CNS 207 3i - Implementing Citrix NetScaler 11.0 for Application and Desktop Solutions

CNS 207 3i - Implementing Citrix NetScaler 11.0 for Application and Desktop Solutions

Authorized
Courseware

Table of Contents

Module 1: Getting Started 11
Lab Overview 13
Lab Diagram 13
Lab IP Addresses 13
Networks 15
NetScaler Management IP Summary 16
NetScaler VIP Summary 16
NetScaler Management URLs 17
Useful Domain and Other Accounts 18
Lab Environment / XenCenter 19
XenCenter Overview 19
Student Desktop 20
Module 1: Getting Started Exercises 22
Exercise 1-1: Performing an Initial Configuration (Configuration Utility) 22
Before You Begin 22
Performing an Initial IP Configuration from the NetScaler Console 23
Installing a License (Configuration Utility) 23
Exercise 1-1: Performing an Initial Configuration (Command Line Interface) 25
Before You Begin 25
Performing an Initial IP Configuration from the NetScaler Console 25
Installing a License (Command Line Interface) 26
Exercise 1-2: Performing Basic Administration (Configuration Utility) 27
Enabling NetScaler Features 27
Configuring an NTP Server 28
Performing a Configuration Backup (Configuration Utility) 29
Exercise 1-2: Performing Basic Administration (Command-Line Interface) 30
Enabling and Disabling Features (Command-Line Interface) 30
Configuring a NTP Server (Command Line Interface) 31
Backing Up System Configuration (Command Line Interface) 32
Exercise 1-3: Upgrading the NetScaler System (Command-Line Interface) 33
Upgrading the NetScaler System (Command-Line Interface) 34
Verifying the NetScaler Upgrade (Command-Line Interface) 35

Module 2: Basic Networking 37
Module 2: Basic Networking Exercises 39
Exercise 2-1: Configuring Basic Networking 39
Enabling Management Access on a Subnet IP Address (Configuration Utility) 39
Adding a SNIP to the NetScaler 39
Configuring VLANs 40
Exercise 2-1: Configuring Basic Networking (Command Line Interface) 41
Configuring Subnet IP Addresses 41

Configuring VLANs 41

Module 3: High Availability 43
Module 3: High Availability Exercises 45
Exercise 3-1: Configuring High Availability 45
Configuring NetScaler High Availability with NSHA1 and NSHA2 (Configuration Utility) 45
Configuring High Availability on NSHA1 and NSHA2 (Configuration Utility) 45
Testing the High-Availability Configuration (Configuration Utility) 46

Module 4: Integrating NS Gateway with Other Resources (Unified Gateway) 49
Module 4: Integrating NetScaler with XenApp and XenDesktop Using the Unified Gateway Wizard 51
Exercise 4-1: Unified Gateway Wizard 51
Launch the Unified Gateway Wizard 51
Unified Gateway Wizard 51
Virtual Server 51
Server Certificate 51
Authentication 52
Portal Theme 52
Applications 52
StoreFront 53
XenDesktop Farm 53
Connect to TrainingLabUGW 54

Module 5: Load Balancing Gateway Services Exercises 55
Module 5: Load Balancing Gateway Services Exercises 57
Exercise 5-1: Load-Balancing Web Servers 57
Add Red, Blue and Green Servers to NetScaler (Configuration Utility) 57
Creating Load Balanced Services 58
Creating a Load-Balancing Virtual Server 58
Testing Load Balancing 59
Resetting Persistence to None 60
Exercise 5-2: Load-Balancing a DNS Server 60
Add DNS Servers to NetScaler 61
Creating DNS Services 61
Creating a DNS Load Balancing Virtual Server 62
Testing DNS Load Balancing 63
Exercise 5-3: Load-Balancing LDAP Servers 65
Create a LDAP Monitor 65
Creating LDAP Services 65
Creating a LDAP Load-Balancing Virtual Server 66

Module 6: NetScaler Security and SSL 69

Module 6: SSL Offload Exercises 71
Exercise 6-1: Configuring SSL Certificates and SSL Offload 71
Before You Begin 71
Creating an RSA Key 71
Creating a Certificate Request 72
Submitting the Certificate Request for the Web Server 73
Configuring a Certificate-Key Pair 74
Creating an SSL Offload Virtual Server 74
Testing SSL Offload 75
Exercise 6-2: Configuring Load Balancing for XenDesktop Delivery Controllers 76
Create Server Instances for the XenDesktop Delivery Controllers 76
Create a Monitor for the XenDesktop Delivery Controller Services 76
Create Load-Balancing Services for the XenDesktop Delivery Controllers 76
Importing a PKCS#12 Certificate 77
Create a Load-Balancing Virtual Server for the XenDesktop Delivery Controllers 78
Verifying the Load-Balancing Configuration 79
Exercise 6-3: Configuring Load Balancing for Citrix StoreFront 79
Create Server Instances for the StoreFront Servers 79
Create a Monitor for the StoreFront Services 80
Create Load-Balancing Services for the StoreFront Servers 80
Configuring Load Balancing for the StoreFront Servers 81
Updating StoreFront to Use Load-Balancing Virtual Servers 82
Testing StoreFront Load-Balancing Configuration 83
Exercise 6-4: Configuring a NetScaler Gateway Virtual Server 83
NetScaler Gateway Wizard 83
Enabling Split Tunneling 84
Testing the NetScaler Gateway Virtual Server 86
Disabling Split Tunneling 86

Module 7: Authentication and Authorization 89
Module 7: Authentication and Authorization Exercises 91
Exercise 7-1: Enabling External Authentication 91
Creating a New Administrator Account 91
Examining Command Policies 92
Enabling LDAP Authentication 92
Binding an LDAP Policy to a NetScaler Gateway Virtual Server 94
Testing the LDAP Policy with the NetScaler Gateway 95

Module 8: Access Policies 97
Module 8: Access Policies Exercises 99
Exercise 8-1: Configuring a Pre-Authentication Policy 99
Configuring a Pre-Authentication Policy 99
Unbinding Pre-Authentication Policies 100
Exercise 8-2: Configuring a NetScaler Gateway Authorization Policy 101
Configuring the Default Authorization Action 101

Creating an Authorization Policy 102
Testing Authorization Policies 103

Module 9: End User Access and Experience (includes RDP Proxy) 105
Module 9: End-User Access and Experience Exercises (Includes RDP Proxy) 107
Exercise 9-1: Displaying Client and Configuration Options 107
Viewing the Contractor Profile 107
Viewing Available Client and Configuration Options 107
Hiding Client and Configuration Options 108
Viewing the Updated Contractor Profile 108
Exercise 9-2: Configuring Clientless Access with Client Choices 109
Configuring Clientless Access on the NetScaler Gateway 109
Testing Clientless Access 110
Configuring Remote Desktop (RDP) Proxy 111

Module 10: NetScaler Gateway and Unified Gateway 115
Module 10: Integrating NetScaler 11 with XenApp and XenDesktop Exercises 117
Exercise 10-1: Configuring StoreFront for NetScaler Gateway 117
Configuring StoreFront Authentication, Gateway, Beacons and Enabling Remote Access 117
Exercise 10-2: Configuring the NetScaler for StoreFront 118
Creating a New Session Policy to Access StoreFront 118
Exercise 10-3: Adding Secure Ticketing Authority Servers to the NetScaler 120
Adding Secure Ticketing Authority Servers to the NetScaler Gateway 120
Exercise 10-4: Updating an Authorization Policy 120
Testing the New Session Policy to Access StoreFront Using NetScaler Gateway 121
Exercise 10-5: Customize the NetScaler Gateway Portal Page 122
Exercise 10-6: Apply an End User License Agreement (EULA) 123

Module 11: AppExpert (Default and Classic Syntax) 125
Module 11: AppExpert Policy Engine 127
Exercise 11-1: Configuring Responder to Redirect to HTTPS 127
Configuring Responder to Use SSL 127
Testing the Redirect to SSL Policy 128
Exercise 11-2: Configuring Content Switching 129
Verifying that the Content-Switching Feature is Enabled 129
Creating Non-Addressable Load-Balancing Virtual Servers 129
Creating Policy Expressions 131
Creating Content-Switching Policies 132
Creating the Content-Switching Virtual Server 132
Testing the Content-Switching Configuration 133

Module 12: Multi-tenancy and SDX NetScaler 135

Module 12: Multi-tenancy and SDX NetScaler 137
Introduction to the NetScaler SDX Appliance 137
Exercise 12-1: Managing a NetScaler SDX Appliance 137
Managing a NetScaler SDX Appliance: Before You Begin 137
Managing a NetScaler SDX Appliance: Adding and Configuring a NetScaler VPX Instance 138

Module 13: Monitoring and Administration 141
Module 13: Monitoring and Management Exercises 143
Before You Begin 143
Exercise 13-1: Auditing and Logging 143
Creating a Syslog Policy and Syslog Server 144
Viewing Recent Audit Messages 145
Viewing Historical Audit Messages 146
Viewing Audit Messages on the Remote Syslog Server 146
Disabling Syslog Audit Messages 147
Exercise 13-2: Monitoring 147
Configuring SNMP Settings 147
Configuring the Kiwi Syslog Daemon and Viewing SNMP Alerts 148
Exercise 13-3: Configuring Insight Center 149
Performing Insight Center Initial Setup 149
Configuring Insight Center 150
Enabling Data Collection 151
Test the HDX Traffic 152

Module 14: Troubleshooting Exercises 153
Module 14: Troubleshooting Exercises 155
Exercise 14: Troubleshooting 155
Before You Begin 155
Preparing the NetScaler for the Troubleshooting Lab 155
Exercise 14-1: Troubleshooting Scenario 1 156
Where to Begin 156
Checkpoint 156
Exercise 14-2: Troubleshooting Scenario 2 156
Where to Begin 156
Checkpoint 156
Exercise 14-3: Troubleshooting Scenario 3 157
Where to Begin 157
Checkpoint 157
Exercise 14-4: Troubleshooting Scenario 4 157
Where to Begin 157
Checkpoint 158
(Optional) Returning the NetScaler to Previous State 158

Citrix Hands-on Labs

What are Hands-on Labs?

Hands-on Labs from Citrix Education allows you to revisit, relearn, and master the lab exercises covered during the course. This offer gives you 25 days of unlimited lab access to continue your learning experience outside of the classroom.

Claim introductory pricing of $500 for 25 days of access. Contact your Citrix Education representative or *purchase online here.*

Why Hands-on Labs?

Practice outside of the classroom

You'll receive a fresh set of labs, giving you the opportunity to recreate and master each step in the lab exercises.

Test before implementing

Whether you're migrating to a new version of a product or discovered a product feature you previously didn’t know about, you can test it out in a safe sandbox environment before putting in live production.

25 days of access

Get unlimited access to the labs for 25 days after you launch, giving you plenty of time to sharpen your skills.

Certification exam preparation

Get ready for your Citrix certification exam by practicing test materials covered by lab exercises.

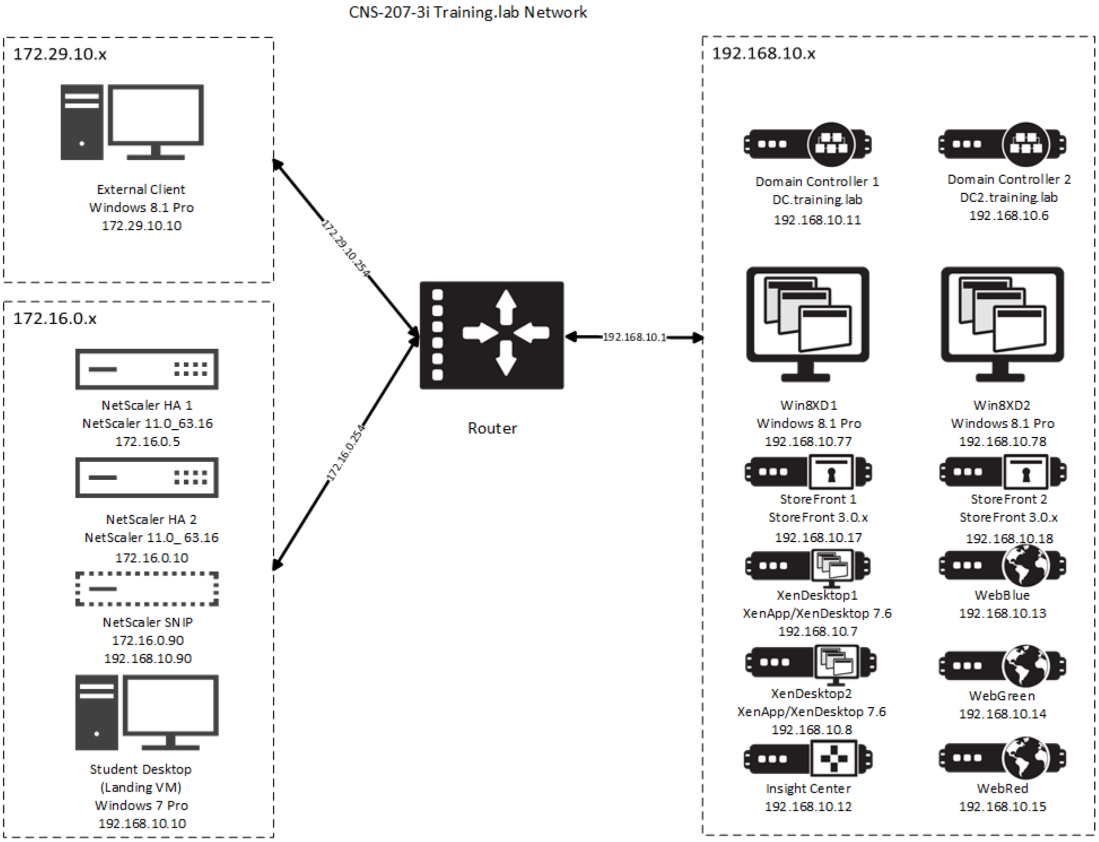
Module 1

Getting Started

1

Lab Overview

Lab Diagram



Lab IP Addresses

The following tables summarize virtual machines, names, IP Addresses and other essential information regarding the lab environment and the configurations that will be made during the lab exercises. Please refer to these tables as needed.

Lab Environment Virtual Machine and IP Address Summary

Resource	Display Name (in XenCenter)	FQDN/Hostname	IP Address
Domain Controller	DC.training.lab	dc.training.lab	192.168.10.11
Domain Controller 2	DC2.training.lab	dc2.training.lab	192.168.10.6
NetScaler HA 1	NSHA1	nsha1.training.lab	172.16.0.5
NetScaler HA 2	NSHA2	nsha2.training.lab	172.16.0.10
NetScaler Insight Center	InsightCenter	insight.training.lab	192.168.10.12
Blue Server	WebBlue	webblue.training.lab also: blue.training.lab	192.168.10.13
Green Server	WebGreen	webgreen.training.lab also: green.training.lab	192.168.10.14
Red Server	WebRed	webred.training.lab also: red.training.lab	192.168.10.15
StoreFront 1	SF1	sf1.training.lab	192.168.10.17
StoreFront 2	SF2	sf2.training.lab	192.168.10.18
XenDesktop 1 (Controller)	XD1	xd1.training.lab	192.168.10.7
XenDesktop 2 (Controller)	XD2	xd2.training.lab	192.168.10.8
Win8XD1 (VDA)	Win8XD1	win8xd1.training.lab	192.168.10.77
Win8XD2 (VDA)	Win8XD2	win8xd2.training.lab	192.168.10.78
External Client	ExternalClient	externalclient (workgroup)	172.29.10.10
Student Desktop (Landing VM)	StudentDesktop (hidden)	studentdesktop.training.lab	192.168.10.10

Networks

Network Role	Subnet	Gateway	Notes
INTERNAL	192.168.10.0/24	192.168.10.1	Lab "backend"; all domain controllers, web servers, XenDesktop components are here. The Student Desktop belongs to this network and will be used to manage the environment.
DMZ	172.16.0.0/24	172.16.0.254	Network for components in our lab's DMZ. NetScaler VIPs and NSIP's belong to this network. Please note it is not recommended for NetScaler NSIP's to be exposed on public-facing networks; this was done to simplify the lab environment.
REMOTE	172.29.10.0/24	172.29.10.254	This represents the public/external network within the lab environment. The External Client resides here and will be used to test VPN connections to the VIP's hosted on the NetScaler via the DMZ network.

NetScaler Management IP Summary

Name	IP Role	DNS Alias	Notes:
NSHA1	NSIP: 172.16.0.5/24	nsha1.training.lb	Mgmt IP for NSHA1
	SNIP1: 172.16.0.90/24	netscaler.training.lab	Mgmt IP for HA Pair
	SNIP2: 192.168.10.90/24		

Name	IP Role	DNS Alias	Notes:
NSHA2	NSIP: 172.16.0.10/24	nsha2.training.lb	Mgmt IP for NSHA2
	SNIP1: 172.16.0.91/24		Removed once joined to HA pair.

NetScaler VIP Summary

DNS Alias	IP Address	Other	Description/vServer name
colors.training.lab	172.16.0.20	VIP (LB)	LB vServer for Red/Blue/Green: lb_vsrv_colors
nimbus.training.lab	172.16.0.21	VIP (LB)	LB vServer for XD Controllers (xml brokers)
storefront.training.lab	172.16.0.22	VIP (LB)	LB vServer for StoreFront: lb_vsrv_storefront, ssl_vsrv_sf
gateway.training.lab	172.16.0.30	VIP (VPN)	VPN vServer
unifiedgateway.training.lab	172.16.0.40	VIP (CS)	FQDN for CS vServer associated with Unified Gateway configuration

DNS Alias	IP Address	Other	Description/vServer name
	172.16.0.99	VIP (LB)	LB vServer for DNS (DC and DC2)
	172.16.0.110	VIP (LB)	LB vServer for LDAP authentication (DC and DC2)
	172.16.0.224	VIP (LB)	LB vServer "testsrv"; remains in a down/unused state.
	172.16.0.84	VIP (CS)	CS vServer used with Red/Blue/Green web servers: cs_vsrv_rbg

NetScaler Management URLs

FQDN/URL	IP Address	Description
http://nsha1.training.lab http://172.16.0.5	172.16.0.5	NSHA1 Configuration Utility (Management GUI)
http://nsha2.training.lab http://172.16.0.10	172.16.0.10	NSHA2 Configuration Utility (Management GUI)
http://netscaler.training.lab http://172.16.0.90	172.16.0.90	Configuration Utility for current primary member of NetScaler HA Pair using the shared management SNIP. (Always connects to primary NetScaler in HA pair.)
http://insight.training.lab	192.168.10.12	NetScaler Insight Center Configuration Utility (GUI)

Useful Domain and Other Accounts

User	Password	Notes
training\administrator	Password1	Domain Admin; full control to Active Directory, all virtual machines, and admin rights in XenDesktop Studio.
training\citrixadmin	Password1	Primary management account in lab exercises; also a member of the Domain Admins group and a XenDesktop admin.
training\contractor	Password1	Primary user to test logons to the NetScaler gateway, though other accounts will be used.
nsroot	nsroot	Primary administrator for NetScaler and Insight Center; default password was retained in lab.
citrix (local)	Password1	Use this account when connecting to the ExternalClient for NetScaler Gateway tests. It has local admin rights. Note: ExternalClient is not a member of the domain; "training" domain accounts will not be able to log on.

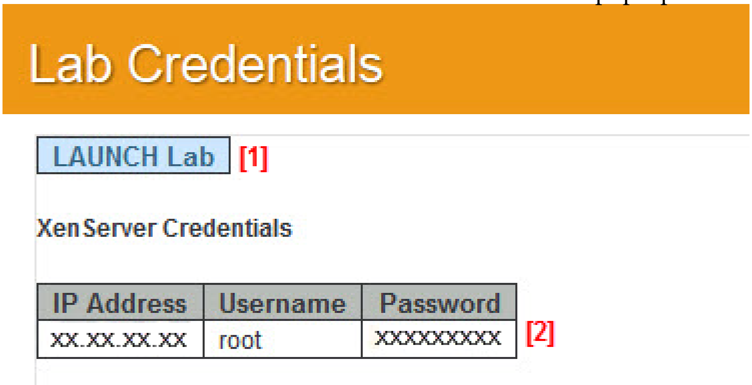
Other accounts used for specific lab exercises		
training\citrixldap	Password1	Service account used as a the LDAP bind account when configuring NetScaler integration with LDAP authentication.
training\citrixrdp	Password1	RDP proxy test user.

Other accounts used for specific lab exercises		
training\citrixuser1	Password1	Alternate user account when testing delegated admin rights.

Lab Environment / XenCenter

To connect to the lab environment:

1. Access training.citrix.com:
    a. In a web browser, go to: http://training.citrix.com
    b. Go to My Trainings.
    c. Log on with your MyCitrix account (if required).
2. Access the Student Resources for the CNS-207 course. If the student resources for this course are not available, inform your instructor.
3. Find the section marked lab and click Launch. The Lab Credentials pop-up window displays:



Lab Credentials

LAUNCH Lab [1]

XenServer Credentials

IP Address	Username	Password
xx.xx.xx.xx	root	xxxxxxxxx

[2]

Click the **LAUNCH** Lab button (Section [1]) to start the ICA connection to the Student Desktop (landing vm). A Citrix Receiver is required to connect. You can download the latest version from: http://www.citrix.com/receiver.

Take note of the IP Address and Password listed (Section [2]). This will be needed to connect to your assigned hypervisor. These will be refereed to as your hypervisor credentials from here on.

XenCenter Overview

XenCenter will be used to manage virtual machines. For most of this class, students will only need to use XenCenter to power virtual machines on and off. Majority of the virtual machines are powered on the entire class.

Students will need to connect to the console of the NetScaler NSHA1 and the Insight Center virtual machines during the initial configuration exercises. Once the initial networking has been configured during the appropriate lab exercises, the rest of the device administration will be handled through the browser-based configuration utilities.

While students can use XenCenter to access the consoles of virtual machines in the "backend" network, such as the domain controllers, StoreFront servers, and XenDesktop controllers; it is recommended that students use the RDP shortcuts located on the Student Desktop.

Student Desktop

The following details how to use the lab environment.

1. Connect to the lab environment via http://training.citrix.com. Follow the instructions provided by your instructor.
2. When you first access the lab environment, you will be connected to the Student Desktop. This will act as the management workstation for most of the lab environment.
3. From the Student Desktop, you have access the rest of the lab environment:
    a. From the Student Desktop, use XenCenter and the supplied XenServer credentials to access the rest of the lab environment. Using XenCenter, you can power virtual machines on or off, as needed. Or access the consoles for the rest of the lab machines.
    b. From the Student Desktop, you can also use the RDP shortcuts to access backend machines, such as the Domain Controllers, Web Servers, StoreFront, and the XenDesktop 7.6 Site. The folder with "windowed" shortcuts will open in 1024x768 resolution. The folder with "fullscreen" shortcuts will open in fullscreen mode.
4. From the Student Desktop, you also have access to the management consoles for the NetScalers and the NetScaler Insight Center appliances.
    a. During the initial lab exercise, you will access the console of the NetScaler using XenCenter.
    b. After the initial exercises, you can use web browsers (Chrome, Firefox, or Internet Explorer) to access the NetScaler's configuration utility (GUI) via the NSIP and/or management SNIP addresses. Example: http://nsha1.training.lab or http://172.16.0.5/.
    c. You can also use PuTTY.exe to connect to the NetScaler command line interface (CLI) over SSH. Use either the PuTTY shortcut on the desktop and use the saved sessions or manually enter destination IP addresses to connect to the NetScalers.
    d. Alternatively, you can manually connect using Start>Run>Putty>IP address>

> Example: Start > Run > putty.exe 172.160.0.5. Example: Start > Run > putty.exe nsha1.training.lab

Unless instructed otherwise, all lab exercises are performed from the Student Desktop. When necessary the lab will identify which virtual machine to connect and which credentials to use.

- Students will connect to StoreFront servers SF1 and SF2 and the XenDesktop Controllers XD1 and XD2 when configuring StoreFront and XenDesktop settings.
- The External Client will be used when testing NetScaler Gateway ICA Proxy and VPN connections.
- While most load balancing/content switching testing will also be performed from the Student Desktop

Module 1: Getting Started Exercises

Exercise 1-1: Performing an Initial Configuration (Configuration Utility)

This exercise demonstrates how to complete initial configuration of a NetScaler system, including how to set the NetScaler IP address, subnet mask and default gateway address. NetScaler license installation is also demonstrated in this exercise.

Before You Begin

Access the lab via the Launch link at http://training.citrix.com.

- Take note of the Hypervisor credentials on the launch page.
- From the Student Desktop (landing vm), Open XenCenter and connect to XenServer using the credentials from the launch page.
- Use XenCenter to start/stop VM's as required.

The landing VM will serve as the primary management workstation for the lab environment.

Before you begin, use XenCenter and start the following virtual machines:

- DC.training.lab (Domain Controller)
- DC2.training.lab (Domain Controller 2)
- NSHA1 (NetScaler HA 1)
- NSHA2 (NetScaler HA 2
- WebBlue
- WebGreen
- WebRed
- SF1
- SF2
- XD1
- XD2
- Win8XD1
- Win8XD2
- ExternalClient

Leave the following virtual machines powered OFF:

- InsightCenter (NetScaler Insight Center)

Estimated time to complete this exercise: 10 minutes

Performing an Initial IP Configuration from the NetScaler Console

Connect to NetScaler NSHA1 via XenCenter console to perform initial configuration.

1. Connect to the NetScaler NSHA1 virtual machine console using XenCenter.
    a. In XenCenter, select NSHA1 in the left pane.
    b. Select the Console tab in the right pane.
2. Configure the NetScaler for use with an IP address of 172.16.0.5, a netmask of 255.255.255.0 and a default gateway of 172.16.0.254.
    a. In the console, enter the following information and press **Enter** to configure the NetScaler:
        - NetScaler's IPv4 address: `172.16.0.5`
        - Netmask: `255.255.255.0`
        - Gateway IPv4 address: `172.16.0.254`

    b. Press **Enter** to accept the default option (option 4) to save and quit the configuration utility and reboot. The NetScaler NSIP management address is now configured and able to be accessed via browser and/or SSH from the Student Desktop.

Installing a License (Configuration Utility)

From the Student Desktop, use an HTTP connection to the NetScaler NSHA1 configuration utility. Log on as the nsroot user for this task.

1. Connect to the configuration utility (GUI) for NSHA1
    a. Open a web browser and browse to `http://nsha1.training.lab` or `http://172.16.0.5.`

    > A DNS entry was already created for http://nsha1.training.lab.

    > Either Firefox or Chrome are recommended browsers for accessing the NetScaler configuration utility.

    b. Log on to the NetScaler using the nsroot/nsroot credentials.
    c. Click Skip to opt out of the Citrix User Experience Improvement Program (if prompted).

> After logging in you will be taken to the **Welcome!** screen where you can add the following information. (Step 2)

2. Enter the NetScaler system information.
    a. Verify that 172.16.0.5 appears in the NetScaler IP address field.
    b. Verify that 255.255.255.0 appears in the Netmask field.
    c. Click the **Subnet IP Address** field and then type `172.16.0.90` in the Subnet IP Address field.
    d. Verify that `255.255.255.0` is specified in the Subnet IP Address Netmask field and then click **Done**.
    e. Click the **Host Name, DNS IP Address and Time Zone** field then type `NSHA1` in the Hostname field.
    f. Leave the DNS (IP address) field blank.
    g. Leave the Time Zone field at the default setting: Universal Coordinated Time.
    h. Click **Done**.
    i. Click **No** on the **Confirm** pop-up window so that the NetScaler does not reboot.
3. Install the platform license on the NetScaler using the license provided in the **C:\resources** folder on the Student Desktop.
    a. Click in the **Licenses** field and verify that the **Upload license files from a local computer** radio button is selected.
    b. Click **Browse**.
    c. Browse to **C:\resources\** in the left pane.
    d. Double-click the **NetScaler License** folder.
    e. Select the **NetScaler_VPX1_PLT_Citrix_Education_Expires_20180109.lic** file and click **Open**.
    f. Click **Reboot**.
    g. Click **Yes** to save the config before rebooting.
    h. Close the browser for the NetScaler.
    i. Wait for the NetScaler reboot to complete (status in browser).

> Wait approximately 3 minutes for the NetScaler to restart.

4. Verify that the NetScaler license has been installed.
    a. Use web browser and browse to `http://nsha1.training.lab`.
    b. Log on to the NetScaler using the **nsroot/nsroot** credentials.
    c. The License Summary window will be displayed.
    d. Examine the available features listed then close the window.

Exercise 1-1: Performing an Initial Configuration (Command Line Interface)

This exercise demonstrates how to enable NetScaler features, configure time zone settings and perform a configuration backup.

The following steps using the Command Line Interface are just for your reference. The commands will not work if the NetScaler was already configured using the GUI. Configuration can be done either by the GUI or CLI.

Before You Begin

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

- DC.training.lab (Domain Controller)
- DC2.training.lab (Domain Controller 2)
- NSHA1 (NetScaler HA 1)
- NSHA2 (NetScaler HA 2)
- WebBlue
- WebGreen
- WebRed
- SF1
- SF2
- XD1
- XD2
- Win8XD1
- Win8XD2
- ExternalClient

Leave the following virtual machine powered OFF:

- InsightCenter

Estimated time to complete this exercise: 20 minutes

Performing an Initial IP Configuration from the NetScaler Console

Connect to NetScaler NSHA1 via XenCenter console to perform initial configuration.

1. Connect to the NetScaler NSHA1 virtual machine console using XenCenter:
   a. In XenCenter, select NSHA1 in the left pane.

    b. Select the **Console** tab in the right pane

2. Configure the NetScaler for use with an IP address of 172.16.0.5, a netmask of 255.255.255.0 and a default gateway of 172.16.0.254.
    a. In the console, enter the following information and press **Enter** to configure the NetScaler:
        - NetScaler's IPv4 address: `172.16.0.5`
        - Netmask: `255.255.255.0`
        - Gateway IPv4 address: `172.16.0.254`
    b. Press **Enter** to accept the defaults option (option 4) to save and quit the configuration utility and reboot. The NetScaler NSIP management address is now configured and able to be accessed via browser and/or SSH from the Student Desktop.

Installing a License (Command Line Interface)

> **The following steps using the Command Line Interface are just for your reference. The commands will not work if the NetScaler was already configured using the GUI. Configuration can be done either by the GUI or CLI.**

From the Student Desktop use a SSH connection (PuTTY) to connect to the NetScaler (172.16.0.5) command-line interface. Log on as the nsroot user for this task.

1. Connect to NetScaler **NSHA1** (172.16.0.5) over SSH.
    a. Open PuTTY.exe (Shortcut on StudentDesktop).
    b. Select **NSHA1** and click **Load**.
    c. Click **Open**
    d. Log on as **nsroot / nsroot** as the username and password.
    e. Alternate method: Go to **Start** > **Run** > **Putty 172.16.0.5** or **Start** > **Run** > **Putty nsha1.training.lab**.
2. Examine the features available without a license on a NetScaler.
    a. Enter the following command to view the list of unlicensed NetScaler features:

```
show license
```

    b. Review the list to determine which features are available without a license.
3. Configure other initial settings: Subnet IP (SNIP) and Host Name:.
    a. Configure SNIP 172.16.0.90 with 255.255.255.0 subnet mask:

```
add ns ip 172.16.0.90 255.255.255.0 -type SNIP
```

    b. Configure Host Name as NSHA1:

```
set ns hostname NSHA1
```

4. Use WinSCP to connect to the NetScaler NSHA1.
    a. On the Student Desktop, double-click the **WinSCP** icon.
    b. Select saved session NSHA1 and click **Login**.
    c. Click **Continue** on the **Warning** banner window.
    d. Type `nsroot` in the Password field and click **OK**.
5. Use WinSCP to install a license on a NetScaler.
    a. In the left pane of the WinSCP window, browse to **C:\resources\NetScaler License**
    b. In the right pane of the WinSCP window, double-click the **uppermost folder**, double-click **nsconfig**, then double-click **license**. The location is **/flash/nsconfig/license**
    c. Click and drag the **NetScaler_VPX1_PLT_Citrix_Education_Expires_20180109.lic** from the left pane to the right pane.
    d. The license is copied to the NetScaler file system.
    e. Close the WinSCP window and click **OK** to confirm ending the session.
6. Save configuration and initiate a warm reboot on NSHA1.
    a. Switch to the open PuTTY session for NSHA1 and save the NetScaler configuration by typing `save ns config`.
    b. Reboot the NetScaler by entering the following commands: `reboot -warm` then `y`.
7. Examine the features available with a license on a NetScaler.
    a. Enter the following command in PuTTY to view the list of licensed NetScaler features:

```
show license
```

Exercise 1-2: Performing Basic Administration (Configuration Utility)

This exercise demonstrates how to enable NetScaler features, configure an NTP server, configure time zone settings and perform a configuration backup.

Enabling NetScaler Features

From the Student Desktop, use an HTTP connection to the NetScaler NSHA1 configuration utility. Log on as the nsroot user for this task.

1. Connect to the configuration utility (GUI) for NSHA1: **http://172.16.0.5** or **http://nsha1.training.lab**.
2. Enable the SSL Offloading, HTTP Compression, Load Balancing, Content Switching, Content Filtering, Rewrite and NetScaler Gateway.
    a. Go to **System** > **Settings** then click **Configure Basic Features** in the Settings node. The Configure Basic Features dialog box opens.

   b. Select to enable the following features:
      - SSL Offloading
      - HTTP Compression
      - Load Balancing
      - Content Switching
      - Content Filter
      - Rewrite
      - NetScaler Gateway
   c. Click **OK**.
3. Enable additional NetScaler Features (under Advanced node):
   a. Go to **System** > **Settings** then click **Configure Advanced Features** in the Settings node.
   b. Select to enable the following feature:
      - Responder
   c. Click **OK**
4. Save the NetScaler configuration.
   a. Click the **Save** icon on the top-right corner of the configuration utility.

   > The Save icon is displayed as a floppy disk.

   b. Click **Yes** to confirm.

Configuring an NTP Server

From the Student Desktop, use an HTTP connection to the NetScaler NSHA1 configuration utility. Log on as the nsroot user for this task.

1. Add a network time protocol (NTP) server to the NetScaler using 192.168.10.11 as the server address.
   a. Go to **System** > **NTP Servers** and click **Add** in the NTP Servers pane. The Create NTP Server window appears.
   b. Type `192.168.10.11` in the NTP Server field, click **Create**. The Create NTP Server window closes.
   c. Highlight the new NTP server and click **Edit**.
   d. Click **Set as preferred NTP server** and then click **OK**.
2. Enable NTP Synchronization for NTP servers.
   a. Select **NTP Synchronization** from the **Action** drop-down list box in the **NTP Servers** pane.

    b. Select **ENABLED** in the **Configure NTP Synchronization** pane and click **OK**.

3. Save the running configuration on the NetScaler.
    a. Click the **Save** icon in the top-right corner of the configuration utility window.
    b. Click **Yes** to confirm saving the configuration.

> The **time** and **date** may need to be set manually on the NetScaler CLI by using the **date** command ran from the Shell. The **date** command will also show the current time and date on the NetScaler and should be ran after configuring the NTP server to verify that the time is correct. The syntax is: **date [yy]mm]dd]HH]MM].ss] e.g. root@NSHA1# date 1511081130.00.** You can determine the correct time and date by checking the time and date on the domain controller.

4. 4. Connect to the NetScaler NSHA1 over SSH using PuTTY to confirm date/time settings:
    a. Go to **Start** > **Run** > **Putty 172.16.0.5**.
    b. Log on as **nsroot / nsroot.**
    c. Go to Shell

```
shell
```

    d. Verify Date/Time/Timezone:

```
date
```

    e. To manually change date/time (based on NetScaler's timezone):

```
date YYYYMMHHSS
    Example:  date 201601151423
    Would change clock to Jan 15, 2016 t 2:23 pm (14:23).
```

Performing a Configuration Backup (Configuration Utility)

From the Student Desktop use the NetScaler NSHA1 (172.16.0.5) configuration utility. Log on as the nsroot user for this task.

1. Use the configuration utility to perform a configuration backup.
    a. Go to **System** > **Backup and Restore**.
    b. In the details pane, click **Backup**.
    c. In the **Backup** screen, specify the details requested to backup the appliance.
    d. Type `Backup` in the **File Name** field.
    e. Select **Full** from the drop-down list box in the **Type** field.
    f. Click **Backup**.

The backup file is stored at /var/ns_sys_backup/. The "Backup.tgz" file is displayed in the Backup and Restore details screen.

Exercise 1-2: Performing Basic Administration (Command-Line Interface)

The following steps using the Command Line Interface are just for your reference. The commands will not work if the NetScaler was already configured using the GUI. Configuration can be done either by the GUI or CLI. Best practice for upgrading the NetScaler should be done from the CLI. Please complete the NetScaler upgrade section below.

From the Student Desktop, use a SSH connection (PuTTY) to the NetScaler NSHA1 command-line interface. Log on as the nsroot user for this task.

Enabling and Disabling Features (Command-Line Interface)

From the Student Desktop use a SSH connection (PuTTY) to connect to the NetScaler NSHA1 (172.16.0.5) command-line interface. Log on as the nsroot user for this task.

1. Connect to the NetScaler NSHA1 (172.16.0.5) over SSH (using PuTTY): putty.exe 172.16.0.5.
2. Verify features available by license file.

   ```
   show ns license
   ```

3. View features currently enabled. (None)

   ```
   show ns feature
   ```

4. Enable the following features:

   ```
   enable ns feature ssl cmp lb cs cf rewrite sslvpn responder
   ```

   This command enables features: SSL Offload, HTTP Compression, Load Balancing, Content Switching, Content Filtering, Rewrite, NetScaler Gateway, and Responder.
5. Save the NetScaler configuration:

   ```
   save ns config
   ```

Configuring a NTP Server (Command Line Interface)

> **The following steps using the Command Line Interface are just for your reference. The commands will not work if the NetScaler was already configured using the GUI. Configuration can be done either by the GUI or CLI.**

From the Student Desktop use a SSH connection (PuTTY) to connect to the NetScaler NSHA1 (172.16.0.5) command-line interface. Log on as the nsroot user for this task

1. Connect to the NetScaler system from the command-line interface using PuTTY and open the NSHA1 saved session. Log on using the nsroot credentials.

   > 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.

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

   a. Enter the following command to add a NTP server to the NetScaler:

   ```
   add ntp server 192.168.10.11
   ```

   b. Set the NTP server as the preferred NTP server:

   ```
   set ntp server 192.168.10.11 -preferredNTPServer YES
   ```

   c. Enter the following command to enable NTP server synchronization:

   ```
   enable ntp sync
   ```

   d. Enter the following command to save the NetScaler running configuration:

   ```
   save ns config
   ```

   > Shorter forms of this command are also accepted.
   >
   > ```
   > save config
   > ```
   >
   > ```
   > save ns c
   > ```
   >
   > ```
   > save c
   > ```

The **time** and **date** may need to be set manually on the NetScaler CLI by using the **date** command ran from the Shell. The **date** command will also show the current time and date on the NetScaler and should be ran after configuring the NTP server to verify that the time is correct. The syntax is: **date [yy]mm]dd]HH]MM].ss] e.g. root@NSHA1# date 1511081130.00.** You can determine the correct time and date by checking the time and date on the domain controller.

3. From the current SSH session, verify current date/time settings:
   a. Go to Shell

   ```
   shell
   ```

   b. Verify Date/Time/Timezone:

   ```
   date
   ```

   c. To manually change date/time (based on NetScaler's timezone):

   ```
   date YYYYMMHHSS
   Example:  date 201601151423
   Would change clock to Jan 15, 2016 t 2:23 pm (14:23).
   ```

   d. Exit Shell to return to CLI:

   ```
   exit
   ```

Backing Up System Configuration (Command Line Interface)

1. Create an archive of the nsconfig directory.
   a. Enter the following command in PuTTY to access the NetScaler BSD shell:

   ```
   shell
   ```

   b. Enter the following command to create an archive of the NetScaler configuration:

   ```
   tar -cvzf /var/tmp/backup.tgz /flash/nsconfig
   ```

   An archive of the nsconfig directory named backup.tgz is created in the /var/tmp directory. This archive will serve as a backup for the NetScaler configuration.

   c. View archive:

   ```
   cd /var/tmp/
   ```

   ```
   ls
   ```

d. Enter the following command to return to the NetScaler PuTTY command-line interface:

```
exit
```

2. Copy the newly created backup of the NetScaler configuration from /var/tmp/backup.tgz to your Student Desktop using WinSCP.

   a. Launch **WinSCP** from the Student Desktop.

   b. Double-click the **NSHA1** in the saved sessions pane.

   c. Check the check box **Never show this banner again** and click **Continue**.

   d. Type `nsroot` in the **Password** field and press **Enter**.

   e. In the right pane, double-click the **folder icon** at the top of the pane to navigate up to /<root>.

   f. Navigate to **var** > **tmp** and drag the **backup.tgz** file from the right pane to the left pane. The file will be automatically copied. You may copy the backup.tgz file to C:\resources.

   g. Close the WinSCP window and click **OK** to confirm.

Exercise 1-3: Upgrading the NetScaler System (Command-Line Interface)

This exercise provides step-by-step instructions for completing "Exercise 1-3: Upgrading a NetScaler System" using the command-line interface. This exercise will only be performed using the Command Line Interface.

> **NetScaler appliances can be upgraded from the Configuration Utility or the Command Line Interface. However, there is a bug in the Upgrade GUI in NetScaler 10.5. For the following builds, upgrades to NetScaler 11.0 are only supported from the Command Line Interface:**
>
> - All builds of NetScaler 9.3
> - All builds of NetScaler 10.1
> - Any builds of NetScaler 10.5 prior to 10.5.57.x
>
> Upgrades from one version of NetScaler 11.0 to another version of NetScaler 11.0 can use the Configuration Utility
>
> For simplicity, this exercise will perform the upgrade from the Command Line Interface only. For more details see the NetScaler 11.0 admin guide:
>
> - Upgrading to Release 11.0: http://docs.citrix.com/en-us/netscaler/11/license-upgrade-downgrade/upgrade-downgrade-the-system-software/upgrading-to-release-11.html
> - Upgrading to a Later Build within Release 11.0: http://docs.citrix.com/en-us/netscaler/11/license-upgrade-downgrade/upgrade-downgrade-the-system-software/upgrade-to-later-build-within-11-0.html

Upgrading the NetScaler System (Command-Line Interface)

From the Student Desktop, use a SSH connection (PuTTY) to the NetScaler NSHA1 command-line interface. Log on as the nsroot user for this task.

1. Connect to the NetScaler NSHA1 (172.16.0.5) over SSH (using PuTTY).
2. Use the PuTTY command-line to view the current NetScaler version and save the configuration.
    a. Enter the following command to view the NetScaler version:

    ```
    show ns version
    ```

    The NetScaler version shows as 11.0 Build 55.23.nc

    b. Enter the following command in PuTTY to save the NetScaler configuration, so you can return to the current configuration if the upgrade fails:

    ```
    save ns config
    ```

    > You may receive a message stating that no changes have been made to save.

3. Upgrade the NetScaler system to build version 11.0-63.16.nc.
    a. Enter the following command in PuTTY to access the BSD shell:

    ```
    shell
    ```

    b. Enter the following command in PuTTY to change to the /var/nsinstall/build-11.0-63.16_nc directory:

    ```
    cd /var/nsinstall/build-11.0-63.16_nc/
    ```

    c. Enter the following command in PuTTY to extract the new build file within this directory:

    ```
    tar -zxvf build-11.0-63.16_nc.tgz
    ```

    Wait for the extraction to complete.

    d. Enter the following command to start the NetScaler upgrade script:

    ```
    ./installns
    ```

    e. Enter `Y` when prompted to reboot NetScaler NSHA1 after the installation has completed.

    f. Click **OK** in the message to acknowledge that PuTTY was unexpectedly closed and then wait for NSHA1 to restart.

Verifying the NetScaler Upgrade (Command-Line Interface)

From the Student Desktop, use a SSH connection (PuTTY) to the NetScaler NSHA1 command-line interface. Log on as the nsroot user for this task.

1. Verify that the NetScaler has been upgraded to build version 11.0 Build 63.16.nc.
    a. After the NetScaler has restarted, log on to the PuTTY command-line interface for NSHA1 with the nsroot credentials.
    b. Enter the following command to verify that the NetScaler has been updated to version NS11.0: Build 63.16.nc:

```
show version
```

Module 2

Basic Networking

2

Module 2: Basic Networking Exercises

Exercise 2-1: Configuring Basic Networking

This exercise demonstrates how to enable management access on a subnet IP address and add VLAN to the NetScaler.

Enabling Management Access on a Subnet IP Address (Configuration Utility)

From the Student Desktop, use an HTTP connection to the NetScaler NSHA1 configuration utility. Log on as the nsroot user for this task

Enabling management access on a SNIP is a good way to ensure you are always connected to the primary NetScaler in an HA pair.

1. In the NetScaler NSHA1 configuration utility, enable management access on the 172.16.0.90 SNIP.
    a. Click **Skip** on the **Citrix User Experience Improvement Program window** if needed.
    b. Go to **System** > **Network** > **IPs** and then double-click **172.16.0.90**.
    c. Verify that **Subnet IP** is selected for the Type.
    d. Scroll to the bottom of the screen and select **Enable Management Access control to support the below listed applications**.
    e. Uncheck **Telnet** and **FTP**.
    f. Check **Allow access only to management applications**
    g. Click **OK**.

Adding a SNIP to the NetScaler

From the Student Desktop, use an HTTP connection to the NetScaler NSHA1 configuration utility. Log on as the nsroot user for this task.

For diagnostic purposes, a command line session is also useful.

1. Test network connectivity to other subnets **(Command-Line Interface)**.
    a. Use PuTTY to connect to NetScaler NSHA1: **Start** > **Run** > **putty 172.16.0.5**.
    b. At the cli type `ping -c 2 192.168.10.17` to ping the StoreFront1 Server (This is a resource in the backend network.).
        - Expected Result: The request will time out after two PINGs. (See Note below; this will NOT fail at this point due to changes in the lab environment.)

c. Determine why the request times out. At the command line, type `show ns ip` and view the SNIPs assigned to NetScaler

d. The NetScaler does not have a SNIP on the 192.168.10.0 network. Is there a route? At the command line, type `show route`.

e. There is a default route in place. The router is not routing to 192.168.10.0 or 172.29.10.0.

> Due to a change in the lab networking, the ping test will succeed to the 192.168.10.0 address. All 3 networks are passing through a single router).

2. Add a **SNIP** to the NetScaler using 192.168.10.90 as the IP and 255.255.255.0 as the netmask **(Configuration Utility)**.

   From the Student Desktop, use an HTTP connection to the NetScaler NSHA1 configuration utility logged on as the nsroot user for this task.

   a. Go to **System** > **Network** > **IPs** and then click **Add**.

   b. Type `192.168.10.90` in the **IP Address** field.

   c. Type `255.255.255.0` in the **Netmask** field.

   d. Verify that the **IP Type** is **Subnet IP**.

   e. Verify **Allow access only to management** applications is NOT SELECTED (Disabled).

   f. Click **Create**.

   g. In the putty session, `ping -c 2 192.168.10.17`. Now the StoreFront1 server will reply because the NetScaler is directly attached to the same network as the StoreFront1 Server via the SNIP and now has a route to it.

Configuring VLANs

From the Student Desktop, use an HTTP connection to the NetScaler NSHA1 configuration utility. Log on as the nsroot user for this task.

1. Add VLAN 2 and bind it to interface 1/2 and SNIP 192.168.10.90.

   a. Go to **System** > **Network** > **VLANs** and then click **Add**.

   b. In the **VLAN ID** field enter `2`.

   c. In the **Alias Name** field enter `Backend network`.

   d. Under **Interface Bindings** check the box for interface **1/2**.

   e. Click on the **IP Bindings** tab and check the box for SNIP **192.168.10.90** then click **Create**.

2. Save the NetScaler Configuration.

Exercise 2-1: Configuring Basic Networking (Command Line Interface)

This exercise demonstrates how to enable management access on a subnet IP address, add a static route to a NetScaler system, and examine the network traffic flow. The static route is added to grant access to the back-end resources on the network for lab exercises later in the course.

Configuring Subnet IP Addresses

From the Student Desktop, use a SSH connection (PuTTY) to connect to the NetScaler NSHA1 (172.16.0.5) command-line interface. Log on as the nsroot user for this task.

1. Connect to the NetScaler NSHA1 (172.16.0.5) over SSH (using PuTTY).
2. Modify the existing SNIP (172.16.0.90) so that management access is enabled and so that it is restricted to management communications only.

   ```
   set ns ip 172.16.0.90 -ftp disabled -telnet disabled -
   mgmtAccess enabled -restrictAccess enabled
   ```

3. Add a second SNIP to the NetScaler to access resources in the Backend Network (192.168.10.0/24):

   ```
   add ns ip 192.168.10.90 255.255.255.0 -type SNIP -
   mgmtAccess enabled
   ```

This IP can be used for NetScaler to Server traffic in addition to management access; it is not restricted to management access only.

Configuring VLANs

Continue connecting to the NetScaler NSHA1 (172.16.0.5) over SSH.

1. Create a VLAN for access to the Backend Network:

   ```
   add vlan 2
   ```

2. Bind the interface 1/2 and an appropriate SNIP to vlan 2:

   ```
   bind vlan 2 -ifnum 1/2 -ipaddress 192.168.10.90 255.255.255.0
   ```

3. Display VLAN and Interface details:

   ```
   show vlan
   ```

   ```
   show int
   show int 1/1
   ```

```
show int 1/2
```

4. From the NetScaler CLI, verify you can ping the following addresses. Both tests should be successful. Use CTRL+C to stop output between tests.

```
ping 172.29.10.10
ping 192.168.10.17
```

5. Save the NetScaler configuration:

```
save ns config
```

Module 3

High Availability

3

Module 3: High Availability Exercises

Exercise 3-1: Configuring High Availability

This exercise demonstrates how to create a high-availability pair and how to test the pair for redundancy.

Estimated time to complete this exercise: 15 minutes

Configuring NetScaler High Availability with NSHA1 and NSHA2 (Configuration Utility)

From the Student Desktop, use a web browse to make an HTTP connection to the NetScaler NSHA1 (http://nsha1.training.lab) and in another browser tab, make a connection to NetScaler NSHA2 (http://nsha2.training.lab) configuration utilities. Log on as the nsroot user on each system for this task.

1. Open the configuration utility for both NetScalers in the Chrome browser.
   a. Open two new Chrome browser tabs. In the first window, browse to `http://nsha1.training.lab` (this will be designated as NSHA1). In the second tab, browse to `http://nsha2.training.lab` (this will be designated as NSHA2).
   b. Log on to both NetScalers using the nsroot credentials.
   c. Click **Skip** on the **Citrix User Experience Improvement Program** window if needed.
2. Verify that high availability monitoring is active on one of the interfaces.
   a. NSHA1 and NSHA2: Navigate to **System** > **Network** > **Interfaces**.
   b. NSHA1 and NSHA2: In the Interfaces pane, scroll to the right to verify that high availability monitoring is enabled on interface 1/1 and 1/2.

Configuring High Availability on NSHA1 and NSHA2 (Configuration Utility)

From the Student Desktop, use an HTTP connection to the NSHA1 and NSHA2 configuration utilities logged on as the nsroot user for this task.

1. Configure NSHA2 to stay secondary during the election process for High Availability. Take note of the settings/configuration prior to configuring HA.
   a. NSHA2: Expand the **System** node and click **High Availability**.
   b. NSHA2: Click **Node ID 0** in the **Nodes** pane, then click **Edit**.

   c. NSHA2: Select **STAY SECONDARY (Remain in Listen Mode)** in the **High Availability Status** drop-down menu.
   d. NSHA2: Click **OK**.
2. Configure NSHA1 and NSHA2 to function as a high availability pair. Set NSHA2 as the remote node on NSHA1 and specify both nodes to use the nsroot logon credentials.
   a. NSHA1: Expand the **System** node, then click **High Availability**.
   b. NSHA1: Click **Add** in the **Nodes** pane. The **Create HA Node** dialog box opens.
   c. NSHA1: Type `172.16.0.10` in the **Remote Node IP Address** field, verify that **Configure remote system to participate High Availability setup** and **Turn off HA Monitor interface/channels that are down** are both selected.
   d. NSHA1: In the **Remote System Login Credential**, enter the nsroot/nsroot credentials, then click **Create.**
3. Refresh the NetScaler system configurations and verify that NSHA2 is set up as the Secondary node on NSHA1.
   a. NSHA1 and NSHA2: Expand the **System** node, then click **High Availability**.
   b. NSHA1 and NSHA2: Click the **Refresh** option in the upper right corner of the **Configuration Utility** window.
   c. NSHA1 and NSHA2: Verify that 172.16.0.5 appears as the Primary and 172.16.0.10 appears as the Secondary.
4. Enable NSHA2 Node state to actively participate in High Availability.
   a. NSHA2: Expand the **System** node, then click **High Availability**.
   b. NSHA2: Click **Node ID 0** in the **Nodes** pane and click **Edit**.
   c. NSHA2: Select **ENABLED (Actively Participate in HA)** in the **High Availability Status** drop-down menu.
   d. NSHA2: Click **OK**.

Testing the High-Availability Configuration (Configuration Utility)

From the Student Desktop, use an HTTP connection to the NSHA1 and NSHA2 configuration utilities logged on as the nsroot user for this task.

1. Verify the current state of the high availability pair.
   a. NSHA1 and NSHA1: Expand the **Network** node and select **IPs**.
   b. NSHA1 and NSHA2: Notice the system-owned IP addresses on both NSHA1 and NSHA2. Verify that the SNIP on NSHA1 is duplicated to NSHA2.
2. Ping the NetScaler SNIP continually
   a. From the Student Desktop, open the **Command Prompt** and type `ping -t 172.16.0.90`.
3. Test the high-availability configuration by forcing a failover on NSHA1.

   a. NSHA1 and NetScaler NSHA2: Expand the **System** node and select **High Availability**.

   b. NSHA1: Click **Actions** > **Force Failover**. Click **Yes** to confirm the **Force Failover** and then click **OK**.

   c. NSHA1 and NSHA2: Click the **Refresh** option in the upper-right corner of the configuration utility.

   d. On NSHA1 and NetScaler NSHA2: Verify that the Master State of both nodes:

      - The master state of 172.16.0.5 (NSHA1) is now **Secondary**.
      - The master state of 172.16.0.10 (NSHA2) is now **Primary**.

   e. Note the ping status. Did any packets drop during the failover?

4. Test the high availability configuration by forcing a failover on NSHA2.

   a. NSHA2: Right click **Node ID 1** and click **Force Failover**. Click **Yes** to confirm the **Force Failover** then click **OK**.

   b. NSHA1 and NSHA2: Click the **Refresh** option in the upper-right corner of the configuration utility.

   c. NSHA1 and NSHA2: Verify the master state of both nodes:

      - The master state of (NSHA1) is **Primary** again.
      - The master state of (NSHA2) is **Secondary** again.

   d. Note the ping status. Did any packets drop during the failover?

   e. Close the **Command Prompt** in the to end the continuous ping.

   f. **Save the NetScaler configuration on NSHA1.**

5. Connect to the shared management SNIP:

   a. Open a new browser tab and browse to http://172.16.0.90 or http://netscaler.training.lab. Log on as nsroot/nsroot.

   b. Go to **System** > **High Availability**.

   c. Identify which NetScaler you are connected to by which NetScaler NSIP is listed as Node 0. Expected Result: NSHA1 (172.16.0.5).

   d. The NetScaler SNIP can be used to ensure that you are connected to the current primary member of any HA pair for configuration tasks.

6. Save NetScaler Configuration.

   a. Click the **Save** icon.

   b. Note: If connected to either the current primary NetScaler NSIP or the shared SNIP, the save command will propagate to the secondary NetScaler. Both configurations are now saved in the HA pair.

   c. To confirm, connect to the current secondary NetScaler (NSHA2). Go to **System** > **Diagnostics** > **Saved v/s running**. Verify no differences are found.

NetScaler 2 can either be shutdown or left running for future lab modules. If you receive Propagation errors, shutdown NetScaler 2. Please **DO NOT** break the HA Pair. If the HA pair is broken the secondary NetScaler has to be **Powered OFF** in order to avoid IP conflicts.

Module 4

Integrating NS Gateway with Other Resources (Unified Gateway)

4

Module 4: Integrating NetScaler with XenApp and XenDesktop Using the Unified Gateway Wizard

Exercise 4-1: Unified Gateway Wizard

This exercise demonstrates how to configure NetScaler Gateway to integrate with XenApp and XenDesktop using the Unified Gateway wizard.

Launch the Unified Gateway Wizard

Unified Gateway Wizard

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. Login to the NetScaler with the nsroot/nsroot credentials.
2. On the NetScaler Configuration tab, at the bottom of the left navigation bar under **Integrate with Citrix Products**, click on **Unified Gateway**. This opens the Welcome Screen to the Unified Gateway Wizard.
3. Click **Get Started**.
4. In the **Single Public Access Point** screen, click **Continue**.

Virtual Server

1. In the **Name** field, enter `TrainingLabUGW`.
2. In the **Unified Gateway IP Address** field, assign the IP of `172.16.0.40`.
3. In the **Port** field, verify the HTTPS port `443` is configured.
4. Click **Continue**.

Server Certificate

Install the wildcard certificate from the local computer.

1. Verify that the **Certificate Format** is **pfx**.
2. Click the drop down menu next to **Browse** under **Certificate File** and select **Local**.
3. Browse to **c:\resources\SSL Certificates**.

4. Select the **wildcard-training** certificate and click **Open**.
5. The **Private key is password protected** box should be checked.
6. In the **Private key password** field enter `Password1`.
7. Click **Continue**.
8. Click **OK** on the **Warning** pop-up if needed. Click Continue again after warning.

> Despite the warning that propagation of the SSL certificate failed, the certificate propagtes to the secondary NetScaler.

Authentication

1. The **Primary authentication Method** field should be set to `Active Directory/LDAP`.
2. In the **IP Address** field, enter `192.168.10.11`.
3. The **Port** field should be `389` which is the port for LDAP.
4. In the **Base DN** field, enter `dc=training,dc=lab`.
5. In the **Service account** field, enter `citrixldap@training.lab`.
6. In the **Password** field, enter `Password1`.
7. In the **Confirm Password** field, enter `Password1`.
8. In the **Time out (seconds)** field, enter `3` if not already configured.
9. In the **Server Logon Name Attribute** field, enter `sAMAccountName`.
10. The **Secondary authentication method** field should be `None`.
11. Click **Continue**.

Portal Theme

1. In the **Portal Theme** pull down menu, select either **Default**, which is a black theme, or **Green Bubble**.
2. Click **Continue**.

Applications

1. Click the **+ sign** next to **Applications** and select the **XenApp & XenDesktop** radio button.
2. In the **Choose Integration Point** drop down menu, verify that `StoreFront` is selected.
3. Click **Continue**.

StoreFront

This information can be found on the StoreFront server.

1. In the **StoreFront FQDN** field, enter `storefront.training.lab`.
2. In the **Site Path** field, enter `/Citrix/StoreWeb`.
3. In the **Single Sign-on Domain** field, enter `training`.
4. In the **Store Name** field, enter `Store`.
5. In the **Secure Ticket Authority Server** field, enter `http://xd1.training.lab`.
6. Click the **+ sign** next to the **Secure Ticket Authority Server** field and enter `http://xd2.training.lab`.
7. In the **StoreFront Server** field, enter `192.168.10.17`.
8. Click the **+ sign** next to the **StoreFront Server IP** field and enter `192.168.10.18`.
9. In the **Protocol** field, verify that `HTTP` is selected.
10. In the **Port** field, verify that port `80` is configured.
11. Check the box for **Load Balancing** and enter `172.16.0.22` for the **Virtual Server IP** to load balance Storefront.
12. Click **Continue**.

XenDesktop Farm

1. In the **Configure** drop down menu, select **XenDesktop**.
2. In the XenDesktop Farm **Desktop Delivery Controller Server** field, enter `192.168.10.7`.
3. Click the **+ sign** next to the **Desktop Delivery Controller Server IP** field and enter `192.168.10.8`.
4. The **Services Port** should be **80**.
5. Check the box for **Load Balancing** and enter `172.16.0.21` for the XenDesktop **Virtual Server** IP.
6. Click **Continue**.
7. Click **Done**.
8. Click **Continue** again.
9. Click **Done** once more to exit the wizard.

> Examine all the resources that were created by the NSG Wizard such as the **NetScaler Gateway Virtual Server**, the **LDAP Policy**, the **Session Policies**, the **Content Switch Virtual Server** and the **Content Switch Action and Policy** along with the **Load balancing Virtual Servers**.

Connect to TrainingLabUGW

1. Use the RDP shortcuts on the Student Desktop to connect to the ExternalClient virtual machine. Log on as the local account externalclient\citrix (Password1). (Note: Do not include training as the domain as this machine is in a workgroup.)
2. Select the **Desktop** tile and launch **Internet Explorer**.
3. In the **Address Bar** enter `https://unifiedgateway.training.lab`.
4. In the **User name** field, enter `citrixadmin`.
5. In the **Password** field, enter `Password1`.
6. You will be presented with a Client Choices page.
7. Select **Network Access** and install the NetScaler Gateway Plug-in.
8. Click **Download** to install the NSG plug-in.
9. Click **Save File** to save the AGEE-setup.exe to **Downloads**.
10. Go to **Downloads** and run the **AGEE_setup.exe**, then click **Install**.
11. Click **Yes** on the **UAC** pop up.
12. Click **Finish** to complete the setup.
13. A VPN connection will be established through the Gateway.

Storefront is not yet configured for gateway access so no applications will be available. The STA Servers will also be in a DOWN state until we configure the NetScaler to use DNS. This will be configured in the next module.

14. Click **Logoff in the NetScaler with Unified Gateway portal page**.
15. Click **Exit** to cancel the Citrix Windows Cleanup from the VPN connection dialog.
16. Click **Log on** and Login again with `citrixadmin/Password1`.
17. Click on **Virtual App and Desktop Access** and examine the URL. You are redirected to the **/Citrix/StoreWeb** site and prompted to login to the Storefront server. If prompted, first click Activate Citrix Receiver and then click Allow and Remember before continuing to the login page.
18. StoreFront is not yet configured for the gateway, so pass-through authentication is failing, close the browser.
19. Save the running configuration on the NetScaler.
    a. Click the **Save** icon in the top-right corner of the configuration utility window.
    b. Click **Yes** to confirm saving the configuration. (The saved configuration may be current as the Unified Gateway wizard automatically saves the config at the end of the wizard.)

Module 5

Load Balancing Gateway Services Exercises

5

Module 5: Load Balancing Gateway Services Exercises

Exercise 5-1: Load-Balancing Web Servers

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. In this exercise, you will eliminate single points of failure in your gateway deployment.

Estimated time to complete: 35 minutes

Add Red, Blue and Green Servers to NetScaler (Configuration Utility)

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. Log on to the NetScaler configuration utility with the nsroot credentials via the shared management SNIP.
2. Create the "srv_red" server with 192.168.10.15 for the IP address.
    a. Go to the **Traffic Management** > **Load Balancing** > **Servers** node.
    b. Click **Add** in the **Servers** pane. The **Create Server** window opens.
    c. Type `srv_red` in the **Name** field and then type `192.168.10.15` in the **IPAddress** field.
    d. Type `RED` in the **Comments** field.
    e. Click **Create**.
3. Create the "srv_green" server with 192.168.10.14 for the IP address.
    a. Click **Add** in the **Servers** pane. The **Create Server** window opens.
    b. Type `srv_green` in the **Name** field and then type `192.168.10.14` in the **IPAddress** field.
    c. Type `GREEN` in the **Comments** field.
    d. Click **Create**.
4. Create the "srv_blue" server with 192.168.10.13 for the IP address.
    a. Click **Add** in the **Servers** pane. The **Create Server** window opens.
    b. Type `srv_blue` in the **Name** field and then type `192.168.10.13` in the **IPAddress** field.
    c. Type `BLUE` in the **Comments** field.
    d. Click **Create**. The web servers appear in the **Servers** list.

Creating Load Balanced Services

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log 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. Go to the **Load Balancing** node and click **Services**.
    b. Click **Add** in the **Services** pane. The **Load Balancing Service** window opens.
    c. Type `svc_red` in the **Service Name** field.
    d. Select the **Existing Server** radio button and then select **srv_red (192.168.10.15)** from the **Server** list.
    e. Verify that **HTTP** is selected from the **Protocol** list and `80` is entered in the **Port** field.
    f. Click **OK**, scroll down and click **Done**.
2. Create an HTTP service called "svc_blue" that will be associated with the WebBlue web server.
    a. Click **Add** in the **Services** pane. The **Load Balancing Service** window opens.
    b. Type `svc_blue` in the **Service Name** field.
    c. Select the **Existing Server** radio button and then select **srv_blue (192.168.10.13)** from the **Server** list.
    d. Verify that **HTTP** is selected from the **Protocol** list and `80` is entered in the **Port** field.
    e. Click **OK**, scroll down and click **Done**.
3. Create an HTTP service called "svc_green" that will be associated with the WebGreen web server
    a. Click **Add** in the **Services** pane. The **Load Balancing Service** window opens.
    b. Type `svc_green` in the **Service Name** field.
    c. Select the **Existing Server** radio button and then select **srv_green (192.168.10.14)** from the **Server** list.
    d. Verify that **HTTP** is selected from the **Protocol** list and `80` is entered in the **Port** field.
    e. Click **OK**, scroll down and click **Done**. The Create Service dialog box closes.
4. Verify that all services display **UP** as the state listed in the **Services** pane.

Creating a Load-Balancing Virtual Server

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. Begin the configuration of a "lb_vsrv_colors" load-balancing virtual server that will be associated with the svc_red, svc_blue and svc_green services.

    a. Go to the **Traffic Management** > **Load Balancing** node and click **Virtual Servers**.
    b. Click **Add** in the **Virtual Servers** pane.
    c. Type `lb_vsrv_colors` in the **Name** field and then verify that **HTTP** is selected from the **Protocol** drop-down list.
    d. Type `172.16.0.20` in the **IP Address** field and verify that `80` appears in the **Port** field.
    e. Click **OK** to proceed to the next window where you will bind the services.
    f. Click **No Load Balancing Virtual Server Service Binding** below the **Services and Service Groups** field to go to the **Service Binding** window.
    g. Click in the field below **Select Service** to add the services.
    h. In the **Service** window, select the check boxes next to **svc_red**, **svc_blue** and **svc_green**, then click **Select**.
    i. Click **Bind**, then click **Continue**.

2. Complete the configuration of the "lb_vsrv_colors" load-balancing virtual server by setting a Round-Robin method for load balancing.
    a. Click **Method** on the right pane under **Advanced Settings** and select **ROUNDROBIN** from the **Load Balancing Method** drop-down menu on the left pane.
    b. Click **OK** and then click **Done**.
    c. Verify that the load-balancing virtual server lb_vsrv_colors state is displayed as **UP**.
3. Save the running configuration.
    a. Click the **Save** icon and click **Yes** to confirm the saving of the running configuration.

Testing Load Balancing

From the Student Desktop, use Chrome to make configuration changes to the NetScaler and use Firefox web browser to test access to web pages. Log on as the nsroot user for this task.

1. Test the load-balancing configuration.
    a. Open a browser (Firefox) and browse to http://colors.training.lab/home.php and press **Enter**.

    > A DNS entry for colors.training.lab/ has already been created for your convenience. If the colors.training.lab/home.php page does not display correctly, access the http://colors.training.lab page first and then go to the http://colors.training.lab/home.php page.

    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 in Chrome and go to the **Traffic Management** > **Load Balancing** node and select **Virtual Servers**.
   b. Double-click the **lb_vsrv_colors** virtual server to open its configuration window.
   c. Click the **Persistence** node in the right pane under **Advanced Settings** and change the **Persistence** from **NONE** to **COOKIEINSERT**.
   d. Type `0` in the **Time-out (mins)** field.
   e. Click **OK**, click **OK** in the Warning message (about changing timeout to default) again and then click **Done**.
3. Test the updated load-balancing configuration.
   a. Refresh the browser several times to verify the effects of load balancing with persistence. With cookie persistence enabled and set to "0", you are directed to the same page each time as this is a session cookie; the page does not load balance to each available server.

Resetting Persistence to None

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. Reset the lb_vsrv_colors load-balancing virtual server persistence to none.
   a. Go to the **Traffic Management** > **Load Balancing** node and select **Virtual Servers**.
   b. Double-click the **lb_vsrv_colors** virtual server to open its configuration window.
   c. Click the **Edit** icon (pencil) in the **Persistence** heading and select **NONE** from the **Persistence** drop-down menu.
   d. Click **OK** and then click **Done**. The warning is displayed since the persistence timeout needs to be removed when disabling persistence; this is an information message only. The change to persistence type is still applied.
2. Save the running configuration.
   a. Click the **Save** icon and click **Yes** to confirm the saving of the running configuration.

Exercise 5-2: Load-Balancing a DNS Server

When you request DNS resolution of a host name, NetScaler uses the configured load-balancing method to select a DNS service. The DNS server to which the service is bound then resolves the host name and returns the IP address as the response. The appliance can also cache DNS responses and use the cached information to respond to future requests for resolution of the same host name. Load balancing DNS servers improves DNS fault tolerance and may improve response times.

Estimated time to complete: 35 minutes

Add DNS Servers to NetScaler

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, logged on as the nsroot user for this task. Connect to the NetScaler HA pair (172.16.0.90) over SSH

> Testing DNS resolution on the NetScaler.

1. Connect to the NetScaler shared management SNIP (172.16.0.90) over SSH: **Start** > **Run** > **putty 172.16.0.90** or **putty netscaler.training.lab**.
2. From the SSH session run the command: ping dc.training.lab.

   > You should get an error: ping: cannot resolve dc.training.lab: Host name lookup failure ERROR: This is due to DNS not being previously configured. We will configure DNS on the NetScaler and test again.

3. Switch to a web browser and connect to the NetScaler Configuration Utility for the HA Pair: http://netscaler.training.lab. Log on to the NetScaler configuration utility with the nsroot credentials.
4. Go to **Traffic Management** > **Load Balancing** > **Servers** node.
5. Create the "srv_dc1" server with 192.168.10.11 for the IP address.
   a. Click **Add** in the **Servers** pane. The **Create Server** window opens.
   b. Type `srv_dc1` in the **Name** field and `192.168.10.11` in the **IPAddress** field.
   c. Type `DC1` in the **Comments** field.
   d. Click **Create**.
6. Create the "srv_dc2" server with 192.168.10.6 for the IP address.
   a. Click **Add** in the **Servers** pane. The **Create Server** window opens.
   b. Type `srv_dc2` in the **Name** field and `192.168.10.6` in the **IPAddress** field.
   c. Type `DC2` in the **Comments** field.
   d. Click **Create**.
7. View the servers from the NetScaler command line in the PuTTY session.
   a. At the NetScaler command line, type `show server` and press **Enter**.
   b. The two servers you created are displayed (along with the previous server objects).

Creating DNS Services

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. Create a DNS service called "svc_dns1" that will be associated with the "srv_dc1" server.

    a. Go to the **Load Balancing** node and click **Services**.
    b. Click **Add** in the **Services** pane. The **Load Balancing Service** window opens.
    c. Type `svc_dns1` in the **Service Name** field.
    d. Select the **Existing Server** radio button and select **srv_dc1 (192.168.10.11)** from the **Server** list.
    e. Verify that **DNS** is selected from the **Protocol** drop down menu and the DNS port of `53` is entered in the **Port** field.
    f. Click **OK**, scroll down and click **Done**.

2. Create a DNS service called "svc_dns2" that will be associated with the "srv_dc2" server.
    a. Go to the **Load Balancing** node and click **Services**.
    b. Click **Add** in the **Services** pane. The **Load Balancing Service** window opens.
    c. Type `svc_dns2` in the **Service Name** field.
    d. Select the **Existing Server** radio button and select **srv_dc2 (192.168.10.6)** from the **Server** list.
    e. Verify that **DNS** is selected from the **Protocol** drop down menu and the DNS port of `53` is entered in the **Port** field.
    f. Click **OK**, scroll down and click **Done**.
3. Verify that all DNS services display **UP** as the state listed in the **Services** pane.
4. Verify that all DNS services display **UP** in the command line interface by typing `show service`, or `show service -summary` from the PuTTY session.
5. Get specific information about one of the services you created by typing `show service svc_dns1`.

Creating a DNS Load Balancing Virtual Server

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. Begin the configuration of a "lb_vsrv_dns" load-balancing virtual server that will be associated with the svc_dns1 and svc_dns2.
    a. Go to the **Traffic Management** > **Load Balancing** node and click **Virtual Servers**.
    b. Click **Add** in the **Virtual Servers** pane.
    c. Type `lb_vsrv_dns` in the **Name** field and select **DNS** from the **Protocol** drop-down list box.
    d. Type `172.16.0.99` in the **IP Address** field and verify that the DNS port `53` appears in the **Port** field.
    e. Click **OK** to proceed to the next window where you will bind the services.
    f. Click **No Load Balancing Virtual Server Service Binding** to go to the **Service Binding** window.

   g. Click in the field below **Select Service** to add the services.
   h. In the **Service** window, select the check boxes next to the **svc_dns1** and **svc_dns2** services then click **Select**.
   i. Click **Bind**, then click **Continue**.

2. Complete the configuration of the "lb_vsrv_dns" load-balancing virtual server by setting a round-robin method for load balancing.
   a. Click the **Method** node in the right pane and select **ROUNDROBIN** from the **Load Balancing Method** drop-down menu.
   b. Click **OK** and then click **Done**.
   c. Verify that the load-balancing virtual server **lb_vsrv_dns** state is displayed as **UP**.
3. Save the running configuration.
   a. Click the **Save** icon and click **Yes** to confirm the saving of the running configuration.

Testing DNS Load Balancing

From the Student Desktop, use the windows command prompt to perform nslookup commands to the DNS load balancing virtual server.

1. Test the load-balancing configuration from the Student Desktop
   a. Open a windows command prompt and type `nslookup` and press **Enter**.
   b. At the nslookup prompt, type `server 172.16.0.99` and press **Enter**. The workstation will now use 172.16.0.99 for DNS queries within this session instead of its default DNS server.
   c. Alternate method. From cmd prompt, run command: nslookup gateway.training.lab 172.16.0.99. This forces nslookup to use the specified DNS server.
   d. Now type `gateway.training.lab` and press **Enter**. The IP address for gateway.training.lab is returned 172.16.0.30.
   e. Type `exit` when ready to exit nslookup.
2. Configure the NetScaler to use the DNS load balancing virtual server.

   Now configure the NetScaler to use a DNS virtual server instead, so that even if one DNS server goes down, the NetScaler will still be able to query the other DNS server.

   a. In the NetScaler configuration utility, go to the **Traffic Management** > **DNS** > **Name Servers** node.
   b. On the right pane click **Add** to open the **Create Name Server** dialogue.
   c. Select the **DNS Virtual Server** radio button.
   d. In the **DNS Virtual Server** drop down menu, select `lb_vsrv_dns`.
   e. In the **Protocol** pull down menu, verify that `UDP` is selected.
   f. Verify that **Enable Name Server** is checked.
   g. Click **Create**.

> Test pinging dc2.training.lab from the PuTTY session and see the result. You should get a response of 192.168.10.6 as DNS resolution now works on the NetScaler. Stop the ping command in the PuTTY session (CTRL + C). The STA servers configured on the Gateway Virtual Server UG_VPN_TrainingLabUGW should also be UP.

3. Create a DNS specific monitor for DNS services

   By default, the NetScaler will monitor UDP services such as DNS with a ping monitor. This means that if the DNS service on the server stops, but the server still replies to pings, the NetScaler would send DNS requests to a down server. In this exercise, you will create a layer 7 monitor which will accurately confirm DNS is functional.

   From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

   a. In the NetScaler configuration utility, go to the **Traffic Management** > **Load Balancing** > **Monitors** node.

   b. Click **Add** to open the **Create Monitor** dialogue.

   c. In the **Name** field, type `mon_dns`.

   d. Select **DNS** from the **Type** drop down menu.

   e. Note the **Interval**, **Response Time-out** and **Down Time** fields. Place the mouse over the question mark next to each field for a description of what it controls and its options.

   f. Select the **Special Parameters** tab.

   g. In the **Query** field, type `gateway.training.lab`.

   h. Confirm the **Query Type** drop down is set to `Address`.

   i. In the **IP Address** field, type the IP of gateway.training.lab which is `172.16.0.30`.

   j. Click the **+ sign** to add the IP address.

   k. Click **Create**.

4. Bind mon_dns to svc_dns1 and svc_dns2. (Resources can be created/configured using different steps on NetScaler).

   a. In the NetScaler configuration utility, go to the **Traffic Management** > **Load Balancing** > **Services** node.

   b. Highlight **svc_dns1**, then click **Edit**.

   c. In the **Monitors** pane, click in the field **1 Service to Load Balancing Monitor Binding**.

   d. Click **Add Binding**.

   e. Under **Select Monitor**, click the arrow to the right of the **Click to select** field.

   f. Select the radio button for **mon_dns**, then click **Select** at the top of the pane.

   g. Then click **Bind**.

   h. Click **Close**, then click **Done**.

   i. Now click the **Refresh** icon next to the save icon on the NetScaler configuration utility and confirm the service shows as up.
   j. Repeat this procedure to bind **mon_dns** to the **svc_dns2** service.
5. Save the NetScaler configuration.

Exercise 5-3: Load-Balancing LDAP Servers

Load balance LDAP servers for redundancy and improved performance for authenticating users.

Create a LDAP Monitor

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. Log on to the NetScaler configuration utility with the nsroot credentials: http://netscaler.training.lab.
2. Create the "mon_ldap" monitor and bind it to the LDAP services. The services will be configured using the existing **srv_dc1** and **srv_dc2** servers.
   a. Go to the **Traffic Management** > **Load Balancing** > **Monitors** node.
   b. Click **Add** in the **Monitors** pane. The **Create Monitor** window opens.
   c. Type `mon_ldap` in the **Name** field and select **LDAP** from the **Type** drop down menu.
   d. Click the **Special Parameters** tab.
   e. Click the arrow under **Script Name** and select **nsldap.pl** from the list.
   f. Enter `dc=training,dc=lab` in the **Base DN** field.
   g. Enter `citrixldap@training.lab` in the **Bind DN** field.
   h. Enter `memberOf` in the **Attribute** field.
   i. Enter `Password1` in the **Password** field.
   j. Click **Create**.

Creating LDAP Services

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. Create a LDAP service called "svc_ldap1" that will be associated with the "srv_dc1" server.
   a. Go to the **Load Balancing** node and click **Services**.
   b. Click **Add** in the **Services** pane. The **Load Balancing Service** window opens.
   c. Type `svc_ldap1` in the **Service Name** field.

   d. Select the **Existing Server** radio button and select **srv_dc1 (192.168.10.11)** from the **Server** list.
   e. Select **TCP** from the **Protocol** drop down menu and `389` is entered in the **Port** field.
   f. Click **OK**.
   g. Under **Monitors**, click **1 Service to Load Balancing Monitor Binding**, then click **Add Binding**.
   h. Click in the field under **Select Monitor** and check the radio button for **mon_ldap** then click **Select**.
   i. Click **Bind**, click **Close**, then click **Done**.

2. Create a DNS service called "svc_ldap2" that will be associated with the "srv_dc2" server.
   a. Click **Add** in the **Services** pane. The **Load Balancing Service** window opens.
   b. Type `svc_ldap2` in the **Service Name** field.
   c. Select the **Existing Server** radio button and select **srv_dc2 (192.168.10.6)** from the **Server** list.
   d. Select **TCP** from the **Protocol** drop down menu and `389` is entered in the **Port** field.
   e. Click **OK**.
   f. Under **Monitors**, click **1 Service to Load Balancing Monitor Binding**, then click **Add Binding**.
   g. Click in the field under **Select Monitor** and check the radio button for **mon_ldap** then click **Select**.
   h. Click **Bind**, click **Close**, then click **Done**.
3. Verify that all services display **UP** as the state listed in the **Services** pane.

Creating a LDAP Load-Balancing Virtual Server

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. Begin the configuration of a "lb_vsrv_ldap" load-balancing virtual server that will be associated with the svc_ldap1 and svc_ldap2.
   a. Go to the **Traffic Management** > **Load Balancing** node and click **Virtual Servers**.
   b. Click **Add** in the **Virtual Servers** pane.
   c. Type `lb_vsrv_ldap` in the **Name** field and select **TCP** from the **Protocol** drop-down list.
   d. Type `172.16.0.110` in the **IP Address** field and `389` in the **Port** field.
   e. Click **OK** to proceed to the next window where you will bind the services.
   f. Click **No Load Balancing Virtual Server Service Binding** to go to the **Service Binding** window.
   g. Click in the field below **Select Service** to add the services.

    h. In the **Service** window, select the check boxes next to the **svc_ldap1** and **svc_ldap2** services then click **Select**.

    i. Click **Bind**, then click **Continue**.

2. Complete the configuration of the "lb_vsrv_ldap" load-balancing virtual server by setting a round-robin method for load balancing.

    a. Click the **Method** node in the right pane and select **ROUNDROBIN** from the **Load Balancing Method** drop-down menu.

    b. Click **OK** and then click **Done**.

    c. Verify that the load-balancing virtual server **lb_vsrv_ldap** state is displayed as **UP (A refresh may be required)**.

    > The lb_vsrv_ldap server will be used for LDAP authentication in future lab modules.

3. Save the running configuration.

    a. Click the **Save** icon and click **Yes** to confirm the saving of the running configuration.

Module 6

NetScaler Security and SSL

6

Module 6: SSL Offload Exercises

Exercise 6-1: Configuring SSL Certificates and SSL Offload

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

Before You Begin

All lab virtual machines, except for Insight Center should be running. In addition, be sure the XenDesktop Controllers, StoreFront servers, and VDA's (Win8XD1 and WinXD2) are also powered on. The VDA's will not power on dynamically due to a launch request and must be powered-on manually via XenCenter. The complete list of virtual machines is included for reference:

- DC.training.lab (Domain Controller)
- DC2.training.lab (Domain Controller 2)
- NSHA1 (NetScaler HA 1)
- NSHA2 (NetScaler HA 2)
- WebBlue
- WebGreen
- WebRed
- SF1
- SF2
- XD1
- XD2
- Win8XD1
- Win8XD2
- ExternalClient

Estimated time to complete this exercise: 20 minutes

Creating an RSA Key

From the Student Desktop, use an HTTP connection to the NetScaler configuration utility (http://netscaler.training.lab) logged on as the nsroot user for this task.

1. Use the NetScaler certificate tools to create an RSA key file called colors.key with a key size of 2048 and DES3 as the encoding algorithm.
    a. Go to the **Traffic Management** > **SSL** node and click **Create RSA Key** in the **SSL** pane on the right. The **Create RSA Key** dialog box opens.

b. Type `colors.key` in the **Key Filename** field and `2048` in the **Key Size** field.

c. Select **3** from the **Public Exponent Value** drop down menu and verify that **PEM** is selected as the **Key Format**.

d. Select **DES3** as the **PEM Encoding Algorithm** and type `Password1` in the **PEM Passphrase** and **Confirm PEM Passphrase** fields.

> In a production environment, specify a secure passphrase.

e. Click **Create**.

Creating a Certificate Request

From the Student Desktop, use an HTTP connection to the NetScaler configuration utility logged on as the nsroot user for this task.

1. Use the NetScaler Certificate tools to create a Certificate Request named colors.csr using colors.key as the key file and Colors Inc. as the company information.

   a. Go to the **Traffic Management** > **SSL** node and select **Create Certificate Signing Request (CSR)** under **SSL Certificates**. The **Create Certificate Signing Request (CSR)** dialog box opens.

   b. Type `colors.csr` in the **Request File Name** field.

   c. Click the **down arrow** to the right of the **Key Filename** field and select **Appliance**.

   d. Select **colors.key** from the current directory, then click **Open**.

   e. Type `Password1` in the **PEM Passphrase** field.

   f. Provide the following information in the **Distinguished Name Fields**:

      - Country: `UNITED STATES`
      - State or Province: `California`
      - Organization Name: `Colors, Inc.`
      - Common Name: `colors.training.lab`

   g. 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.

   h. Type `Colors, Inc.` in the **Company Name** field.

   i. Click **Create**.

Submitting the Certificate Request for the Web Server

From the Student Desktop, use an HTTP connection to the NetScaler configuration utility logged on as the nsroot user for this task.

1. Open and view the certificate request.
   a. Go to the **Traffic Management** > **SSL** node and click **Manage Certificates/Keys/CSRs** under **Tools** on the right pane. The **Manage Certificates** dialog box opens.
   b. Select the **colors.csr** file and click **View**.
   c. Click in the **View File** window and press **Ctrl + A** to select all of the contents of the Certificate Request, then press **Ctrl +C** to copy the contents to the clipboard.

   > Ensure that you copy the entire contents of the request including the first and last lines. You can also click the link that appears at the top of the window after the CSR is created.

   d. Click **Close** and then click **Close** to close the **Manage Certificates** window.
2. Submit the certificate request to the Certificate Authority on dc.training.lab and download the certificate.
   a. Open a browser and browse to `http://dc.training.lab/certsrv` and then log on using the CitrixAdmin and Password1 credentials, if prompted.
   b. Select **Request a certificate** and then select **advanced certificate request**.
   c. Right-click within the **Base-64-encoded certificate request** field and select **Paste**.
   d. Select **Web Server** in the **Certificate Template** field and click **Submit**. The Certificate Authority will take a few moments to process the request and will then present the certificate for download.

   > If you have problems with the Microsoft Certificate Services, then restart the Active Directory Certificate Services service on the Domain Controller Server.

3. Download the certificate and save the file as **colors_cert.cer**.
   a. Select **Base 64 encoded** and click **Download certificate**.
   b. Select **Save File** and select the **Downloads** folder.

   > If you are using the Chrome browser, you will not be presented with the Save File option. Click **Downloads** to continue. Rename the file if needed.

   c. Type `colors_cert` for the file name and then click **Save**.
   d. Close the browser.

Configuring a Certificate-Key Pair

From the Student Desktop, use an HTTP connection to the NetScaler 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. Go to **Traffic Management** > **SSL** > **Certificates** and click **Install**. The **Install Certificate** dialog box opens.
    b. Type `colors.training.lab` in the **Certificate-Key Pair Name** field.
    c. Click the **down arrow** to the right of the **Certificate File Name** field and select **Local**.
    d. Select **colors_cert** from the **Downloads** directory and click **Open**.
    e. Click the **down arrow** to the right of the **Key File Name** field and select **Appliance**.
    f. Select the **colors.key** file and click **Open**.
    g. Verify that **PEM** is selected for the **Certificate Format**.
    h. Type `Password1` in the **Password** field and click **Install**. The window will close.
2. Verify that colors.training.lab is displayed in the SSL Certificates pane and the status is shown as VALID. Click OK on the synchronization error if encountered; note the certificate files still synchronized to the secondary NetScaler.

> If you get a message that the **certificate is not yet valid**, verify the time on NSHA1 matches the time on NSHA2. From the CLI, use the Date command on the Shell to check the date and time on the NetScaler.

Creating an SSL Offload Virtual Server

From the Student Desktop, use an HTTP connection to the NetScaler configuration utility logged on as the nsroot user for this task.

1. Begin the configuration of the "ssl_vsrv_colors" SSL-offload virtual server with an IP address of 172.16.0.20 and Round Robin as the load balancing method.
    a. Go to **Traffic Management** > **Load Balancing** > **Virtual Servers** and click **Add**. The **Load Balancing Virtual Server** dialog box opens.
    b. Type `ssl_vsrv_colors` in the **Name** field.
    c. Select **SSL** in the **Protocol** field and verify that `443` appears in the **Port** field.
    d. Type `172.16.0.20` in the **IP Address** field.
    e. Click **OK**.
    f. Click **No Load Balancing Virtual Server Service Binding** below **Services and Service Groups** section to bind services to the virtual server.
    g. In the **Service Binding** window, click in the field below **Select Service** and select the check boxes next to **svc_red**, **svc_blue** and **svc_green** then click **Select**, then click **Bind**.

    h. Click **Continue**.
    i. Click **Continue** again.
    j. Click the **Method** node under **Advanced Settings** on the right.
    k. Select **ROUNDROBIN** as the **Load Balancing Method** on the left pane.
    l. Click **OK**.

2. Complete the configuration of the ssl_vsrv_colors SSL-offload virtual server by adding the colors.training.lab certificate to the virtual server.
    a. Click in the **No Server Certificate** field under **Certificates** and then click in field below **Select Server Certificate**.
    b. Click the radio button next to the **colors.training.lab** certificate.
    c. Click **Select**.
    d. Click **Bind** and then click **Done**. The **Load Balance Virtual Server** dialog box closes.
    e. Verify that the ssl_vsrv_colors SSL virtual server displays the state as **UP**.

    > If the Virtual Server shows as Down, you will need to click the refresh button on the top right of the GUI.

3. Save the NetScaler configuration by clicking the **Save** icon in the upper-right corner of the configuration utility.
4. Click **Yes** to confirm the saving of the configuration.

Testing SSL Offload

From the Student Desktop, use an HTTP connection to the **NetScaler SNIP** logged on as the nsroot user for this task.

1. Open a secure connection to the virtual server and test the SSL Offload configuration.
    a. Open a Firefox or Chrome browser, browse to `https://colors.training.lab/home.php` and press **Enter**.
    b. 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.

    > This is an effective way to secure simple HTTP servers. All communication between the client and NetScaler is secured with SSL while back end communications are still over HTTP. This does not require extra resources of the back end servers while providing the benefit of front end security.

Exercise 6-2: Configuring Load Balancing for XenDesktop Delivery Controllers

This exercise demonstrates how to configure a load-balancing virtual server for XenDesktop Delivery Controllers.

Create Server Instances for the XenDesktop Delivery Controllers

From the Student Desktop, use an HTTP connection to the **NetScaler SNIP** logged on as the nsroot user for this task.

1. Browse to `http://netscaler.training.lab` and log on to the configuration utility with the `nsroot` credentials.

> The Server objects were already created by the NetScaler Gateway Wizard. Servers 192.168.10.7 and 192.168.10.8 already exist so we can bind them to the Services.

Create a Monitor for the XenDesktop Delivery Controller Services

From the Student Desktop, use an HTTP connection to the **NetScaler SNIP** logged on as the nsroot user for this task.

1. Create a new monitor for the XenDesktop Delivery Controllers called "mon_xd_ddc".
    a. Go to the **Traffic Management** > **Load Balancing** node and select **Monitors**.
    b. Click **Add** at the top of the **Monitors** pane.
    c. Type `mon_xd_ddc` in the **Name** field and then select **CITRIX-XD-DDC** from the **Type** drop-down menu.
    d. Scroll to the bottom of the page and select the **Secure** check box.
    e. Click **Create**.

Create Load-Balancing Services for the XenDesktop Delivery Controllers

From the Student Desktop, use an HTTP connection to the **NetScaler SNIP** logged on as the nsroot user for this task.

1. Create the "svc_xd1" service for the 192.168.10.7 server and bind the mon_xd_ddc monitor to it.

    a. Go to the **Traffic Management** > **Load Balancing** node and select **Services**.
    b. Click **Add** at the top of the **Services** pane.
    c. Type `svc_xd1` in the **Service Name** field, select the **Existing Server** radio button, then select **192.168.10.7 (192.168.10.7)** from the **Server** drop-down list.
    d. Select **SSL** as the **Protocol** and verify that `443` is listed as the port.
    e. Click **OK**, then click **1 Service to Load Balancing Monitor Binding** under the **Monitors** section.
    f. Click **Add Binding**, then click in the field below **Select Monitor**.
    g. Select the **mon_xd_ddc** monitor from the list and then click **Select**.

> If you do not see the **mon_xd_ddc** monitor it might be located on page 2 of the monitor list.

    h. Click **Bind**, click **Close** and then click **Done**.

2. Create the "svc_xd2" service for the 192.168.10.8 server and bind the mon_xd_ddc monitor to it.
    a. Click **Add** at the top of the **Services** pane.
    b. Type `svc_xd2` in the **Service Name** field, select the **Existing Server** radio button, then select **192.168.10.8 (192.168.10.8)** from the **Server** drop-down list.
    c. Select **SSL** as the **Protocol** and verify that `443` is listed as the port.
    d. Click **OK**, then click **1 Service to Load Balancing Monitor Binding** under the **Monitors** section.
    e. Click **Add Binding**, then click in the field below **Select Monitor**.
    f. Select the **mon_xd_ddc** monitor from the list and click **Select**.
    g. Click **Bind**, click **Close** and then **Done**.

Importing a PKCS#12 Certificate

> This is just for student Reference as the certificate was previously imported by the NSG Wizard. This step can be skipped.

From the Student Desktop, use an HTTP connection to the **NetScaler SNIP** logged on as the nsroot user for this task.

1. Import a certificate file named wildcard.cert and convert it to PEM format to be used on the NetScaler.
    a. Go to **Traffic Management** > **SSL** and click **Import PKCS#12** under the **Tools** section.
    b. Type `wildcard.cert` in the **Output File Name** field.

c. Click **Browse** next to the **PKCS12 File** field (browse local), type `C:\resources\SSL Certificates\` and click **Open**.

d. Double-click the **SSL Certificates** folder, select **wildcard-training.pfx** and click **Open**.

e. Type `Password1` in the **Import Password** field.

f. Select **DES3** in the **Encoding Format** field.

g. Type `Password1` in the **PEM Passphrase** field and in the **Confirm PEM Passphrase** field.

h. Click **OK**.

2. Create a new certificate object on the NetScaler that uses the files you just imported.

> This is just for student Reference as the certificate was previously imported by the NSG Wizard. This step can be skipped.

a. Go to the **Traffic Management** > **SSL** > **Certificates** node.

b. Click **Install**. The **Install Certificate** screen opens.

c. Type `wildcard.training.lab` in the **Certificate-Key Pair Name** field.

d. Click **Browse** next to the **Certificate File Name** field, select **wildcard.cert** then click **Open**.

e. Click **Browse** next to the **Key File Name** field and select **wildcard.cert** then click **Open**.

f. Type `Password1` in the **Password** field, then click **Install**.

Create a Load-Balancing Virtual Server for the XenDesktop Delivery Controllers

In the Student Desktop virtual machine, use an HTTP connection to the **NetScaler SNIP** logged on as the nsroot user for this task.

1. Create the "ssl_vsrv_xd" load-balancing virtual server with an IP address of 172.16.0.21 and bind the svc_xd1 and svc_xd2 services.

a. Go to the **Traffic Management** > **Load Balancing** node and select **Virtual Servers**.

b. Click **Add** at the top of the **Virtual Servers** pane.

c. Type `ssl_vsrv_xd` in the **Name** field.

d. Select **SSL** as the protocol and verify that `443` is listed as the port.

e. Type `172.16.0.21` in the **IP Address** field.

f. Click **OK**, click **No Load Balancing Virtual Server Service Binding** under the **Services and Service Groups** section.

g. Click in the field below **Select Service**, then click the check boxes next to **svc_xd1** and **svc_xd2**.

h. Click **Select**, click **Bind** and then click **Continue**.

i. Click **Continue**.

j. Scroll to the top and then click the **Edit** icon (pencil) in the **Basic Settings** heading and then click **More**.

k. Scroll to the bottom of the page and type `XenDesktop Delivery Controllers LB virtual server` in the **Comments** field.

l. Click **Continue** and then **Continue** again.

m. Click **No Server Certificate** under the **Certificates** field.

n. Click in the field below **Select Server Certificate** and select the **wildcard-training.pfx_CERT_KEY** radio button.

o. Click **Select**.

p. Click **Bind** and then click **Done**.

Verifying the Load-Balancing Configuration

From the Student Desktop, use an HTTP connection to the **NetScaler SNIP** logged on as the nsroot user for this task.

1. View the load-balancing virtual servers and verify that the new XenDesktop virtual server state displays as **UP**.
   a. Go to the **Traffic Management** > **Load Balancing** > **Virtual Servers** nodes.
   b. Verify that the load balancing virtual server titled **ssl_vsrv_xd** effective state shows as **UP**. This virtual server will take incoming Delivery Controller connections and forward the traffic to their respective services. It may take a few moments for the virtual server to register as UP. Refresh the load-balancing virtual servers pane after a minute if the virtual server appears to be **DOWN**.
   c. Save the NetScaler configuration by clicking the **Save** icon in the upper-right corner of the configuration utility.
   d. Click **Yes** to confirm the saving of the configuration.

Exercise 6-3: Configuring Load Balancing for Citrix StoreFront

This exercise demonstrates how to configure load balancing for StoreFront servers on the NetScaler.

Create Server Instances for the StoreFront Servers

From the Student Desktop, use an HTTP connection to the **NetScaler SNIP** logged on as the nsroot user for this task.

The Server objects were already created by the NetScaler Gateway Wizard. Servers 192.168.10.17 and 192.168.10.18 already exist so we can bind them to the Services.

Create a Monitor for the StoreFront Services

In the Student Desktop virtual machine, use an HTTP connection to the **NetScaler SNIP** logged on as the nsroot user for this task.

1. Create a new monitor for the StoreFront servers called "mon_storefront".
    a. Go to the **Traffic Management** > **Load Balancing** node and select **Monitors**.
    b. Click **Add** at the top of the **Monitors** pane.
    c. Type `mon_storefront` in the **Name** field and then select **STOREFRONT** from the **Type** drop-down list.
    d. Scroll to the bottom of the page and select **Secure**.
    e. Click **Create**.

Create Load-Balancing Services for the StoreFront Servers

From the Student Desktop, use an HTTP connection to the **NetScaler SNIP** logged on as the nsroot user for this task.

1. Create the "svc_sf1" service that has the 192.168.10.17 server and bind the mon_storefront monitor to it.
    a. Go to the **Traffic Management** > **Load Balancing** node and select **Services**.
    b. Click **Add** at the top of the **Services** pane.
    c. Type `svc_sf1` in the **Service Name** field and select the **Existing Server** radio button.
    d. Select **192.168.10.17 (192.168.10.17)** from the **Server** drop-down list.
    e. Select **SSL** from the **Protocol** drop-down list and verify that `443` is listed as the port.
    f. Click **OK**.
    g. Click **1 Service to Load Balancing Monitor Binding** below the **Monitors** section and then click **Add Binding**.
    h. Click in the field below **Select Monitor**.
    i. Select the **mon_storefront** radio button, then click **Select**.
    j. Click **Bind**, then click **Close**.
    k. Click **Done**.
2. Create the "svc_sf2" service that has the 192.168.10.18 server and bind the mon_storefront monitor to it.
    a. Click **Add** at the top of the **Services** pane.

b. Type `svc_sf2` in the **Service Name** field and select the **Existing Server** radio button.

c. Select **192.168.10.18 (192.168.10.18)** from the **Server** drop-down list.

d. Select **SSL** from the **Protocol** drop-down list and verify that `443` is listed as the port.

e. Click **OK**.

f. Click **1 Service to Load Balancing Monitor Binding** below the **Monitors** section and then click **Add Binding**.

g. Click in the field below **Select Monitor**.

h. Select the **mon_storefront** radio button, then click **Select**.

i. Click **Bind**, click **Close**, then click **Done**.

Configuring Load Balancing for the StoreFront Servers

From the Student Desktop, use an HTTP connection to the **NetScaler SNIP** logged on as the nsroot user for this task.

1. Create the "ssl_vsrv_sf" load-balancing virtual server with an IP address of 172.16.0.22 and bind the svc_sf1 and svc_sf2 services.

    a. Go to the **Traffic Management** > **Load Balancing** node and select **Virtual Servers**.

    b. Click **Add** at the top of the **Virtual Servers** pane.

    c. Type `ssl_vsrv_sf` in the **Name** field.

    d. Select **SSL** in the **Protocol** drop-down list and verify that `443` is listed as the port.

    e. Type `172.16.0.22` in the **IP Address** field.

    f. Click **More**, type `StoreFront LB virtual server` in the **Comments** field and then click **OK**.

    g. Click **No Load Balancing Virtual Server Service Binding** under the **Services and Service Groups** section.

    h. Click in the field below **Select Service** and check the boxes next to **svc_sf1** and **svc_sf2**.

    i. Click **Select**, then click **Bind**.

    j. Click **Continue**, then click **Continue** again.

    k. Select the **Persistence** node in the right pane, select **SOURCEIP** from the **Persistence** drop down menu and change the **Time-out (mins)** to `20` minutes, then click **OK**.

    l. Click **No Server Certificate** under **Certificates** on the left pane.

    m. Click in the field below **Select Server Certificate** and check the radio button next to **wildcard-training.pfx_CERT_KEY**.

    n. Click **Select**, then click **Bind**.

    o. Click **Done**.

    p. Click the **Save** icon and click **Yes** to confirm the saving of the running configuration.

Updating StoreFront to Use Load-Balancing Virtual Servers

Connect to StoreFront1 (SF1) as training\CitrixAdmin (Password1) to modify the StoreFront configuration. Use the RDP shortcuts on the desktop or the XenCenter console.

1. Connect to the SF1 virtual machine:
    a. Use the RDP shortcut (Windowed or FullScreen) on the desktop to connect to SF1.
    b. Log on as training\citrixadmin. The password is Password1.
2. Click the **Citrix StoreFront** icon in the taskbar of the StoreFront 1 virtual machine and click on Yes to accept the User Access Control dialog box.

    > It may take a moment to load the snap-in for the MMC. If you receive a message that the snap-in is not responding, click the X in the upper-right corner of the message and continue with this exercise.

3. Update the StoreFront store to use the XenDesktop Delivery Controller load-balancing virtual server.
    a. Select **Stores** from the left pane and then click **Manage Delivery Controllers** in the right pane.
    b. Select **Nimbus** and then click **Edit**.
    c. Select **xd1.training.lab** in the **Servers** field and then click **Edit**.
    d. Type `nimbus.training.lab` in the **Server name** field and then click **OK**.

        > A DNS entry has already been configured for nimbus.training.lab and http://storefront.training.lab for your convenience.

    e. Select **xd2.training.lab** in the **Servers** field, click **Remove**, click **OK** and then click **OK** again.
4. Update the Base URL for StoreFront to respond to storefront.training.lab.
    a. Select **Server Group** in the left pane and then click **Change Base URL** in the right pane.
    b. Type `https://storefront.training.lab` in the **Base URL** field and then click **OK**.
5. Propagate all changes to the Storefront 2 server.
    a. Select **Server Group** in the left pane, click **Propagate Changes** in the right pane, then click **Yes**.

        > This process will take a moment to complete.

    b. When the propagate changes process is completed, click **OK**.
6. Exit the RDP session and switch to the Student Desktop.

Testing StoreFront Load-Balancing Configuration

From the Student Desktop, use an HTTP connection to the NetScaler SNIP. Log on as the nsroot user for this task.

1. Log on to the StoreFront website using the load-balanced servers and launch a published desktop.
   a. Open a new browser window on the Student Desktop and go to `https://storefront.training.lab/Citrix/StoreWeb`.

      > Ignore any Certificate warnings or add exceptions if needed.

      > If prompted, select **Activate Citrix Receiver** or **Allow plugins from the StoreFront URL to run**.

      > It may take a few moments for the logon page to display.

   b. Log on to StoreFront using the following credentials:
      - Username: `training\CitrixAdmin`
      - Password: `Password1`

   c. Click the **XenDesktop** icon in the StoreFront interface. The published desktop launches.
   d. Close the published desktop and close the browser window.

Exercise 6-4: Configuring a NetScaler Gateway Virtual Server

This exercise demonstrates how to configure a NetScaler Gateway virtual server using the wizard.

NetScaler Gateway Wizard

From the Student Desktop, use an HTTP connection to the NetScaler configuration utility logged on as the nsroot user for this task.

1. From the Student Desktop, connect to the configuration utility for NetScaler: http://172.16.0.90 or http://netscaler.training.lab.
2. In the NetScaler configuration utility, select the **NetScaler Gateway** node and click **NetScaler Gateway wizard** under **Getting Started** in the **NetScaler Gateway** pane.

3. Click on **Create New NetScaler Gateway** on the top right of the Dashboard.
4. Configure a NetScaler Gateway virtual server with an IP address of 172.16.0.30 on port 443 called gateway.training.lab.
    a. Type `172.16.0.30` in the **NetScaler Gateway IP Address** field and verify that `443` appears in the **Port** field.
    b. Type `gateway.training.lab` in the **Virtual Server Name** field.
    c. Check the box **Redirect requests from port 80 to secure port**.
    d. Type `gateway.training.lab` in the **Gateway FQDN** field, then click **Continue**.
    e. Select **Use existing certificate** option and select **wildcard-training.pfx_CERT_KEY** from the **Server Certificate** drop-down list, then click **Continue**.
    f. Select **Local** from the **Primary authentication method** drop-down list and type `test` in the **User Name** field.
    g. Type `test` in the **Password** field, then click **Continue**.
    h. Review all settings. Click **Done**. The **Dashboard** is displayed.
    i. Close the NetScaler Gateway page to return to the **Configuration** tab.
    j. Select the **NetScaler Gateway** node and then select **Virtual Servers**.
    k. Select the **gateway.training.lab** virtual server and click **Edit**.
    l. Scroll down and select **1 Session Policy** from the **Policies** section.
    m. Select the **172.16.0.30_443_POL** policy, click the **Edit** button and then select **Edit Profile** from the drop-down list.
    n. Select the **Override Global** box next to **DNS Virtual Server** and verify that **lb_vsrv_dns** is pre-selected in the **DNS Virtual Server** field.
    o. Click **OK**.
    p. Click the **Edit** button and then select **Edit Binding**.
    q. Change the priority to `100`, click **Bind**, **Close** and then click **Done**.
5. Save the NetScaler configuration by clicking the **Save** icon in the upper-right corner of the configuration utility.
6. Click **Yes** to confirm the saving of the configuration.

Enabling Split Tunneling

From the Student Desktop, use an HTTP connection to the NetScaler configuration utility logged on as the nsroot user for this task.

1. Enable NetScaler Gateway split tunneling using the NetScaler configuration utility.
    a. Go to the **NetScaler Gateway** > **Global Settings** node.
    b. Select **Change global settings**.
    c. Click the **Client Experience** tab and select **ON** in the **Split Tunnel** drop-down menu.
    d. Click **OK**.

> This step is not necessary for NetScaler Gateway functionality. However, enabling split tunneling ensures that connections to the configuration utility and other open applications will be maintained while you are logged on to NetScaler Gateway.

> Split tunneling will be enabled for all NetScaler Gateway virtual servers unless it has been disabled in a session policy bound at the virtual servers, groups or users level.

2. Create an intranet application called "172.16.0.0_network" in the NetScaler Gateway Resources.
    a. In the left pane, select **NetScaler Gateway** > **Resources**.
    b. Select **Intranet Applications** and then click **Add** in the right pane.
    c. Type `172.16.0.0_network` in the **Name** field and then select the **TRANSPARENT** option.
    d. Verify that the protocol is set to **TCP**.
    e. Select **IP Address and Netmask** as the **Destination Type** and type `172.16.0.0` in the IP Address field.
    f. Verify that the **Destination Port** field is blank.
    g. Type `255.255.255.0` in the **Netmask** field.
    h. Click **Create**.
3. Create an intranet application called "192.168.10.0_network" in the NetScaler Gateway Resources.
    a. Select the **Intranet Applications** node and then click **Add** in the right pane.
    b. Type `192.168.10.0_network` in the **Name** field and then select the **TRANSPARENT** option.
    c. Verify that the protocol is set to **TCP**.
    d. Select **IP Address and Netmask** as the **Destination Type**, and type `192.168.10.0` in the **IP Address** field.
    e. Verify that the **Destination Port** field is blank.
    f. Type `255.255.255.0` in the **Netmask** field.
    g. Click **Create**.
4. Bind the newly created intranet applications to the NetScaler Gateway Global settings.
    a. Browse to **NetScaler Gateway** > **Global Settings**.
    b. Click the links under **Intranet Applications** in the right pane.
    c. In the **Configure VPN Intranet Application** window, click **Add**.
    d. Click **Select All** to select the 172.16.0.0_network and 192.168.10.0_network intranet applications from the **Available** column.
    e. Click the right arrow to move the selected applications to the **Configured** column.
5. Click **OK**.

6. Save the NetScaler configuration by clicking the **Save** icon in the upper-right corner of the configuration utility.
7. Click **Yes** to confirm the saving of the configuration.

Testing the NetScaler Gateway Virtual Server

Use the ExternalClient virtual machine logged on as the Citrix user for this task.

1. Use the RDP shortcuts on the Student Desktop to connect to the ExternalClient. Log on as the local account externalclient\citrix (Password1). (Note: Do not include training as the domain as this machine is in a workgroup.)
2. Log on to the NetScaler Gateway virtual server URL from the previous exercise using the test/test credentials.

   a. Open the Mozilla Firefox browser, type `http://gateway.training.lab` into the Address bar and press **Enter**. Notice that you are redirected to "https://gateway.training.lab".

   b. Type `test` in the **User Name** field, type `test` in the **Password** field, then click **Log On**.

   c. Click **Network Access**.

   d. Install the Gateway plugin and reboot if prompted.
3. Log off the gateway.

   a. Close the Firefox window.

   b. Right-click the **Citrix Receiver** icon in the system tray.

   c. Select **Advanced Preferences** > **NetScaler Gateway Settings** > **Exit**.

   d. Click **Yes** to confirm. Click **Exit**.

   > If Mozilla Firefox browser keeps prompting to install the Gateway plugin, test with Google Chrome. If you receive the Citrix Receiver cleanup dialog box, click Exit.

Disabling Split Tunneling

From the Student Desktop, use an HTTP connection to the NetScaler configuration utility logged on as the nsroot user for this task.

1. Switch to the Student Desktop. Open a web browser and connect to http://netscaler.training.lab.
2. Disable NetScaler Gateway split tunneling using the NetScaler configuration utility.

   a. Go to the **NetScaler Gateway** > **Global Settings** node.

   b. Select **Change global settings**.

   c. Click the **Client Experience** tab and select **OFF** in the **Split Tunnel** drop-down list.

    d. Click **OK**.

3. Save the NetScaler configuration by clicking the **Save** icon in the upper-right corner of the configuration utility.
4. Click **Yes** to confirm the saving of the configuration.

Module 7

Authentication and Authorization

7

Module 7: Authentication and Authorization Exercises

Exercise 7-1: Enabling External Authentication

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

Creating a New Administrator Account

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. Create a new administrator account called "testuser" with read-only permissions.
   a. Go to **System** > **User Administration** > **Users** and click **Add**. The **Add System User** window opens.
   b. Type `testuser` in the **User Name** field, and then type `Password1` in the **Password** and the **Confirm Password** field then click **Continue**.
   c. Under **Bindings** click **No System Command Policy**.
   d. In the **User Command Policy Binding** window, click in the field below **Select Policy**.
   e. Select **read-only** radio button then click **Select**.
   f. Click **Bind**, click **Save** then click **Done**.
   g. Click **Logout** in the upper-right corner of the NetScaler page to log off from 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.
   b. The **Welcome** screen is displayed. Before you proceed, note that the license file is listed as no longer present on the NetScaler. (The license file is still on the NetScaler, just not available to be read by this account.)
   c. Click **Continue**.
   d. Go to **System** > **Licenses:** Confirm the features are still enabled. This confirms the appliance is still licensed.
   e. Go to **System** > **Settings**.
   f. Click **Configure basic features** in the **Settings** node. The **Configure Basic Features** window opens.
   g. Select the feature **Application Firewal**l to enable and click **OK**.

h. Verify that the chosen feature cannot be enabled with read-only access, an error is displayed stating that you are "**Not authorized to execute this command**". Click **OK**, and then click **Close**.

i. Click **Logout** to log off from the current session.

Examining Command Policies

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. Log on to the configuration utility with the nsroot/nsroot credentials to return to superuser permissions.
2. Examine the expression for the superuser policy.
    a. Go to **System** > **User Administration** > **Command Policies**.
    b. Double-click the **superuser** policy in the **Command Policies** section. Notice that the policy allows any command to be permitted using the ".*" expression.
    c. Click **Close**

Enabling LDAP Authentication

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. Create an "srv_auth_ldap" entry for the lb_vsrv_ldap server with 172.16.0.110 as the IP address and 389 as the port.
    a. Go to **System** > **Authentication** > **LDAP**.
    b. Select the **Servers** tab in the right pane and then click **Add**.
    c. Complete the Create Authentication LDAP Server form as follows:
        - **Name**: `srv_auth_ldap`
        - Select the **Server IP** option.
        - **IP Address**: `172.16.0.110`
        - **Port**: `389`
        - **Base DN**: `dc=training,dc=lab`
        - **Administrator Bind DN**: `CitrixLdap@training.lab`
        - Select **BindDN Password** check box to enter the password.
        - **Administrator Password**: `Password1`
        - **Confirm Administrator Password**: `Password1`
        - **Server Logon Name Attribute** from drop down list: `sAMAccountName`
        - **Group Attribute**: `memberOf`

- **Sub Attribute Name**: `cn`

> In a live environment, you should never use a domain administrator account or a single IP address when configuring LDAP.

d. Click **Create**.

2. Create an "auth_ldap_policy" authentication policy for the LDAP server with an expression of ns_true.

    a. Select **System** > **Authentication** > **LDAP** in the right pane.

    b. Select the **Policies** tab and click **Add**.

    c. Type `auth_ldap_policy` in the **Name** field and select **srv_auth_ldap** from the **Server** drop down list.

    d. Click **Saved Policy Expression** and select **ns_true** from the list.

    e. Verify that the **Expression** field contains the expression "ns_true".

    f. Click **Create** to close the **Create Authentication LDAP Policy** window.

3. Bind the auth_ldap_policy globally.

    a. Click **Global Bindings** in the right pane.

    b. Click in the field below **Select Policy**, select the **auth_ldap_policy** radio button and then click **Select**.

    c. Click **Bind** and then click **Done** to bind the policy to System Global.

    d. Click the **Save** icon in the upper-right corner of the configuration utility to save the NetScaler configuration.

    e. Click **Yes** to confirm the saving of the configuration.

4. Grant superuser access to the Domain Admins Active Directory group.

    a. Go to **System** > **User Administration** > **Groups**.

    b. Click **Add**.

    c. Type `Domain Admins` in the **Group Name** field. (Note there is a "space" in "Domain Admins".)

    > Group names on the NetScaler must correspond to the group names in Active Directory and are case sensitive.

    d. Click **Insert** under **Command Policies**.

    e. Select the **superuser** command policy radio button and click **Insert**.

    f. Click **Create**.

5. Grant read-only access to the Remote Users Active Directory group.

    a. Click **Add**.

    b. Type `Remote Users` in the **Group Name** field. (There is a "space" in Remote Users.)

    c. Under **Command Policies** and click **Insert**.
    d. Select the **read-only** command policy radio button and click **Insert**.
    e. Click **Create**.
    f. Click the **Save** icon in the upper-right corner of the configuration utility to save the NetScaler configuration.
    g. Click **Yes** to confirm the saving of the configuration.

6. Click **Logout** in the upper-right corner of the NetScaler and then log on again using the `CitrixAdmin` and `Password1` credentials.
7. Add a load balancing virtual server called testsrv with an IP address of 192.168.10.224 to verify that an Active Directory Domain Admin user has superuser access.
    a. Go to **Traffic Management** > **Load Balancing** > **Virtual Servers** and click **Add**.
    b. Type `testsrv` in the **Name** field.
    c. Type `192.168.10.224` in the **IP Address** field.
    d. Click **OK**, click **Continue**, then click **Done**. The CitrixAdmin user was allowed to add the server.
    e. Click **Save** in the upper-right corner of the configuration utility, and then click **Yes** to confirm saving the configuration.
    f. Click **Logout**.
8. Verify that an Active Directory Remote User is able to log on to the NetScaler.
    a. Type `citrixuser1` in the User name field.
    b. Type `Password1` in the Password field.
    c. Click **Login**. Click **Continue** on the **Welcome** screen. The citrixuser1 user is logged on to the configuration utility.
9. Verify that an Active Directory Remote User is able to view settings but is not allowed to make changes by attempting to remove the load balancing virtual server called testsrv.
    a. Go to **Traffic Management** > **Load Balancing** > **Virtual Servers**. You are able to view the testsrv server created by the CitrixAdmin user.
    b. Select the **testsrv** server and click **Delete**.
    c. Click **Yes** to confirm. An error stating that you are **Not authorized to execute this command** is displayed. Click **OK**.
    d. Click **Logout**.

Binding an LDAP Policy to a NetScaler Gateway Virtual Server

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. Log on to the configuration utility with the nsroot/nsroot credentials to return to superuser permissions.
2. Bind the LDAP policy to the gateway.training.lab NetScaler Gateway virtual server.
   a. Select the **NetScaler Gateway** node and click **Virtual Servers**.
   b. Select the **gateway.training.lab** virtual server and then click **Edit**.
   c. Click the + to the right of the Authentication heading to add the policy.
   d. Select **LDAP** from the **Choose Policy** drop-down menu and click **Continue**.
   e. Click in the field below **Select Policy**, select the **auth_ldap_policy** radio button and then click **Select**.
   f. Click **Bind**.
   g. Click **1 Local Policy** under **Authentication** to unbind the local policy.
   h. Highlight the **NS_GATEWAY_DEFAULT_LOCAL_POL** policy and click **Unbind**.
   i. Click **Yes** to confirm, then click **Close**, then click **Done**.
   j. Click **Save** in the upper-right corner of the configuration utility, and then click **Yes** to confirm saving the configuration.

Testing the LDAP Policy with the NetScaler Gateway

Use the ExternalClient virtual machine logged on as the Citrix user for this task.

1. Switch to the **ExternalClient** virtual machine and log on using the citrix/Password1 credentials. Use the RDP shortcut on the Student Desktop to connect.
2. Test the authentication policies that were just bound to gateway.training.lab.
   a. Open a Firefox browser, browse to `https://gateway.training.lab` and press **Enter**.
   b. Log on with the following credentials:
      - `contractor`
      - `Password1`
   c. Click **Network Access**.
   d. Close the web browser.
   e. Right-click the Receiver icon in the system tray then click **Advanced Preferences**.
   f. Click **NetScaler Gateway settings**.

      > If NetScaler Gateway settings is not visible, connect to https://gateway.training.lab with a Chrome browser.

   g. View the available choices to verify the options menu opens and you have successfully connected as an LDAP user.
   h. Click **Logoff** to end this VPN session and logout as the contractor **user**.

i. Minimize the ExternalClient RDP session and return to the Student Desktop.

Module 8

Access Policies

8

Module 8: Access Policies Exercises

Exercise 8-1: Configuring a Pre-Authentication Policy

This exercise demonstrates how to configure and test a NetScaler Gateway Pre-Authentication policy.

Configuring a Pre-Authentication Policy

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. Set the default pre-authentication settings to DENY.
    a. In the Configuration utility, go to the **NetScaler Gateway** node and click **Global Settings**.
    b. Click **Change Preauthentication settings** in the left pane.
    c. In the **Action** drop-down list, select **DENY**.
    d. Click **OK**.
2. Go to the **NetScaler Gateway** node and click **Policies**.
3. Configure a Pre-Authentication policy called allow_notepad.

> Verifying that Notepad is running simulates verifying the presence of a running security application such as antivirus software.

    a. Select the **Preauthentication** node and click **Add** on the Preauthentication Policies pane.
    b. Type `allow_notepad` in the **Name** field and then click the **+** next to the **Request Action** field.
    c. In the **Create Preauthentication Profile** window, type `allow_logon` in the **Name** field, verify that **ALLOW** is selected in the **Action** field, then click **Create**.
    d. Click **Expression Editor** to the right of the **Expression** heading and select the following items to complete the policy:
        - **Client Security** in the **Select Expression Type** drop-down list.
        - **Process** in the **Component** drop-down list box.
        - Type `notepad.exe` in the **Name** field.
    e. Click **Done**. The resulting expression will read **CLIENT.APPLICATION.PROCESS(notepad.exe) EXISTS**.
    f. Click **Create**.

   g. Click the **NetScaler Gateway** node and in the right pane under **Policy Manager**, click **NetScaler Gateway Policy Manager**.

   h. Click the + next to **AAA Global** and then click **Add Binding** in the **Preauthentication Policy** window.

   i. Click in the field below **Select Policy** and select the **allow_notepad** policy radio button.

   j. Click **Select** and then click **Bind**.

   k. Click **Done** and then click **Done** again.

4. Use the RDP shortcuts on the Student Desktop to connect to the ExternalClient. Log on as the local account externalclient\citrix (Password1).
5. On the ExternalClient virtual machine, test the newly created allow_notepad policy.

   a. Open **Notepad** Start > Run > notepad. Local Notepad application launches.

   b. Open a Firefox browser window and browse to `https://gateway.training.lab`. A warning will appear stating that the endpoint analysis scan will start in a few seconds.

   c. Click **Yes** to run the endpoint analysis scan (The warning may appear behind the browser; look in the taskbar to see if a NetScaler Gateway icon is present). Access to the logon page is granted because the local Notepad application is running.

   > If the EPA client is not detected with Firefox, try IE or Chrome.

   d. Close the web browser without logging on.

   > The endpoint analysis menu is another window.

6. Reconnect to the NetScaler Gateway with the local application closed.

   a. Close the web browser and then close the local Notepad application.

   b. Reconnect to `https://gateway.training.lab`.

   c. Click **Yes** to run the endpoint analysis scan.

   d. Since the local Notepad application is not running, access to the logon page is denied.

7. Minimize the RDP session to the ExternalClient and return to the Student Desktop.

Unbinding Pre-Authentication Policies

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. Unbind the allow_notepad policy from the NetScaler Gateway.

   a. Go to the **NetScaler Gateway** node in the left pane and select the **NetScaler Gateway Policy Manager** in the right pane.
   b. Expand the **AAA Global** section and click **1 AAA Global to AAA Preauthentication Policy Binding**.
   c. Select the **allow_notepad** policy and click **Unbind**.
   d. Click **Yes** to unbind the policy and then click **Done**.
   e. Click **Done** again to close the **NetScaler Gateway Policy Manager**.
   f. In the configuration utility, go to the **NetScaler Gateway** node and click **Global Settings**.
   g. Click **Change Preauthentication settings**.
   h. In the **Action** drop-down list box, select **ALLOW**.
   i. Click **OK**.

Exercise 8-2: Configuring a NetScaler Gateway Authorization Policy

This exercise demonstrates how to configure basic authorization policies for the NetScaler Gateway.

Configuring the Default Authorization Action

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. Set the default authorization to Authorization DENY.
   a. Go to **NetScaler Gateway** > **Global Settings** > **Change Global Settings**.
   b. Select the **Security** tab and then verify that **DENY** is selected in the **Default Authorization Action** drop-down list.
   c. Click **OK**.
2. Unbind the 172.16.0.30_443_POL access policy from the virtual server.
   a. Go to **NetScaler Gateway** > **Virtual Servers**.
   b. Select the **gateway.training.lab** virtual server and click **Edit**.
   c. Under the **Policies** field click **1 Session Policy**.
   d. Click the **172.16.0.30_443_POL** policy and click **Unbind**.
   e. Click **Yes**.
   f. Click **Close**.
   g. Click **Done**.
3. Switch to the ExternalClient using the RDP Shortcut.
4. On the ExternalClient virtual machine, test the edited default authorization policy.

   a. Open a Firefox browser window and browse to `https://gateway.training.lab` and log on using the following credentials:

      - contractor
      - Password1

      > If the EPA client is not detected with Firefox, try IE or Chrome.

   b. Browse to `http://blue.training.lab/home.php`.

      > The browser will timeout, or display a message that it is unable to access that web site as a result of the Global "Deny" security setting.

5. Close the Firefox window and log off from the gateway.
   a. Close the Firefox window.
   b. Right-click the **Citrix Receiver** icon in the system tray.
   c. Click **Advanced Preferences** > **NetScaler Gateway Settings** > **Exit**.
   d. Click **Yes** to confirm session closure and click **Exit** on the Citrix Windows Cleanup dialog box.
6. Create a Contractors group for LDAP extraction.
   a. Return to the Student Desktop, select the **NetScaler Gateway** node and click **User Administration**.
   b. Select the **AAA Groups** node.
   c. Click **Add**.
   d. Type `Contractors` in the **Group Name** field.
   e. Click **OK** and then click **Done**.

Creating an Authorization Policy

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. Create a new authorization policy that will allow access from the ExternalClient virtual machine to the back-end servers.
   a. Click the **NetScaler Gateway** node, click the **Policies** node, then select the **Authorization** node.
   b. Click **Add**.
   c. Type `web_servers` in the **Name** field and verify that **ALLOW** is selected in the **Action** drop-down list.

   d. Click the **Switch to Classic Syntax** link to create a classic syntax expression, then click the **Expression Editor** link on the right.

2. Configure the web_servers policy to select traffic going to any destination IP address that contains 192.168.10.0 with a netmask of 255.255.255.0.
   a. Select **General** in the **Select Expression Type** field, select **REQ** in the **Flow Type** field.
   b. Select **IP** from the **Protocol** drop-down list.
   c. Select **DESTIP** from the **Qualifier** drop-down list.
   d. Verify that == appears in the **Operator** field.
   e. Type `192.168.10.0` in the **IP Value** field.
   f. Type `255.255.255.0` in the **Netmask** field.
   g. Click **Done**. The resulting expression will display: REQ.IP.DESTIP == 192.168.10.0 -netmask 255.255.255.0.
   h. Click **Create**.
3. Bind the web_servers policy to the Contractors group.
   a. Click the **NetScaler Gateway** node and then click **User Administration** > **AAA Groups** node.
   b. Select the **Contractors** group and click **Edit**.
   c. In the right pane, click **Authorization Policies**.
   d. Under the **Authorization Policies** field on the left, click **No Authorization Policy** to add the web_servers policy.
   e. In the **Policy Binding** window, click in the **Select Policy** field and select the **web_servers** policy radio button.
   f. Click **Select**, change the **Priority** to `100`, click **Bind**, then click **Done**.
   g. Click **Save** to save the NetScaler configuration and then click **Yes** to confirm the saving of the configuration.

Testing Authorization Policies

Use the ExternalClient virtual machine logged on as the Citrix user for this task.

1. Switch to the ExternalClient using the RDP Shortcut. Log on using the citrix/Password1 credentials.
2. Test the newly-created web_servers policy on the NetScaler Gateway.
   a. Open a new Firefox browser on the ExternalClient, browse to `https://gateway.training.lab` and press **Enter**.
   b. Log on using the contractor/Password1 credentials.
   c. Browse to `http://blue.training.lab/home.php` and press **Enter**. Access is now allowed to this server. If there are connection issues, verify that the Group name you created is Contractors because the name must be an exact match (case sensitive) to the name listed in the Active Directory server.

3. Close the Firefox window and log off from the gateway.
    a. Close the Firefox window.
    b. Right-click the **Citrix Receiver** icon in the system tray, and click **Advanced Preferences**.
    c. Click **NetScaler Gateway Settings** > **logoff**.
    d. Click **Yes** to confirm log-off, click **Exit** to close the Citrix Windows Cleanup dialog box, and **OK** to close the Receiver window.
4. Minimize the ExternalClient RDP session and return to the Student Desktop.
5. Bind the 172.16.0.30_443_POL session policy to the virtual server.
    a. Go to **NetScaler Gateway** > **Virtual Servers**.
    b. Select the **gateway.training.lab** virtual server and click **Edit**.
    c. Click the **+ sign** to the right of the **Policies** field.
    d. Verify that the **Choose Policy** value is set to **Session** then click **Continue**.
    e. Click in the field below **Select Policy**.
    f. Click the radio button for the **172.16.0.30_443_POL** policy and click **Select**.
    g. Click **Bind**.
    h. Click **Done**.
6. Save the NetScaler configuration.

Module 9

End User Access and Experience (includes RDP Proxy)

9

Module 9: End-User Access and Experience Exercises (Includes RDP Proxy)

Exercise 9-1: Displaying Client and Configuration Options

This exercise demonstrates how to display client and configuration options on the NetScaler Gateway.

Viewing the Contractor Profile

Use the ExternalClient virtual machine logged on as the citrix user for this task.

1. Use the RDP shortcuts on the Student Desktop to connect to the ExternalClient. Log on as the local account externalclient\citrix (Password1)
2. View the available profile options for the Contractors group.
    a. Open a new Firefox browser, browse to `http://gateway.training.lab` then press **Enter**.
    b. Log on using the **Contractor/Password1** credentials.
    c. Click **Network Access**.
    d. Right-click the **Citrix Receiver** icon in the system tray and click **Advanced Preferences**.
    e. Click **NetScaler Gateway Settings** > **Configure NetScaler Gateway**. Notice the available tabs in the **NetScaler Gateway Configuration** window.
    f. Click **Cancel** in the **NetScaler Gateway Configuration** Window.
    g. Select **NetScaler Gateway Settings** > **Log off**.
    h. Click **Yes** and then click **Exit** to log off.
    i. Close the browser.

Viewing Available Client and Configuration Options

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. Minimize the ExternalClient RDP session and return to the Student Desktop.
2. Create a session profile and policy.
    a. Click the **NetScaler Gateway** > **Policies** > **Session** and then click **Add**.
    b. Type `contractor_pol` in the **Name** field and then click + sign next to the **Profile** field to create the **Session Profile**.

    c. Type `contractor_prof` in the **Name** field and then click **Create**.
    d. Select **Saved Policy Expressions** and then select **ns_true**.
    e. Click **Create**.
3. Bind the contractor_prof policy to the Contractors group.
    a. Select the **NetScaler Gateway** > **User Administration** > **AAA Groups** node.
    b. Select the **Contractors** group in the right pane and click **Edit**.
    c. Click **Policies** in the right pane.
    d. Click in the + sign under the **Policies** section.
    e. Select **Session** in the **Choose Policy** field and then click **Continue**.
    f. In the **Policy Binding** section, click in the field below **Select Policy**.
    g. Select the **contractor_pol** radio button, click **Select** and then click **Bind**.
    h. Click **Done**.

Hiding Client and Configuration Options

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. Hide client and configuration options, and disable the client cleanup feature.
    a. Select the **NetScaler Gateway** > **Policies** > **Session** node.
    b. In the right pane, click the **Session Profiles** tab and select the **contractor_prof** profile.
    c. Click **Edit**.
    d. Select the **Client Experience** tab, scroll to the bottom of the page and select **Advanced Settings**.
    e. Click the **Client Options** tab.
    f. Under **Clients Configuration**, select the **Custom** option.
    g. Select **General** and **Tunnel** in the **Clients Configuration** section.
    h. Click **OK** to complete the change.
2. Click the **Save** icon to save the NetScaler configuration and then click **Yes** to confirm the saving of the configuration.

Viewing the Updated Contractor Profile

Use the ExternalClient virtual machine logged on as the citrix user for this task.

1. Switch to the ExternalClient RDP. Remain logged on with the citrix/Password1 credentials.
2. View the available profile options for the Contractors group.
    a. Open a new Firefox browser, browse to `https://gateway.training.lab` and log on using the **contractor** credentials.

b. Click **Network Access**.

c. Right-click the **Citrix Receiver** icon in the system tray and select **Advanced Preferences**.

d. Select **NetScaler Gateway Settings**.

e. Select **Configure NetScaler Gateway**. Notice that the **Trace** and **Compression** tabs are no longer available.

f. Click **Cancel** in the open window to close it.

g. Select **NetScaler Gateway Settings** > **Log off**.

h. Click **Yes** to log off, and then click **Exit**.

i. Close the browser window.

3. Minimize the ExternalClient RDP session and return to the Student Desktop.

Exercise 9-2: Configuring Clientless Access with Client Choices

This exercise demonstrates how to configure Clientless Access on the NetScaler Gateway.

Configuring Clientless Access on the NetScaler Gateway

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. Create a new policy that configures Clientless Access on the NetScaler Gateway.

a. Select the **NetScaler Gateway** > **Policies** > **Session** node.

b. In the **Session Policies** tab on the right, click **Add** to create a new policy.

c. Type `choices_pol` in the **Name** field and then click + next to the **Profile** field to create the **Session Profile**.

d. Type `choices_prof` in the **Name** field.

e. Select the **Client Experience** tab and click **Override Global** check box next to **URL for Web-Based Email**.

f. In the **URL for Web-Based Email** field, type `http://blue.training.lab/home.php`.

> The blue server URL for web-based email is to simulate OWA or a similar web email portal.

2. Complete the choices_prof profile configuration for Clientless Access on the NetScaler Gateway by allowing Client Choices and Clientless Access.

a. Scroll to the bottom of the profile page and click the **Advanced Settings** link.

   b. Scroll to the bottom of the page and select **Override Global** next to **Client Choices** and then select the **Client Choices** check box.

   c. Click **Create**.

   d. Click **Saved Policy Expressions** and then select **ns_true**.

   e. Click **Create**.

3. Bind the choices_pol session policy to the gateway.training.lab virtual server.

   a. Click the **NetScaler Gateway** > **Virtual Servers** node.

   b. In the right pane, select the **gateway.training.lab** virtual server and click **Edit**.

   c. Click the + next to the **Policies** heading at the bottom of the window.

   d. Verify that **Session** is selected in the **Choose Policy** field.

   e. Verify that **Request** is selected in the **Choose Type** field.

   f. Click **Continue**.

   g. Click **Add Binding**.

   h. Click in the field below **Select Policy** and select the **choices_pol** radio button.

   i. Click **Select** then click **Bind**.

   j. Click the **172.16.0.30_443_POL** then click **Unbind**, click **Yes** to Confirm and then click **Close** then **Done**.

Testing Clientless Access

Use the ExternalClient virtual machine logged on as the Citrix user for this task.

1. Switch to the RDP session for ExternalClient. Continue to log on with the citrix/Password1 credentials.

2. View the available profile options for the Contractors group.

   a. Open a new Firefox browser on the ExternalClient, browse to `https://gateway.training.lab` and press **Enter**.

   b. Log on using the **contractor/Password1** credentials. You are forwarded to the Client Choices page.

   c. Click the **Clientless Access** link.

   > "Clientless" means "web proxy" and no VPN connection is made. Notice the concealed URL.

   d. Click the **Email** tab of the NetScaler Gateway portal. The blue homepage is displayed. If not Try again or refresh the page.

   e. Click **Log Off** in the top-right corner of the window.

3. Minimize the ExternalClient RDP session.

4. Switch to the Student Desktop virtual machine to unbind the choices_pol session policy from the gateway.training.lab virtual server in preparation for future exercises.
    a. Go to **NetScaler Gateway** > **Virtual Servers** and then select the **gateway.training.lab** virtual server.
    b. Select **Edit** and then scroll down to the **Policies** section.
    c. Select **1 Session Policy**.
    d. Select the **choices_pol** policy, click **Unbind** and then click **Yes** to unbind the policy from the gateway.training.lab virtual server.
    e. Click **Close**, then click **Done**.

Configuring Remote Desktop (RDP) Proxy

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. **Create RDP Client and Server Profiles.**
    a. Right click on **NetScaler Gateway** > **Policies** > **RDP** node and **Enable Feature**.
    b. Select the **Client Profiles** tab on the right, click **Add** to create a RDP client profile.
    c. Type `rdp_client_pro` in the **Name** field.
    d. Scroll down and type `gateway.training.lab` in the **RDP Host** field.
    e. At the very bottom, type `Password1` in the **Pre Shared Key** field and then click **Create**.
    f. Select the **Server Profiles** tab on the right, click **Add** to create a RDP server profile.
    g. Type `rdp_server_pro` in the **Name** field.
    h. Type `172.16.0.30` in the **RDP IP** field.
    i. Type `3389` in the **Port** field which is the default port for RDP protocol.
    j. Type `Password1` in the **Pre Shared Key** field and then click **Create**.
2. **Create a Session Profile and Policy for RDP Proxy Users.**
    a. Select the **NetScaler Gateway** > **Policies** > **Session** node.
    b. In the **Session Policies** tab on the right, click **Add** to create a new Session Policy.
    c. Type `rdp_pol` in the **Name** field and then click + next to the **Profile** field to create the Session Profile.
    d. Type `rdp_prof` in the **Name** field.
    e. Select the **Security** tab and click **Override Global** check box next to **Default Authorization Action** and set the Action to **ALLOW**.
    f. Select the **Client Experience** tab and click **Override Global** check box next to **Clientless Access** and set the Action to **ON**.
    g. Select the **Published Applications** tab and click **Override Global** check box next to **ICA Proxy** and set the Action to **OFF**.

   h. Select the **Remote Desktop** tab and click **Override Global** check box next to **RDP Profile Client Name** and select **rdp_client_pro** from the drop-down list.

   i. Click **Create**.

   j. Click **Saved Policy Expressions** and then select **ns_true**.

   k. Click **Create**.

3. **Edit the gateway.training.lab virtual server.**

   a. Click the **NetScaler Gateway** > **Virtual Servers** node.

   b. In the right pane, select the **gateway.training.lab** virtual server and click **Edit**.

   c. Click the **Edit** Icon in **Basic Settings** then click on the arrow next to **More** at the bottom of the field.

   d. Uncheck the **ICA Only** box if checked.

   e. In the **RDP Server Profile** pulldown menu, select **rdp_server_pro**.

   f. Click **OK** to exit the basic settings configuration.

   g. Click **Continue**, **Continue** then **Done** to exit the gateway configuration.

4. **Configure a User for RDP Proxy.**

   a. Click the **NetScaler Gateway** > **User Administration** > **AAA Users** node.

   b. In the right pane, click **Add**.

   c. Type `citrixrdp` in the **User Name** field. Be sure **External Authentication** is checked. The click **OK**.

   d. Click the + sign in **Policies** field to the right. Then click + sign in **Policies** field on the left pane.

   e. In the **Choose Policy** field, select **Session** the click **Continue**.

   f. Click in the field below **Select Policy**.

   g. Select the Radio Button next to **rdp_pol** then click **Select** above.

   h. Click **Bind** to bind the policy to the citrixrdp user.

   i. Click the **+ sign** in the **Bookmarks** field to the right. Then click in the **No URL** field, under the **Published Applications** field in the center.

   j. Click the + sign in the **Select URL** field.

   k. In the **Name** field, type `rdp_dc2`.

   l. In the **Text to Display** field, type `MGMT`.

   m. In the **Bookmark** field, type `rdp://192.168.10.6`.

   n. Check the box to **Use NetScaler Gateway As a Reverse Proxy**.

   o. Click **Create**, then **Bind** to bind the bookmark to the citrixrdp user. Then click **Done**.

> DNS names are also supported. If you wish to use DNS, a DNS virtual server must be specified in the session profile.

5. Use the RDP shortcuts on the Student Desktop to connect to the ExternalClient. Log on as the local account externalclient\citrix (Password1)
6. **Test the RDP proxy configuration.**

   Use the ExternalClient virtual machine logged on as the Citrix user for this task.

   a. Open a new Firefox browser on the ExternalClient, browse to `https://gateway.training.lab` and press **Enter**.
   b. Log on using the **citrixrdp/Password1** credentials. You are forwarded to the Clientless Access page. You will see a link for **MGMT**.
   c. Click on the **MGMT** link to download and then open the **app.rdp** file with **Remote Desktop Connection**.
   d. Click **Connect** in the **Remote Desktop Connection** dialogue box to connect to the management workstation via RDP.
   e. You can connect to other domain machines without shortcuts as well. For example, to connect to the dc.training.lab, in your browser address bar, type `https://gateway.training.lab/rdpproxy/192.168.10.11`.
   f. If the RDP link fails do the following:

   > If you have issues connecting, confirm you can connect to the machine from another via RDP. If you receive errors related to domain trusts, on the Domain Controller 2 to which you cannot connect, run Powershell as administrator and run the following command: **$credential = Get-Credential (when prompted enter: citrixadmin/Password1)**. Then run: **Reset-ComputerMachinePassword -Server dc.training.lab**.

7. Close the open RDP sessions to DC.training.lab and DC2.training.lab opened via the RDP Proxy.
8. Return to the NetScaler Gateway portal page and click Log off.
9. Minimize the ExternalClient RDP session and return to the Student Desktop.
10. Save the NetScaler configuration.

Module 10

NetScaler Gateway and Unified Gateway

10

Module 10: Integrating NetScaler 11 with XenApp and XenDesktop Exercises

Exercise 10-1: Configuring StoreFront for NetScaler Gateway

This exercise demonstrates how to configure StoreFront for use with NetScaler Gateway.

Configuring StoreFront Authentication, Gateway, Beacons and Enabling Remote Access

Use the StoreFront SF1 virtual machine logged on as the training\CitrixAdmin user for this task.

1. Connect to the SF1 virtual machine:
    a. Use the RDP shortcut (Windowed or FullScreen) on the Student Desktop to connect to SF1.
    b. Log on as training\citrixadmin. The password is Password1.
2. Enable domain pass-through and pass-through from Citrix NetScaler Gateway authentication on StoreFront.
    a. In the StoreFront SF1 virtual machine, click the **Citrix StoreFront** icon in the taskbar. The Citrix StoreFront console opens.
    b. Select **Authentication** in the left pane and click **Add/Remove Methods** in the right pane.
    c. Select **Domain pass-through** and **Pass-through from NetScaler Gateway**, then click **OK** (these are added to the existing authentication methods).
3. Add a gateway to the StoreFront.
    a. Select **NetScaler Gateway** in the left pane and click **Add NetScaler Gateway Appliance** in the right pane.
    b. Type the following information for the new gateway server:
        - Display Name: `gateway.training.lab`
        - NetScaler Gateway URL: `https://gateway.training.lab`
        - Subnet IP address: *LEAVE BLANK*
    c. Type `https://gateway.training.lab` in the Callback URL field and then click **Next**.
    d. Click **Add** and type `https://xd1.training.lab` in the STA URL field and click **OK**.

e. Click **Add** and type `https://xd2.training.lab` in the STA URL field and click **OK**.

f. Click **Create**, then click **Finish**.

4. Enable remote access on StoreFront.

    a. Select **Stores** in the left pane and click **Enable Remote Access** in the right pane.

    b. Select **No VPN Tunnel** radio button, check the box next to **gateway.training.lab**, and verify that **gateway.training.lab** is selected as the **Default appliance**.

    c. Click **OK**.

5. Propagate all changes to the StoreFront 2 server.

    a. Select **Server Group** in the left pane.

    b. Click **Propagate Changes**.

    c. Click **Yes** then click **OK**.

> If you receive a Windows remote login error message, click OK.

6. Minimize the RDP session for SF1 and return to the Student Desktop.

> - If the same NetScaler appliance is being used to load balance StoreFront and for the NetScaler Gateway ICA Proxy configuration, issues can exist if one SNIP is used for both types of traffic. On NetScaler 10 and later versions, the solution is to leave the Subnet IP address blank. This will allow the load balanced StoreFront traffic to co-exist with the ICA Proxy traffic originating from the same NetScaler. This will also allow StoreFront to accept both external connections with the NetScaler Gateway and internal connections in direct mode.
> - If a separate appliance is being used to load balance StoreFront, then the Gateway appliance's SNIP should continue to be listed on the StoreFront system as part of the Gateway settings. Alternatively, a NetScaler administrator could use net profiles (on the NetScaler) to assign a separate SNIP to the load balancing virtual server and to the gateway virtual server. The StoreFront would then be configured with the gateway virtual servers SNIP.

Exercise 10-2: Configuring the NetScaler for StoreFront

This exercise demonstrates how to configure NetScaler to use Storefront.

Creating a New Session Policy to Access StoreFront

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. Open a browser and connect to the configuration utility for http://netscaler.training.lab.
2. Create a new session policy called "storefront_pol" and corresponding profile called "storefront_prof" that allows ICA proxy with NetScaler Gateway.
    a. Go to **NetScaler Gateway** > **Policies** > **Session** in the left pane.
    b. In the right pane, click **Add** and type `storefront_pol` in the **Name** field.
    c. Click the **+ sign** next to the **Profile** field to configure the NetScaler Gateway Session Profile.
    d. Type `storefront_prof` in the **Name** field.
    e. Select the **Client Experience** tab, scroll to the bottom of the page and select the check box for **Override Global** next to **Single Sign-on to Web Applications** along with the check box for **Single Sign-on to Web Applications**.
    f. Scroll up to the top of the page and select the **Security** tab.
    g. Select the **Override Global** check box for the **Default Authorization Action** field and verify that the action is set to **ALLOW**.
    h. Select the **Published Applications** tab and select **Override Global** for the following options settings and then select their matching values:
        - **ICA Proxy**: **ON**
        - **Web Interface Address**: `https://storefront.training.lab/Citrix/StoreWeb`
        - **Web Interface Portal Mode**: **NORMAL**
        - **Single Sign-on Domain**: `training`
        - **Citrix Receiver Home Page**: `https://storefront.training.lab/Citrix/StoreWeb`
    i. Click **Create** to create the policy profile.
    j. Click **Saved Policy Expressions** and then select **ns_true** from the drop-down list.
    k. Click **Create**.
3. Bind the newly created storefront_pol to the Virtual Server.
    a. Go to **NetScaler Gateway** > **Virtual Servers** in the left pane.
    b. Select the virtual server **gateway.training.lab** and then click **Edit**.
    c. Scroll to the bottom of the page and select the **+ sign** in the **Policies** heading.
    d. Verify that **Session** is selected in the **Choose Policy** field.
    e. Verify that **Request** is selected in the **Choose Type** field.
    f. Click **Continue**.
    g. Click in the **Click to select** field under **Select Policy**.
    h. Select the **storefront_pol** radio button.
    i. Click **Select** and then click **Bind**.
    j. Click **Done**.
    k. Click **Save** and then click **Yes** to save the NetScaler configuration.

Exercise 10-3: Adding Secure Ticketing Authority Servers to the NetScaler

This exercise demonstrates how to add Secure Ticketing Authority servers to a NetScaler.

Adding Secure Ticketing Authority Servers to the NetScaler Gateway

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. Bind the XenDesktop Controllers XD1 and XD2 servers as STAs on the NetScaler.
    a. Select the **NetScaler Gateway** node and click **Virtual Servers**.
    b. Highlight the **gateway.training.lab** virtual server and click **Edit**.
    c. Click the **Published Applications** node in the right pane.
    d. Under **Published Applications**, click **No STA Server**.
    e. Type `https://xd1.training.lab/` in the **Secure Ticket Authority Server** field and select **IPV4** from the **Secure Ticket Authority Server Address Type** then click **Bind**.
    f. Under **Published Applications**, click **1 STA Server** to add the other STA.
    g. Click **Add Binding**.
    h. Type `https://xd2.training.lab/` in the **Secure Ticket Authority Server** field and select **IPV4** from the **Secure Ticket Authority Server Address Type** then click **Bind**.
    i. Click **Close** and then click **Done**.

> Note that the new STA bindings are green and each have a unique STA ID.

Exercise 10-4: Updating an Authorization Policy

1. Modify the value of the expression in the web_servers policy to allow access to the 172.16.0.0/24 network.
    a. Go to the **NetScaler Gateway** > **Policies** > **Authorization** node.
    b. In the right pane, select the **web_servers** policy and then click **Edit**.
    c. Under **Expression**, modify the existing expression by simply clicking in the **Expression** field.

    d. Change the IP address to `172.16.0.0`. The expression now reads: REQ.IP.DESTIP == 172.16.0.0 -NETMASK 255.255.255.0. This allows the user access to the NetScaler Gateway VIP for ICA Proxy communications.

    e. Click **OK**.

2. Save the NetScaler configuration.

Testing the New Session Policy to Access StoreFront Using NetScaler Gateway

Use the ExternalClient virtual machine logged on as the Citrix user for this task.

1. Use the RDP shortcuts on the Student Desktop to connect to the ExternalClient. Log on as citrix/Password1.
2. Test the StoreFront connection through the NetScaler Gateway.

    a. Open a **Firefox** browser window on the ExternalClient, browse to `https://gateway.training.lab` and press **Enter**.

    b. Log on using the **Contractor/Password1** credentials.

    > After login if you are prompted to install the Receiver client, Select the **I agree with the Citrix License Agreement** check box and click on **Log on**.

    c. Select **Apps** at the bottom of the screen.

    d. Click the + icon on the left side of the window, select **All Apps**, then click the **Microsoft Excel 2013** application to add it to your account.

    e. Click **Microsoft Excel 2013** to open the application. The published application opens as expected.

    > If you receive a pop-up window, click Activate or Allow.
    >
    > If you receive a message saying you cannot connect to Excel, but you have already connected to a published desktop, try logging off the published desktop first and then repeating the application launch.

    f. Close the published application.

    g. At the top of the Storefront browser screen, click **Joe Q. Contractor** and then click **Log Off**.

    h. Close the web browser.

3. Minimize the RDP session for ExternalClient and return to the Student Desktop.

Exercise 10-5: Customize the NetScaler Gateway Portal Page

NetScaler 11 features a simple and powerful graphical configuration utility to customize the gateway portal pages

1. Create a new portal theme based off the Green Bubble Theme, the Default Theme (Black), or the X1 Theme.
    a. Go to **NetScaler Gateway** > **Portal Themes** then click **Add** in the main pane.
    b. In the **Theme Name** field, type `CustomTheme1`.
    c. In the **Template Theme** pull down, select the theme upon which you wish to base your custom theme and click **OK**.
    d. Scroll down to the **Common Attributes** section, click the **Background Image** drop down menu and select **EDIT**.
    e. Click **Browse** and browse to **C:\resources\Portal images** and choose one of the images to apply as your background image.
    f. Scroll to the bottom and click **OK**.

    > At this point you can click **Click to view and bind configured theme** but it will open the page in a tab via IP so you will get a certificate error. We suggest not clicking there and moving to the next step.

    g. At the top, click **Back**.
    h. Go to **NetScaler Gateway** > **Virtual Servers**, highlight the **gateway.training.lab** virtual server and click **Edit**.
    i. Click on the **+ Symbol** in the **Portal Themes** field to the right.
    j. Locate the **Portal Themes** pane and click on the arrow to the right of the **No Portal Theme** field.
    k. Select the arrow in the **Select Portal Theme** field.
    l. Select the radio button to select the **Custom Theme** which you previously created and click **Select** above.
    m. Now click **Bind**, then **Done**.
    n. With a Firefox browser, browse to **https://gateway.training.lab** and view your new page.

    > If the new portal theme does not display, refresh the page. The theme should update, however if not, then clear your browser cache. You can also go back to your portal theme and experiment with other changes such as button colors, or change the image or base theme.

Exercise 10-6: Apply an End User License Agreement (EULA)

NetScaler 11 features a simple and powerful graphical configuration utility to configure a EULA which users must accept before they can login.

1. Create a EULA using some simple per-written HTML on the management workstation, or write your own EULA
    a. Go to **NetScaler Gateway** > **Resources** > **EULA** then click **Add** in the main pane.
    b. In the **Name** field, type `EULA`.
    c. Be sure the **English** tab is selected if you want to use English. In the **End User License Agreement in English** type in a message you wish to present for your EULA. You may also use HTML instead of simple text. If you wish, copy and the paste the simple HTML from **C:\resources\Portal images\EULA.txt** instead. This will present your EULA in very simple HTML.

    > The HTML in EULA.txt would likely not be an appropriate EULA for a business. Be sure to consult with your legal team when enabling a EULA for your business.

    d. When you have written your EULA, scroll down to the bottom of the page and click **Create**.
    e. Bind the EULA to the gateway virtual server. Go to **NetScaler Gateway** > **Virtual Servers**, highlight the **gateway.training.lab** virtual server and click **Edit**.
    f. Click on the **+ Symbol** in the **EULA** field to the right.
    g. Locate the **EULA** pane and click on the arrow to the right of the **NO EULA** field.
    h. Click in the field below **Select EULA**.
    i. Select the radio button next to **EULA** which was previously created, then click **Select**.
    j. Click **Bind**.
    k. Click **Done**.
    l. Open a web browser on the **ExternalClient** and browse to **https://gateway.training.lab** and view your new page. You should see a check box next to **I accept the Terms & Conditions**. Click on the **Terms & Conditions** hyperlink to review the EULA you bound to the virtual server.

    > The EULA check box should display. If the EULA check box does not display, refresh the page. If that does not help, then clear your browser cache

    m. Go back to the **Student Desktop** and Click **Save** in the top right corner and then click **Yes** to save the NetScaler configuration.

Module 11

AppExpert (Default and Classic Syntax)

11

Module 11: AppExpert Policy Engine

Exercise 11-1: Configuring Responder to Redirect to HTTPS

This exercise will demonstrate how to create a Responder Policy that will redirect an HTTP request to an HTTPS request.

Configuring Responder to Use SSL

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. Create a Responder Action to redirect any URL, including path and query, from HTTP to HTTPS.
    a. Go to the **AppExpert** node, right-click the **Responder** node and select **Enable Feature** (If not already enabled).
    b. Go to **AppExpert** > **Responder** > **Actions** and click **Add**.
    c. Type `rs_act_sendtossl` in the **Name** field.
    d. Select **Redirect** for the Type.
    e. Type the following text in the **Expression** field.

    ```
    "https://" + HTTP.REQ.HOSTNAME.HTTP_URL_SAFE +
    HTTP.REQ.URL.PATH_AND_QUERY.HTTP_URL_SAFE
    ```

    f. Verify that the **Response Status Code** contains **302** for the redirect.
    g. Click **Create**.
2. Create a policy named rs_pol_sendtossl for for the rs_act_sendtossl action.
    a. Go to **AppExpert** > **Responder** > **Policies** and click **Add**.
    b. Type `rs_pol_sendtossl` in the **Name** field.
    c. Select **rs_act_sendtossl** from the **Action** drop-down list.
    d. Verify that -**Global undefined-result action**- is selected for the **Undefined-Result Action**.
    e. Type the following in the **Expression** field.

    ```
    !CLIENT.SSL.IS_SSL
    ```

    f. Click **Create**.
3. Bind the rs_pol_sendtossl policy to the lb_vsrv_colors virtual server.
    a. Right-click the **rs_pol_sendtossl** policy and click **Policy Manager**.

   b. Select **Load Balancing Virtual Server** from the **Bind Point** drop down list and then verify that **HTTP** is the Protocol.
   c. Select **lb_vsrv_colors** from the **Virtual Server** drop down list and then click **Continue**.
   d. Click in the field below **Select Policy** and select the **rs_pol_sendtossl** policy radio button.
   e. Click **Select**.
   f. Scroll to the bottom of the page, click **Bind**, then click **Done**.
4. Click the **Save** icon to save the NetScaler configuration and click **Yes** to confirm the saving of the configuration.

Testing the Redirect to SSL Policy

From the Student Desktop, open a web browser to complete this task.

1. Open a new browser window and browse to the lb_vsrv_colors virtual server and verify that the page is redirected to an SSL connection.
   a. Open a Firefox window.
   b. Open LiveHTTPHeaders: **Tools** > **Live HTTP Headers**.
   c. Browse to `http://colors.training.lab/home.php` and press **Enter**. The page should be redirected to https://colors.training.lab/home.php.
   d. You can view the redirect by returning to the LiveHTTPHeaders tab and scrolling to the top of the capture. Clear the capture or close the LiveHTTPHeaders tab when done.
2. Unbind the rs_pol_sendtossl policy.
   a. Switch to the NetScaler configuration utility and go to **AppExpert** > **Responder** > **Policies**.
   b. Right-click the **rs_pol_sendtossl** policy and select **Policy Manager**.
   c. Select **Load Balancing Virtual Server** from the **Bind Point drop** down list, then verify that **HTTP** is the Protocol.
   d. Verify that the **Virtual Server** is **lb_vsrv_colors** and click **Continue**.
   e. Select the **rs_pol_sendtossl** policy, click **Unbind** and then click **Yes** to confirm.
   f. Click **Done**.
3. Click the **Save** icon to save the NetScaler configuration and click **Yes** to confirm the saving of the configuration.

Exercise 11-2: Configuring Content Switching

This exercise demonstrates how to configure content switching on a NetScaler system, including creating non-addressable virtual servers, content switching virtual servers and using policies and expressions to switch content at the servers.

Verifying that the Content-Switching Feature is Enabled

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. Verify that the content-switching feature is enabled.
   a. Go to **System** > **Settings**.
   b. Click **Configure Basic Features** under the **Modes and Features** pane.
   c. Verify that the **Load Balancing** and **Content Switching** features are selected and click **Close**.

Creating Non-Addressable Load-Balancing Virtual Servers

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log 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. Go to **Traffic Management** > **Load Balancing** > **Virtual Servers**.
   b. Click **Add** in the **Load Balancing Virtual Servers** pane. The Load Balancing Virtual Server settings window opens.
   c. Type `lb_vsrv_red` in the **Name** field and verify that **HTTP** is selected in the **Protocol** drop-down list.

   > This virtual server is dedicated to iPhone users.

   d. In the **IP Address Type** drop down menu select **Non Addressable** and click **OK** 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. Click **No Load Balancing Virtual Server Service Binding** and click in the field below **Select Service**.
   f. Select **svc_red** and click **Select**.
   g. Click **Bind**, click **Continue** and then click **Done**.

> 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.

> This virtual server is dedicated for Internet Explorer 6 users.

   a. Click **Add** in the **Load Balancing Virtual Servers** pane. The Load Balancing Virtual Server settings window opens.

   b. Type `lb_vsrv_blue` in the **Name** field and verify that **HTTP** is selected in the **Protocol** drop-down list.

   c. In the **IP Address Type** drop down menu, select **Non Addressable** and click **OK** to confirm the change. This action disables the IP address and Port fields. No VIP address is assigned to this load-balancing virtual server.

   d. Click **No Load Balancing Virtual Server Service**, click in the field below **Select Service** and then select the **svc_blue** service.

   e. Click **Select** and then click **Bind**.

   f. Click **Continue** and then click **Done**.

3. Create a non-addressable "lb_vsrv_green" load-balancing virtual server for the WebGreen web server.

   a. Click **Add** in the Load Balancing Virtual Servers pane. The Load Balancing Virtual Server settings window opens.

> This virtual server is dedicated to default users.

   b. Type `lb_vsrv_green` in the **Name** field and verify that **HTTP** is selected in the **Protocol** drop-down list.

   c. In the **IP Address Type** drop down menu, select **Non Addressable** and click **OK** to confirm the change. This action disables the IP address and Port fields. No VIP address is assigned to this load-balancing virtual server.

   d. Click **No Load Balancing Virtual Server Service Binding** and click in the field below **Select Service**.

   e. Select **svc_green** and click **Select**.

   f. Click **Bind** and then click **Continue**.

   g. Click **Done**.

Creating Policy Expressions

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. Create a policy expression that will respond to requests from iPhone clients.
   a. Go to **AppExpert** > **Expressions** > **Advanced Expressions**.
   b. Click **Add** in the **Advanced Expressions** pane. The Create Advanced Expressions window opens.
   c. Type `iPhone` in the **Expression Name** field and click **Expression Editor** to the right of the **Expression** field. The Expression Editor window opens.
   d. Configure the policy expression with the following settings using the drop down menu:
      - 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 **Done** and then click **Create**. The iPhone expression is created and the Create Policy Expression dialog box closes.
      - Final Expression: HTTP.REQ.HEADER("User-Agent").CONTAINS("iPhone")
      - Please note, the header value (iPhone) is case-sensitive in this expression.
2. Create a policy expression that responds to requests from Internet Explorer 6 clients.
   a. Click **Add** in the **Advanced Expressions** pane. The Create Policy Expression dialog box opens.
   b. Type `IE6` in the **Expression Name** field then click **Expression Editor** to the right of the **Expression** field. The Expression Editor window opens.
   c. Configure the policy expression with the following settings using the drop down menu:
      - 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` (There is a "space" between MSIE and 6.0.)
   d. Click **Done** and then click **Create**. The IE6 expression is created and the Create Policy Expression dialog box closes.
      - Final Expression: HTTP.REQ.HEADER("User-Agent").CONTAINS("MSIE 6.0")

- Please note, the header value (MSIE 6.0) is case-sensitive in this expression.

Creating Content-Switching Policies

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. Create a content-switching policy for iPhone clients.
   a. Go to the **Traffic Management** > **Content Switching** > **Policies** node, then click **Add**. The Create Content Switching Policy window opens.
   b. Type `cs_pol_mobile` in the **Name** field and then click **Saved Policy Expressions** in the **Expression** field.
   c. Select **iPhone** from the list.
   d. Click **Create**. This step creates the cs_pol_mobile policy.
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 window opens.
   b. Type `cs_pol_legacy` in the **Name** field, then click **Saved Policy Expressions** in the **Expression** field.
   c. Select **IE6** from the list.
   d. Click **Create**. This step creates the cs_pol_legacy policy.
3. Click the **Save** icon to save the NetScaler configuration and click **Yes** to confirm the saving of the configuration.

Creating the Content-Switching Virtual Server

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. Create a content-switching virtual server called cs_vsrv_rbg with an IP address of 172.16.0.84.
   a. Go to the **Traffic Management** > **Content Switching** > **Virtual Servers** node and click **Add** in the **Content Switching Virtual Servers** pane. The Content Switching Virtual Server settings window opens.
   b. Type `cs_vsrv_rbg` in the **Name** field and then type `172.16.0.84` in the **IP Address** field.
   c. Verify that the **Protocol** is set to **HTTP** and that the **Port** is set to `80`.
   d. Click **OK** to go to the next step.
2. Bind the cs_pol_mobile policy to the content-switching virtual server.
   a. Click **No Content Switching Policy Bound** and then click in the field below **Select Policy**.

   b. Select **cs_pol_mobile** and click **Select** to bind the mobile policy to the content switching virtual server. You should be back at the Policy Binding window where you will choose the Target Load Balancing Virtual Server to bind the cs_pol_mobile to.
   c. Click in the field below **Target Load Balancing Virtual Server** and select **lb_vsrv_red**.
   d. Click **Select**.
   e. A **Priority** is mandatory when using Advanced Expressions, so type **10** as the priority and click **Bind**.
   f. Click **OK**.
3. Bind the cs_pol_legacy policy to the content-switching virtual server.
   a. Click **1 Content Switching Policy** and then click **Add Binding**.
   b. Click in the field below **Select Policy** then select **cs_pol_legacy** radio button.
   c. Click **Select** to bind the legacy policy to the content-switching virtual server.
   d. Click in the field below **Target Load Balancing Virtual Server**, select **lb_vsrv_blue** and then click **Select**.
   e. Set Priority to 20.
   f. Click **Bind** and then click **Close**.
4. Set up the default user policy and bind it to the content switching virtual server.
   a. Click **No Default Load Balancing Virtual Server Bound** to bind the default policy to the content switching virtual server.
   b. Click in the field below **Default Load Balancing Virtual Server Name** and select **lb_vsrv_green**.
   c. Click **Create**, then click **Done**. This creates the virtual server.
5. Click the **Save** icon to save the NetScaler configuration and click **Yes** to confirm the saving of the configuration.

Testing the Content-Switching Configuration

Use a browser on the Student Desktop for this task.

1. Test the configuration to observe the content-switching behavior.
   a. Open a new Firefox browser window, browse to `http://172.16.0.84/home.php` and press **Enter**. The Green server displays for all other users (Firefox, IE 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.
   c. Click the **Refresh** button. The Red server displays only to mobile users (iPhone).
   d. Change the browser user agent to Internet Explorer 6 by clicking **Tools** > **iPhone 3.0** > **Internet Explorer** > **Internet Explorer 6** in Firefox.
   e. Click the **Refresh** button. The Blue server displays only to legacy browser users (MSIE 6.0).

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

g. Click the **Refresh** button. The Green server displays.

h. Close Firefox.

Module 12

Multi-tenancy and SDX NetScaler

12

Module 12: Multi-tenancy and SDX NetScaler

Introduction to the NetScaler SDX Appliance

The Citrix NetScaler SDX appliance is a multi-tenant platform on which you can provision and manage multiple NetScaler virtual machines (instances). The SDX appliance addresses cloud computing and multi-tenancy requirements by allowing a single administrator to configure and manage the appliance and delegate the administration of each hosted instance to tenants. The SDX appliance enables you to provide each tenant the following benefits:

- One complete instance - Each instance has identical privileges.
- A completely isolated network - Traffic meant for a particular instance is sent only to that instance.

Each complete instance has the following privileges:

- Dedicated CPU and memory resources
- A separate space for entities
- The independence to run the release and build of the administrator's choice
- Lifecycle independence

The Citrix NetScaler SDX appliance provides a Management Service that is pre-provisioned on the appliance. The Management Service provides a user interface (HTTP and HTTPS modes) and an API to configure, manage and monitor the appliance, the Management Service and the instances. A Citrix self-signed certificate is pre-packaged for HTTPS support. Citrix recommends that HTTPS mode is used to access the Management Service user interface.

Exercise 12-1: Managing a NetScaler SDX Appliance

This interactive exercise demonstrates how to log on to a NetScaler SDX appliance, create a new NetScaler VPX instance, bind two NetScaler VPX instances as an HA pair and log on to the NetScaler HA pair through the SNIP address. This exercise is based on a SIMULATION available within the eCourseware.

Managing a NetScaler SDX Appliance: Before You Begin

- **The Simulation for the following exercises can be found in the eCourseware.**
- Ensure that Adobe Flash Player (v.9 or above) is installed on your computer.
- Access the student resource kit and open the interactive activity in a web browser.

Estimated time to complete this exercise: 15 minutes

Managing a NetScaler SDX Appliance: Adding and Configuring a NetScaler VPX Instance

1. **Access the SDX Simulation from the link in the eCourseware manual in Module 12: Section 51 Managing a NetScaler SDX Appliance: Before You Begin.**
2. Log on to the NetScaler SDX Service VM.
    a. Select the **User Name** text box and type `nsroot`, then press **Enter**.
    b. Type `nsroot` in the Password field and then press **Enter**.
3. Create a new NetScaler VPX instance called CitrixEdu-2 with an IP address of 10.54.156.16 using an Enterprise-level feature license.
    a. Click on the **NetScaler** node, then **Instances**.
    b. Click the **Add** button at the top of the **Instances** pane on the home screen.
    c. Type `CitrixEdu-2` in the Name field, then press **Enter**.
    d. Type `10.54.156.16` in the IP Address field, then press **Enter**.
    e. Type `10.54.156.1` in the Gateway field, then press **Enter**.
    f. Click the drop down list next to the **Browse** button under the **XVA File** option and select **Appliance**.
    g. Select the **NSVPX-XEN-11.0-63.16_nc.xva** file then click **Open**.
    h. Select **Enterprise** from the Feature License drop-down list box.
4. Finish configuring the CitrixEdu-2 NetScaler VPX instance.
    a. Under **Instance Administration**.
    b. Type `CitrixAdmin` in the User Name field, then press **Enter**.
    c. Type `Password1` in the Password field, then press **Enter**.
    d. Type `Password1` in the Confirm Password field, then press **Enter**.
    e. Click **Add** under the Data Interfaces field and verify that **LA/1 (STATIC)** is selected then click **Add**.
    f. Click **Done** to complete the NetScaler VPX instance configuration.

> The Username and Password are case sensitive on the NetScaler.

5. Log on to the newly created NetScaler VPX instance using the CitrixAdmin/Password1 credentials.
    a. Open a **new tab** in the Firefox browser window.
    b. Type `10.54.156.16`, then press **Enter**.
    c. Select the **User Name** field, type `CitrixAdmin` and then press **Enter**.
    d. Type `Password1` in the Password field and then press **Enter**.
    e. Click **Login**.

6. Configure the CitrixEdu-2 with a SNIP address of 10.54.156.251.
    a. Click **Skip** on the **Citrix User Experience Improvement Program** pop-up window.
    b. On the **Welcome** screen click in the **Subnet IP Address** field.
    c. Type `10.54.156.251` in the IP Address field and press **Enter**, click **Done**, then click **Continue**.
7. Join the CitrixEdu-1 and CitrixEdu-2 NetScaler VPX instances in a High-Availability pair, with CitrixEdu-2 being the primary node.
    a. Select the **System** node, select the **High Availability** sub-node and then click **Add**.
    b. Type `10.54.156.15` in the Remote Node IP Address field, press **Enter**.
    c. Click in the **User name** field and enter `CitrixAdmin` then press enter.
    d. Type `Password1` in the Password field and then press **Enter**.
    e. Click **Create**, confirming that the High Availability pair has been set up.

    > The CitrixEdu-1 node is listed as Secondary and the CitrixEdu-2 node is listed as Primary.

    f. Click **Logout** at the top of the screen. This ends the simulation.

Module 13

Monitoring and Administration

13

Module 13: Monitoring and Management Exercises

Before You Begin

Before you begin, use XenCenter on the Student Desktop to power on (in addition to the other running VM's):

- InsightCenter (NetScaler Insight Center)

All virtual machines will now be powered on:

- DC.training.lab (Domain Controller)
- DC2.training.lab (Domain Controller 2)
- NSHA1 (NetScaler HA 1)
- NSHA2 (NetScaler HA 2)
- InsightCenter
- WebBlue
- WebGreen
- WebRed
- SF1
- SF2
- XD1
- XD2
- Win8XD1
- Win8XD2
- ExternalClient

If there are not enough resources to run all virtual machines, shutdown NSHA2 (secondary member of HA pair).

Estimated time to complete this exercise: 20 minutes

Exercise 13-1: Auditing and Logging

Use the Student Desktop to access the Kiwi Syslog Server and to manage the NetScaler configuration.

1. Configure the Kiwi Syslog Server to receive messages from the NetScaler IP.
    a. Start Kiwi Syslog Daemon: C:\Program Files\Syslogd\Syslogd.exe (or use the shortcut on the Student Desktop).

   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`. Retain all other default settings.
   e. Click **OK**.

Creating a Syslog Policy and Syslog Server

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. Configure a Syslog Policy and Syslog Server using 192.168.10.10 for the IP address.
   a. Switch to the configuration utility for the NetScaler SNIP.
   b. Browse to **System** > **Auditing** > **Syslog**.
   c. Click **Add**.
   d. Type `Ext_Kiwi` in the **Name** field.
   e. Click the + symbol next to the **Server** field.
   f. Enter `192.168.10.10` in the **IP Address** field and `514` in the **Port** field.
   g. Make sure the radio button for **All** under the **Log Levels** field is selected 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** appears in the **Server** field, click **Create**. This step creates the Syslog policy.
2. Bind the Syslog policy globally.
   a. Click the **Action** drop-down list and select **Global Bindings**.
   b. Click in the field below **Select Policy** and select **Ext_Kiwi** radio button.
   c. Click **Select**.
   d. Click **Bind** and then click **Done**.
   e. Click **Save** to save the NetScaler configuration and select **Yes** to confirm the saving of the configuration. By saving the running configuration, a Syslog audit message is generated. Syslog messages are sent to the Kiwi Syslog Server running on the Student Desktop. This message will be searchable in an upcoming task.
3. Configure a Syslog policy and Syslog server using 192.168.10.10 for the IP address.
   a. Go to **NetScaler Gateway** > **Policies** > **Auditing** > **Syslog**.
   b. Click **Add**.
   c. Type `Ext_Kiwi_NSG` in the **Name** field.
   d. Click the + symbol next to the **Server** field.
   e. Type `Ext_Kiwi_NSG` in the **Name** field, type `192.168.10.10` in the **IP Address** field and type `514` in the **Port** field.

    f. Select the radio button for **All** in the **Log Levels** field, set the **Log Facility** to **LOCAL1**.
    g. Click **Create**.
    h. Verify that **Ext_Kiwi_NSG** is selected in the **Server** field and then click **Create**.

4. Bind the Syslog Policy to the gateway.training.lab NetScaler Gateway virtual server.
    a. Go to the **NetScaler Gateway** > **Virtual Servers** node.
    b. Select the **gateway.training.lab** virtual server and click **Edit**.
    c. Scroll to the bottom of the page and select the **+ sign** in the **Policies** heading.
    d. Select **Audit Syslog** in the **Choose Policy** field.
    e. Click **Continue**
    f. Click in the field below **Select Policy**, select the **Ext_Kiwi_NSG** policy and then click **Select**.
    g. Click **Bind** and then click **Done**.

> Ensure that the gateway.training.lab virtual server is enabled. If it is not, right-click and select Enable.

5. Log on to gateway.training.lab in order to send Syslog data to the Kiwi Syslog Daemon.
    a. Switch to the ExternalClient virtual machine using the existing RDP shortcut. If needed, log on as citrix/Password1.
    b. Open a new web browser window and browse to `https://gateway.training.lab` and log on using the contractor/Password1 credentials. By logging on, Syslog messages specific to the gateway.training.lab virtual server are sent to the Kiwi Syslog Server running on the Student Desktop. This message will also be searchable in an upcoming task.
    c. Minimize the RDP session for ExternalClient and return to the Student Desktop.

Viewing Recent Audit Messages

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. View recent audit messages.
    a. Go to **System** > **Auditing**, then click **Recent audit messages** in the **Audit Messages** pane. The Audit Messages dialog box opens.
    b. Select one or more log levels to display, set the number of audit messages to be shown, then click **Run**. The viewer will be updated with the specified number of messages for the selected log levels. Check the Word Wrap box if needed. 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

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. View historical audit messages.
   a. Go to **System** > **Auditing** and select **Syslog messages** in the **Audit Messages** pane. The Syslog Viewer dialog box opens.
   b. On the right side of the window, click the **Severity** filter or other filter to sort the log messages.
      - Use the Module filter set to SSLVPN to see VPN and gateway specific events. (Click Apply to apply filter).
      - Use the Module filter set to AAA to see events related to external authentication.
   c. Select an historical log file from the File list on the right side of the window.

      > Historical log files are maintained by default under /var/log and are in ns.log.#.gz form.

   d. Click **Apply**. The Syslog Viewer updates and displays messages from the historical log.
   e. Type a search string under the Search field at the top of the Syslog Viewer and then click **Go** to view the search results.

      > Possible values for search string include: "lb vserver," "ns conf," or "config."", or "contractor"

   f. On the left side of the window, click **Back**. The Syslog Viewer dialog box closes.

Viewing Audit Messages on the Remote Syslog Server

From the Student Desktop, view the syslog records displayed in Kiwi Syslog Daemon.

1. View audit messages on the remote Syslog server.
   a. Switch to the Kiwi Syslog Daemon. View the Syslog messages from the NetScaler in the Display 00 (Default) Syslog window. Note that the "Priority" column shows a mix of "Local0.Info" and "Local1.Info" entries: the "Local0.Info" are global events, the "Local1.Info" are NetScaler Gateway vserver specific events. Also note that anything logged for the virtual server (Local1.Info) is also logged globally (Local0.Info). The systems in the lab will only have INFORMATIONAL messages to display.
   b. Close the Kiwi Syslog Service Manager.

Disabling Syslog Audit Messages

From the Student Desktop, use an HTTP connection to the NetScaler SNIP configuration utility logged on as the nsroot user for this task.

1. Disable logging of Global Syslog Audit Messages to the Kiwi Syslog Server.
    a. Switch to the configuration utility for the NetScaler SNIP.
    b. Go to **System** > **Auditing** > **Syslog**.
    c. Click the **Actions** drop-down list and select **Global Bindings**. The Bind/Unbind Auditing Policies to Global dialog box opens.
    d. Select the **Ext_Kiwi** policy, click **Unbind**, click **Yes** to confirm and then click **Done**. The Bind/Unbind Auditing Policies to Global dialog box closes.
2. Disable logging of virtual server-specific Syslog audit messages to the Kiwi Syslog Daemon.
    a. Switch to the configuration utility for the NetScaler SNIP.
    b. Go to **NetScaler Gateway** > **Virtual Servers**.
    c. Select **gateway.training.lab** and click **Edit**.
    d. Under Policies, select **1 Audit Syslog Policy**.
    e. Select the **Ext_Kiwi_NSG** policy, click **Unbind**, click **Yes** to confirm, click **Close** and then click **Done**. The dialog box closes.

Exercise 13-2: Monitoring

This exercise demonstrates how to configure SNMP monitoring on the NetScaler.

Configuring SNMP Settings

From the Student Desktop, use an HTTP connection to http://netscaler.training.lab, which resolves to the NetScaler SNIP 172.16.0.90, log on as the nsroot user for this task.

1. Configure an SNMP manager with a management host of 192.168.10.10.
    a. Go to **System** > **SNMP** > **Managers**.
    b. Click **Add** in the **SNMP Managers** pane. The Create SNMP Manager dialog box opens.
    c. Select the **Management Network** radio button and type `192.168.10.10` in the **IP Address** field.
    d. Click **Create**.
2. Configure an SNMP community named "ctxtrainsnmp" with permissions set to ALL.
    a. Go 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**.

3. Configure a specific SNMPv2 trap for the destination IP address 192.168.10.10. Associate the trap with the ctxtrainsnmp SNMP community.

    a. Go to **System** > **SNMP** > **Traps** and click **Add** in the SNMP Traps pane. The Create SNMP Trap Destination dialog box opens.

    b. Select the **Specific** radio button in the **Type** field and verify that **V2** is selected in the **Version** field.

    c. Type `192.168.10.10` in the **Destination IP address** field and leave the **Source IP Address** field blank.

    > The NSIP address is used by default as the Source IP when left blank. A specific SNIP may be specified when needed as an alternate Source IP.

    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**.

4. Enable and configure an SNMP alarm for save configuration events. Verify that the alarm is enabled and save the NetScaler configuration.

    a. Go to **System** > **SNMP** > **Alarms**.

    b. Select the **CONFIG-SAVE** alarm and click **Edit**. The Configure SNMP Alarm dialog box opens.

    c. Verify that Logging is **Enabled** and click **OK**. The Configure SNMP Alarm dialog box closes.

    d. Save the NetScaler config to generate an event.

Configuring the Kiwi Syslog Daemon and Viewing SNMP Alerts

Run Kiwi Syslog Daemon from the Student Desktop.

1. Start the Kiwi Syslog Daemon listening for SNMP traps on UDP port 162.

    a. Start Kiwi Syslog Daemon: C:\Program Files\Syslogd\Syslogd.exe (or use the shortcut on the Student Desktop).

    b. Click **File** and click **Setup**.

    c. Disable the UDP Syslog listener (so only the SNMP events will be displayed)

    d. Go to Inputs UDP. Disable (uncheck) Listen for UDP Syslog messages.
    e. Expand the **Inputs** node and select **SNMP**.
    f. Check **Listen for SNMP Traps** and verify that `162` appears in the **UDP Port** field.
    g. Select **Info** from the **Syslog Level** drop-down list and click **OK**.

2. Prepare the listener for an informational trap from the Syslog Level drop-down list box. Clear any previously captured data.
    a. Click **View** and select **Clear display**.
3. Switch to the NetScaler configuration utility and click the **Save** icon to save the running configuration and send an SNMP trap.
4. Click **Yes** to confirm the saving of the configuration.
5. View the SNMP traps in the Kiwi Syslog Daemon. The SNMP Syslog will resemble the following:

```
01-15-
2016 16:22:43 Local7.Info 172.16.0.5 community=ctxtrainsnmp,
enterprise=1.3.6.1.4.1.5951.1.1.0.28,
enterprise_mib_name=netScalerConfigSave, uptime=8249804,
agent_ip=192.168.10.10, version=Ver2, nsUserName.0=nsroot,
sysIpAddress.0=172.16.0.5
```

6. Close the Kiwi Syslog Daemon application.

Exercise 13-3: Configuring Insight Center

This exercise demonstrates how to configure Insight Center to monitor HDX traffic.

Performing Insight Center Initial Setup

1. Perform the initial configuration for Insight Center using an IP address of 192.168.10.12, netmask of 255.255.255.0 and gateway of 192.168.10.1
2. From the Student Desktop, use XenCenter to access the InsightCenter virtual machine console:
    a. In XenCenter, select **InsightCenter** in the left pane.
    b. Select the **Console** tab in the right pane.
    c. The Initial Network Address Configuration menu will appear after the machine is started.
3. Assign 192.168.10.12 as the IP address for Insight Center.
    a. Type `1` and press **Enter**.
    b. Type `192.168.10.12` and press **Enter**.
4. Assign 255.255.255.0 as the netmask for Insight Center.
    a. Type `2` and press **Enter**.

    b. Type `255.255.255.0` and press **Enter**.

5. Assign 192.168.10.1 as the gateway IP address for Insight Center.
    a. Type `3` and press **Enter**.
    b. Type `192.168.10.1` and press **Enter**.
6. Save the Insight Center settings.
    a. Type `6` and then press **Enter** to save the configuration.
    b. Type `1` and then press Enter
    c. Type `yes` and press Enter to reboot.

> It will take a minute for the GUI to respond after the Insight Server shows the login prompt.

Configuring Insight Center

Connect to the Insight Center and NetScaler configuration utilities from a web browser on the Student Desktop.

1. Specify Insight Center to monitor the HA_1 NetScaler appliance.
    a. Open a browser, browse to `http://insight.training.lab` or `http://192.168.10.12` and press **Enter**.
    b. Type `nsroot` in the User Name and Password fields, then click **Login**. This will bring up the **NetScaler Insight Center Welcome** screen. Click **Skip** on the Citrix User Experience Improvement program window.
    c. Click **Get Started**.
    d. Type the following values in the **NetScaler Insight Center Inventory Setup** screen.
        - NetScaler IP address: `172.16.0.5`
        - User name: `nsroot`
        - Password: `nsroot`
    e. Click **Add**. The Application List is populated with the load-balancing and VPN virtual servers from the NetScaler.
    f. Click **Return to Inventory list**.
2. Add an NTP server.
    a. Click **NTP Servers** under the **System** node and click **Add**.
    b. Type `192.168.10.11` and then click **Create**.
    c. Right-click the 192.168.10.11 NTP server and select **NTP Synchronization**.
    d. Select **Enable NTP Synchronization** and click **OK**.

Enabling Data Collection

From the Student Desktop, use an HTTP connection to the Insight Center configuration utility logged on as the nsroot user for this task.

1. Enable AppFlow on the VPN virtual servers.
    a. Click the **Configuration** tab in Insight Center (at 192.168.10.12).
    b. Click the **172.16.0.5 (NSHA1)** link.
    c. Select **VPN** from the **View** drop-down list.
    d. Right-click the **172.16.0.30** virtual server and select **Enable AppFlow**.

    > You can enable data collection on a virtual server only if the operational state is UP.

    e. Select `true` from the **Select Expression** drop-down list and click **OK**.
2. Verify that AppFlow and EdgeSight Monitoring are enabled on the NetScaler.
    a. Switch to the NetScaler configuration utility for NetScaler NSHA1 and log on using the nsroot credentials. For best results, open this in a different tab in the browser: http://netscaler.training.lab.
    b. Click the **Configuration** tab and go to **System** > **Settings**.
    c. Click **Configure Advanced Features**.
    d. Ensure that the AppFlow feature is enabled and click **Close**.
3. Verify that policies were bound correctly to the NetScaler Gateway.
    a. Navigate to **NetScaler Gateway** > **Virtual Servers**.
    b. Double-click the **gateway.training.lab** virtual server and verify that AppFlow Logging is enabled (true).
    c. Scroll to the bottom of the page and click **1 Appflow Policy** under the **ICA Request Policies**.
    d. Verify that the **af_policy_gateway.training.lab_192.168.10.12** policy is bound to the virtual server, click **Close** and then click **Done**.
4. Bind the AppFlow policy to the load-balancing virtual server.
    a. Click the **Configuration** tab and go to **Traffic Management** > **Load Balancing** > **Virtual Servers**.
    b. Double-click the **ssl_vsrv_sf** virtual server.
    c. Select **Policies** in the right pane.
    d. Click the **+ sign** to the right of the **Policies** heading.
    e. Select **App Flow** from the **Choose Policy** drop-down.
    f. Click **Continue**.
    g. Under the **Policy Binding** section, click inside the **Select Policy** field.

    h. Select the **af_policy_gateway.training.lab_192.168.10.12** policy and click **Select**.
    i. Assign a priority of `10`.
    j. Click **Bind** and then click **Done**.
    k. Click the **Save** icon to save the NetScaler configuration and then click **Yes** to confirm saving the configuration.

Test the HDX Traffic

Use the ExternalClient virtual machine logged on as the citrix user for this task

1. Switch to the RDP session for ExternalClient. Log on as citrix/Password1, if not already connected.
2. Log on to the NetScaler Gateway to generate HDX traffic.
    a. Open a Firefox browser, browse to `http://gateway.training.lab` and click **Enter**.
    b. Log on with the contractor/Password1 credentials. You should be connected to the StoreFront.
    c. Click **XenDesktop**.
    d. Start the XenDesktop session and launch Internet Explorer.
    e. Browse to `http://blue.training.lab/home.php` and press **Enter**.
3. Return to the Student Desktop.
4. View HDX Insight traffic.
    a. Switch to Insight Center (at 192.168.10.12) on the browser from the Student Desktop.
    b. Go to the Dashboard tab.
    c. Go to **HDX Insight** > **Users**.

    > The HDX Insight dashboard may take as long as five minutes to display any data.

    The graph should indicate user activity and the users logged on through the Gateway.

    d. Select the other nodes under HDX Insight to view the activity.
    e. To get better data, try logging off and logging on to the session to see a new session start as opposed to reconnecting to a disconnected session.
5. When you have finished viewing the traffic in Insight Center, close your browser window and shut down the Insight Center virtual machine.

Module 14

Troubleshooting Exercises

14

Module 14: Troubleshooting Exercises

Exercise 14: Troubleshooting

The following scenarios are based on the lab exercises that you performed during the week. Each troubleshooting scenario presents a problem that you need to resolve. There are checkpoints in each lab to help you determine the solution.

You will be working on the NetScaler NSHA1 virtual machine. During this exercise, NetScaler NSHA2 will be powered off. To start the troubleshooting lab, you will run a script that will back up your current configuration and then introduce a bad configuration for the NetScaler for you to investigate.

Before You Begin

Before you begin, power off:

- NSHA2 (NetScaler HA 2)

Estimated time to complete this exercise: 30 minutes

Preparing the NetScaler for the Troubleshooting Lab

From the Student Desktop use XenCenter to manage the virtual machines and a web browser to connect to the NetScaler NSHA1 configuration utility. At various points in the lab you have to switch from using the shared management IP accessed via http://netscaler.training.lab (172.16.0.90) to the NSHA1 NSIP at http://nsha1.training.lab (172.16.0.5).

1. Use XenCenter or power off NetScaler NSHA2.
    a. Select NSHA2 in the XenCenter console.
    b. Right-click and select Shut down.
    c. Wait for NSHA2 to shutdown completely before continuing.
2. Run a batch script on the NetScaler configuration to begin the troubleshooting scenario.
    a. Launch a PuTTY session to the NetScaler NSHA1 virtual machine (172.16.0.5) and log on to the command-line interface using the nsroot credentials.
    b. Run the script on the NetScaler configuration by entering the following commands:

```
batch -f /var/labstuff/troubleshoot/break.txt
y
```

The batch script saves and moves the current NetScaler configuration to a different location, loads a bad configuration file, then restarts the NetScaler.

Exercise 14-1: Troubleshooting Scenario 1

You have just returned to work after a vacation and noticed that when you attempt to access the NetScaler using the subnet IP address (172.16.0.90), you get an error.

Where to Begin

Access the NetScaler and browse to the **Network** node. Check the settings for the routes and IPs.

Checkpoint

Checking the following items may help you troubleshoot this issue.

- Are you able to log on to NetScaler NSHA1 by browsing to nsha1.training.lab and logging on?
- Can you access the NetScaler via the shared management SNIP netscaler.training.lab and logging on?
- Is your Subnet IP address properly configured?
- Are the routes to the NetScaler properly configured?

The issue is considered resolved when the following conditions have been met:

- You are able to log on to the NetScaler using the SNIP address.

Exercise 14-2: Troubleshooting Scenario 2

While attempting to browse to http://colors.training.lab, you notice that the page does not automatically forward to https://colors.training.lab.

Where to Begin

Go to **Traffic Management** > **Load Balancing** and check the load balancing settings.

Checkpoint

Checking the following items may help you troubleshoot this issue:

- Are the WebRed, WebBlue and WebGreen virtual machines started in XenCenter?
- Are the corresponding services for WebRed, WebBlue, and WebGreen in an UP state?
- Are the HTTP and SSL lb virtual servers in an UP state?
- Are the policies applied to the virtual servers still bound?
- When you test do you see policy hits occur?

- Is feature enabled?

The issue is considered resolved when the following conditions have been met:

- You can browse to http://colors.training.lab and the address automatically changes to https://colors.training.lab.

Exercise 14-3: Troubleshooting Scenario 3

One morning you discover that you are unable to log on to the NetScaler using your domain credentials. You are able to log on using the local accounts.

- Test authentication to a management IP as nsroot (or other local account).
- Test authentication to a management IP as a domain account: citrixadmin / Password1.

Where to Begin

Go to **System** > **Authentication** > **LDAP** and verify that the settings for the LDAP server and policies are correct.

Checkpoint

Checking the following items may help you troubleshoot this issue:

- Is the Domain Controller VM started in XenCenter?
- Is the LDAP load balancing virtual server in an UP state?
- Is LDAP Authentication properly configured on the NetScaler?

The issue is considered resolved when you can log on to the NetScaler using the training\CitrixAdmin credentials.

Exercise 14-4: Troubleshooting Scenario 4

After logging on to the NetScaler Gateway, the contractor user is unable to reach StoreFront. He only sees the NetScaler Gateway homepage.

- To test, from ExternalClient attempt to connect to https://gateway.training.lab as contractor/Password1.
- Do you see the Gateway Portal page, a choices page, or StoreFront?

Where to Begin

Log on to NetScaler NSHA1 and browse to the NetScaler Gateway Policy Manager to verify the policy and group settings.

Checkpoint

Checking the following items may help you troubleshoot this issue:

- Is the gateway.training.lab virtual server in an UP state?
- Can StoreFront be directly addressed outside of the gateway from the Student Desktop as an "internal" user Console? Test url: https://storefront.training.lab/Citrix/StoreWeb/
- Are the session policies bound to the NetScaler vpn vServer or the appropriate AAA group?

The issue is considered resolved when the following conditions have been met:

- You are able to log on to the NetScaler Gateway and launch a published desktop through StoreFront. Test from the ExternalClient at https://gateway.training.lab.

(Optional) Returning the NetScaler to Previous State

Use the Student Desktop virtual machine logged on as the training\CitrixAdmin user for this task.

1. Run a batch script to revert the NetScaler to the state that it was before beginning the troubleshooting labs.
    a. Launch a PuTTY session to the NetScaler NSHA1 virtual machine and log on to the command-line interface using the nsroot credentials.
    b. Run a batch script to return the NetScaler to its previous state using the following command:

    ```
    batch -f /var/labstuff/troubleshoot/fix.txt
    y
    ```

    The batch script moves the broken NetScaler configuration to a different location, loads the previously saved configuration file, then restarts the NetScaler.

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