
- WebRed
- Win7Client

Estimated time to complete: 20 minutes

Exercise 3-1: Step by Step (Configuration Utility)

This exercise provides step-by-step instructions for completing "Exercise 3-1: Configuring Load Balancing" using the configuration utility.

Creating Servers

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Start the WebBlue, WebGreen, and WebRed virtual machines from the XenCenter console.
   a. Select the **WebBlue** virtual machine and click the **Start** button in the XenCenter toolbar.
   b. Repeat the previous substep for the WebGreen and WebRed virtual machines.
2. Configure the WebRed server as a "srv_red" load-balancing server with a 192.168.10.205 IP address.
   a. Switch to the Win7Client virtual machine and select the **Console** tab.
   b. Expand the **Load Balancing** node and select **Servers**.
   c. Click **Add** in the Servers pane.
      The Create Server dialog box opens.

d. Type `srv_red` in the Server Name field and then type `192.168.10.215` in the IP Address/Domain Name field.

e. Click **Create**.

The server appears in the Servers list.

3. Configure the WebGreen server as "srv_green" load-balancing server with a 192.168.10.210 IP address.

a. Type `srv_green` in the Server Name field and then type `192.168.10.210` in the IP Address field.

b. Click **Create**.

4. Configure the WebBlue server as a "srv_blue" load-balancing server with a 192.168.10.205 IP address.

a. Type `srv_blue` in the Server Name field and then type `192.168.10.205` in the IP Address field.

b. Click **Create** and then click **Close**.

Creating Services

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Create an HTTP service called svc_red that will be associated with the WebRed web server.

a. Expand the **Load Balancing** node and click **Services**.

b. Click **Add** in the Services pane.

The Create Service dialog box opens.

c. Type `svc_red` in the Service Name field.

d. Select **srv_red** from the Server list, and verify that **HTTP** is selected from the Protocol list and `80` is entered in the Port field.

e. Click **Create**.

2. Create an HTTP service called svc_blue that will be associated with the WebBlue web server.

a. Type `svc_blue` in the Service Name field.

b. Select **srv_blue** from the Server list, and verify that **HTTP** is selected from the Protocol list and `80` is entered in the Port field.

c. Click **Create**.

3. Create an HTTP service called svc_green that will be associated with the WebGreen web server.

a. Type `svc_green` in the Service Name field.

b. Select **srv_green** from the Server list, and verify that **HTTP** is selected from the Protocol list and `80` is entered in the Port field.

c. Click **Create**, then click **Close**.

The Create Service dialog box closes.

4. Verify that all services display the state listed as UP in the Services pane.

Creating a Load-Balancing Virtual Server

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Begin the configuration of a "lb_vsrv_rbg" load-balancing virtual server that will be associated with the red, blue, and green services.
   a. Expand the **Load Balancing** node and click **Virtual Servers**.
   b. Click **Add** in the Load Balancing Virtual Servers pane.
   c. Type `lb_vsrv_rbg` in the Name field and then type `10.0.0.80` in the IP Address field.
   d. Verify that **HTTP** is selected from the Protocol drop-down list and that `80` is entered in the Port field.
   e. Select the **Active** box for the following services on the Services tab:
      - svc_red
      - svc_blue
      - svc_green

      This action binds the selected services to the LB virtual server.
2. Complete the lb_vsrv_rbg load-balancing virtual server configuration by setting a round robin method and persistence. Create the virtual server.
   a. Click the **Method and Persistence** tab and select **Round Robin** from the LB Method drop-down list.
   b. Click **Create** and then click **Close**.
   c. Verify that the load-balancing virtual server lb_vsrv_rbg state is displayed as UP.
3. Save the running configuration.
   a. Click **Save** and click **Yes** to confirm saving the running configuration.
   b. Click **OK** once the configuration has successfully saved.

Testing Load Balancing

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Test the load-balancing configuration.
   a. Open a new Firefox window and browse to `http://10.0.0.80/home.php`
   b. Refresh the browser several times to verify load-balancing activity.

      With the round-robin method specified, the page should refresh and rotate through the Red, Blue, and Green home pages.

2. Change the persistence of the load-balancing virtual server to COOKIEINSERT.
   a. Switch back to the NetScaler configuration utility and expand the **Load Balancing** node and select **Virtual Servers**.
   b. Double-click the **lb_vsrv_rbg** virtual server to open its configuration window.
   c. Click on the **Method and Persistence** tab and change the Persistence from **NONE** to **COOKIEINSERT**.
   d. Click **OK**.
3. Test the updated load balancing configuration.
   a. Switch back to the other Firefox window and refresh the browser several times to verify the effects of load balancing with persistence.

      With cookie persistence enabled, you are directed to the same page each time until the cookie expires; the page does not load balance to each available server.

Resetting Persistence to None

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Reset the lb_vsrv_rbg load-balancing virtual server persistence to none.
   a. Expand the **Load Balancing** node and select **Virtual Servers**.
   b. Double-click the **lb_vsrv_rbg** virtual server to open its configuration window.
   c. Select the **Method and Persistence** tab, and select **NONE** from the Persistence drop-down list.

      Time-out and version settings are left as the default values.
   d. Click **OK**.
2. Save the running configuration.
   a. Click **Save** and click **Yes** to confirm saving the running configuration.
   b. Click **OK** once the configuration has successfully saved.

Exercise 3-1: Step by Step (Command-Line Interface)

This exercise provides step-by-step instructions for completing "Exercise 3-1: Configuring Load Balancing" using the command-line interface.

Procedure for Configuring Servers, Services, and Virtual Servers

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Start the WebBlue, WebGreen, and WebBlue virtual machines from the XenCenter console:

a. In XenCenter, click the WebBlue virtual machine, and click the **Start** button in the XenCenter toolbar.

b. Repeat the previous step for the WebGreen and WebRed virtual machines.

2. Configure the WebRed, WebBlue, and WebGreen web servers as load-balancing servers on the NetScaler.

   a. Switch to the PuTTY session to access the command-line interface for NS_VPX_0.

   b. Create the Red, Blue, and Green web servers using the following commands:

```
add server srv_red 192.168.10.215
```

```
add server srv_blue 192.168.10.205
```

```
add server srv_green 192.168.10.210
```

3. Create the svc_red, svc_blue, and svc_green HTTP services that will be associated with the web servers.

   a. Create HTTP services for Red, Blue, and Green web servers using the following commands:

```
add service svc_red srv_red HTTP 80
```

```
add service svc_blue srv_blue HTTP 80
```

```
add service svc_green srv_green HTTP 80
```

4. Create the lb_vsrv_rbg load-balancing virtual server that will be associated with the WebRed, WebBlue, and WebGreen web servers using Round Robin for the load balancing method.

   a. Create the load-balancing virtual server using the following command:

```
add lb vserver lb_vsrv_rbg HTTP 10.0.0.80 80 -
lbmethod ROUNDROBIN
```

   b. Bind the services to the load-balancing virtual server using the following commands:

```
bind lb vserver lb_vsrv_rbg svc_red
```

```
bind lb vserver lb_vsrv_rbg svc_blue
```

```
bind lb vserver lb_vsrv_rbg svc_green
```

Testing Load Balancing

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Test the load balancing configuration.
   a. Open a new Firefox window and browse to `http://10.0.0.80/home.php`
   b. Refresh the browser several times to verify load-balancing activity.

      With the round-robin method specified, the page should refresh and rotate through the Red, Blue, and Green home pages.
2. Change the persistence of the load-balancing virtual server to COOKIEINSERT.
   a. Set persistence for the existing load-balancing virtual server to COOKIEINSERT by entering the following command:

      ```
      set lb vserver lb_vsrv_rbg -persistenceType COOKIEINSERT
      ```
3. Test the updated load balancing configuration.
   a. Close the open Firefox window and open a new window and browse to `http://10.0.0.80/home.php`.
   b. Refresh the browser several times to verify the effects of load balancing with persistence.

      With cookie persistence enabled, you are directed to the same page each time until the cookie expires; the page does not load balance to each available server.
4. Change the persistence of the load-balancing virtual server to NONE.
   a. Set persistence for the existing load balancing virtual server to NONE by entering the following command:

      ```
      set lb vserver lb_vsrv_rbg -persistenceType NONE
      ```
   b. Save the configuration by entering the following command:

      ```
      save ns config
      ```


Module 4

Exercises for High Availability

Exercise 4-1: Configuring High Availability

Overview

This exercise will demonstrate how to create a high-availability pair, how to test the pair for redundancy, and how to properly break a high-availability pair.

Before You Begin

To begin this lab, ensure that the following virtual machines are started:

- AD.training.lab
- NS_VPX_1
- NS_VPX_2
- Router-Vyatta
- Win7Client

Estimated time to complete this exercise: 25 minutes

Exercise 4-1: Step by Step (Configuration Utility)

This exercise provides step-by-step instructions for completing "Exercise 4-1: Configuring High Availability" using the configuration utility.

Configuring NS_VPX_1 and NS_VPX_2

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_1 and 2 configuration utilities logged on as the nsroot user for this task.

1. Start NS_VPX_1 and NS_VPX_2 in XenCenter.
   a. In XenCenter, click the NS_VPX_1 virtual machine and click **Start** at the top of the window.

      Repeat this step for NS_VPX_2 as well.
2. Open the configuration utility for both NetScalers in Firefox and save their current configuration.
   a. In XenCenter, click on the Win7Client virtual machine and select the **Console** tab.
   b. Open two new Firefox browser windows. In the first Firefox window browse to `http://10.0.0.110` (this will be designated as NS_VPX_1) and in the second Firefox window, browse to `http://10.0.0.120` (this will be designated as NS_VPX_2).
   c. Log on to both NetScalers using the nsroot credentials.

d. On both NS_VPX_1 and 2, click the **Save** button in the upper-right corner of the configuration utility windows, click **Yes** to confirm saving the running configuration, and then click **OK** to confirm the save is complete.

3. Verify that high availability monitoring is active on NS_VPX_1 and NS_VPX_2 interfaces.
   a. NS_VPX_1 and 2: Expand the **Network** node and click **Interfaces**.
   b. NS_VPX_1 and 2: In the interfaces pane, scroll to the right to verify that high availability monitoring is enabled on the active interfaces.

Configuring High Availability on NS_VPX_1 and NS_VPX_2

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_1 and 2 configuration utilities logged on as the nsroot user for this task.

1. Configure NS_VPX_1 and 2 to function as a high availability pair. Set NS_VPX_2 (10.0.0.120) as the remote node on NS_VPX_1 and specify both nodes to use the nsroot logon credentials.

There are slightly different settings required on each NetScaler system.

   a. NS_VPX_1 and 2: Expand the **System** node and click **High Availability** in the System pane.
   b. NS_VPX_1 and 2: Click **Add** in the high availability pane.

      The High Availability Setup dialog box opens.
   c. NS_VPX_1: Type `10.0.0.120` in the Remote Node IP Address field, verify that **Configure remote system to participate in High Availability setup** and **Turn off HA Monitor on interfaces/channels that are down** are both selected.
   d. Select **Login credentials for remote system are different from self node**, enter the nsroot credentials, and then click **OK**.

2. Refresh the NetScaler system configurations and verify that NS_VPX_2 is setup as the remote node on NS_VPX_1.
   a. NS_VPX_1 and 2: Click the **Refresh** button in the upper right corner of the Configuration Utility window.
   b. NS_VPX_1: Verify that 10.0.0.120 appears as a remote node.

Testing the High-Availability Configuration

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_1 and 2 configuration utilities logged on as the nsroot user for this task.

1. Verify the current state of the high availability pair.

In this exercise, the system that is configured first is the primary system.

a. NS_VPX_1 and 2: Expand the **Network** node and select **IPs**.

b. NS_VPX_1 and 2: Compare the system-owned IP addresses on both NS_VPX_1 and 2. Notice which system retained its original SNIP address and which system configuration is overwritten by the high-availability configuration.

The system that is configured first will have the primary state (NS_VPX_1).

c. NS_VPX_1 and 2: Expand the **System** node and select **High Availability**.

d. NS_VPX_1 and 2: Click the **Refresh** button in the upper-right corner of the configuration utility.

e. NS_VPX_1 and 2: Verify that the node state on both nodes is **UP**.

- The Master State of NS_VPX_1 is primary.
- The Master State of NS_VPX_2 is secondary.

2. Test the high-availability configuration by forcing a failover on NS_VPX_1.

a. NS_VPX_1: Right-click Node ID **1** and click **Force Failover**. Click **Yes** to confirm the force failover then click **OK** twice.

b. NS_VPX_1 and 2: Click the **Refresh** button in the upper-right corner of the configuration utility.

c. NS_VPX_1 and 2: Verify the master state of both nodes.

- The master state of NS_VPX_1 is now secondary.
- The master state of NS_VPX_2 is now primary.

3. Test the high-availability configuration by forcing a failover on NS_VPX_2.

a. NS_VPX_2: Right-click Node ID **1** and click **Force Failover**. Click **Yes** to confirm the force failover then click **OK** twice.

b. NS_VPX_1 and 2: Click the **Refresh** button in the upper-right corner of the configuration utility.

c. NS_VPX_1 and 2: Verify the master state of both nodes.

- The master state of NS_VPX_1 is primary again.
- The master state of NS_VPX_2 is secondary again.

Removing a High Availability from NS_VPX_1 and NS_VPX_2

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_1 and 2 configuration utilities logged on as the nsroot user for this task.

1. Verify the current high-availability status on NS_VPX_1.

a. NS_VPX_1: Expand the **System** node and select **High Availability**.
b. Verify that the Node 0 master state is Primary, and the node state for both nodes is UP.

If NS_VPX_1 is not listed as the primary node, use the force high-availability failover command to promote NS_VPX_1 as the primary node.

2. Remove the secondary node from the high-availability configuration on NS_VPX_1.
   a. Select Node 1 from the high-availability pane and click **Remove**.
   b. Click **Yes** to confirm the removal of the node.
   c. Click **Save** in the upper-right corner of the configuration utility window.
3. Remove high availability node 1 from NS_VPX_2.
   a. Expand the **System** node and select **High Availability**.
   b. Select Node 1 from the high-availability pane and click **Remove**.
   c. Click **Yes** to confirm the removal of the node.
   d. Click **Save** in the upper-right corner of the configuration utility window.
4. Create a new subnet IP address for NS_VPX_2, and then remove the subnet IP address created during the high availability configuration.
   a. Expand the **Network** node and select **IPs**.
   b. Click Add.
   c. Type `10.0.0.92` in the IP Address field and `255.255.255.0` in the Netmask field.
   d. Leave all other default settings and click **Create** then click **Close**.
   e. Select the **10.0.0.91** IP address and click **Remove**.
   f. Click **Yes** to confirm removal of the subnet IP address.
5. Save the configuration on both NetScalers and then close both Firefox browser windows.
6. In XenCenter, click NS_VPX_1 and then click **Shut Down** in the top toolbar.

   Repeat this step for NS_VPX_2 as well.

Exercise 4-1: Step by Step (Command-Line Interface)

This exercise provides step-by-step instructions for completing "Exercise 4-1: Configuring High Availability" using the command-line interface.

Configuring NS_VPX_1 and NS_VPX_2

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_1 and NS_VPX_2 command-line interfaces logged on as the nsroot user for this task.

1. Prepare NS_VPX_1 and NS_VPX_2 for high availability configuration.

a. Open the command-line interface program (PuTTY) from the Win7Client desktop. Select the **NS_VPX_1** saved session and click **Open**.

b. Open another command-line interface window and select the **NS_VPX_2** saved session and click **Open**.

Be very cognizant of the NetScaler window you are working in at any given time.

c. On both NS_VPX_1 and NS_VPX_2, save the running configuration before proceeding by entering the following command:

```
save ns config
```

d. NS_VPX_1 and NS_VPX_2: Identify critical interfaces by entering the following command:

```
show node
```

The show node command lists high-availability nodes on the current system only. However, it also identifies which critical interfaces are in use.

Notice which interfaces are listed as critical interfaces. Do not disable these interfaces.

e. NS_VPX_1 and NS_VPX_2: View the interfaces on the system by entering the following command:

```
show interface
```

Notice which interfaces are in an UP state versus a DOWN state. Interfaces in an UP state should correspond to the critical interfaces in the previous step.

Configuring High Availability on NS_VPX_1 and NS_VPX_2

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_1 and 2 command-line interfaces logged on as the nsroot user for this task.

1. Configure NS_VPX_1 and NS_VPX_2 as a high-availability pair.

   a. NS_VPX_1: Add NS_VPX_2 as a high-availability node on NS_VPX_1 using the following command:

   ```
   add ha node 1 10.0.0.120
   ```

   b. NS_VPX_1: Sync the high-availability configuration with NS_VPX_2 using the following command:

```
set ha node -haSync ENABLED
```

c. NS_VPX_2: Add NS_VPX_1 as a high-availability node on NS_VPX_2 using the following command:

```
add ha node 1 10.0.0.110
```

d. NS_VPX_1 and 2: View the status of the node and note the Master State of each node using the following command:

```
show ha node
```

The Master State for NS_VPX_1 should show as Primary and NS_VPX_2 should show as Secondary.

e. Save the NetScaler configuration.

```
save ns config
```

Testing the High-Availability Configuration

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_1 and 2 command-line interfaces logged on as the nsroot user for this task.

1. Use the following procedure to test the high-availability configuration:
   a. NS_VPX_1 and 2: Verify the status of the system IP addresses by entering the following command:

```
show ns ip
```

Note which IP addresses are the same and which are different on each system. Also note which subnet IPs of the system are preserved and which subnet IPs of the system are overwritten.

   b. NS_VPX_1 and NS_VPX_2: Verify the status of the nodes by entering the following command:

```
show ha node
```

NS_VPX_1 (10.0.0.110) should be the Primary.

   c. NS_VPX_1: Force a failover by entering the following command:

```
force ha failover
```

```
y
```


d. NS_VPX_1 and NS_VPX_2: View the node status by entering the following command:

```
show ha node
```

NS_VPX_2 becomes Primary.

e. NS_VPX_2: Force a failover by entering the following command:

```
force ha failover
```

```
y
```

f. NS_VPX_1 and NS_VPX_2: View the node status by entering the following command:

```
show ha node
```

NS_VPX_1 is Primary again.

Removing High Availability from NS_VPX_1 and NS_VPX_2

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_1 and 2 command-line interfaces logged on as the nsroot user for this task.

1. NS_VPX_1: Verify the current high availability status.
   a. Verify that the node status is UP and that NS_VPX_1 is the primary node:

```
show ha node
```

If NS_VPX_1 is not listed as the primary node, use the force high availability failover command to promote NS_VPX_1 as the primary node.

2. NS_VPX_1 and NS_VPX_2: Remove the secondary node from the high availability configuration using the following command:

```
rm ha node 1
```

3. NS_VPX_1: Verify the high availability status using the following command:

```
show ha node
```

4. Switch to NS_VPX_2 to verify the high availability status using the following command:

```
show ha node
```

5. Create a new subnet IP address for NS_VPX_2, and then remove the subnet IP address created during the high availability configuration using the following command:

a. NS_VPX_2: Create a new subnet IP address.

```
add ns ip 10.0.0.92 255.255.255.0 -type SNIP
-mgmtAccess ENABLED
```

b. NS_VPX_2: Remove the subnet IP address created while configuring the high availability pair.

```
rm ns ip 10.0.0.91
```

c. NS_VPX_2: View the NetScaler IP addresses to make sure that there is only one SNIP address using the following command:

```
sh nsip
```

6. NS_VPX_1 and 2: Save the NetScaler configuration using the following command:

```
save ns config
```

7. Close the PuTTY sessions for NS_VPX_1 and NS_VPX_2.
8. In XenCenter, click NS_VPX_1 and then click **Shut Down** in the top toolbar.

   Repeat this step for NS_VPX_2 as well.

Module 5

Exercises for Introduction to Policies and Expressions

Exercise 5-1: Creating Policies and Expressions

Overview

This exercise will demonstrate how to create policies and policy expressions that will be used in later exercises.

Exercise Details

To begin this lab, ensure that the following virtual machines are started:

- AD.training.lab
- NS_VPX_0
- Router-Vyatta
- Win7Client

Estimated time to complete this exercise: 15 minutes

Exercise 5-1: Step by Step (Configuration Utility)

This exercise provides step-by-step instructions for completing "Exercise 5-1: Creating Policies and Expressions" using the configuration utility.

Creating Policy Expressions

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Create a policy expression that will respond to requests from iPhone clients.
   a. Expand the **AppExpert** node, expand the **Expressions** sub-node, then select **Advanced Expressions**.
   b. Click **Add** in the Advanced Expressions pane.
      The Create Policy Expression dialog box opens.
   c. Type `iPhone` in the Expression Name field and click **Add** under Expression.
      The Add Expression dialog box opens.
   d. Configure the policy expression using the following settings:
      - HTTP as the protocol
      - REQ as the flow type

- HEADER (String) as the qualifier
- Header name: `User-Agent`
- Contains (String) as the operator
- Pattern string: `iPhone`

e. Click **OK**, click **Create**, then click **Close**.
The iPhone expression is created and the Create Policy Expression dialog box closes

2. Create a policy expression that responds to requests from Internet Explorer 6 clients.
   a. Click **Add** in the Expressions pane.
   The Create Policy Expression dialog box opens.
   b. Type `IE6` in the Expression Name field and click **Add** under Expression.
   The Add Expression dialog box opens.
   c. Configure the policy expression using the following settings:
      - HTTP as the protocol
      - REQ as the flow type
      - HEADER (String) as the qualifier
      - Header name: `User-Agent`
      - Contains (String) as the operator
      - Pattern string: `MSIE 6.0`
   d. Click **OK**, click **Create**, and then click **Close**.
   The IE6 expression is created and the Create Policy Expression dialog box closes.

Creating Content-Switching Policies

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Create a content-switching policy expression for iPhone clients.
   a. Expand the **Content Switching** node and then select **Policies**.
   b. Click **Add** in the Content Switching Policies pane.
   The Create Content Switching Policy dialog box opens.
   c. Type `cs_pol_mobile` in the Name field, then click **Configure**.
   The Create Expression dialog box opens.
   d. Click the arrow to the right of the Add button and select **iPhone** from the drop-down list.
   e. Click **Create**, then click **Create** again.
   This step creates the cs_pol_mobile policy.
   f. Click **Close**.
   The Create Content Switching Policy dialog box closes.

2. Create a content-switching policy expression for Internet Explorer 6 clients.
   a. Click **Add** in the Content Switching Policies pane.
      The Create Content Switching Policy dialog box opens.
   b. Type `cs_pol_legacy` in the Name field, then click **Configure**.
      The Create Expression dialog box opens.
   c. Click the arrow to the right of the Add button and select **IE6** from the drop-down list.
   d. Click **Create**, then click **Create** again.
      This step creates the cs_pol_legacy policy.
   e. Click **Close**.
      The Create Content Switching Policy dialog box closes.
   f. Click **Save** in the upper-right corner of the configuration utility window to save the running configuration.

Exercise 5-1: Step by Step (Command-Line Interface)

This exercise provides step-by-step instructions for completing "Exercise 5-1: Creating Policies and Expressions" using the command-line interface.

Creating Policies and Policy Expressions

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Create a policy expression and content-switching policy to recognize iPhone users by entering the following commands:

```
add policy expression iPhone "REQ.HTTP.HEADER User-
Agent CONTAINS iPhone"
```

```
add cs policy cs_pol_mobile -rule iPhone
```

2. Create a policy expression and content-switching policy to recognize Internet Explorer 6 users by entering the following commands:

```
add policy expression IE6 "REQ.HTTP.HEADER User-
Agent CONTAINS \"MSIE 6.0\""
```

```
add cs policy cs_pol_legacy -rule IE6
```

3. Save the configuration by entering the following command:

```
save ns config
```


Exercise 5-2: Converting a Policy Expression (Optional)

Overview

This exercise demonstrates the nspepi tool and how it converts policy expressions from classic to default syntax.

Before You Begin

To begin this lab, ensure that the following virtual machines are started:

- AD.training.lab
- NS_VPX_0
- Router_Vyatta
- Win7Client

Estimated time to complete this exercise: 10 minutes

The policy expression conversion tool, nspepi, is only available through the command-line interface.

Exercise 5-2: Step by Step (Command-Line Interface)

This exercise provides step-by-step instructions for completing "Exercise 5-2: Converting a Policy Expression."

Converting Classic Expressions to Default Expressions

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Access the command-line interface though PuTTY
   a. From the Win7Client desktop, double click the PuTTY icon.
   b. Select NS_VPX_0 from the saved sessions pane, and click **Open**.
   c. Type `nsroot` then press **Enter**. Type `nsroot` again and press **Enter**.
      User is now logged on to the command-line interface for NS_VPX_0
2. Enter the NetScaler operating system shell.
   a. Type `shell` then press **Enter**.

3. Convert a classic expression to a default expression using the following command:

```
nspepi -e "REQ.HTTP.URL == /*.htm"
```

The nspepi command displays the corresponding default expression.

4. Convert a classic expression to a default expression using the following command:

```
nspepi -e "REQ.HTTP.HEADER User-Agent CONTAINS "MSIE 6.0""
```

View the returned expression from the nspepi tool.

5. Exit the NetScaler shell using the following command:

```
exit
```


Module 6

Exercises for Configuring Content Switching

Exercise 6-1: Configuring Content Switching

Overview

This exercise will demonstrate how to configure content switching on a NetScaler, including creating non-addressable virtual servers, content switching virtual servers, and using the policies and expressions created in the previous module to switch content at the servers.

Before You Begin

To begin this lab, ensure that the following virtual machines are started:

- AD.training.lab
- NS_VPX_0
- Router-Vyatta
- Web_Blue
- Web_Green
- Web_Red
- Win7Client

Estimated time for complete this exercise: 20 minutes

Exercise 6-1: Step by Step (Configuration Utility)

This exercise provides step-by-step instructions for completing "Exercise 6-1: Configuring Content Switching" using the configuration utility.

Verifying Content-Switching Feature Enablement

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Verify enablement of the content-switching feature.
   a. Switch configuration utility for NS_VPX_0 and log on using the nsroot credentials.
   b. Expand the **System** node and select **Settings**.
   c. Click **Configure basic features** in the Settings pane.

      The Configure Basic Features dialog box opens.
   d. Verify that the **Load Balancing** and **Content Switching** features are selected and click **Close**.

      The Configure Basic Features dialog box closes.

Creating Non-Addressable Load-Balancing Virtual Servers

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Create a non-addressable "lb_vsrv_red" load-balancing virtual server for the WebRed web server.
   a. Expand the **Load Balancing** node and select **Virtual Servers**.
   b. Click **Add** in the Load Balancing Virtual Servers pane.
      The Create Virtual Server (Load Balancing) dialog box opens.
   c. Type `lb_vsrv_red` in the Name field, then verify that **HTTP** is selected in the Protocol drop-down list.

This virtual server is dedicated to iPhone users.

   d. Deselect **Directly Addressable** and click **Yes** to confirm the change.
      This action disables the IP address and Port fields. No VIP address is assigned to this load-balancing virtual server.
   e. Check the **Active** field for svc_red on the Services tab and click **Create**.

This step binds the service to the virtual server.

2. Create a non-addressable "lb_vsrv_blue" load-balancing virtual server for the WebBlue web server.
   a. Type `lb_vsrv_blue` in the Name field, then verify that **HTTP** is selected in the Protocol drop-down list.

This virtual server is dedicated for Internet Explorer 6 users.

   b. Deselect the **Active** field for svc_red on the Services tab.
   c. Select the **Active** field for svc_blue on the Services tab and click **Create**.
3. Create a non-addressable "lb_vsrv_green" load-balancing virtual server for the WebGreen web server.
   a. Type `lb_vsrv_green` in the Name field, then verify that **HTTP** is selected in the Protocol drop-down list.

This virtual server is dedicated to default users.

b. Deselect the **Active** field for svc_blue on the Services tab.

c. Select the **Active** field for svc_green on the Services tab and click **Create**.

d. Click **Close**.

The Create Virtual Server (Load Balancing) dialog box closes.

Creating the Content-Switching Virtual Server

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Create a content-switching virtual server called cs_vsrv_rbg with an IP address of 10.0.0.82.
   a. Expand the **Content Switching** node and select **Virtual Servers**.
   b. Click **Add** in the Content Switching Virtual Servers pane.

      The Create Virtual Server (Content Switching) dialog box opens.
   c. Type `cs_vsrv_rbg` in the Name field and then type `10.0.0.82` in the IP Address field.
   d. Verify the Protocol is set to **HTTP** and that the port is set to `80`.
2. Bind the cs_pol_mobile policy to the content-switching virtual server.
   a. Click **Insert Policy** and select **cs_pol_mobile** to bind the mobile policy to the content switching virtual server.
   b. Click the Target cell for **cs_pol_mobile** and select **lb_vsrv_red**.
3. Bind the cs_pol_legacy policy to the content switching virtual server.
   a. Click **Insert Policy** and select **cs_pol_legacy_browser** to bind the legacy policy to the content-switching virtual server.
   b. Click the Target cell for **cs_pol_legacy_browser** and select **lb_vsrv_blue**.
4. Set up the default user policy and bind it to the content switching virtual server.
   a. Click **Insert Policy** and select **(Default)** to bind the default policy to the content switching virtual server.
   b. Click the Target cell for **(Default)** and select **lb_vsrv_green**.
5. Create the virtual server and save the NetScaler configuration.
   a. Click **Create** and then click **Close**.

      This creates the virtual server.
   b. Click **Save** and click **Yes** to verify that you want to save the running configuration.

Testing the Content-Switching Configuration

Use the Win7Client virtual machine logged on as the CitrixAdmin user for this task.

1. Test the configuration and to observe content-switching behavior.

a. Open a new Firefox browser window and browse to `http://10.0.0.82/home.php`.

   The Green server displays for all other users (Firefox, IE 7.0, or any other agent) as the default policy.

b. Change the browser user agent to iPhone by clicking **Tools > Default User Agent > iPhone 3.0** in Firefox, then click the **Refresh** button.

   The Red server displays only to mobile users (iPhone).

c. Change the browser user agent to Internet Explorer 6 by clicking **Tools > iPhone 3.0 > Internet Explorer > Internet Explorer 6** in Firefox, then click the **Refresh** button.

   The Blue server displays only to legacy browser users (MSIE 6.0).

d. Change the browser user agent to the default by clicking **Tools > Internet Explorer 6 > Default Usert Agent**.

Exercise 6-1: Step by Step (Command-Line Interface)

This exercise provides step-by-step instructions for completing "Exercise 6-1: Configuring Content Switching" using the command-line interface.

Configuring Content Switching

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Create a non-addressable load-balancing virtual server for the Red server and bind it to the svc_red service.

   a. Create the load-balancing virtual server using the following command:

   ```
   add lb vserver lb_vsrv_red HTTP
   ```

   b. Bind the service to the load-balancing virtual server using the following command:

   ```
   bind lb vserver lb_vsrv_red svc_red
   ```

   This server will be dedicated to mobile users.

The load-balancing virtual server is being created without assigning a virtual IP address or a port.

2. Create a non-addressable load-balancing virtual server for the Blue server and bind it to the svc_blue service by entering the following commands:

   a. Create the load-balancing virtual server using the following command:

   ```
   add lb vserver lb_vsrv_blue HTTP
   ```


b. Bind the service to the load-balancing virtual server using the following command:

```
bind lb vserver lb_vsrv_blue svc_blue
```

This server will be dedicated to legacy browser users.

3. Create a non-addressable load-balancing virtual server for the Green server and bind it to the svc_green service by entering the following commands:
   a. Create the load-balancing virtual server using the following command:

```
add lb vserver lb_vsrv_green HTTP
```

   b. Bind the service to the load-balancing virtual server using the following command:

```
bind lb vserver lb_vsrv_green svc_green
```

This server will be dedicated to default users.

4. Create a content-switching virtual server and bind the load-balancing virtual servers to the new content-switching virtual server.
   a. Create a content-switching virtual server by entering the following command:

```
add cs vserver cs_vsrv_rbg HTTP 10.0.0.82 80
```

   b. Bind the load-balancing virtual servers and the corresponding policies to the content-switching virtual server by entering the following commands:

```
bind cs vserver cs_vsrv_rbg -lbvserver lb_vsrv_green
```

```
bind cs vserver cs_vsrv_rbg -policyName cs_pol_mobile
-targetLBVserver lb_vsrv_red
```

```
bind cs vserver cs_vsrv_rbg -policyName cs_pol_legacy
-targetLBVserver lb_vsrv_blue
```

   c. Save the configuration by entering the following command:

```
save ns config
```

Testing the Content-Switching Configuration

Use the Win7Client virtual machine logged on as the CitrixAdmin user for this task.

1. Test the configuration and to observe content-switching behavior.
   a. Open a new Firefox browser window and browse to `http://10.0.0.82/home.php`.

The Green server displays for all other users (Firefox, IE 7.0, or any other agent) as the default policy.

b. Change the browser user agent to iPhone by clicking **Tools > Default User Agent > iPhone 3.0** in Firefox, then click the **Refresh** button.

   The Red server displays only to mobile users (iPhone).

c. Change the browser user agent to Internet Explorer 6 by clicking **Tools > iPhone 3.0 > Internet Explorer > Internet Explorer 6** in Firefox, then click the **Refresh** button.

   The Blue server displays only to legacy browser users (MSIE 6.0).

d. Change the browser user agent to the default by clicking **Tools > Internet Explorer 6 > Default Usert Agent**.

Module 7

Exercises for Connection Tuning

Exercise 7-1: Configuring the NetScaler in the Network

Overview

This exercise will demonstrate how to configure the NetScaler's network interfaces and IP addresses, and manage DNS entries.

Before You Begin

To begin this lab, ensure that the following virtual machines are started:

- AD.training.lab
- NS_VPX_0
- Router_Vyatta
- Win7Client

Information required for this lab:

System	Username	Password
NetScaler	nsroot	nsroot
Windows 7	CitrixAdmin	Password1

Estimated time to complete this exercise: 10 minutes

Exercise 7-1: Step by Step (Configuration Utility)

This section provides step-by-step instructions for completing "Exercise 7-1: Configuring the NetScaler in the Network" using the configuration utility.

Identifying the NetScaler Product Type

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Log on to the NetScaler configuration utility.
   a. Launch the Mozilla Firefox browser and browse to the NetScaler IP address at `http://10.0.0.100`.

b. Log on to the configuration utility using the nsroot credentials.

Close the Configuration wizard if it opens.

2. Identify the NetScaler product type.
   a. Click the **Configuration** tab.
   b. Click the **System** node.
   c. Note the Platform information in the Hardware Information section.

   In this example, the NetScaler Platform is NetScaler Virtual Appliance 450000.

Creating a DNS Record

Use the AD.training.lab virtual machine logged on as the CitrixAdmin user for this task.

1. Log on as the CitrixAdmin user to the AD.training.lab virtual machine from the XenCenter console.
   a. Switch to XenCenter and select the AD.training.lab virtual machine.
   b. Click the **Console** tab.
   c. Log on to the Windows Server using the CitrixAdmin credentials.
2. Start the DNS Manager and begin creating a new host for rbg.training.lab.
   a. Double-click the **DNS** icon on the Desktop to launch the DNS Manager.
   b. Navigate to **AD** > **Forward Lookup Zones** > **training.lab**.
   c. Right-click **training.lab** and select **New Host (A or AAAA)**.

      The New Host window appears.
3. Create an "rbg" DNS record using 10.0.0.80 as the host IP address.
   a. Type `rbg` in the Name field.
   b. Type 10.0.0.80 in the IP Address field.
   c. Click **Add Host**.
   d. Click **OK** in the confirmation window, then click **Done**.

      A DNS record is now created for rbg.training.lab. You will use this hostname in a later exercise.

Exercise 7-1: Step by Step (Command-line Interface)

This section provides step by step instructions for completing "Exercise 7-1: Configuring the NetScaler in the Network" using the command-line interface.

Identifying the NetScaler Product Type

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Log on to the NetScaler command line interface.
   a. Switch to the Win7Client virtual machine on the XenCenter console and log on using the CitrixAdmin credentials.
   b. Launch a PuTTY session and open the NS_VPX_0 saved session.
   c. Log on to the NS_VPX_0 command-line interface using the nsroot credentials.
2. Identify the NetScaler product type.
   a. Access the BSD shell using the following command:

      ```
      shell
      ```

   b. Display the NetScaler system information using the following command:

      ```
      sysctl -a | grep netscaler
      ```

      The results will be similar to the following information:

      ```
      debug.netscaler_panic: ˚Aÿ
      netscaler.developer: 0
      netscaler.recovery: 0
      netscaler.sysid: 450000
      netscaler.serial: 98310000cb254307ee78
      netscaler.descr: NetScaler Virtual Appliance 3G
      netscaler.pitbossexitcode: -559039810
      ```

      In this example, the netscaler.descr identifies the NetScaler platform, which is a VPX appliance.

   c. Exit the BSD shell using the following command:

      ```
      exit
      ```

Creating a DNS Record

Use the AD.training.lab virtual machine logged on as the CitrixAdmin user for this task.

1. Log on as the CitrixAdmin user to the AD.training.lab virtual machine from the XenCenter console.
   a. Switch to XenCenter and select the AD.training.lab virtual machine.
   b. Click the **Console** tab.

c. Log on to the Windows Server using the CitrixAdmin credentials.

2. Start the DNS Manager and begin creating a new host for rbg.training.lab.
   a. Double-click the **DNS** icon on the Desktop to launch the DNS Manager.
   b. Navigate to **AD > Forward Lookup Zones > training.lab**.
   c. Right-click **training.lab** and select **New Host (A or AAAA)**.

      The New Host window appears.
3. Create an "rbg" DNS record using 10.0.0.80 as the host IP address.
   a. Type `rbg` in the Name field.
   b. Type 10.0.0.80 in the IP Address field.
   c. Click **Add Host**.
   d. Click **OK** in the confirmation window, then click **Done**.

      A DNS record is now created for rbg.training.lab. You will use this hostname in a later exercise.

Exercise 7-2: Configuring a Load-Balancing HTTP-ECV Monitor

Overview

This exercise will demonstrate how to monitor the status of a specific HTTP service bound to a load-balancing virtual server.

Before You Begin

To begin this lab, ensure that the following virtual machines are started:

- AD.training.lab
- NS_VPX_0
- Router_Vyatta
- Win7Client
- WebBlue
- WebGreen
- WebRed

Estimated time to complete this lab: 20 minutes

Exercise 7-2: Step by Step (Configuration Utility)

This section provides step-by-step instructions for completing "Exercise 7-2: Configuring a Load-Balancing HTTP-ECV Monitor" using the configuration utility.

Creating a Load-Balancing HTTP-ECV Monitor

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Switch to the NS_VPX_0 configuration utility on the Win7Client virtual machine.
2. Create a load-balancing HTTP-ECV monitor named "mon_RBG_HTTPECV." Configure the monitor to use a send string of "GET /home.php" and a receive string of "serverinfo".
   a. Navigate to **Load Balancing** > **Monitors**.
   b. Click **Add**.
   c. Type the following information in the Configure Monitor window and leave other values in their default state.

- Name: `mon_RBG_HTTPECV`
- Type: `HTTP-ECV`
- Interval: `5 Seconds`
- Down Time: `5 Seconds`

d. Click the Special Parameters tab and type the following values in the specified fields:
   - Send String: `GET /home.php`
   - Receive String: `serverinfo`

e. Click **Create** and then click **Close**.

The Receive String parameter is a string value and should be set to a string or phrase which appears on the web site in the first 24 KB of the response. For this exercise, you specify "serverinfo". Other valid strings include "Viewing this page" and "this page indicates."

String matches are case sensitive.

3. Bind the load-balancing HTTP-ECV monitor to the service svc_red.
   a. Navigate to **Load Balancing** > **Services**.
   b. Select the **svc_red** service and click **Open**.
   c. Select the **mon_RBG_HTTPECV** monitor from the Available list and click **Add**.
   d. Click **OK**.

Testing the Load-Balancing HTTP-ECV Monitor

Use the Win7Client virtual machine logged on as the CitrixAdmin user for this task.

1. Open a new Firefox window and browse to `http://rbg.training.lab/home.php`. Refresh the page several times.

The page load balances between the RED, BLUE, and GREEN servers while the monitor status shows as UP.

2. Ensure that the monitor status for the mon_RBG_HTTPECV monitor is green.
   a. Switch to the configuration utility for NS_VPX_0.
   b. Navigate to **Load Balancing** > **Monitors**.
   c. Verify that the mon_RBG_HTTPECV monitor status is green.
3. Ensure that the red service for the mon_RBG_HTTPECV monitor is successfully responding.
   a. Navigate to **Load Balancing** > **Services**.
   b. Select the **svc_red** service and click **Open**.
   c. Note the information for the configured monitor.

The monitor details display the response status "Success - Pattern found in response."

d. Click **Close**.

4. Change the monitor string to use the invalid string "bad string".
   a. Navigate to **Load Balancing > Monitors**.
   b. Select the **mon_RBG_HTTPECV** monitor and click **Open**.
   c. Click the **Special Parameters** tab.
   d. Change the Receive String field to "`bad string`".

      For this step, set the Receive string (-recv) to a string not found on the page; this creates a failed status. Any string not found on the page could be used.

   e. Click **OK**.
5. Clear the cache before the next test to avoid issues with the browser caching the server response. Close additional instances if more than one browser window is open.
   a. Open a new Firefox instance, not just a new tab.
   b. Click **Tools > Clear Recent History**.
   c. Click **OK** in the popup window.
6. Browse to `http://rbg.training.lab/home.php`. Refresh the page several times.

The red server home.php page will not load while the monitor reports the service as DOWN.

7. Ensure that the monitor status for the mon_RBG_HTTPECV monitor is green.
   a. Switch to the configuration utility for NS_VPX_0.
   b. Navigate to **Load Balancing > Monitors**.
   c. Verify that the mon_RBG_HTTPECV monitor status is green.
8. Ensure that the red service for the mon_RBG_HTTPECV monitor is no longer responding.
   a. Navigate to **Load Balancing > Services**.
   b. Select the **svc_red** service and click **Open**.
   c. Note the information for the configured monitor.

      The service state shows as DOWN and the monitor response shows "Failure - Pattern not found in response."
9. Remove the mon_RBG_HTTPECV monitor from the load balancing virtual server.
   a. Select the **mon_RBG_HTTPECV** monitor from the Configured list and click **Remove**.
   b. Click **OK**.
   c. Click **Refresh**.

      The svc_red service State should now show as UP.

Exercise 7-2: Step by Step (Command-line Interface)

This section provides step by step instructions for completing "Exercise 7-2: Configuring a Load-Balancing HTTP-ECV Monitor" using the command-line interface.

Creating a Load-Balancing HTTP-ECV Monitor

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Switch to the command-line interface on NS_VPX_0.
2. Create a load-balancing HTTP-ECV monitor named "mon_RBG_HTTPECV". Configure the monitor to use a send string of "GET /home.php" and a receive string of "serverinfo" using the following command:

   ```
   add lb monitor mon_RBG_HTTPECV HTTP-ECV -send "GET /home.php"
   -recv "serverinfo" -interval 5 SEC -downTime 5 SEC
   ```

   The Receive parameter (-recv) uses a string value and should be set to a string or phrase which appears on the website in the first 24 KB of the response. For this exercise, specify "serverinfo". Other valid strings include "Viewing this page" and "This page indicates".

   String matches are case sensitive.

3. Bind the load-balancing HTTP-ECV monitor to the svc_red service using the following command:

   ```
   bind service svc_red -monitorName mon_RBG_HTTPECV
   ```

Testing the Load-Balancing HTTP-ECV Monitor

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Open a new Firefox window and browse to `http://rbg.training.lab/home.php`. Refresh the page several times.

The page load-balances between the RED, BLUE, and GREEN servers while the monitor status is UP.

2. Switch to the command-line interface for NS_VPX_0 and ensure that the monitor status for the mon_RBG_HTTPECV monitor is UP using the following command:

   ```
   show lb monitor mon_RBG_HTTPECV
   ```


3. Ensure that the red service for the mon_RBG_HTTPECV monitor is successfully responding using the following command:

```
show service svc_red
```

The monitor details display the response status "Success - Pattern found in response".

4. Change the monitor string to the invalid string "bad string" using the following command:

```
set lb monitor mon_RBG_HTTPECV HTTP-ECV -recv "bad string"
```

For this step, set the Receive parameter (-recv) to a string not found on the page; this creates a failed status. Any string not found on the page could be used.

5. Clear the cache before the next test to avoid issues with the browser caching the server response. Close additional instances if more than one browser window is open.
   a. Open a new Firefox instance, not just a new tab.
   b. Click **Tools > Clear Recent History** .
   c. Click **OK** in the popup window.
6. Browse to `http://rbg.training.lab/home.php`. Refresh the page several times.

The RED server home.php page will not load while the monitor reports the service as DOWN.

7. Ensure that the monitor status for the mon_RBG_HTTPECV monitor is UP using the following command:

```
show lb monitor mon_RBG_HTTPECV
```

8. Ensure that the red service for the mon_RBG_HTTPECV monitor is successfully responding using the following command:

```
show service svc_red
```

The state shows as DOWN.

9. Unbind the mon_RBG_HTTPECV monitor from the scv_red service using the following command:

```
unbind service svc_red -monitorName mon_RBG_HTTPECV
```

10. Verify svc_red is now bound to the tcp-default monitor using the following command:

```
sh service svc_red
```


Module 8

Exercises for Global Server Load Balancing

Exercise 8-1: Configuring Global Server Load-Balancing (GSLB)

Overview

This exercise wll demonstrate how to configure two NetScaler systems located in different locations for global server load balancing (GSLB).

You must begin configuring the GSLB pair by setting up the first NetScaler at the Frankfurt site.

Before You Begin

To begin this lab, ensure that the following virtual machines are started:

- AD.training.lab
- NS_VPX_1
- NS_VPX_2
- Router_Vyatta
- Web_Blue
- Web_Green
- Web_Red
- Win7Client
- Win7Ext_Site1

Information required for this lab:

Variable	Frankfurt	Tokyo
NSIP	10.0.0.110	10.0.0.120
SNIP (Site IP)	10.0.0.93	10.0.0.94
VIP1	10.0.0.66	10.0.0.76
VIP2	10.0.0.68	10.0.0.78
Name Server	10.0.0.87	

Estimated time to complete this lab: 50 minutes

Exercise 8-1: Step by Step (Configuration Utility)

This section provides step-by-step instructions for completing "Exercise 8-1: Configuring Global Server Load Balancing" using the configuration utility.

Enabling Global Server Load Balancing on the Frankfurt NetScaler

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_1 configuration utility logged on as the nsroot user for this task.

1. Switch to the Win7client virtual machine.
2. Enable the GSLB feature on the NS_VPX_1 (Frankfurt) system.
   a. Open a browser connection to http://10.0.0.110 (Frankfurt).
   b. Navigate to **System** > **Settings**.
   c. Click **Configure advanced features**.
   d. Select **Global Server Load Balancing** and click **OK**.

Adding a Subnet IP Address to the Frankfurt NetScaler

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_1 configuration utility logged on as the nsroot user for this task.

1. Add a SNIP to the Frankfurt NetScaler with a 10.0.0.93 IP address and a 255.255.255.0 netmask.
   a. Navigate to **Network** > **IPs** and click **Add**.
   b. Type `10.0.0.93` in the IP Address field and `255.255.255.0` in the Netmask field.
   c. Select **Subnet IP** from the IP Type menu.
   d. Click **Create** and then click **Close**.
2. Save the running NetScaler configuration.
   a. Click **Save**.
   b. Click **Yes** to confirm and click **OK** once the configuration is successfully saved.

Adding a Load-Balancing Virtual Server to the Frankfurt NetScaler

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_1 configuration utility logged on as the nsroot user for this task.

1. Verify that the status of the svc_red and svc_green services show as UP.
   a. Navigate to **Load Balancing** > **Services**.
   b. Note the status of the svc_red and svc_green services.

2. Begin configuration of a "lb_vsrv_FRK" HTTP load-balancing virtual server using a 10.0.0.66 IP address. Bind the svc_green service to the lb_vsrv_FRK virtual server.
   a. Navigate to **Load Balancing > Virtual Servers** and click **Add**.
   b. Type `lb_vsrv_FRK` in the Name field and `10.0.0.66` in the IP Address field.
   c. Select **HTTP** from the Protocol drop-down menu and type `80` in the Port field.
   d. Select **svc_green** as an active service.
3. Complete the configuration by setting the lb_vsrv_FRK virtual server for round-robin load balancing. Create the new load-balancing virtual server.
   a. Click the **Method and Persistence** tab.
   b. Select **Round Robin** for the LB Method.
   c. Click **Create** and then click **Close**.
4. Test the load-balancing virtual server configuration by browsing to the http://10.0.0.66/remote.php site.

Configuring the GSLB Sites on the Frankfurt NetScaler

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_1 configuration utility logged on as the nsroot user for this task.

1. Add a "site_FRK" (10.0.0.93) GSLB site to the Frankfurt NetScaler.
   a. Navigate to **GSLB > Sites** and click **Add**.
   b. Type `site_FRK` in the Name field and `10.0.0.93` in the Site IP Address field.
   c. Click **Create**.
2. Add a "site_TOK" (10.0.0.94) GSLB site to the Frankfurt NetScaler.

The site_TOK Site Metric MEP Status will show as Down until the site_TOK is configured on a remote GSLB site.

   a. Type `site_TOK` in the Name field and `10.0.0.94` in the Site IP Address field.
   b. Click **Create** and then click **Close**.

Creating the Load-Balancing Servers on the Frankfurt NetScaler

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_1 configuration utility logged on as the nsroot user for this task.

1. Create a "srv_FRK" server with a 10.0.0.66 IP address on the Frankfurt NetScaler.
   a. Navigate to **Load Balancing > Servers** and click **Add**.
   b. Type `srv_FRK` in the Server Name field and `10.0.0.66` in the IP Address field.
   c. Click **Create**.

2. Create a "srv_TOK" server with a 10.0.0.76 IP address on the Frankfurt NetScaler.
   a. Type `srv_TOK` in the Server Name field and `10.0.0.76` in the IP Address field.
   b. Click **Create** and then click **Close**.

Configuring GSLB Services on the Frankfurt NetScaler

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_1 configuration utility logged on as the nsroot user for this task.

1. Create a "gslb_svc_FRK" GSLB service on the Frankfurt NetScaler. Configure the service to communicate over HTTP on port 80.
   a. Navigate to **GSLB > Services** and click **Add**.
   b. Type `gslb_svc_FRK` in the Service Name field, select **site_FRK** from the Site Name drop-down menu, and select **srv_FRK** from the Server Name drop-down menu.
   c. Select **HTTP** as the Service Type and type `80` in the Port field.
   d. Click **Create**.
2. Create a "gslb_svc_TOK" GSLB service on the Frankfurt NetScaler. Configure the service to communicate over HTTP on port 80.
   a. Type `gslb_svc_TOK` in the Service Name field, select **site_TOK** from the Site Name drop-down menu, and select **srv_TOK** from the Server Name drop-down menu.
   b. Select **HTTP** as the Service Type and type `80` in the Port field.
   c. Click **Create** and then click **Close**.
3. Verify that the state for gslb_svc_FRK service shows as UP.

The gslb_svc_TOK service will show as DOWN until the remote GSLB service is configured.

Adding and Binding the GSLB Virtual Server to the Frankfurt NetScaler

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_1 configuration utility logged on as the nsroot user for this task.

1. Begin configuration of a "GSLB_vsrv_global" HTTP GSLB virtual server on the Frankfurt NetScaler. Bind the new virtual server to the gslb_svc_FRK and gslb_svc_TOK GSLB services.
   a. Navigate to **GSLB > Virtual Servers** and click **Add**.
   b. Type `GSLB_vsrv_global` in the Name field and select **HTTP** from the Service Type drop-down menu.
   c. Select both **gslb_svc_FRK** and **gslb_svc_TOK** services.

2. Complete the configuration by setting the GSLB_vsrv_global virtual server for round-robin load balancing. Create the new GSLB virtual server.
   a. Click the **Method and Persistence** tab and select **Round Robin** for the Method.
   b. Click **Create** and then click **Close**.
3. Verify that the GSLB_vsrv_global virtual server shows as UP after creating it.

The health for the GSLB_vsrv_global virtual server will show as 50 percent until an additional NetScaler system is configured.

Exercise 8-1: Step by Step (Command-line Interface)

This section provides step-by-step instructions for completing "Exercise 8-1: Configuring Global Server Load Balancing" using the command-line interface.

Enabling Global Server Load Balancing on the Frankfurt NetScaler

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_1 command-line interface logged on as the nsroot user for this task.

1. Log on to the Frankfurt NetScaler (NS_VPX_1) command-line interface using the nsroot credentials.
2. Enable the GSLB feature using the following command:

```
enable ns feature GSLB
```

Adding a Subnet IP Address to the Frankfurt NetScaler

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_1 command-line interface logged on as the nsroot user for this task.

1. Add 10.0.0.93 as the SNIP for the Frankfurt site using the following command:

```
add ns ip 10.0.0.93 255.255.255.0 -type SNIP
```

2. Save the running configuration using the following command:

```
save ns config
```

Adding a Load-Balancing Virtual Server to the Frankfurt NetScaler

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_1 command-line interface logged on as the nsroot user for this task.

1. Verify that the status of the svc_red and svc_green services show as UP.
   a. Verify that the svc_red service is UP using the following command:

      ```
      show service svc_red
      ```

   b. Verify that the svc_green service is UP using the following command:

      ```
      show service svc_green
      ```

2. Add the "lb_vsrv_FRK" (10.0.0.66) load balancing virtual server to the Frankfurt NetScaler and bind the svc_green service to the new virtual server.
   a. Add a new virtual server to the Frankfurt NetScaler using the following command:

      ```
      add lb vserver lb_vsrv_FRK HTTP 10.0.0.66 80
      -lbMethod ROUNDROBIN
      ```

   b. Bind the svc_green service to the lb_vsrv_FRK virtual server using the following command:

      ```
      bind lb vserver lb_vsrv_FRK svc_green
      ```

3. Browse to http://10.0.0.66/remote.php to test the load-balancing virtual server configuration. The GREEN page should load for the Frankfurt virtual server.

Configuring the GSLB Sites on the Frankfurt NetScaler

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_1 command-line interface logged on as the nsroot user for this task.

1. Add the "site_FRK" and "site_TOK" GSLB sites to the Frankfurt NetScaler.
   a. Add the Frankfurt GSLB site using the following command.

      ```
      add gslb site site_FRK 10.0.0.93
      ```

   b. Add the Tokyo GSLB site using the following command.

      ```
      add gslb site site_TOK 10.0.0.94
      ```

2. Display the NetScaler IP address using the following command:


```
show ns ip
```

3. Display the GSLB site using the following command:

```
show gslb site
```

Configuring GSLB Services on the Frankfurt NetScaler

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_1 command-line interface logged on as the nsroot user for this task.

1. Add the gslb_svc_FRK service to the Frankfurt NetScaler using the following command:

```
add gslb service gslb_svc_FRK 10.0.0.86 HTTP 80
-siteName site_FRK
```

This command will create a server object for Frankfurt VIP 1.

2. Add the gslb_svc_TOK service using the following command:

```
add gslb service gslb_svc_TOK 10.0.0.88 HTTP 80
-siteName site_TOK
```

This command will create a server object for Tokyo VIP 1.

3. Display the GSLB site using the following commands:

```
show gslb site
```

```
show gslb site site_FRK
```

```
show gslb site site_TOK
```

Verify that the correct service is bound to each site.

Adding and Binding the GSLB Virtual Server to the Frankfurt NetScaler

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_1 command-line interface logged on as the nsroot user for this task.

1. Add the GSLB virtual server GSLB_vsrv_global of type HTTP using round robin for the load-balancing method using the following command:

```
add gslb vserver GSLB_vsrv_global HTTP -lbMethod ROUNDROBIN
```

The LB method is being set to Round Robin for purposes of the lab demonstration only. A production implementation of GSLB would not be based on round robin.

2. Bind the Frankfurt and Tokyo GSLB services to the GSLB virtual server.
   a. Bind the Frankfurt GSLB service to the GSLB virtual server using the following command.

```
bind gslb vserver GSLB_vsrv_global -service gslb_svc_FRK
```

   b. Bind the Tokyo GSLB service to the GSLB virtual server using the following command.

```
bind gslb vserver GSLB_vsrv_global -service gslb_svc_TOK
```

3. Display the GSLB virtual server using the following command:

```
show gslb vserver
```

   Verify that the GSLB virtual server State shows as UP.

4. Display the GSLB virtual server GSLB_vsrv_global by entering the following command:

```
show gslb vserver GSLB_vsrv_global
```


Exercise 8-2: Configuring Additional NetScaler Systems for Global Server Load Balancing (GSLB)

Overview

This exercise will demonstrate how to configure GSLB on the second NetScaler. at the Tokyo site.

Before You Begin

To begin this lab, ensure that the following virtual machines are started:

- AD.training.lab
- NS_VPX_1
- NS_VPX_2
- Router_Vyatta
- Web_Blue
- Web_Green
- Web_Red
- Win7Client
- Win7Ext_Site1

Information required for this lab:

Variable	Frankfurt	Tokyo
NSIP	10.0.0.110	10.0.0.120
SNIP (Site IP)	10.0.0.93	10.0.0.94
VIP1	10.0.0.66	10.0.0.76
VIP2	10.0.0.68	10.0.0.78
Name Server	10.0.0.87	

Estimated time to complete this lab: 50 minutes

Exercise 8-2: Step by Step (Configuration Utility)

This section provides step-by-step instructions for completing "Exercise 8-2: Configuring Additional NetScaler Systems for Global Server Load Balancing" using the configuration utility.

Enable Global Server Load Balancing on the Tokyo NetScaler

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_2 configuration utility logged on as the nsroot user for this task.

1. Open a browser connection to http://10.0.0.110 (Tokyo).
2. Enable the GSLB feature on the NS_VPX_2 (Tokyo) system.
   a. Navigate to **System** > **Settings**.
   b. Click **Configure advanced features**.
   c. Select **Global Server Load Balancing** and click **OK**.

Adding a Subnet IP Address to the Tokyo NetScaler

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_2 configuration utility logged on as the nsroot user for this task.

1. Add a SNIP to the Tokyo NetScaler with a 10.0.0.94 IP address and a 255.255.255.0 netmask.
   a. Navigate to **Network** > **IPs** and click **Add**.
   b. Type `10.0.0.94` in the IP Address field and `255.255.255.0` in the Netmask field.
   c. Select **Subnet IP** from the IP Type menu.
   d. Click **Create** and then click **Close**.
2. Save the running NetScaler configuration.
   a. Click **Save**.
   b. Click **Yes** to confirm and click **OK** once the configuration is successfully saved.

Adding a Load-Balancing Virtual Server to the Tokyo NetScaler

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_2 configuration utility logged on as the nsroot user for this task.

1. Verify that the status of the svc_red and svc_green services show as UP.
   a. Navigate to **Load Balancing** > **Services**.
   b. Note the status of the svc_red and svc_green services.
2. Begin configuration of a "lb_vsrv_TOK" HTTP load-balancing virtual server using a 10.0.0.76 IP address. Bind the svc_red service to the lb_vsrv_TOK virtual server.
   a. Navigate to **Load Balancing** > **Virtual Servers** and click **Add**.

b. Type `lb_vsrv_TOK` in the Name field and `10.0.0.76` in the IP Address field.
c. Select **HTTP** from the Protocol drop-down menu and type `80` in the Port field.
d. Select **svc_red** as an active service.

3. Complete the configuration by setting the lb_vsrv_TOK virtual server for round-robin load balancing. Create the new load-balancing virtual server.
   a. Click the **Method and Persistence** tab.
   b. Select **Round Robin** for the LB Method.
   c. Click **Create** and then click **Close**.
4. Test the load-balancing virtual server configuration by browsing to the http://10.0.0.76/remote.php site.

Configuring the GSLB Sites on the Tokyo NetScaler

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_2 configuration utility logged on as the nsroot user for this task.

1. Add a "site_FRK" (10.0.0.93) GSLB site to the Frankfurt NetScaler.
   a. Navigate to **GSLB > Sites** and click **Add**.
   b. Type `site_FRK` in the Name field and `10.0.0.93` in the Site IP Address field.
   c. Click **Create**.
2. Add a "site_TOK" (10.0.0.94) GSLB site to the Frankfurt NetScaler.

You may need to refresh the view for the Site Metric MEP Status to show as Active.

   a. Type `site_TOK` in the Name field and `10.0.0.94` in the Site IP Address field.
   b. Click **Create** and then click **Close**.

Creating the Load-Balancing Servers on the Tokyo NetScaler

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_2 configuration utility logged on as the nsroot user for this task.

1. Create a "srv_FRK" server with a 10.0.0.66 IP address on the Tokyo NetScaler.
   a. Navigate to **Load Balancing > Servers** and click **Add**.
   b. Type `srv_FRK` in the Server Name field and `10.0.0.66` in the IP Address field.
   c. Click **Create**.
2. Create a "srv_TOK" server with a 10.0.0.76 IP address on the Tokyo NetScaler.
   a. Type `srv_TOK` in the Server Name field and `10.0.0.76` in the IP Address field.

b. Click **Create** and then click **Close**.

Configuring GSLB Services on the Tokyo NetScaler

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_2 configuration utility logged on as the nsroot user for this task.

1. Create a "gslb_svc_FRK" GSLB service on the Tokyo NetScaler. Configure the service to communicate over HTTP on port 80.
   a. Navigate to **GSLB > Services** and click **Add**.
   b. Type `gslb_svc_FRK` in the Service Name field, select **site_FRK** from the Site Name drop-down menu, and select **srv_FRK** from the Server Name drop-down menu.
   c. Select **HTTP** as the Service Type and type `80` in the Port field.
   d. Click **Create**.
2. Create a "gslb_svc_TOK" GSLB service on the Tokyo NetScaler. Configure the service to communicate over HTTP on port 80.
   a. Type `gslb_svc_TOK` in the Service Name field, select **site_TOK** from the Site Name drop-down menu, and select **srv_TOK** from the Server Name drop-down menu.
   b. Select **HTTP** as the Service Type and type `80` in the Port field.
   c. Click **Create** and then click **Close**.
3. Verify that the State for both services shows as UP.

Adding and Binding the GSLB Virtual Server to the Tokyo NetScaler

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_2 configuration utility logged on as the nsroot user for this task.

1. Begin configuration of a "GSLB_vsrv_global" HTTP GSLB virtual server on the Tokyo NetScaler. Bind the new virtual server to the gslb_svc_FRK and gslb_svc_TOK GSLB services.
   a. Navigate to **GSLB > Virtual Servers** and click **Add**.
   b. Type `GSLB_vsrv_global` in the Name field and select **HTTP** from the Service Type drop-down menu.
   c. Select both **gslb_svc_FRK** and **gslb_svc_TOK** services.
2. Complete the configuration by setting the GSLB_vsrv_global virtual server for round-robin load balancing. Create the new GSLB virtual server.
   a. Click the **Method and Persistence** tab and select **Round Robin** for the Method.
   b. Click **Create** and then click **Close**.
3. Verify that the GSLB_vsrv_global virtual server shows as UP after creating it.

Exercise 8-2: Step by Step (Command-line Interface)

This section provides step-by-step instructions for completing "Exercise 8-2: Configuring Additional NetScaler Systems for Global Server Load Balancing" using the command-line interface.

Enabling Global Server Load Balancing on the Tokyo NetScaler

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_2 command-line interface logged on as the nsroot user for this task.

1. Log on to the Tokyo NetScaler (NS_VPX_2) command-line interface using the nsroot credentials.
2. Enable the GSLB feature using the following command:

```
enable ns feature gslb
```

Adding a Subnet IP Address to the Tokyo NetScaler

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_2 command-line interface logged on as the nsroot user for this task.

1. Add 10.0.0.94 as the SNIP for the Frankfurt site using the following command:

```
add ns ip 10.0.0.94 255.255.255.0 -type SNIP
```

2. Save the running configuration on using the following command:

```
save ns config
```

Adding a Load-Balancing Virtual Server to the Tokyo NetScaler

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_2 command-line interface logged on as the nsroot user for this task.

1. Verify that the status of the svc_red and svc_green services show as UP.
   a. Verify that the svc_red service is UP using the following command:

```
show service svc_red
```

   b. Verify that the svc_green service is UP using the following command:

```
show service svc_green
```

2. Add the "lb_vsrv_TOK" (10.0.0.76) load-balancing virtual server to the Tokyo NetScaler and bind the svc_red service to the new virtual server.
   a. Add a new virtual server to the Tokyo NetScaler using the following command:

```
add lb vserver lb_vsrv_TOK HTTP 10.0.0.76 80
-lbMethod ROUNDROBIN
```

   b. Bind the svc_red service to the lb_vsrv_TOK virtual server using the following command:

```
bind lb vserver lb_vsrv_TOK svc_red
```

3. Open the Firefox browser and browse to `http://10.0.0.76/remote.php` to test the load-balancing virtual server configuration.
   The RED page should load for the Tokyo virtual server.

Configuring the GSLB Sites on the Tokyo NetScaler

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_2 command-line interface logged on as the nsroot user for this task.

1. Add the "site_FRK" and "site_TOK" GSLB sites to the Tokyo NetScaler.
   a. Add the Frankfurt GSLB site using the following command.

```
add gslb site site_FRK 10.0.0.93
```

   b. Add the Tokyo GSLB site using the following command.

```
add gslb site site_TOK 10.0.0.94
```

2. Display the NetScaler IP address using the following command:

```
show ns ip
```

3. Display the GSLB site using the following command:

```
show gslb site
```

Configuring GSLB Services on the Tokyo NetScaler

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_2 command-line interface logged on as the nsroot user for this task.

1. Add the gslb_svc_FRK service to the Tokyo NetScaler using the following command:


```
add gslb service gslb_svc_FRK 10.0.0.86 HTTP 80
-siteName site_FRK
```

This command will create a server object for Frankfurt VIP 1.

2. Add the gslb_svc_TOK service using the following command:

```
add gslb service gslb_svc_TOK 10.0.0.88 HTTP 80
-siteName site_TOK
```

This command will create a server object for Tokyo VIP 1.

3. Display the GSLB site using the following commands:

```
show gslb site
```

```
show gslb site site_FRK
```

```
show gslb site site_TOK
```

Verify that the correct service is bound to each site.

Adding and Binding the GSLB Virtual Server to the Tokyo NetScaler

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_2 command-line interface logged on as the nsroot user for this task.

1. Add the GSLB virtual server GSLB_vsrv_global of type HTTP using round robin for the load-balancing method using the following command:

```
add gslb vserver GSLB_vsrv_global HTTP -lbMethod ROUNDROBIN
```

The LB method is being set to Round Robin for purposes of the lab demonstration only. A production implementation of GSLB would not be based on round robin.

2. Bind the Frankfurt and Tokyo GSLB services to the GSLB virtual server.
   a. Bind the Frankfurt GSLB service to the GSLB virtual server using the following command.

```
bind gslb vserver GSLB_vsrv_global -service gslb_svc_FRK
```

b. Bind the Tokyo GSLB service to the GSLB virtual server using the following command.

```
bind gslb vserver GSLB_vsrv_global -service gslb_svc_TOK
```

3. Display the GSLB virtual server using the following command:

```
show gslb vserver
```

Verify that the GSLB virtual server State shows as UP.

4. Display the GSLB virtual server GSLB_vsrv_global by entering the following command:

```
show gslb vserver GSLB_vsrv_global
```


Exercise 8-3: Configuring DNS to Test a Global Server Load-Balancing (GSLB) Configuration

Overview

This exercise will demonstrate how to test the GSLB configuration using DNS.

Before You Begin

To begin this lab, ensure that the following virtual machines are started:

- AD.training.lab
- NS_VPX_1
- NS_VPX_2
- Router_Vyatta
- Web_Blue
- Web_Green
- Web_Red
- Win7Client
- Win7Ext_Site1

Information required for this lab:

Variable	Frankfurt	Tokyo
NSIP	10.0.0.110	10.0.0.120
SNIP (Site IP)	10.0.0.93	10.0.0.94
VIP1	10.0.0.66	10.0.0.76
VIP2	10.0.0.68	10.0.0.78
Name Server	10.0.0.87	

Estimated time to complete this lab: 50 minutes

Exercise 8-3: Step by Step (Configuration Utility)

This section provides step-by-step instructions for completing "Exercise 8-3: Configuring DNS to Test a Global Server Load-Balancing (GSLB) Configuration" using the configuration utility.

Configuring DNS Settings

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_1 configuration utility logged on as the nsroot user for this task.

Configuring ADNS is only necessary on one NetScaler.

1. Switch to the Frankurt NetScaler (10.0.0.110) configuration utility.
2. Bind the "www.gslbdomain.com" domain alias to the GSLB_vsrv_global virtual server on the Frankfurt NetScaler.
   a. Navigate to **GSLB > Virtual Servers**.
   b. Select the **GSLB_vsrv_global** virtual server and click **Open**.
   c. Click the **Domains** tab and click **Add**.
   d. Type `www.gslbdomain.com` in the Domain Name field.
   e. Click **Create** and then click **OK**.
3. Create an authoritative DNS service using the 10.0.0.87 IP address on the Frankfurt NetScaler.
   a. Navigate to **DNS > Name Servers** and click **Add**.
   b. Type `10.0.0.87` in the IP Address field and select **Local**.
   c. Click **Create** and then click **Close**.
4. Switch to the Frankfurt NetScaler command-line interface and ping the www.gslbdomain.com domain to verify the DNS setup.
   a. Launch a PuTTY session and open the NS_VPX_1 saved session.
   b. Log on to the NS_VPX_1 command-line interface using the nsroot credentials.
   c. Ping the www.gslbdomain.com domain several times using the following command:

```
ping www.gslbdomain.com
```

Note the IP address, then press `CTRL+C` to stop the ping.

If GSLB is configured correctly on both systems, the ping response should alternate between the VIP addresses of the Frankfurt and Tokyo NetScaler systems during alternating tests.

Be aware that pinging the address from multiple locations at once can hide the round-robin load-balancing behavior, since subsequent requests can get load balanced (correctly) back to the first server.

5. Enable Multiple IP Response (MIR) on the Frankfurt NetScaler.
   a. Switch to the configuration utility for NS_VPX_1.
   b. Navigate to **GSLB > Virtual Servers**.
   c. Select **GSLB_vsrv_global** and click **Open**.
   d. Click the **Advanced** tab.
   e. Select **Send all "active" service IP's in response (MIR)** and click **OK**.

Configuring Local DNS Settings to Test the GSLB Configuration

Use the Win7Ext-Site1 virtual machine logged on as the CitrixAdmin user for this task.

1. Switch to the Win7Ext-Site1 virtual machine and log on using the CitrixAdmin/Password1.
2. Open the Local Area Network settings.
   a. Click **Start > Control Panel** to open the Control Panel dialog box on the hosted workstation.
   b. Click **Network and Internet**, click **Network and Sharing Center**, and then click **Local Area Connection 2**.
   c. Click **Properties** to open the Local Area Connection Properties dialog box.
3. Configure the local DNS settings to use the 10.0.0.87 GSLB virtual server.
   a. Highlight **Internet Protocol Version 4 (TCP/IPv4)**.
   b. Click **Properties** to open the Internet Protocol (TCP/IP) Properties dialog box.
   c. Select **Use the following DNS server addresses**.
   d. Set the Preferred DNS Server to `10.0.0.87`.

It is recommended to use only one NetScaler system as a DNS.

4. Close the Local Area Network settings.
   a. Click **OK** to save the settings.
   b. Click **Close** and then click **Close** again.
   c. Close the Network and Sharing Center window.

Testing the GSLB Configuration

Use the Win7Ext-Site1 virtual machine logged on as the CitrixAdmin user for this task.

1. Log on to the Win7Ext-Site1 virtual machine.
   a. Start the Win7Ext-Site1 virtual machine in XenCenter.
   b. Click the **Console** tab and log on using the CitrixAdmin credentials.
2. Ping the www.gslbdomain.com domain using a Windows command prompt.
   a. Click **Start**, type `cmd`, and press **Enter** to open a command prompt.
   b. Ping the www.gslbdomain.com domain using the following command:

```
ping www.gslbdomain.com
```

3. Repeat the ping 5 more times.
   Expected result: The server IP address of the response changes with some of the pings.

   If the responses do not alternate between Frankfurt and Tokyo, try flushing the DNS with the command: `ipconfig /flushdns`.
4. Open Internet Explorer and browse to `http://www.gslbdomain.com/remote.php` to view the global load-balancing server.
   Either the Red Tokyo (remote.php) screen on NetScaler Tokyo or the Green Frankfurt (remote.php) screen on NetScaler Frankfurt appears.
5. Open Firefox and browse to `http://www.gslbdomain.com/remote.php` to view the global load-balancing server.
   The alternate remote.php screen will load in the new browser.

If ping responses are displaying alternating IP addresses as expected, but the content in the web browsers is not reflecting load balancing between the Frankfurt and Tokyo NetScaler systems, close all open web browsers. Repeat the test with only one web browser and close and open the browser between each test.

6. Switch back to the command prompt on the Win7Ext-Site1 virtual machine and perform an nslookup on the www.gslbdomain.com domain.
   a. Switch to the Win7Ext_Site1 command prompt.
   b. Perform an nslookup using the following command:

```
nslookup www.gslbdomain.com
```

   The GSLB virtual server returns two IP addresses, 10.0.0.86 and 10.0.0.88.
7. Shut down the Win7Ext_Site1 virtual machine.
8. Switch back to the console of the Win7Client virtual machine.

Exercise 8-3: Step by Step (Command-line Interface)

This section provides step-by-step instructions for completing "Exercise 8-3: Configuring DNS to Test a Global Server Load-Balancing (GSLB) Configuration" using the command-line interface.

Configuring DNS Settings

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_1 command-line interface logged on as the nsroot user for this task.

Configuring ADNS is only necessary on one NetScaler.

1. Bind the domain alias to the GSLB virtual server using the following command:

```
bind gslb vserver GSLB_vsrv_global
-domainName www.gslbdomain.com
```

2. Create an authoritative DNS service on the Frankfurt NetScaler using the following command:

```
add dns nameserver 10.0.0.87 -local
```

3. Ping the domain name from the NetScaler command-line interface and verify the results using the following command:

```
ping www.gslbdomain.com
```

Note the IP address then enter `CTRL+C` to stop the ping.

4. Repeat the ping to domain name from the NetScaler command-line interface and verify the results using the following command:

```
ping www.gslbdomain.com
```

Note the IP address then enter `CTRL+C` to stop the ping.

If GSLB is configured correctly on both systems, the ping response should alternate between the VIP addresses of the Frankfurt and the Tokyo NetScaler systems during alternating tests.

Be aware that pinging the address from multiple locations at once can hide the round-robin load-balancing behavior, since subsequent requests can get load balanced (correctly) back to the first server.

5. Enable Multiple IP Response (MIR) on the Frankfurt NetScaler.
   a. Enable MIR using the following command:

```
set gslb vserver GSLB_vsrv_global -MIR ENABLED
```

Verifying the Configuration

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_1 and 2 command-line interfaces logged on as the nsroot user for this task.

Perform these steps on both the Frankfurt and Tokyo NetScalers.

1. Display the GSLB site using the following command:

```
show gslb site
```

2. Display the GSLB virtual server GSLB_vsrv_global using the following command:

```
show gslb vserver gslb_vsrv_global
```

3. Display the GSLB service gslb_svc_FRK using the following command:

```
show gslb service gslb_svc_FRK
```

4. Display the GSLB service gslb_svc_TOK using the following command:

```
show gslb service gslb_svc_TOK
```

Configuring Local DNS Settings to Test the GSLB Configuration

Use the Win7Ext-Site1 virtual machine logged on as the CitrixAdmin user for this task.

1. Switch to the Win7Ext-Site1 virtual machine and log on using the CitrixAdmin/Password1.
2. Open the Local Area Network settings.
   a. Click **Start** > **Control Panel** to open the Control Panel dialog box on the hosted workstation.
   b. Click **Network and Internet**, click **Network and Sharing Center**, and then click **Local Area Connection 2**.
   c. Click **Properties** to open the Local Area Connection Properties dialog box.
3. Configure the local DNS settings to use the 10.0.0.87 GSLB virtual server.
   a. Highlight **Internet Protocol Version 4 (TCP/IPv4)**.
   b. Click **Properties** to open the Internet Protocol (TCP/IP) Properties dialog box.

c. Select **Use the following DNS server addresses**.
d. Set the Preferred DNS Server to `10.0.0.87`.

It is recommended to use only one NetScaler system as a DNS.

4. Close the Local Area Network settings.
   a. Click **OK** to save the settings.
   b. Click **Close** and then click **Close** again.
   c. Close the Network and Sharing Center window.

Testing the GSLB Configuration

Use the Win7Ext-Site1 virtual machine logged on as the CitrixAdmin user for this task.

1. Log on to the Win7Ext-Site1 virtual machine.
   a. Start the Win7Ext-Site1 virtual machine in XenCenter.
   b. Click the **Console** tab and log on using the CitrixAdmin credentials.
2. Ping the www.gslbdomain.com domain using a Windows command prompt.
   a. Click **Start**, type `cmd`, and press **Enter** to open a command prompt.
   b. Ping the www.gslbdomain.com domain using the following command:

```
ping www.gslbdomain.com
```

3. Repeat the ping 5 more times.
   Expected result: The server IP address of the response changes with some of the pings.

   If the responses do not alternate between Frankfurt and Tokyo, try flushing the DNS with the command: `ipconfig /flushdns`.
4. Open Internet Explorer and browse to `http://www.gslbdomain.com/remote.php` to view the global load-balancing server.
   Either the Red Tokyo (remote.php) screen on NetScaler Tokyo or the Green Frankfurt (remote.php) screen on NetScaler Frankfurt appears.
5. Open Firefox and browse to `http://www.gslbdomain.com/remote.php` to view the global load-balancing server.
   The alternate remote.php screen will load in the new browser.

If ping responses are displaying alternating IP addresses as expected, but the content in the web browsers is not reflecting load balancing between the Frankfurt and Tokyo NetScaler systems, close all open web browsers. Repeat the test with only one web browser and close and open the browser between each test.

6. Switch back to the command prompt on the Win7Ext-Site1 virtual machine and perform an nslookup on the www.gslbdomain.com domain.
   a. Switch to the Win7Ext_Site1 command prompt.
   b. Perform an nslookup using the following command:

```
nslookup www.gslbdomain.com
```

   The GSLB virtual server returns two IP addresses, 10.0.0.86 and 10.0.0.88.
7. Shut down the Win7Ext_Site1 virtual machine.
8. Switch back to the console of the Win7Client virtual machine.

GSLB Troubleshooting Tips

If the procedure for testing the GSLB configuration does not produce the expected results, use the following tips to troubleshoot the lab configuration.

Unable to Resolve www.gslbdomain.com

- Ensure that you are pointing to the correct DNS server. For this lab, you should point to one of the ADNS IP addresses on either the Frankfurt or Tokyo NetScaler systems.
- Ensure that that you set the DNS setting on the correct network connection, if multiple networks are present. Consult with your instructor if required.
- Ensure that your web browser does not have a proxy server configured.
- Ensure that you are not connecting from a workstation behind a firewall that is blocking UDP port 53 (DNS).

Load Balancing between NetScaler Systems Not Occurring

- If the issue is at the browser test, clear the cache between test runs. For best results, close and re-open the browser between each test.
- If the issue is at the ping response from the workstation and only 1 IP address is being returned, verify that the GSLB sites, services, and virtual servers appear as UP and that MEP status shows as UP/Active.
- Multiple browser instances can also affect the results. Close all open browsers and start from a fresh session. Close and open browsers between tests.
- Conduct tests from only one hosted workstation at a time.
- Ensure that the GSLB and load-balancing (LB) features are ENABLED on both NetScaler systems.
- Verify on the NetScaler system that the resolution is alternating between GSLB services. Example: From the command-line interface on a given NetScaler system, ping www.gslbdomain.com; stop and re-ping. Verify that you receive the two expected IP addresses.

Other Issues

- Verify that the correct IP addresses are used for the load-balancing virtual server, GSLB services, and GSLB virtual server. Confirm that sites, virtual servers, services, and domains are bound appropriately.
- Verify that MEP is functioning and that both sites and services show as UP on both NetScaler systems. Using the configuration utility instead of the command-line interface may be easier to quickly verify the configured settings.

Module 9

Exercises for Clustering

Exercise 9-1: Configuring the Initial Cluster Setup

Overview

This exercise will demonstrate how to create a cluster instance and add nodes to the cluster.

Before You Begin

To begin this lab, ensure that the following virtual machines are started:

- AD.training.lab
- NS_VPX_1
- NS_VPX_2
- NS_VPX_3
- Router_Vyatta
- Win7Client

Estimated time to complete this exercise: 15 minutes

Exercise 9-1: Step by Step (Configuration Utility)

This section provides step by step instructions for completing "Exercise 9-1: Configuring the Initial Cluster Setup" using the configuration utility.

Configuring the Initial Cluster Setup

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_1, 2, and 3 configuration utilities logged on as the nsroot user for this task.

1. Start the NS_VPX_3 virtual machine from XenCenter.
2. Log on to the configuration utility for NS_VPX_1 using the nsroot credentials.
   a. Switch to the Win7client virtual machine and log on using the CitrixAdmin credentials.
   b. Launch the Firefox browser and browse to `http://10.0.0.110` and log on using the nsroot credentials.
3. Open the Cluster Configuration page.
   a. Navigate to **System** > **Cluster**.
   b. Click **Manager Cluster**.

4. Configure the cluster instance with a IP address of 10.0.0.150, an ID of 1, and a backplane interface of 1/2.
   a. Type `1` in the Cluster instance id field.
   b. Type `10.0.0.150` in the Cluster IP address field.
   c. Select `1/2` for the Backplane interface.
   d. Click **Create** and then click **Yes** to restart the system.
5. Log on to the cluster IP address to enable USNIP mode.
   a. Open a new browser window and browse to `http://10.0.0.150`.
   b. Log on to the NetScaler cluster using the nsroot credentials.
   c. Navigate to **System > Settings** and click **Configure modes**.
   d. Select **Use Subnet IP** and click **OK**.
6. Add NS_VPX_2 and NS_VPX_3 to the cluster on backplane interface 1/2.

These steps must be performed on the cluster IP configuration utility or the changes will not be replicated to other nodes in the cluster.

   a. Navigate to **System > Cluster > Nodes**.
   b. Click **Discover NetScalers**.
   c. Click the IP address range field and type `10.0.0.120 - 130`.
   d. Click the Backplane interface field and type `1/2`.
   e. Click **OK**.

      The search result should show the IP addresses for NS_VPX_2 and NS_VPX_3.
7. Complete adding the nodes to the cluster.
   a. Select both IP Addresses and click **OK**.
   b. Click **Yes** to confirm then click **Close**.

      The NS_VPX_1 and NS_VPX_2 nodes are now added to the cluster instance.
8. Assign 10.0.0.61 as a spotted SNIP to node 0 with a subnet mask of 255.255.255.0.
   a. Navigate to **Network > IPs** and click **Add**.
   b. Click the IP Address field and type `10.0.0.61`.
   c. Click the Netmask field and type `255.255.255.0`.
   d. Select `0` from the Owner Node drop-down menu.
   e. Select **Subnet IP** for the IP Type.
   f. Click **Create**.
9. Assign 10.0.0.62 as a spotted SNIP to node 1 with a subnet mask of 255.255.255.0.
   a. Click the IP Address field and type `10.0.0.62`.
   b. Click the Netmask field and type `255.255.255.0`.

c. Select `1` from the Owner Node drop-down menu.
d. Select **Subnet IP** for the IP Type.
e. Click **Create**.

10. Assign 10.0.0.63 as a spotted SNIP to node 2 with a subnet mask of 255.255.255.0.
    a. Click the IP Address field and type `10.0.0.63`.
    b. Click the Netmask field and type `255.255.255.0`.
    c. Select `2` from the Owner Node drop-down menu.
    d. Select **Subnet IP** for the IP Type.
    e. Click **Create** and click **Close**.
11. Create the LS/1 linkset to the cluster.

Since this lab environment is virtualized, you will use the "link set" deployment type. This does not require any router or switch configuration.

    a. Navigate to **Network > Linksets** and click **Add**.
    b. Click the Linkset id field and type `LS/1`.
    c. Click **Available**.
12. Add the three nodes to the linkset.
    a. Click the + next to 0/1/2.
    b. Click the + next to 1/1/2.
    c. Click the + next to 2/1/2.
    d. Click **Create** and click **Close**.

Exercise 9-1: Step by Step (Command-line Interface)

This section provides step by step instructions for completing "Exercise 9-1: Configuring the Initial Cluster Setup" using the command-line interface.

Configuring the Initial Cluster Setup

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_1, 2, and 3 command-line interfaces logged on as the nsroot user for this task.

1. Add and configure the first node to the cluster with an IP address of 10.0.0.110, a backplane of 1/2, and a state of PASSIVE.
    a. Switch to the NetScaler command-line interface on NS_VPX_1 and add the node to the cluster instance using the following command:

```
add cluster instance 1
```

b. Add node1 to the cluster instance with interface 1/2 as the backplane interface using the following command:

```
add cluster node 1 10.0.0.110 -state PASSIVE -backplane 1/2
```

c. Enable the cluster instance using the following command:

```
enable cluster instance 1
```

d. Save the configuration using the following command:

```
save ns config
```

e. Restart the system using the following command:

```
reboot -warm
```

```
y
```

Wait for the NetScaler system to restart.

2. Add the 10.0.0.150 cluster IP to the cluster using a netmask of 255.255.255.255.
   a. Switch to the NetScaler command-line interface onNS_VPX_1 and log back on using the nsroot credentials.
   b. Add the cluster IP to the cluster using the following command:

```
add ns ip 10.0.0.150 255.255.255.255 -type CLIP
```

   c. Verify the cluster instance using the following commands:

```
show cluster instance
```

```
show cluster node
```

3. Log on to the cluster IP address to enable USNIP mode.
   a. Open a new PuTTy session to the cluster IP at 10.0.0.150.
   b. Log on to the NetScaler cluster using the nsroot credentials.
   c. Enable USNIP mode using the following command:

```
enable ns mode usnip
```

4. Add NS_VPX_2 and NS_VPX_3 to the cluster.

These commands must be performed on the cluster IP or the changes will not be replicated to other nodes in the cluster.

a. Add NS_VPX_2 and NS_VPX_3 to the cluster using the following commands:

```
add cluster node 2 10.0.0.120 -state PASSIVE
-backplane 2/1/2
```

```
add cluster node 3 10.0.0.130 -state PASSIVE
-backplane 3/1/2
```

b. Save the configuration using the following command:

```
save ns config
```

5. Switch to the NetScaler command-line interface on NS_VPX_2 and join it to the cluster.
   a. Open a new PuTTy session to NS_VPX_2 and log on using the nsroot credentials.
   b. Add the node to the cluster using the following command:

```
join cluster -clip 10.0.0.150 -password nsroot
```

   c. Save the configuration using the following command:

```
save ns config
```

   d. Restart the system using the following command:

```
reboot -warm
```

6. Switch to the NetScaler command-line interface on NS_VPX_3 and join it to the cluster.
   a. Open a new PuTTy session to NS_VPX_3 and log on using the nsroot credentials.
   b. Add the node to the cluster using the following command:

```
join cluster -clip 10.0.0.150 -password nsroot
```

   c. Save the configuration using the following command:

```
save ns config
```

   d. Restart the system using the following command:

```
reboot -warm
```

Wait for node2 and node3 to come back on line before continuing.

7. Verify that the nodes show as PASSIVE and that node1 is the CCO.
   a. Return to the command-line interface for the cluster IP at 10.0.0.150.
   b. Verify that the nodes show as PASSIVE and that node1 is the CCO using the following command:

```
show cluster node
```

8. Assign 10.0.0.61 as a spotted SNIP to node 1 with a subnet mask of 255.255.255.0 using the following command:

```
add ns ip 10.0.0.61 255.255.255.0 -type SNIP -ownerNode 1
```

9. Assign 10.0.0.62 as a spotted SNIP to node 2 with a subnet mask of 255.255.255.0 using the following command:

```
add ns ip 10.0.0.62 255.255.255.0 -type SNIP -ownerNode 2
```

10. Assign 10.0.0.63 as a spotted SNIP to node 3 with a subnet mask of 255.255.255.0 using the following command:

```
add ns ip 10.0.0.63 255.255.255.0 -type SNIP -ownerNode 3
```

11. View and verify the cluster IP addressses using the following command:

```
show ip
```

12. Set the node state to ACTIVE on all the nodes in the cluster.
    a. Set an ACTIVE state on node 1 using the following command:

```
set cluster node 1 -state ACTIVE
```

    b. Set an ACTIVE state on node 2 using the following command:

```
set cluster node 2 -state ACTIVE
```

    c. Set an ACTIVE state on node 3 using the following command:

```
set cluster node 3 -state ACTIVE
```

13. Verify the cluster nodes using the following command:

```
show cluster node
```

Nodes that successfully synchronize will show its Health status as UP.

14. Remove a node from the cluster and rejoin it to the cluster.

This is an optional step. If all nodes synchronized successfully, proceed to the next step. Perform these steps if any of the nodes is not synchronized with the cluster.

a. Identify the node that did not synchronize using the following command:

```
show cluster node
```

A node that did not synchronize with the cluster will show its Health status as NOT UP.

b. Switch the command-line interface of that node and remove the cluster instance using the following command, where `n` is the node number.

```
rm cluster instance n
```

c. Rejoin the node to the cluster using the following command:

```
join cluster -clip 10.0.0.150 -password nsroot
```

d. Save the configuration using the following command:

```
save ns config
```

e. Restart the system using the following command:

```
reboot -warm
```

```
y
```

15. Verify that the Mode for each node shows as ACTIVE using the following command:

```
show ip
```

16. Configure the cluster to use the link set traffic distribution method and bind the interfaces for all three nodes in the cluster.

Since this lab environment is virtualized, you will use the link set deployment type, as this does not require any router or switch configuration.

a. Switch to the command-line interface for the cluster IP at 10.0.0.150.

b. Create the link set definition using the following command:

```
add linkset LS/1
```

c. Bind the interfaces connected to the link set using the following command:

```
bind linkset LS/1 -ifnum 1/1/2 2/1/2 3/1/2
```

d. Verify the link set binding using the following command:

```
show linkset LS/1
```

Exercise 9-2: Configuring Load Balancing on a Cluster

Overview

This exercise will demonstrate how to configure load balancing on a cluster.

Before You Begin

To begin this lab, ensure that the following virtual machines are started:

- AD.training.lab
- NS_VPX_1
- NS_VPX_2
- NS_VPX_3
- Router_Vyatta
- WebBlue
- WebGreen
- WebRed
- Win7Client

Estimated time to complete this exercise: 10 minutes

Exercise 9-2: Step by Step (Configuration Utility)

This section provides step by step instructions for completing "Exercise 9-2: Configuring Load Balancing on a Cluster" using the configuration utility.

Configuring Load Balancing on a Cluster

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_1, 2, and 3 configuration utilities logged on as the nsroot user for this task.

1. Enable the load-balancing feature for the cluster.
   a. Navigate to **System** > **Settings**.
   b. Click **Configure Basic Features**.
   c. Select **Load Balancing** and click **OK**.
2. Add the "WebBlue" server to the cluster with an IP Address of 192.168.10.205.
   a. Navigate to **Load Balancing** > **Servers** and click **Add**.

b. Click the Server Name field and type WebBlue.
c. Click the IP Address field and type `192.168.10.205`.
d. Click **Create**.

3. Add the "WebGreen" server to the cluster with an IP Address of 192.168.10.210.
   a. Click the Server Name field and type WebGreen.
   b. Click the IP Address field and type `192.168.10.210`.
   c. Click **Create**.
4. Add the "WebRed" server to the cluster with an IP Address of 192.168.10.215.
   a. Click the Server Name field and type WebRed.
   b. Click the IP Address field and type `192.168.10.215`.
   c. Click **Create** and click **Close**.
5. Add the svc_blue service for HTTP to the cluster.
   a. Navigate to **Load Balancing** > **Services** and click **Add**.
   b. Click the Service Name Field and type `svc_blue`.
   c. Select **WebBlue** from the Server drop-down menu.
   d. Select **HTTP** from the Protocol drop-down menu.
   e. Click the Port field and type `80`.
   f. Click **Create**.
6. Add the svc_green service for HTTP to the cluster.
   a. Click the Service Name Field and type `svc_green`.
   b. Select **WebGreen** from the Server drop-down menu.
   c. Select **HTTP** from the Protocol drop-down menu.
   d. Click the Port field and type `80`.
   e. Click **Create**.
7. Add the svc_red service for HTTP to the cluster.
   a. Click the Service Name Field and type `svc_red`.
   b. Select **WebRed** from the Server drop-down menu.
   c. Select **HTTP** from the Protocol drop-down menu.
   d. Click the Port field and type `80`.
   e. Click **Create** and click **Close**.
8. Create the "lb_vsrv_rbg" load-balancing virtual server on the cluster for HTTP.
   a. Navigate to **Load Balancing** > **Virtual Servers** and click **Add**.
   b. Click the Name field and type `lb_vsrv_rbg`.
   c. Select HTTP from the Protocol drop-down menu.
   d. Type `10.0.0.80` in the IP Address field.
   e. Type `80` in the Port field.

9. Select the checkboxes for the svc_blue, svc_green, and svc_red services to bind them to the lb_vsrv_rbg virtual server.
10. Configure the virtual server to use the Round Robin load balancing method.
    a. Click the **Method and Persistence** tab.
    b. Select **Round Robin** for the LB Method.
    c. Click **Create**, and then click **Close**.

       The virtual server was created and the state should be UP.
11. Test load balancing by browsing to the "lb_vsrv_rbg" IP address.
    a. Open another browser window and browse to `http://10.0.0.80/home.php`.

       The Citrix Home page should appear displaying one of the color pages.
    b. Refresh the web page.

       The web page should cycle through the three different color pages.

Exercise 9-2: Step by Step (Command-line Interface)

This section provides step by step instructions for completing "Exercise 9-2: Configuring Load Balancing on a Cluster" using the command-line interface.

Configuring Load Balancing on a Cluster

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_1, 2, and 3 command-line interfaces logged on as the nsroot user for this task.

1. Add the Web_Blue, Web_Green, and Web_Red servers to the cluster and create the corresponding services for HTTP.
    a. Switch to the command-line interface for the cluster IP at 10.0.0.150. Log on to the NetScaler system using the nsroot credentials if necessary.
    b. Add the servers using the following commands:

```
add server WebBlue 192.168.10.205
```

```
add server WebGreen 192.168.10.210
```

```
add server WebRed 192.168.10.215
```

    c. Add the HTTP services for the servers using the following commands:

```
add service svc_blue WebBlue HTTP 80
```

```
add service svc_green WebGreen HTTP 80
```

```
add service svc_red WebRed HTTP 80
```

2. Enable the load balancing feature using the following command:

```
enable ns feature lb
```

3. Create the lb_vsrv_rbg load-balancing virtual server for HTTP and bind the svc_blue, svc_green, and svc_red services to it.
   a. Create the HTTP load-balancing virtual server using the following command:

```
add lb vserver lb_vsrv_rbg HTTP 10.0.0.80 80
-lbMethod ROUNDROBIN
```

   b. Bind the HTTP load-balancing virtual server to the HTTP services using the following commands:

```
bind lb vserver lb_vsrv_rbg svc_blue
```

```
bind lb vserver lb_vsrv_rbg svc_green
```

```
bind lb vserver lb_vsrv_rbg svc_red
```

4. Test load balancing by browsing to the **lb_vsrv_rbg** IP address.
   a. Open another browser window and browse to `http://10.0.0.80`.

      The Citrix Welcome page should appear and display one of the color pages.
   b. Refresh the web page.

      The web page should cycle through the three different color pages.

Module 10

Exercises for Security and Authentication

Exercise 10-1: Configuring SSL Certificates and SSL Offload

Overview

This exercise demonstrates the use of SSL Certificates with a NetScaler system and how to configure SSL Offload.

Before You Begin

To begin this lab, ensure that the following virtual machines are started:

- AD.training.lab
- NS_VPX_0
- Router-Vyatta
- SQLServer
- WebBlue
- WebGreen
- WebRed
- Win7Client

Estimated time to complete this exercise: 20 minutes

Exercise 10-1: Step by Step (Configuration Utility)

This exercise provides step-by-step instructions for completing "Exercise 10-1: Configuring SSL Certificates and SSL Offload" using the configuration utility.

Creating an RSA Key File

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Use the NetScaler certificate tools to create an RSA key file called TestKey.pem with a key size of 2048 and DES3 as the encoding algorithm.
   a. Expand the **SSL** node and click **Create RSA Key** in the SSL pane.

      The Create RSA Key dialog box opens.
   b. Type `TestKey.pem` in the Key Filename field and then type `2048` in the Key Size field.

c. Verify that **F4** is selected as the public exponent value and that **PEM** is selected as the key format.

d. Select **DES3** as the PEM encoding algorithm and type `Password1` in the PEM Passphrase field. Then re-type `Password1` in the Verify Passphrase field.

In a production environment, specify a secure passphrase.

e. Click **Create** then click **Close**.

The Create RSA Key dialog box closes.

Creating a Certificate Request

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Use the NetScaler certificate tools to create a certificate request named TestCSR.csr using TestKey.pem as the key file and the MillennialGadgets.com company information.

   a. Expand the **SSL** node and select **Create CSR (Certificate Signing Request)** in the SSL pane.

   The Create CSR (Certificate Signing Request) dialog box opens.

   b. Type `TestCSR.csr` in the Request File Name field.

   c. Click **Browse** next to the Key File Name field, and select **TestKey.pem** from the current directory and click **Select**.

   d. Type `Password1` in the PEM Passphrase field.

   e. Provide the following information under Distinguished Name Fields:

   - Common Name: `MillennialGadgets.com`
   - Organization Name: `MillennialGadgets.com`
   - Country Name: `UNITED STATES`
   - State or Province Name: `California`

   f. Type `Password1` in the Challenge Password field.

This password does not have to be same as the PEM passphrase. However, outside of the lab environment, it is recommended that you specify a secure passphrase.

   g. Type `MillennialGadgets.com` in the Company Name field.

   h. Click **Create** then click **Close**.

   The Create Certificate Request dialog box closes.

Creating a Certificate

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Use the NetScaler certificate tools to start creating a self-signed certificate named TestCert.cert with a validity period of 1825 days.
   a. Expand the **SSL** node and click **Create Certificate** in the SSL pane.
   b. Type `TestCert.cert` in the Certificate File Name field, verify that **PEM** is selected as the certificate format, and then select **Server** as the certificate type.
   c. Click **Browse** next to the Certificate Request File Name field and select **TestCSR.csr** in the displayed directory and click **Select**.
   d. Type `1825` in the Validity Period field.
2. Use the NetScaler certificate tools to continue creating a self-signed certificate named TestCert.cert using ns-root.cert and ns-root.key as the CA certificate file and CA key file.
   a. Click **Browse** next to the CA Certificate File Name field and select **ns-root.cert** in the current directory and click **Select**.
   b. Verify that **PEM** is selected as the CA certificate file format.
   c. Click **Browse** next to the CA Key File Name field and select **ns-root.key** in the current directory and click **Select**.
   d. Verify that **PEM** is selected as the CA key file format.
   e. Type `Password1` in the PEM Passphrase field.
3. Use the NetScaler certificate tools to complete creating a self-signed certificate named TestCert.cert using ns-root.srl as the CA serial number file.
   a. Click **Browse** next to the CA Serial Number File field and select **ns-root.srl** in the displayed directory and click **Select**.
   b. Click **Create** then click **Close**.

      The Create Certificate dialog box closes.

Configuring a Certificate-Key Pair

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Create a certificate-key pair on the NetScaler system using the new certificate and key.
   a. Expand the **SSL** node and click **Certificates**.
   b. Click **Install** in SSL Certificates pane.

      The Install Certificate dialog box opens.
   c. Type `TestCertKey` in the Certificate-Key Pair Name field.
   d. Click **Browse** next to Certificate File Name field and select **TestCert.cert** in the displayed directory and click **Select**.

e. Click **Browse** next to the Private Key File Name field and select **TestKey.pem** in the displayed directory and click **Select**.

f. Type `Password1` in the Password field, then verify that **PEM** is selected as the certificate format, and then click **Install** to create the certificate-key pair.

g. Click **Close**.

2. Verify that TestCertKey is displayed in the SSL Certificates pane and the status is shown as Valid.

Creating an SSL Offload Virtual Server

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Begin configuration of an "ssl_vsrv_rbg" SSL-offload virtual server with an IP address of 10.0.0.81.
   a. Expand the **SSL Offload** node and click **Virtual Servers**.
   b. Click **Add** in the SSL Offload Virtual Servers pane.
      The Create Virtual Server (SSL Offload) dialog box opens.
   c. Type `ssl_vsrv_rbg` in the Name field and type `10.0.0.81` in the IP Address field.
   d. Select **SSL** as the protocol and verify that `443` is entered in the Port field.
   e. Check the **Active** box for the following services on the Services tab:
      - svc_red
      - svc_blue
      - svc_green
2. Complete the configuration of the ssl_vsrv_rbg SSL-offload virtual server by adding the TestCertKey to the virtual server. Create the virtual server.
   a. Click the **SSL Settings** tab and select **TestCertKey** from the list of available certificates.
   b. Click **Add** to move the certificate to the list of configured certificates.
   c. Click **Create** then click **Close**.
      The Create Virtual Server (SSL Offload) dialog box closes.
   d. Verify the SSL virtual server (**ssl_vsrv_rbg**) displays the State as UP.
3. Click **Save** in the upper-right corner of the configuration utility to save the running configuration.

Testing SSL Offload

Use the Win7Client virtual machine, logged on as the CitrixAdmin user for this task.

1. Open a secure connection to the virtual server and test the SSL offload configuration.
   a. Open a Firefox window and browse to `https://10.0.0.81/home.php`.

b. Click **I Understand the Risks**, click **Add Exception**, and then click **Confirm Security Exception** to continue to the web site.

A certificate error will be displayed within Firefox because the test certificate was not created by a trusted certificate authority and a root certificate was not installed. Disregard these errors for this lab exercise.

c. Refresh the web site multiple times.

The site is now secured with SSL. The web page load-balances between the Red, Blue, and Green web servers based on the services bound to the SSL-offload virtual server.

Exercise 10-1: Step by Step (Command-Line Interface)

This exercise provides step-by-step instructions for completing "Exercise 10-1: Configuring SSL Certificates and SSL Offload" using the command-line interface.

Configuring a Self-Signed Certificate (Command-Line Interface)

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Create an RSA Key called TestKey.pem with a key size of 2048 and DES3 as the encoding algorithm..
   a. Create the RSA key file using the following command:

```
create ssl rsakey TestKey.pem 2048 -exponent F4
-keyform PEM -des3 -password Password1
```

2. Create a certificate request called TestCSR.csr using TestKey.pem as the key file and the MillennialGadgets.com company information.
   a. Create the certificate request using the following command:

```
create ssl certreq TestCSR.csr -keyFile
TestKey.pem -keyForm PEM -PEMPassPhrase Password1
-countryName US -stateName California
-organizationName MillennialGadgets.com
-commonName MillennialGadgets.com
-challengePassword Password1
```

3. Create a self-signed certificate named TestCert.cert with a validity period of 1825 days.
   a. Create the SSL certificate using the following command:

```
create ssl cert TestCert.cert TestCSR.csr
SRVR_CERT
-CAcert /nsconfig/ssl/ns-root.cert
-CAkey /nsconfig/ssl/ns-root.key
-CAserial /nsconfig/ssl/ns-root.srl
```

4. Create the Certificate Key Pair by using the created RSA Key and Certificate.
   a. Create the certkey using the following command:

```
add ssl certkey TestCertKey -cert TestCert.cert
-key TestKey.pem -password Password1
```

   b. View the certkey using the following command:

```
show ssl certkey
```

5. Save the NetScaler configuation.
   a. Save the configuration using the following command:

```
save ns config
```

Configuring SSL Offload (Command-Line Interface)

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Create an SSL virtual server called ssl_vsrv_rbg, bind the certificate key-pair to the virtual server and then bind the services to the virtual server.
   a. Create the SSL virtual server.

```
add lb vserver ssl_vsrv_rbg SSL 10.0.0.81 443
```

   b. Bind the certificate-key pair to the SSL virtual server using the following command:

```
bind ssl vserver ssl_vsrv_rbg -certkeyName TestCertKey
```

   c. Bind services to the SSL virtual server using the following commands:

```
bind lb vserver ssl_vsrv_rbg svc_red
```

```
bind lb vserver ssl_vsrv_rbg svc_blue
```



```
bind lb vserver ssl_vsrv_rbg svc_green
```

d. Save the configuration using the following command:

```
save ns config
```

Testing SSL Offload

Use the Win7Client virtual machine, logged on as the CitrixAdmin user for this task.

1. Open a secure connection to the virtual server and test the SSL offload configuration.
   a. Open a Firefox window and browse to `https://10.0.0.81/home.php`.
   b. Click **I Understand the Risks**, click **Add Exception**, and then click **Confirm Security Exception** to continue to the web site.

A certificate error will be displayed within Firefox because the test certificate was not created by a trusted certificate authority and a root certificate was not installed. Disregard these errors for this lab exercise.

   c. Refresh the web site multiple times.

      The site is now secured with SSL. The web page load-balances between the Red, Blue, and Green web servers based on the services bound to the SSL-offload virtual server.

Exercise 10-2: Enabling External Authentication

Overview

This exercise will demonstrate how to configure the NetScaler system to use an LDAP server to authenticate system users.

There are no command-line instructions for this exercise.

Before You Begin

To begin this lab, ensure that the following virtual machines are started:

- AD.training.lab
- NS_VPX_0
- Router_Vyatta
- Win7Client

To complete this exercise, you need to have the following information:

Active Directory architecture

Active Directory	Value
AD Domain Controller	192.168.10.11
AD Domain Name: Base DN	DC=Training,DC=LAB
Administrator BindDN	CitrixAdmin@training.lab
Administrator Password	Password1
Server Login Name Attribute (case sensitive)	samAccountName

Groups and User Credentials

Group	User	Password	Policy
Domain Admins	citrixadmin	Password1	Superuser
Remote Userrs	user1	Password1	Show Only

Estimated time to complete this exercise: 15 minutes

Exercise 10-2: Step by Step (Configuration Utility)

This section provides step by step instructions for completing "Exercise 10-2: Enabling External Authentication" using the configuration utility.

Examining Command Policies

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Open Firefox and browse to the configuration utility for NS_VPX_0 and log on using the nsroot credentials, if necessary.
2. Examine the expression for the superuser policy.
   a. Navigate to **System** > **Command Policies**.
   b. Expand the **superuser** policy in the Policies section.
      Note the policy allows any command to be permitted using the ".*" expression.
3. Create a new policy that only allows the show command using the string (^show\s+x*) as the command spec.
   a. Click **Add** in the Policies section.
   b. Type `show_only` in the Policy Name field.
   c. Select **Allow** from the drop-down list for the Action.
   d. Click in the Command Spec field and clear any existing text, then type `(^show\s+.*)`.
   e. Click **Create** and then click **Close**.

Enabling LDAP Authentication

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Grant superuser access to the Domain Admins Active Directory group.
   a. Navigate to **System** > **Groups**.
   b. Click **Add**.
   c. Type `Domain Admins` in the Group Name field.
      Group names must correspond to the group in the directory service and are case sensitive.
   d. Select **superuser** in the Command Policies field to make it active and bind the group to the command policy.
      Note that the Details pane lists the commands allowed by the selected command policies.
   e. Click **Create** and then click **Close**.

2. Grant show-only access to the Remote Users Active Directory group.
   a. Click **Add**.
   b. Type `Remote Users` in the Group Name field.
      Group names must correspond to the group in the directory service and are case sensitive.
   c. Select **show_only** in the Command Policies field.
   d. Click **Create** and then click **Close**.
3. Create an "auth_ldap_srv" entry for the LDAP server with 192.168.10.11 as the IP address and 389 as the port.
   a. Navigate to **System** > **Authentication** > **LDAP** and click the **Servers** tab.
   b. Click **Add**.
   c. Complete the Create Authentication Server form as follows:
      - Name: `auth_ldap_srv`
      - IP Address: `192.168.10.11`
      - Port: `389`
      - Base DN: `DC=Training,DC=LAB`
      - Administrator Bind DN: `CitrixAdmin@training.lab`
      - Administrator Password: `Password1`
      - Confirm Administrator Password: `Password1`
      - Server Logon Name Attribute: `samAccountName`
   d. Click **Create**, and then click **Close**.
4. Create an "auth_ldap_policy" authentication policy for the LDAP server with an expression of True.
   a. Click the **Policies** tab.
   b. Click **Add** and type `auth_ldap_policy` in the Name field.
   c. Verify that **auth_ldap_srv** is specified in the Server field.
   d. Select **True value** from the drop-down menu to the left of the Add Expression button and then click **Add Expression**.
      The Expression field should contain the expression ns_true.
   e. Click **Create** then click **Close** to close the Create Authentication policy field.
5. Bind the auth_ldap_policy globally.
   a. Right-click the **auth_ldap_policy** and then click **Global Bindings**.
   b. Click **Insert Policy**, select **auth_ldap_policy**, and then click **OK** to bind the policy to System Global.
6. Click **Save** to save the NetScaler configuration and then click **Yes** in the Save Configuration dialog box.
7. Verify that an Active Directory Domain Administrator is able to log on to the NetScaler.
   a. Launch a PuTTY session to NS_VPX_0 to access the command-line interface.

b. Log on using the CitrixAdmin credentials.

c. Type the following command to create a test server on the NetScaler system and verify that a new server can be added.

```
add server testsrv 192.168.10.224
```

The CitrixAdmin user was allowed to add the server because of the superuser command policy.

d. Close the PuTTy window to terminate the session.

8. Verify that an Active Directory Remote User is able to log on to the NetSclaer and view settings but is not allowed to make changes.

a. Open a new PuTTY session to NS_VPX_0 to access the command-line interface.

b. Log on using the user1 credentials.

c. View the NetScaler information using the following commands.

```
show ns ip
```

```
show version
```

The user1 user is allowed to run the show commands because of the show_server command policy.

d. Attempt to delete the testsrv server using the following command.

```
rm server testsrv
```

You will receive an error because the user1 user does not have permissions to make changes on the NetScaler.

e. Close the PuTTY window to terminate the session.

Module 11

Exercises for Configuring Rewrite, Responder, and URL Transform

Exercise 11-1: Configuring Rewrite, Responder, and URL Transformation

Overview

This exercise will demonstrate how to create a rewrite rule that appends home.php to the URL when a request is sent to the web server.

Before You Begin

To begin this exercise, ensure that the following virtual machines are started:

- AD.training.lab
- NS_VPX_0
- Router_Vyatta
- Web_Blue
- Web_Green
- Web_Red
- Win7Client

Estimated time to complete this exercise: 10 minutes

Exercise 11-1: Step by Step (Configuration Utility)

This section provides step by step instructions for completing "Exercise 11-1: Configuring Rewrite" using the configuration utility.

Viewing the Default Web Page

Use the Win7Client virtual machine and log on as the CitrixAdmin user for this task.

1. Launch Mozilla Firefox.
2. Browse to the RBG virtual server by navigating to http://10.0.0.80.
   Note that the index page is displayed for one of the RBG servers.
3. Browse to the RBG virtual server home page by navigating to http://10.0.0.80/home.php.
   Note that the home page is displayed for one of the RBG servers.

Using Rewrite to Modify a URL

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Switch to the configuration utility for NS_VPX_0 at http://10.0.0.100 and log on using the nsroot credentials if necessary.
2. Enable the Rewrite feature for the NetScaler.
   a. Navigate to **System** > **Settings**.
   b. Click **Configure basic features**.
   c. Select **Rewrite** and click **OK**.
3. Add the rw_act_SendToHome rewrite action to replace an unspecified URL path with "/home.php."
   a. Navigate to **Rewrite** > **Actions** and click **Add**.
   b. Click the Name field and type `rw_act_SendToHome`.
   c. Select **REPLACE** from the Type drop-down menu and type `HTTP.REQ.URL.PATH` in the Expression to choose target text reference field.
   d. Click the String expression for replacement text and type `"/home.php"`.
   e. Click **Create** and then click **Close**.
4. Add the req_pol_SendToHome rewrite policy using the rw_act_SendToHome action that matches the forward slash (/) character.
   a. Navigate to **Rewrite** > **Policies** and click **Add**.
   b. Click the Name field and type `req_pol_SendToHome`.
   c. Select **rw_act_SendToHome** in the Action field.
   d. Click the Expression field and type `HTTP.REQ.URL.PATH.EQ("/")`.
   e. Click **Create** and click **Close**.
5. Globally bind the rewrite policy.
   a. Click **Policy Manager**.
   b. Select **Override Global** under Bind Points.
   c. Click **Insert Policy** and select **req_pol_SendToHome** from the Policy Name drop-down menu.
   d. Select **NEXT** for the Goto Expression.
   e. Click **Apply Changes** and then click **Close**.
6. Click **Save** to save the NetScaler configuration.
7. Verify the rewrite policy works by browsing to http://10.0.0.80/.
   The home.php page for one of the RGB servers is displayed without having to specify it in the URL.
8. Unbind the req_pol_SendToHome policy for future exercises.
   a. Navigate to **Rewrite** > **Policies**.

b. Click **Policy Manager**.
c. Select the **req_pol_SendToHome** policy and click **Unbind Policy**.
d. Click **Apply Changes** and click **Close**.

Exercise 11-1: Step by Step (Command-Line Interface)

This section provides step by step instructions for completing "Exercise 11-1: Configuring Rewrite, Responder, and URL Transformation" using the command-line interface.

Viewing the Default Web Page

Use the Win7Client virtual machine and log on as the CitrixAdmin user for this task.

1. Launch Mozilla Firefox.
2. Browse to the RBG virtual server by navigating to http://10.0.0.80.
   Note that the index page is displayed for one of the RBG servers.
3. Browse to the RBG virtual server home page by navigating to http://10.0.0.80/home.php.
   Note that the home page is displayed for one of the RBG servers.

Using Rewrite to Modify a URL

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Log on to the command-line interface for NS_VPX_0 using the nsroot credentials.
2. Enable the Rewrite feature using the following command:

```
enable ns feature rewrite
```

3. Add the rw_act_SendToHome rewrite action to replace the URL path "/home.php" using the following command:

```
add rewrite action rw_act_SendToHome REPLACE HTTP.REQ.URL.PATH
'"/home.php"'
```

4. Add the req_pol_SendToHome rewrite policy using the re_act_SendToHome action using the following command:

```
add rewrite policy req_pol_SendToHome
'HTTP.REQ.URL.PATH.EQ("/")' rw_act_SendToHome
```

The Policy is not yet active.

5. Globally bind the rewrite policy using the following command:

```
bind rewrite global req_pol_SendToHome 10 NEXT
-type REQ_OVERRIDE
```

6. Save the NetScaler configuration using the following command:

```
save ns config
```

7. Verify that the rewrite policy worked by browsing to `http://10.0.0.80/`.
The "home.php" page for one of the RBG servers is displayed without having to specify it in the URL.
8. Unbind the rewrite policy for future exercises using the following command:

```
unbind rewrite global req_pol_SendToHome
```

Exercise 11-2: Removing HTTP Header

Overview

This exercise demonstrates how to configure a rewrite policy that modifies the server response and removes the HTTP header that identifies the web server hosting the web site.

Before You Begin

To begin this exercise, ensure the following virtual machines are started:

- AD.training.lab
- NS_VPX_0
- Router_Vyatta
- Web_Blue
- Web_Green
- Web_Red
- Win7Client

Estimated time to complete this exercise: 15 minutes

Exercise 11-2: Step by Step (Configuration Utility)

This section provides step by step instructions for completing "Exercise 11-2: Removing HTTP Header" using the configuration utility.

Viewing the Default Header Information

Use the Win7Client virtual machine logged on as the CitrixAdmin user for this task.

1. Open the HttpFox add-on in the Firefox browser.
   a. Launch the **Firefox** browser.
   b. Select **Tools** > **Web Developer** > **HttpFox** > **Toggle HttpFox**.
      The HttpFox window appears at the bottom of the browser.
   c. Click **Start** in the HttpFox window.
2. View the header information for the server that is hosting the RBG web page.
   a. Browse to `http://10.0.0.80`.
   b. Select one of the items in the top box that does not say `(cache)` in the HttpFox Result column.

c. View the header information in the Response header pane.

Verify that the Server header is displayed as Server: Microsoft-IIS/7.5.

3. Close the HttpFox window.

Using Rewrite to Remove Header Information

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Switch to the configuration utility for NS_VPX_0. Log on using the nsroot credentials if necessary.
2. Add the rw_act_RemoveSrvID rewrite action to remove the Server ID from the header.
   a. Navigate to **Rewrite > Actions** and click **Add**.
   b. Click the Name field and type `rw_act_RemoveSrvID`.
   c. Select **DELETE_HTTP_HEADER** from the Type drop-down menu.
   d. Click the Header Name field and type `Server`.
   e. Click **Create**, and then click **Close**.
3. Add a "res_pol_RemoveSrvID" rewrite policy to remove the Server ID with an IS_VALID http response.
   a. Click the **Policies** node and click **Add**.
   b. Click the Name field and type `res_pol_RemoveSrvID`.
   c. Select **rw_act_RemoveSrvID** in the Action field.
   d. Click the Expression field and type `HTTP.RES.IS_VALID`.
   e. Click **Create**, and then click **Close**.
4. Bind the res_pol_RemoveSrvID globally.
   a. Click **Policy Manager**.
   b. Click **Response** then click **Override Global** under Bind Points.
   c. Click **Insert Policy** and select **res_pol_RemoveSrvID** for the Policy Name.
   d. Select **NEXT** for the Goto Expression.
   e. Click **Apply Changes**, and then click **Close**.

Verifying the Header Information

Use the Win7Client virtual machine logged on as the CitrixAdmin user for this task.

Do not replace the server header with strings or phrases such as "Hack this" or "Try to hack me now." Potential legal implications with such a statement may exist because you could be granting permission to hackers to attempt to violate your security. As always, consult the appropriate security experts within your organization for guidelines and requirements for your environment.

1. Open the HttpFox add-on in the Firefox browser.
   a. Launch the **Firefox** browser.
   b. Select **Tools** > **Web Developer** > **HttpFox** > **Toggle HttpFox**.
      The HttpFox window appears at the bottom of the browser.
   c. Click **Clear** in the HttpFox window.
2. Verify that the Header information for the server is not displayed.
   a. Browse to the RBG virtual server by navigating to `http://10.0.0.80`.
   b. Select one of the items in the top box which does not say `(cache)` in the HttpFox Result column.
   c. View the Header information in the Response header pane.
      Verify the Server does not display.
3. Close the HttpFox window.

Exercise 11-2: Step by Step (Command-line Interface)

This section provides step by step instructions for completing "Exercise 11-2: Removing HTTP Header" using the command-line interface.

Viewing the Default Header Information

Use the Win7Client virtual machine logged on as the CitrixAdmin user for this task.

1. Open the HttpFox add-on in the Firefox browser.
   a. Launch the **Firefox** browser.
   b. Select **Tools** > **Web Developer** > **HttpFox** > **Toggle HttpFox**.
      The HttpFox window appears at the bottom of the browser.
   c. Click **Start** in the HttpFox window.
2. View the header information for the server that is hosting the RBG web page.
   a. Browse to `http://10.0.0.80`.
   b. Select one of the items in the top box that does not say `(cache)` in the HttpFox Result column.
   c. View the header information in the Response header pane.
      Verify that the Server header is displayed as Server: Microsoft-IIS/7.5.

3. Close the HttpFox window.

Using Rewrite to Remove Header Information

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Switch to the NS_VPX_0 command-line interface and log on using the nsroot credentials if necessary.
2. Add the rw_act_RemoveSrvID rewrite action to remove the Server ID from the header using the following command:

```
add rewrite action rw_act_RemoveSrvID delete_http_header
Server
```

3. Add the res_pol_RemoveSrvID rewrite policy to remove the Server ID using the following command:

```
add rewrite policy res_pol_RemoveSrvID 'HTTP.RES.IS_VALID'
rw_act_RemoveSrvID
```

4. Bind the res_pol_RemoveSrvID globally using the following command:

```
bind rewrite global res_pol_RemoveSrvID 10 NEXT
-type RES_OVERRIDE
```

Verifying the Header Information

Use the Win7Client virtual machine logged on as the CitrixAdmin user for this task.

Do not replace the server header with strings or phrases such as "Hack this" or "Try to hack me now." Potential legal implications with such a statement may exist because you could be granting permission to hackers to attempt to violate your security. As always, consult the appropriate security experts within your organization for guidelines and requirements for your environment.

1. Open the HttpFox add-on in the Firefox browser.
   a. Launch the **Firefox** browser.
   b. Select **Tools** > **Web Developer** > **HttpFox** > **Toggle HttpFox**.
      The HttpFox window appears at the bottom of the browser.
   c. Click **Clear** in the HttpFox window.
2. Verify that the Header information for the server is not displayed.

a. Browse to the RBG virtual server by navigating to `http://10.0.0.80`.

b. Select one of the items in the top box which does not say `(cache)` in the HttpFox Result column.

c. View the Header information in the Response header pane.

   Verify the Server does not display.

3. Close the HttpFox window.

Exercise 11-3: Inserting HTTP Header

Overview

This exercise demonstrates how to add a rewrite policy to insert information into the HTTP headers.

Before You Begin

To begin this exercise, ensure the following virtual machines are started:

- AD.training.lab
- NS_VPX_0
- Router_Vyatta
- Web_Blue
- Web_Green
- Web_Red
- Win7Client

Estimated time to complete this exercise: 15 minutes

Exercise 11-3: Step by Step (Configuration Utility)

This section provides step by step instructions for completing "Exercise 11-3: Inserting Server Data" using the configuration utility.

Using Rewrite to Insert Header Information

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Log on to the NetScaler system and add a rewrite action.
   a. Switch to the configuration utility for NS_VPX_0 and log on using the nsroot credentials if necessary.
   b. Navigate to **Rewrite** > **Actions** and click **Add**.
2. Complete the rw_act_NewSrvID rewrite action to insert the string "Unspecified" for the HTTP Server Header value.
   a. Click the Name field and type `rw_act_NewSrvID`.
   b. Select **INSERT_HTTP_HEADER** for the Type.
   c. Click the Header Name field and type `Server`.

d. Click the String expression for Header value field and type "Unspecified".

e. Click **Create**, and then click **Close**.

3. Add the res_pol_NewSrvID rewrite policy using the rw_act_NewSrvID action with an http IS_VALID response.
   a. Select the **Policies** node and click **Add**.
   b. Click the Name field and type res_pol_NewSrvID.
   c. Select **rw_act_NewSrvID** for the Action.
   d. Click the Expression field and type HTTP.RES.IS_VALID.
   e. Click **Create**, and then click **Close**.
4. Bind the rewrite policy res_pol_NewSrvID globally.
   a. Click **Policy Manager**.
   b. Click **Response**, and then click **Override Global** under Bind Points.
   c. Click **Insert Policy** and select **res_pol_NewSrvID** for the Policy Name.
   d. Select **NEXT** for the Goto Expression.
   e. Click **Apply Changes**, and then click **Close**.
5. Add the rw_act_NoCache rewrite action to insert "no-cache" in the cache-control of the HTTP Header.
   a. Select the **Actions** node and click **Add**.
   b. Click the Name field and type rw_act_NoCache.
   c. Select **INSERT_HTTP_HEADER** for the Type.
   d. Click the Header Name field and type Cache-Control, then type "no-cache" in the String expression for Header value field.
   e. Click **Create**, and then click **Close**.
6. Add the res_pol_NoCache rewrite policy using the rw_act_NoCache action.
   a. Click the **Policies** Node and click **Add**.
   b. Click the Name field and type res_pol_NoCache.
   c. Select **rw_act_NoCache** for the Action.
   d. Click the Expression field and type HTTP.RES.IS_VALID.
   e. Click **Create**, and then click **Close**.
7. Bind the res_pol_NoCache policy globally.
   a. Click **Policy Manager**.
   b. Click **Response**, and then click **Override Global** under Bind Points.
   c. Click **Insert Policy** and select **res_pol_NoCache** for the Policy Name.
   d. Select **NEXT** for the Goto Expression.
   e. Click **Apply Changes**, and then click **Close**.

Verifying the Header Information

Use the Win7Client virtual machine logged on as the CitrixAdmin user for this task.

Do not replace the server header with strings or phrases such as "Hack this" or "Try to hack me now." Potential legal implications with such a statement may exist because you could be granting permission to hackers to attempt to violate your security. As always, consult the appropriate security experts within your organization for guidelines and requirements for your environment.

1. Open the HttpFox add-on in the Firefox browser.
   a. Launch the **Firefox** browser.
   b. Select **Tools** > **Web Developer** > **HttpFox** > **Toggle HttpFox**.
      The HttpFox window appears at the bottom of the browser.
   c. Click **Clear** in the HttpFox window.
2. Browse to the RBG server and verify that the Server header shows "Unspecified" and that the Cache-control header shows "no-cache".
   a. Browse to the RBG virtual server at `http://10.0.0.80`.
   b. Select one of the items in the top box of the HttpFox window that does not say `(cache)` in the HttpFox Result column.
   c. View the Header information in the Response header pane.
      The Server header value should display "Unspecified" and the Cache-Control header value displays "no-cache".
3. Close the HttpFox window.

Exercise 11-3: Step by Step (Command-line Interface)

This section provides step by step instructions for completing "Exercise 11-3: Inserting HTTP Header" using the command-line interface.

Using Rewrite to Insert Header Information

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Add the rw_act_NewSrvID rewrite action to insert the HTTP header "Unspecified" for the Server value using the following command:

```
add rewrite action rw_act_NewSrvID insert_http_header
"Server" "\"Unspecified\""
```

2. Add the res_pol_NewSrvID rewrite policy using the rw_act_NewSrvID action using the following command:

```
add rewrite policy res_pol_NewSrvID 'HTTP.RES.IS_VALID'
rw_act_NewSrvID
```

3. Bind the rewrite policy res_pol_NewSrvID globally using the following command:

```
bind rewrite global res_pol_NewSrvID 20 NEXT -type RES_OVERRIDE
```

4. Add the rw_act_NoCache rewrite action to insert the string “no-cache” in the cache-control of the HTTP Header using the following command:

```
add rewrite action rw_act_NoCache insert_http_header
"Cache-Control" "\"no-cache\""
```

5. Add the res_pol_NoCache rewrite policy using the rw_act_NoCache action using the following command:

```
add rewrite policy res_pol_NoCache 'HTTP.RES.IS_VALID'
rw_act_NoCache
```

6. Bind the res_pol_NoCache policy globally using the following command:

```
bind rewrite global res_pol_NoCache 30 NEXT -type RES_OVERRIDE
```

Verifying the Header Information

Use the Win7Client virtual machine logged on as the CitrixAdmin user for this task.

Do not replace the server header with strings or phrases such as "Hack this" or "Try to hack me now." Potential legal implications with such a statement may exist because you could be granting permission to hackers to attempt to violate your security. As always, consult the appropriate security experts within your organization for guidelines and requirements for your environment.

1. Open the HttpFox add-on in the Firefox browser.
   a. Launch the **Firefox** browser.
   b. Select **Tools** > **Web Developer** > **HttpFox** > **Toggle HttpFox**.
      The HttpFox window appears at the bottom of the browser.
   c. Click **Clear** in the HttpFox window.
2. Browse to the RBG server and verify that the Server header shows "Unspecified" and that the Cache-control header shows "no-cache".

a. Browse to the RBG virtual server at `http://10.0.0.80`.

b. Select one of the items in the top box of the HttpFox window that does not say `(cache)` in the HttpFox Result column.

c. View the Header information in the Response header pane.

   The Server header value should display "Unspecified" and the Cache-Control header value displays "no-cache".

3. Close the HttpFox window.

Exercise 11-4: Configuring Responder

Scenario

This exercise will demonstrate how to create a responder policy that will redirect an unspecified URL request to a specified page, such as /home.php.

Before You Begin

To begin this exercise, ensure that the following virtual machines are started:

- AD.training.lab
- NS_VPX_0
- Router_Vyatta
- Web_Blue
- Web_Green
- Web_Red
- Win7Client

Estimated time to complete this exercise: 10 minutes

Exercise 11-4: Step by Step (Configuration Utility)

This section provides step by step instructions for completing "Exercise 11-4: Configuring Responder" using the configuration utility.

Enabling the Responder Feature

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Switch to the configuration utility for NS_VPX_0 and log on using the nsroot credentials if necessary.
2. Enable the responder feature.
   a. Navigate to **System** > **Settings**.
   b. Click **Configure Advanced Features**.
   c. Select **Responder** and click **OK**.
   d. Click **Save** to save the configuration and then click **Yes** to confirm.

Using Responder to Modify a URL

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Add the rs_act_RedirectToHome responder action that redirects requests to the home.php page.
   a. Navigate to **Responder** > **Actions** and click **Add**.
   b. Click the Name field and type `rs_act_RedirectToHome`.
   c. Select **Redirect** for the Type.
   d. Click the Target field and type `"/home.php"`.
   e. Click **Create**, and then click **Close**.
2. Add the rs_pol_RedirectToHome responder policy using the rs_act_RedirectToHome action that matches any URL ending with a forward slash (/).
   a. Click the **Policies** node and click **Add**.
   b. Click the Name field and type **rs_pol_RedirectToHome**.
   c. Select **rs_act_RedirectToHome** for the Action.
   d. Click the Expression field and type `HTTP.REQ.URL.PATH.EQ("/").`
   e. Click **Create**, and then click **Close**.
3. Bind the rs_pol_RedirectToHome policy globally.
   a. Click **Policy Manager**.
   b. Select **Default Global** under Bind Points.
   c. Click **Insert Policy** and select **rs_pol_RedirectToHome** for the Policy Name.
   d. Select **END** for the Goto Expression.
   e. Click **Apply Changes**, and then click **Close**.
4. Click **Save** to save the configuration changes.

Testing the Responder Policy

Use the Win7Client virtual machine logged on as the CitrixAdmin user for this task.

1. Browse to the RBG virtual server and verify that "/home.php" is appended to the URL.
   a. Switch to the FireFox broswer.
   b. Browse to `http://10.0.0.80/`.

      The RBG home page is displayed and home.php is appended to the URL.

      If the responder policy is disabled but the rewrite policy is still enabled, then users will still successfully reach the home.php page due to the rewrite request policy.

Responder actions occur before URL rewrite actions. RespondWith actions bypass NetScaler processing.

Exercise 11-4: Step by Step (Command-line Interface)

This section provides step by step instructions for completing "Exercise 11-4: Configuring Responder" using the command-line interface.

Enabling the Responder Feature

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Switch to the NS_VPX_0 command-line interface and log on using the nsroot credentials if necessary.
2. Enable the responder feature using the following command.

```
enable ns feature responder
```

3. Save the configuration using the following command.

```
save ns config
```

```
y
```

Using Responder to Modify a URL

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Add the rs_act_RedirectToHome responder action that redirects to home.php using the following command:

```
add responder action rs_act_RedirectToHome redirect
"\"/home.php\""
```

2. Add the rs_pol_RedirectToHome responder policy using the rs_act_RedirectToHome action using the following command:

```
add responder policy rs_pol_RedirectToHome
'HTTP.REQ.URL.PATH.EQ("/")' rs_act_RedirectToHome
```

3. Bind the rs_pol_RedirectToHome policy globally using the following command:

```
bind responder global rs_pol_RedirectToHome 10 END
-type Default
```

4. Save the NetScaler configuration using the following command:

```
save ns config
```

Testing the Responder Policy

Use the Win7Client virtual machine logged on as the CitrixAdmin user for this task.

1. Browse to the RBG virtual server and verify that "/home.php" is appended to the URL.
   a. Switch to the FireFox broswer.
   b. Browse to `http://10.0.0.80/`.

      The RBG home page is displayed and home.php is appended to the URL.

      If the responder policy is disabled but the rewrite policy is still enabled, then users will still successfully reach the home.php page due to the rewrite request policy.

Responder actions occur before URL rewrite actions. RespondWith actions bypass NetScaler processing.

Exercise 11-5: Adding a Custom Response

Scenario

This exercise demonstrates how to create a custom response to a URL request to a restricted page or directory.

Before You Begin

To begin this exercise, ensure the following virtual machines are started:

- AD.training.lab
- NS_VPX_0
- Router_Vyatta
- Web_Blue
- Web_Green
- Web_Red
- Win7Client

Estimated time to complete this exercise: 10 minutes

Exercise 11-5: Step by Step (Configuration Utility)

This section provides step by step instructions for completing "Exercise 7-5: Adding a Custom Response" using the configuration utility.

Using Responder to Display a Custom Response

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Switch to the configuration utility for NS_VPX_0.
2. Add a "rs_act_RespondWithCustom" custom responder action.
   a. Navigate to **Responder** > **Actions** and click **Add**.
   b. Click the Name field and type `rs_act_RespondWithCustom`.
   c. Select **Respond with** for the Type.
   d. Click the Target field and type the following text:

```
"http/1.1 200 OK\r\n\r\n" + "Client: " + CLIENT.IP.SRC
+ " is not authorized to access URL: "
+ HTTP.REQ.URL.HTTP_URL_SAFE
```

e. Click **Create**, and then click **Close**.

3. Add the rs_pol_RespondWithCustom responder policy using the rs_act_RespondWithCustom action for any URL that contains "private."
   a. Click the **Policies** node and click **Add**.
   b. Type `rs_pol_RespondWithCustom` in the Name field.
   c. Select **rs_act_RespondWithCustom** for the Action.
   d. Type `HTTP.REQ.URL.PATH.Contains("private")` in the Expression field.
   e. Click **Create**, and then click **Close**.
4. Bind the rs_pol_RespondWithCustom policy globally.
   a. Click **Policy Manager**.
   b. Select **Default Global** under Bind Points.
   c. Click **Insert Policy** and select **rs_pol_RespondWithCustom** for the Policy Name.
   d. Select **END** for the Goto Expression.
   e. Click **Apply Changes**, then click **Close**.
5. Save and confirm the configuration changes.

Testing the Responder Policy

Use the Win7Client virtual machine logged on as the CitrixAdmin user for this task.

1. Browse to `http://10.0.0.80/private` to test the responder policy.
   An attempt to browse to /private results in the NetScaler system returning the custom response text. The “not authorized” message configured appears in the policy action.
2. Use the HttpFox add-on to verify that the proper response code was generated.
   a. Select **Tools** > **Web Developer** > **HttpFox** > **Toggle HttpFox** .
   b. Refresh the page and verify that the HTTP response code HTTP/1.x 200 OK was properly generated.

      This responder value indicates a successful response to the client browser.
   c. Browse to `http://10.0.0.80/`.

      The page loads as expected. The previously configured responder policy allows redirection to home.php for a successful page load.
3. Close the HttpFox window.

Exercise 11-5: Step by Step (Command-line Interface)

This section provides step by step instructions for completing "Exercise 11-5: Adding a Custom Response" using the command-line interface.

Using Responder to Display a Custom Response

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Switch to the command-line interface at 10.0.0.100 and log on using the nsroot credentials if necessary.
2. Add the rs_act_RespondWithCustom custom responder action for unauthorized requests using the following command:

```
add responder action rs_act_RespondWithCustom respondwith
q{"http/1.1 200 OK\r\n\r\n" + "Client: "
+ CLIENT.IP.SRC + " is not authorized to access URL: "
+ HTTP.REQ.URL.HTTP_URL_SAFE}
```

3. Add the rs_pol_RespondWithCustom responder policy for requests in the URL that contains "private" using the following command:

```
add responder policy rs_pol_RespondWithCustom
'HTTP.REQ.URL.PATH.Contains("private")'
rs_act_RespondWithCustom
```

4. Bind the rs_pol_RespondWithCustom policy globally using the following command:

```
bind responder global rs_pol_RespondWithCustom 20 END
-type Default
```

5. Save the NetScaler configuration using the following command:

```
save ns config
```

Testing the Responder Policy

Use the Win7Client virtual machine logged on as the CitrixAdmin user for this task.

1. Browse to `http://10.0.0.80/private` to test the responder policy.
   An attempt to browse to /private results in the NetScaler system returning the custom response text. The “not authorized” message configured appears in the policy action.
2. Use the HttpFox add-on to verify that the proper response code was generated.

a. Select **Tools** > **Web Developer** > **HttpFox** > **Toggle HttpFox** .

b. Refresh the page and verify that the HTTP response code HTTP/1.x 200 OK was properly generated.

   This responder value indicates a successful response to the client browser.

c. Browse to `http://10.0.0.80/`.

   The page loads as expected. The previously configured responder policy allows redirection to home.php for a successful page load.

3. Close the HttpFox window.

Exercise 11-6: Adding URL Transforms

Scenario

This exercise demonstrates how to transfom URL requests to expired web pages into URLs of current pages.

Before You Begin

To begin this exercise, ensure the following virtual machines are started:

- AD.training.lab
- NS_VPX_0
- Router_Vyatta
- Web_Blue
- Web_Green
- Web_Red
- Win7Client

Estimated time to complete this exercise: 15 minutes

Exercise 11-6: Step by Step (Configuration Utility)

This section provides step by step instructions for completing "Exercise 11-6: Adding URL Transforms" using the configuration utility.

Previewing Pages for URL Transformation

Use the Win7Client virtual machine logged on as the CitrixAdmin user for this task.

1. Open a Firefox browser and browse to `http://10.0.0.80/dist_red.php`.
   Expected Result: The dist_red.php page should display normally (Japan). The dist_blue.php (US) and dist_green.php (Germany) pages may be tested as well.
2. Browse to `http://10.0.0.80/international_red.php`.

   You will receive a Server Error 404 - File or directory not found.

Using Responder to Transform URLs

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Switch to the configuration utility for NS_VPX_0 and log on using the nsroot credentials if necessary.
2. Add the trns_remote_URL transform profile to transform requests for "/dist_page.php" into "/internationald_page.php".
   a. Navigate to **Rewrite > URL Transformation > Profiles**.
   b. Click **Add**.
   c. Type `trns_remote_URL` in the Name field.
   d. Type the following text in the Comments field.

```
"Transform /dist_page.php (actual) to
/international_page.php (display)"
```

   e. Click **Create**, and then click **Close**.
3. Add the act_trns_DistToInt transform action to the trns_remote_URL profile with a priority of 50.
   a. Select the trns_remote_URL profile and click **Open**.
   b. Click **Add** to add an action.
   c. Click the Name field and type **act_trns_DistToInt**.
   d. Click the Priority field and type **50**.
   e. Select **Enabled**.
4. Set the actions for the act_trns_DistToInt transform to change requests for "/dist*" into "/international*".
   a. Click the Request URL From field and tyype the following text:

```
http://10.0.0.80/international_(.*)
```

   b. Click the Request URL Into field and type the following text:

```
http://10.0.0.80/dist_$1
```

   c. Click the Response URL From field and type the following text:

```
http://10.0.0.80/dist_(.*)
```

   d. Click the Response URL Into field and type the following text:

```
http://10.0.0.80/international_$1
```

   e. Click **Create**, and then click **Close**.
5. Create a transform policy by entering the following command:
   a. Navigate to **Rewrite > URL Transformation > Policies** and click **Add**.
   b. Click the Name field and type `trns_pol_remote`in the Name field.

c. Select **trns_remote_URL** for the profile.
d. Click the the Expression field and type `TRUE`.
e. Click **Create**, and then click **Close**.

6. Bind the trns_pol_Remote policy globally.
   a. Click **Policy Manager**.
   b. Select **Override Global** under Bind Points.
   c. Click **Insert Policy** and select **trns_pol_remote** for the Policy name.
   d. Click **Apply Changes**, then click **Close**.
7. Save and confirm the configuration changes.

Testing the URL Transform Policy

Use the Win7Client virtual machine logged on as the CitrixAdmin user for this task.

1. Open the Firefox browser and browse to `http://10.0.0.80/dist_red.php`.
   Expected Result: The dist_red.php page should display normally (Japan). The dist_blue.php (US) and dist_green.php (Germany) pages may be tested as well.
2. Browse to `http://10.0.0.80/international_red.php`.

   The same page loads as expected.

   The URL displays "international_red.php," but the content that is loading is the "dist_red.php" page.

   The server request is load-balanced and accesses the alternate pages international_blue.php and international_green.php, resulting in the dist_blue.php and dist_green.php content, respectively.

Exercise 11-6: Step by Step (Command-line Interface)

This section provides step by step instructions for completing "Exercise 11-6: Adding URL Transforms" using the command-line interface.

Previewing Pages for URL Transformation

Use the Win7Client virtual machine logged on as the CitrixAdmin user for this task.

1. Open a Firefox browser and browse to `http://10.0.0.80/dist_red.php`.
   Expected Result: The dist_red.php page should display normally (Japan). The dist_blue.php (US) and dist_green.php (Germany) pages may be tested as well.
2. Browse to `http://10.0.0.80/international_red.php`.

   You will receive a Server Error 404 - File or directory not found.

Using Responder to Transform URLs

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Switch to the command-line interface for NS_VPX_0 and log on using the nsroot credentials if necessary.
2. Add the trns_remote_URL transform profile using the following command:

```
add transform profile trns_remote_URL
```

3. Configure the profile comment to display the dist_page.php for requests to international_page.php using the following command:

```
set transform profile trns_remote_URL -type URL
-comment '"Transform /dist_page.php (actual)
to /international_page.php (display)"'
```

4. Add the act_trns_DistToInt transform action using the following command:

```
add transform action act_trns_DistToInt trns_remote_URL 50
```

5. Configure the act_trns_DistToInt transform action to display the dist_page.php for requests to international_page.php using the following command:

```
set transform action act_trns_DistToInt -priority 50
-reqUrlFrom "http://10.0.0.80/international_(.*)"
-reqUrlInto "http://10.0.0.80/dist_$1"
-resUrlFrom "http://10.0.0.80/dist_(.*)"
-resUrlInto "http://10.0.0.80/international_$1"
```

The transform action name is case-sensitive.

6. Create the trns_pol_remote transform policy to use the trns_remote_URL profile using the following command:

```
add transform policy trns_pol_remote TRUE trns_remote_URL
```

7. Bind the trns_pol_Remote policy globally using the following command:

```
bind transform global trns_pol_remote 50
```

8. Save the NetScaler configuration using the following command:

```
save ns config
```

Testing the URL Transform Policy

Use the Win7Client virtual machine logged on as the CitrixAdmin user for this task.

1. Open the Firefox browser and browse to `http://10.0.0.80/dist_red.php`.
   Expected Result: The dist_red.php page should display normally (Japan). The dist_blue.php (US) and dist_green.php (Germany) pages may be tested as well.
2. Browse to `http://10.0.0.80/international_red.php`.

   The same page loads as expected.

   The URL displays "international_red.php," but the content that is loading is the "dist_red.php" page.

   The server request is load-balanced and accesses the alternate pages international_blue.php and international_green.php, resulting in the dist_blue.php and dist_green.php content, respectively.

Module 12

Exercises for Optimizing Traffic

Exercise 12-1: Optimizing Traffic

Scenario

This exercise will demonstrate how to configure an integrated-caching solution for web content.

Before You Begin

To begin this lab, ensure that the following virtual machines are started:

- AD.training.lab
- Router-Vyatta
- NS_VPX_0
- WebBlue
- WebGreen
- WebRed
- Win7client

Information required for this lab:

System	Username	Password
NetScaler	nsroot	nsroot
Windows 7	CitrixAdmin	Password1

Estimated time to complete this exercise: 20 minutes

Exercise 12-1: Step by Step (Configuration Utility)

This section provides step by step instructions for completing "Exercise 12-1: Integrated Caching" using the configuration utility.

Configuring Global Cache Parameters

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Connect to the configuration utility for the NS_VPX_0 virtual machine and log on using the nsroot credentials.

a. Switch to the Win7client virtual machine.
b. Open the Firefox browser and browse to `http://10.0.0.100`.
c. Log on to the configuration utility using the nsroot credentials.

2. Verify the Integrated Caching feature is disabled.
   a. Navigate to **System > Settings**.
   b. Click **Configure basic features**.
   c. Verify that Integrated Caching is not selected.
   d. Click **Close**.

Citrix recommends to first configure the settings for integrated caching before enabling the feature.

3. Change the default global cache parameters for Memory Usage Limit to 512 MB and the Via Header to the string "Served from Cache".
   a. Navigate to **Integrated Caching**.
   b. Click **Change cache settings**.
   c. Click the Memory Usage Limit field and type `512`.
   d. Click the Via Header field and type `Served from Cache`.
   e. Click **OK**.

The default string identifies the NetScaler system and may include version information. In a production environment, you should modify this string and, for security purposes, not identify the specific device type in use.

Configuring Integrated Caching

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Create the cache_cg_colorpage cache content group with the cache duration set to 10 minutes and the cache memory limit set to 10 MB.
   a. Navigate to **Integrated Caching > Content Groups** and click **Add**.
   b. Click the Name field and type `cache_cg_colorpage`.
   c. Click the Expire content after field and type `600`.
   d. Click the **Memory** tab and type `10` in the Maximum memory usage limit field.
   e. Click **Create**.
2. Create a second cache content group named cache_cg_image with cache duration set to 10 minutes and the cache memory limit set to 10 MB.
   a. Click the Name field and type `cache_cg_image`.

b. Click the Expire content after field and type `600`.
c. Click the **Memory** tab and type `10` in the Maximum memory usage limit field.
d. Click **Create**, and then click **Close**.

The two content groups now appear in the Content Groups list.

3. Create the cache_pol_blue cache policy to cache the blue.php page.
   a. Navigate to **Integrated Caching** > **Policies** and click **Add**.
   b. Click the Name field and type `cache_pol_blue`.
   c. Select **CACHE** from the Action drop-down menu.
   d. Select **cache_cg_colorpage** from the Store in Group drop-down menu.
   e. Click the Expression field and type `HTTP.REQ.URL.CONTAINS("blue").`
   f. Click **Create**.
4. Create the cache_pol_image cache policy to cache .png image files.
   a. Click the Name field and type `cache_pol_image`.
   b. Select **CACHE** from the Action drop-down menu.
   c. Select `cache_cg_image` from the Store in Group drop-down menu.
   d. Click the Expression field and type `HTTP.REQ.URL.CONTAINS(".png").`
   e. Click **Create**.
5. Create the cache_pol_nocache cache policy that prevents caching of all other content.
   a. Click the Name field and type `cache_pol_nocache`.
   b. Select NOCACHE for the Action.
   c. Click the Expression field and type `TRUE`.
   d. Click **Create**, and then click **Close**.

   The three policies now appear in the Policies list.
6. Bind the cache_pol_image policy globally.
   a. Click **Policy Manager**.
   b. Select **Request**, then select **Default Global**.
   c. Click **Insert Policy**.
   d. Click the Priority field and type `80`.
   e. Select `cache_pol_image` for the Policy Name.
   f. Select `END` for the Goto Expression.
7. Bind the cache_pol_blue policy globally.
   a. Click **Insert Policy**.
   b. Click the Priority field and type `90`.
   c. Select `cache_pol_blue` for the Policy Name.
   d. Select `END` for the Goto Expression.
8. Bind the cache_pol_nocache policy globally and save the changes.

a. Click **Insert Policy**.
b. Click the Priority field and type `100`.
c. Select `cache_pol_nocache` for the Policy Name.
d. Select `END` for the Goto Expression.
e. Click **Apply Changes**, then click **Close**.

9. Enable the Integrated Caching feature for the NetScaler.
   a. Navigate to **System** > **Settings**.
   b. Click **Configure basic features**.
   c. Select **Integrated Caching** and click **OK**.

The feature is enabled after configuration to prevent ongoing traffic from being cached mid-configuration.

Configuring Invalidation Cache Policies

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Create the cache_pol_invalcolor invalidation cache policy for URLs containing "red".
   a. Navigate to **Integrated Caching** > **Policies** and click **Add**.
   b. Click the Name field and type `cache_pol_invalcolor`.
   c. Select **INVAL** for the Action.
   d. Click the Expression field and type `HTTP.REQ.URL.CONTAINS("red")`.
   e. Select **cache_cg_colorpage** from the Invalidate all objects in the following groups list and click **Add**.
   f. Click **Create**, and then click **Close**.
2. Bind the cache_pol_invalcolor cache policy globally.
   a. Click **Policy Manager**.
   b. Select **Request**, then select **Default Global**.
   c. Click Insert and select **cache_pol_invalcolor** for the Policy Name.
   d. Click the Priority field and type `70`.
   e. Select **END** for the Goto Expression.
   f. Click **Apply Changes**, then click **Close**.

Testing the Caching Configuration

Use the Win7client virtual machine logged on as the CitrixAdmin user for this task.

1. Launch the Firefox browser and browse to `http://10.0.0.80/green.php` to verify initial load balancing behavior.

   Refresh the browser several times.
   Expected Result: The Green.php page loads. Since none of the caching policies will match this URL, the page should load balance between the Red, Green, and Blue Servers. The page background and server information section (lower half) will load balance between the RBG servers.
2. Browse to `http://10.0.0.80/blue.php`. Refresh the browser several times.
   Expected result: After the first page loads, subsequent requests are served from cache; the page background color (which indicates the host server) does not change.
3. View header information using the HttpFox add-on in the Firefox browser.
   a. Click **Tools** > **Web Developer** > **HttpFox** > **Toggle HttpFox**.
   b. Select the entry with the 304 Result code.

      The Via Response Header should display the string configured on the NetScaler system.
   c. Close the HttpFox window.
4. Switch to the configuration utility for NS_VPX_0 and view the cached objects.
   a. Navigate to **Integrated Caching**.
   b. Click **Cache Objects**.
5. Switch to the Firefox browser and browse to `http://10.0.0.80/media.php` and download the image several times.
   Expected result: After the image loads the first time, subsequent requests are served from cache.
6. Switch to the configuration utility for NS_VPX_0 and navigate to **Integrated Caching** and click **Cache Objects** to view the cached objects.
   The file media_main.png is now cached.
7. Navigate to **Integrated Caching** > **Policies** to view the cache policies.
   The details are displayed for all cache policies. Note the values of hits for each cache policy.

Testing the Caching Configuration with Invalidation

Use the Win7Client virtual machine logged on as the CitrixAdmin user for this task.

1. Open a URL that contains "red" by browsing to `http://10.0.0.80/red.php`.
   Red.php matches the cache_inval_color invalidation cache policy.
2. Switch to the configuration utility for NS_VPX_0 and view the cached objects.
   a. Navigate to **Integrated Caching**.
   b. Click **Cache Objects**.

   Blue.php should be listed as cached within the cache_cg_colorpage content group but red.php is not.
3. Navigate to **Integrated Caching** > **Policies** to view the cache policies.
   The details are displayed for all cache policies. Note the values of hits for each cache policy.

Exercise 12-1: Step by Step (Command-line Interface)

This section provides step by step instructions for completing "Exercise 12-1: Integrated Caching" using the command-line interface.

Configuring Global Cache Parameters

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Connect to the command-line interface NS_VPX_0 and log on using the nsroot credentials.
2. Verify the Integrated Caching feature is disabled using the following command:

```
show ns feature
```

During this exercise, warnings that the integrated caching feature is disabled will be displayed as various integrated cache settings are configured. This feature may be configured without it being enabled. The warnings within the command-line interface will remind you to enable the feature before testing.

Citrix recommends to first configure the settings for integrated caching before enabling the feature.

3. Set the caching global parameter for cache size to 512 MB using the following command:

```
set cache parameter -memLimit 512
```

4. Set the caching global parameter for the VIA string to "Served from Cache" using the following command:

```
set cache parameter -via "Served from Cache"
```

This string is used to identify cached content served by the NetScaler system.

The default string identifies the system as a NetScaler system and may include version information. In a production environment, you should modify this string and, for security purposes, not identify the specific device type in use.

Configuring Integrated Caching

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Create the named cache_cg_colorpage cache content group with the cache duration set to 10 minutes and the cache memory limit set to 10 MB.


```
add cache contentGroup cache_cg_colorpage -relExpiry 600
-memLimit 10
```

2. Create the cache blue.php page cache policy to the cache_cg_colorpage content group.

```
add cache policy cache_pol_blue
-rule 'HTTP.REQ.URL.CONTAINS("blue")' -action CACHE
-storeInGroup cache_cg_colorpage
```

3. Create the cache_cg_image content group with cache duration set to 10 minutes and the cache memory limit set to 10 MB.

```
add cache contentGroup cache_cg_image -relExpiry 600
-memLimit 10
```

4. Create the cache_pol_image cache policy to cache .png files to the cache_cg_image content group.

```
add cache policy cache_pol_image
-rule 'HTTP.REQ.URL.CONTAINS(".png")' -action CACHE
-storeInGroup cache_cg_image
```

5. Create the cache_pol_nocache cache policy to prevent caching of all content.

```
add cache policy cache_pol_nocache -rule true -action NOCACHE
```

6. Bind the cache policies globally.

```
bind cache global cache_pol_image -priority 80
-gotoPriorityExpression END -type REQ_DEFAULT
```

```
bind cache global cache_pol_blue -priority 90
-gotoPriorityExpression END -type REQ_DEFAULT
```

```
bind cache global cache_pol_nocache -priority 100
-gotoPriorityExpression END -type REQ_DEFAULT
```

The cache_pol_blue policy is bound with a higher priority than the cache_pol_nocache policy.

7. Enable the Integrated Caching feature.

```
enable ns feature IC
```

The feature is enabled after configuration to prevent ongoing traffic from being cached mid-configuration.

Configuring Invalidation Cache Policies

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Create the cache_pol_invalcolor invalidation cache policy to use the cache_cg_colorpage cache group for the red.php page using the following command:

```
add cache policy cache_pol_invalcolor
-rule 'HTTP.REQ.URL.CONTAINS("red")' -action INVAL
-invalGroups cache_cg_colorpage
```

2. Bind the cache policy globally using the following command:

```
bind cache global cache_pol_invalcolor -priority 70
-gotoPriorityExpression END -type REQ_DEFAULT
```

Testing the Caching Configuration

Use the Win7Client virtual machine logged on as the CitrixAdmin user for this task.

1. Launch the Firefox browser and browse to `http://10.0.0.80/green.php` to verify initial load balancing behavior.

   Refresh the browser several times.
   Expected Result: The Green.php page loads. Since none of the caching policies will match this URL, the page should load balance between the Red, Green, and Blue Servers. The page background and server information section (lower half) will load balance between the RBG servers.
2. Browse to `http://10.0.0.80/blue.php`. Refresh the browser several times.
   Expected result: After the first page loads, subsequent requests are served from cache; the page background color (which indicates the host server) does not change.
3. View header information in the HttpFox add-on in the Firefox browser.
   a. Click **Tools > Web Developer > HttpFox > Toggle HttpFox**.
   b. Select the entry with the 304 Result code.

      The Via Response Header should dislpay the string configured on the NetScaler system.
   c. Close the HttpFox window.
4. View the cached objects using the following command:


```
show cache objects
```

5. View the content groups using the following command:

```
show cache contentgroup cache_cg_colorpage
```

6. Browse to `http://10.0.0.80/media.php`. Download the image several times.
   Expected result: After the image loads the first time, subsequent requests are served from cache.
7. View the contents of cache on the NetScaler system using the following command:

```
show cache object
```

8. View the cache policy using the following command:

```
show cache policy
```

   The details are displayed for all cache policies. Note the values of hits for each cache policy.

Testing the Caching Configuration with Invalidation

Use the Win7Client virtual machine logged on as the CitrixAdmin user for this task.

1. Browse to `http://10.0.0.80/red.php`.
   Red.php matches the invalidation cache policy (cache_inval_color).
2. View the cache objects using the following command:

```
show cache object | grep cache_cg_colorpage
```

   Blue.php should be listed as cached within the cache_cg_colorpage content group but red.php is not.
3. View the cache policy using the following command:

```
show cache policy
```

   The details are displayed for all cache policies. Note the Hit values for each cache policy.

Exercise 12-2: Configuring SQL Database Caching

Scenario

This exercise will demonstrate how to configure a caching solution for SQL queries.

Before You Begin

To begin this lab, ensure that the following virtual machines are started:

- AD.training.lab
- Router-Vyatta
- NS_VPX_0
- LAMP_1
- LAMP_2
- Win7client

Information required for this lab:

System	Username	Password
NetScaler	nsroot	nsroot
Windows 7	CitrixAdmin	Password1
Linux	root	Password1
MySQL	netscalersql	netscaler
MySQL	root	Password1

Estimated time to complete this exercise: 15 minutes.

Exercise 12-2: Step by Step (Configuration Utility)

This section provides step by step instructions for completing "Exercise 12-2: Configuring SQL Database Caching" using the configuration utility.

SQL Caching

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

Ensure that the LAMP_1 and LAMP_2 virtual machines are started and that the LAMP_3 virtual machine is shut down before beginning this lab.

1. Switch to the configuration utility for NS_VPX_0 at http://10.0.0.100 and log on using the nsroot credentials if necessary.
2. Add the netscalersql database user.
   a. Navigate to **System > Database Users** and click **Add**.
   b. Click the User Name field and type `netscalersql`.
   c. Click the Password field and type `netscaler`.
   d. Click the Confirm Password field and type `netscaler`.
   e. Click **Create** and then click **Close**.
3. Create the LAMP_1 virtual server with the IP address 192.168.10.13.
   a. Navigate to **Load Balancing > Servers** and click **Add**.
   b. Click the Server Name field and type `LAMP_1`.
   c. Click the IP Address field and type `192.168.10.13`.
   d. Click **Create** and then click **Close**.
4. Create the LAMP_1_MYSQL_3306 service for the LAMP_1 server using MYSQL as the protocol and 3306 as the port.
   a. Navigate to **Load Balancing > Services** and click **Add**.
   b. Click the Service Name field and type `LAMP_1_MYSQL_3306`.
   c. Select **LAMP_1** from the Server drop-down menu.
   d. Select **MYSQL** from the Protocol drop-down menu.
   e. Click the Port field and type `3306`.
   f. Click **Create** and then click **Close**.
5. Create the MYSQL_vsvr virtual server with the IP address 10.0.0.18 on port 3306.
   a. Navigate to **Load Balancing > Virtual Servers** and click **Add**.
   b. Click the Name field and type `MYSQL_vsvr`.
   c. Select **MYSQL** from the Protocol drop-down menu.
   d. Click the IP Address field and type `10.0.0.18`.
   e. Click the Port field and type `3306`.
6. Bind the LAMP_1_MYSQL_3306 service to the virtual load-balancing server.

To simplify the configuration, only one service will be bound to the virtual server.

a. Select the **LAMP_1_MYSQL_3306** service.

b. Click **Create** and then click **Close**.

7. Log on to the LAMP_2 virtual machine and open a MySQL session to the IMDB database. Show the available tables to verify connectivity.

   a. Switch to the XenCenter console and select the LAMP_2 virtual machine.

   b. Click the **Console** tab and log on to the LAMP_2 server using the root credentials.

   c. Open a MySQL session to the IMDB database and log on as the netscalersql user using the following command:

   ```
   mysql -h 10.0.0.18 -u netscalersql -p -D imdb
   ```

   d. Type "netscaler" for the password when prompted.

   ```
   netscaler
   ```

   e. Show the available database table information using the following command:

   ```
   show tables;
   ```

   A list of the tables in the IMDB database is displayed.

8. Execute a CPU-intensive query on the IMDB database using a query file.

   a. Execute a query that identifies movies where directors also performed as actors using the following command:

   ```
   source query.sql;
   ```

   b. Note the query execution time.

9. Switch to the configuration utility for NS_VPX_0 and create the cache_cg_mysql content group that retains content for 10 minutes.

   a. Navigate to **Integrated Caching > Content Groups** and click **Add**.

   b. Click the Name field and type `cache_cg_mysql`.

   c. Select **MYSQL** from the Type drop-down menu.

   d. Click the Expire content after field and type `600`.

10. Configure the content group with a minimum response size of 500 MB and a maximum of 1024 MB.

    a. Click the **Memory** tab and complete the form as follows:

    - Do not cache, if size is less than: `500`
    - Do not cache, if size exceeds: `1024`

b. Click **Create** and then click **Close**.

11. Create a cache policy "cache_select_queries" for SELECT statements with a CACHE action.
    a. Navigate to **Integrated Caching > Policies** and click **Add**.
    b. Click the Name field and type `cache_select_queries`.
    c. Select **CACHE** from the Action drop-down menu.
    d. Select **cache_cg_mysql** from the Store in Group drop-down menu.
    e. Click the Expression field and type `MYSQL.REQ.QUERY.COMMAND.CONTAINS("select").`
    f. Click **Create**, and then click **Close**.
12. Define a HIT selector "cache_selector1" that matches against SQL query text. Add the "cache_selector1" selector to the MYSQL content group hit selector list.
    a. Navigate to **Integrated Caching > Cache Selectors** and click **Add**.
    b. Click the Name field and type `cache_selector1`.
    c. Click the Expressions field and type `MYSQL.REQ.QUERY.TEXT`.
    d. Click **Add** next to the Expressions field.
    e. Click **Create**, and then click **Close**.
13. Add the HIT selector to the cache_cg_mysql content group hit selector list.
    a. Navigate to **Integrated Caching > Content Groups**.
    b. Select the **cache_cg_mysql** content group and click **Open**.
    c. Cick the **Parameterization** tab.
    d. Select **cache_selector1** from the Hit selector list.
    e. Click **OK**.
14. Open the MYSQL_vsrv virtual server.
    a. Navigate to **Load Balancing > Virtual Servers**.
    b. Select the **MYSQL_vsrv** virtual server and click **Open**.
15. Bind the cache_select_queries policy to the MYSQL_vsvr.
    a. Click the **Policies** tab.
    b. Click **Cache (Request)**.
    c. Click Insert Policy and select `cache_select_queries` for the Policy Name.
    d. Click the Priority field and type `100`.
    e. Click **OK**.
16. Verify that the cache_cg_mysql content group does not contain cached objects.
    a. Navigate to **Integrated Caching > Cache Objects**.
    b. Select **cache_cg_mysql** from the Content Group Name list.
    c. Click **Go** at the right side of the Cache Objects pane.
    There should be no cached objects for this content group.

17. Switch to the MySQL session on LAMP_2 and execute the last database query again. Allow the query to complete. Note the query execution time.
    a. Run the query using the following command.

    ```
    source query.sql;
    ```

    b. Note the query execution time once the query is complete.

    The query execution time should be similar to the previous query.
18. Switch to the configuration utility for NS_VPX_0 and view the cached objects. Verify the resultant set has been cached.
    a. Navigate to **Integrated Caching > Cache Objects**.
    b. Click **Refresh** in the Cache Objects pane.

    A cached object appears for the cache_cg_mysql content group.
19. Switch to the MySQL session on LAMP_2 and execute the last database query again. Note the query execution time.
    a. Run the query using the following command.

    ```
    source query.sql;
    ```

    b. Note the query execution time.

    The result of the query is called from cache, significantly reducing the execution time.

Caching Modified Data

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Switch to the configuration utility for NS_VPX_0. Modify the minimum response size to 0 KB to cache all responses.

Avoid setting the content group to response size to 0 KB in a real-world scenario as this caches empty resultant sets.

    a. Navigate to **Integrated Caching > Content Groups**.
    b. Select the **cache_cg_mysql** content group and click **Open**.
    c. Select the **Memory** tab.
    d. Change the value for Do not cache, if size is less than to `0`.
    e. Click **OK**.
2. Execute a MySQL query statement on actors with a "Stooge" last name. This query will be saved in the cache content group.
    a. Switch to the XenCenter console and select the LAMP_2 virtual machine.

b. Open a MySQL session to the MySQL virtual server and log using the netscalersql credentials if necessary using the following command:

```
mysql -h 10.0.0.18 -u netscalersql -p -D imdb
```

```
netscaler
```

c. Execute a query using the following command:

```
select * from actors where actors.last_name = "Stooge";
```

The query returns an empty set.

3. Insert new values for "Larry Stooge" and "Moe Stooge" into the actors table. Execute the basic select statement again and verify that the result is served from cache.

a. Insert new values into the actors table using the following commands:

```
insert into actors values ("999999","Moe","Stooge","M");
```

```
insert into actors values ("999998","Larry","Stooge","M");
```

b. Execute a query using the following command and verify that the resultant set is empty:

```
select * from actors where actors.last_name = "Stooge";
```

The query again returns an empty set since the result was served from cache.

4. Switch to the configuration utility on NS_VPX_0. Create an "invalidate_when_modified" cache policy to identify any modification operation and configure an INVAL action.

a. Navigate to **Integrated Caching** > **Policies** and click **Add**.

b. Click the Name field and type `invalidate_when_modified`.

c. Select **INVAL** from the Action drop-down menu.

d. Click the Expression field and type the following text:

```
MYSQL.REQ.QUERY.COMMAND.CONTAINS("insert")
|| MYSQL.REQ.QUERY.COMMAND.CONTAINS("delete") ||
MYSQL.REQ.QUERY.COMMAND.CONTAINS("alter")
```

5. Invalidate objects from the cache_cg_mysql content group.

a. Select **cache_cg_mysql** from the Invalidate all objects in the following groups list and click **Add**.

b. Click **Create** then click **Close**.

6. Bind the invalidate_when_modified policy to the MYSQL virtual server.

a. Navigate to **Load Balancing** > **Virtual Servers**.

b. Select the **MYSQL_vsvr** virtual server and click **Open**.

c. Click the **Policies** tab and then click **Cache (Request)**.

d. Click **Insert Policy** and select `invalidate_when_modified` from the Policy Name drop-down menu.

e. Click **OK**.

7. Flush the objects from the cache_cg_mysql content group cache.

   a. Navigate to **Integrated Caching > Content Groups**.

   b. Select the **cache_cg_mysql** content group and click **Invalidate**.

   c. Select **Flush** and click **OK**.

8. Execute a MySQL query to select actors with a "Stooge" last name to be cached. Insert a new value for "Curly Stooge" into the actors table. Execute the basic select statement again and verify the result is served from cache.

   a. Switch to the MySQL session on the LAMP_2 virtual machine.

   b. Execute a basic select statement using the following command:

   ```
   select * from actors where actors.last_name = "Stooge";
   ```

   The query returns the two records inserted earlier.

   c. Insert a new value into the actors table using the following command:

   ```
   insert into actors values ("999997","Curly","Stooge","M");
   ```

   d. Execute the basic select statement again using the following command:

   ```
   select * from actors where actors.last_name = "Stooge";
   ```

   The new resultant set is fetched from the back-end server, automatically caching the new data for the next request.

   e. Exit the MySQL session using the following command:

   ```
   exit
   ```

Exercise 12-2: Step by Step (Command-line Interface)

This section provides step-by-step instructions for completing "Exercise 12-2: Configuring SQL Database Caching" using the command-line interface.

SQL Caching

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

Ensure that the LAMP_1 and LAMP_2 virtual machines are started and that the LAMP_3 virtual machine is shut down before beginning this lab.

1. Create the LAMP_1 virtual server with the IP address 192.168.10.13.
   a. Switch to the command-line interface for NS_VPX_0 and log on as the nsroot user if necessary.
   b. Create the MySQL servers using the following command:

```
add server LAMP_1 192.168.10.13
```

2. Create the LAMP_1_MYSQL_3306 service for MYSQL using port 3306 using the following command:

```
add service LAMP_1_MYSQL_3306 LAMP_1 MYSQL 3306
```

3. Create the MYSQL_vsvr virtual server with the IP address 10.0.0.18 using port 3306 and bind the MySQL service to it.
   a. Create the MySQL load balancing virtual server using the following command:

```
add lb vserver MYSQL_vsvr MYSQL 10.0.0.18 3306
```

   b. Bind the LAMP_1_MYSQL_3306 service to MYSQL_vsvr load balancing virtual server using the following command:

```
bind lb vserver MYSQL_vsvr LAMP_1_MYSQL_3306
```

To simplify the configuration, only one service will be bound to the virtual server.

4. Add the netscalersql database user using the following command:

```
add db user netscalersql -password netscaler
```

5. Log on to the LAMP_2 virtual machine and connect to the IMDB database. Show the available tables to verify connectivity.
   a. Double-click the **PuTTY** icon on the Win7Client virtual machine desktop, select LAMP_2 from the Saved Sessions field, and click **Open**.
   b. Log on to the LAMP_2 server using the root credentials.
   c. Open a MySQL session to the IMDB database and log on as the netscalersql user using the following command:

```
mysql -h 10.0.0.18 -u netscalersql -p -D imdb
```

d. Type "netscaler" for the password when prompted.

```
netscaler
```

e. Show the available database table information using the following command:

```
show tables;
```

6. Execute a CPU-intensive query on the IMDB database from a query file.
   a. Switch to the MySQL session on LAMP_2.
   b. Execute a query that identifies movies where directors also performed as actors.

```
source query.sql;
```

   c. Note the query execution time.
7. Switch to the command-line interface for NS_VPX_0 and create the cache_cg_mysql content group with a minimum response size of 500 KB and a maximum of 1024 KB.

```
add cache contentGroup cache_cg_mysql -relExpiry 500
-minResSize 500 -maxResSize 1024 -type MYSQL
```

8. Create the cache_select_queries cache policy for SELECT statements with a CACHE action. Bind the policy to the MYSQL_vserver.
   a. Create a cache policy for SELECT statements using the following command:

```
add cache policy cache_select_queries
-rule "MYSQL.REQ.QUERY.COMMAND.CONTAINS(\"select\")"
-action CACHE -storeInGroup cache_cg_mysql
```

9. Define a HIT selector "cache_selector1" that matches against SQL query text. Add the "cache_selector1" selector to the MYSQL content group hit selector list and bind the "cache_select_queries" policy to the MYSQL_vsvr. Verify the content group does not contain any cached objects.
   a. Define a HIT selector that matches against SQL query text using the following command:

```
add cache selector cache_selector1 MYSQL.REQ.QUERY.TEXT
```

   b. Add the HIT selector to the cache_cg_mysql content group hit selector list using the following command:

```
set contentGroup cache_cg_mysql -hitSelector cache_selector1
```

   c. Bind the cache policy to the MYSQL_vserver using the following command:


```
bind lb vserver MYSQL_vsvr -policyName
cache_select_queries -priority 100 -type REQUEST
```

d. Verify that the cache_cg_mysql content group does not contain cached objects using the following command:

```
show cacheObjects
```

10. Switch to the LAMP_2 session and execute the last database query again. Allow the query to complete. Note the query execution time.
    a. Switch to the MySQL session on LAMP_2 and run the query.

```
source query.sql;
```

    b. Note the query execution time once the query is complete.

    The query execution time should be similar to the previous query.
11. Switch to the NS_VPX_0 session and view the cached objects. Verify the resultant set has been cached.
    a. Switch to the NS_VPX_0 session and view the cached objects using the following command:

```
show cacheObjects
```

    The last executed query is cached in the cache_cg_mysql content group.
12. Switch to the LAMP_2 server and execute the last database query again. Note the query execution time.
    a. Switch to the MySQL session on the LAMP_2 server and run the query.

```
source query.sql;
```

    b. Note the query execution time once the query is complete.

    The resultant set is called from cache, significantly reducing the execution time.
13. Exit the MySQL session using the following command:

```
exit
```

Caching Modified Data

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Switch to the NS_VPX_0 session. View the Relative expiry time defined for cached objects within the MYSQL content group. Modify the minimum response size to 0 KB to cache all responses.

You should avoid setting the content group to response size to 0 KB in a real-world scenario as this caches empty resultant sets.

   a. View the cache_cg_mysql content group configuration using the following command:

```
show contentgroup cache_cg_mysql | grep Minimum
```

   b. Modify the minimum response size to 0 KB using the following command:

```
set contentGroup cache_cg_mysql -minResSize 0
```

2. Switch to the MySQL session on LAMP_2. Execute a basic select statement on actors with a "Stooge" last name. This query will be saved in the cache content group.
   a. Switch to the MySQL session on LAMP_2 and open a MySQL session to the MySQL virtual server using the netscalersql credentials if necessary using the following command:

```
mysql -h 10.0.0.18 -u netscalersql -p -D imdb
```

```
netscaler
```

   b. Execute a query using the following command:

```
select * from actors where actors.last_name = "Stooge";
```

   The query shows an empty set.

3. Insert new values for "Larry Stooge" and "Moe Stooge" into the actors table. Execute the basic select statement again and verify the result is served from cache.
   a. Insert new values into the actors table using the following command:

```
insert into actors values ("999999","Moe","Stooge","M");
```

```
insert into actors values ("999998","Larry","Stooge","M");
```

   b. Execute a select statement and verify that the resultant set is empty using the following command:

```
select * from actors where actors.last_name = "Stooge";
```

   The query again returns an empty set since the result was served from cache.

4. Switch to the command-line session on NS_VPX_0. Create an "invalidate_when_modified" cache policy to identify any modification operation and configure an INVAL action to the objects in the cache_cg_mysql content group.
   a. Switch to the command-line session on NS_VPX_0.
   b. Create an "invalidate_when_modified" cache_policy using the following command:

```
add cache policy invalidate_when_modified
-rule "MYSQL.REQ.QUERY.COMMAND.CONTAINS(\"insert\") ||
MYSQL.REQ.QUERY.COMMAND.CONTAINS(\"delete\") ||
MYSQL.REQ.QUERY.COMMAND.CONTAINS(\"alter\")"
-action INVAL -invalObjects cache_cg_mysql
```

5. Bind the invalidate_when_modified policy to the MYSQL virtual server. Flush the objects from the cache_cg_mysql content group.
   a. Bind the invalidate_when_modified policy to the MYSQL virtual server using the following command:

```
bind lb vserver MYSQL_vserver
-policyName invalidate_when_modified -priority 110
-type REQUEST
```

   b. Flush the objects from the MYSQL cache using the following command:

```
flush contentGroup cache_cg_mysql
```

6. Switch to the command-line session on NS_VPX_0. Execute a basic select statement on actors with a "Stooge" last name to be cached. Insert a new value for "Curly Stooge" into the actors table. Execute the basic select statement again and verify the result is served from cache.
   a. Switch to the command-line session on LAMP_2 and execute a basic query using the following command:

```
select * from actors where actors.last_name = "Stooge";
```

   The query returns the two records inserted earlier.
   b. Insert a new value into the actors table using the following command:

```
insert into actors values ("999997","Curly","Stooge","M");
```

   c. Execute the basic select statement again using the following command:

```
select * from actors where actors.last_name = "Stooge";
```

   The new resultant set is fetched from the backend server, automatically caching the new data for the next request.
   d. Exit the MySQL session using the following command:

```
exit
```


Module 13

Exercises for Monitoring

Exercise 13-1: Auditing and Logging

Overview

This exercise demonstrates how to configure a syslog server and view syslog messages on the NetScaler.

Before You Begin

To begin this lab, ensure that the following virtual machines are started:

- AD.training.lab
- NS_VPX_0
- Router-Vyatta
- Win7Client

Estimated time to complete this exercise: 20 minutes

Exercise 13-1: Step by Step (Configuration Utility)

This exercise provides step-by-step instructions for completing "Exercise 13-1: Auditing and Logging" using the configuration utility.

Configuring the Kiwi Syslog Daemon

Use the Win7Client virtual machine logged on as the CitrixAdmin user for this task.

1. Configure the Kiwi Syslog Daemon for UDP messages on port 514.
   a. Click **Start > All Programs > Kiwi Enterprises > Kiwi Syslog Daemon > Kiwi Syslog Daemon** .

      The Kiwi Syslog Service Manager opens.
   b. Click **File** and select **Setup**.
   c. Expand the **Inputs** node and click **UDP**.
   d. Verify that **Listen for UDP Syslog messages** is selected and that the UDP Port is set to `514`. Leave all other default settings.
   e. Click **OK**.

Creating a Syslog Policy and Syslog Server

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Configure a syslog policy and syslog server using 192.168.10.103 for the IP address.
   a. Switch to the NetScaler configuration utility.
   b. Expand the **System** node, expand the **Auditing** sub-node, then select **Syslog**.
   c. Click **Add**.
   d. Type `Ext_Kiwi` in the Name field.
   e. Click **New**.
   f. Type `Ext_Kiwi` in the Name field and enter `192.168.10.103` in the IP Address field.

Leave the Port field blank as the NetScaler will default to UDP port 514.

   g. Select **All** in the Log Levels field, and verify that Log Facility is set to **LOCAL0**.
   h. Click **Create**.

      This step creates the Ext_Kiwi server object.
   i. Verify that **Ext_Kiwi** is selected in the Server field, click **Create** and then click **Close**.

      This step creates the syslog policy.
2. Bind the syslog policy to the syslog server.
   a. Click **Global Bindings** in the Auditing Policies and Servers pane.
   b. Click **Insert Policy** and select **Ext_Kiwi** from the Policy Name drop-down list, then click **OK**.
   c. Click **Save** in the upper-right corner of the configuration utility to save the running configuration. Click **Yes** to confirm saving the configuration, then click **OK** when successfully saved.

      By saving the running configuration, a syslog audit message is generated. Syslog messages are sent to the Kiwi Syslog Server running on the Win7Client. This message will be searchable in an upcoming task.

Viewing Recent Audit Messages

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. View recent audit messages.
   a. Expand the **System** node, expand the **Auditing** sub-node, and then click **Recent audit messages** in the Auditing pane.

      The Audit Messages dialog box opens.
   b. Select one or more log levels to display and set the number of audit messages to be shown, then click **Refresh**.

      The viewer will update with the specified number of messages for the selected log levels. In most cases, systems in the lab will only have INFORMATIONAL messages to display.

c. Click **Close**.

The Audit Messages dialog box closes.

Viewing Historical Audit Messages

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. View historical audit messages.
   a. Expand the **System** node and then expand the **Auditing** sub-node. Select **Syslog messages** in the Auditing pane.

      The Syslog Viewer dialog box opens.
   b. Click the **Severity** drop-down list or other drop-down lists to sort the log messages.
   c. Select a historical log file from the Log Files list.

Historical log files are maintained by default under /var/log and are in ns.log.#.gz form.

   d. Click **View**.

      The Syslog Viewer updates and displays messages from the historical log.
   e. Enter a search string under Filter Log, then click **Go** to view the search results.

Possible values for search string include: "lb vserver", "ns conf", or enable feature.

   f. Click **Close**.

      The Syslog Viewer dialog box closes.

Viewing Audit Messages on the Remote Syslog Server

Use the Win7Client vitual machine logged on as the CitrixAdmin user for this task.

1. View audit messages on the remote syslog server.
   a. Start the **Kiwi Syslog Daemon**.
   b. The syslog messages from the NetScaler will display in the Display 00 (Default) syslog window.

      The systems in the lab will only have INFORMATIONAL messages to display.

Disabling Syslog Audit Messages

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Disable logging of Syslog Audit Messages to the Kiwi Syslog Server.
   a. Switch to the configuration utility for NS_VPX_0.
   b. Expand the **System** node, then expand the **Auditing** sub-node and select **Syslog**.
   c. Click **Global Bindings** in the Syslog pane.
      The Bind/Unbind Auditing Policies to Global dialog box opens.
   d. Select the **Ext_Kiwi** policy, and click **Unbind Policy**, then click **OK**.
      The Bind/Unbind Auditing Policies to Global dialog box closes.

Exercise 13-1: Step by Step (Command-Line Interface)

This exercise provides step-by-step instructions for completing "Exercise 13-1: Auditing and Logging" using the command-line interface.

Configuring the Kiwi Syslog Daemon

Use the Win7Client virtual machine logged on as the CitrixAdmin user for this task.

1. Configure the Kiwi Syslog Daemon for UDP messages on port 514.
   a. Click **Start > All Programs > Kiwi Enterprises > Kiwi Syslog Daemon > Kiwi Syslog Daemon** .
      The Kiwi Syslog Service Manager opens.
   b. Click **File** and select **Setup**.
   c. Expand the **Inputs** node and click **UDP**.
   d. Verify that **Listen for UDP Syslog messages** is selected and that the UDP Port is set to `514`. Leave all other default settings.
   e. Click **OK**.

Configuring and Viewing the Syslog

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Switch to the configuration utility for NS_VPX_0 and log on using the nsroot credentials.
2. Create a Syslog Server named Ext_Kiwi on the NetScaler system with the IP address 192.168.10.103 on port 514 using the following command:


```
add audit syslogAction Ext_Kiwi 192.168.10.103
-serverPort 514 -loglevel ALL -logFacility LOCAL0 -tcp All
```

3. Create a Syslog Policy named Ext_Kiwi_policy on the NetScaler system.
   a. Add a syslog policy on the NetScaler system:

   ```
   add audit syslogPolicy Ext_Kiwi_policy ns_true Ext_Kiwi
   ```

   b. Bind the audit policy to the system global to enable audit logging:

   ```
   bind system global Ext_Kiwi_policy
   ```

   c. Save the running configuration:

   ```
   save ns config
   ```

4. View recent audit messages.
   a. Show recent audit messages:

   ```
   show audit messages
   ```

   The results will look like the following text:

   ```
   NS_VPX_0> show audit messages

   1) 10/07/2008:22:30:44 GMT edulabvpn1
   Informational : UI CMD_EXECUTED 96357 :  User
   nsroot - Remote_ip 0.0.0.0 - Command "save ns
   config" - Status "Success"

   2) 10/07/2008:22:30:44 GMT edulabvpn1
   Informational : TCP CONN_TERMINATE 96358 :  Source
   192.168.1.3:80 - Destination 192.168.1.21:40284 -
   Start Time 10/07/2008:22:30:44 GMT -
   End Time 10/07/2008:22:30:44 GMT - Total_bytes_send 0
   - Total_bytes_recv 1

   3) 10/07/2008:22:30:45 GMT edulabvpn1
   Informational : TCP CONN_TERMINATE 96359 :  Source
   192.168.1.4:80 - Destination 192.168.1.21:17855 -
   Start Time 10/07/2008:22:30:45 GMT -
   End Time 10/07/2008:22:30:45 GMT - Total_bytes_send 0
   - Total_bytes_recv 1
   ```

Notice the save ns config command that was run in the previous step.

b. Verify syslog audit messages are received by Kiwi Syslog Daemon.

c. Disable syslog audit logging before continuing to next lab exercise using the following command:

```
unbind system global Ext_Kiwi_policy
```

This stops syslog audit messages from being sent from the NetScaler to the SyslogManagerIP.

d. Close the Kiwi Syslog Service Manager.

Exercise 13-2: Monitoring

Scenario

Management would like to know the best way to track bandwidth utilization of the web servers to measure the effectiveness of compression. To do this, you decide to first configure SNMP monitoring on the NetScaler to gather more information.

Before You Begin

To begin this lab, ensure that the following virtual machines are started:

- AD.training.lab
- NS_VPX_0
- Router-Vyatta
- Win7Client

Estimated time to complete this exercise: 20 minutes

Exercise 13-2: Step-by-Step (Configuration Utility)

This section provides step-by-step instructions for completing "Exercise 13-2: Advanced Monitoring" using the configuration utility.

Configuring SNMP Settings (Configuration Utility)

In the Win7Client virtual machine, use an HTTP connection to the NS_VPX_0 configuration utility logged on as the nsroot user for this task.

1. Switch to the configuration utility for NS_VPX_0 at http://10.0.0.100 and log on using the nsroot credentials if necessary.
2. Configure an SNMP manager with a management host of 192.168.20.103.
   a. Navigate to **System** > **SNMP** > **Managers**.
   b. Click **Add** in the SNMP Managers pane.
      The Add SNMP Manager dialog box opens.
   c. Select **Management Host** and type `192.168.10.103` in the IP Address field.
   d. Click **Create** and then click **Close**.
3. Configure a SNMP community named ctxtrainsnmp with permissions set to ALL.
   a. Navigate to **System** > **SNMP** > **Community**.
   b. Click **Add** in the SNMP Community pane.

The Create SNMP Community dialog box opens.

c. Type `ctxtrainsnmp` in the Community String field and select **ALL** from the permission drop-down list.

d. Click **Create** and then click **Close**.

4. Configure a specific SNMPv2 trap for the destination IP address 192.168.10.103. Associate the trap with the ctxtrainsnmp SNMP community.

   a. Navigate to **System > SNMP > Traps** and click **Add** in the SNMP Traps pane.

   The Create SNMP Trap Destination dialog box opens.

   b. Select **Specific** in the Type field and verify that **V2** is selected in the Version field.

   c. Type the SNMP IP `192.168.10.103` in the Destination IP address field and leave the Source IP Address field blank.

The NSIP address is used by default.

   d. Type `ctxtrainsnmp` in the Community Name field.

The community name must match the community string specified when configuring the SNMP community in this lab.

   e. Click **Create**.

5. Configure an SNMP alarm as type CONFIG-SAVE. Verify the alarm is enabled and save the NetScaler configuration.

   a. Navigate to **System > SNMP > Alarms**.

   b. Select the **CONFIG-SAVE** alarm and click **Open**.

   The Configure SNMP Alarm dialog box opens.

   c. Verify **Enabled** is selected and click **OK**.

   The Configure SNMP Alarm dialog box closes.

   d. Click **Save** to save the configuration and trigger an SNMP alert.

Configuring the Kiwi Syslog Daemon and Viewing SNMP Alerts (Configuration Utility)

Use the Win7Client virtual machine logged on as the CitrixAdmin user for this task.

1. Switch to the Win7client virtual machine.
2. Start the Kiwi Syslog Daemon listening for SNMP traps on UDP port 162.

   a. Click **Start > All Programs > Kiwi Enterprises > Kiwi Syslog Daemon > Kiwi Syslog Daemon**.

The Kiwi Syslog Daemon opens.

b. Click **File** and select **Setup**.

c. Expand the **Inputs** node and select **SNMP**.

d. Check **Listen for SNMP Traps** and verify that `162` is entered in the UDP Port field.

3. Prepare the listener for an informational trap from the Syslog Level drop-down menu. Clear any previously captured data and send an SNMP trap.

   a. Select **Info** from the Syslog Level list and click **OK**.

   b. Click **View** and select **Clear display**.

   a. Switch to the NetScaler configuration utility and click **Save** to save the running configuration and send an SNMP trap.

4. View the SNMP traps in the Kiwi Syslog Daemon. The SNMP syslog will resemble the following:

```
12-02-2008 16:22:43 Local7.Info 172.30.108.5
community=ctxtrainsnmp,
enterprise=1.3.6.1.4.1.5951.1.1.0.28,
enterprise_mib_name=netScalerConfigSave,
uptime=508021, agent_ip=172.168.10.103,
version=Ver2, nsUserName.0=nsroot,
sysIpAddress.0=10.0.0.100
```

Exercise 13-2: Step-by-Step (Command-Line-Interface)

This section provides step-by-step instructions for completing "Exercise 13-2: Advanced Monitoring" using the command-line interface.

Configuring SNMP Settings (Command-Line Interface)

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Configure an SMNP manager with a 192.168.10.103 IP address. Create a "ctxtrainsnmp" community with permissions set to ALL.

   a. Add the SNMP manager by entering the following command:

```
add snmp manager 192.168.10.103
```

   b. Add the SNMP community with ALL permissions by entering the following command:

```
add snmp community ctxtrainsnmp ALL
```

2. Configure both a generic and specific SNMPv2 trap. Attach each to the ctxtrainsnmp SNMP community.
   a. Configure the specific SNMP trap by entering the following command:

```
add snmp trap specific 192.168.10.103 -version V2
-communityName ctxtrainsnmp
```

   b. Configure the generic SNMP trap by entering the following command:

```
add snmp trap generic 192.168.10.103 -version V2
-communityName ctxtrainsnmp
```

3. Configure an SNMP alarm of type CONFIG-SAVE and save the NetScaler configuration to trigger an SNMP alert. View the trap results.
   a. Set an SNMP alarm by entering the following command:

```
set snmp alarm CONFIG-SAVE -state ENABLED
```

   b. Save the NetScaler configuration by entering the following command:

```
save ns config
```

   c. View the SNMP results by entering the following command:

```
stat snmp
```

Configuring the Kiwi Syslog Daemon and Viewing SNMP Alerts (Command-Line Interface)

In the Win7Client virtual machine, use an SSH connection (PuTTY) to the NS_VPX_0 command-line interface logged on as the nsroot user for this task.

1. Start the Kiwi Syslog Daemon listening for SNMP traps on UDP port 162.
   a. Click **Start > All Programs > Kiwi Enterprises > Kiwi Syslog Daemon > Kiwi Syslog Daemon**.

      The Kiwi Syslog Daemon opens.
   b. Click **File** and select **Setup**.
   c. Expand the **Inputs** node and select **SNMP**.
   d. Check **Listen for SNMP Traps** and verify that `162` is entered in the UDP Port field.
2. Prepare the listener for an informational trap from the Syslog Level list. Clear any previously captured data and send an SMNP trap.
   a. Select **Info** from the Syslog Level list and click **OK**.

b. Click **View** and select **Clear display**.

3. Switch to the command-line interface for NS_VPX_0 and configure an SNMP alarm to trigger on configuration save. Then save the NetScaler configuration.

   a. Add the SNMP alarm by entering the following command:

   ```
   set snmp alarm CONFIG-SAVE -state ENABLED
   ```

   b. Save the NetScaler configuration by entering the following command:

   ```
   save ns config
   ```

4. View the SNMP traps in the Kiwi Syslog Daemon. The SNMP syslog will resemble the following:

```
12-02-2008 16:22:43 Local7.Info 172.30.108.5
community=ctxtrainsnmp,
enterprise=1.3.6.1.4.1.5951.1.1.0.28,
enterprise_mib_name=netScalerConfigSave,
uptime=508021, agent_ip=172.168.10.103,
version=Ver2, nsUserName.0=nsroot,
sysIpAddress.0=10.0.0.100
```

Module 14

Exercises for Troubleshooting

Exercise 14-1: Troubleshooting Scenario 1

Scenario

You have configured a virtual server that uses the round-robin method of load-balancing. The load-balancing virtual server on http://10.0.0.80 is configured to serve the Blue, Green, and Red home pages. During some internal tests, you find that only the Red home page is being displayed by the server. You refresh the page, clear the cache, and try a different browser, so you think the problem is on the server side.

The web site needs to go live tomorrow and you need to find out why load balancing is not working.

Where to Begin

Turn off the NS_VPX_0 virtual machine and use the NS_VPX_4 virtual machine for this exercise.

Access the NetScaler and browse to the **Load Balancing** node. Check the settings for the servers, services, and load balancing virtual servers.

Browse to the **System** node. Check the NetScaler settings.

Checkpoint

Checking the following items may help you troubleshoot this issue.

- Are the Blue and Green servers configured, and does the state show as UP?
- Are the services for the Blue and Green servers properly configured?
- Is the load-balancing virtual server configured?
- Are the Blue and Green services bound to the virtual server?
- Are the required features enabled?

The issue is considered resolved when the following conditions have been met:

- One of the color pages appears when you browse to http://10.0.0.80
- The web page cycles through the Blue, Green, and Red home pages when the browser is refreshed.

Before You Begin

To begin this lab, ensure that the following virtual machines are started:

- AD.training.lab
- NS_VPX_4

- Router_Vyatta
- Win7Client

Estimated time to complete this exercise: 10 minutes

Exercise 14-2: Troubleshooting Scenario 2

Scenario

You have configured a virtual server for SSL Offload. The page was working find until you installed a new server certificate. You followed the procedures to create a certificate request and then downloaded the server certificate. However, the SSL virtual server at https://10.0.0.85 is not responding.

The old certificate expires today and customers will need access to the secure web site. You need to determine why SSL offload is not working and then fix the problem.

Where to Begin

Turn off the NS_VPX_0 virtual machine and use the NS_VPX_4 virtual machine for this exercise.

Navigate to **SSL Offload** and check the SSL settings.

Checkpoint

Checking the following items may help you troubleshoot this issue:

- Are the proper services bound to the virtual server?
- Is the new certificate installed on the server?
- Is the new certificate bound to the server?

The issue is considered resolved when the following conditions have been met:

- You browse to https://10.0.0.82 and the page loads.
- The page cycles through the Blue, Green, and Red home pages when the browser is refreshed.

Before You Begin

To begin this lab, ensure that the following virtual machines are started:

- AD.training.lab
- NS_VPX_4
- Router_Vyatta
- Win7Client

Estimated time to complete this exercise: 10 minutes

Exercise 14-3: Troubleshooting Scenario 3

Scenario

The company home page includes content for most browsers. In order to accomodate users on legacy browsers and users on iPhones, you have configured the NetScaler to switch content requested from IE6 and iPhones to different servers. IE6 users are directed to the Blue server and iPhone users are directed to the Red server.

The NetScaler was restarted after some updates were applied. Shortly after that, you receive complaints from IE6 and iPhone users that they are not able to view the proper content.

Where to Begin

Turn off the NS_VPX_0 virtual machine and use the NS_VPX_4 virtual machine for this exercise.

Use the Firefox browser to use the IE6 and iPhone user agents to verify the problem by clicking **Tools** > **Default User Agent** .

Navigate to **Content Switching** > **Virtual Servers** and verify that the settings for the virtual server are correct and the correct policies are applied.

Checkpoint

Checking the following items may help you troubleshoot this issue:

- Is the content switching virtual server UP?
- Are the appropriate policies bound to the server?
- Do the policies have the correct targets?

The issue is considered resolved when you browse to http://10.0.0.85 and the following conditions have been met:

- The Blue home page appears when using Firefox with the Default User Agent set to IE6.
- The Red home page appears when using Firefox with the Default User Agent set to iPhone.
- The Green home page appears when using Firefox with the Default User Agent set to Default.

Before You Begin

To begin this lab, ensure that the following virtual machines are started:

- AD.training.lab
- NS_VPX_4
- Router_Vyatta

- Win7Client

Estimated time to complete this exercise: 10 minutes

Exercise 14-4: Troubleshooting Scenario 4

Scenario

The web administrators need to update certain information on the web site and they want to be able to deny access to the pages while they are being updated. The hidden pages will contain the string "private" and the administrators have asked you to configure the NetScaler to deny access to these pages with a custom response.

You create a Responder action, a policy, and bind the policy globally. However, during tests the server does not return the custom response and instead returns an error 404 - File or directory not found.

Where to Begin

Turn off the NS_VPX_0 virtual maching and use the NS_VPX_4 virtual machine for this exercise.

Navigate to **Responder** and verify the actions and policies.

Checkpoint

Checking the following items may help you troubleshoot this issue:

- Does the policy have the correct action applied to it?
- Is the policy bound globally?
- Does the policy contain the correct expression?

The issue is considered resolved when the following conditions have been met:

- You browse to http://10.0.0.80/private and the server returns the custom response.

Before You Begin

To begin this lab, ensure that the following virtual machines are started:

- AD.training.lab
- NS_VPX_4
- Router_Vyatta
- Win7Client

Estimated time to complete this exercise: 10 minutes

Exercise 14-5: Troubleshooting Scenario 5

Scenario

A Windows application connects to the NetScaler using a Windows Active Directory user credential. The application needs to be able to view certain NetScaler settings for reporting purposes. You decide to test the user credentials and log on to the NetScaler at http://10.0.0.100. You are able to log onn successfully, but you receive an error and are not able to view any settings. You verify that the user is a member of an Active Directoy group; username is user1.

Where to Begin

Turn off the NS_VPX_0 virtual machine and use the NS_VPX_4 virtual machine for this exercise.

Log on to the AD.training.lab virtual machine and examine the group membership for the user1 user.

Log on to the NetScaler and browse to **System > Groups** to verify the group settings.

Checkpoint

Checking the following items may help you troubleshoot this issue:

- Is user1 a member of the appropriate group?
- Is the group added to the NetScaler?
- Are the appropriate policies bound to the group?

The issue is considered resolved when the following conditions have been met:

- You are able to log on to the NetScaler command-line interface as user1.
- You run several show commands and are able to view the NetScaler settings.

Before You Begin

To begin this lab, ensure that the following virtual machines are started:

- AD.training.lab
- NS_VPX_4
- Router_Vyatta
- Win7Client

Estimated time to complete this exercise: 10 minutes

851 West Cypress Creek Road Fort Lauderdale, FL 33309 USA (954) 267 3000 www.citrix.com

Rheinweg 9 8200 Schaffhausen Switzerland +41 (0) 52 63577 00 www.citrix.com