CITRIX®

Education

XenApp, XenDesktop, and Provisioning Services 7.1x Administration (Fast Track)

Citrix Course: CMB-310-1i

Exercise Workbook

Version 1.1

Credits

Title	Name
Architect	Justin Apsley
Product Manager	Amit Ben-Chanoch
Technical Solutions Developers	Carsten Thue Jessica Biesel Natanael De Leon Prabhjot Singh Bhatia Daniel Wipperfürth Edwin Villafana Karthik Raja Nitesh Sharma Ryan Keller
Instructional Designer	Elizabeth Diaz
Graphic Designer	Ryan Flowers

Contents

Credits 2

Exercise Workbook Overview 7

Lab Environment Overview 8

LAB ACCESS 10

Citrix Hands-on Labs 11

Module 3: Installing and configuring a XenApp and XenDesktop Site 12

- Exercise 3-1: Install the Citrix License Server and the Citrix License Server Administration Console 12
- Exercise 3-2: Activate, allocate and download a License File 16
- Exercise 3-3: Upload a license file to the Citrix License Server 22
- Exercise 3-4: Install the Delivery Controller role 29
- Exercise 3-5: Create and configure a XenApp and XenDesktop Site 36
- Exercise 3-6: Install Citrix Director 43

Module 4: Provision and deliver application and desktop resources 50

- Exercise 4-1: Prepare the Server OS image 50
- Exercise 4-2: Create a Machine Catalog for Server OS using MCS 61
- Exercise 4-3: Create a Machine Catalog for Server OS using Manual Provisioning 69
- Exercise 4-4: Create two Delivery Groups for Server OS Catalogs 72
- Exercise 4-5: Create a Machine Catalog for Remote PC 87
- Exercise 4-6: Create a Delivery Group for Remote PC 91
- Exercise 4-7: Create a snapshot of the Desktop OS VM 97
- Exercise 4-8: Create Machine Catalog for Desktop OS 98
- Exercise 4-9: Create a Delivery Group for Desktop OS 105
- Exercise 4-10: Update a Machine Catalog for Desktop OS 111

Module 5: Providing access with StoreFront and Receiver 119

- Exercise 5-1: Install the StoreFront Server 119
- Exercise 5-2: Create a StoreFront Store 124
- Exercise 5-3: Encrypt StoreFront store traffic 132
- Exercise 5-4: Set the StoreFront default page 155
- Exercise 5-5: Configure the default domain 157
- Exercise 5-6: Adjust the StoreFront timeout 164
- Exercise 5-7: Configure StoreFront store branding 168
- Exercise 5-8: Deploy Citrix Receiver through StoreFront 172
- Exercise 5-9: Configure email-based account discovery 182
- Exercise 5-10: Configure Delegated Authentication 190
- Exercise 5-11: Add Favorites to the StoreFront store 195
- Exercise 5-12: Disable Desktop Auto-launch 199
- Exercise 5-13: Launch an application and desktop from a Server OS 201
- Exercise 5-14: Launch a desktop from a Remote PC 202
- Exercise 5-15: Launch a desktop from a Desktop OS 203

Module 6: Understanding and configuring Citrix policies 205

- Exercise 6-1: Create a Group Policy to set Baseline- Computer settings 205
- Exercise 6-2: Configure baseline Citrix user policy using Group Policy 212
- Exercise 6-3: Configure Group Policy loopback processing 216
- Exercise 6-4: Create Citrix policies from templates 222
- Exercise 6-5: Configuring client drive mapping using Studio 228

Exercise 6-6: Run the Policy Modeling Wizard from Studio 232
Exercise 6-7: Create a load management policy using Studio 237
Exercise 6-8: Test the newly configured load management policy settings 245
Module 7: Application presentation and management 253

Exercise 7-1: Configure and test Application Limits 253
Exercise 7-2: Configure subscription keywords 256
Exercise 7-3: Test subscription keywords 260
Exercise 7-4: Configure and test Application Prelaunch and Application Lingering 262
Exercise 7-5: Configuring File Type Associations 270
Exercise 7-6: Test File Type Associations 272
Exercise 7-7: Configure Featured App Groups and App Categories 275
Exercise 7-8: Test the App Group and App Categories 282
Exercise 7-9: Configure Shortcut Placement 283
Exercise 7-10: Test Shortcut Placement 287
Exercise 7-11: Disable Self-Service Mode and Test 289
Exercise 7-12: Create and Test Application Group 292
Module 8: Printing with XenApp and XenDesktop 297

Exercise 8-1: Configure Printer Auto Creation 297
Exercise 8-2: Test that Auto Creation was Successful 301
Exercise 8-3: Configure Session Printers 303
Exercise 8-4: Test that the Session Printers Mapped to the Session 310
Exercise 8-5: Configure Print Job Routing 311
Exercise 8-6: Configure Print Driver Mapping 316
Exercise 8-7: Test the Print Driver Mapped 320
Exercise 8-8: Configure the Universal Print Driver 321
Exercise 8-9: Test that the Printer Auto-created with the Universal Print Driver 324
Exercise 8-10: Configure the Universal Print Server Component 326
Module 9: Citrix Profile Management 333

Exercise 9-1: Configure Citrix Profile Management Using Group Policy 333
Exercise 9-2: Test Citrix Profile Management 342
Exercise 9-3: Configure Profile Protection 344
Exercise 9-4: Test Profile Protection 346
Module 10: Managing the XenApp and XenDesktop Site 352

Exercise 10-1: Create a Custom Role 352
Exercise 10-2: Create a Custom Scope 354
Exercise 10-3: Create Delegated Administrator Accounts 356
Exercise 10-4: Create Help Desk Delegated Administrator 360
Exercise 10-5: Login and Test the Delegated Administrator 363
Exercise 10-6: Create a Delegated Administration Report 365
Exercise 10-7: Create a Configuration Logging Report 367
Module 11: XenApp and XenDesktop Site Redundancy Considerations 372

Exercise 11-1: Install the Second Delivery Controller Server 372
Exercise 11-2: Join the Second Delivery Controller to the Site 378
Exercise 11-3: Configure and Test Local Host Cache 382
Exercise 11-4: Install the Second StoreFront Server 395
Exercise 11-5: Join the Second StoreFront Server to the Server Group 401
Exercise 11-6: Edit the Store to Add the Second Delivery Controller 405
Exercise 11-7: Configuring Load Balancing of the StoreFront Servers 408
Exercise 11-8: Test the Load Balancing of the StoreFront Servers 417
Module 12: XenApp and XenDesktop Site Basic Network Security Considerations 419

Exercise 12-1: Secure XML Traffic on NYC-XDC-001 419
Exercise 12-2: Secure XML Traffic on NYC-XDC-002 425
Exercise 12-3: Configure the Store to Use Secure XML Connections 435
Exercise 12-4: Integrate StoreFront with the NetScaler Gateway 438
Exercise 12-5: Enable Remote Access to the Store 442
Exercise 12-6: Propagate the StoreFront Settings to the Server Group 444
Exercise 12-7: Test External Access through the NetScaler Gateway 446
Module 13: Monitoring the XenApp and XenDesktop Site 447

Exercise 13-1: Launch and Login to Citrix Director 447
Exercise 13-2: Login to Citrix Director as a Delegated Help Desk Administrator 448
Exercise 13-3: Use Citrix Director to View Alerts 450
Exercise 13-4: View the Session Default View Page 453
Exercise 13-5: View the Session Details Page 456
Exercise 13-6: Log Off a User Session 458
Exercise 13-7: Disconnect a User Session 461
Exercise 13-8: Shadow a User Session 464
Exercise 13-9: Reset the User Profile 467
Exercise 13-10: End a Process within a User Session 471
Exercise 13-11: Send a Message to a User Session 473
Exercise 13-12: Integrate HDX Insight with Director 476
Exercise 13-13: View and Interact with the New Trends Page 477
Exercise 13-14: View and Interact with the New User Details Page 479
Module 14: Troubleshooting 482

Exercise 14-1: Leverage the Citrix Supportability Pack and use the Citrix Health Assistant 482
Exercise 14-2: Leverage the Citrix Supportability Pack and use the Citrix Receiver Clean-Up Utility 488
Exercise 14-3: Leverage the Citrix Supportability Pack and use the HDX Monitor 492
Exercise 14-4: Leverage the Citrix Supportability Pack and use the Scout Utility 500
Module 16: Provisioning Services Infrastructure. 505

Exercise 16-1: Install Provisioning Services 505
Exercise 16-2: Configure Provisioning Services Farm 511
Exercise 16-3: Configure the Farm Store 525
Module 17: Streaming the vDisk 530

Exercise 17-1: Create vDisk for Server OS 530
Exercise 17-2: Create VDisk for Desktop OS 545
Exercise 17-3: Verify the Store via File Explorer 562
Exercise 17-4: Verify the Store via PVS Console 564
Exercise 17-5: Configure DHCP Options (66 and 67) 566
Exercice 17-6: Configure Boot ISO 571
Module 18: Target Devices 577

Exercise 18-1: Set the Write Cache location for the Server OS vDisk 577
Exercise 18-2: Set the Write Cache location for the Desktop OS vDisk 580
Exercise 18-3: Add a Persistent Drive and Redirect Event Logs 582
Module 19: Integrating Provisioning Services with XenApp and XenDesktop 593

Exercise 19-1: Copy the Server OS Master and convert to a template 593
Exercise 19-2: Copy the Desktop OS Master and convert to a template 596
Exercise 19-3: XDSW for Server OS 598
Exercise 19-4: XDSW Desktop OS 611
Exercise 19-5: Streamed VM Setup Wizard 622
Exercise 19-6: Manually Adding Machines to the Device collection 628
Exercise 19-7: Create a Delivery Group for Server OS 632

Exercise 19-8: Create a Delivery Group for Desktop OS 636
Exercise 19-9: Launch Published Application and Desktop 640
Module 20-1: Advanced Architecture 644
Exercise 20-1: Join Second PVS server to the Farm 644
Exercise 20-2: Reconfigure the Store for Redundancy 657
Exercise 20-4: Verify vDisk Replication 659
Exercise 20-5: Copy a vDisk from One Store to Another 661
Exercise 20-6: Import a Pre-Existing vDisk and Create a New .pvp File 664
Exercise 20-7: TFTP Load Balancing Configuration 668
Module 21: Supporting PVS 688
Exercise 21-1: Update the vDisk 688
Exercise 21-2: Promote the vDisk 693
Exercise 21-3: Rollback the vDisk 695
Exercise 21-4: Merge the vDisk 697
Exercise 21-5: Enable Provisioning Service Auditing 700
Exercise 21-6: Use the Console to view Auditing 702
Exercise 21-7: Use PowerShell to view Auditing 704

Exercise Workbook Overview

Lab Exercises:
The exercises in this Exercise Workbook were developed for use with the CMB-310-1i Citrix XenApp and XenDesktop course. The virtual machines in this lab are running on Windows Server 2016 and Windows 10 Desktop.

At the completion of these exercises, you will gain valuable hands-on experience in installing, configuring, administering and supporting XenApp, XenDesktop and Provisioning Services 7.13.

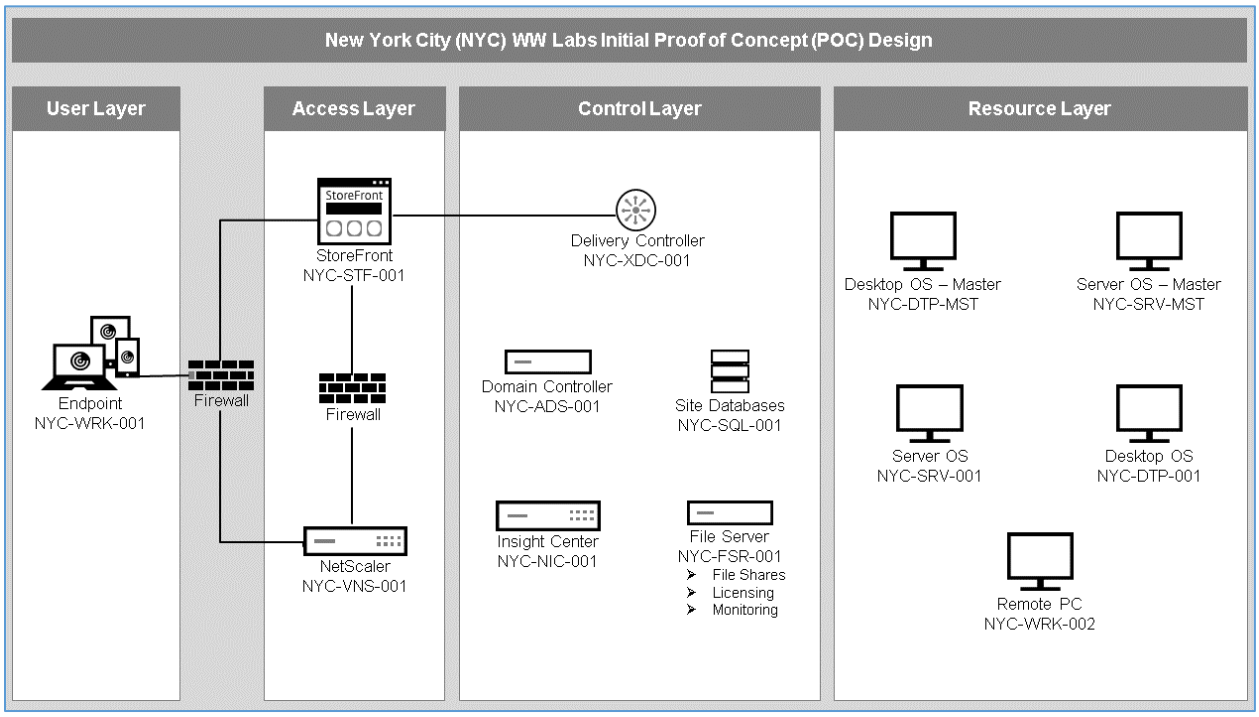
Lab Scenario:
WW Labs is a technical company whose infrastructure topology is centrally located in New York City, referenced as NYC in the company naming convention. The CTO has authorized the purchase of XenDesktop Platinum licenses. This license edition includes all of the features of both XenApp, XenDesktop, and Provisioning Services. The Lead Citrix Architect has tasked the Citrix Administrator team to implement a Proof of Concept (POC) XenApp, XenDesktop, and Provisioning Services environment utilizing the current implementation of Active Directory, DHCP, DNS, and SQL Server. Pending the resultant POC, the Citrix Administrator team will be further tasked to scale the environment to include redundancy and security considerations.

The Lead Citrix Architect has concluded that XenApp, XenDesktop, and Provisioning Services 7.13 meets the company's requirements and has instructed the Citrix Administrator team to validate this XenApp and XenDesktop and PVS POC for three specific use cases:

- ✓ HR User Group: Hosted Shared Desktop and Published Apps
- ✓ Technician User Group: Hosted VDI (Random/Non-Persistent)
- ✓ Designer User Group: Remote PC

You are a Citrix Administrator on the WW Labs Citrix Administrator team and you have been tasked to assist with this implementation.

Lab Environment Overview



SERVER LIST

Virtual Machine Name	IP Address	Operating System	Description
NYC-ADS-001	192.168.10.11	Windows Server 2016	Domain Controller, DNS, DHCP
NYC-SQL-001	192.168.10.21	Windows Server 2016	SQL Server
NYC-FSR-001	192.168.10.17	Windows Server 2016	File Server, Print Server, License Server
NYC-XDC-001	192.168.10.46	Windows Server 2016	Delivery Controller
NYC-XDC-002	192.168.10.47	Windows Server 2016	Delivery Controller
NYC-STF-001	192.168.10.31	Windows Server 2016	StoreFront 3.8
NYC-STF-002	192.168.10.32	Windows Server 2016	StoreFront 3.8
NYC-PVS-001		Windows Server 2016	Provisioning Services Server
NYC-PVS-002		Windows Server 2016	Provisioning Services Server
NYC-MAN-001	192.168.10.59	Windows Server 2016	Server OS VDA – Manually Provisioned
NYC-SRV-001	DHCP	Windows Server 2016	Server OS VDA – MCS Provisioned
NYC-DTP-001	DHCP	Windows 10	Desktop OS VDA 7.13
NYC-WRK-001	192.168.10.56	Windows 10	Managed Endpoint
NYC-WRK-002	192.168.10.61	Windows 10	Internal Design Workstation
NYC-WRK-004	DHCP	Windows 10	Existed Machine to add into a PVS device collection
NYC-VNS-001	192.168.10.100	11 Build 64.34	NetScaler
NYC-NIC-001	192.168.10.118	11 Build 64.34	NetScaler Insight Center
NYC-TDS-MST	DHCP	Windows Server 2016	NYC-SRV-MST after imaging - PVS

NYC-TDS-001	DHCP	Windows Server 2016	Server OS VDA – Provisioned from PVS XenDesktop Setup Wizard
NYC-TDD-001	DHCP	Windows 10	Desktop OS VDA – Provisioned from PVS XenDesktop Setup Wizard
NYC-TDD-002	DHCP	Windows 10	Desktop OS VDA – Provisioned from PVS Streamed Setup Wizard
MCS-SRV-MST	192.168.10.48	Windows Server 2016	Windows 2016 Master Template - MCS
MCS-DTP-MST	192.168.10.60	Windows 10	Windows 10 Master Template - MCS
PVS-SRV-MST	DHCP	Windows Server 2016	Windows 2016 Master Template - PVS
PVS-TDS-MST	DHCP	Windows 10	Windows 10 Master Template - PVS

CREDENTIALS LIST

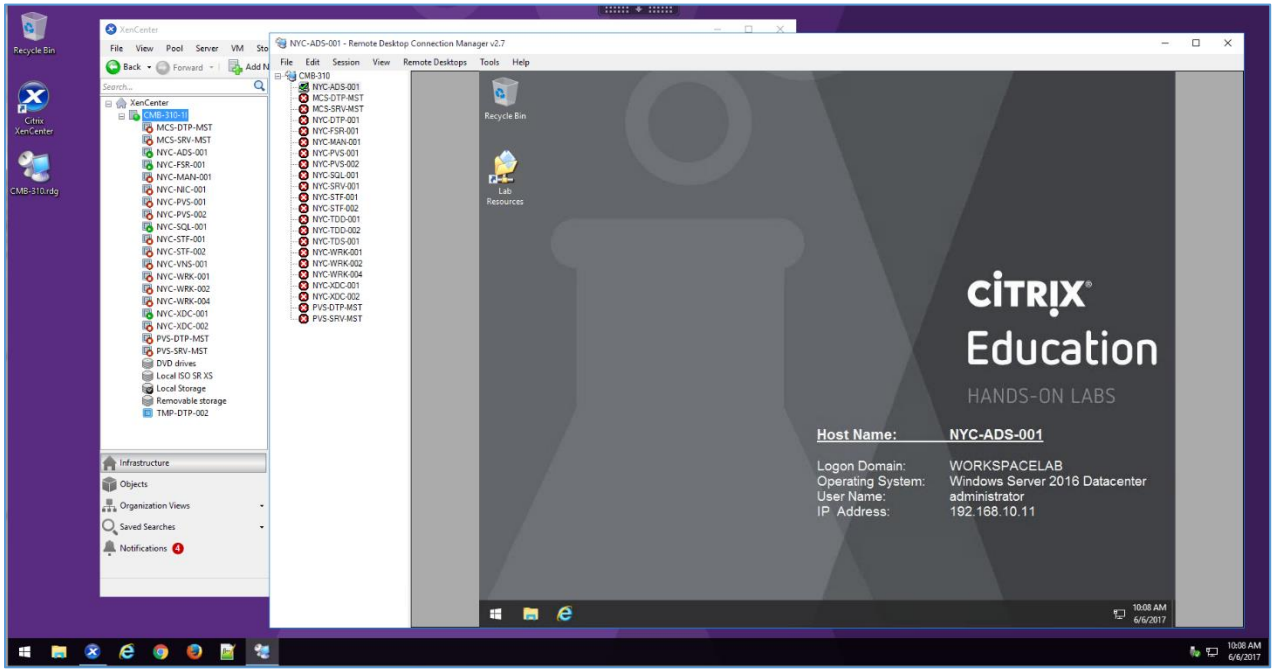
User Name	Password	Description
Workspacelab\Administrator	Password1	Domain Administrator (workspacelab.com)
Administrator	Password1	Local (non-domain) user
Citrix	Password1	Local (non-domain) user
Workspacelab\HR1	Password1	HR User
Workspacelab\Engineer1	Password1	Engineering User
Workspacelab\Marketing1	Password1	Domain User
Workspacelab\XDAdmin	Password1	XenDesktop Admin
Workspacelab\HDAdmin	Password1	License Administrator

LAB ACCESS

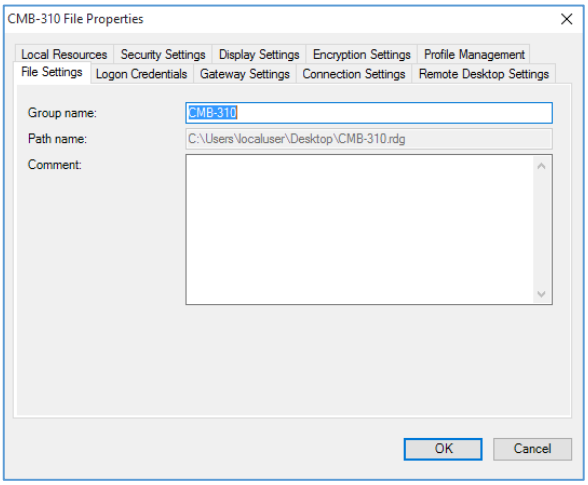
Once connected to the Student Desktop, launch both the lab management consoles: the Remote Desktop Connection Manager and XenCenter as shown in the example below.

The icon to launch the Remote Desktop Connection Manager is named *CMB-310.rdg* and the icon to launch XenCenter is *Citrix XenCenter*.

You will primarily use the Remote Desktop Connection Manager to log on and interact with your virtual lab machines. You will primarily use XenCenter to manage the power state of the virtual machines and manage the mounting and un-mounting of ISOs used in installations.



Remote Desktop Connection Manager is pre-configured with the credentials required for this lab. To select the credentials you wish to use as shown in the example below, right-click the machine and select **Connect server as**.



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 will 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 are migrating to a new version of a product or discovered a product feature, you previously did not know about, you could 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 3: Installing and configuring a XenApp and XenDesktop Site

Overview:

This module presents the steps to implement the initial XenApp and XenDesktop components to create a licensed Site.

A Site is the term used to represent the management scope of a XenApp and XenDesktop deployment. To create this Site, we will address the following core tasks:

- Install, configure, and license a Citrix License Server
- Install and configure a Delivery Controller
- Create the Site and manage the Site databases

Before you begin:

Estimated time to complete Module 3 lab exercises: 55 minutes

Exercise 3-1: Install the Citrix License Server and the Citrix License Server Administration Console

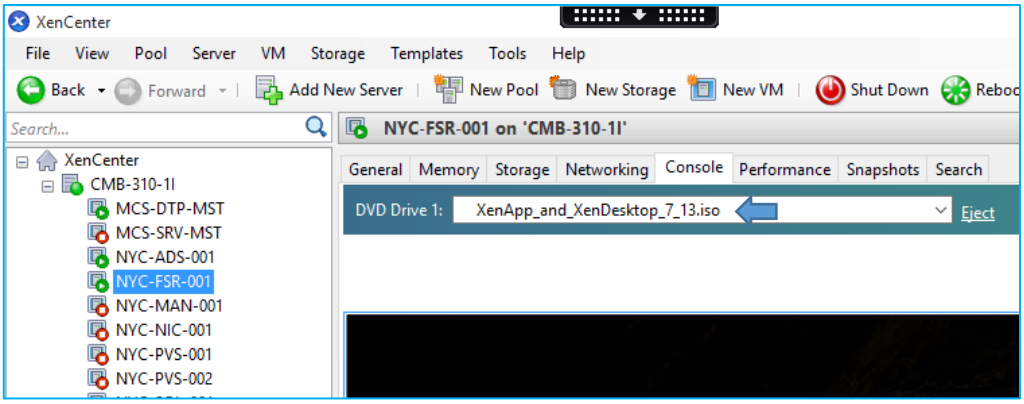
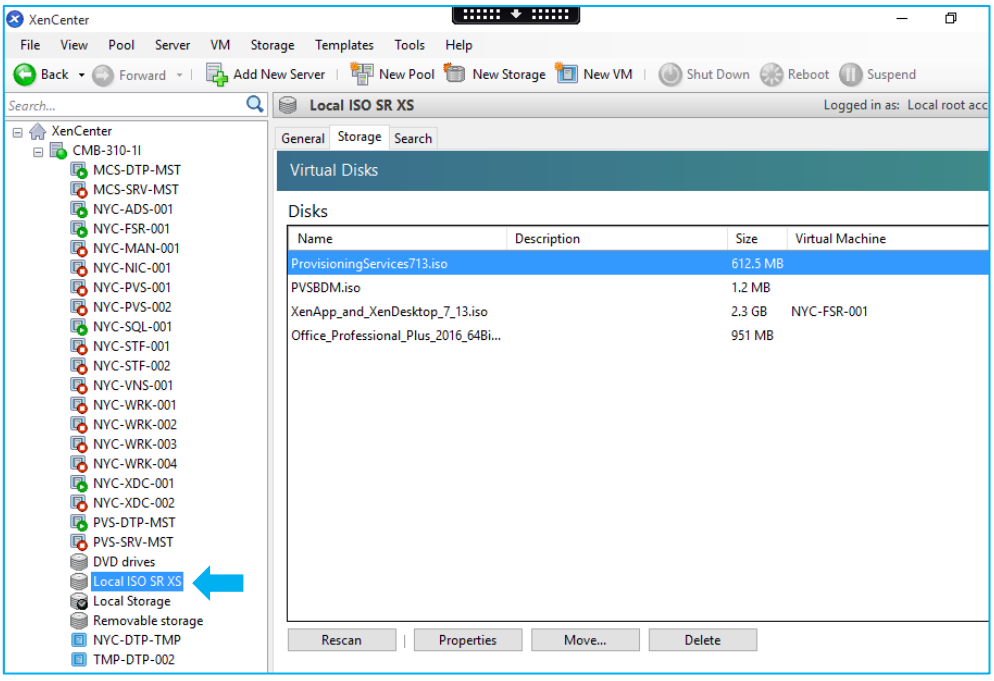
Scenario:

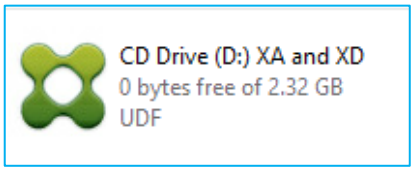
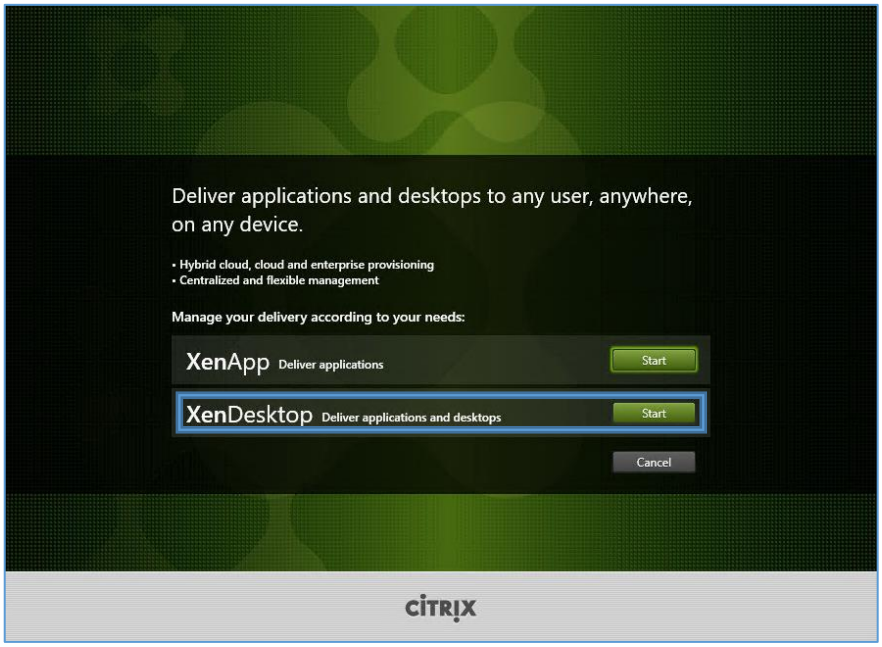
The Lead Citrix Architect has explained to the Citrix Administrator team that Citrix Leading Practice to begin deployment of XenApp and XenDesktop is to start with licensing. That way, licensing is already established when you configure the Site, so you only have to point to the license in order to continue.

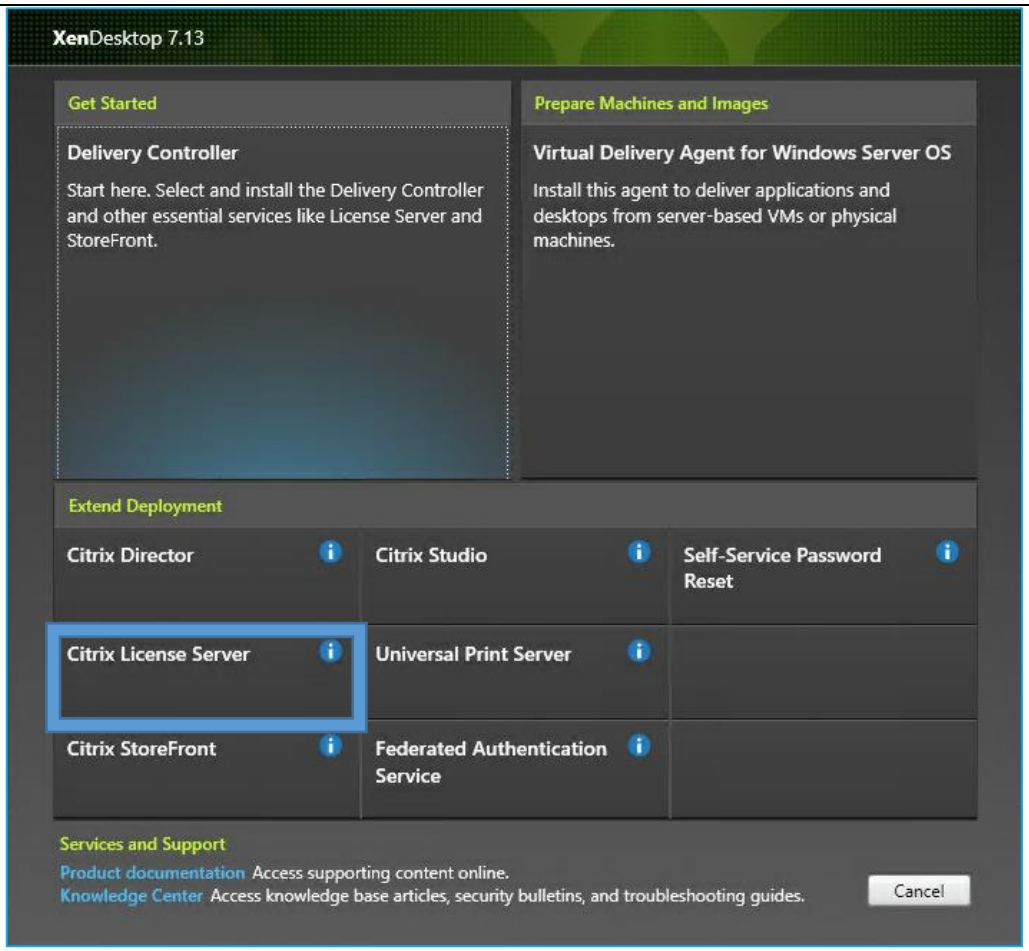
You have been tasked with installing the Citrix License Server and the Citrix License Administration Console.

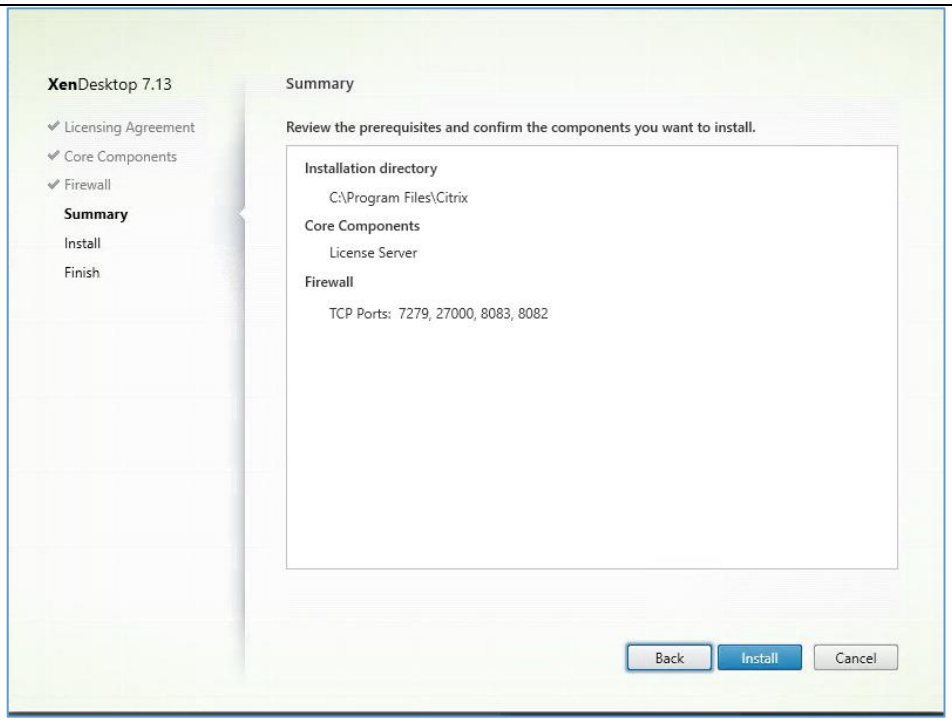
The WW Labs initial Proof of Concept (POC) deployment has limited resources, so you have been tasked to perform this installation on a server that will share several roles throughout this course. Many organizations benefit from separating roles to dedicated servers, but in small deployments, such as a POC, it may be acceptable to combine roles.

Step	Action
1.	The following VMs are required before beginning the exercises for this Module; all others may be powered down. To power manage your VMs, switch to XenCenter, right-click on the VM in the left pane and select Start or Shut Down. If prompted click Yes. • NYC-ADS-001 • NYC-SQL-001 • NYC-FSR-001 • NYC-XDC-001 **Note:** These above VMs are listed in the start-up order.
2.	Using XenCenter, mount the XenApp and XenDesktop installation media ISO to NYC-FSR-001.

	To mount the installation media ISO, select **NYC-FSR-001** in the left pane of XenCenter. In the right pane, select the **Console** tab. Using the **DVD Drive 1:** drop-down menu, select **XenApp_and_XenDesktop_7_13.iso**.  **Note**: If there are no ISOs listed in the DVD Drive 1: drop-down menu, then the Local ISO Storage Repository (SR) that contains the ISO library may need to be re-scanned. To perform the rescan, select **Local ISO SR XS** from the left pane of XenCenter. Then, in the right pane select the Storage tab and click on the **Rescan** button. This task may need to be repeated later in the course.  **Note**: If the above rescan of the **Local ISO SR XS** does not show the specific ISO for installation: XenApp_and_XenDesktop_7_13.iso, then please tell your instructor.
3.	Using the Remote Desktop Connection Manager, connect to NYC-FSR-001. To log on to NYC-FSR-001, right-click this machine and select **Connect server**. **Note**: The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1

4.	Launch the installation for the Citrix License Server. Open the **File Explorer** application from the Windows Taskbar. Click on **This PC** on the left. Double-click the **green Citrix logo** next to CD Drive under Devices and drives.  **Note**: If the main XenApp and XenDesktop menu screen does not launch after double-clicking the green Citrix logo, then double-click the **AutoSelect.exe** file.
5.	On the Deliver applications and desktops to any user, anywhere, on any device screen, click **Start** next to the XenDesktop option.  **Note**: XenApp and XenDesktop share infrastructure components. Choosing to click on the Start option for XenApp will present the same components for install. The difference is in the title at the top of the next screen.
6.	Select **Citrix License Server**.

	 **Note**: The wizard displays all possible installation options that are compatible with the Operating System of the machine that you are on.
7.	Review the Software License Agreement page. If you agree, respond to the Software License Agreement and then click **Next**.
8.	On the Core Components page, leave the default install location and click **Next**. **Note**: You have not been tasked to perform any custom installations in the implementation of this POC.
9.	On the Firewall page, leave the default selection of **Automatically** and click **Next**. **Note**: We are opening the ports required for license communication and these ports should be checked and opened with a network security team. **Review**: The ports for Citrix Licensing are: • 27000: Citrix License Server Manager Port • 7279: Citrix Vendor Daemon Port • 8082: License Administration Console Web Server Port • 8083: Citrix Web Services for Licensing Port
10	On the Summary page, review the summary and click **Install**.

	
11	On the Finish page, click **Finish**.
12	Switch back to XenCenter and eject the XenApp and XenDesktop installation media ISO. To eject the installation media ISO, select **NYC-FSR-001** in the left pane of XenCenter. In the right pane, select the **Console** tab and click **Eject** to remove. **XenApp_and_XenDesktop_7_13.iso** from the DVD Drive 1. **Note**: The Eject option can be difficult to see. It is an underlined word to the right side of the DVD Drive 1 drop-down menu.

Key Takeaways:

- The Citrix License server uses port 27000, 7279, 8082 and 8083.
- Citrix recommends installing the Citrix License Server on a dedicated server, but for smaller deployments such as this POC, shared role servers are sometimes acceptable to help save resource consumption.

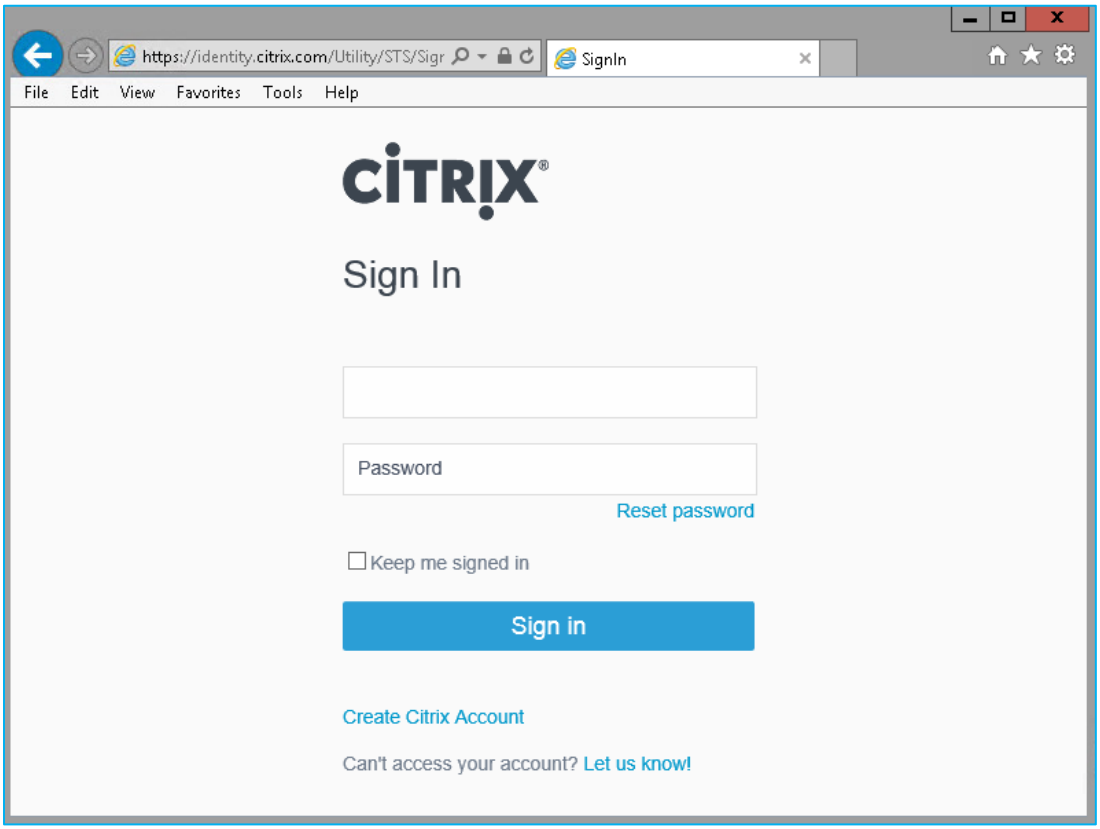
Exercise 3-2: Activate, allocate and download a License File

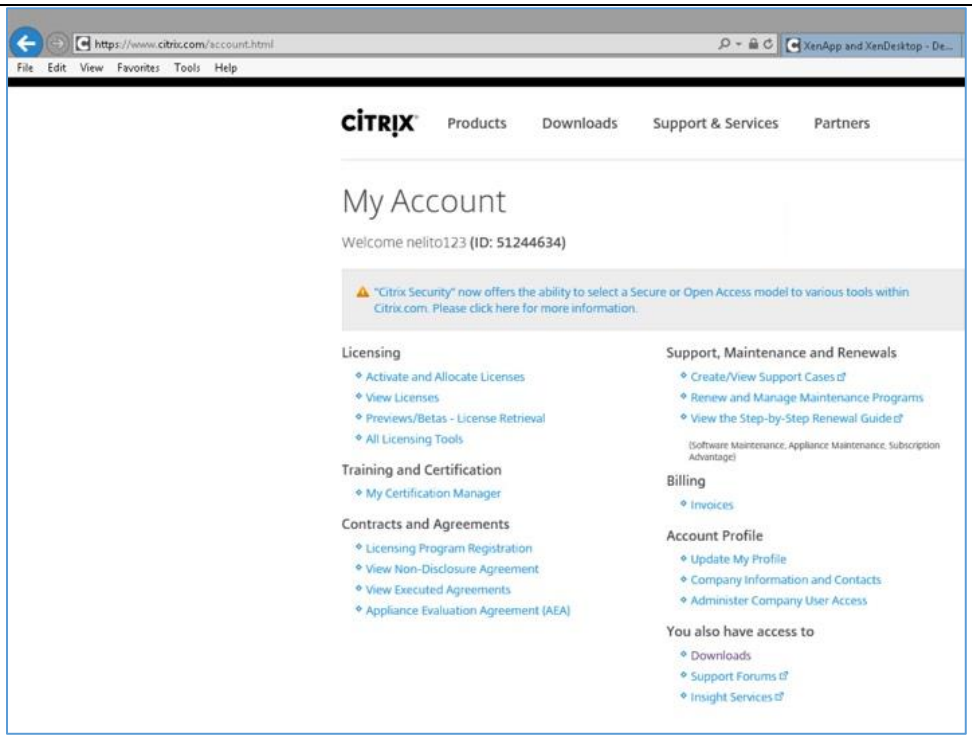
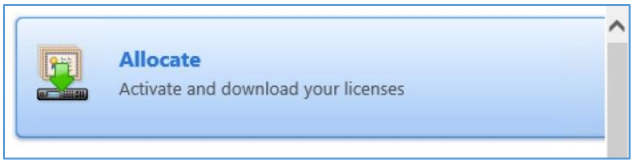
Scenario:

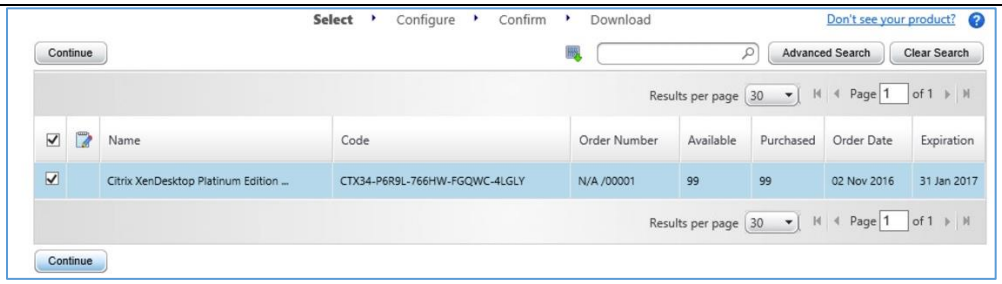
Another Administrator on the Citrix team at WW Labs was tasked to allocate a Platinum edition product license.

This exercise reviews the Citrix License allocation process steps taken by another Administrator on the Citrix team. **This exercise is for review purposes only, none of the below steps will be performed.** As a result of another administrator on your Citrix team, a XenDesktop Platinum Edition license file has already been allocated and downloaded to be used in Exercise 3-3**.**

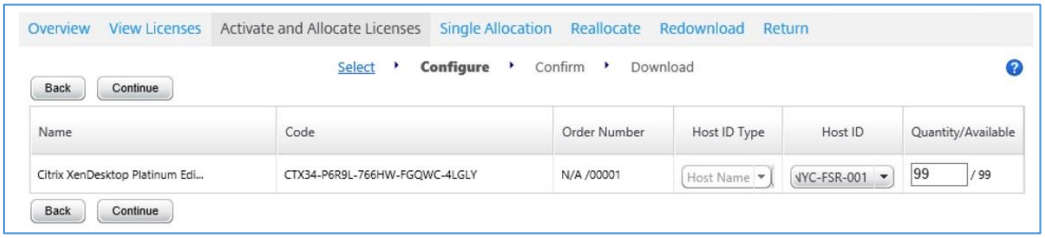
Both methods of license management through the Citrix Licensing Manager and the Citrix License Administration Console are reviewed in this exercise.

Step	Action
1.	Using the Remote Desktop Connection Manager, confirm you are still connected to **NYC-FSR-001**. **Note:** In a previous exercise, you had logged on to **NYC-FSR-001** using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-FSR-001 by right-clicking this machine and selecting Connect server.
2.	The administrator opened an Internet browser window and navigated to the www.citrix.com/myaccount webpage and logged in. 

	
3.	The administrator selected the **All Licensing Tools** option under the **Licensing** section.
4.	The administrator selected **Allocate**. 
5.	The administrator selected the **Citrix XenDesktop Platinum Edition** license that was just allocated and clicked **Continue**.



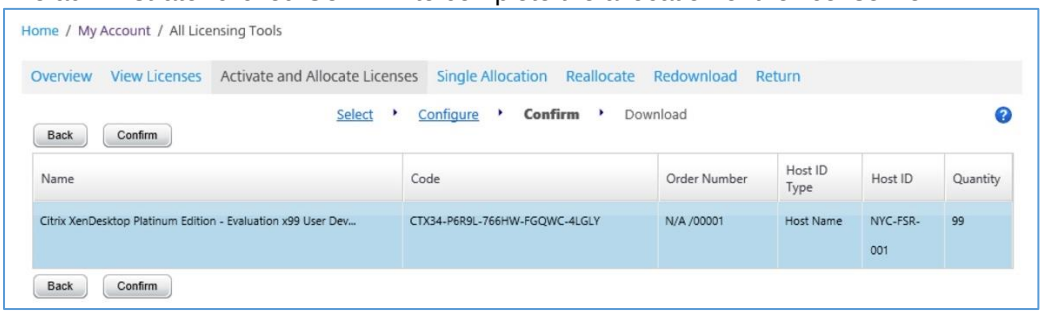
6. The administrator entered the hostname of the Citrix License Server, **NYC-FSR-001**, in the Host field ID and clicked **Continue**.



7. The administrator confirmed the following:

- Name: **Citrix XenDesktop Platinum Edition - Evaluation x99 User Devise - Electronic Software Delivery (90Day)**
- Host ID: **NYC-FSR-001**

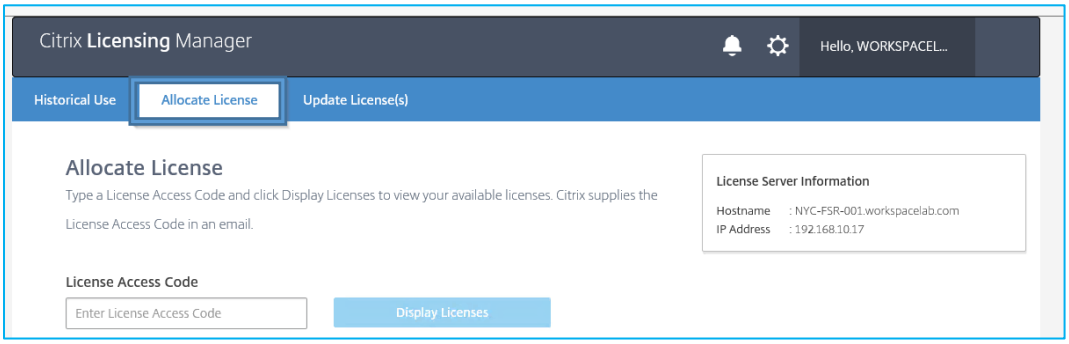
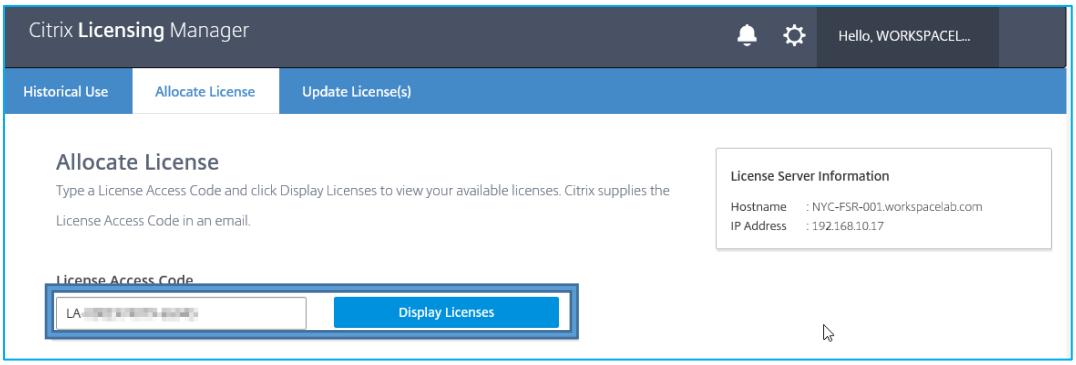
The administrator clicked **Confirm** to complete the allocation of the license file.

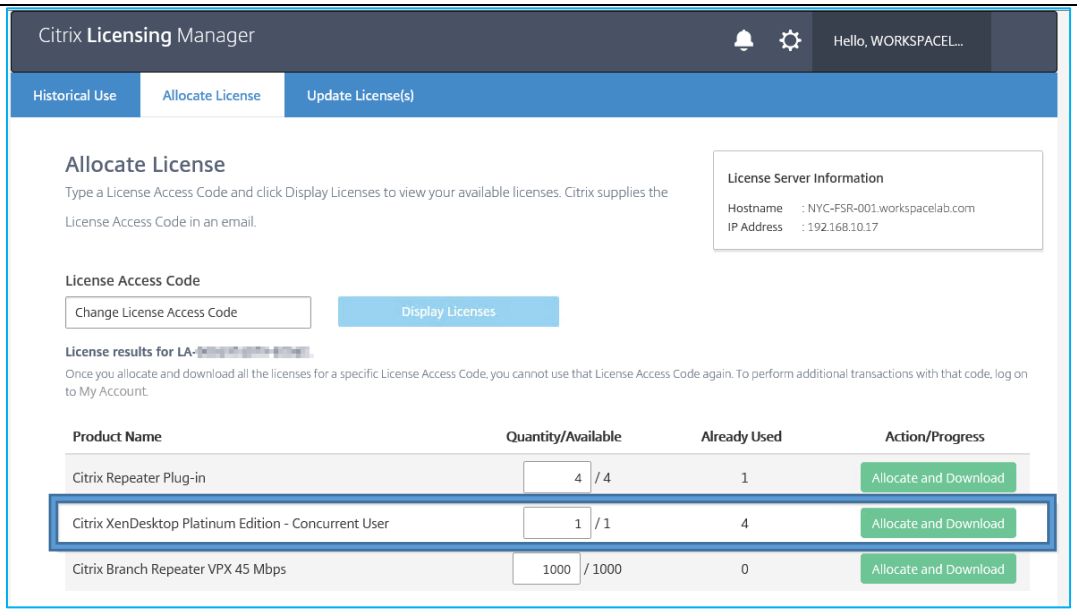


8. The administrator downloaded the license file to the C:\License\ directory on the NYC-FSR-001 server. The license file was renamed, because of WW Labs policy to XenAppAndXenDesktopTraining.lic.

Note: The extension of the license file is ".lic". This file may be renamed to match your company's naming convention as long as you maintain the extension. This file can be opened with a text editor like notepad. One reason for opening the file is to verify the hostname of the Citrix License Server that was specified when downloading the license file. It is located near the top middle with "HOSTNAME=_____."

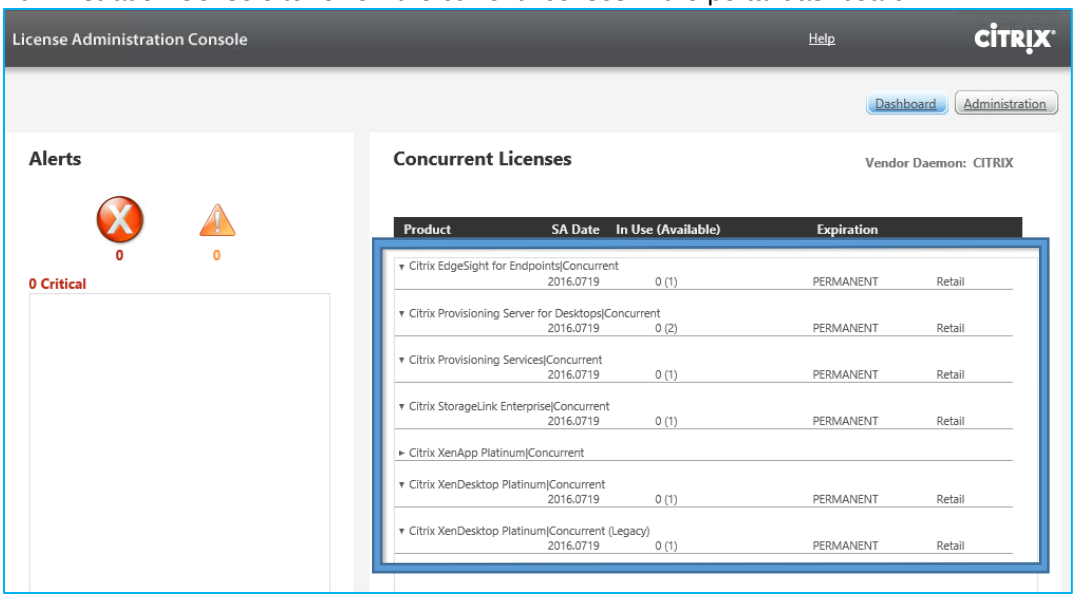
Note: The administrator could have also acquired and configured Citrix licensing by using the Citrix Licensing Manager console. Citrix Licensing Manager enables downloading and allocation of license files from the License Server on which the Citrix Licensing Manager is installed. You can specify a date range for the historical usage and export it to a CSV file. The CSV file provides daily usage information including the number of licenses in overdraft. The Citrix Licensing Manager console is a web portal that is installed, in addition to the Citrix Licensing Administration Console. By using the Citrix Licensing Manager, the administrator is

	not required to download a License file from the Citrix Web Portal. Instead, Citrix Licensing is allocated and downloaded by entering the license code displayed at the license portal, in the Citrix Licensing Manager.
9.	To launch the Citrix Licensing Manager the administrator clicked on **Start** and navigated to Citrix to click on **Citrix Licensing Manager**.
10.	The Citrix Licensing Manager opened in a web browser. The administrator then clicked on the **Allocate License** tab. 
11.	The administrator entered the License Access Code provided by Citrix and then clicked on the **Display Licenses** button. 
12.	The administrator proceeded to obtain the Citrix Licensing file by clicking on the **Allocate and Download** button.



Note: The Citrix Licensing Manager communicates with the Citrix Licensing Cloud portal and downloads and installs the appropriate license on the local server.

13. The administrator can confirm, the license installation, by launching the Citrix License Administration Console to review the current licenses in the portal dashboard.



Key Takeaways:

- For additional information, follow the guidelines at http://support.citrix.com/article/CTX126387.
- When you download a license file, remember that the name of the license server must be specified and that this text entry is case-sensitive.
- The Citrix Licensing Manager console can be used allocate and download Citrix Licenses to the license server, without the need of downloading a license file from the Citrix.Com Manage Licenses page.

Exercise 3-3: Upload a license file to the Citrix License Server

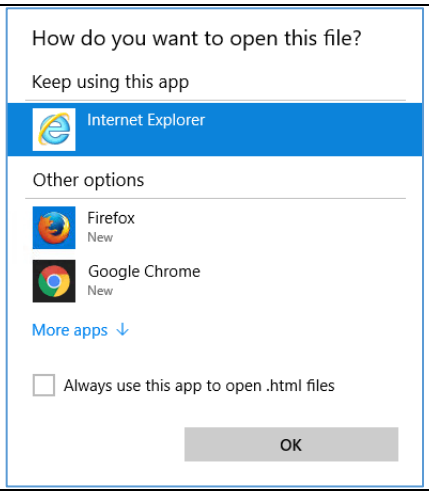
Scenario:

Your next task is to upload the license file, obtained by the Administrator in the previous section, to the Citrix License Server using the Citrix License Administration Console.

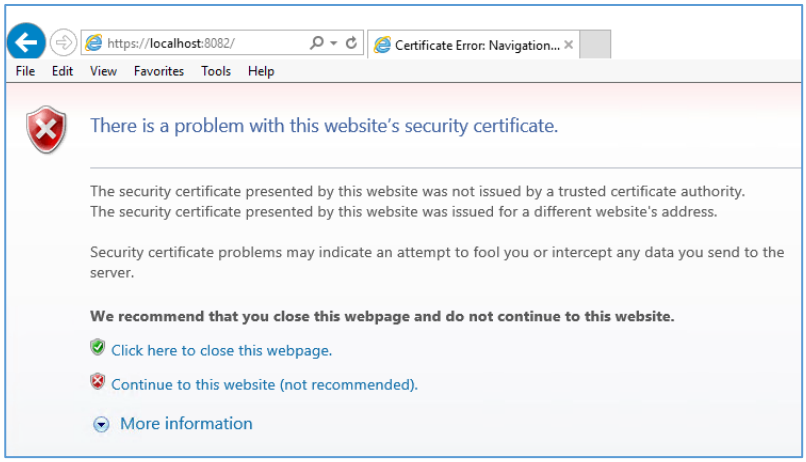
Your Lead Citrix Architect has informed you that as a result of installing the Citrix License Server software, several changes were made to the Windows Server running this software. A new directory to store the license files was created and several Citrix License Services were automatically installed.

You have been assigned an additional task to interact with both the new license storage directory and the Citrix License Services.

Step	Action
1.	Using the Remote Desktop Connection Manager, confirm you are still connected to **NYC-FSR-001**. **Note:** In a previous exercise, you had logged on to **NYC-FSR-001** using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-FSR-001 by right-clicking this machine and selecting Connect server.
2.	Click **Start** and select **Citrix**. From the drop-down, click **Citrix License Administration Console**.
3.	Specify to use the preferred Internet Browser for WW Labs. In the dialog box: *How do you want to open this type of file (.html)?* select **Internet Explorer** and click **OK**.



4. Click **Continue to this website (not recommended)**.

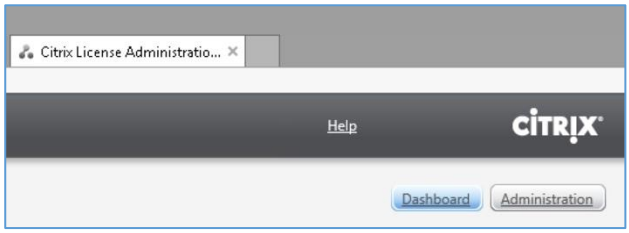


Note: It is a leading practice to consider securing all websites. The License Administration Console is a website. You have been tasked with leaving the default website for this POC build.

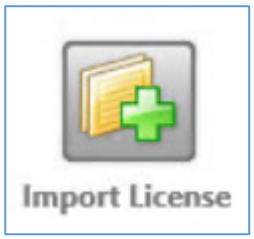
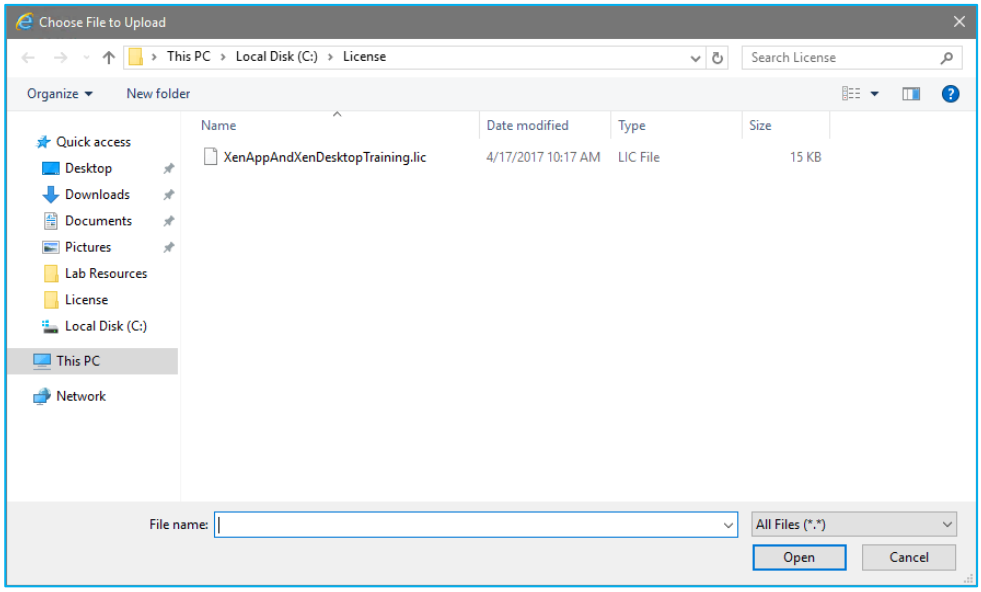
5. Using the **Dashboard** view, confirm that no licenses are currently installed.

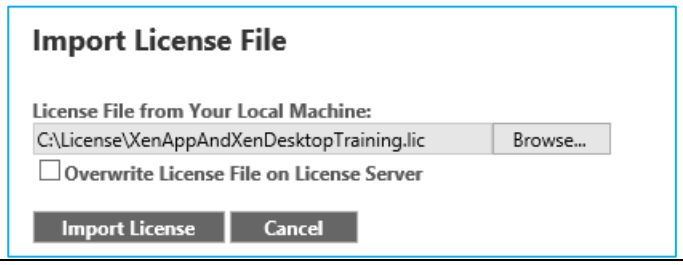
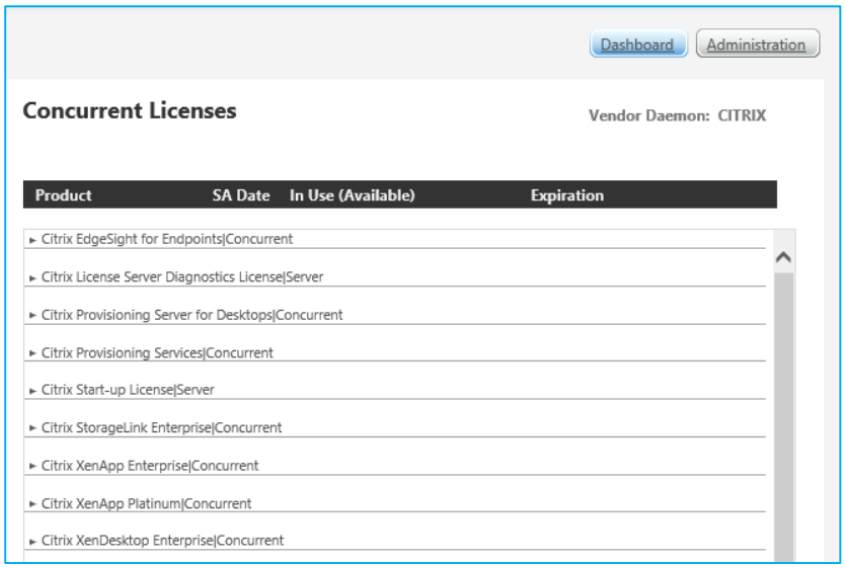
6. Log on to the License Administration Console.

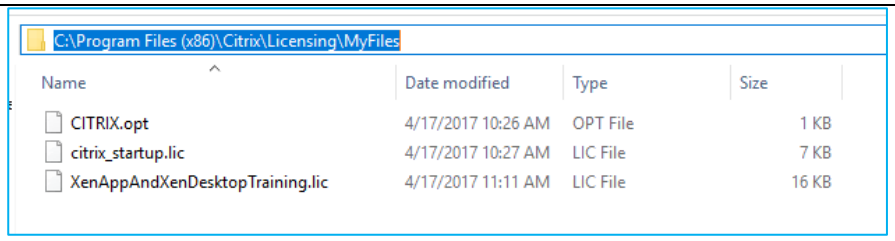
   Click the **Administration** tab in the upper-right corner of the console.



Note: The License Administration Console has two tab, or pages. The Dashboard page is the home page of the License Administration Console. Using Dashboard, you can view license allocation, use, and alerts. To perform configurations, such as delegating administration, you have to launch the Administration page. The Administration page requires permissions. By default, the administrator account used to perform the license server installation has authorization to log on to the administration page.

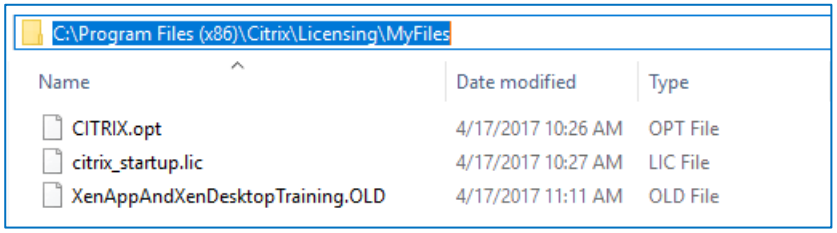
7.	Log on to the License Administration Console with authorized administrator credentials. Use the following credentials: • User name: **Workspacelab\Administrator** • Password: **Password1**
8.	Following WW Labs Leading Practices, do not store your password for this site. On the dialog box at the bottom of the License Administration Console, it asks *Would you like to store your password for localhost*? Click **Not for this site**.
9.	On the left side of the pane, click **Vendor Daemon Configuration**.
10.	On the center pane, click **Import License**. 
11.	Click **Browse**, and navigate to **C:\License**. 
12.	Select the license file **XenAppAndXenDesktopTraining.lic**, and click **Open**.

13.	Click **Import License** to import the license file to the license server. 
14.	On the Important Information screen, click **OK**.
15.	Click **Dashboard** on the upper-right corner and verify that the licenses were added to the license server successfully.  **Note**: If you do not see the Product licenses, go to services console, **restart the Citrix Licensing service**, and then refresh the Citrix License Administration webpage. You may see critical alerts in the license server dashboard. These alerts are related to the short lifespan of the demo licenses and they should not be present in a production environment with valid licenses.
16.	Close the browser running the **License Administration Console**.
17.	Right-click the **Start Menu** on NYC-FSR-001 and select **File Explorer**.
18.	Using File Explorer, navigate to **C:\Program Files (x86)\Citrix\Licensing\MyFiles**.
19.	Verify the license file you have just uploaded **XenAppAndXenDesktopTraining.lic** is there.



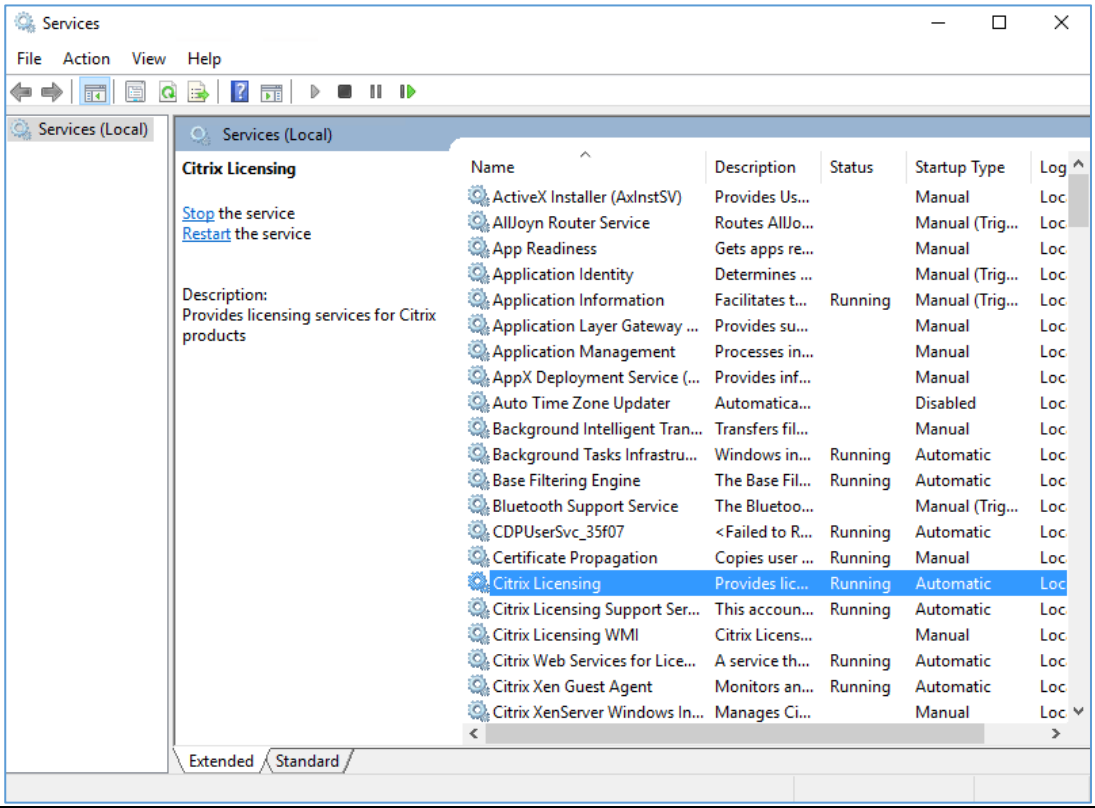
Note: Every download will receive a unique name. The screenshot above is just an example.

20. **Rename** the license file to have the same file name, but use **OLD** as the extension.
    - For Example: **XenAppAndXenDesktopTraining.OLD**

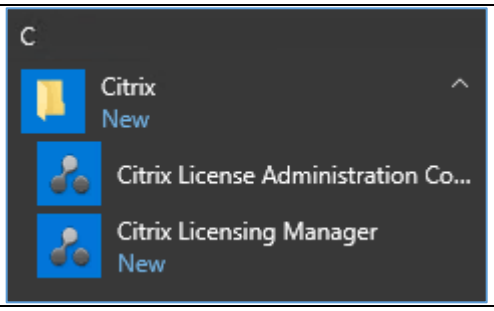
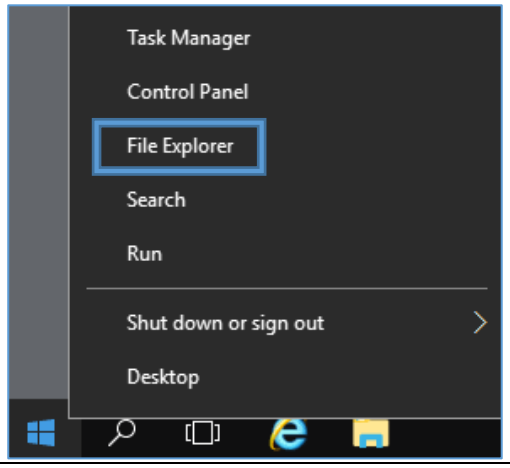
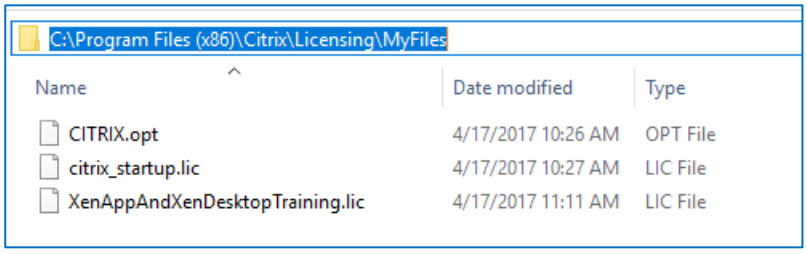


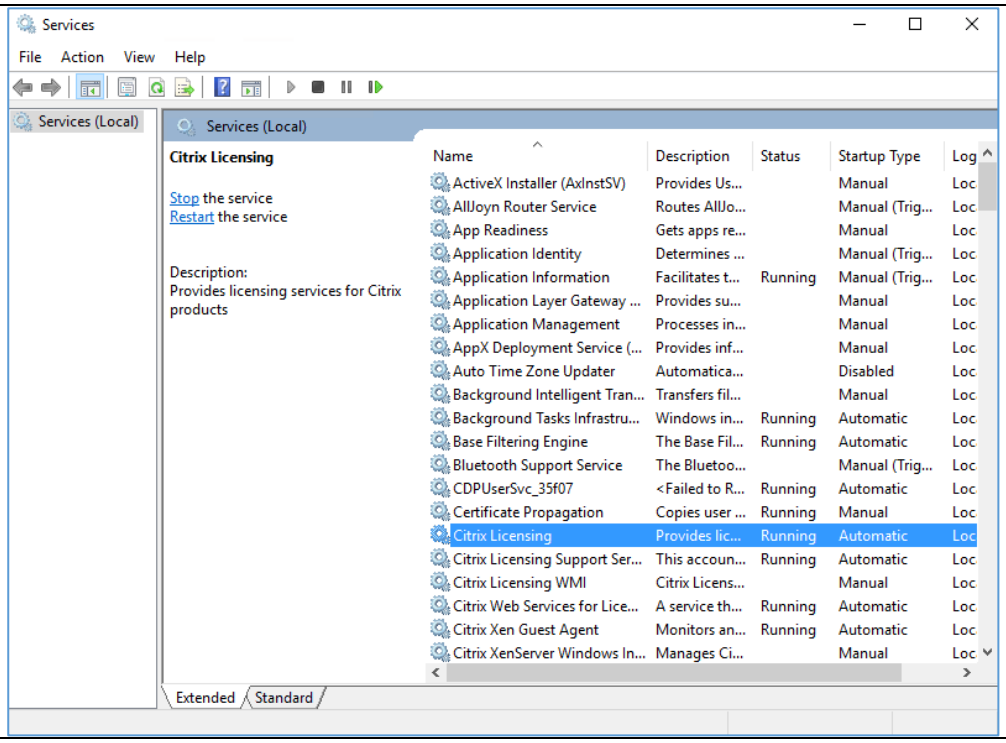
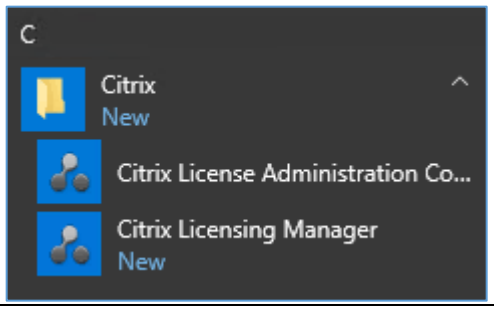
20. Right-click the **Start** menu, click **Run**, and type **Services.msc**.

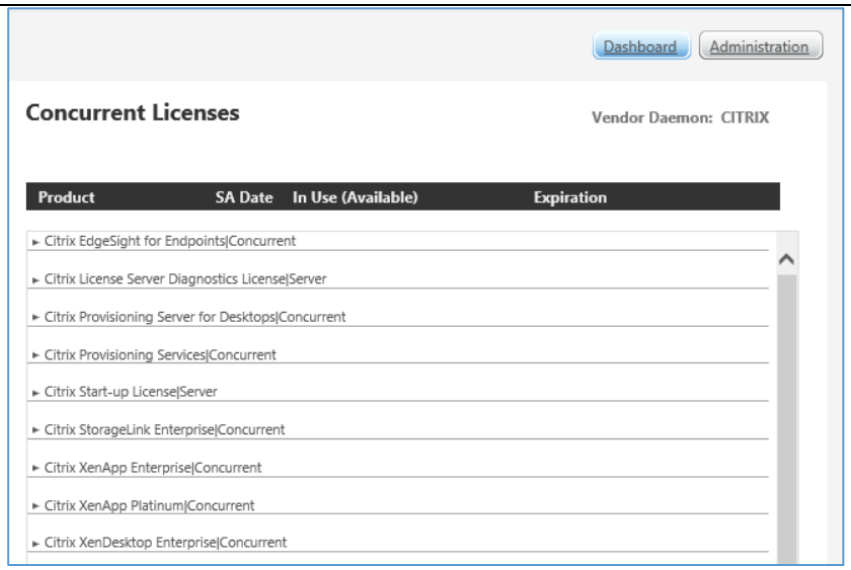
Locate and select the **Citrix Licensing** Service, and click **Restart**.



21. Click **Start** and select **Citrix**. From the drop-down, click **Citrix License Administration Console**.

	
22.	Verify that renaming the license file and restarting the service resulted in the Citrix License Server now being without licenses.
23.	Right-click the **Start Menu** on NYC-FSR-001 and select **File Explorer**. 
24.	Using File Explorer, navigate to **C:\Program Files (x86)\Citrix\Licensing\MyFiles**.
25.	Rename the license file again, this time replace **OLD** with **LIC**. • For Example: **XenAppAndXenDesktopTraining.lic**  **Note**: Every download will receive a unique name. The screenshot above is just an example.
26.	Switch back to the Services console window. Locate and select the **Citrix Licensing** Service, and click **Restart**.

	
27.	Click **Start** and select **Citrix**. From the drop-down, click **Citrix License Administration Console**. 
28.	Verify that all licenses are now back in operational state on the Citrix License Server.

	 **Note**: It is important to understand that the Citrix Licensing Service reads the content of C:\Program Files (x86)\Citrix\Licensing\MyFiles every time it starts and that all the files being read will be shown in the License Administration console.
29.	**Close** any running applications on NYC-FSR-001.

Key Takeaways:

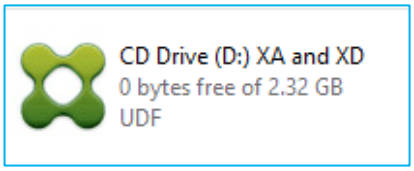
- Licenses are added to a Citrix License Server using the License Administration Console.
- When restarting the Citrix License service, all the ".lic" files from the MyFiles directory are read and applied to the license server.
- The license files can be re-named; however, the files should never be edited. Changing content inside the license file will render it corrupt.

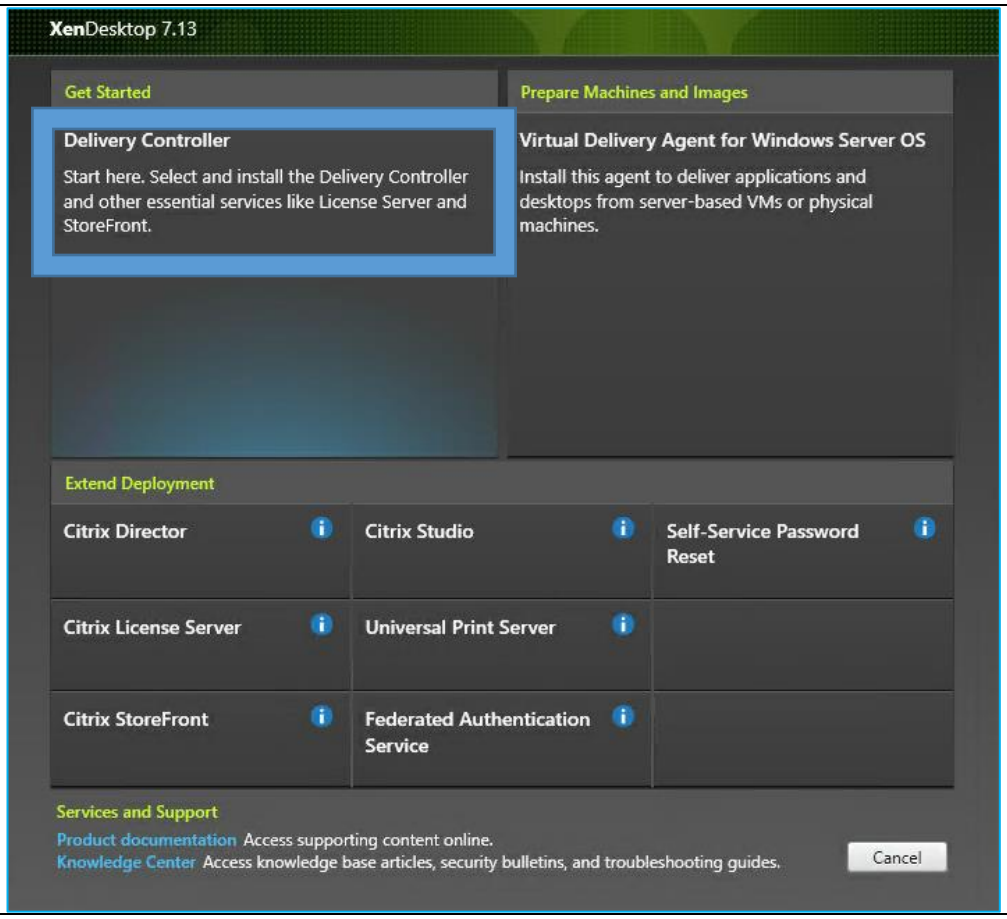
Exercise 3-4: Install the Delivery Controller role

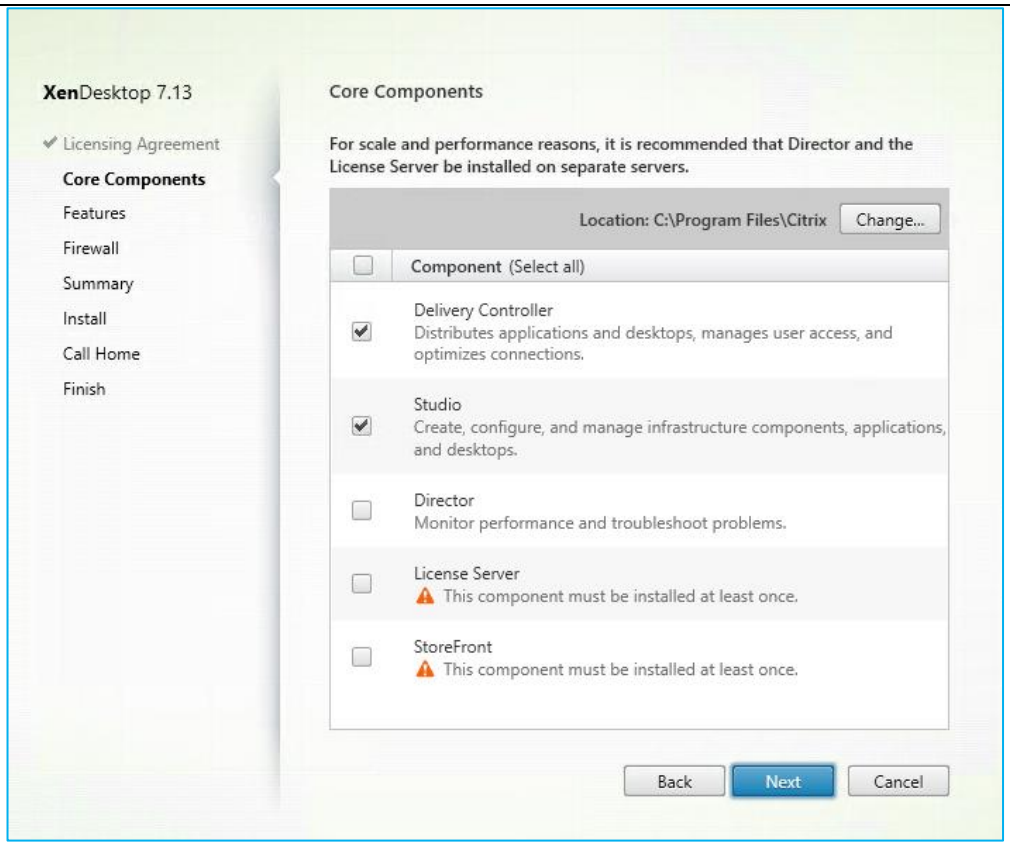
Scenario:

After completing the Citrix License Server configuration, including activating and uploading a license, the next step is to install the XenApp and XenDesktop Delivery Controller Role. Following the WW Labs guidelines, you will install the Delivery Controller on a server running Windows Server 2016.

Step	Action
1.	Using XenCenter mount the XenApp and XenDesktop installation media ISO to NYC-XDC-001. To mount the installation media ISO, select **NYC-XDC-001** in the left pane of XenCenter. In the right pane, select the **Console** tab. Using the **DVD Drive 1:** drop-down menu, select **XenApp_and_XenDesktop_7_13.iso**. **Note**: If there are no ISOs listed in the DVD Drive 1: drop-down menu, then the Local ISO Storage Repository (SR) that contains the ISO library may need to be re-scanned. In the left pane of XenCenter, select the **Local ISO SR XS**. In the right pane select the Storage tab and click on the Rescan button.

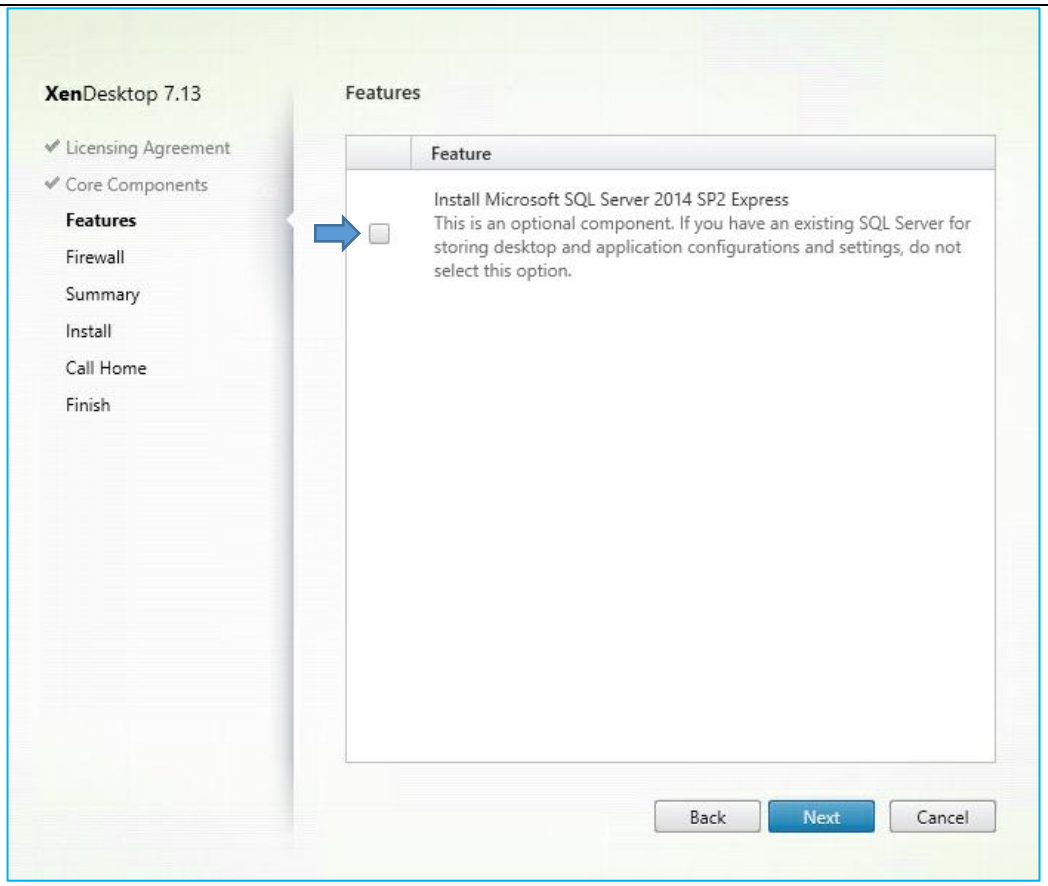
	Note: If the above rescan of the **Local ISO SR XS** does not show the specific ISO for installation, XenApp_and_XenDesktop_7_13.iso, then please tell your instructor.
2.	Using the Remote Desktop Connection Manager, connect to NYC-XDC-001. To log on to NYC-XDC-001, right-click this machine and select **Connect server**. **Note**: The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1
3.	Launch the installation for the Citrix Delivery Controller. Open the **File Explorer** application from the Windows Taskbar. Double-click the **green Citrix logo** next to CD Drive under Devices and drives.  **Note**: If the main XenApp and XenDesktop menu screen does not launch after double-clicking the green Citrix logo, then double-click the **AutoSelect.exe** file.
4.	On the Deliver applications and desktops to any user, anywhere, on any device screen, click **Start** next to the XenDesktop option.
5.	Select **Delivery Controller**.

	
6.	Review the Software License Agreement page. If you agree, respond to the Software License Agreement and then click **Next**.
7.	On the Core Components page, uncheck all options except for **Delivery Controller** and **Studio**, and then click **Next**.



Note: You have selected Delivery Controller because this is the XenApp and XenDesktop core server component. You have selected Studio because this is the primary management console and is used in conjunction with the Delivery Controller to build the XenApp and XenDesktop Site. You are deselecting Director because you will be tasked to deploy Director onto a separate server in a later exercise. You are deselecting License Server because you have already deployed and configured the Citrix License Server. You are deselecting StoreFront because you will be tasked to deploy StoreFront onto a separate server in a later exercise.

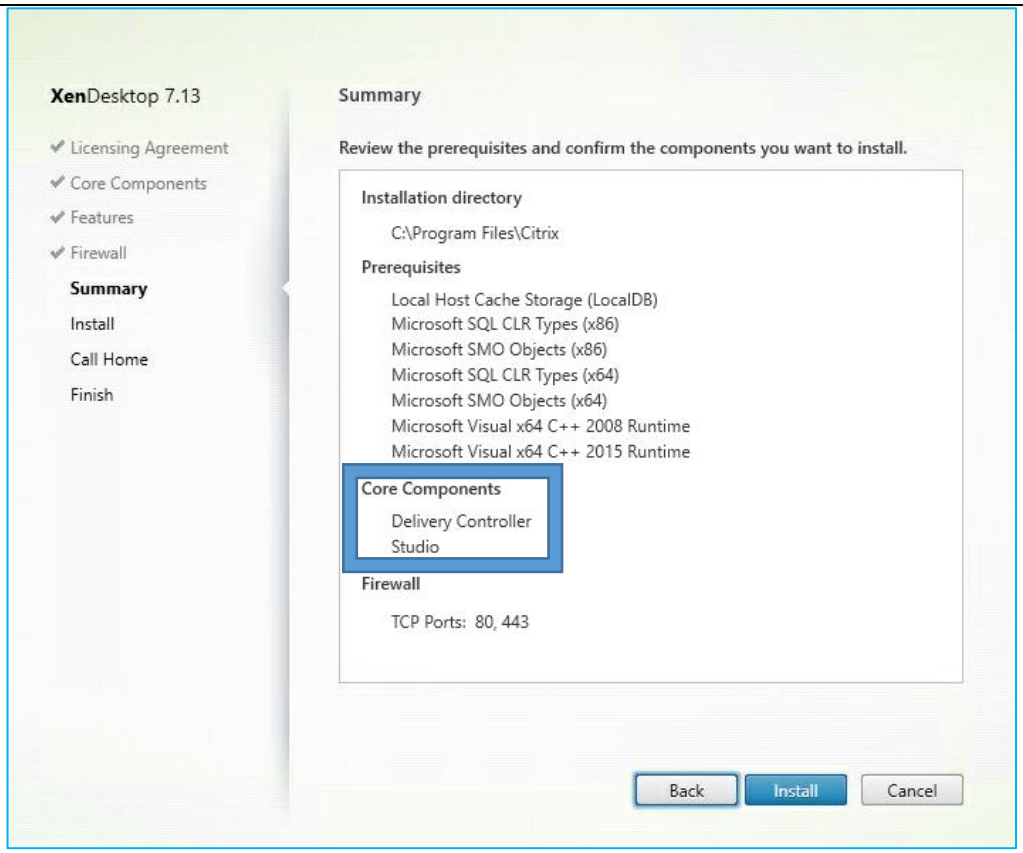
8. On the Features page, uncheck the **Install Microsoft SQL Server 2014 SP2 Express** option and click **Next**.



Note: You have deselected the option to Install Microsoft SQL Server 2014 SP2 Express because although this database type may be acceptable for a POC deployment, you have been notified by the Lead Citrix Architect that WW Labs will use a full SQL server deployment instead.

9. On the Firewall page, leave the default **Automatically** selected and click **Next**.

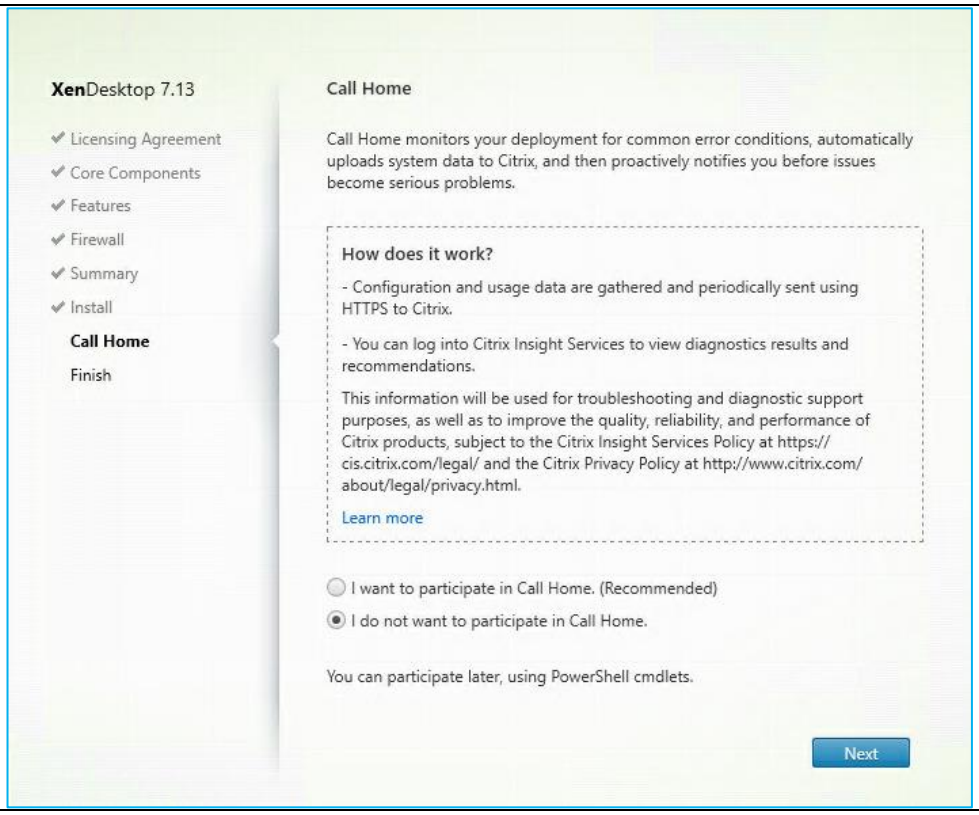
10. On the Summary page, verify that the following selected Core Components are listed:
    - Delivery Controller
    - Studio



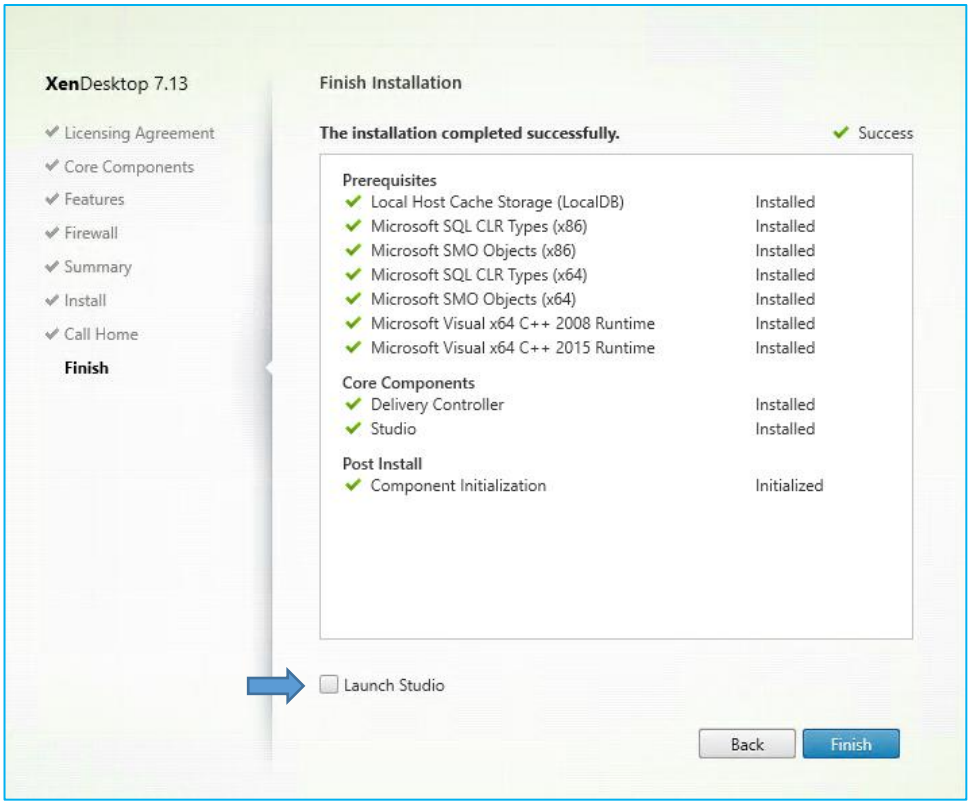
Click **Install**.

Note: The installation will take a few minutes to complete.

11. On Call Home Screen, select **I do not want to participate in Call Home** and click **Next**.



12. When the installation has completed, uncheck the option to **Launch Studio** and click **Finish**.



13.	Using XenCenter eject the XenApp and XenDesktop installation media from NYC-XDC-001. To eject the installation media ISO, select **NYC-XDC-001** in the left pane of XenCenter. In the right pane, select the **Console** tab and click **Eject** to remove XenApp_and_XenDesktop_7_13.iso from the DVD Drive 1. **Note**: The Eject option can be difficult to see. It is an underlined word to the right side of the DVD Drive 1 drop-down menu.

Key Takeaways:

- The installation wizard can rapidly deploy all components required for a small deployment, such as a Proof of Concept, including a database engine; but Citrix recommends keeping the different roles separated in a production environment.
- The installation wizard will install any pre-requisites needed.

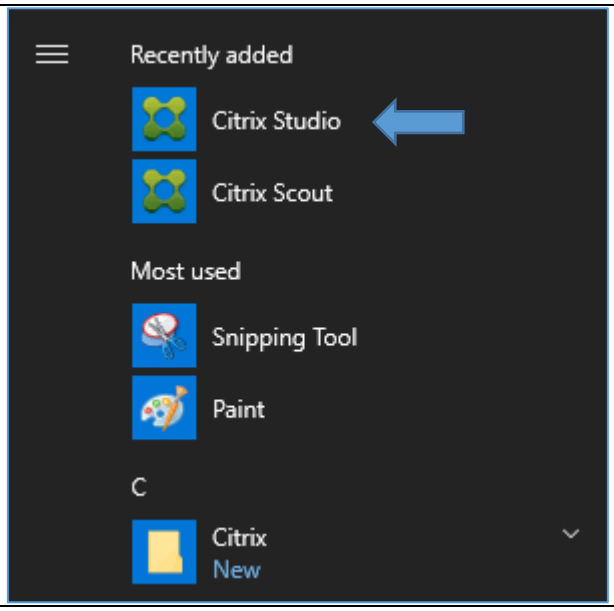
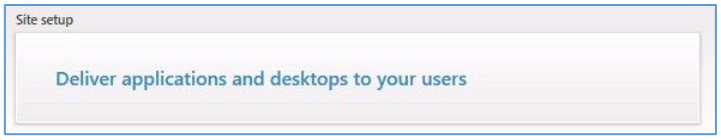
Exercise 3-5: Create and configure a XenApp and XenDesktop Site

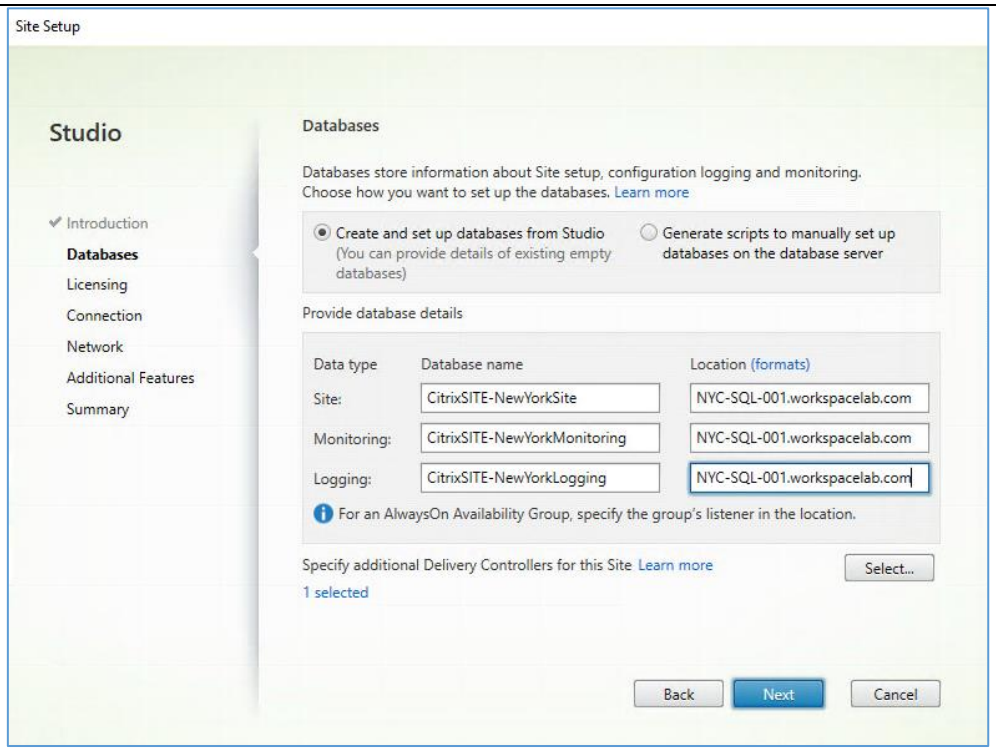
Scenario:

The Delivery Controller has been installed. When you launch the primary XenApp and XenDesktop management console, Citrix Studio, on the new Delivery Controller, an option presents itself to create a new Site.

There are several parameters for creating and configuring a Site, such as defining the database to use and the hypervisor to map. Your task is to navigate the Site creation wizard and supply the parameters necessary to create a Site.

Step	Action
1.	Using the Remote Desktop Connection Manager, connect to NYC-XDC-001. To log on to NYC-XDC-001, right-click this machine and select **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1
2.	Start the Citrix Studio management console. To start Citrix Studio**,** click **Start** and then select **Citrix Studio** under Recently added programs.

	
3.	Use Citrix Studio to create a new XenApp and XenDesktop Site. To start the wizard to create this new Site, click **Deliver applications and desktops to your users** under Site setup.  **Note**: A Site is the name you give to a XenApp and XenDesktop deployment. The Site is comprised of the Delivery Controllers and other core components, such as VDA, Machine Catalogs, Delivery Groups and more, all of which you will deploy and administer in this and further exercises.
4.	On the Introduction page, verify that the default value **A fully configured, production-ready Site (recommended for new users)** is selected under *What kind of site do you want to create?* Enter **SITE-NewYork** in the Site name field. Click **Next** to continue the Site creation wizard.
5.	On the Database page, select **Create and set up databases from Studio**. Under the Provide database details section, leave the default database names for each Database type and enter **NYC-SQL-001.workspacelab.com** under the Location fields. Click **Next**.



Note: In order for Studio to create the Site database on the SQL servers specified, your user account must have the necessary permissions to perform the operations in creating the Site database. These permissions are explicitly configured or acquired by Active Directory group membership. The following is a list of the operations, the purpose of the operations, the Server role and the Database role necessary to continue:

- The database creation operation is used to create a suitable empty database and requires the *dbcreator* Server role.
- The schema creation operation is used to create all service-specific schemas and add the first Controller to the Site and requires both the *securityadmin* Server role and the *db_owner* Database role.
- The add Controller operation adds a Controller (other than the first one) to the Site and requires both the *securityadmin* Server role and the *db_owner* Database role.
- The Add Controller (if mirror server) operation adds a Controller login to the database server currently in the mirror role of a mirrored database and requires the *securityadmin* Server role.
- The schema update operation applies schema updates or hotfixes and requires the *db_owner* Database role.

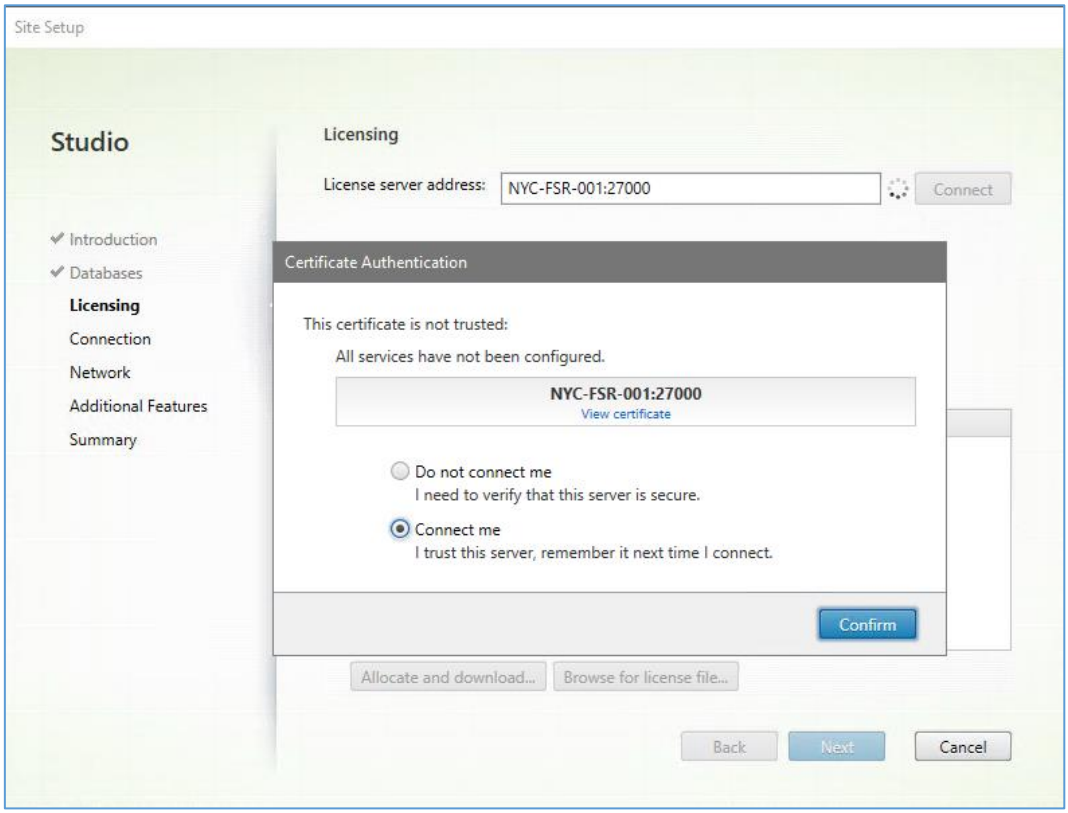
Note: You have been granted the necessary permissions to allow Studio to create the Site database.

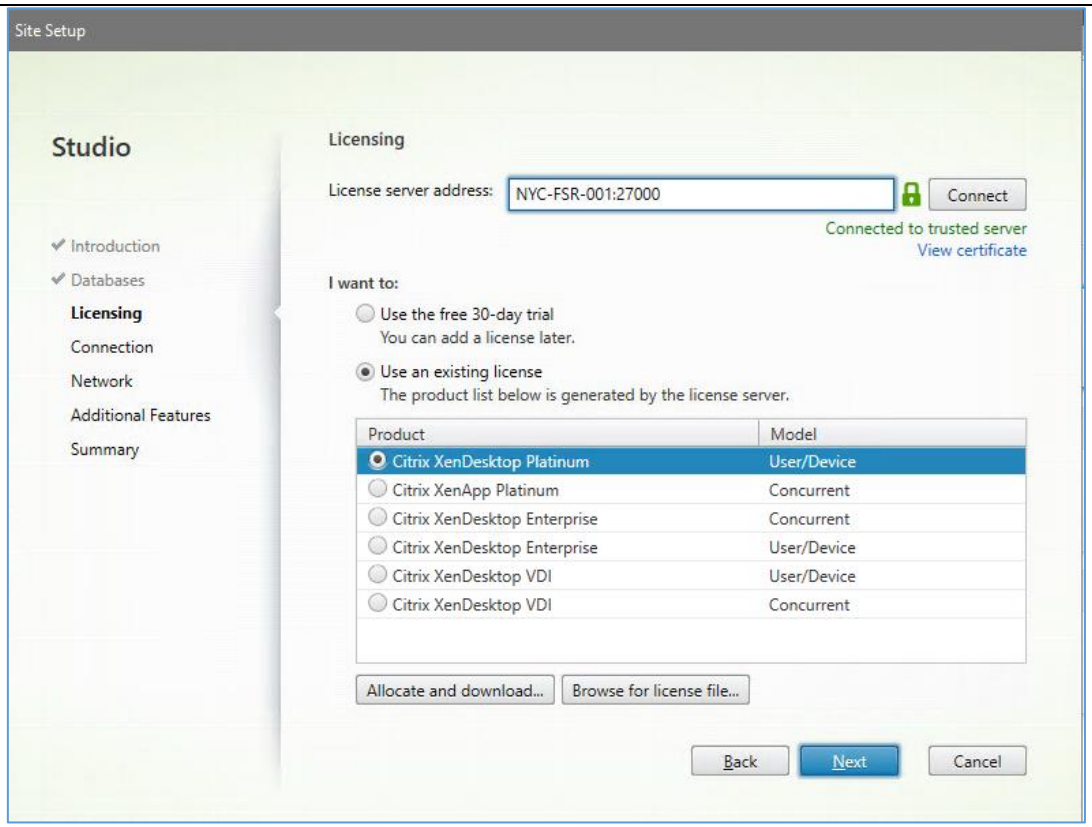
6. On the Licensing page, enter the hostname and network port of the Citrix License Server you deployed in an earlier exercise.

   Enter **NYC-FSR-001:27000** for the License server address and click the **Connect** button.

   Note: Make sure no extra spaces are present after NYC-FSR-001:27000.

   Note: If the license uploaded to the License Server in Exercise 3-3 does not appear to be valid, then replace NYC-FSR-001:27000 with Licenses.citrixvirtualclassroom.com.

	On the Certificate Authentication dialog box, click the **Connect me** radio button and click **Confirm**.  Under Product, select the **Citrix XenDesktop Platinum** radio button and click **Next**.



Note: Remember that when this project began, the Citrix Lead Architect purchased XenDesktop Platinum. This license edition includes all XenApp and XenDesktop features.

7. On the Connection page, enter your XenServer hypervisor connection resource details.

To locate your XenServer connection resource details, minimize the **lab environment**, return to **Training.Citrix.Com (TCC)**, and click on the **Launch** button for the labs, which launches a small window with some connection details.

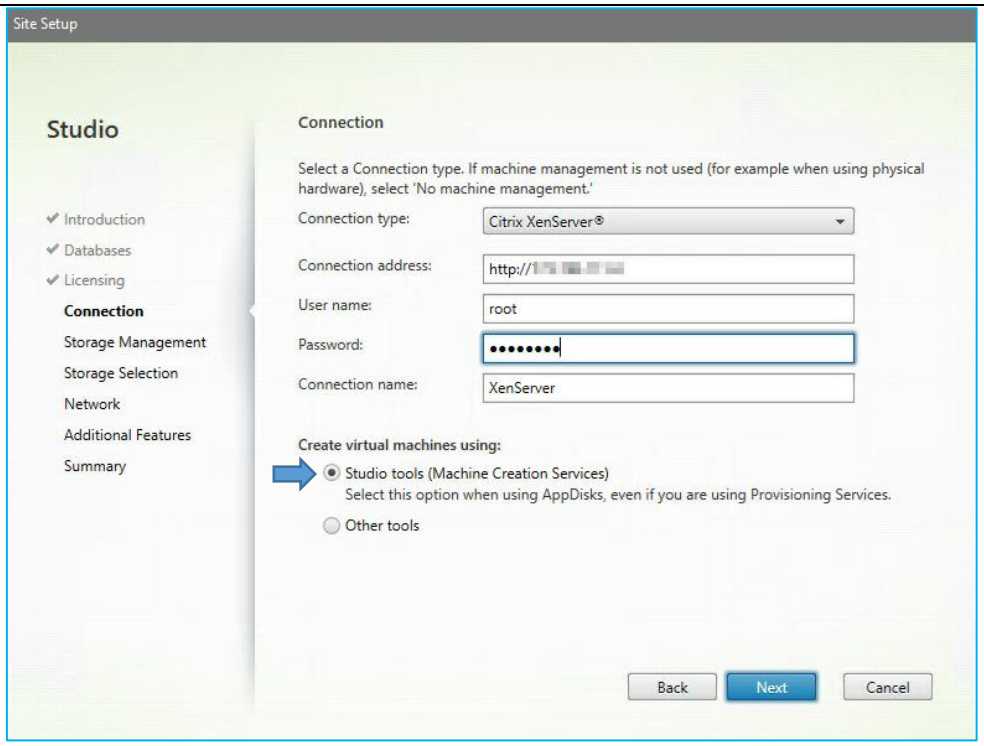
Note: You may have to log back in with the MyCitrix credentials used to register for this course.

Take note of the XenServer hypervisor connection details and enter this information to create a Resource Connection for the XenApp and XenDesktop Site.

- Connection type: **Citrix XenServer**
- Connection address: **http://<XenServer IP Address>**
- User name: **root**
- Password: **<XenServer credentials password>**
- Connection name: **XenServer**

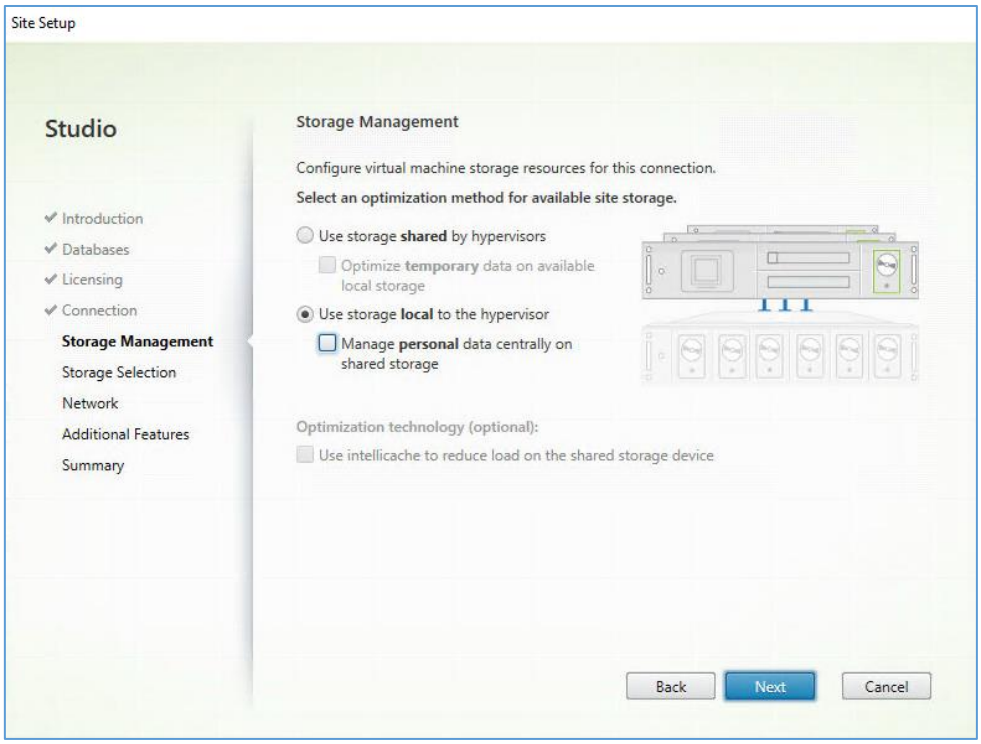
Verify that for the Create virtual machines using option, **Studio tools (Machine Creation Services)** is selected.

Click **Next** to continue the Site creation wizard.

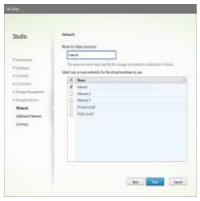
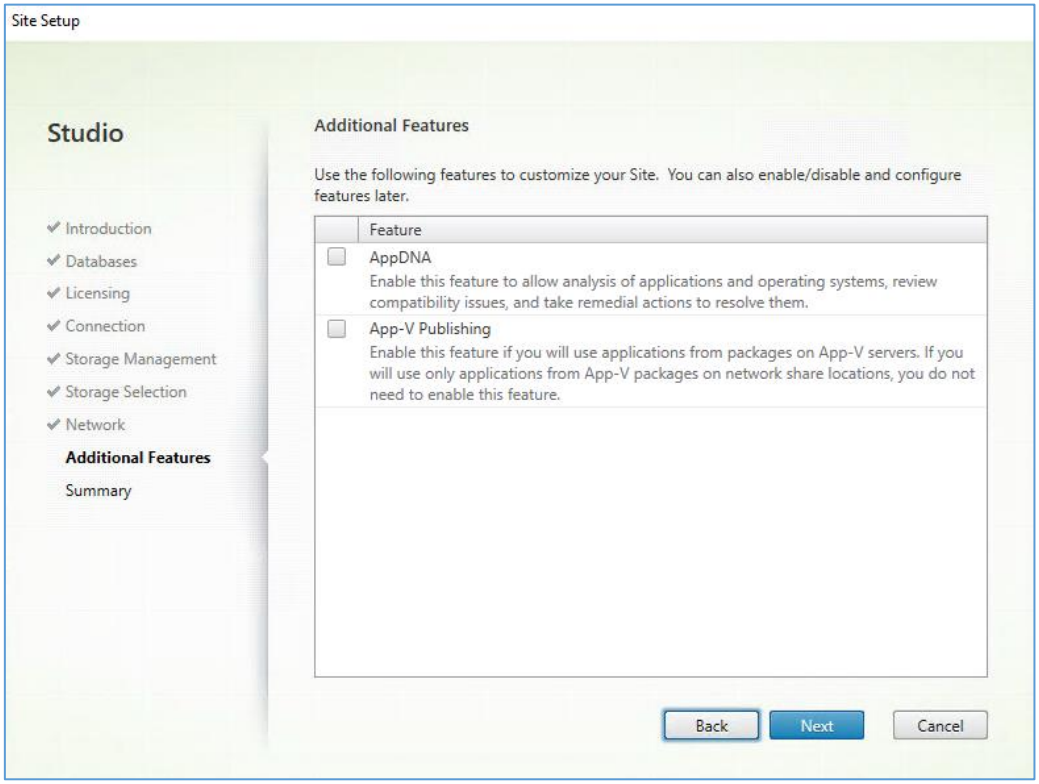


Note: XenApp and XenDesktop equally supports all three industry standard hypervisors agnostically. The Site wizard can connect its Resource Connection settings to Citrix XenServer, Microsoft Hyper-V, or VMware vSphere.

8. On the Storage Management page, select **Use storage local to the hypervisor** and click **Next**.



Note: Since this a lab environment, local storage will be used.

9.	On the Storage Selection page, leave the default selections and click **Next**. **Note**: For this deployment, your XenServer local storage is adequate. You have met with the Lead Citrix Architect and agree that in the WW Labs production deployment, you will need to consider a fast and redundant storage solution.
10.	On the Network page, specify the name and the network that the future Machine Catalog machines will use. In the Name for these resources field, type **Internal**. Select the **Internal** checkbox under the Select one or more networks for the virtual machines to use section and click **Next**.  **Note**: You have been tasked to use this specific network for the Machine Catalog machines. You will be creating and working with Machine Catalog machines in later exercises.
11.	On the Additional features page, verify that AppDNA and App-V Publishing are unchecked and click **Next**.  **Note**: Although AppDNA and App-V are both fully supported, integration with these features is not in the scope that your Lead Citrix Architect has designed.
12.	On the Summary page, verify that the configuration information is correct. Click **Finish**. Wait for the site setup to complete.

Key Takeaways:

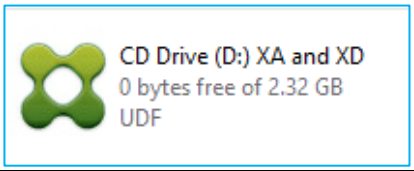
- If you have sysadmin permissions to SQL, let Citrix Studio create the databases automatically. The install used the default Administrator account that, by default, has the required permissions to create the database.
- Pointing to the Citrix License server will enumerate all licenses installed on that server.
- The configuration wizard can deploy a fully functional site with an easy-to-follow wizard.
- Additional configurations and connections can be added later using Citrix Studio.

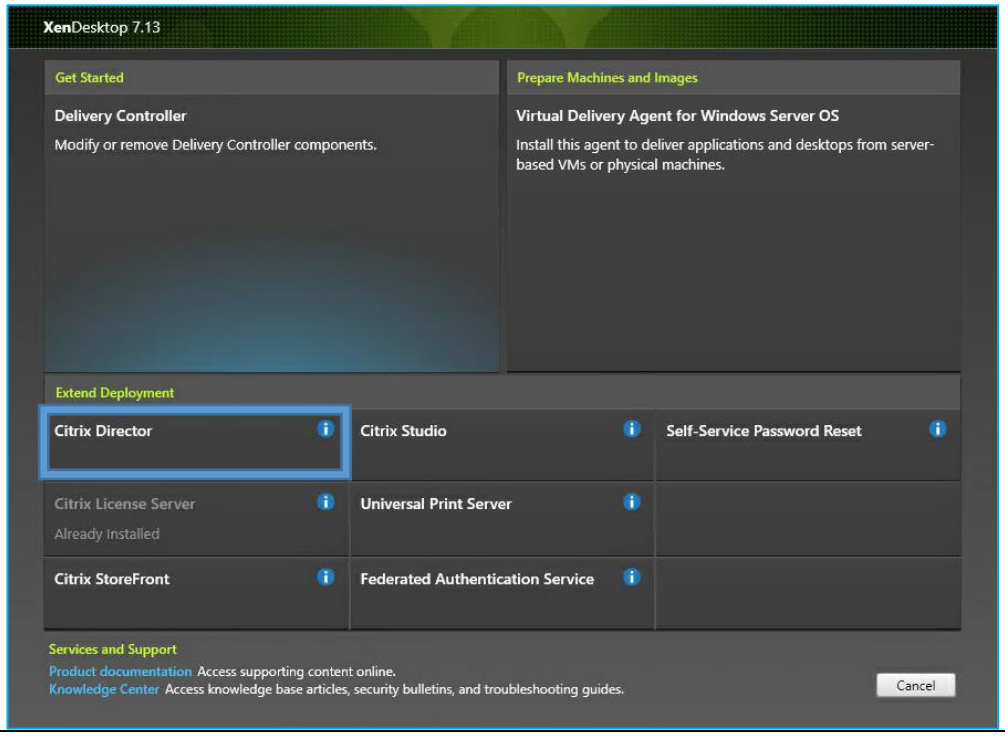
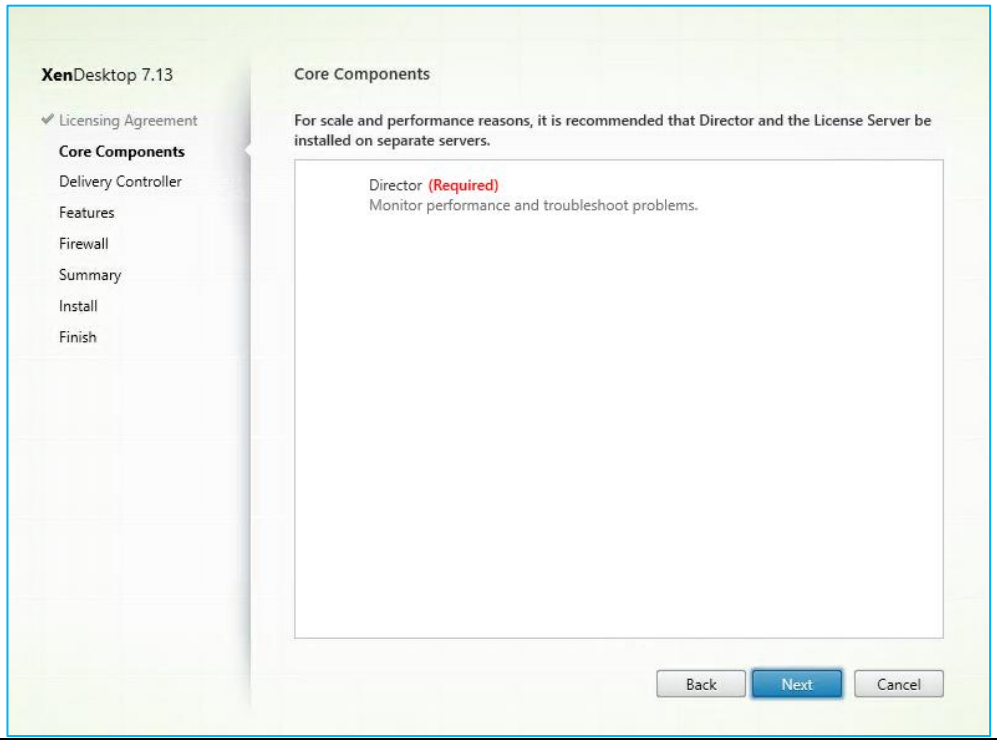
Exercise 3-6: Install Citrix Director

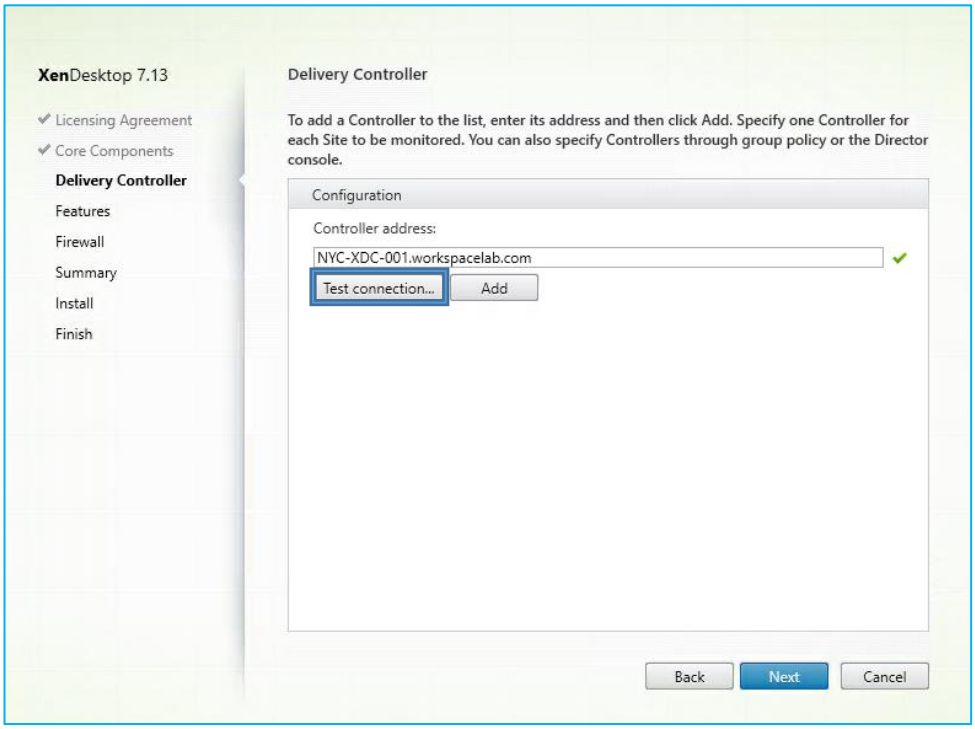
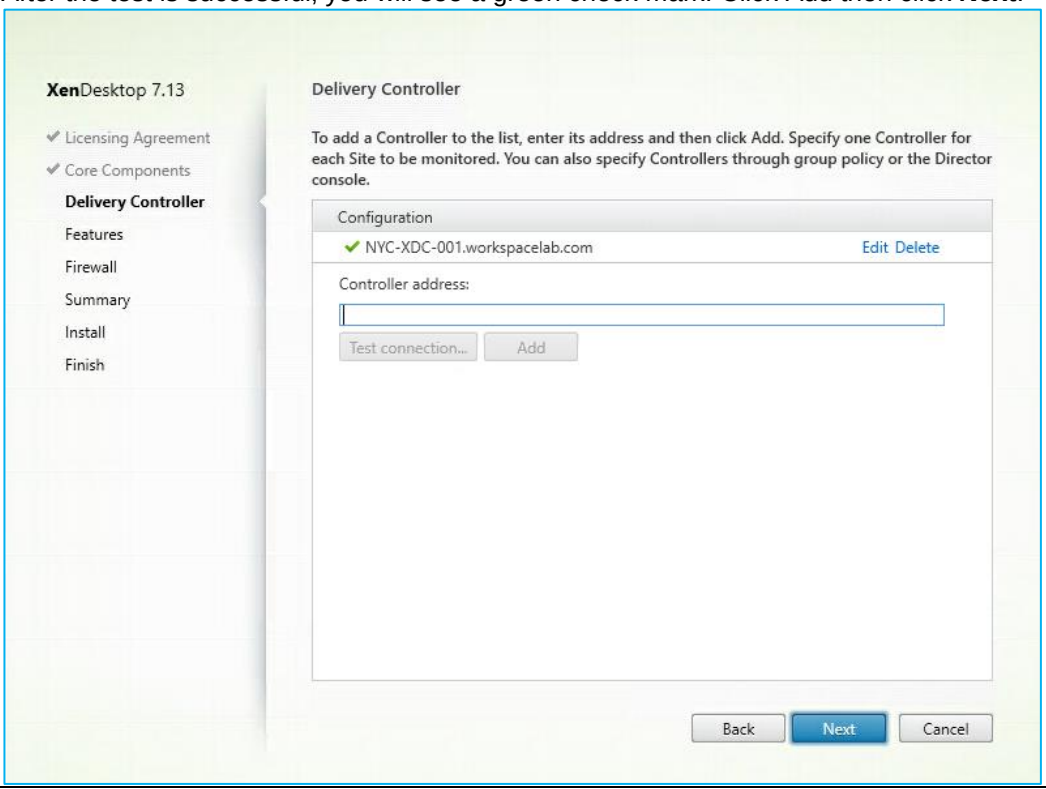
Scenario:

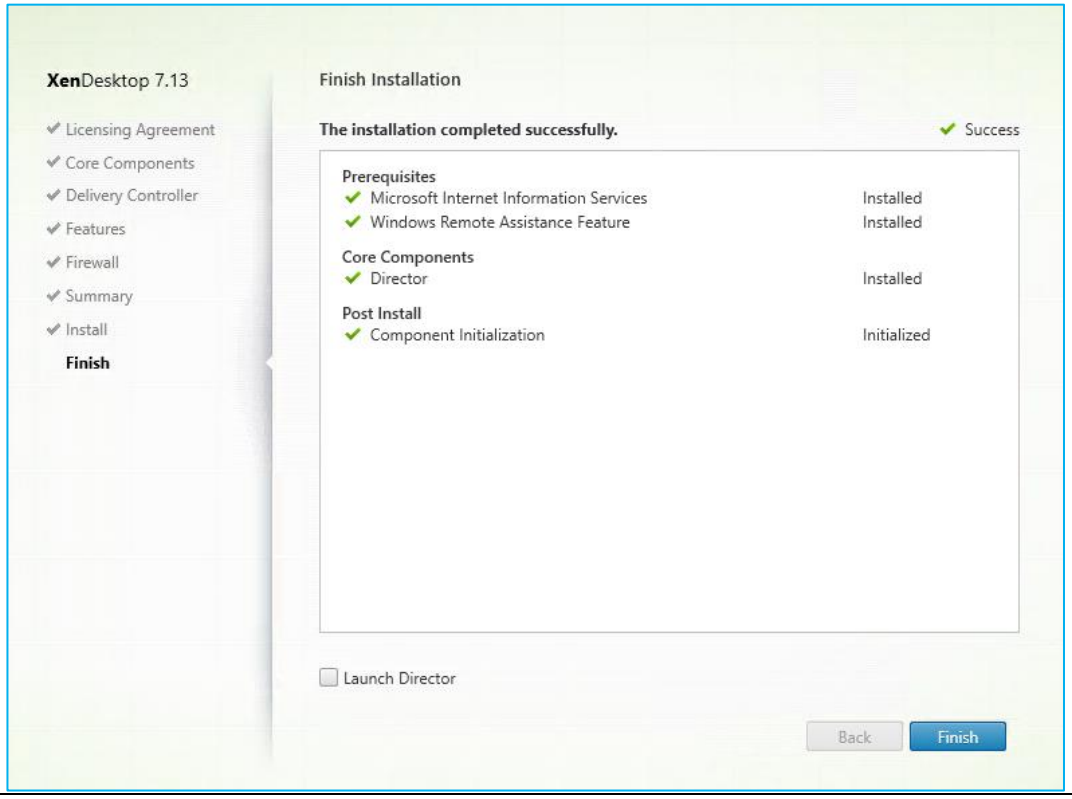
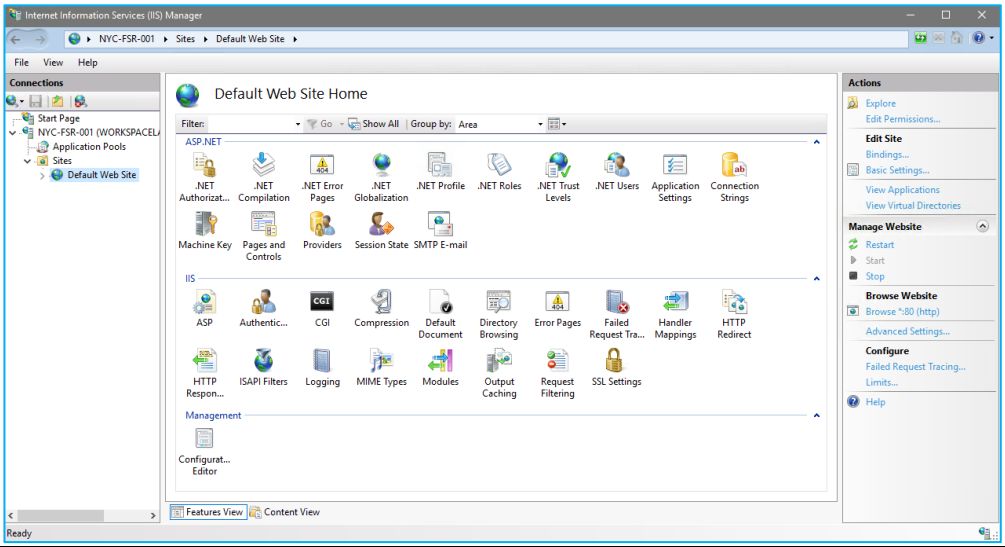
Your Citrix Lead Architect has informed you that the Citrix Director monitoring component should be installed next so that data can be collected during the rest of the POC build. In accordance with Citrix leading practices, Citrix Director should not be installed onto the Delivery Controller. In evaluating the environment, you choose to install Director onto the NYC-FSR-001 machine as this is already being used as a shared role server.

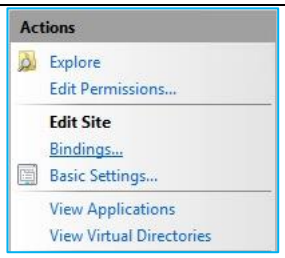
Your task is to install Citrix Director. In Module 13, Director will be used to monitor the Site.

Step	Action
1.	Using **XenCenter** mount the XenApp and XenDesktop installation media ISO to **NYC-FSR-001**. To mount the installation media ISO, select **NYC-FSR-001** in the left pane of the XenCenter. In the right pane, select the **Console** tab. Using the **DVD Drive 1:** drop-down menu select **XenApp_and_XenDesktop_7_13.iso**. **Note**: If there are no ISOs listed in the **DVD Drive 1:** drop-down menu, then the Local ISO Storage Repository (SR) that contains the ISO library may need to be re-scanned. In the left pane of **XenCenter** select the **Local ISO SR XS**. In the right pane select the **Storage** tab and click on the **Rescan** button. This task may need to be repeated later in the course. **Note:** If the above rescan of the **Local ISO SR XS** does not show the specific ISO for installation: XenApp_and_XenDesktop_7_13.iso, then please tell your instructor.
2.	Using the Remote Desktop Connection Manager, connect to **NYC-FSR-001**. To log on to NYC-FSR-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password.
3.	Launch **File Explorer** from the Windows Taskbar or Start Menu. Double-click the green Citrix logo next to **CD drive** under Devices and Drives, and double-click on **AutoSelect.exe**. 

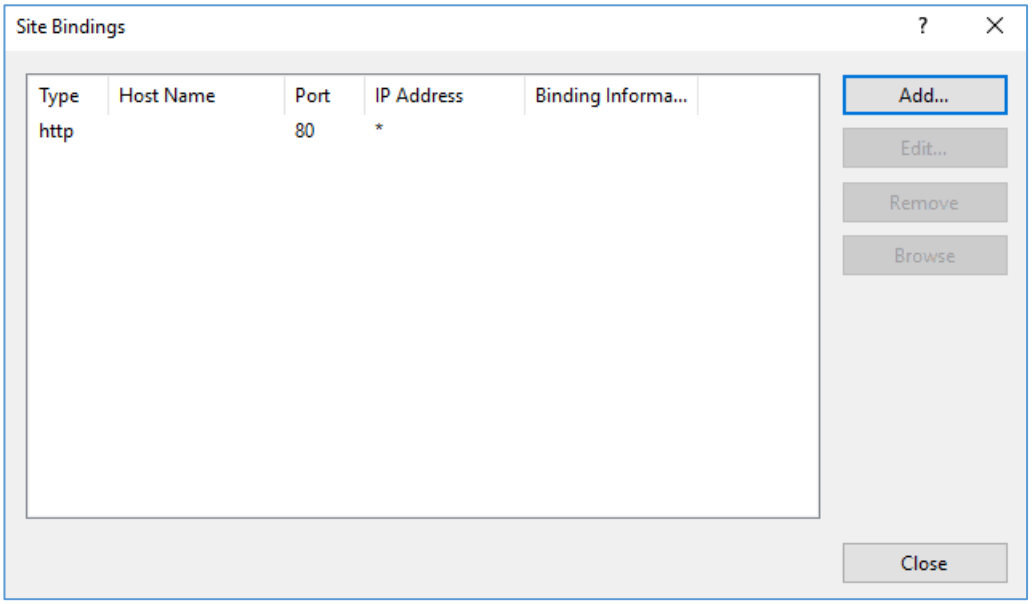
4.	The wizard will now display all possible installation options that are compatible with the Operating System of the machine that you are on. Select **Citrix Director**. 
5.	Review the Software License Agreement page. If you agree, respond to the Software License Agreement and then click **Next**.
6.	On the Core Components page, leave the default and click **Next**. 

7.	On the Delivery Controller page, type **NYC-XDC-001.workspacelab.com** and click **Test connection**.  After the test is successful, you will see a green check mark. Click Add then click **Next**. 
8.	On the Features page, leave the default and click **Next**.
9.	On the Firewall page, leave the default **Automatically**, and click **Next**.

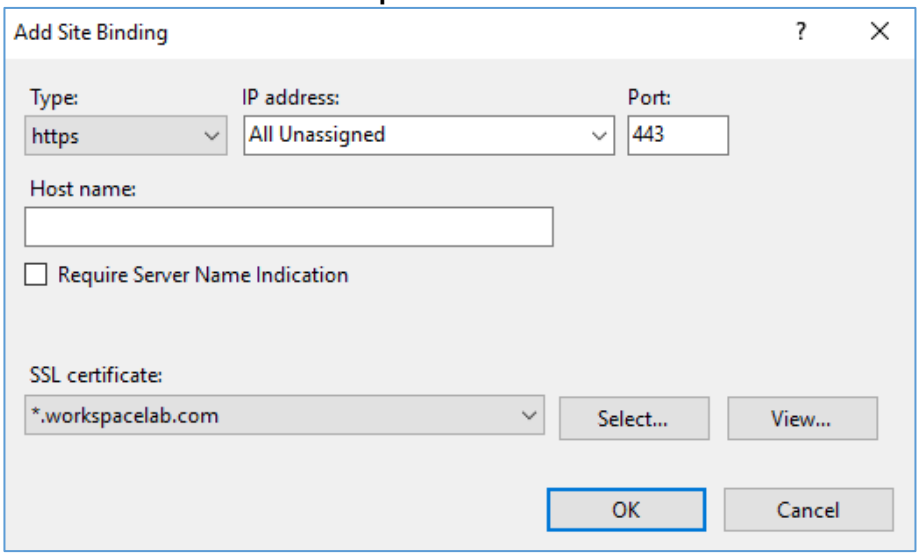
10.	On the Summary page, review the summary and click **Install**.
11.	Once the installation completes, uncheck the option to **Launch Director** and click **Finish**. 
12.	Click **Start > Windows Administrative Tools > Internet Information Services**.
13.	In IIS Manager, expand **NYC-FSR-001 (WORKSPACELAB\Administrator) > Sites** and click **Default Web Site**. 
14.	On the right pane under Actions, click **Bindings**.



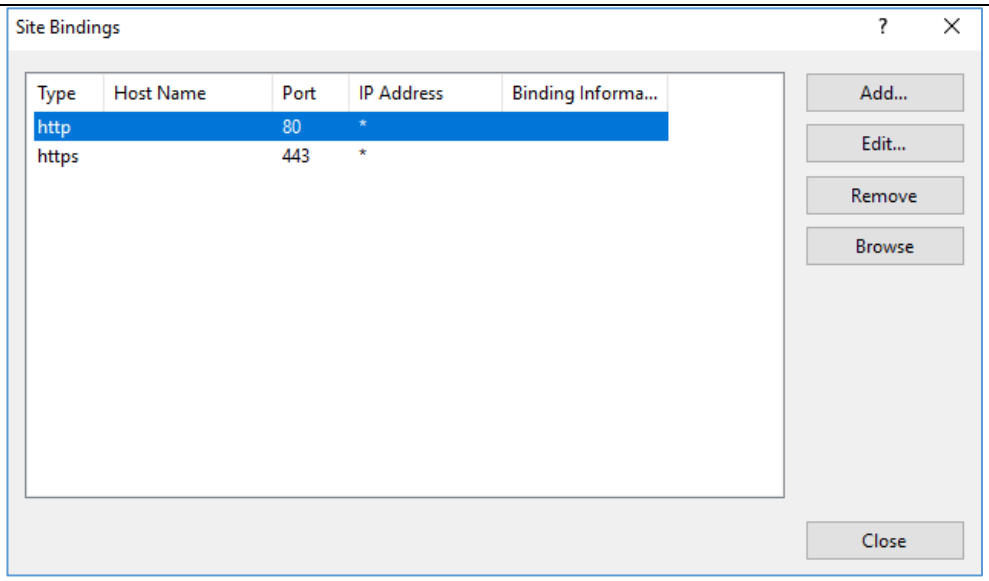
On the Site Bindings dialog box, click **Add**.



15. Set the Binding settings to the following:
    - Type: **https**
    - SSL certificate: ***.workspacelab.com**

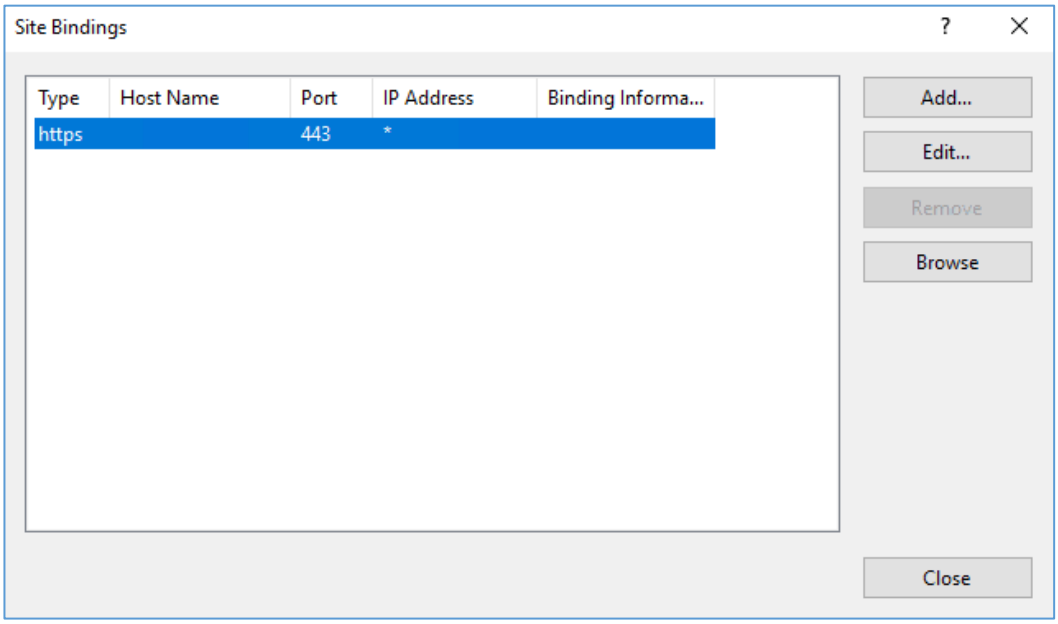


16. Click **OK** to close the Bindings dialog box.
17. In the Site Bindings dialog box, select the **http** binding and click **Remove**.



Click **Yes** to accept.

Click **Close** on the Site Bindings window.



Note: Another administrator has already installed a wildcard security certificate on NYC-FSR-001. Binding the Certificate secures the Director website.

18. Close the **Internet Information Services (IIS) Manager** Console.

19. Using **XenCenter,** eject the XenApp and XenDesktop installation media from **NYC-FSR-001**.

    To eject the installation media ISO, select **NYC-FSR-001** in the left pane of XenCenter. In the right pane, select the **Console** tab and click **Eject** to remove **XenApp_and_XenDesktop_7_13.iso** from the **DVD Drive 1**.

    Note: The Eject option can be difficult to see. It is an underlined word to the right side of the DVD Drive 1 drop-down menu.

Key Takeaways:

- When installing Citrix Director using the ISO file, all pre-requisites are installed during the installation.

Module 4: Provision and deliver application and desktop resources

Overview:

This module presents the Virtual Delivery Agent (VDA), its installation, and its role in the delivery of resources to users. Directly following the preparation and installation of the VDA, you will create Catalogs and Delivery Groups to complete the resource delivery to the users.

Although not all of the Machine Catalog machines are virtual, most are and this course focuses on the Citrix Machine Creation Services feature and its role in the creation of virtual machines.

Before you begin:

Estimated time to complete Module 4 lab exercises: 115 minutes

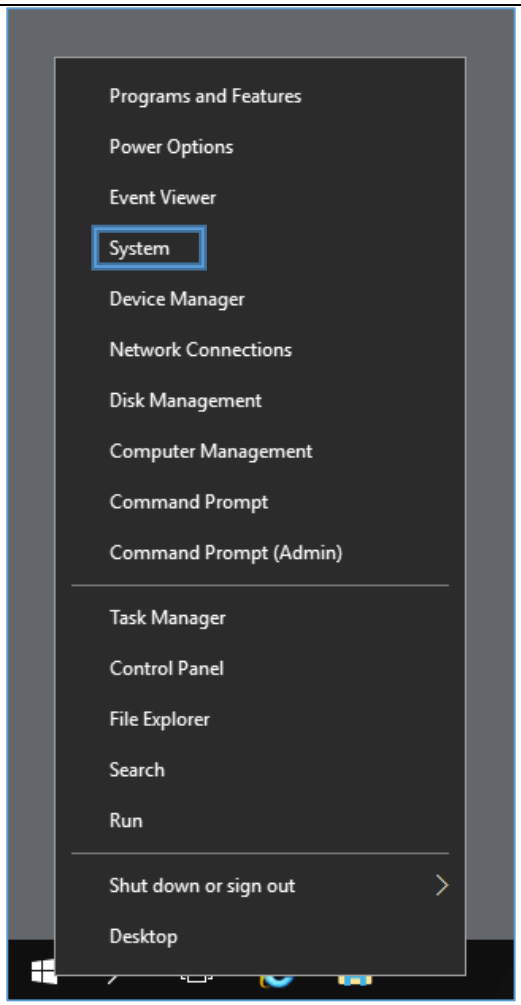
Exercise 4-1: Prepare the Server OS image

Scenario:

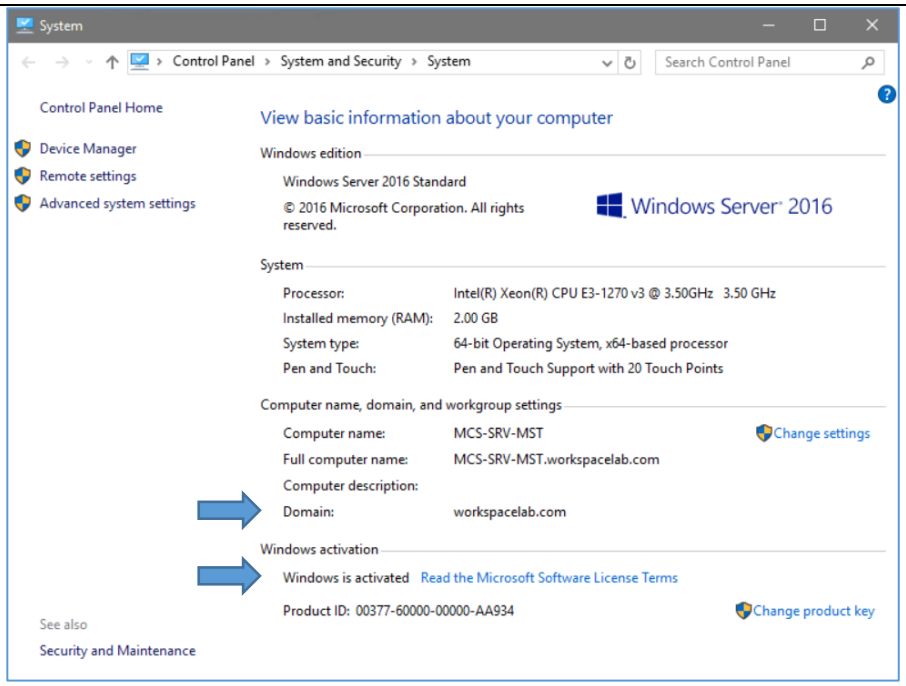
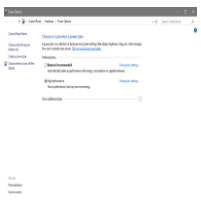
One of the platforms that WW Labs will use to host user resource sessions is Server OS running Windows Server 2016.

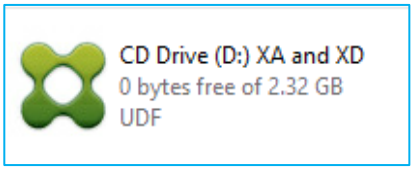
Your task is to prepare a Server OS to host user resources by setting machine parameters that meet WW Labs requirements and by installing the Virtual Delivery Agent.

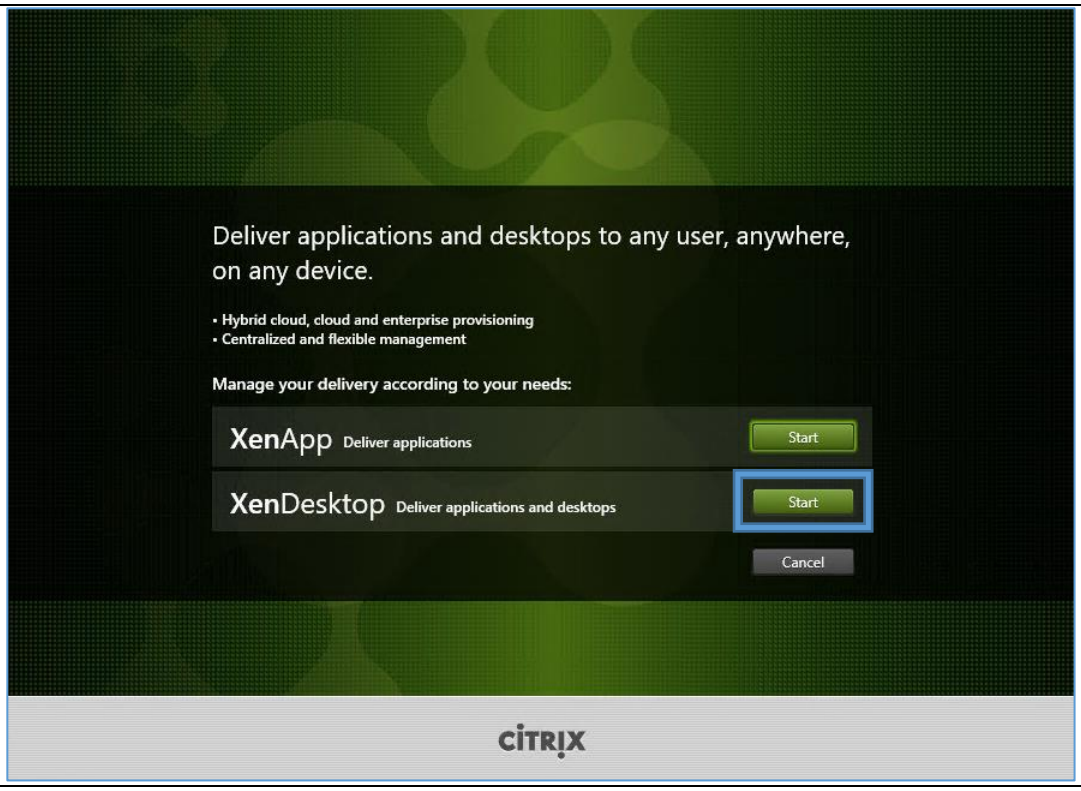
Step	Action
1.	The following VMs are required before beginning the exercises for this Module; all others may be powered down. To power manage your VMs, switch to XenCenter, right-click on the VM in the left pane and select Start or Shut Down. If prompted click Yes. • NYC-ADS-001 • NYC-SQL-001 • NYC-FSR-001 • NYC-XDC-001 • NYC-MAN-001 • NYC-WRK-002 • MCS-DTP-MST • MCS-SRV-MST If needed, you can power off any other VMs for this Module. **Note:** These above VMs are listed in the start-up order.
2.	Using the Remote Desktop Connection Manager, connect to MCS-SRV-MST. To log on to MCS-SRV-MST, right-click this machine and select **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1
3.	Right-click **Start** and click **System**.



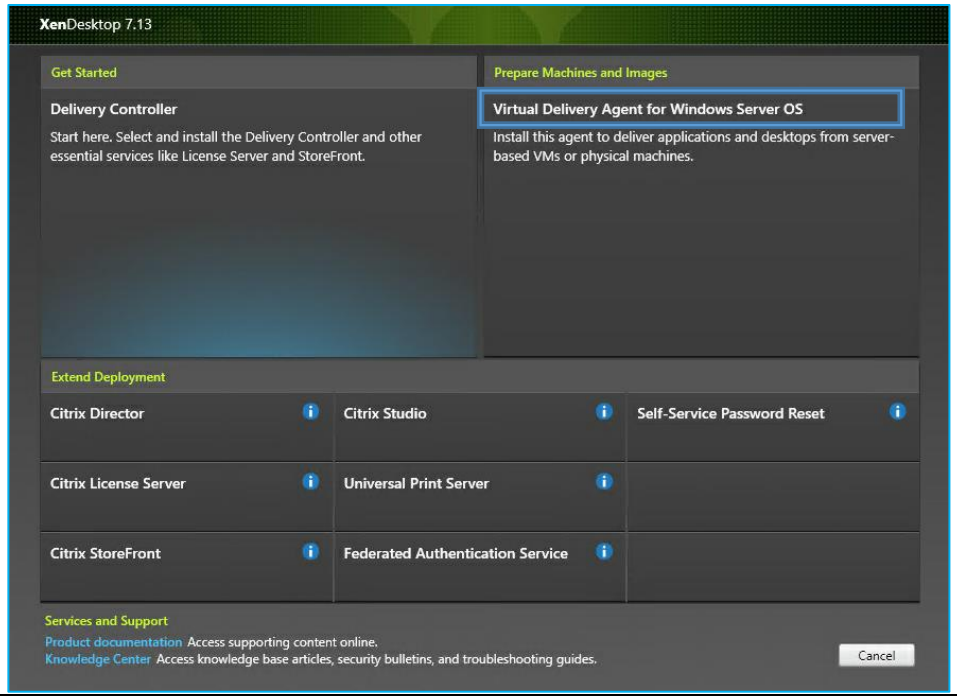
Verify that the machine is joined to the **workspacelab.com** domain and that **Windows is activated**.

	 **Note**: This machine will be used as a Master to create a Machine Catalog. To enable machines in this Machine Catalog to join the domain, we have to ensure that this Master is joined to the domain.
4.	Verify that the date and time are correct on MCS-SRV-MST. Click on the **current time** in the system tray. Click **Date and time settings**. **Note:** If the time or the time zone needed to be changed, you would click on Change date and time or Change time zone. For the purpose of this lab, you will leave the default settings. Click **OK** or **Cancel** to close the Date and Time dialog box.
5.	Modify the power plan for MCS-SRV-MST. Right-click **Start** and click **Power Options**. Under Choose or customize a power plan select **High performance**.  **Close** the **Power Options** window. **Note**: When selecting High Performance mode as a power plan, the computer does not lower the CPU's speed when it is not being used causing the CPU to run at higher speeds. It also increases screen brightness. Other components, such as your Wi-Fi or disk drive, may also

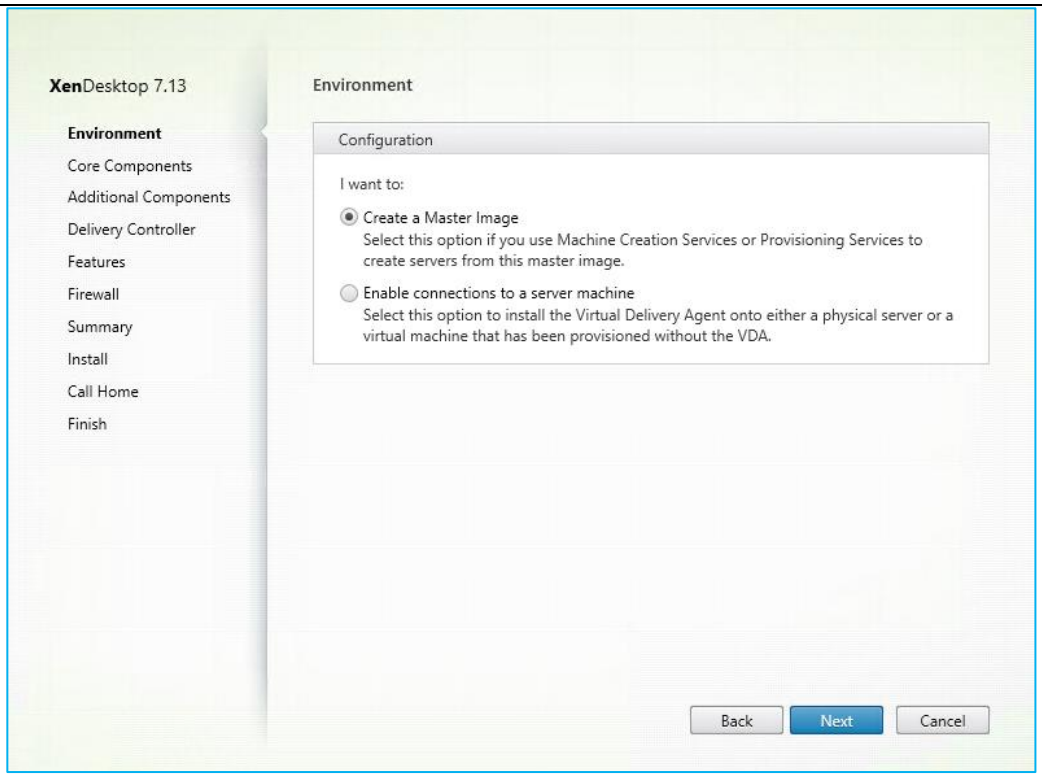
	not go into power-saving modes. High Performance favors performance, but may use more energy.
6.	Now that you have verified configurations for this VM, you will install the Virtual Delivery Agent so that it can communicate and register with the Delivery Controller. Using XenCenter mount the XenApp and XenDesktop installation media ISO to MCS-SRV-MST. To mount the installation media ISO, select **MCS-SRV-MST** in the left pane of XenCenter. In the right pane, select the **Console** tab. Using the **DVD Drive 1:** drop-down menu, select **XenApp_and_XenDesktop_7_13.iso**. **Note**: If there are no ISOs listed in the **DVD Drive 1:** drop-down menu, then the Local ISO Storage Repository (SR) that contains the ISO library may need to be re-scanned. In the left pane of XenCenter select the **Local ISO SR XS**. In the right pane select the **Storage** tab and click on the **Rescan** button. **Note**: If the above rescan of the **Local ISO SR XS** does not show the specific ISO for installation: XenApp_and_XenDesktop_7_13.iso, then please tell your instructor.
7.	Using the Remote Desktop Connection Manager, switch back to **MCS-SRV-MST**.
8.	Open the **File Explorer** application from the Windows Taskbar or Start Menu and double-click the **green Citrix logo** next to CD Drive under Devices and drives.  **Note**: If the screen in step 8 does not launch from double-clicking the green Citrix logo next to CD Drive under Devices and drives, then double-click the **AutoSelect.exe** file.
9.	On the Deliver applications and desktops to any user, anywhere, on any device screen, click **Start** next to the XenDesktop option.



10. Select **Virtual Delivery Agent for Windows Server OS**.

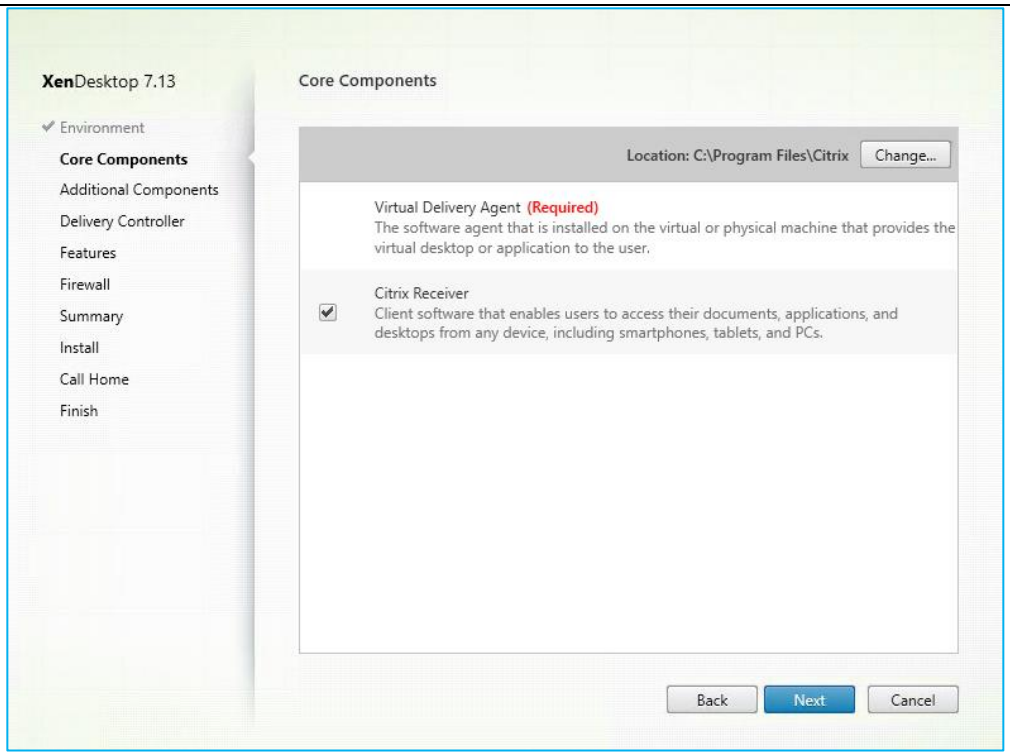


11. Verify that **Create a Master Image** is selected and click **Next**.



Note: Master is a term used to reference a machine that will be used as a base to create other machines nearly identical to the Master. You will be tasked to use this Master machine in a future exercise for this type of machine creation.

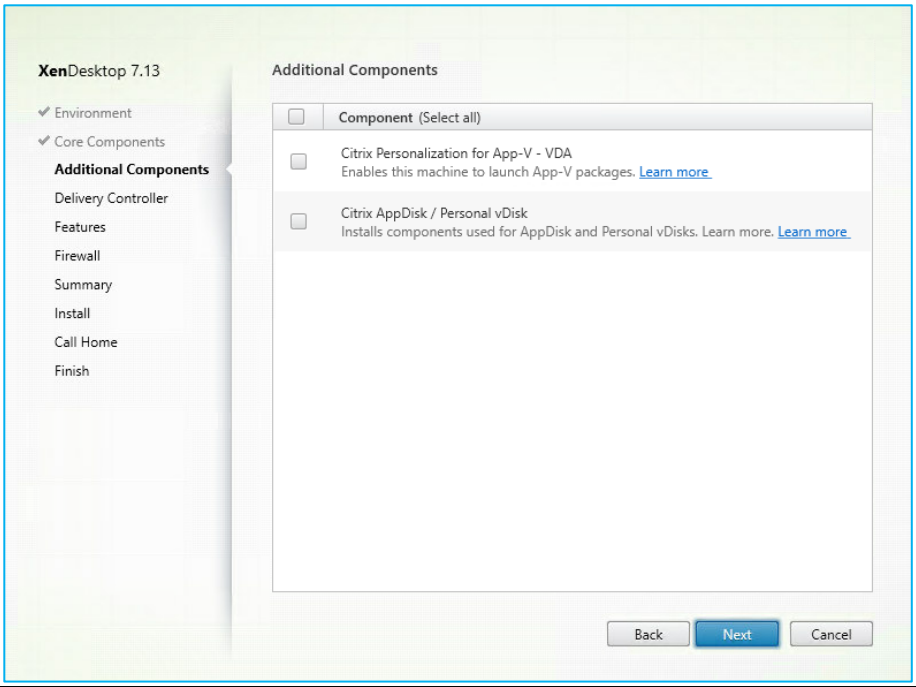
12. On the Core Components page, verify that the Virtual Delivery Agent is marked as **Required** and that **Citrix Receiver** is selected.



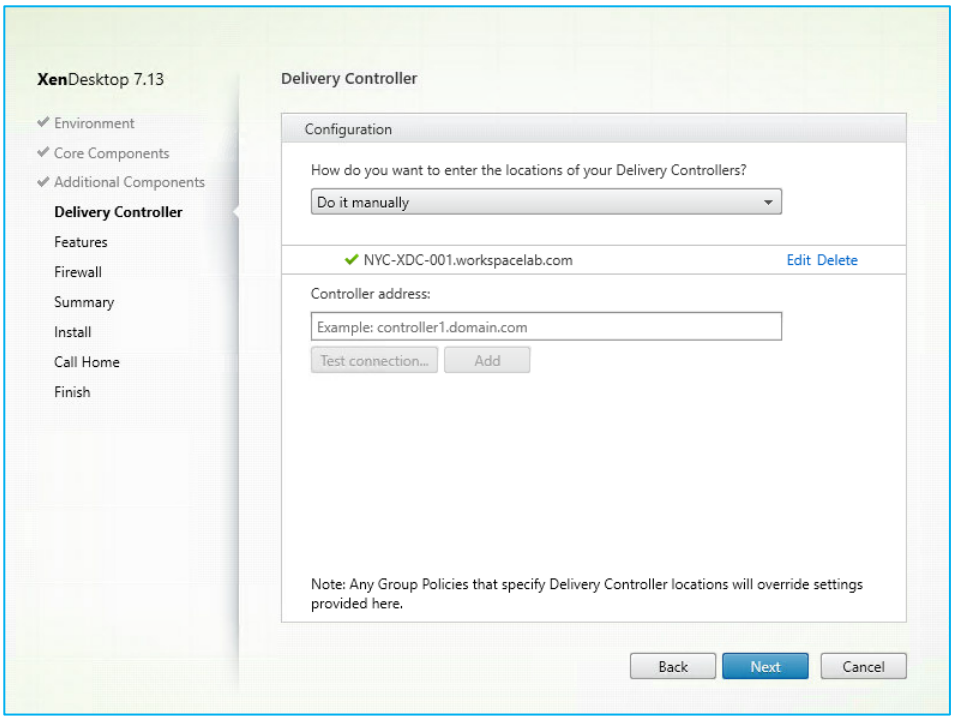
Click **Next** to continue the Virtual Delivery Agent installation wizard.

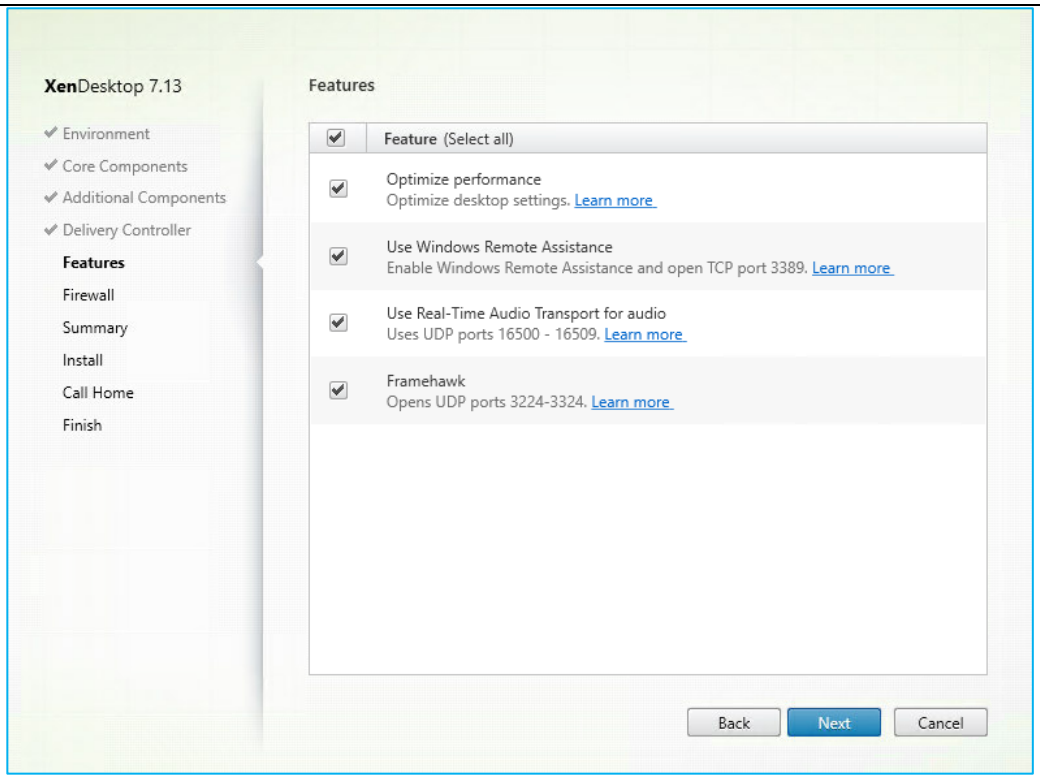
Note: You could choose to de-select Citrix Receiver here, but for this lab, we are installing it on the VDA.

13. On Additional Components Page, uncheck both check boxes and click **Next**.



14. Configure the Virtual Delivery Agent to register with the Controller deployed in a previous exercise.

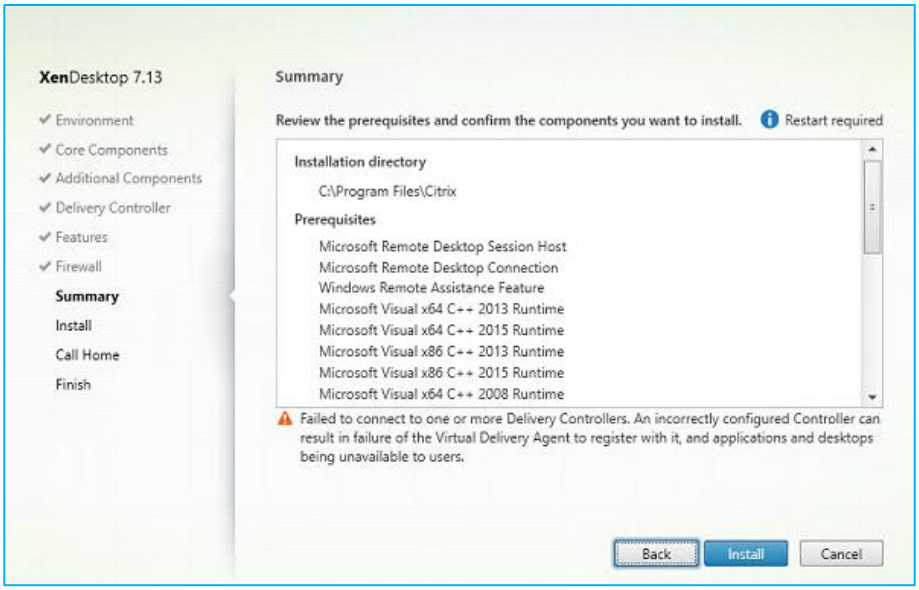
	On the Delivery Controller page, under Configuration, confirm the drop-down menu is set to **Do it manually**. Enter **NYC-XDC-001.workspacelab.com** in the Controller address field. Click **Test connection**. If the test is successful, as indicated by a green check mark to the right of the Controller address field, click **Add**.  Click **Next** to continue the Virtual Delivery Agent installation wizard. **Note**: The XenApp and XenDesktop Site has only one Controller to add. If the environment had additional Controllers, this method could be used to add the additional Controllers. **Note**: This Controller address step in the Virtual Delivery Agent (VDA) installation wizard saves the Controller address into the registry of the Master that you are installing the VDA on. This is important, because as mentioned above, all machines created from this Master will be nearly identical, which means all machines will have the same registry entry that can be used by the VDA to register with and find the Controller.
15.	On the Features page, verify that the following four checkboxes are enabled: • **Optimize performance** • **Use Windows Remote Assistance** • **Use Real-Time Audio Transport for audio** • **Framehawk**



Click **Next** to continue the Virtual Delivery Agent installation wizard.

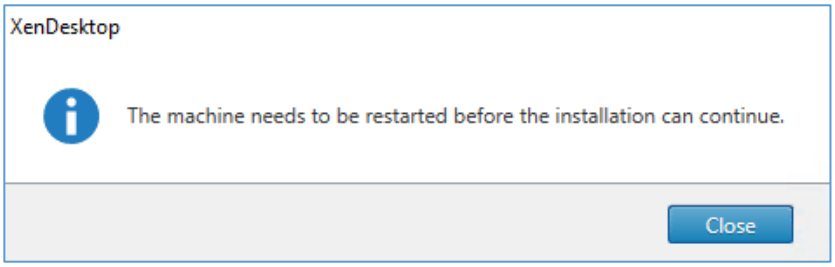
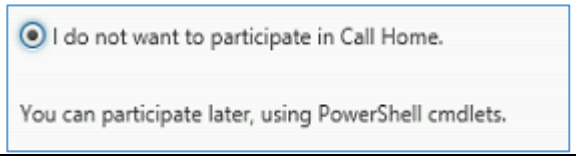
16. On the Firewall page, verify that the **Automatically** option is selected for configuring the firewall rules. Click **Next**.

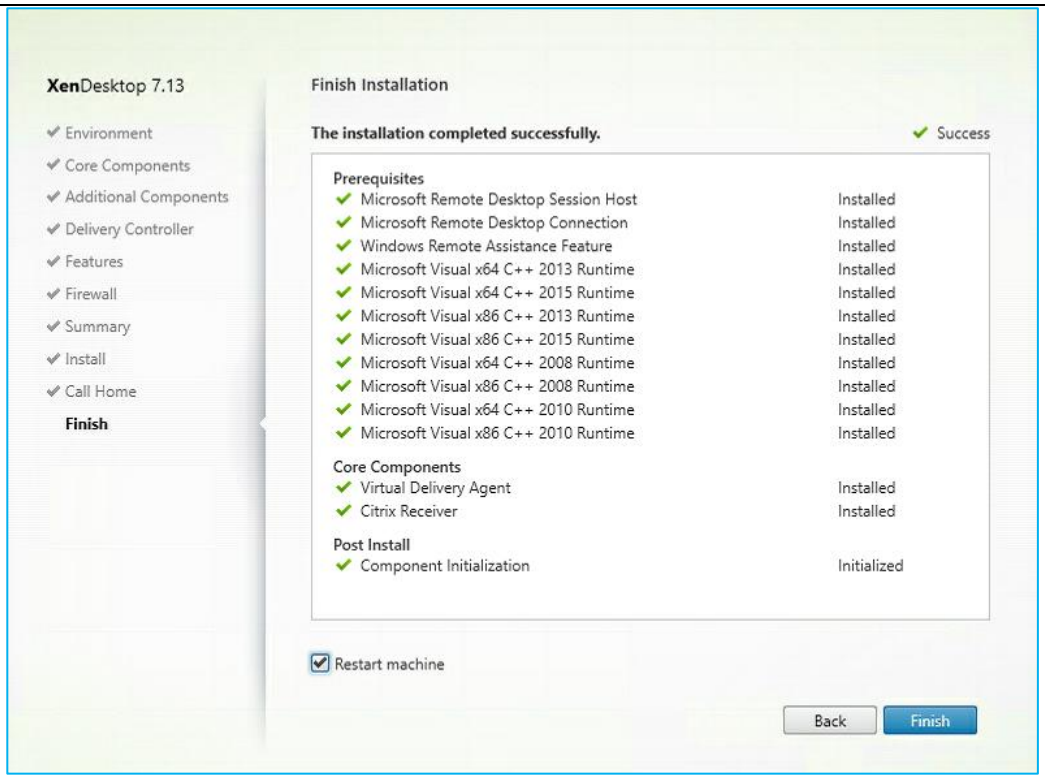
17. On the Summary page, review and confirm the configurations.



Click **Install**.

Note: The installation will take a few minutes.

	Note: Please ignore the “Failed to connect to one or more delivery controllers.” warning. Citrix XenDesktop development is aware of the error and will be resolving the issue in a future release. Refer [#HDX-5012] on https://docs.citrix.com/en-us/xenapp-and-xendesktop/7-13/whats-new/known-issues.html for more details.
18.	Click **Close** on the XenDesktop dialog box informing that a restart is required for the installation to continue.  **Note:** MCS-SRV-MST will reboot and then will continue with the installation of the VDA. Ensure that each time you log on after a reboot, you use the same credentials that were used to perform this installation. You may want to switch to XenCenter to monitor the progress of the reboot. To do this, select MCS-SRV-MST in the left pane and the Console tab in the right pane. Using the Remote Desktop Connection Manager, connect to MCS-SRV-MST after reboot. To log on to MCS-SRV-MST, switch back to the Remote Desktop Connection Manager, right-click this machine, and select **Connect server**. **Note**: The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1
19.	Wait for the installation to resume.
20.	On the Call Home page, select **I do not want to participate in Call Home** and click **Next**. 
21.	Verify that the pre-requisites, core components, and post install items completed successfully. Ensure that the **Restart machine** option is enabled (default) and click **Finish**.



Note: You may want to switch to XenCenter to monitor the progress of the reboot. To do this, select MCS-SRV-MST in the left pane and the Console tab in the right pane.

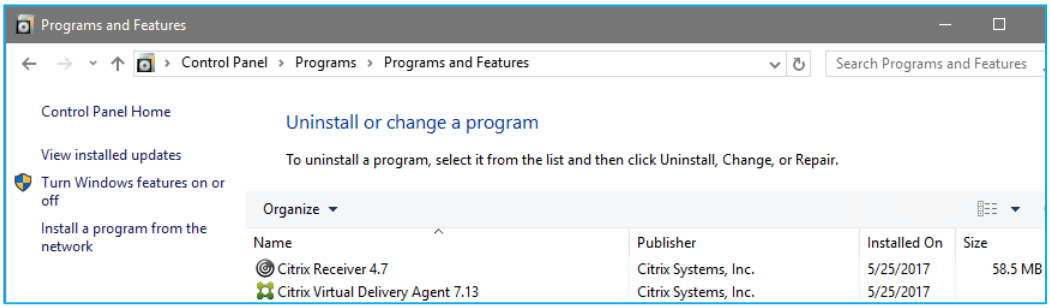
22. After MCS-SRV-MST has finished rebooting, switch back to the Remote Desktop Connection Manager, and connect to MCS-SRV-MST.

    To log on to MCS-SRV-MST, right-click this machine and choose **Connect server**.

    Note: The following credentials are used to make the connection:
    - User name: Workspacelab\Administrator
    - Password: Password1

23. Verify that the expected Virtual Delivery Agent (VDA) software and version was installed.

    Right-click **Start** and select **Program and Features**.



    Close the **Programs and Features** window.

24. Using **XenCenter,** eject the XenApp and XenDesktop installation media from **MCS-SRV-MST**.

    To eject the installation media ISO, select **MCS-SRV-MST** in the left pane of XenCenter. In the

	right pane, select the **Console** tab and click **Eject** to remove **XenApp_and_XenDesktop_7_13.iso** from the DVD-Drive 1. **Note**: The Eject option can be difficult to see. It is an underlined word to the right side of the DVD Drive 1 drop-down menu.

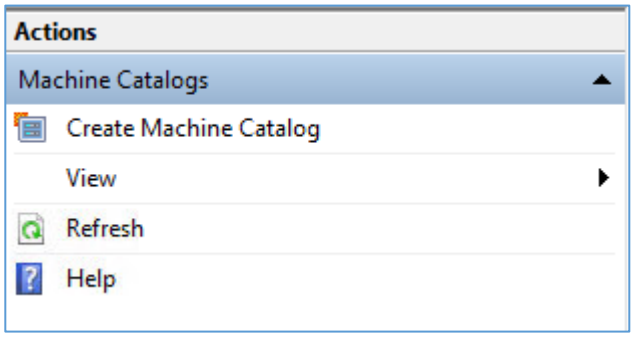
Key Takeaways:

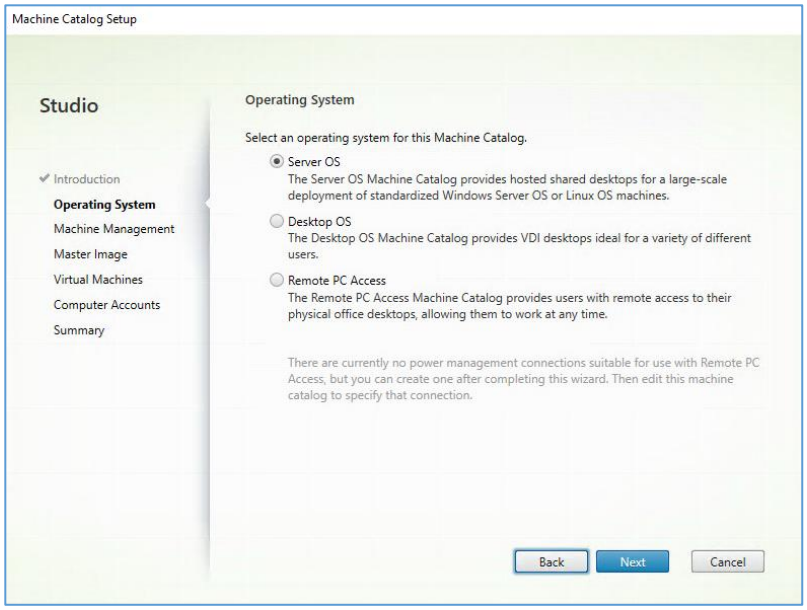
- The Server OS VDA installation allows for two different installation methods: create a master image or enable connections to a server machine. Create a master image will install the VDA in a "sysprepped" state. Enable connections to a server machine is used when no image management is required.
- The Server OS VDA installation adds the required Remote Desktop Services Session Host role and other dependencies automatically.
- The installation of the VDA component is required for all machines that will be used to deliver applications or desktops to end users.

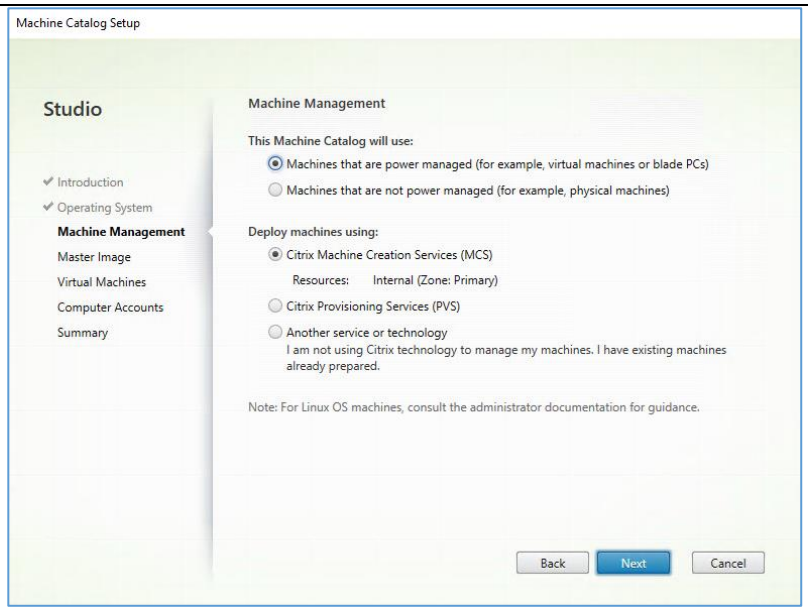
Exercise 4-2: Create a Machine Catalog for Server OS using MCS

Scenario:

Your task is to proceed with the next step in creating resources for users that are hosted on a Server OS. You will create a Machine Catalog using the Server OS that you prepared previously.

Step	Action
1.	Using the Remote Desktop Connection Manager, connect back to NYC-XDC-001. To log on to NYC-XDC-001, right-click this machine and select **Connect server**. **Note**: The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1
2.	Using Studio, expand **Citrix Studio (SITE-NewYork)** and click **Machine Catalogs**. From the Actions pane on the right side of the console, click **Create Machine Catalog**.  **Note**: Studio was started in a previous exercise. If Studio was closed in a previous exercise, then click Start > Citrix > Citrix Studio.
3.	On the Introduction page, click **Next** to continue the Machine Catalog creation wizard.

	Note: Machine Catalogs are collections of physical or virtual machines that you assign to users. You create Machine Catalogs from Master Images or physical machines in your environment. The Master Image or physical machine that you use to create a Machine Catalog must have a Virtual Delivery Agent installed. Also, ensure that the operating system is up-to-date and that applications are installed.
4.	On the Operating System page, verify that **Server OS** is selected and click **Next**.  **Note**: When selecting an operating system for the Machine Catalog, there are three options: • **Server OS**: The Server OS Machine Catalog provides hosted shared desktops for a large-scale deployment of standardized Windows Server OS or Linux OS machines. • **Desktop OS**: The Desktop OS Machine Catalog provides VDI desktops ideal for a variety of different users. • **Remote PC Access**: The Remote PC Access Machine Catalog provides users with remote access to their physical office desktops, allowing them to work at any time.
5.	On the Machine Management page, verify that the following two options are selected: • **Machines that are power managed (for example, virtual machines or blade PCs)** • **Citrix Machine Creation Services (MCS)** Click **Next** to continue the Machine Catalog creation wizard.

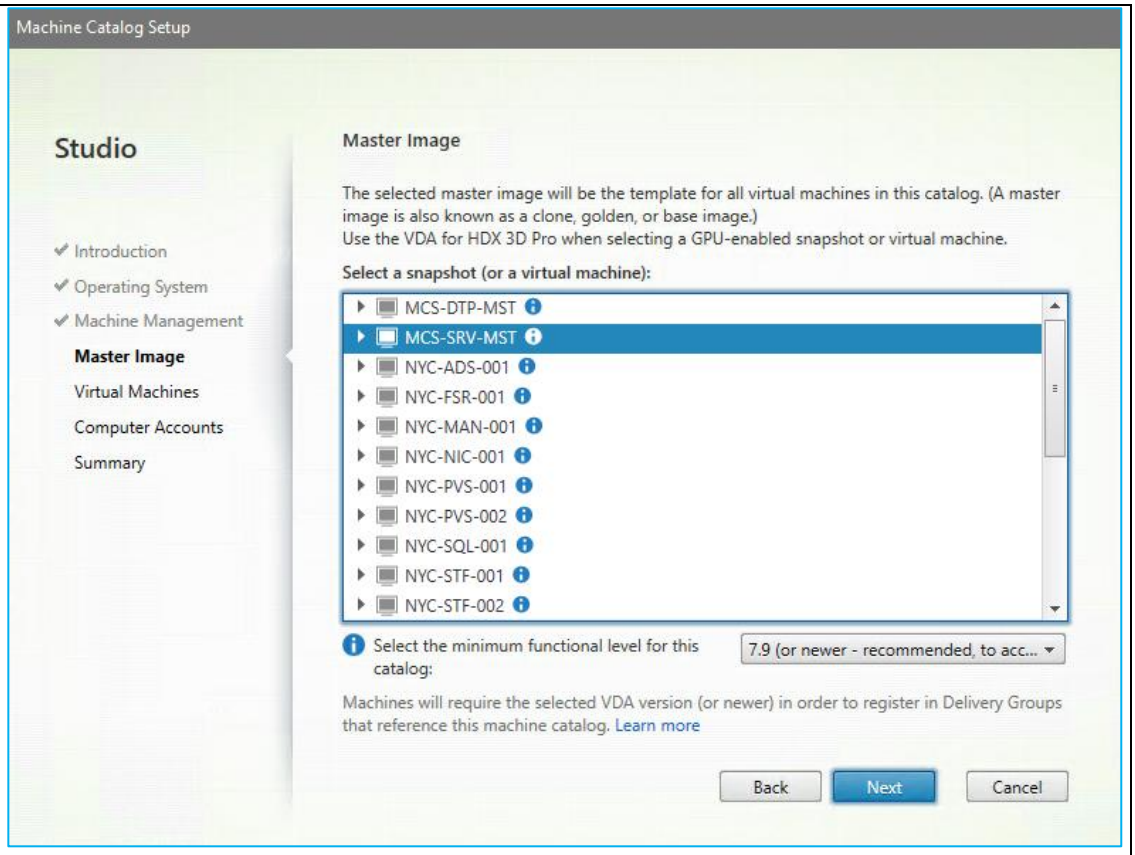


Note: There are three options for the type of tool that will be used to deploy machines:

- Citrix Machine Creation Services (MCS) – Uses a master image or template to create and manage virtual machines.
    - MCS is not available for physical machines.
    - Machine Catalogs in cloud environments use MCS.
- Citrix Provisioning Services (PVS) – Manages target devices as a device collection. A Provisioning Services vDisk imaged from a master target device delivers desktops and applications.
- Another service or technology – A tool that manages machines already in the data center. Citrix recommends you use Microsoft System Center Configuration Manager or another third-party application to ensure that the machines in the catalog are consistent.

6. On the Master Image page, select **MCS-SRV-MST** as the Master machine.

   Click **Next** to continue the Machine Catalog creation wizard.

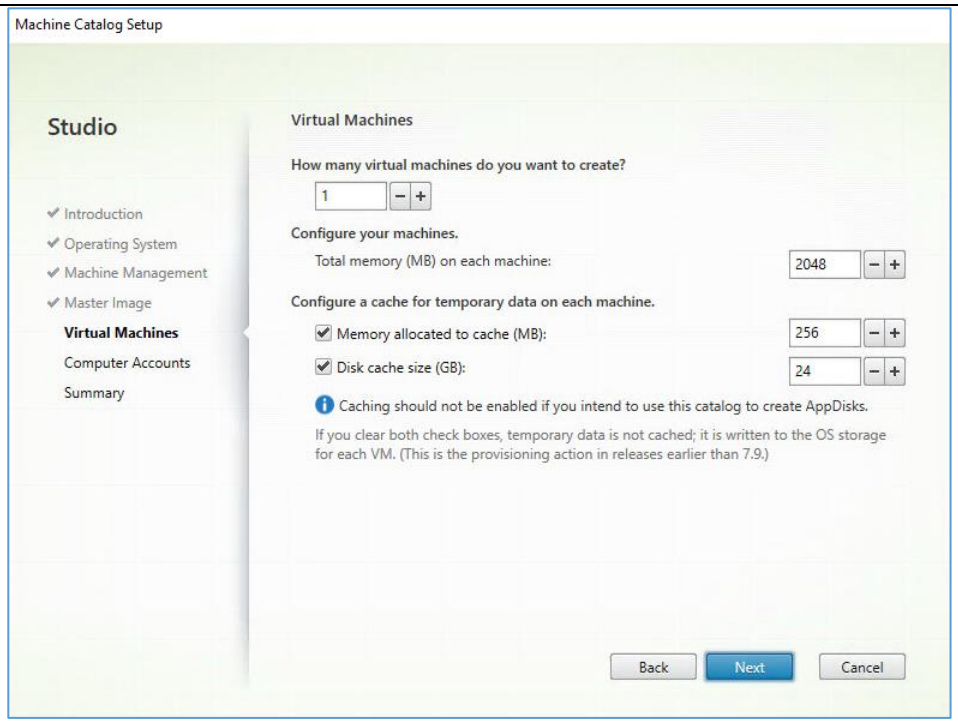


Note: If snapshots existed for the machine, you could select a specific snapshot to be used for the master. Since there are no snapshots, the resultant process of this wizard will create one automatically.

Note: Version 7.13 does not have the option to Customize virtual CPUs from the MCS wizard.

7. On the Virtual Machines page, verify that the following default settings are configured:

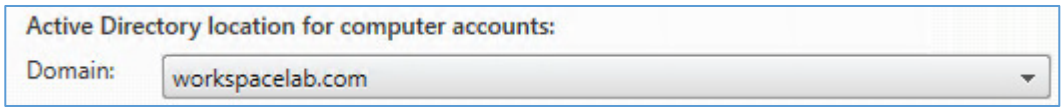
   - Number of Virtual machines needed: **1**
   - Memory: **2048 MB**
   - Memory allocated to cache (MB): **256**
   - Disk cache size (GB): **24**



Click **Next** to continue the Machine Catalog creation wizard.

8. On the Computer Accounts page, verify that the **Create new Active Directory accounts** radio button is selected.

   In the drop-down next to Domain for the Active Directory location for computer accounts field, verify that **workspacelab.com** is selected.



   Using the arrows, expand **Citrix > New York > VDA**.

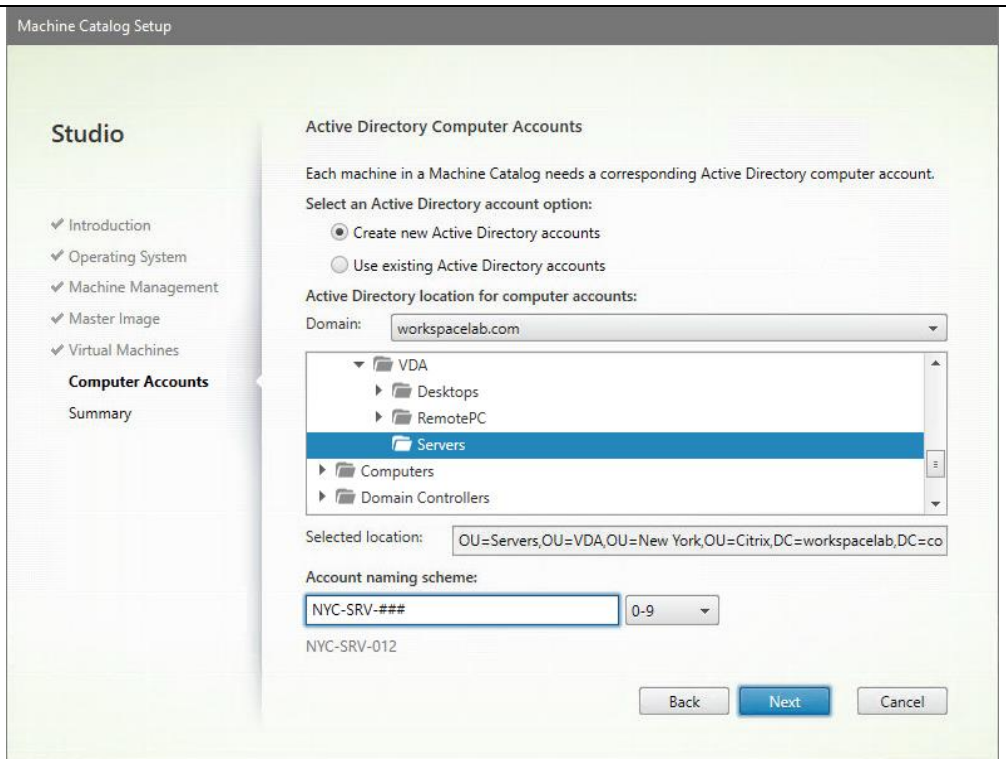
   Select the **Servers** Organizational Unit (OU)**.**

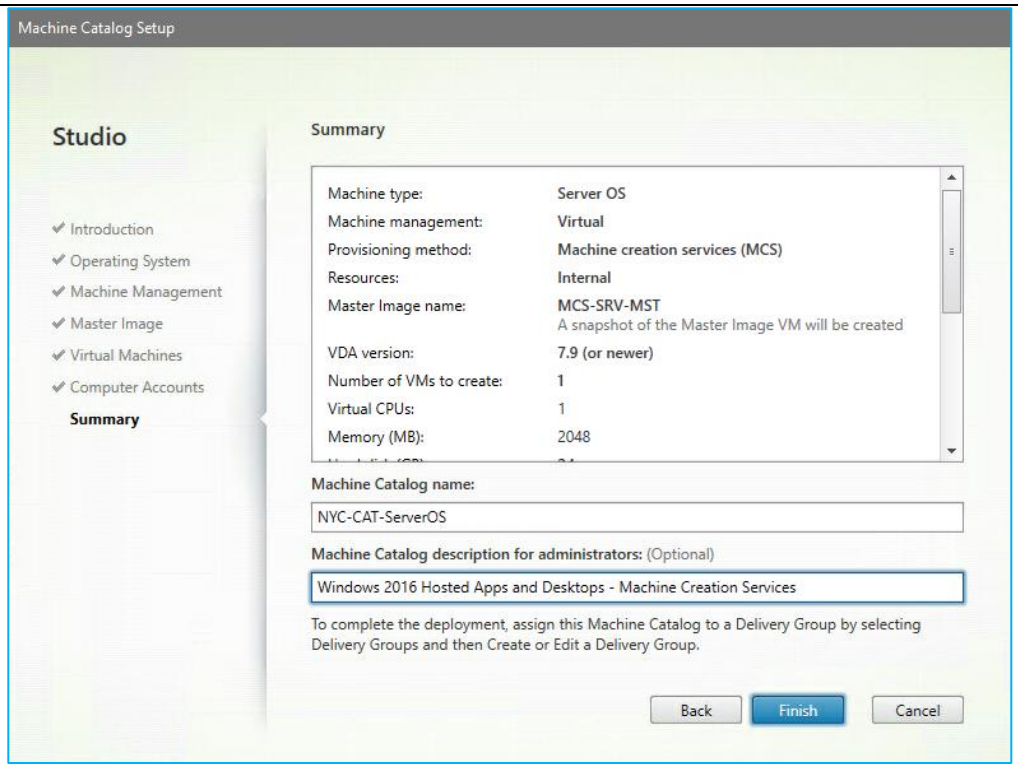
   Note: The Servers OU is the WW Labs location designated for machines running the Virtual Delivery Agent (VDA) that are used to host Server OS apps and desktop resources for users.

   Enter **NYC-SRV-###** in the Account naming scheme field.

   Verify that **0-9** is selected from the drop-down menu to the right of the naming scheme.

   Note: If this wizard was being used to create machines on an existing naming convention, then the resultant machines from this Machine Creation Services (MCS) process would increment to the next numerical sequence numbers available.

	 Click **Next** to continue the Machine Catalog creation wizard.
9.	On the Summary page, review the configurations and enter the following information: • Machine Catalog name: **NYC-CAT-ServerOS** • Machine Catalog description for administrators: **Windows 2016 Hosted Apps and Desktops - Machine Creation Services**



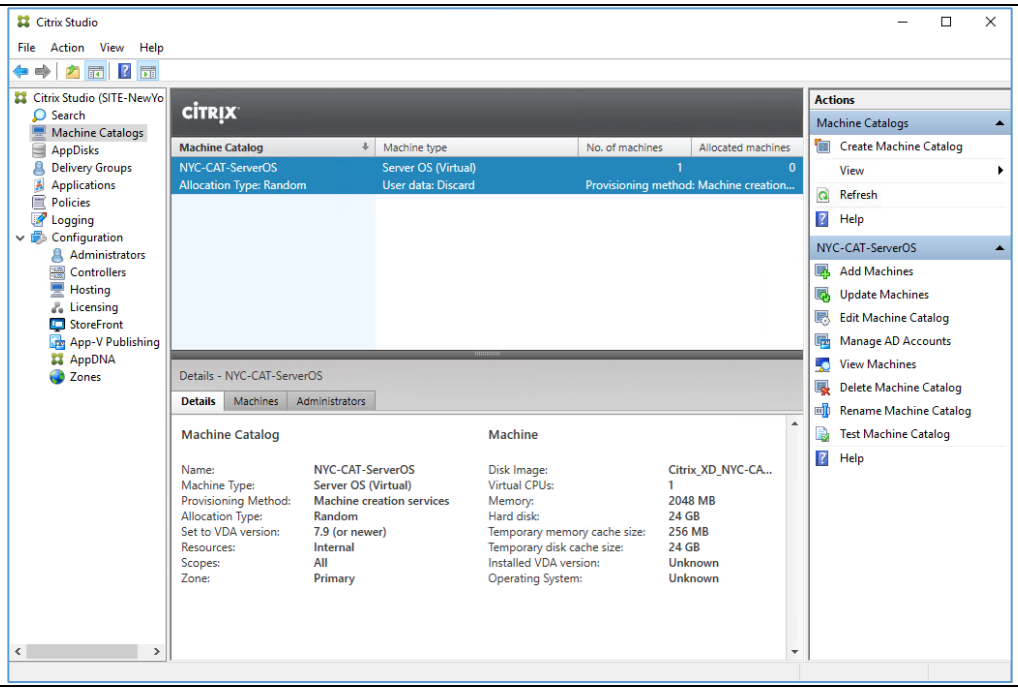
Click **Finish**.

Note: Clicking Finish begins the Machine Creation Services (MCS) process in which a combination of the parameters specified in this Machine Catalog creation wizard and the parameters of the XenApp and XenDesktop Site are used to create complete virtual machines from the Master machine specified earlier in said wizard. Each virtual machine created is built into a Machine Catalog, visible from Studio. Each virtual machine created has a nearly identical build to its Master machine, with a unique SID, machine account in Active Directory, unique MAC, and using the DHCP scope we verified in an earlier exercise these virtual machines have a unique IP address.

Note: With the XenServer resources allocated to this XenApp and XenDesktop POC project by the Lead Citrix Architect, it is expected that the Machine Creation Services (MCS) process will take an estimated 15 minutes to complete. This process may appear hung, however, it is not; just let it continue and complete itself.

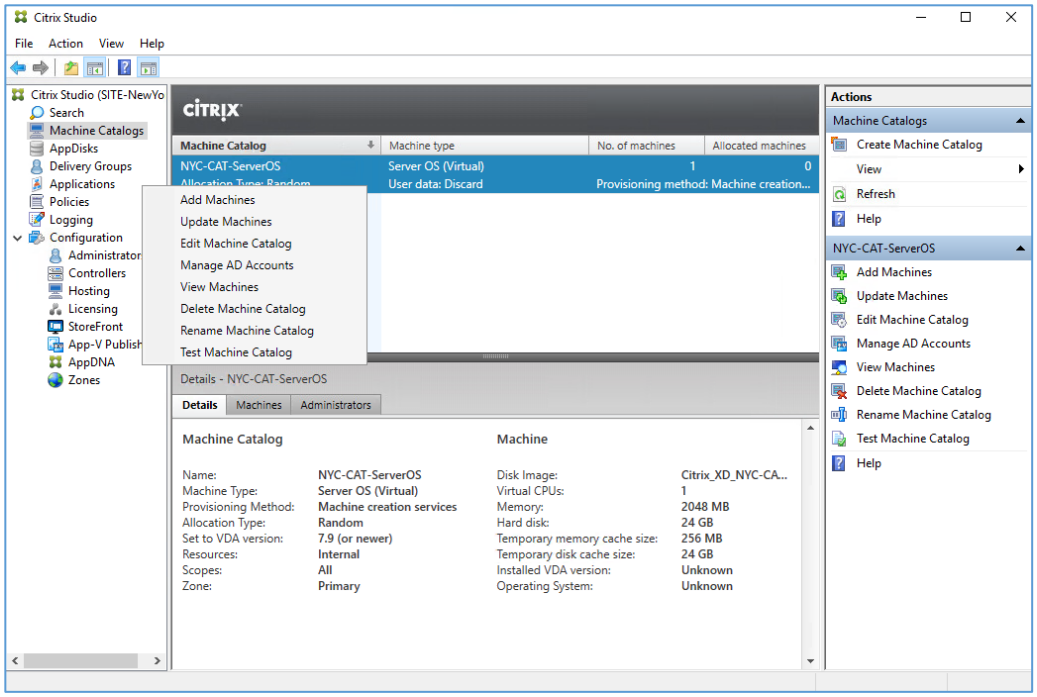
10. Verify that the Machine Creation Services (MCS) process has completed. Using Studio, verify that the Machine Catalog has been created.

    Click **Machine Catalogs** in the left pane of Studio and view the **NYC-CAT-ServerOS** Machine Catalog in the middle pane.

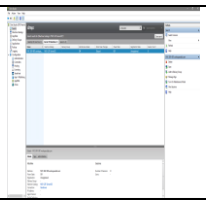
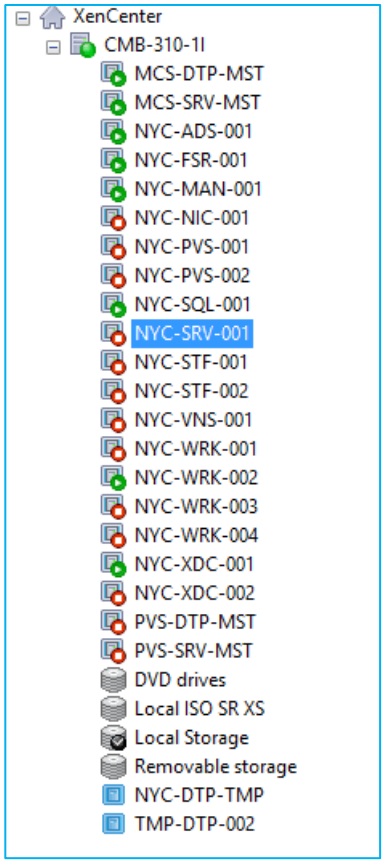


11. Verify that the virtual machine that was specified to be created using Machine Creation Services (MCS) has been successfully created and added to the NYC-CAT-ServerOS Machine Catalog.

Using Studio, right-click the **NYC-CAT-ServerOS** Machine Catalog and select **View Machines**.



Verify that **NYC-SRV-001.workspacelab.com** displays.

	
12.	Additionally, verify that the virtual machine NYC-SRV-001 was created in the environment. Using XenCenter, in the left pane, confirm that **NYC-SRV-001** is listed to verify that this machine was created. 
13.	Using XenCenter, right-click **NYC-SRV-001** and select **Start**.

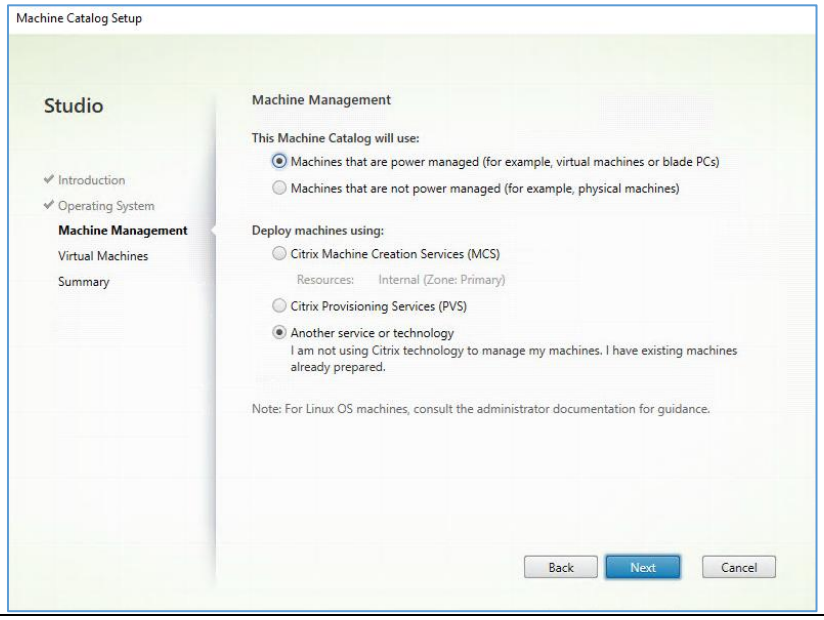
Key Takeaways:

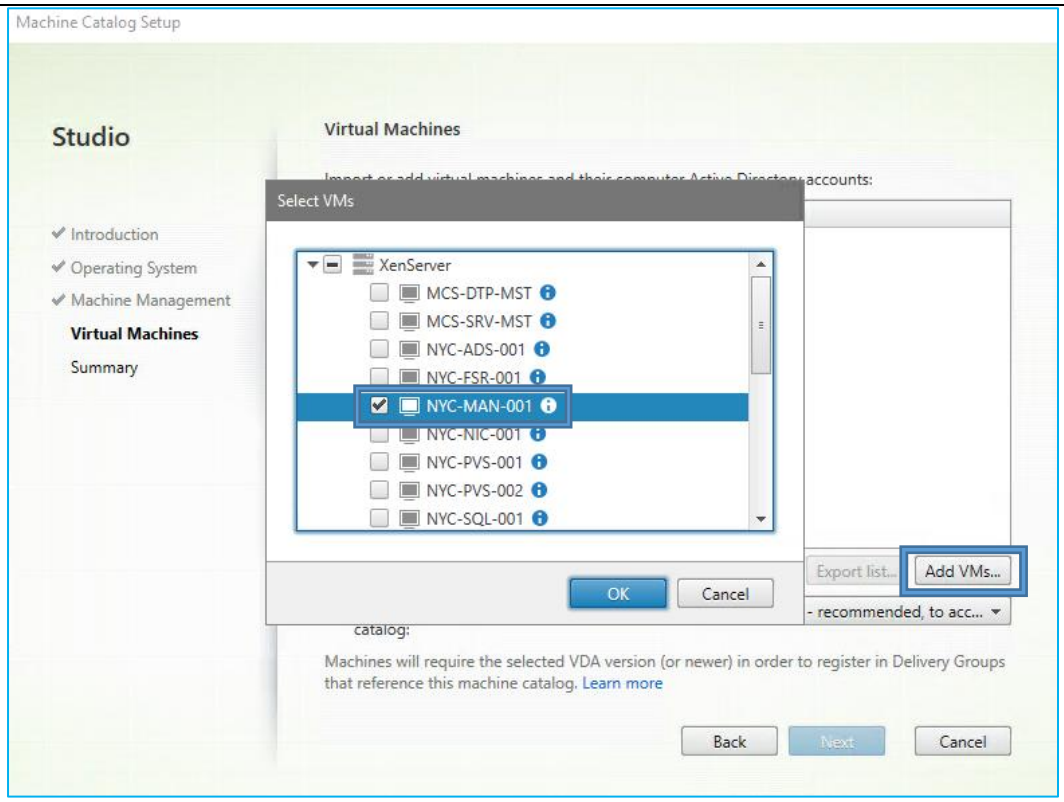
- Machine Catalogs group machines together that are similar in function, purpose, and capabilities.
- All machines within a Machine Catalog need to be either Server OS or Desktop OS and cannot be mixed.

Exercise 4-3: Create a Machine Catalog for Server OS using Manual Provisioning

Scenario:

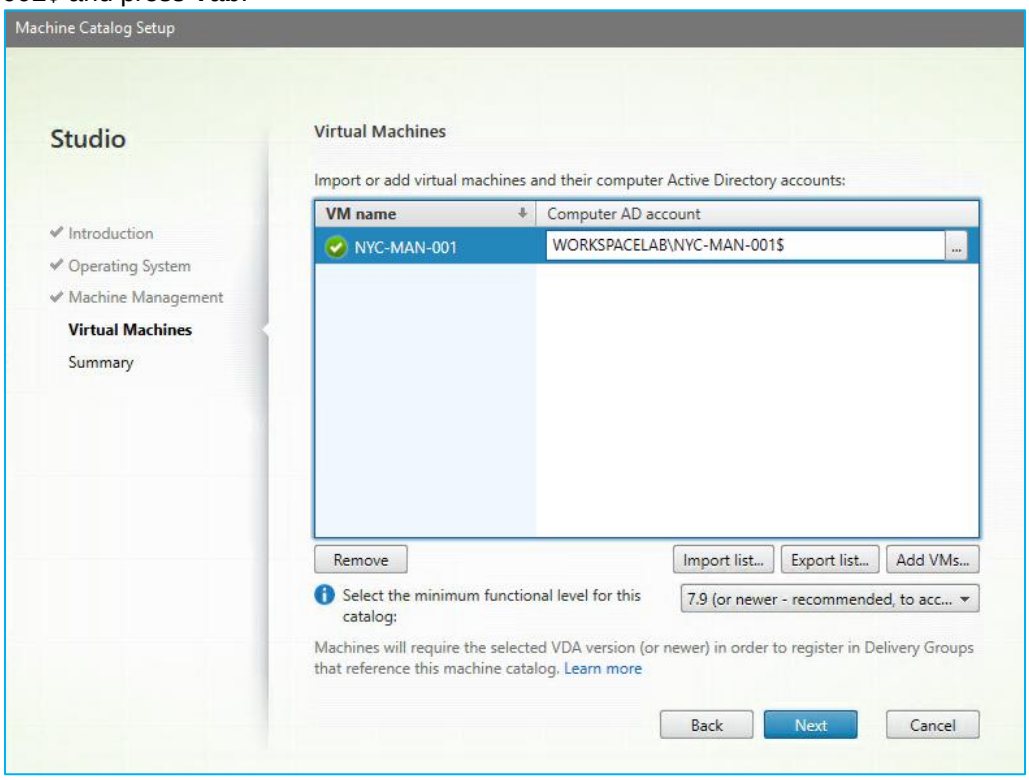
You will create a Machine Catalog using the Server OS that has been pre-created in the lab. This machine already has VDA software installed.

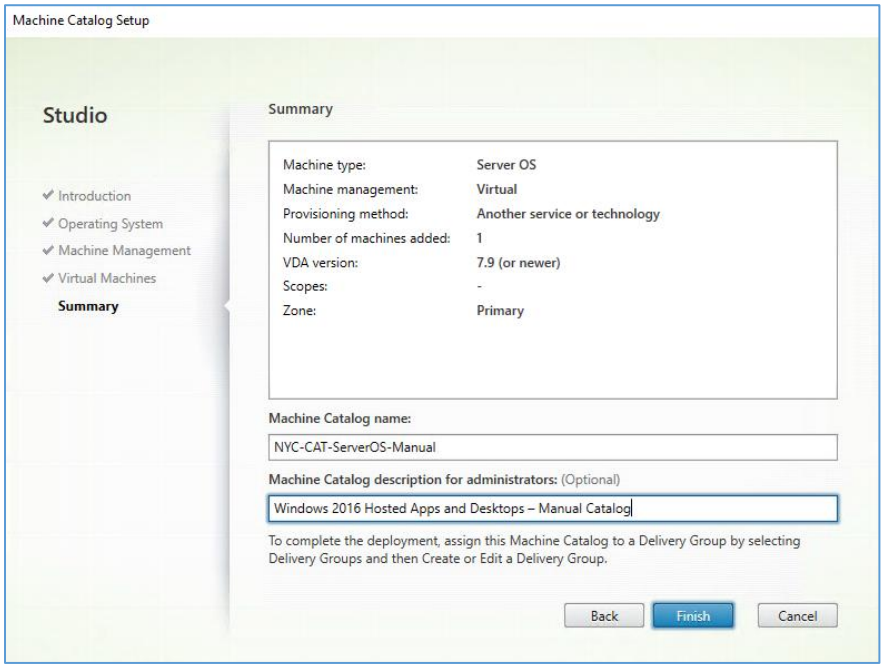
Step	Action
1.	Using the Remote Desktop Connection Manager, confirm that you are still connected to **NYC-XDC-001**. **Note**: In a previous exercise, you had logged on to NYC-XDC-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-XDC-001 by right-clicking this machine and selecting Connect server.
2.	Using Studio, expand **Citrix Studio (SITE-NewYork)** and click **Machine Catalogs**. From the Actions pane on the right side of the console, click **Create Machine Catalog**. **Note**: Studio was started in a previous exercise. If Studio was closed in a previous exercise, then click Start > Citrix > Citrix Studio.
3.	On the Introduction page, click **Next** to continue the Machine Catalog creation wizard.
4.	On the Operating System page, verify that **Server OS** is selected and click **Next**.
5.	On the Machine Management page, verify that the following two options are selected: • **Machines that are power managed (for example, virtual machines or blade PCs)** • **Another service or technology** Click **Next** to continue the Machine Catalog creation wizard. 
6.	On the Virtual Machines page, click **Add VMs** and select **NYC-MAN-001** from the list of machines.



Click **OK** on the Select VMs window.

7. On Virtual Machines page, under Computer AD account, type **WORKSPACELAB\NYC-MAN-001$** and press **Tab**.



	Click **Next**.
8.	On the Summary page, review the configurations and enter the following information: • Machine Catalog name: **NYC-CAT-ServerOS-Manual** • Machine Catalog description for administrators: **Windows 2016 Hosted Apps and Desktops – Manual Catalog**  Click **Finish**.

Key Takeaways:

- Although Citrix recommends using either the MCS or PVS provisioning method, it is also possible to create a Catalog from machines that have been installed manually.

Exercise 4-4: Create two Delivery Groups for Server OS Catalogs

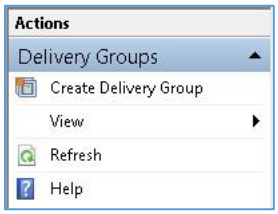
Scenario:

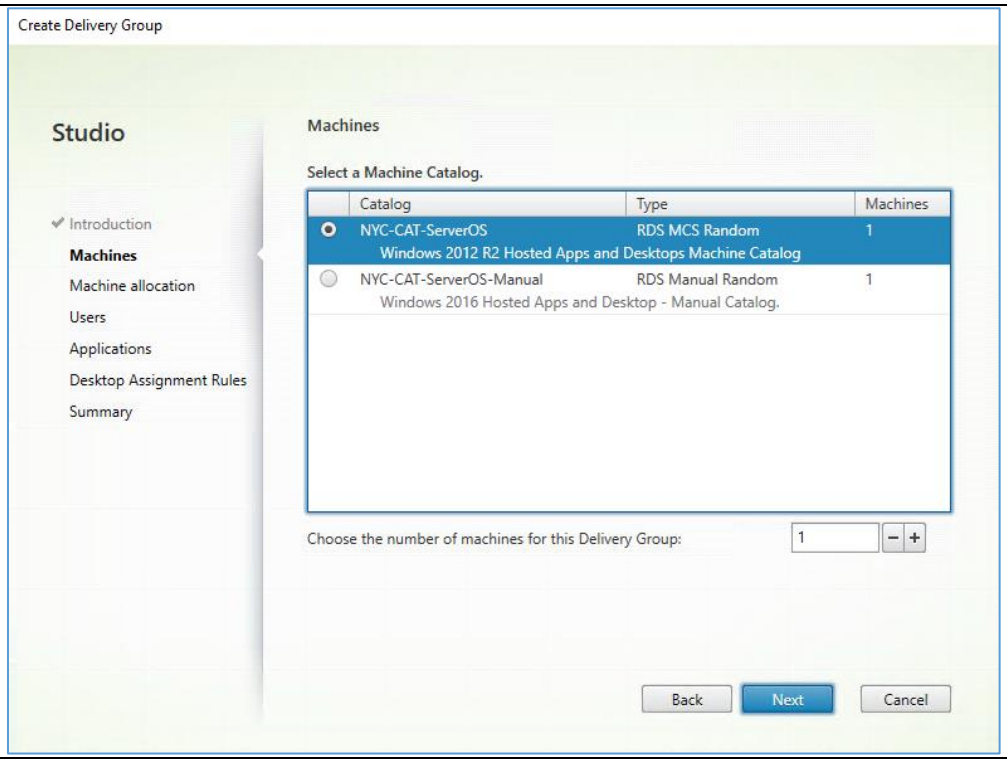
Server OS Machine Catalogs contain a group of identical Server OS machines that can be used to deliver a set of resources to users. The delivery of these resources to users is controlled through Delivery Groups.

WW Labs has several user groups that require access to resources, including the Human Resources, Engineers, and Auditors departments. These user groups will be dependent on Server OS-based resources.

Your task is to create two Delivery Groups and assign resources to the HR and Engineers Groups from two different Server OS catalogs using Delivery Groups.

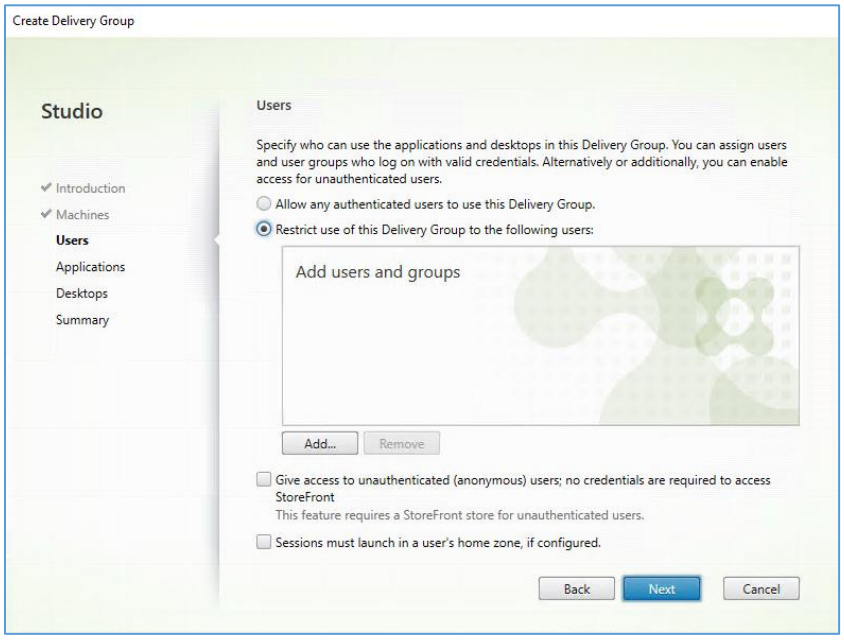
Step	Action
1.	Using the Remote Desktop Connection Manager, confirm that you are still connected to **NYC-**

	XDC-001. **Note:** In a previous exercise, you had logged on to **NYC-XDC-001** using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-XDC-001 by right-clicking this machine and selecting Connect server.
2.	Using Studio, expand **Citrix Studio (SITE-NewYork)** and click **Delivery Groups**. From the Actions pane on the right side of the console, click **Create Delivery Group**.  **Note**: Studio was started in a previous exercise. If Studio was closed in a previous exercise, then click Start > Citrix > Citrix Studio.
3.	On the Introduction page, click **Next** to continue the Delivery Group creation wizard. **Note**: Delivery Groups are collections of desktops and applications that created from Machine Catalogs. Create Delivery Groups for specific teams, departments, or types of users, and base them on either a desktop or a server operating system. Make sure you have enough machines available in a suitable Catalog to create the Delivery Groups you need.
4.	On the Machines page, verify that the previously created Machine Catalogs are listed. Select **NYC-CAT-ServerOS**. Enter **1** in the Choose the number of machines for this Delivery Group field. Click **Next** to continue the Delivery Group creation wizard.

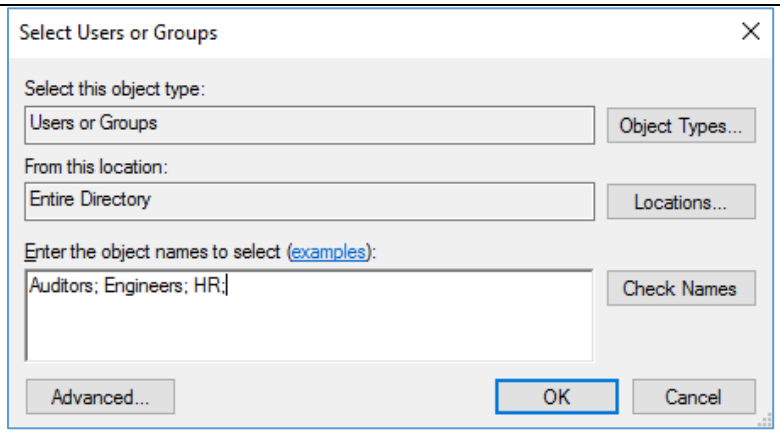


5. On the Users page, select **Restrict use of this Delivery Group to the following users.**

   Click the **Add** button under the Add users and groups box.

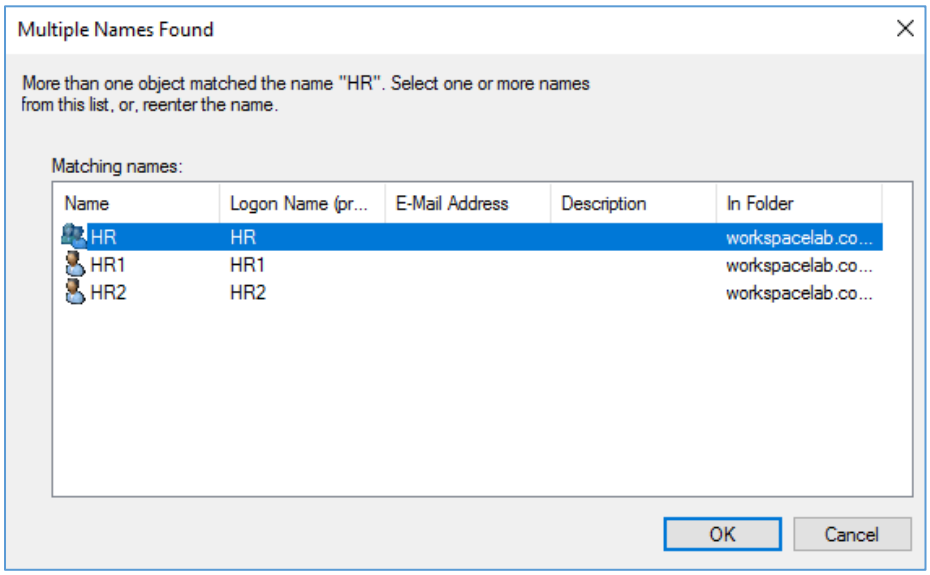


   Enter **Auditors; Engineers; HR;** in the Select Users or Groups dialog box that appears.

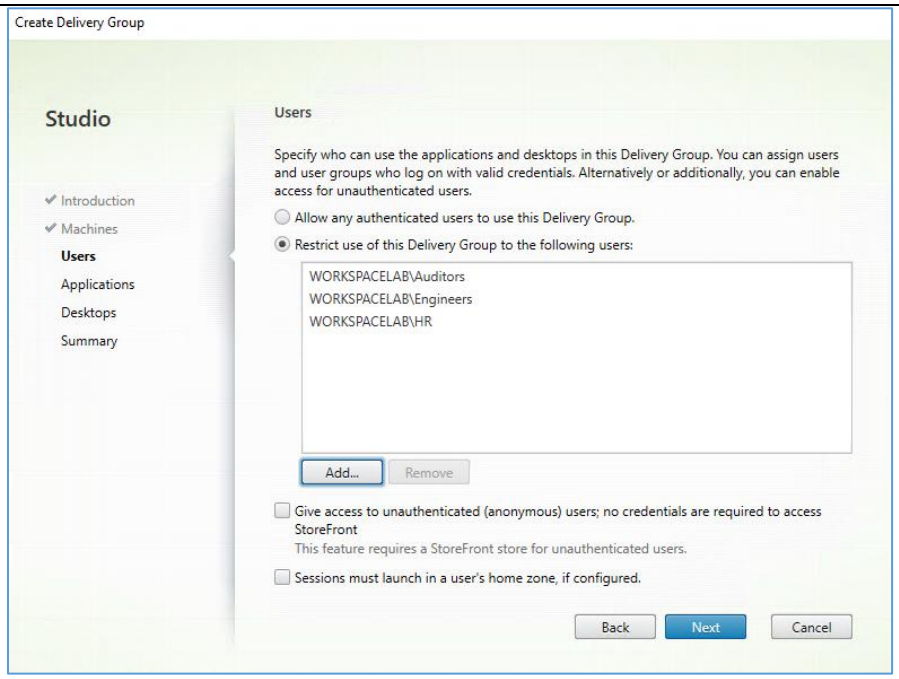


Click **Check Names**.

Click **OK** on the HR Group highlighted, and click **OK** on the Select Users or Groups dialog box.

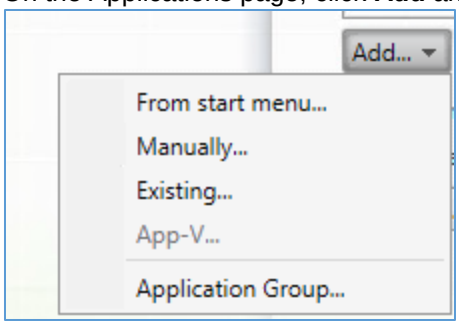


Click **Next** to continue the Delivery Group creation wizard.



Note: The WW Labs design scope for this XenApp and XenDesktop POC deployment has specified these user groups in Active Directory for testing these published applications (as seen in the next step) for this POC.

6. On the Applications page, click **Add** and select **From start menu**.



Note: The wizard will begin the process of discovering applications found on NYC-SRV-001.

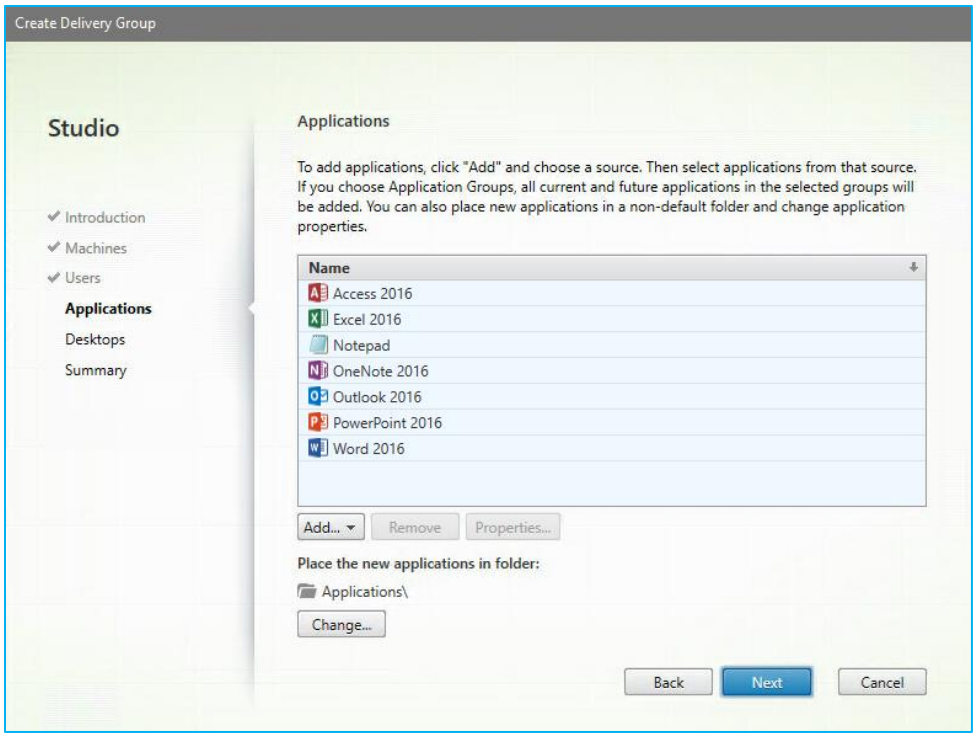
Click the checkbox next to each of the following applications to select them:

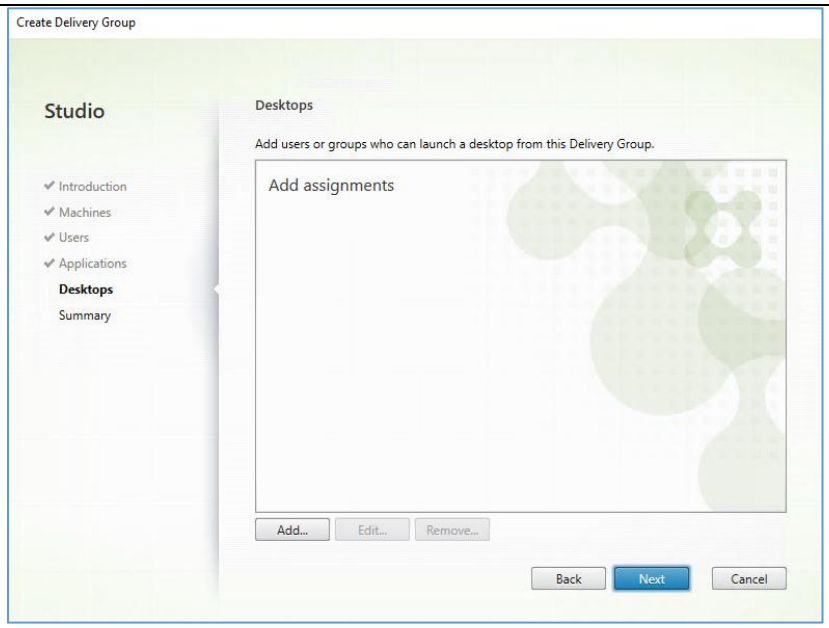
- **Access 2016**
- **Excel 2016**
- **Notepad**
- **OneNote 2016**
- **Outlook 2016**
- **PowerPoint 2016**
- **Word 2016**

Click **OK**.

Note: Other than Microsoft Office applications, you are only publishing the Notepad application from this Delivery Group.

Click **Next** to continue the Delivery Group creation wizard.

	 **Note**: The applications can take a while to populate, because the NYC-SRV-001 machine may have been powered off by the Controller to save on resource consumption. In order to return a list of the applications installed, the Controller has to call to the hypervisor hosting NYC-SRV-001 and have it powered on. Once powered on, the VDA will register with the Controller and send a list of installed applications to publish. **Note**: If this application list does not appear after five minutes, use XenCenter to verify that NYC-SRV-001 is powered on. **Note**: You can also add (create) applications manually by providing the executable path, working directory, optional command line arguments, and a display name visible to users in Receiver and administrators in Studio.
7.	On the Desktops page, click **Add**.



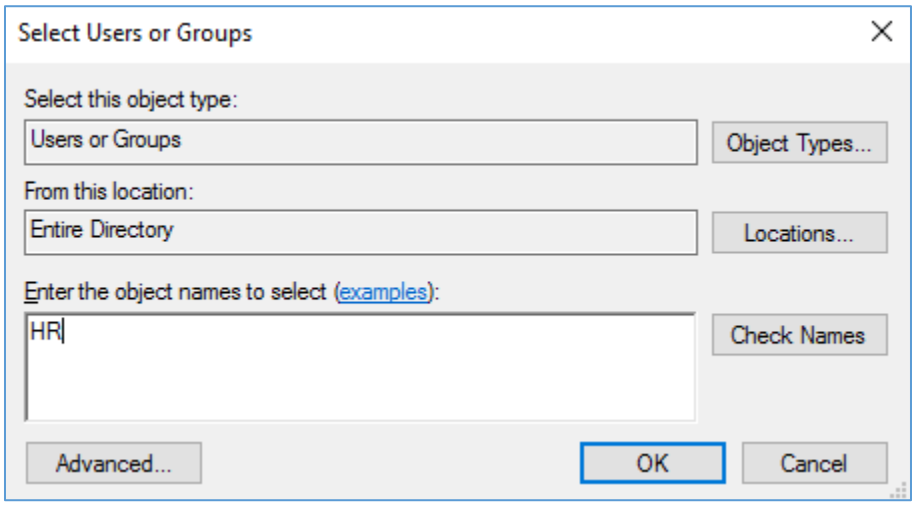
On the Add Desktop page, enter the following information:

- Display Name: **HR Desktop**
- Description: **Desktops for HR Group**

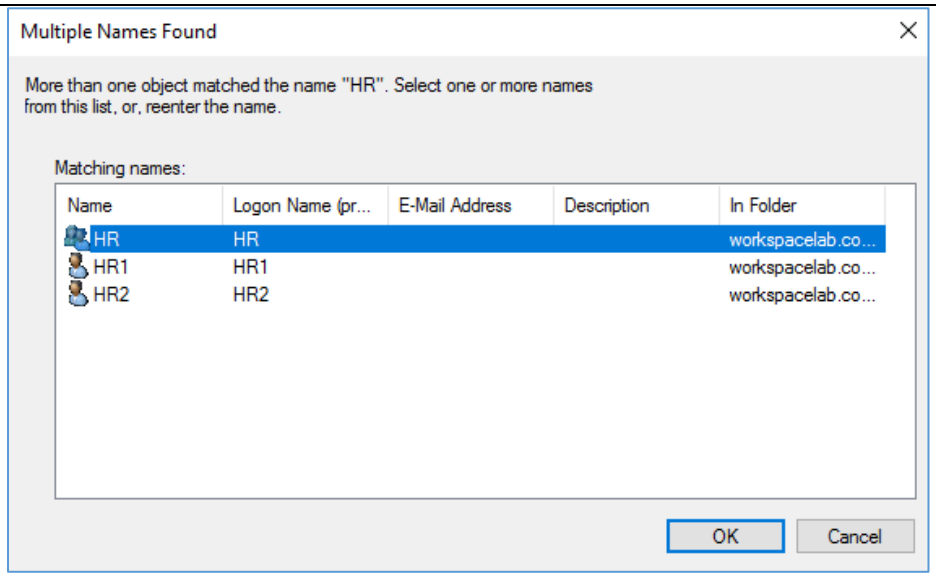
Select **Restrict desktop use to** and click **Add.**

Enter **HR** on the Select Users or Groups window.

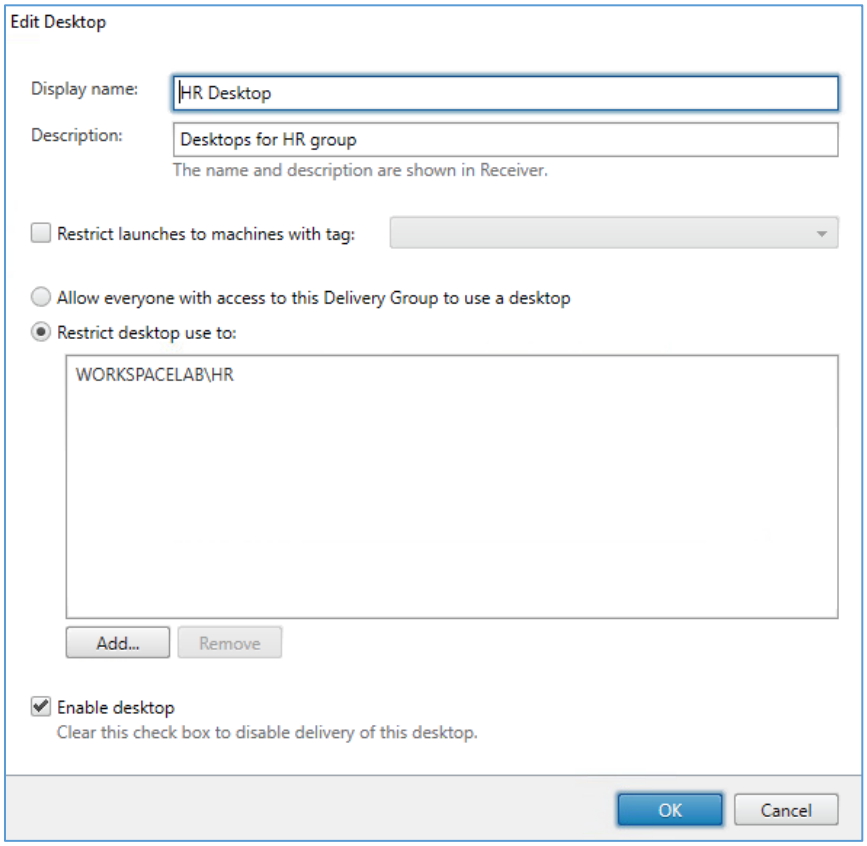
Click the **Check Names** button.



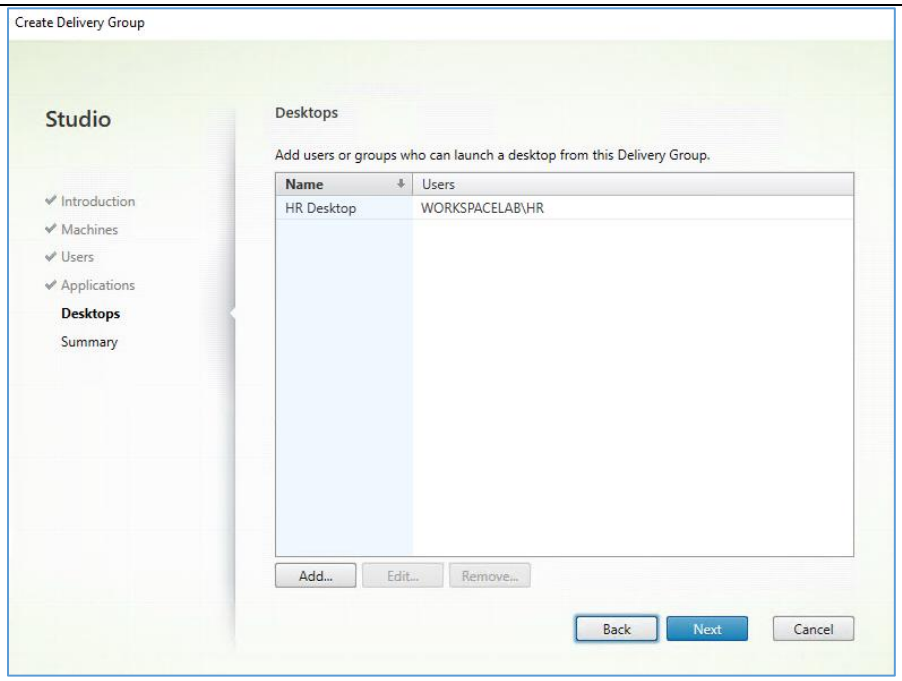
Click **OK** on the HR Group highlighted, and click **OK** on the Select Users or Groups dialog box.



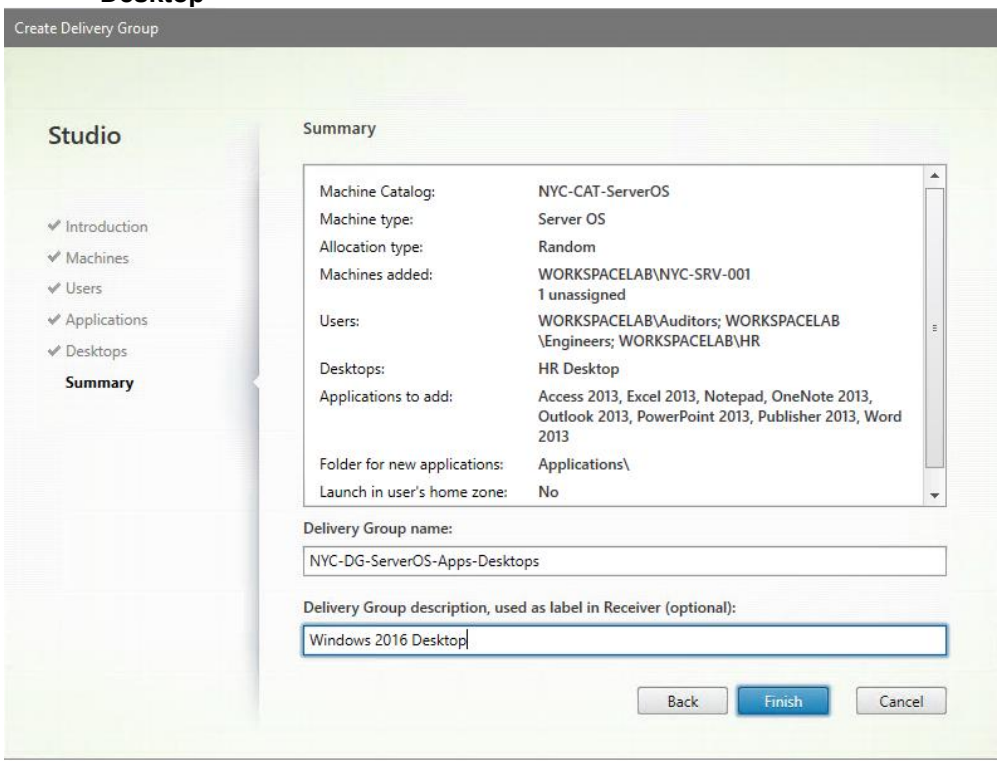
Click **OK** to close the Add Desktop page**.**



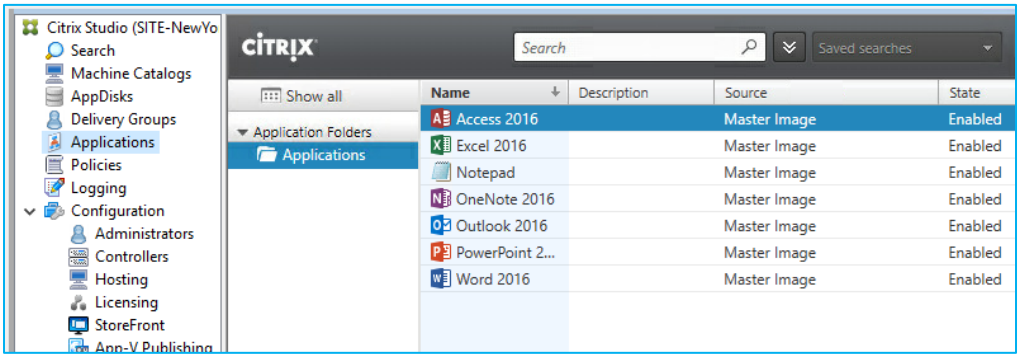
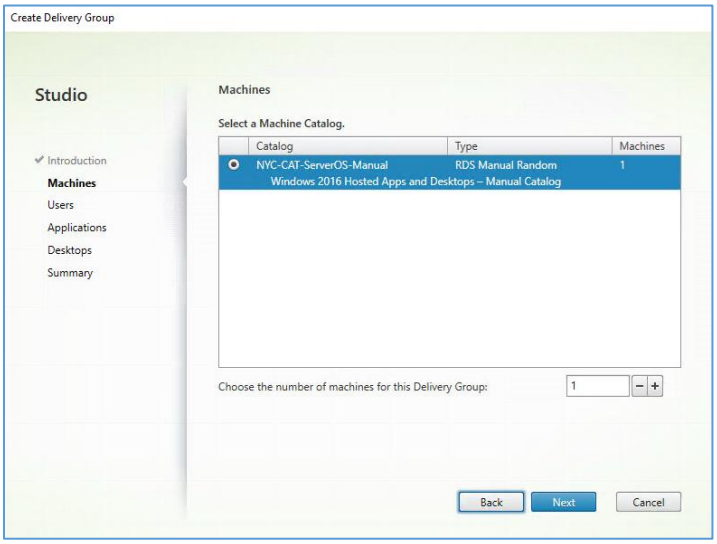
Click **Next** to continue the Delivery Group creation wizard.



8. On the Summary page, verify the previously configured information and enter the following:
   - Delivery Group name: **NYC-DG-ServerOS-Apps-Desktops**
   - Delivery Group description, used as label in Receiver (optional): **Windows 2016 Desktop**

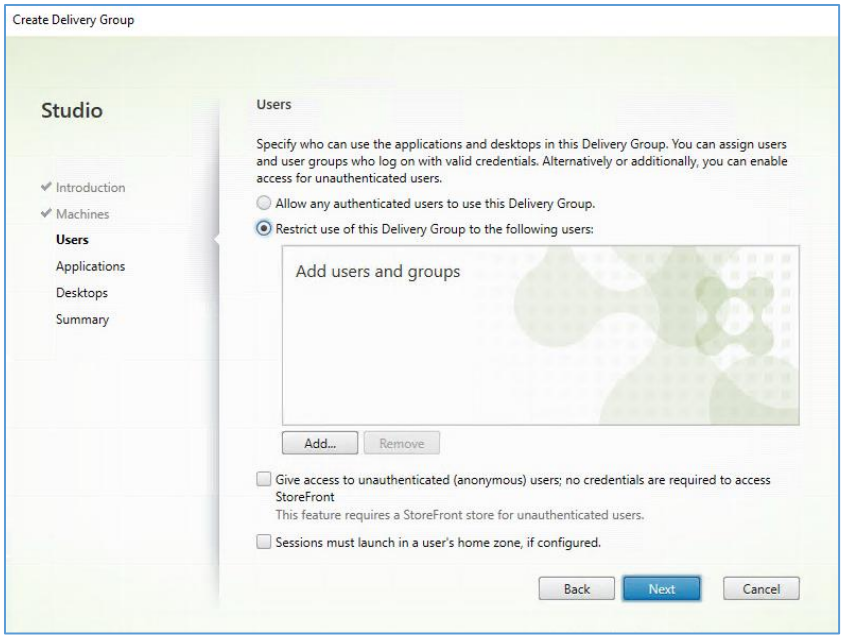


Click **Finish**.

	Note: The display name will appear for the published desktop and the application names will appear for each published application to the user, using Receiver.
9.	Verify that the applications selected during the Delivery Group creation wizard appear under the Applications node. Using Studio, select the **Applications** node in the left pane. Verify that you can see the following published apps: • **Access 2016** • **Excel 2016** • **Notepad** • **OneNote 2016** • **Outlook 2016** • **PowerPoint 2016** • **Word 2016** 
Creating the Second Delivery Group from Manually Created Catalog.	
10.	Click **Delivery Groups** on the left pane and on the right pane click **Create Delivery Group**.
11.	On the Introduction page, click **Next** to continue with Delivery Group creation wizard.
12.	On the Machines page, select **NYC-CAT-ServerOS-Manual**. Enter **1** in the Choose the number of machines for this Delivery Group field.  Click **Next** to continue the Delivery Group creation wizard.

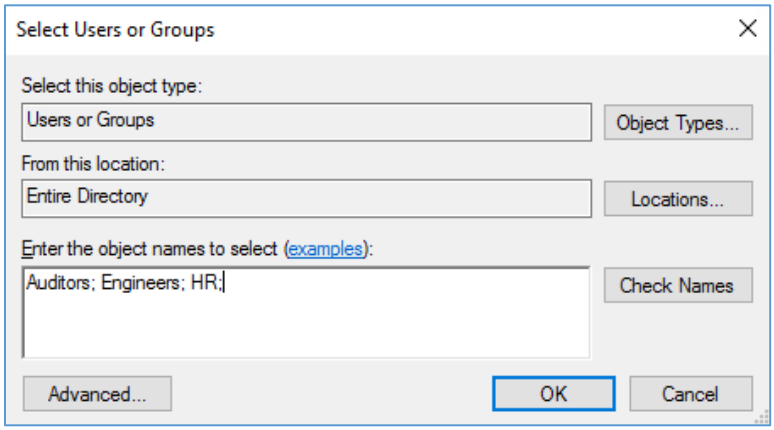
13. On the Users page, select **Restrict use of this Delivery Group to the following users**.

Click the **Add** button under the Add users and group's box.

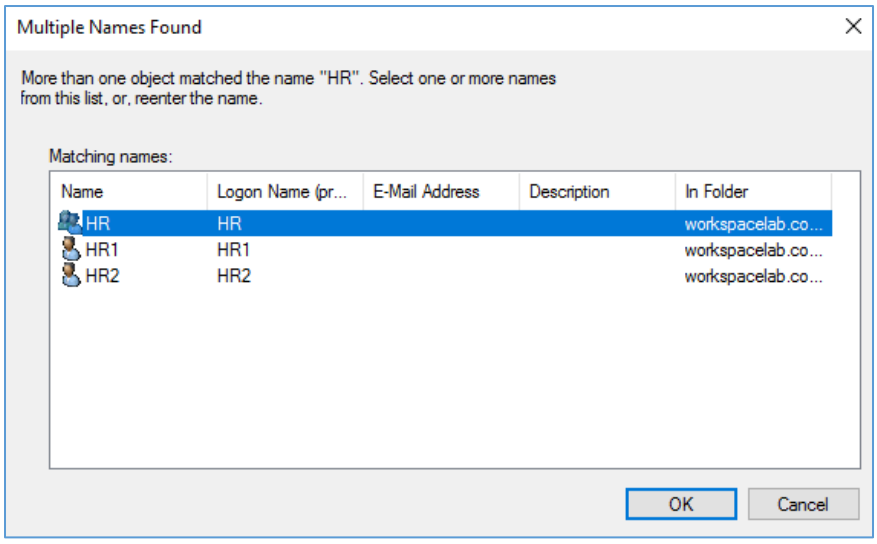


Enter **Auditors; Engineers; HR;** in the Select Users or Groups dialog box that appears.

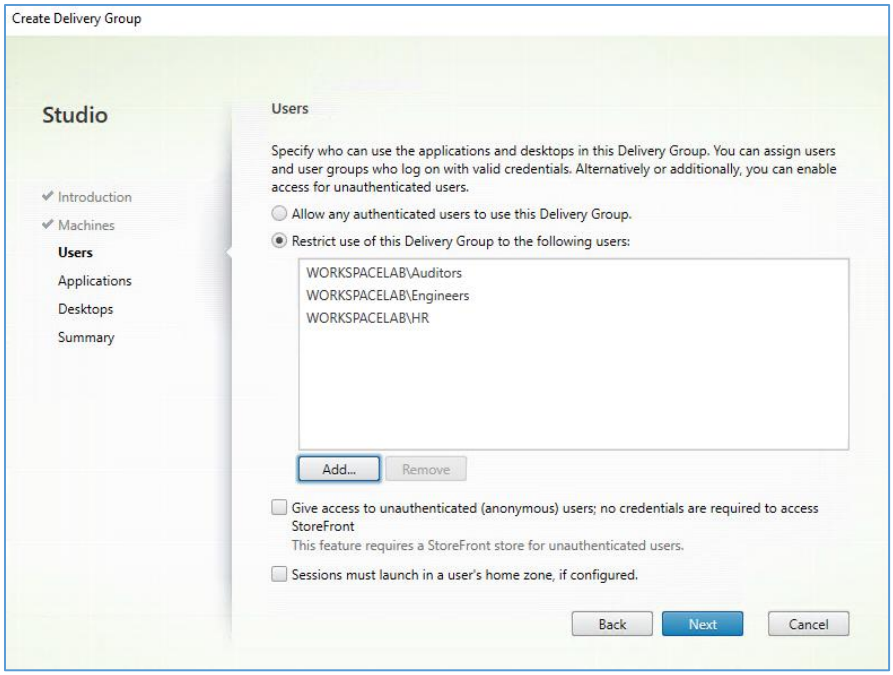
Click **Check Names**.



Click **OK** on the HR Group highlighted, and click **OK** on the Select Users or Groups dialog box.



Click **Next** to continue the Delivery Group creation wizard.



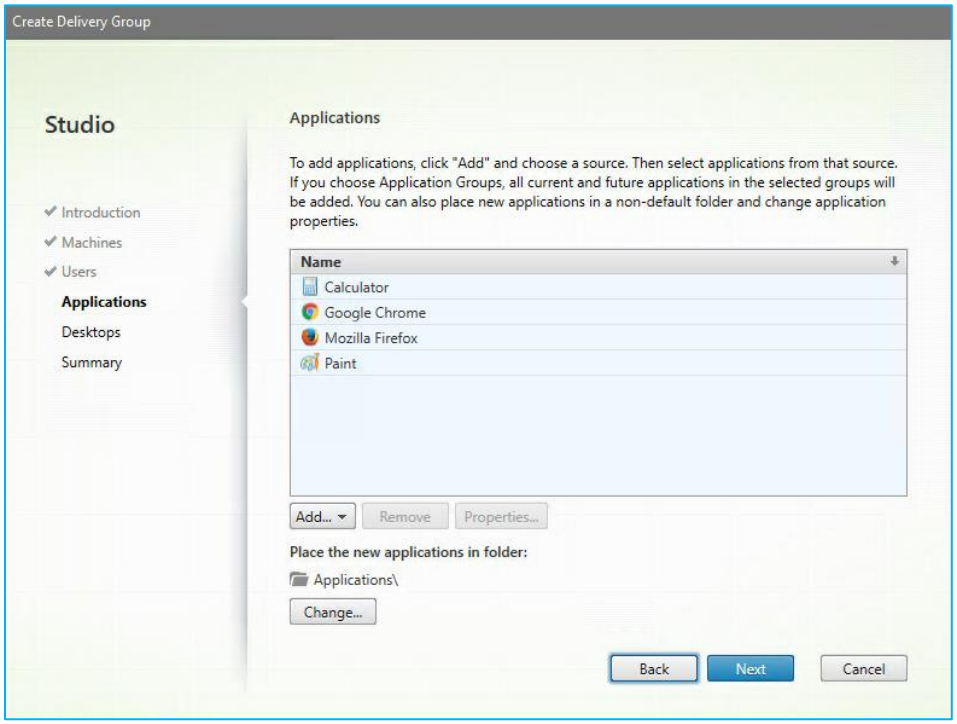
Note: The WW Labs design scope for this XenApp and XenDesktop POC deployment has specified these user groups in Active Directory for testing these published applications (as seen in the next step) for this POC.

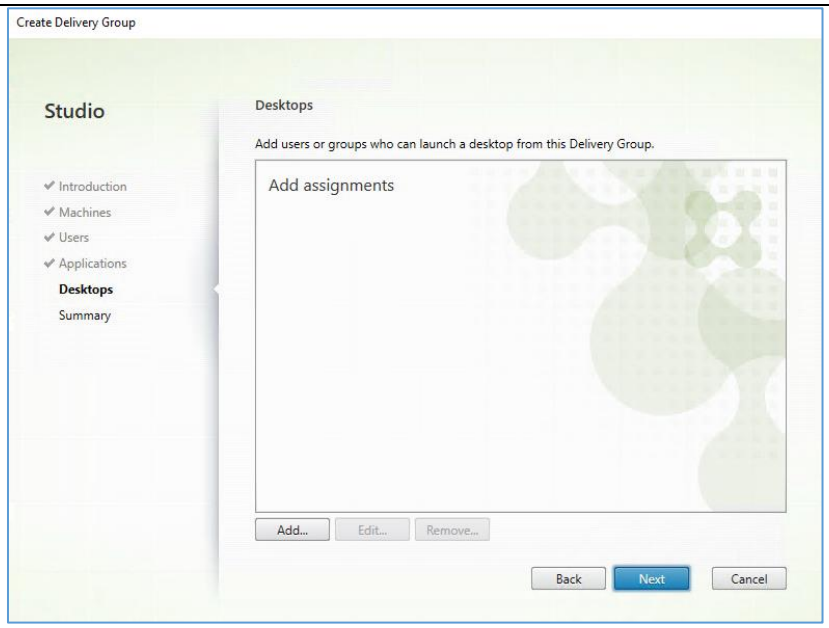
14. On the Applications page, click **Add** and select **From start menu**.

Note: The wizard will begin the process of discovering applications on NYC-MAN-001.

Click the checkbox next to each of the following applications to select them:

- **Calculator**
- **Google Chrome**
- **Mozilla Firefox**
- **Paint**

	Click **OK**. Click **Next** to continue the Delivery Group creation wizard.  **Note**: The applications can take a while to populate, because the Controller may have powered off the NYC-MAN-001 machine. In order to return a list of the applications installed, the Controller has to call to the hypervisor hosting NYC-MAN-001 and have it powered on. Once powered on, the VDA will send a list of installed applications to the Controller. **Note**: If this application list does not appear after five minutes, use XenCenter to verify that NYC-MAN-001 is powered on. **Note**: You can also add (create) applications manually by providing the path to the executable, working directory, any optional command line arguments and specifying a display name visible to users in Receiver and administrators in Studio.
15.	On the Desktops page, click **Add**.



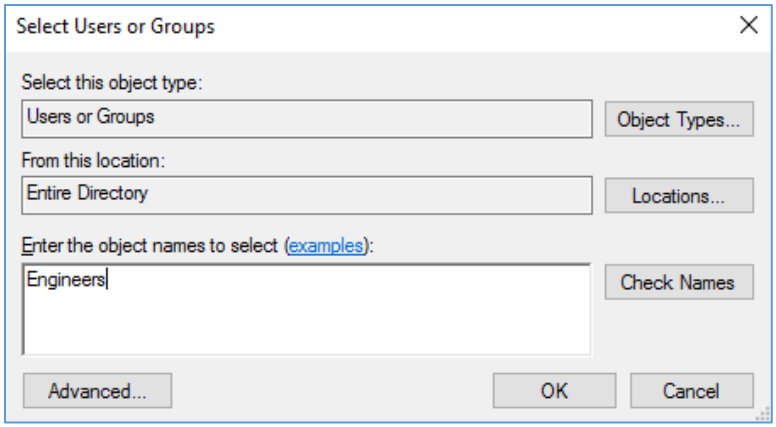
On the Add Desktop page, enter the following information:

- Display Name: **Engineer Desktop**
- Description: **Desktop for Engineers**

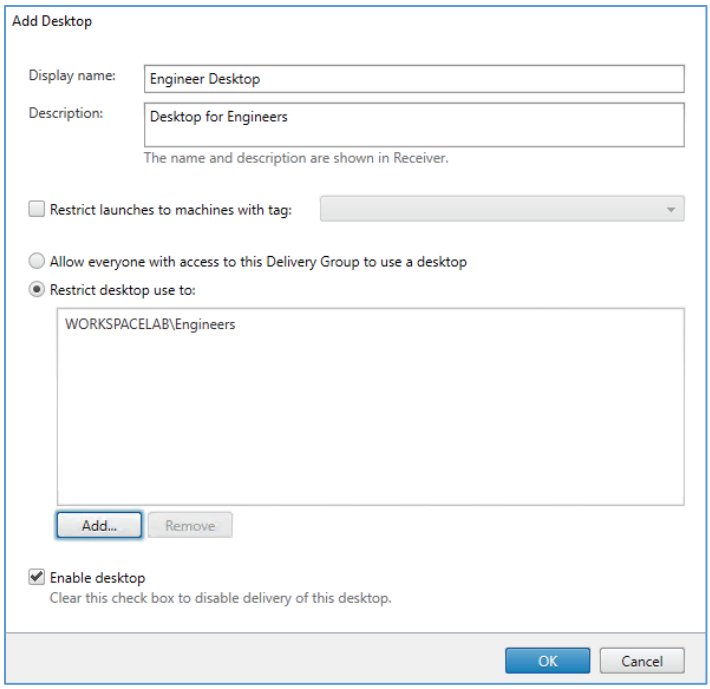
Select **Restrict desktop use to** and click **Add**.

Enter **Engineers** on the Select Users or Groups window.

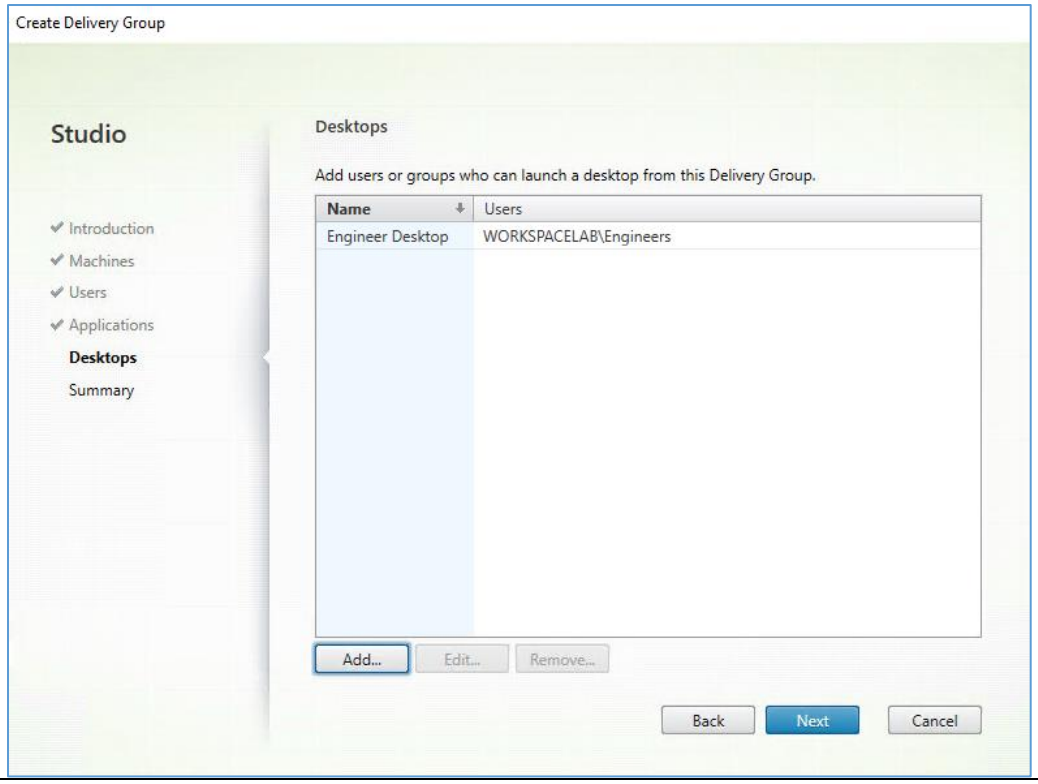
Click **Check Names** and then click **OK**.



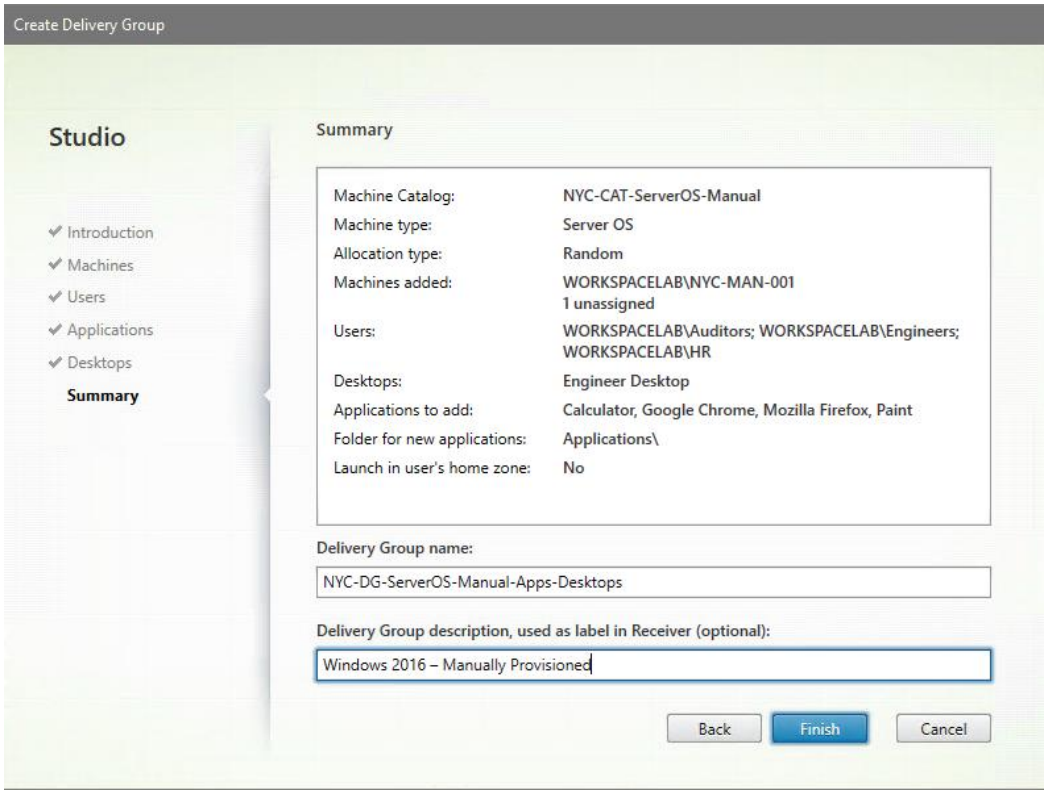
Click **OK** to close the Add Desktop page.



Click **Next** to continue the Delivery Group creation wizard.



16. On the Summary page, verify the previously configured information and enter the following:
    - Delivery Group name: **NYC-DG-ServerOS-Manual-Apps-Desktops**
    - Delivery Group description, used as label in Receiver (optional): **Windows 2016 – Manually Provisioned**

	 Click **Finish**. **Note**: The display name will appear for the published desktop and the application names will appear for each published application to the user.
17.	Verify that the applications selected during the Delivery Group creation wizard appear under the Applications node. Using Studio, select the **Applications** node in the left pane. Verify that you can see the following published apps in addition to previously published apps: • **Calculator** • **Google Chrome** • **Mozilla Firefox** • **Paint**

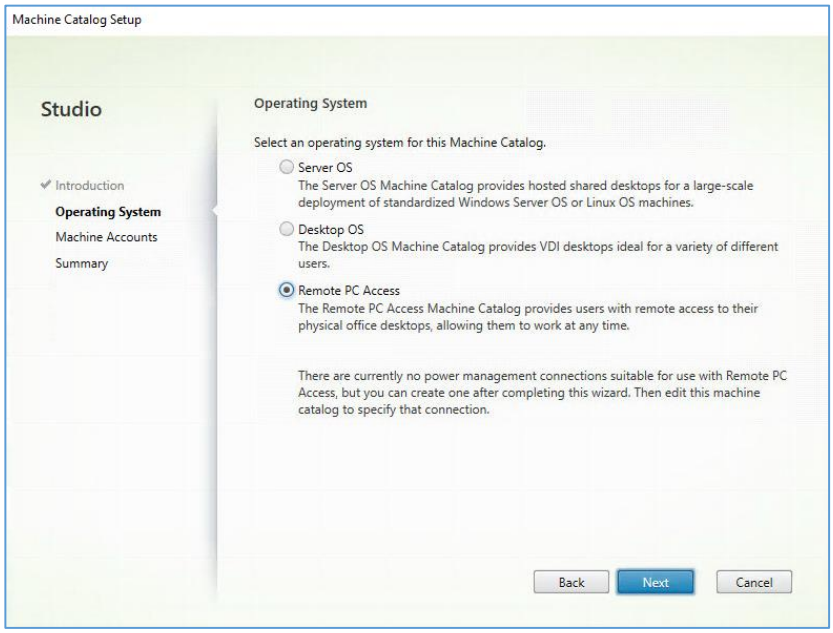
Key Takeaways:

- Use Delivery Groups to publish Desktops or Applications to users.
- A Delivery Group uses the machines from one or multiple Machine Catalogs of the same type.

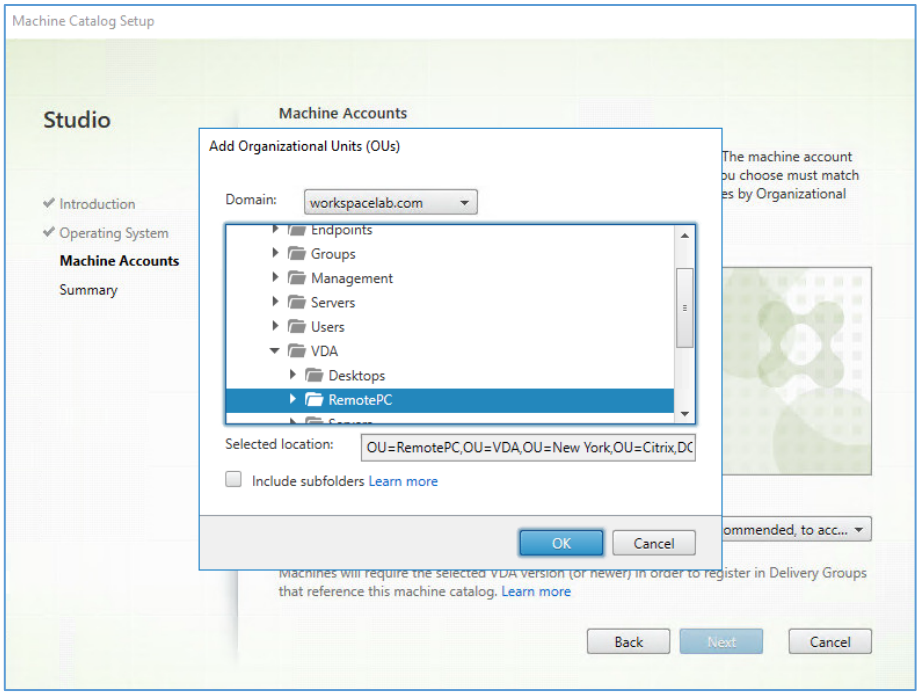
Exercise 4-5: Create a Machine Catalog for Remote PC

Scenario:

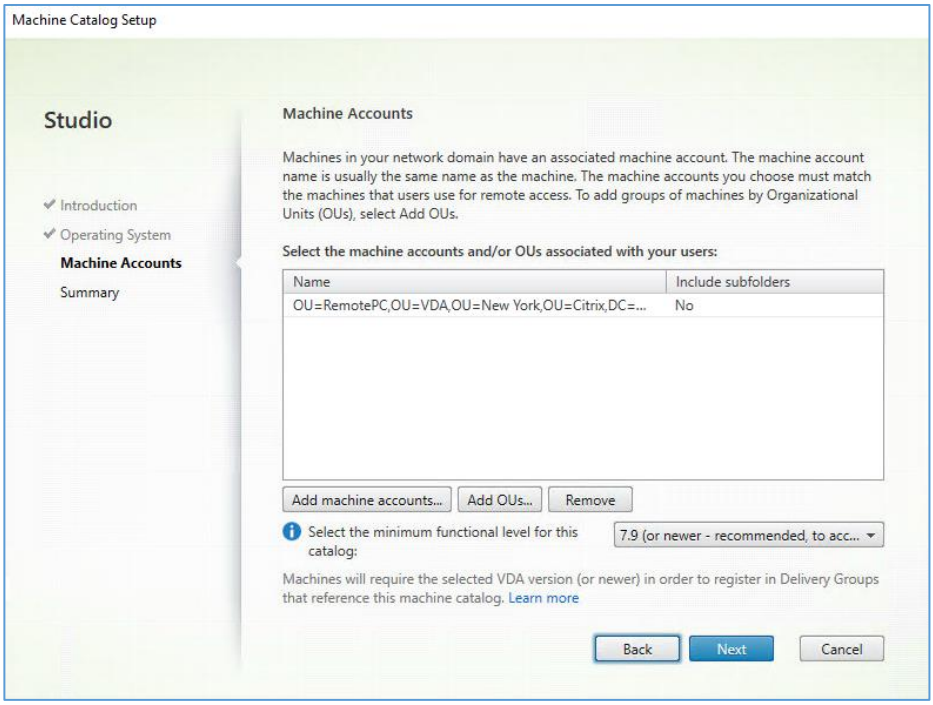
To further your action to deliver remote access to endpoints in the office running Windows, your task is to take a previously prepared Remote PC, by another administrator, and create a Machine Catalog.

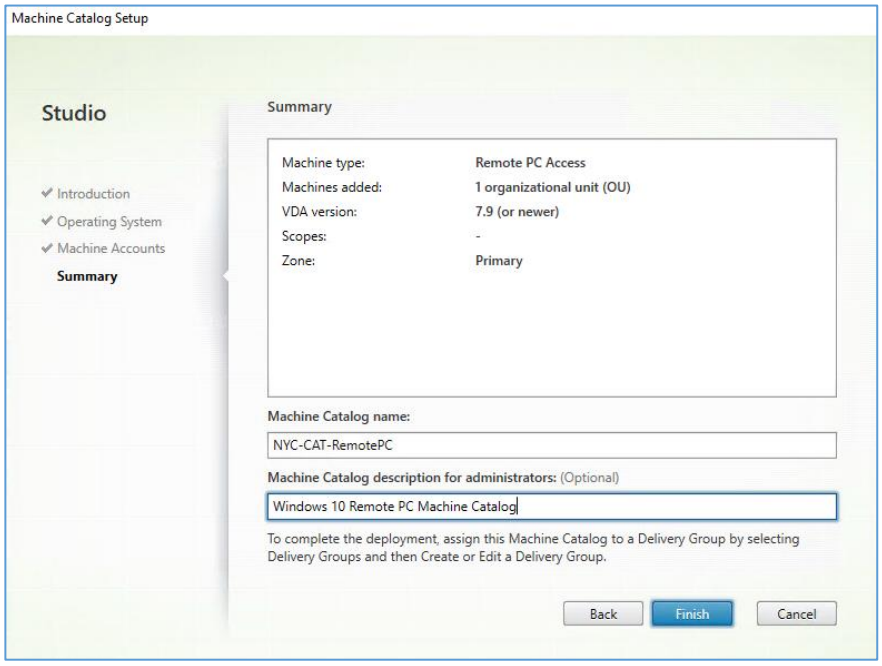
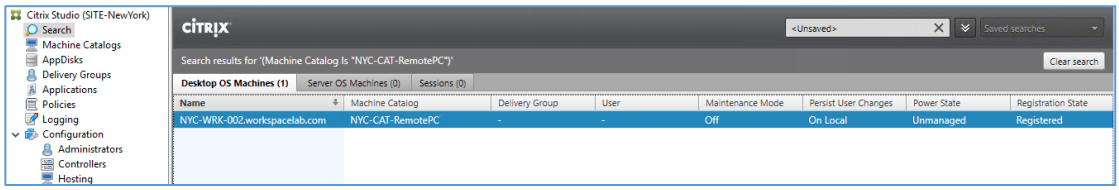
Step	Action
1.	Using the Remote Desktop Connection Manager, confirm that you are still connected to **NYC-XDC-001**. **Note**: In a previous exercise, you had logged on to NYC-XDC-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-XDC-001 by right-clicking this machine and selecting Connect server.
2.	Using Studio, expand **Citrix Studio (SITE-NewYork)** and click **Machine Catalogs**. From the Actions pane on the right side of the console, click **Create Machine Catalog**. **Note**: Studio was started in a previous exercise. If Studio was closed in a previous exercise, then click **Start > Citrix > Citrix Studio**.
3.	On the Introduction page, click **Next** to continue the Machine Catalog creation wizard. **Note**: Before you begin, make sure that you: • Identify the types of desktops and applications your users need. • Choose a Catalog infrastructure (for example, whether to power manage virtual machines). • Have a technology for creating and managing machines (such as Machine Creation Services or Provisioning Services). • Prepare your environment, including the Master Image, computer accounts, and network interface card configuration.
4.	On the Operating System page, select **Remote PC Access** and click **Next**. 
5.	On the Machine Accounts page, click the **Add OUs** button. Using the arrows, expand **Citrix > New York > VDA**.

Select the **RemotePC** Organizational Unit (OU) and click **OK** to close the Add Organizational Units window.



Click **Next** to continue the Machine Catalog creation wizard.



	Note: The RemotePC OU is the WW Labs location designated for physical endpoint machines running the Virtual Delivery Agent (VDA), used to host user apps and desktop resources.
6.	On the Summary Page, review the configurations and enter the following information: • Machine Catalog name: **NYC-CAT-RemotePC** • Machine Catalog description for administrators: **Windows 10 Remote PC Machine Catalog**  Click **Finish**. **Note**: Machine Creation Services (MCS) is not used to create this catalog because Remote PC Catalogs are intended to use existing endpoints to provide access rather than using virtual servers and desktops.
7.	Using Studio, verify that the Machine Catalog has been created. Click **Machine Catalogs** in the left pane of Studio. Verify that the **NYC-CAT-RemotePC** Machine Catalog displays in the middle pane.
8.	Using Studio, verify that the expected machine was successfully added to the NYC-CAT-RemotePC Machine Catalog. Right-click the **NYC-CAT-RemotePC** Machine Catalog and select **View Machines**. Verify that **NYC-WRK-002.workspacelab.com** displays. 

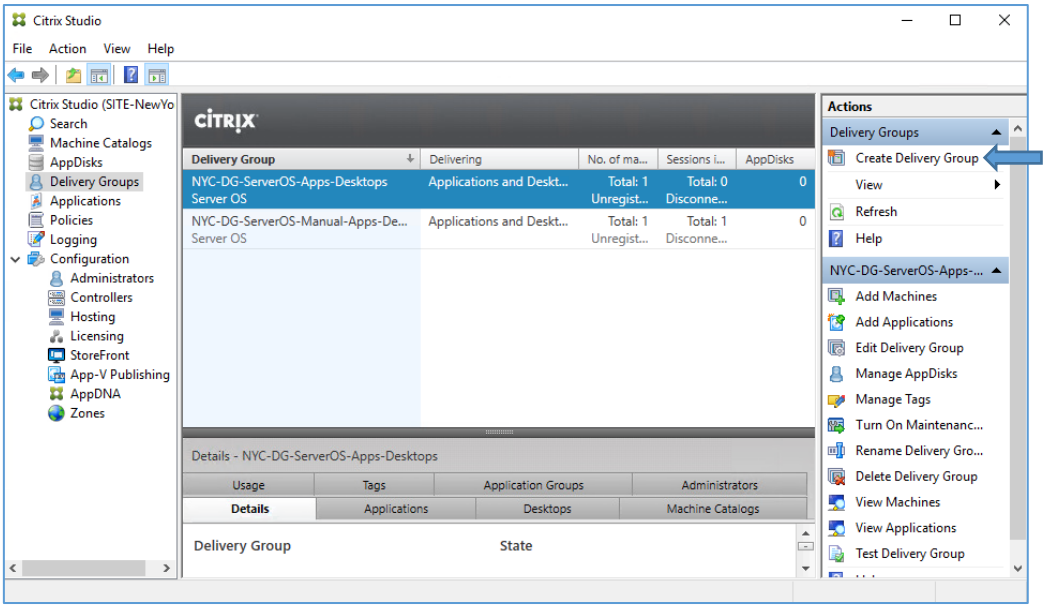
Key Takeaways:

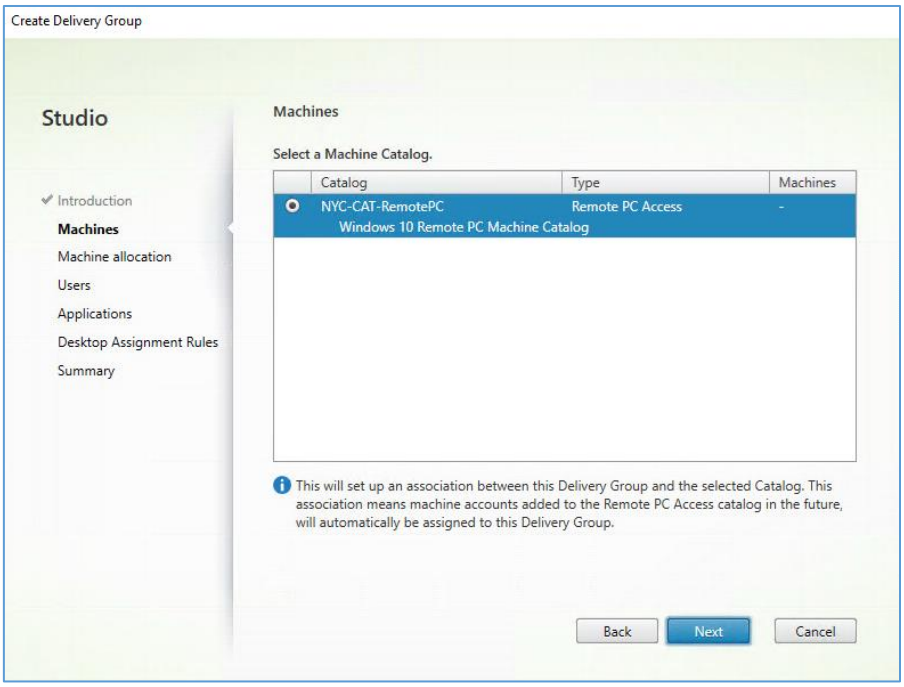
- The Remote PC Access Machine Catalog provides users with remote access to their physical office desktops, allowing them to work at any time.
- Add office PCs with the VDA component to a Machine Catalog to administer them with XenDesktop.

Exercise 4-6: Create a Delivery Group for Remote PC

Scenario:

Your task is to finish the delivery of endpoints running Windows to users by creating a Delivery Group to assign Remote PCs to a specific user group.

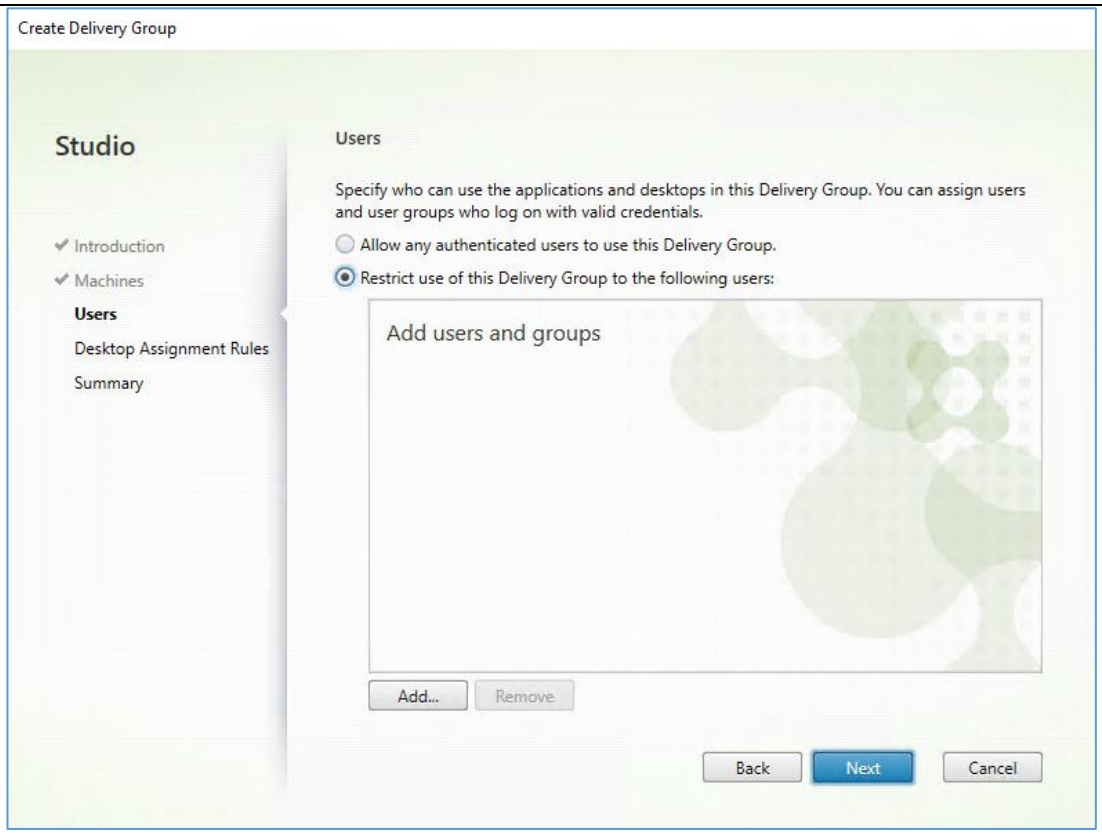
Step	Action
1.	Using the Remote Desktop Connection Manager, confirm that you are still connected to **NYC-XDC-001**. **Note:** In a previous exercise, you had logged on to NYC-XDC-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-XDC-001 by right-clicking this machine and selecting Connect server.
2.	Using Studio, expand **Citrix Studio (SITE-NewYork)** and click **Delivery Groups**. In the actions pane on the right side of the console, click **Create Delivery Group**.  **Note**: Studio was started in a previous exercise. If Studio was closed in a previous exercise, then click **Start > Citrix > Citrix Studio**.
3.	On the Introduction page, click **Next** to continue the Delivery Group creation wizard.
4.	On the Machines page, verify that the previously created Machine Catalog is listed. Select **NYC-CAT-RemotePC** and click **Next**.



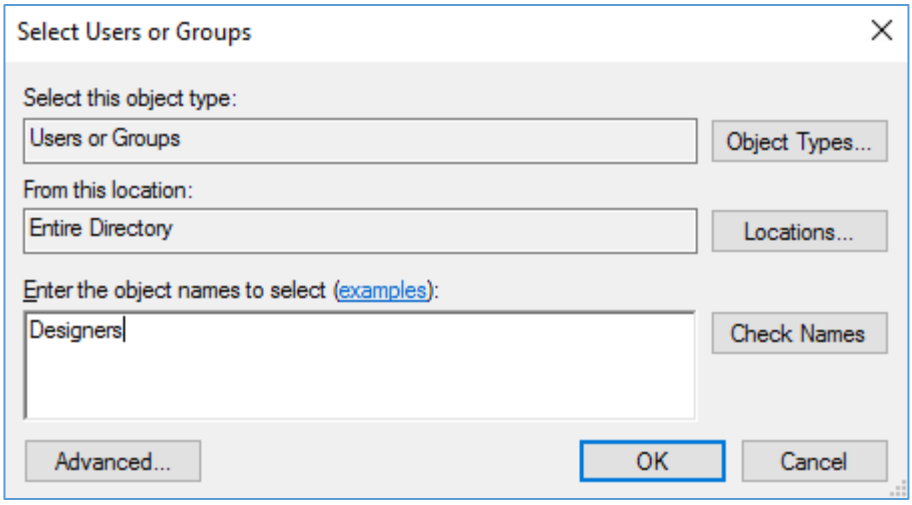
Note: Here it does not provide/require an additional step to select the number of VMs to add from a Machine Catalog to a Delivery Group. Remember, the Remote PC is an association configured between a Machine Catalog and a Delivery Group. When an association is established, machine accounts assigned to the Machine Catalog are automatically assigned to the associated Delivery Group.

5. On the Users page, configure this Delivery Group to assign a specific user group in Active Directory to the apps and desktops delivered.

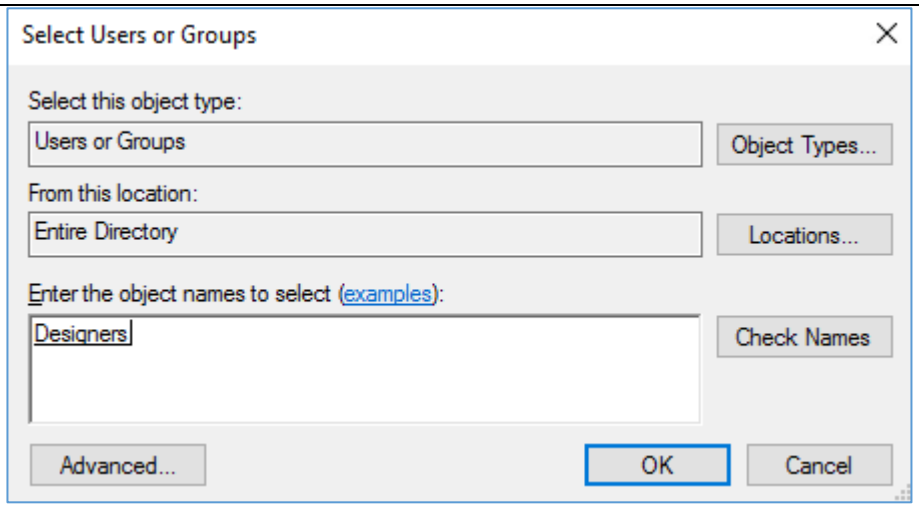
   Select **Restrict use of this Delivery Group to the following users** and click the **Add** button.



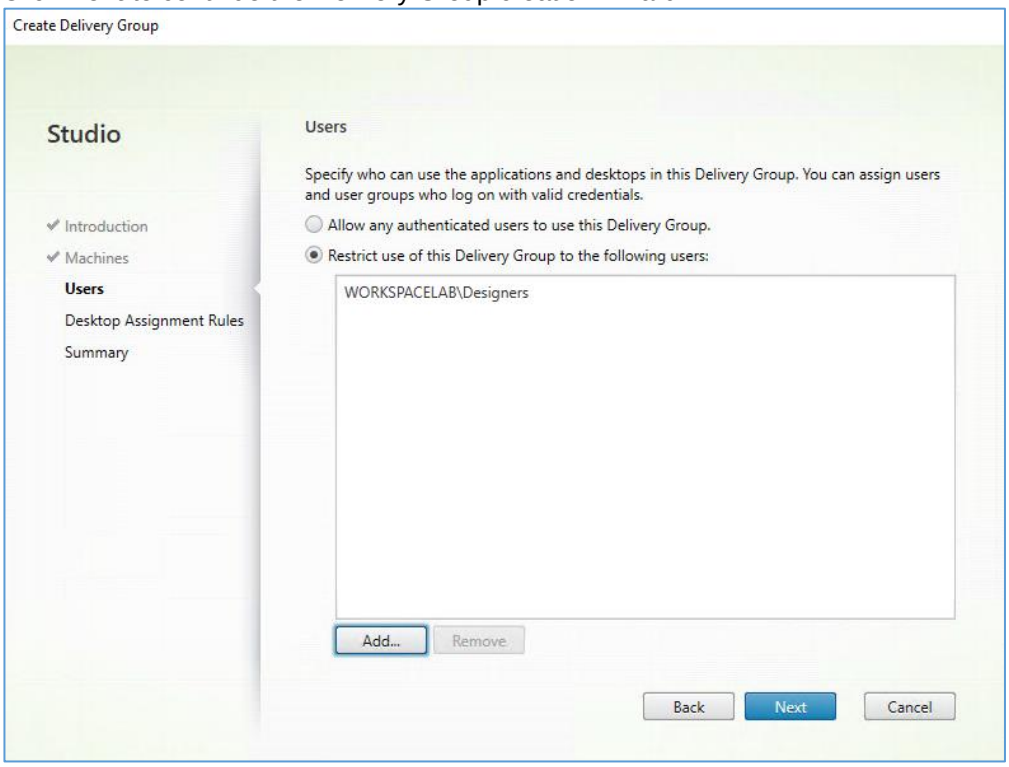
In the Select Users or Groups dialog box that appears, enter **Designers** and then click **Check Names**.



Click **OK** on the Select Users or Groups dialog box.



Click **Next** to continue the Delivery Group creation wizard.



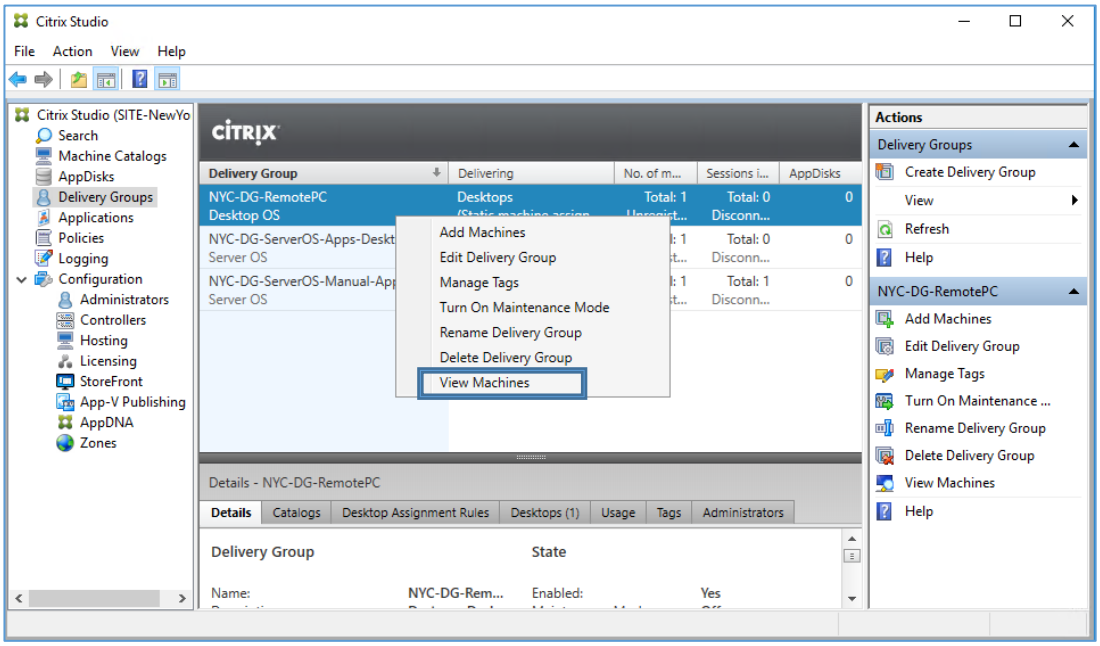
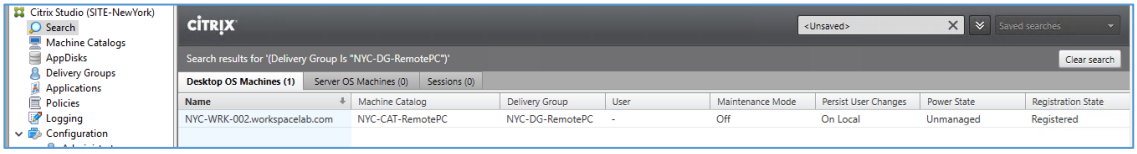
Note: The WW Labs design scope for this XenApp and XenDesktop POC deployment has specified this user group in Active Directory for testing Remote PC Access in this POC.

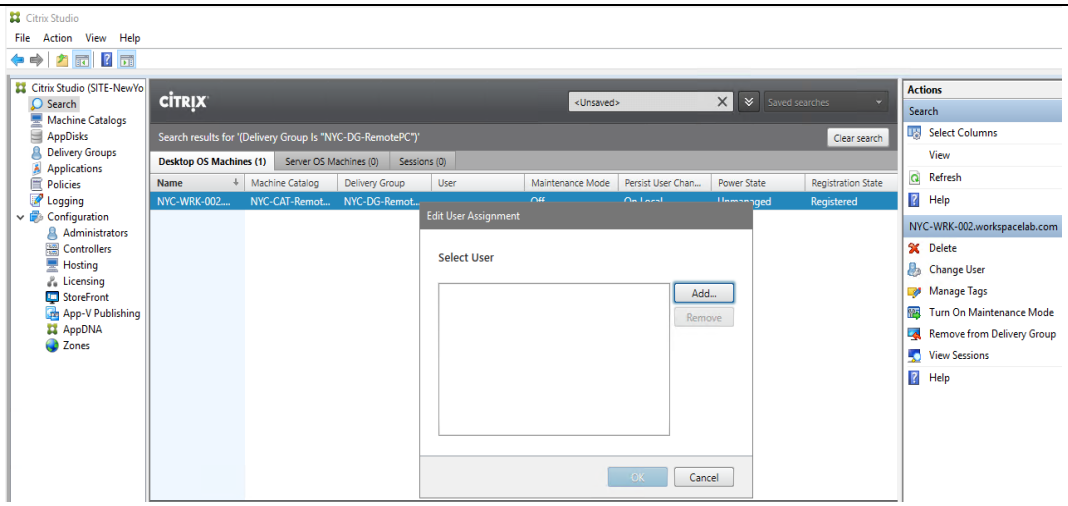
6. On the Desktop Assignment Rules page, click **Add** and enter the following details:
   - Display name: **Designer Desktop**
   - Description: **Remote PC Desktop**

   Click **Add**.

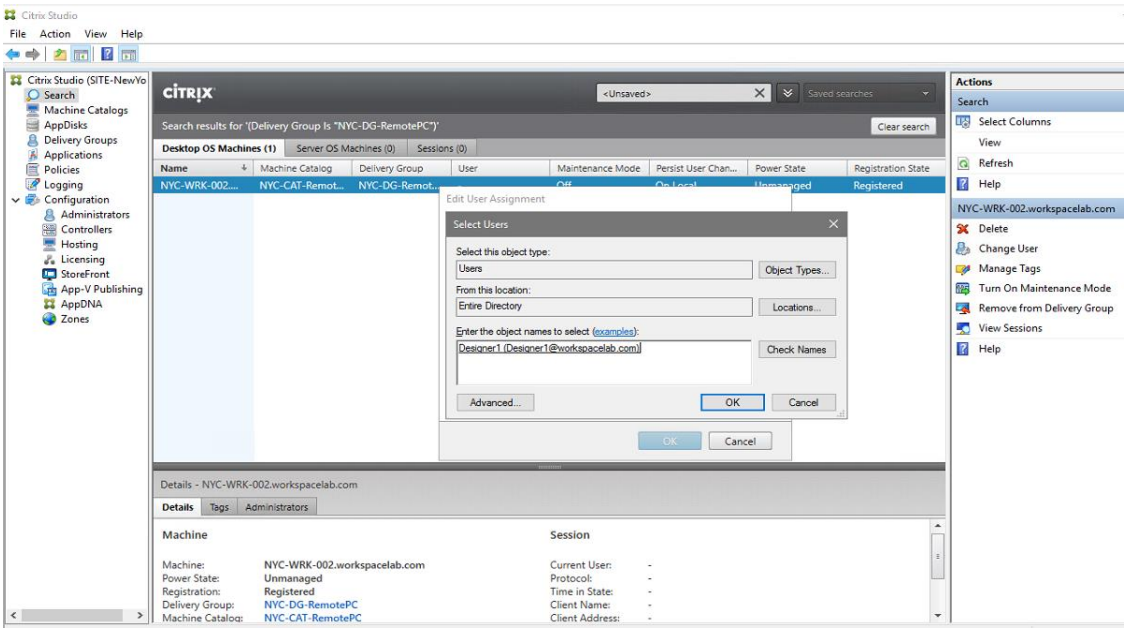
   In the Select Users or Groups dialog box that appears, enter **Designer1** and then click **Check Names**.

   Click **OK** twice to return to the Desktop Assignment Rules page and then click **Next**.

7.	On the Summary page, verify the configuration information and enter the following: • Delivery Group name: **NYC-DG-RemotePC** • Delivery Group description, used as label in Receiver (optional): **Remote PC Windows 10 Desktop For Designer1** Click **Finish**. **Note**: The display name for the published desktop will appear to the user.
8.	Verify that the Delivery Group was created and that NYC-WRK-002 has been successfully added to the Delivery Group. Using Studio, select the **Delivery Groups** node in the left pane. In the center pane, right-click the **NYC-DG-RemotePC** Delivery Group, and select **View Machines**.  Verify that **NYC-WRK-002.workspacelab.com** displays.  In the center pane, select **NYC-WRK-002.workspacelab.com**. From the right pane, under NYC-WRK-002, click **Change User** and click **Add**.



Type **Designer1**, click **Check Names**, and then click **OK**.



Click **OK** to accept the user assignment.

Key Takeaways:

- When providing applications or desktops from Remote PC Access Catalogs, all machines in the Catalog are associated with the Delivery Groups at once.

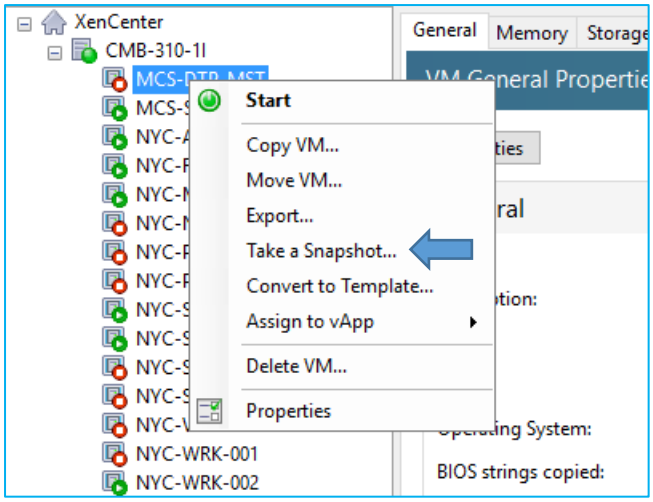
Exercise 4-7: Create a snapshot of the Desktop OS VM

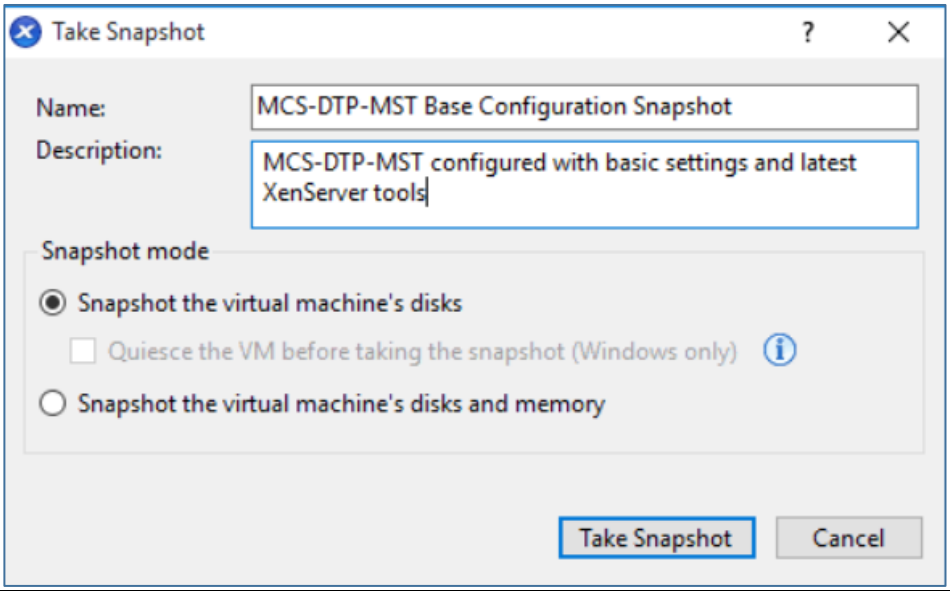
Scenario:

Your Lead Citrix Architect has explained that one of the common management tasks when administering a XenApp and XenDesktop environment that primarily uses virtual machines to host user resources is to take and manage snapshots.

Your task is to create a snapshot of the Desktop OS you previously used in the creation of a Machine Catalog.

If there is no snapshot present, the Machine Creation Services process will automatically create one snapshot of the VM while creating the catalog. This exercise is to become familiarized on how to create a snapshot manually from XenCenter.

Step	Action
1.	Using XenCenter, perform a Snapshot on MCS-DTP-MST. In XenCenter, right-click **MCS-DTP-MST** in the left pane and select **Shutdown**. Click **Yes** to confirm shutdown of the VM. **Note**: You can perform a snapshot on a running virtual machine, but it is a good practice to shut down a VM when using the snapshot as a platform to create other machines. Once shut down, right-click **MCS-DTP-MST** and select **Take a Snapshot**.  **Note**: XenCenter should already be open and authenticated to the hypervisor host. If not, using the Student Desktop, launch Citrix XenCenter. If the hypervisor host does not automatically connect, use your Training.Citrix.Com (TCC) connections page to obtain the IP address and password to connect and then, using XenCenter, click on Add a Server.
2.	In the Take Snapshot dialog box, enter the following text into the appropriate fields: • Name: **MCS-DTP-MST Base Configuration Snapshot** • Description: **MCS-DTP-MST configured with basic settings and latest XenServer tools**. Click **Take Snapshot**.

	Note: The name and description used here is only to represent that we have created a base configuration. When creating a base image in a production environment, more software and settings would typically be included. 
3.	In the XenCenter console for MCS-DTP-MST, click on the **Snapshots** tab on the right side of the console. Verify that the **MCS-DTP-MST Base Configuration Snapshot** created in the previous step is present.

Key Takeaways:

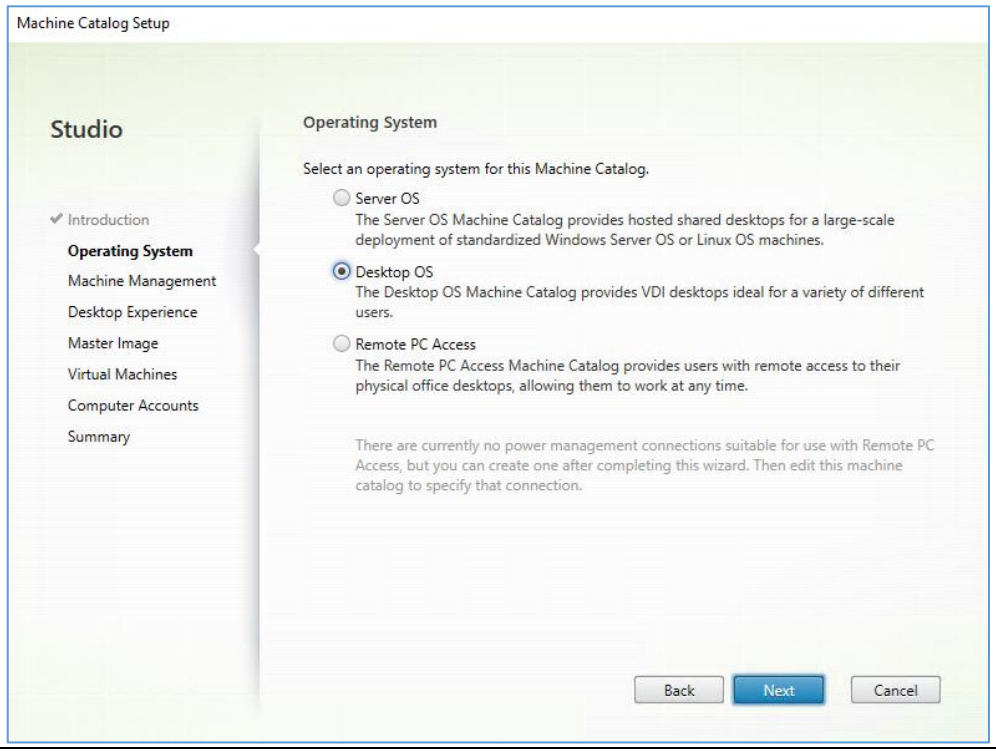
- Snapshots provide access to point-in-time copies of virtual machines.
- Ensure to keep the length of the snapshot chain to less than 30 (on XenServer).

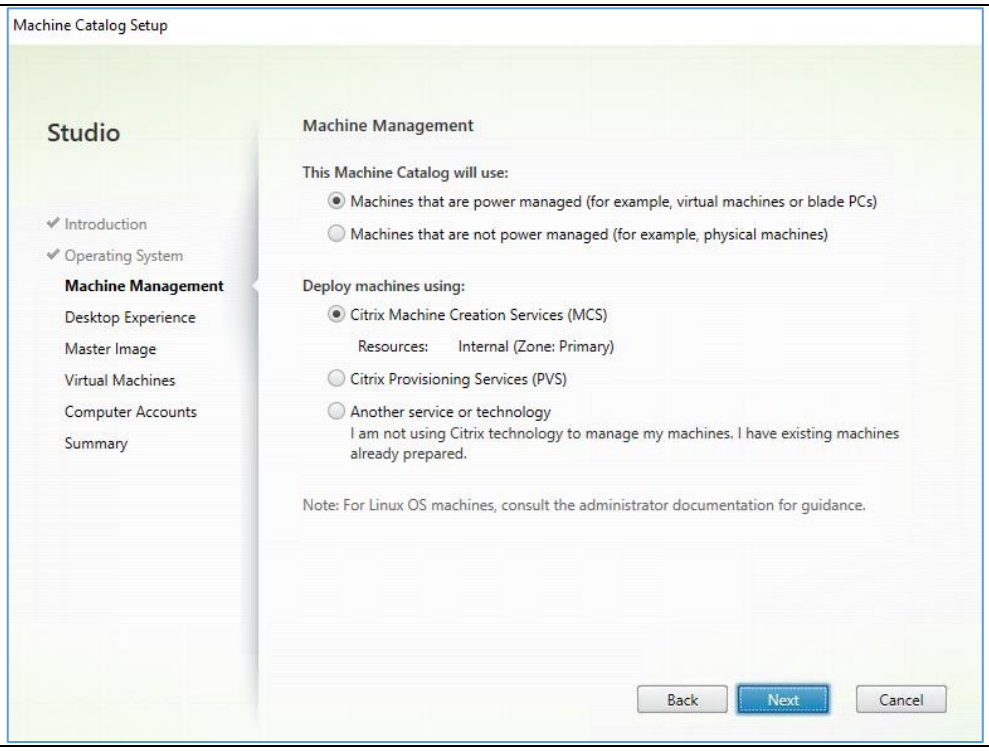
Exercise 4-8: Create Machine Catalog for Desktop OS

Scenario:

You have already used Machine Creation Services (MCS) to create a Machine Catalog for Server OS. During that process, you used a Server OS Machine as the Machine Catalog master image. Your task now is to use MCS to create a Machine Catalog for Desktop OS using a virtual machine snapshot.

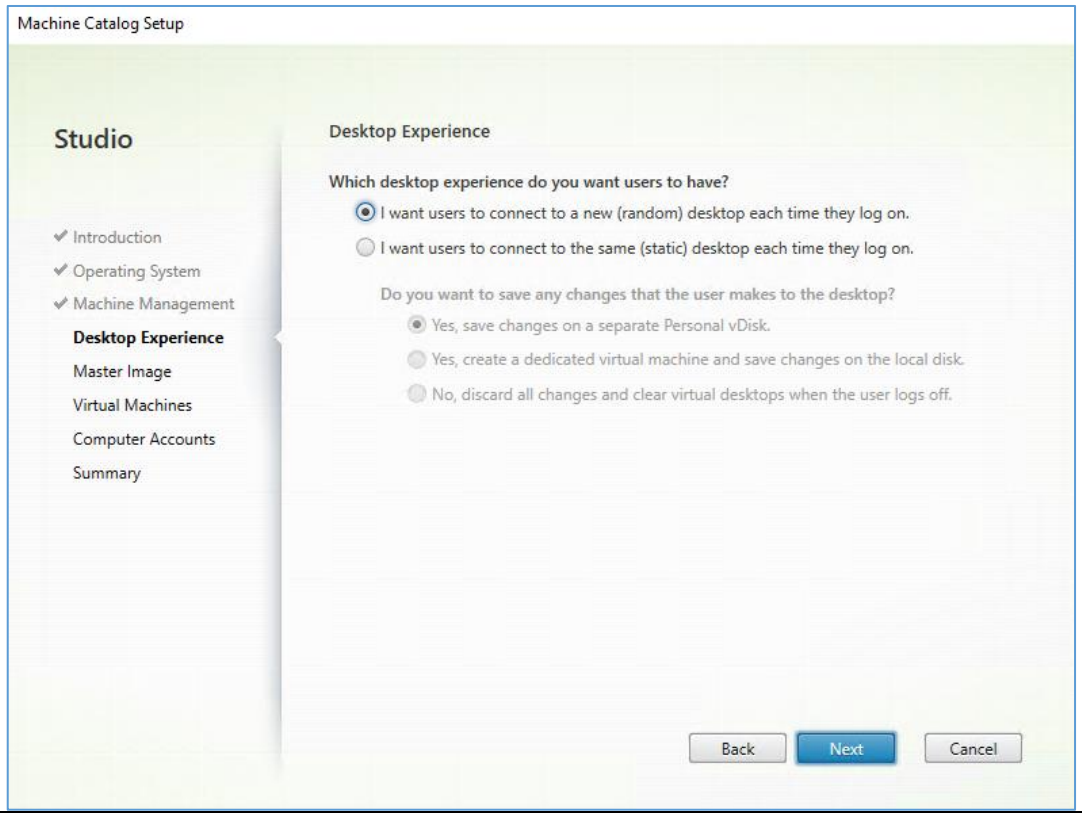
Step	Action
1.	Using the Remote Desktop Connection Manager, confirm that you are still connected to **NYC-XDC-001**. **Note**: In a previous exercise, you had logged on to NYC-XDC-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-XDC-001** by right-clicking this machine and selecting Connect server.
2.	Using Studio, expand **Citrix Studio (SITE-NewYork)** and click **Machine Catalogs**.

	From the Actions pane on the right side of the console, click **Create Machine Catalog**.
3.	On the Introduction page, click **Next** to continue the Machine Catalog creation wizard.
4.	On the Operating System page, select **Desktop OS** and click **Next** to continue the Machine Catalog creation wizard. 
5.	On the Machine Management page, verify that the following options are selected: • **Machines that are power managed (for example, virtual machines or blade PCs)** • **Citrix Machine Creation Services (MCS)** Click **Next** to continue the Machine Catalog creation wizard.

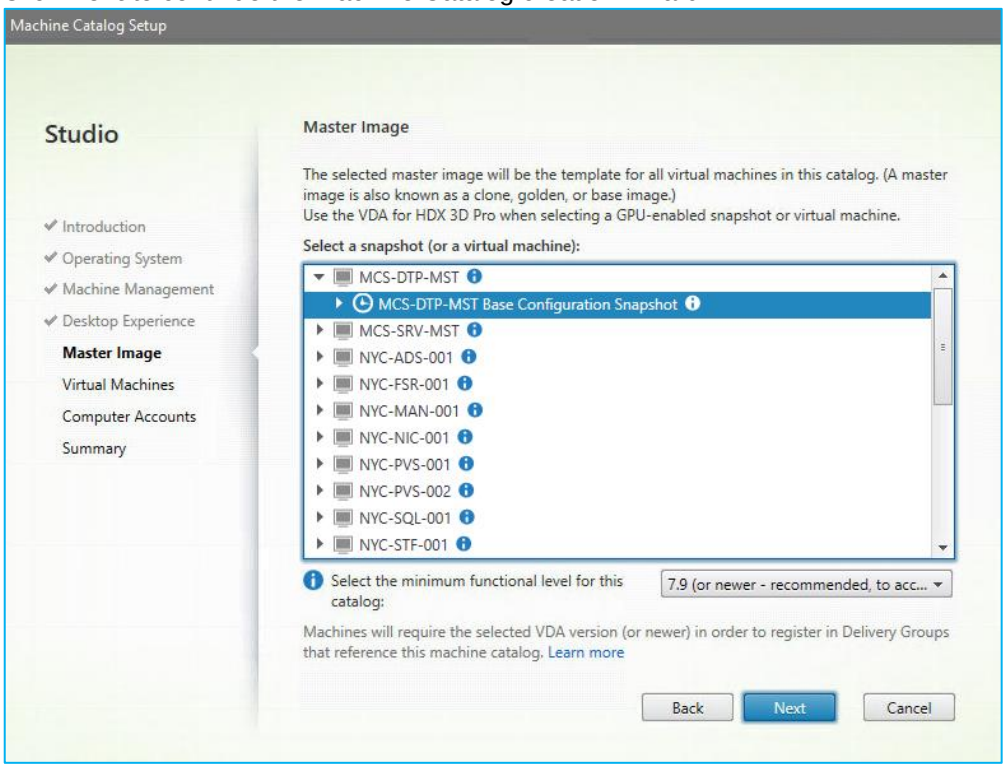


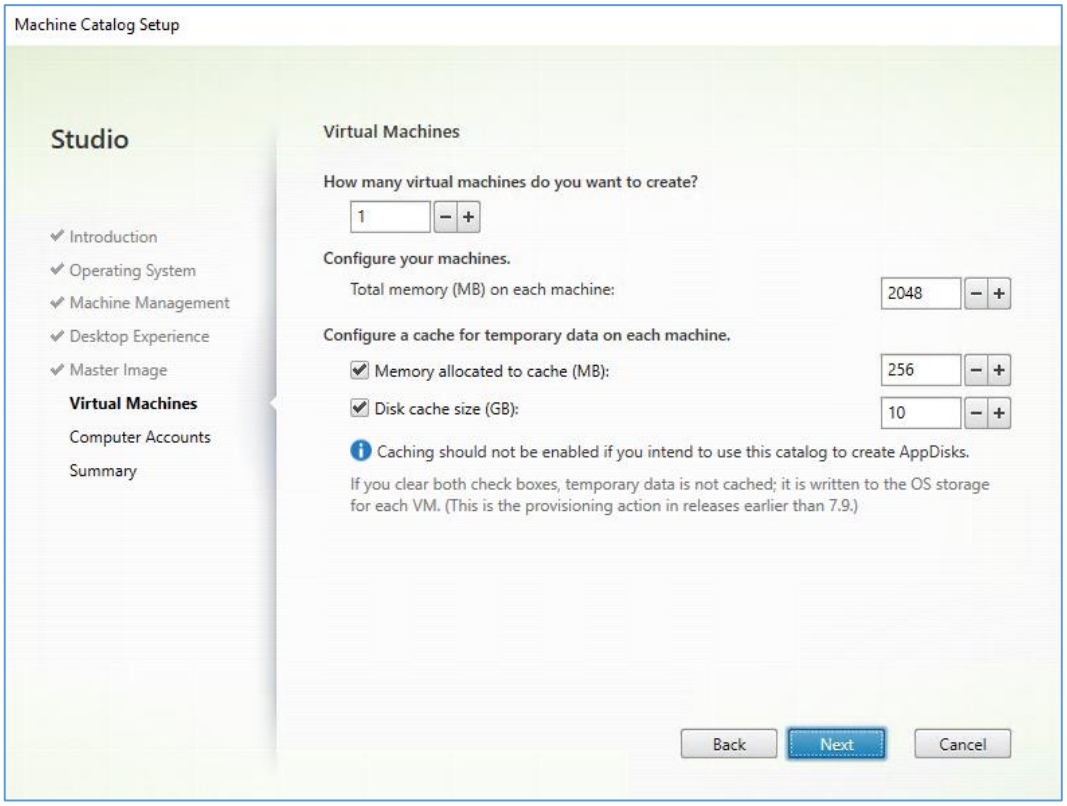
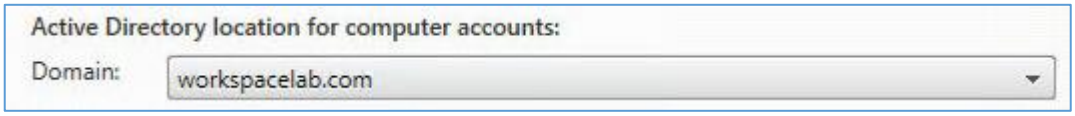
6. On the Desktop Experience page, select **I want users to connect to a new (random) desktop each time they log on**.

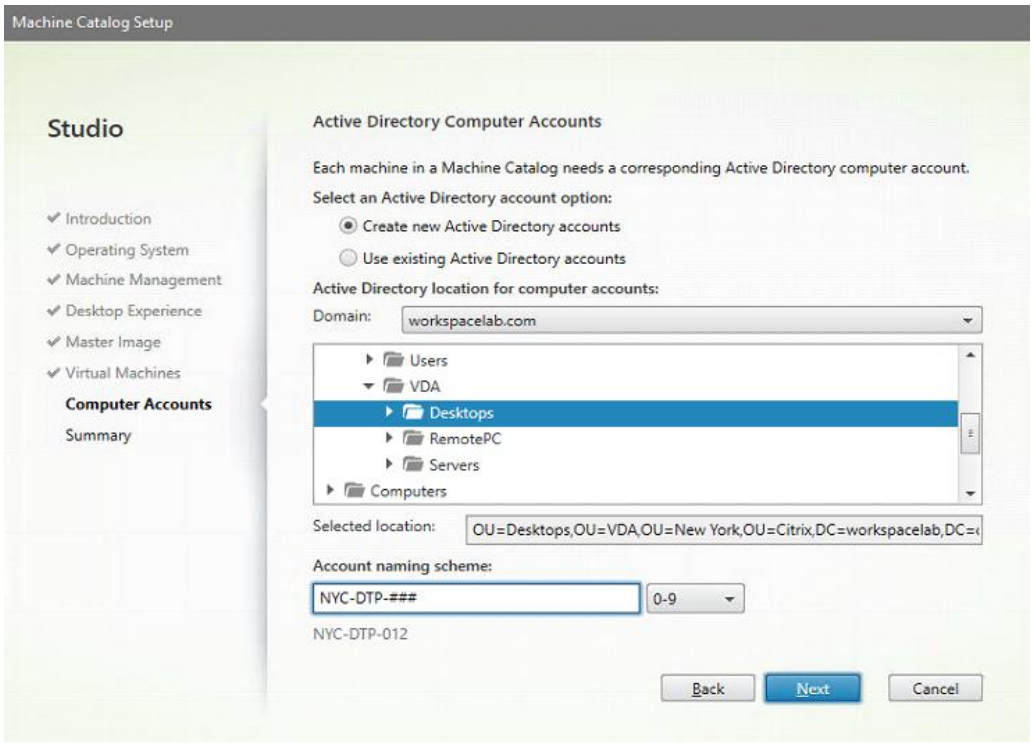
   Click **Next** to continue with Machine Catalog creation wizard.

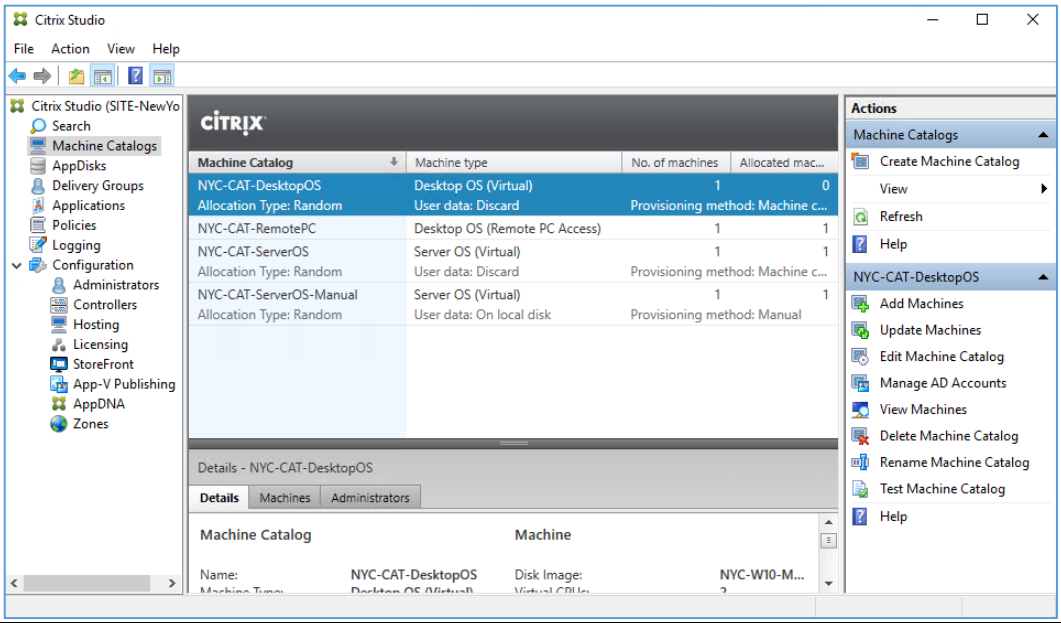
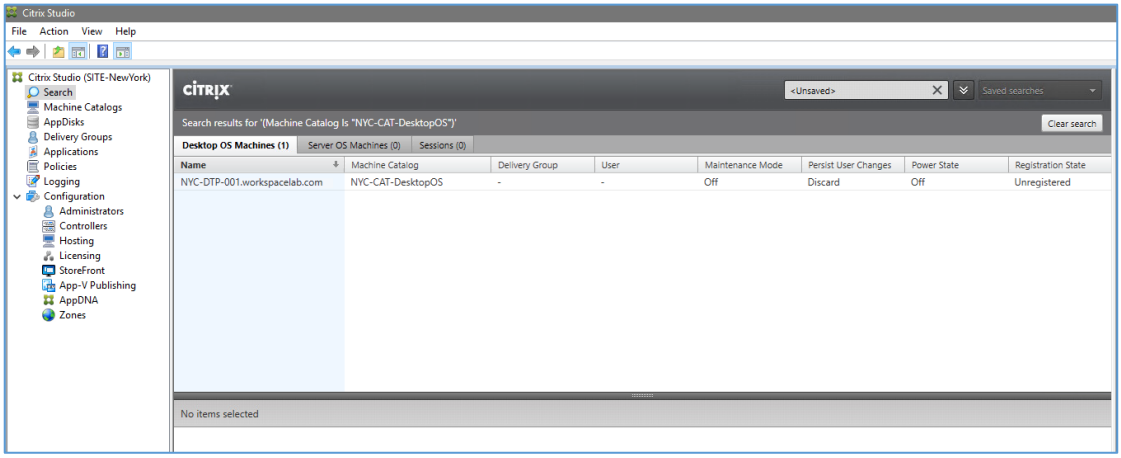


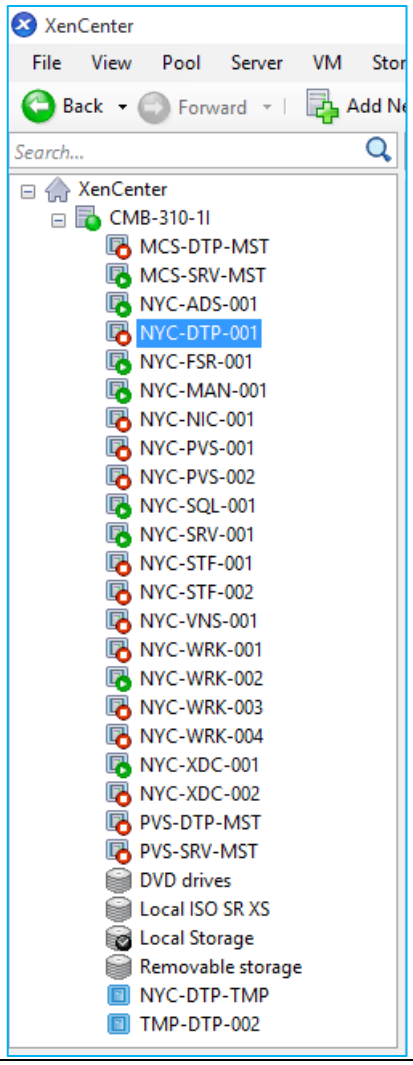
	Note: Unlike Server OS Machine Catalog, there are multiple options to select how the desktops are delivered with Desktop OS Machine Catalog:
	• **Random**: A new machine is given to the user every time a connection is made from the pool of available machines and changes done by the user are lost on reboot.
	• **Static**: Machine is assigned to the user who logs on to the machine first. Changes are saved depending on the option selected:
	  ○ **Personal vDisk**: Changes are saved on the additional disk that is attached to each VM when the catalog is created. Changes stored in the Personal vDisk are not erased.
	  ○ **Dedicated**: Changes are saved on the differencing disk and are not lost on reboots.
	  ○ **Pooled Static**: Changes are not saved after a reboot, but the user gets the same machine every time since the Static type is selected.

7.	On the Master Image page, expand **MCS-DTP-MST** and select **MCS-DTP-MST Base Configuration Snapshot**. **Note**: This snapshot is the snapshot created in the previous exercise. Verify that **7.9 (or newer recommended, to access the latest features)** is selected. **Note**: This is the version of the Virtual Delivery Agent (VDA) installed on the master machine for this Machine Catalog. Click **Next** to continue the Machine Catalog creation wizard.  **Note**: In an earlier exercise, you created a Machine Catalog for a Server OS, using a virtual machine as the master machine. Machine Creation Services (MCS) supports the use of either a virtual machine or a virtual machine snapshot to be used as the master machine or image to create the Machine Catalog. When using a snapshot as the master image, you should

	consider naming the snapshot, because when the MCS process runs, a snapshot is created by Studio and a name is assigned that you cannot change.
8.	On the Virtual Machines page, enter the following configuration values: • Number of virtual machines needed: **1** • Memory (MB): **2048** • Memory allocated to cache (MB): **256** • Disk cache size (GB): **10**  Click **Next** to continue the Machine Catalog creation wizard.
9.	On the Computer Accounts page, verify that the **Create New Active Directory accounts** radio button is selected. In the drop-down next to Domain for the Active Directory location for computer accounts, verify that **workspacelab.com** is selected.  Using the arrows, expand **Citrix > New York > VDA**. Select the **Desktops** Organizational Unit (OU). **Note**: The Desktops OU is the WW Labs location designated for machines running the Virtual Delivery Agent (VDA) that are used to host user desktop OS desktop resources. Enter **NYC-DTP-###** in the Account naming scheme field.

	Verify that **0-9** is selected from the drop-down menu to the right of the naming scheme.  **Note**: If this wizard was used to create machines on an existing naming convention, then the resultant machines from this Machine Creation Services (MCS) process would increment to the next numerical sequence numbers available. Click **Next** to continue the Machine Catalog creation wizard.
10.	On the Summary page, review configurations and enter the following information: • Machine Catalog name: **NYC-CAT-DesktopOS** • Machine Catalog description for administrators: **Windows 10 Desktop MCS Machine Catalog** Click **Finish**. **Note**: Clicking **Finish** begins the Machine Creation Services (MCS) process in which a combination of the parameters specified in this Machine Catalog creation wizard and the parameters of the XenApp and XenDesktop Site are used to create complete virtual machines from the Master machine specified earlier in the wizard. Each virtual machine created is built into a Machine Catalog, visible from Studio. Each virtual machine created has a nearly identical build to its Master machine, with a unique SID, machine account in Active Directory, unique MAC, and using the DHCP scope we verified in an earlier exercise these virtual machines have a unique IP address.

	Note: With the XenServer resources allocated to this XenApp and XenDesktop POC project by the Citrix Lead Architect, we can expect this Machine Creation Services (MCS) process to take an estimated 10 minutes to complete.
11.	Verify that the Machine Creation Services (MCS) process has completed and that the Machine Catalog was created. Click **Machine Catalogs** in the left pane of Studio and view the **NYC-CAT-DesktopOS** Machine Catalog in the middle pane. 
12.	Verify that the virtual machine specified to be created by Machine Creation Services (MCS) has been successfully created and added to the NYC-CAT-DesktopOS Machine Catalog. In Studio, right-click the **NYC-CAT-DesktopOS** Machine Catalog and select **View Machines**. Verify that **NYC-DTP-001.workspacelab.com** displays. 
13.	Additionally, verify that the virtual machine NYC-DTP-001 was created in the environment. Using XenCenter, in the left pane, confirm that **NYC-DTP-001** is listed to prove that this machine was created.



Key Takeaways:

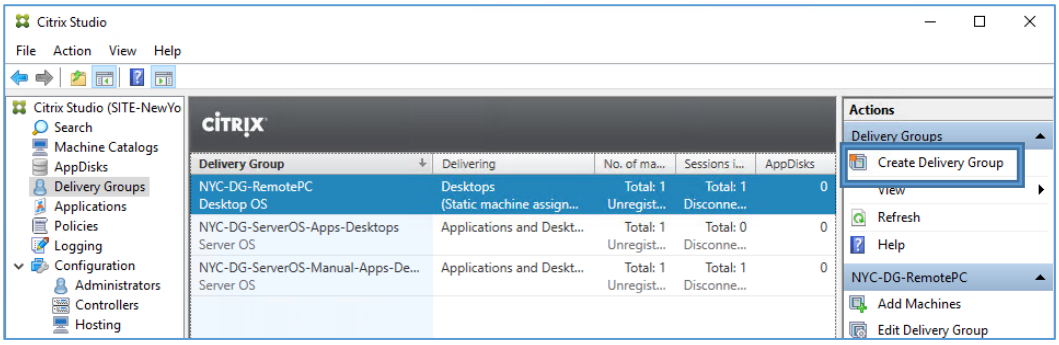
- The Desktop OS Machine Catalog provides VDI desktops ideal for a variety of different users.
- MCS can create multiple machines automatically from a machine or snapshot, including both Server OS and Desktop OS machines.
- MCS requires certain permissions to access a pre-configured Hypervisor.
- MCS relies on storage level cloning; make sure that the selected storage repository has the necessary capacity and performance available.

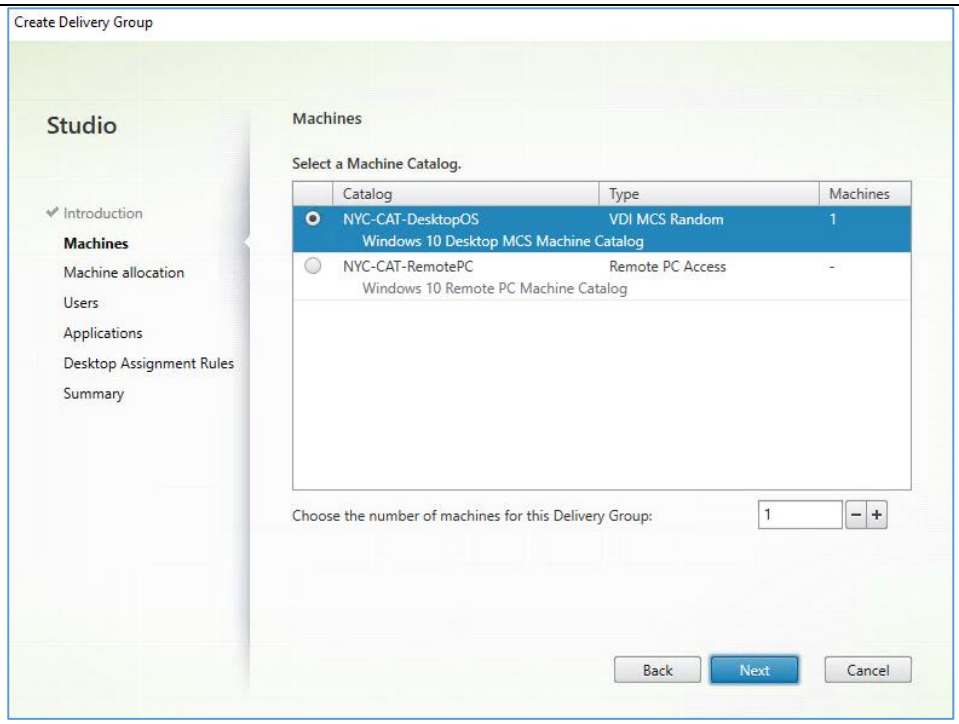
Exercise 4-9: Create a Delivery Group for Desktop OS

Scenario:

To complete the assignment of a Desktop from a VDI Machine Catalog, you will create a Delivery Group.

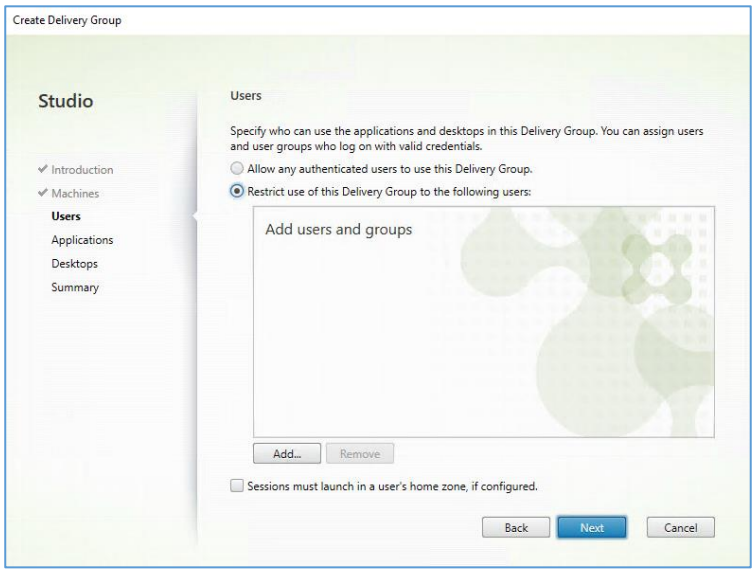
Your task is to create a Delivery Group and set the assignment of non-persistent desktops to the Technicians user group.

Step	Action
1.	Using the Remote Desktop Connection Manager, confirm that you are still connected to **NYC-XDC-001**. **Note:** In a previous exercise, you had logged on to NYC-XDC-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-XDC-001 by right-clicking this machine and selecting Connect server.
2.	Using Studio, expand **Citrix Studio (SITE-NewYork)** and click **Delivery Groups**. From the Actions pane on the right side of the console, click **Create Delivery Group**.  **Note**: Studio was started in a previous exercise. If Studio was closed in a previous exercise, then click **Start** > **Citrix** > **Citrix Studio**.
3.	On the Introduction page, click **Next** to continue the Delivery Group creation wizard.
4.	On the Machines page, verify that the previously created Machine Catalog is listed. Select **NYC-CAT-DesktopOS**. Specify the number of machines to include for this Delivery Group. Enter **1** in the Choose the number of machines for this Delivery Group field.



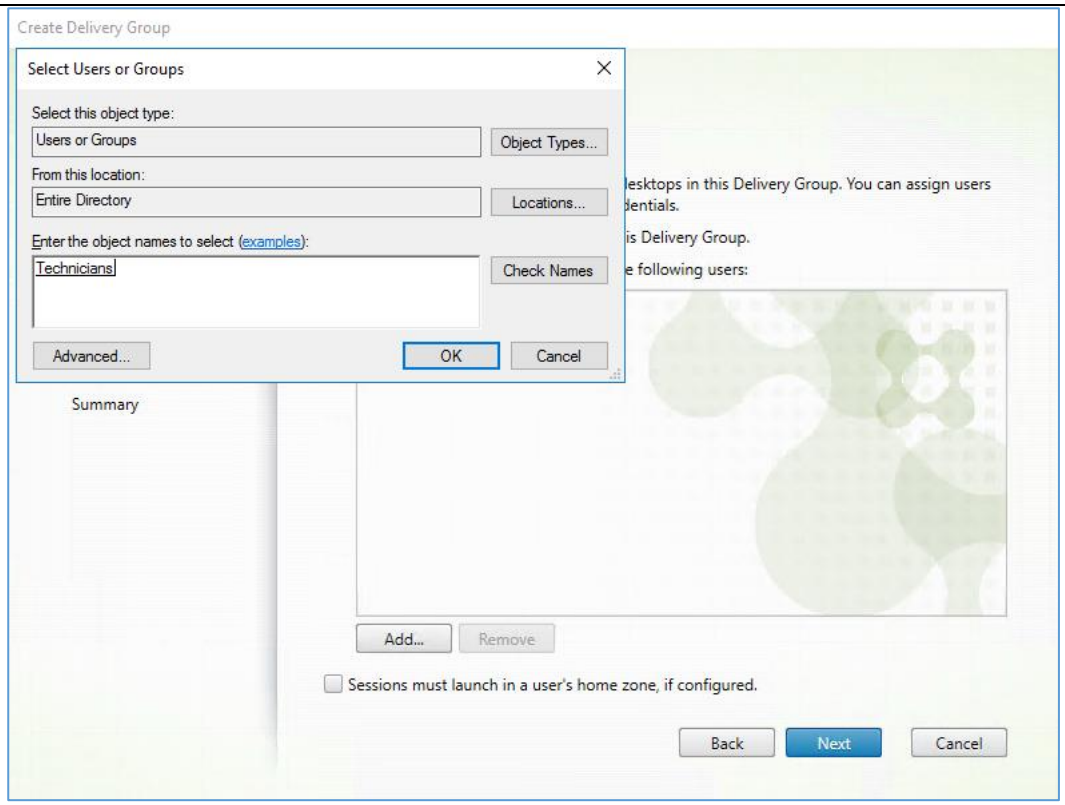
Click **Next** to continue the Delivery Group creation wizard.

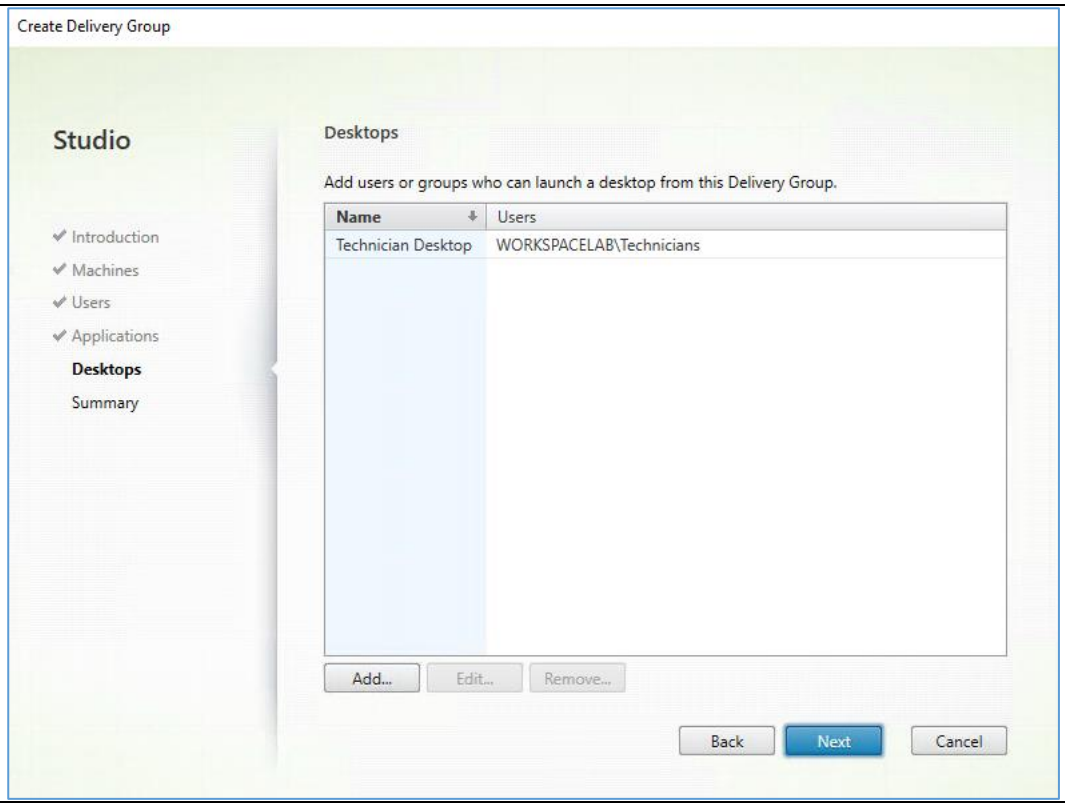
5. On the Users page, select **Restrict use of this Delivery Group to the following users**.

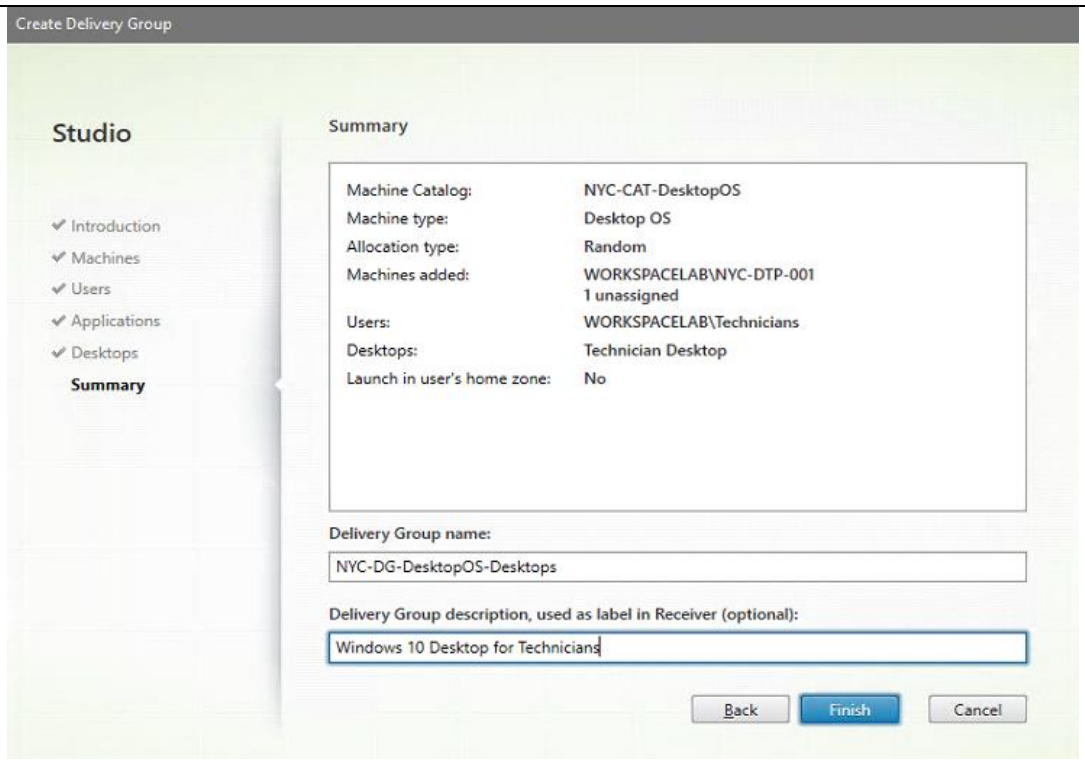


Click **Add** below Add users and groups. In the Select Users or Groups dialog box that appears, enter **Technicians** and then click on the **Check Names** button.

Click **OK** on the Select Users or Groups dialog box.

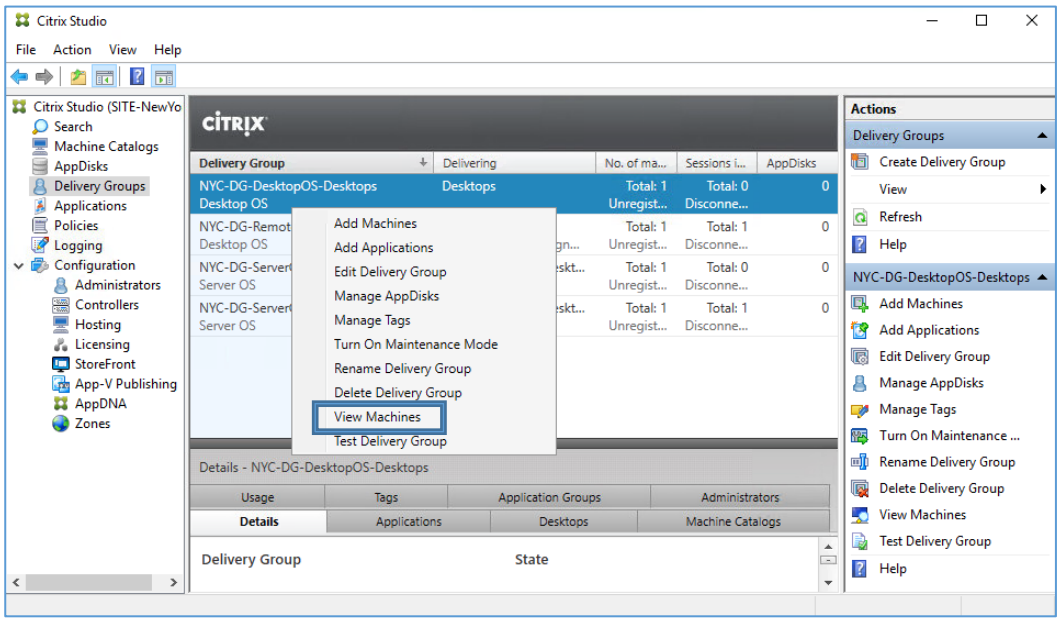
	 Click **Next** to continue the Delivery Group creation wizard. **Note**: The WW Labs design scope for this XenApp and XenDesktop POC deployment has specified this user group in Active Directory for testing this published desktop (as seen in the next step) for this POC.
6.	On the Applications page, click **Next**. **Note**: NYC-CAT-DesktopOS has Windows 10 machine and you are only publishing Desktops using this catalog.
7.	On the Desktops page, click **Add** and enter the following information: • Display name: **Technician Desktop** • Description: **Windows 10 Desktop** Select **Restrict desktop use to.** Click **Add** below Add users and groups. In the Select Users or Groups dialog box that appears, enter **Technicians** and then click on the **Check Names** button. Click **OK** twice to return to Desktops page and then click **Next**.

	
8.	On the Summary page, verify the configuration information and enter the following: • Delivery Group name: **NYC-DG-DesktopOS-Desktops** • Delivery Group description, used as label in Receiver (optional): **Windows 10 Desktop for Technicians** Click **Finish**.

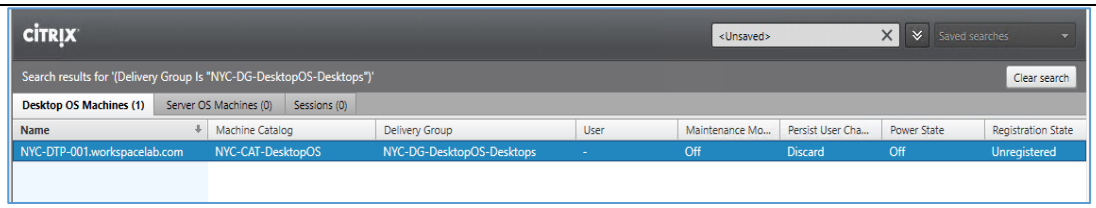


9. Verify that the expected desktop was successfully added to the Delivery Group.

In Studio, select the **Delivery Groups** node in the left pane. In the center pane, right-click the **NYC-DG-DesktopOS-Desktops** Delivery Group, and select **View Machines**.



Verify that **NYC-DTP-001.workspacelab.com** displays.

Key Takeaways:

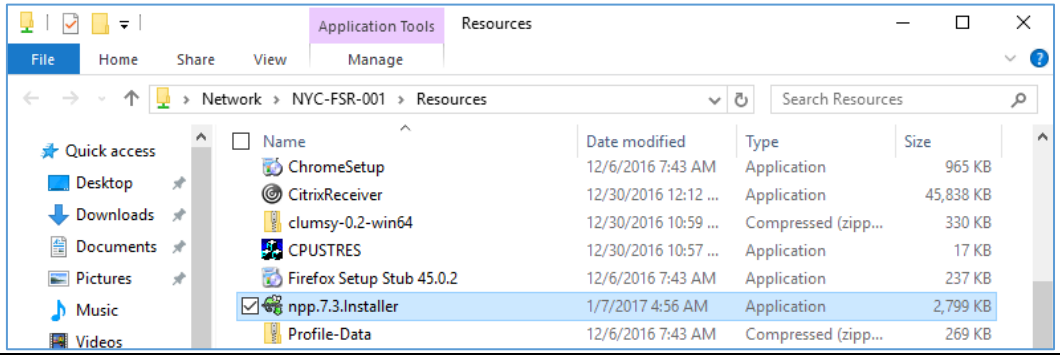
- The desktops provided in this Delivery Group are set to be shared between the configured users and will lose every change on reboot; this option is referred to as Random non-persistent desktops.
- Other options include: Static non-persistent desktop and Static persistent, where users will receive the same desktop at each logon, changes will either be discarded or saved during reboot.

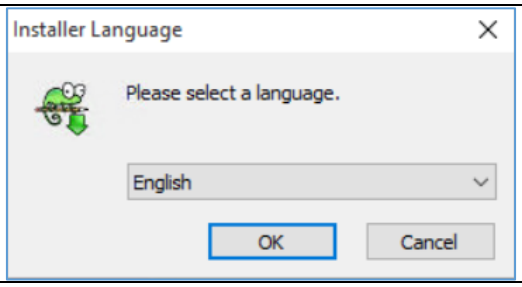
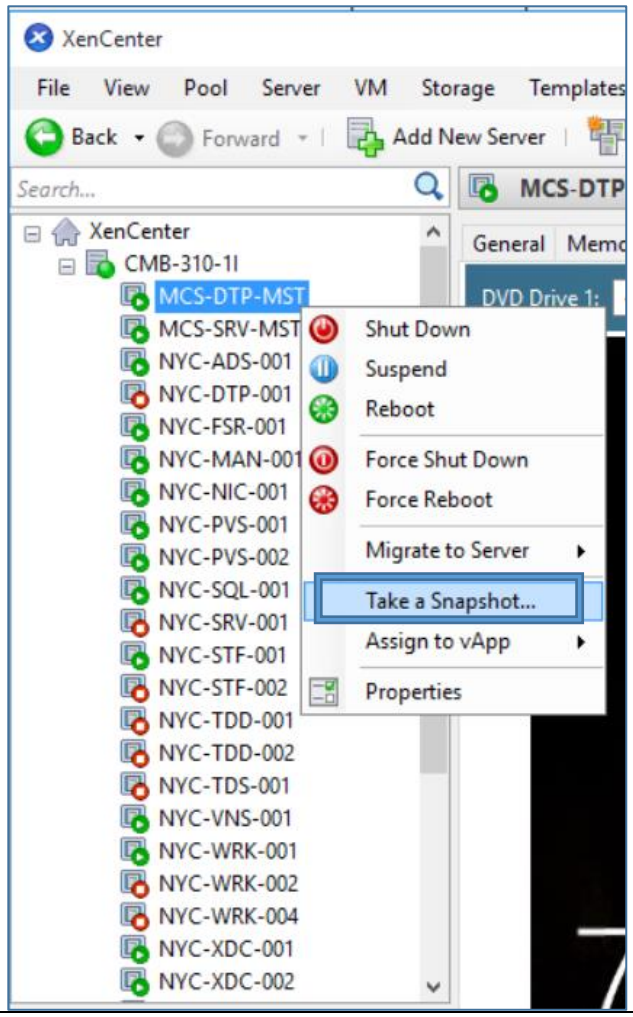
Exercise 4-10: Update a Machine Catalog for Desktop OS

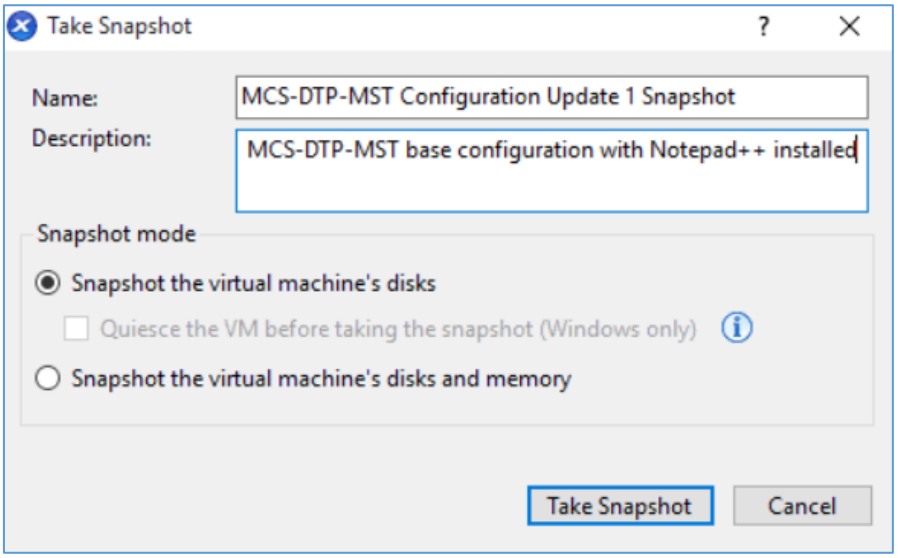
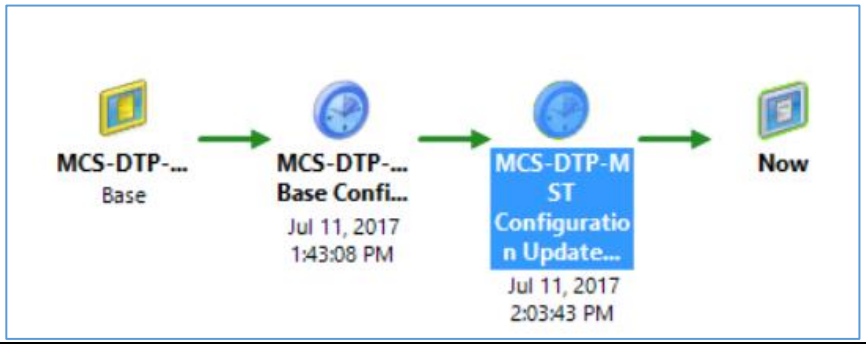
Scenario:

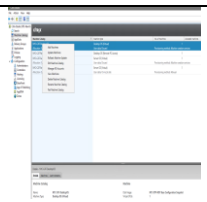
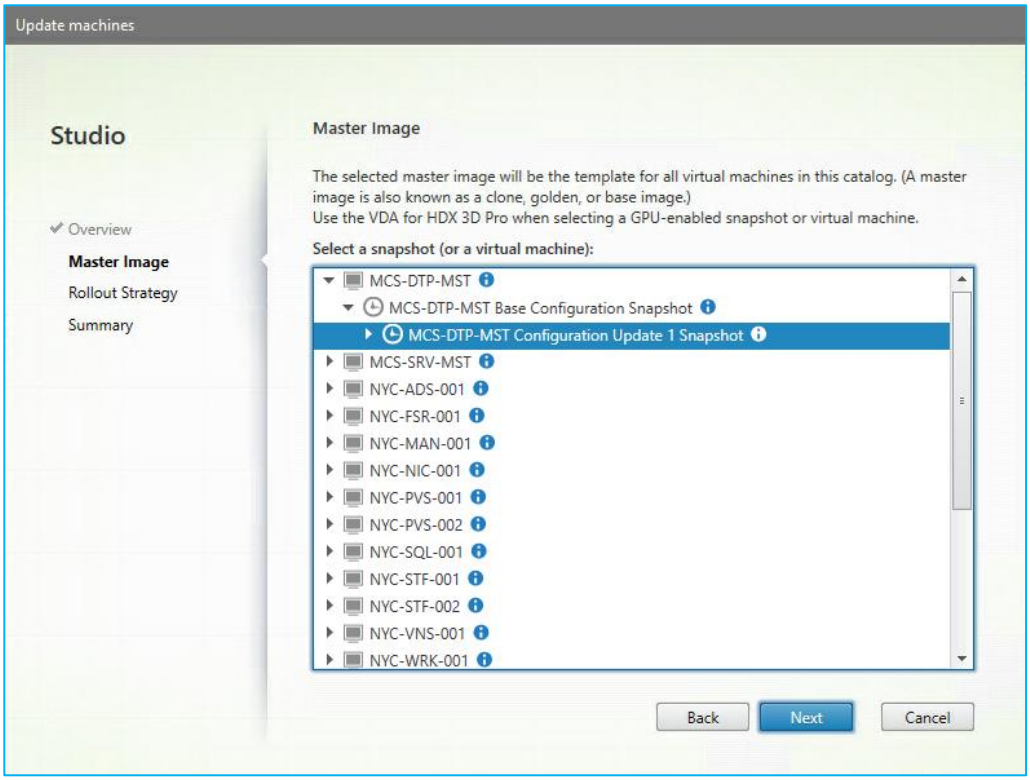
Your Lead Citrix Architect has reviewed your recent Machine Catalog and Delivery Group tasks and has identified missing software from the Desktop OS Catalog.

Your task is to perform an update to the Desktop OS Catalog.

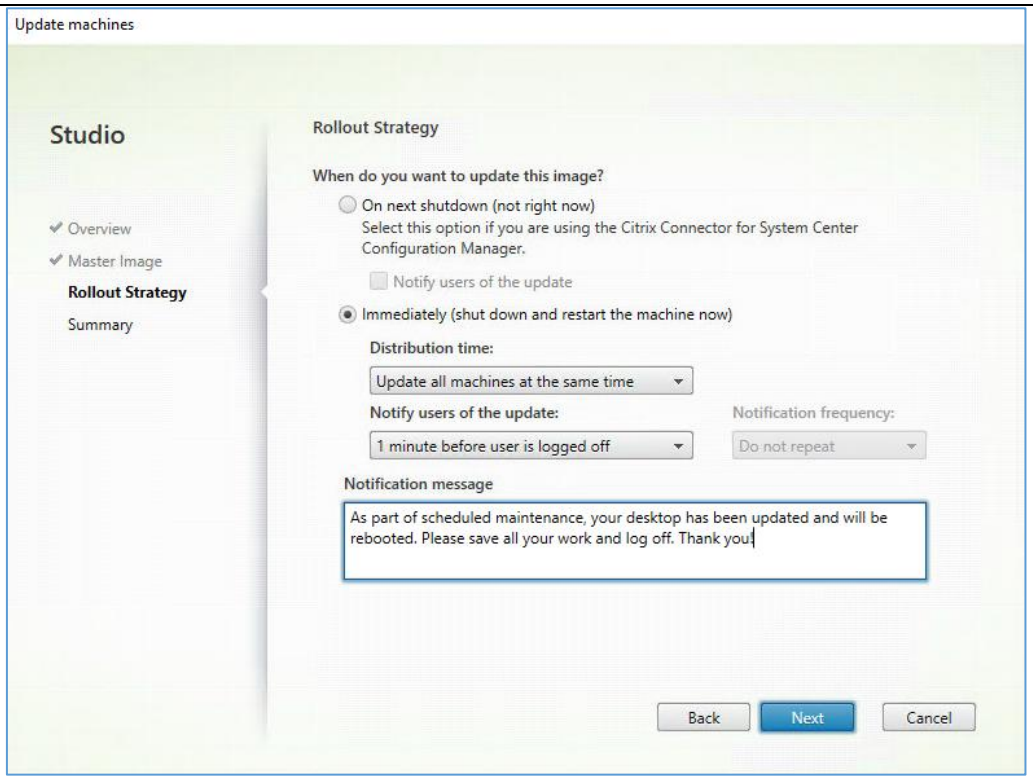
Step	Action
1.	Using XenCenter, right-click **MCS-DTP-MST** and click **Start**. Using the Remote Desktop Connection Manager, connect to MCS-DTP-MST. To log on to MCS-DTP-MST, right-click this machine and choose **Connect server**. **Note**: The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1
2.	On the Desktop of MCS-DTP-MST, double-click the **Lab Resources** icon.
3.	Double-click **npp.7.3.Installer.exe** to start the Notepad++ installation. 
4.	On the Installer Language menu, select **English** and click **OK**.

	
5.	On the Notepad++ Setup page, click **Next**.
6.	On the License Agreement page, review the license agreement, and if you agree, click **I Agree**.
7.	On the Choose Install Location page, click **Next**.
8.	On the first Choose Components page, click **Next**.
9.	On the second Choose Components page, leave the default selection and click **Install**.
10.	Wait for the installation to complete, uncheck **Run Notepad++ 7.3**, and click **Finish**.
11.	Using XenCenter, right-click **MCS-DTP-MST** in the left pane and select **Shut Down**. Click **Yes** to confirm the shutdown of the virtual machine. Once MCS-DTP-MST is shut down, right-click **MCS-DTP-MST** and select **Take a Snapshot**. 
12.	In the Take Snapshot dialog box, enter the following text into the appropriate fields:

	• Name: **MCS-DTP-MST Configuration Update 1 Snapshot** • Description: **MCS-DTP-MST base configuration with Notepad++ installed** Click **Take Snapshot**. 
13.	Using XenCenter, verify that the Snapshot was taken. In the left pane of XenCenter, select **MCS-DTP-MST**. In the right pane, click on the **Snapshots** tab and verify that the second snapshot is present. 
14.	Using the Remote Desktop Connection Manager, switch to **NYC-XDC-001**. **Note:** In a previous step, you had logged on to **NYC-XDC-001** using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-XDC-001 by right-clicking this machine and selecting Connect server.
15.	Using Studio, expand **Citrix Studio (SITE-NewYork)** and click **Machine Catalogs**. In the center pane, right-click the **NYC-CAT-DesktopOS** Machine Catalog and click **Update Machines**.

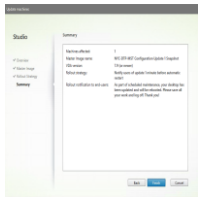
	 **Note**: Studio was started in a previous exercise. If Studio was closed in a previous exercise, then click Start > Citrix > Citrix Studio.
16.	On the Overview page, click **Next**.
17.	On the Master Image page, expand **MCS-DTP-MST** > **MCS-DTP-MST Base Configuration Snapshot**. Select **MCS-DTP-MST Configuration Update 1 Snapshot**. **Note**: This snapshot is the snapshot taken in a previous step. Click **Next** to continue the Machine Catalog update wizard.  **Note**: In an earlier exercise, you created a Machine Catalog for a Server OS, using a virtual machine as the master machine. Machine Creation Services (MCS) supports the use of both a virtual machine or a virtual machine snapshot to be used as the master machine or image to create the Machine Catalog. When using a snapshot as the master image, you should consider naming the snapshot, because when the MCS process runs a snapshot is created by Studio and a name is assigned that you cannot change.
18.	On the Rollout Strategy page, select **Immediately (shut down and restart the machine now)**. **Note:** If you choose to update the image immediately, configure a distribution time and a notification.

	• **Distribution time:** You can choose to update all machines at the same time, or specify the total length of time it should take to begin updating all machines in the catalog. An internal algorithm determines when each machine is updated and restarted during that interval. • **Notification:** In the left notification drop-down, choose whether to display a notification message on the machines before an update begins. By default, no message is displayed. If you choose to display a message 15 minutes before the update begins, you can choose (in the right drop-down) to repeat the message every five minutes after the initial message. By default, the message is not repeated. Unless you choose to update all machines at the same time, the notification message displays on each machine at the appropriate time before the update begins, calculated by an internal algorithm. In the drop-down menu for Distribution time, verify that **Update all machines at the same time** is selected. **Note**: You chose this Distribution time option because no users are logged on and you only have one virtual machine (VM). If this Machine Catalog had multiple VMs running and you did not want to restart them all at once, then you could have chosen one of the following options: • 30 minutes • 1 hour • 2 hours • 3 hours • 4 hours • 5 hours All the VMs would then be rebooted during that time interval. An internal algorithm determines when each machine is updated and restarted during that interval. The default application of this internal algorithm is to reboot machines in sets of 10. This parameter can only be adjusted using PowerShell. In the drop-down menu for Notify users of the update, select **1 minute before user is logged off**. Enter the following text in the Message box: **As part of scheduled maintenance, your desktop has been updated and will be rebooted. Please save all your work and log off. Thank you!** Click **Next** to continue the Machine Catalog Update wizard.



Note: Citrix warns all Citrix Administrators, when configuring messages to users to be mindful of both company and legal rules and to not offend, nor violate a user's rights. Instead keep these messages as brief and as formal as possible.

19. On the Summary page, review the configurations and click **Finish**.



Note: Click Close if the confirmation prompt appears.

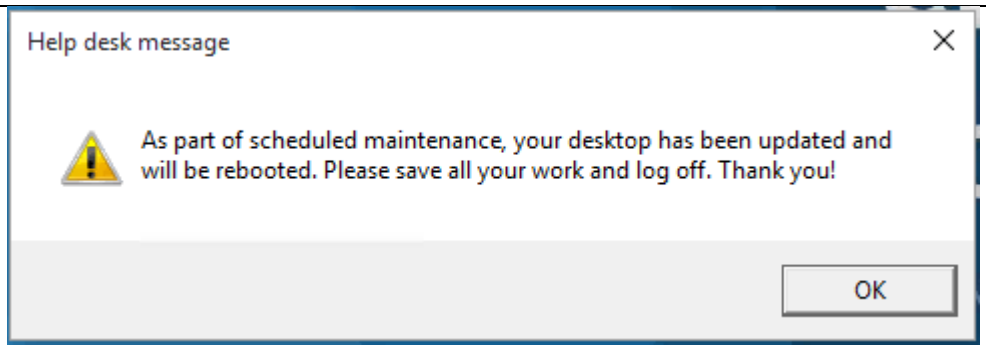
20. While the Machine Creation Services (MCS) process runs to update the Machine Catalog, switch to NYC-DTP-001 from within the Remote Desktop Connection Manager.

To log on to NYC-DTP-001, right-click this machine and choose **Connect server**.

Note: The following credentials are used to make the connection:

- User name: Workspacelab\Administrator
- Password: Password1

Verify that a dialog box shows up with the expected message: **As part of scheduled maintenance, your desktop has been updated and will be rebooted. Please save all your work and log off. Thank you!**



Note: This message may take a few minutes to appear. This message means that the message you configured in the Machine Catalog Update wizard under the notification only applies to active sessions currently logged on. This message in not queued for new sessions, it behaves more like a net send message.

Wait for a minute and verify that **NYC-DTP-001** completes the reboot process.

Note: You may want to switch to XenCenter to monitor the progress of the reboot. To do this, select NYC-DTP-001 in the left pane and the Console tab in the right pane.

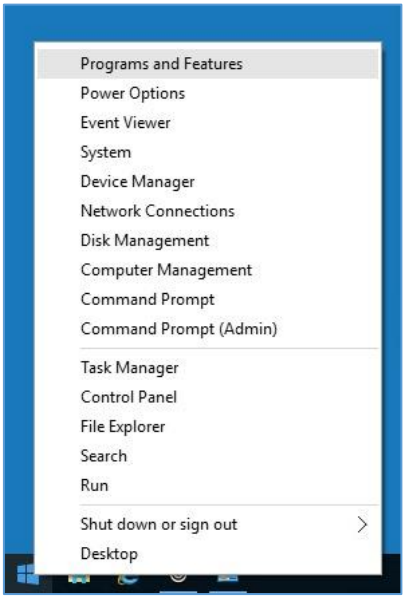
21. Using the Remote Desktop Connection Manager, connect to **NYC-DTP-001**.

To log on to NYC-DTP-001, right-click this machine and choose **Connect server**.

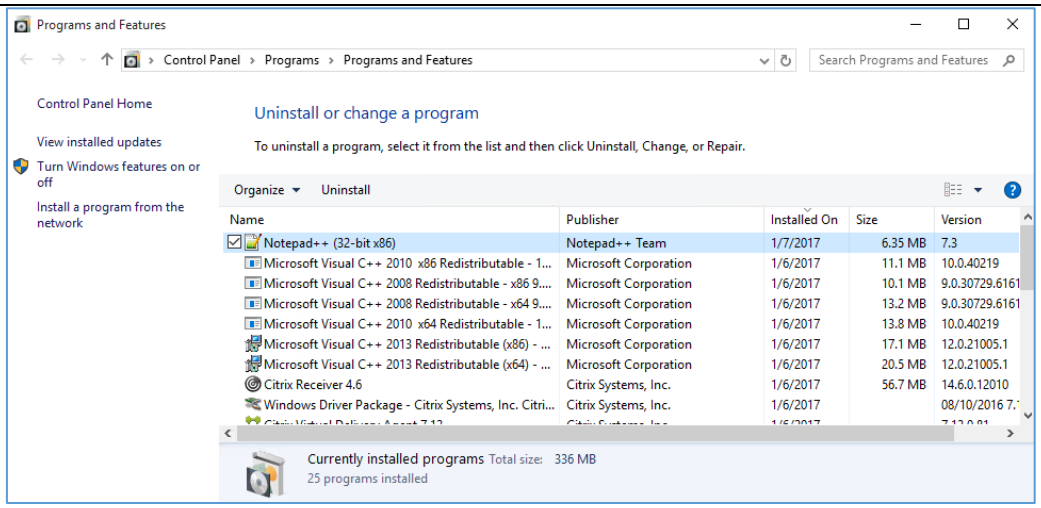
Note: The following credentials are used to make the connection:

- User name: Workspacelab\Administrator
- Password: Password1

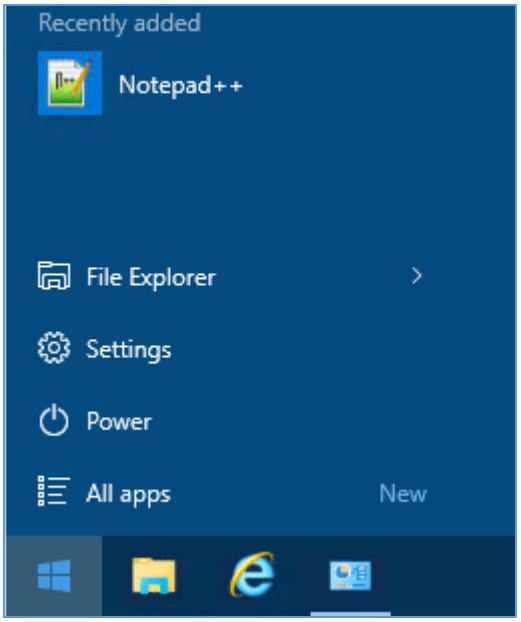
22. Right-click **Start** and select **Programs and Features**.



Verify that **Notepad++** now appears as an installed program.



Close the **Control Panel**.
Note: If you don't see the application Notepad++ (32-bit x86) in the **Programs and Features**, then click on **Start menu** and see if you find **Notepad++** in the **Recently added** application list. Also reboot the VM NYC-DTP-001 from Studio and then see if Notepad++ shows up in the Programs and Features once the VM is back online.



23.	Log off NYC-DTP-001. To log off, right-click **Start** > select **Shut down or sign out** > and click **Sign out**.

Key Takeaways:

- To update multiple machines in an MCS catalog at once, update the master machine and use the update Catalog function.
- An update can only be made to a complete Catalog and all machines in it, not to Delivery Groups.
- Updating the Catalog can also be used to point to an older snapshot or a different machine of the same type.
- After completing the update, a rollback option will appear in Studio, which can be used to undo the recent update.

Module 5: Providing access with StoreFront and Receiver

Overview:

This module presents the role of StoreFront and Receiver in the user access of XenApp and XenDesktop resources. You will identify the architecture considerations, determine the installation requirements, and perform the deployment.

Before you begin:

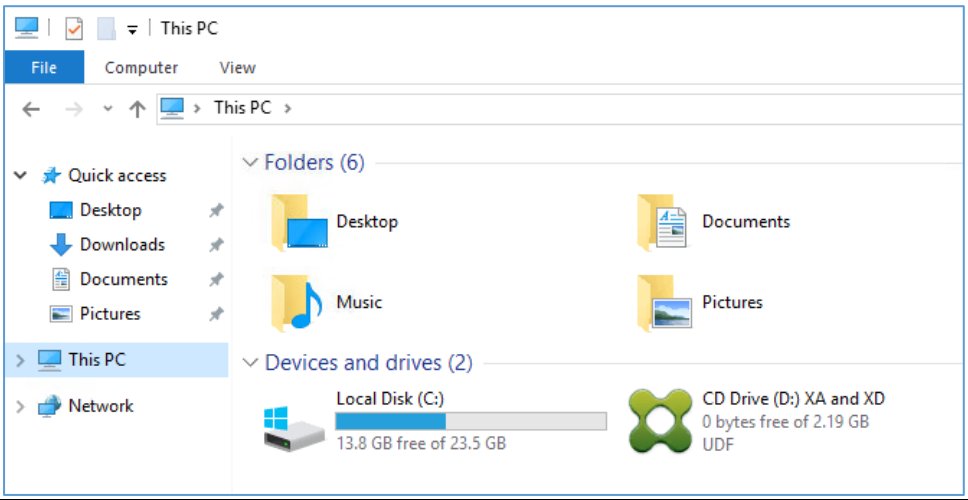
Estimated time to complete Module 5 lab exercises: 140 minutes

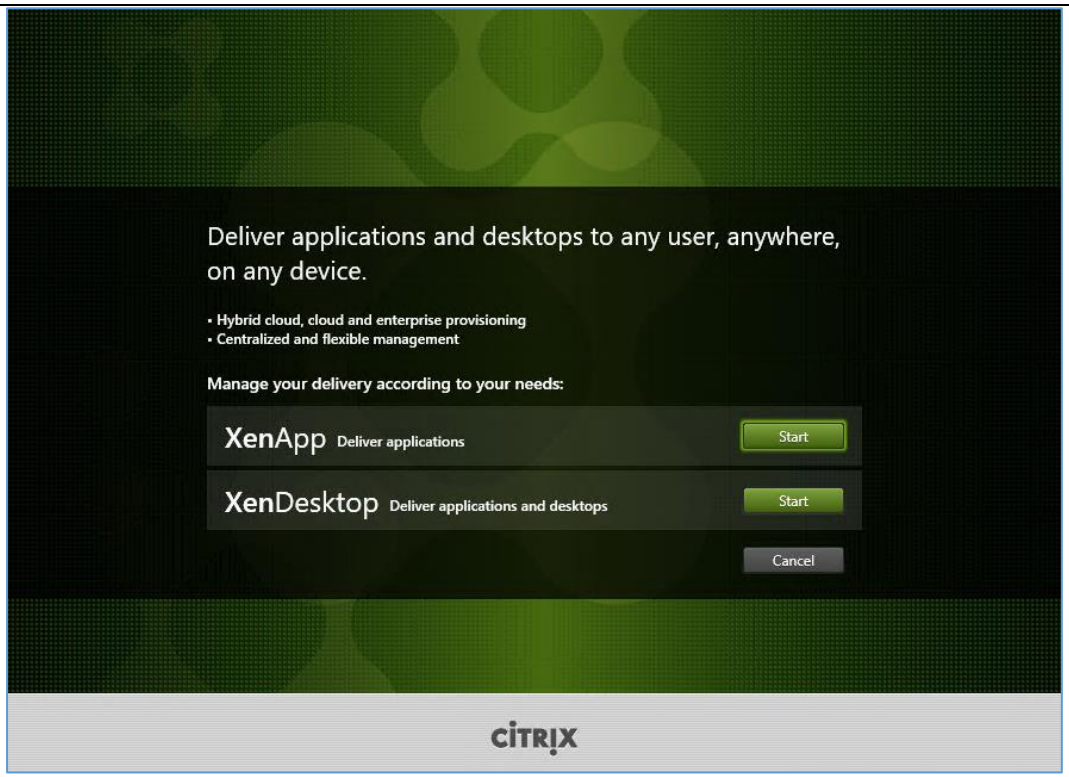
Exercise 5-1: Install the StoreFront Server

Scenario:

The StoreFront Server is a key component of XenApp and XenDesktop that is used to provide a point of access for users to log on and access resources. Your task is to install and configure the StoreFront Server, including the setup to distribute the installation of Citrix Receiver.

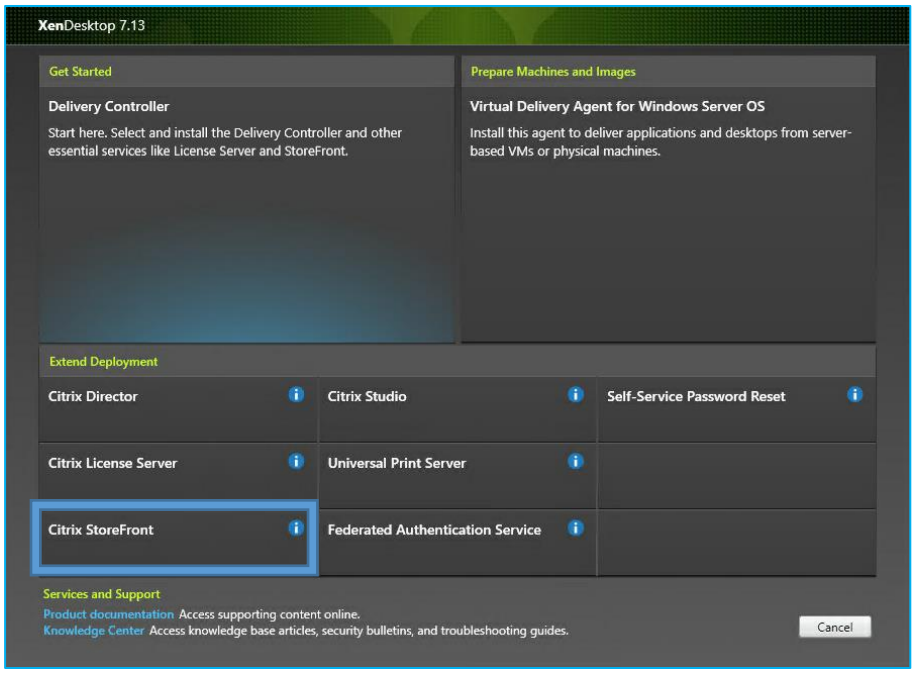
Step	Action
1.	The following VMs are required before beginning the exercises for this Module; all others may be powered down. To power manage your VMs, switch to XenCenter, right-click on the VM in the left pane and select Start or Shut Down. If prompted click Yes. • NYC-ADS-001 • NYC-SQL-001 • NYC-FSR-001 • NYC-XDC-001 • NYC-STF-001 • NYC-MAN-001 • NYC-SRV-001 • NYC-DTP-001 • NYC-WRK-001 • NYC-WRK-002 **Note**: These above VMs are listed in the start-up order.

2.	Using XenCenter, mount the XenApp and XenDesktop installation media ISO to NYC-STF-001. To mount the installation media ISO, select **NYC-STF-001** in the left pane of the XenCenter. In the right pane, select the **Console** tab. Using the DVD Drive 1: drop-down menu, select **XenApp_and_XenDesktop_7_13.iso**. **Note**: If there are no ISOs listed in the DVD Drive 1: drop-down menu, then the Local ISO Storage Repository (SR) that contains the ISO library may need to be re-scanned. In the left pane of XenCenter select the **Local ISO SR XS**. In the right pane select the Storage tab and click on the **Rescan** button. This task may need to be repeated later in the course. **Note:** If the above rescan of the **Local ISO SR XS** does not show the specific ISO for installation, XenApp_and_XenDesktop_7_13.iso, then please inform your Instructor.
3.	Using the Remote Desktop Connection Manager, connect to NYC-STF-001. To log on to NYC-STF-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1
4.	Open the **File Explorer** application from the Windows Taskbar or Start Menu. Select **This PC** on the left and double-click the **green Citrix logo** next to CD Drive under Devices and drives. 
5.	On the Deliver applications and desktops to any user, anywhere, on any device screen, click **Start** next to the XenDesktop option.



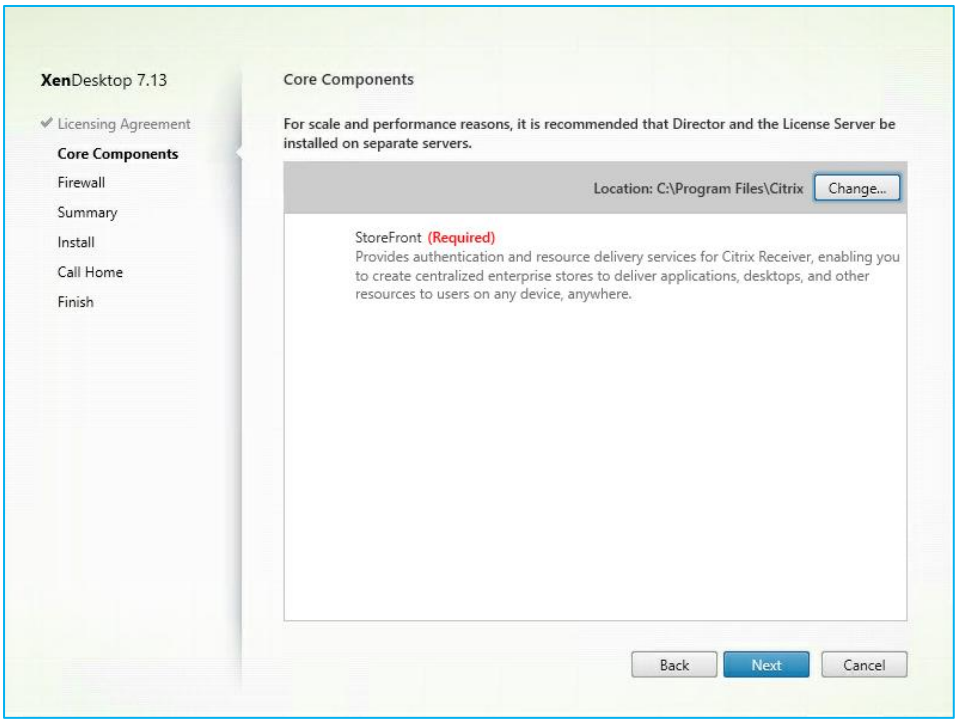
Note: If the above screen does not launch from double-clicking the green Citrix logo next to CD Drive under Devices and drives, then double-click the **AutoSelect.exe** file.

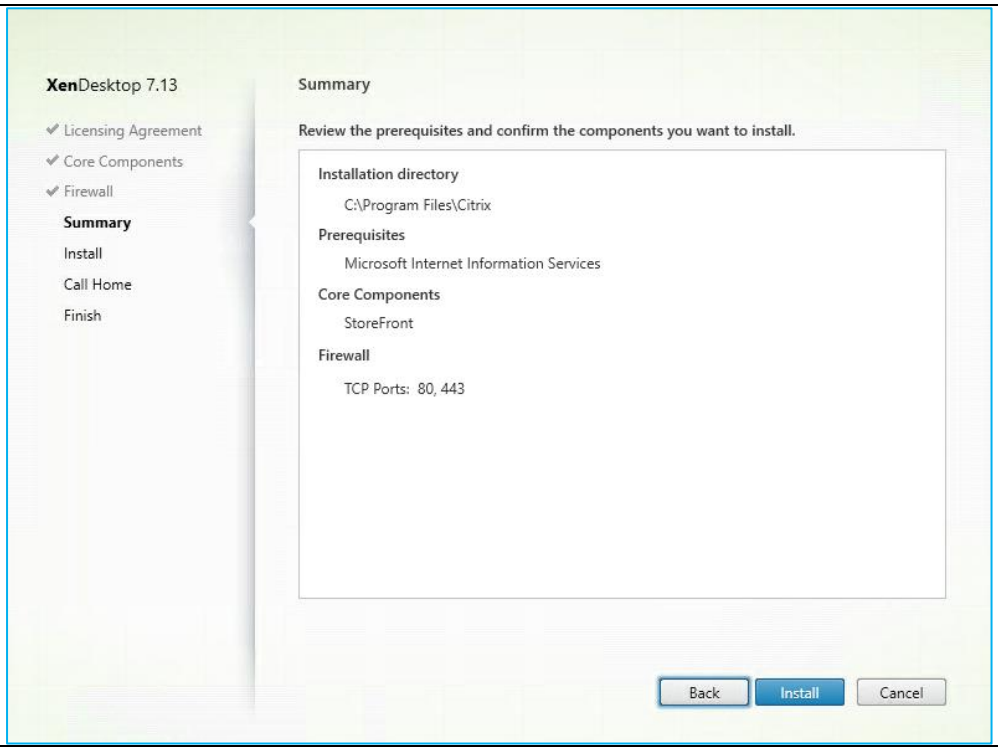
6. Select **Citrix StoreFront**.



7. Review the Software License Agreement page. If you agree, respond to the Software License Agreement and then click **Next**.

8. On the Core Components page, leave the default location and click **Next**.

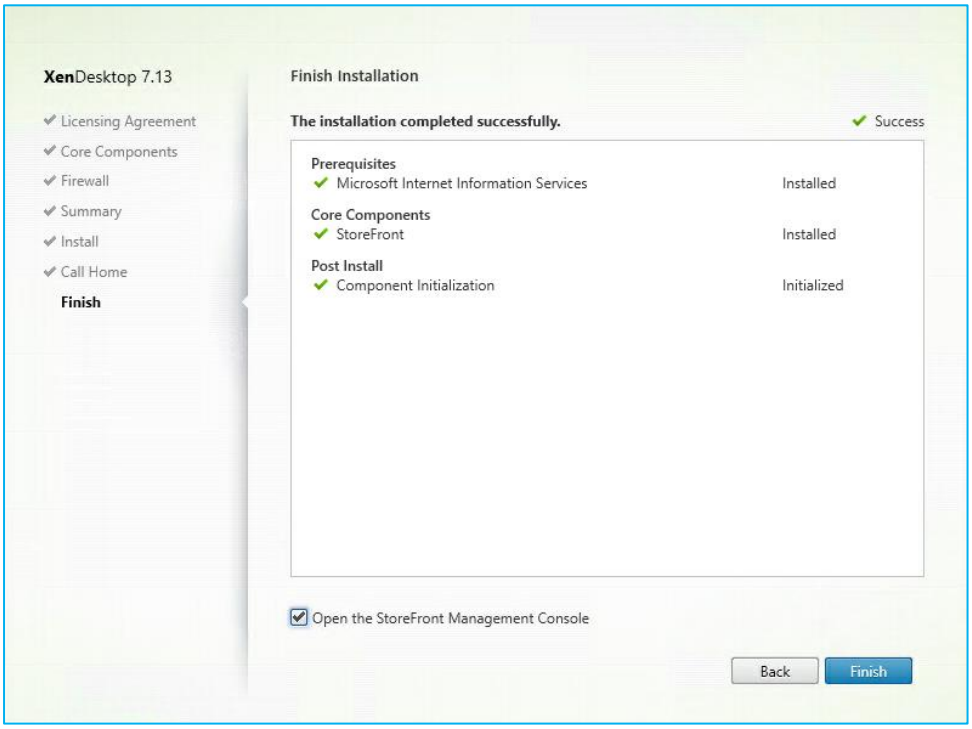
	 **Note**: The StoreFront Server component provides authentication and resource delivery services for Citrix Receiver, enabling you to create centralized enterprise stores to deliver applications, desktops, and other resources to users on any device, anywhere.
9.	On the Firewall page, verify that the Automatically option is selected for configuring the firewall and click **Next**. **Note**: When automatically is selected, rules are automatically created in the Windows Firewall. The rules will be created even if the Windows Firewall is turned off.
10.	On the Summary page, review the summary and click **Install**.



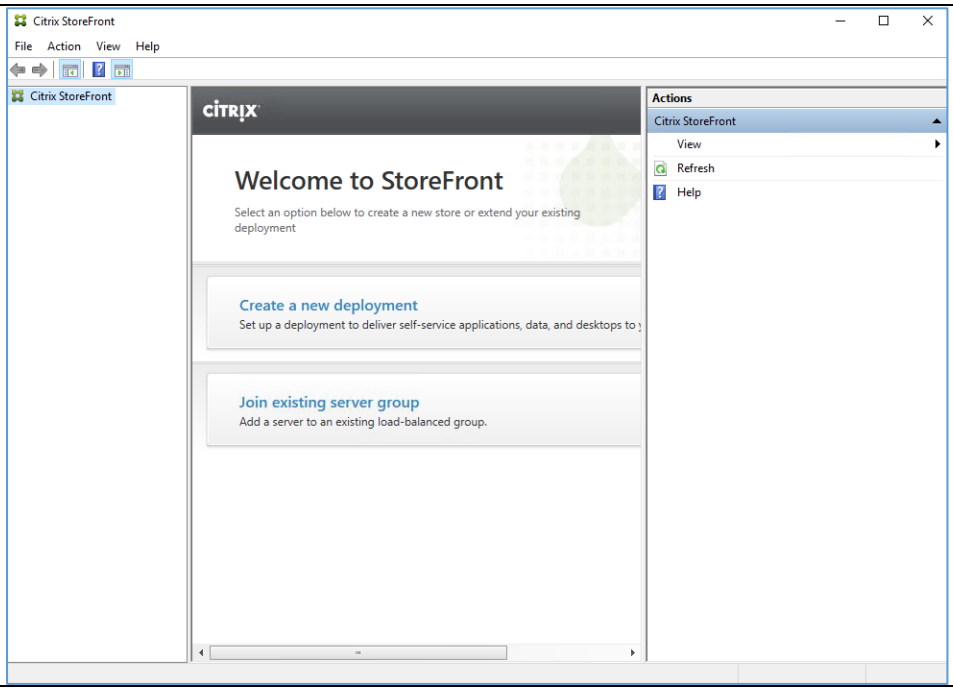
11. On the Call Home page, select **I do not want to participate in Call Home** and click **Next.**

    Note: The installation process may take a few minutes.

12. On the Finish page, click **Finish**.



Wait for the StoreFront console to open.

	
13.	Using XenCenter, eject the XenApp and XenDesktop installation media from NYC-STF-001. To eject the installation media ISO, select **NYC-STF-001** in the left pane of XenCenter. In the right pane, select the **Console** tab and click **Eject** to remove XenApp_and_XenDesktop_7_13.iso from the DVD Drive 1. **Note**: The Eject option can be difficult to see. It is an underlined word to the right side of the DVD Drive 1 drop-down menu.

Key Takeaways:

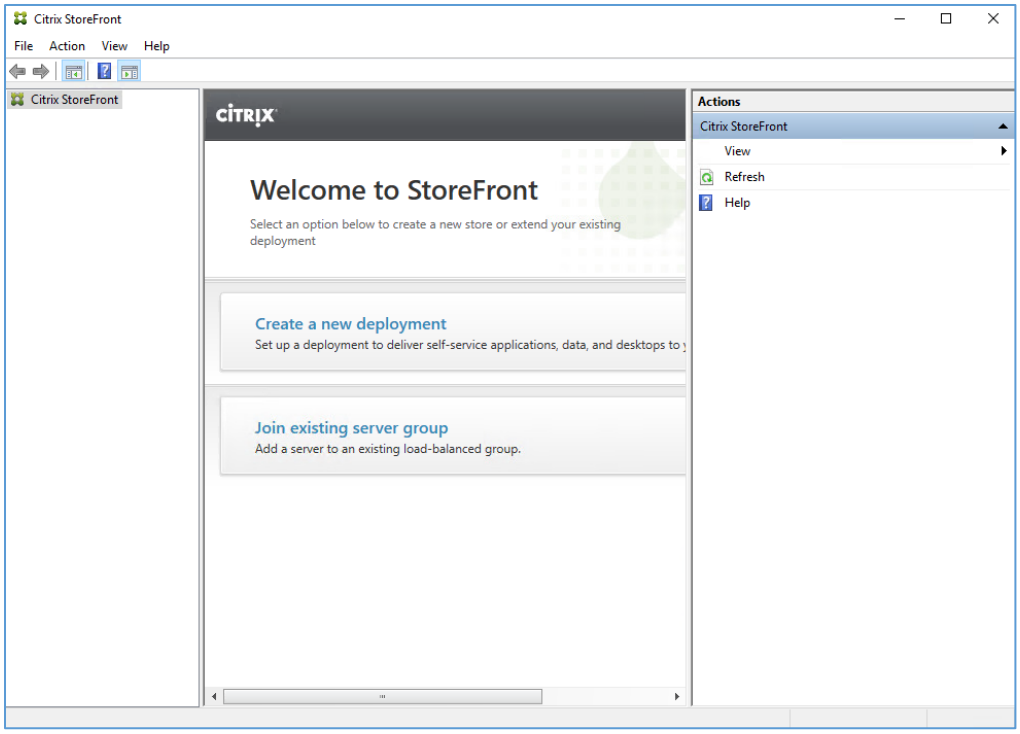
- The StoreFront installation requires IIS and installs this component automatically if missing.
- To achieve LTSR compliance, ensure that the correct StoreFront version (including required updates) have been installed.

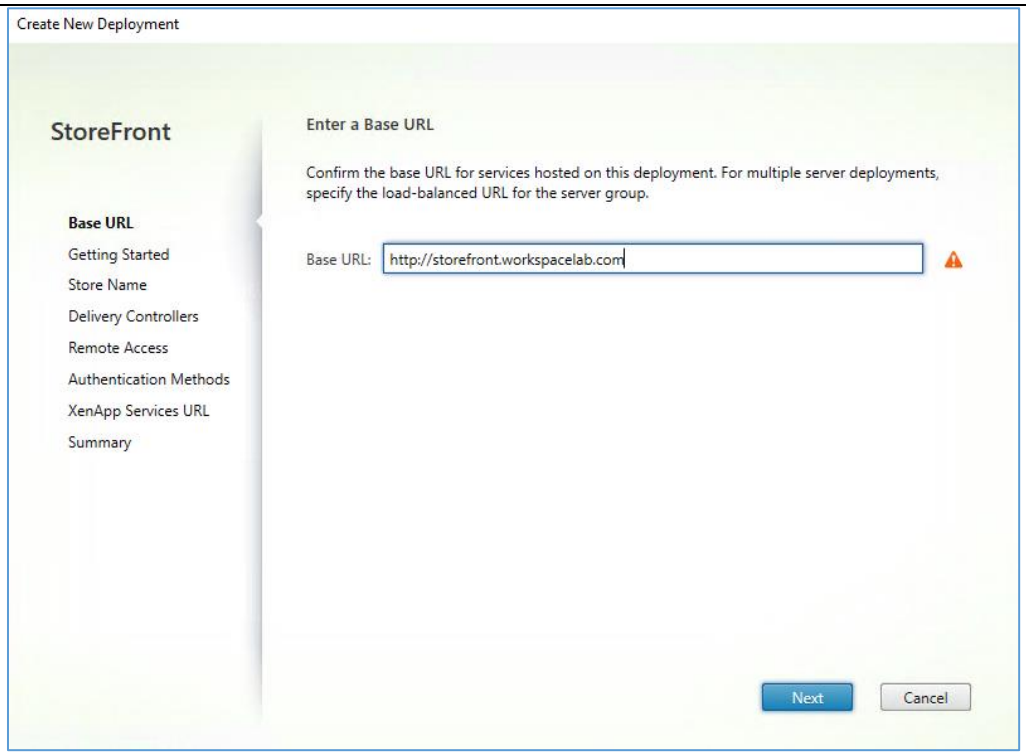
Exercise 5-2: Create a StoreFront Store

Scenario:

To give users access to the StoreFront server, StoreFront has to host a web based access called a Store. Your task is to create a Store that integrates with the Citrix Site Delivery Controller previously configured.

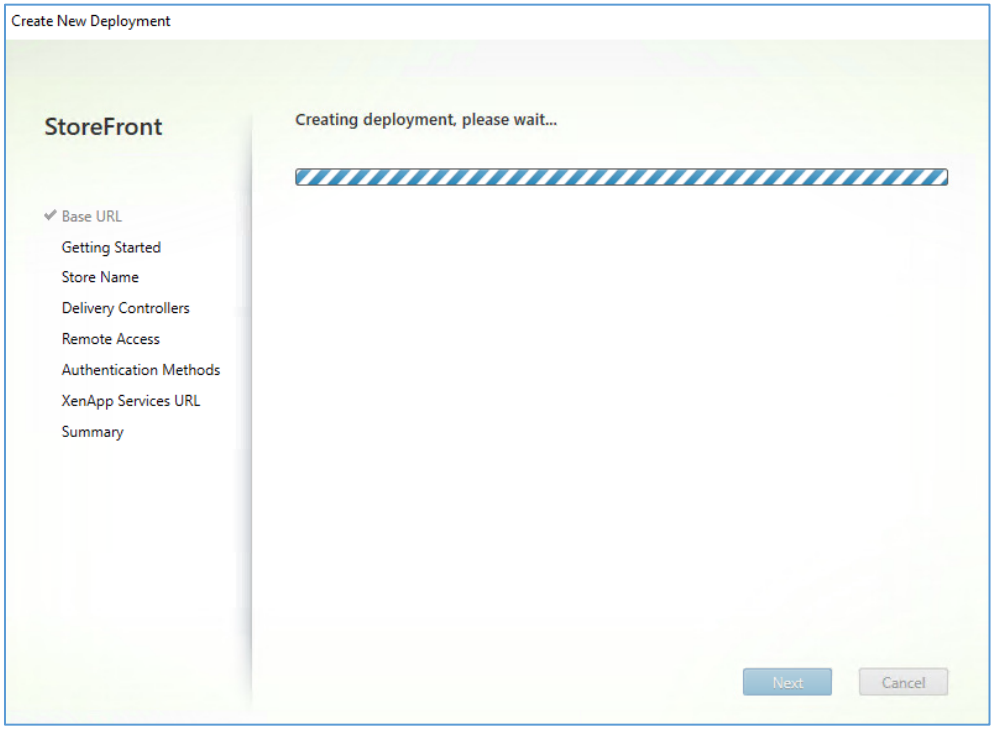
Step	Action
1.	Using the Remote Desktop Connection Manager, confirm that you are still connected to **NYC-STF-001**. **Note:** In a previous exercise, you had logged on to NYC-STF-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-STF-001 by right-clicking this machine and selecting **Connect server**.

2.	Using the StoreFront Management Console, create a new Deployment. In the middle pane, select **Create a new deployment**.  **Note**: The StoreFront Management Console was started in a previous exercise. If the console was closed in a previous exercise, then click Start > Citrix > Citrix StoreFront.
3.	Configure the Base URL for the Store in the new deployment. On the Base URL page, enter **http://storefront.workspacelab.com** in the Base URL field.

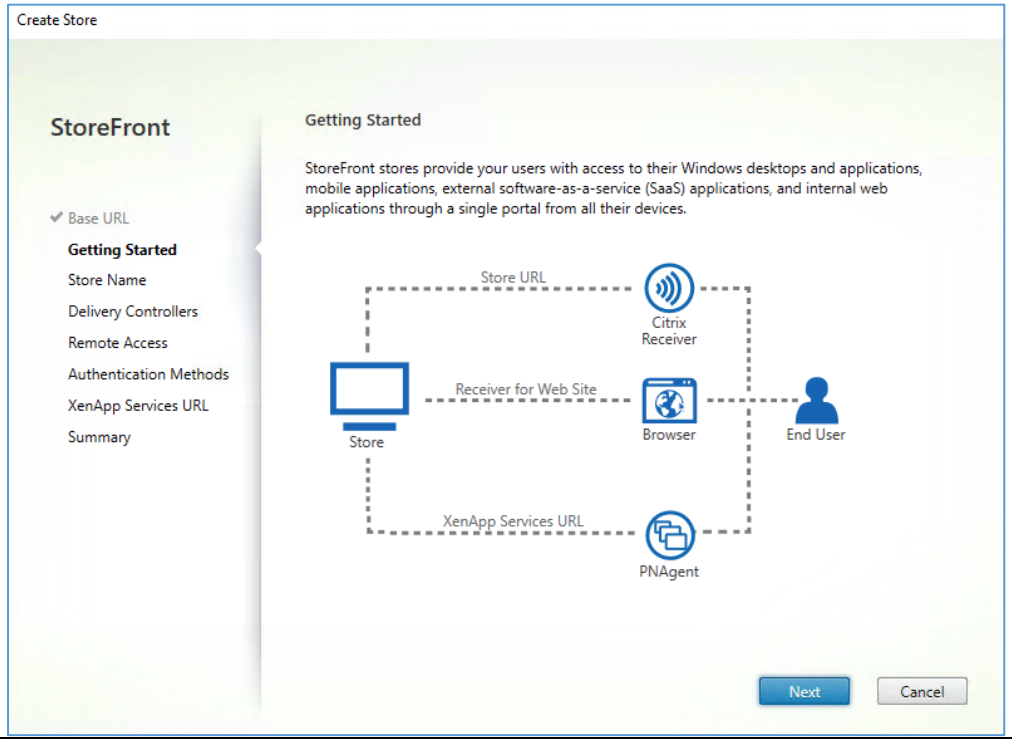
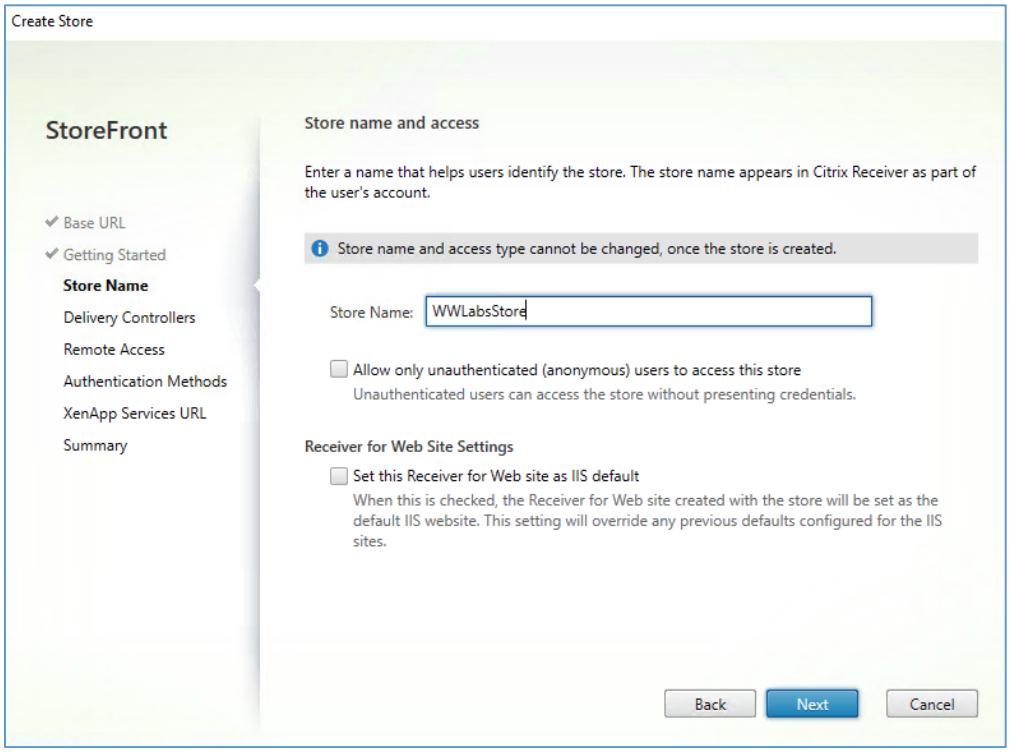


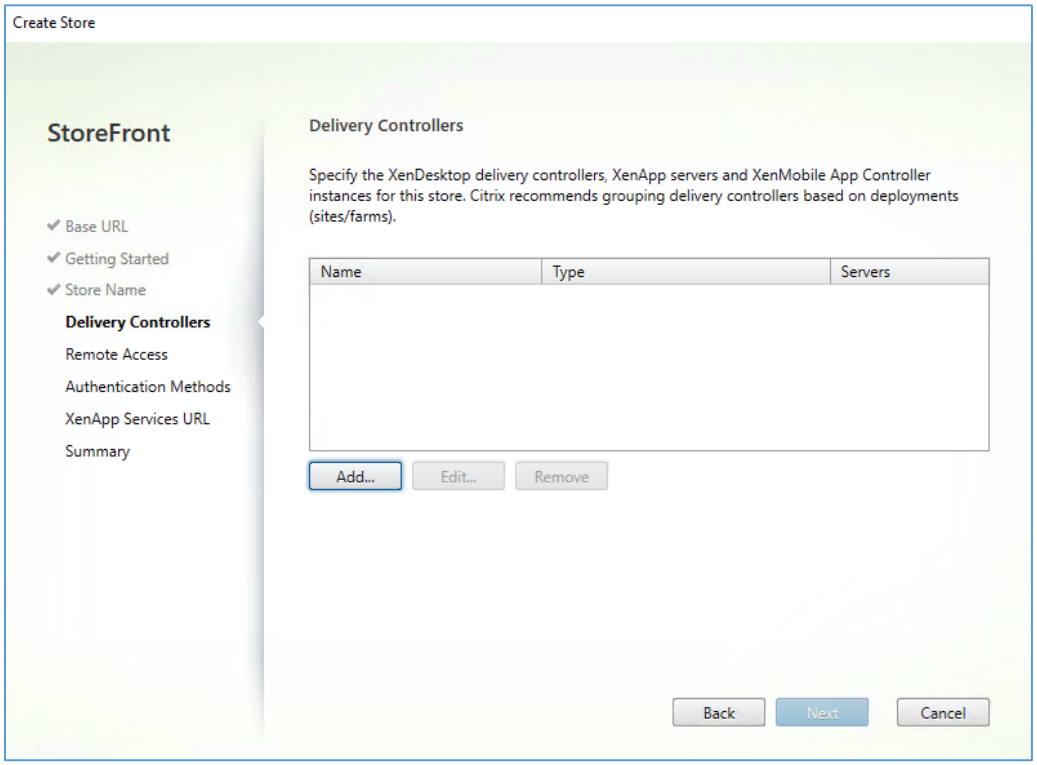
Click **Next** to continue the new deployment creation wizard.

Note: The deployment creation process takes a few minutes.

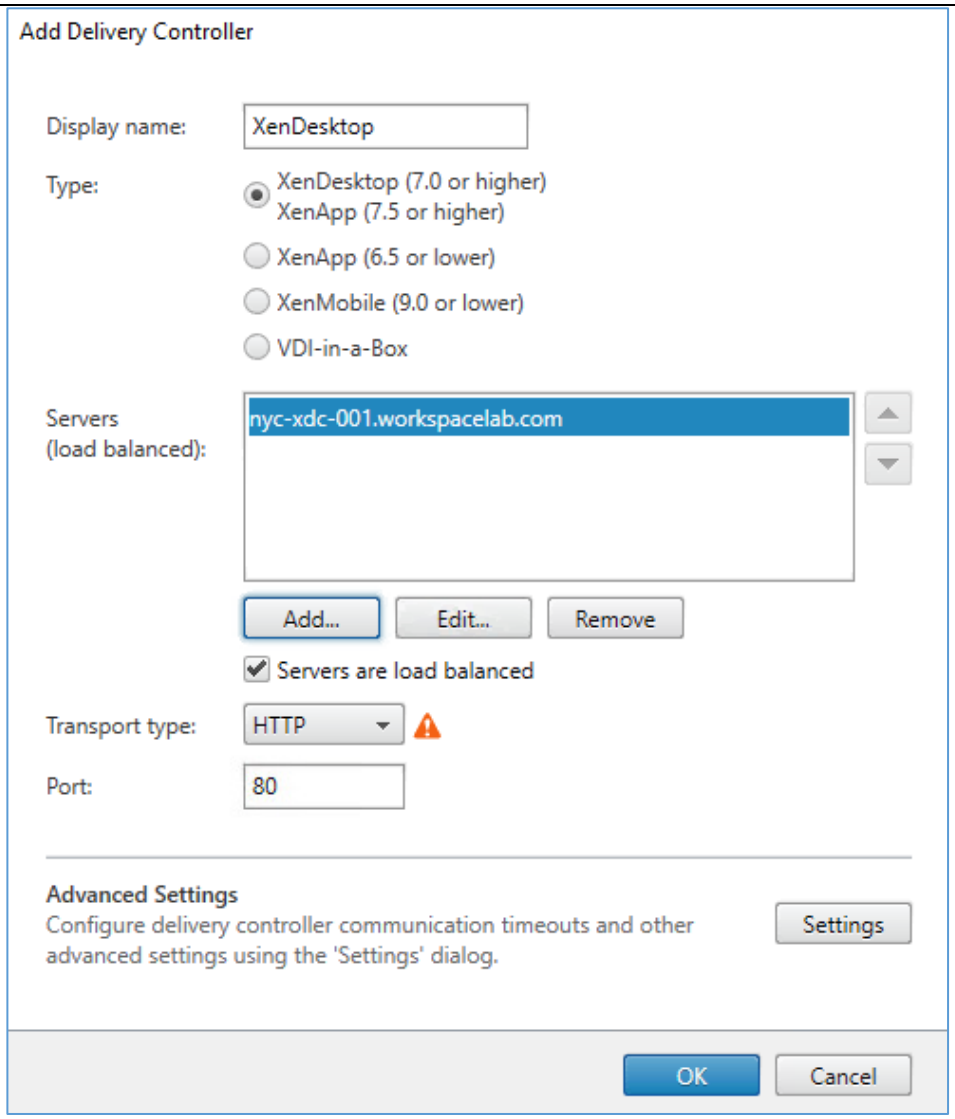


Note: A DNS entry was previously created for storefront.workspacelab.com to resolve to this StoreFront Server.

4.	On the Getting Started page, click **Next**. 
5.	On the Store Name page, enter **WWLabsStore** in the Store Name field.  Click **Next** to continue the new deployment creation wizard.
6.	Add a Delivery Controller to this new store deployment.

	On the Delivery Controllers page, below the box for Delivery Controllers, click **Add**. 

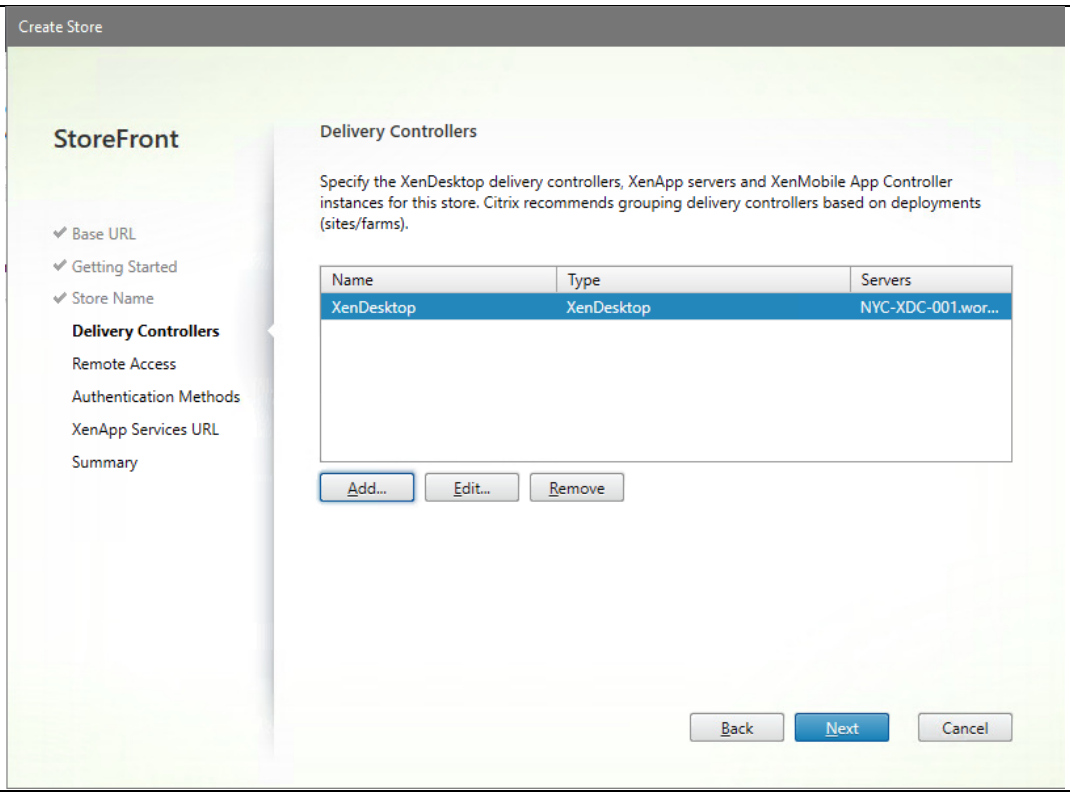
7.	Configure the following settings to add a Delivery Controller:
	• Display name: **XenDesktop**
	• Type: **XenDesktop (7.0 or higher) XenApp (7.5 or higher)**
	• Below the Servers box, click **Add**.
	  ○ Server name: **NYC-XDC-001.workspacelab.com**
	  ○ Click **OK**. The Delivery Controller should now appear in the Servers box.
	• Transport type: **HTTP**
	• Port: **80**
	
	Click **OK** to close the Add Delivery Controller dialog box.



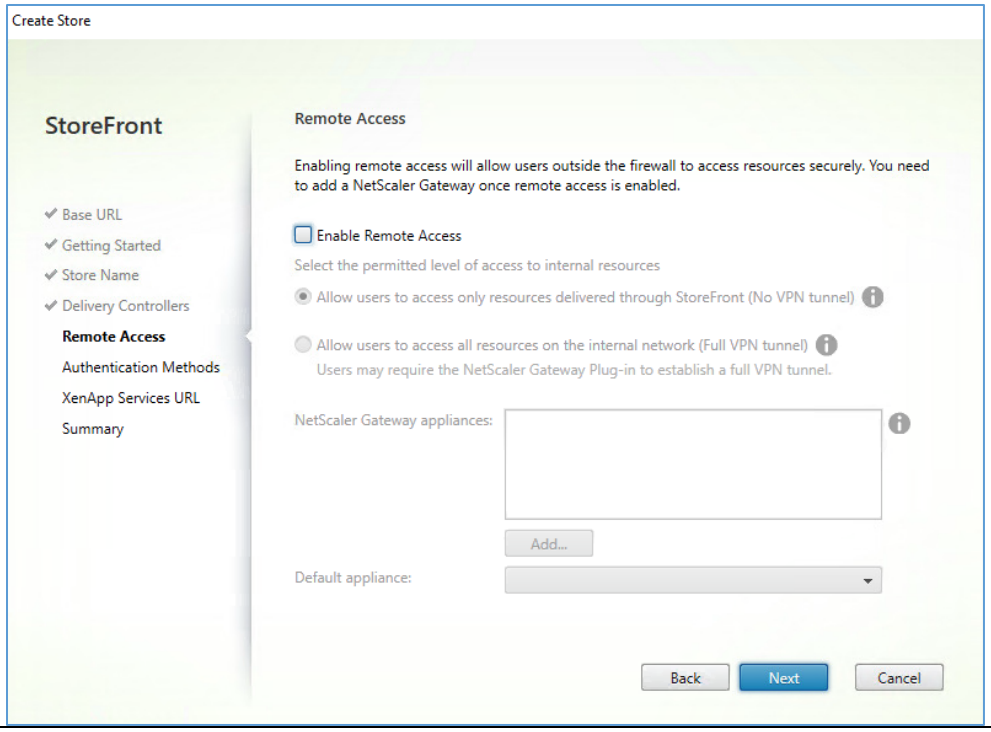
Note: On the Type field, setting XenDesktop (7.0 or Higher) XenApp (7.5 or Higher) is the base option for all FMA platforms both XenApp and XenDesktop combined.

Note: Although port 80 is used here, Citrix recommends using HTTPS. You will change this in a later exercise.

8. On the Delivery Controllers page, verify that the information appears correct and click **Next**.

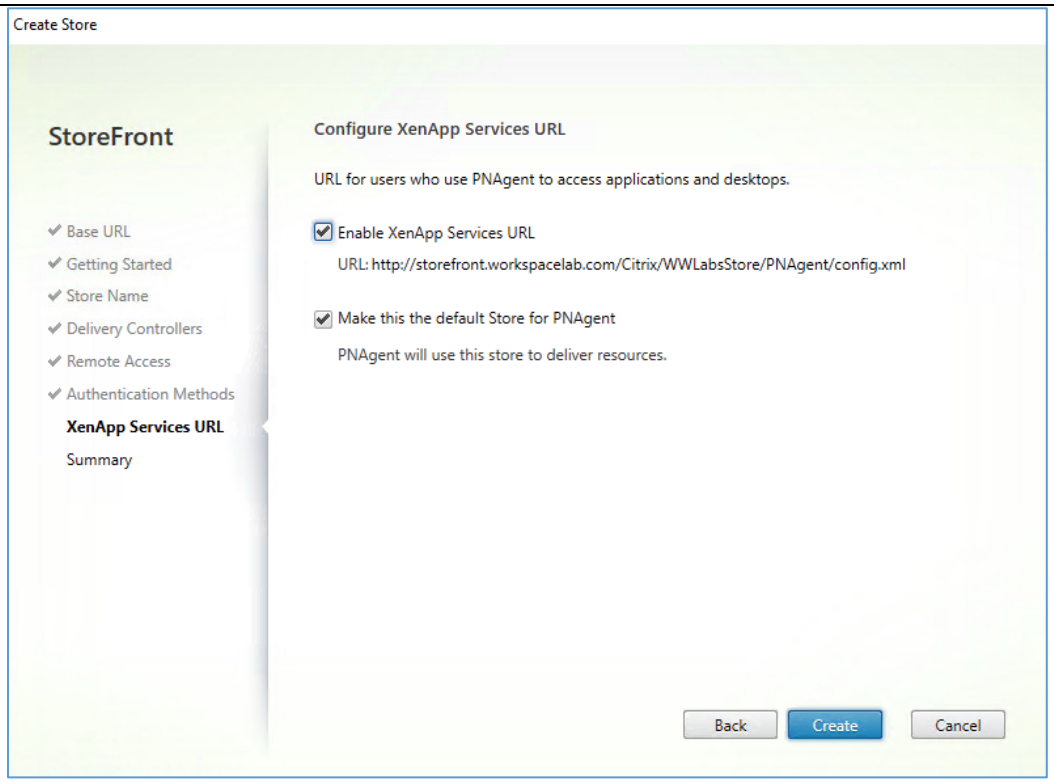


9. On the Remote Access page, leave the defaults and click **Next**.



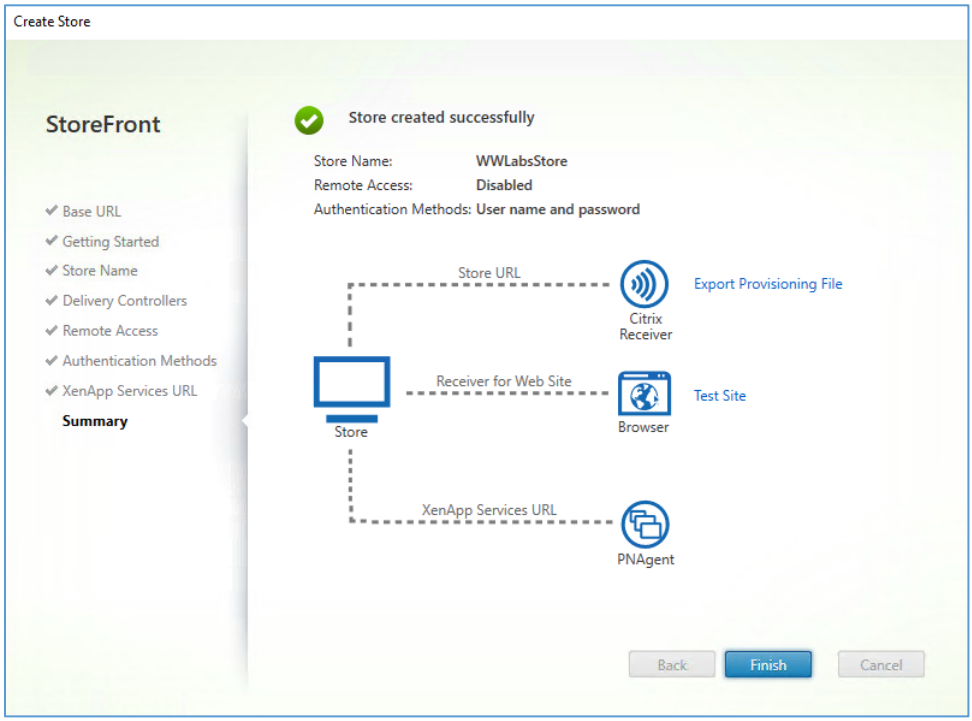
10. On the Configure Authentication Methods page, verify that **User name and password** is enabled and click **Next**.

11. On the XenApp Services URL page, leave the defaults and click **Create**.



Note: Creating the store will take a few minutes.

12. On the Summary page, click **Finish**.



Note: The website automatically created by the store deployment has the same address as the store, with the word *web* added at the end.

Key Takeaways:

- The initial configuration includes setting up a store and a website using the store.
- The base URL should be set to the name of the StoreFront Server or the name of a load balancer serving multiple StoreFront Servers.
- The store name chosen during this wizard will be presented to users either through the browser URL or when adding the store to Receiver.
- Citrix recommends securing the traffic between StoreFront and Delivery Controllers using SSL. Although port 80 is used in this exercise, this configuration is changed in a later exercise.

Exercise 5-3: Encrypt StoreFront store traffic

There is more than one method to encrypt StoreFront traffic. One method uses the Internet Information Services (IIS) Manager and the other does not. Both methods are valid here in this environment and by Citrix. You must choose either Option 1 or Option 2. You will be unable to perform the steps for both options.

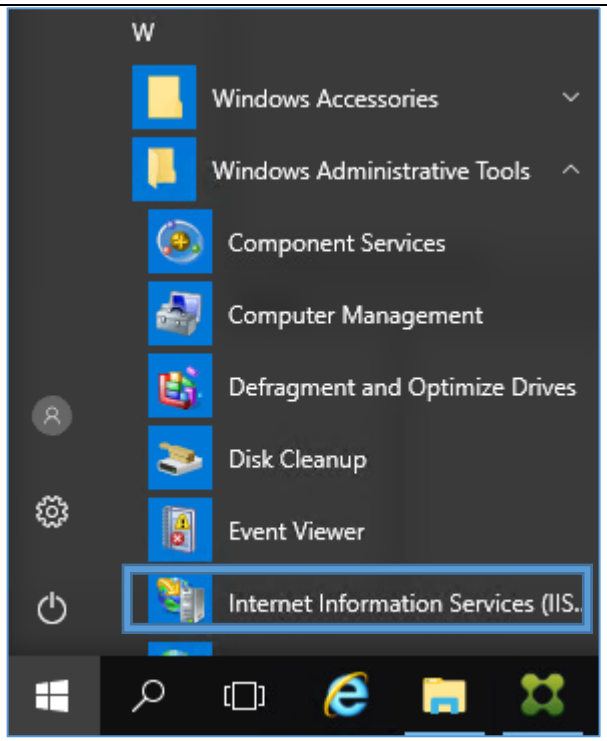
Scenario:

Your Lead Citrix Architect has informed you that network access to the Store must be secured to meet WW Labs standards. Encrypting traffic to StoreFront Servers is a leading practice since user credentials are sent over the network connection and need to be protected.

Your task is to secure network access to the StoreFront store by requesting and installing a valid SSL certificate on the StoreFront Server.

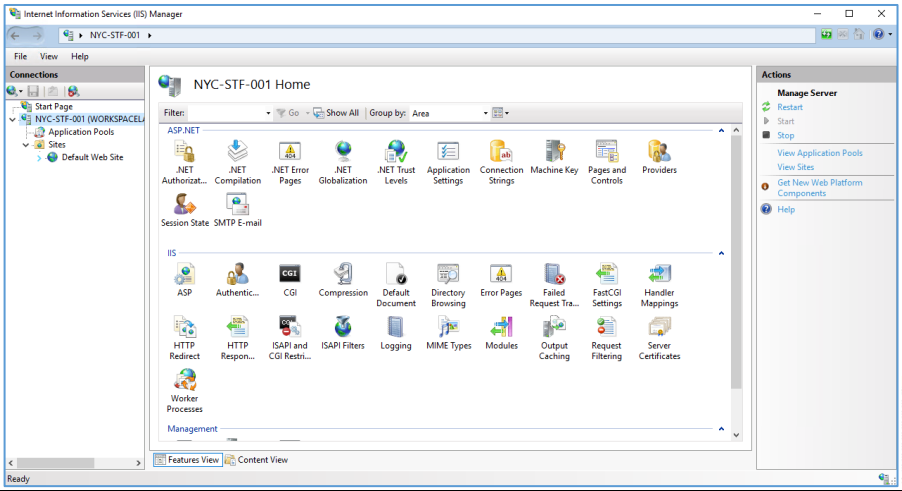
Option 1: Step-by-Step

Step	Action
1.	Using the Remote Desktop Connection Manager, confirm that you are still connected to **NYC-STF-001**. **Note:** In a previous exercise, you had logged on to NYC-STF-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-STF-001 by right-clicking this machine and selecting **Connect server**.
2.	Click **Start** and select **Windows Administrative Tools**. Open **Internet Information Services (IIS) Manager**.

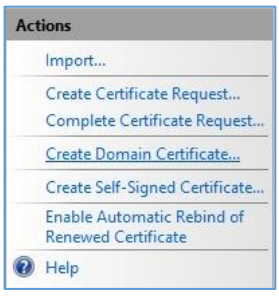


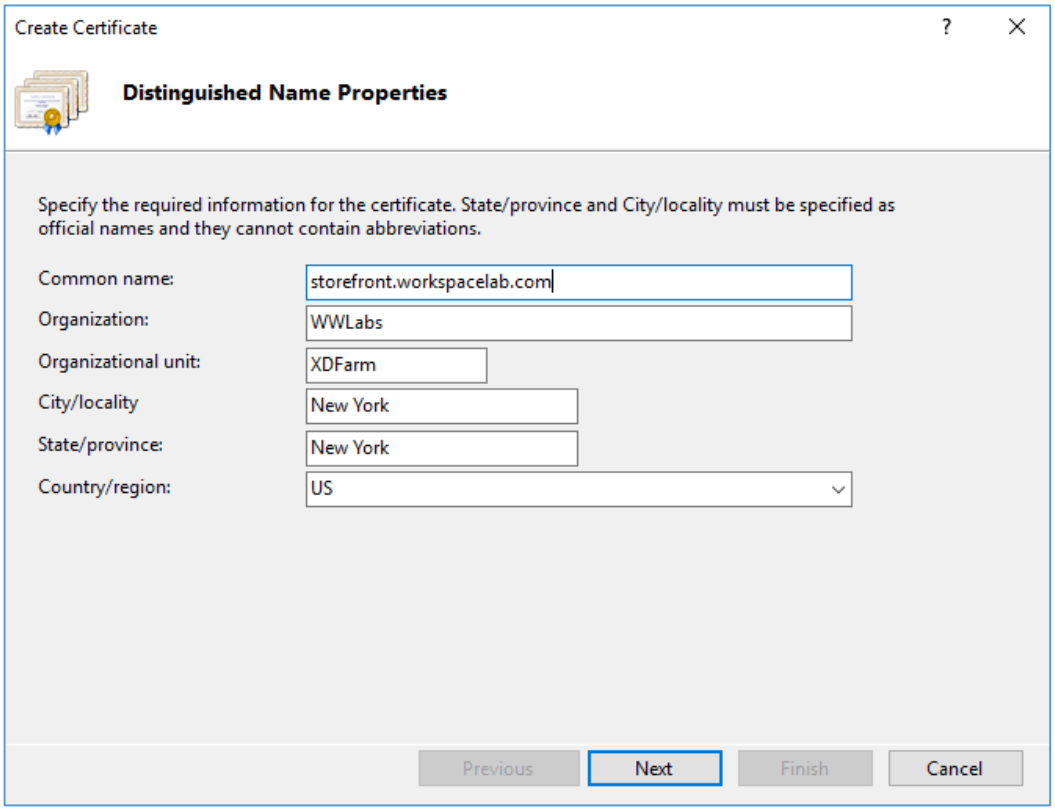
3. Using IIS, expand **NYC-STF-001 (WORKSPACELAB\Administrator).**

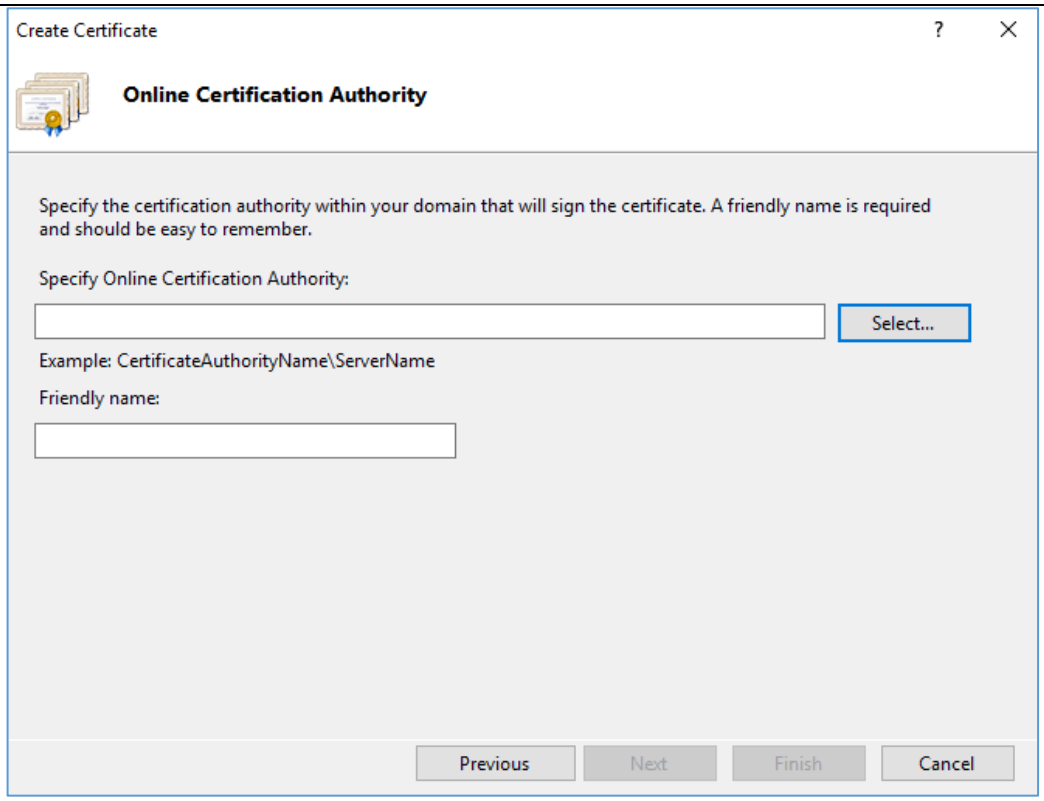
4. In the middle pane, double-click **Server Certificates**.



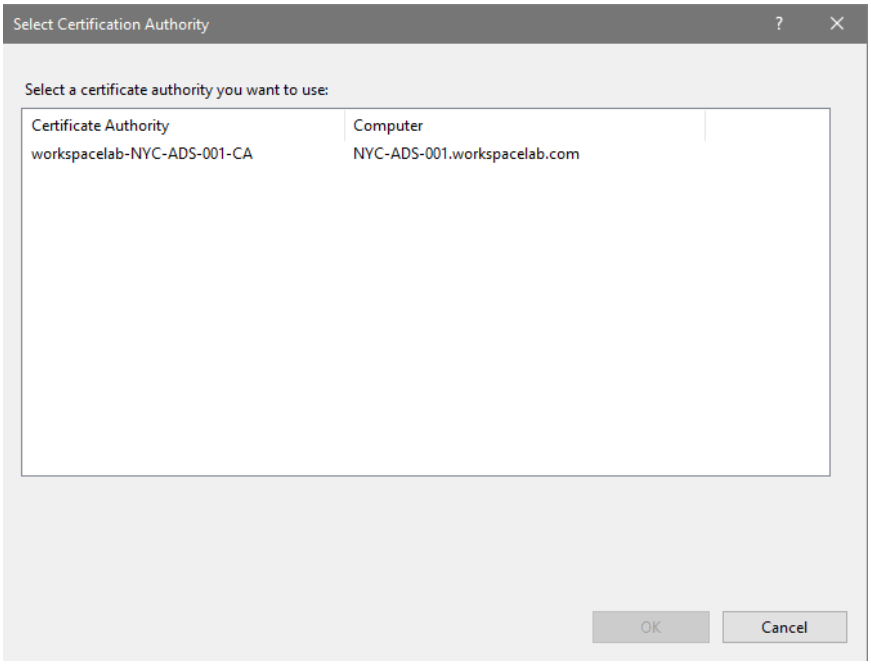
5. On the right pane under Actions, click **Create Domain Certificate**.



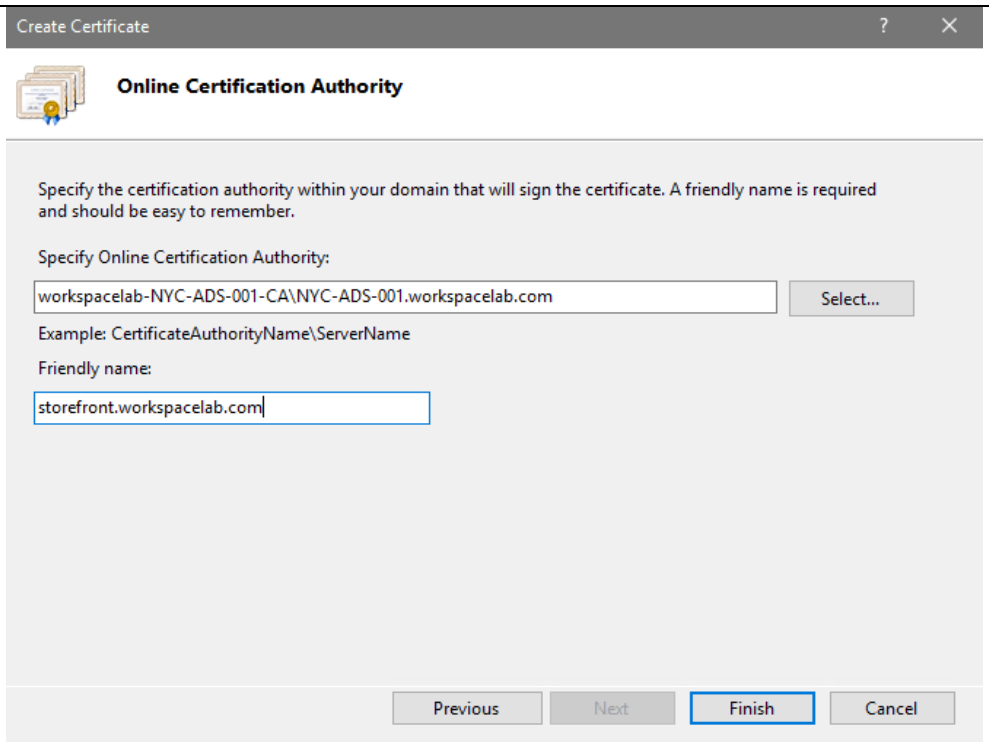
	Enter the following settings: • Common name: **storefront.workspacelab.com** • Organization: **WWLabs** • Organizational unit: **XDFarm** • City/locality: **New York** • State/province: **New York** • County/region: **US**  Click **Next**.
6.	On the Online Certificate Authority page, click **Select** to the right of Specify Online Certification Authority.



On the Select Certification Authority dialog box, select **workspacelab-NYC-ADS-001-CA** and click **OK**.

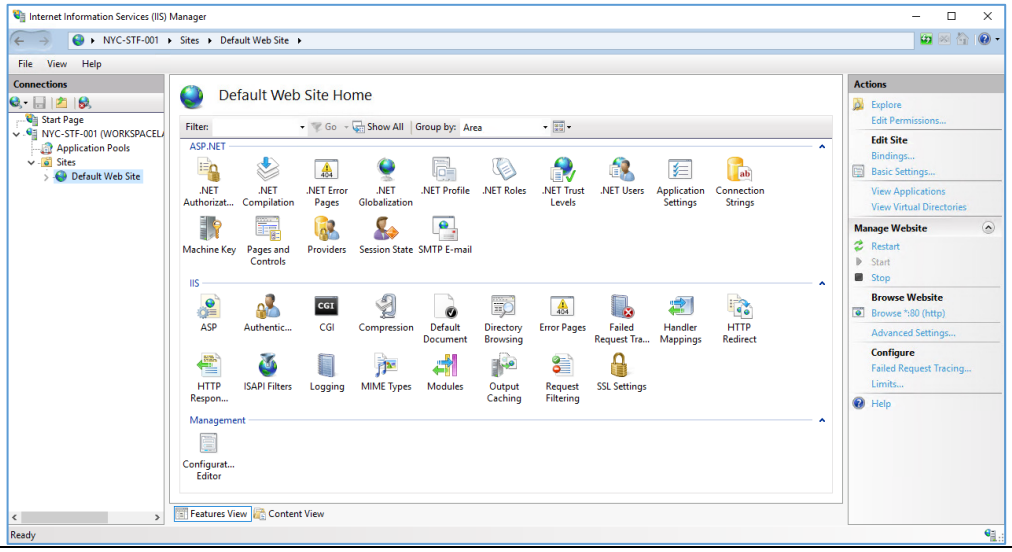


7.	Enter **storefront.workspacelab.com** in the Friendly name field.

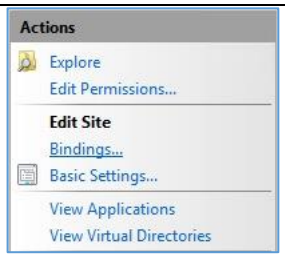


Click **Finish**.

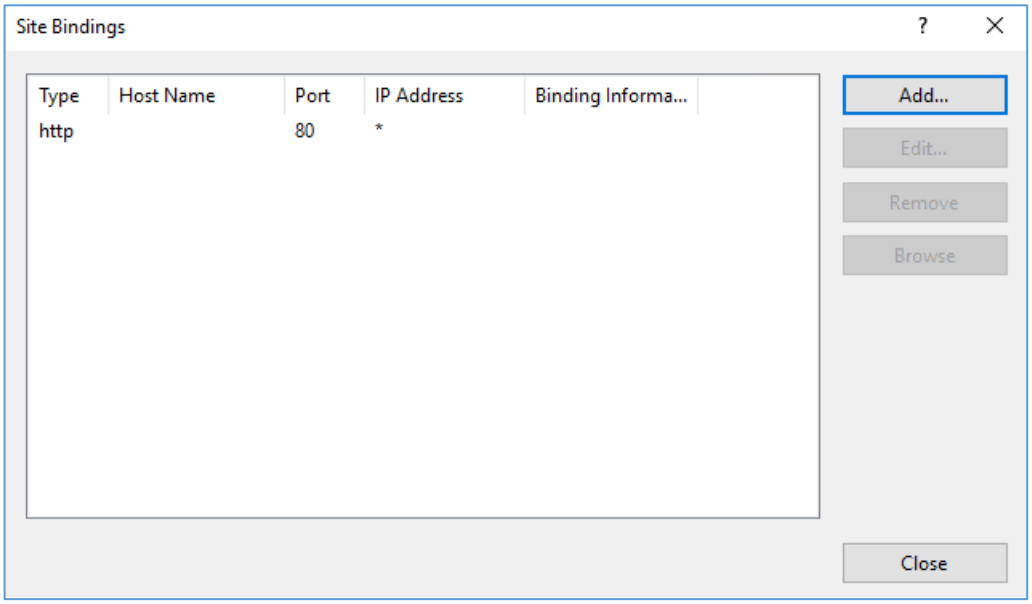
8. In IIS Manager, expand **NYC-STF-001 (WORKSPACELAB\Administrator)** > **Sites** and click **Default Web Site**.



9. On the right pane under Actions, click **Bindings**.

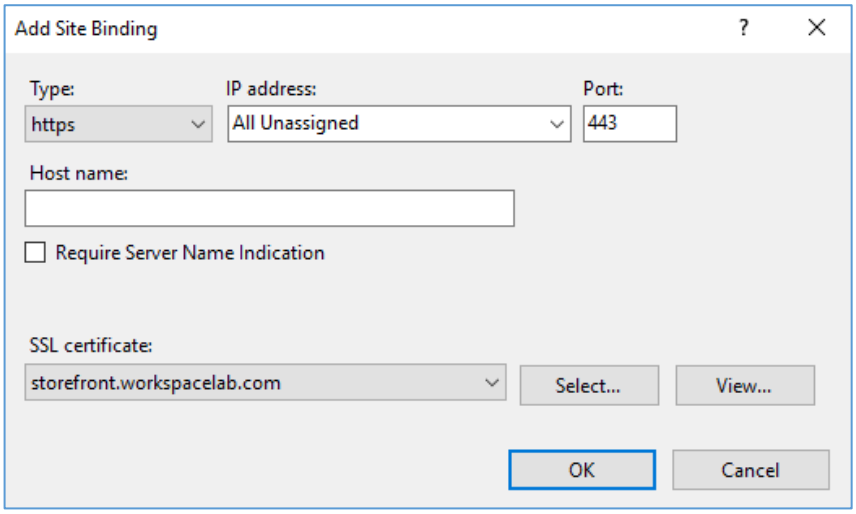


On the Site Bindings dialog box, click **Add**.

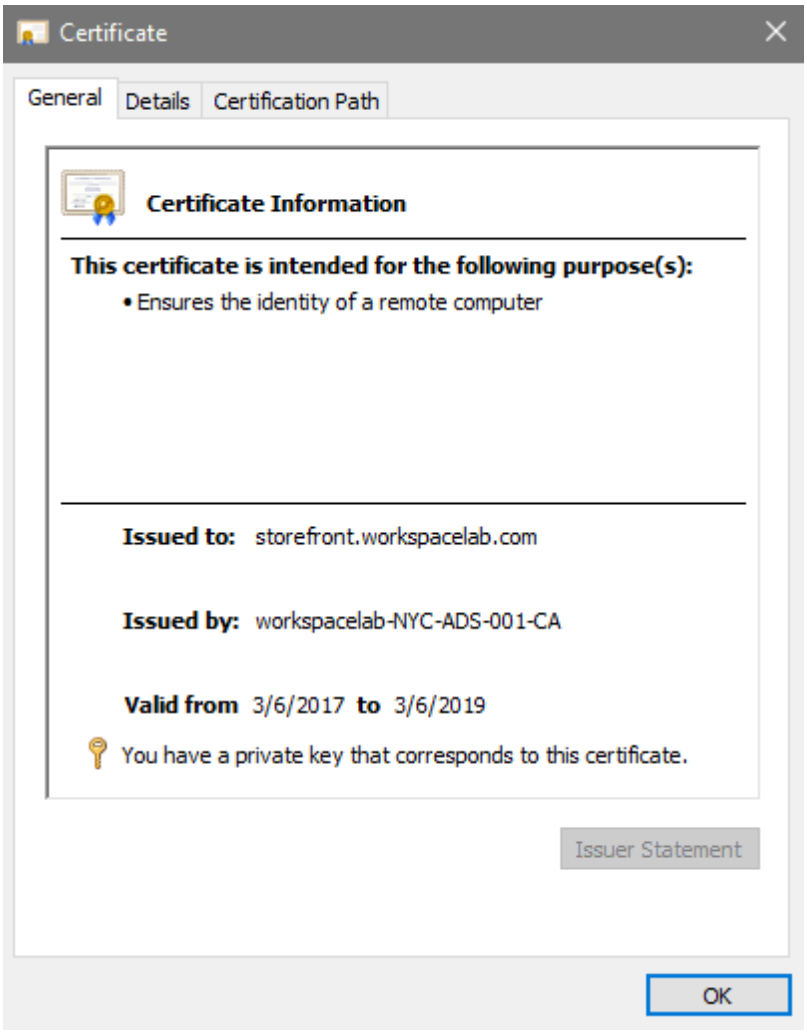


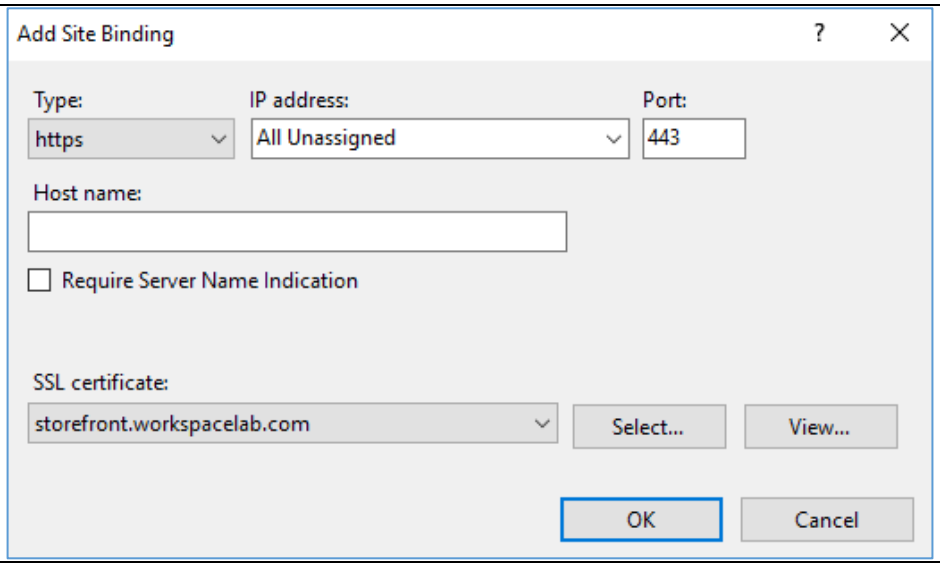
Set the Add Site Binding settings to the following:

- Type: **https**
- SSL certificate: **storefront.workspacelab.com**

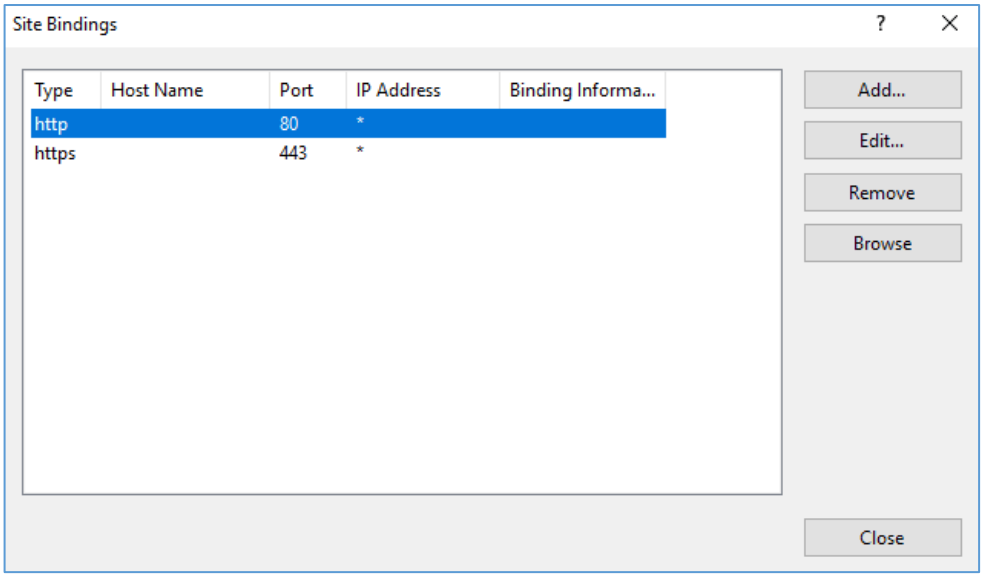


Click **View** to see that this is the SSL Certificate that you were tasked to create earlier.

	Click **OK** to close the Certificate details.  Click **OK** to close the Add Site Binding dialog box.

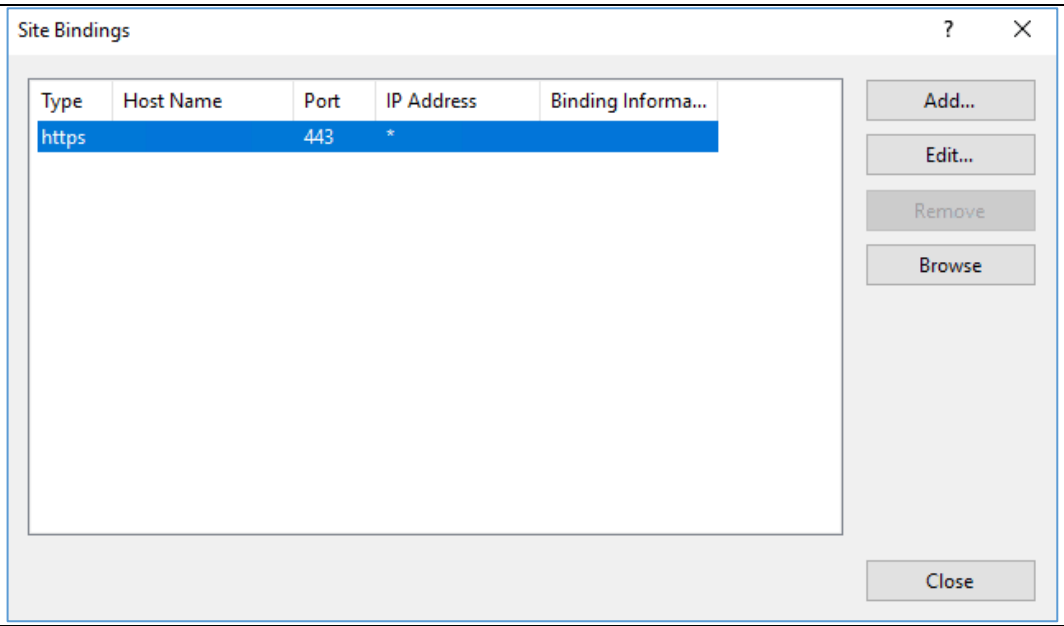
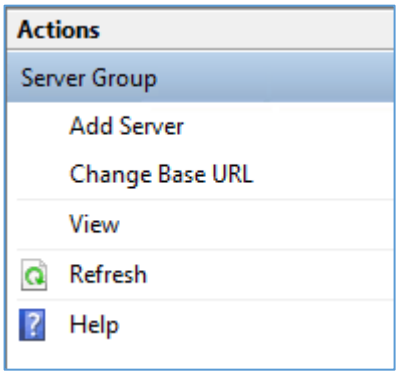


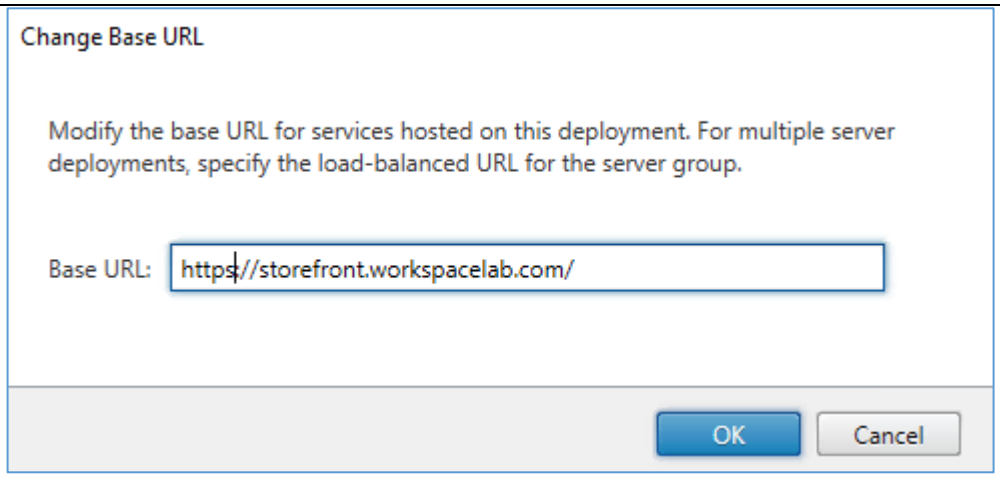
10. In the Site Bindings dialog box, select the **http** binding and click **Remove**.



Click **Yes** to accept.

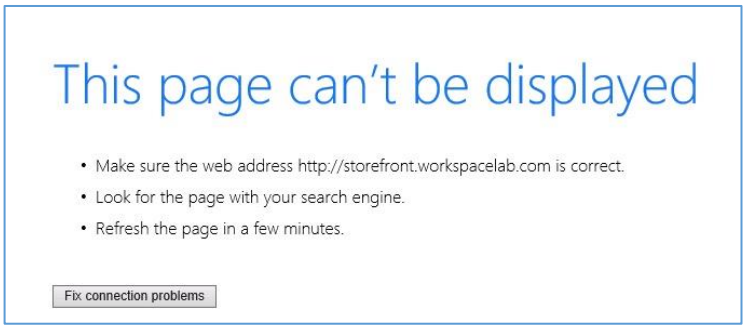
Click **Close** on the Site Bindings window.

	
11.	Close the **Internet Information Services (IIS) Manager** Console.
12.	Using the StoreFront Management Console, change the Base URL to respond to the new IIS Bindings with an SSL Certificate. In the left pane of the StoreFront console, select **Server Group** and then in the right pane click **Change Base URL**.  **Note**: The StoreFront Management Console was started in a previous exercise. If the console was closed in a previous exercise, then click Start > Citrix > Citrix StoreFront.
13.	In the Base URL field, enter **https://storefront.workspacelab.com** and click **OK**.



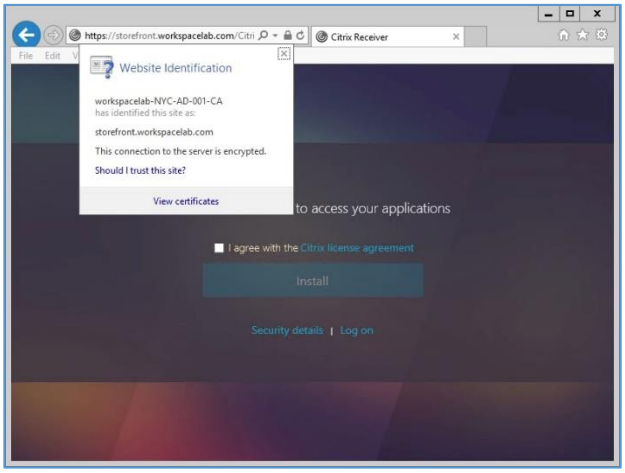
14. Open an Internet browser session and browse to the Store's website.

Start **Internet Explorer** from the Windows Taskbar and browse to **http://storefront.workspacelab.com/Citrix/WWLabsStoreWeb**



Note: The StoreFront server is no longer listening on insecure requests on port 80 using the HTTP Protocol.

15. Close and re-open **Internet Explorer**. Browse to **https://storefront.workspacelab.com/Citrix/WWLabsStoreWeb**



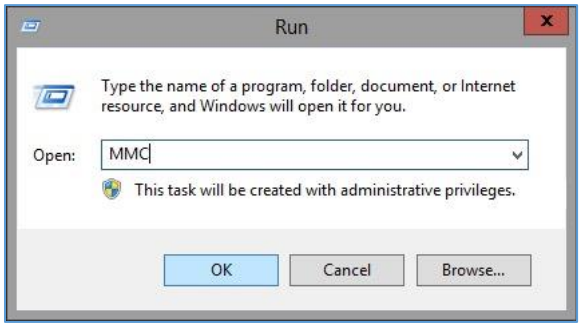
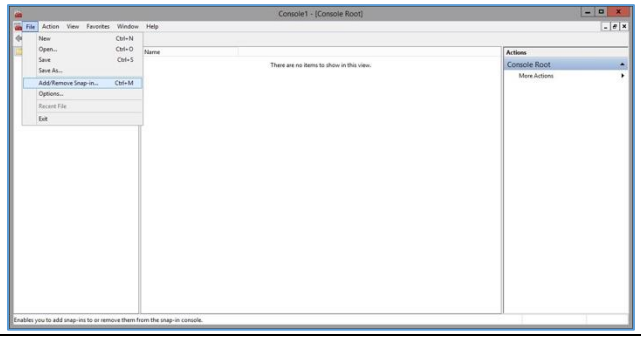
	Note: Notice that the StoreFront site is displayed and is using a secured connection. You can view this secured connection information by clicking the small lock symbol to the right side of the site URL in the browser. Close **Internet Explorer**.

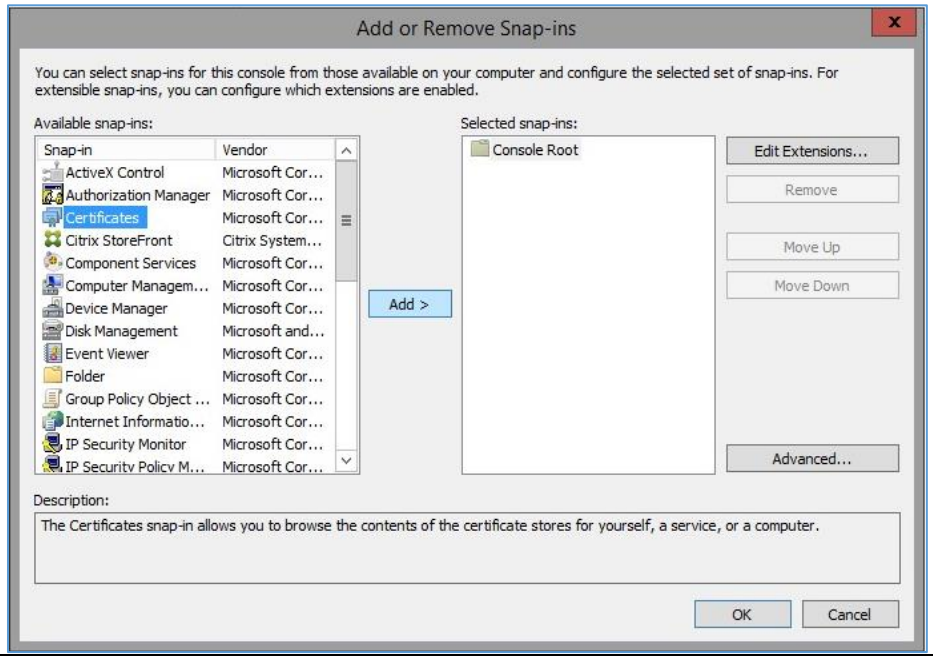
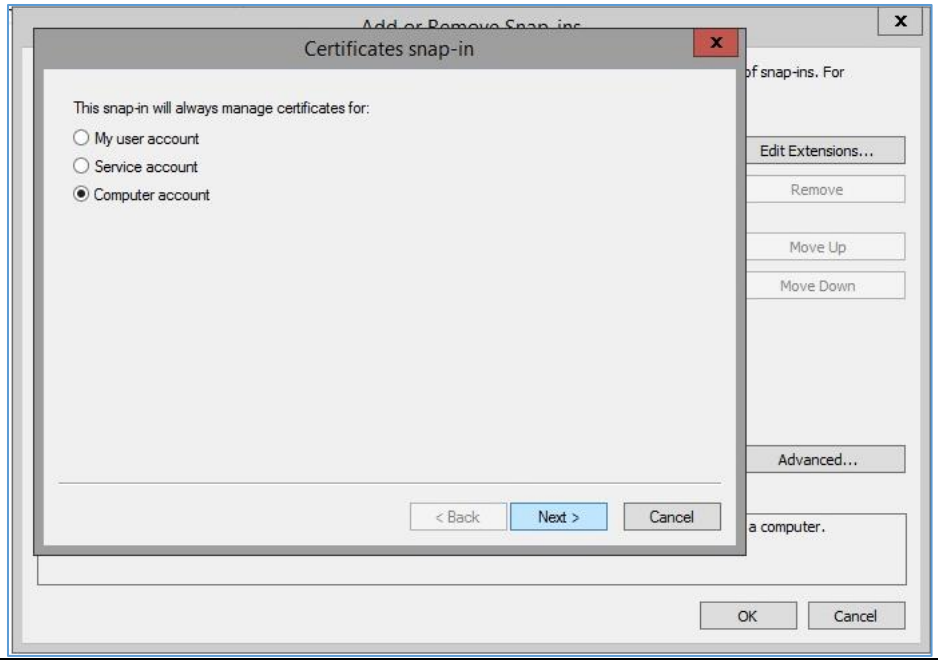
Key Takeaways:

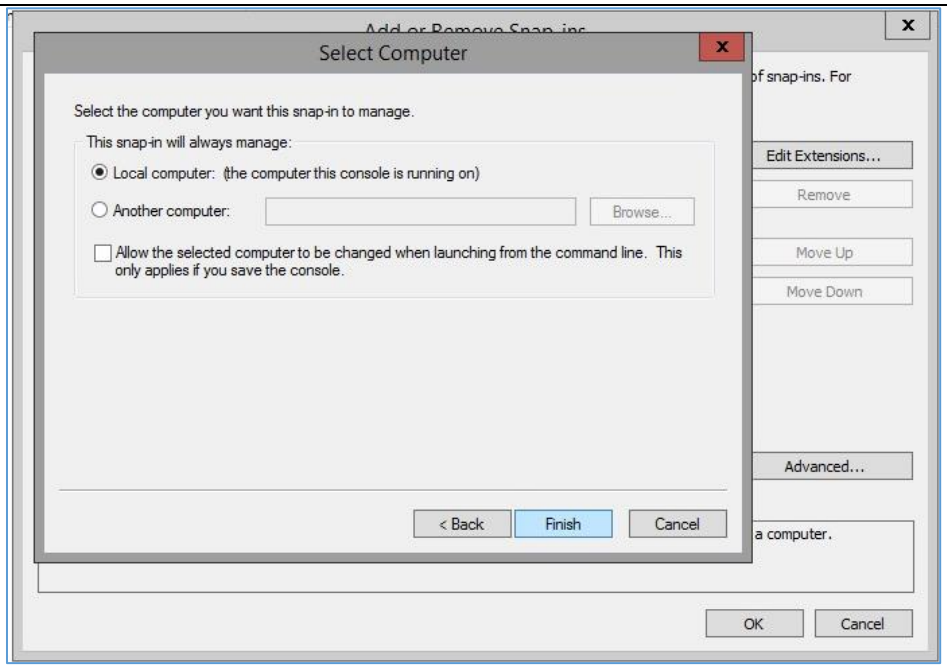
- Since credentials of the users will be sent to StoreFront, access should be secured against attacks using SSL.
- StoreFront needs a certificate where the subject name (or DNS alternate name) matches the configured base URL.

Option 2: Step-by-Step

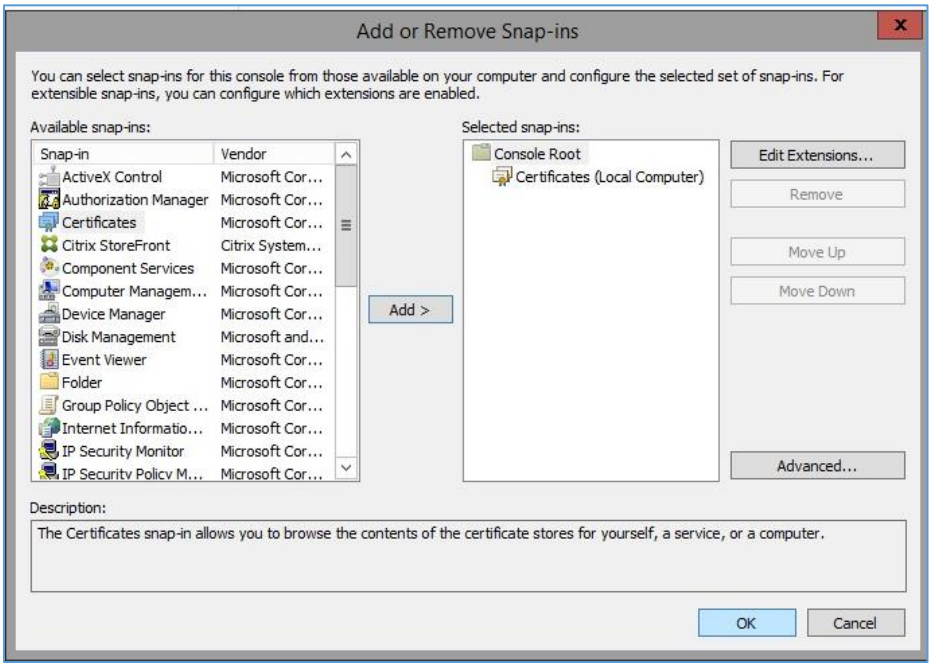
If you have completed Exercise 5.3 Option 1, this exercise must be skipped.

Step	Action
1.	Using the Remote Desktop Connection Manager, confirm that you are still connected to **NYC-STF-001**. **Note:** In a previous exercise, you had logged on to NYC-STF-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-STF-001 by right-clicking this machine and selecting Connect Server.
2.	Right-click **Start** > click **Run** > type **MMC** and click **OK** or press **Enter** on the keyboard to open the MMC snap-in.  In the MMC console, click **File** and select **Add/Remove Snap-in**. 

3.	On the Add or Remove Snap-ins dialog box, in the left side of the box, select **Certificates** and click **Add**. 
4.	On the Certificates snap-in page, select **Computer account** and click **Next**. 
5.	On the Select Computer page, verify that **Local Computer** is selected and click **Finish**.



Click **OK** to close the Add or Remove Snap-ins window.

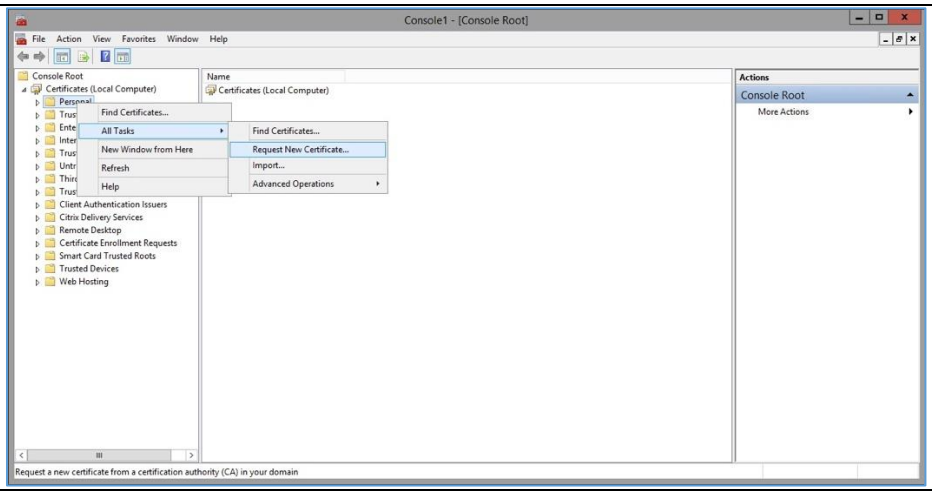
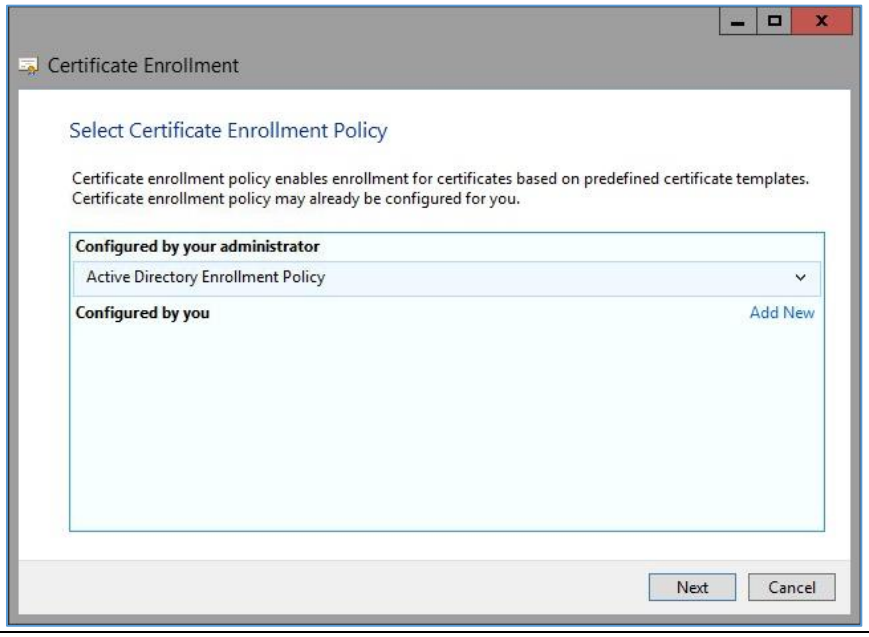


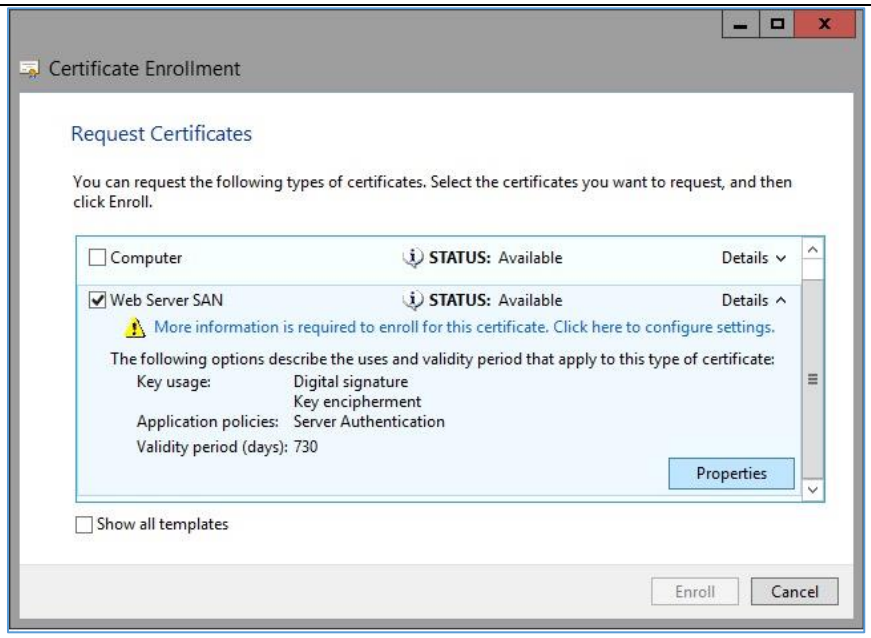
Note: Local computer is selected since you want to enumerate the certificate snap-in running on this local machine. In order to enumerate the Certificate snap-in for another machine, you would select the Another computer radio button and browse to it.

6. Using the Certificates MMC Snap-in, request a new certificate.

   In the left side of the snap-in, expand the **Certificates (Local Computer)** section.

   Right-click **Personal,** select **All Tasks**, and then select **Request New Certificate**.

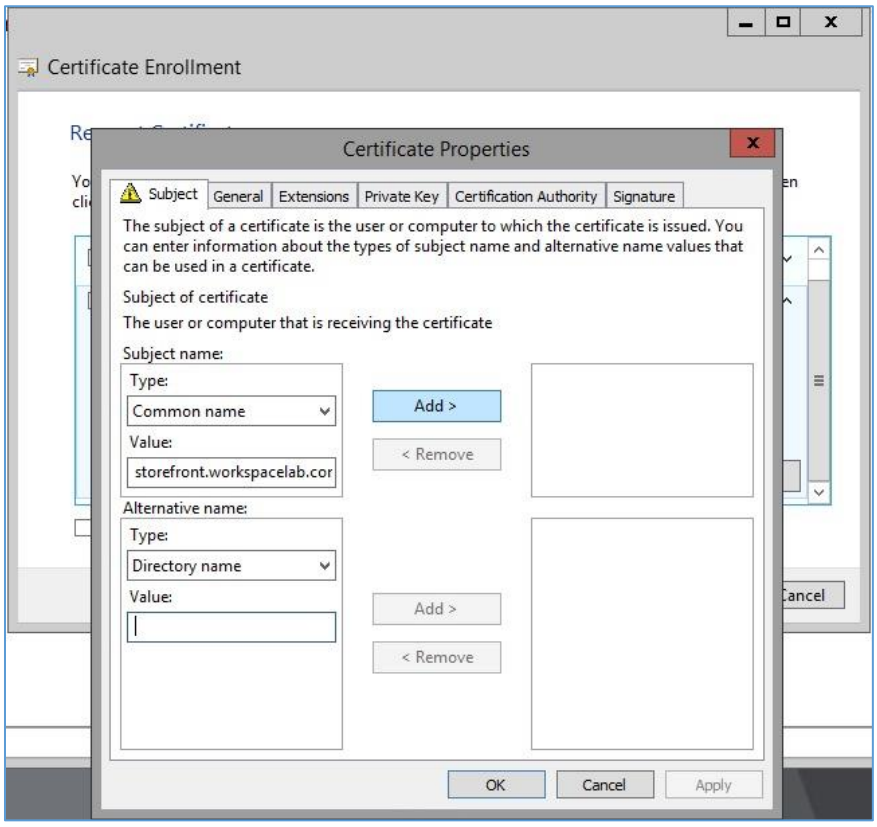
	
7.	On the Certificate Enrollment page, click **Next**.
8.	On the Select Certificate Enrollment Policy page, verify that **Active Directory Enrollment Policy** is highlighted and click **Next**. 
9.	On the Request Certificates page, select **Web Server SAN**. Click the **Details** drop-down and click **Properties**.



Under the Subject name field, configure the following:

- Type: **Common name**
- Value: **storefront.workspacelab.com**

Click **Add**.

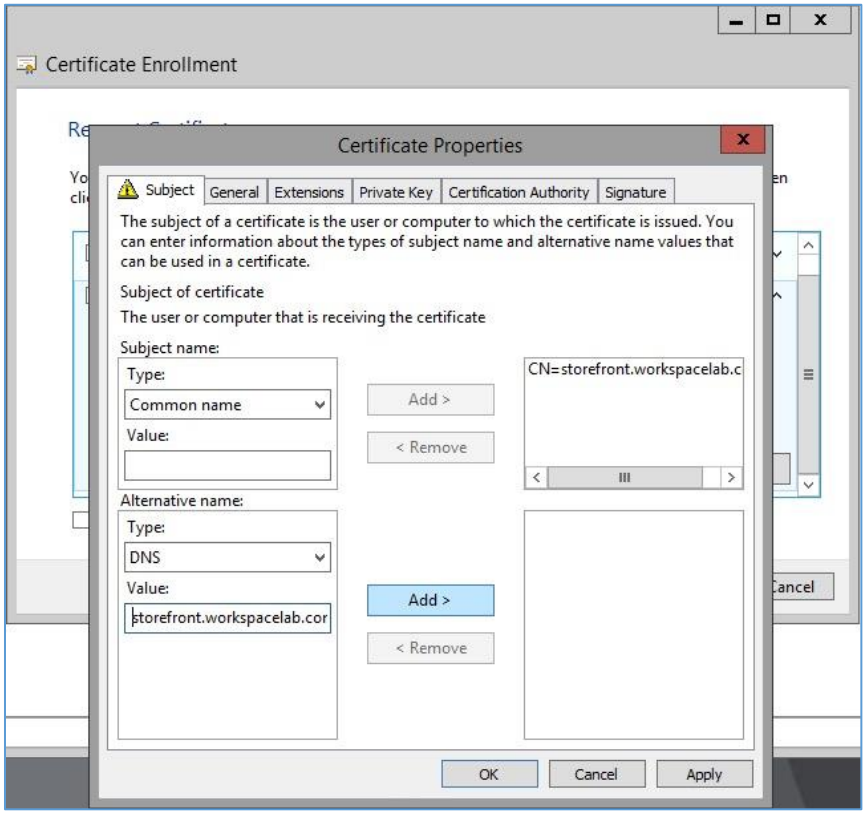


Under the Alternative name field, configure the following:

- Type: **DNS**

- Value: **storefront.workspacelab.com**

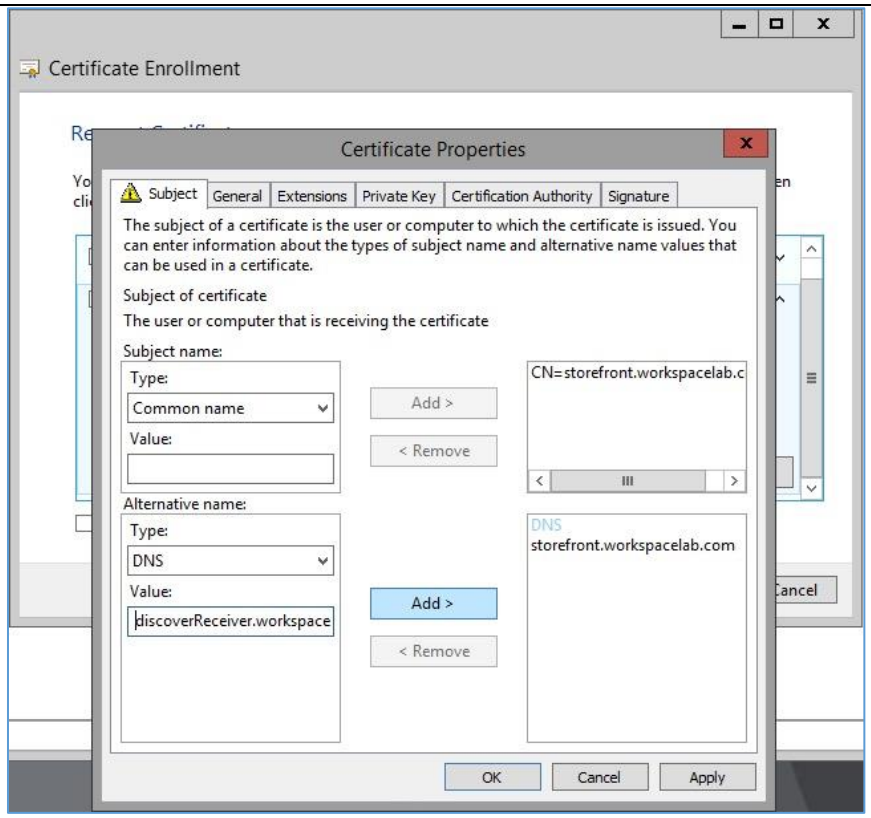
Click **Add**.



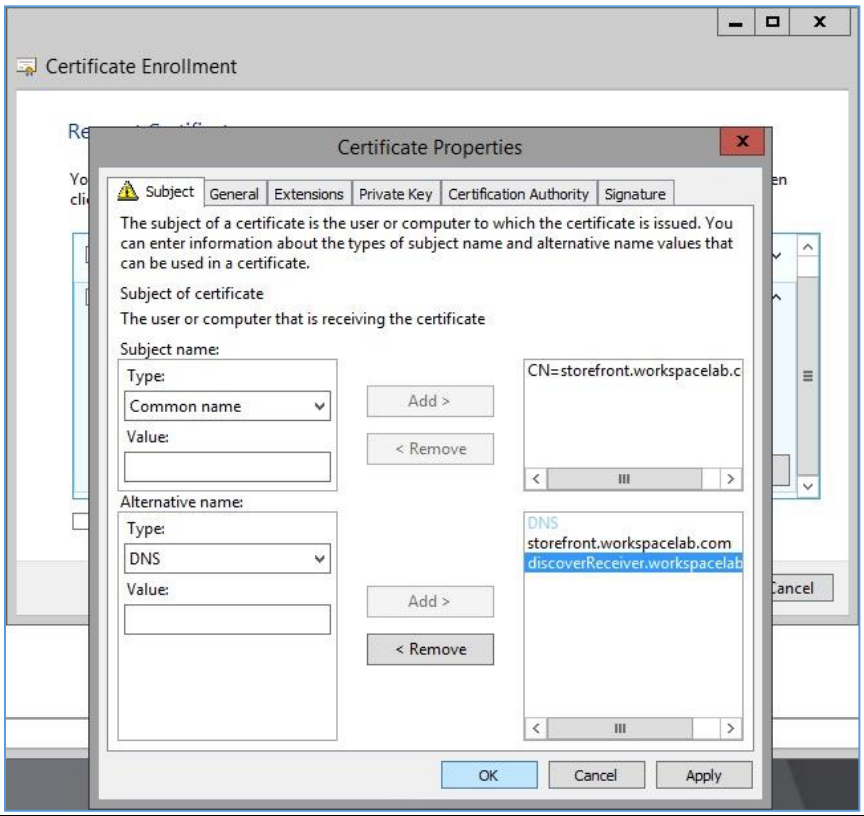
Under the Alternative name field, configure a second entry:

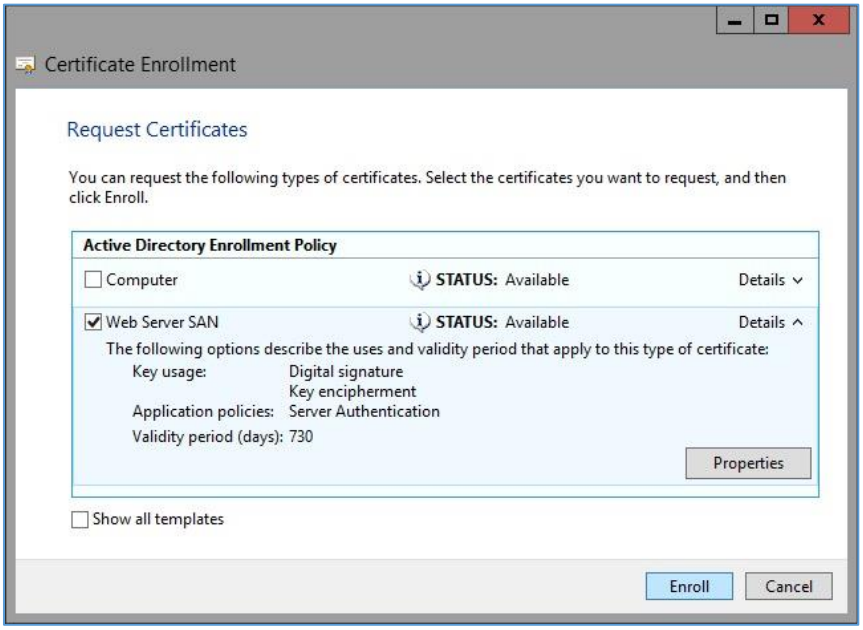
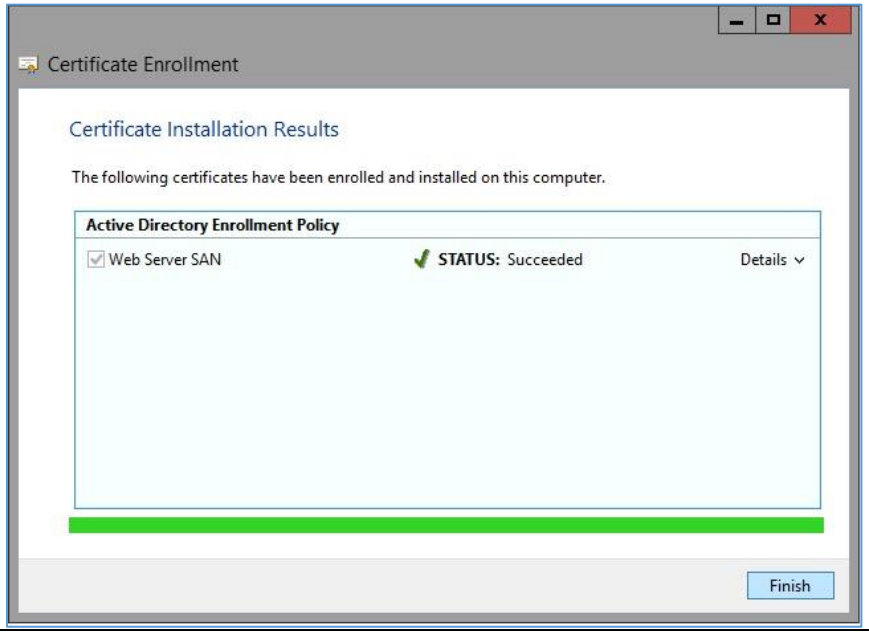
- Type: **DNS**
- Value: **discoverReceiver.workspacelab.com**

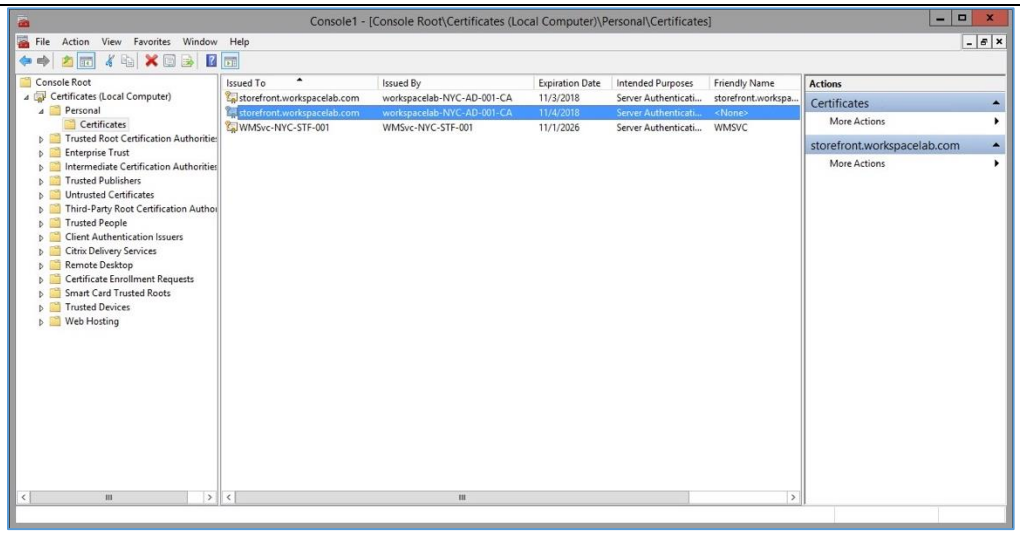
Click **Add**.



In the Certificate Properties dialog box, click **OK**.



10.	On the Request Certificates page, click **Enroll**.  After the request is complete, click **Finish**. 
11.	Verify that the certificate now appears in the Personal > Certificates store. From the MMC Certificate Console, expand **Certificates (Local Computer)** > **Personal** > and click **Certificates**, and verify that the certificate appears.

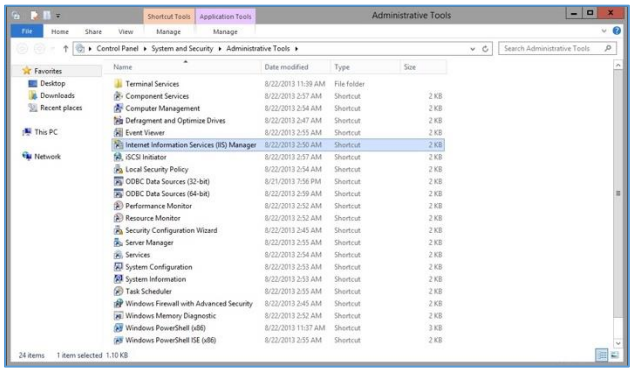


Note: Please ignore if you see any other certificates in your lab.

Close the **MMC console** window.

When prompted to save the Microsoft Management Console settings, select **No**.

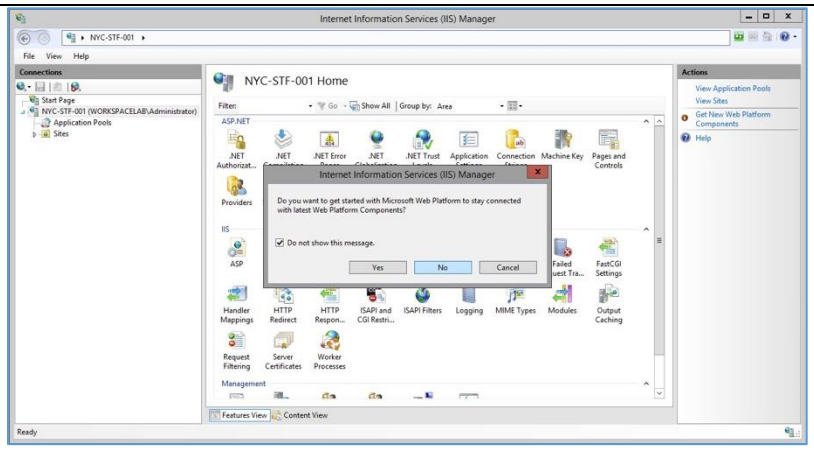
12. Click **Start** and select **Administrative Tools**. Double-click **Internet Information Services (IIS) Manager**.



Note: Internet Information Services (IIS) Manager can also be opened from the Server Manager window. Click the Server Manager icon in Task Bar > click Tools > and then click Internet Information Services(IIS)Manager.

13. Using Internet Information Services, expand **NYC-STF-001 (WORKSPACELAB\Administrator).**

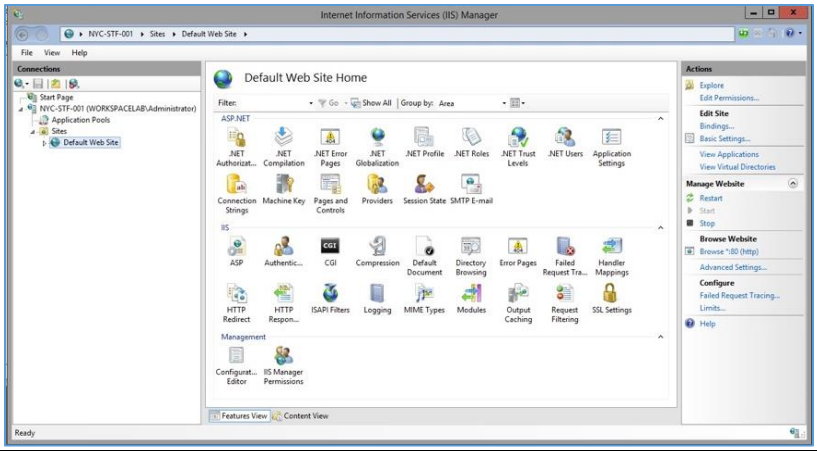
In the Internet Information Services (IIS) Manager dialog box, select **Do not show this message again** and click **No**.



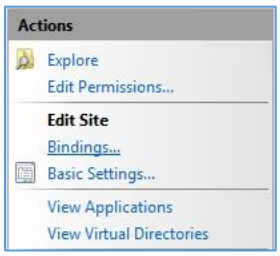
Note: If you click Yes on the dialog box, Internet Explorer will open and will take you to http://www.microsoft.com/web/downloads/platform.aspx providing information about IIS 5.0.

Note: Please ignore if you don't see this prompt.

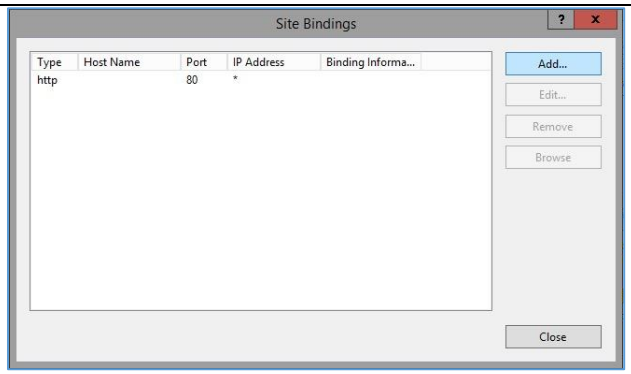
14. In IIS Manager, expand **NYC-STF-001 (WORKSPACELAB\Administrator)** > **Sites** and click **Default Web Site.**



15. On the right pane under Actions, click **Bindings**.

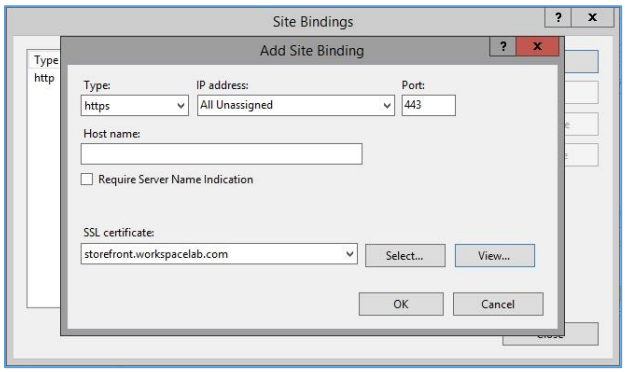


On the Site Bindings dialog box, click **Add**.

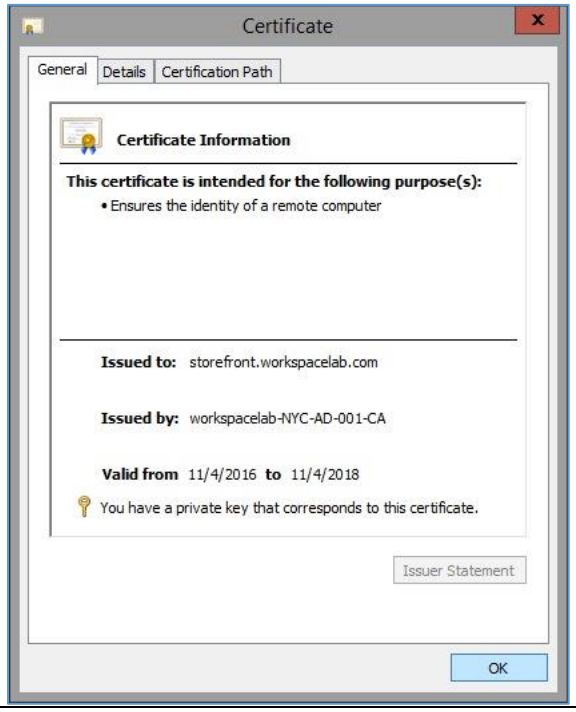


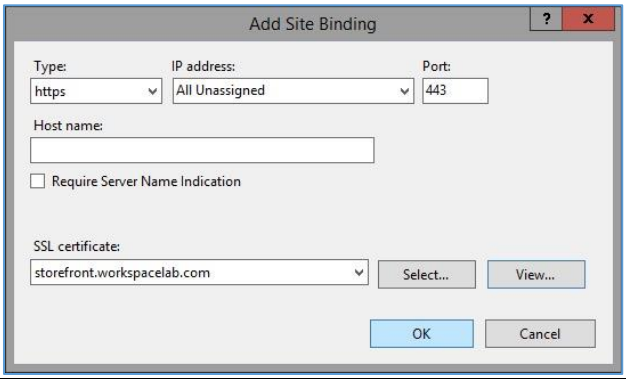
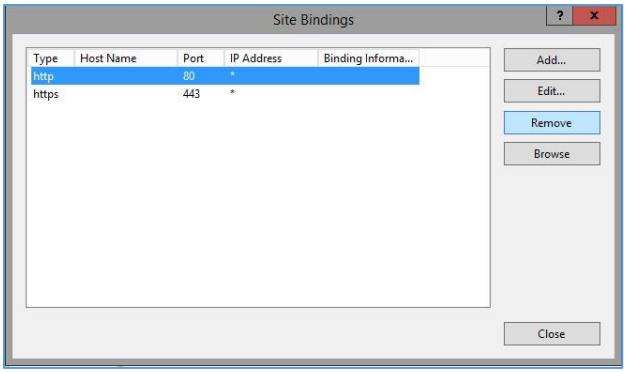
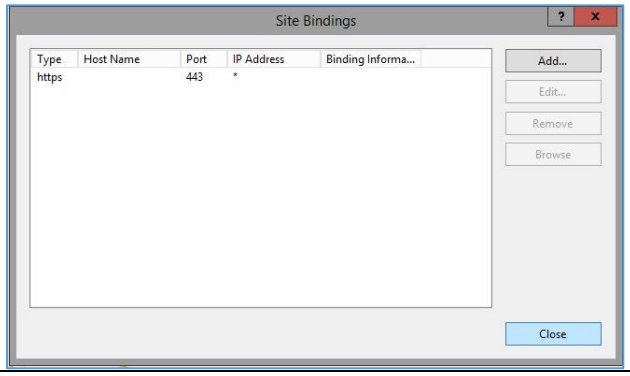
Set the Binding settings to the following:

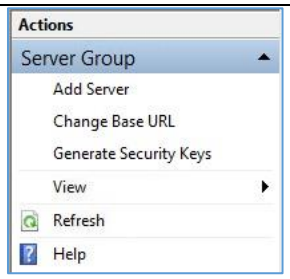
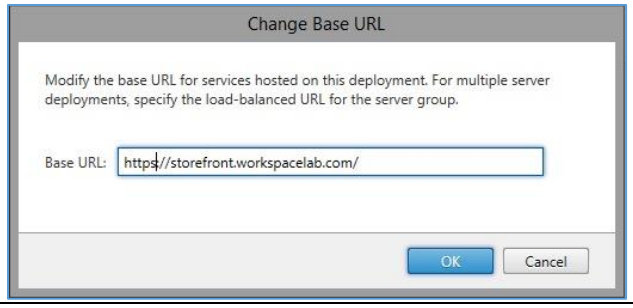
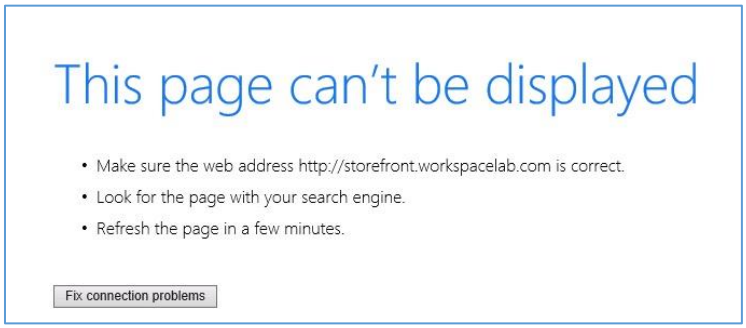
- Type: **https**
- SSL Certificate: **storefront.workspacelab.com**

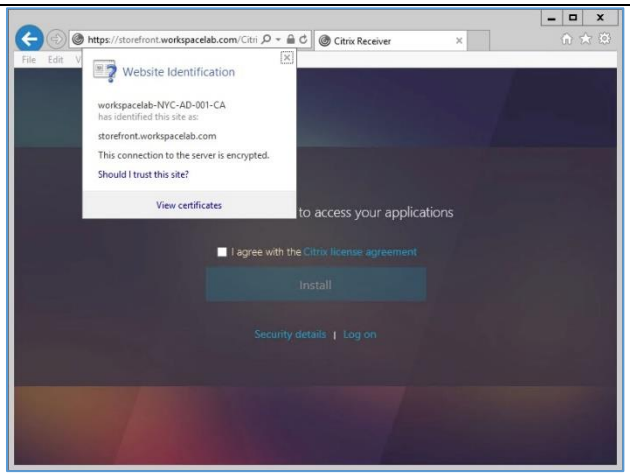


Click **View** to see that this is the SSL Certificate that you were tasked to create earlier. Click **OK** to close the Certificate details.



	Click **OK** to close the Bindings dialog box. 
16.	In the Site Bindings dialog box, select the **http** binding and click **Remove**.  Click **Yes** to accept. Click **Close** on the Site Bindings window. 
17.	Close the **Internet Information Services (IIS) Manager** Console.
18.	Using the StoreFront Management Console, change the Base URL to respond to the new IIS Bindings with an SSL Certificate. In the left pane of the StoreFront console, select **Server Group** and then in the right pane click **Change Base URL**.

	 **Note**: The StoreFront Management Console was started in a previous exercise. If the console was closed in a previous exercise, then click Start > Citrix > and click Citrix StoreFront.
19.	In the Base URL field, enter **https://storefront.workspacelab.com** and click **OK**. 
20.	Open an Internet browser session and browse to the Store's website. Start Internet Explorer and browse to **http://storefront.workspacelab.com/Citrix/WWLabsStoreWeb**.  **Note**: The StoreFront server is no longer listening on insecure requests on port 80 using the HTTP Protocol.
21.	Close and re-open **Internet Explorer**. Browse to **https://storefront.workspacelab.com/Citrix/WWLabsStoreWeb**.

	 **Note**: Notice that the StoreFront site is displayed and is using a secured connection. You can view this secured connection information by clicking the small lock symbol to the right side of the site URL in the browser. Close **Internet Explorer**.

Key Takeaways:

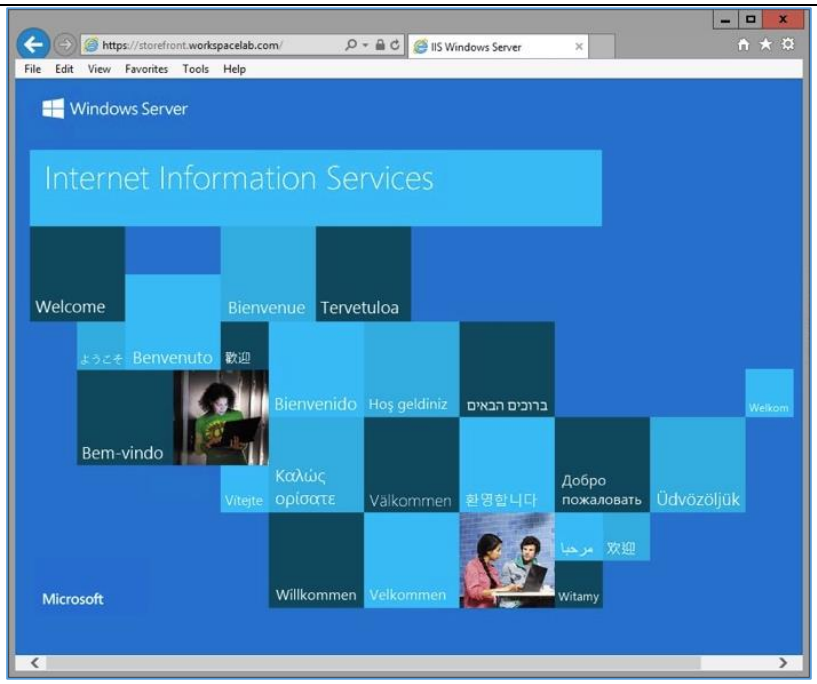
- Since credentials of the users will be sent to StoreFront, access should be secured against attacks using SSL.
- Storefront needs a certificate where the subject name (or DNS alternate name) matches the configured base URL.
- By default, Citrix Receiver does not accept adding a store using HTTP.

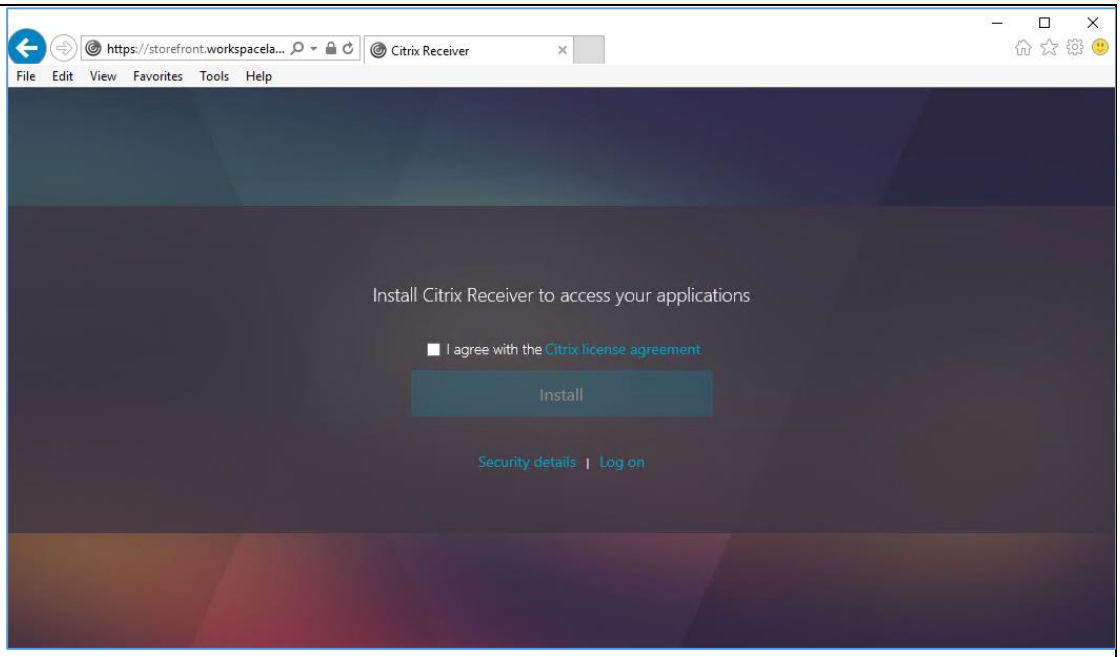
Exercise 5-4: Set the StoreFront default page

Scenario:

WW Labs has a written policy to address all web site parameters hosted on company systems. Your task is to redirect users from the current default landing page of the StoreFront webserver to a special logon page provided by StoreFront.

Step	Action
1.	Using the Remote Desktop Connection Manager, confirm that you are still connected to **NYC-STF-001**. **Note:** In a previous exercise, you had logged on to NYC-STF-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-STF-001 by right-clicking this machine and selecting Connect server.
2.	Open an Internet browser and navigate to the default store address. Start **Internet Explorer** and browse to **https://storefront.workspacelab.com**

	 **Note**: The site does not redirect to the Receiver for Web site. Instead it displays the default IIS page.
3.	Open the StoreFront console. Click **Start** > **Citrix** > **Citrix StoreFront**.
4.	In the left side of the StoreFront console, select **Stores**. In the middle pane, verify that **WWLabsStore** is selected, and then in the right side of the console, click **Set Default Website**.
5.	In the Set Default Website dialog box, select **Set a Receiver for Web site as the default page in IIS** and verify that the following settings are configured: • Store: **WWLabsStore** • Receiver for Web Sites: **/Citrix/WWLabsStoreWeb** Click **OK**.
6.	Open an Internet browser to test your connection to the default store address and to verify that the redirect you configured works as expected. Open **Internet Explorer** and navigate to **https://storefront.workspacelab.com**. **Note:** If Internet Explorer is still open from a previous exercise, close Internet Explorer and reopen it. **Note:** The Receiver for Web page now displays with the full URL pointing to https://storefront.workspacelab.com/Citrix/WWLabsStoreWeb.

	 Close **Internet Explorer**.

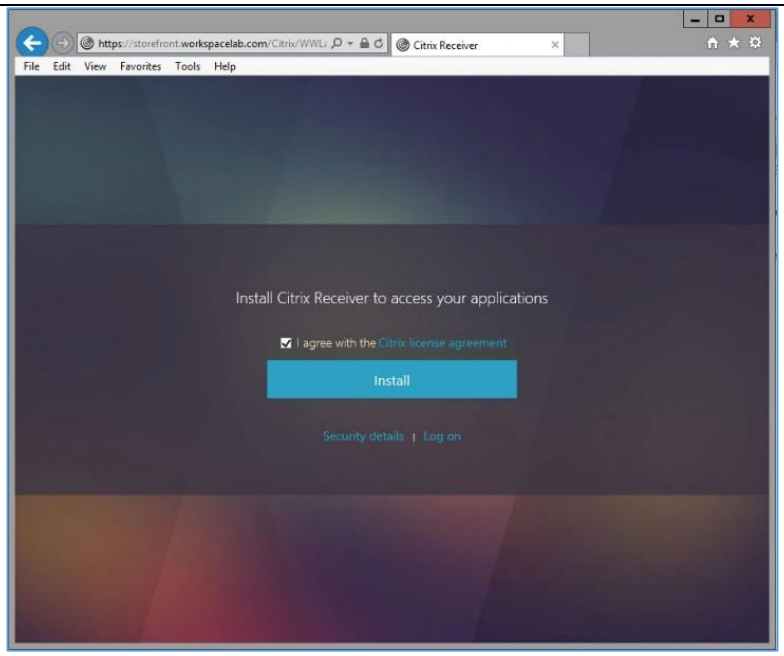
Key Takeaways:

- Microsoft IIS can be configured to automatically direct users to a default StoreFront site without users needing to enter the full path to the store. The Microsoft URL Rewrite extension allows HTTP requests to be redirected to HTTPS.
- If multiple StoreFront Servers are used, implement the same redirection on all of them.
- If using NetScaler to load balance StoreFront, this action could also be accomplished using NetScaler policies.

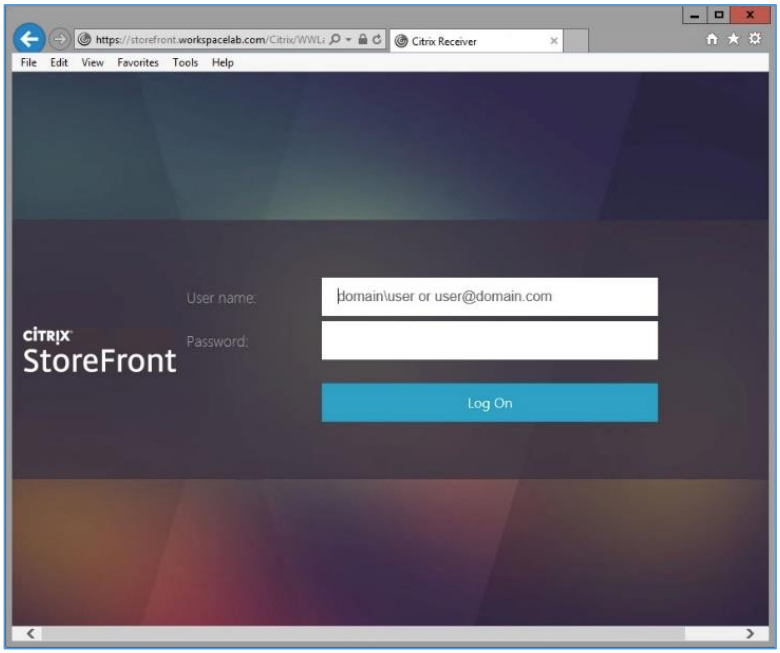
Exercise 5-5: Configure the default domain

In this exercise, you will learn to modify the authentication method from StoreFront to preconfigure a domain so that users do not need to specify the domain during each logon.

Step	Action
1.	Using the Remote Desktop Connection Manager, confirm that you are still connected to **NYC-STF-001**. **Note:** In a previous exercise, you had logged on to NYC-STF-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-STF-001 by right-clicking this machine and selecting Connect server.
2.	Open an Internet browser and navigate to the StoreFront store and log on. Open **Internet Explorer** and browse to **https://storefront.workspacelab.com**. Select **I agree with the Citrix license agreement** and click **Log on**.



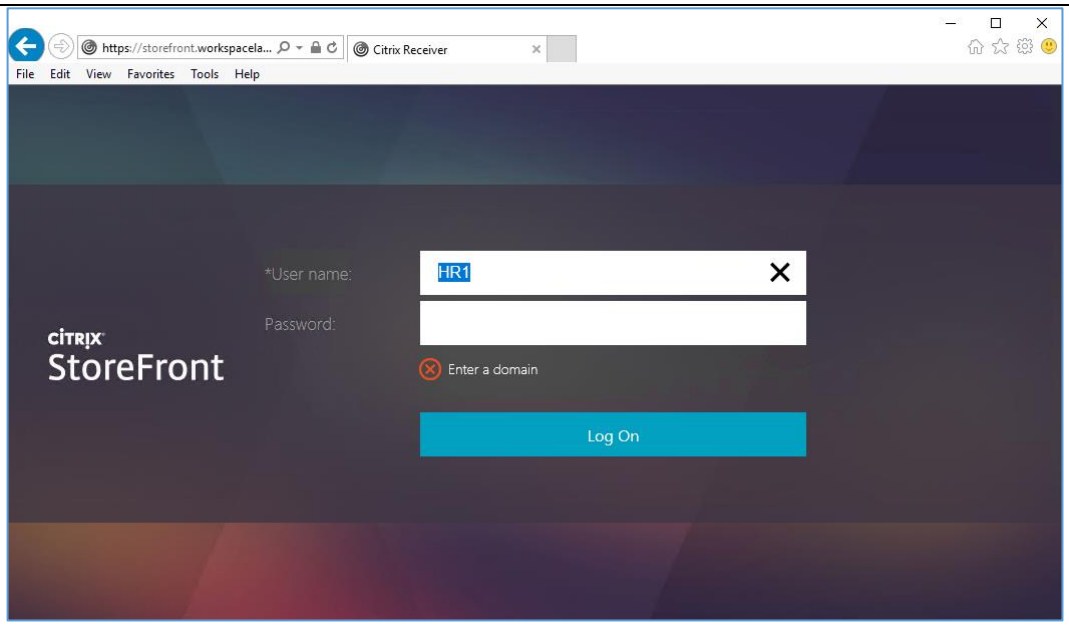
Note: The User name field prompts for a domain\user or user@domain.com account information, indicating that a domain is required.



Attempt to log on to this StoreFront page using the following credentials:

- User name: **HR1**
- Password: **Password1**

This logon attempt failed with a message indicating to Enter a domain. This logon box requires a domain, and only a user name and password was specified.

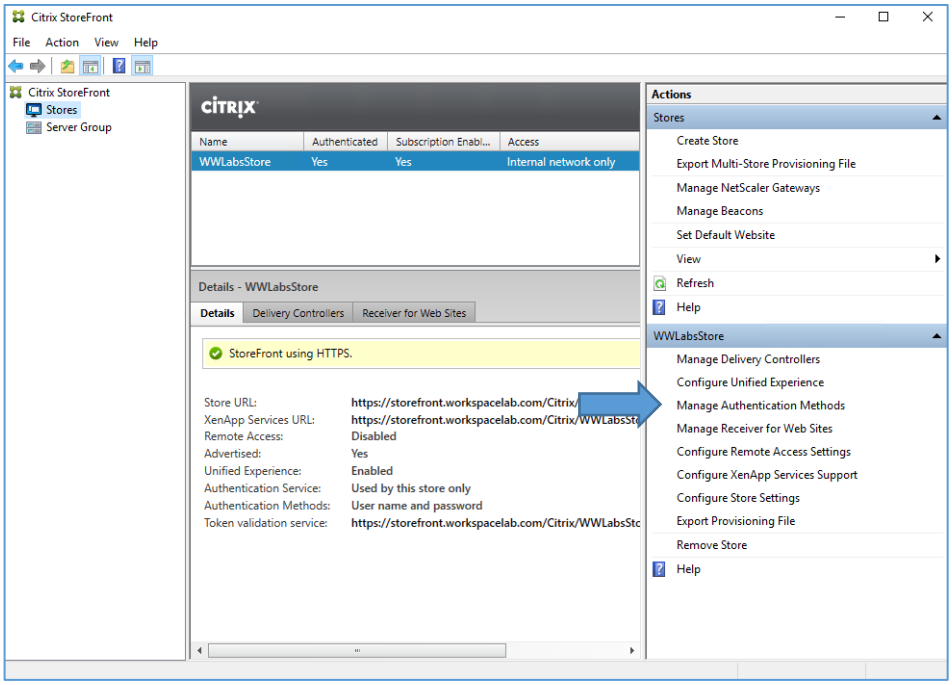


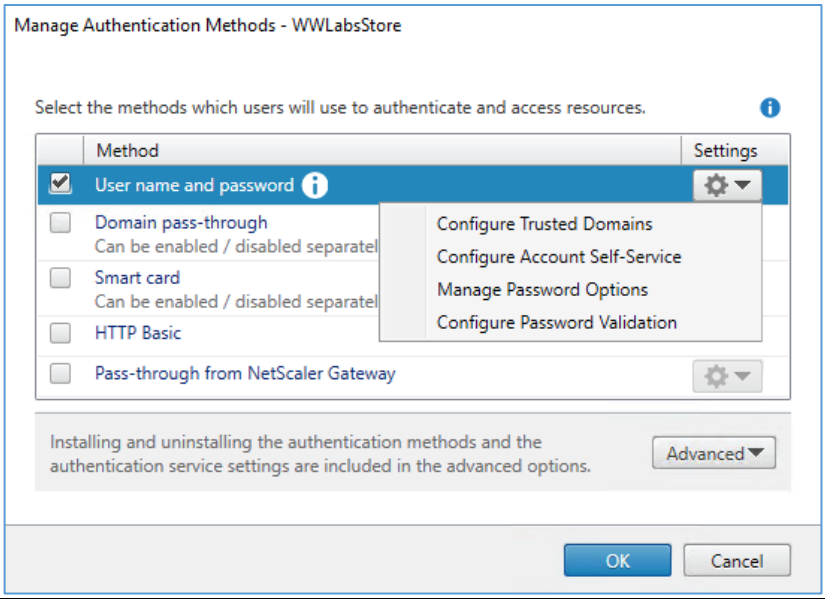
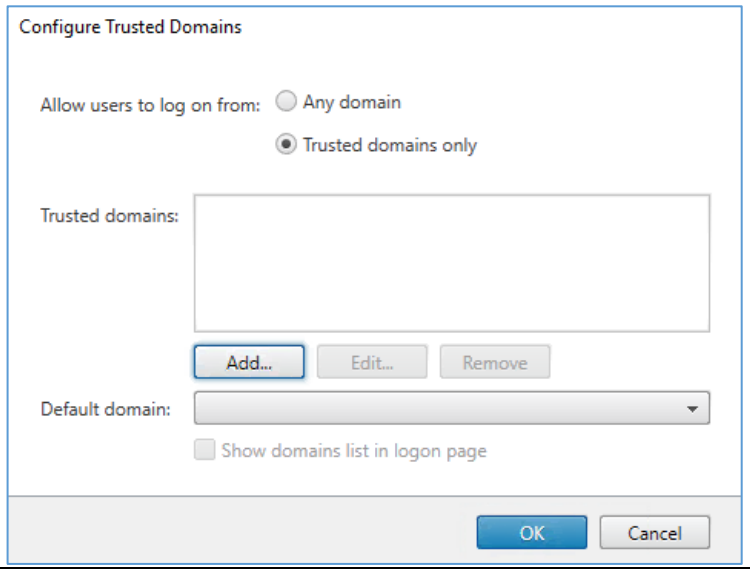
Close **Internet Explorer**.

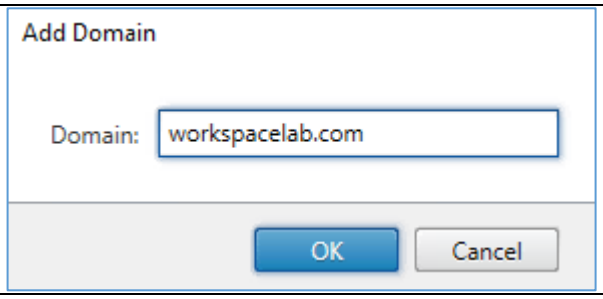
Note: To allow users to log on to a StoreFront store with a user name and a password but without specifying a domain, you have to configure a Trusted Domain. You have been tasked by your Lead Citrix Architect to configure this Trusted Domain in your XenApp and XenDesktop POC environment.

3. Using the StoreFront Management Console, configure a Trusted Domain.

In the left pane, select **Stores**. In the right pane, under WWLabsStore, click **Manage Authentication Methods**.

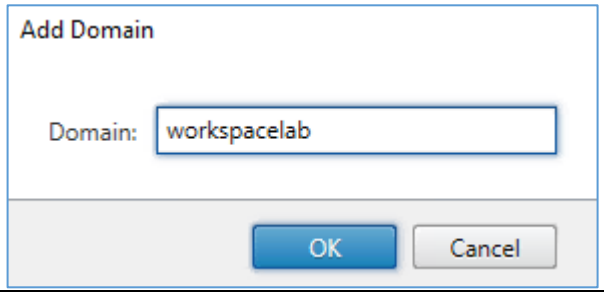


	Note: The StoreFront Management Console was started in a previous exercise. If the console was closed in a previous exercise, then click Start > Citrix > Citrix StoreFront.
4.	On the Manage Authentication Methods – WWLabsStore page, click on the **Settings** drop-down next to User name and password and select **Configure Trusted Domains.** 
5.	In the Configure Trusted Domains window, select **Trusted domains only** for the Allow users to log on from field. 
6.	Below the Trusted domains box, click **Add**. Enter **workspacelab.com** in the Add Domain dialog box and click **OK**.



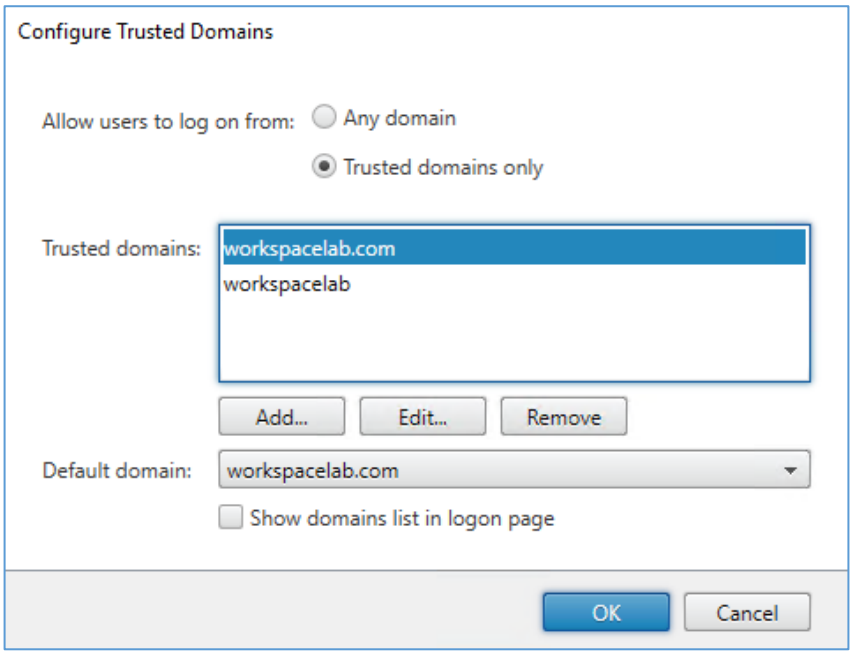
7. Below the Trusted domains box, click **Add**.

   Enter **workspacelab** in the Add Domain dialog box and click **OK**.



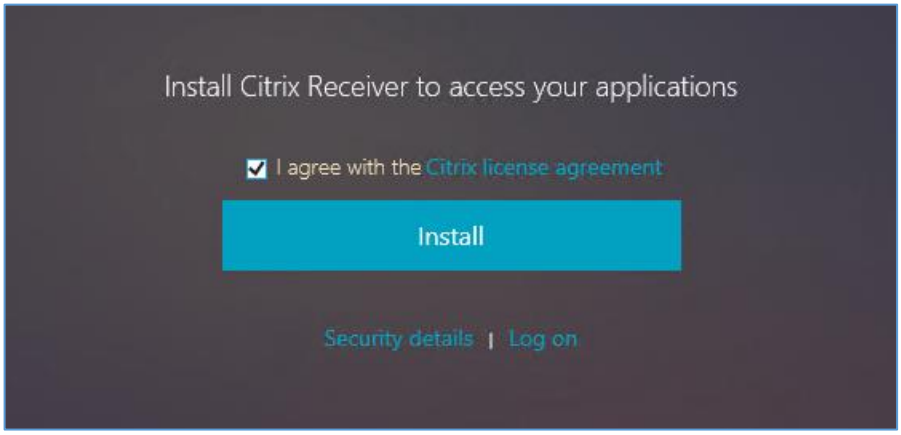
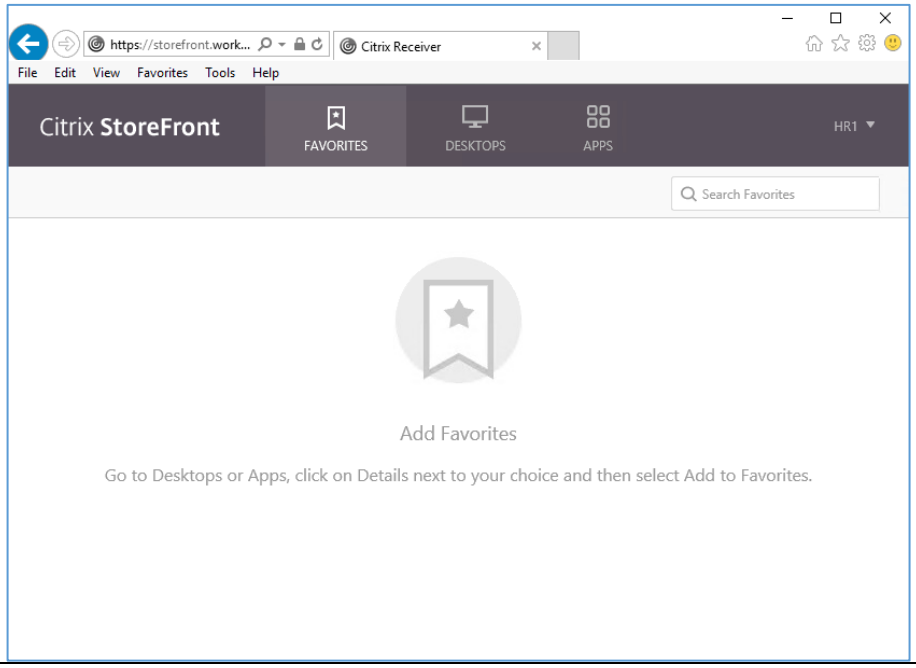
8. In the Configure Trusted Domains dialog box, verify that the following is configured:
   - In the Default domain drop-down, **workspacelab.com** is selected.
   - The Show domains list in logon page is **deselected**.

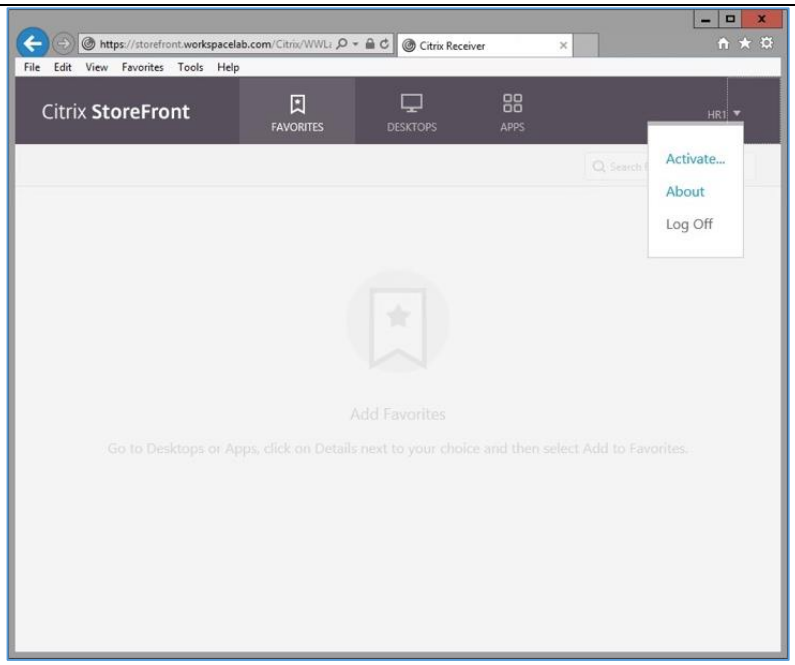
   Click **OK** to accept the changes.



   Click **OK** again on the Manage Authentication Methods – WWLabsStore dialog box.

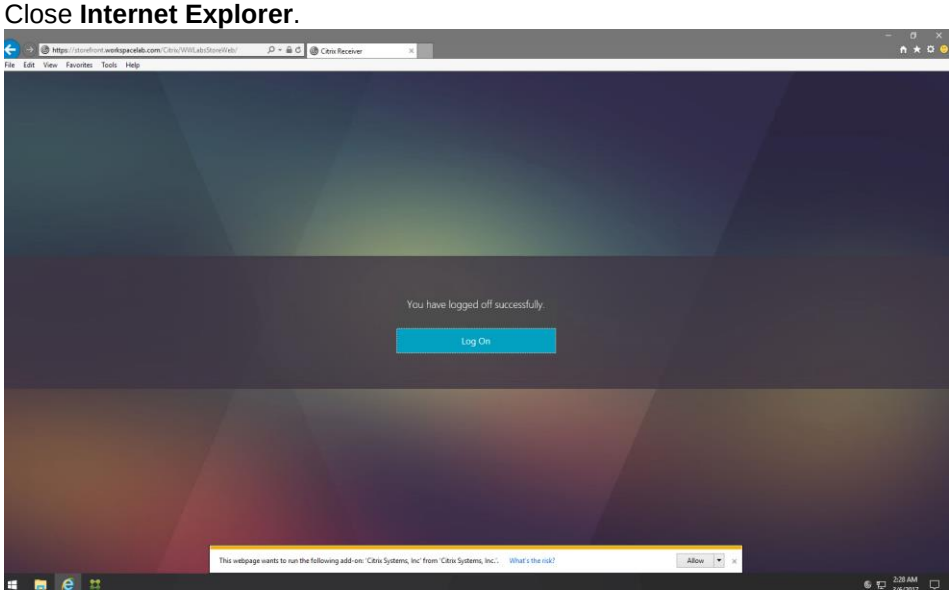
   Note: If users need to access multiple domains, enable the box to Show domains list in logon page so that users can see a drop-down list in the StoreFront store logon screen that will show the pre-defined list of available domains that a user can select and log on to.

9.	Open an Internet browser to navigate to the StoreFront store and test that the Trusted Domains was configured successfully by logging on with a user name and a password, but without a domain. Open **Internet Explorer** and browse to **https://storefront.workspacelab.com**. Select **I agree with the Citrix license agreement**, if prompted. Then click **Log on**.  Log on to the StoreFront page using the following credentials: • User name: **HR1** • Password: **Password1** **Note**: Notice that the user is able to log on without specifying a domain. 
10.	**Close** the store session. In the top right corner of the browser, click the user name that was used to log on to this store and select **Log Off**.



Note: Internet Explorer will log out the user and will present a message stating that You have logged off successfully. At this point, you could log back on by clicking Log On, but for now you will close Internet Explorer.

Close **Internet Explorer**.



Key Takeaways:

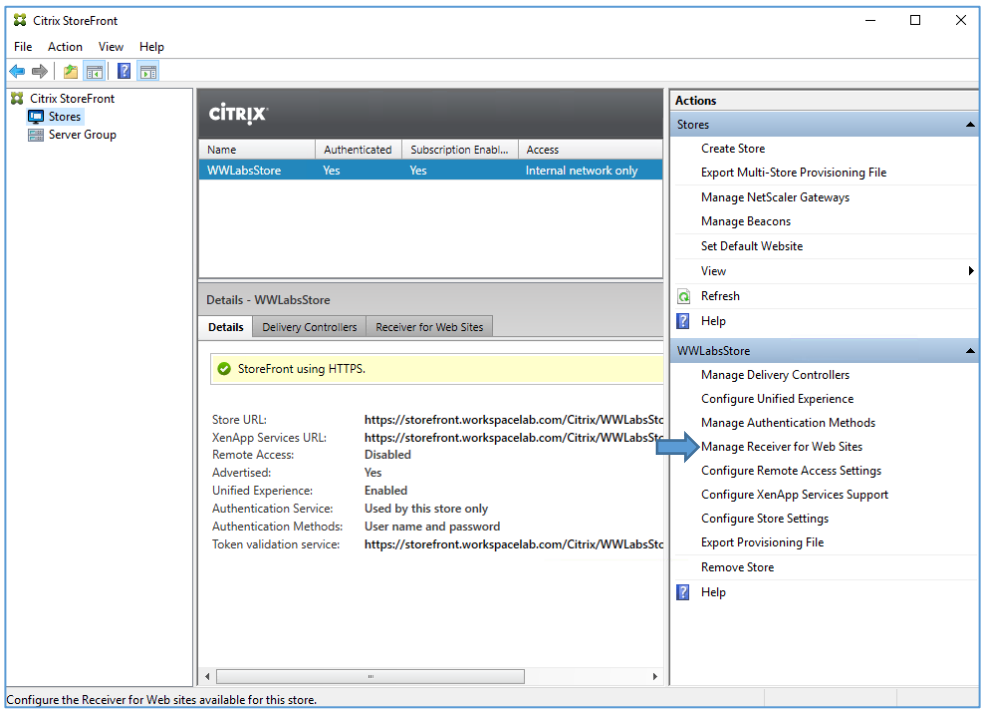
- Using default and trusted domains prevents users from having to manually enter a domain during the authentication process. This will help prevent users from incorrectly entering their domain, failing to log on, and calling the helpdesk.
- If the Trusted domains only option is selected, and multiple domains are specified, users will be presented with a drop-down list of domains from which to choose.
- The first trusted domain entered is automatically configured as the default logon domain. This is the domain used by default when users log on and do not specify a domain.

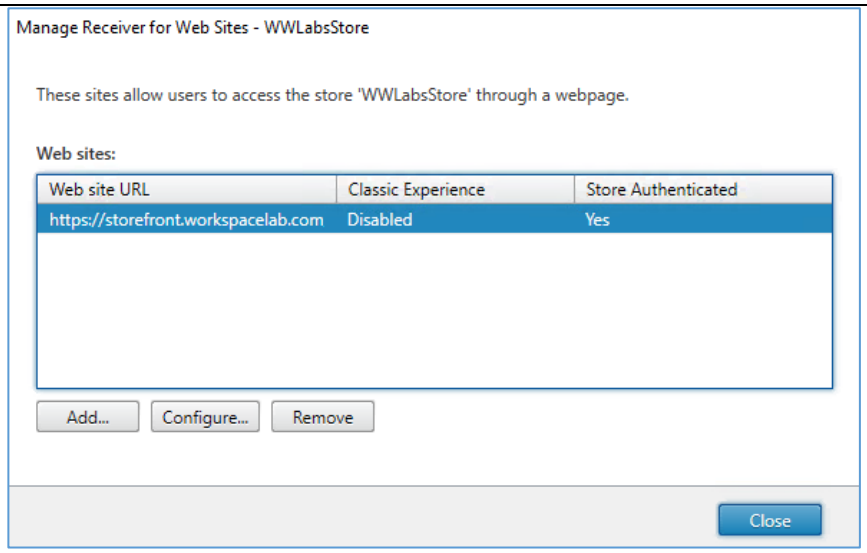
Exercise 5-6: Adjust the StoreFront timeout

Scenario:

StoreFront Server enforces a default timeout on the store to automatically log users out of their web session after being inactive for a preset amount of time.

Your task is to modify the inactive web session timeout value.

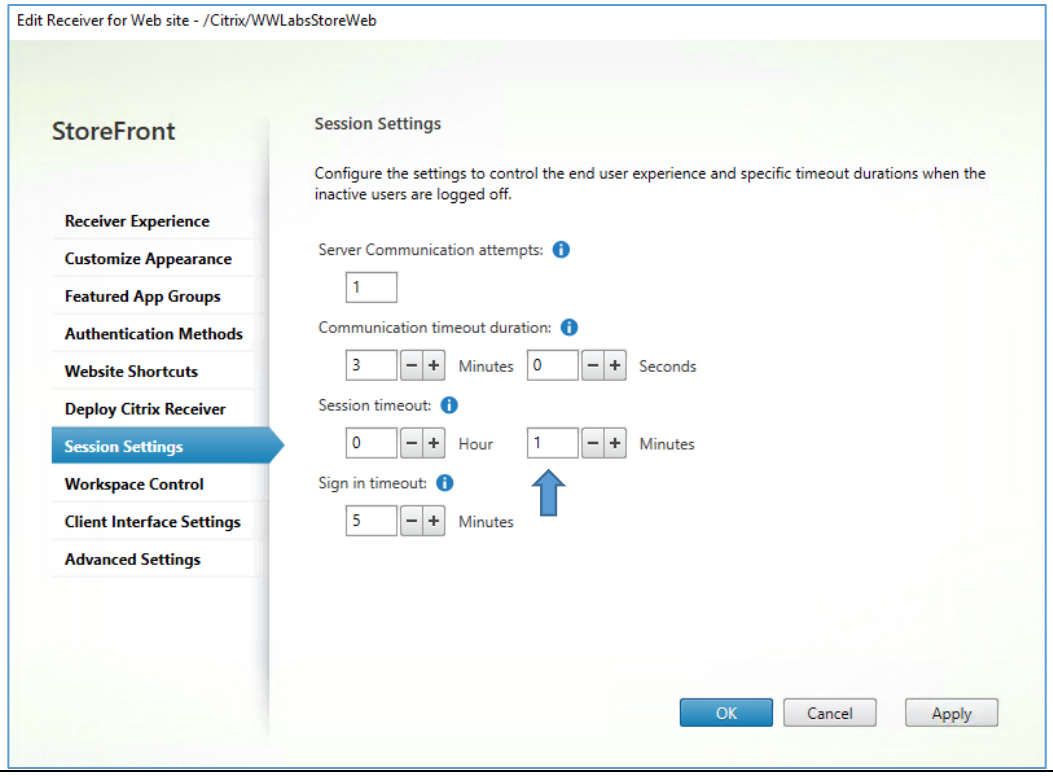
Step	Action
1.	Using the Remote Desktop Connection Manager, confirm that you are still connected to **NYC-STF-001**. **Note:** In a previous exercise, you had logged on to NYC-STF-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-STF-001 by right-clicking this machine and selecting Connect server.
2.	Using the StoreFront Management Console, set the session timeout. In the left pane, select **Stores**. In the center pane, verify that **WWLabsStore** store is selected. In the right pane, click **Manage Receiver for Web Sites**.  **Note**: The StoreFront Management Console was started in a previous exercise. If the console was closed in a previous exercise, then click Start > Citrix > Citrix StoreFront.
3.	On the Manage Receiver for Web Sites – WWLabsStore dialog box, click **Configure**.



4. Select **Session Settings** on the left side of the dialog box and change Session timeout value to **1 Minute**.

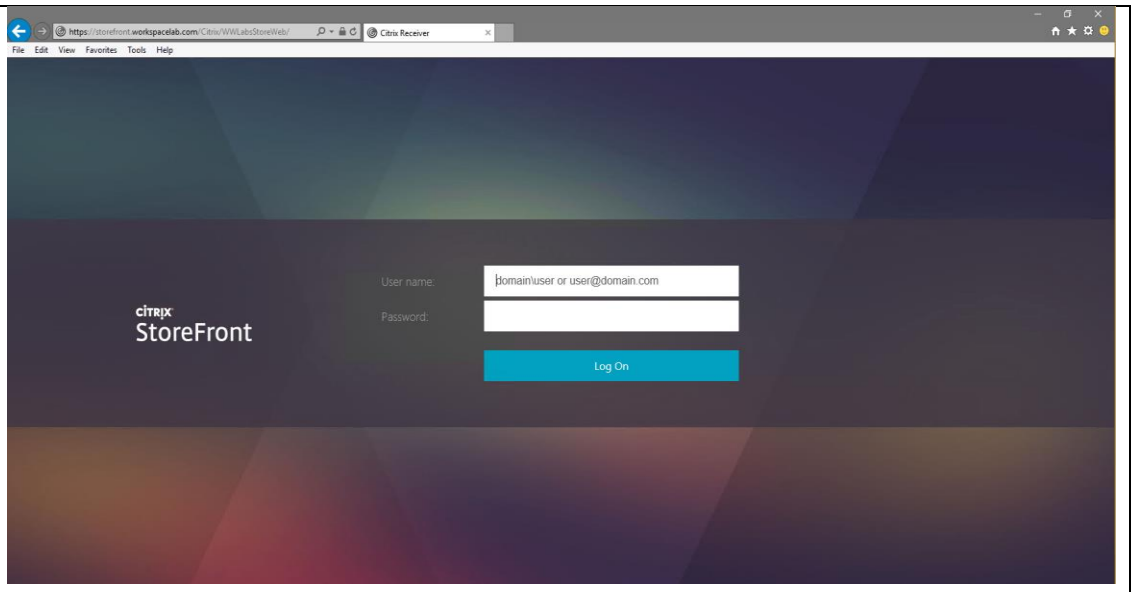
   Click **Apply** and then click **OK**.

   Click **Close** to exit the Manage Receiver for Web Sites – WWLabsStore window.



5. Open an Internet browser and navigate to your StoreFront store to test the new session timeout.

   Open **Internet Explorer** and browse to **https://storefront.workspacelab.com**.

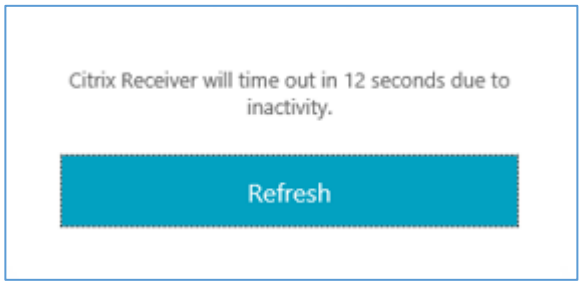


Log on to the StoreFront page using the following credentials:

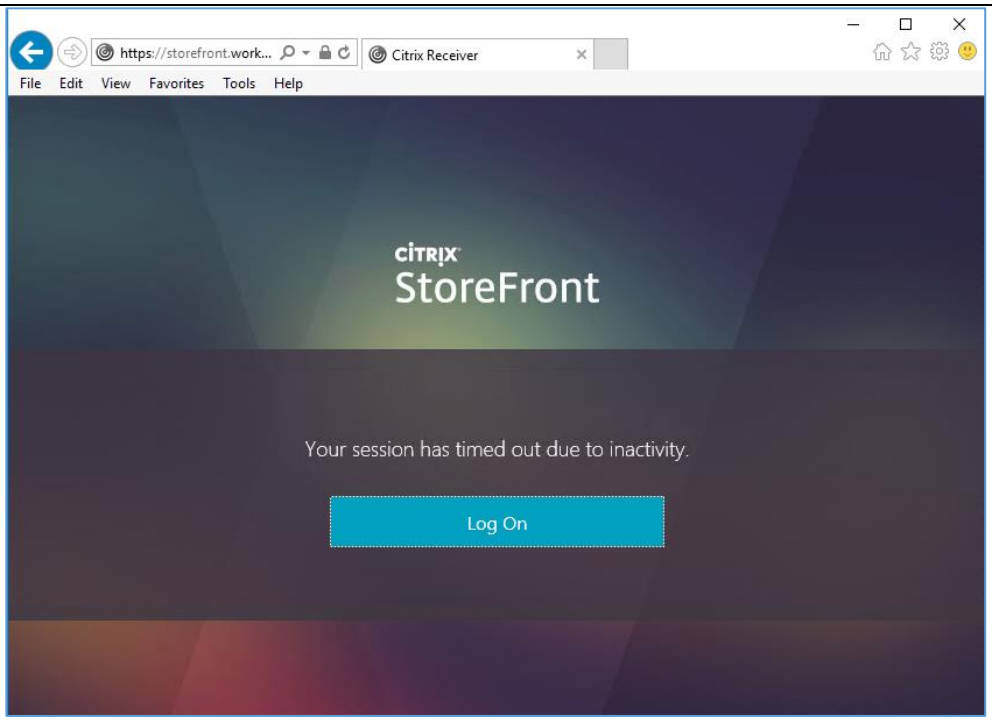
- User name: **HR1**
- Password: **Password1**

6. Do not interact with the **web browser** or the **published desktop**.

Note: After a few seconds of idle time, you will see a message counting down from 15 seconds letting you know that Citrix Receiver will timeout due to inactivity.



Note: After the timeout expires, the user account is logged out. Internet Explorer will display a message that “Your session has timed out due to inactivity”.

	 Close **Internet Explorer**.
7.	Change the timeout setting to the default value of 20 minutes. Switch to the StoreFront Management Console and select **Stores** in the left pane. Verify that WWlabsStore is selected in the middle pane. In the right pane, click **Manage Receiver for Web Sites**. On Manage Receiver for Web Sites – WWLabsStore dialog box, click **Configure**. Select **Session Settings** on the left and change the session timeout value to **20** Minutes. Click **Apply** and then click **OK**. Click **Close** to exit the Manage Receiver for Web Sites – WWLabsStore window. **Note**: You have tested this feature and will report back to the Citrix Administrator team the results of your test. Moving forward, your environment depends on this feature being set to a more reasonable timeout.

Key Takeaways:

- The StoreFront timeout can be extended to allow users longer periods without requiring a logon.
- Set the timeout for the web session to a reasonable amount for security purposes – if users forget to log out of the website the session will be rendered useless for attackers after the specified amount of time.
- IIS also has some configurable timeouts that should be adjusted accordingly since the smallest one determines the actual time before the session will be closed.

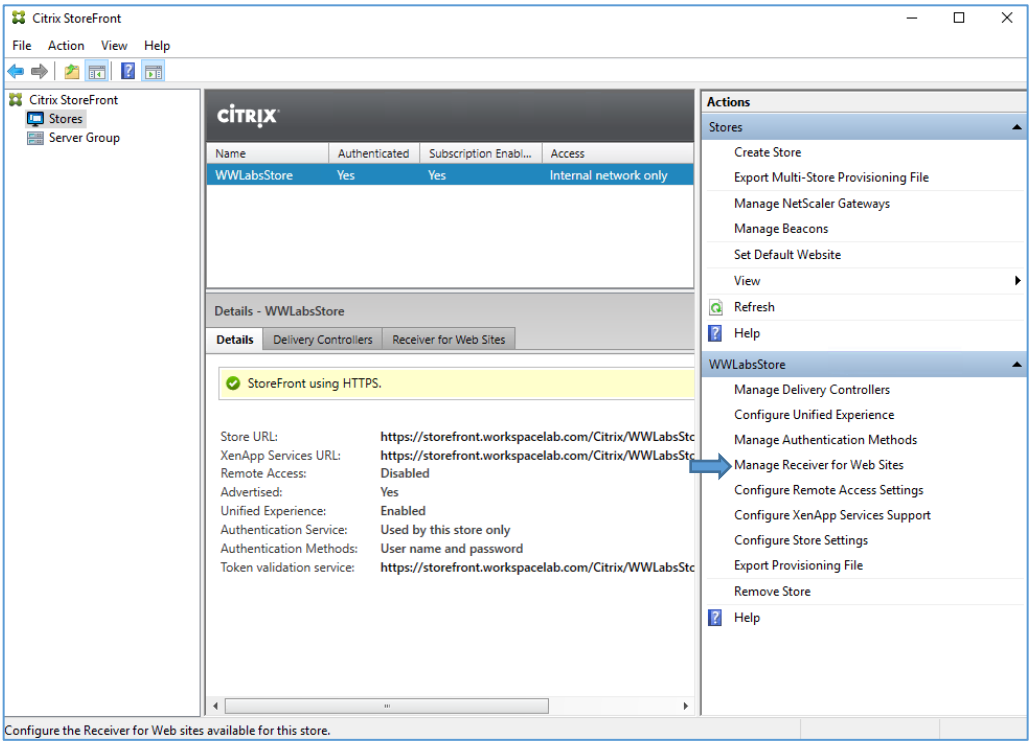
Exercise 5-7: Configure StoreFront store branding

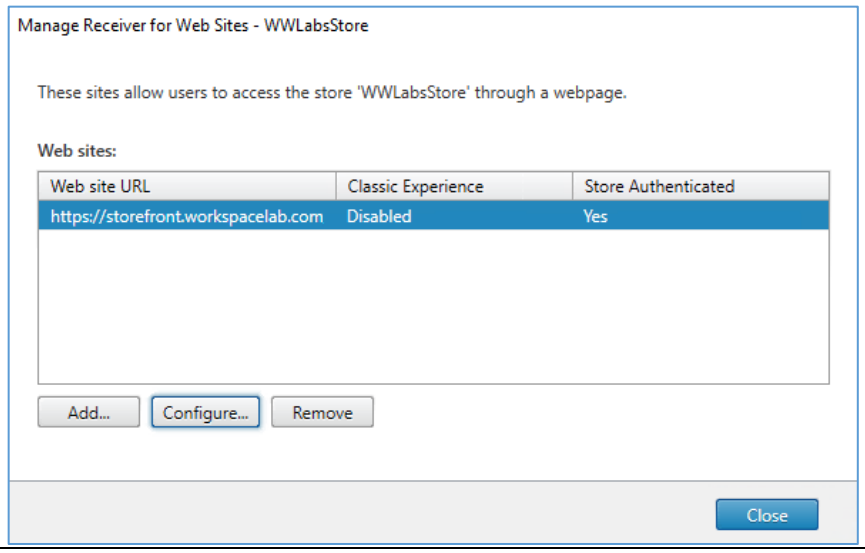
Scenario:

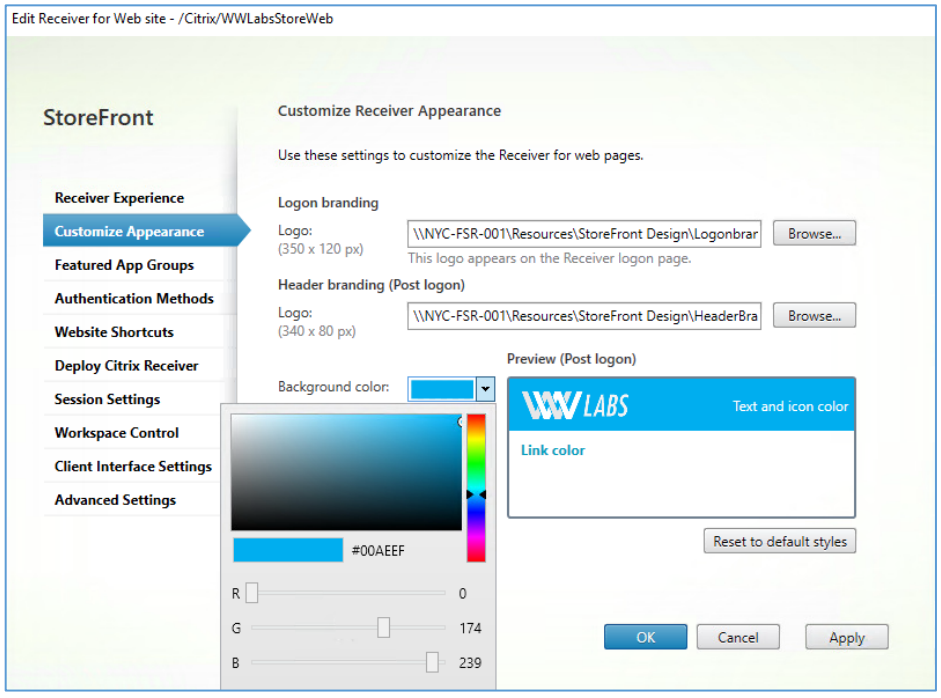
WW Labs has set expectations that all websites used for company business must be branded using the standard appearance as defined in WW Labs written policy.

Your task is to update the Storefront store and the Store for Web to match corporate branding. This task brings into compliance the store with WW Labs written policy by providing a familiar appearance for employees.

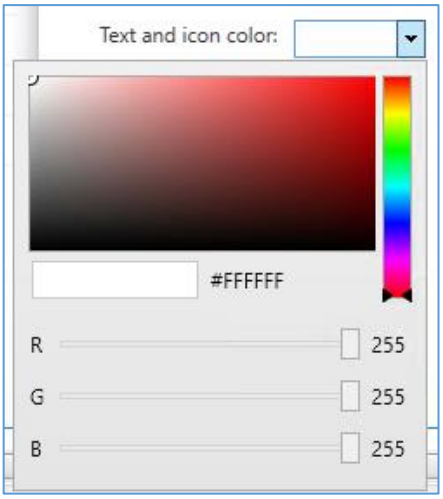
You decide to start the customization by using the basic branding features available in the StoreFront console.

Step	Action
1.	Using the Remote Desktop Connection Manager, confirm that you are still connected to **NYC-STF-001**. **Note**: In a previous exercise, you had logged on to NYC-STF-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-STF-001 by right-clicking this machine and selecting Connect server.
2.	Using the StoreFront Management Console, customize the Receiver appearance. In the left pane, select **Stores**. In the right pane, under WWLabsStore, click **Manage Receiver for Web Sites**.  **Note**: The StoreFront Management Console was started in a previous exercise. If the console was closed in a previous exercise, then click Start > Citrix > Citrix StoreFront.

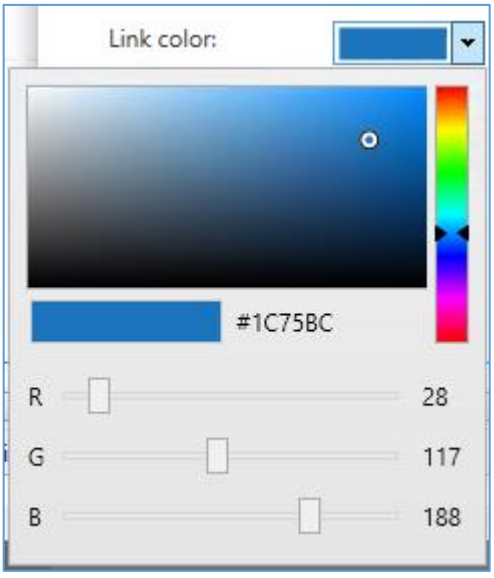
3.	On the Manage Receiver for Web Sites – WWLabsStore dialog box, click **Configure**. 

4.	On Edit Receiver for Web site dialog box, select **Customize Appearance** on the left side of the dialog box and set the following customizations:
	• Logon branding: Click **Browse** and browse to **\\NYC-FSR-001\Resources\StoreFront Design**. Select **Logonbranding.png** and click **Open**.
	• Header branding (Post logon): Click **Browse** and browse to **\\NYC-FSR-001\Resources\StoreFront Design**. Select **HeaderBranding.png** and click **Open**.
	• Background color: Click the drop-down and define the WW Labs RGB Values set to:
	  ○ R: **0**
	  ○ G: **174**
	  ○ B: **239**
	 

- Text and icon color:
  - R: **255**
  - G: **255**
  - B: **255**



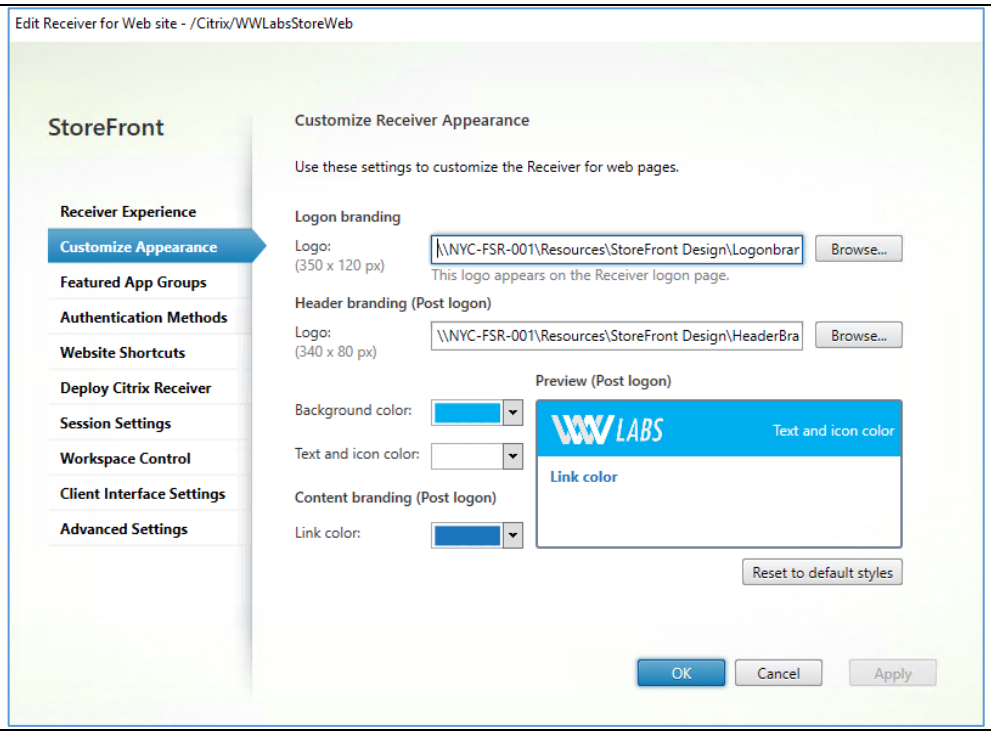
- Link color:
  - R: **28**
  - G: **117**
  - B: **188**



Note: You can use the keyboard arrow keys for granular adjustments or double-click the numbers to enter them manually.

Click **OK** to accept the changes made.

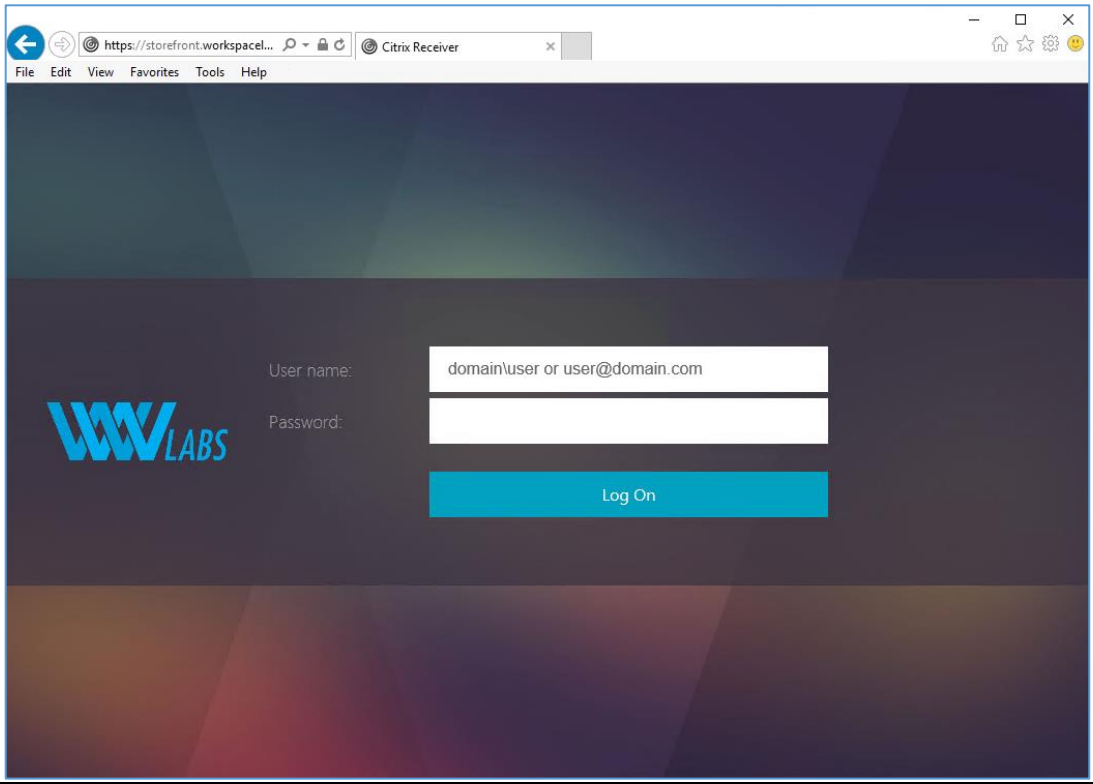
Click **Close** to exit the Manage Receiver for Web Sites – WWLabsStore window.

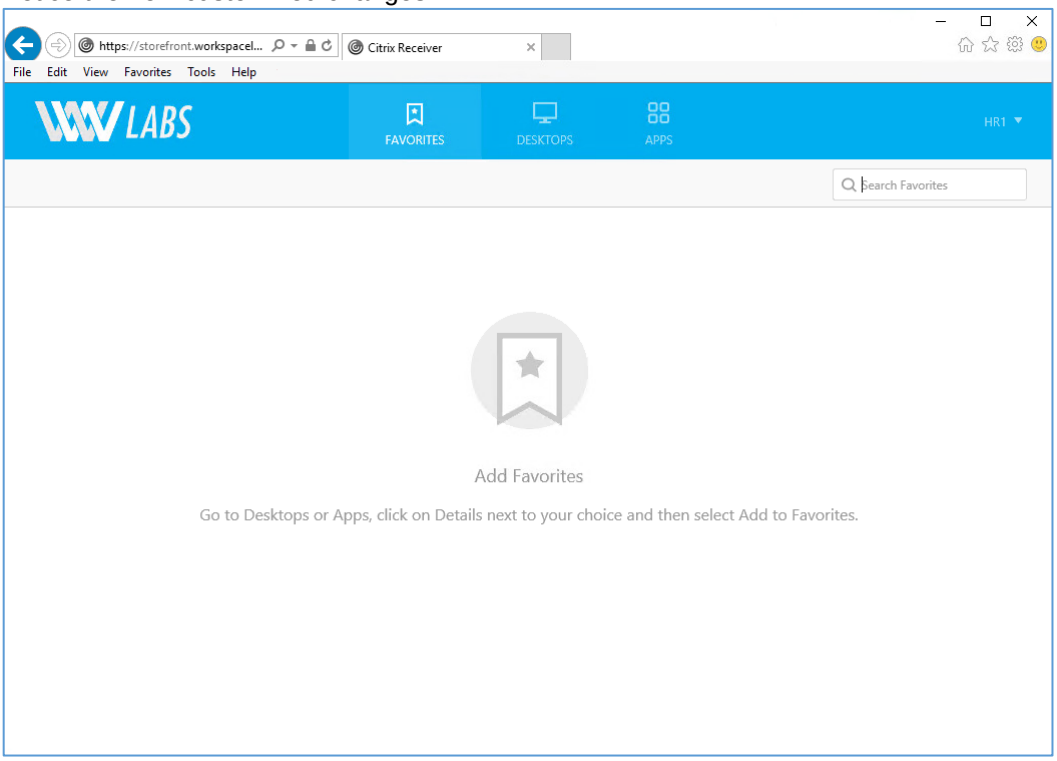


5. Open an Internet browser and navigate to the StoreFront store to experience the new custom Receiver appearance.

   Open **Internet Explorer** and browse to **https://storefront.workspacelab.com**.

   Note: Notice the WW Labs logo.



	Log on to the StoreFront page using the following credentials: • User name: **HR1** • Password: **Password1** Notice the new customized changes.  Click **HR1** and choose **Log Off** and then close **Internet Explorer**.

Key Takeaways:

- You can customize the appearance of Receiver with a logo and specify different color schemes using the StoreFront console.
- Advanced customizations can be made through the use of Cascading Style Sheets.

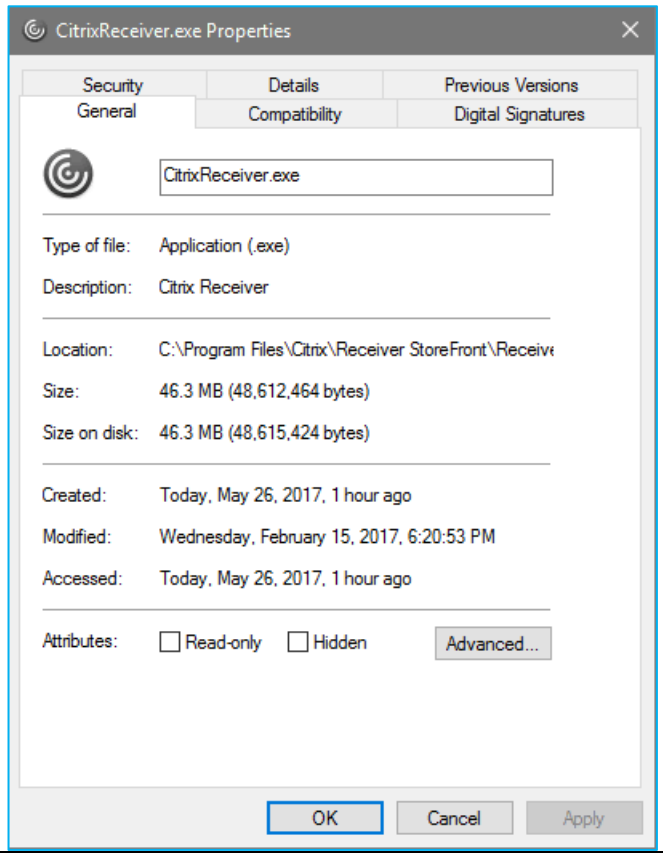
Exercise 5-8: Deploy Citrix Receiver through StoreFront

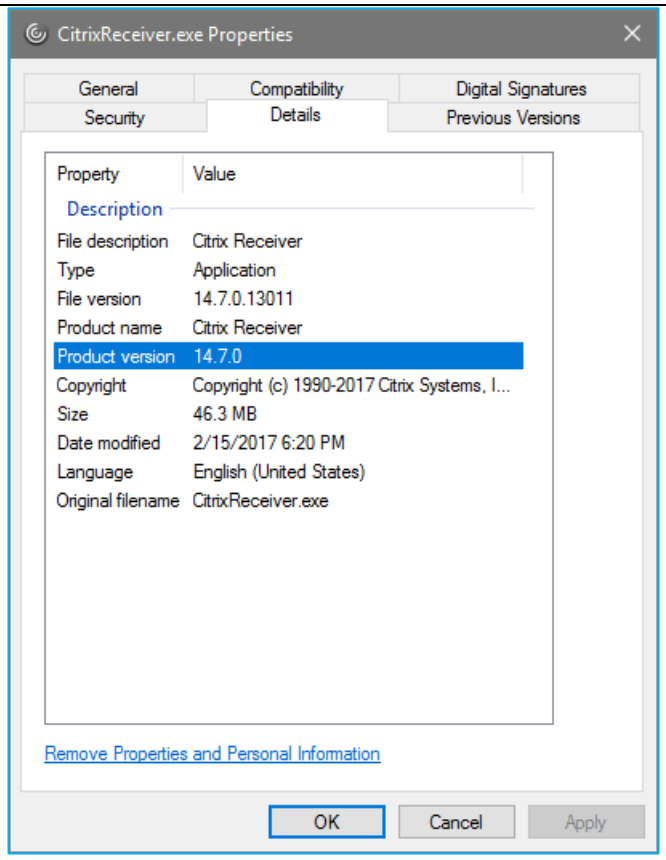
Scenario:

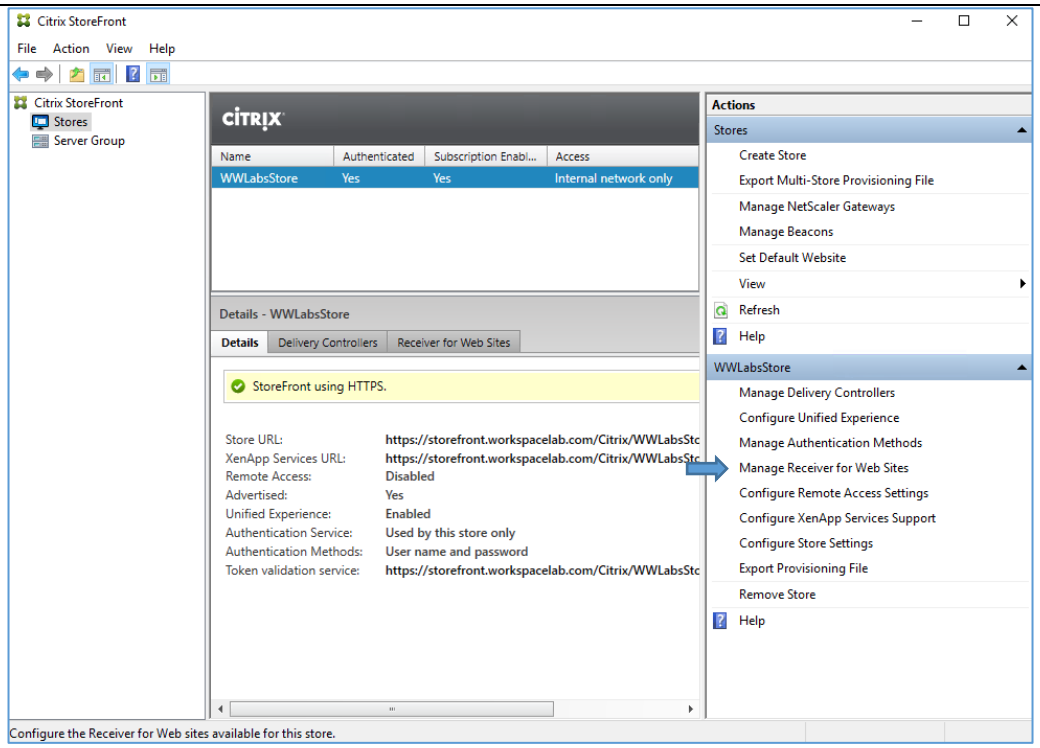
One method to deploy Citrix Receiver is to use StoreFront as the distribution platform. Additionally, you can also enable a built-in Receiver update functionality.

Your task is to test the functionality of the StoreFront Server by configuring both the deployment and the update of Citrix Receiver.

Step	Action
1.	Using the Remote Desktop Connection Manager, switch back to **NYC-STF-001**. **Note**: In a previous exercise, you had logged on to NYC-STF-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1

	Note: If your Remote Desktop Connection session disconnected, log on to NYC-STF-001 by right-clicking this machine and selecting Connect server.
2.	Open the **File Explorer** application from the Windows Taskbar or Start Menu.
3.	Browse to **C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients\Windows**.
4.	Right-click **CitrixReceiver.exe** and select **Properties**. **Note**: If the option to unblock appears**,** then click the option to Unblock in the General section. 
5.	Click the **Details** tab and validate that the version of Citrix Receiver is **14.7.0**.

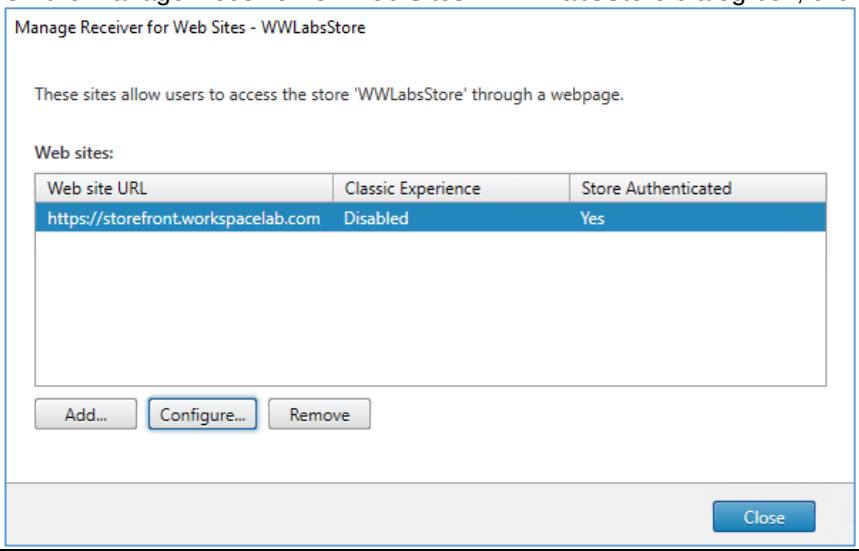
	 Click **OK**.
6.	Using the StoreFront Management Console, customize the deployment of Citrix Receiver. In the left pane, select **Stores**. In the right pane, under WWLabsStore, click **Manage Receiver for Web Sites**.



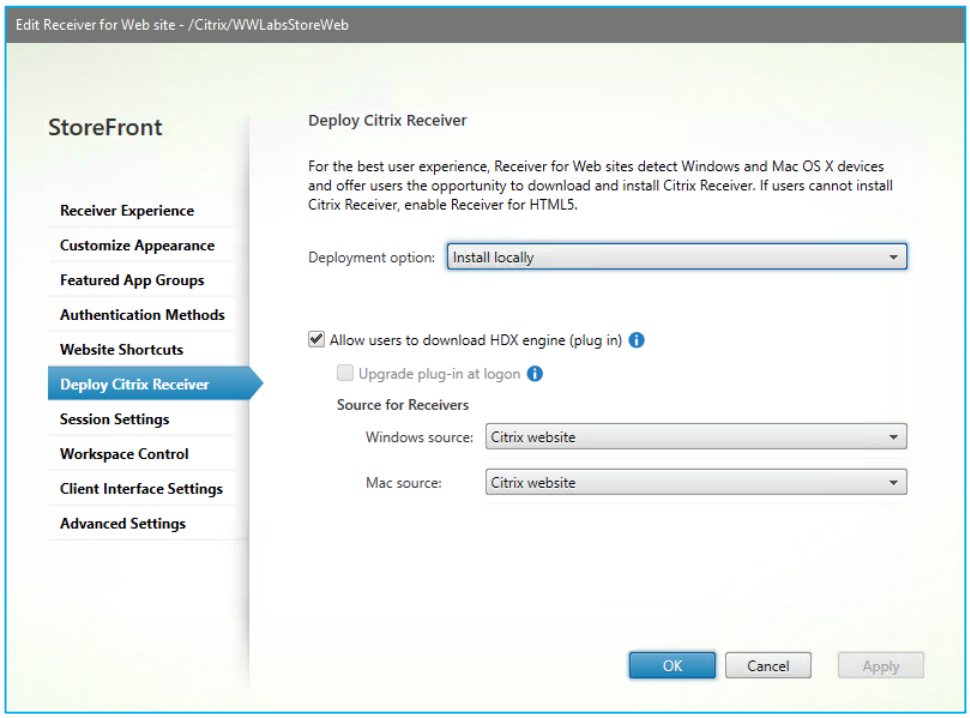
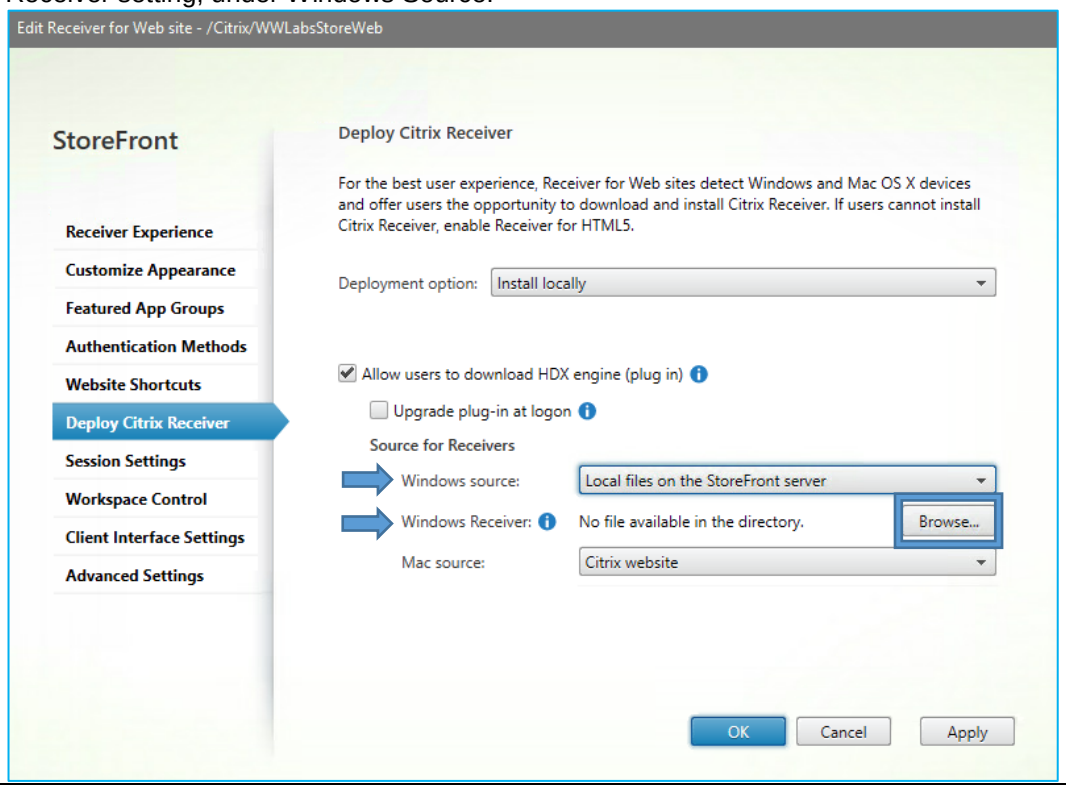
Note: The StoreFront Management Console was started in a previous exercise. If the console was closed in a previous exercise, then click Start > Citrix > Citrix StoreFront.

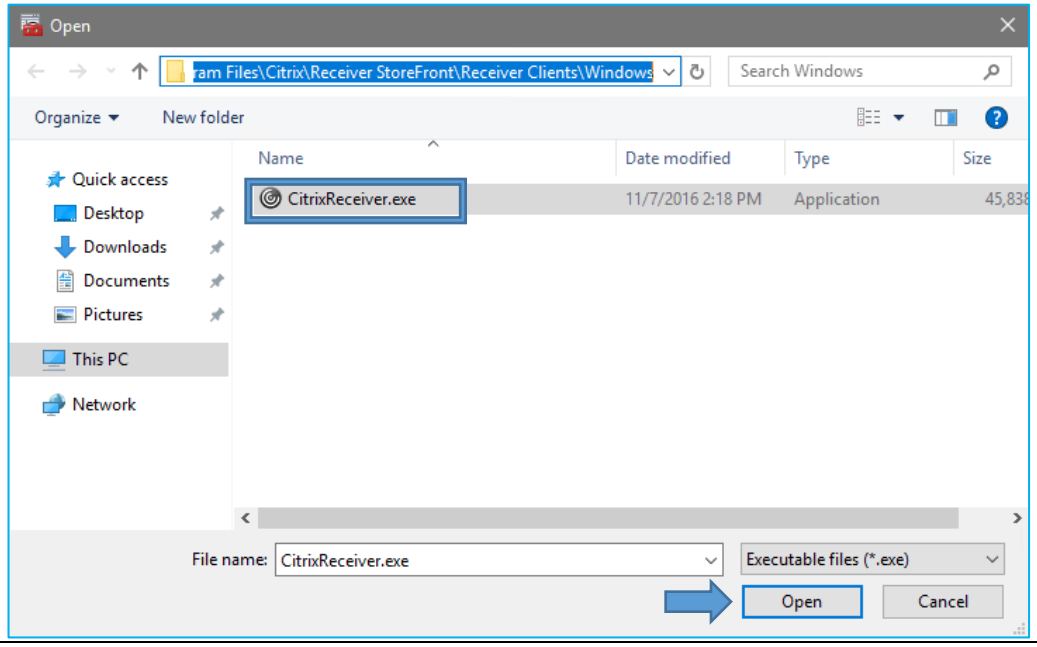
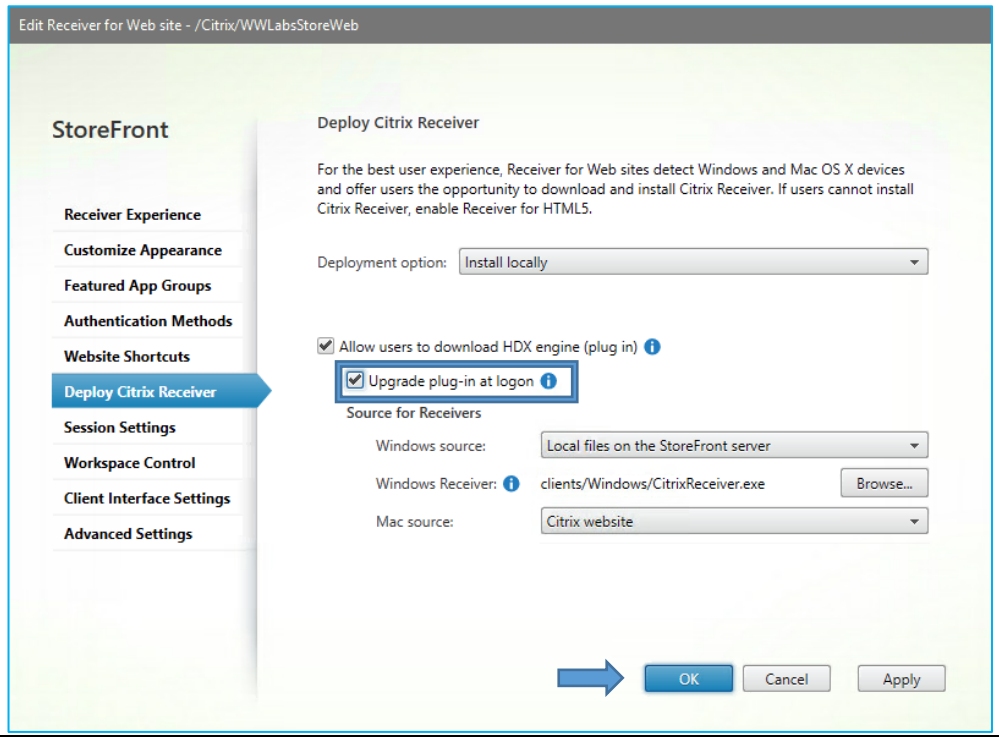
Note: The StoreFront Store Receiver settings can be managed from the StoreFront console. By default, Citrix Receiver for Web sites automatically attempt to determine whether Citrix Receiver is installed when accessed from computers running Windows or Mac OS X. If Citrix Receiver cannot be detected, the user is prompted to download and install the appropriate Citrix Receiver for their platform. The default download location is the Citrix website, but you can also copy the installation files to the StoreFront server and provide users with these local files instead.

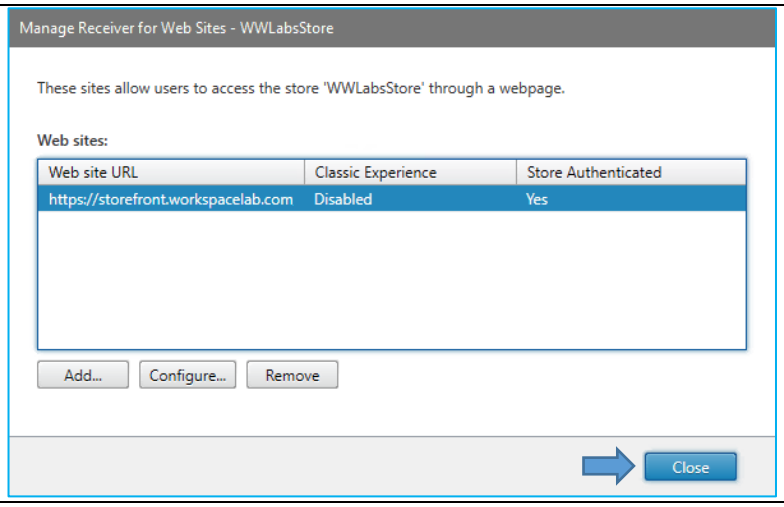
7. On the Manage Receiver for Web Sites – WWLabsStore dialog box, click **Configure**.



8. On Edit Receiver for Web site dialog box, select **Deploy Citrix Receiver** on the left-hand

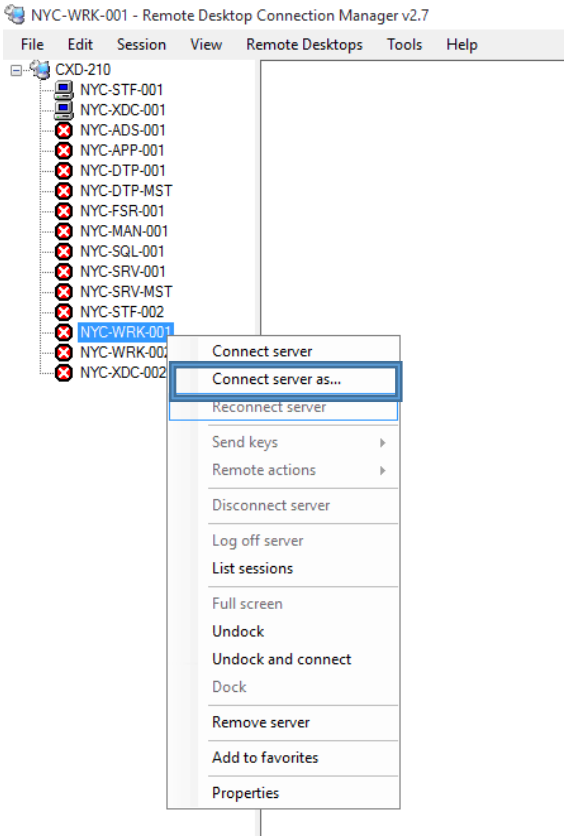
	side of the dialog box. . 
9.	On the left side of the **Deploy Citrix Receiver** dialog box, change the Windows Source drop-down setting to **Local Files on the StoreFront server.** Then click **Browse** in the Windows Receiver setting, under Windows Source. 
10.	Browse to **C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients\Windows**.

	Select the **CitrixReceiver.exe** file and click **Open**. 
11.	Enable the checkbox for **Upgrade plug-in at logon** and click **OK**. 
12.	Click **Close** on the **Manage Receiver for WebSites – WWLabStore** dialog box**.**

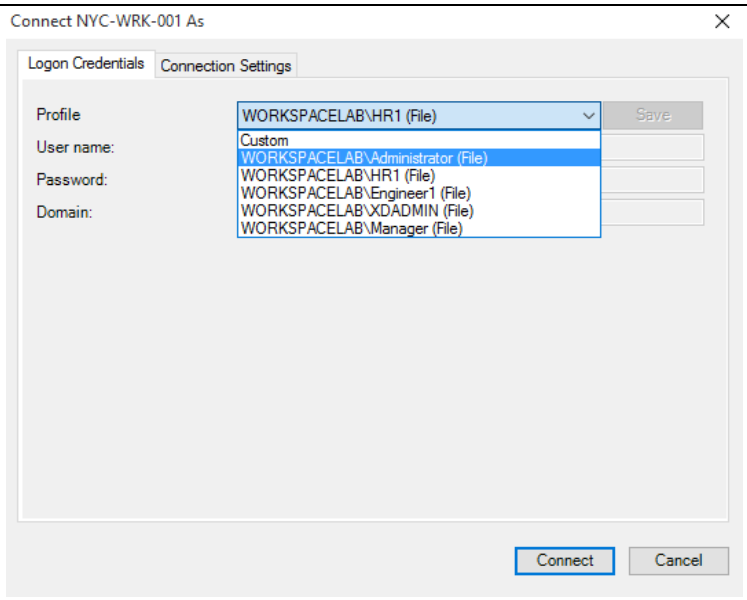


13. Using the Remote Desktop Connection Manager, connect to NYC-WRK-001 as an Administrator.

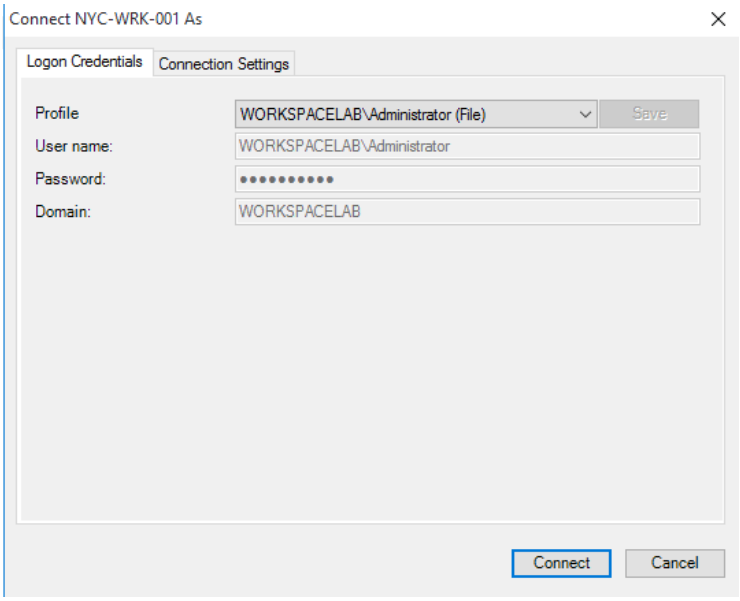
To log on to NYC-WRK-001 as an Administrator, right-click this machine and choose **Connect server as**.



Click the Profile drop-down list and select **WORKSPACELAB\Administrator**.



Click **Connect**.



Note: Primarily in these exercises, you have been using the Remote Desktop Connection Manager to right-click and connect to a machine using the saved credentials. In this step, you are logging on to a machine with a different set of credentials than the pre-configured default Remote Desktop Connection Manager credentials.

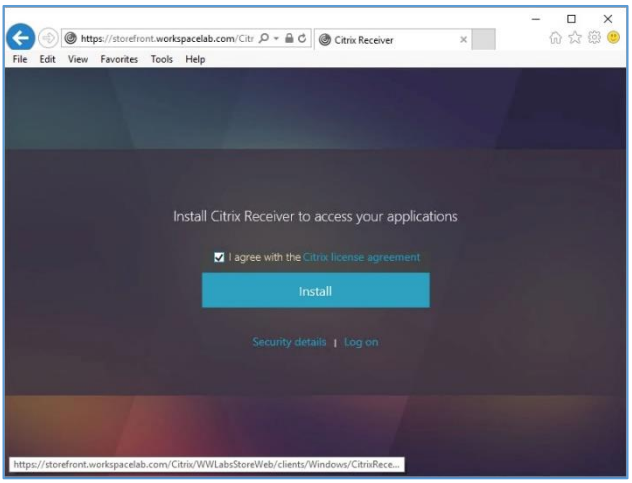
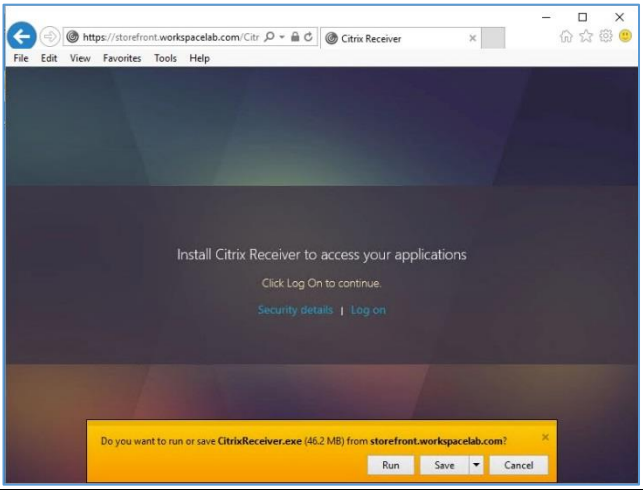
14. Test the web.config modification by browsing to the StoreFront store.

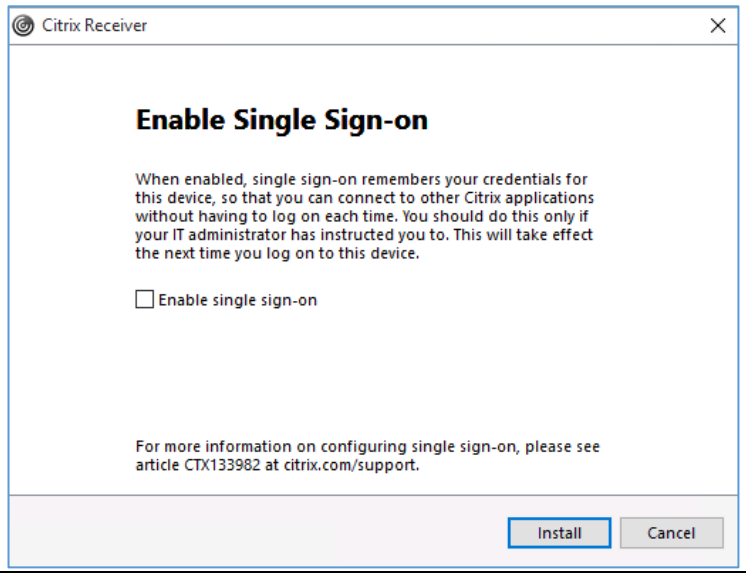
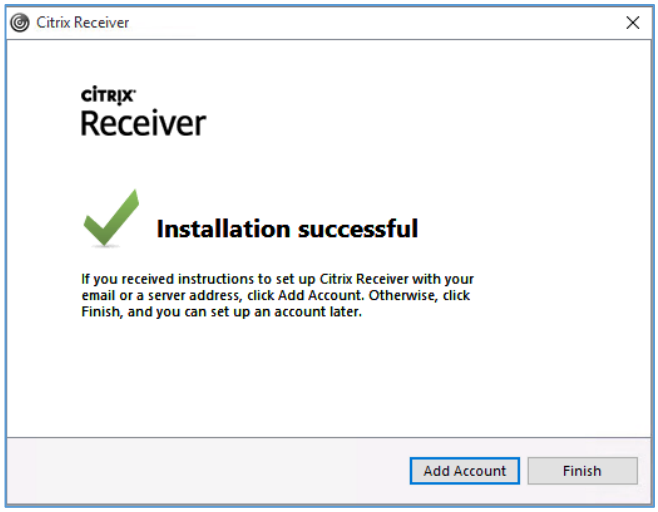
Open **Internet Explorer** and browse to **https://storefront.workspacelab.com**.

Note: On the StoreFront logon page, there is a prompt asking to Install Citrix Receiver to access your applications.

Click **Detect Receiver,** if prompted.

If you agree, select **I accept the license agreement** and click **Install**.

	 **Note**: Internet Explorer will download the installation file and present a Run option at the bottom of the page.
15.	Click **Run** on the bottom of the Internet Explorer page. 
16.	On the Welcome to Citrix Receiver page, click **Start**.

17.	On the License Agreement page, review the license agreement, and if you agree, select **I accept the license agreement** and click **Next**.
18.	On the Enable Single Sign-on page, click **Install**. 
19.	On the Installation successful page, click **Finish**.  Close **Internet Explorer**.
20.	Log off from NYC-WRK-001. To log off, right-click **Start** > choose **Shut down or sign out** > and click **Sign out**.

Key Takeaways:

- Use Citrix StoreFront to simplify the deployment of your customized version of Citrix Receiver to unmanaged endpoint devices.
- StoreFront can deploy and update Citrix Receiver for Windows and Mac OS computers.
- If you change the Receiver binary on the StoreFront Server, a PowerShell command needs to be run to align the configuration.

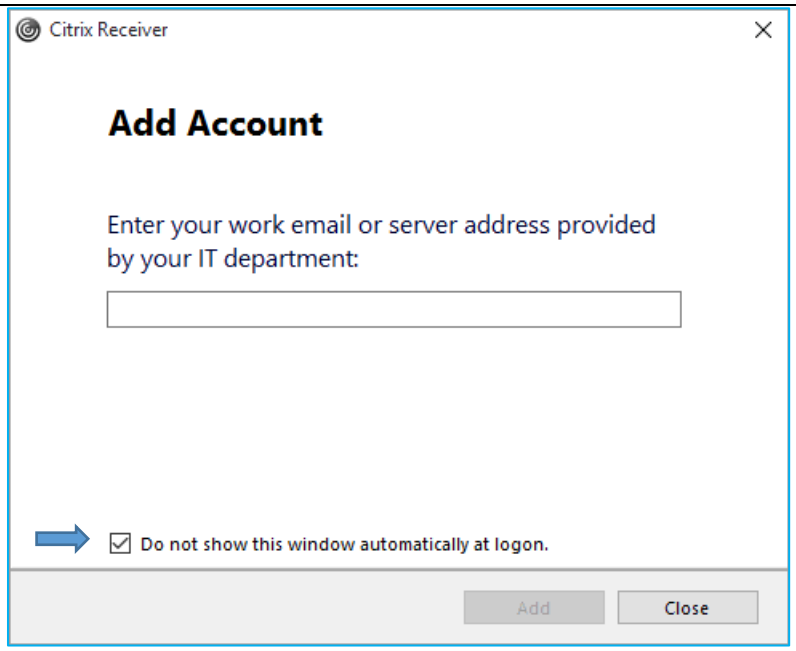
Exercise 5-9: Configure email-based account discovery

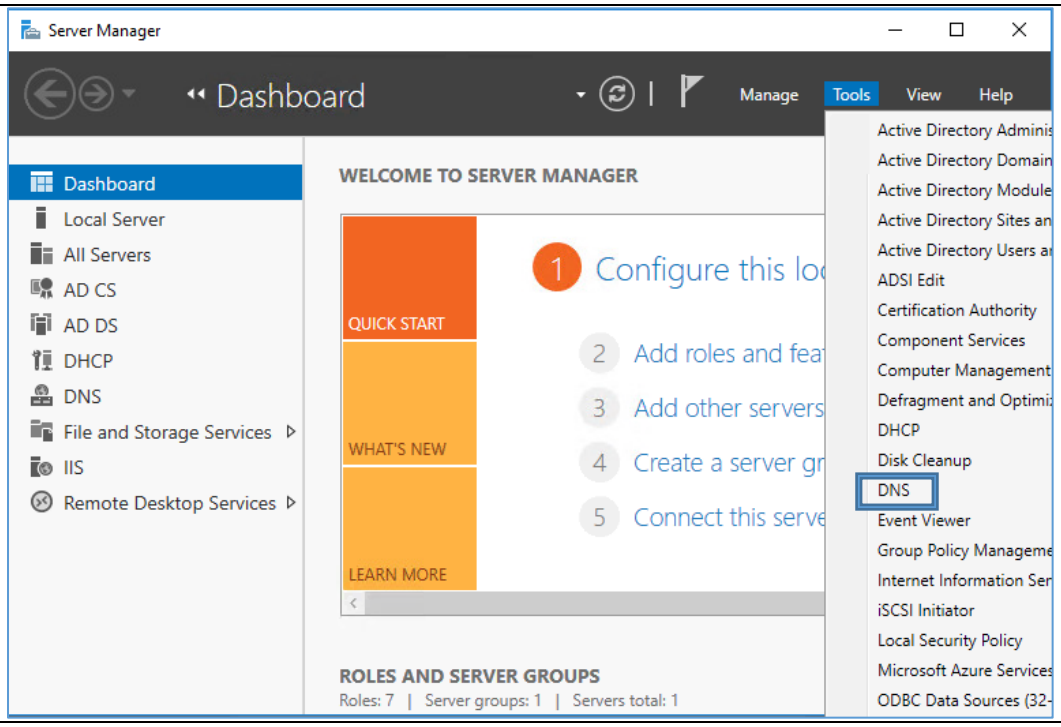
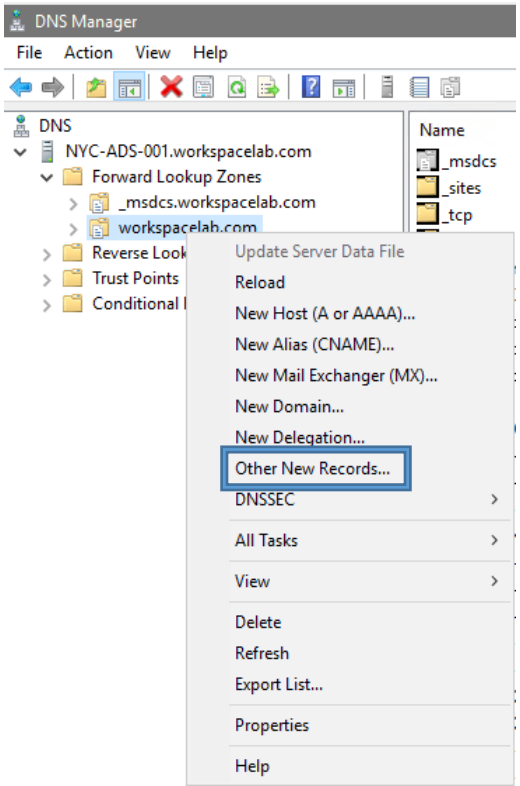
Scenario:

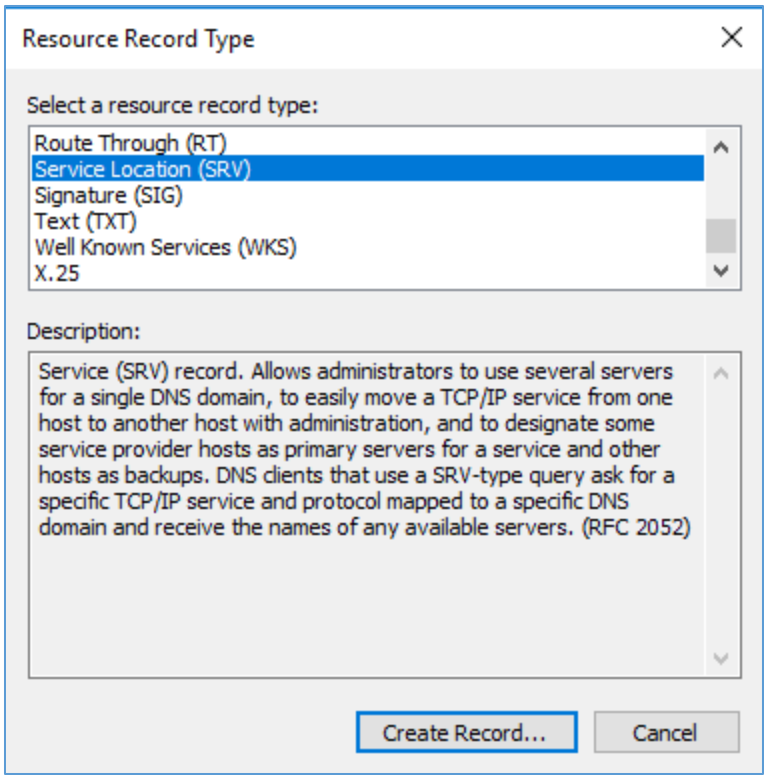
The WW Labs CTO just met with your Lead Citrix Architect for a status update on the POC deployment. After watching a brief demonstration of the setup so far, the CTO is concerned that the user configuration and logon process for access to the store might be too complicated and has asked for a simplified solution. The Lead Citrix Architect has decided to add into the production deployment scope the configuration of email-based account discovery.

Your task is to edit the DNS configuration and point specific requests to the StoreFront Server, so that users can configure a Citrix Receiver by entering their email address, instead of having to know the URL of the StoreFront Server.

Step	Action
1.	Using the Remote Desktop Connection Manager, connect to NYC-WRK-001. To log on to NYC-WRK-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\HR1 • Password: Password1
2.	Click **Start**, and in the left pane of the Start menu under Recently added, click **Citrix Receiver**.
3.	The Citrix Receiver Add Account page should automatically load at logon. On the Add Account page, notice that it asks the user to **Enter your work email or server address provided by your IT department**.

	 Check the “Do not show this window automatically at logon” box. Then click **Close** on the Citrix Receiver: Add Account page. **Note**: You have been tasked by your Lead Citrix Architect to implement the email-based account discovery feature. **Note:** Just click on Close if you do not see the box to uncheck **Do not show this window automatically at logon**.
4.	Using the Remote Desktop Connection Manager, connect to NYC-ADS-001. To log on to NYC-ADS-001, right-click this machine and choose **Connect server**. **Note**: The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1
5.	Open the DNS management console to create a new record as a part of implementing the email-based account discovery feature of Receiver. Click **Start** and select **Server Manager**. Click **Tools** and select **DNS** to start the DNS Manager console.

	
6.	In the left pane of DNS Manager, expand **NYC-ADS-001** > **Forward Lookup Zones** and select **workspacelab.com**. Right-click **workspacelab.com** and select **Other New Records**. 
7.	In the Resource Record Type dialog box, select **Service Location (SRV)** and then click **Create Record**.

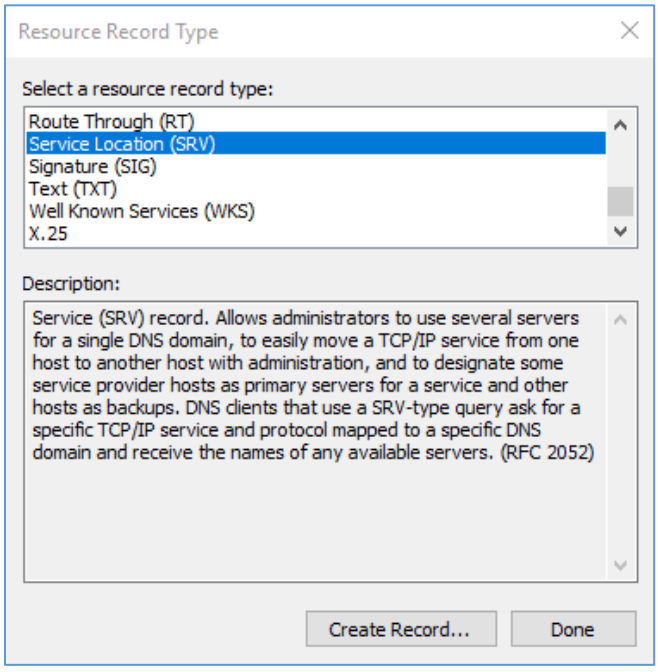


Note: Service (SRV) records allow administrators to use several servers for a single DNS domain, to easily move a TCP/IP service from one host to another host with administration, and to designate some service provider hosts as primary servers for a service and other hosts as backups. DNS clients that use a SRV-type query ask for a specific TCP/IP service and protocol mapped to a specific DNS domain and receive the names of any available servers. (RFC 2052).

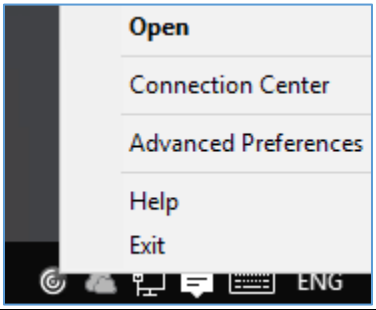
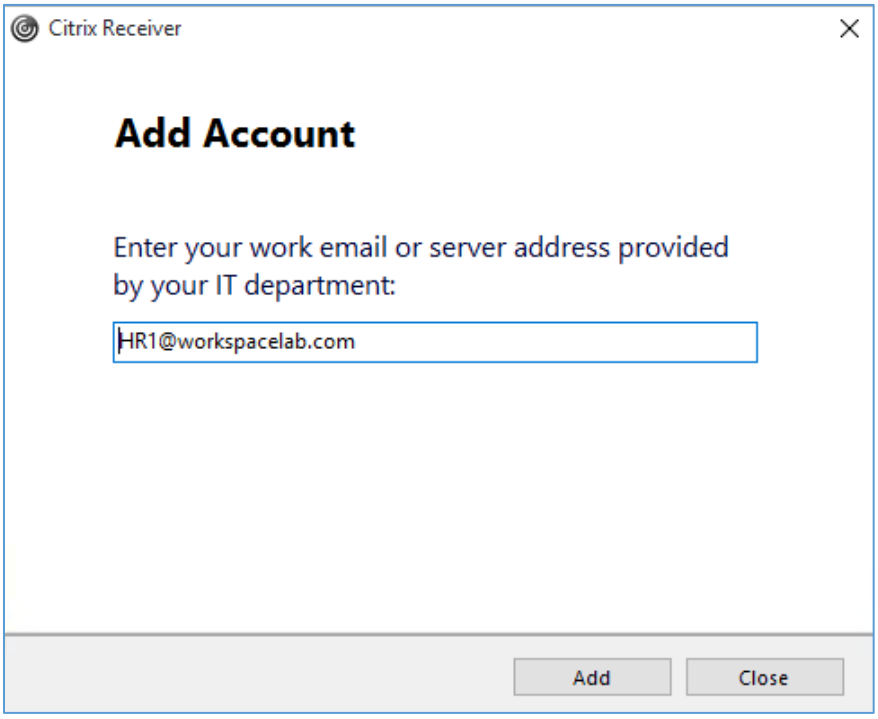
8. In the New Resource Record dialog box, enter the following information:
   - Service: _**citrixreceiver**
   - Protocol: _**tcp**
   - Priority: **0**
   - Weight: **0**
   - Port number: **443**
   - Host offering this service: **storefront.workspacelab.com**

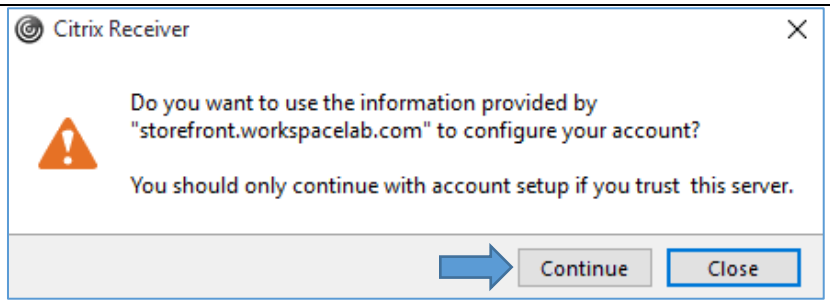
   Click **OK** on the New Resource Record window.

Click **Done** on the Resource Record Type window.



Close the **DNS Manager** console.

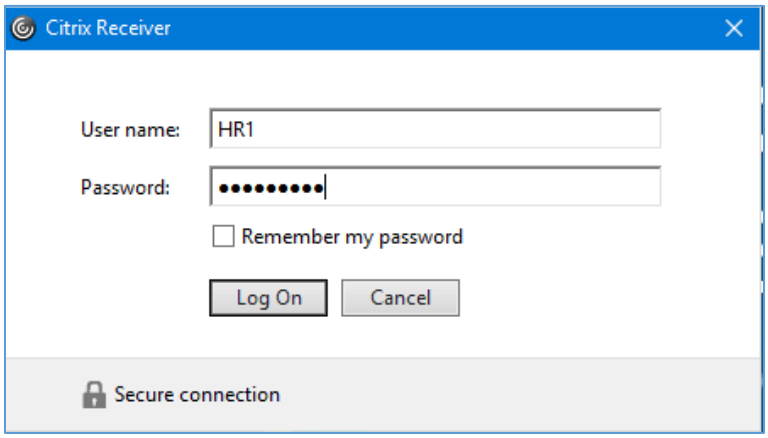
9.	Using the Remote Desktop Connection Manager, switch back to **NYC-WRK-001**. **Note**: In a previous exercise, you had logged on to NYC-WRK-001 using the following credentials to make the connection: • User name: Workspacelab\HR1 • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-WRK-001 by right-clicking this machine and selecting Connect server.
10.	On the lower-right corner of the Taskbar, right-click the **Receiver** icon and click **Open**. 
11.	On the Add Account page, enter **HR1@workspacelab.com** as the email address for HR1 and click **Add**.  Click **Continue** on the confirmation dialog box.



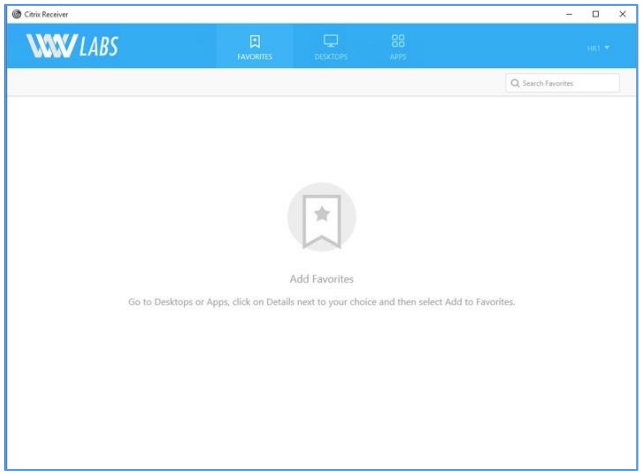
Note: You have successfully configured and tested email-based account discovery. Now you can give your test users at WW Labs the instructions to install Citrix Receiver and further instructions on how to configure Receiver using their own email address.

12. In the logon dialog box that opens, enter in the following credentials:
    - User name: **HR1**
    - Password: **Password1**

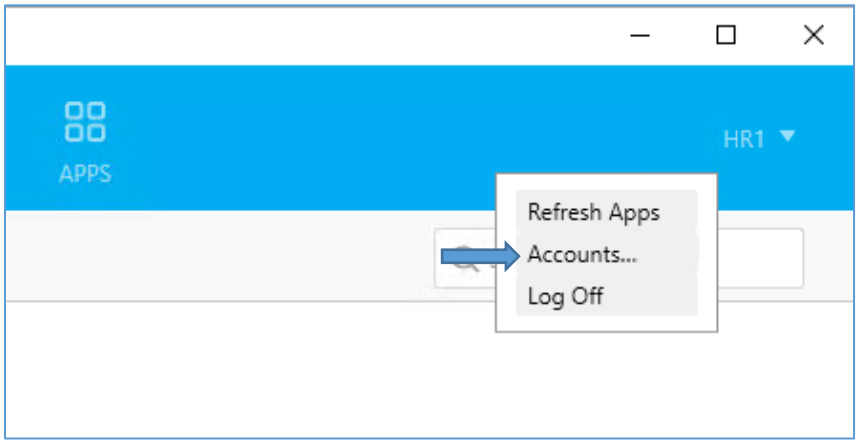
    Click **Log On**.



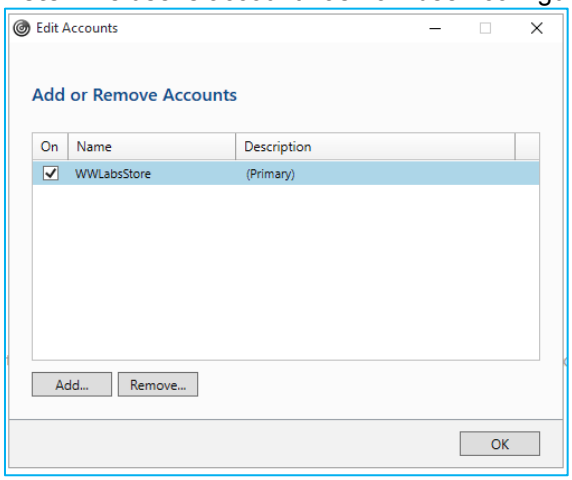
13. The user HR1 has now configured Citrix Receiver using his email address. The user is now logged on to Citrix Receiver and is pointing to the Citrix StoreFront Store.



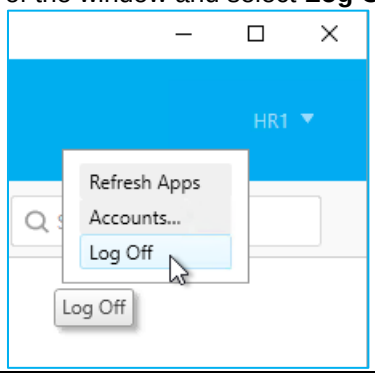
In the upper-right corner of Citrix Receiver, click the **down arrow** to the right of the HR1 user name and select **Accounts**.



Note: The user's account has now been configured for access to the WWLabsStore.



Click **OK** to close the Add or Remove Account window. Click on **HR1** in the upper-right corner of the window and select **Log Off**. Close **Citrix Receiver**.



Key Takeaways:

- Users can configure Citrix Receiver by entering their email address.
- This feature provides a much easier way for users to configure Citrix Receiver on unmanaged devices; alternatively, users would have to know both the internal and external connection URL.

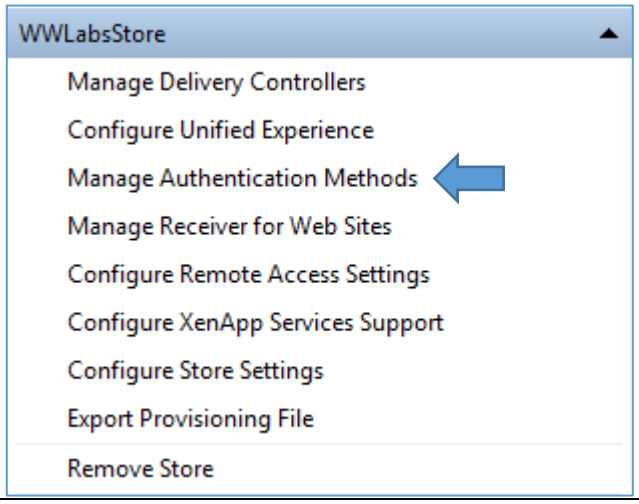
- Changes to the internal or external DNS server are required to support email-based discovery of stores.

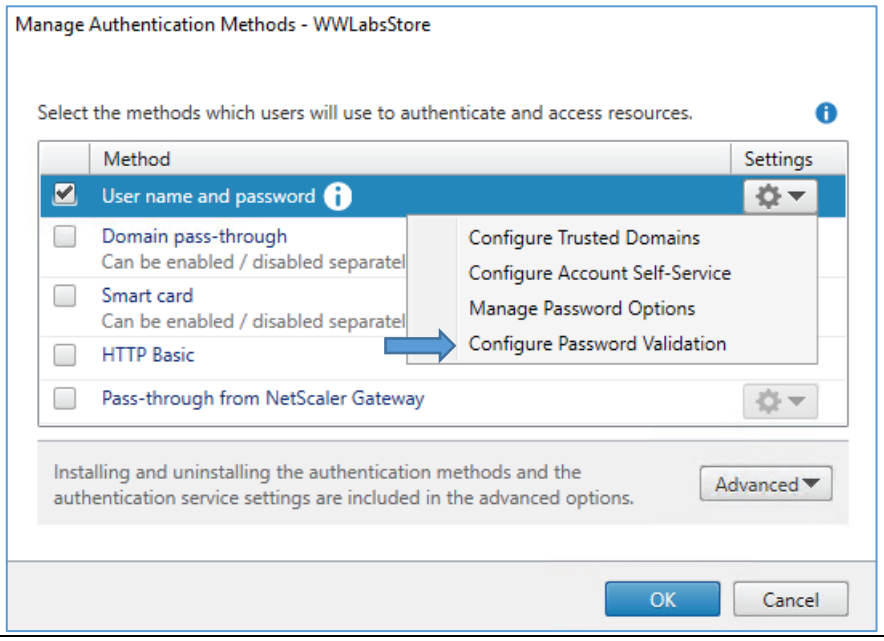
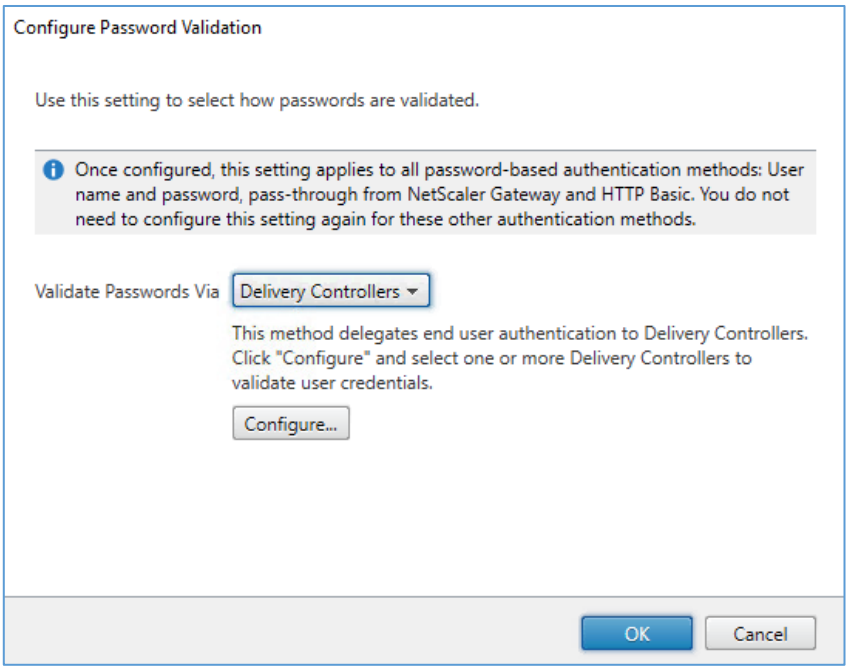
Exercise 5-10: Configure Delegated Authentication

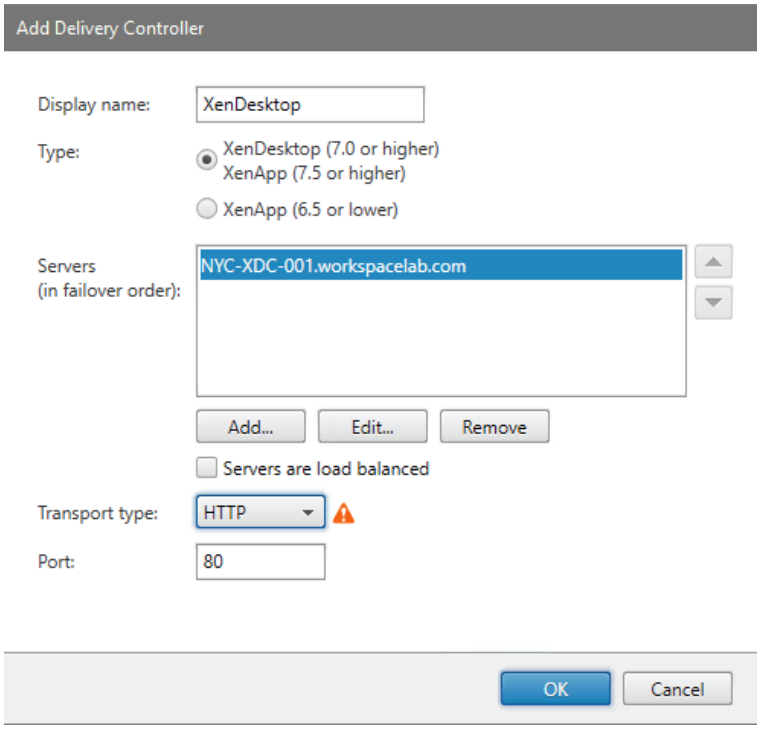
Scenario:

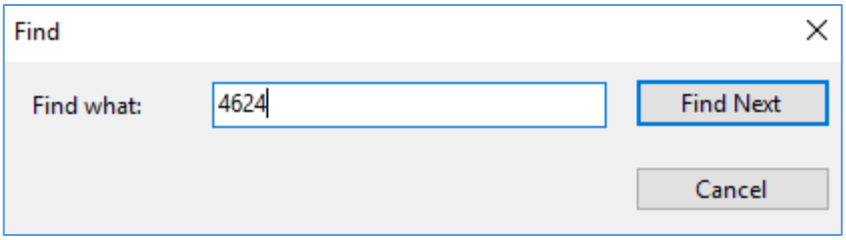
The WWLabs help desk team has experienced an increase in the amount of help desk calls related to resetting users' passwords and unlocking their Active Directory accounts. The increase is most likely related to a recent strengthening in the password complexity required by the security team. The CTO wants to implement a solution that will allow users to reset their own passwords and unlock their Active Directory accounts in case they type the wrong password multiple times.

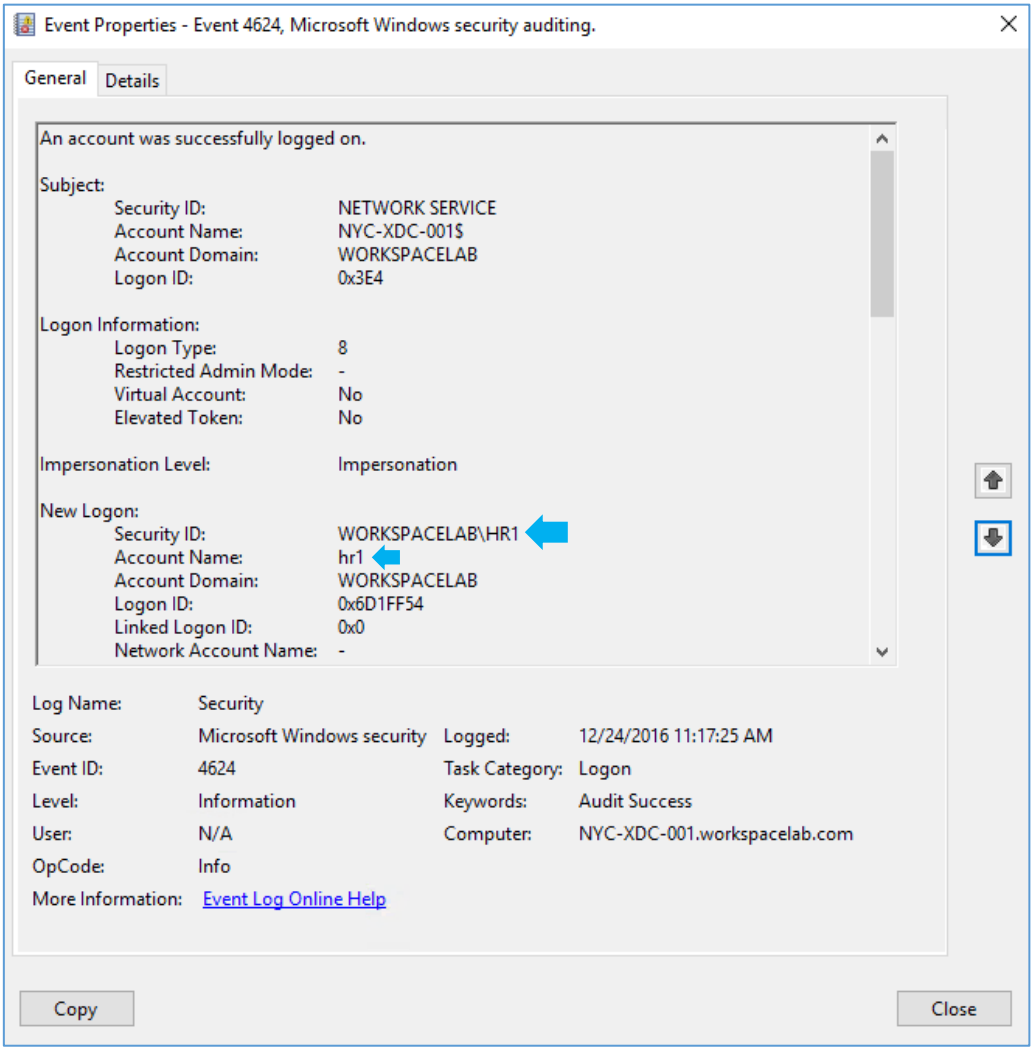
As a Citrix Administrator, you have been assigned the task of implementing the Self-Service Password Reset (SSPR) feature in the New York Data Center.

Step	Action
1.	Using the Remote Desktop Connection Manager, connect to **NYC-STF-001**. **Note**: The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1
2.	Start the **Citrix StoreFront** management console from the Windows Taskbar or Start menu. In the left pane, select the **Stores** node. In the middle pane, select **WWLabsStore**. In the right pane, under WWLabsStore, select **Manage Authentication Methods**. 

Step	Action
3.	Click the **Settings** icon for User name and password and select **Configure Password Validation**. 
4.	Using the drop-down menu next to Validate Passwords Via, select **Delivery Controllers**.  **Note**: Passwords are validated with Active Directory using the XML service on the Delivery Controllers. This can be used when the StoreFront server is not in the same domain as XenApp or XenDesktop and Active Directory trusts are unavailable.
5.	Click **Configure** and then click **Add**.

Step	Action
6.	In the Add Delivery Controller window, change the Display name to **XenDesktop**. Under servers, add **NYC-XDC-001.workspacelab.com**. Ensure that the **Servers are load balanced** option is *not* selected. Select Transport type as **HTTP**.  Click **OK**.
7.	Click **OK** on the Configure Delivery Controllers window. Click **OK** on the Configure Password Validation window.
8.	Click **OK** to close the Manage Authentication Methods – Store window.
9.	Using the Remote Desktop Connection Manager, connect to **NYC-WRK-001**. **Note**: The following credentials are used to make the connection: • User name: Workspacelab\HR1 • Password: Password1 **Note**: NYC-WRK-001 is a managed device on the internal network.
10.	Open **Internet Explorer** from the Desktop and browse to **https://storefront.workspacelab.com/Citrix/WWLabsStoreWeb**. Enter the following credentials to log on to Receiver for Web as HR1: • User name: **HR1** • Password: **Password1** **Note**: Wait for Receiver for Web to complete the logon before continuing. **Note**: You may experience Receiver automatically launching a desktop session at this point; this is default behavior when a user only has access to one virtual desktop. You will change this behavior in Exercise 5-12.

Step	Action
11.	Using the Remote Desktop Connection Manager, connect to **NYC-XDC-001**. **Note**: The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1
12.	Right-click the Start menu and open **Event Viewer**. Navigate to **Event Viewer** > **Windows Logs** > **Security**. In the right corner of the console, select **Find**. Enter **4624** in the Find what field and click **Find Next**.  Locate the most recent **4624** event where the Security ID is **Network Service**. Close the **Find window**. Double-click this event log.

Step	Action
13.	Note that this event captures an **impersonation request** for HR1.  Click **Close** to close the Event Properties dialog box. Close the **Event Viewer**.

Key Takeaways:

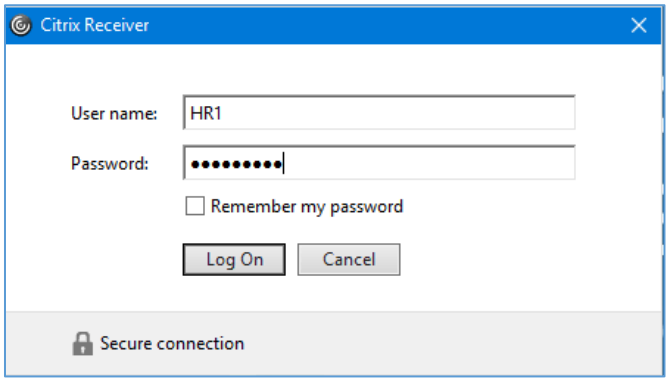
- Citrix StoreFront can be configured to use Active Directory or Delivery Controllers for authentication.
- Active Directory is the default configuration.
- The Delivery Controllers should be used for authentication when the StoreFront server is a member of a domain that does not trust the domain containing the user accounts.

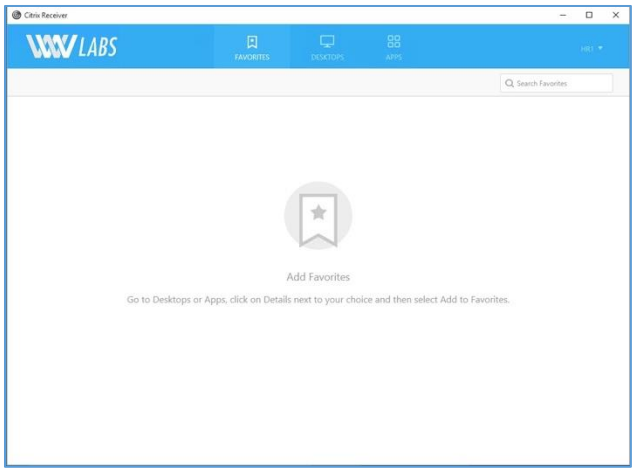
Exercise 5-11: Add Favorites to the StoreFront store

Scenario:

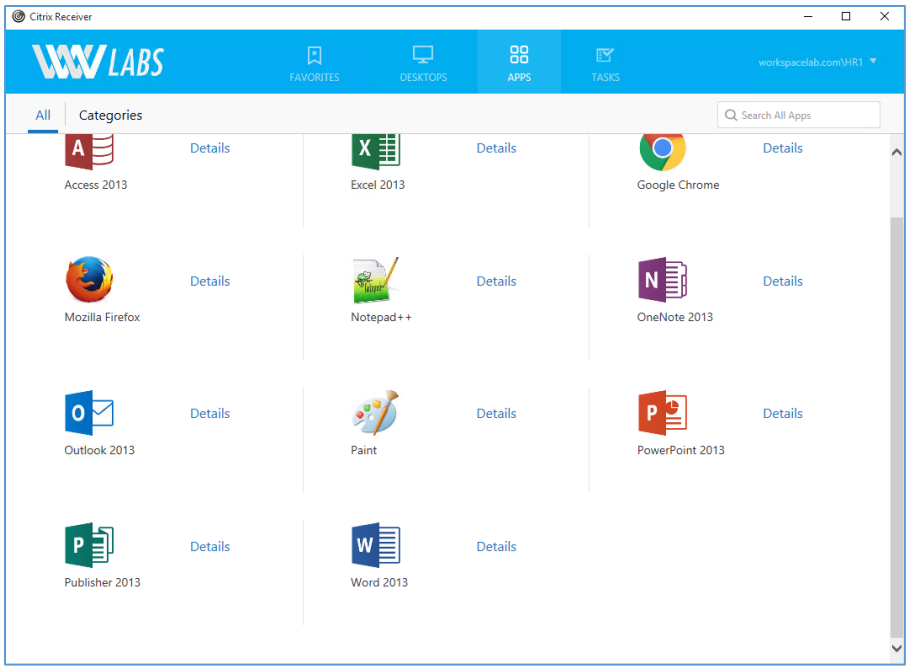
To further address the CTO's concerns for ease of access for the users, you have been tasked to add Favorites to the store.

A Favorite is a subscription to an application that is duplicated into the Favorite area of Receiver, which allows for quick navigation and shortcut placements on the Desktop or Start screen of the endpoint.

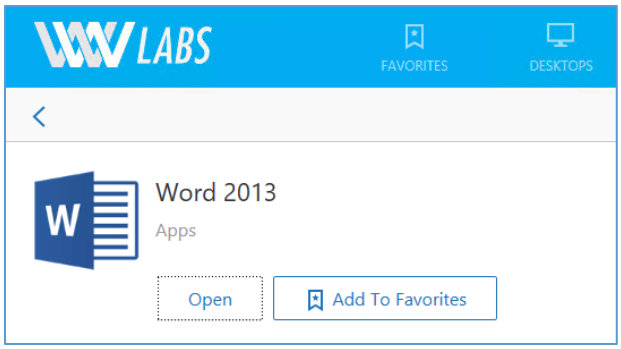
Step	Action
1.	Using the Remote Desktop Connection Manager, verify that you are still connected to **NYC-WRK-001**. **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-WRK-001 by right-clicking this machine and selecting Connect server. **Note**: The following credentials are used to make the connection: • User name: Workspacelab\HR1 • Password: Password1
2.	Click **Start** and in the left pane of the Start menu under Recently added, click **Citrix Receiver**. Log on with the following credentials: • User name: **HR1** • Password: **Password1** 
3.	Review the **Favorites** tab and notice that there are no applications listed.

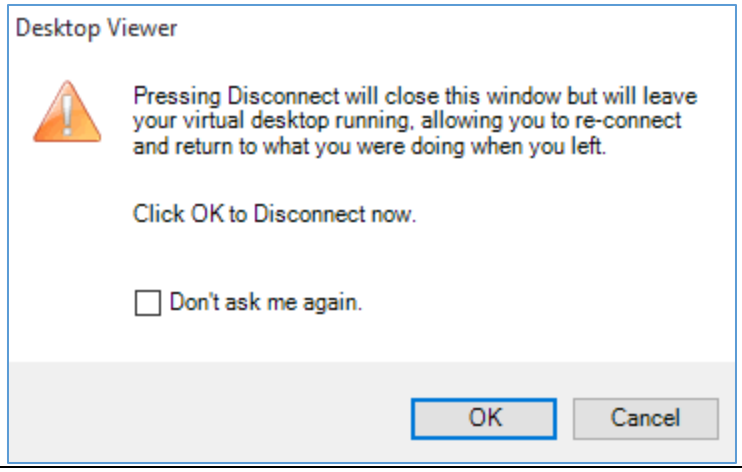
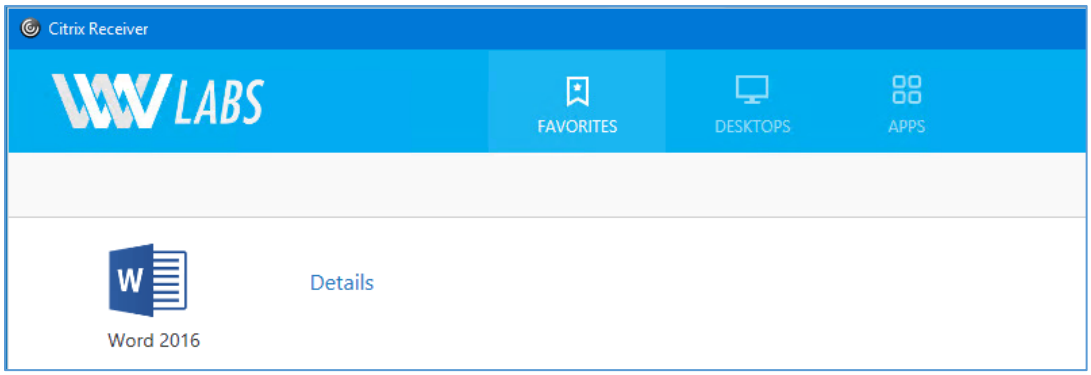


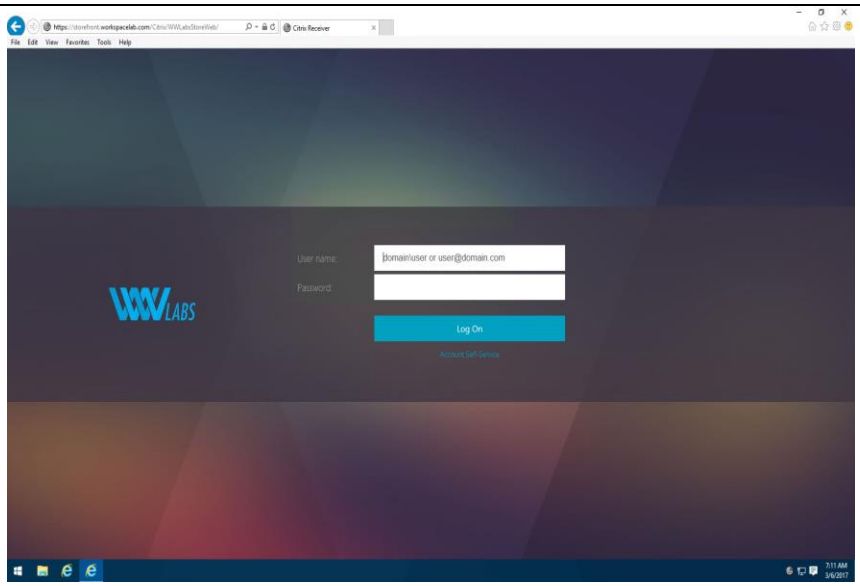
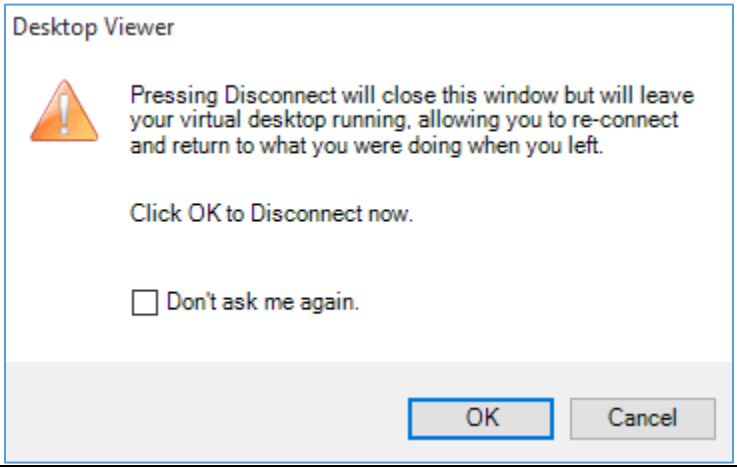
Click on the **APPS** tab on the top banner of Receiver.



To the right of Word 2016, click **Details**, and then click **Add to Favorites**.



	Note: A Desktop session automatically opens for HR1. This is because Auto-launch Desktop is enabled by default. You will disable this in Exercise 5-12. Click **X** to disconnect the desktop session. Click **OK** on the warning message. 
4.	Navigate back to the **FAVORITES** tab on the top banner of Receiver. Notice that **Word 2016** now appears as one of the Favorite applications. 
5.	Close **Citrix Receiver**, open **Internet Explorer**, and browse to the Receiver for Web by navigating to **https://storefront.workspacelab.com**.

	 **Note**: Click Allow on the dialog box on the bottom of the browser, if prompted. Log on using the following credentials: • User name: **HR1** • Password: **Password1** Notice that **Word 2016** appears in the Favorites tab when accessing from the StoreFront page as well. **Note**: A Desktop session automatically opens for HR1. This is because Auto-launch Desktop is enabled by default. You will disable this in Exercise 5-14. Click **X** to disconnect the desktop session. Click **OK** on the warning message. 
6.	Log off the **StoreFront page**, close **Internet Explorer**, and log off **NYC-WRK-001**.

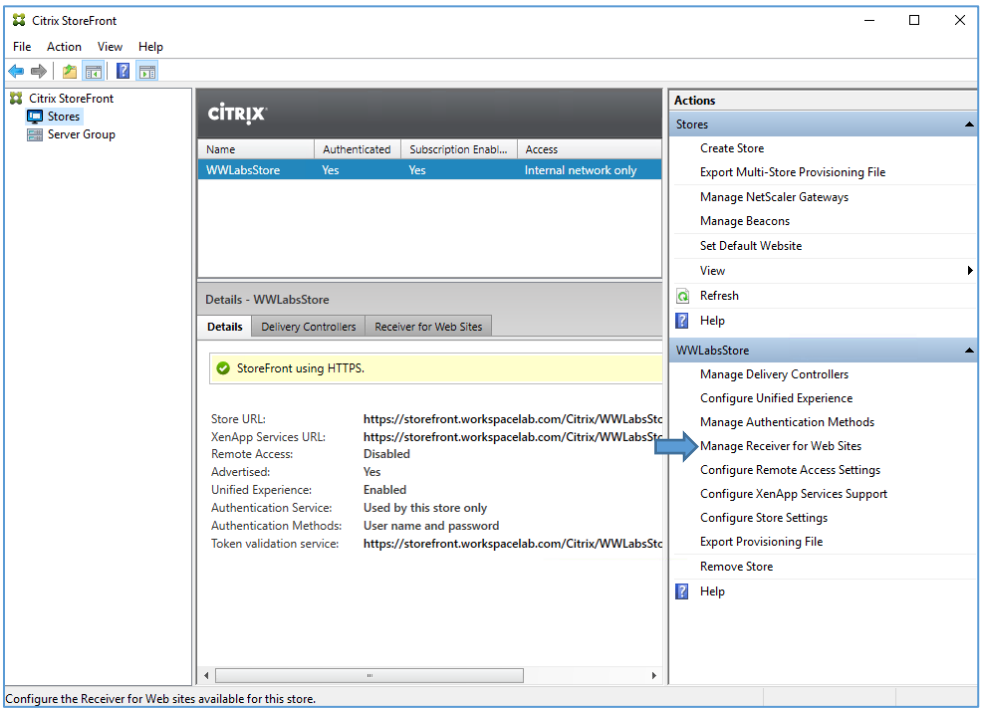
Key Takeaways:

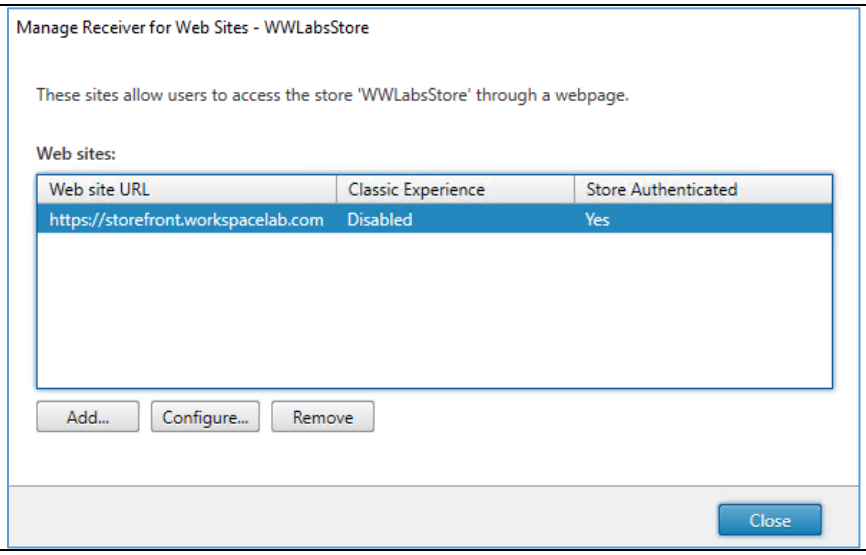
- StoreFront uses a device-independent subscription store to present the user with all chosen applications on any device used.
- When hosting multiple stores on the same StoreFront Server, each store will have its own subscription database; however, this is customizable using PowerShell.

Exercise 5-12: Disable Desktop Auto-launch

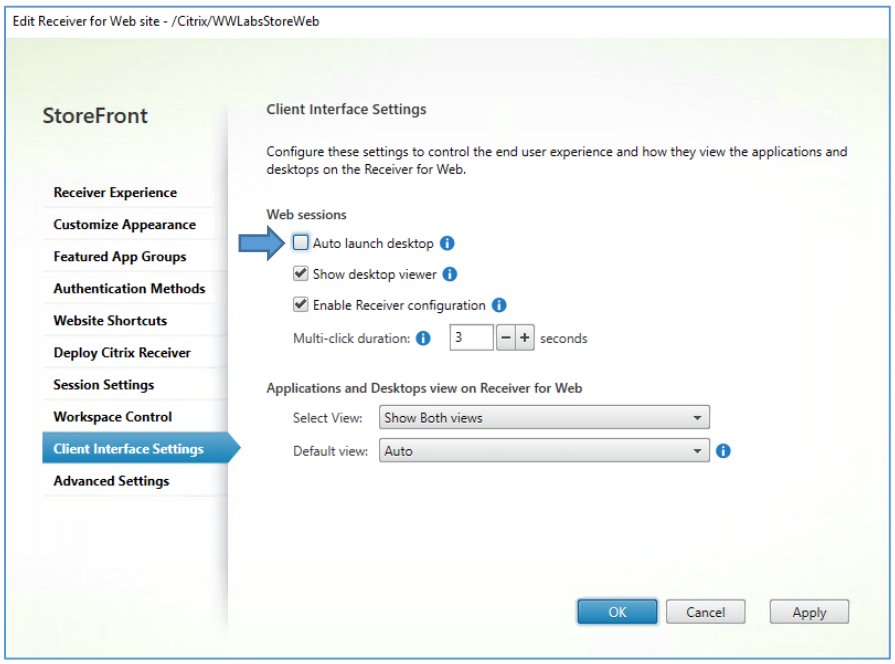
Scenario:

The WW Labs CTO has expressed concerns that the automatic launch of a desktop session every time a user signs into StoreFront may cause confusion for the users. You have been tasked to disable this functionality for the remainder of the POC.

Step	Action
1.	Using the Remote Desktop Connection Manager, confirm that you are still connected to **NYC-STF-001**. **Note**: In a previous exercise, you had logged on to NYC-STF-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-STF-001 by right-clicking this machine and selecting Connect server.
2.	Switch to the **StoreFront Management Console**. In the left pane, select **Stores**. In the center pane, verify that the **WWLabsStore** store is selected. In the right pane, click **Manage Receiver for Web Sites**.  **Note**: The StoreFront Management Console was started in a previous exercise. If the console was closed in a previous exercise, then click Start > Citrix > Citrix StoreFront.
3.	On the Manage Receiver for Web Sites – WWLabsStore dialog box, click **Configure**.



4. In the left side of the dialog box, select **Client Interface Settings**. In the right side of the dialog box, uncheck **Auto launch desktop**.



Click **Apply** and then click **OK**.

Click **Close** to exit the Manage Receiver for Web Sites – WWLabsStore window.

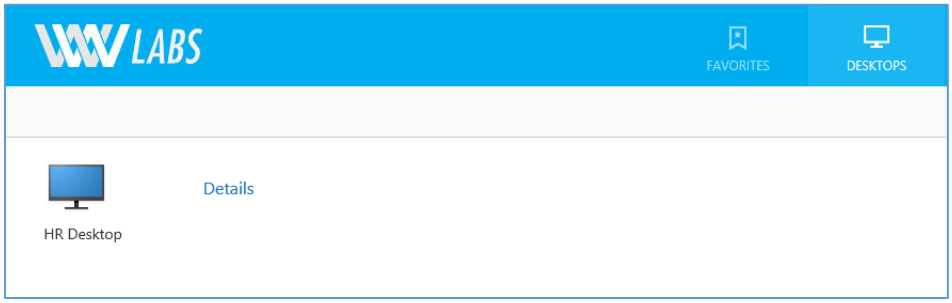
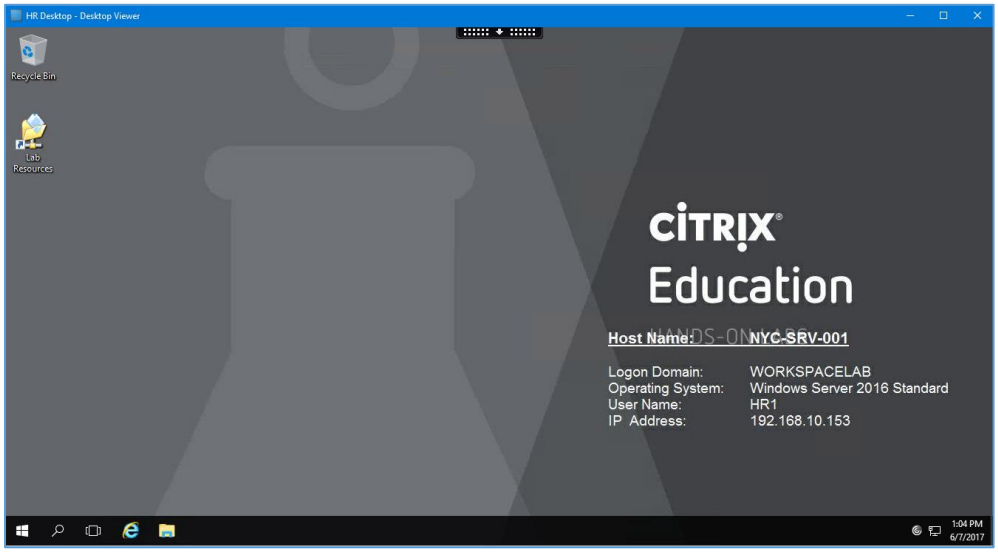
Key Takeaways:

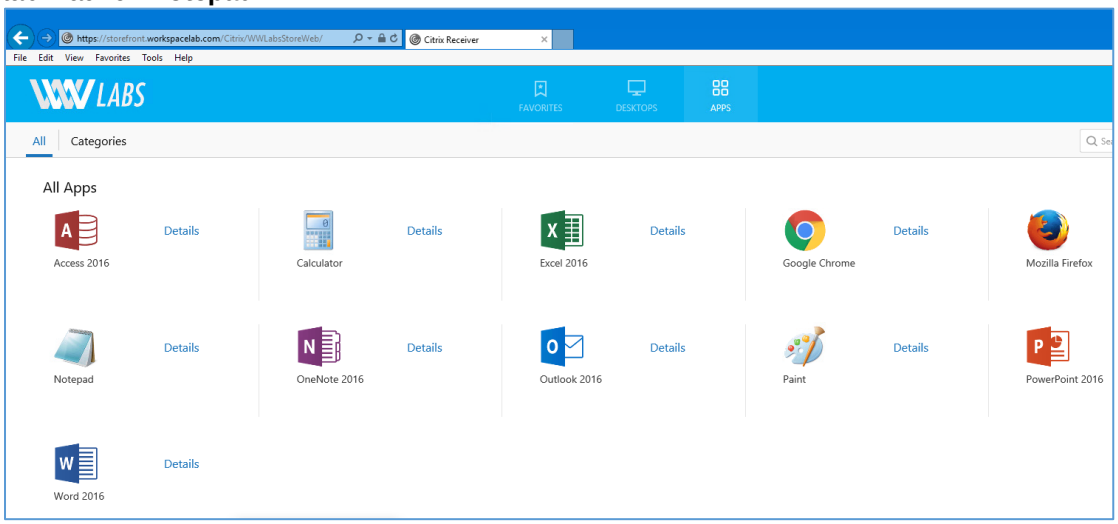
- Desktop Auto-launch is a great feature when users are only integrating with one single desktop each time they log on to StoreFront.
- For users that have access to both a desktop and published applications, the feature might launch unnecessary items, both leading to user frustration and extra resource usage.

Exercise 5-13: Launch an application and desktop from a Server OS

Scenario:

Having completed your StoreFront and Receiver deployment tasks, you will test the ability to launch an application and a desktop hosted on a Server OS machine using the StoreFront store.

Step	Action
1.	Using the Remote Desktop Connection Manager, connect to NYC-WRK-001. To log on to NYC-WRK-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\HR1 • Password: Password1
2.	Open **Internet Explorer** and browse to **https://storefront.workspacelab.com**. Log on using the following credentials: • User name: **HR1** • Password: **Password1**
3.	Click the **DESKTOPS** tab and launch the **HR Desktop**.  Verify that the **HR Desktop** starts. 

4.	From the Internet Explorer window that the HR Desktop was launched from, click the **APPS** tab. Launch **Notepad**.  Interact with the **HR Desktop** and the **Notepad** sessions. When finished, log off the **HR Desktop** and click **File** > **Exit** on the Notepad session.
5.	Log off Receiver for Web. Click **HR1** and select **Log Off**. Close **Internet Explorer**.

Key Takeaways:

- Users are able to launch an application and desktop from a Server OS in XenDesktop.

Exercise 5-14: Launch a desktop from a Remote PC

Scenario:

Your task is to test the Remote PC feature by launching a desktop from the Remote PC machine.

Step	Action
1.	Using the Remote Desktop Connection Manager, connect to NYC-WRK-001. To log on to NYC-WRK-001, right-click this machine and choose **Connect server**. **Note**: The following credentials are used to make the connection: • User name: Workspacelab\HR1 • Password: Password1
2.	Open **Internet Explorer** and browse to **https://storefront.workspacelab.com**.
3.	Log on using the following credentials: • User name: **Designer1** • Password: **Password1**
4.	Click on the **DESKTOPS** view in the middle and launch the **NYC-DG-RemotePC**. **Note**: If you receive a Cannot start desktop error, check if there is still a session connected to NYC-WRK-002. Verify that you have logged off the machine using Remote Desktop Connection Manager, or check the status of the machine using Studio. Alternatively, reboot NYC-WRK-002 to clear out any hanging sessions.

	Note: Remote PC Access provides users with remote access to their physical office desktops, allowing them to work at any time from any location. **Note**: There may be several windows that open, triggered by the logon to the NYC-DG-RemotePC Desktop, such as a *Setting up your apps* welcome screen and / or a Receiver Add Account screen. It may take a few minutes for the *Setting up your apps* window to disappear.
5.	Close any open application and log off the desktop. Log off Receiver for Web and close Internet Explorer. Log off **NYC-WRK-002** and **Receiver for Web**. Close **Internet Explorer**.

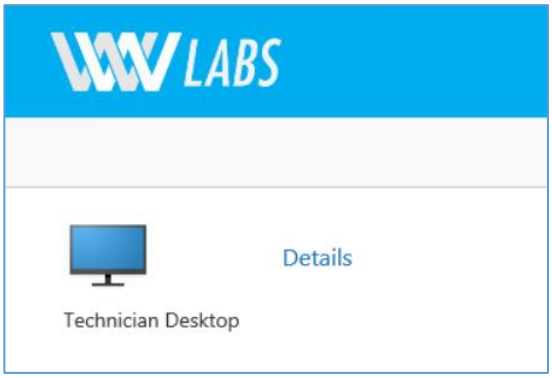
Key Takeaways:

- Designer1 is able to launch a Remote PC desktop to the NYC-WRK-002 Workstation.

Exercise 5-15: Launch a desktop from a Desktop OS

Scenario:

Your task is to test a desktop launch from a VDI machine by launching a desktop on a Desktop OS.
In this exercise, you will learn to launch a desktop on a Desktop OS.

Step	Action
1.	Using the Remote Desktop Connection Manager, connect to NYC-WRK-001. To log on to NYC-WRK-001, right-click this machine and choose **Connect server**. **Note**: The following credentials are used to make the connection: • User name: Workspacelab\HR1 • Password: Password1
2.	Open **Internet Explorer** and browse to **https://storefront.workspacelab.com**.
3.	Log on using the following credentials: • User name: **Technician1** • Password: **Password1**
4.	Click the **DESKTOPS** view and launch the **Technician Desktop**.  If needed, select **Read/write access** in the HDX File Access window. **Note**: The Citrix Receiver Add Account window may open. If so, close it.

	Note: There may be several windows that open, triggered by the logon to the Technician Desktop, such as a *Setting up your apps* welcome screen and / or a Receiver Add Account screen. It may take a few minutes for the *Setting up your apps* window to disappear.
5.	Spend a few minutes interacting with this **Desktop OS session** and then log off the **Technician Desktop**.
6.	Log off Receiver for Web. Click **Technician1** and choose **Log Off**. Close **Internet Explorer**.
7.	Log off **NYC-WRK-001**.

Key Takeaways:

- Technician users are able to launch desktop sessions hosted on a Desktop OS.

Module 6: Understanding and configuring Citrix policies

Overview:

This module presents the role of policies in customizing the end user experience and the process for configuring policies and determining the resultant set of policy. You will identify how policies can be used to control session management and user connectivity through features such as Load Management, Session Reliability, and Auto Client Reconnect.

Before you begin:

Estimated time to complete Module 6 lab exercises: 75 minutes

Exercise 6-1: Create a Group Policy to set Baseline-Computer settings

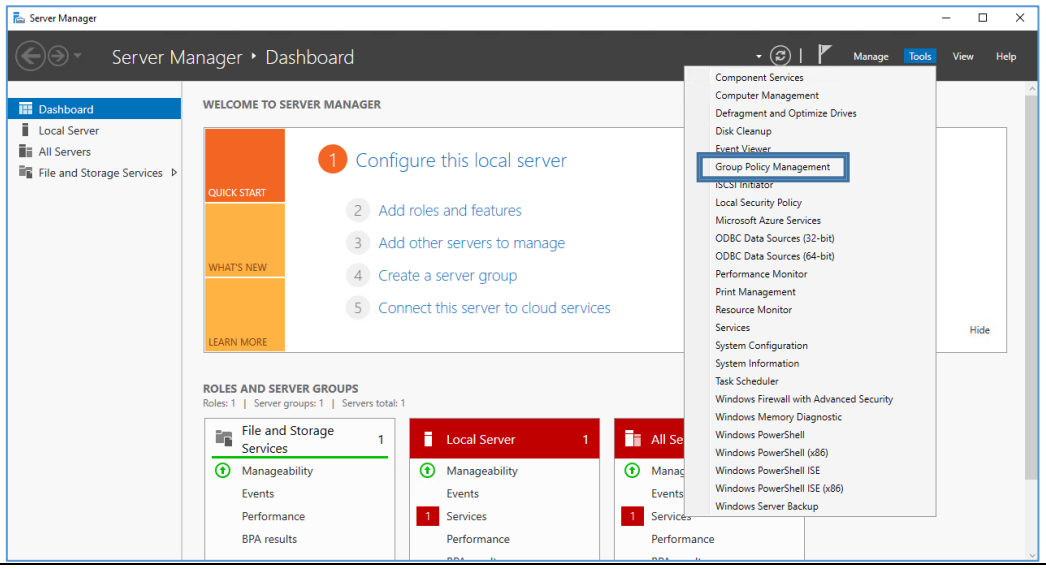
Scenario:

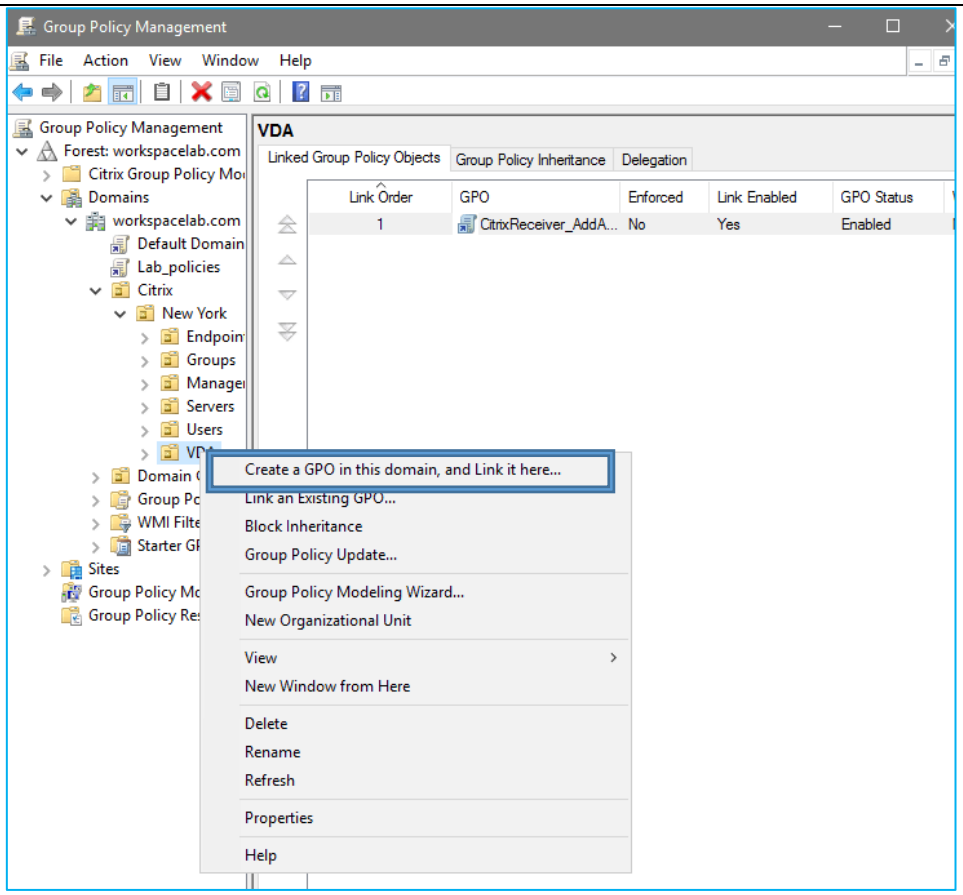
You have been tasked to create a Group Policy Object (GPO) to enforce a set of settings that can be applied to all VDAs distributed in this environment.

This type of policy configuration is called a baseline policy because you are creating a standard set of common parameters to apply to a complete set of objects, such as in this case, machines running the VDA.

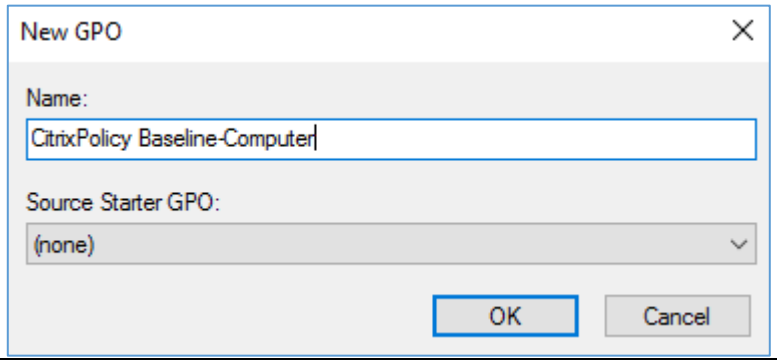
In many environments, these computer settings baseline policies are set to configure security, accessibility, or performance settings to common values that are dependent on the specific company directives.

Step	Action
1.	The following VMs are required before beginning the exercises for this Module; all others may be powered down. To power manage your VMs, switch to XenCenter, right-click on the VM in the left pane and select Start or Shut Down. If prompted click Yes. • NYC-ADS-001 • NYC-SQL-001 • NYC-FSR-001 • NYC-XDC-001 • NYC-STF-001 • NYC-MAN-001 • NYC-SRV-001 • NYC-DTP-001 • NYC-WRK-001 **Note**: These above VMs are listed in the start-up order.
2.	Using the Remote Desktop Connection Manager, connect to NYC-XDC-001. To log on to NYC-XDC-001, right-click this machine and choose **Connect server**. **Note**: The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1

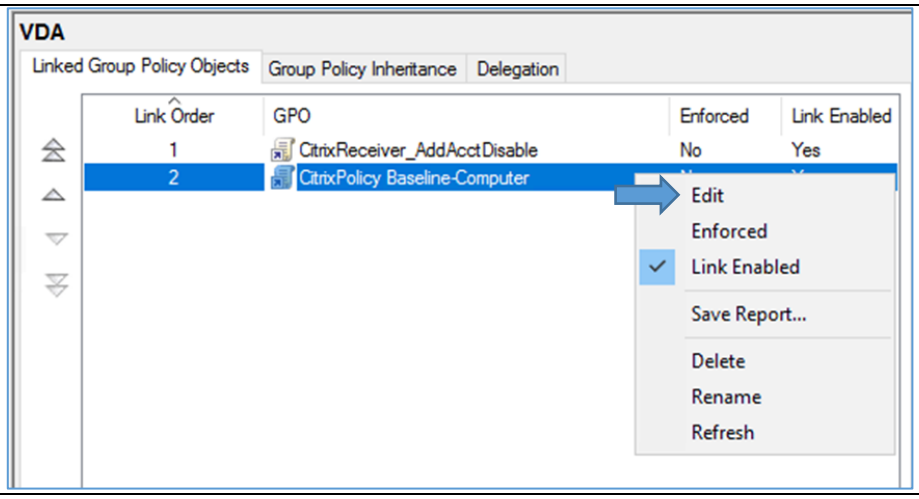
3.	Start the Group Policy Management Console. Click **Start** > **Server Manager**. **Note**: Wait for the Server Manager to open. Click **Tools** > **Group Policy Management** to start the Group Policy Management Console (GPMC). 
4.	Expand the Organizational Unit (OU) structure to the OU you have been tasked to create this baseline policy in. Expand **Forest: workspacelab.com** > **Domains** > **workspacelab.com** > **Citrix** > **New York** > **VDA** to view the **VDA** OU. Right-click the **VDA** OU and select **Create a GPO in this domain, and Link it here**.



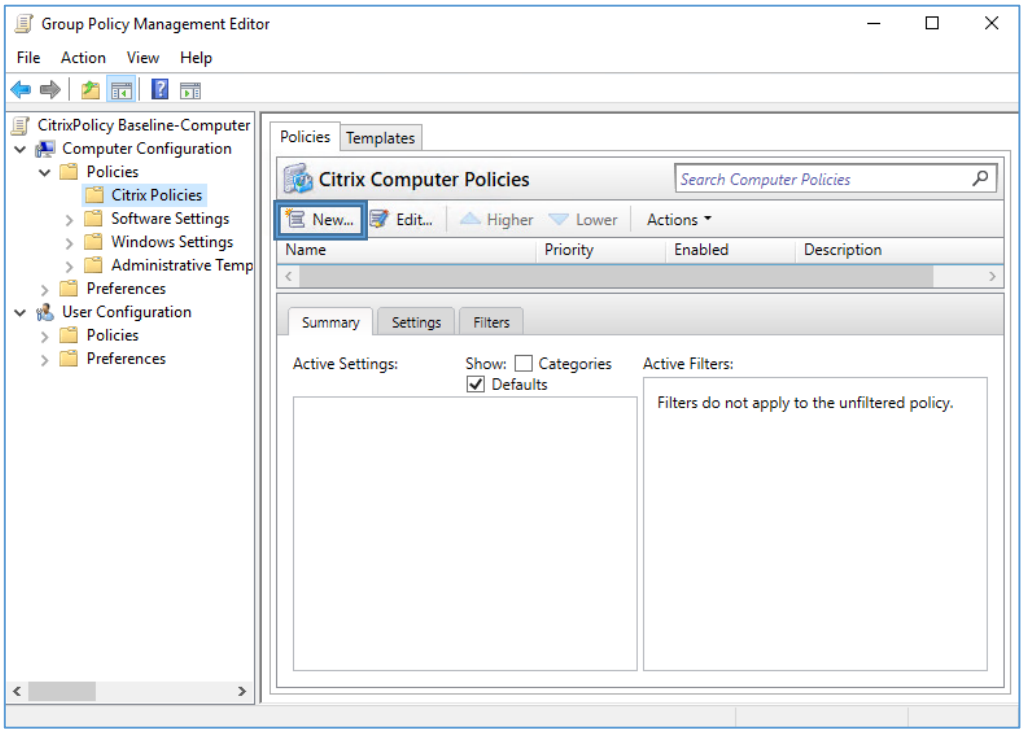
5. In the New GPO dialog box, enter **CitrixPolicy Baseline-Computer** for the Name. Click **OK**.



6. Right-click the **CitrixPolicy Baseline-Computer** Group Policy Object (GPO) just created and select **Edit**.



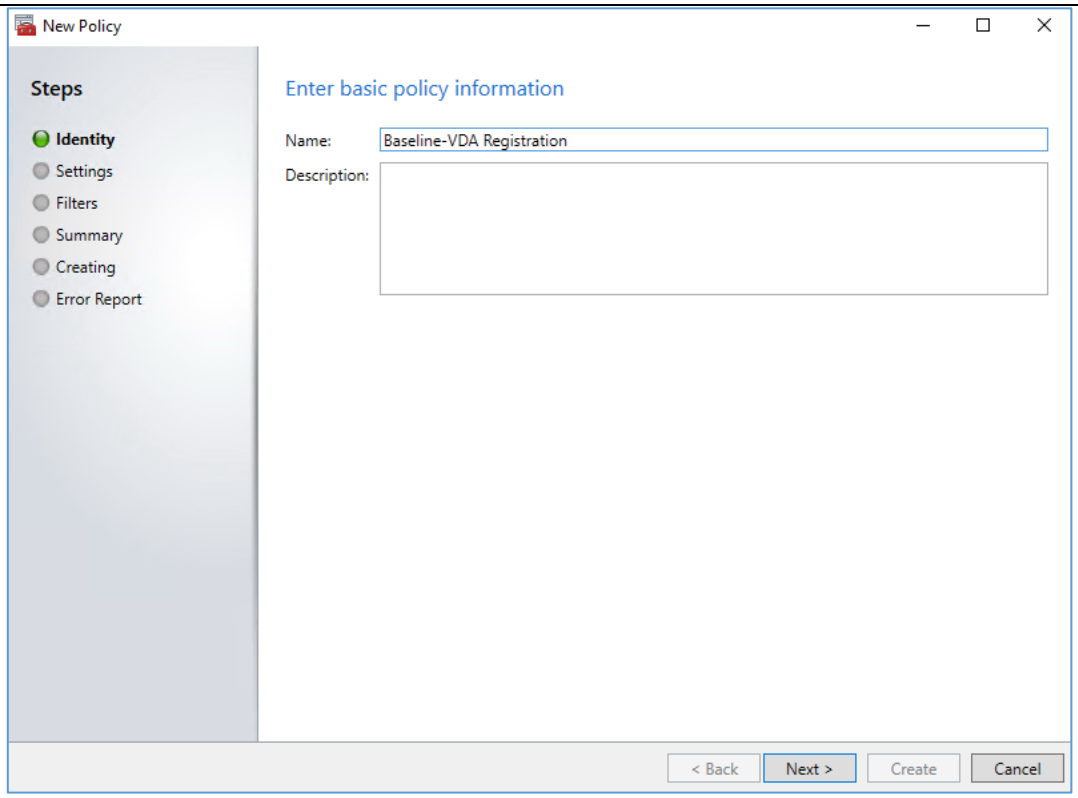
7. In the Group Policy Management Editor dialog box, in the left pane, expand **Computer Configuration** > **Policies** > **Citrix Policies**.



Note: There is a Citrix Policies element under the Policies container for both Computer Configuration and User Configuration.

In the center pane, click **New**.

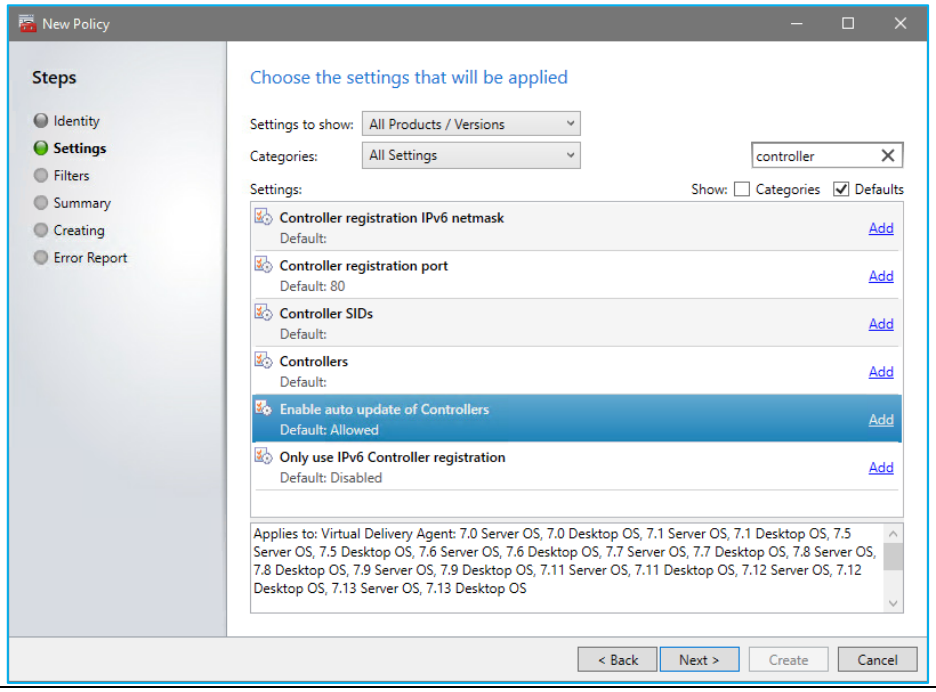
8. On the Identity page, enter **Baseline-VDA Registration** in the Name field.

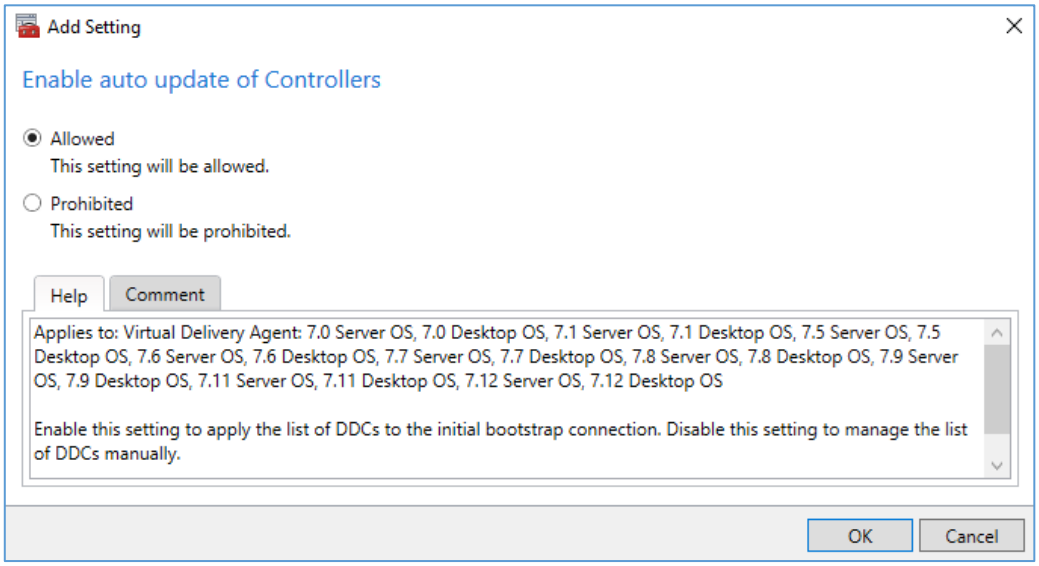
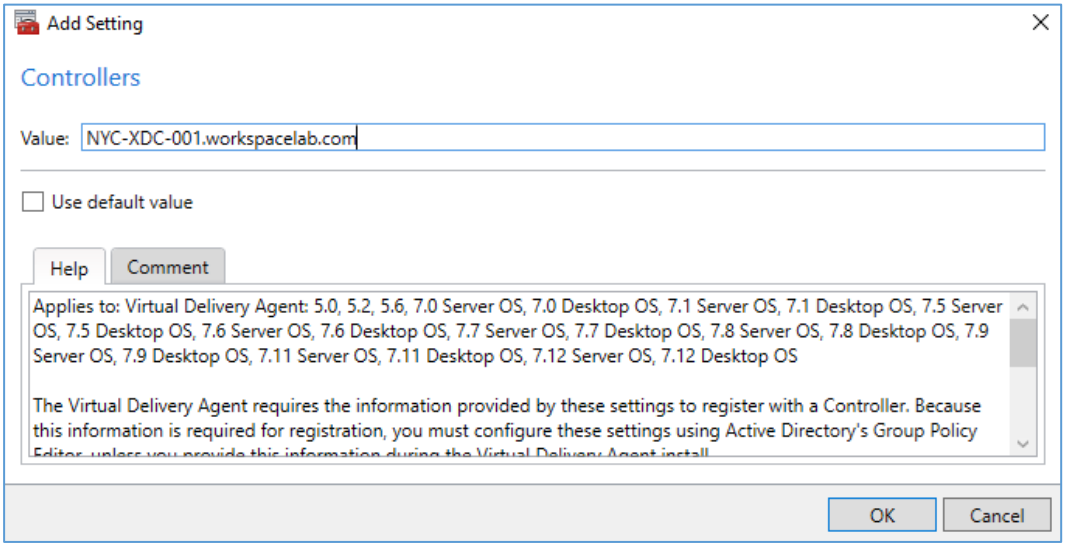


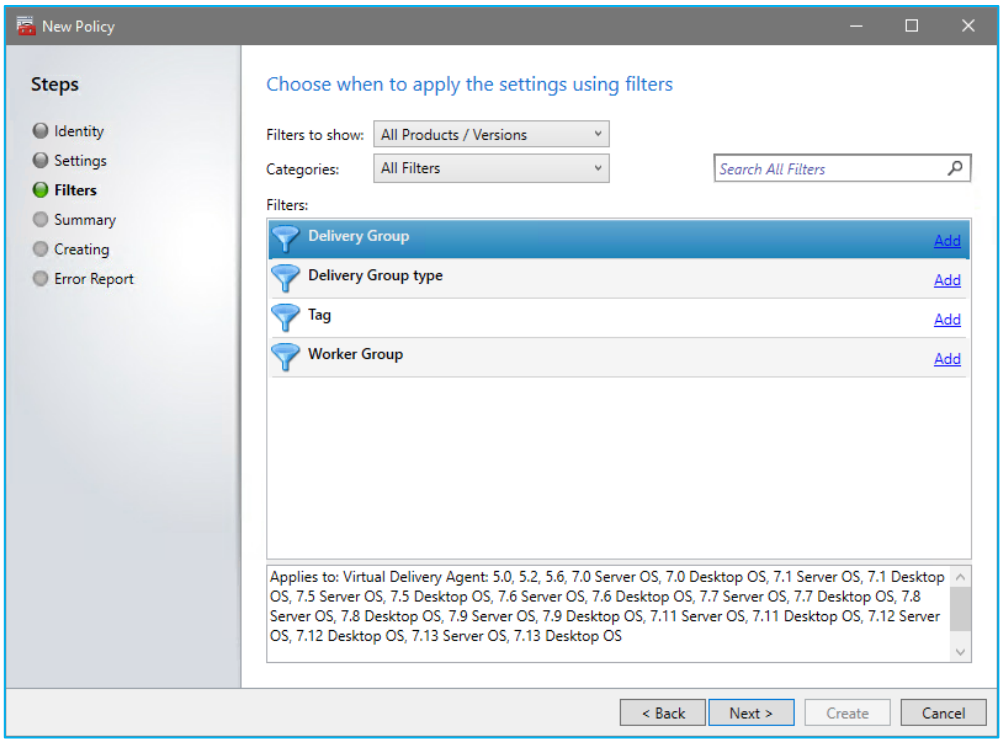
Click **Next** to continue the policy creation wizard.

9. On the Settings page, locate the search field on the top right and type **Controller**.

Note: This is to filter the policy rules to display only those rules to set parameters for/with Controllers.

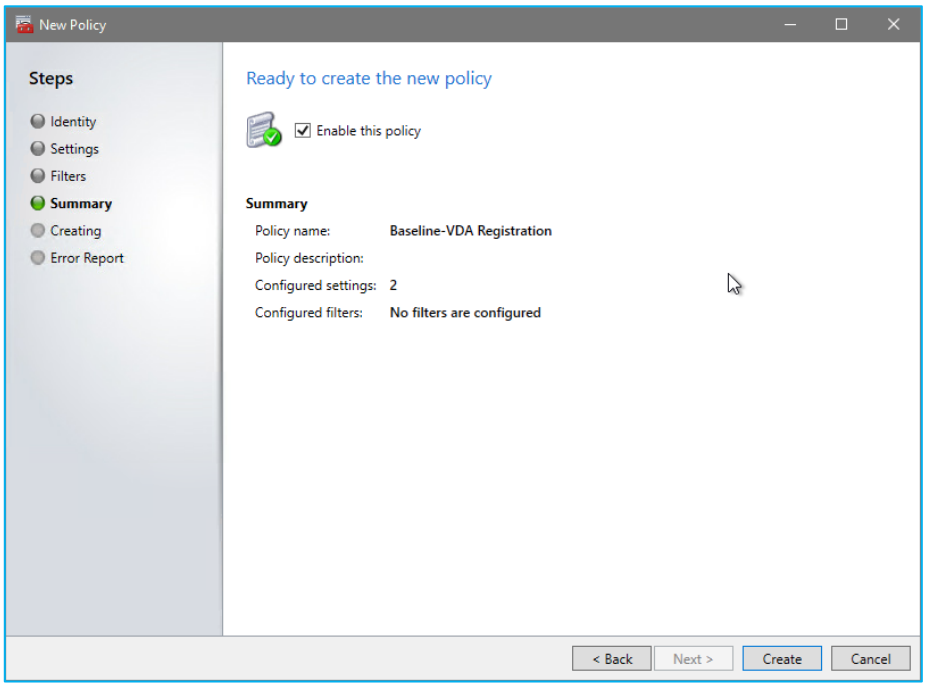


10	Under Settings, next to the Enable auto update of Controllers setting, click **Add**. In the Add Setting dialog box, verify that the **Allowed** radio button is selected.  Click **OK**. **Note**: This policy rule impacts the VDA to Delivery Controllers registration. New Delivery Controllers added to a farm or any Delivery Controller removed from the farm, then an updated list of Delivery Controllers are sent to the VDAs for registration. The next policy setting to use this Enable auto update of Controllers is to specify the list of Controllers to use.
11	Under Settings, next to the **Controllers** setting, click **Add**. In the Add Setting dialog box, enter **NYC-XDC-001.workspacelab.com** as the value.  Click **OK**, and then click **Next**. **Note**: If more than one Delivery Controller is being used, input the list separating the FQDN names with a space. The Virtual Delivery Agent requires this information provided by these settings to register with a Controller.
12	On the Filters page, click **Next**.

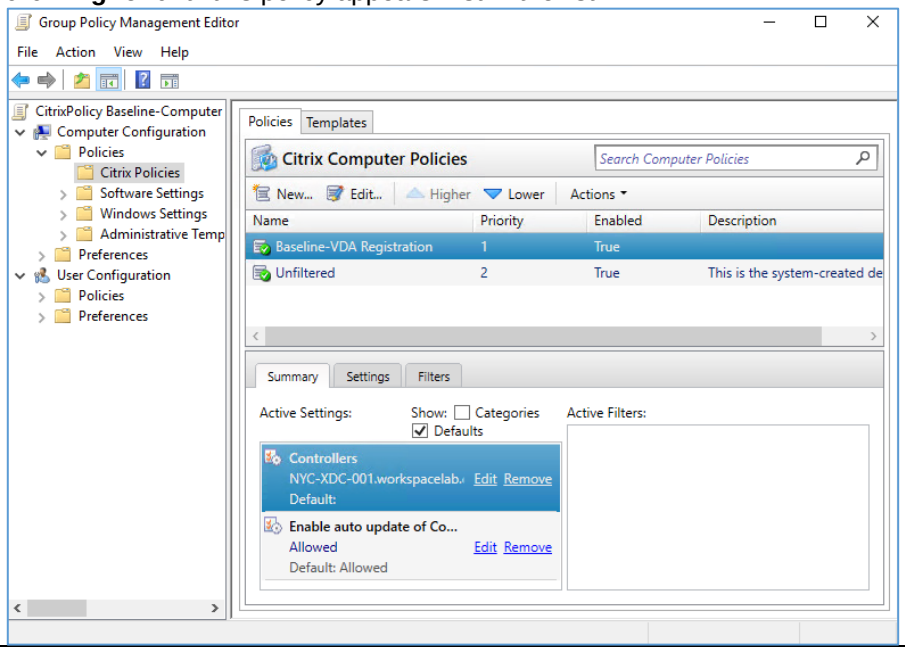


Note: In general, a policy is applied using a filter. A policy created within the Group Policy Management Console (GPMC) additionally applies depending on the OU in which the policy was created.

13 On the Summary page, verify that the checkbox to **Enable this policy** is selected.



Click **Create**.

14	In the middle pane under Policies, select **Baseline-VDA Registration** and in the menu above, click **Higher** until this policy appears first in the list. 
15	Click **X** in the top right corner to close the Group Policy Management Editor dialog box.

Key Takeaways:

- As a leading practice, create a baseline policy matching the settings for most company users, then build exceptions to this baseline for groups of users or special scenarios.
- Policies that are not filtered apply to all computers or all sessions.
- Avoid using the pre-created unfiltered policy because this name exists across all policies and will make troubleshooting more difficult.

Exercise 6-2: Configure baseline Citrix user policy using Group Policy

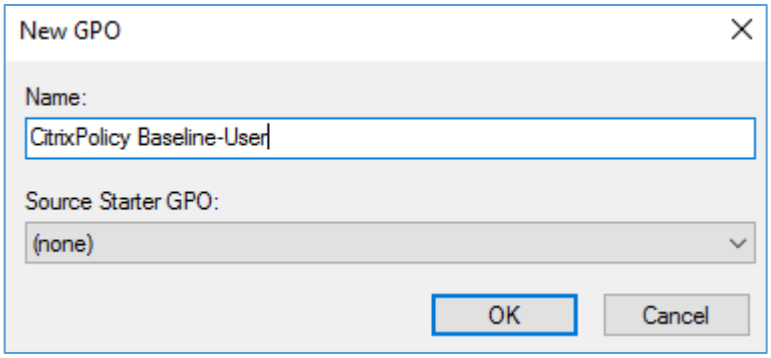
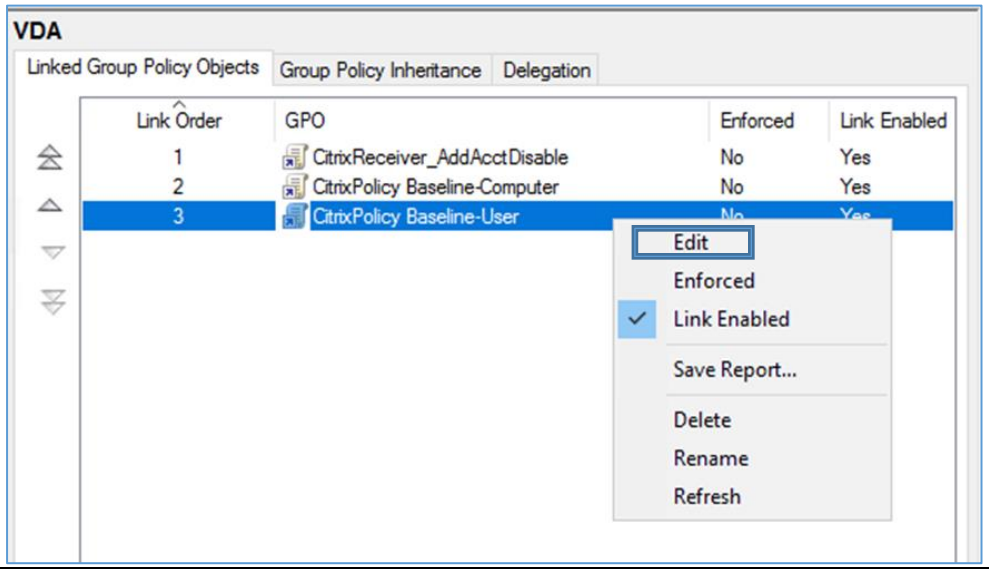
Scenario:

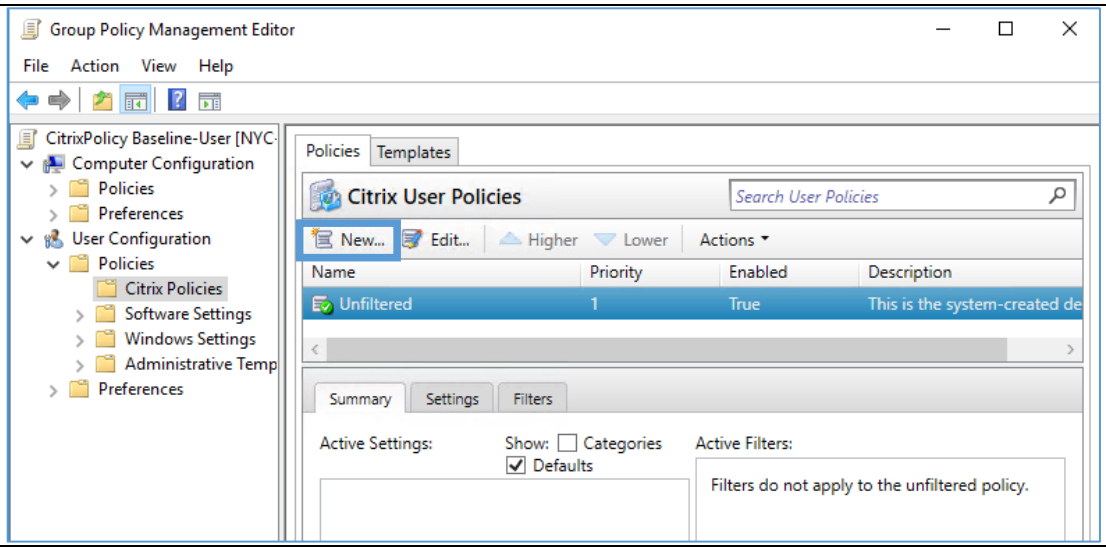
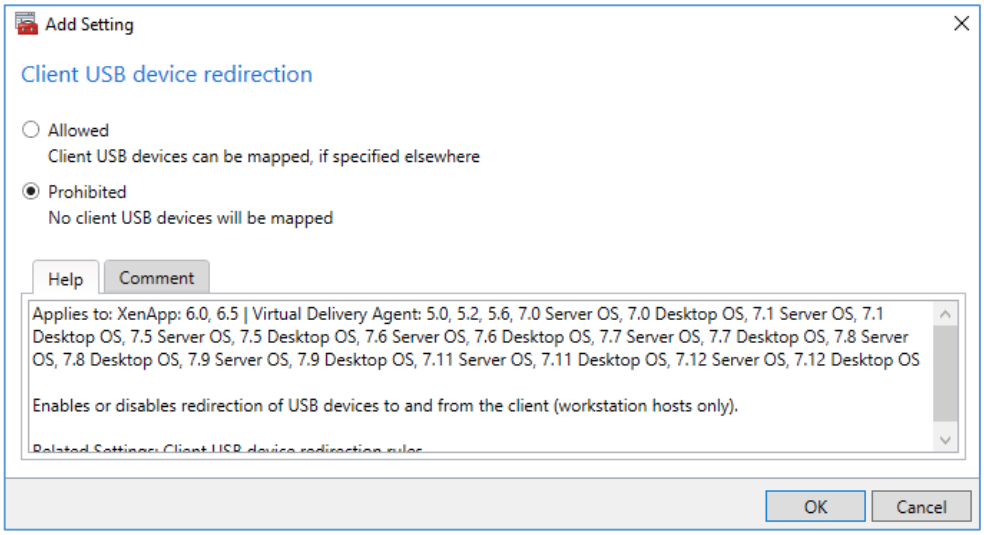
You have been tasked to create a Group Policy Object (GPO) to configure a set of settings that can be applied to all users in this environment.

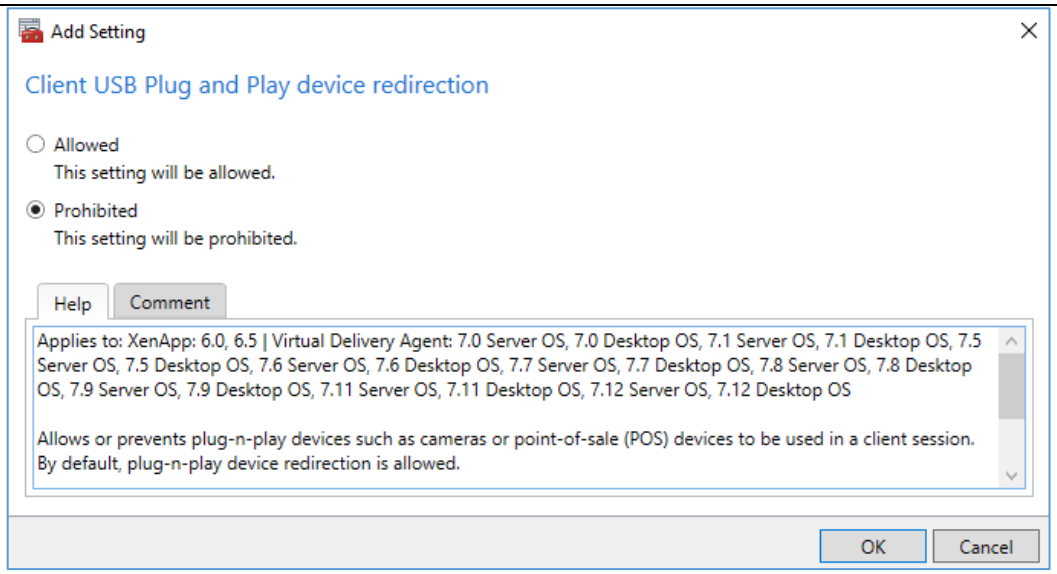
This type of policy configuration is called a baseline policy because you are creating a standard set of common parameters to apply to a complete set of objects, such as in this case, all users.

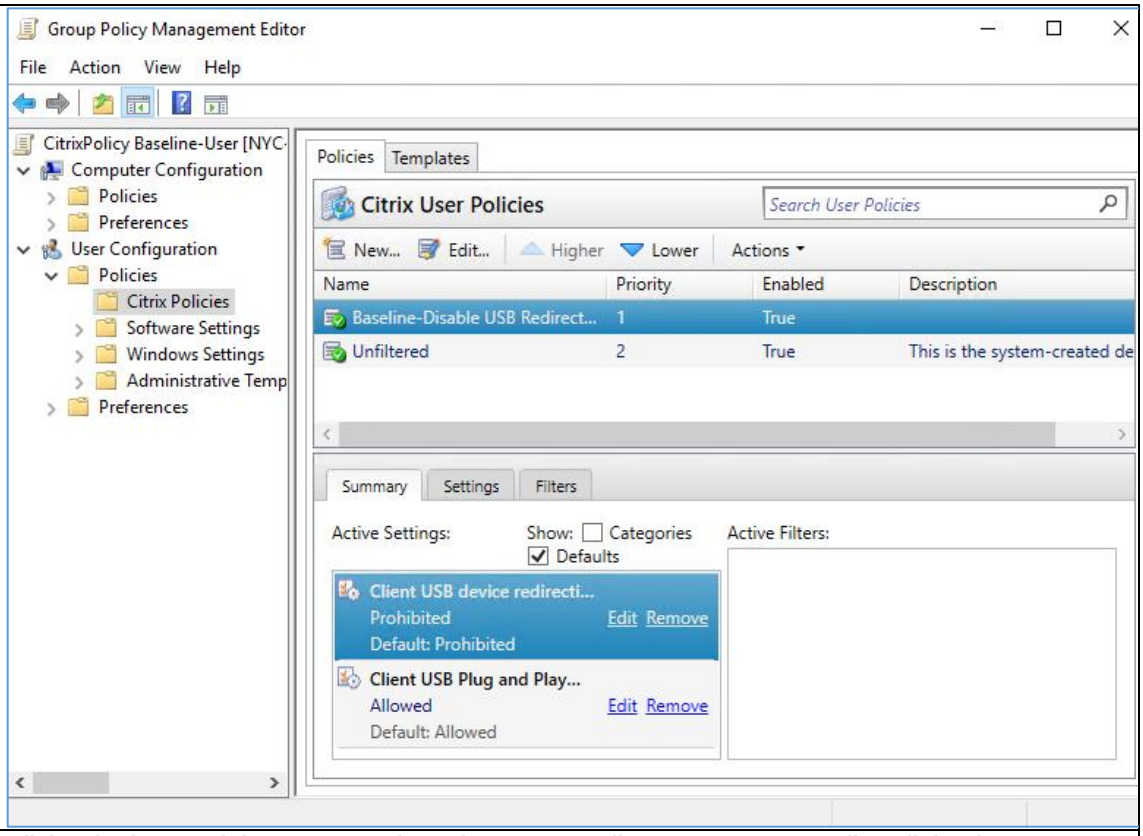
In many environments, these user settings baseline policies are set to configure security, accessibility, or performance settings to common values that are dependent on the specific company directives.

Step	Action
1.	Using the Remote Desktop Connection Manager, confirm that you are still connected to **NYC-XDC-001**. **Note**: In a previous exercise, you had logged on to NYC-XDC-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1

	Note: If your Remote Desktop Connection session disconnected, log on to NYC-XDC-001 by right-clicking this machine and selecting Connect server.
2.	Using the Group Policy Management Console (GPMC), create a new Group Policy Object (GPO). Expand the OU structure **Forest: workspacelab.com** > **Domains** > **workspacelab.com** > **Citrix** > **New York** > **VDA** to view the **VDA** OU. Right-click the **VDA** OU and select **Create a GPO in this domain, and Link it here**. **Note**: The Group Policy Management Console (GPMC) was started in a previous exercise. If the console was closed in a previous exercise, then click Server Manager from the Windows Taskbar, select Tools, and click Group Policy Management to start the Group Policy Management Console (GPMC).
3.	In the New GPO dialog box, enter **CitrixPolicy Baseline-User** for the Name. Click **OK**. 
4.	Right-click the **CitrixPolicy Baseline-User** GPO just created and select **Edit**. 
5.	In the Group Policy Management Editor dialog box, in the left, expand **User Configuration** > **Policies** > **Citrix Policies**. **Note**: There is a Citrix Policies element under the Policies container for both Computer Configuration and User Configuration. In the center pane, click **New**.

	
6.	On the Identity page, enter **Baseline-Disable USB Redirection** in the Name field. Click **Next** to continue the policy creation wizard.
7.	On the Settings page, locate the search field on the top right and type **USB**. **Note**: This is so that only policy settings regarding USB functionality will be displayed.
8.	Under Settings, next to the Client USB device redirection setting, click **Add**. In the Add Setting dialog box, verify that the **Prohibited** radio button is selected.  Click **OK**. **Note**: This policy rule affects the ability to map USB devices from workstations into the sessions. Client drive mapping should also be considered when creating a secure environment; however, Client drive mapping needs to be enabled for a later exercise.
9.	Under Settings, next to the Client USB Plug and Play device redirection setting, click **Add**. In the Add Setting dialog box, change the radio button to **Prohibited**.

	 Click **OK** and click **Next**. **Note**: This setting allows or prevents plug-n-play devices, such as cameras or point-of-sale (POS) devices, to be used in a client session. By default, plug-n-play device redirection is allowed.
10.	On the Filters page, click **Next**.
11.	On the Summary page, verify that the checkbox next to **Enable this policy** is selected. Click **Create**.
12.	In the middle pane under Policies, select **Baseline-Disable USB Redirection**, and in the menu above, click **Higher** until this policy appears first in the list.

	
13.	Click **X** in the top right corner to close the Group Policy Management Editor dialog box.

Key Takeaways:

- In this example, there is only one setting added to the Citrix Baseline-user policy; however, in a production environment more policies would typically be added.
- The naming and structuring of policies typically varies per installation.

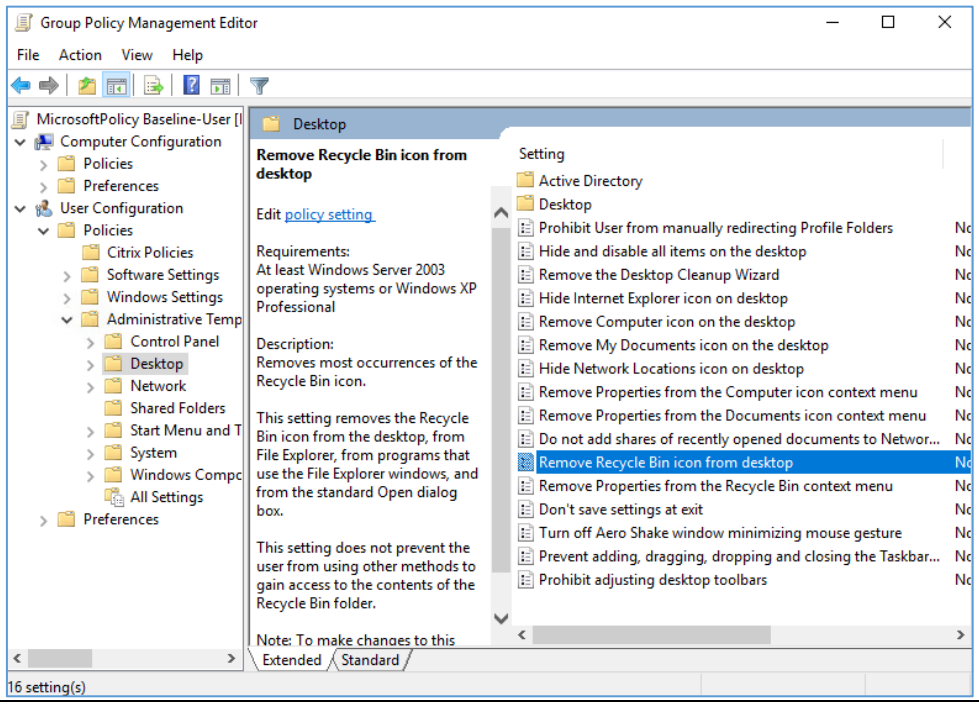
Exercise 6-3: Configure Group Policy loopback processing

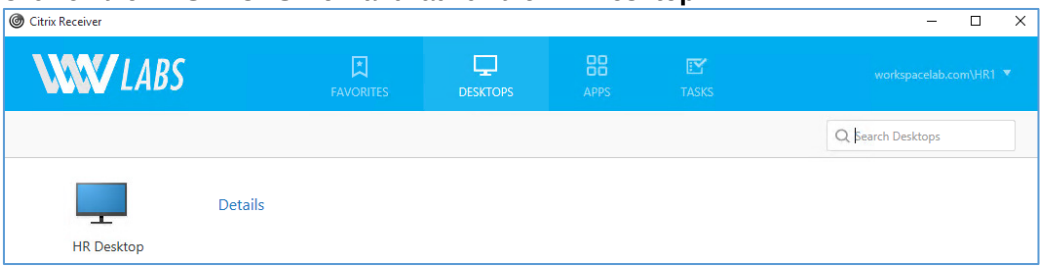
Scenario:

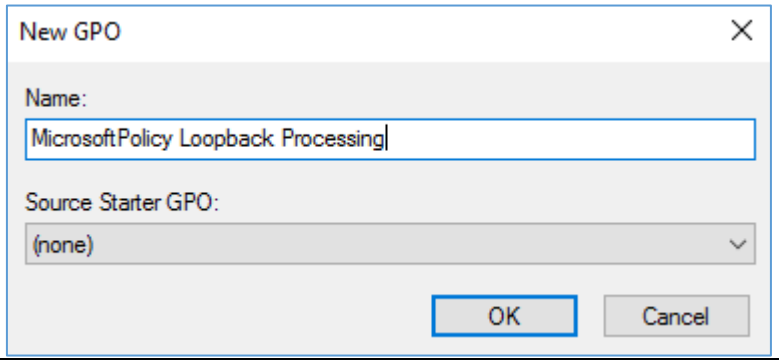
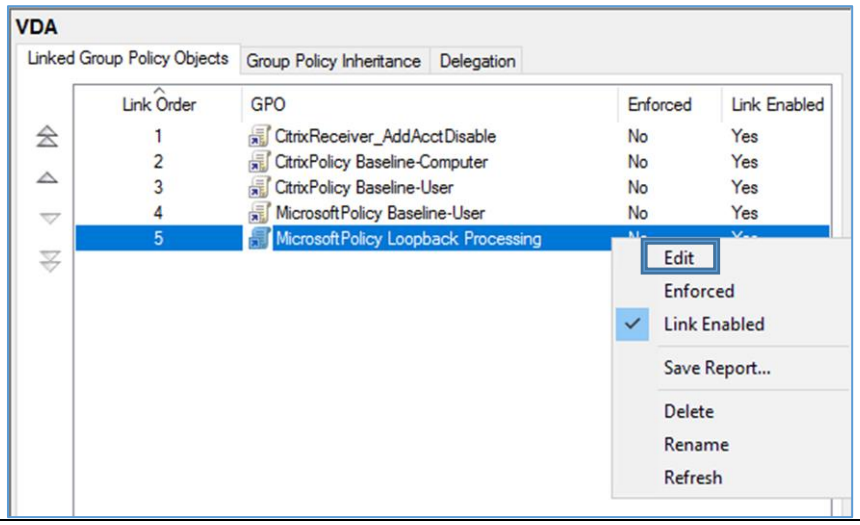
The Microsoft group policy engine has a special processing mode called loopback. Group Policy applies to the user or computer in a manner that depends on where both the user and the computer objects are located in Active Directory. However, in some cases, users may need a policy applied to them based on the location of the computer object alone. You can use the Group Policy loopback feature to apply Group Policy Objects (GPOs) that depend only on which computer the user logs on to.

Your task is to configure Group Policy loopback.

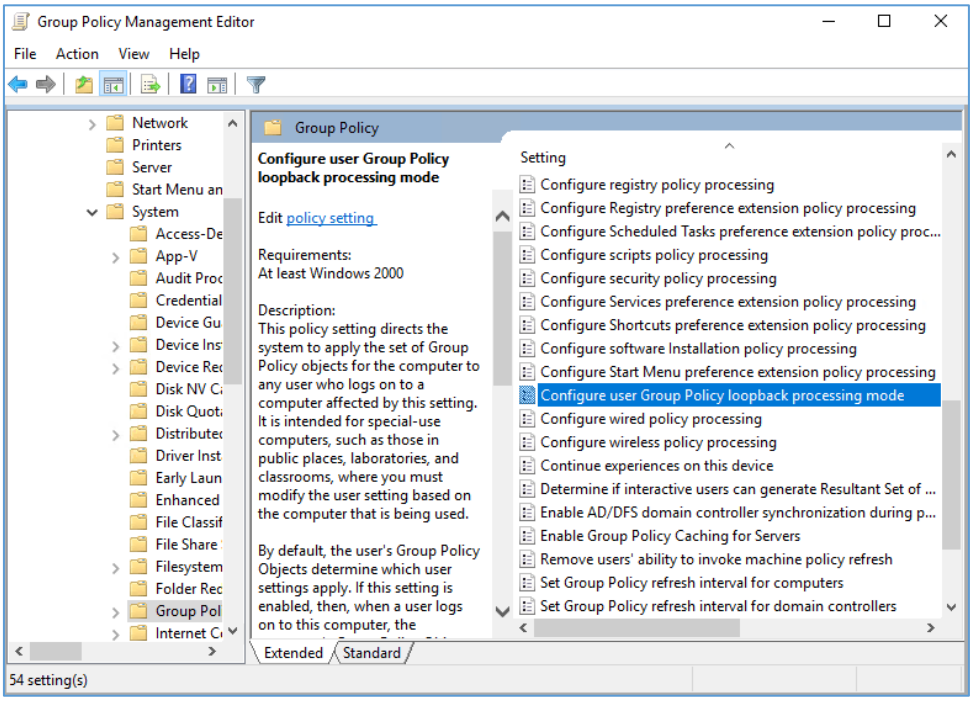
Step	Action
1.	Using the Remote Desktop Connection Manager, confirm that you are still connected to **NYC-XDC-001**. **Note***:* In a previous exercise, you had logged on to NYC-XDC-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1

	Note: If your Remote Desktop Connection session disconnected, log on to NYC-XDC-001 by right-clicking this machine and selecting Connect server.
2.	Using the Group Policy Management Console (GPMC), create a new Group Policy Object (GPO). Expand the OU structure **Forest: workspacelab.com** > **Domains** > **workspacelab.com** > **Citrix** > **New York** > **VDA** to view the **VDA** OU. Right-click the **VDA** OU and select **Create a GPO in this domain, and Link it here**. **Note**: The Group Policy Management Console (GPMC) was started in a previous exercise. If the console was closed in a previous exercise, then start the Server Manager from the Windows Taskbar, select Tools, and click Group Policy Management to start the Group Policy Management Console (GPMC).
3.	In the New GPO dialog box, enter **MicrosoftPolicy Baseline-User** for the Name. Click **OK**.
4.	Right-click the **MicrosoftPolicy Baseline-User** GPO just created and select **Edit**.
5.	In the Group Policy Management Editor dialog box, in the left, navigate to **User Configuration** > **Policies** > **Administrative Templates** > **Desktop**. 
6.	In the right side of the console, double-click the setting **Remove Recycle Bin icon from desktop** and select the **Enabled** radio button. Click **OK** and close the **Group Policy Management Editor** dialog box. **Note:** You are removing the Recycle Bin only to easily prove that the policy configuration works. In production environments, a baseline policy will set a number of desktop lockdown settings for users; however, we do not want to limit too much in the lab moving forward.
7.	Using the Remote Desktop Connection Manager, connect to NYC-SRV-001. To log on to NYC-SRV-001, right-click this machine and select **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1

	Right-click **Start** and select **Command Prompt** to start a command prompt. Type the following command and press enter: **gpupdate /force** Close the **Command Prompt** after the command has completed successfully. **Note**: Alternatively, you could reboot the NYC-SRV-001 machine and have the same group policy update result as running gpupdate /force from the command prompt.
8.	Using the Remote Desktop Connection Manager, connect to NYC-WRK-001. To log on to NYC-WRK-001, right-click this machine and select **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\HR1 • Password: Password1
9.	Wait for the **Citrix Receiver** system tray icon to show up on the lower-right corner, right-click the **Receiver** icon, and click **Log On**. Log on to Citrix Receiver with the following credentials: • User name: **HR1** • Password: **Password1** Open Citrix Receiver from the system tray. Right-click **Citrix Receiver** and select **Open**. Click on the **DESKTOPS** view and launch the **HR Desktop**.  **Note**: The HR Desktop is running on NYC-SRV-001, where the GPO was just applied.
10.	In the HR Desktop connection, verify that the **Recycle Bin** is still present on the Desktop. **Note**: The Recycle Bin is still available and the user is able to access it because the GPO setting is a User Configuration and the GPO is applied to a machine account.
11.	Log off the HR Desktop. To log off, right-click **Start** > choose **Shut down or sign out** > and click **Sign out**. **Note**: Make sure to log off and not to disconnect the session.
12.	Log off Citrix Receiver. Click **HR1** and select **Log Off**. Log off NYC-WRK-001. To log off, right-click **Start** > choose **Shut down or sign out** > and click **Sign out**.

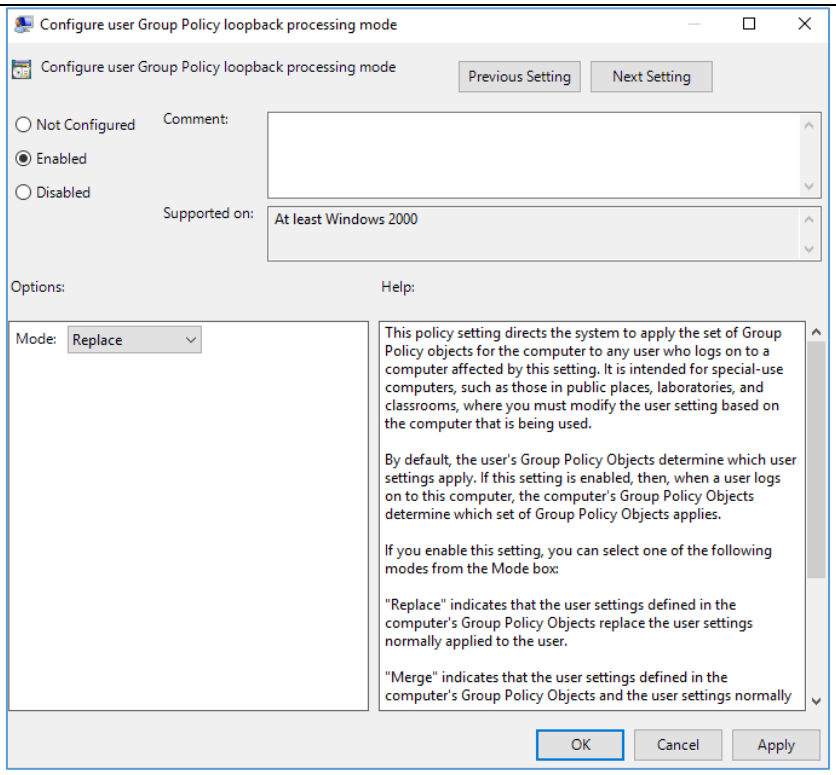
13.	Using the Remote Desktop Connection Manager, switch back to **NYC-XDC-001**. **Note:** You had logged on to NYC-XDC-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-XDC-001 by right-clicking this machine and selecting Connect server.
14.	Using the Group Policy Management Console (GPMC), create a new Group Policy Object (GPO). Expand the OU structure **Forest: workspacelab.com** > **Domains** > **workspacelab.com** > **Citrix** > **New York** > **VDA** to view the **VDA** OU. Right-click the **VDA** OU and select **Create a GPO in this domain, and Link it here**. **Note**: The Group Policy Management Console (GPMC) was started in a previous exercise. If the console was closed in a previous exercise, then start Server Manager from the Windows Taskbar, select Tools, and click Group Policy Management to start the Group Policy Management Console (GPMC).
15.	In the New GPO dialog box, enter **MicrosoftPolicy Loopback Processing** for the Name. Click **OK**. 
16.	Right-click the **MicrosoftPolicy Loopback Processing** GPO just created and select **Edit**. 

17. In the Group Policy Management Editor dialog box, navigate to **Computer Configuration** > **Policies** > **Administrative Templates** > **System** > **Group Policy**.



In the right side of the console, double-click the setting **Configure user Group Policy loopback processing mode** and configure the following:

- **Enabled**
- Mode: **Replace**



Click **OK** and close the **Group Policy Management Editor** dialog box.

Note: The computer object reads the loopback processing setting, and the setting is applied to the computer's registry, so you only need to configure loopback processing once in a specific OU, not for each individual policy.

18. Using the Remote Desktop Connection Manager, switch back to **NYC-SRV-001**.

Note: In a previous exercise, you had logged on to NYC-SRV-001 using the following credentials to make the connection:

- User name: Workspacelab\Administrator
- Password: Password1

Note: If your Remote Desktop Connection session disconnected, log on to NYC-SRV-001 by right-clicking this machine and selecting **Connect server**.

19. Click **Start**, type **Command Prompt**, and select **Command Prompt** to start a command prompt. Type the following command and press **Enter**:

gpupdate /force

Close the **Command Prompt** after the command has completed successfully.

20. Using the Remote Desktop Connection Manager, connect to NYC-WRK-001.

To log on to NYC-WRK-001, right-click this machine and choose **Connect server**.

Note: The following credentials are used to make the connection:

- User name: Workspacelab\HR1
- Password: Password1

21.	Wait for the **Citrix Receiver** system tray icon to show up on the lower-right corner, right-click the **Receiver** icon, and click **Log On**. Log on to Citrix Receiver with the following credentials: • User name: **HR1** • Password: **Password1** Open Citrix Receiver from the system tray. Right-click **Citrix Receiver** and select **Open**. Click on the **DESKTOPS** view and launch the **HR Desktop**.
22.	In the HR Desktop connection, verify that the **Recycle Bin** icon was removed from the Desktop. **Note**: The Recycle Bin was hidden using the MicrosoftPolicy Baseline-User; however, since this was a user setting configured on a computer OU, the functionality of Loopback Processing was needed to also read user policy settings defined on computer OUs.
23.	Log off the HR Desktop. To log off, right-click **Start** > choose **Shut down or sign out** > and click **Sign out**. Log off Citrix Receiver. Click **HR1** and select **Log Off**. Log off NYC-WRK-001. To log off, right-click **Start** > select **Shut down or sign out** > and click **Sign out**.

Key Takeaways:

- Use Loopback Processing mode to allow the user settings from a GPO to be read despite the GPO being linked to a computer OU.
- Loopback processing gives the option of selecting Merge or Replace. Merge will combine all user settings from GPOs in both the user OU and the user settings on the computer OU. Replace will discard any user settings read from the user OU and only the user settings from the computer OU will be applied.

Exercise 6-4: Create Citrix policies from templates

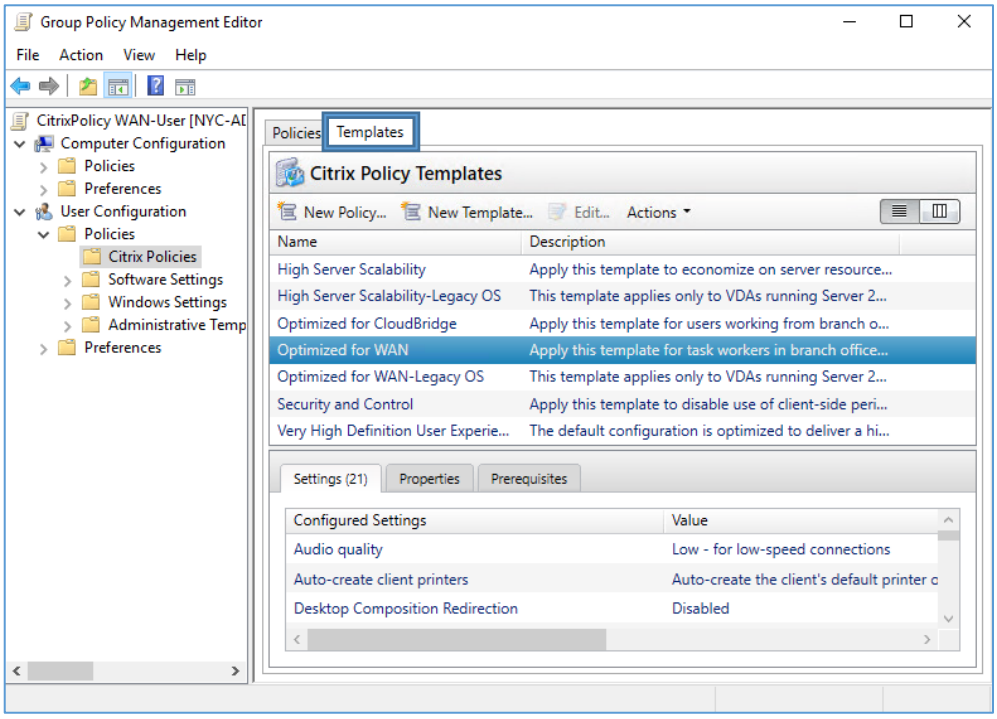
Scenario:

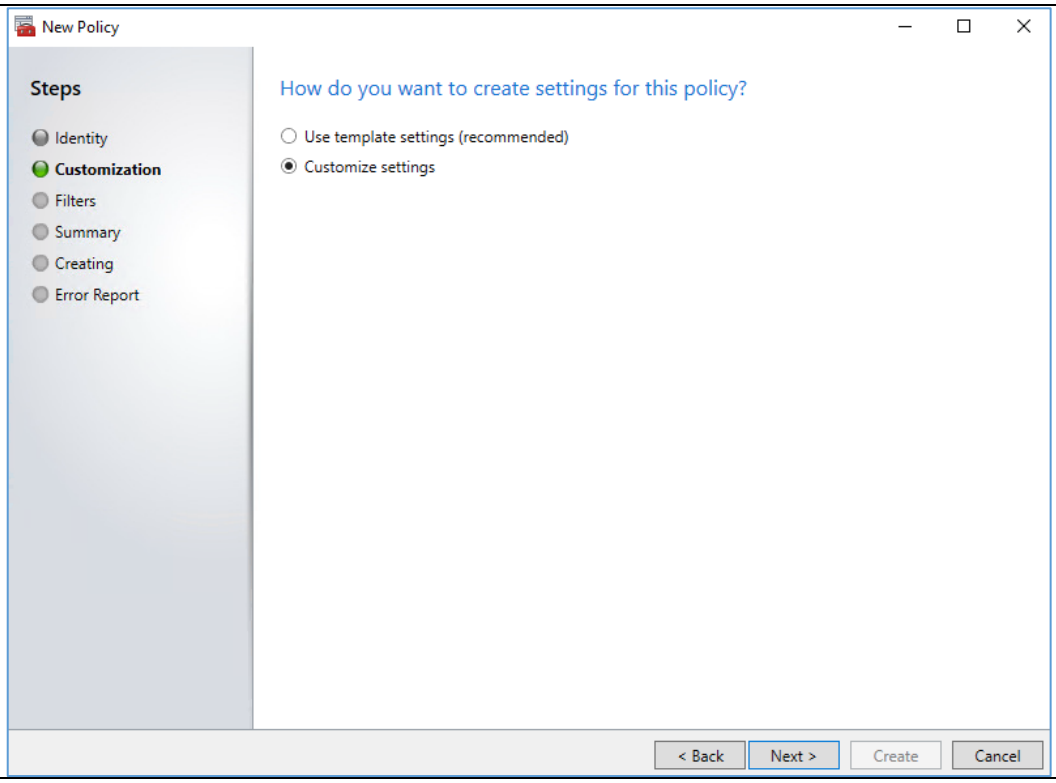
Policy Templates provide a quick method to create policies with many optimized settings for different scenarios.

You have been tasked to create a Citrix GPO from a template.

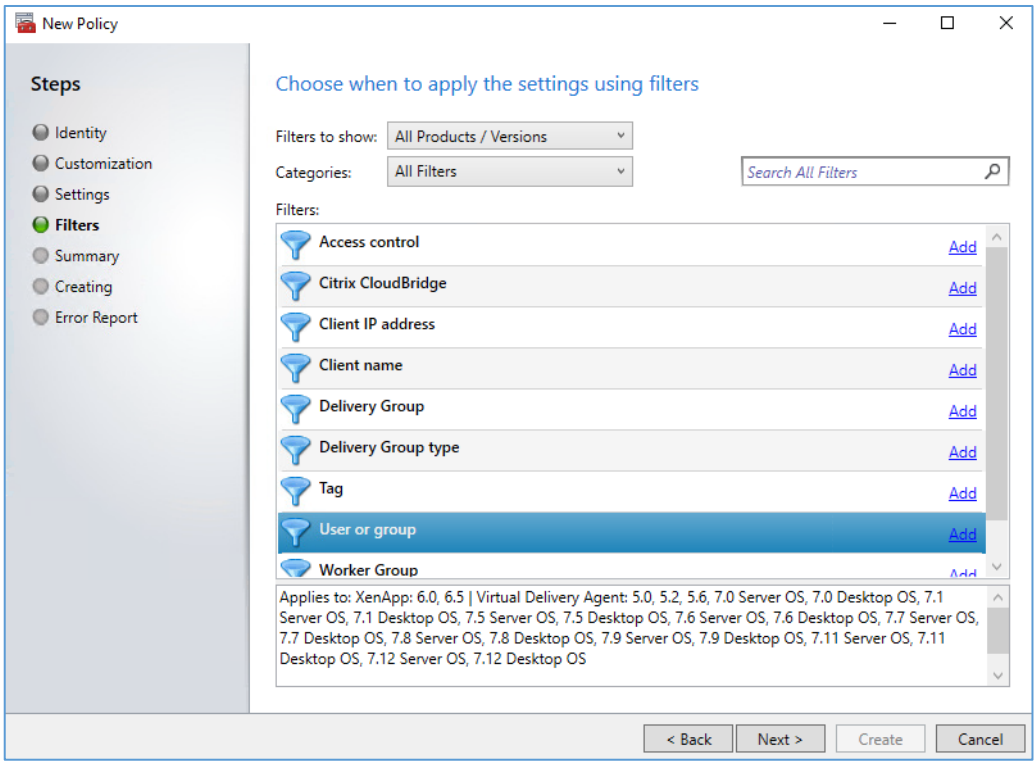
Note: Your task includes setting an exaggeration for a parameter to make the change appear more obvious.

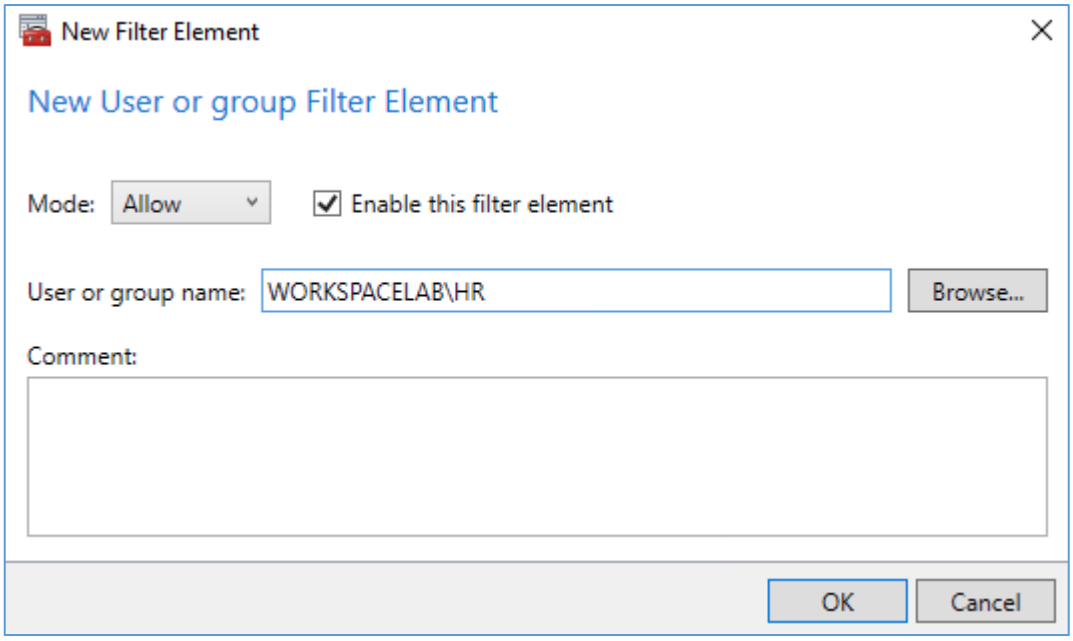
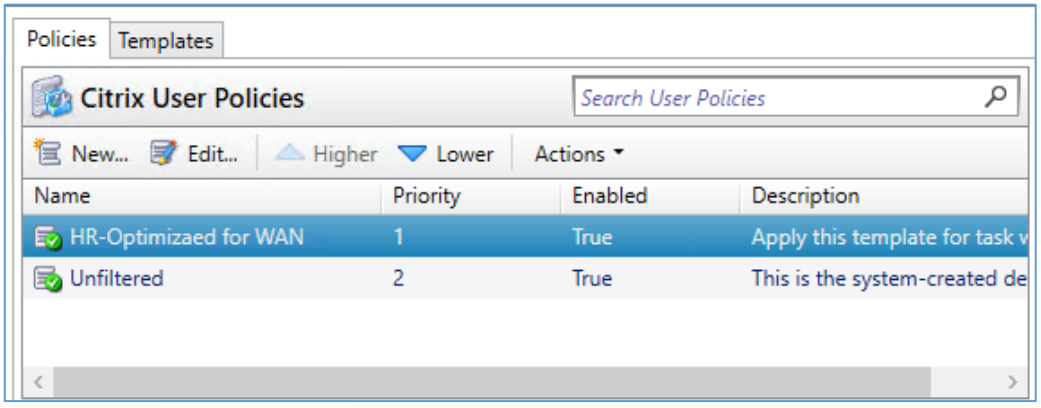
Step	Action
1.	Using the Remote Desktop Connection Manager, verify that you are still connected to NYC-XDC-001. To log on to NYC-XDC-001, right-click this machine and select **Connect server**.

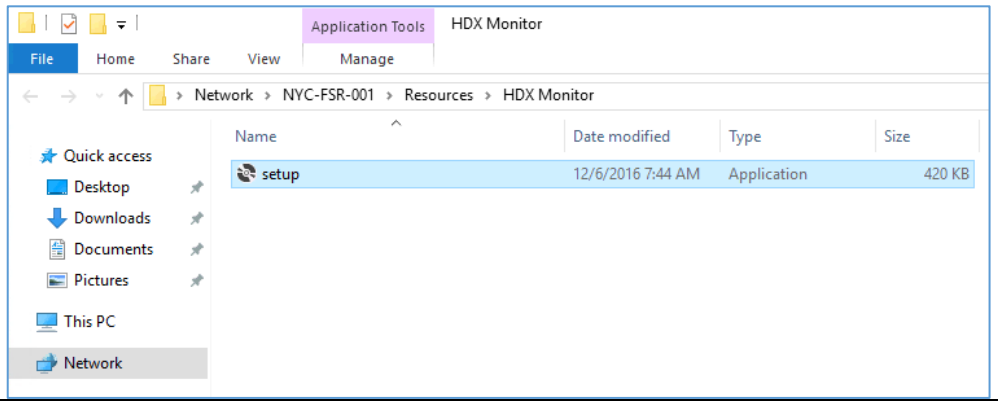
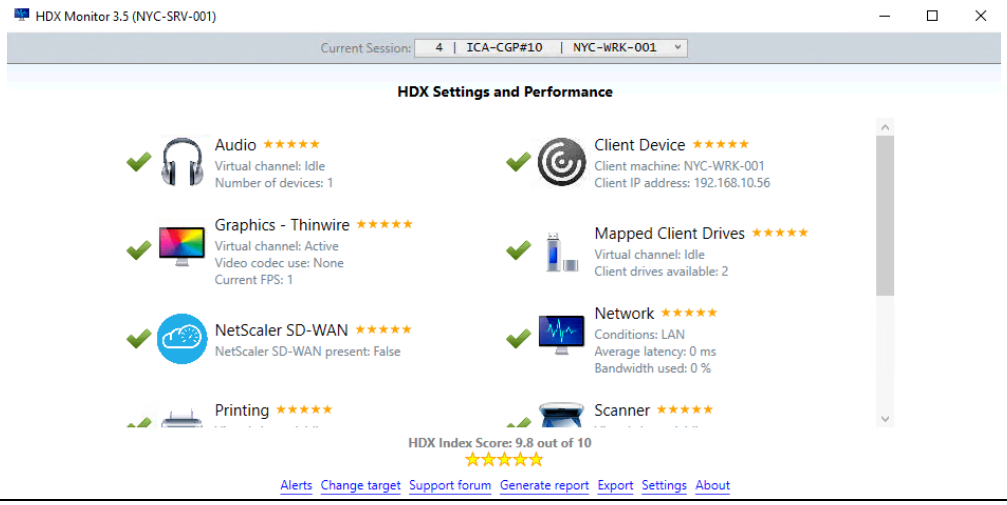
	Note: The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1
2.	You will now configure a policy template that will enable the settings pre-defined by Citrix in the Optimized for WAN policy template. Using the Group Policy Management Console (GPMC), create a new Group Policy Object (GPO). Expand the OU structure **Forest: workspacelab.com** > **Domains** > **workspacelab.com** > **Citrix** > **New York** to view the **VDA** OU. **Note**: The Group Policy Management Console (GPMC) was started in a previous exercise. If the console was closed in a previous exercise, then start Server Manager from the Windows Taskbar, select Tools, and click Group Policy Management to start the Group Policy Management Console (GPMC). Right-click the **VDA** OU and select **Create a GPO in this domain, and Link it here**. In the New GPO dialog box, enter **CitrixPolicy WAN-User** for the Name. Click **OK**.
3.	Right-click the **CitrixPolicy WAN-User** policy and select **Edit**.
4.	Navigate to **User Configuration** > **Policies** > **Citrix Policies**.  Select the **Templates** tab and then select **Optimized for WAN**. Click **New Policy**. Enter **HR-Optimized for WAN** for the name and click **Next**.
5.	On the Customization page, select **Customize settings** and click **Next**.



6. On the Settings page, enter **target** in the search bar, and click **Edit** next to Target Frame rate.
7. On the Target frame rate setting dialog box, enter **8** as the value and click **OK**.
8. Click **Next**.
9. Select the **User or group** filter and click **Add**.



	Click the **Add** button, enter the following values, and then click **OK**: • Mode: **Allow** • Enable this filter element: **Enabled** • User or group name: **WORKSPACELAB\HR**  **Note:** In this exercise, you are applying the policy to a user group for testing purposes. In production, you could apply the policy to an IP range. Click **OK** on the New Filter window.
10.	Click **Next** and then click **Create**.
11.	Select the **Policies** tab and move the **HR-Optimized for WAN** policy above the Unfiltered policy by clicking the **Higher** button.  Close the **Group Policy Management Editor**.
12.	Using the Remote Desktop Connection Manager, switch to **NYC-SRV-001**.
13.	From NYC-SRV-001, click **Start** and type **Command Prompt**. Select **Command Prompt** to start a command prompt. Type the following command and press **Enter**: **gpupdate /force** Close the **Command Prompt** after the command has completed successfully.

14.	Using the Remote Desktop Connection Manager, connect to NYC-WRK-001. To log on to NYC-WRK-001, right-click this machine and select **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\HR1 • Password: Password1
15.	Double-click the **Citrix Receiver** application from the system tray. Log on using the following credentials: • User name: **HR1** • Password: **Password1** Launch the **HR Desktop** and open **Internet Explorer** from the Taskbar. Notice that by default the **http://training.citrix.com** site displays. **Note:** The rotating banner on the http://training.citrix.com is graphic intensive on the user session. Notice that the graphics now appear grainier, and the animation appears less smooth as the frame rate and the visual quality has been adjusted by using the Optimized for WAN settings.
16.	From within the HR Desktop session, browse to the **\\NYC-FSR-001\Resources\HDX Monitor** directory and double-click the **setup.exe** application to start Citrix HDX Monitor. 
17.	On the Application Install – Security Warning dialog box, click **Install**.
18.	Verify that the **System** radio button is selected and click **Open**. 

	Select **Graphics - Thinwire Advanced** and view the value for **Frames Per Second**. **Note:** Notice the FPS values spike since the IE page open has graphics displayed.
19.	Keep the Internet Explorer maximized in the background and try to move the **HDX Monitor Window** around the screen quickly while looking at the **Frames Per Second** value; it should never go above **8**. **Note:** This means that the WAN Policy is working. **Note:** In a production environment, you should avoid setting the Frames Per Second value lower than 16. Setting Frames Per Second too low will cause user experience degradation.
20.	Log off the HR Desktop. To log off, right-click **Start**, choose **Shut down or sign out**, and click **Sign out**. Click **HR1** and log off of Receiver.
21.	You will now delete the HR - Optimized for WAN policy. This policy currently implements printer settings that will conflict with future exercises in Module 8. Using the Remote Desktop Connection Manager, connect to NYC-XDC-001. To log on to NYC-XDC-001, right-click this machine and select **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1 Expand the OU structure **Forest: workspacelab.com** > **Domains** > **workspacelab.com** > **Group Policy Objects** to view all the configured Group Policy Objects. Right-click **CitrixPolicy WAN-User** in the center pane and select **Delete**. **Note:** This policy must be deleted in order for future lab exercises to work. Select **Yes** on the warning message. After the GPO has been successfully deleted, click **OK** on the Delete dialog box. **Note**: The Group Policy Management Console (GPMC) was started in a previous exercise. If the console was closed in a previous exercise, then start Server Manager from the Windows Taskbar, select Tools, and click Group Policy Management to start the Group Policy Management Console (GPMC).
22.	Using the Remote Desktop Connection Manager, switch to **NYC-SRV-001**.
23.	From NYC-SRV-001, click **Start**, type **Command Prompt**, and select **Command Prompt** to start a command prompt. Type the following command and press **Enter**: **gpupdate /force** Close the **Command Prompt** after the command has completed successfully.

Key Takeaways:

- Leverage the HDX policy templates as the starting point for configuring policies for a graphic delivery method that is not the default.
- Use the HDX Monitor or PowerShell to verify session information such as the graphic delivery mode.

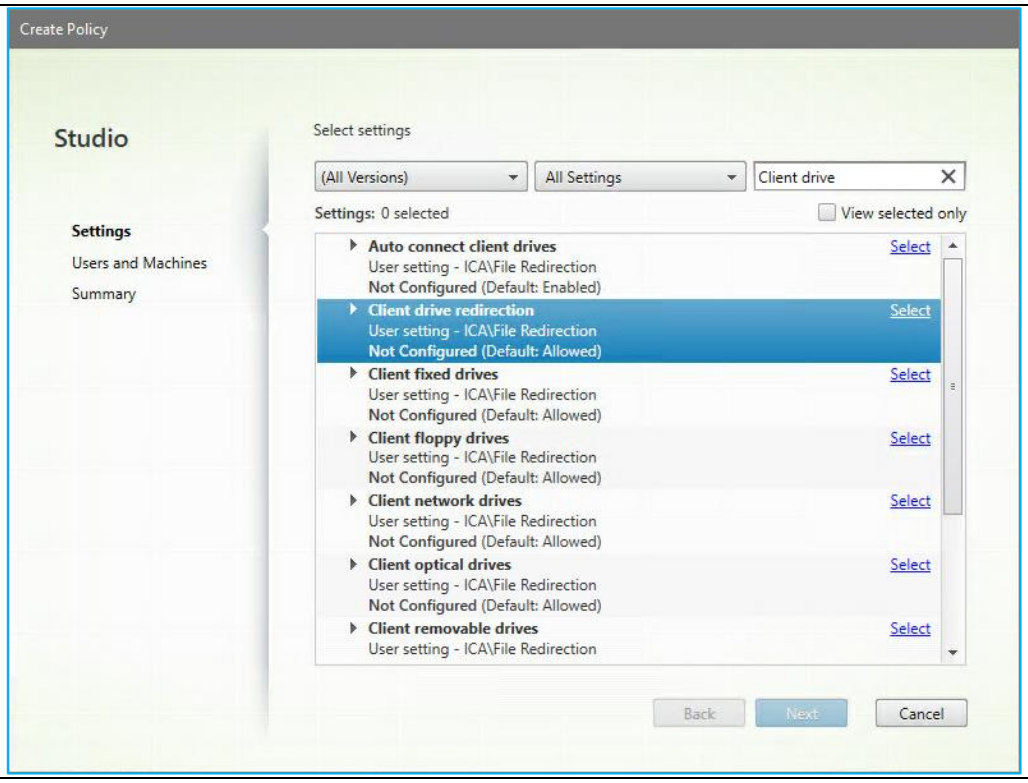
Exercise 6-5: Configuring client drive mapping using Studio

Scenario:

The WW Labs CTO met with the Lead Citrix Architect to express concerns over security around access to user intellectual property. Specifically, the CTO wants to ensure that no user connection from outside of the WW Labs office can map their client drives into the session and thereby potentially steal data.

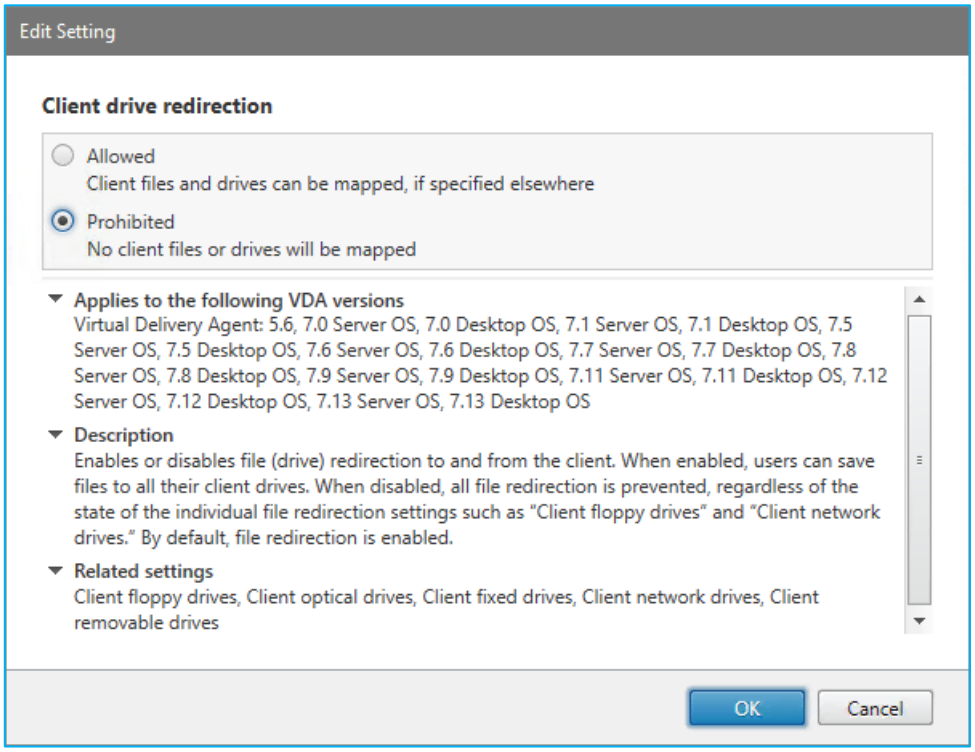
Your task is to create a Citrix policy using Studio to configure client drive mapping in a manner that prohibits only external users the ability to map client drives. You have decided to use IP addresses to determine the user location.

Step	Action
1.	Using the Remote Desktop Connection Manager, verify that you are still connected to NYC-XDC-001. To log on to NYC-XDC-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1
2.	Use Citrix Studio to create a new policy for client drive mapping. In the Studio console, in the left pane, click **Policies**. In the right pane, select **Create Policy**. **Note**: If the Citrix Policies Welcome screen is displayed, then click **Don't show this again** and then Close. **Note**: Citrix recommends that you standardize on one management console method, GPMC or Studio, to minimize conflicts and confusion. You have created all of your policies in Group Policy so far; however, you want to ensure that you fully understand both consoles during the POC so you can choose the best console for production roll out. **Note**: Studio was started in a previous exercise. If Studio was closed in a previous exercise, then click Start > Citrix > Citrix Studio.
3.	In the Create Policy wizard, type **Client drive** in the search bar on the top right.

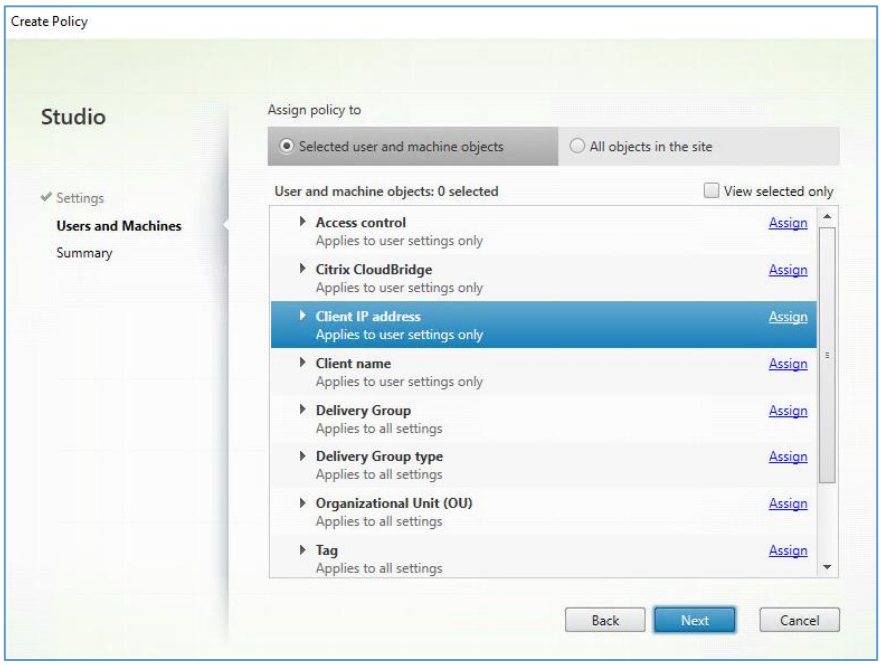


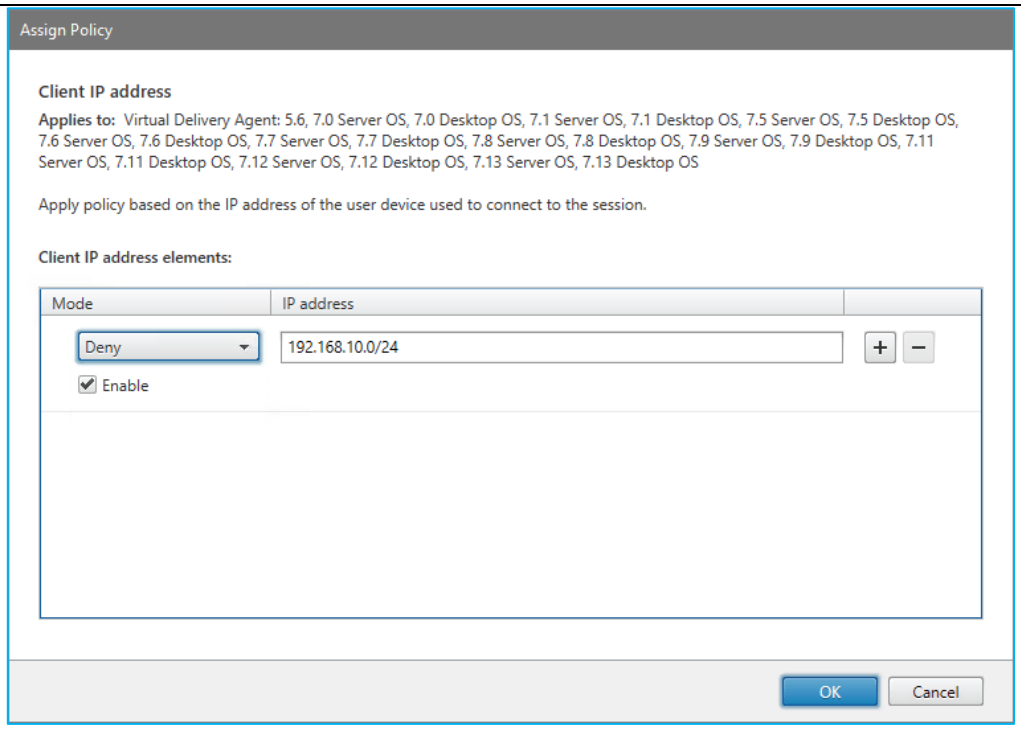
4. Under Settings, click **Select** next to the Client drive redirection setting.

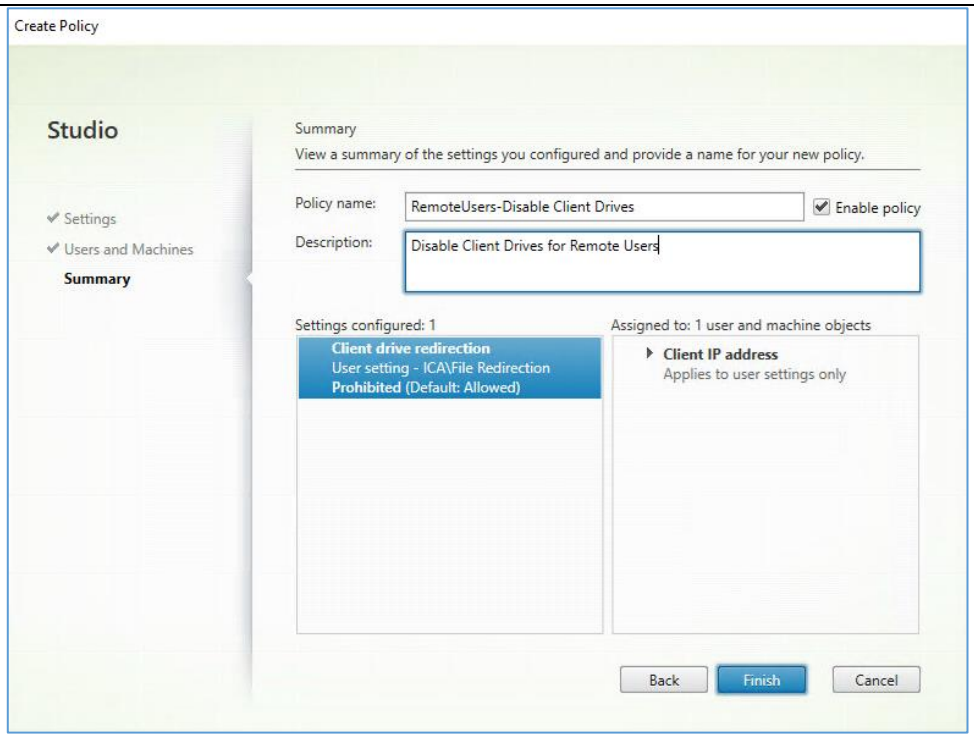
   In the Edit Setting dialog box, change the radio button to **Prohibited**.



   Click **OK**.

5.	On the Settings page, click **Next**.
6.	On the Users and Machines page, verify that **Selected user and machine objects** is selected under the Assign policy to section.  Click **Assign** to the right of the Client IP address under User and machine objects.
7.	In the Assign Policy dialog box, set the following options: • Mode: **Deny** • IP address: **192.168.10.0/24**

	 Click **OK** to close the dialog box. Click **Next** on the Users and Machines page. **Note**: This policy configuration means that every connection will receive the policy, except for those connections initiated from internal IP addresses (192.168.10.1 - 192.168.10.254).
8.	On the Summary page, configure the following: • Policy name: **RemoteUsers-Disable Client Drives** • Description: **Disable Client Drives for Remote Users**

	 Verify that the checkbox next to **Enable policy** is selected. Click **Finish**.
9.	Verify that the **RemoteUsers-Disable Client Drives** policy appears in the list of Policies.
10.	Using the Remote Desktop Connection Manager, connect to **NYC-SRV-001**.
11.	Right-click **Start** and select **Command Prompt**. Type the following command and press **Enter**: **gpupdate /force** Close the **Command Prompt** after the command has completed successfully.

Key Takeaways:

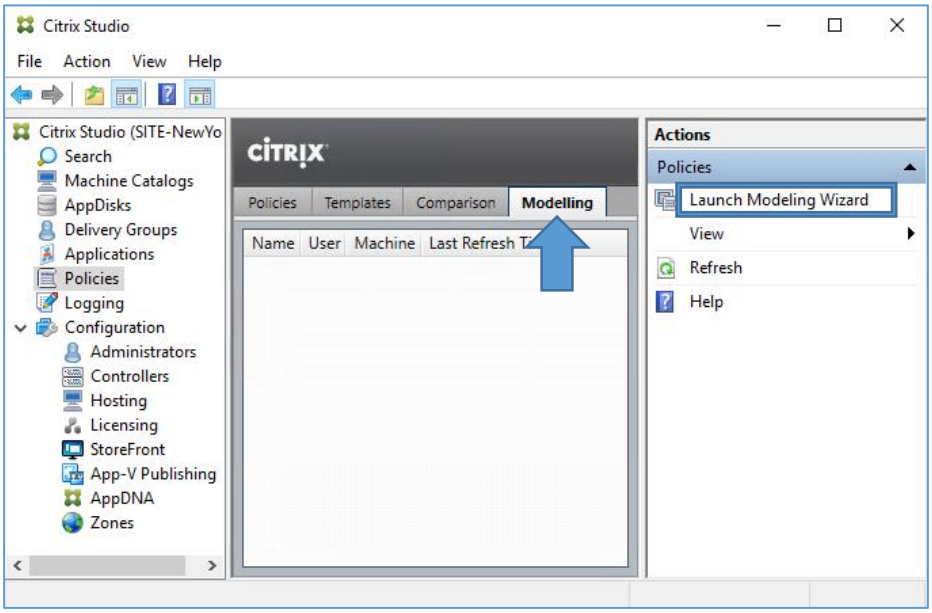
- While Client Drive Mapping is widely used and offers a great user experience, some organizations limit the feature for external locations, or untrusted devices due to security concerns.
- Client Drive Mapping is enabled by default and should be considered in any deployment.

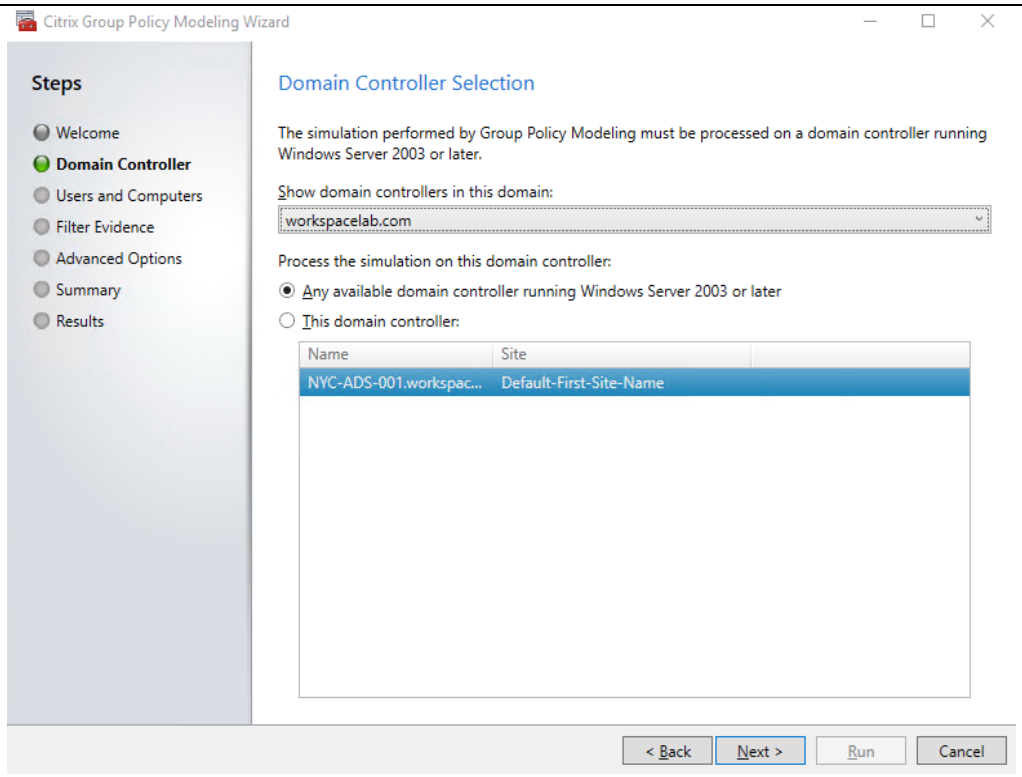
Exercise 6-6: Run the Policy Modeling Wizard from Studio

Scenario:

Earlier in Module 2 you created a Resultant Set of Policies (RSOP) using the Group Policy Management Consoler (GPMC). When running the Resultant Set of Policies within Studio, both settings from GPOs and policy configurations from Studio are analyzed.

Your task is to run the Policy Modeling Wizard from Citrix Studio.

Step	Action
1.	Using the Remote Desktop Connection Manager, switch back to **NYC-XDC-001**. **Note:** In a previous exercise, you had logged on to NYC-XDC-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-XDC-001 by right-clicking this machine and selecting **Connect server**.
2.	Use Citrix Studio to run the Policy Modeling Wizard. In the left pane click **Policies**. In the top of the middle pane, select the **Modelling** tab. In the right pane, click **Launch Modeling Wizard**.  **Note**: Studio was started in a previous exercise. If Studio was closed in a previous exercise, then click Start > Citrix > Citrix Studio.
3.	On the Welcome page, review the introduction for the wizard and click **Next**.
4.	On the Domain Controller page, verify that the following is configured: • Show domain controllers in this domain: **workspacelab.com** • Process the simulation on this domain controller: **Any available domain controller running Windows Server 2003 or later**

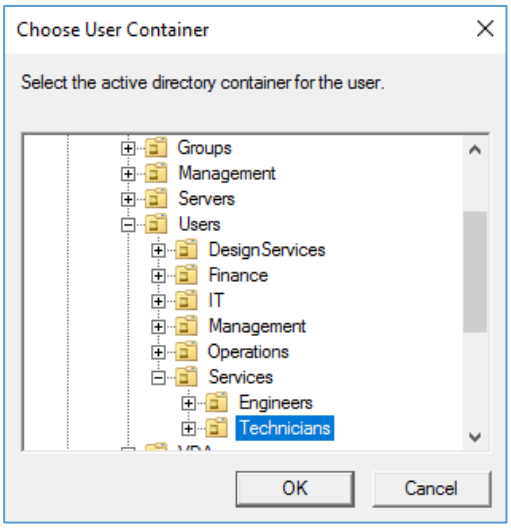


Click **Next** to continue the modeling wizard.

5. On the Users and Computers page, for the User Information field, verify that **Container** is selected.

   Click **Browse** next to the container field.

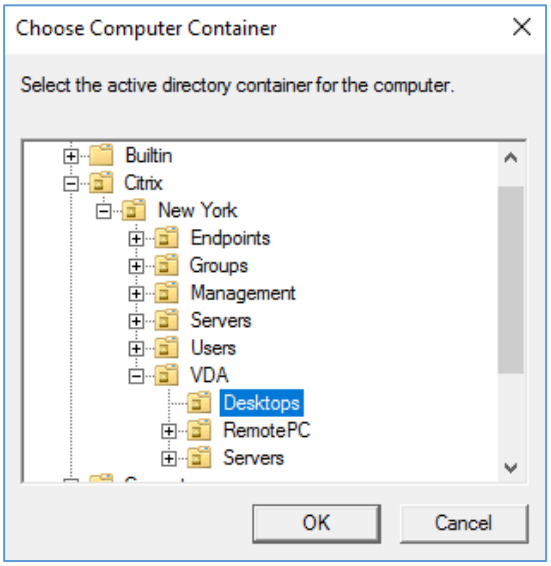
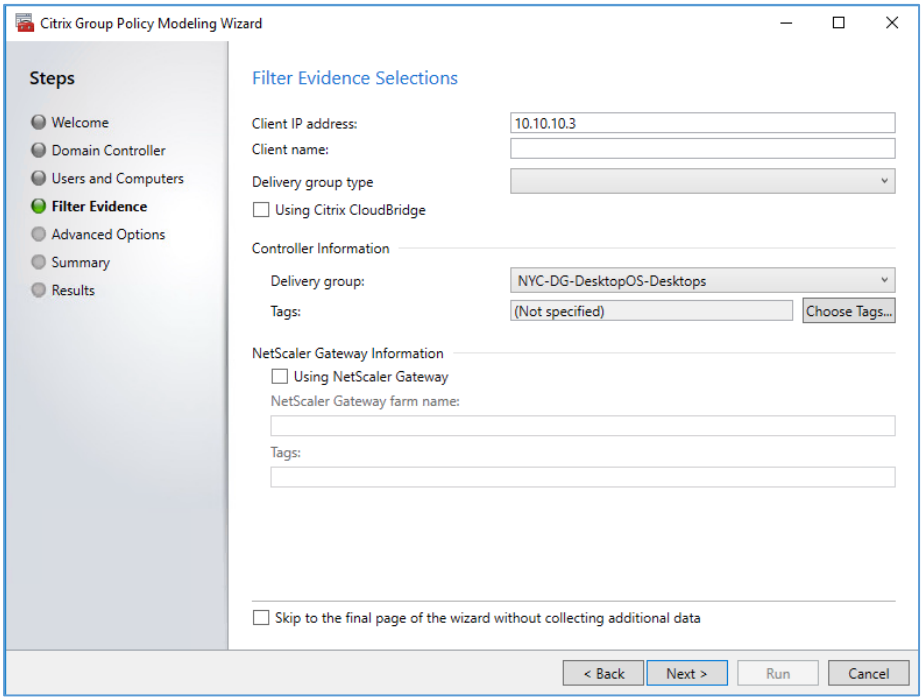
6. In the Choose User Container dialog box, expand the workspacelab tree to navigate to **workspacelab** > **Citrix** > **New York** > **Users** > **Services** >**Technicians**.



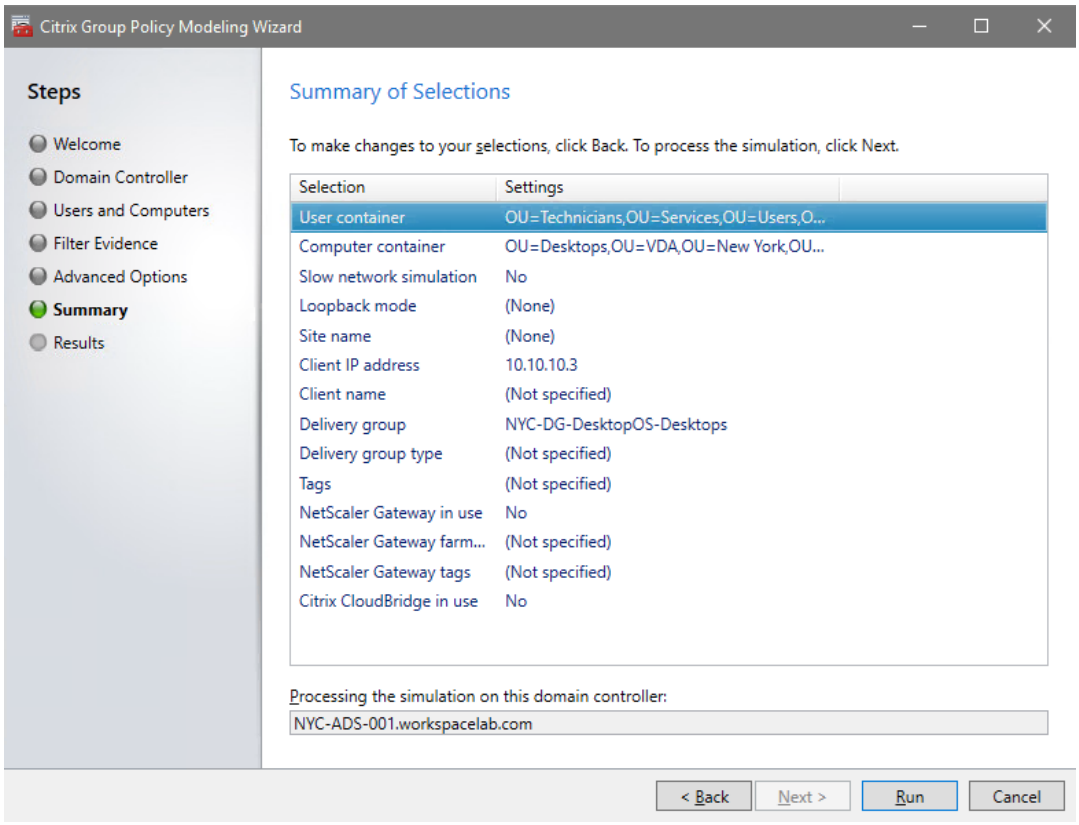
   Select the **Technicians** OU and click **OK**.

7. On the Users and Computers page, for the Computer Information field, verify that **Container** is selected.

   Click **Browse** next to the container field.

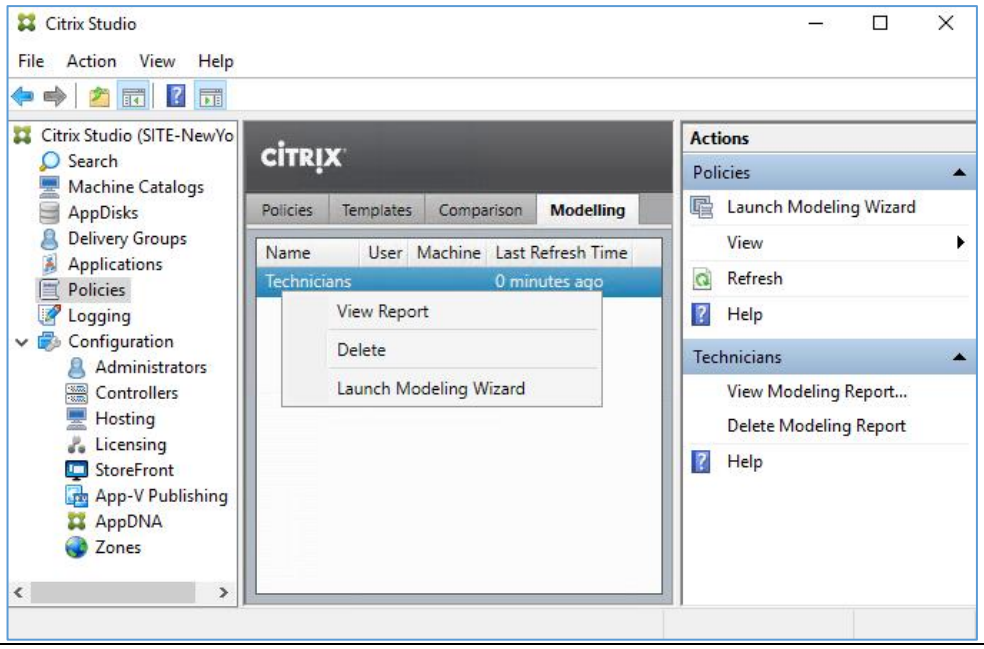
8.	In the Choose Computer Container dialog box, expand the workspacelab tree to navigate to **workspacelab** > **Citrix** > **New York** > **VDA**.  Select the **Desktops** OU and click **OK**.
9.	On the Users and Computers page, click **Next** to continue the modeling wizard.
10.	On the Filter Evidence page, configure the following: • Client IP address: **10.10.10.3** • Delivery group: **NYC-DG-DesktopOS-Desktops**  Click **Next** to continue the modeling wizard.
11.	On the Advanced Simulation Options page, leave the defaults and click **Next**.

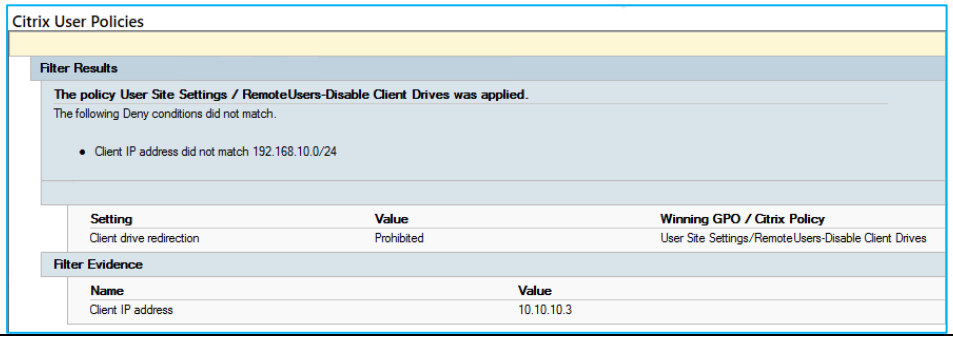
12. On the Summary page, review and confirm the settings, and click **Run** to run the modeling wizard.



After the wizard has completed, click **Close**.

13. Right-click the **Technicians** Policy Modeling report and click **View Report** to view the report.



14.	Scroll down within the report to the **Citrix User Policies** section and review the **Client drive redirection** setting that was configured in a previous exercise. 
15.	**Close** the report when finished reviewing.

Key Takeaways:

- Use the Citrix Group Policy Modeling Wizard within Citrix Studio to display all applicable settings from both GPO and Studio-based policies.
- The report will show each policy setting applied and the associated policy the setting was read from.
- Citrix Group Policy Modeling Wizard is a very helpful tool when troubleshooting policies.
- Citrix Policy Modeling can also be performed through GPMC; however, this tool will only traverse policies created in GPMC (not Studio-based policies).

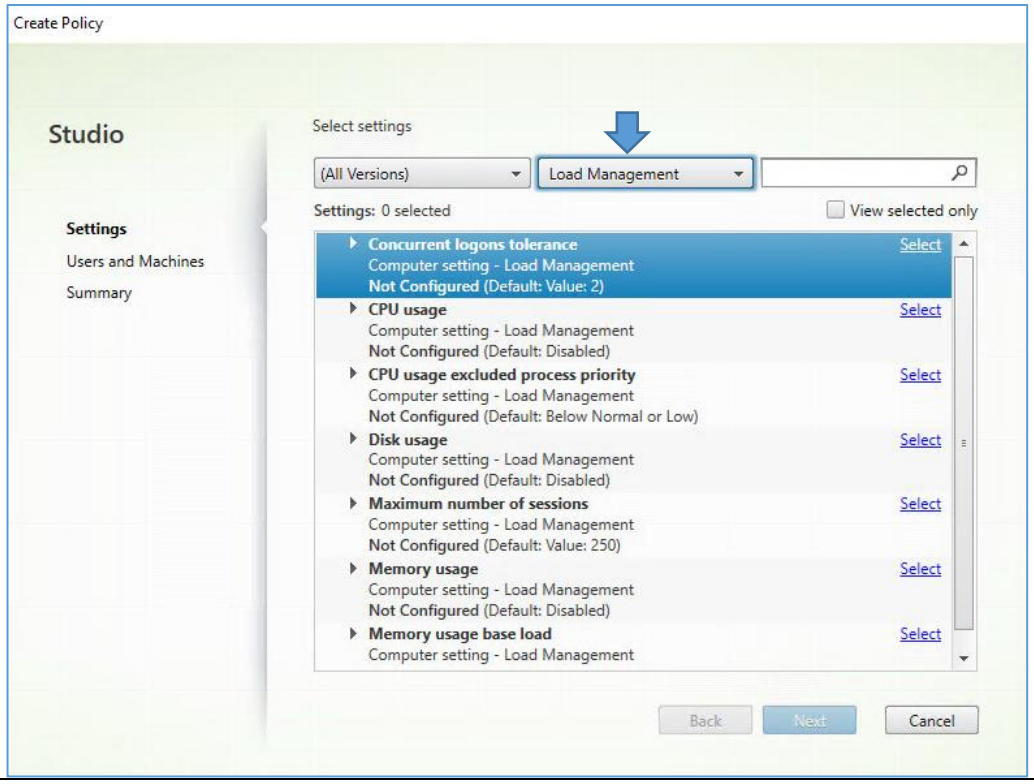
Exercise 6-7: Create a load management policy using Studio

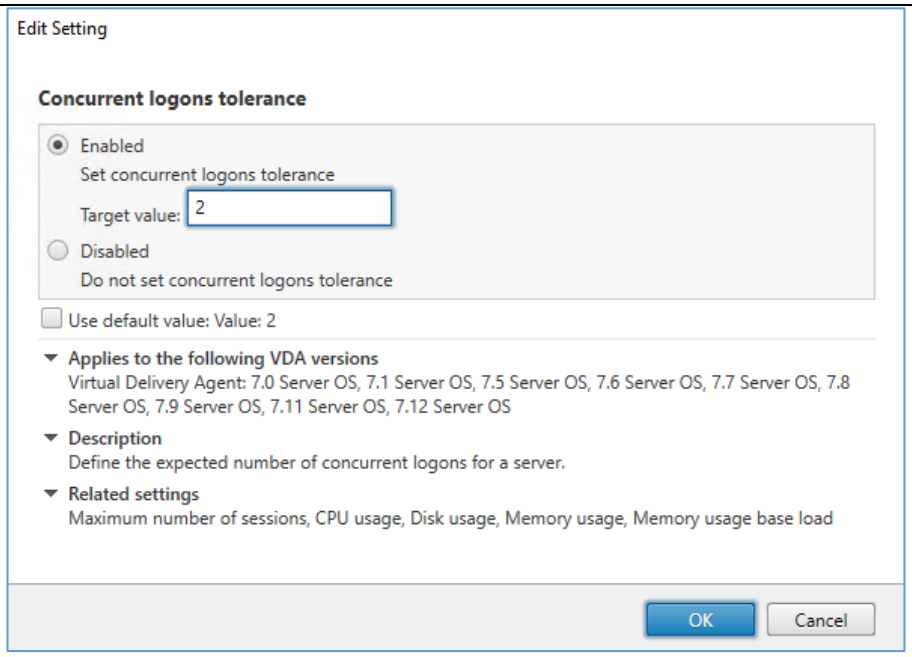
Scenario:

Hosting user sessions on Server OS can be tuned to provide the best performance by configuring load management policies. Load balancing functions out of the box by distributing the number of sessions evenly amongst server VDAs, but can be configured to measure the load using counters such as Memory, CPU and Disk Activity because most users do not consume the same amount of resources.

Your task is to create a load management policy.

Step	Action
1.	Using the Remote Desktop Connection Manager, verify that you are still connected to **NYC-XDC-001**. **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-XDC-001 by right-clicking this machine and selecting Connect server. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1
2.	Use Citrix Studio to create a new policy for Load Management. On the left pane, click **Policies**. In the right pane, select the **Create Policy**. **Note**: Citrix recommends that you standardize on one management console method, GPMC or Studio, to minimize conflicts and confusion. You have created all of your policies in Group

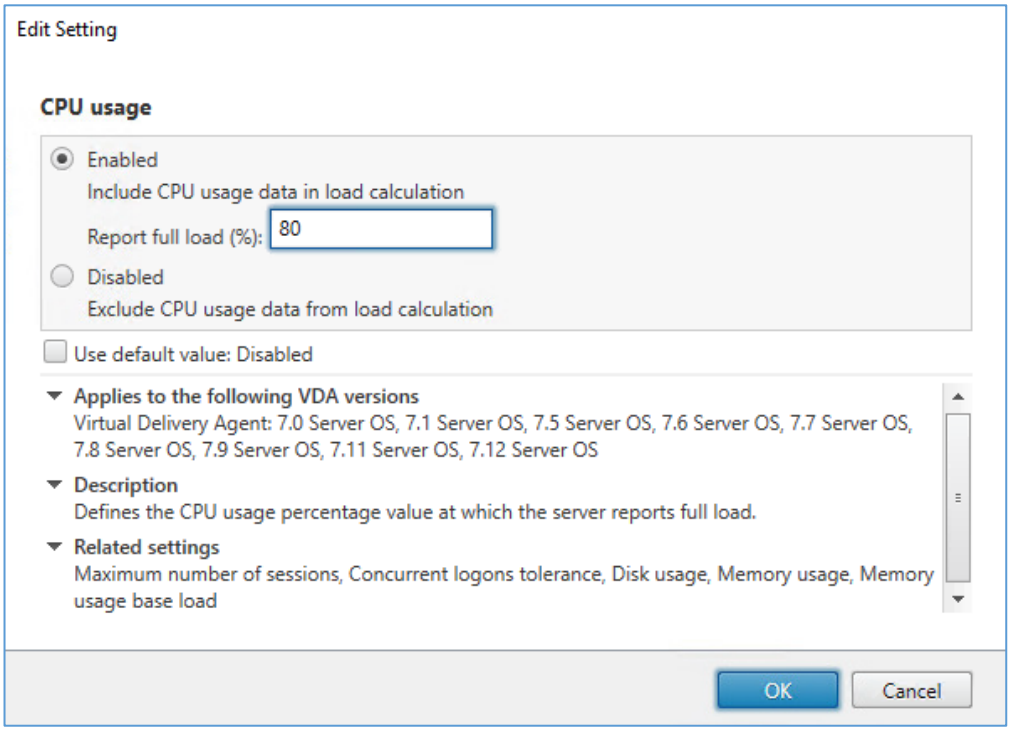
	Policy so far; however, your Lead Citrix Architect has tasked you to also build some policies in Studio. **Note**: Studio was started in a previous exercise. If Studio was closed in a previous exercise, then click **Start** > **Citrix** > **Citrix Studio**.
3.	In the Create Policy wizard, click the drop-down for **All Settings** and select **Load Management**. 
4.	Under the Settings, click **Select** next to the **Concurrent logons tolerance** setting. In the Edit Setting dialog box, leave the default radio button set to **Enabled** and the Target value of **2**.



Click **OK**.

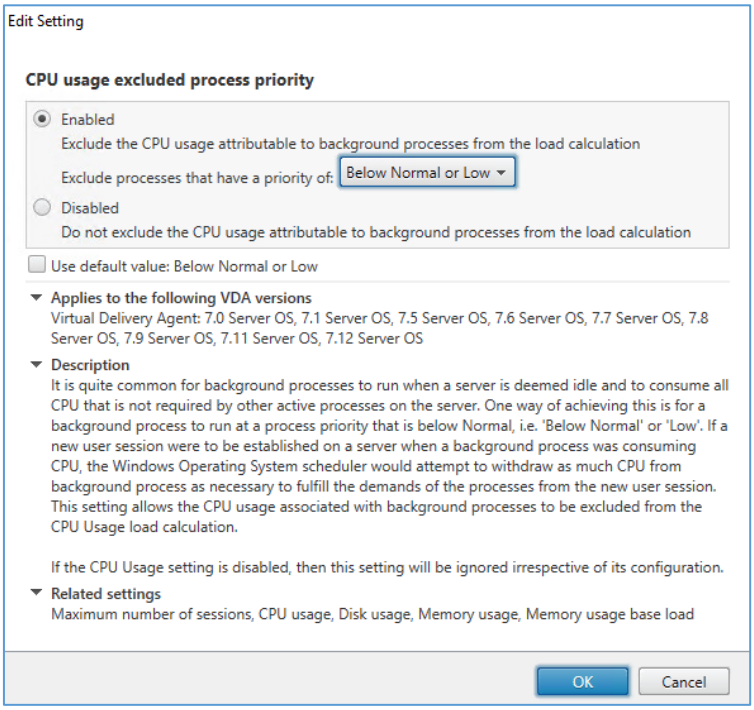
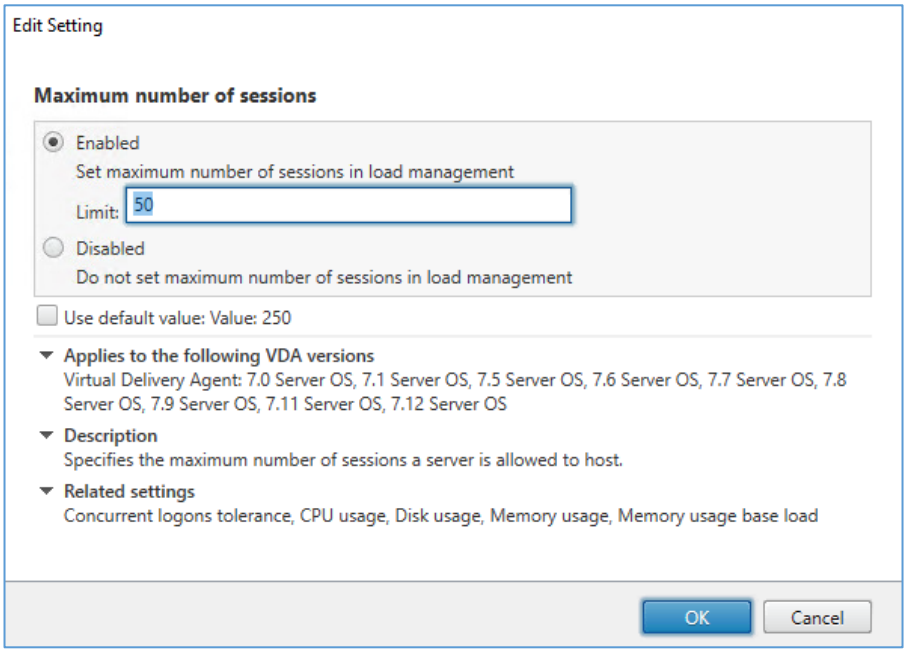
5. Under Settings, click **Select** next to the CPU usage setting.

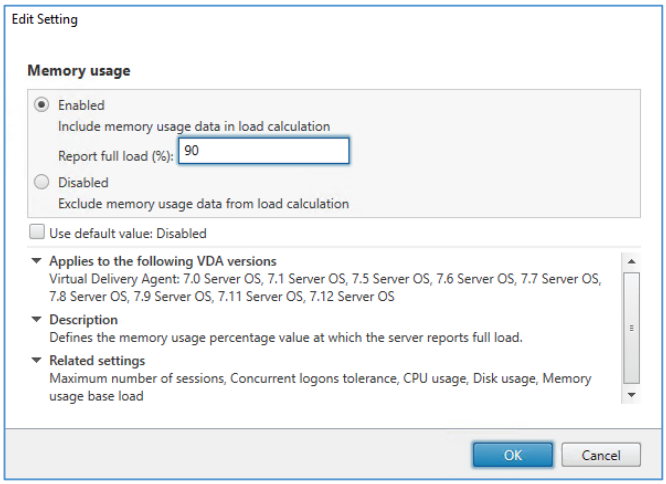
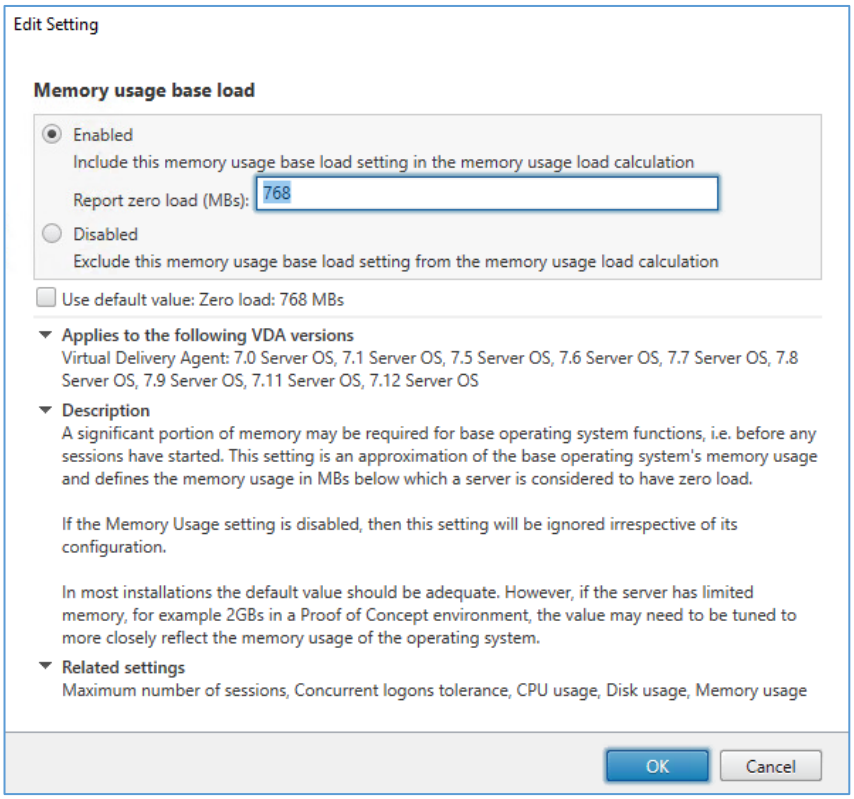
   In the Edit Setting dialog box, select the **Enabled** radio button and set Report full load (%) to **80**.

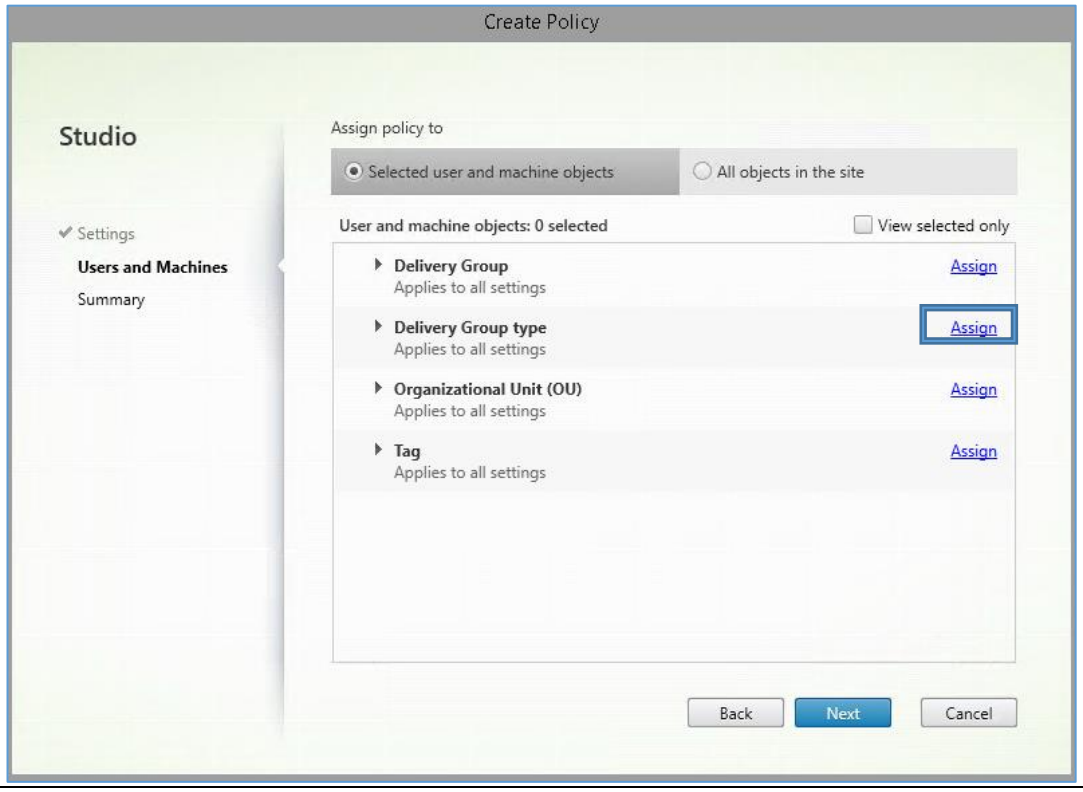
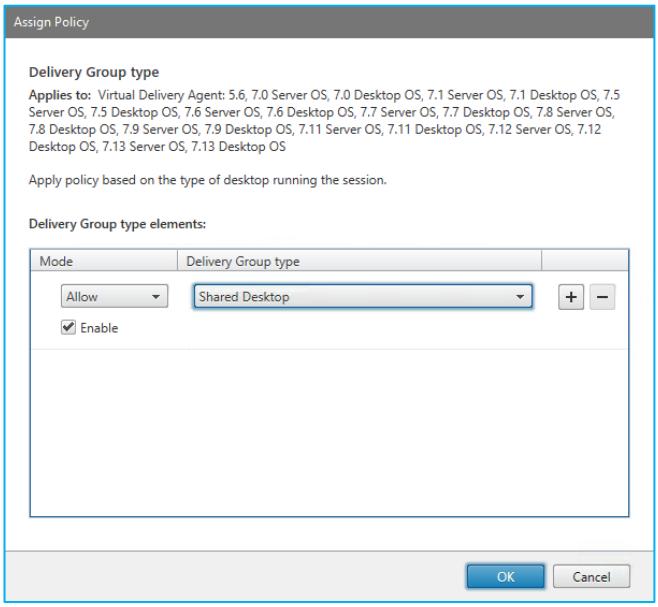


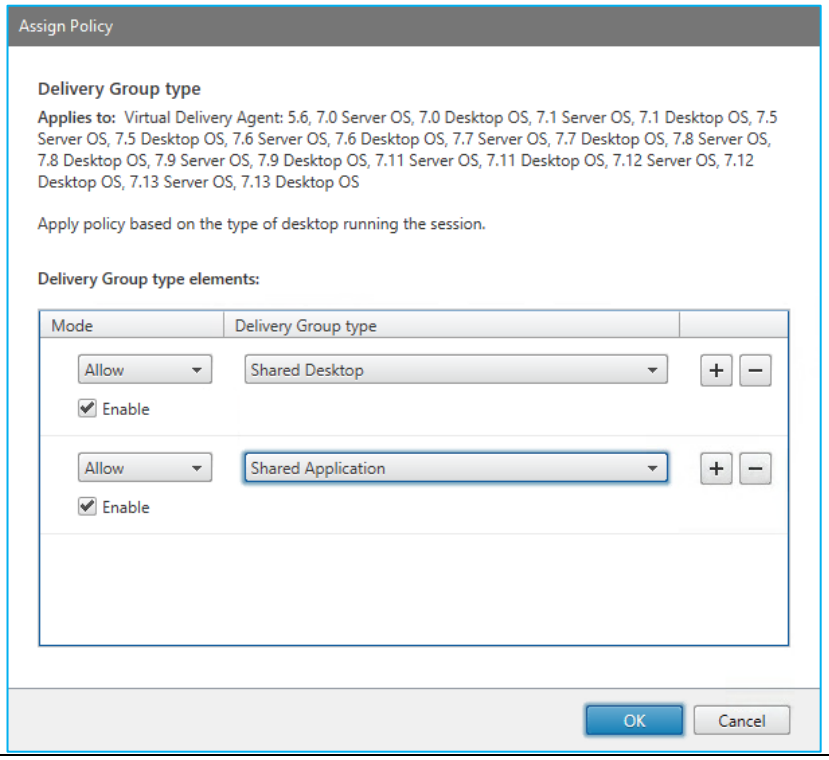
   Click **OK**.

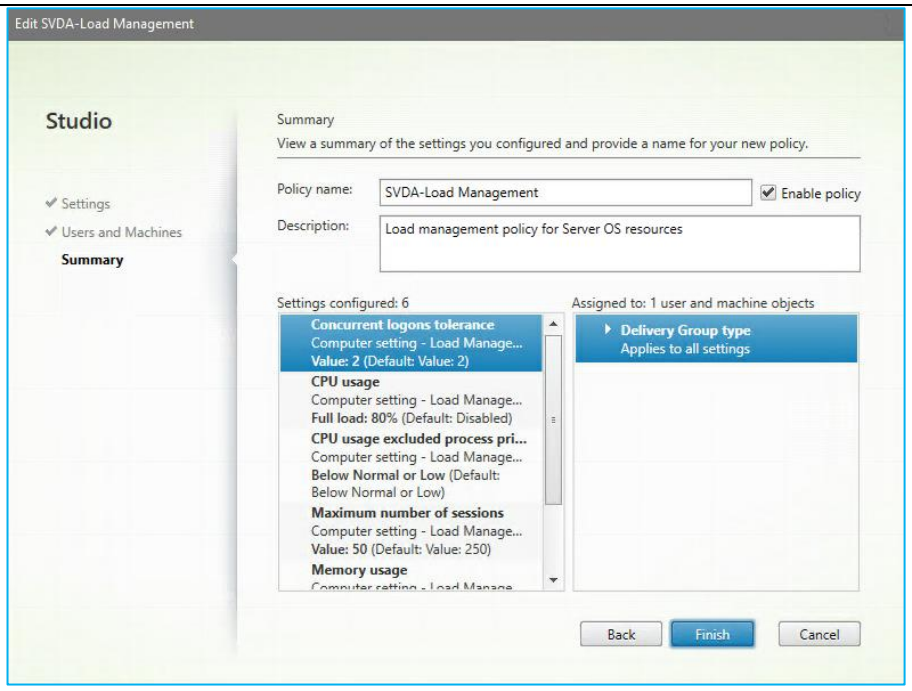
6. Under the Settings, click **Select** next to the CPU usage excluded process priority setting.

	In the Edit Setting dialog box, leave the default radio button **Enabled**. Set the Exclude processes that have a priority of value to **Below Normal or Low**.  Click **OK**.
7.	Under the Settings, click **Select** next to the Maximum number of sessions setting. In the Edit Setting dialog box, leave the default radio button **Enabled**. Set the maximum number of session in load management to **50**.  Click **OK**.

8.	Under the Settings, click **Select** next to the Memory usage setting. In the Edit Setting dialog box, select the **Enabled** radio button. Leave the default value for Report full load (%) at **90**.  Click **OK**.
9.	Under the Settings, click **Select** next to the Memory usage base load setting. In the Edit Setting dialog box, leave the default radio button **Enabled.** Leave the default value for Report zero load (MBs) at **768**.  Click **OK**.
10.	On the Settings page, click **Next**.

11.	On the Users and Machines page, verify that **Selected user and machine objects** is selected. On the User and machine page, click **Assign** next to **Delivery Group type**. 
12.	In the Assign Policy dialog box, verify that the following settings are configured: • Mode: **Allow** • Delivery Group type: **Shared Desktop** • Checkbox set: **Enable** 

13.	To the right of **Shared Desktop**, click the **+** option. In the additional element, verify that the following settings are configured: • Mode: **Allow** • Delivery Group type: **Shared Application** • Checkbox set: **Enable** Click **OK** and then click **Next**. 
14.	On the Summary page, configure the following: • Policy name: **SRV-Load Management** • Description: **Load management policy for Server OS resources** Verify that the checkbox next to **Enable policy** is selected.

	 Click **Finish**.
15.	Verify that the **SRV-Load Management** policy appears in the list of Policies.
16.	Using the Remote Desktop Connection Manager, connect to **NYC-SRV-001**.
17.	Right-click **Start** and select **Command Prompt** to launch a command prompt. Enter the following command: **gpupdate /force** Close the **Command Prompt** after the command has completed successfully.

Key Takeaways:

- Load Management rules help distribute users evenly amongst servers and protect servers from overload. They are only evaluated for new sessions, so define load values to conserve some performance for users already running sessions on the servers.
- Load Management only applies to Server OS VDAs.
- The Load Management rules should be carefully evaluated before enabling them into production, to ensure they meet expectations.

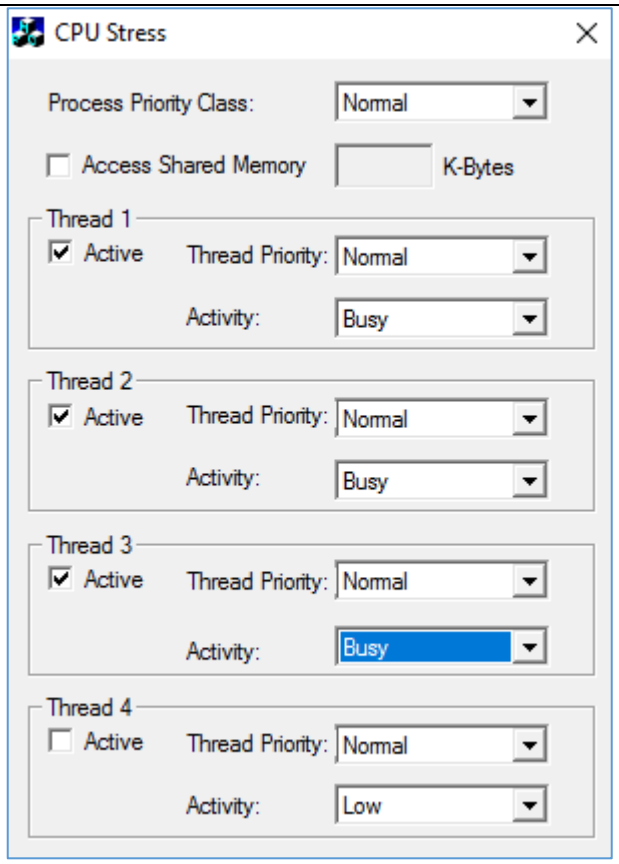
Exercise 6-8: Test the newly configured load management policy settings

Scenario:

Users are occasionally reporting a “Cannot start application” error when launching published applications. The issue is not consistent and occurs maybe once a week to a few users. You check the Controller server and do not find anything in the event logs. Over the past few months, the number of users accessing published applications has increased, which could be causing the servers to get overloaded. You suspect that adding another controller could fix the issue.

To confirm this, your task is to test your theory by using the CPUStress tool to generate extra load on the server to see if it generates the error.

Step	Action
1.	Using the Remote Desktop Connection Manager, verify that you are still connected to **NYC-SRV-001**. **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-SRV-001 by right-clicking this machine and selecting Connect server. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1
2.	Open **File Explorer** from the Windows Taskbar. Browse to **C:\Temp**. Launch **CPUSTRES.exe** to start the CPS Stress tool. **Note**: CPU Stress is a tool from Microsoft (part of Windows SysInternals suite). This utility is used to simulate high CPU usage by a user mode process. You will use it to generate enough CPU load to have an impact on load balancing.
3.	Select the **Active** check box under Thread 1 and set the Activity to **Busy**. Select the **Active** check box under Thread 2 and set the Activity to **Busy**. Select the **Active** check box under Thread 3 and set the Activity to **Busy**.

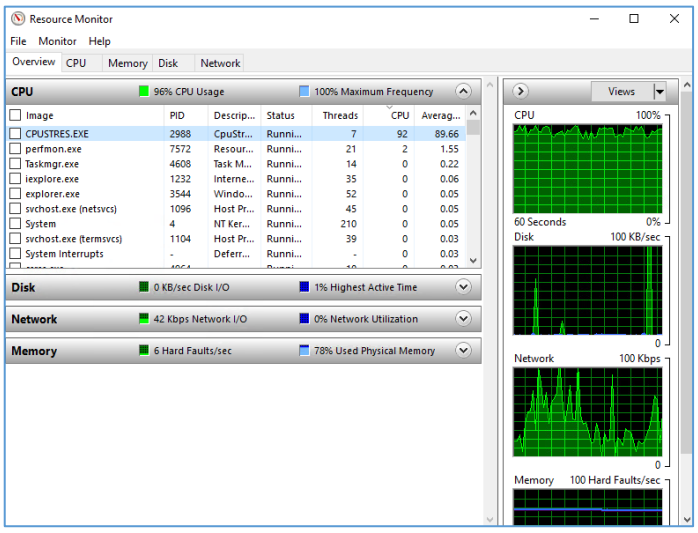


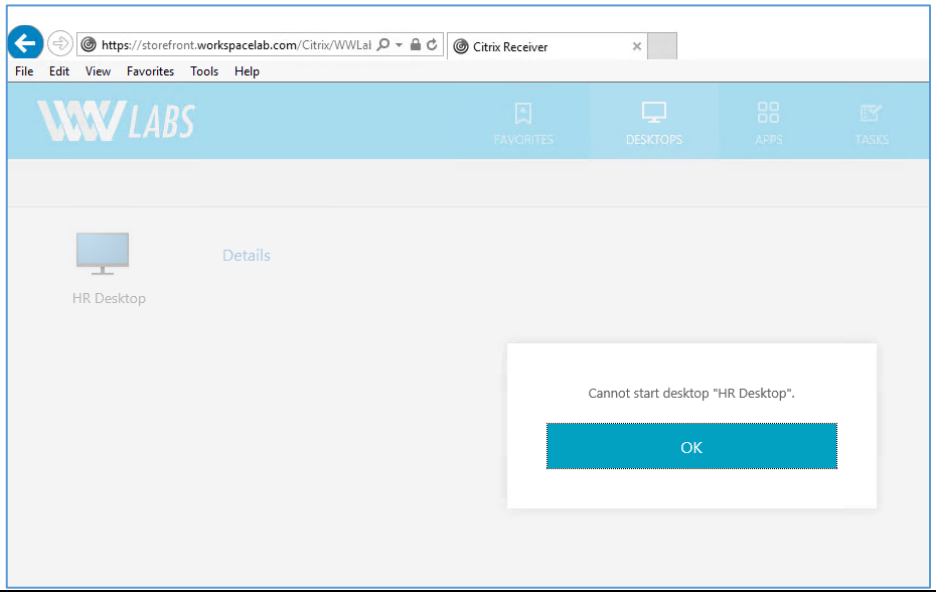
With these settings, CPU usage should average at **+90%**.

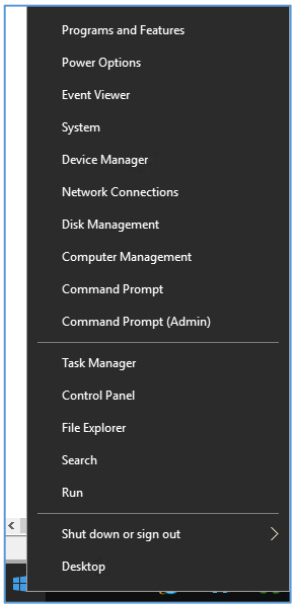
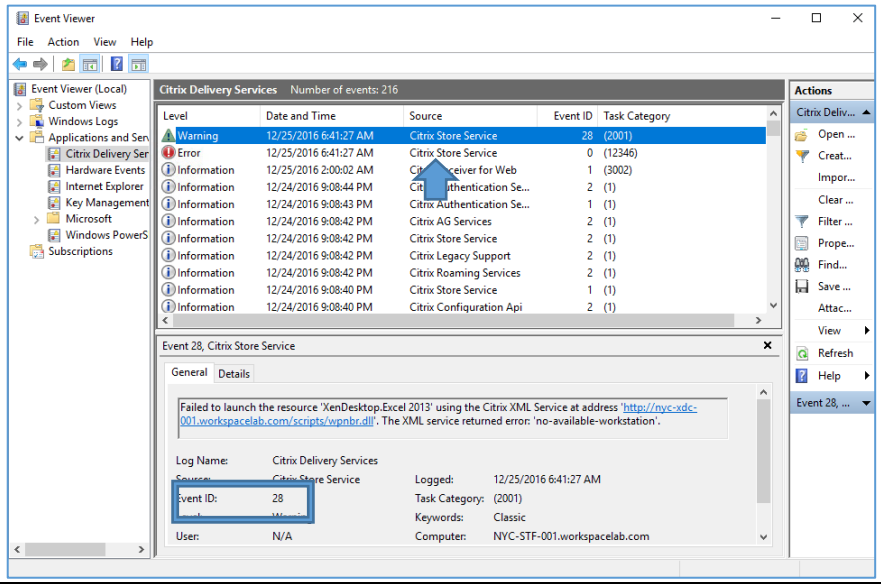
4. Click on **Start menu** and type **resmon.exe** to launch Resource Monitor.

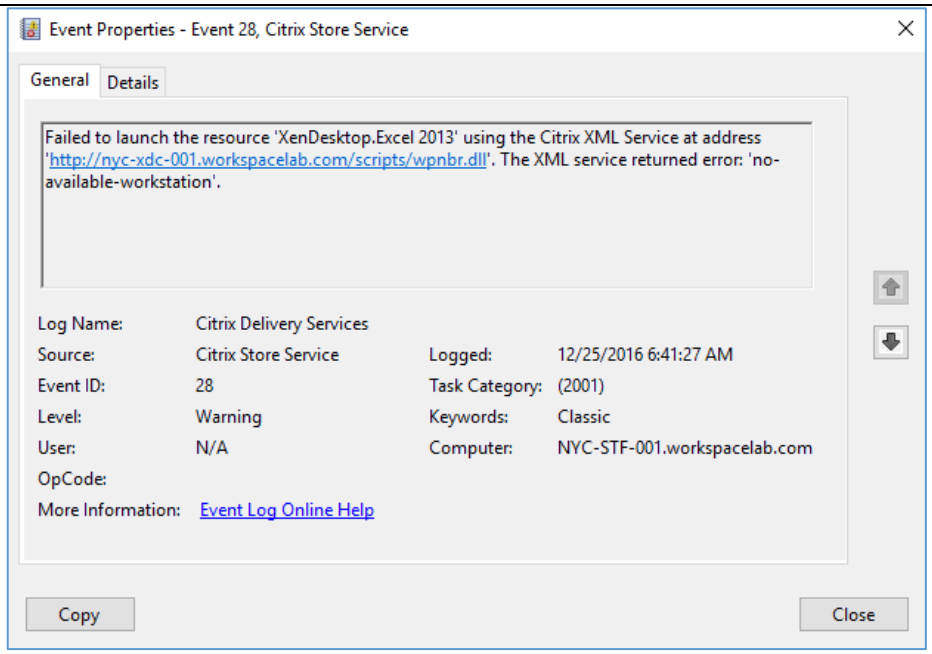
   Note: Resource Monitor is one of the most useful performance troubleshooting tools that built-in to Windows. While most people still refer to Task Manager or Performance Monitor, Resource Monitor is better at a just in time overview of performance.

5. **Review** the CPU graph on the right side of the screen. Confirm that CPU usage is, on the average, above 90%.



6.	Using the Remote Desktop Connection Manager, switch to NYC-WRK-001. To log on to NYC-WRK-001, right-click this machine and select **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\HR1 • Password: Password1
7.	Log on to the store and attempt to launch a session to test high CPU load response. Open **Internet Explorer** and browse to **https://storefront.workspacelab.com**. Log on to the Store using the following credentials: • User name: **HR1** • Password: **Password1** Attempt to **launch** any Microsoft Office application. **Note:** Microsoft Office applications are published only from NYC-SRV-001. **Note:** The application should not launch. If the application does launch successfully, wait 5 minutes and try launching the application again and it should fail with message Cannot start app. Attempt to launch the **HR Desktop**. **Note:** The HR Desktop launch will fail with an error message Cannot start desktop “HR Desktop”. 
8.	Using the Remote Desktop Connection Manager, connect to NYC-STF-001. To log on to NYC-STF-001, right-click this machine and select **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1

9.	**Review** the Event Log on StoreFront to find details about the error message received from the attempted launch of the HR Desktop. Right-click **Start** and select **Event Viewer**.  Expand **Applications and Services Logs** and click **Citrix Delivery Services**. Search for **Event ID 28** Warning from **Citrix Store Service.** This should be the latest event message in the log. 
10.	Review the message within the recorded event. Note that communication with the XML broker works as expected; however, the XML broker cannot provide any machines for connection. You will see the error message “**no-available-workstation**”.



This error means that there are no machines available to users (workers are offline, in maintenance mode or are not properly registered); or machines are not able to host any sessions (overloaded). In the next step, you will see the current state of machines in the impacted Delivery Group.

11. Using the Remote Desktop Connection Manager, connect to NYC-XDC-001.

To log on to NYC-XDC-001, right-click this machine and select **Connect server**.

Note: The following credentials are used to make the connection:

- User name: Workspacelab\Administrator
- Password: Password1

12. Click the **Windows PowerShell** icon in the Start menu.

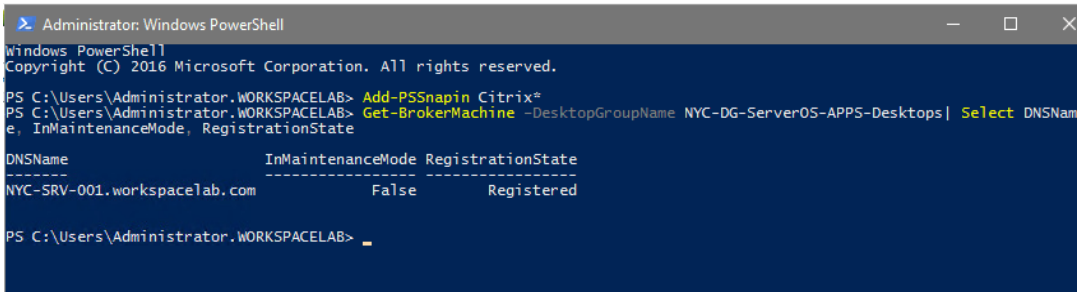
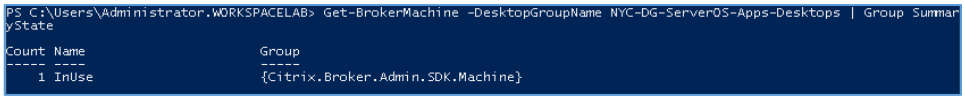
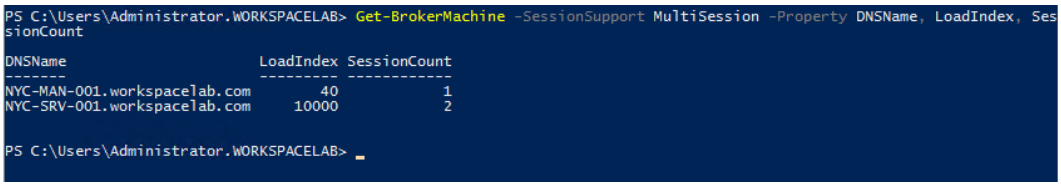
Execute the following command:

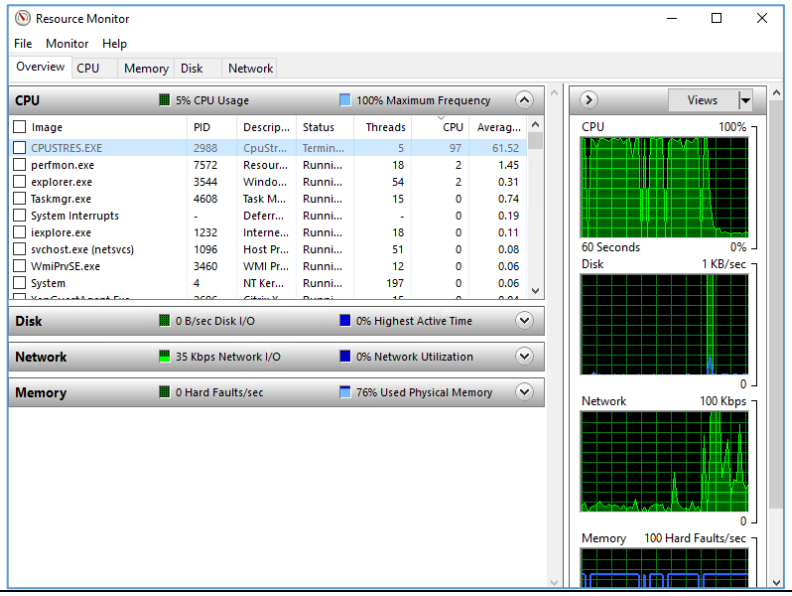
Add-PSSnapin Citrix* and press **Enter**.

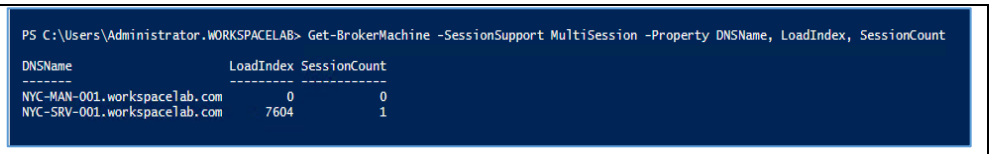
```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.WORKSPACELAB> Add-PSSnapin citrix*
PS C:\Users\Administrator.WORKSPACELAB> _
```

Note: Add-PSSnapin Citrix* loads the Citrix-specific PowerShell modules.

Execute the following command:

	Get-BrokerMachine –DesktopGroupName NYC-DG-ServerOS-APPS-Desktops| Select DNSName, InMaintenanceMode, RegistrationState  Review the output. Notice that all machines in the Delivery Group are registered properly (RegistrationState is **Registered**) and are not in the maintenance mode (InMaintenanceMode is **False**). **Note**: If the machine is in maintenance mode, which may be due to a missed step in one of the previous exercises. You can execute "*Get-BrokerMachine* | *Set-BrokerMachine -InMaintenanceMode $False"* to quickly disable maintenance mode on all the machines in the site.
13.	Display the summary information for all machines and group them by the current state. While this might not seem to be important with only a single Server OS running VDA, it's a useful function if hundreds of machines are part of the Delivery Group. Execute the following command: **Get-BrokerMachine –DesktopGroupName NYC-DG-ServerOS-APPS-Desktops | Group SummaryState**  **Note:** This command consists of two parts. In the first part, you will retrieve all the VDA machines in a specific Delivery Group and then group the results by the SummaryState property. SummaryState can have the following values – "Off," "Unregistered," "Available," "Disconnected," "InUse," and "Preparing." **Note:** You have confirmed that VDA machines are properly configured and should be able to accept new connections.
14.	You are need to confirm the actual load reported by these servers. Execute following command: **Get-BrokerMachine -SessionSupport MultiSession -Property DNSName, LoadIndex, SessionCount**  Notice that LoadIndex for NYC-SRV-001 is reporting full load (**10000**).

	Note: This command is a modern equivalent of running a QFARM (XenApp IMA Era). It will display the current load index on all servers. A 10000 load reported indicates a full load on the VDA, and thus no more connections will be allowed at that time. Unlike the old QFARM, this command is actually more powerful, because it allows you to filter displayed machines (for example, based on Delivery Group or specific catalog). You have identified that all available VDA machines are overloaded and are not accepting new connections.
15.	Using the Remote Desktop Connection Manager, switch back to NYC-SRV-001. To log on to NYC-SRV-001, right-click this machine and select **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1
16.	Close the **CPU Stress** Tool. Switch to the **Resource Monitor** and confirm that the CPU load is reduced to less than **5%**. 
17.	Using the Remote Desktop Connection Manager, switch back to NYC-XDC-001. To log on to NYC-XDC-001, right-click this machine and select **Connect Server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1
18.	Using PowerShell re-execute the commands to verify the reported load is ready to accept new connections. Execute following command: **Get-BrokerMachine -SessionSupport MultiSession -Property DNSName, LoadIndex, SessionCount**

	 The LoadIndex for NYC-SRV-001 is reporting a lower load and is now ready for new sessions. If the load still shows 10000, wait for 2 minutes and execute the command again. **Note**: **PowerShell** was left running. If PowerShell was closed, re-launch it from the taskbar by clicking the Windows **PowerShell** icon. Execute the following command: **Add-PSSnapin Citrix*** and press **Enter**.
19.	Using the Remote Desktop Connection Manager, switch back to **NYC-WRK-001**.
20.	Log on to the store and attempt to launch a session to test the CPU reporting is back to normal levels. Open **Internet Explorer** and browse to **https://storefront.workspacelab.com**. Log on to the store using the following credentials: • User name: **HR1** • Password: **Password1** Attempt to launch any application. **Note:** The application should launch. If it does not, wait 5 minutes and try launching the application again. Attempt to launch the **HR Desktop**. **Note**: The HR Desktop launches.
21.	Log off any running applications and the HR Desktop. **Log Off** the Citrix Receiver.

Key Takeaways:

- Load index is a value that defines the current load of the server.
- Load index is reported to the controller, which uses it to load balance incoming connections across available servers.
- The command *"Get-BrokerMachine -SessionSupport MultiSession -Property DNSName, LoadIndex, SessionCount"* is used to review current load on servers.

Module 7: Application presentation and management

Overview:

This module presents the properties of published resources. We will identify File Type Association and published shortcut placement options.

Before you begin:

Estimated time to complete Module 7 lab exercises: 75 minutes

Exercise 7-1: Configure and test Application Limits

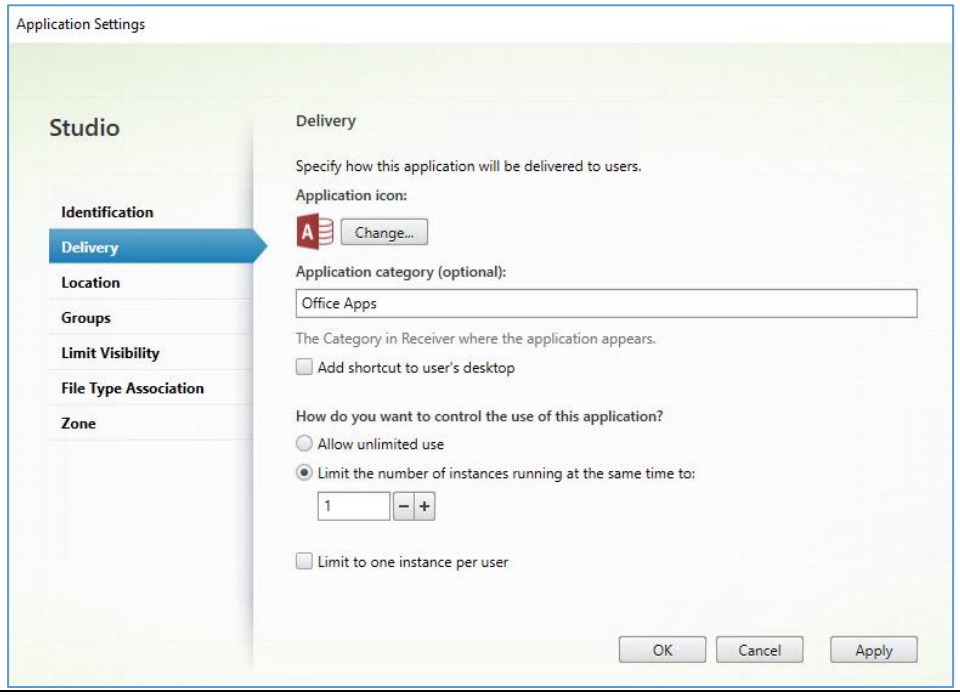
Scenario:

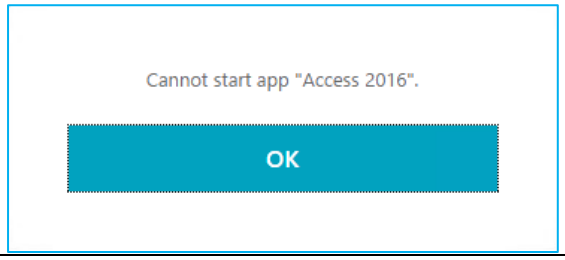
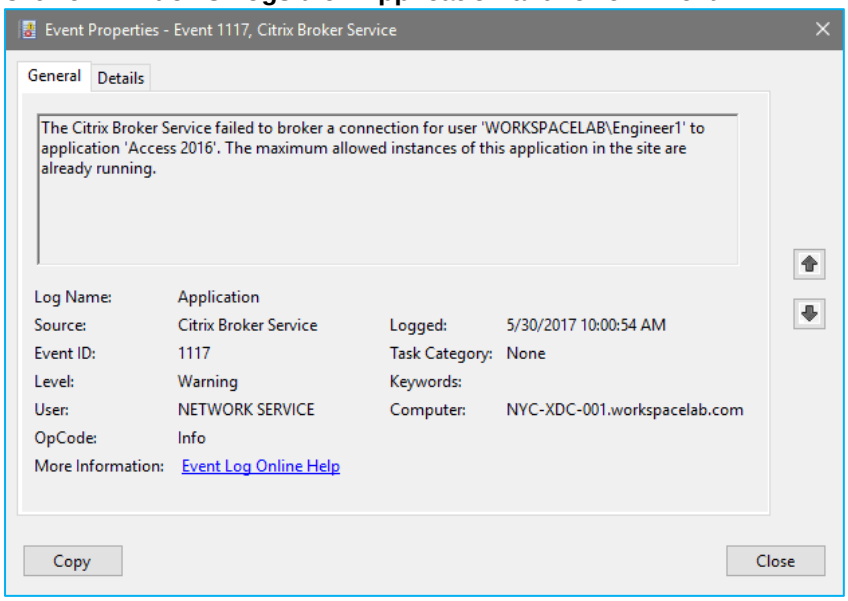
Application Limits allow Citrix Administrators to control total active sessions on per app basis. Configure application limits to help manage application use. For example, you can use application limits to manage the number of users accessing an application simultaneously. Similarly, application limits can be used to manage the number of simultaneous instances of resource-intensive applications, this can help maintain server performance and prevent deterioration in service.

Important: This feature limits the number of application launches that are brokered by the Controller (for example, from Citrix Receiver and StoreFront), and not the number of running applications that could be launched by other methods. This means that application limits assist administrators when managing concurrent usage, but do not provide enforcement in all scenarios. For example, application limits cannot be applied when the Controller is in leased connection mode.

Your task is to configure application limit on Microsoft Access since it has paid licenses. No user should have more than 1 instance of any Microsoft office application and at any point in time total number of Microsoft Access sessions should not exceed 1.

Step	Action
1.	The following VMs are required before beginning the exercises for this Module; all others may be powered down. To power manage your VMs, switch to XenCenter, right-click on the VM in the left pane and select Start or Shut Down. If prompted click Yes. • NYC-ADS-001 • NYC-SQL-001 • NYC-FSR-001 • NYC-XDC-001 • NYC-STF-001 • NYC-MAN-001 • NYC-SRV-001 • NYC-DTP-001 • NYC-WRK-001 **Note**: These above VMs are listed in the start-up order.

2.	Using the Remote Desktop Connection Manager, verify that you are still connected to **NYC-XDC-001**. **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-XDC-001 by right-clicking this machine and selecting Connect server. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1
3.	Using Studio, expand **Citrix Studio (SITE-NewYork)** and click **Applications**. In the middle pane, right-click on the **Access 2016** application and select **Properties**. **Note**: Studio was started in a previous exercise. If Studio was closed in a previous exercise, then click Start > Citrix > Citrix Studio.
4.	On Application Settings window, select **Delivery** on the left and click on radio button for **Limit the number of instances running at the same time to**. Set instances to **1**. 
5.	Click **Apply,** then **OK**.
6.	Using the Remote Desktop Connection Manager, switch to **NYC-WRK-001**.
7.	Log on to the Store and launch Microsoft Access 2016. Open **Internet Explorer** and browse to **https://storefront.workspacelab.com**. Log on to the store using the following credentials: • User name: **HR1** • Password: **Password1** Click on the **APPS** view and launch **Microsoft Access 2016**.

8.	Launch a second instance of Microsoft Access 2016 to validate the Application limit setting is working. Open **Google Chrome** from Desktop and browse to **https://storefront.workspacelab.com**. Log on to the store using the following credentials: • User name: **Engineer1** • Password: **Password1** **Note:** Click Detect Receiver, if prompted. Click on the **APPS** view and launch **Microsoft Access 2016**. Application will not launch and show an error **Cannot start app "Access 2016"**. 
9.	Using the Remote Desktop Connection Manager, switch to **NYC-XDC-001**.
10.	Validate why the second instance of Microsoft Access 2016 failed to launch. Right-click **Start** and launch **Event Viewer**. Click on **Windows Logs** then **Application** and review Event **1117**.  Close **Event Viewer**.
11.	Using the Remote Desktop Connection Manager, switch to **NYC-WRK-001**.
12.	Close the **Access 2016** application.
13.	**Logout** Engineer1 and HR1 from Google Chrome and Internet Explorer. Close **Google Chrome** and **Internet Explorer**.
14.	Log off NYC-WRK-001. To log off, right-click **Start** > choose **Shut down or sign out** > and click **Sign out**.

Key Takeaways:

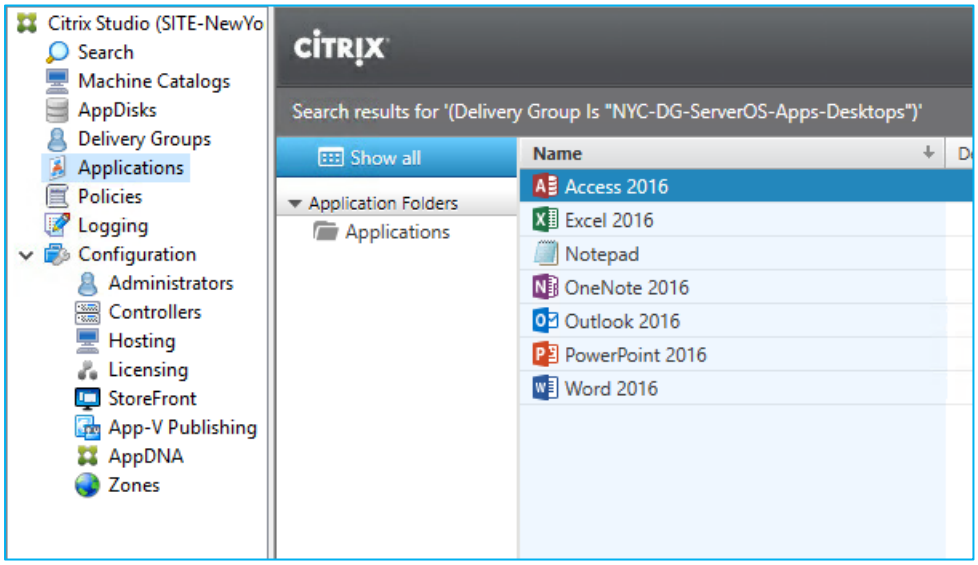
- Application limits can be used to limit applications to only be brokered in x amount of instances, for example: one application is using many resources, so it is desirable to only have 10 instances of this application running at any given time.
- We can also limit the application to only support one instance per user. For example, let's say finance has figured out they can open 10 SAP instances each to support different views, rather than changing the view inside the application. This behavior might cause unnecessary resource usage, in which case we could limit each user to only allow a single instance of SAP.

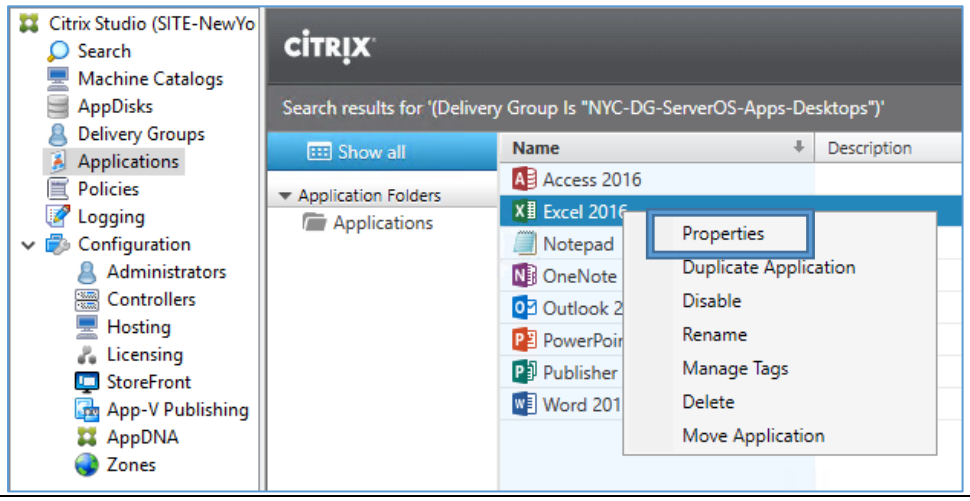
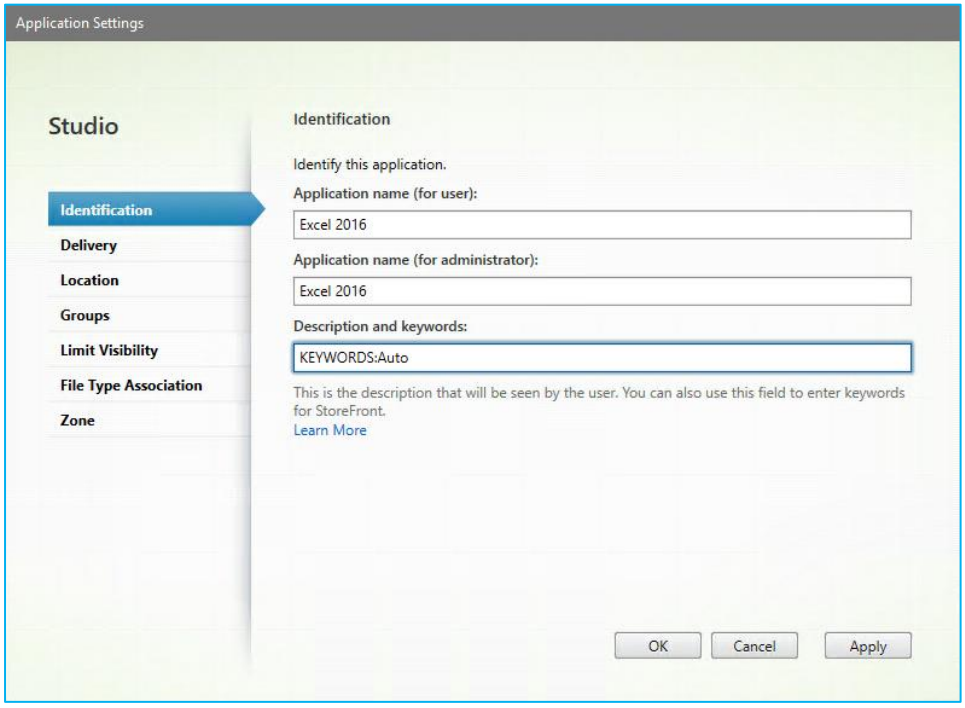
Exercise 7-2: Configure subscription keywords

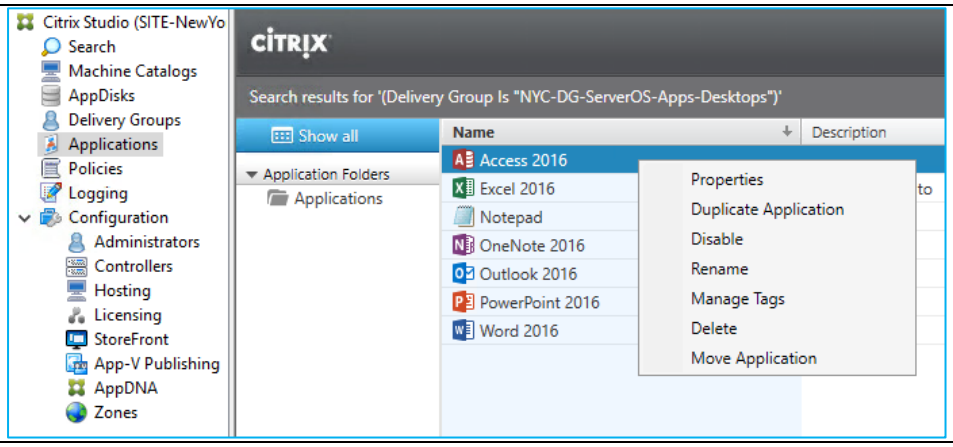
Scenario:

Subscription Keywords allow Citrix Administrators to automatically subscribe users to specific apps. This feature can make it easier for users to navigate large application sets and quickly find regularly used applications.

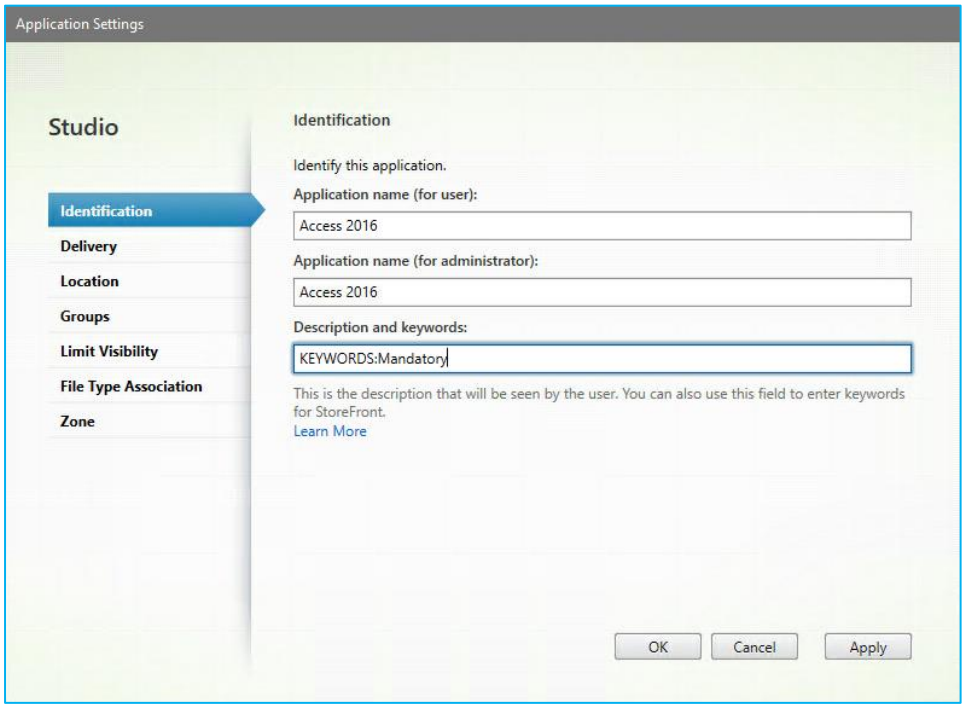
Your task is to modify the properties of some of the published apps and configure subscription Keywords.

Step	Action
1.	Using the Remote Desktop Connection Manager, verify that you are still connected to **NYC-XDC-001**. **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-XDC-001 by right-clicking this machine and selecting Connect server. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1
2.	Using Studio, expand **Citrix Studio (SITE-NewYork)** and click **Delivery Groups**. On the middle pane, select the **NYC-DG-ServerOS-APPS-Desktops** Delivery Group. In the right pane, click **View Applications**. 

	Note: Studio was started in a previous exercise. If Studio was closed in a previous exercise, then click Start > Citrix > Citrix Studio.
3.	In the middle pane, right-click **Excel 2016** and then select **Properties**. 
4.	In the Application Settings page, verify that **Identification** is selected on the left menu. Enter **KEYWORDS:Auto** in the Description and keywords field.  Click **OK**. **Note**: Keywords are not case-sensitive.
5.	In the middle pane, right-click **Access 2016** and then select **Properties**.



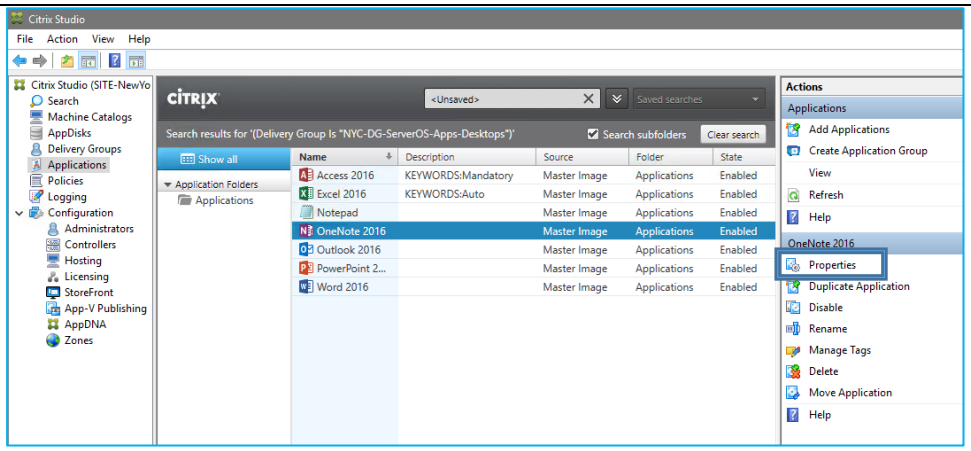
6. In the Application Settings page, verify that **Identification** is selected on the left menu. Enter **KEYWORDS:Mandatory** in the Description and keywords field.



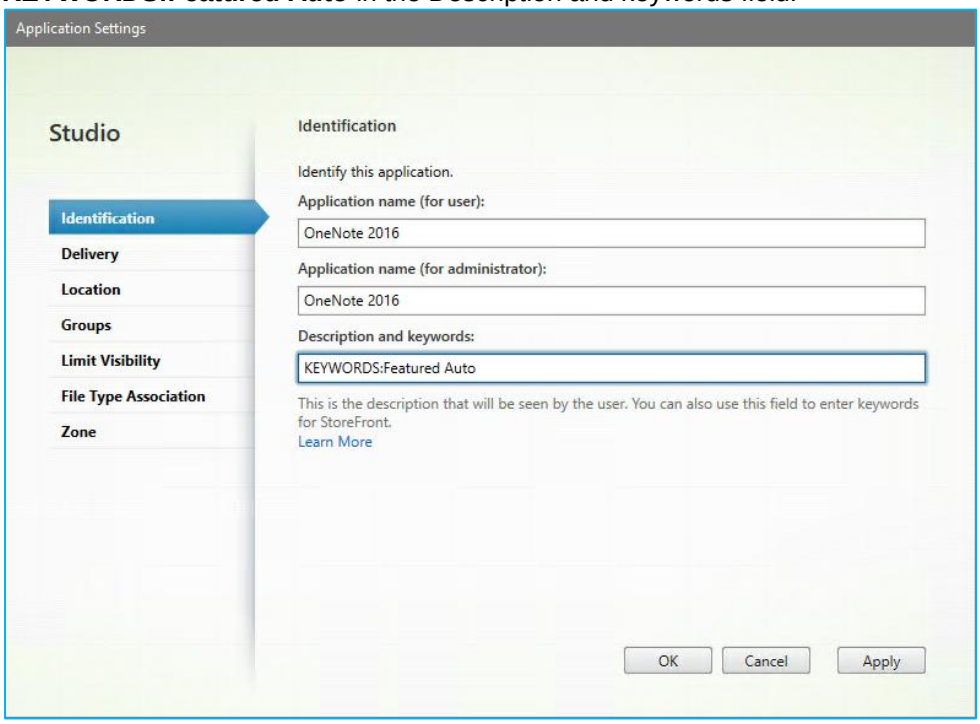
Click **OK**.

Note: KEYWORDS:Auto automatically subscribes users to the application, but provides them with the option to remove it from their favorites tab if they do not want it there. Mandatory will not allow removal.

7. In the middle pane, select **OneNote 2016** and then select **Properties** in the Actions pane.



8. In the Application Settings page, verify that **Identification** is selected in the left menu. Enter **KEYWORDS:Featured Auto** in the Description and keywords field.



Click **OK**.

Note: KEYWORDS:Featured Auto adds the application to the featured list in Citrix Receiver to make the application easy to find. As demonstrated earlier, **Auto** automatically subscribes user to the application and adds the application to favorites.

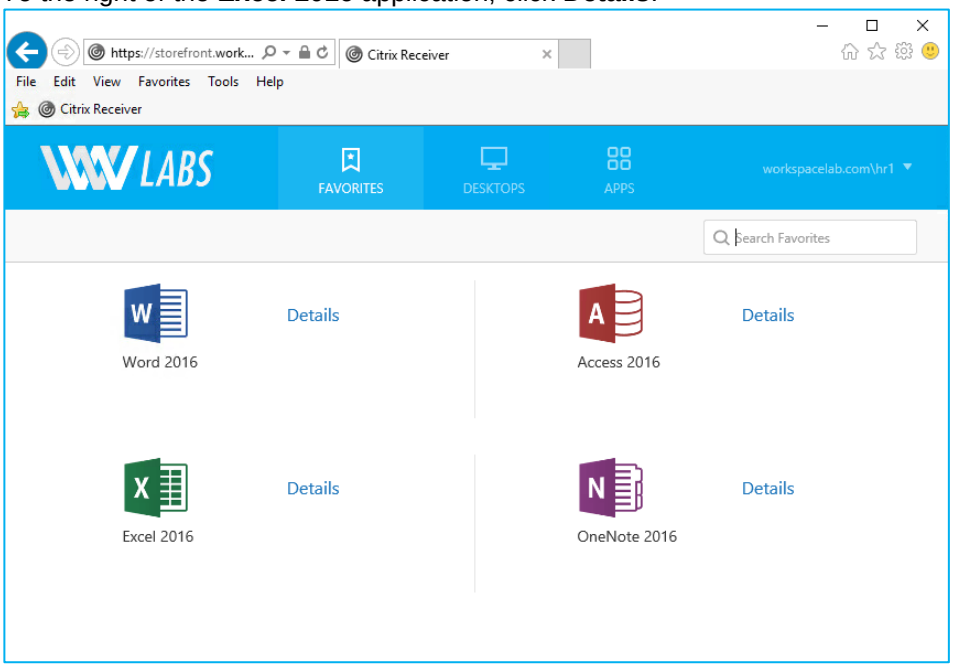
Key Takeaways:

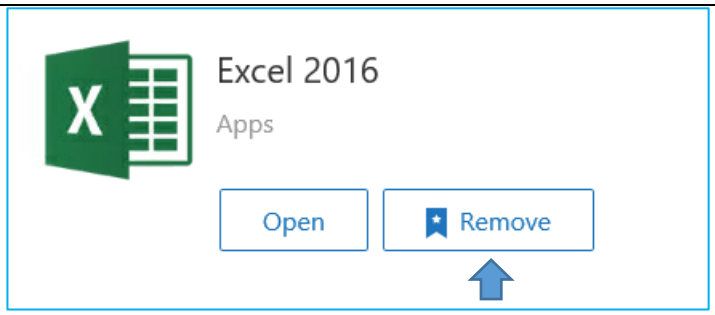
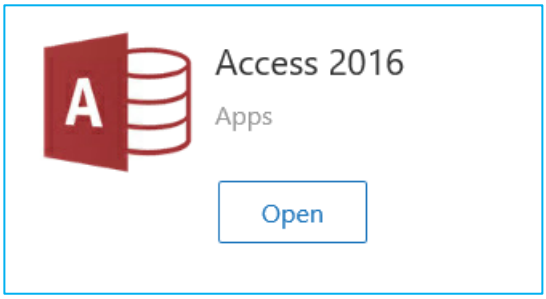
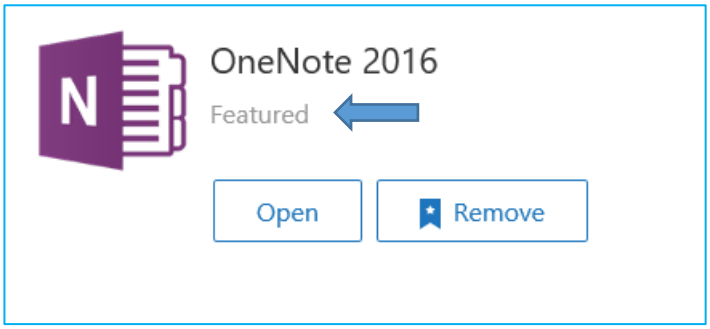
- Several space separated KEYWORDS can be combined, everything after “KEYWORDS:” is treated as keyword.
- For a full list of available KEYWORDS please refer to Citrix Production Documentation using docs.citrix.com.
- It is possible to define custom KEYWORDS like Office or Sales and make StoreFront filter the resources based on these KEYWORDS.

Exercise 7-3: Test subscription keywords

Scenario:

Your task is to test the Subscription Keywords you configured in the previous exercise, by logging into the Store and viewing the subscriptions.

Step	Action
1.	Using the Remote Desktop Connection Manager, connect to NYC-WRK-001. To log on to NYC-WRK-001, right-click this machine and select **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\HR1 • Password: Password1
2.	Open **Internet Explorer** and browse to **https://storefront.workspacelab.com**. Log on with the following credentials: • User name: **HR1** • Password: **Password1**
3.	Click the **APPS** tab and notice the apps HR1 has available. Click the **FAVORITES** tab and notice that the **Word 2016**, **Access 2016, Excel 2016** and **OneNote 2016** applications appear automatically without requiring the user to manually add them to their favorites.
4.	To the right of the **Excel 2016** application, click **Details**. 

	 **Note**: There is a **Remove** option next to the application, so that the user has the option to remove the application. To the right of **Access 2016**, click **Details**.  **Note**: There is no option to remove the application, so the user is not able to unsubscribe or remove the application from the Favorites tab. To the right of **OneNote 2016**, click **Details**.  **Note**: Take notice that the word **Featured** is displayed below the application name.
5.	Log off the Receiver. Select **HR1** and **Log Off**. Close the **browser**.

Key Takeaways:

- Without the use of KEYWORDS, every user will be presented with an empty favorites area in Receiver, and they would need to subscribe to each application they want to launch.
- It may provide an improved user experience to automatically subscribe users to specific company wide applications, such as Office Suite, Adobe Reader or Intranet.

Exercise 7-4: Configure and test Application Prelaunch and Application Lingering

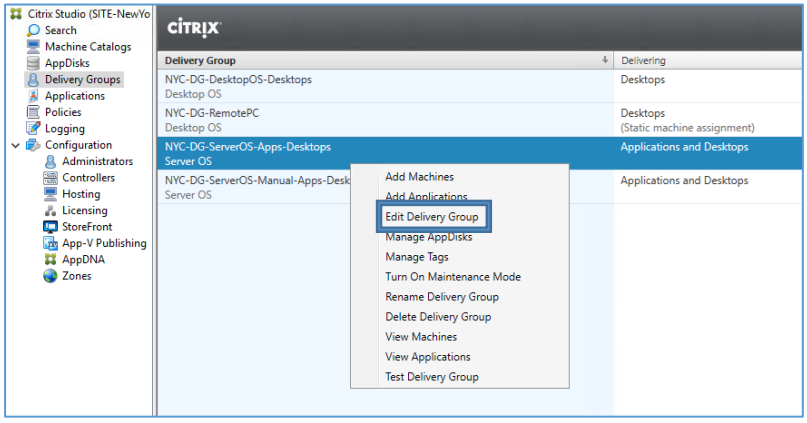
Scenario:

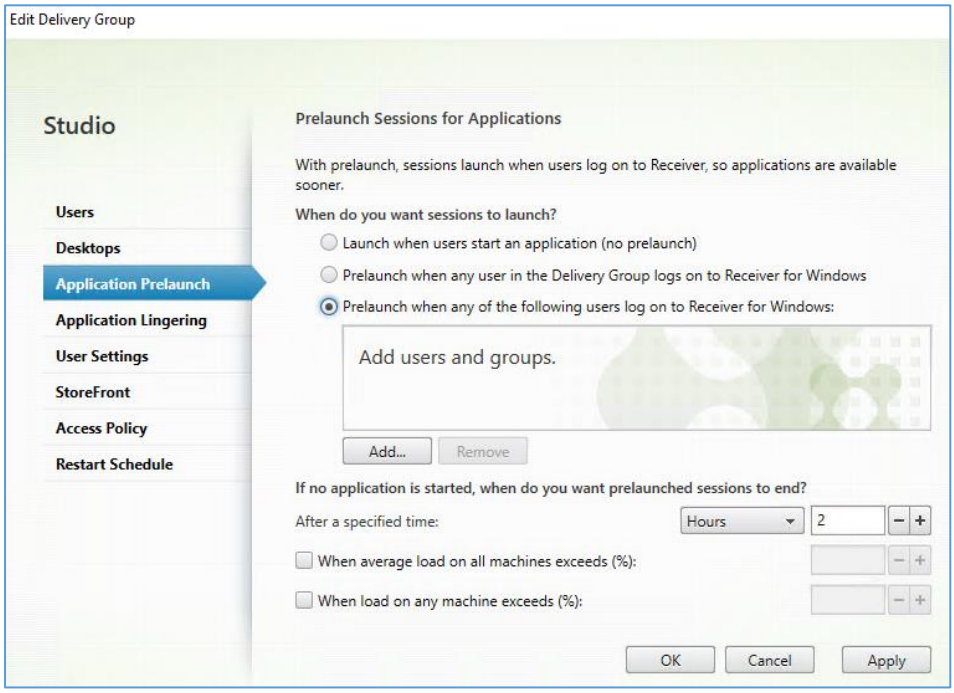
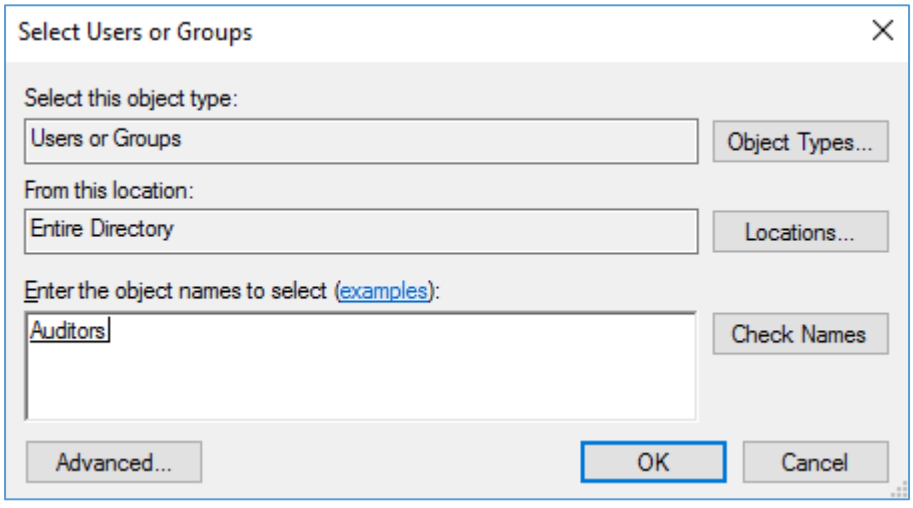
Session prelaunch is a feature that helps reduce the waiting time for users when they start published applications. Session Lingering keeps the session open although the last application in the session closes, that way when a user opens a new application shortly after they will see a quick launch.

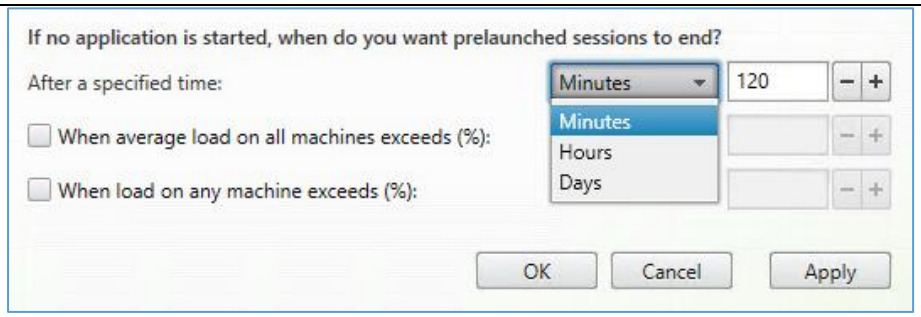
The Citrix Lead Architect has requested you to ensure the Auditors user group has the best user experience when logging on to the POC environment. This user group currently utilizes a legacy Citrix farm that was poorly configured; resulting in logon delays.

These users expressed to the WW Labs CTO they do not want to use the planned production environment if this problem persists.

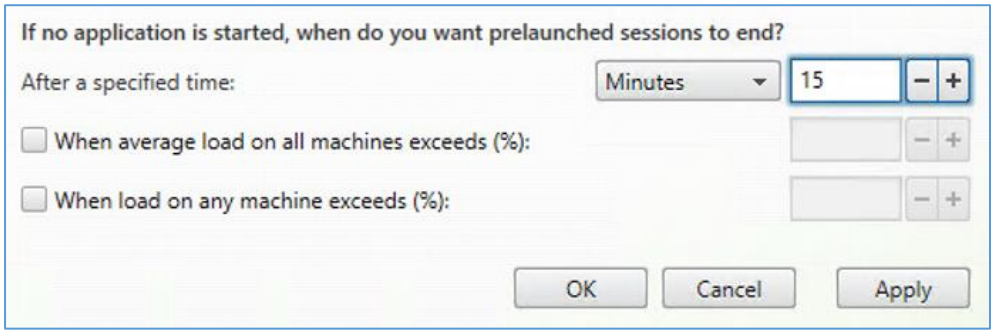
Your task is to enable and test Session Prelaunch and Session Lingering to improve the Auditors group logon experience, and get the Auditors group's acceptance during the POC phase.

Step	Action
1	Using the Remote Desktop Connection Manager, confirm that you are still connected to **NYC-XDC-001**. **Note:** In a previous exercise, you had logged on to NYC-XDC-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-XDC-001 by right-clicking this machine and selecting **Connect server**.
2	Using Studio, expand **Citrix Studio (SITE-NewYork)** and click **Delivery Groups**. On the center pane, right-click on the **NYC-DG-ServerOS-Apps-Desktops** and select **Edit Delivery Group**.  **Note**: Studio was started in a previous exercise. If Studio was closed in a previous exercise, then click Start > Citrix > Citrix Studio.
3	In the Edit Delivery Group window, select the **Application Prelaunch** section.

4	Within the Prelaunch Sessions for Applications settings, select the **Prelaunch when any of the following users log on to Receiver for Windows** radio button.  Click the **Add** button.
5	In the Select Users or Groups window, type **Auditors,** click **Check Names**.  Click **OK**.
6	To the right of **After a specified time**, click the drop-down and select **Minutes**.



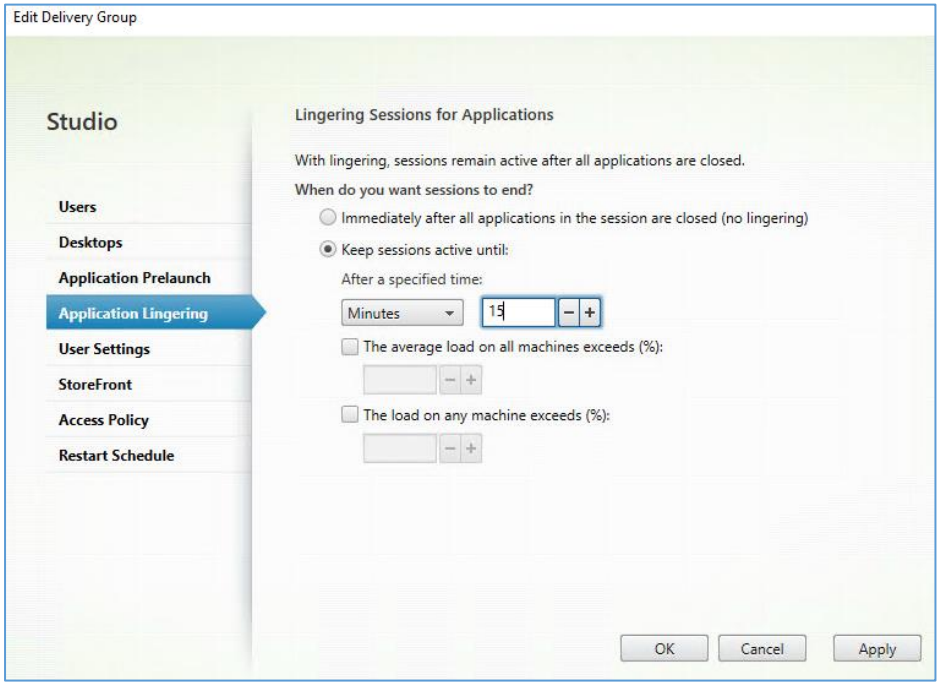
To the right of the Minutes drop-down, type **15**.



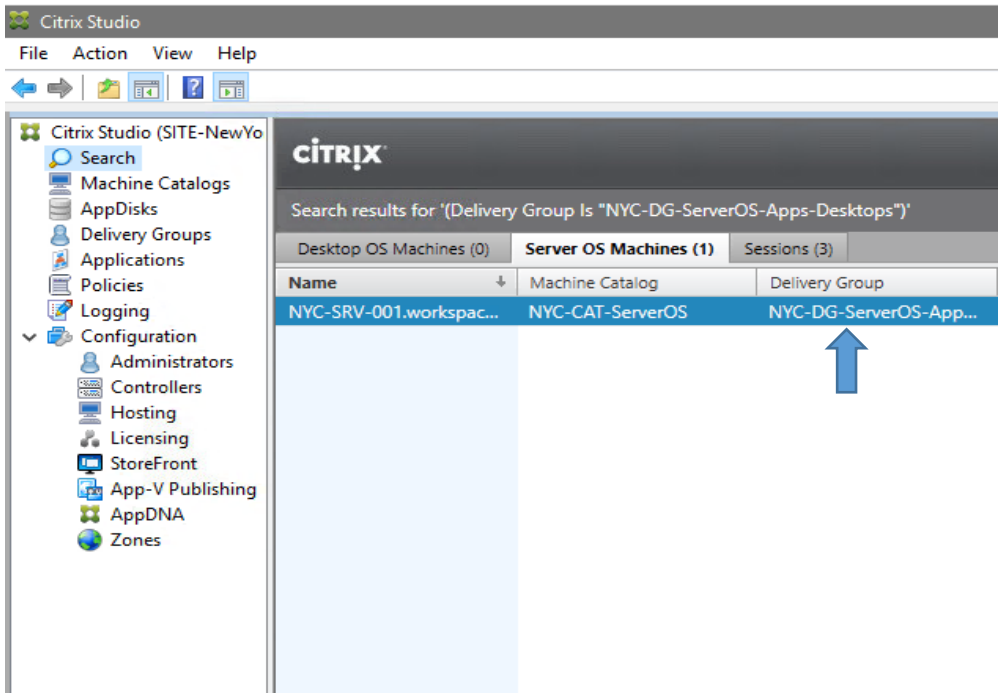
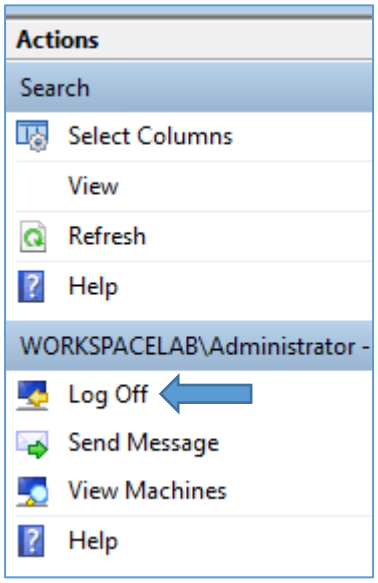
Note: This setting ensures that only Auditors can use the prelaunch feature; and if they have not launched any applications in the first 15 minutes after connecting, their prelaunch session is terminated and applications will subsequently start up using the normal process.

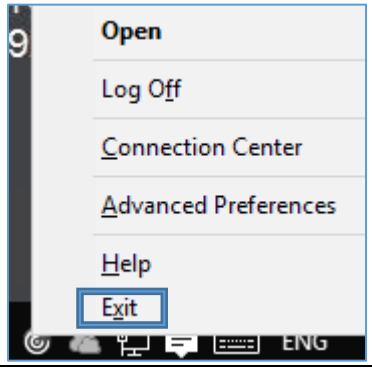
7. In the Edit Delivery Group window, select the **Application Lingering** section.

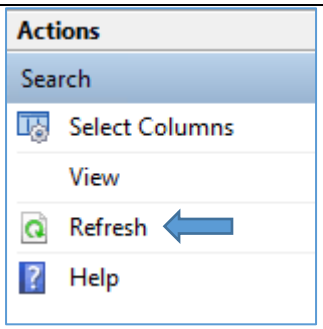
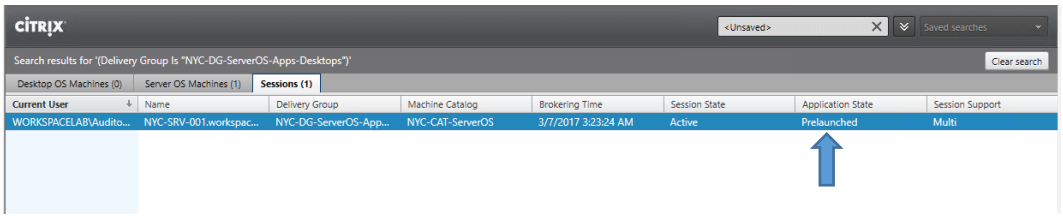
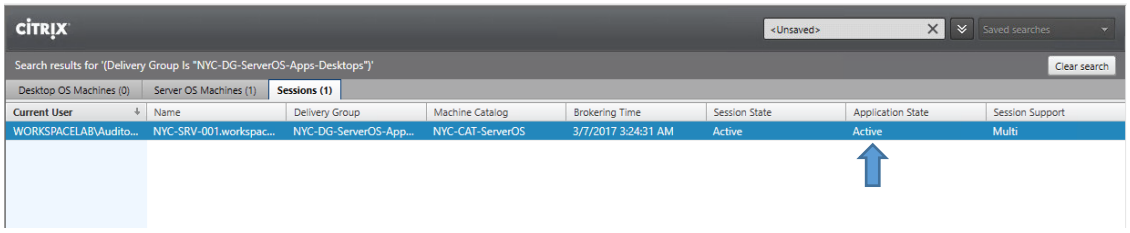
8. Within the Application Lingering settings, change the radio button to **Keep sessions active until,** click the drop-down menu and select **Minutes**.

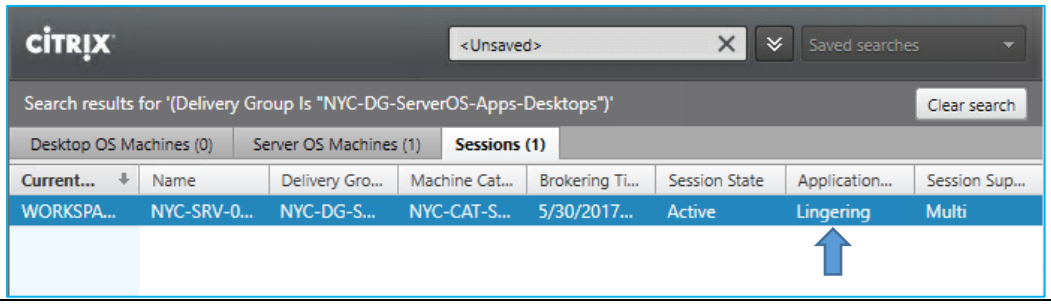


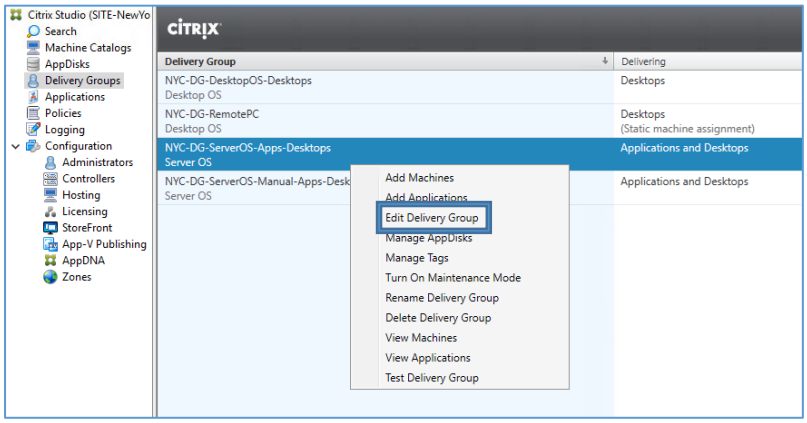
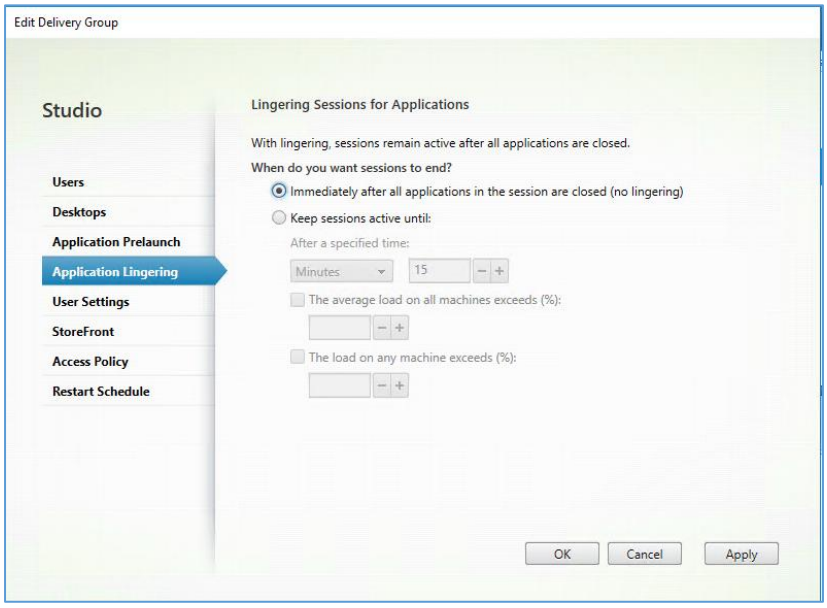
To the right of the Minutes drop-down, type **15**.

9.	Click **OK** to close the Edit Delivery Group window.
10.	On the center pane double-click on the **NYC-DG-ServerOS-Apps-Desktops**. This will take you to the **Search** pane of Studio, listing only results for the NYC-DG-ServerOS-Apps-Desktops.  On the top of the center pane, click the **Sessions** tab.
11.	On the Sessions tab, highlight any running sessions and click **Log Off** in the right pane. Click **Yes** to confirm.  Wait for the sessions to disappear; use the **Refresh** button in the right pane to refresh the view.

12.	Using the Remote Desktop Connection Manager, connect to NYC-WRK-001. To log on to NYC-WRK-001, right-click this machine and select **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\HR1 • Password: Password1
13.	In the bottom right of the screen, right-click the **Citrix Receiver** icon and select **Exit**. 
14.	Click **Start menu** and launch **Citrix Receiver**. Log on with the following credentials: • User name: **Auditor1** • Password: **Password1** **Note:** If an Add Account wizard is shown after starting Receiver, please complete the wizard by typing Auditor1@workspacelab.com and click Next and Continue.
15.	Using the Remote Desktop Connection Manager, switch back to **NYC-XDC-001**. **Note:** In a previous exercise, you had logged on to NYC-XDC-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-XDC-001 by right-clicking this machine and selecting **Connect server**.
16.	Using Studio, verify that you are still in the **Search** window, and verify that the **Sessions** tab is selected in the center pane. If you have lost your way in Studio, select **Delivery Groups** and on the center pane double-click on the **NYC-DG-ServerOS-Apps-Desktops**. This will take you to the **Search** part of Studio, listing only results for the NYC-DG-ServerOS-Apps-Desktops.
17.	Click **Refresh** in the Actions menu in the right pane.

	
18.	Notice that a new session appears and the Application State is **Prelaunch**. 
19.	Using the Remote Desktop Connection Manager, switch back to **NYC-WRK-001**.
20.	In **Citrix Receiver**, click **APPS** and locate **Word 2016**. Click **Word 2016** to start the application. Notice the launch time for Word should now be very fast. **Note**: If you receive the User Account Control prompt grant permission to continue.
21.	Using the Remote Desktop Connection Manager, switch back to **NYC-XDC-001**. **Note:** In a previous exercise, you had logged on to **NYC-XDC-001** using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-XDC-001 by right-clicking this machine and selecting Connect server.
22.	Using Studio, verify that you are still in the **Search** window and verify that the **Sessions** pane is selected in the center pane. If you have lost your way in Studio, select **Delivery Groups** and on the center pane double-click on the **NYC-DG-ServerOS-Apps-Desktops.** This will take you to the **Search** part of Studio, listing only results for the NYC-DG-ServerOS-Apps-Desktops.
23.	Click **Refresh** in the Actions menu on the right pane.
24.	Notice that the session appears, and the Application State is now **Active**. 
25	Using the Remote Desktop Connection Manager, switch back to NYC-WRK-001.

	To log on to NYC-WRK-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\HR1 • Password: Password1
26.	Close any **Microsoft Word related popups** and close **Word 2016**.
27.	Using the Remote Desktop Connection Manager, switch back to **NYC-XDC-001**. **Note:** In a previous exercise, you had logged on to NYC-XDC-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-XDC-001 by right-clicking this machine and selecting Connect server.
28.	Using Studio, verify that you are still in the **Search** window and verify that the **Sessions** pane selected in the center pane. If you have lost your way in Studio, select **Delivery Groups** and on the center pane double-click on the **NYC-DG-ServerOS-Apps-Desktops.** This will take you to the **Search** part of Studio, listing only results for the NYC-DG-ServerOS-Apps-Desktops.
29.	Click **Refresh** in the Actions menu in the right pane.
30.	Notice that the session appears, and the Application State is now **Lingering**. 
31.	Using the Remote Desktop Connection Manager, switch back to **NYC-WRK-001**.
32.	In **Citrix Receiver**, click **APPS** and locate **Excel 2016**. Click **Excel 2016** to start the application. Notice the launch time for Excel 2016 is also very fast, despite the fact that we just closed Word 2016.
33.	Close **Excel 2016**. Log off the Store. Click **Auditor1** and **Log Off**.
34.	Using the Remote Desktop Connection Manager, confirm that you are still connected to **NYC-XDC-001**. **Note:** In a previous exercise, you had logged on to NYC-XDC-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-XDC-001 by right-clicking this machine and selecting Connect server.

35.	Using Studio, expand **Citrix Studio (SITE-NewYork)** and click **Delivery Groups**. On the center pane right-click on the **NYC-DG-ServerOS-Apps-Desktops**, select **Edit Delivery Group**.  **Note**: Studio was started in a previous exercise. If Studio was closed in a previous exercise, then click Start > Citrix > Citrix Studio.
36.	In the Edit Delivery Group window, select the **Application Lingering** section.
37.	Within the Application Lingering settings, select the **Immediately after all applications in the session are closed (no lingering)** radio button.  Click the **OK** button. **Note:** The application lingering feature might cause sessions not to close when you expect them to in later exercises; therefore, we are disabling the feature again after successful verification of the feature.

Key Takeaways:

- Application prelaunch can reduce the perceived launch time for hosted applications.

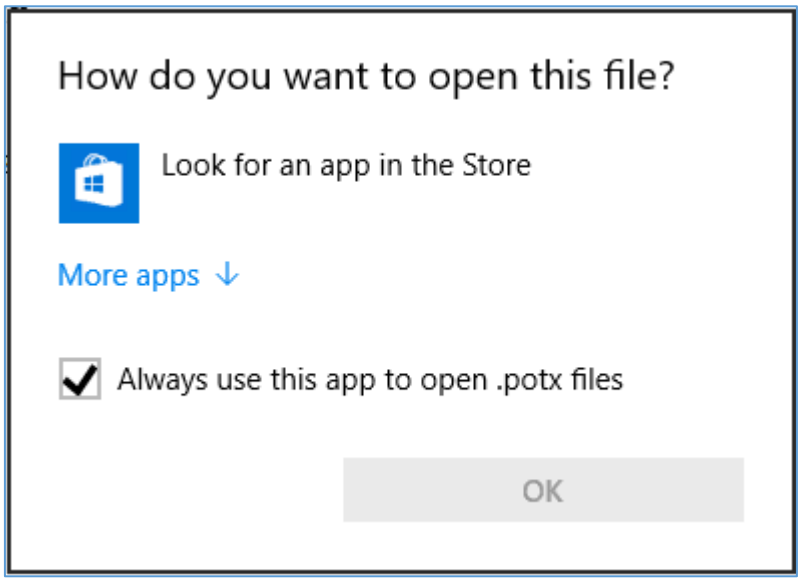
- With prelaunch enabled, a session is created when the user logs on to Citrix Receiver. However, the application is not presented to the user.
- Application lingering keeps the session running, instead of the session terminating when the last hosted application is closed.
- Application lingering ensures quick launch after a user has closed the last hosted application.
- Both technologies rely on actual sessions being opened and maintained, so licenses and resources will be consumed even if the user does not start any hosted applications.
- Application prelaunch requires the use of Citrix Receiver as Receiver for Web does not support prelaunch of user sessions.

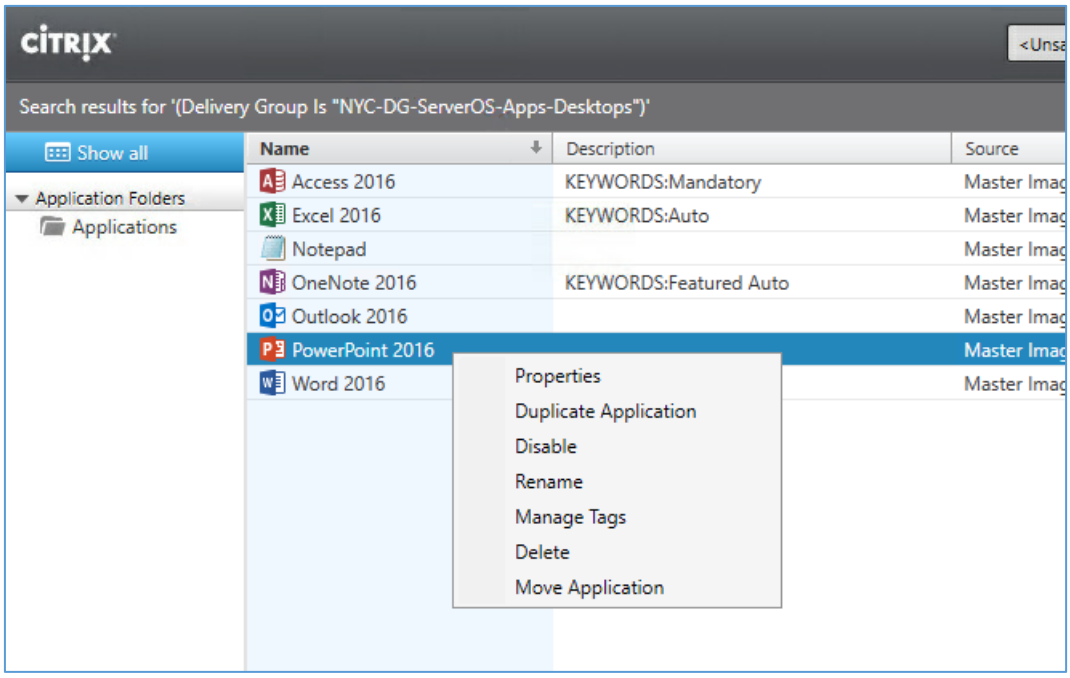
Exercise 7-5: Configuring File Type Associations

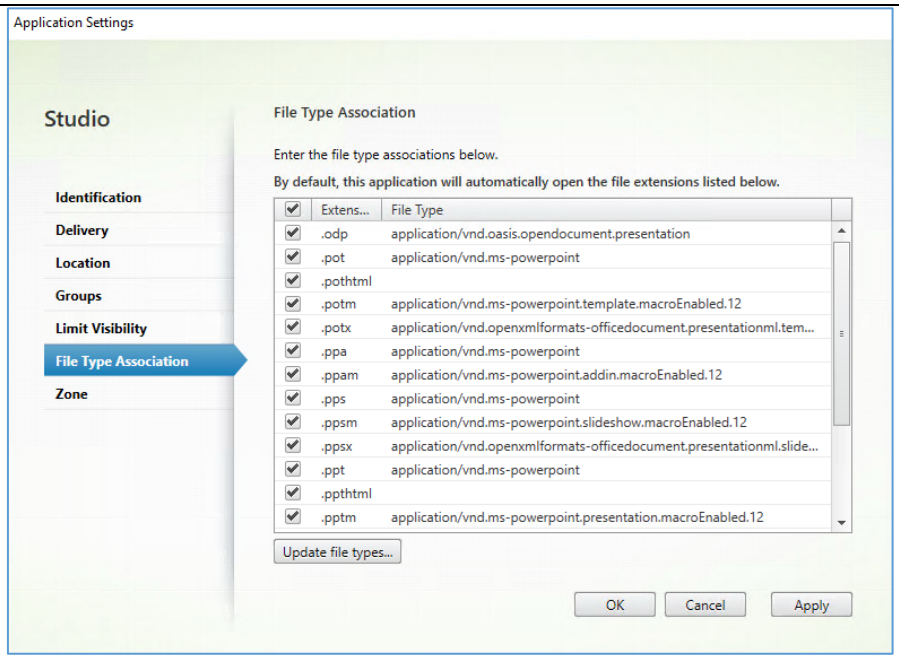
Scenario:

File Type Association is a feature that allows users to open documents from their local endpoint devices or from network shares using published applications. When the document is opened the registered application from a VDA is started automatically to open the document.

Your task is to configure File Type Associations.

Step	Action
1.	Using the Remote Desktop Connection Manager, confirm that you are still connected to **NYC-WRK-001**. **Note:** In a previous exercise, you had logged on to NYC-WRK-001 using the following credentials to make the connection: • User name: Workspacelab\HR1 • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-WRK-001 by right-clicking this machine and selecting **Connect server**.
2.	Launch **File Explorer** from the Windows Taskbar. Navigate to **\\NYC-FSR-001\Resources** and double-click the **WWLabs PPT Template v1.potx** file. 

	You will see a dialog box asking you how you want to open the file. This is because **Microsoft PowerPoint** is not currently installed locally on **NYC-WRK-001**. Press the **ESC** key to close the dialog box.
3.	Using the Remote Desktop Connection Manager, verify that you are still connected to **NYC-XDC-001**. **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-XDC-001 by right-clicking this machine and selecting Connect server. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1
4.	Using Studio, expand **Citrix Studio (SITE-NewYork)** and click **Applications**. In the center pane, right-click **PowerPoint 2016** and select **Properties**.  Select **File Type Association** on the left menu. Select the top checkbox to choose **all extensions** then click **Apply** and **OK**.

	 **Note**: Studio was started in a previous exercise. If Studio was closed in a previous exercise, then click Start > Citrix > Citrix Studio.

Key Takeaways:

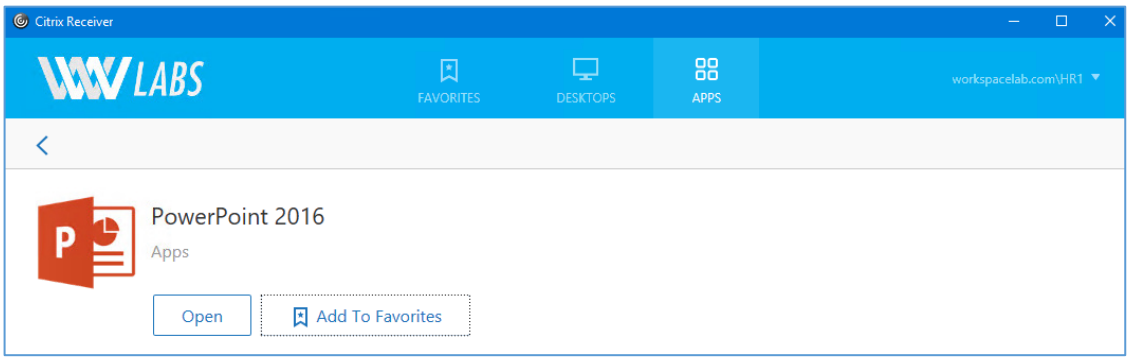
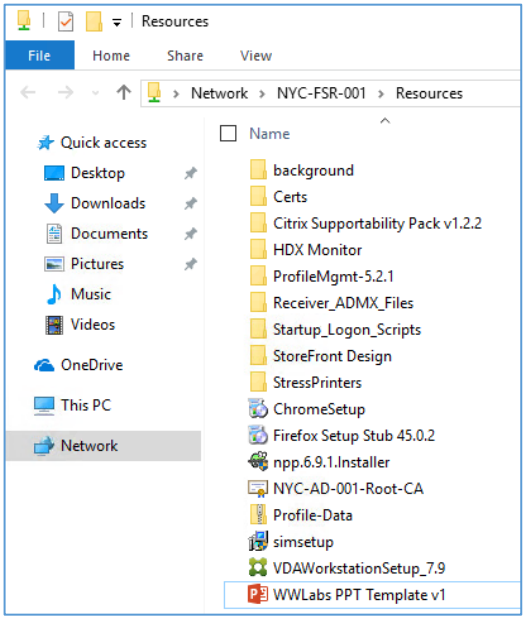
- File Type Associations are not enabled by default. They must be configured by editing the application properties in Studio.
- Citrix Receiver automatically changes Windows File Type Association on managed and unmanaged endpoint devices.
- If File Type Associations are not configured, users will have to launch the appropriate virtual app and navigate to the file on the endpoint device via a mapped drive. This does not provide a good user experience.

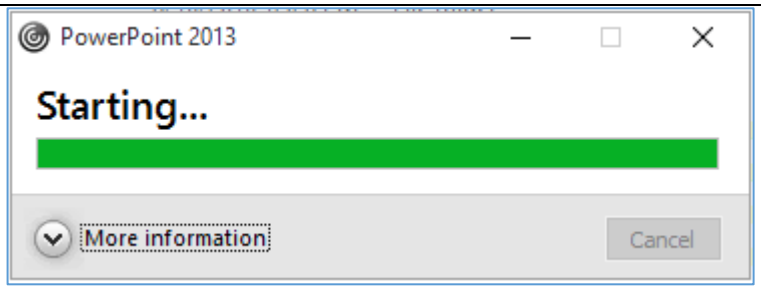
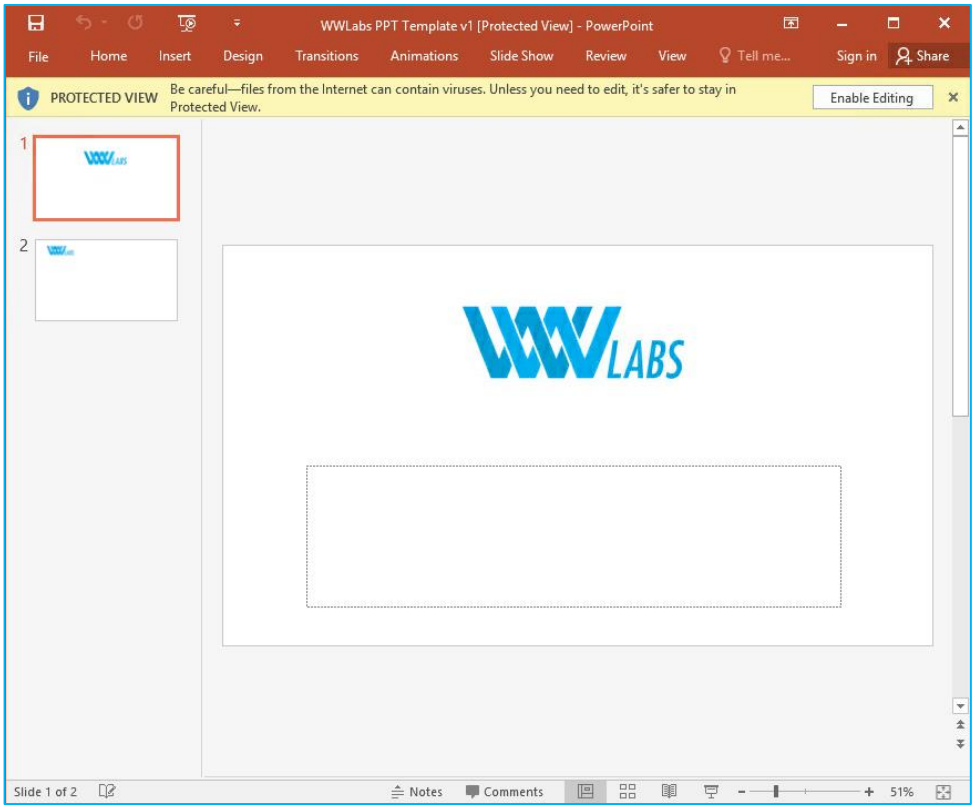
Exercise 7-6: Test File Type Associations

Scenario:

Your task is to test the previously configured File Type Association feature, by launching a PowerPoint .potx file from outside of the Citrix published PowerPoint app.

Step	Action
1.	Using the Remote Desktop Connection Manager, connect to NYC-WRK-001. To log on to NYC-WRK-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\HR1 • Password: Password1
2.	Launch the **Citrix Receiver** application from the system tray or Start Menu. Log on with the following credentials: • User name: **HR1** • Password: **Password1**

	Note: If Log On is not available, you may still be logged on as Auditor1. Select Log Off and exit Receiver. Re-launch Receiver and log on as HR1.
3.	Click **APPS** on the top bar; locate **PowerPoint 2016** in the list of available applications. Click **Details** next to PowerPoint, and on the details view select **Add To Favorites** to add the application to your Favorites view.  **Note:** In order to use FTA you must ensure the applications needed to open the desired file types are added to Favorites, this can be done either manually by the user or by the Admin through the use of KEYWORDS.
4.	Launch **File Explorer** from the Windows Taskbar. Navigate to **\\NYC-FSR-001\Resources** and open the **WWLabs PPT Template v1.potx** file.  In the prompt that opens *How do you want to open this file?* ,select **Always use this app to open .potx files** and click **OK**. The published PowerPoint 2016 opens the file successfully, even though NYC-WRK-001 does not have the PowerPoint application installed locally. The PowerPoint application is running in a session hosted on NYC-SRV-001.

	  **Note:** Microsoft PowerPoint must be added as a favorite in **Citrix Receiver** for the file type association to apply on the endpoint.
5.	Close **PowerPoint 2016**. Log off Citrix Receiver. Click **HR1** and **Log Off**.

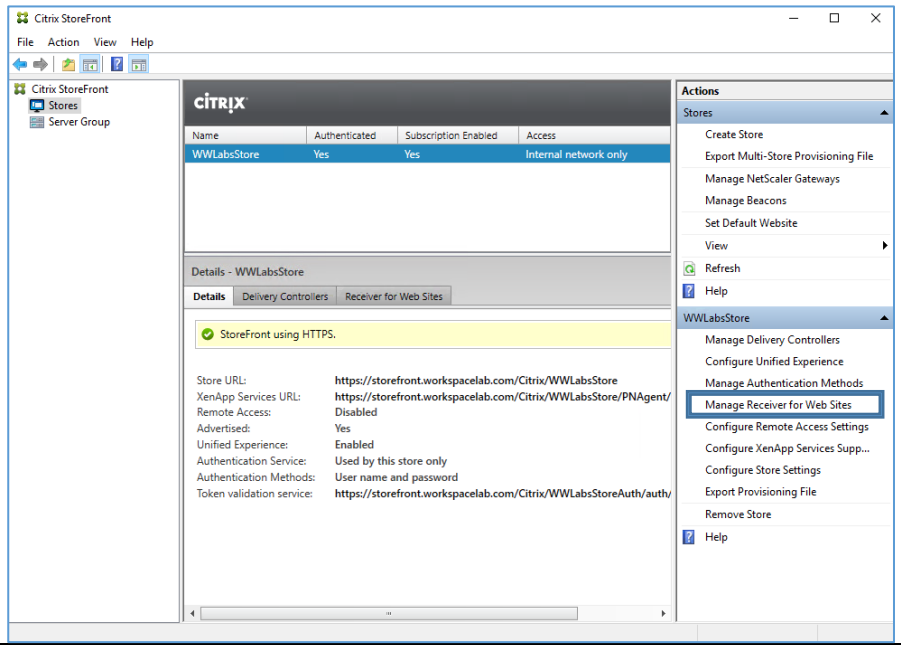
Key Takeaways:

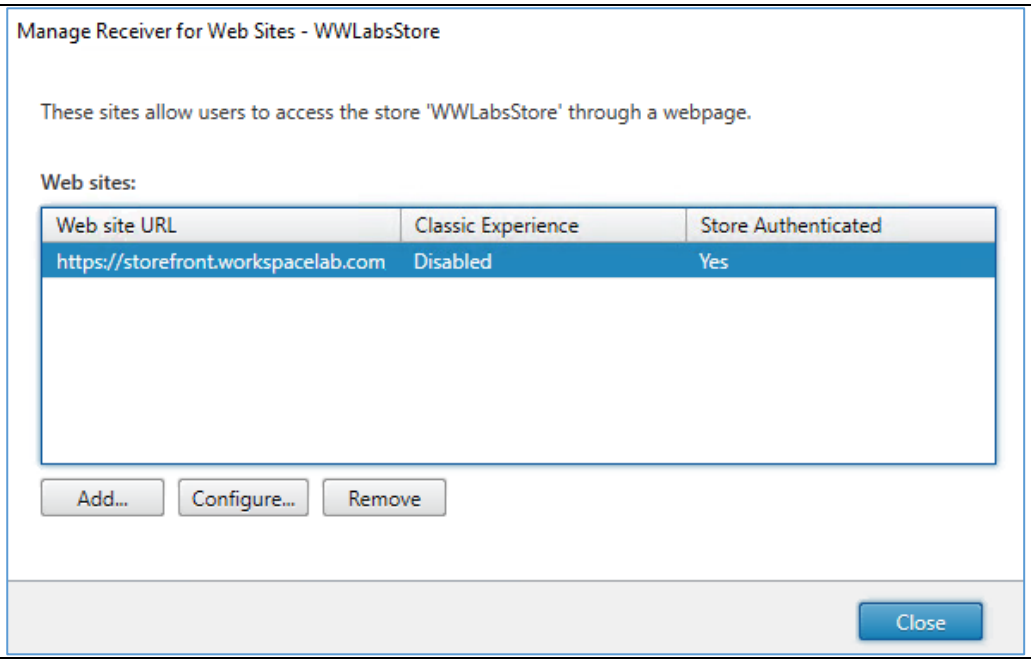
- This feature requires the Citrix Receiver to be installed and configured as Receiver for Web does not include this capability.
- If the required application is not added as a favorite, Citrix Receiver will not be able to update the FTA settings on the endpoint.

Exercise 7-7: Configure Featured App Groups and App Categories

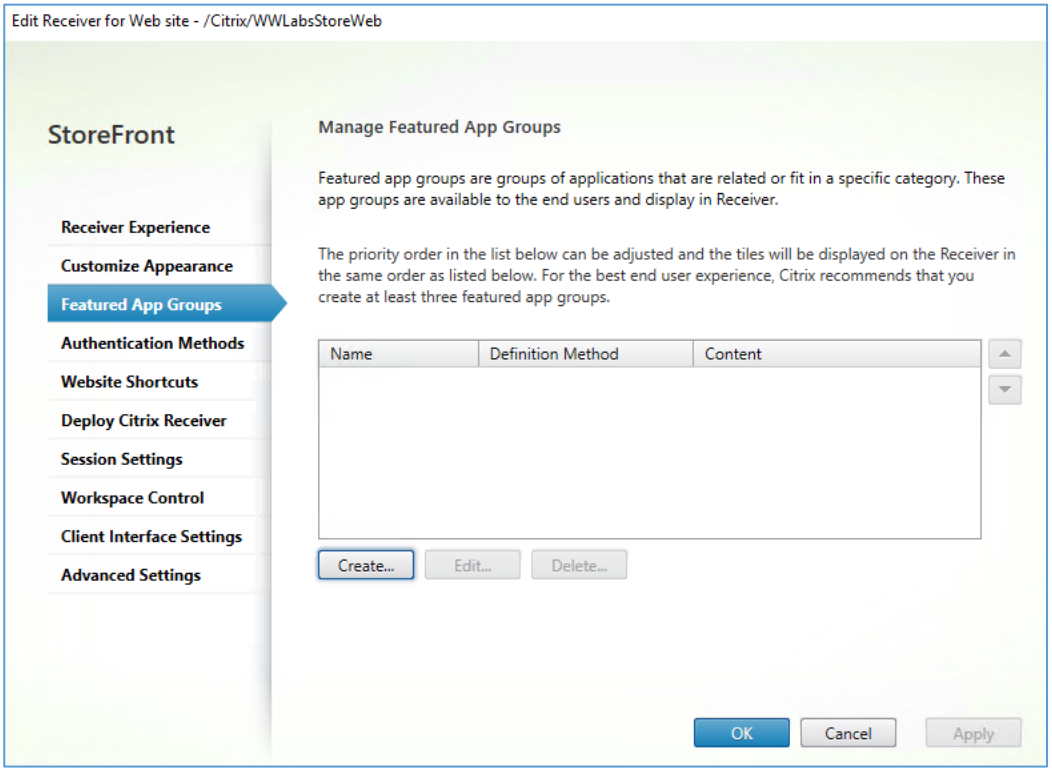
Scenario:

Published Apps can be bundled together and presented to users as a featured app group.
Your task is to configure Featured App Groups and App Categories.

Step	Action
1.	Using the Remote Desktop Connection Manager, connect to NYC-STF-001. To log on to NYC-STF-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1
2.	Verify the **Citrix StoreFront** console is still open. In the left pane, select **Stores**. In the middle pane select **WWLabsStore** and under WWLabsStore on the right select **Manage Receiver for Web Sites**. 
3.	Click **Configure** on Manage Receiver for Web Sites – WWLabsStore page.

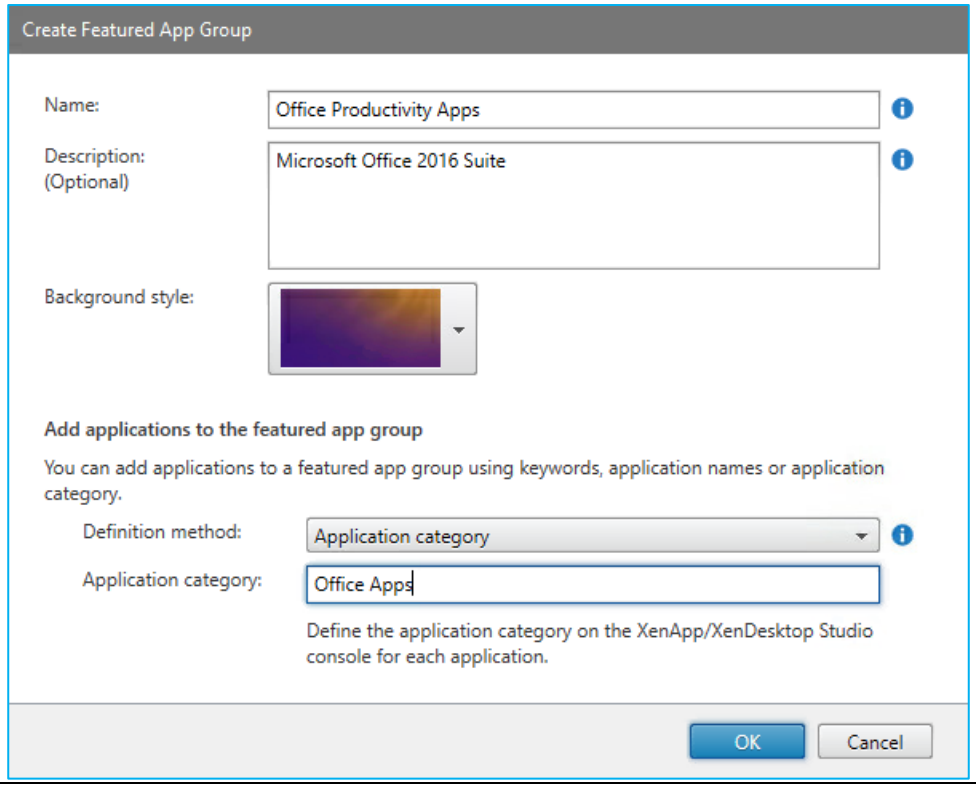


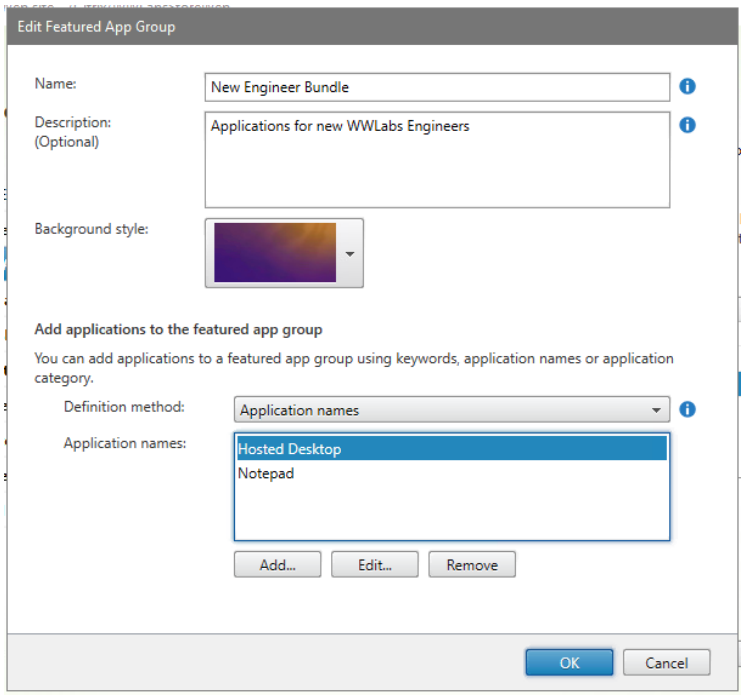
4. Select **Featured App Group** on the left menu and you will now see a blank box where your Featured App Group configurations can be added.

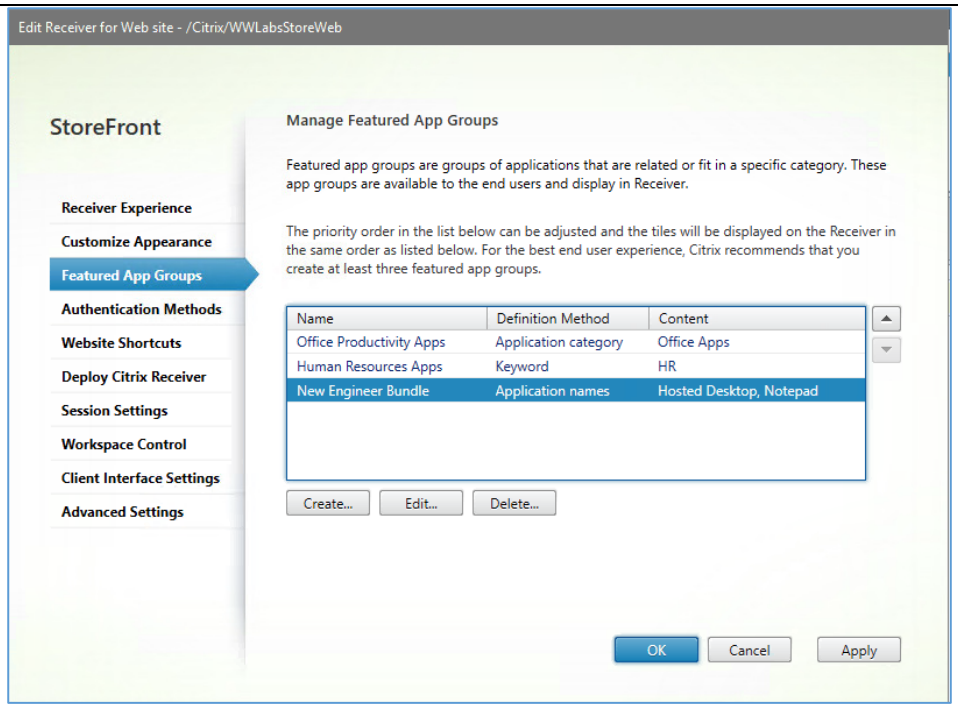


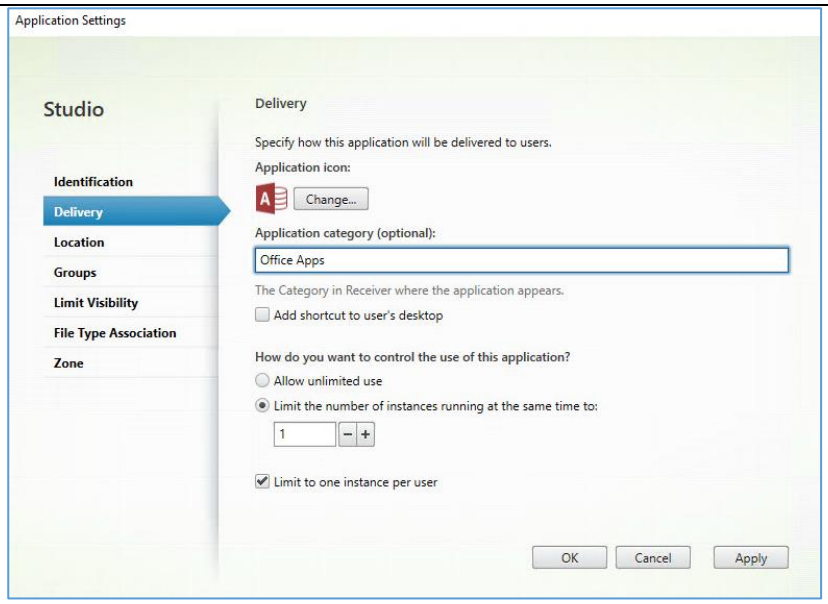
Click **Create** to begin configuring Featured App Groups and then enter the following:

- Name: **Office Productivity Apps**
- Description: **Microsoft Office 2016 Suite**
- Definition method: **Application category**

	Note: There are three options available when defining a Featured App Group: • **Keywords**: Adds apps with a matching keyword. Use Citrix Studio to add keywords to the description field of an application. • **Application names**: Includes apps with a matching name. Wildcards not supported. The match is not case-sensitive, but it does match whole words. For example, excel would match Microsoft Excel 2016, but Exc would not result in a match. • **Application categories**: Matches the application category defined within Citrix Studio. Type **Office Apps** for the Application category and click **OK**. 
5.	Create two additional featured app groups, one for the HR department and one for new employees. Click **Create** to configure the next Featured App Group. Complete the following fields: • Name: **Human Resources Apps** • Description: **Recommended applications for HR employees** • Definition method: **Keyword** • Keyword: **HR** Click **OK**. Click **Create** to configure the next Featured App Group. Complete the following fields: • Name: **New Engineer Bundle** • Description: **Applications for new WWLabs Engineers** • Definition Method**: Application names**

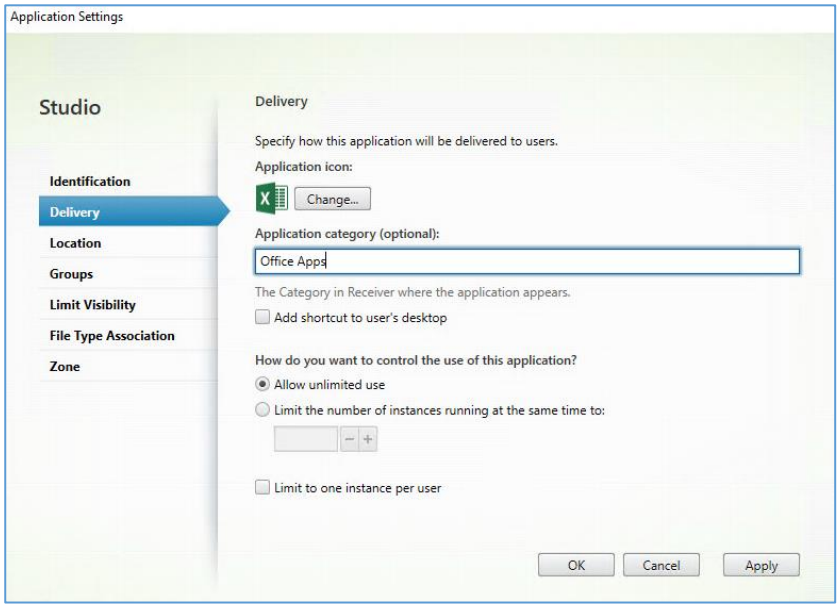
	Click **Add**. In the Application name field, enter **Hosted Desktop** and click **OK**. Click **Add**. In the Application name field, enter **Notepad** and click **OK**. On the Create Featured App Group dialog box, click **OK**. Click **OK**.  **Note:** Make sure to enter the apps for New Engineer Bundle as separate entries. Do not enter a single list separated by commas. Verify the three below Featured App Groups are listed and match the screen shot below:

	 Click **OK** and then click **Close**.
6.	To complete this task, you need to define the Office apps group using categories and the HR app group using keywords in Studio.
7.	Using the Remote Desktop Connection Manager, switch to **NYC-XDC-001**. **Note:** In a previous exercise, you had logged on to NYC-XDC-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-XDC-001 by right-clicking this machine and selecting Connect server.
8.	Using Studio, expand **Citrix Studio (SITE-NewYork)** and click **Applications**. On the center pane, right-click **Access 2016** and select **Properties**. Click **Delivery** on the left menu. Type **Office Apps** in the Application category field.



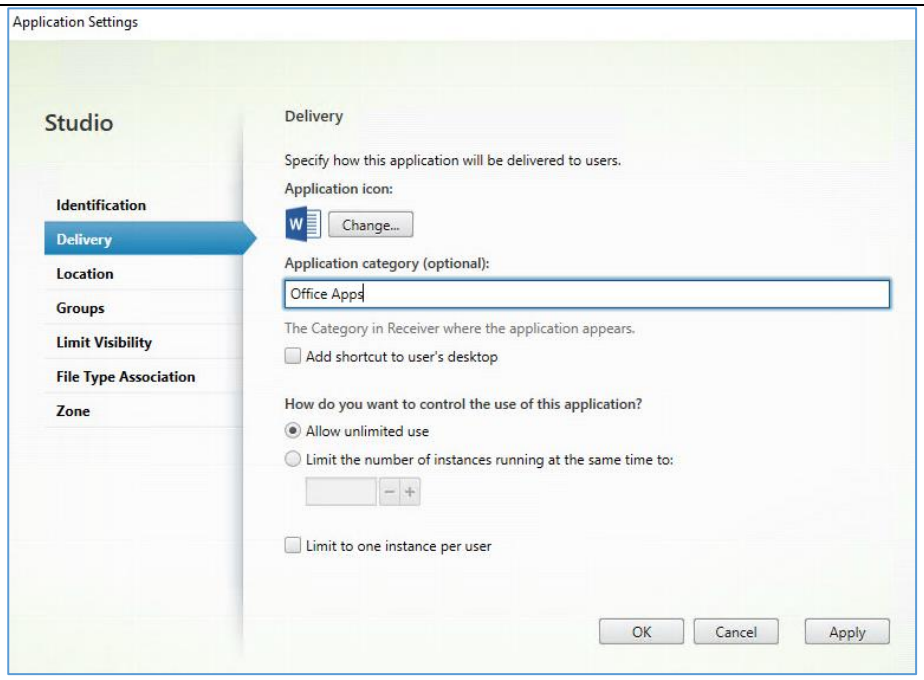
Click **Apply** and then click **OK**.

Select **Excel 2016** and then **Properties** from the Actions pane. Click **Delivery** on the left menu. Type **Office Apps** in the Application category field.



Click **Apply** and then click **OK**.

Select **Word 2016** and then **Properties** from the Actions pane. Click **Delivery** on the left menu. Type **Office Apps** in the Application category field.

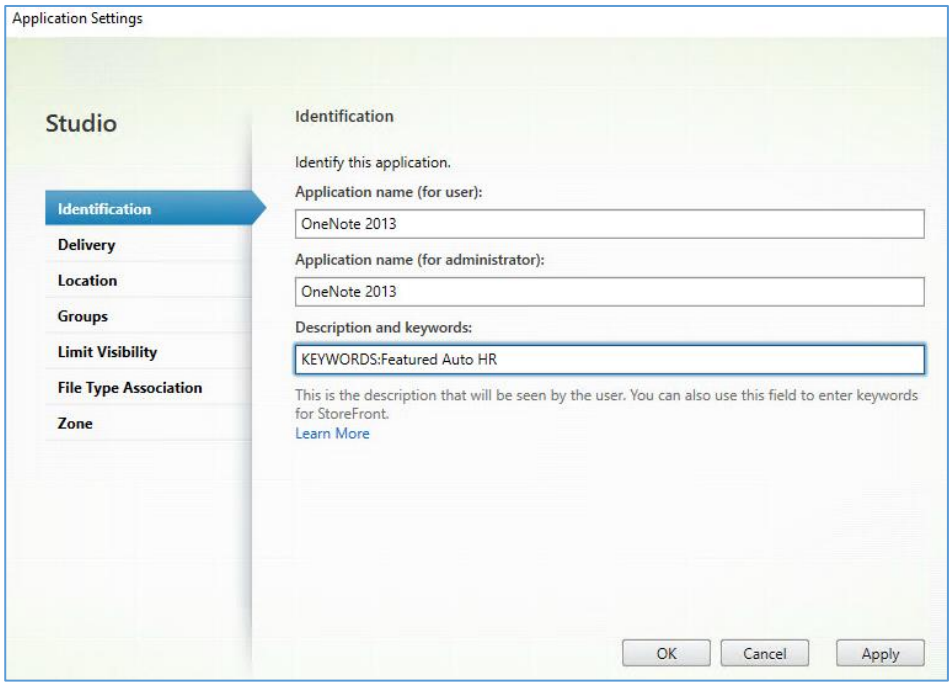


Click **Apply** and then click **OK**.

Note: Studio was started in a previous exercise. If Studio was closed in a previous exercise, then click Start > Citrix > Citrix Studio.

9. Select **OneNote 2016** and then **Properties** from the Actions pane. Click **Identification** on the left menu.

In the Description and keywords field, add **HR** to the keywords section. The line will now read: **KEYWORDS:Featured Auto HR**



	Click **Apply** and then click **OK**. **Note**: OneNote was not configured with an application category, but rather with a keyword.

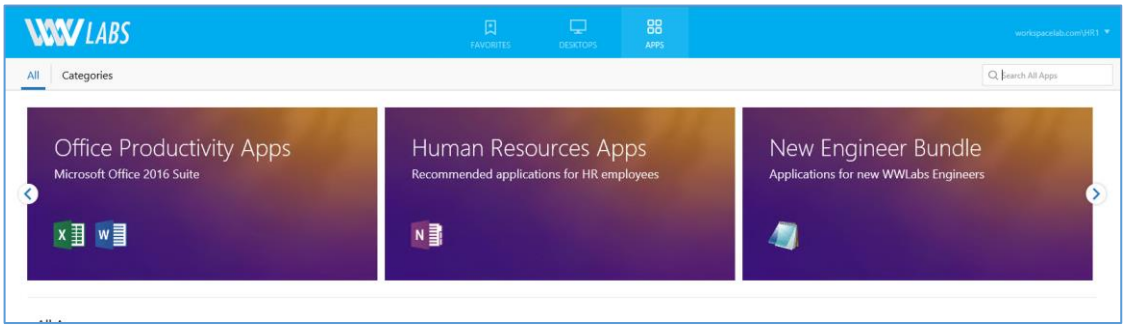
Key Takeaways:

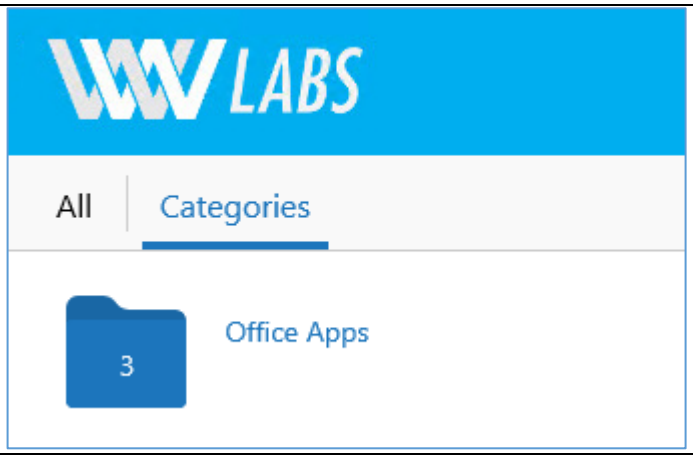
- Use application groups to give users easy access to application bundles.
- Applications can be grouped by keywords, category or by application name.
- Keywords can be any custom word defined after KEYWORDS in the Published Resource properties.

Exercise 7-8: Test the App Group and App Categories

Scenario:

Your task is to test the App Group and App Categories just configured to identify the change in the user experience when accessing resources.

Step	Action
1.	Using the Remote Desktop Connection Manager, switch to **NYC-WRK-001**. **Note:** In a previous exercise, you had logged on to NYC-WRK-001 using the following credentials to make the connection: • User name: Workspacelab\HR1 • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-WRK-001 by right-clicking this machine and selecting Connect server.
2.	Launch **Internet Explorer** and navigate to **https://storefront.workspacelab.com**. Log on with the following credentials: • User name: **HR1** • Password: **Password1**
3.	Click on the **APPS** view to review the Featured App Groups.  Then, click the **Categories** tab to view the Office Apps Folder.

	
4.	Log off the Receiver Store. Click **HR1** and **Log Off**.

Key Takeaways:

- Featured App Groups are highlighted at the top of Receiver under the APPS section; use the arrows to scroll between the different groups.
- The Categories are displayed above Featured Apps; the same categories are used to create a folder structure when using Citrix Receiver for desktop and start menu shortcuts.

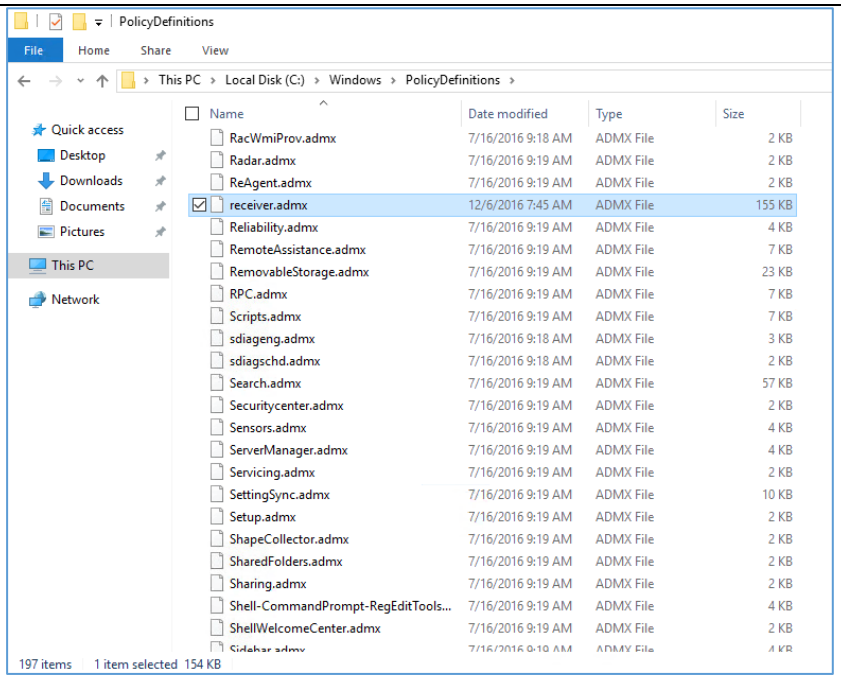
Exercise 7-9: Configure Shortcut Placement

Scenario:

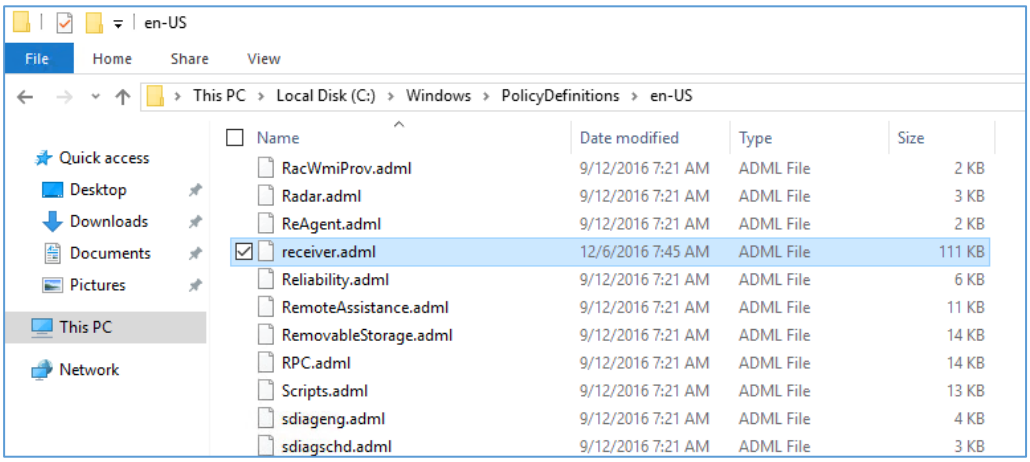
Your Citrix Lead Architect has explained that for some use case scenarios within WW Labs, it is expected that users launch their company apps from the Start Menu or the Desktop.

Your task is to create a Group Policy Object (GPO) to configure the Receiver's feature for managing subscribed application shortcuts on the Start Menu and Desktop.

Step	Action
1.	Using the Remote Desktop Connection Manager, switch back to **NYC-XDC-001**. **Note:** In a previous exercise, you had logged on to NYC-XDC-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-XDC-001 by right-clicking this machine and selecting Connect server.
2.	In order to configure shortcut placement, you will need to copy two configuration files into **Windows policy definitions** so they can be available in the Group Policy Management tool. From the Desktop of NYC-XDC-001 double-click the **Lab Resources** folder and open the **Receiver_ADMX_Files** folder. Copy **receiver.admx** and paste it inside the folder **C:\Windows\PolicyDefinitions**.



Copy **receiver.adml** and paste it inside the folder **C:\Windows\PolicyDefinitions\en-US**.

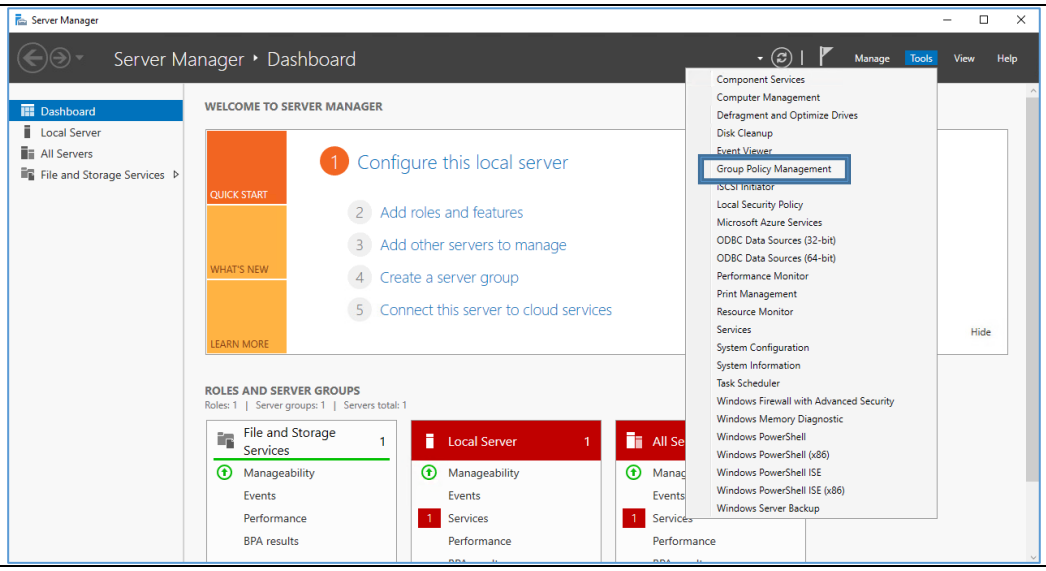
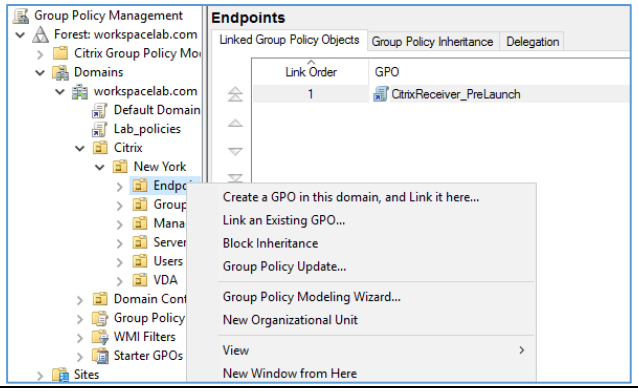


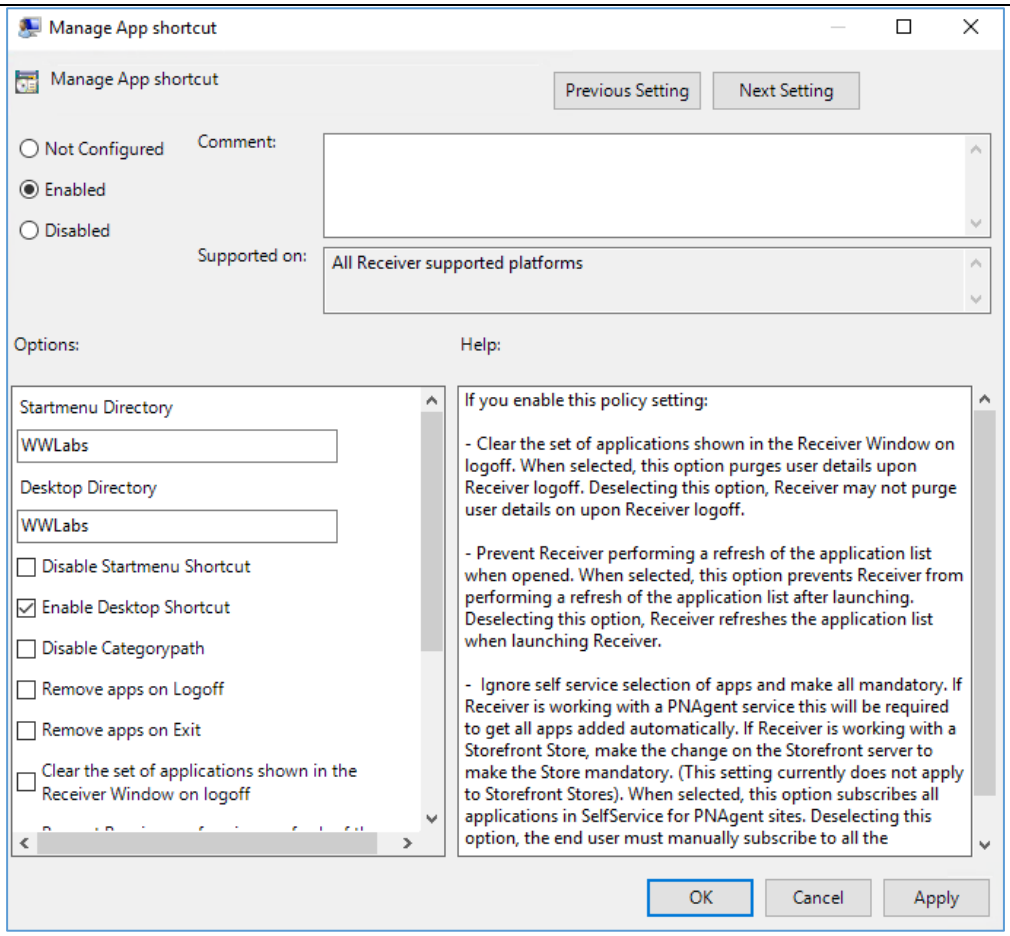
Note: The Receiver ADMX file is available in the C:\Program Files\Citrix\ICA Client\Configuration folder of a Windows machine with Citrix Receiver installed. Remember there are two files and two file locations to address in this step.

3. Launch the Group Policy Management Console.

   Click **Start > Server Manager**. Wait for the Server Manager to launch.

   Click **Tools** and click **Group Policy Management** to launch the Group Policy Management Console (GPMC).

	
4.	Expand **Forest: workspacelab.com** > **Domains** > **workspacelab.com** > **Citrix** > **New York** > **Endpoints**. Right-click the **Endpoints** OU and select **Create a GPO in this domain, and Link it here**. 
5.	In the New GPO dialog box, enter **CitrixPolicy ReceiverShortcuts** in the name field and click **OK**.
6.	Right-click the **CitrixPolicy ReceiverShortcuts** GPO and select **Edit**.
7.	Using the Group Policy Management Editor window navigate to **Computer Configuration** > **Policies** > **Administrative Templates** > **Citrix Receiver** > **SelfService**. Double-click **Manage App shortcut** and configure the setting as **Enabled**. Configure the following options: • Startmenu Directory: **WWLabs** • Desktop Directory: **WWLabs** • Enable Desktop Shortcut: **Enabled**



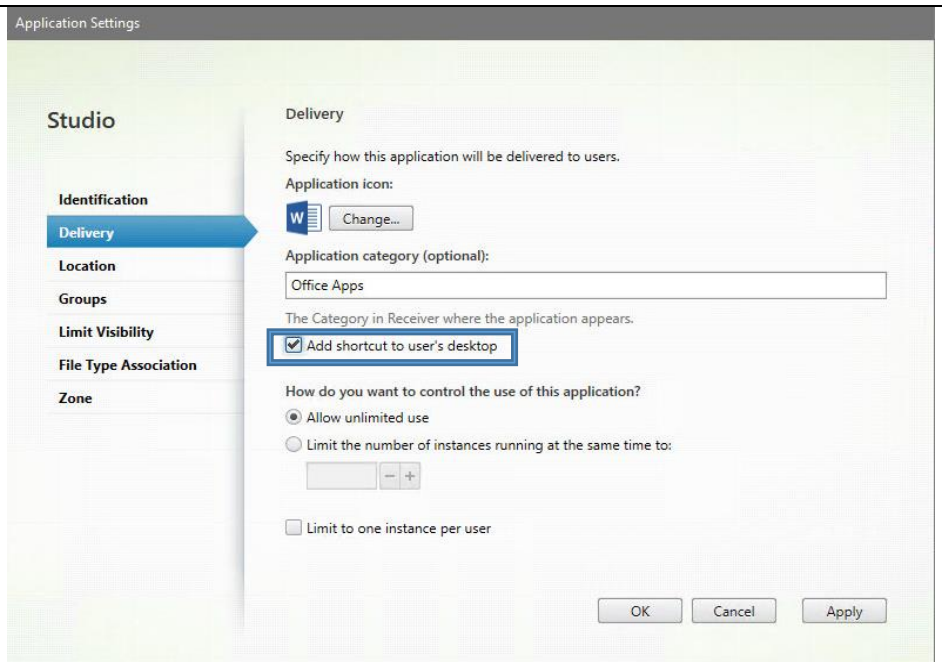
Click **Apply** and **OK**. Close the **Group Policy Management Editor**.

Note: Using a Citrix policy is one method to control shortcut behavior. You can also modify shortcut behavior under the Properties of the application in Studio, by enabling the Add shortcut to user's desktop option under the Delivery tab.

You can create sub-folders for the shortcuts by updating the Application Category field within the Delivery tab of the application within Studio.

8. Using Citrix Studio, navigate to Applications, right-click **Word 2016** and select **Properties**.

   On the left side select **Delivery**, on the right side enable **Add shortcut to user's desktop**.

	 Click **Apply** and then click **OK**.

Key Takeaways:

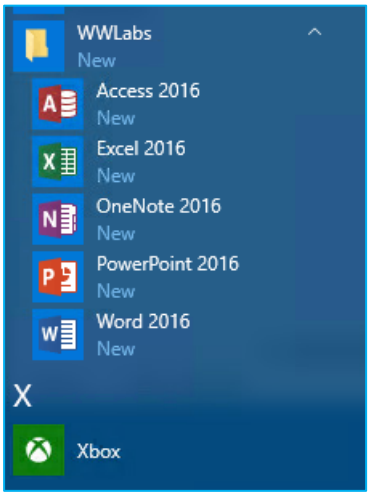
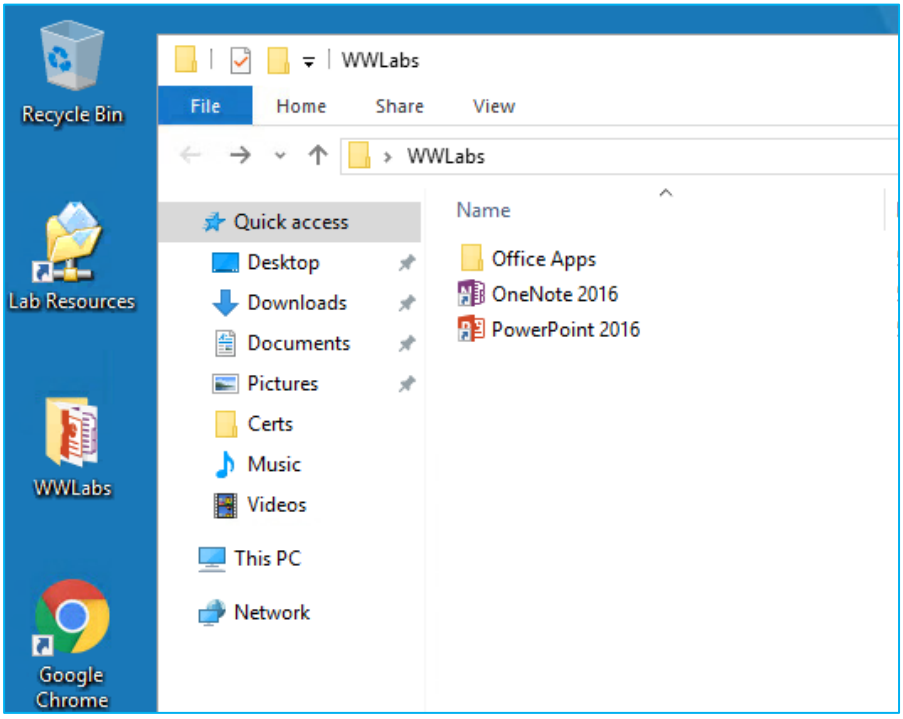
- You can manage Receiver Desktop and Start Menu application shortcut placements by using Group policies with the Receiver ADMX template.

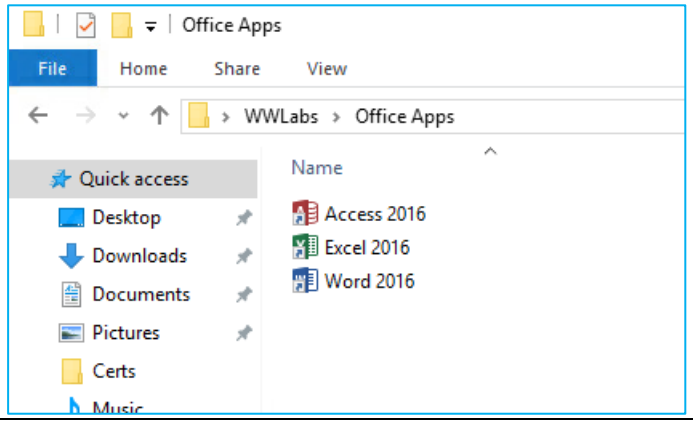
Exercise 7-10: Test Shortcut Placement

Scenario:

Your task is to verify your previous shortcut configurations by logging on and verifying the shortcuts.

Step	Action
1.	Using the Remote Desktop Connection Manager, connect to NYC-WRK-001. To log on to NYC-WRK-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\HR1 • Password: Password1
2.	In the bottom right of the screen, right-click the **Citrix Receiver** icon and select **Exit**.
3.	Right-click **Start**, select **Command Prompt** to launch a command prompt. Enter the following command: **gpupdate /force** Close the **Command Prompt** after the command has completed successfully.
4.	Click **Start** and launch **Citrix Receiver**. Log on with the following credentials: • User name: **HR1** • Password: **Password1**

	Notice the **WWLabs** shortcut folder that appears on the Desktop and in the Start Menu. **Note:** In the event that the applications fail to show up, and you have confirmed the GPO settings are correct, try to reboot NYC-WRK-001. If this does not help, re-install Citrix Receiver using the Administrator account.
5.	Click **Start** > **All apps** on **NYC-WRK-001**, and select the **WWLabs** folder to view the application shortcuts.  Double-click the **WWLabs** folder on the desktop to view the application shortcuts.  **Note**: When the self-service mode is enabled, the applications that a user is subscribed to are placed in the shortcuts folder.

6.	To verify you can launch a published resource from a shortcut placement, test launch an application. In the **WWLabs > Office Apps** folder on the Desktop, double-click **Word 2016** to launch the application. 
7.	Close **Word 2016**. Log off the Store. Click **HR1** and **Log Off**. Log off NYC-WRK-001. To log off, right-click **Start** > choose **Shut down or sign out** > and click **Sign out**.

Key Takeaways:

- Citrix Receiver will create the folders specified and load shortcuts for all subscribed resources at launch time.
- Citrix recommends setting the policy to delete shortcuts at logoff to create a more dynamic user experience.

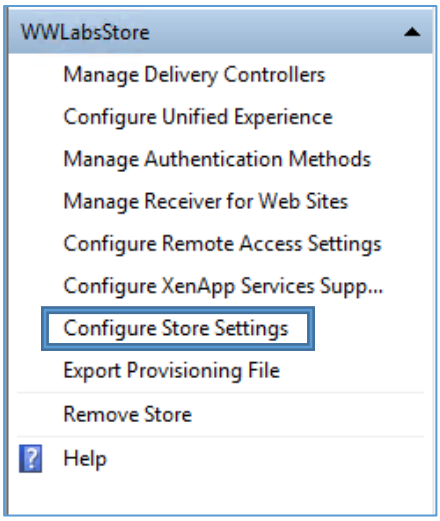
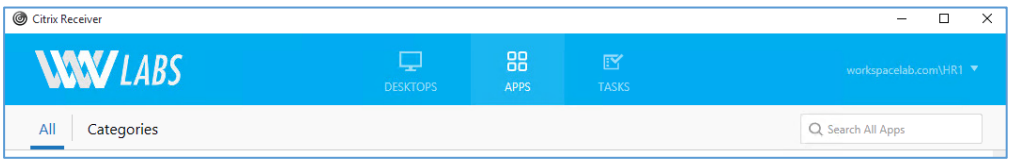
Exercise 7-11: Disable Self-Service Mode and Test

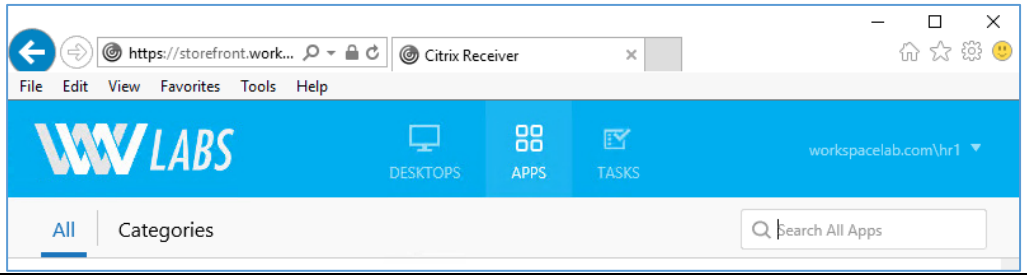
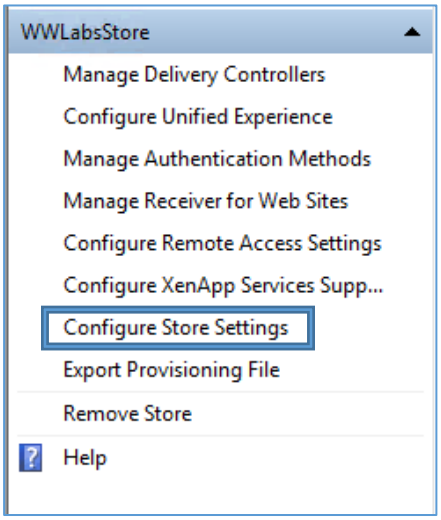
Scenario:

In some situations, it may be preferable to disable the favorites menu within Receiver.

Your task is to disable the favorites menu within Receiver by disabling User Subscriptions.

Step	Action
1.	Using the Remote Desktop Connection Manager, connect to **NYC-STF-001**. **Note:** In a previous exercise, you had logged on to NYC-STF-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-STF-001 by right-clicking this machine and selecting Connect server.
2.	Confirm the **Citrix StoreFront** Management Console is still open.

	Note: If the Citrix StoreFront Management Console was closed in a previous exercise, click Start > Citrix > Citrix Storefront to launch the Citrix StoreFront Management Console. Select the **Stores** node, and then verify **WWLabsStore** is selected. Then, select **Configure Store Settings** under WWLabsStore.  On Manage User Subscriptions select **Disable User Subscriptions (Mandatory Store)** and click **OK**.
3.	Using the Remote Desktop Connection Manager, connect to NYC-WRK-001. To log on to NYC-WRK-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\HR1 • Password: Password1
4.	Right-click the **Citrix Receiver** icon in the system tray and select **Exit**. Click **Start** and launch **Citrix Receiver**. Log on with the following credentials: • User name: **HR1** • Password: **Password1** Notice that the **FAVORITES** view is removed.  Log off Citrix Receiver. Click **HR1** and **Log Off**. Close **Citrix Receiver**.

5.	Launch **Internet Explorer** and navigate to **https://storefront.workspacelab.com**. Log on to the store page using the following credentials: • User name: **HR1** • Password: **Password1**
6.	Notice that the **FAVORITES** view is removed. 
7.	Using the Remote Desktop Connection Manager, switch back to **NYC-STF-001**. **Note:** In a previous exercise, you had logged on to NYC-STF-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-STF-001 by right-clicking this machine and selecting Connect server.
8.	Return to the **Citrix StoreFront** Management Console. Select the **Stores** node, and then verify **WWLabsStore** is selected. Then, select **Configure Store Settings** under WWLabsStore.  On Manage User Subscriptions select **Enable User Subscriptions (Self Service Store)** and click **OK**.

Key Takeaways:

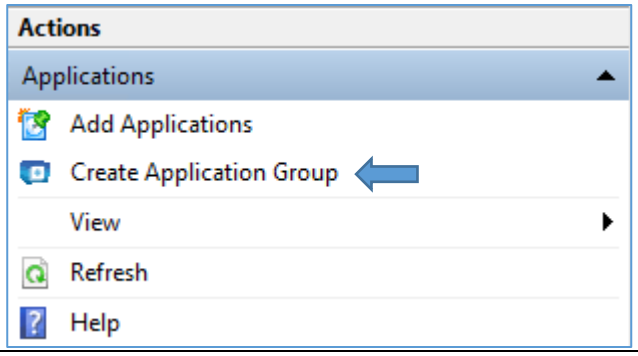
- The Self-Service feature is great when administrators wish to simplify the user experience and allow users to select only the specific applications they need; however, this approach works best when using Citrix Receiver as the launch interface.

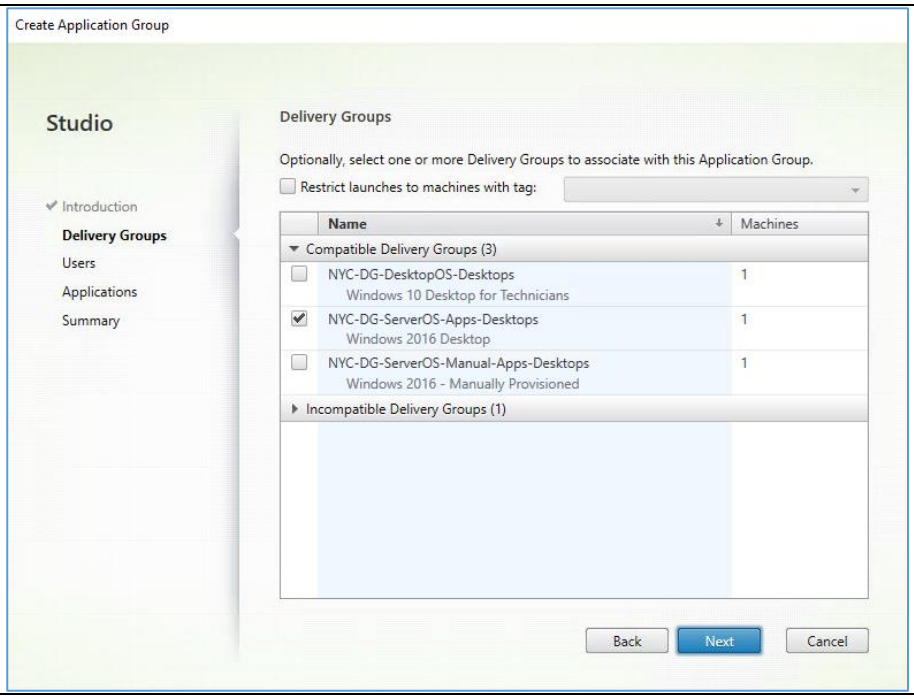
- Disabling User Subscriptions will remove the favorites item in Receiver and make the APPS view default.
- When you disable subscriptions, StoreFront will stop filtering the resources and users will see all available applications when they connect to the store. Their previous subscriptions however, are not deleted in the database and users can recover them if you re-enable the feature.

Exercise 7-12: Create and Test Application Group

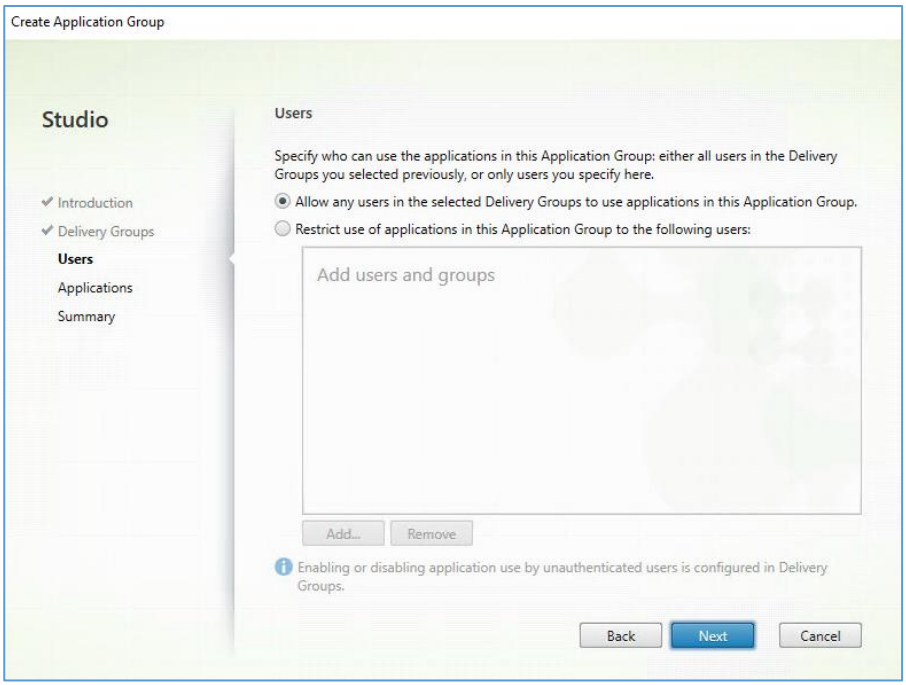
Scenario:

Your lead Citrix admin has tasked you to investigate the new Application Group feature. This feature allows for applications from multiple Delivery Groups to be tied together as one administrative entity. For now, you will only use applications from a single Delivery Group.

Step	Action
1.	Using the Remote Desktop Connection Manager, connect to **NYC-XDC-001**. **Note:** In a previous exercise, you had logged on to NYC-XDC-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-XDC-001 by right-clicking this machine and selecting Connect server.
2.	Click **Start** > **Citrix** > **Citrix Studio** to launch **Citrix Studio**.
3.	From the left pane select **Applications** and from the Actions pane on the right-click **Create Application Group**. 
4.	Click **Next** on the Introduction page.
5.	Select **NYC-DG-ServerOS-Apps-Desktops** and click **Next**.



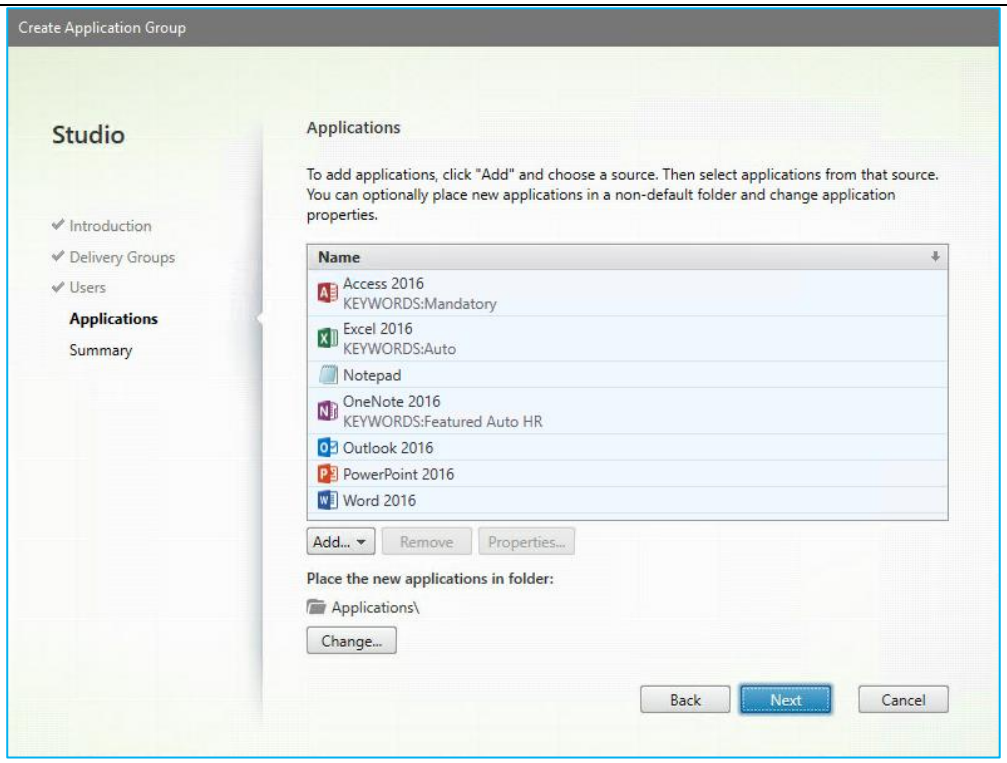
6. On the Users page, leave defaults and click **Next**.



Note: Any users configured in this Delivery Group will be able to access applications provided by the Application Group, by selecting the above option.

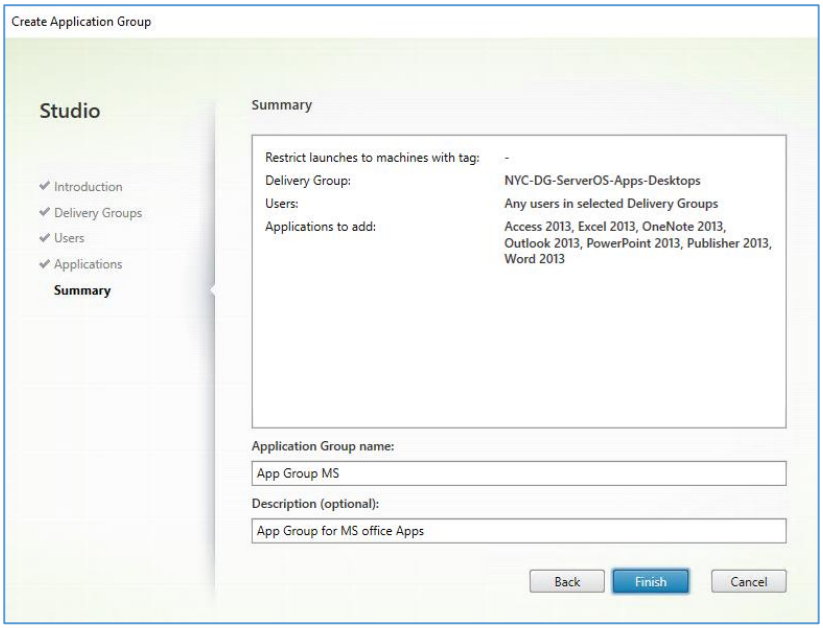
7. On Applications page, click on the **Add** drop-down and select **Existing**.

   Wait for the applications to enumerate. Select all **Microsoft Office applications** and **Notepad,** then click **OK**.



Click **Next**.

8. On Summary page type the following information:
   - Application Group name: **App Group MS Office**
   - Description (optional): **App Group for MS Office Apps**



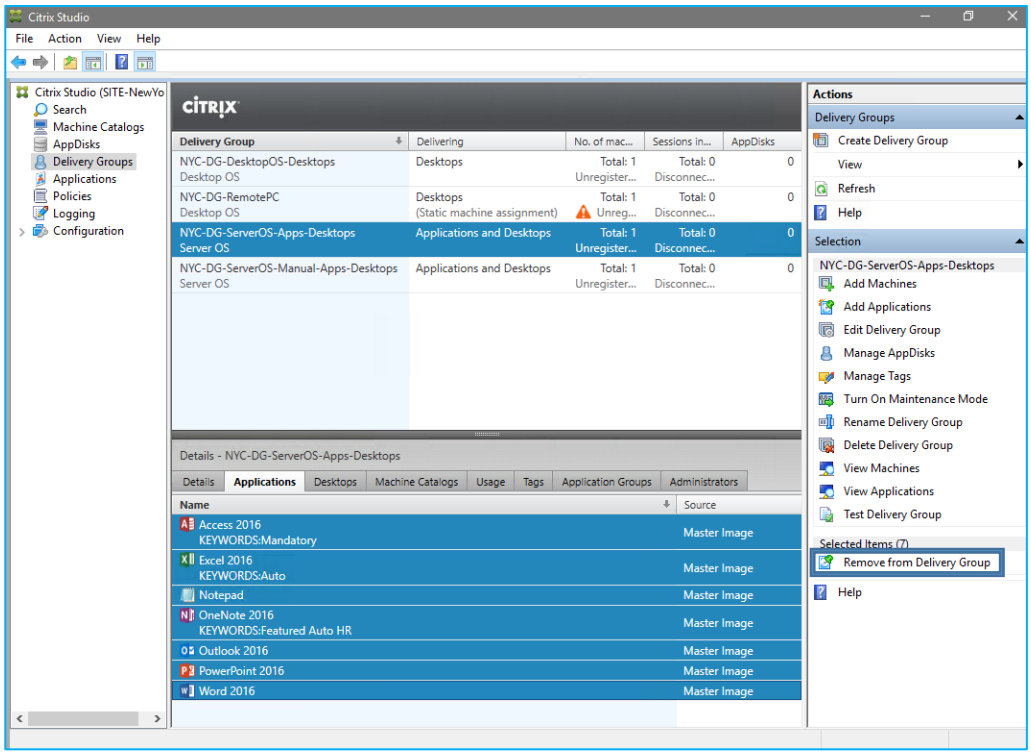
Click **Finish**.

9. It is recommended to publish applications from either Application Groups or Delivery Groups, so we will remove all Microsoft Office applications from the Delivery Group.

From the left pane, select **Delivery Groups** and in the middle pane click on **NYC-DG-ServerOS-Apps-Desktops**.

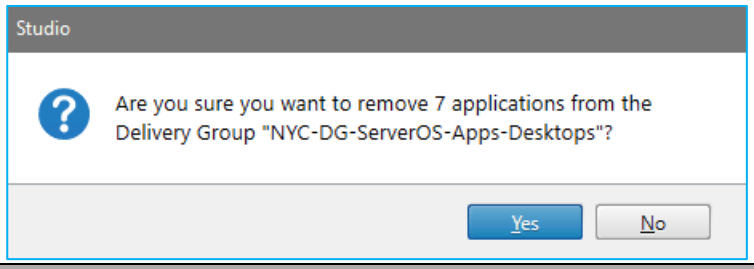
In the lower middle pane, select the **Applications** tab and select all **7** applications.

On the Actions pane under selection, select **Remove from Delivery Group**.



Note: For multiple selection, press the Ctrl Key and select each app one by one.

10. When prompted for confirmation click **Yes**.



Test Application Launch of App Group Applications

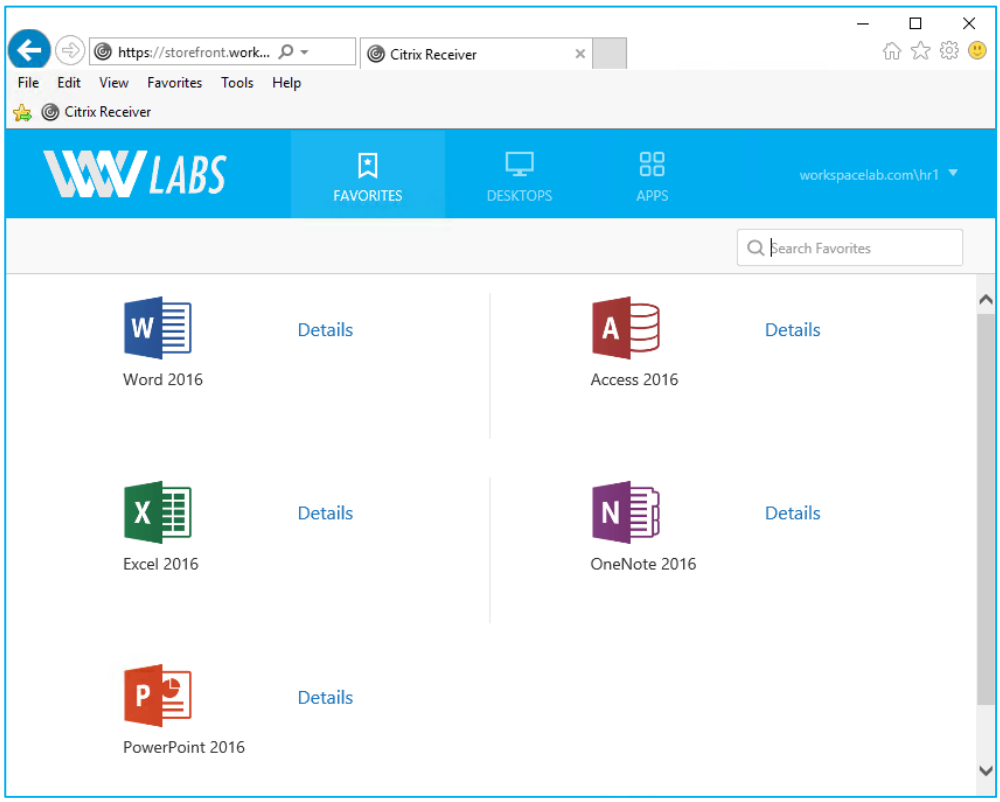
11. Using the Remote Desktop Connection Manager, switch to **NYC-WRK-001**.

Note: In a previous exercise, you had logged on to NYC-WRK-001 using the following credentials to make the connection:

- User name: Workspacelab\Administrator
- Password: Password1

Note: If your Remote Desktop Connection session disconnected, log on to NYC-WRK-001 by right-clicking this machine and selecting **Connect server**.

12. Launch **Internet Explorer** and navigate to **https://storefront.workspacelab.com**.

	Log on with the following credentials: • User name: **HR1** • Password: **Password1**
13.	The Microsoft Office applications are still present under **FAVORITES**.  This verifies all application properties and keywords are intact and applications have been successfully moved from a Delivery Group to Application Groups.
14.	Log off the Receiver for Web. Click **HR1** and **Log Off**.

Key Takeaways:

- Application Groups consists of three elements: applications from one or more Delivery Groups, users that can access the applications and settings that apply to the Application Group.
- When adding applications from multiple Delivery Groups we can load balance the users across those different Delivery Groups or we can assign priority to prefer a specific Delivery Group for a set of users.
- Citrix recommends using either Delivery Groups or Application Groups, avoiding using both since this may lead to unnecessary complexity and administrative overhead.

Module 8: Printing with XenApp and XenDesktop

Overview:

This module presents the basic concepts of printing in a XenApp and XenDesktop environment.

Before you begin:

Estimated time to complete Module 8 lab exercises: 65 minutes

Exercise 8-1: Configure Printer Auto Creation

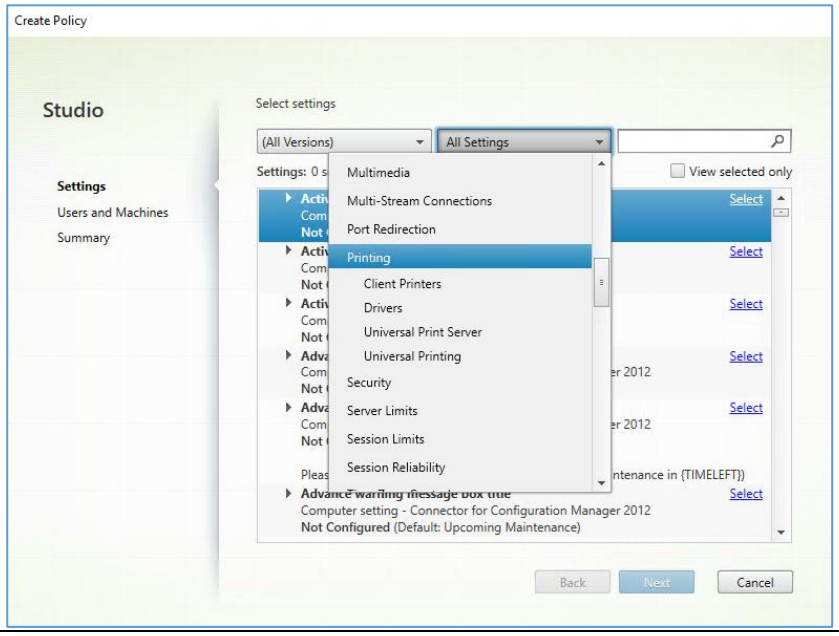
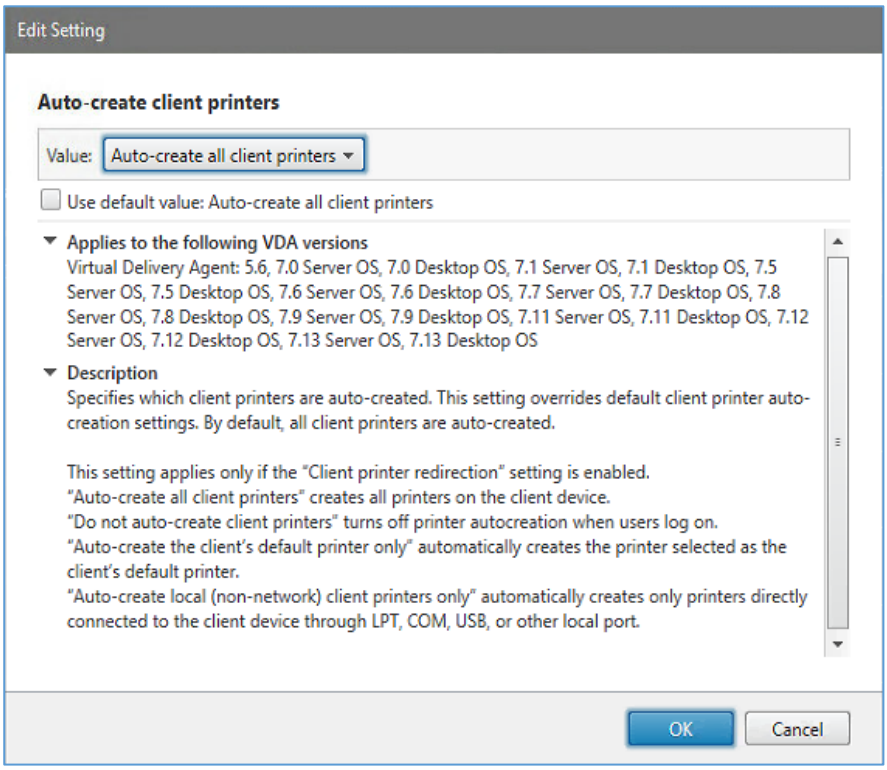
Scenario:

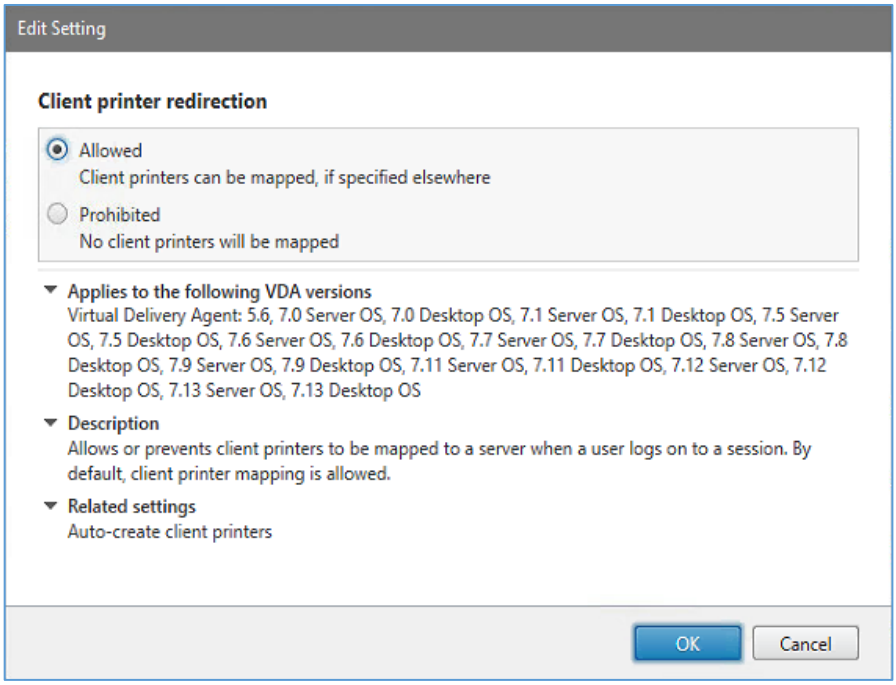
The default Auto-Creation policy is to auto-create all printers mapped and attached to the endpoint device that the user is using to make an HDX connection to a resource session.

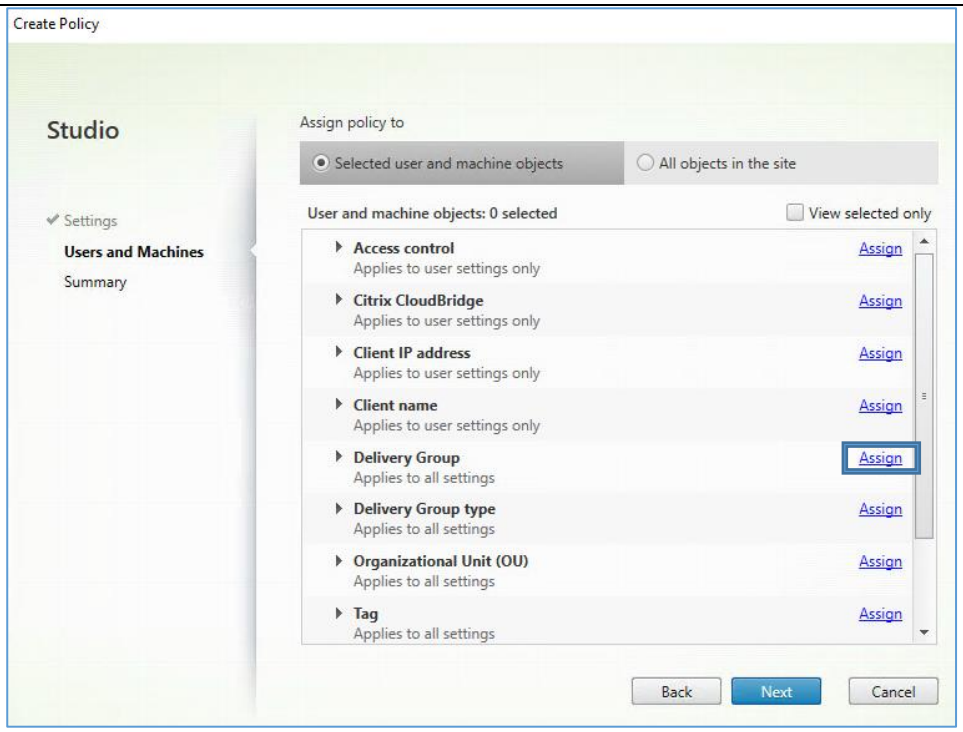
WW Labs new written policy enforces users to have limited printing sources to cut down on printing supplies overhead. Additionally, your Lead Citrix Architect has reinforced this written policy to address performance, because the fewer printers created during the session start up, the faster the session starts.

Your task is to configure the Auto-Creation policy to minimize the number of printers created during session start up for a user to only create the default printer in the session to free up resources on the VDA, and speed up logon duration.

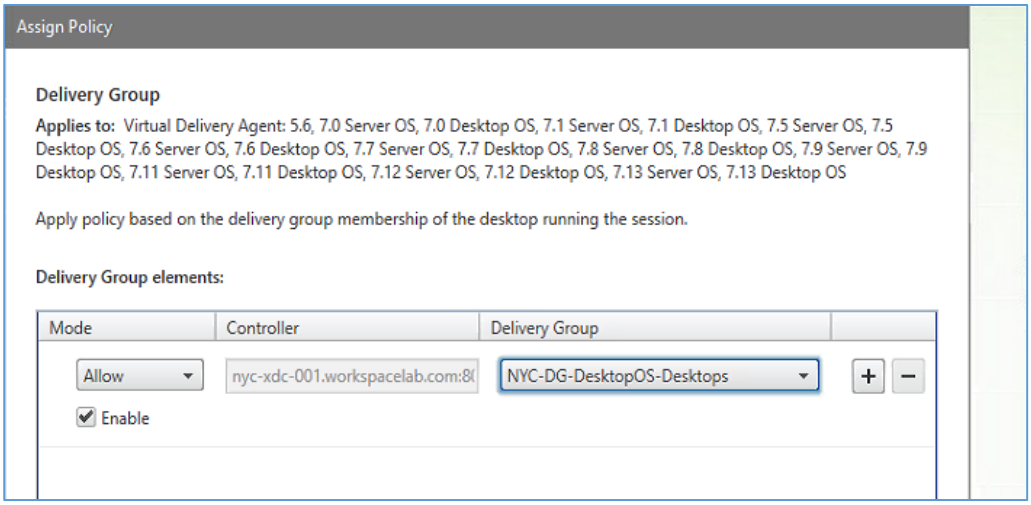
Step	Action
1.	The following VMs are required before beginning the exercises for this Module; all others may be powered down. To power manage your VMs, switch to XenCenter, right-click on the VM in the left pane and select Start or Shut Down. If prompted click Yes. • NYC-ADS-001 • NYC-SQL-001 • NYC-FSR-001 • NYC-XDC-001 • NYC-STF-001 • NYC-MAN-001 • NYC-SRV-001 • NYC-DTP-001 • NYC-WRK-001 **Note**: These above VMs are listed in the start-up order.
2.	Using the Remote Desktop Connection Manager, connect to NYC-XDC-001. To log on to NYC-XDC-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1
3.	Using Studio, expand **Citrix Studio (SITE-NewYork)** and click **Policies**. On the right pane, click **Create Policy**.

	Note: Studio was started in a previous exercise. If Studio was closed in a previous exercise, then click **Start** > **Citrix** > **Citrix Studio**.
4.	On the Settings page, in the All Settings drop-down, select **Printing** (under ICA heading). 
5.	Scroll down to the **Auto-create client printers** setting, and click **Select** for this setting. Verify the **Auto-create all client printers** option is selected as the Value.  Click **OK**.

6.	Locate the **Client printer redirection** setting, and next to this setting click **Select**. Leave the default setting of **Allowed**.  Click **OK** and click **Next**. **Note**: By not changing any settings, you are still making a change by selecting to include this setting in the new policy.
7.	On the Users and Machines page, for the Assign policy to option, select **Assign** next to **Delivery Group**.

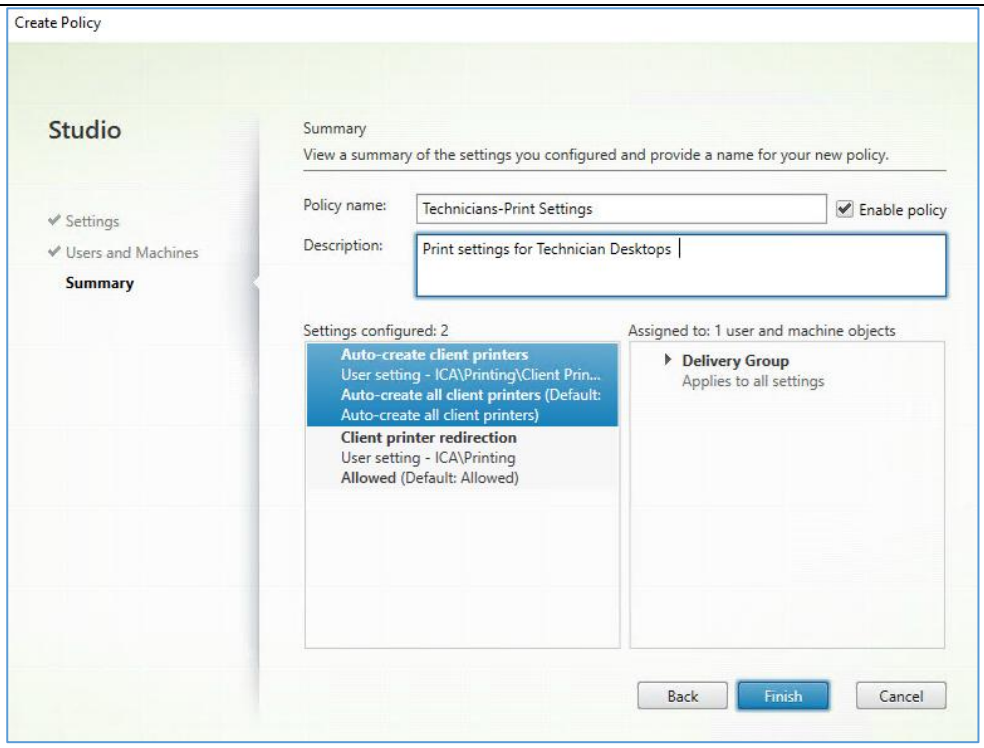


In the Assign Policy menu, select **NYC-DG-DesktopOS-Desktops** in the Delivery Group drop-down menu and click **OK**.



Click **Next**.

8. On the Summary page, enter the following information:
   - Policy name: **Technicians-Print Settings**
   - Description: **Print settings for Technician Desktops**

	 Click **Finish**.

Key Takeaways:

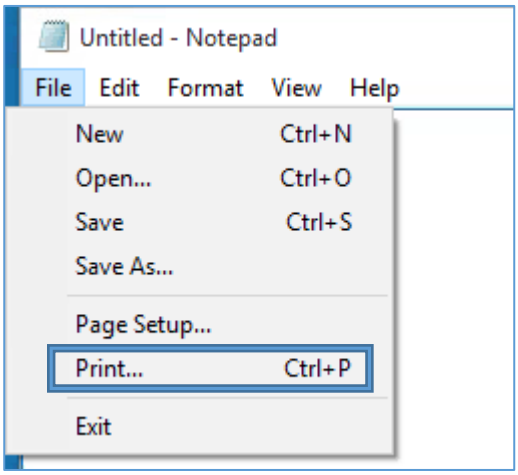
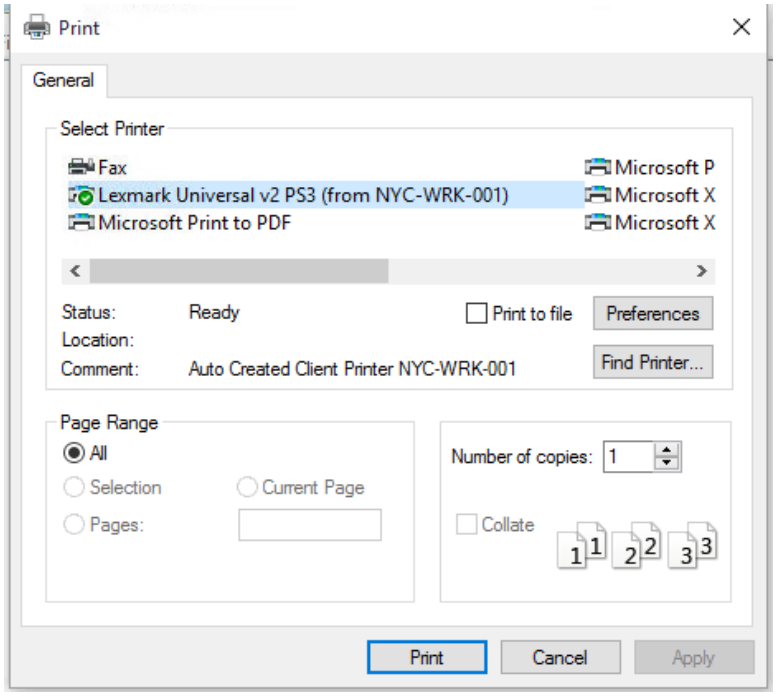
- For most client scenarios, having the default printer available in a session is sufficient – define exceptions to this policy when needed.
- This method of mapping printers is referred to as Client Print, because the print will flow from the VDA to the client endpoint device, and then to the printer device.

Exercise 8-2: Test that Auto Creation was Successful

Scenario:

Your task is to verify the previously configured Auto-Creation policy was successful in auto-creating only the endpoint's default printer. To verify that the printer in the session is auto-created, look at the name of the printer, which should include both a session number and the name of the endpoint PC.

Step	Action
1.	Using the Remote Desktop Connection Manager, connect to NYC-WRK-001. To log on to NYC-WRK-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\HR1 • Password: Password1
2.	Click **Start** and launch **Citrix Receiver**. Log on with the following credentials: • User name: **Technician1** • Password: **Password1**

	Select the **DESKTOPS** tab and launch **Technician Desktop**. **Note**: If Technician Desktop does not appear automatically, you may need to select Refresh Apps from the Citrix Receiver menu. If the Desktop fails to launch, switch to XenCenter and reboot NYC-DTP-001. **Note**: There may be several windows that open, triggered by the logon to the Technician Desktop, such as a *Setting up your apps* welcome screen and / or a Receiver Add Account screen. It may take a few minutes for the *Setting up your apps* window to disappear.
3.	Click the **Start menu**, and then type **Notepad**. Click **Notepad** from the list to open it.
4.	In Notepad, click **File** > **Print**. 
5.	In the **Print** dialog box, review the printers that appear.  The policy setting is applying and therefore only auto-creating the user's default printer.
6.	On the Print dialog box, click **Cancel**.

	Close **Notepad**, and log off **Technician Desktop**. Log off Citrix Receiver. Click **Technician1** and **Log Off**. **Close** the Receiver window.

Key Takeaways:

- The default printer from the endpoint connects through the HDX channel to the user's session.
- Every subsequent connection, or reconnection, will initiate a mapping of the default printer on the endpoint device, allowing users to change their printer inside the session by specifying a new default printer.

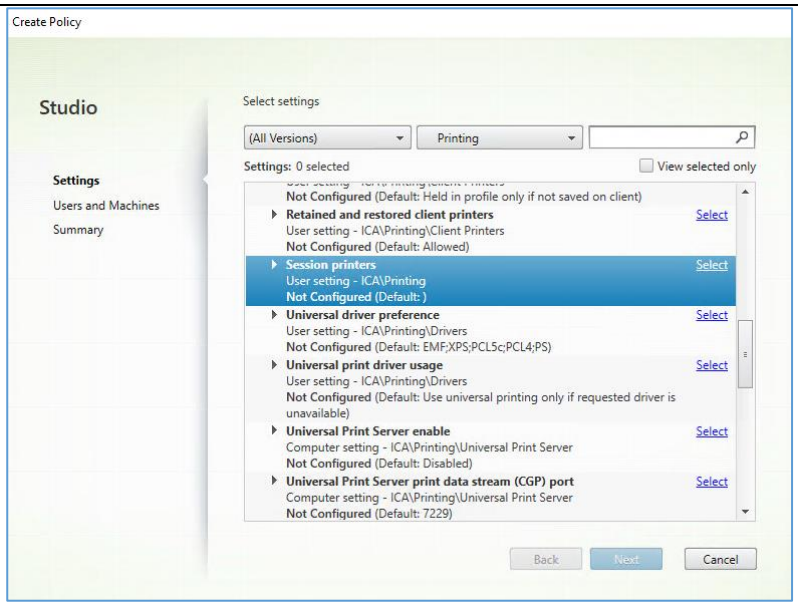
Exercise 8-3: Configure Session Printers

Scenario:

Your Citrix Lead Architect has informed the Citrix Administrator team that users will need to print from Citrix Sessions to mapped printers managed by print servers.

Your task is to ensure users receive different printers, depending on which floor of the building they connect to the sessions from. You have decided to use the Session Printers policy to supply the printers to users and use the different subnets as filters. This will allow you to provide users with a printer closest to their current location.

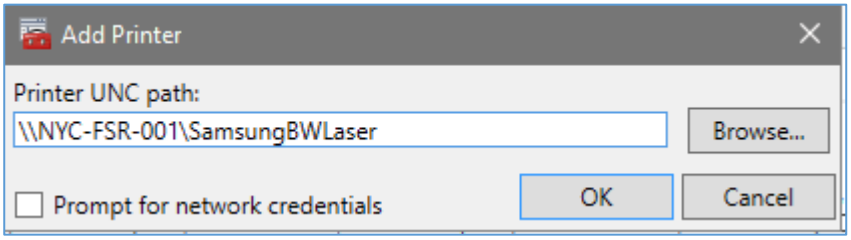
Step	Action
1.	Using the Remote Desktop Connection Manager, connect to **NYC-XDC-001**. **Note:** In a previous exercise, you had logged on to NYC-XDC-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-XDC-001 by right-clicking this machine and selecting Connect server.
2.	Using Studio, expand **Citrix Studio (SITE-NewYork)** and click **Policies**. On the right pane, click **Create Policy**. **Note**: Studio was started in a previous exercise. If Studio was closed in a previous exercise, then click **Start** > **Citrix** > **Citrix Studio**.
3.	On the Settings page, in the All Settings drop-down, select **Printing** (under ICA heading).
4.	Locate the **Session printers** setting, and next to this setting click **Select**.



In the Edit Setting dialog box that opens, under Session printers, click **Add**.

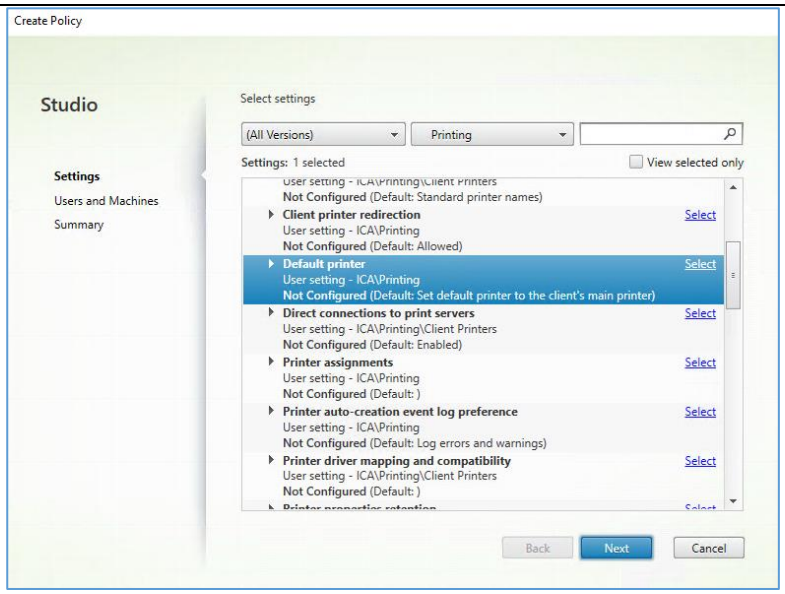
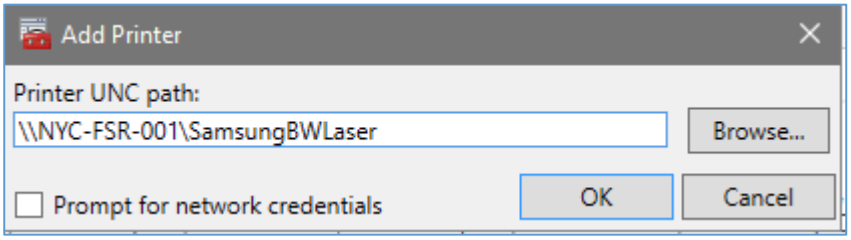
5. In the Add Printer dialog box that opens, enter the following text for the Printer UNC path:

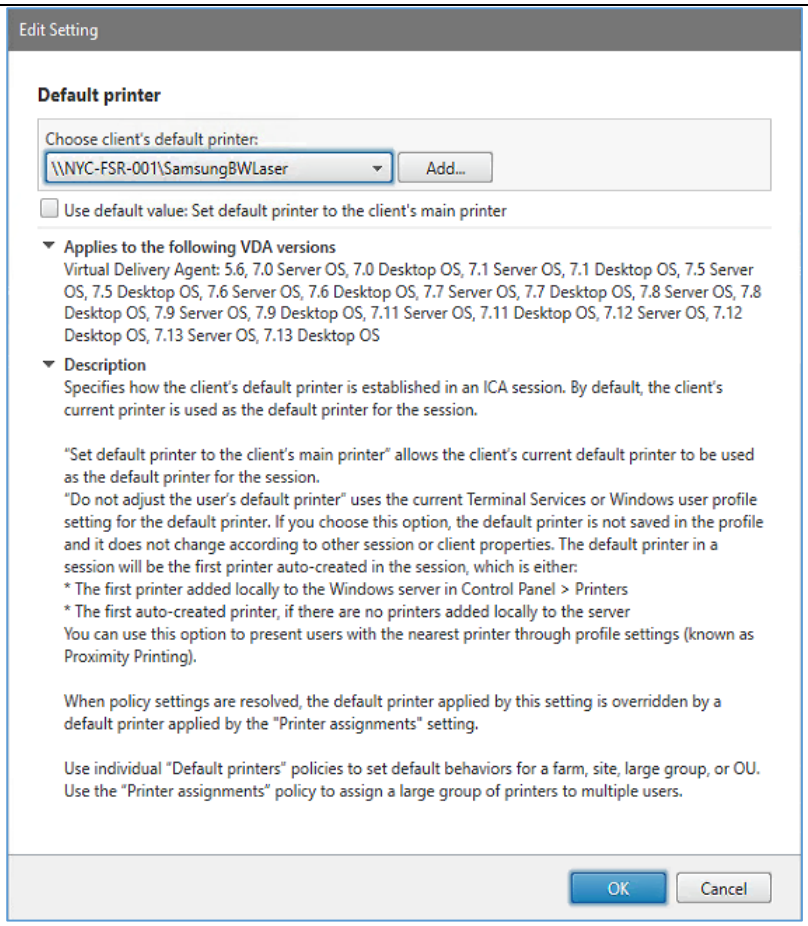
   \\NYC-FSR-001\SamsungBWLaser



   On the Add Printer dialog box, click **OK**. On the Edit Setting dialog box, click **OK**.

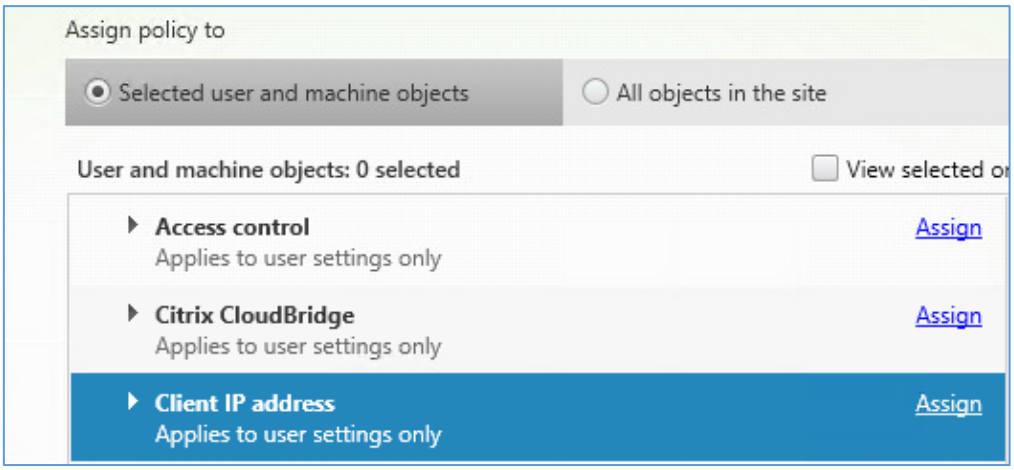
6. Locate the **Default printer** setting, and next to this setting click **Select**.

	 In the Edit Setting dialog box that opens, click **Add**.
7.	In the Add Printer dialog box that opens, enter the following text for the Printer UNC path: **\\NYC-FSR-001\SamsungBWLaser**  On the Add Printer dialog box, click **OK**.
8.	In the Edit Setting dialog box, click the drop-down list and select **\\NYC-FSR-001\SamsungBWLaser**.

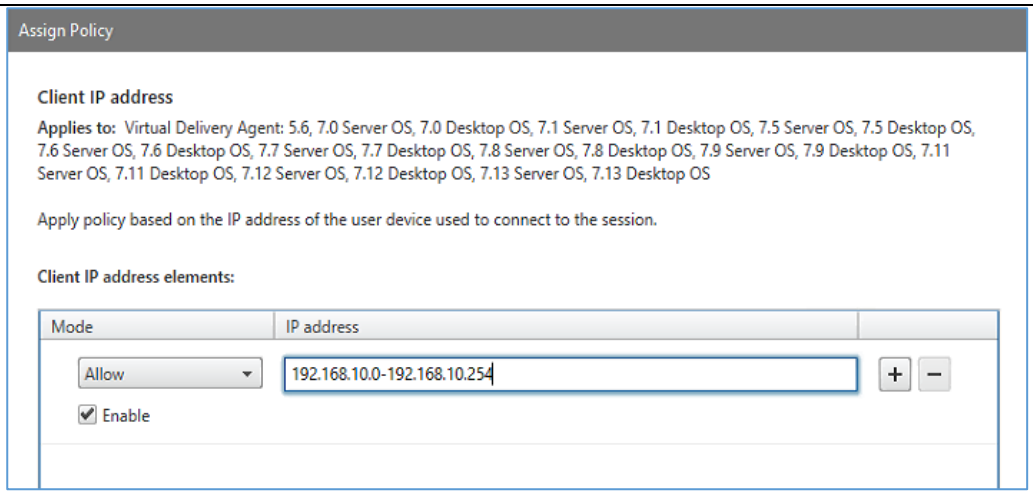


Click **OK** and then click **Next**.

9. In the Users and Machines page, click **Assign** next to the **Client IP address** option under the Assign policy to field.



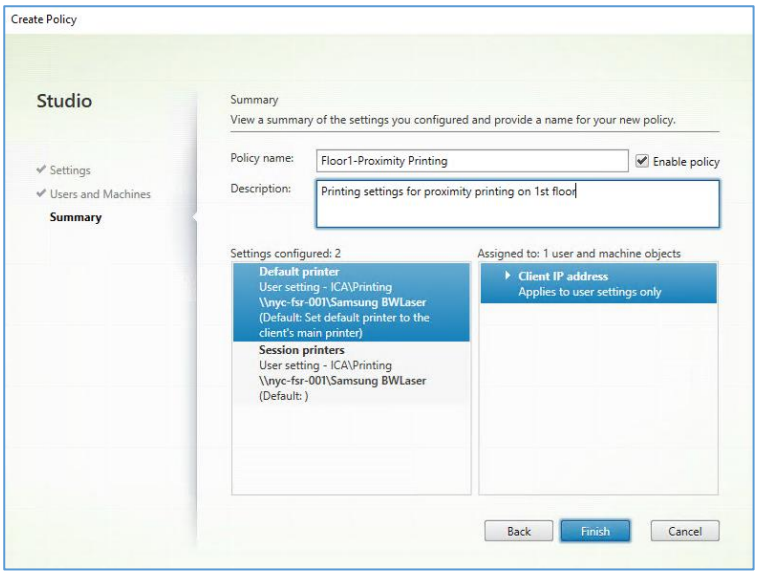
10. In the Assign Policy dialog box, configure the following settings:
    - Mode: **Allow**
    - IP address: **192.168.10.0-192.168.10.254**



Click **OK**.

11. On the Users and Machines page, click **Next**.

12. On the Summary page, configure the following:
    - Policy name: **Floor1-Proximity Printing**
    - Description: **Printing settings for proximity printing on 1st floor**



Click **Finish**.

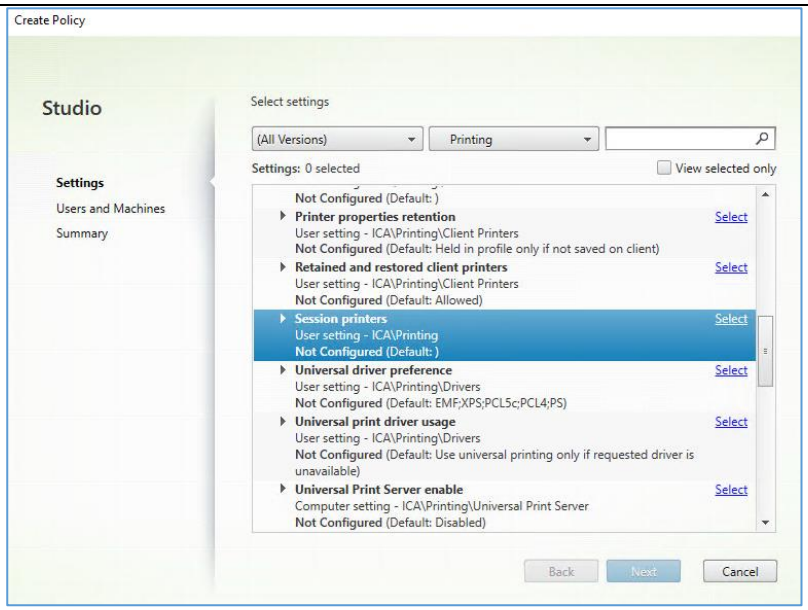
13. Using Studio, expand **Citrix Studio (SITE-NewYork)** and click **Policies**.

    On the right pane, click **Create Policy**.

    Note: Studio was launched in a previous exercise. If Studio was closed in a previous exercise, then click Start > Citrix > Citrix Studio.

14. On the Settings page, in the All Settings drop-down, select **Printing** (under ICA heading).

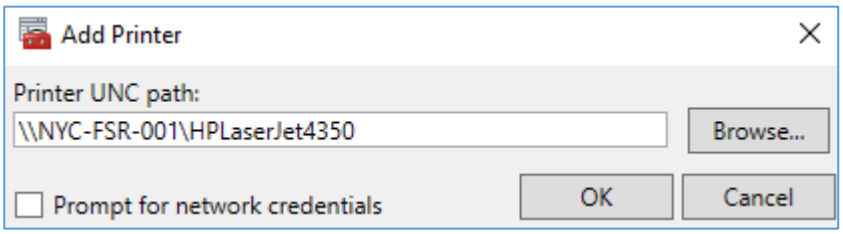
15. Locate the **Session printers** setting, and next to this setting click **Select**.



In the Edit Setting dialog box that opens, under Session printers, click **Add**.

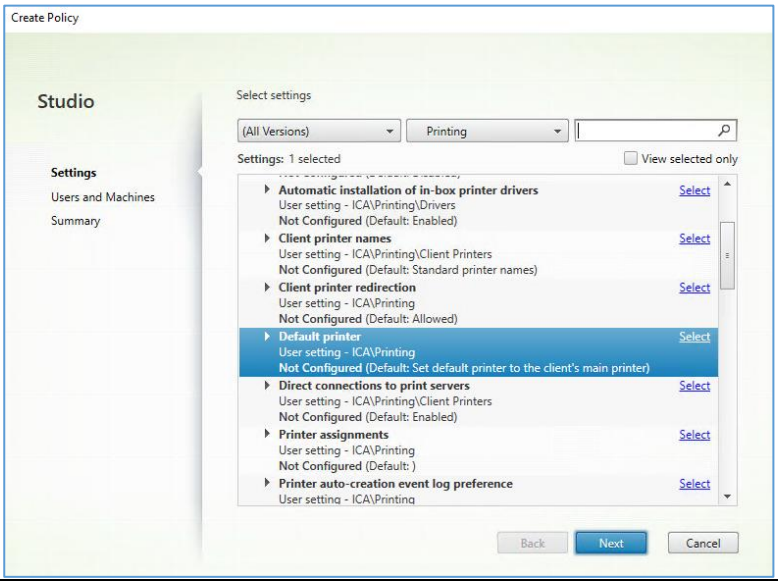
16. In the Add Printer dialog box that opens, enter the following text for the Printer UNC path:

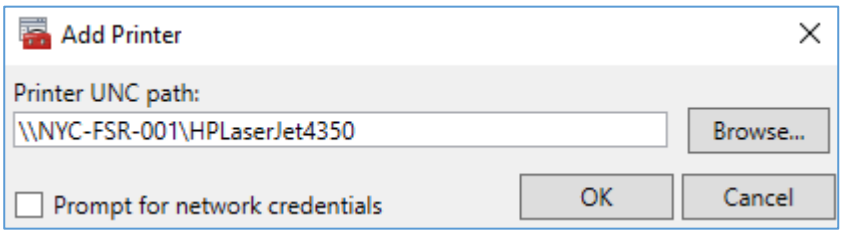
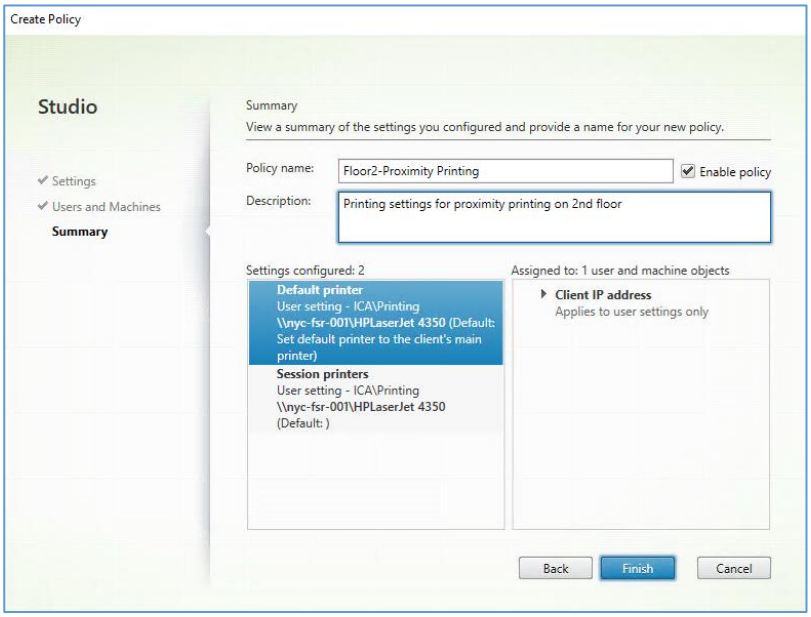
\\NYC-FSR-001\HPLaserJet4350



On the Add Printer dialog box, click **OK**. On the Edit Setting dialog box, click **OK**.

17. Locate the **Default printer** setting, and next to this setting click **Select**.



	In the Edit Setting dialog box that opens, click **Add**.
18.	In the Add Printer dialog box that opens, enter the following text for the Printer UNC path: **\\NYC-FSR-001\HPLaserJet4350**  On the Add Printer dialog box, click **OK**.
19.	In the Edit Setting dialog box, click the drop-down list and select **\\NYC-FSR-001\HPLaserJet4350**. Click **OK** and then click **Next**.
20.	On the Users and Machines page, click **Assign** next to the **Client IP address** option under the Assign policy to field.
21.	In the Assign Policy dialog box, verify the following settings: • Mode: **Allow** • IP address: **192.168.20.0-192.168.20.254** Click **OK**.
22.	On the Users and Machines page, click **Next**.
23.	On the Summary page, configure the following: • Policy name: **Floor2-Proximity Printing** • Description: **Printing settings for proximity printing on 2nd floor**  Click **Finish**.

Key Takeaways:

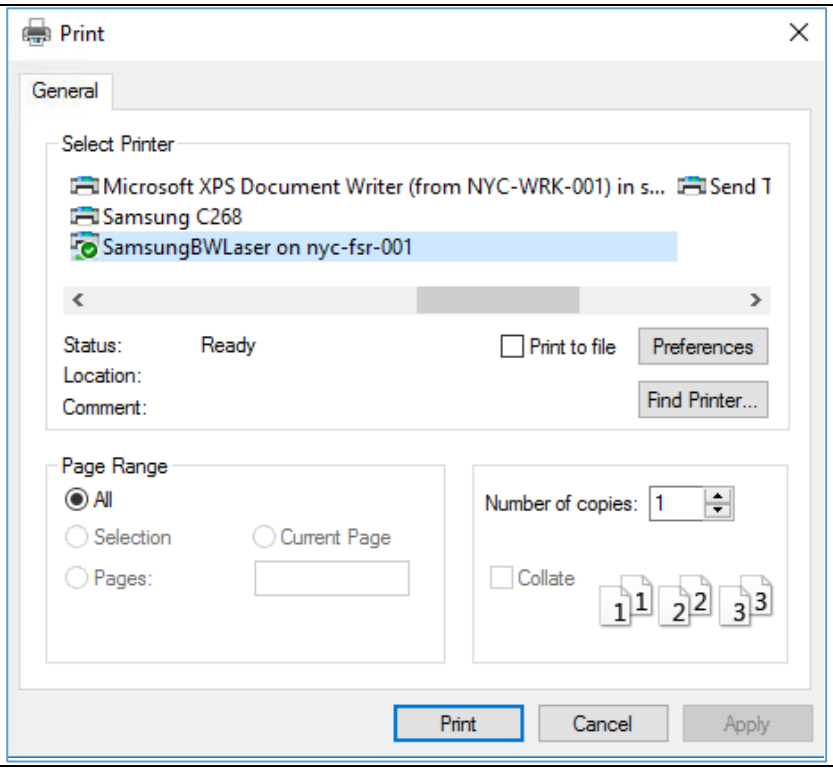
- Session printers are a list of network printer shares that connect inside the session on the VDA, and route the print action directly to the print server.
- Using a Citrix Policy to define session printers ensures a high-level of granularity, since we can filter the policy on various elements, such as endpoint IP addresses.
- The term proximity printing covers mapping printers to sessions based on which IP the session was initiated from, this way we can ensure that users roaming different locations will always be assigned a printer close to their endpoint.
- All printers defined in multiple session printer policies accumulate for each user.
- Session printer policies are evaluated during both logon and reconnection. For example, if a user starts a session from the 1st floor, and then disconnects, and then re-connects to the session on the 2nd floor, their printers would be refreshed.

Exercise 8-4: Test that the Session Printers Mapped to the Session

Scenario:

Your task is to test the previously configured Session Printers policy rule, by verifying a user connection to a session from an endpoint device on the second floor IP Subnet gets the Samsung BW Laser Printer.

Step	Action
1.	Using the Remote Desktop Connection Manager, switch to **NYC-WRK-001**. **Note:** In a previous exercise, you had logged on to NYC-WRK-001 using the following credentials to make the connection: • User name: Workspacelab\HR1 • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-WRK-001 by right-clicking this machine and selecting Connect server.
2.	Log on to **Citrix Receiver** with the following credentials: • User name: **HR1** • Password: **Password1** Select the **APPS** tab and launch **Notepad**.
3.	In Notepad window, click **File** > **Print**.
4.	In the Print dialog box, note that the session printer **SamsungBWLaser on NYC-FSR-001** is mapped in the session and is set as the default printer.

	
5.	On the Print dialog box, click **Cancel**. Close **Notepad.** Log off Citrix Receiver. Click **HR1** and **Log Off**.

Key Takeaways:

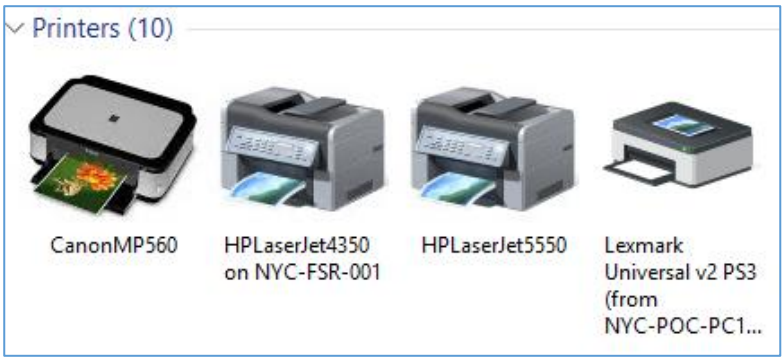
- Since the client is connecting from the 192.168.10.0 subnet, the VDA will activate the 1st floor printing policy and subsequently map the Samsung printer.
- Printers can be mapped into the session in a number of different ways, including logon scripts, group policies, group policy preferences and Citrix policies.

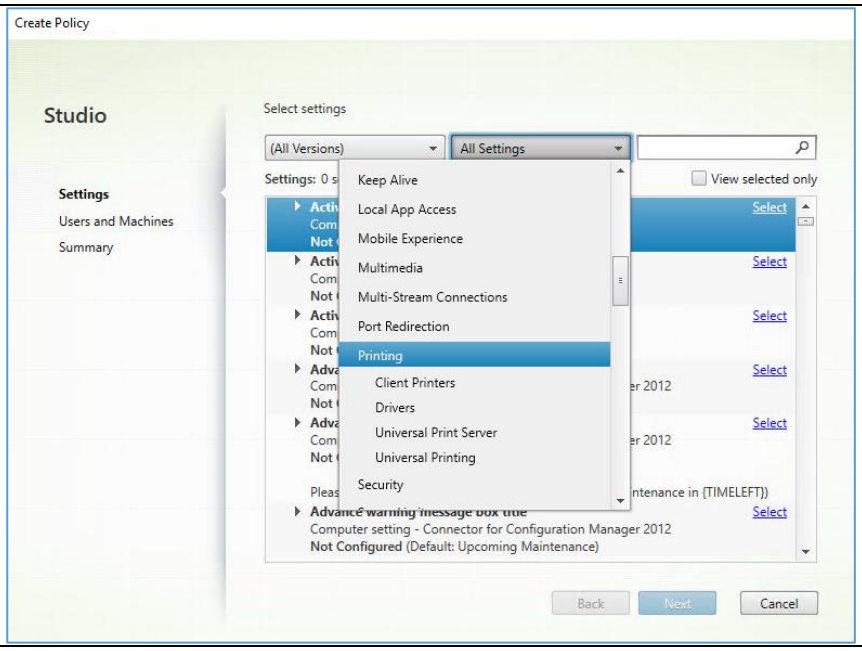
Exercise 8-5: Configure Print Job Routing

Scenario:

Your Citrix Lead Architect has tasked you to research why some printers in the POC installation show up as being mapped from the client, and other printers look like they are being mapped from a print server. In order to research this, you decide to start up a session and see if you can replicate the issue, before trying to identify a solution.

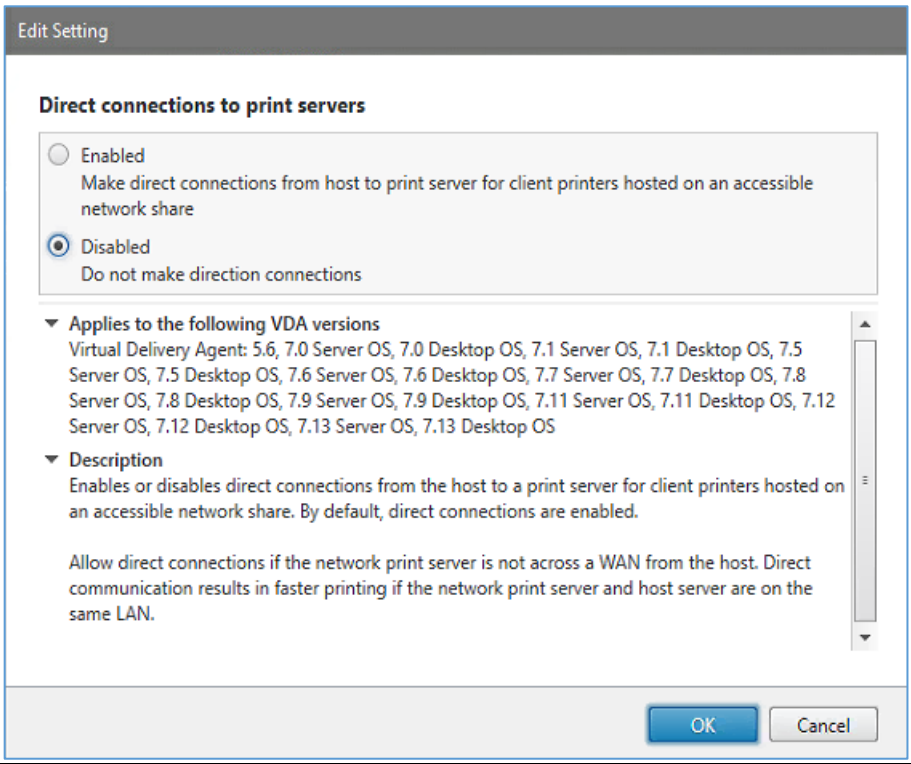
Step	Action
1.	Using the Remote Desktop Connection Manager, confirm that you are still connected to **NYC-WRK-001**. **Note:** In a previous exercise, you had logged on to NYC-WRK-001 using the following credentials to make the connection: • User name: Workspacelab\HR1 • Password: Password1

	Note: If your Remote Desktop Connection session disconnected, log on to NYC-WRK-001 by right-clicking this machine and selecting **Connect server**.
2.	On the taskbar of NYC-WRK-001, open **File Explorer** and browse to **\\NYC-FSR-001** to see a list of shared printers. Right-click **HPLaserJet4350** and click **Connect**.
3.	Log on to **Citrix Receiver** with the following credentials: • User name: **HR1** • Password: **Password1** Select the **DESKTOPS** tab and launch **HR Desktop**. **Note**: The Add Account window for Receiver may open when the Desktop is launched.
4.	Within the HR Desktop session, right-click **Start Menu** and select **Control Panel**.
5.	In the Control Panel, type **print** in the search field, and select **Devices and Printers**.
6.	Compare the HPLaserJet4350 printer and the Lexmark Universal v2 PS3 printer. Note that the HP LaserJet includes **on NYC-FSR-001** in the name.  **Note:** Both printers are auto-created from the endpoint into the session, but since the HP LaserJet is a network printer that the VDA can connect to, the VDA will initiate a direct connection to the printer, instead of mapping the printer through the client print path.
7.	Within the HR Desktop, right-click the **Start Menu**, click on **Shut down or sign out** and select **Sign out**.
8.	Using the Remote Desktop Connection Manager, connect to NYC-XDC-001. To log on to NYC-XDC-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1
9.	Using Studio, expand **Citrix Studio (SITE-NewYork)** and click **Policies**. On the right pane, click **Create Policy**. **Note**: Studio was started in a previous exercise. If Studio was closed in a previous exercise, then click Start > Citrix > Citrix Studio.
10.	On the Setting page, in the All Settings drop-down, select **Printing** (under ICA heading).



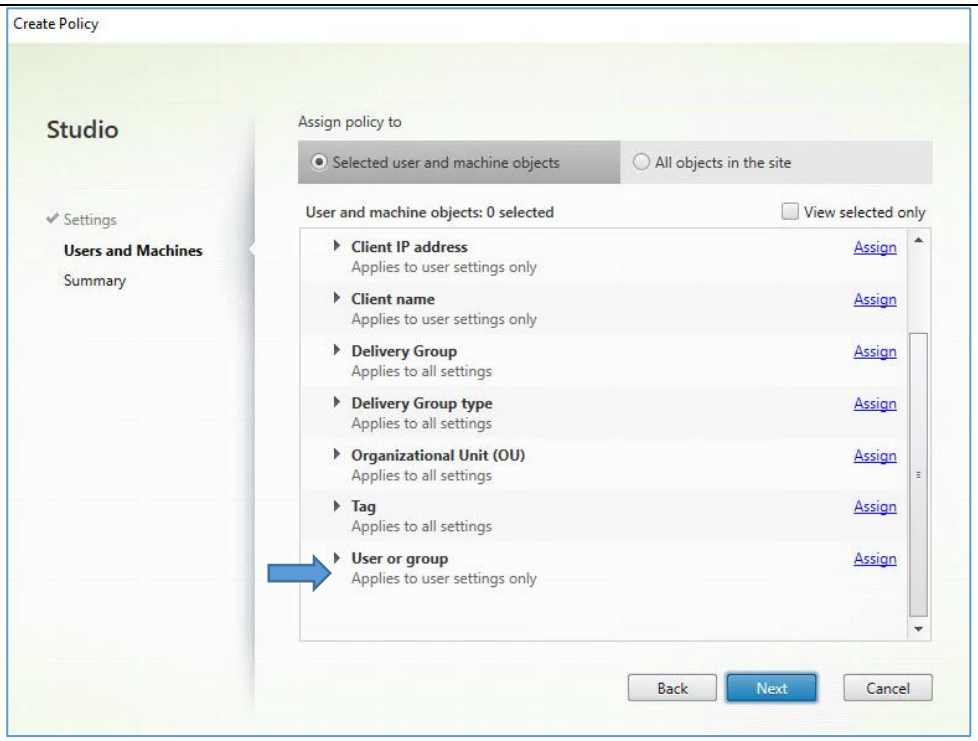
11. Locate the **Direct connections to print servers** setting, and click **Select**.

    Click the **Disabled** radio button, and click **OK**.

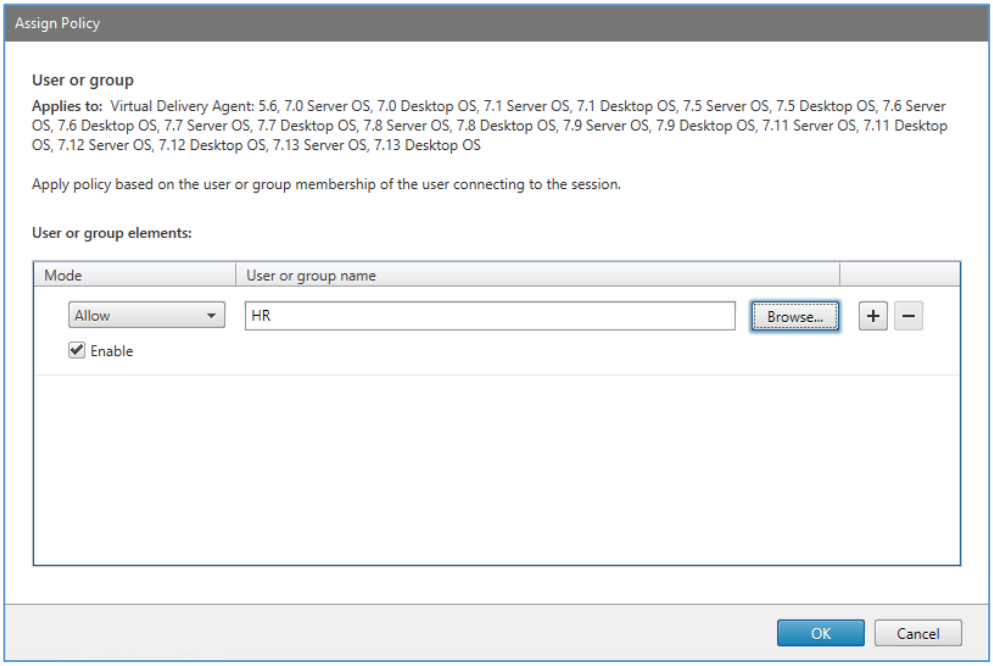


12. On the Settings page, click **Next**.

13. On the Users and Machines page, select **Assign** next to **User or group**.

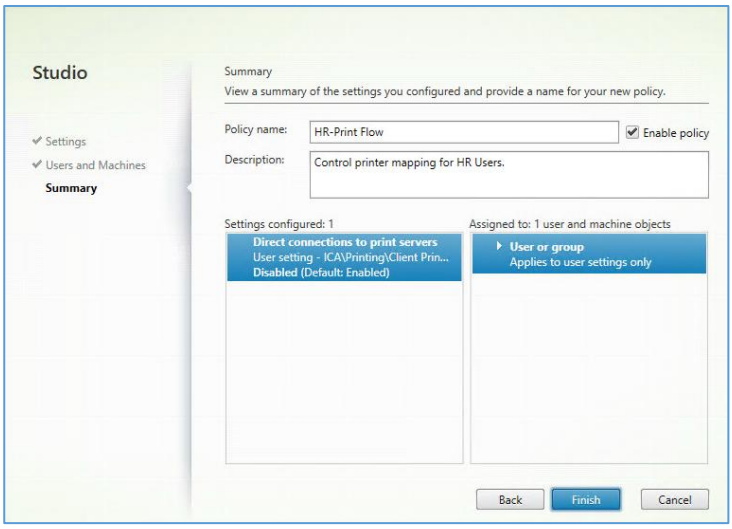
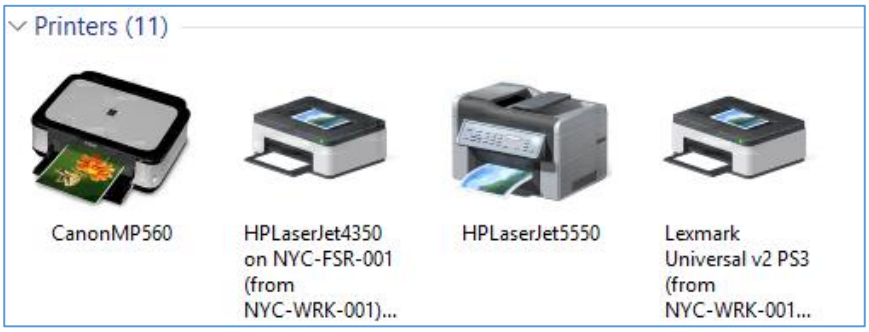


In the **Assign Policy** dialog box, click **Browse** and type **HR**. Click **Check Names** and select the HR Group. On the **Select User, Computer, or Group** dialog box click **OK** and then click **OK** on the **Assign Policy** dialog box.



Click **Next**.

14. In the Summary page, enter the following information:
    - Policy Name: **HR-Print Flow**
    - Description: **Control printer mapping for HR Users**.

	 Click **Finish**.
15.	Using the Remote Desktop Connection Manager, switch back to **NYC-WRK-001**. **Note:** In a previous exercise, you had logged on to NYC-WRK-001 using the following credentials to make the connection: • User name: Workspacelab\HR1 • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-WRK-001 by right-clicking this machine and selecting Connect server.
16.	Log on to **Citrix Receiver** with the following credentials: • User name: **HR1** • Password: **Password1** Launch **HR Desktop**.
17.	Within the **Hosted Desktop** session, right-click **Start** and select **Control Panel**.
18.	In Control Panel, type **print** in the search field, and select **Devices and Printers**.
19.	Compare the HPLaserJet4350 printer and the Lexmark Universal v2 PS3 printer. Note that both printers should now include **from NYC-WRK-001** in the name. This means that the HPLaserJet4350 is now following the client print pathway, instead of being directly connected from the print server. 

	Note: The HPLaserJet4350 printer has not changed, but the policy is now instructing the VDA to only connect this printer from the endpoint and not to try to map the printer directly from the print server.
20.	Within the Hosted Desktop, right-click **Start** > choose **Shut down or sign out** > and click **Sign out**.
21.	Using the Remote Desktop Connection Manager, connect to NYC-XDC-001. To log on to NYC-XDC-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1
22.	Using Studio, expand **Citrix Studio (SITE-NewYork)** and click **Policies**. In the middle pane, select **HR-Print Flow** and from the action pane select **Disable Policy**.

Key Takeaways:

- XenApp and XenDesktop will automatically map any client network printer as a direct mapping from the print server if the print server is on the local network and the printer object is accessible.
- Instead of sending the print job via the client to the print server, the print job is sent directly to the print server.
- This behavior can be controlled through Citrix policies.
- In some WAN designs, using the client print route can enable less bandwidth usage and faster print for the users.

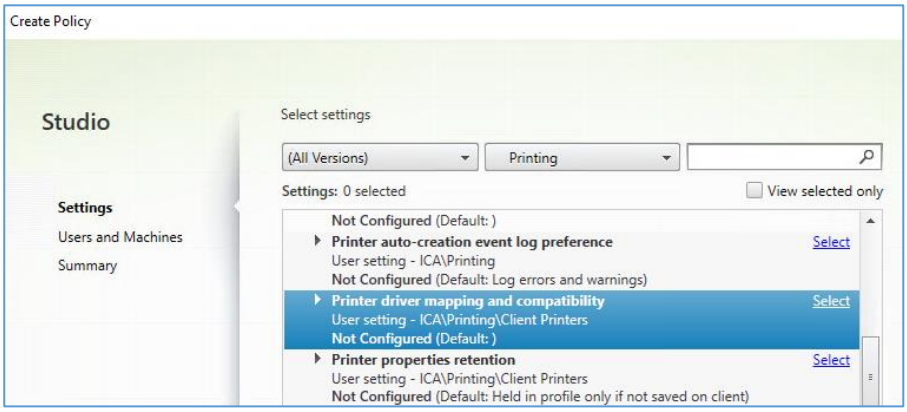
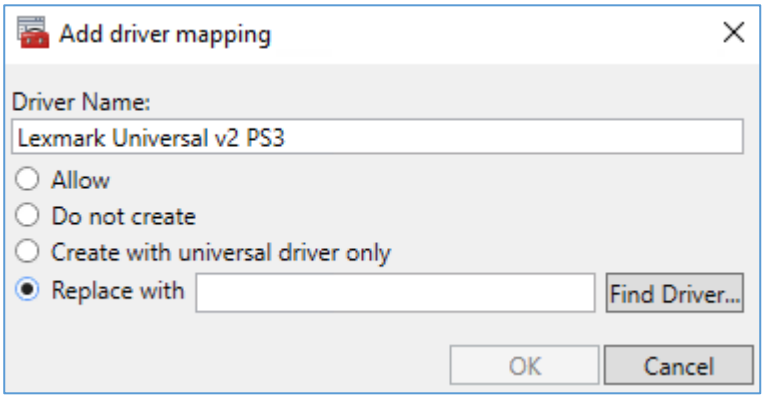
Exercise 8-6: Configure Print Driver Mapping

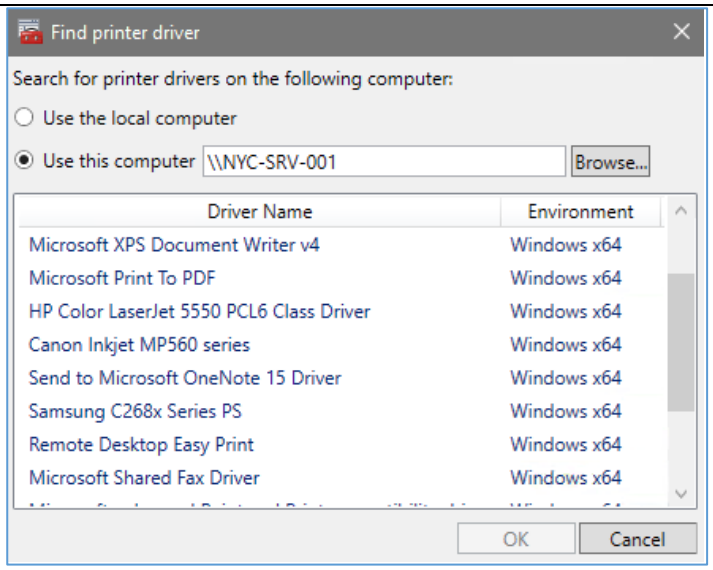
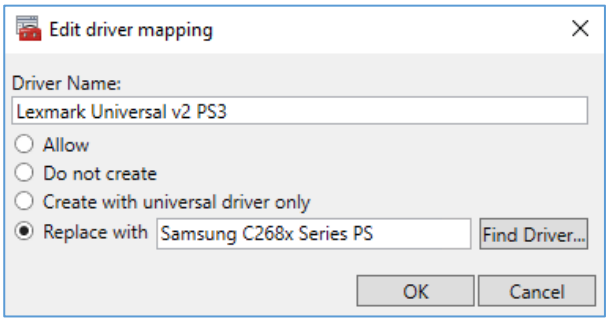
Scenario:

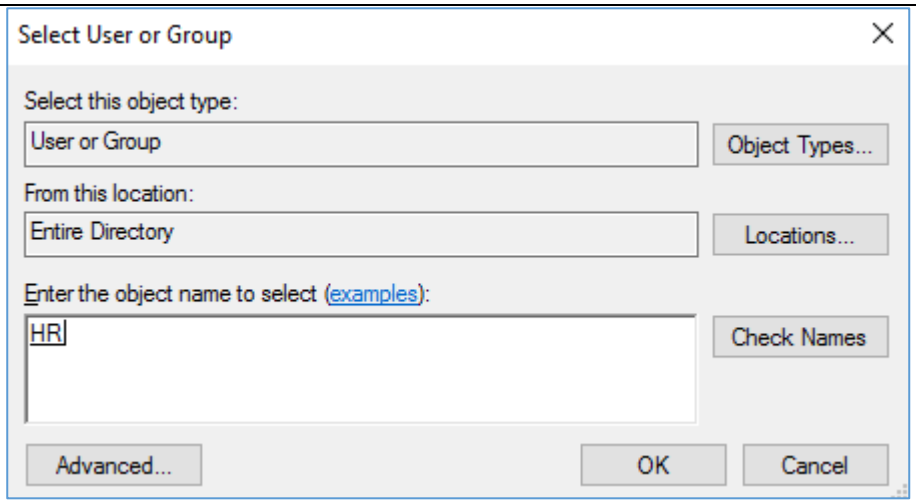
Most printing scenarios, when printing from sessions, require specific drivers running on the machines running the VDA hosting these sessions. One method to limit the number of drivers needed is to create a mapping table that allows a single driver to be used when compatible and reduce the number of printer drivers to install, test and maintain on the VDA machines.

Your task is to set the Print Driver Mapping policy to configure this mapping table.

Step	Action
1.	Using the Remote Desktop Connection Manager, confirm you are still connected to **NYC-XDC-001**. **Note:** In a previous exercise, you had logged on to NYC-XDC-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-XDC-001 by right-clicking this machine and selecting **Connect server**.
2.	Using Studio, expand **Citrix Studio (SITE-NewYork)** and click **Policies**. On the right pane, click **Create Policy**. **Note**: Studio was started in a previous exercise. If Studio was closed in a previous exercise, then click Start > Citrix > Citrix Studio.
3.	On the Settings page, in the All Settings drop-down, select **Printing** (under ICA heading).

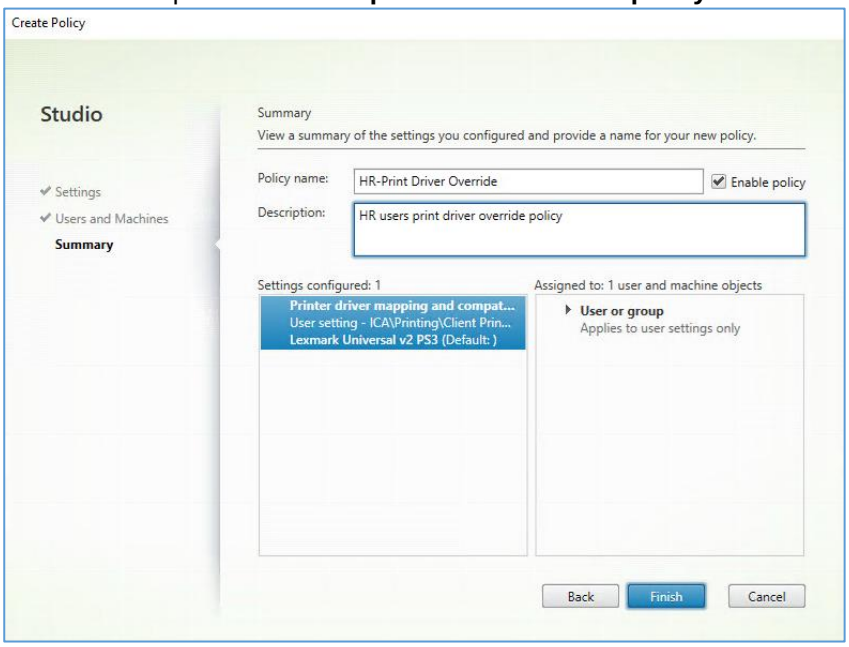
4.	Locate the **Printer driver mapping and compatibility** setting, and next to this setting click **Select**.  Under the Driver Name heading, click **Add**.
5.	The Add driver mapping dialog box opens. Type **Lexmark Universal v2 PS3** in the Driver Name field and select the **Replace with** radio button.  Click **Find Driver**.
6.	In the Find printer driver dialog box that opens, select the **Use this computer** radio button, click **Browse**, select **NYC-SRV-001** and click **OK**.

	 Wait for the Driver Names on NYC-SRV-001 to populate in the Driver Name box. Select **Samsung C268x Series PS** and click **OK**. In the Add driver mapping dialog box, click **OK**.  In the Edit Setting dialog box, click **OK**. Click **Next**.
7.	In the Users and Machines page, next to the **User or group** option for the Assign policy to field, click **Assign**.
8.	In the Assign Policy dialog box, verify that in the Mode drop-down, **Allow** is selected. Next to the **User or group name** field, click **Browse**.
9.	In the Select User, Computer, or Group dialog box, type **HR** and click **Check Names**.



Select the **HR** group and click **OK**. After the name is successfully added, click **OK**. Click **Next**.

10. On the Summary page, configure the following:
    - Policy name: **HR-Print Driver Override**
    - Description: **HR users print driver override policy**



Click **Finish**.

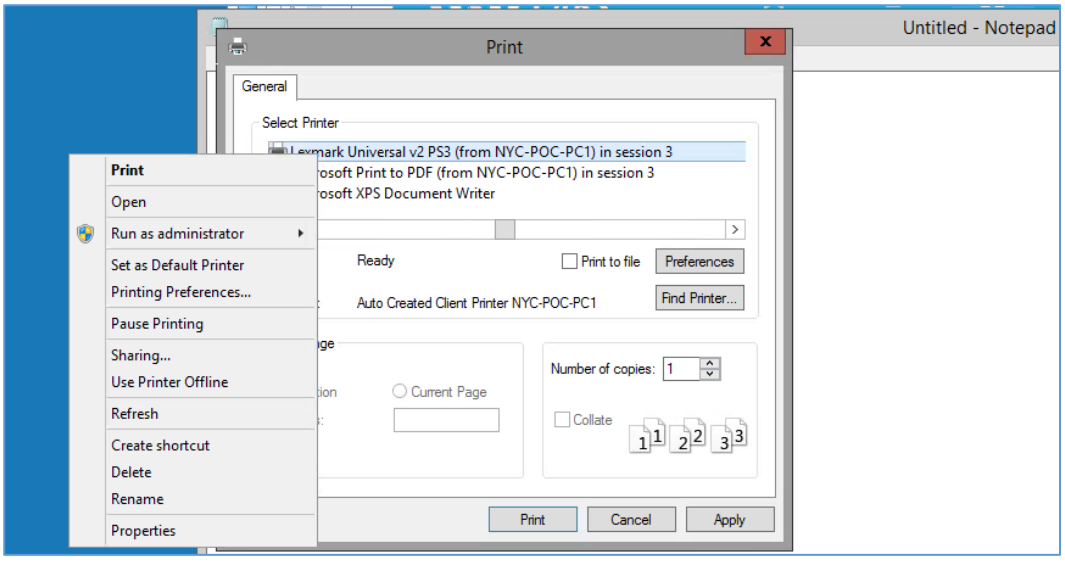
Key Takeaways:

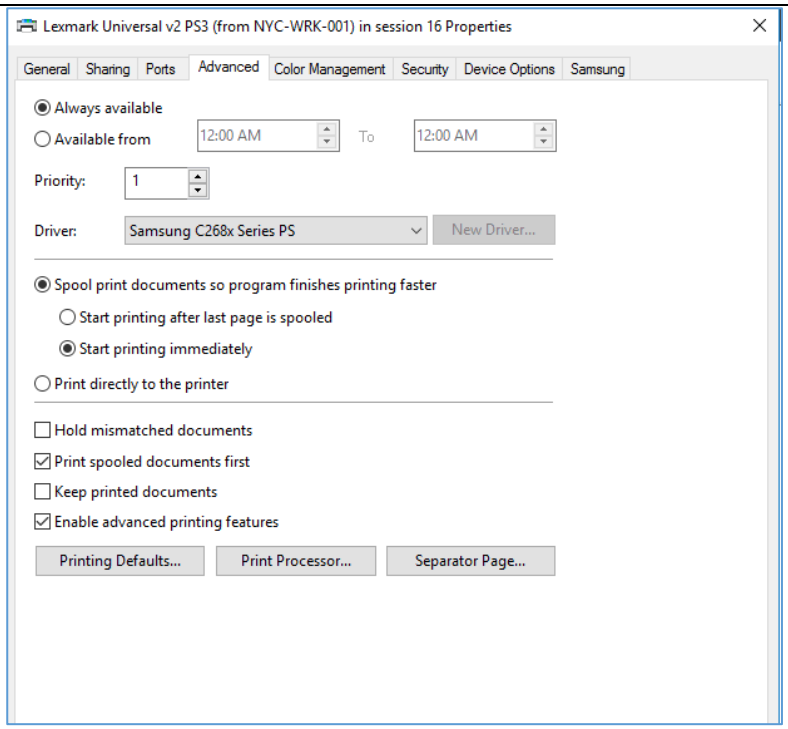
- Use driver mapping to reduce the number of required drivers on VDAs.
- Test for compatibility of the mappings before issuing them in production.
- Can also be used to blacklist a certain printer driver with the function do not create.
- Wildcards can be used when creating the rules (HP* > HP Universal PCL6 driver).

Exercise 8-7: Test the Print Driver Mapped

Scenario:

Your task is to identify which driver is used to map a specific printer inside a session.

Step	Action
1.	Using the Remote Desktop Connection Manager, switch back to **NYC-WRK-001**. **Note:** In a previous exercise, you had logged on to NYC-WRK-001 using the following credentials to make the connection: • User name: Workspacelab\HR1 • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-WRK-001 by right-clicking this machine and selecting Connect server.
2.	Log on to **Citrix Receiver** with the following credentials: • User name: **HR1** • Password: **Password1** Select the **DESKTOPS** tab and launch **HR Desktop** Launch **Notepad**.
3.	In Notepad, click **File** > **Print**.
4.	In the Print dialog box, right-click **Lexmark Universal v2 PS3 (from NYC-WRK-001) in session x** and select **Properties**.  In the Properties dialog box, click the **Advanced** tab and view the Driver drop-down menu, and notice that the driver defined in the printing policy **Samsung C268x Series PS** is being used.

	
5.	On the Properties dialog box, click **Cancel**. On the Print dialog box, click **Cancel**. Close **Notepad**, and log off **HR Desktop**. Log off Citrix Receiver. Click **HR1** and **Log Off**. **Close** the Receiver window.

Key Takeaways:

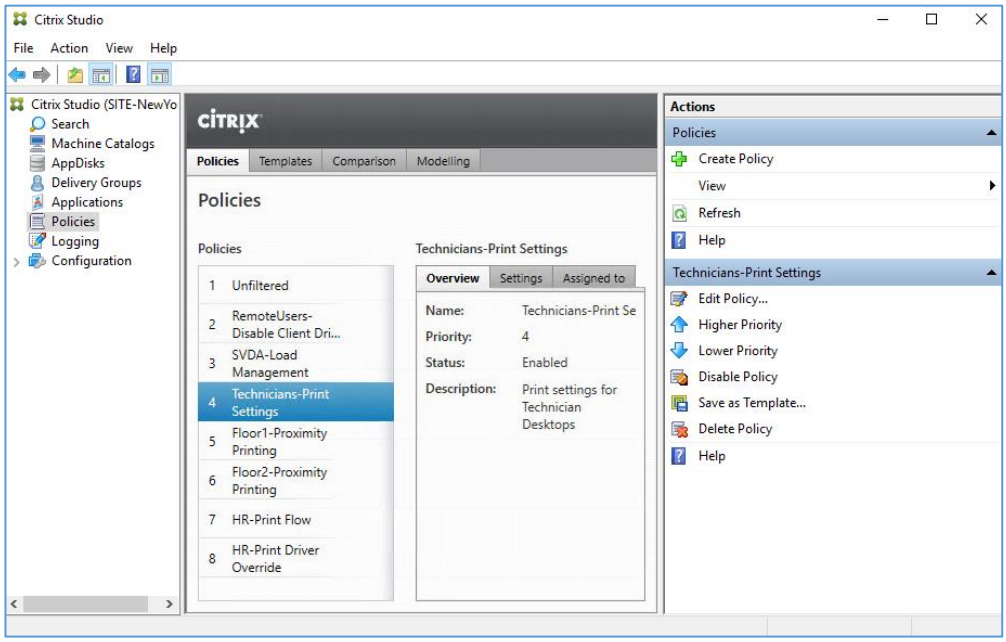
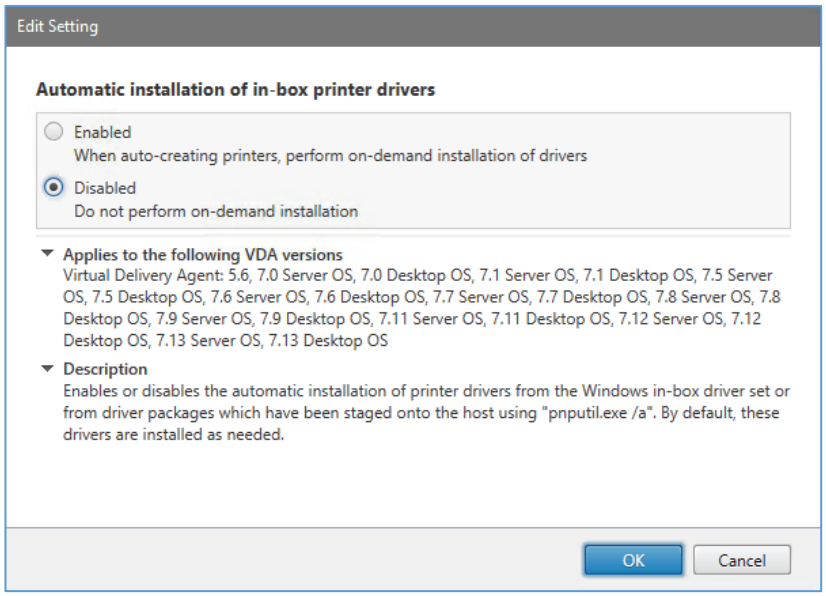
- The successful mapping of a printer with another driver does not mean that the printer will actually work. This will need to be tested and may require a different driver to be used.
- Ensure to refer to print manufactures documentation and test thoroughly before releasing mappings into production.

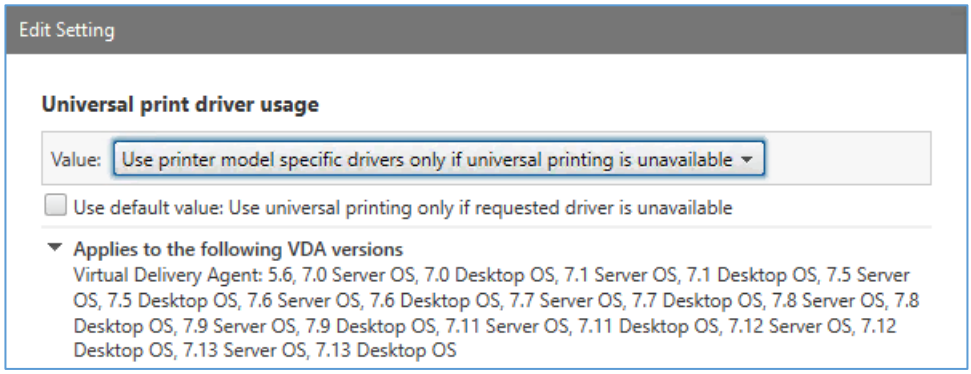
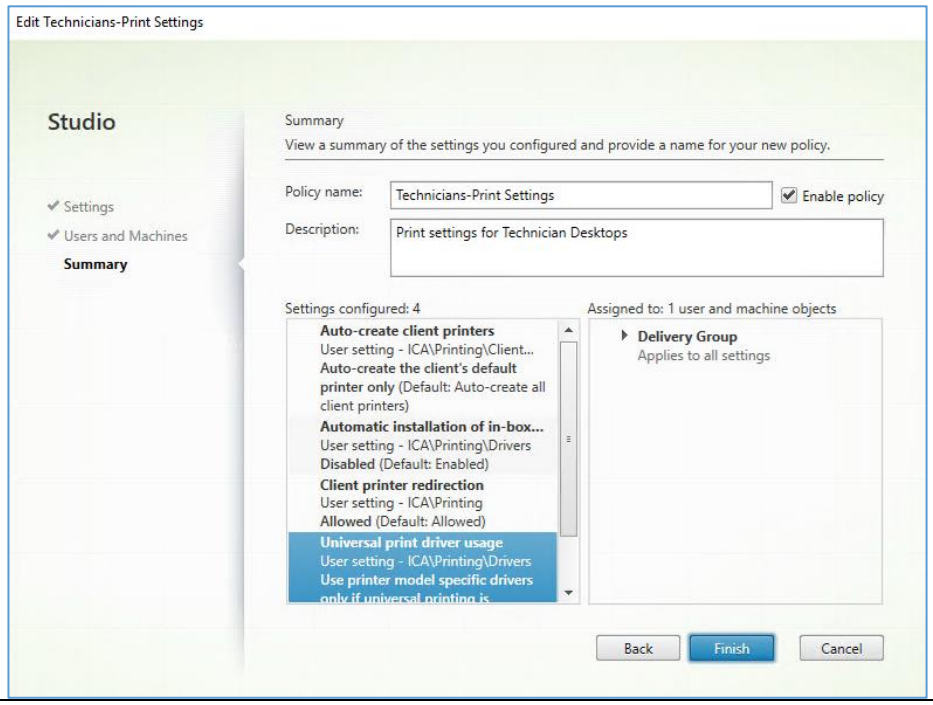
Exercise 8-8: Configure the Universal Print Driver

Scenario:

Your task is to configure the use of the Universal Print Driver for all users to limit the amount of necessary 3rd party printer drivers.

Step	Action
1.	Using the Remote Desktop Connection Manager, switch back to **NYC-XDC-001**. **Note:** In a previous exercise, you had logged on to NYC-XDC-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-XDC-001 by right-clicking this machine and selecting **Connect server**.

2.	Using Studio, expand **Citrix Studio (SITE-NewYork)** and click **Policies**. In the middle pane under policies, select **Technicians-Print Settings**. In the right pane, click **Edit Policy**.  **Note**: Studio was started in a previous exercise. If Studio was closed in a previous exercise, then click Start > Citrix > Citrix Studio.
3.	On the Settings page, in the **All Settings** drop-down, select **Drivers** (under ICA\Printing).
4.	Locate the **Automatic installation of in-box printer drivers** setting, and next to this setting click **Select**. Select the **Disabled** radio button.  Click **OK**.
5.	Locate the **Universal print driver usage** setting, and next to this setting click **Select**.

	In the Value drop-down field, select **Use printer model specific drivers only if universal printing is unavailable**.  Click **OK** and then click **Next**.
6.	On the Users and Machines page, click **Next**.
7.	On the Summary page, click **Finish**. 

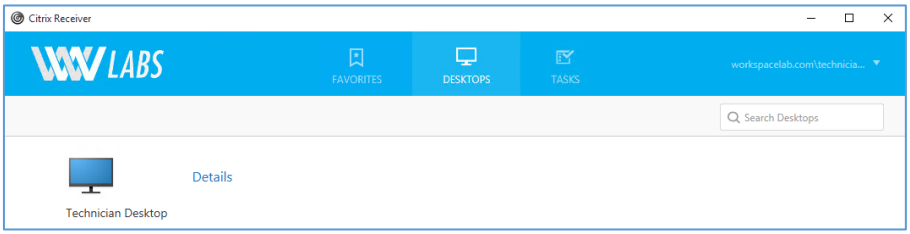
Key Takeaways:

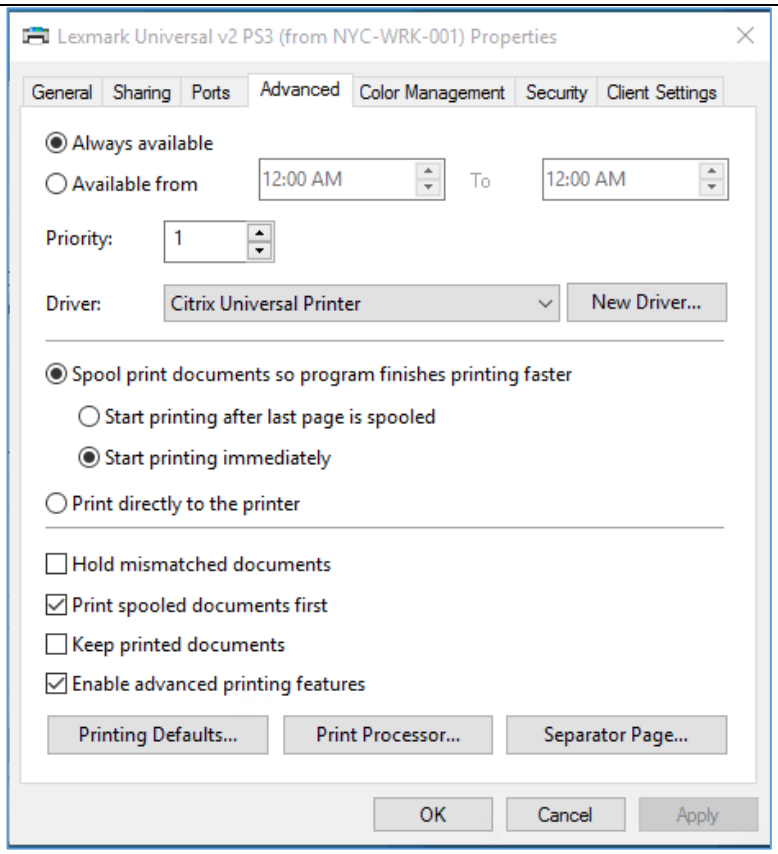
- For a stable printing system, try to use the Universal Print Driver unless specific printer functions are required.
- The Universal Print Driver currently requires Windows Endpoints to benefit from all functions.
- Make sure not to confuse the Citrix Universal Printer Driver with product specific Universal drivers, such as HP and Lexmark.

Exercise 8-9: Test that the Printer Auto-created with the Universal Print Driver

Scenario:

Your task is to log on and test that the Universal Print Driver is in use when auto-creating the printer.

Step	Action
1.	Using the Remote Desktop Connection Manager, switch back to **NYC-WRK-001**. **Note:** In a previous exercise, you had logged on to NYC-WRK-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-WRK-001 by right-clicking this machine and selecting Connect server.
2.	Log on to **Citrix Receiver** with the following credentials: • User name: **Technician1** • Password: **Password1** Select **DESKTOPS** and then launch **Technician Desktop**. 
3.	Click **Start** and type **Notepad**. Launch **Notepad** from the list.
4.	In Notepad, click **File** > **Print**.
5.	In the Print dialog box, right-click **Lexmark Universal v2 PS3 (from NYC-WRK-001)** and select **Properties**. In the Properties dialog box, click the **Advanced** tab and view the Driver drop-down menu. Notice the printer was auto-created with the **Citrix Universal Printer** driver.

	 On the Properties dialog box, click **Cancel**. Then, on the Print dialog box, click **Cancel** to exit the dialog box.
6.	Close **Notepad** and log off the **Technician Desktop**. Log off Citrix Receiver. Click **Technician1** and **Log Off**.
7.	Switch back to **NYC-XDC-001** using the Remote Desktop Connection Manager.
8.	Click **Start** and click **Citrix Studio**. **Note**: Ignore if Studio is already open.
9.	Click on **Machine Catalogs** in left pane. Double-click **NYC-CAT-DesktopOS**.
10.	Right-click **NYC-DTP-001.workspacelab.com**, select **Turn On Maintenance Mode** and click **Yes** to confirm.
11.	Connect to XenCenter and shut down **NYC-DTP-001**.

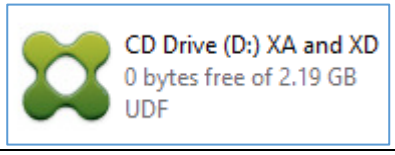
Key Takeaways:

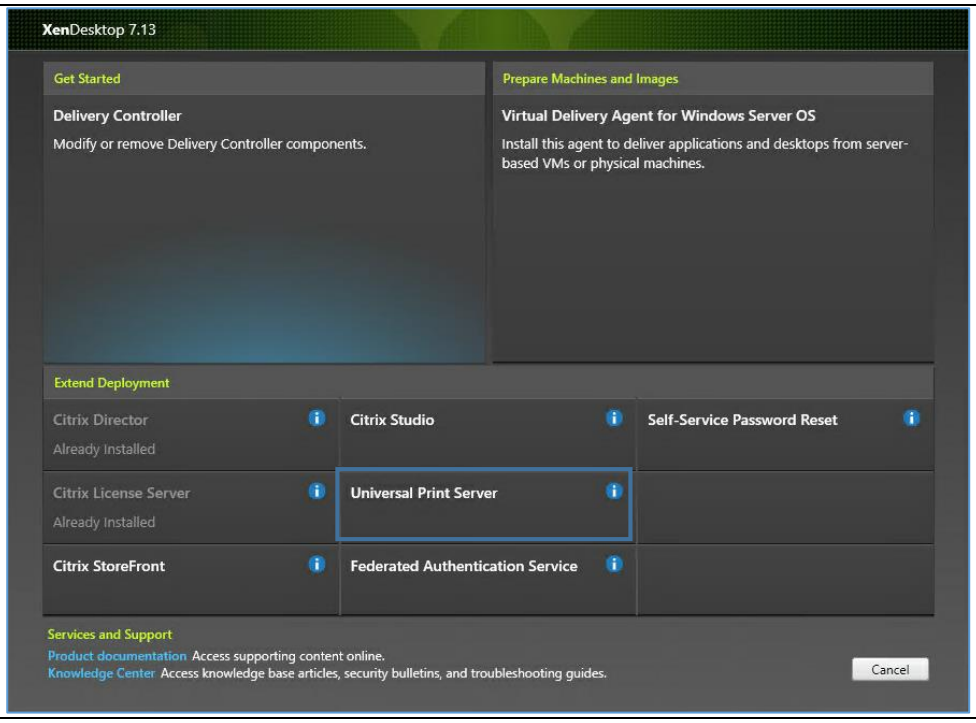
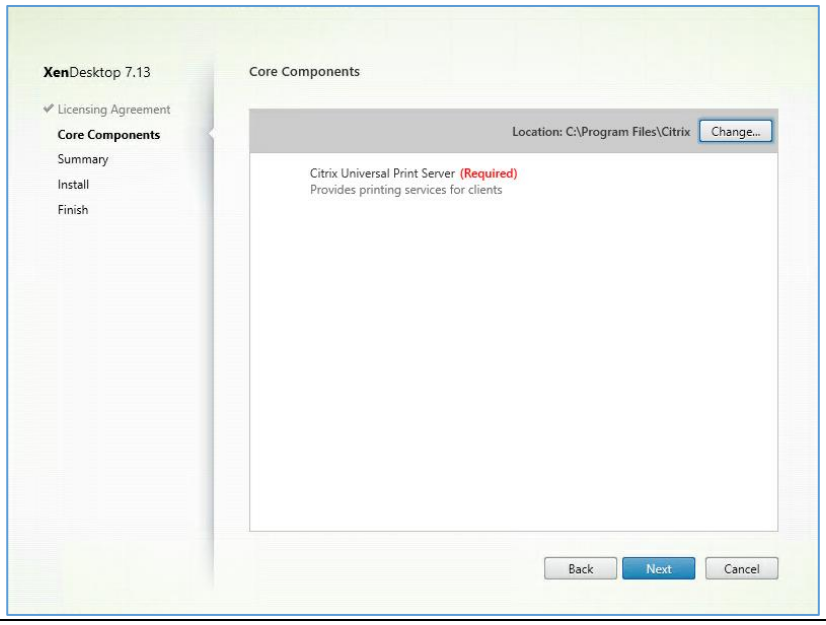
- Using the Universal Print Driver will not use the native installed drivers and will help to prevent performance issues.

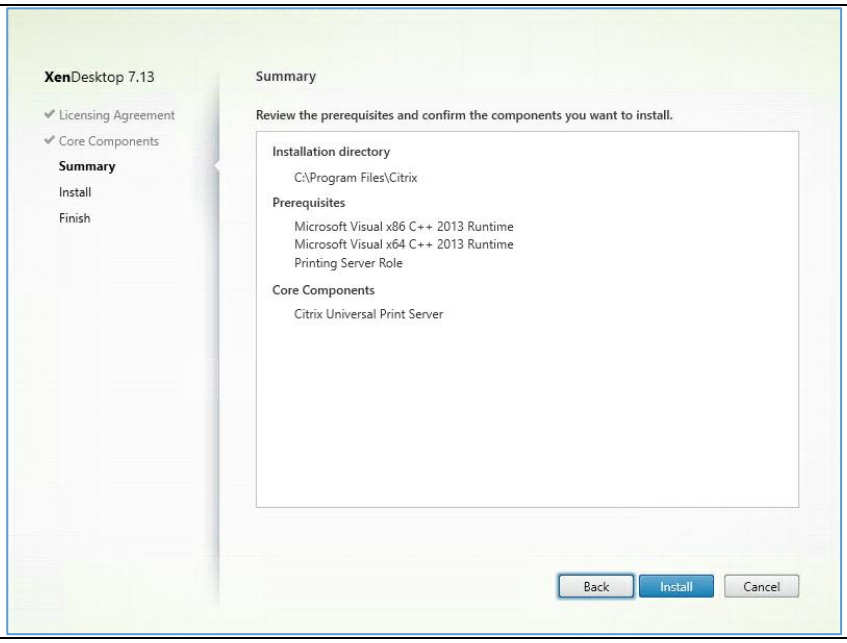
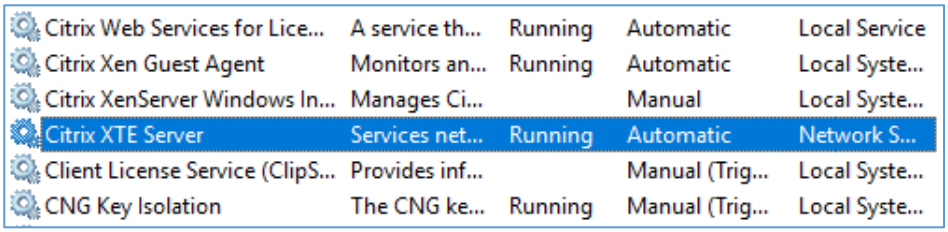
Exercise 8-10: Configure the Universal Print Server Component

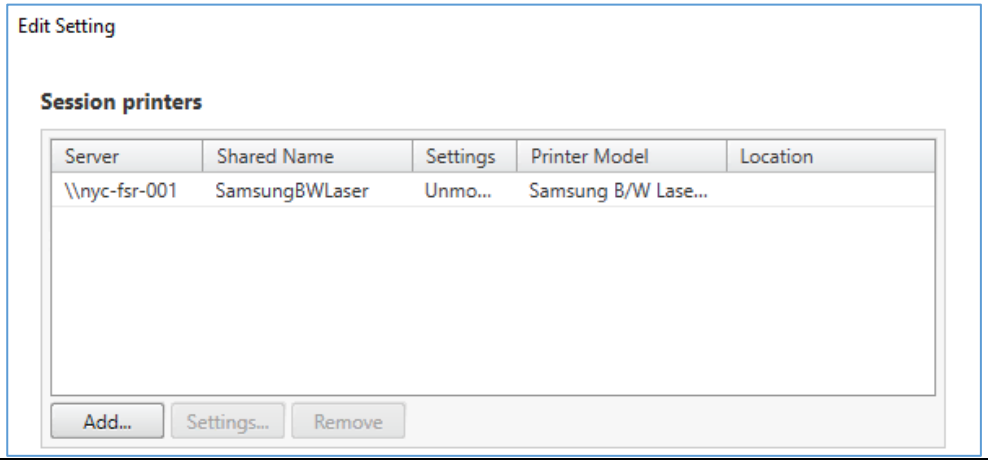
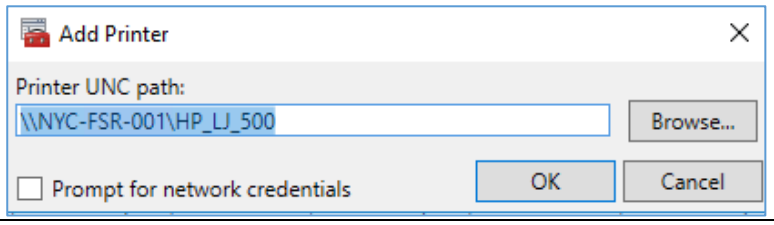
Scenario:

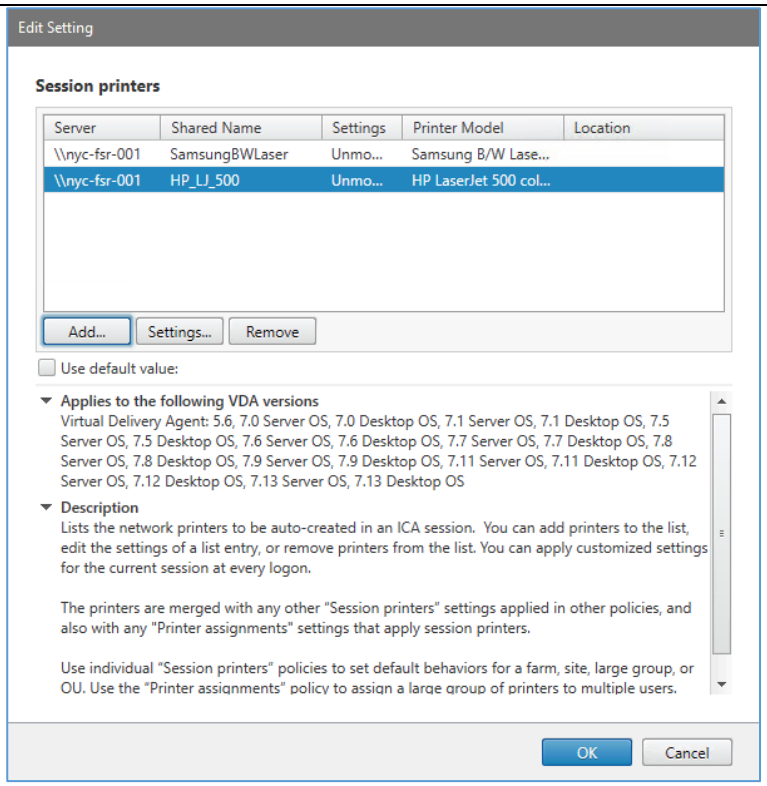
Your task is to install the Citrix Universal Printer Server on an existing print server and to enable the use of the universal print driver for common print servers.

Step	Action
1.	Using **XenCenter** mount the XenApp and XenDesktop installation media ISO to **NYC-FSR-001**. To mount the installation media ISO, select **NYC-FSR-001** in the left pane of the XenCenter. In the right pane, select the **Console** tab. Using the **DVD Drive 1:** drop-down menu, select **XenApp_and_XenDesktop_7_13.iso**. **Note**: If there are no ISOs listed in the **DVD Drive 1:** drop-down menu, then the Local ISO Storage Repository (SR) that contains the ISO library may need to be re-scanned. In the left pane of **XenCenter** select the **Local ISO SR XS**. In the right pane select the **Storage** tab and click on the **Rescan** button. This task may need to be repeated later in the course. **Note:** If the above rescan of the **Local ISO SR XS** does not show the specific ISO for installation: XenApp_and_XenDesktop_7_13.iso, then please tell your instructor.
2.	Using the Remote Desktop Connection Manager, connect to NYC-FSR-001. To log on to NYC-FSR-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1
3.	Launch **File Explorer** from the Windows Taskbar or Start menu. Double-click the **green Citrix logo** next to CD Drive under Devices and drives, and double-click on **AutoSelect.exe**. 
4.	The wizard will now display all possible installation options that are compatible with the Operating System of the machine that you are on. Under Extend Deployment, click **Universal Print Server**.

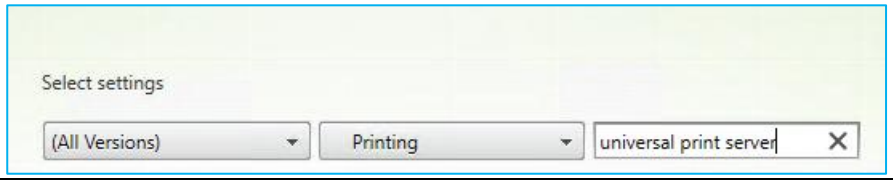
	
5.	On the Software License Agreement page, read the Citrix License Agreement and if you agree, select **I have read, understand, and accept the terms of the license agreement**. Click **Next**.
6.	On the Core Components page, verify that Citrix Universal Print Server is set as **Required** and click **Next**. 
7.	Review the settings on the Summary page and click **Install**.

	
8.	After the installation has successfully completed, click **Finish**.
9.	Restart the **Citrix XTE Server** service. Right-click **Start**, and click **Run**. Type **services.msc** and press **Enter**. **Note:** In some cases, the print server is a dedicated machine where the machine can just be restarted. 
10.	Right-click **Start** and select **Programs and Features**.
11.	Verify that the **Citrix Universal Print Server** version is **7.13.0.84**.
12.	Using **XenCenter** eject the XenApp and XenDesktop installation media from **NYC-FSR-001**. To eject the installation media ISO, select **NYC-FSR-001** in the left pane of XenCenter. In the right pane, select the **Console** tab and click **Eject** to remove **XenApp_and_XenDesktop_7_13.iso** from the DVD Drive 1. **Note**: The Eject option can be difficult to see. It is an underlined word to the right side of the DVD Drive 1 drop-down menu.
13.	Using the Remote Desktop Connection Manager, switch to **NYC-XDC-001**. **Note:** In a previous exercise, you had logged on to NYC-XDC-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1

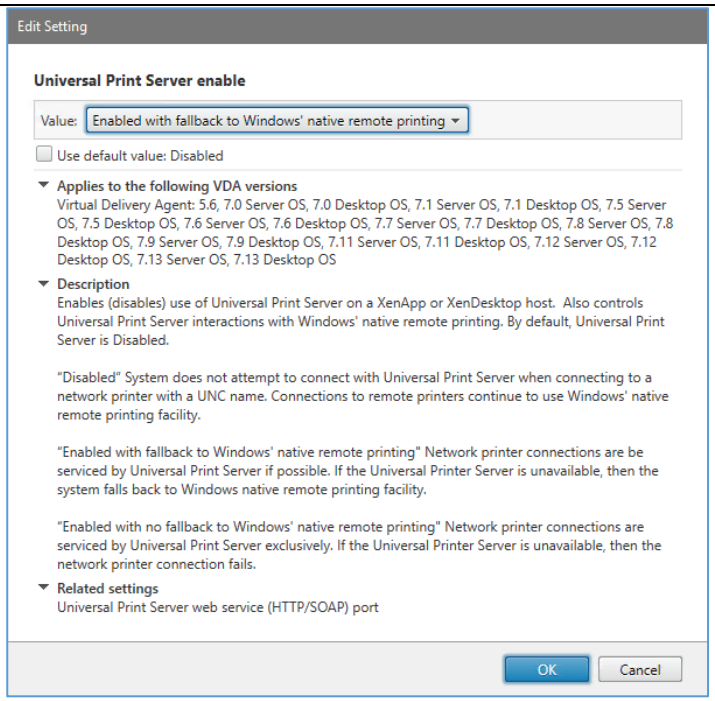
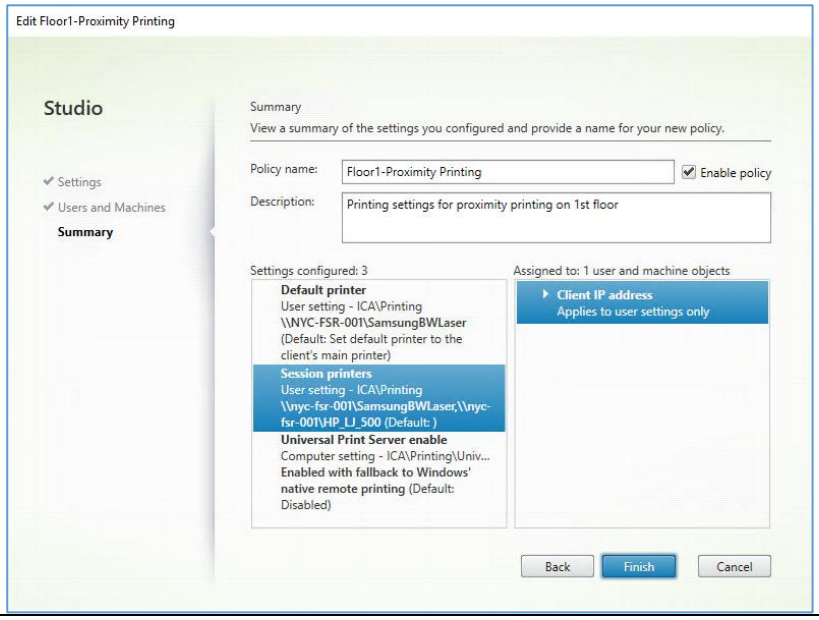
	Note: If your Remote Desktop Connection session disconnected, log on to NYC-XDC-001 by right-clicking this machine and selecting **Connect server**.
14.	Using Studio, expand **Citrix Studio (SITE-NewYork)** and click **Policies**. In the middle pane under Policies, select **Floor1-Proximity Printing**. In the right pane, click **Edit Policy**. **Note**: Studio was started in a previous exercise. If Studio was closed in a previous exercise, then click Start > Citrix > Citrix Studio.
15.	On the Settings page, in the All Settings drop-down, select **Printing** (under ICA heading) and type **Session** in the search box to the right of the drop-down box.
16.	Click **Edit** next to the **Session printers** setting.
17.	Within **Session printers**, click **Add** to add a new printer mapping. 
18.	On the **Add Printer** input box, type **\\NYC-FSR-001\HP_LJ_500** and click **OK**. 
19.	Click **OK** on the **Session printers** window.



20. On the Setting page, in the All Settings drop-down, select **Printing** (under ICA heading) and **Universal Print Server**.



21. Next to the **Universal Print Server enable**, click **Select**. Configure the following:
    - Value: **Enabled with fallback to Windows' native remote printing**

	 Click **OK** and click **Next**.
22.	On the Users and Machines page click **Next**.
23.	On the Summary page, click **Finish**. 
24.	Using the Remote Desktop Connection Manager, switch to **NYC-SRV-001**.
25.	Right-click **Start** and select **Command Prompt** to launch a command prompt. Enter the following command: **gpupdate /force** Close the **Command Prompt** after the command has completed successfully.

Key Takeaways:

- Before installing Citrix Universal Print Server software, every session printer would require a corresponding driver installed on the VDAs.
- The Citrix Universal Print Server reduces the amount of required printer drivers on VDAs for network based printers or session printer functionality.

Module 9: Citrix Profile Management

Overview:

This module presents the impact of user profiles in a XenApp and XenDesktop environment by focusing on Remote Desktop Services User Profiles and how to overcome issues with large profiles by using Citrix Profile Manager.

Before you begin:

Estimated time to complete Module 9 lab exercises: 45 minutes

Exercise 9-1: Configure Citrix Profile Management Using Group Policy

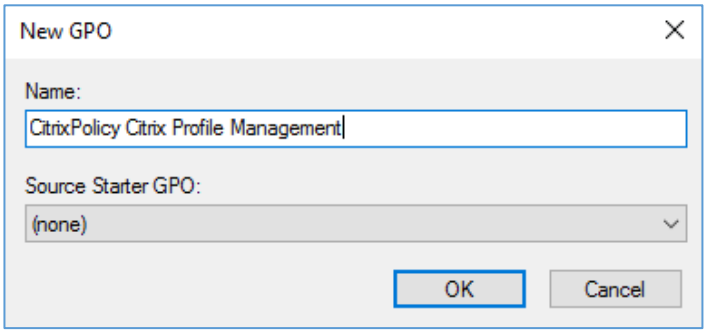
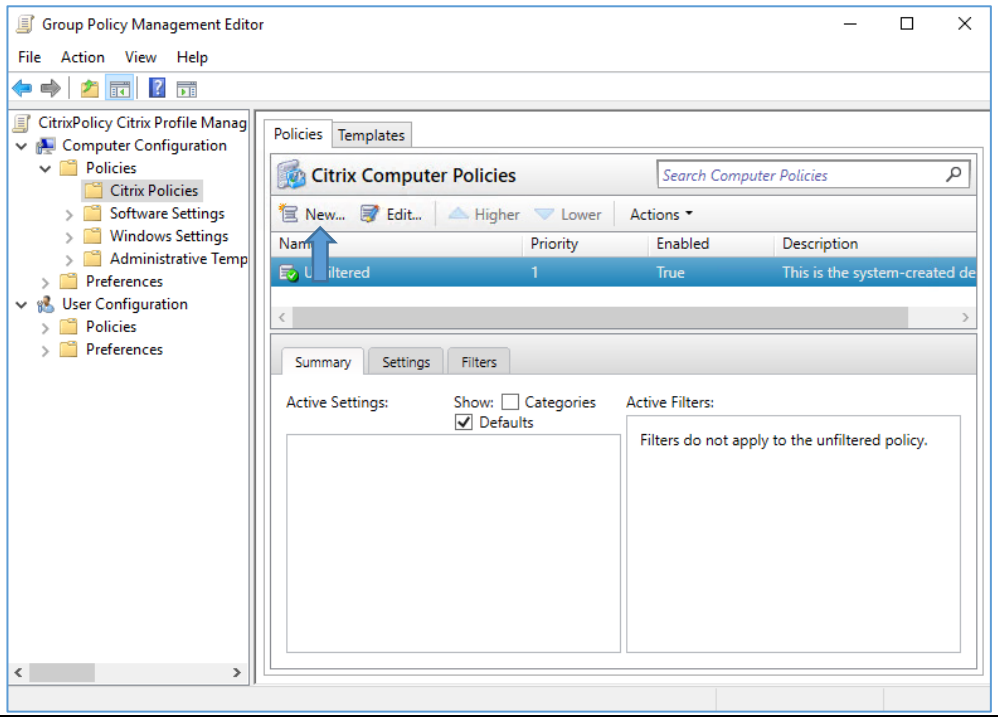
Scenario:

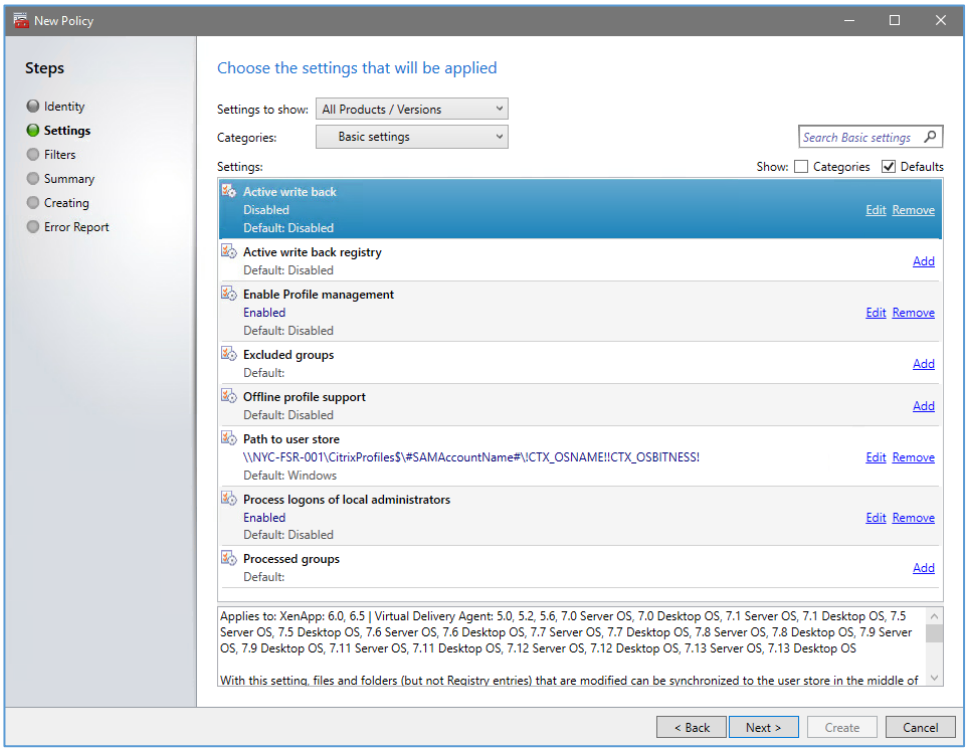
Citrix Profile Management is a Citrix solution that optimizes user profiles. It is both a Microsoft and Citrix Leading Practice to configure Folder Redirection using a GPO, to limit the amount of data copied into the session at logon time.

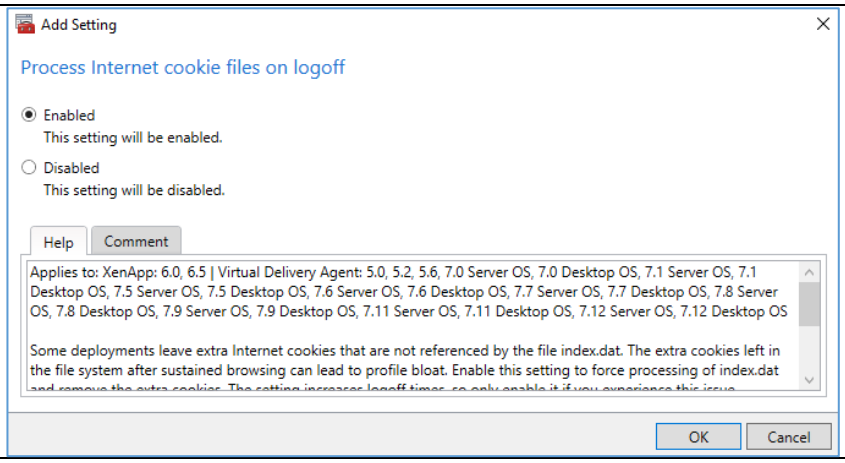
Your tasks are to configure the basic and the advanced settings for Citrix Profile Management using group policies; and to configure folder redirection.

The profile shares (HomeDrive$ & CitrixProfiles$) were pre-built into the lab, to improve the lab exercise efficiency. For more information about Configuring the User Profile Share, refer to the Exercise 9-1.

Step	Action
1.	The following VMs are required before beginning the exercises for this Module; all others may be powered down. To power manage your VMs, switch to XenCenter, right-click on the VM in the left pane and select Start or Shut Down. If prompted click Yes. • NYC-ADS-001 • NYC-SQL-001 • NYC-FSR-001 • NYC-XDC-001 • NYC-STF-001 • NYC-MAN-001 • NYC-SRV-001 • NYC-WRK-001 **Note**: These above VMs are listed in the start-up order.
2.	Using the Remote Desktop Connection Manager, connect to NYC-XDC-001. To log on to NYC-XDC-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1
3.	Launch **Server Manager** from the Windows Taskbar > click **Tools** > and then select **Group Policy Management** to launch the Group Policy Management Console.

4.	Expand **Forest: workspacelab.com** > **Domains** > **workspacelab.com** > **Citrix** > **New York** hierarchy and select the **VDA** OU. Right-click the **VDA** OU and select **Create a GPO in this domain, and Link it here**.
5.	In the New GPO dialog box, enter the following text for the Name: **CitrixPolicy Citrix Profile Management**  Click **OK**.
6.	Right-click the newly created **CitrixPolicy Citrix Profile Management** GPO and select **Edit**.
7.	Navigate to **Computer Configuration** > **Policies** > **Citrix Policies**.
8.	In the **Citrix Computer Policies** view, click **New** to create a new Citrix policy within the GPO. 
9.	On the Identity page, type **All Users-Citrix Profile Management** in the name field**,** and then click **Next**.
10.	On the Settings page, click the **Categories** drop-down and select **Profile Management\Basic settings**. **Note:** Selecting sub-categories will give you a simpler view and make it easier to locate the settings you are adjusting.
11.	Configure the following settings:

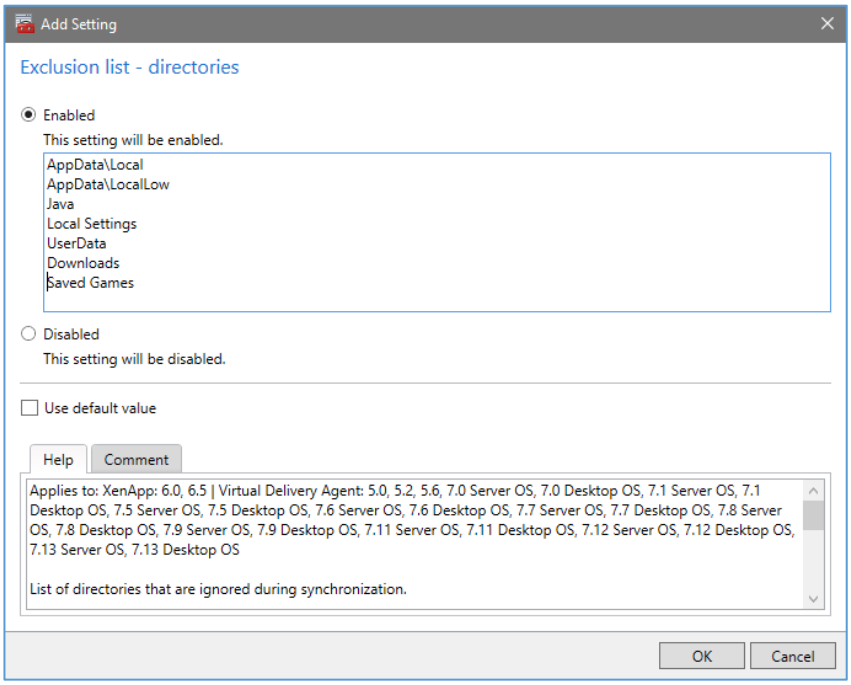
	• Active write back: **Disabled** • Enable Profile management: **Enabled** • Path to user store: **Enabled; \\NYC-FSR-001\CitrixProfiles$\#SAMAccountName#\!CTX_OSNAME!!CTX_OSBITNESS!** • Process logons of local administrators: **Enabled**  **Note**: When Active Write back is enabled, Citrix Profile Manager detects when an application has written and closed a file and copies the file back to the network copy of the profile during idle periods. In scenarios where a single user leverages multiple virtual desktops or hosted shared desktops simultaneously, this feature can be tremendously beneficial. Previously with Active Write back, Citrix Profile Management did not copy any registry changes back to the network, except during an ordered logoff. As such, there was a risk that the registry and files may get out of alignment on provisioned systems, where locally cached profile information is wiped upon reboot. This risk has now been mitigated with the new support for Registry Active Write Back.
12.	On the Settings page, click the **Categories** drop-down and select **Profile Management\Advanced settings**.
13.	Configure the following policy setting: • Process Internet cookie files on logoff: **Enabled**



14. On the Settings page, click the **Categories** drop-down and select **Profile Management\File system**.

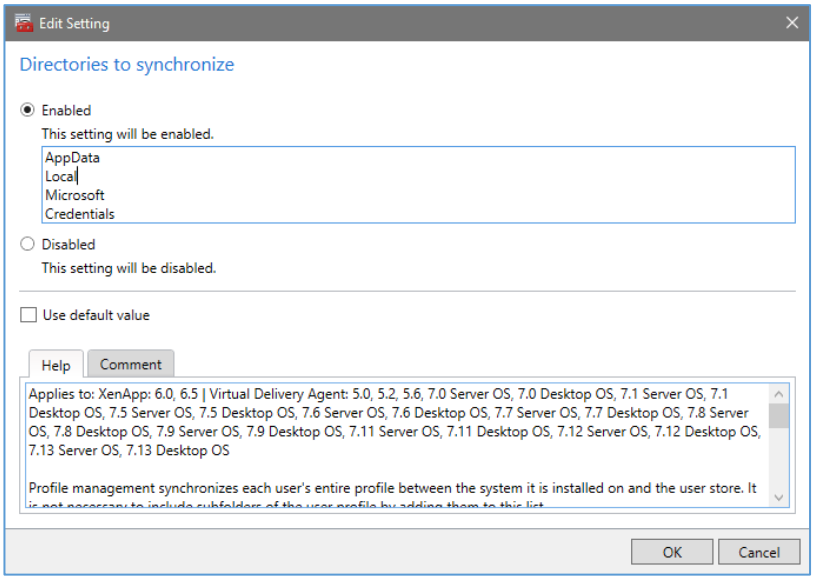
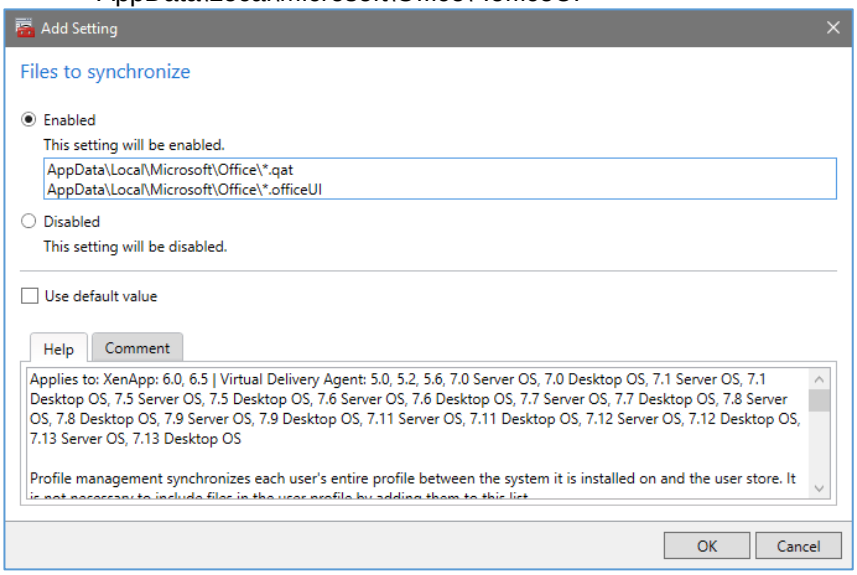
15. Configure the following policy setting:
    - Exclusion list – directories: **Enabled**

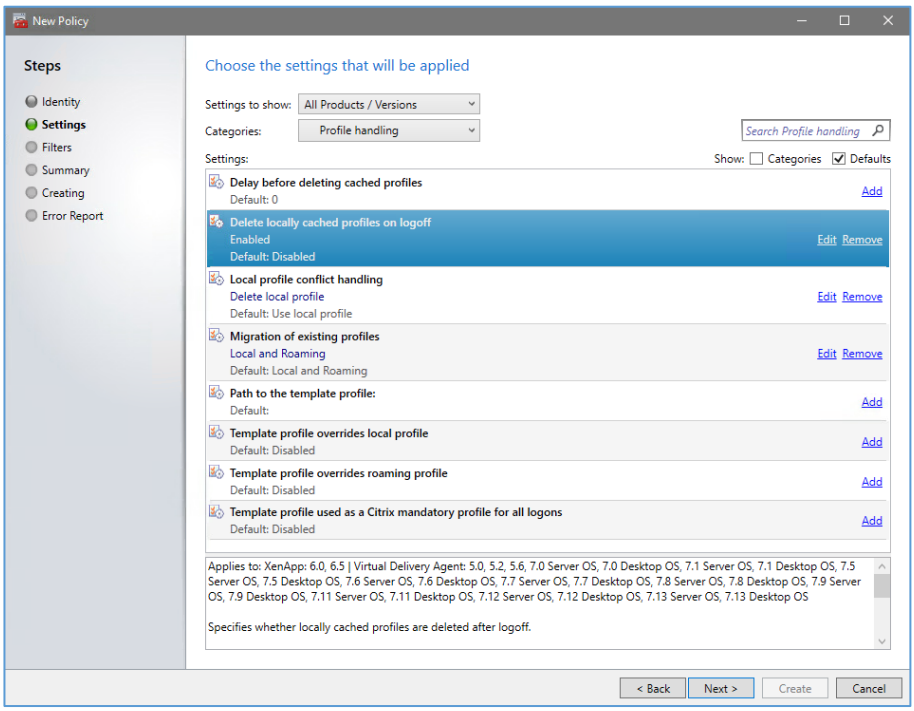
    Click **Enabled** and configure the following list of directories to exclude:
    - AppData\Local
    - AppData\LocalLow
    - Java
    - Local Settings
    - UserData
    - Downloads
    - Saved Games

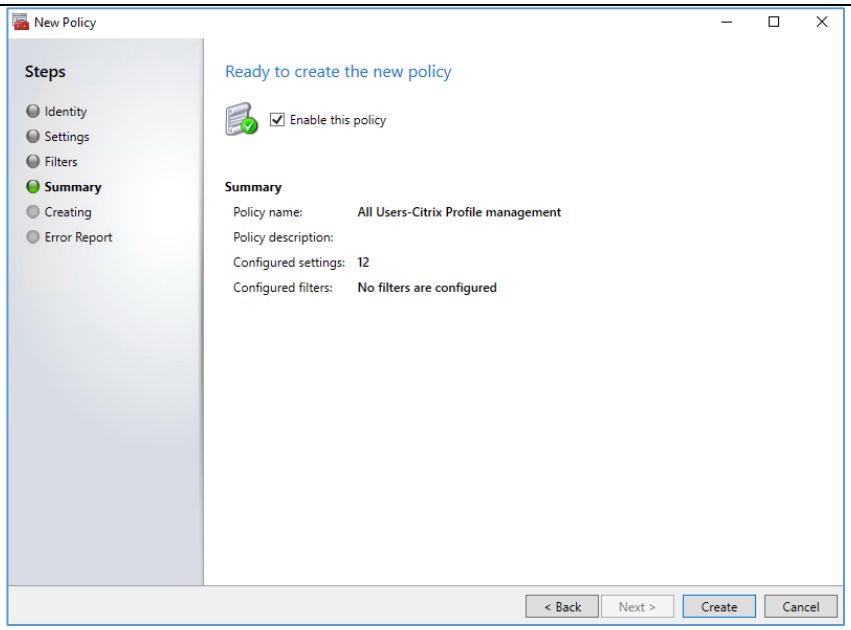


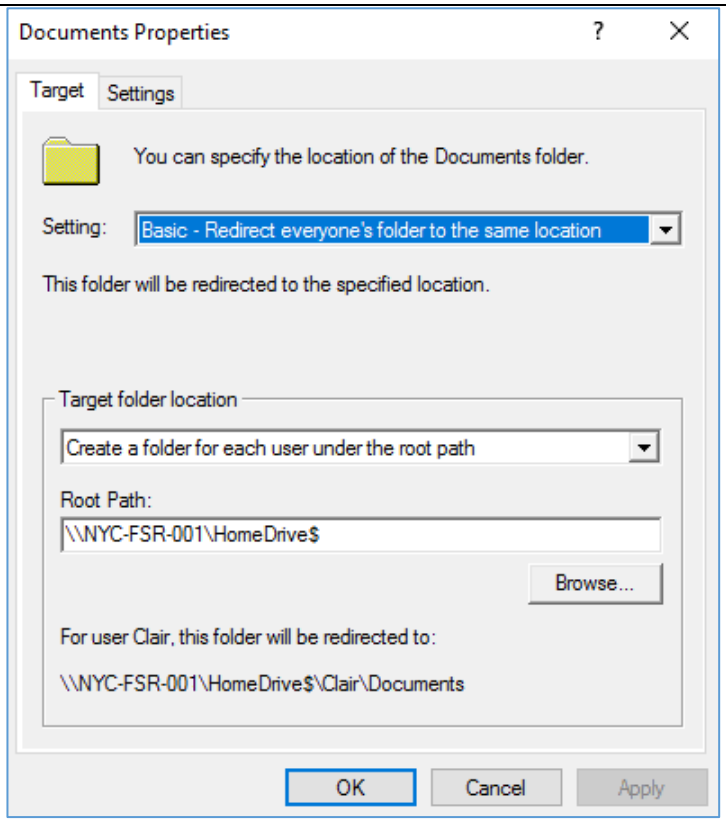
    Click **OK**.

16. Configure the following policy setting:
    - Directories to synchronize: **Enabled**

	Click **Enabled** and configure the following list of directories to synchronize: • AppData • Local • Microsoft • Credentials  Click **OK**.
17.	Files to synchronize: **Enabled** Click **Enabled** and configure the following list of files to synchronize: • AppData\Local\Microsoft\Office*.qat • AppData\Local\Microsoft\Office*.officeUI  Click **OK**.

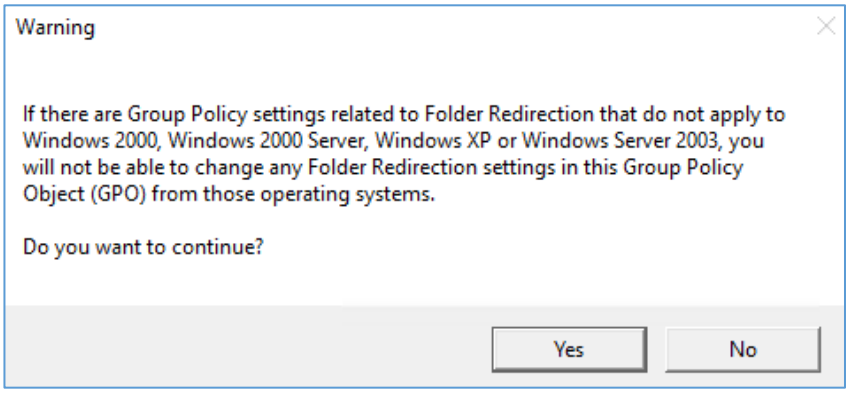
18.	On the Settings page, click the **Categories** drop-down and select **Profile Management\Profile handling**.
19.	Configure the following policy settings: • Delete locally cached profiles on logoff: **Enabled** • Migration of existing profiles: **Local and Roaming** • Local profile conflict handling: **Delete local profile**  **Note**: Citrix recommends deleting locally cached profiles on logoff to avoid the proliferation of stale profiles on the following two scenarios: • Hosted shared desktop servers • Hosted VDI pooled without immediate reboot on log off
20.	On the Settings page, click the **Categories** drop-down and select **Profile Management\Streamed user profiles**.
21.	Configure the following policy setting: • Profile streaming - **Enabled**. **Note:** With Profile streaming, files and folders contained in a profile are fetched from the user store (file server) to the local computer only when a user accesses them. During the logon process, Citrix Profile Management immediately reports that the profile load process has completed, reducing profile load time to almost zero.
22.	Click **Next** on the Settings page.
23.	On the Filters page, click **Next**.

	 **Note:** You can create multiple Citrix Policies with different settings and apply them to individual filters to make profile management more granular, but for this lab we are configuring identical settings for all users and Delivery Groups.
24.	On the Summary page, click **Create**.
25.	On the Citrix Computer Policies view, highlight the new policy and click **Higher** until the policy is on the top of the list.
26.	In the left pane of Group Policy Management Editor, navigate to **User Configuration** > **Policies** > **Windows Settings** > **Folder Redirection**. Right-click **Documents** and select **Properties**. Configure the following settings: • Setting: **Basic – Redirect everyone's folder to the same location** • Target folder location: **Create a folder for each user under the root path** • Root Path: **\\NYC-FSR-001\HomeDrive$**



Select the **Settings** tab on the top of the Properties dialog box and unselect **Grant the user exclusive rights to Documents**.

Click **OK**, then click **Yes** when prompted with the following warning:



Right-click each of the following folders and choose **Properties**.

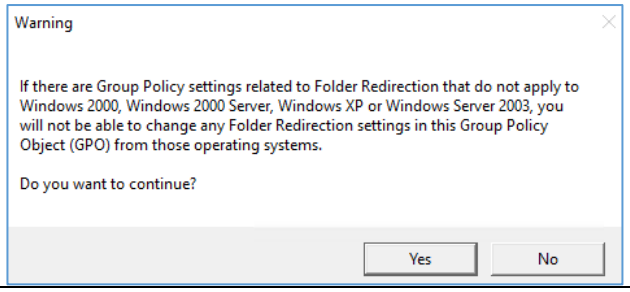
- AppData(Roaming)
- Desktop
- Start Menu
- Favorites
- Contacts
- Downloads
- Links
- Searches

Configure the following settings for each folder:

- Setting: **Basic – Redirect everyone's folder to the same location**
- Target folder location: **Create a folder for each user under the root path**
- Root Path: **\\NYC-FSR-001\HomeDrive$**

Select the **Settings** tab on the top of the Properties dialog box and unselect **Grant the user exclusive rights to Documents**.

Click **OK**, then click **Yes** when prompted with the following warning:

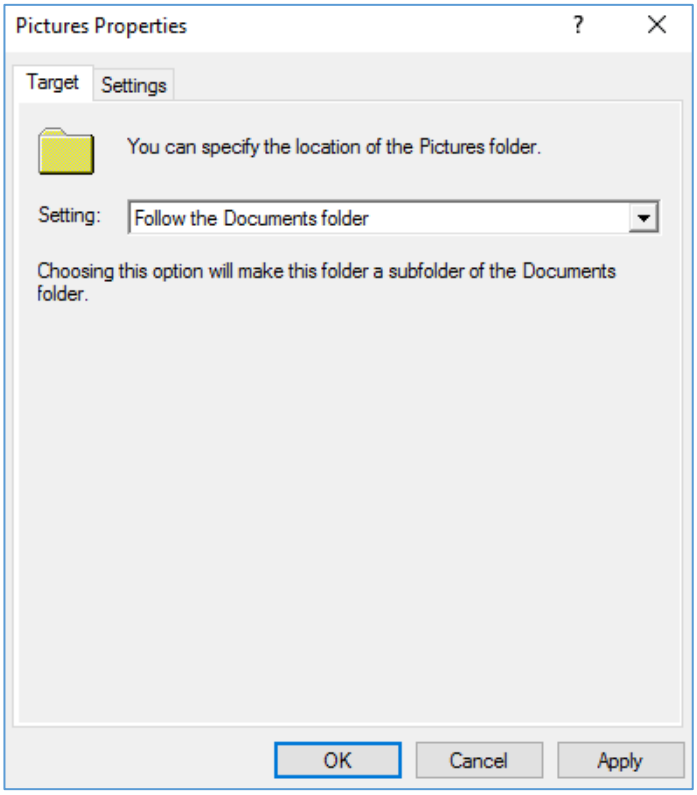


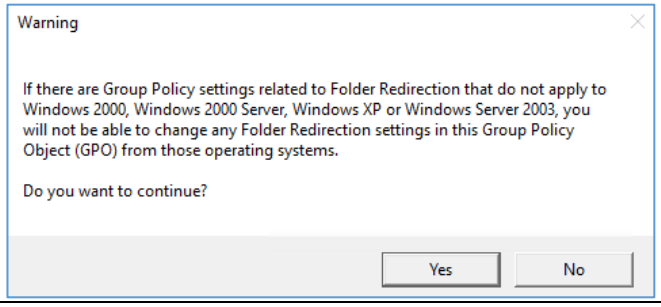
27. Right-click each of the following folders and choose **Properties**.

- Pictures
- Music
- Videos

Configure the following setting:

- Setting: **Follow the Documents folder**



	Click **OK**, then click **Yes** when prompted with the following warning: 
28.	**Close** the Group Policy Management Editor and **close** the Group Policy Management Console.

Key Takeaways:

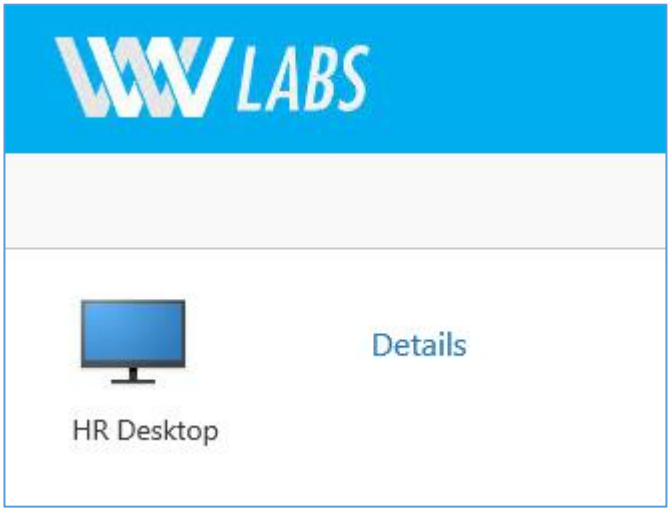
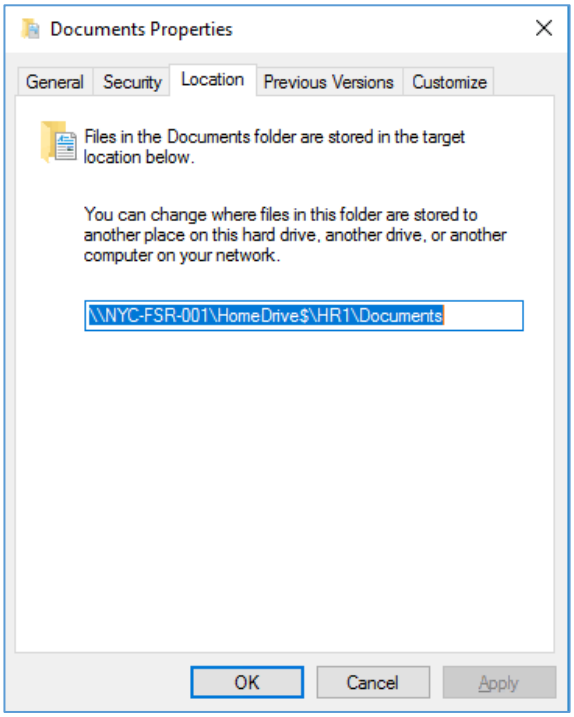
- Citrix Profile Management is installed together with the VDA component, but can be installed separately if required.
- Configure streaming profiles, folder redirection and exclusions to maximize logon performance.
- Redirected folders are simultaneously accessible from multiple sessions and can be used to interchange files between applications running on different VDAs or endpoint computers.
- Redirected folders induce some delay when manipulating files but save time during logon.
- Monitor file server performance when enabling folder redirection for large number of users.

Exercise 9-2: Test Citrix Profile Management

Scenario:

Your task is to test the profile login experience by validating the configured Citrix Profile Management group policies from a users' perspective and experiencing a faster logon with the optimized profile settings.

Step	Action
1.	Using the Remote Desktop Connection Manager, connect to NYC-SRV-001. To log on to NYC-SRV-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1
2.	Right-click **Start** and select **Command Prompt** to launch a command prompt. Enter the following command: **gpupdate /force** When prompted, type **Y** and press **Enter** to confirm that it is OK to log off.
3.	Using the Remote Desktop Connection Manager, connect to NYC-WRK-001. To log on to NYC-WRK-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\HR1 • Password: Password1
4.	Log on to **Citrix Receiver** using the following credentials: • User name: **HR1** • Password: **Password1**

	Select the **DESKTOPS** tab and launch the **HR Desktop**.  **Note**: During this first logon (remember this is the first logon for HR1), the folders are redirected to the new location. The **logon process will not be fast**.
5.	Log off the **HR Desktop**. **Note:** Make sure to log off the desktop by right-clicking **Start** > choosing **Shut down or sign out** > **Sign out**. Do not disconnect the desktop.
6.	Launch the **HR Desktop**. **Note:** The logon time is much quicker with folder redirection enabled.
7.	Within the HR Desktop, open **File Explorer**, right-click **Documents**, and select **Properties**. Select the **Location** tab to verify that the folder is successfully redirected. 

8.	Log off the **HR Desktop** and log off **NYC-WRK-001**. Log HR1 out of Receiver.

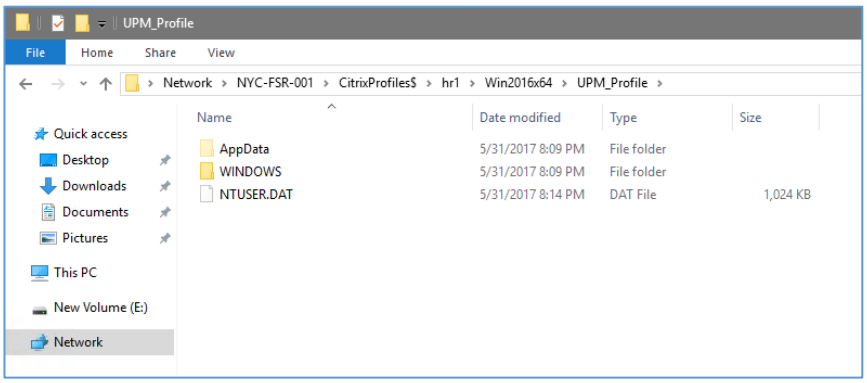
Key Takeaways:

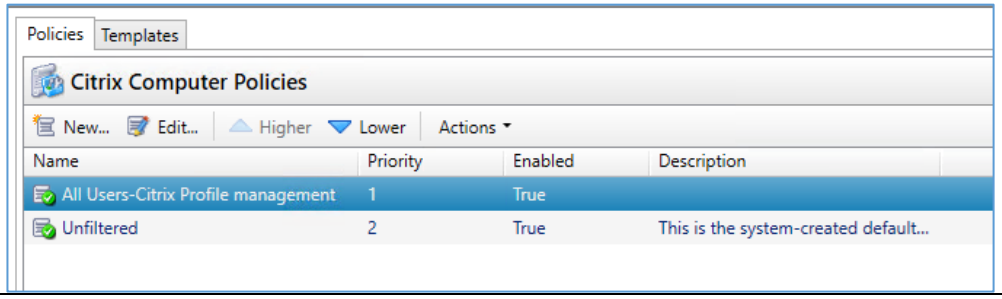
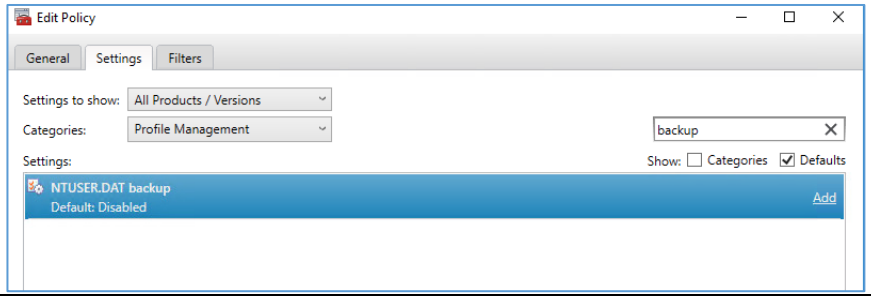
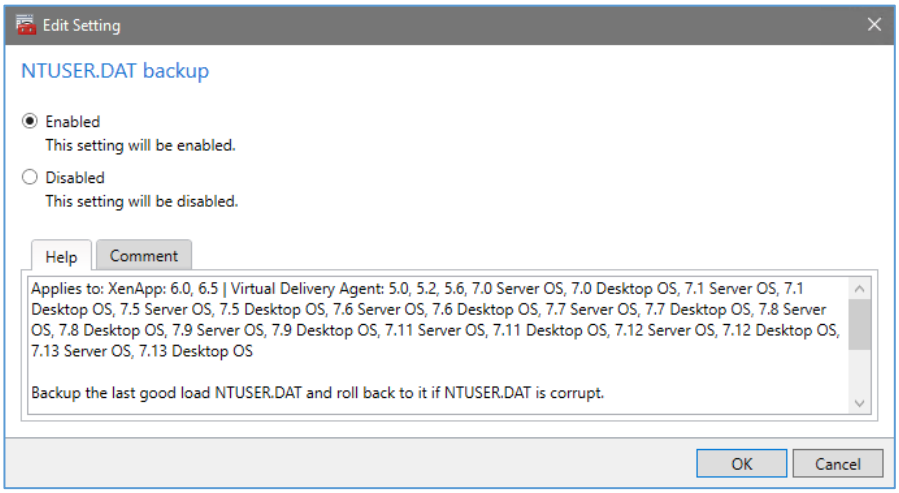
- Streaming the profile means that we only load the necessary files and folders from the profile as a needed throughout the session; a much lighter approach than copying the full profile during logon.
- Use folder redirection to speed up profile loading and to share common folders amongst different sessions.

Exercise 9-3: Configure Profile Protection

Scenario:

The WW Labs CTO has tasked the Citrix team to ensure that the roaming profile solution used in the POC will provide both fast user logons and profile stability. You are tasked to enable the profile protection feature of Citrix Profile Management, which you expect will reduce the amount of help desk calls related to profile corruptions.

Step	Action
1.	Using the Remote Desktop Connection Manager, confirm that you are still connected to **NYC-FSR-001**.
2.	Browse to **\\NYC-FSR-001\CitrixProfiles$\HR1\Win2016x64\UPM_Profile**. Click the **view** tab and enable **File name extensions** and **Hidden Items**. Validate the profile directory does not have a file by the name – **NTUSER.DAT.LASTGOODLOAD.** 
3.	Using the Remote Desktop Connection Manager, switch to **NYC-XDC-001**. **Note**: In a previous exercise, you had logged on to NYC-XDC-001 using the following credentials to make the connection: • User name: Workspacelab\Administrator • Password: Password1 **Note**: If your Remote Desktop Connection session disconnected, log on to NYC-XDC-001 by right-clicking this machine and selecting Connect server.

4.	Maximize the **Group Policy Management Console** and click on **VDA** OU on the left.
5.	Right-click **CitrixPolicy Citrix Profile Management** policy and select **Edit**.
6.	In the left pane of Group Policy Management Editor, navigate to **Computer Configuration** > **Policies** > **Citrix Policies**. Select **All Users-Citrix Profile management** and click **Edit**. 
7.	Click the **Settings** tab in the edit window and select **Profile Management** in the Categories drop-down. Type **Backup** in the top right search bar. 
8.	Click **Add** next to NTUSER.DAT backup policy and select the **Enabled** radio button.  Click **OK** twice.
9.	**Close** the Group Policy Management Editor for CitrixPolicy Citrix Profile Management.

Key Takeaways:

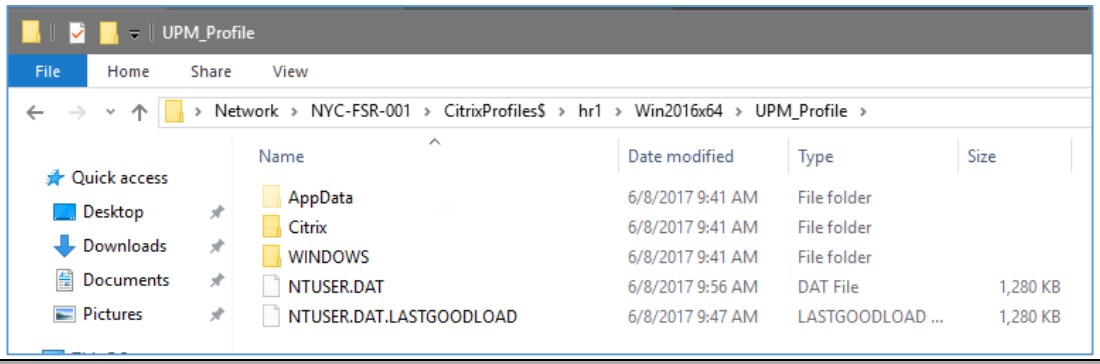
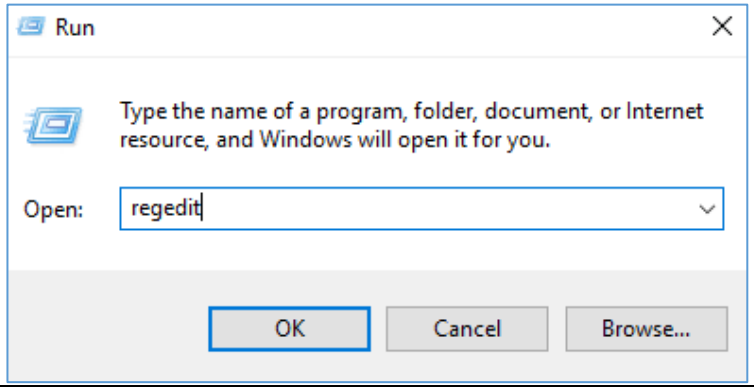
- Enabling Profile Protection is simple when your profile strategy is already based on Citrix Profile Management.
- The feature can also be enabled through .ini file configuration of Citrix Profile Management.

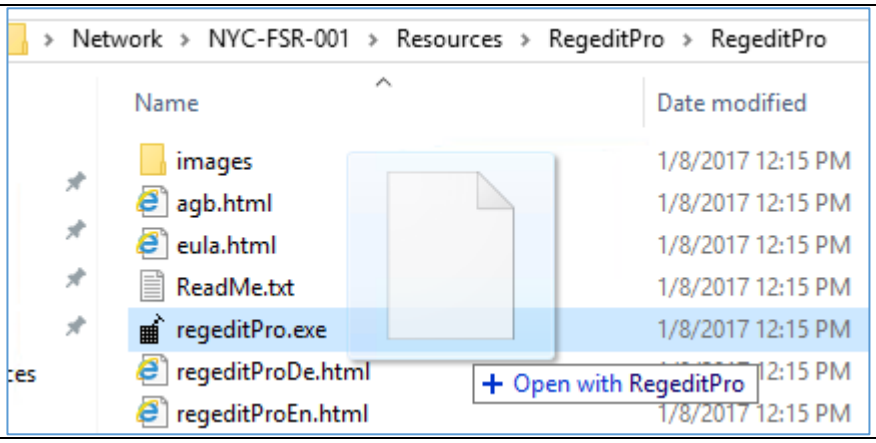
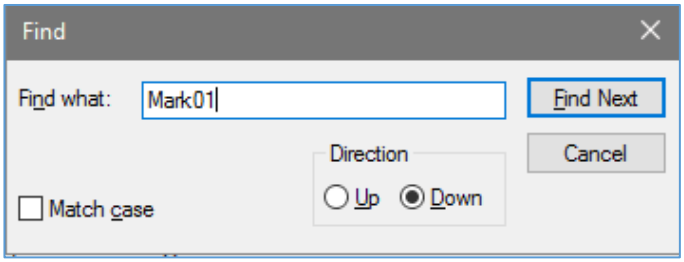
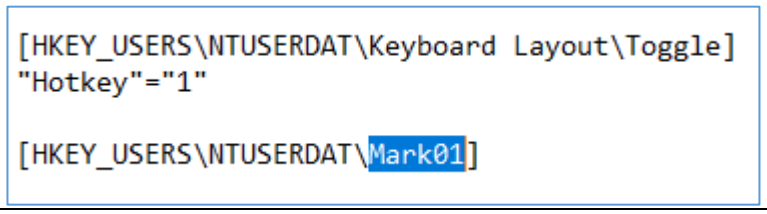
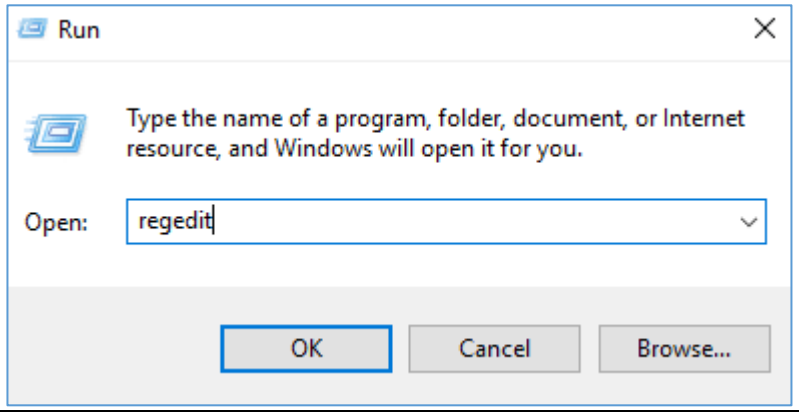
Exercise 9-4: Test Profile Protection

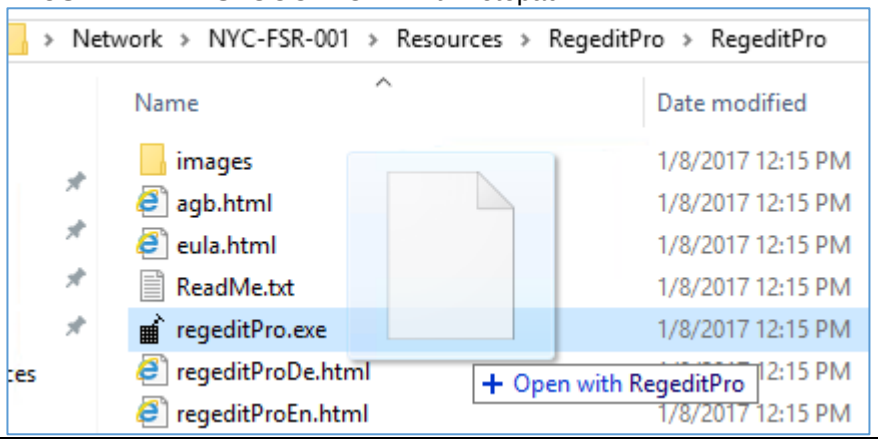
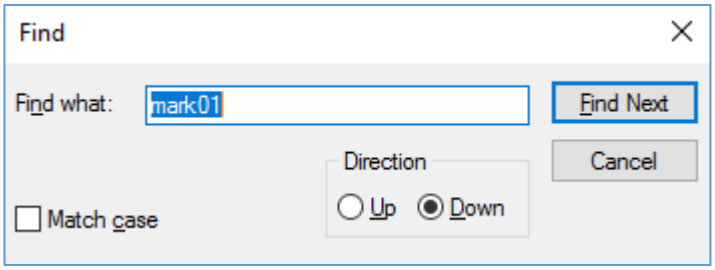
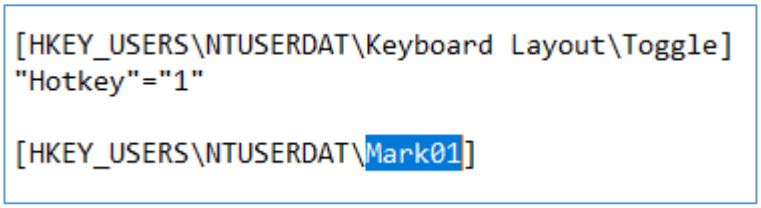
Scenario:

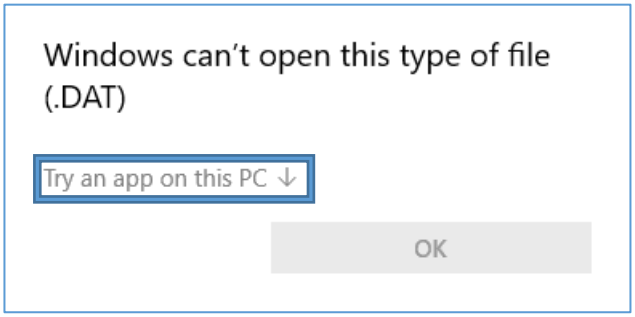
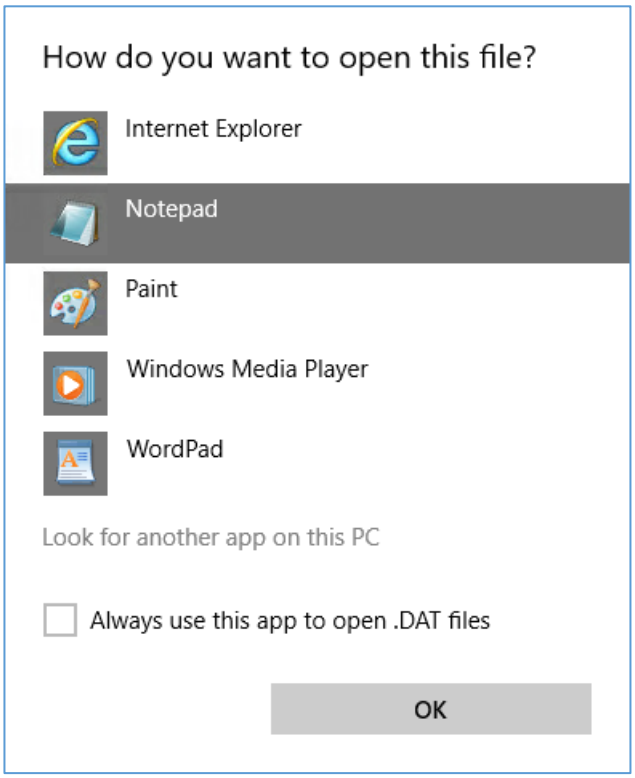
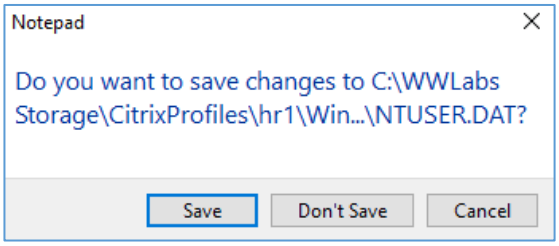
Upon completing the configuration of Profile Protection, you decide to test the feature. You investigate old help desk tickets and learn that most of the profile problems were caused by the NTUser.DAT being corrupted. In order to simulate this behavior, you decide to manually corrupt a user's profile and then have Profile Protection restore the last known good NTUser.DAT for the test user.

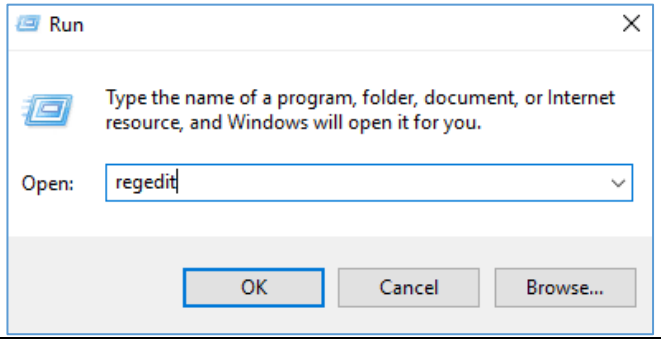
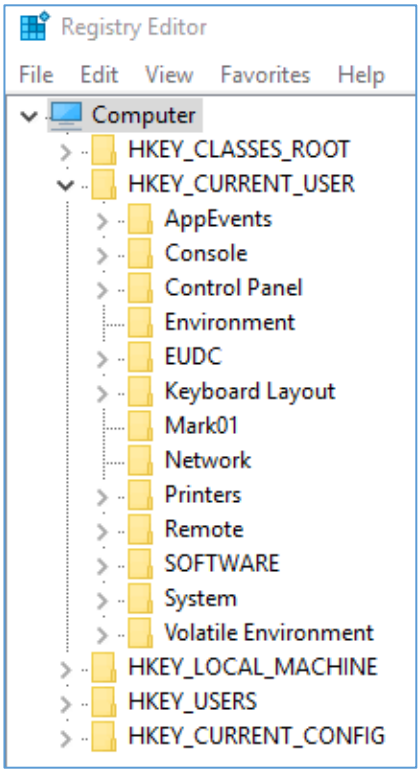
Step	Action
1.	Using the Remote Desktop Connection Manager, connect to NYC-SRV-001. To log on to NYC-SRV-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\Administrator • Password: Password1
2.	Right-click **Start**, select **Command Prompt** to launch a command prompt. Enter the following command: **gpupdate /force** When prompted, type **Y** and press **Enter** to log off.
3.	Using the Remote Desktop Connection Manager, connect to NYC-WRK-001. To log on to NYC-WRK-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\HR1 • Password: Password1
4.	Log on to **Citrix Receiver** using the following credentials: • User name: **HR1** • Password: **Password1** Select the **DESKTOPS** tab to launch the **HR Desktop**.
5.	Wait for the Desktop launch to complete. Log off the **HR Desktop**. **Note**: Make sure to log off the desktop by right-click **Start** > choose **Shut down or sign out** > and click **Sign out**. Do not disconnect the desktop.

6.	Switch back to **NYC-FSR-001** using the Remote Desktop Connection Manager. Browse to **\\NYC-FSR-001\CitrixProfiles$\HR1\Win2016x64\UPM_Profile**. Validate the profile directory has backup of NTUSER.DAT file- **NTUSER.DAT.LASTGOODLOAD**. 
Test the NTUSER.DAT backup.	
7.	Switch to NYC-WRK-001 and launch the **HR Desktop**.
8.	Within the HR Desktop, right-click **Start** select **Run**. Type **Regedit** and click **OK**. 
9.	Under HKEY_CURRENT_USER create a registry key – Mark01 Right-click **HKEY_CURRENT_USER > New > Key** Type **Mark01** in the key name.
10.	Log off the **HR Desktop**. **Note**: Make sure to log off the desktop by right-click **Start** > choose **Shut down or sign out** > and click **Sign out**. Do not disconnect the desktop.
11.	Switch back to **NYC-FSR-001** using the Remote Desktop Connection Manager. Browse to **\\NYC-FSR-001\CitrixProfiles$\HR1\Win2016x64\UPM_Profile**. In a separate File Explorer browse to **\\NYC-FSR-001\Resources\RegeditPro**.
12.	Drag **NTUSER.DAT** and drop onto **Regeditpro.exe** to read NTUSER.DAT with notepad.

	
13.	In the Notepad window press Ctrl+F and type **Mark01** in the Find what field. 
14.	Validate that the recently created Registry key is present in the NTUSER.DAT file. 
15.	**Close** the Notepad window.
16.	Switch to **NYC-WRK-001** and launch the **HR Desktop**.
17.	Within the HR Desktop, right-click **Start** and select **Run**. Type **Regedit** and click **OK**. 
18.	Under HKEY_CURRENT_USER create a registry key – Mark02 Right-click **HKEY_CURRENT_USER > New > Key**. Type **Mark02** in the key name. **Close** Regedit.

19.	Log off the **HR Desktop**. **Note**: Make sure to log off the desktop by right-click **Start** > choose **Shut down or sign out** > and click **Sign out**. Do not disconnect the desktop.
20.	Switch back to **NYC-FSR-001** using the Remote Desktop Connection Manager. Browse to **\\NYC-FSR-001\CitrixProfiles$\HR1\Win2016x64\UPM_Profile**. In a separate File Explorer browse to **\\NYC-FSR-001\Resources\RegeditPro**.
21.	Drag **NTUSER.DAT.LASTGOODLOAD** and drop onto **Regeditpro.exe** to read NTUSER.DAT.LASTGOODLOAD with notepad. 
22.	In the Notepad window press Ctrl+F and type **Mark01** in the Find what field. 
23.	Validate that the recently created Registry key is present in the NTUSER.DAT.LASTGOODLOAD file.  **Close** the Notepad window. **Note:** Similarly read the NTUSER.DAT file using the regeditpro tool. NTUSER.DAT has mark01 and mark02 keys both. Now we will make NTUSER.DAT corrupt to demonstrate how UPM uses the backup file.
24.	On **NYC-FSR-001** browse to **C:\WWLabs Storage\CitrixProfiles\hr1\Win2016x64\UPM_Profile** and double-click on **NTUSER.DAT**.

	On the **Windows can't open this type of file (.DAT)** window, click on **Try an app on this PC**  Select **Notepad** and click **OK**. 
25.	Select the initial 50-100 lines and press **delete** to remove the content. **Note**: Manually tampering with the NTUSER.DAT will make it a corrupt file.
26.	**Close** Notepad. When prompted to save changes click **Save**. 

27.	Switch to **NYC-WRK-001** and launch the **HR Desktop**.
28.	Within the HR Desktop, right-click **Start** and select **Run**. Type **Regedit** and click **OK**. 
29.	Under HKEY_CURRENT_USER locate the registry key **Mark01**.  **Note**: Mark01 is available but Mark02 is not available. This proves that UPM used the backup file to accomplish the user logon.
30.	Log off the **HR Desktop**. **Note**: Make sure to log off the desktop by right-click **Start** > choose **Shut down or sign out** > and click **Sign out**. Do not disconnect the desktop.

Key Takeaways:

- Profile management maintains a last known good backup of the NTUSER.DAT file. If Profile management detects corruption, it uses the last known good backup copy to recover the profile.

Module 10: Managing the XenApp and XenDesktop Site

Before you begin:

Estimated time to complete Module 10 lab exercises: 25 minutes

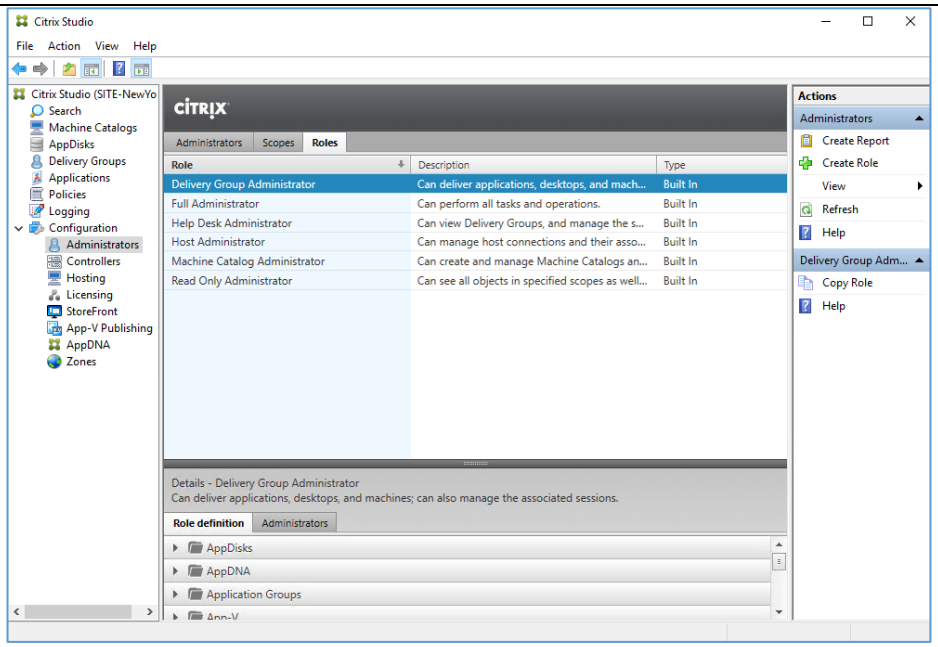
Exercise 10-1: Create a Custom Role

Scenario:

The Citrix Lead Architect has requested that a manager receive access to the management consoles of this POC environment. Specifically, this manager needs visibility into the progress of this POC and all configured elements in the Site database; however, you must limit this manager's permission to allow the right to view, but not to make any changes. You also need to grant some license viewing capabilities without seeing the license warnings from your Evaluation and Trial license.

Your task is to delegate these permissions by first creating a Custom Role.

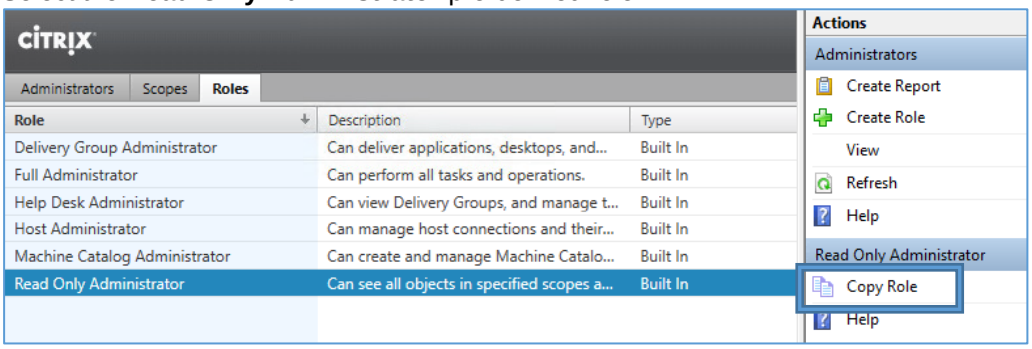
Step	Action
1.	The following VMs are required before beginning the exercises for this Module; all others may be powered down. To power manage your VMs, switch to XenCenter, right-click on the VM in the left pane and select Start or Shut Down. If prompted click Yes. • NYC-ADS-001 • NYC-SQL-001 • NYC-FSR-001 • NYC-XDC-001 • NYC-STF-001 • NYC-MAN-001 • NYC-SRV-001 • NYC-WRK-001 **Note**: These above VMs are listed in the start-up order.
2.	Using the Remote Desktop Connection Manager, confirm you are still connected to **NYC-XDC-001**. **Note**: In a previous exercise, you had logged on to **NYC-XDC-001** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-XDC-001**, right-click this machine and choose **Connect server**.
3.	Using Studio, expand **Citrix Studio (SITE-NewYork)** > **Configuration** and select **Administrators**. In the center pane click on the **Roles** tab.



Note: The Welcome Delegated Administration dialog box shows. Read the definition of Scopes, Administrators and Roles, click **Don't show this again** and then click **Close**.

Note: Studio was launched in a previous exercise. If Studio was closed in a previous exercise, then click **Start** > **Citrix** > **Citrix Studio**.

4. Select the **Read Only Administrator** pre-defined role.

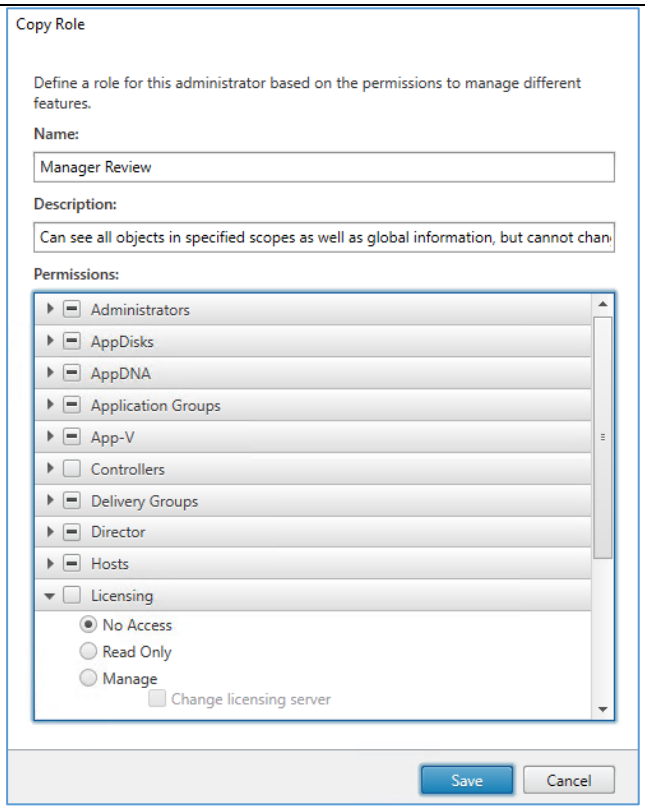


In the right pane, under Read Only Administrator click **Copy Role**.

5. In the Name field, type **Manager Review**.

   On the Description field leave the default description: **Can see all objects in specified scopes as well as global information, but cannot change anything**.

6. Under Permissions, expand **Licensing** and change the radio button to **No Access**.

	 **Note**: Click on Wait for the program to respond on Microsoft Management Console window, if prompted.
7.	Click **Save**.

Key Takeaways:

- For each object type that you want the new role to have permissions for, select the object type, and then select the permissions.
- Built-in Roles can be used to create new Custom Roles.

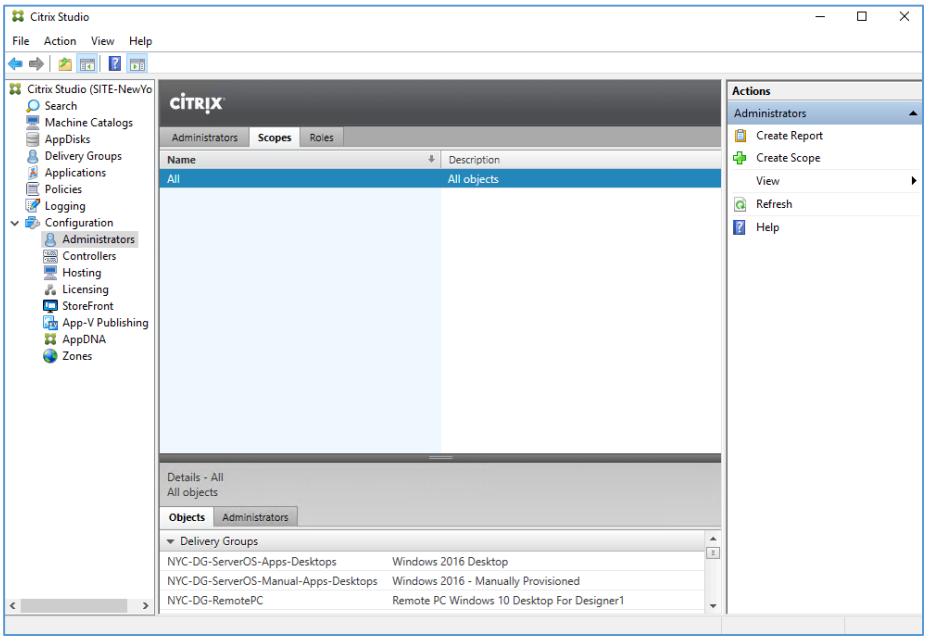
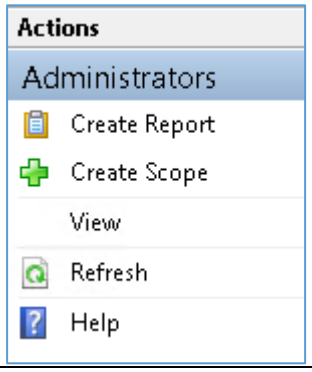
Exercise 10-2: Create a Custom Scope

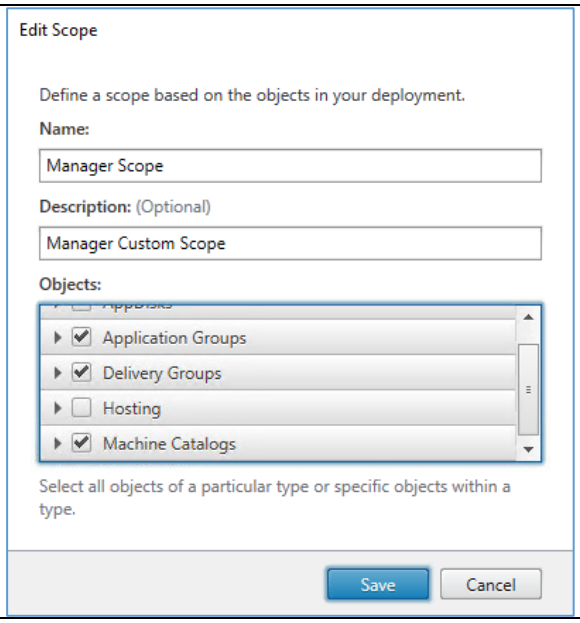
Scenario:

Your task is to continue to delegate permissions to this manager and further limit the viewing of the hosting connections when logging into Studio.

Since this is a POC and production hypervisor decisions have yet to be made, you want to ensure that the manager does not think that the production environment is limited to only one brand of hypervisors.

Step	Action
1.	Using the Remote Desktop Connection Manager, confirm you are still connected to **NYC-XDC-001**. **Note:** In a previous exercise, you had logged on to **NYC-XDC-001** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-XDC-001**, right-click this machine and choose **Connect server**.

2.	Using Studio, expand **Citrix Studio (SITE-NewYork)** > **Configuration** and select **Administrators**. In the center pane click on the **Scopes** tab.  **Note**: Studio was launched in a previous exercise. If Studio was closed in a previous exercise, then click **Start** > **Citrix** > **Citrix Studio**.
3.	In the Actions pane, click **Create Scope**. 
4.	In the Name field type **Manager Scope** and for the Description field type **Manager Custom Scope**. Under the Objects field, select only **Application Groups, Delivery Groups** and **Machine Catalogs**.

	
5.	Click **Save**.

Key Takeaways:

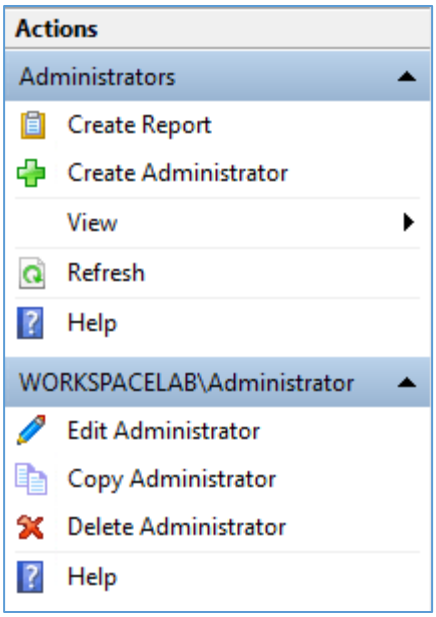
- During installation, only one scope is configured, which is called All and contains all objects in the database.
- The All Scope cannot be adjusted.
- Custom scopes can be created to partition the objects in the database, allowing a delegated administrator to see only a subset of objects from the database.
- When creating a custom Scope, you can only add objects that are currently created on the database; as you create more Catalogs and Delivery Groups, you may need to edit the scopes to ensure these new objects are added.

Exercise 10-3: Create Delegated Administrator Accounts

Scenario:

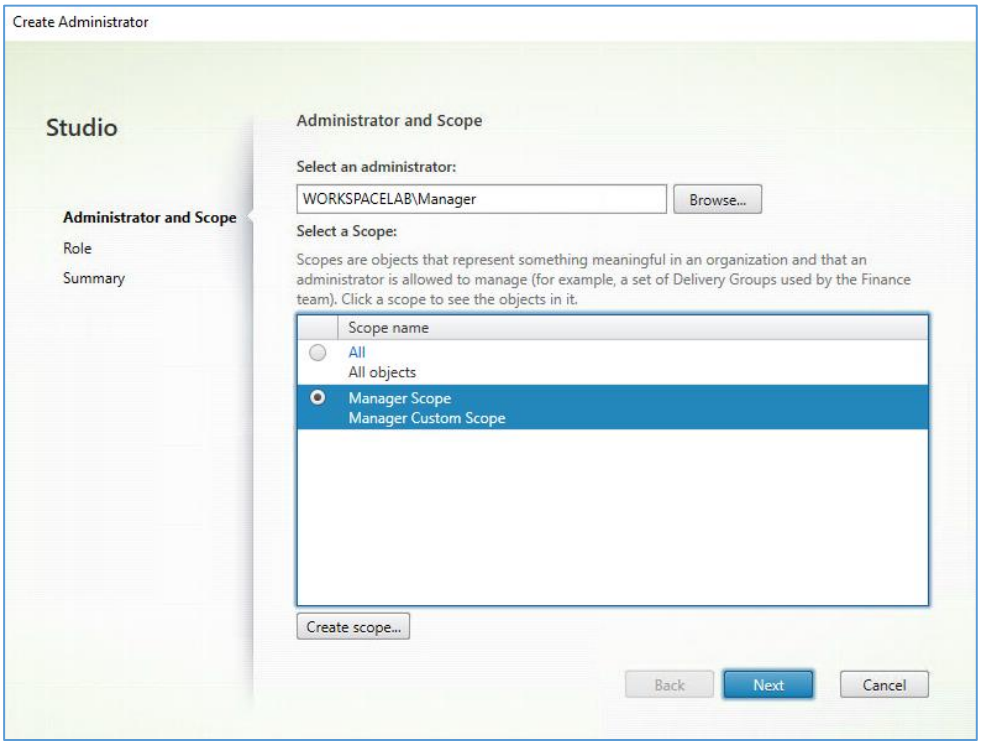
With the Role and Scope configured, the final step in delegating administration permissions to the manager is to create the Administrator.

Step	Action
1.	Using the Remote Desktop Connection Manager, confirm you are still connected to **NYC-XDC-001**. **Note:** In a previous exercise, you had logged on to **NYC-XDC-001** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-XDC-001**, right-click this machine and choose **Connect server**.
2.	Using Studio, expand **Citrix Studio (SITE-NewYork)** > **Configuration** and select **Administrators**. In the center pane click on the **Administrators** tab. In the right pane, under Actions click **Create Administrator**.



Note: Studio was launched in a previous exercise. If Studio was closed in a previous exercise, then click **Start** > **Citrix** > **Citrix Studio**.

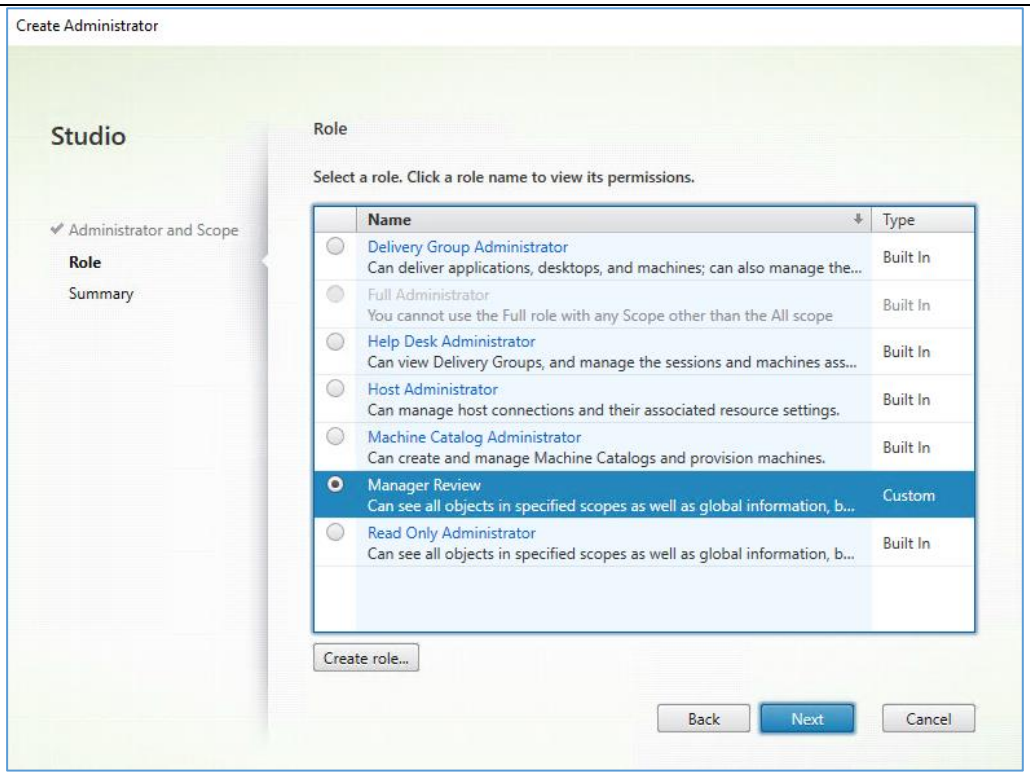
3. Type **WORKSPACELAB\Manager** in the Select an administrator field.



Click the **Manager Scope** radio button.

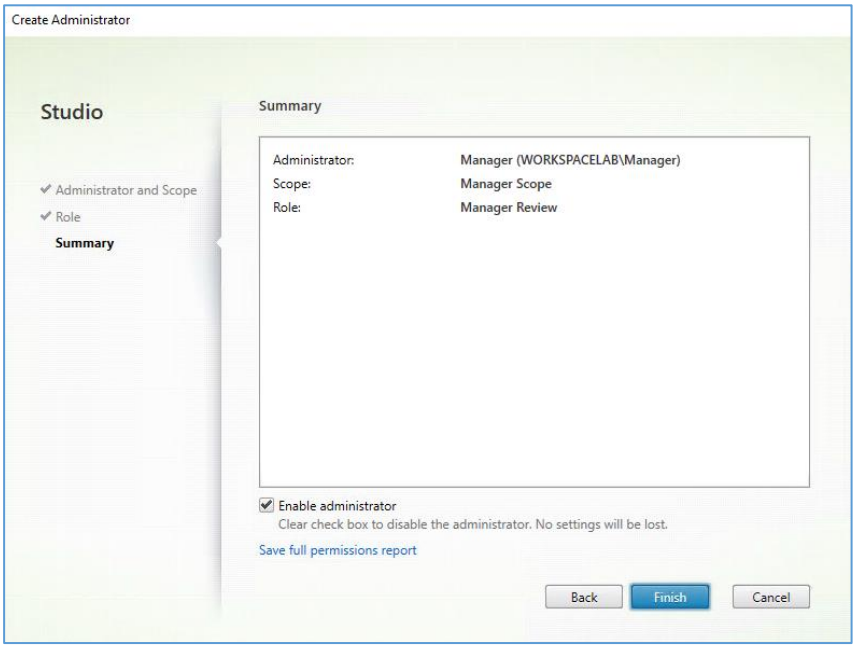
Click **Next**.

4. On the Role page, select the **Manager Review** role created previously.



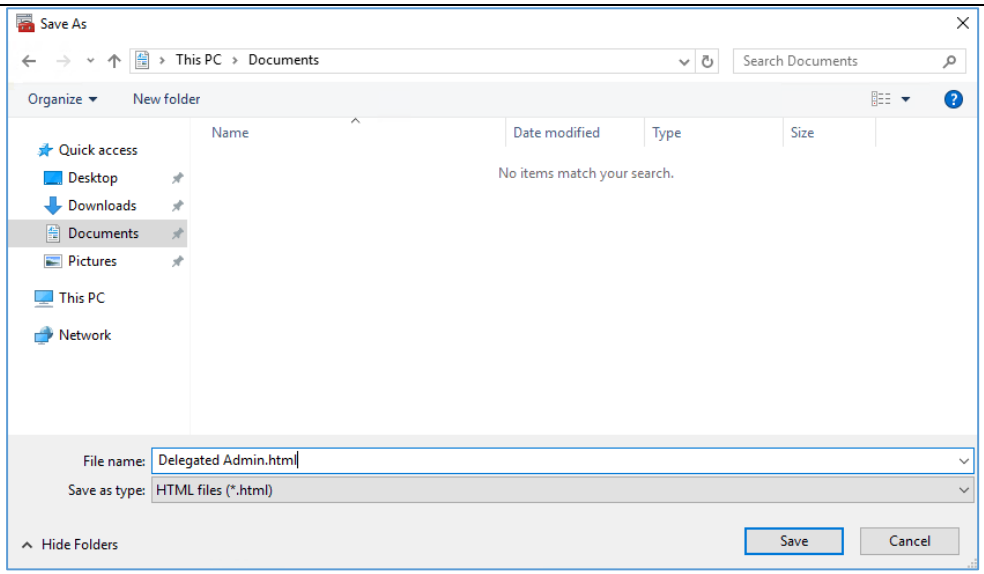
Click **Next**.

5. On the Summary page, review the details of the new administrator.



To create a report listing all the permissions the administrator will have, click **Save full permissions report**.

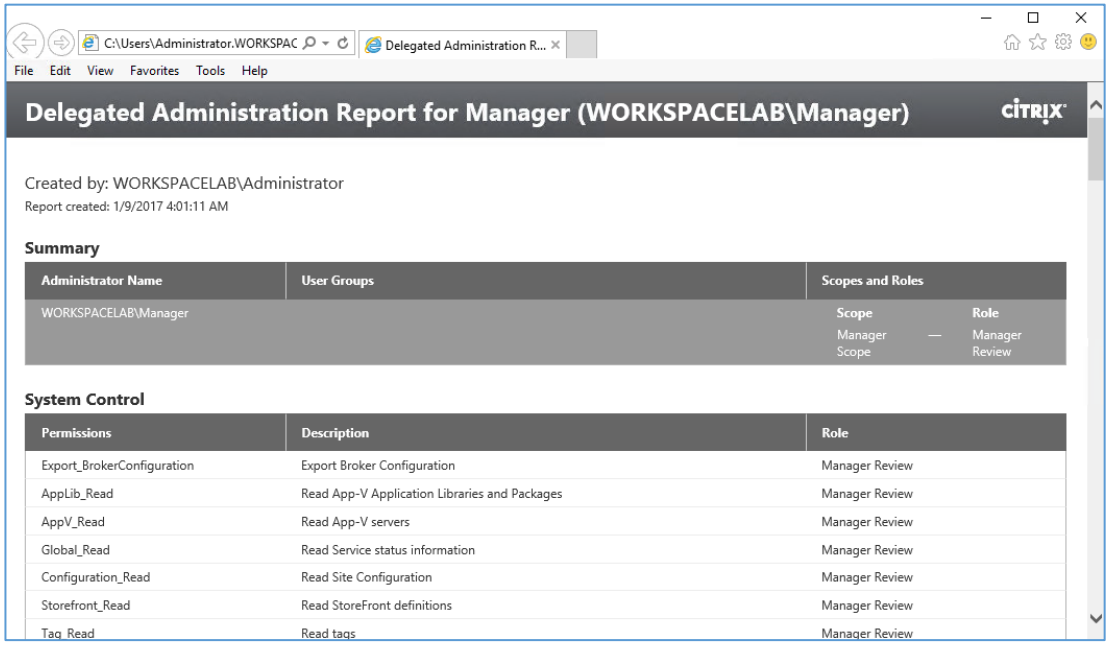
Save the report to the **Documents** folder with the name **Delegated Admin.html**.



Click **Save** and then click **Finish**.

6. Launch **File Explorer** from the Windows Taskbar.

   Click **This PC** on the left column, double-click the **Documents** folder and then double-click the **Delegated Admin.html** file.



   Note: If prompted with a message **How do you want to open this type of file (.html)?**, select a browser to use for the report.

7. Once you are done reviewing the content of the report, **close** the report and close the **File Explorer**.

Takeaways:

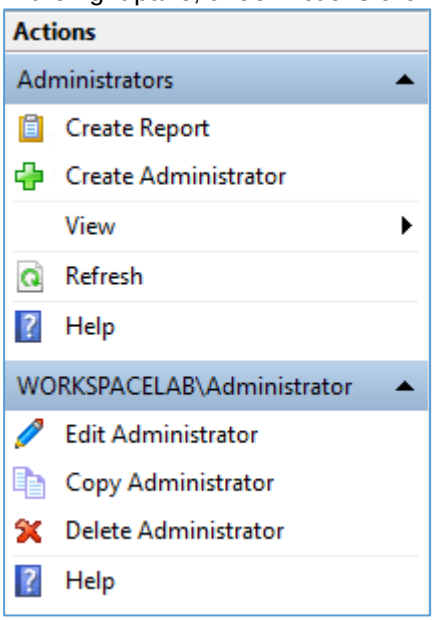
- When creating an Administrator, you can specify the objects the administrator can access by selecting a scope. You can select an existing scope or create a new one.

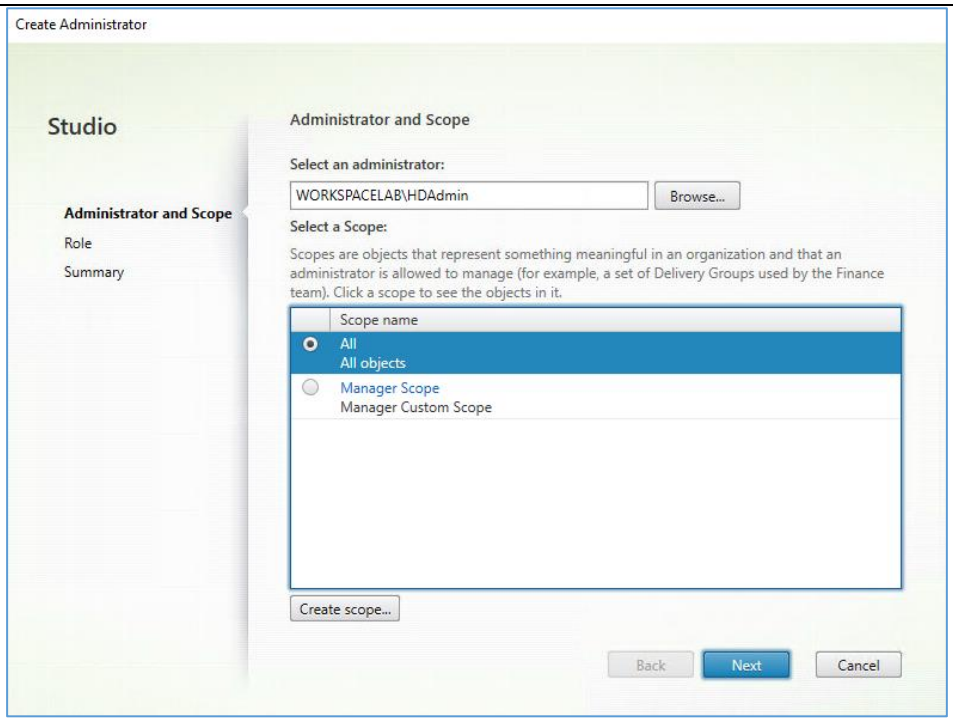
- To define the permissions an administrator has for the scoped objects, a role needs to be defined.
- A new administrator is enabled by default. To disable the new administrator, clear the Enable Administrator checkbox.
- To create a report listing all the permissions the administrator will have, click Create a full permissions report for this Administrator (HTML format).

Exercise 10-4: Create Help Desk Delegated Administrator

Scenario:

Your task is to continue delegating administration to the Citrix Site, by creating a Help Desk delegated administrator with the parameters that set the appropriate rights to execute helpdesk related tasks in Studio and Director. This task must ensure the Help Desk delegated administrator is not limited from viewing any objects in the site.

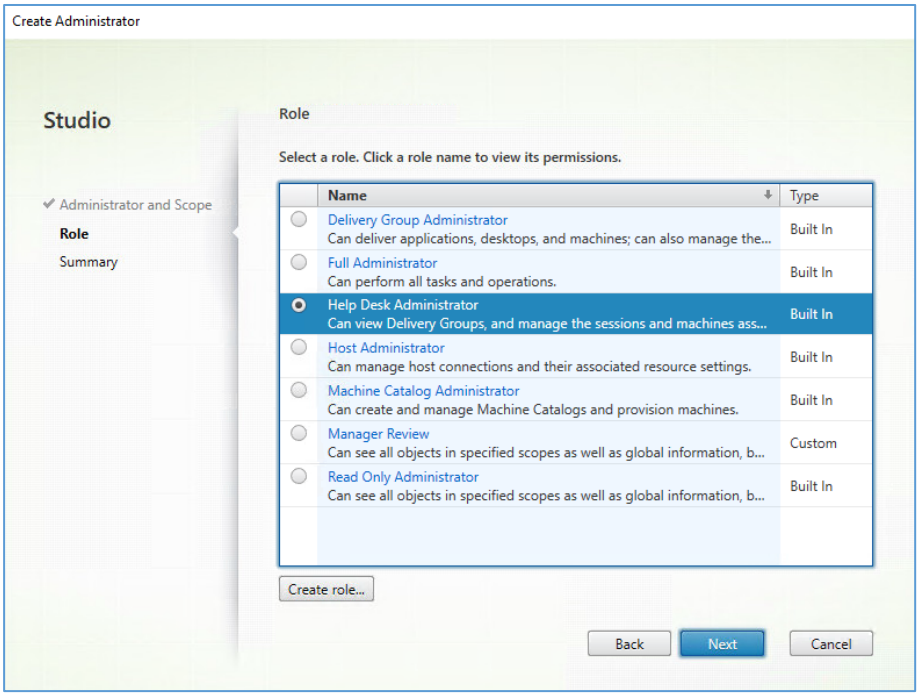
Step	Action
1.	Using the Remote Desktop Connection Manager, confirm you are still connected to **NYC-XDC-001**. **Note:** In a previous exercise, you had logged on to **NYC-XDC-001** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-XDC-001**, right-click this machine and choose **Connect server**.
2.	Using Studio, expand **Citrix Studio (SITE-NewYork)** > **Configuration** and select **Administrators**. In the center pane click on the **Administrators** tab. In the right pane, under Actions click **Create Administrator**.  **Note**: Studio was launched in a previous exercise. If Studio was closed in a previous exercise, then click **Start** > **Citrix** > **Citrix Studio**.
3.	Type **WORKSPACELAB\HDAdmin** in the Select an administrator field.



Click the **All** radio button.

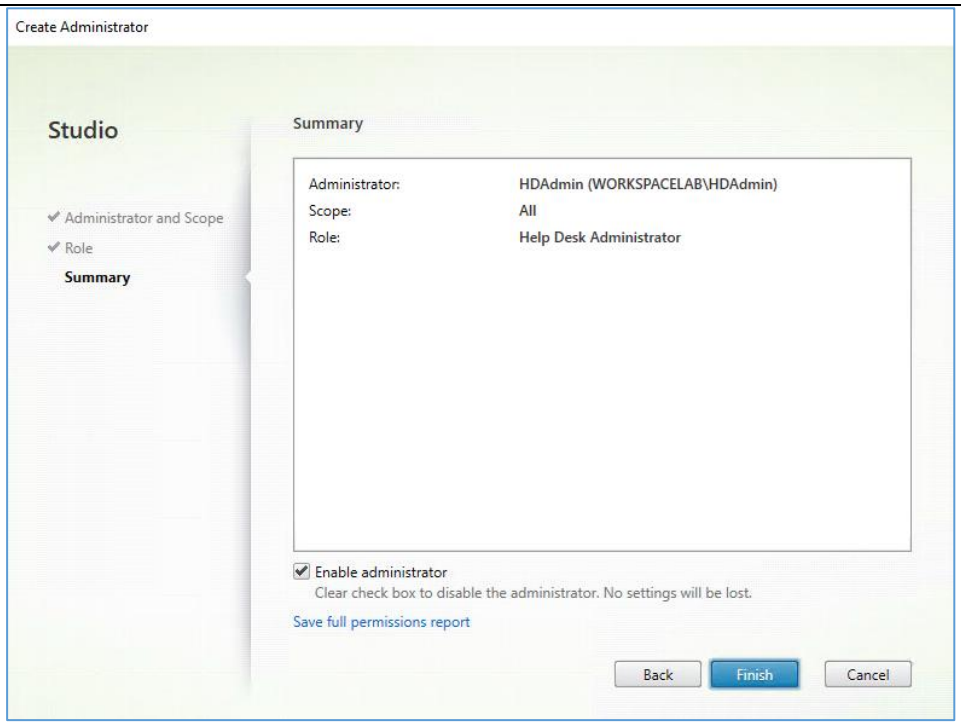
Click **Next**.

4. On the Role page, select the built-in **Help Desk Administrator** role.

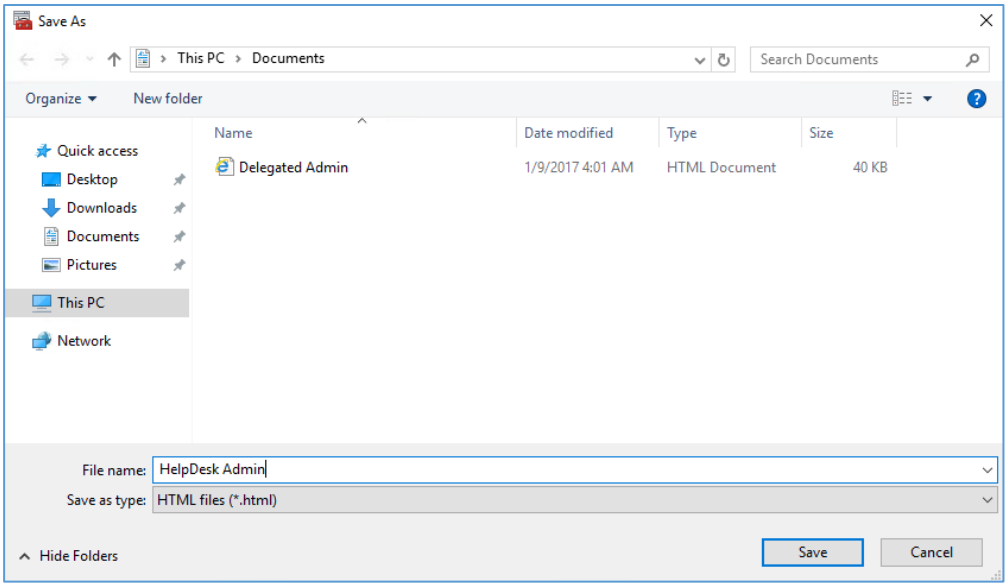


Click **Next**.

5. On the Summary page, review the details of the new administrator.



To create a report listing all the permissions the administrator will have, click **Save full permissions report**.

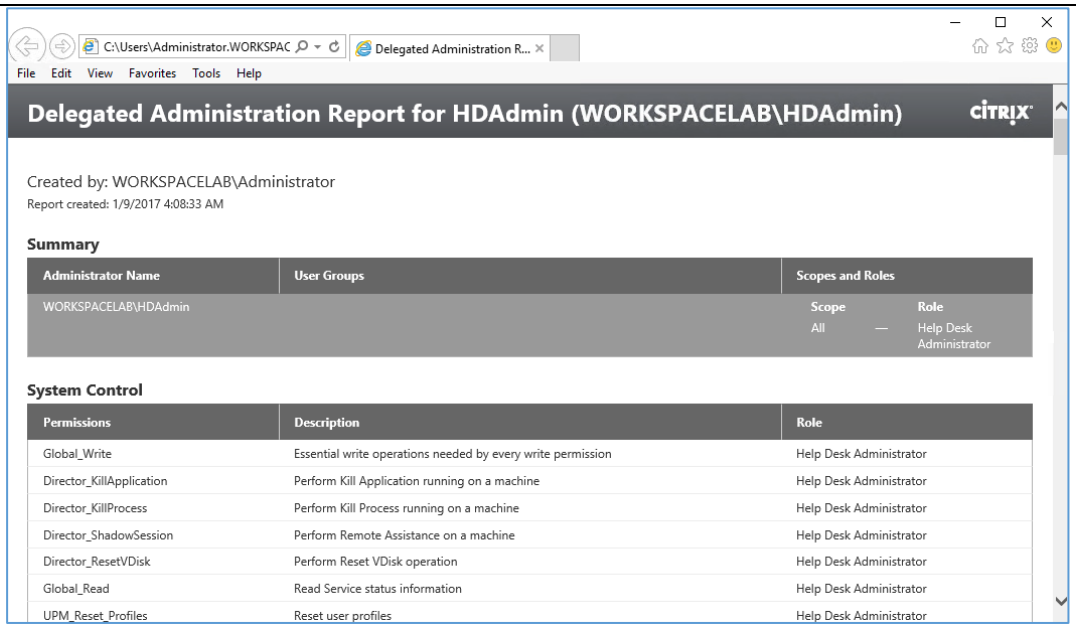


Save the report to the **Documents** folder with the name **Helpdesk Admin.html**.

Click **Save** and then click **Finish**.

6. Launch **File Explorer** from the Windows Taskbar.

Click **This PC** on the left column, double-click the **Documents** folder and then double-click the **Helpdesk Admin.html** file.

	 **Note**: If prompted with a message **How do you want to open this type of file (.html)?**, select a browser to use for the report.
7.	Once you are done reviewing the content of the report, **close** the report and close **File Explorer**.
8.	Close **Citrix Studio** and **log off** the **NYC-XDC-001** machine.

Takeaways:

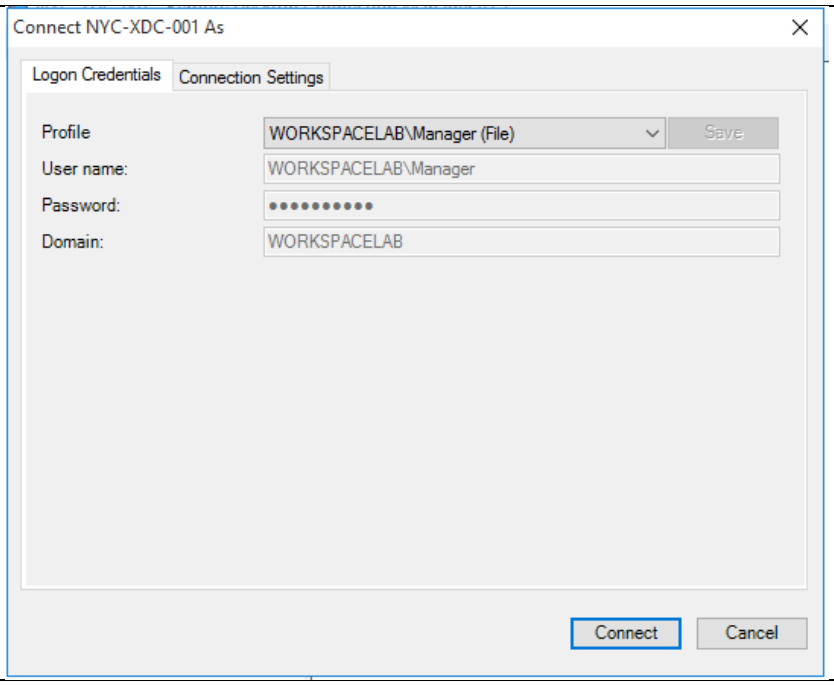
- Creating Delegated Administrators involves three elements; a user or a group, the scope on which the permissions apply and the set of permissions defined in the role.
- For complex environments, creating a proper delegation configuration will take some planning.

Exercise 10-5: Login and Test the Delegated Administrator

Scenario:

Your task is to log on to the Delivery Controller and as the delegated administrator and launch Studio.

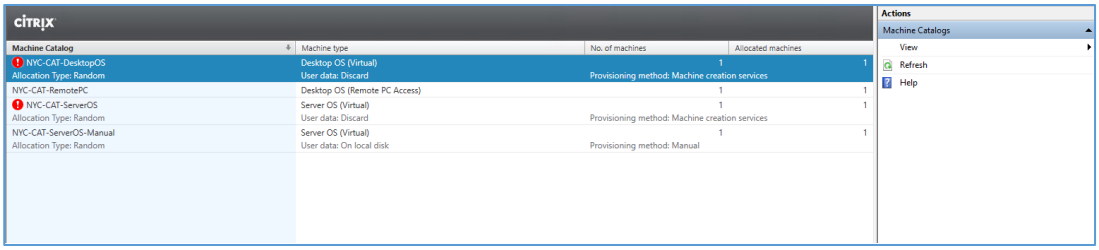
Step	Action
1.	Using the Remote Desktop Connection Manager, connect to **NYC-XDC-001**. To log on to NYC-XDC-001, right-click this machine and choose **Connect Server as**. Click the Profile drop-down list, select **WORKSPACELAB\Manager (File)** and click **Connect**.



2. Click **Start** and then locate and launch **Citrix Studio**.

3. Using Studio, expand **Citrix Studio (SITE-NewYork)** and click **Machine Catalogs**.

4. Notice that the Manager user is able to see the configured catalogs; however, is not able to see the option to Create Machine Catalog.



Note: The Manager has not been delegated permissions to see the hypervisor connection, so the Catalogs view will display a warning. This is by design.

5.	**Log off** NYC-XDC-001 as the Delegated Administrator. To log off, right-click **Start** > choose **Shut down or sign out** > and click **Sign out**.

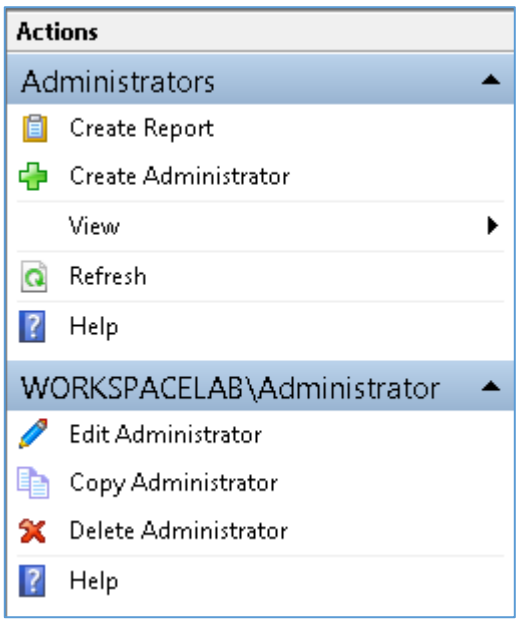
Key Takeaways:

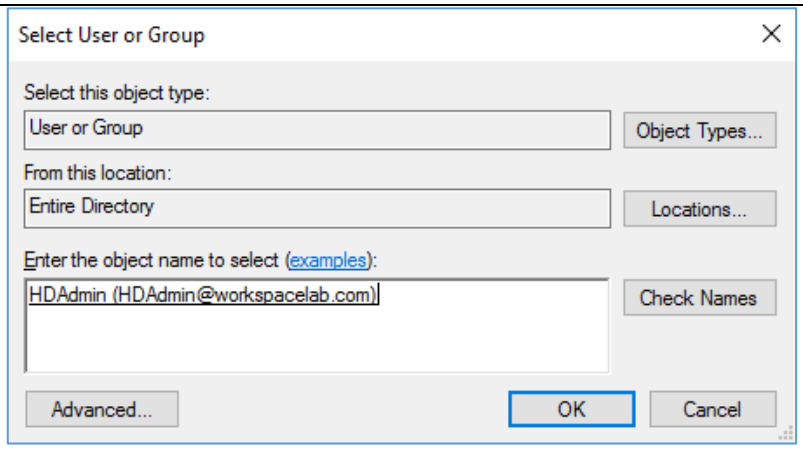
- To manage Studio as a specific Delegated Administrator, you can log on locally to the server with that administrator account.
- When logged on as a specific Delegated Administrator, you will have functions based on the permissions pre-defined for them.

Exercise 10-6: Create a Delegated Administration Report

Scenario:

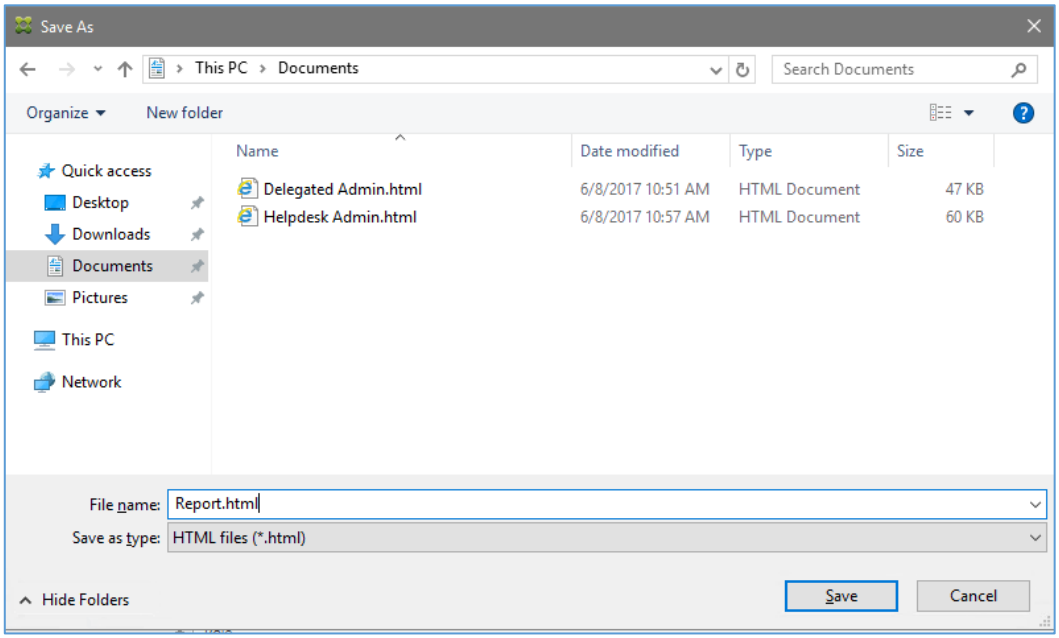
Your task is to create a delegated administration report so that you can review the delegated permission for those you have given access to the Citrix Site.

Step	Action
1.	Using the Remote Desktop Connection Manager, connect to **NYC-XDC-001**. To log on to NYC-XDC-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password.
2.	Click **Start** > and then click **Citrix Studio**. Using Studio, expand **Citrix Studio (SITE-NewYork)** > **Configuration** and select **Administrators**. In the right pane, under Actions click **Create Report**.  **Note**: You can also create a report when creating, copying, or editing an administrator.
3.	Type **WORKSPACELAB\HDAdmin** in the Enter the object name to select (examples) field.



Click **Check Names**. Once verified, click **OK**.

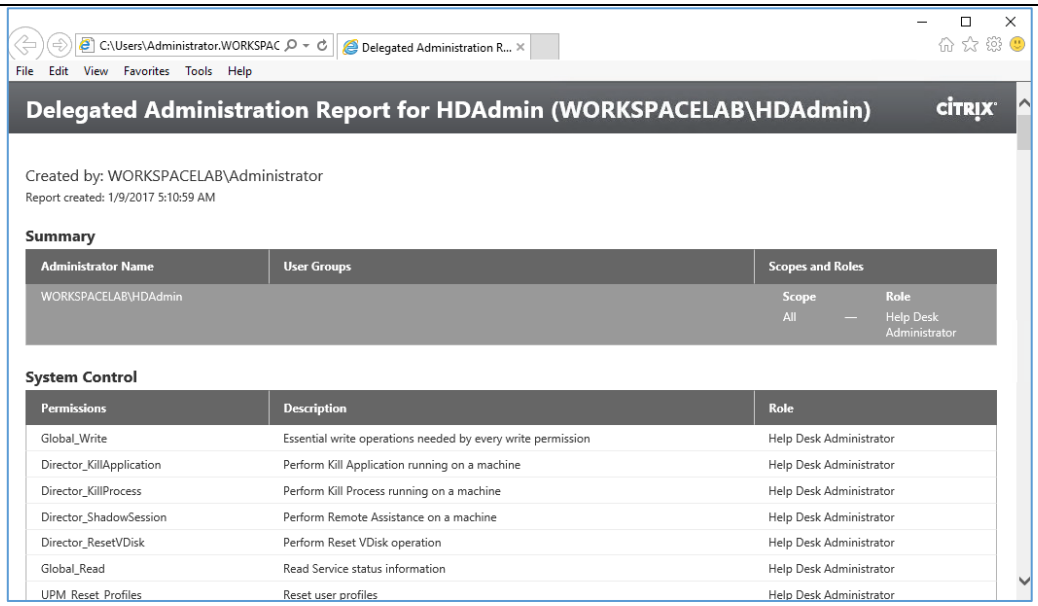
4. Save the report to the default **Documents** location with the name **Report.html**.



Click **Save**.

5. Launch **File Explorer** from the Windows Taskbar.

Click **This PC** on the left column, double-click the **Documents** folder and then double-click the **Report.html** file.

	 **Note**: If prompted with a message **How do you want to open this type of file (.html)?** select a browser to use for the report.
6.	Once you are done reviewing the content of the report, **close** the report and close **File Explorer**.

Key Takeaways:

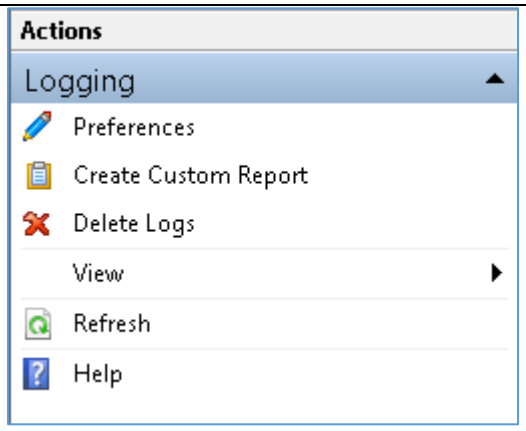
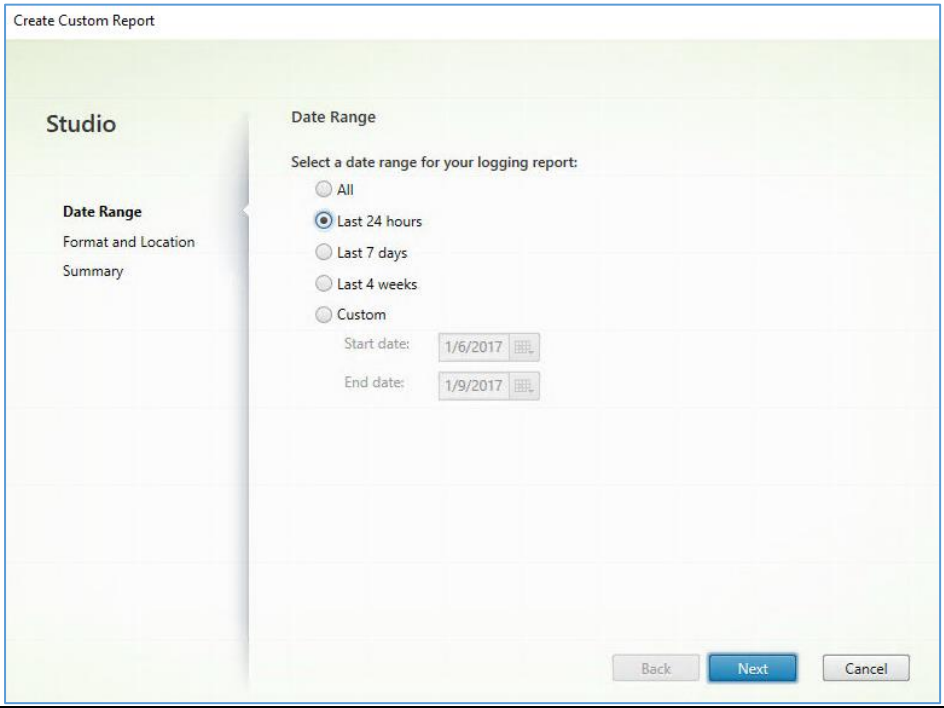
- The Delegated Administrator reports are very helpful when analyzing complex environments, in which a specific user received permissions from several Delegated Administrator groups.
- Many customers and consultants use these reports as part of their environment documentation.

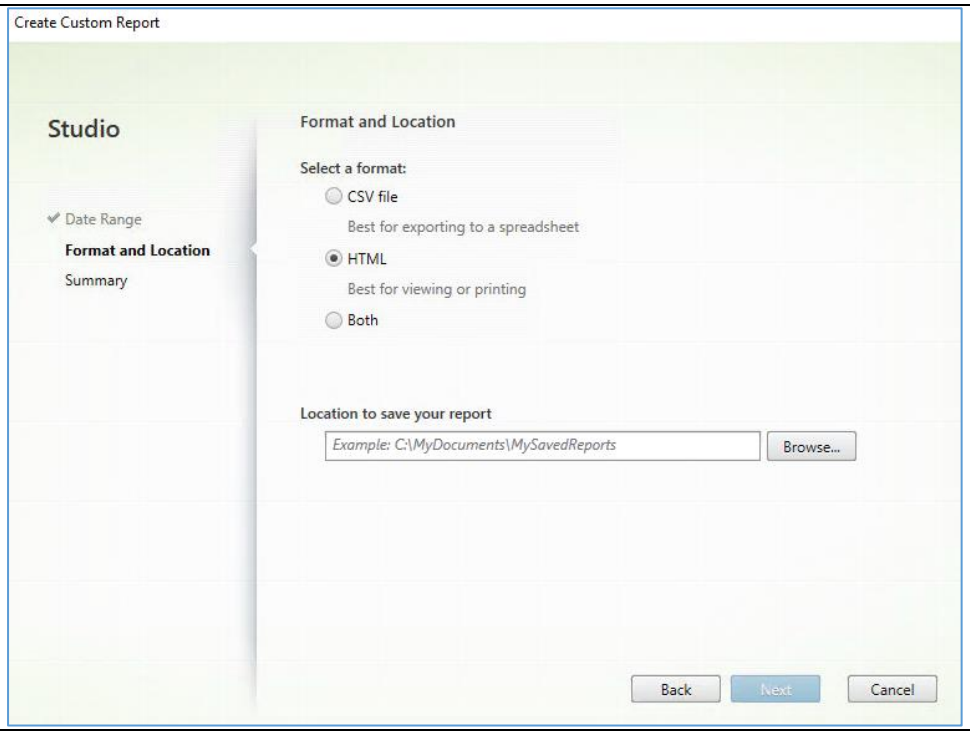
Exercise 10-7: Create a Configuration Logging Report

Scenario:

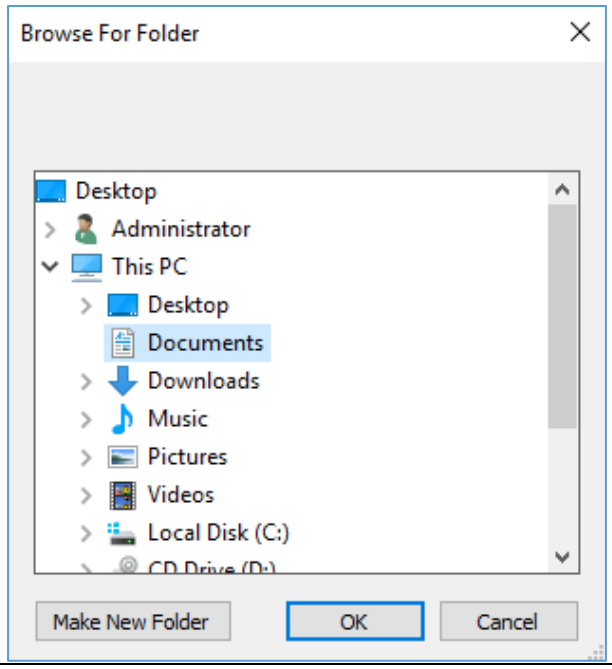
Your task is to create a configuration logging report so that you can review the changes made by said delegated administration.

Step	Action
1.	Using the Remote Desktop Connection Manager, confirm you are still connected to **NYC-XDC-001**. **Note:** In a previous exercise, you had logged on to **NYC-XDC-001** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-XDC-001**, right-click this machine and choose **Connect server**.
2.	Using Studio, expand **Citrix Studio (SITE-NewYork)** and click **Logging**. In the right pane, under Actions click **Create Custom Report**.

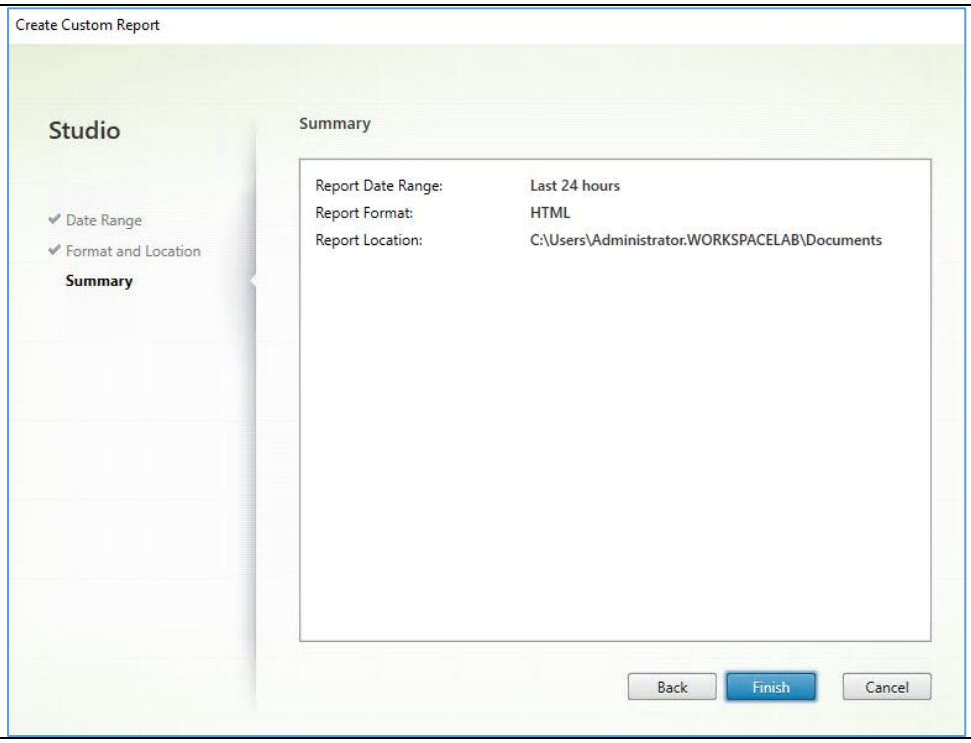
	 **Note**: The Welcome Configuration Logging and Reports dialog box shows. Read the definition of Configuration logging and Custom reports, click **Don't show this again** and then click **Close**. **Note**: Studio was launched in a previous exercise. If Studio was closed in a previous exercise, then click **Start** > **Citrix** > **Citrix Studio**.
3.	On the Date Range page select **Last 24 hours** radio button and click **Next**. 
4.	On the Format and Location page verify **HTML** is selected and click **Browse**.



5. Leave the default **Documents** folder selected, click **OK**, and then click **Next**.

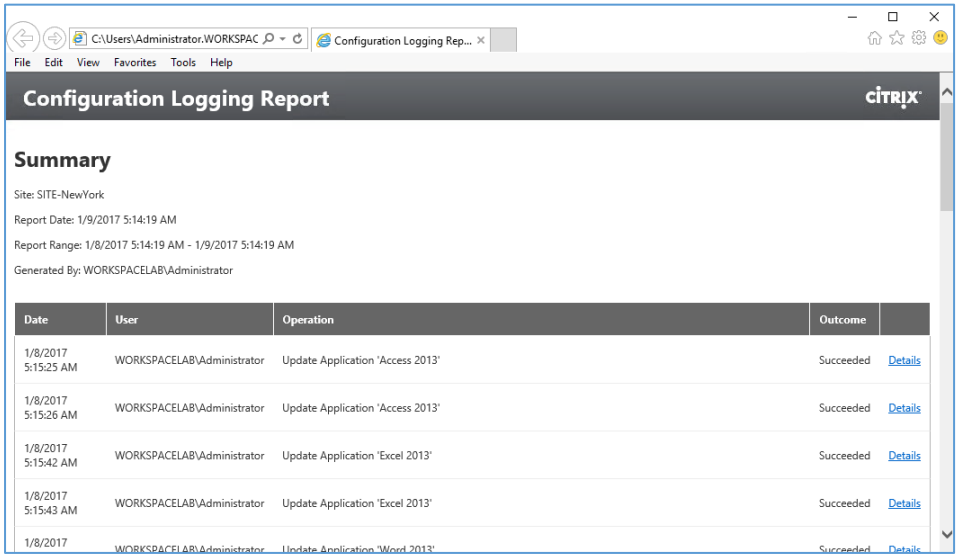


6. On the Summary page click **Finish**.



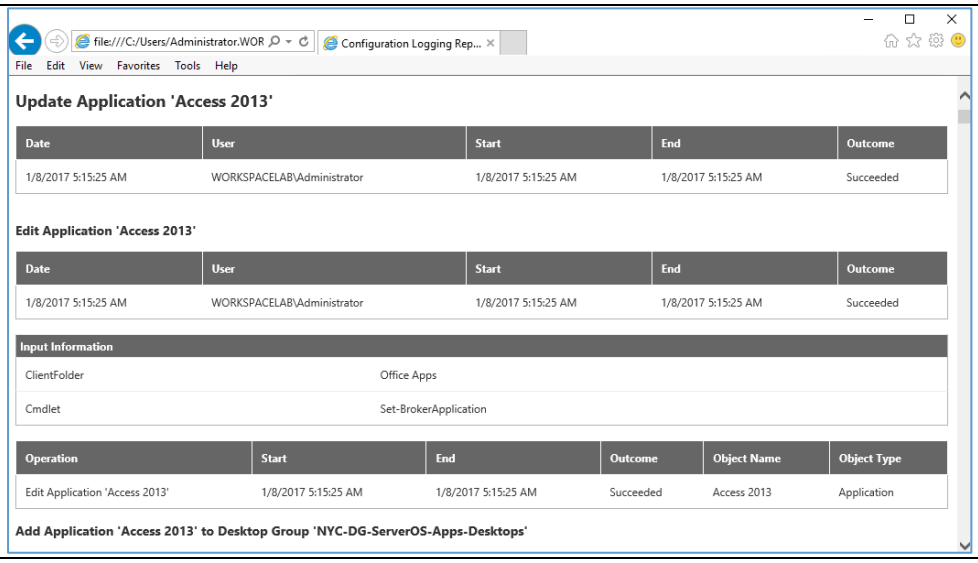
7. Launch **File Explorer** from the Windows Taskbar and double-click the **Documents** folder.

8. Double-click the **Summary.html** report to review a summary of user, operation and outcome by the date.



Click **Details** on the right side of the report for the latest entry.

9. Review the details of the operation performed that the Configuration Logging Report Details page displays.

	
10.	**Close** the Configuration Logging Report.

Key Takeaways:

- Reports are generated from the Citrix Studio Logging Pane.
- When creating the report, various options are available for selecting a date range.
- A configuration logging report displays any changes made within Citrix Studio, PowerShell or Director.

Module 11: XenApp and XenDesktop Site Redundancy Considerations

Overview:

This module presents the business need to grow the WW Labs POC environment to become more like a production environment, which requires the current Site to be set up for redundancy in case of a failure. This module identifies the capable components in this POC able to support redundancy.

Before you begin:

Estimated time to complete Module 11 lab exercises: 85 minutes

Exercise 11-1: Install the Second Delivery Controller Server

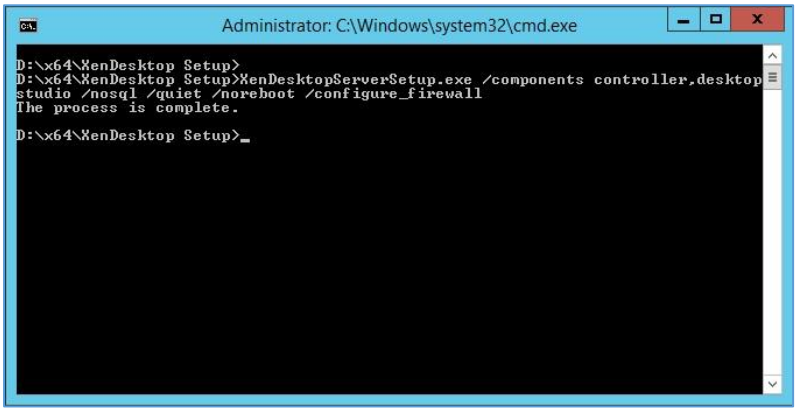
There is more than one method to install this Second Delivery Controller. One method uses the Command Prompt and the other use the same GUI method as the First Delivery Controller installation. Both methods are valid in this environment and by Citrix. You must choose either Option 1 or Option 2. You will be unable to perform the steps for both options.

Scenario:

Your task is to install a Second Delivery Controller.

Option 1: Step-by-Step using the Command Prompt

Step	Action
1.	The following VMs are required before beginning the exercises for this Module; all others may be powered down. To power manage your VMs, switch to XenCenter, right-click on the VM in the left pane and select Start or Shut Down. If prompted click Yes. • NYC-ADS-001 • NYC-SQL-001 • NYC-FSR-001 • NYC-VNS-001 • NYC-NIC-001 • NYC-XDC-001 • NYC-XDC-002 • NYC-STF-001 • NYC-STF-002 • NYC-SRV-001 • NYC-WRK-001 **Note**: These above VMs are listed in the start-up order.
2.	In the left pane of **XenCenter**, select **NYC-XDC-002**. In the right pane, select the **Console** tab and select **XenApp_and_XenDesktop_7_13.iso** from the **DVD Drive 1:** drop-down menu. Using the Remote Desktop Connection Manager, connect to **NYC-XDC-002**. To log on to NYC-XDC-002, right-click this machine and choose **Connect server**.

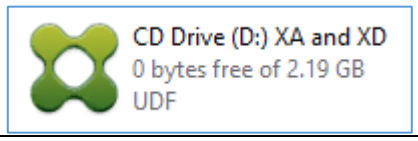
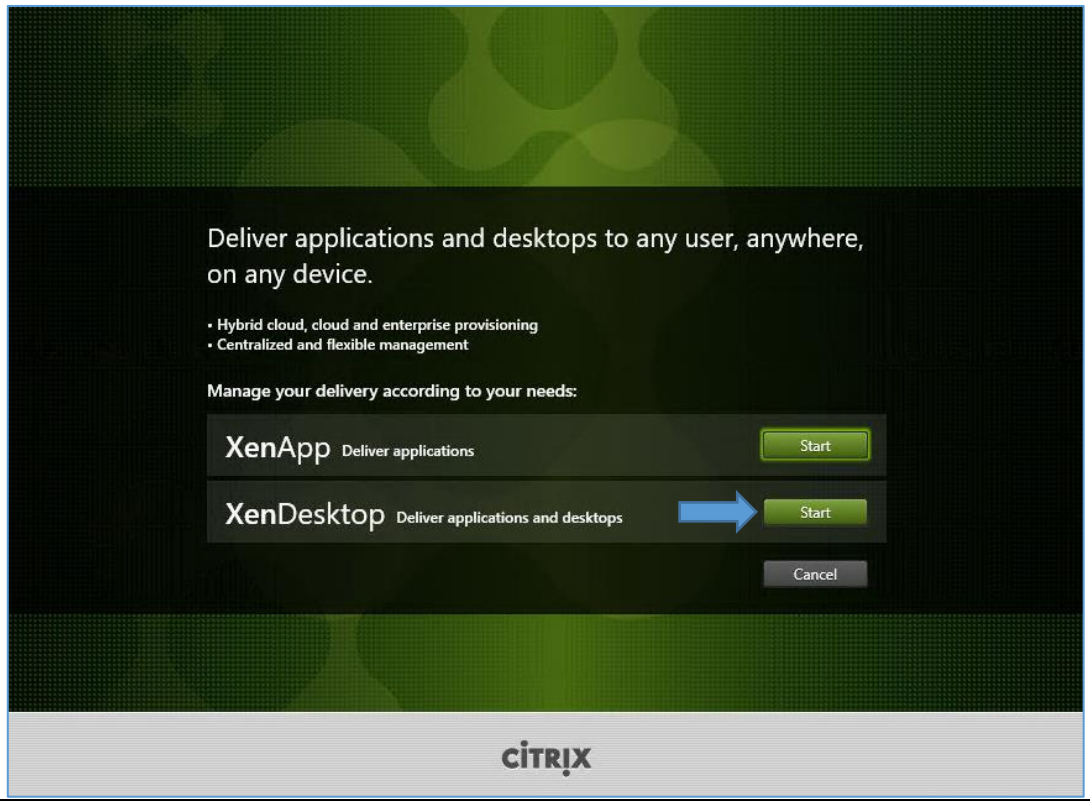
	Note: The following credentials are used to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password.
3.	Launch the Command Prompt by clicking the **Start** menu, typing **Command Prompt** and pressing **Enter**.
4.	Type **D:** and press **Enter**. Type **cd D:\x64\XenDesktop Setup** and press **Enter**.
5.	Type **XenDesktopServerSetup.exe /components controller,desktopstudio /nosql /quiet /noreboot /configure_firewall** and press **Enter**.
6.	When the command is successful, you will see message stating: **The process is complete**.  **Note**: This command does not provide a progress status. The process takes approximately 5 minutes.
7.	In the left pane of **XenCenter**, select **NYC-XDC-002**. In the right pane, select the **Console** tab and click **Eject** to remove **XenApp_and_XenDesktop_7_13.iso** from the **DVD Drive 1:**.
8.	Using XenCenter right-click **NYC-XDC-002** and choose **Reboot** and then click **OK**.

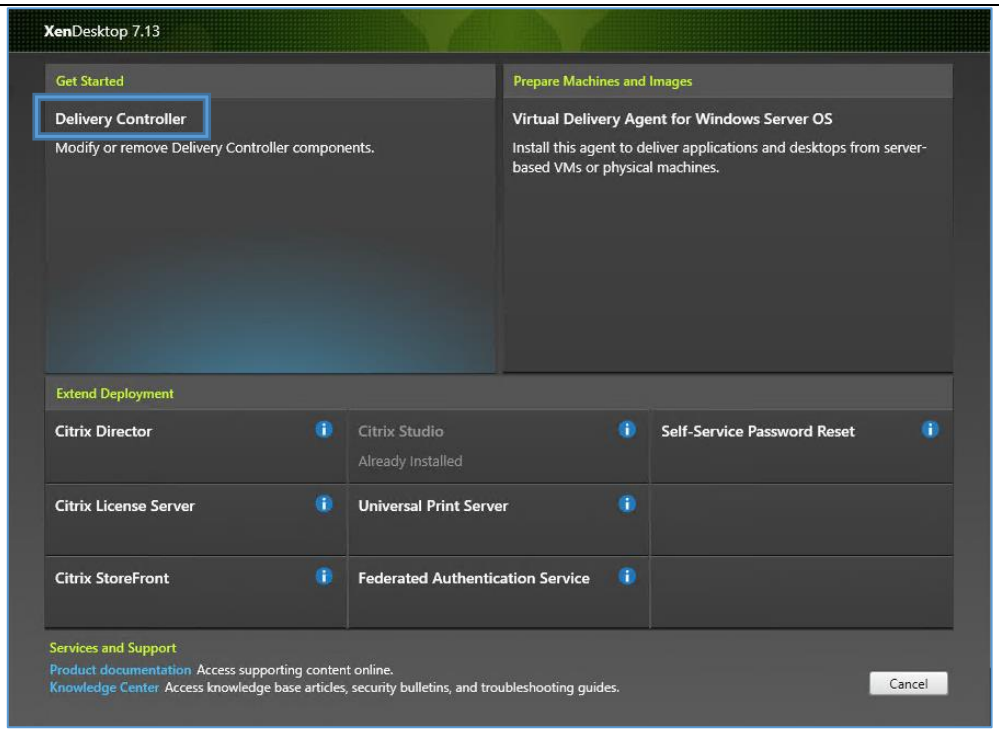
Key Takeaways:

- The command line can be used to install the Delivery Controller role.

Option 2: Step-by-Step using the GUI

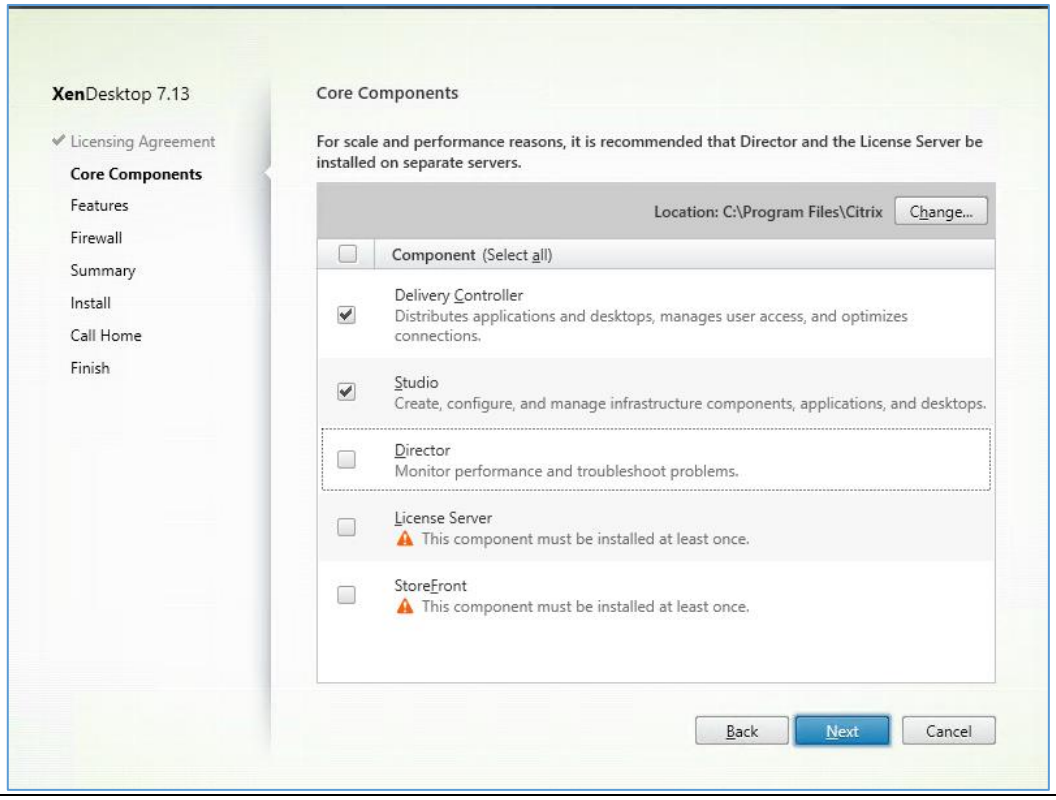
Step	Action
1.	Using **XenCenter** mount the XenApp and XenDesktop installation media ISO to **NYC-XDC-002**. To mount the installation media ISO, select **NYC-XDC-002** in the left pane of the XenCenter. In the right pane, select the **Console** tab. Using the **DVD Drive 1:** drop-down menu select **XenApp_and_XenDesktop_7_13.iso**. **Note**: If there are no ISOs listed in the **DVD Drive 1:** drop-down menu, then the Local ISO Storage Repository (SR) that contains the ISO library may need to be re-scanned. In the left pane of **XenCenter** select the **Local ISO SR XS**. In the right pane select the **Storage** tab and click on the **Rescan** button. This task may need to be repeated later in the course. **Note:** If the above rescan of the **Local ISO SR XS** does not show the specific ISO for installation: XenApp_and_XenDesktop_7_13.iso, then please tell your instructor.
2.	Using the Remote Desktop Connection Manager, connect to **NYC-XDC-002**. To log on to NYC-XDC-002, right-click this machine and choose **Connect server**.

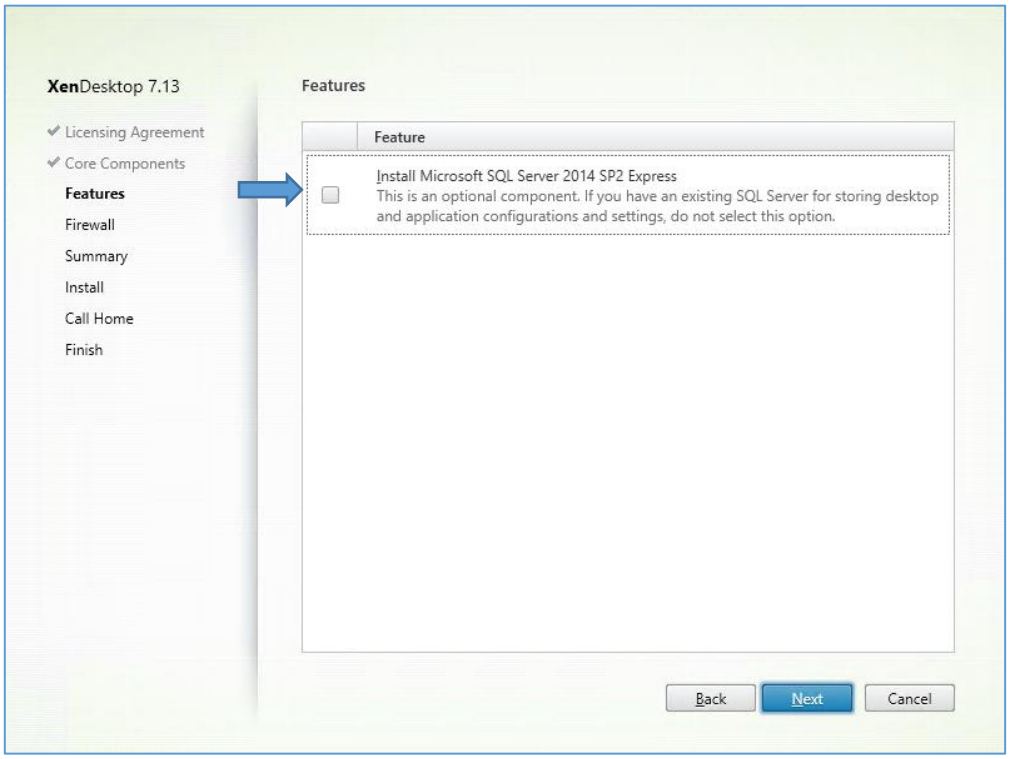
	Note: The following credentials are used to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password.
3.	Launch **File Explorer** from the Windows Taskbar or Start Menu. Double-click the green Citrix logo next to **CD Drive** under Devices and drives, and double-click **AutoSelect.exe**. 
4.	On the Deliver applications and desktops to any user, anywhere, on any device screen, click **Start** next to the XenDesktop option. 
5.	The wizard will now display all possible installation options that are compatible with the Operating System of the machine that you are on. Select **Delivery Controller**.

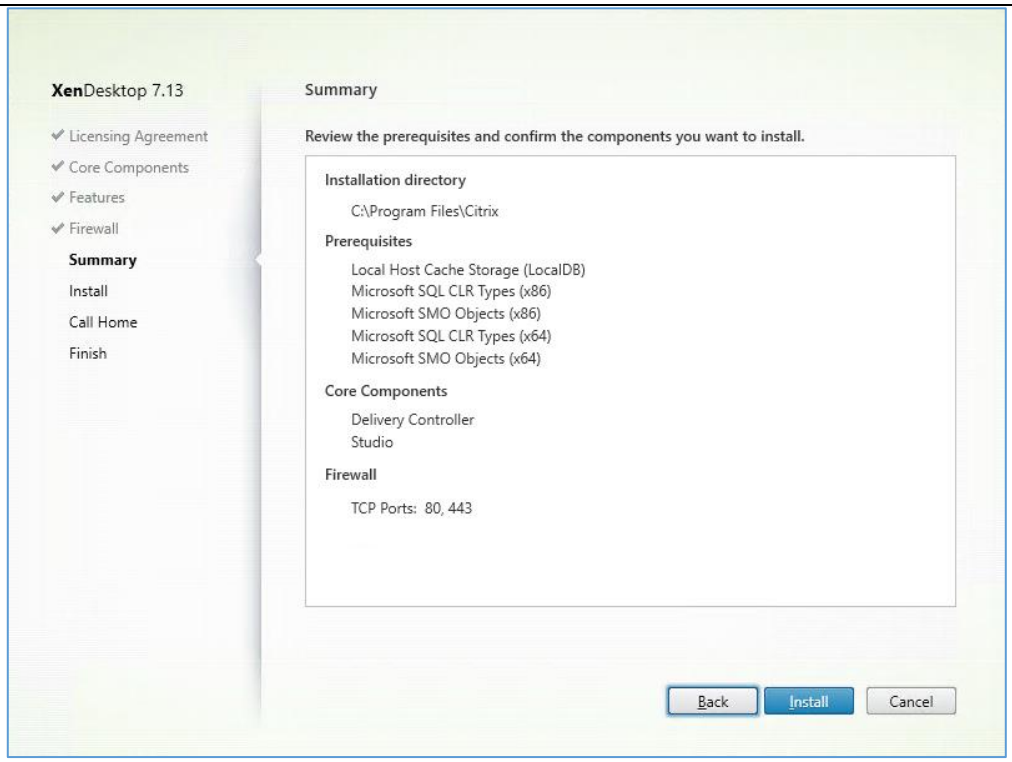


6. Review the Licensing Agreement page. If you agree, respond to the Software License Agreement and then click **Next**.

7. On the Core Components page, there will be multiple options to select for the installation. Uncheck all options except for **Delivery Controller** and **Studio** and click **Next**.



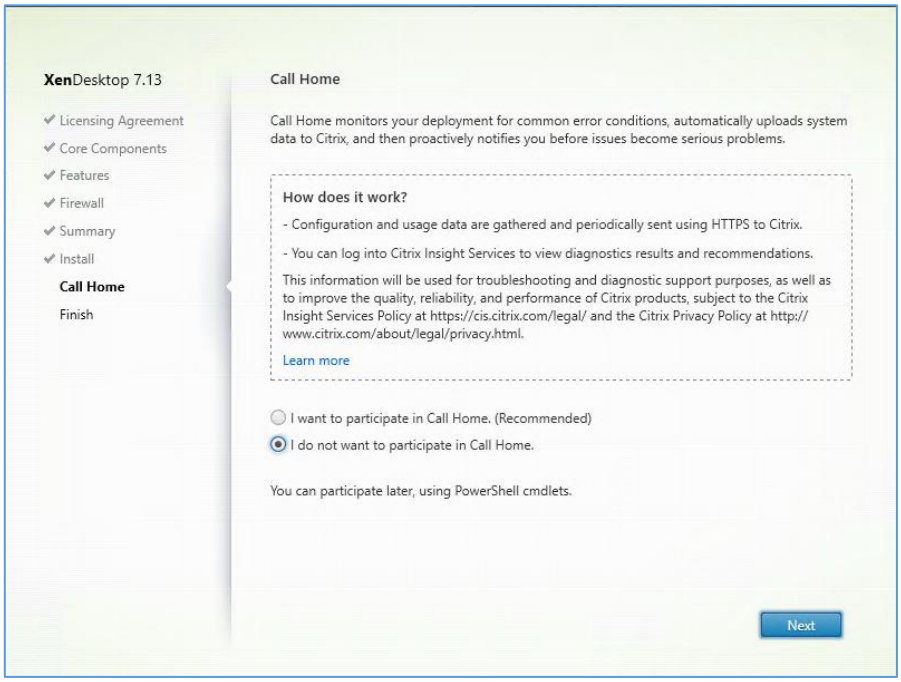
	Note: You are deselecting Director because you will install this component in a future task. You are deselecting License Server because you have already deployed this component. You are deselecting StoreFront because this component will be installed on another dedicated server. This NYC-XDC-002 server will be a new dedicated, Delivery Controller that will add redundancy to the POC environment.
8.	On the Features page, uncheck the **Install Microsoft SQL Server 2014 SP2 Express** option and click **Next**.  **Note**: Remember, you have already deployed the Site database on SQL.
9.	On the Firewall page, leave the default **Automatically** option selected and click **Next**.
10.	On the Summary page, verify all options and click **Install**. The installation will take a few minutes to complete.

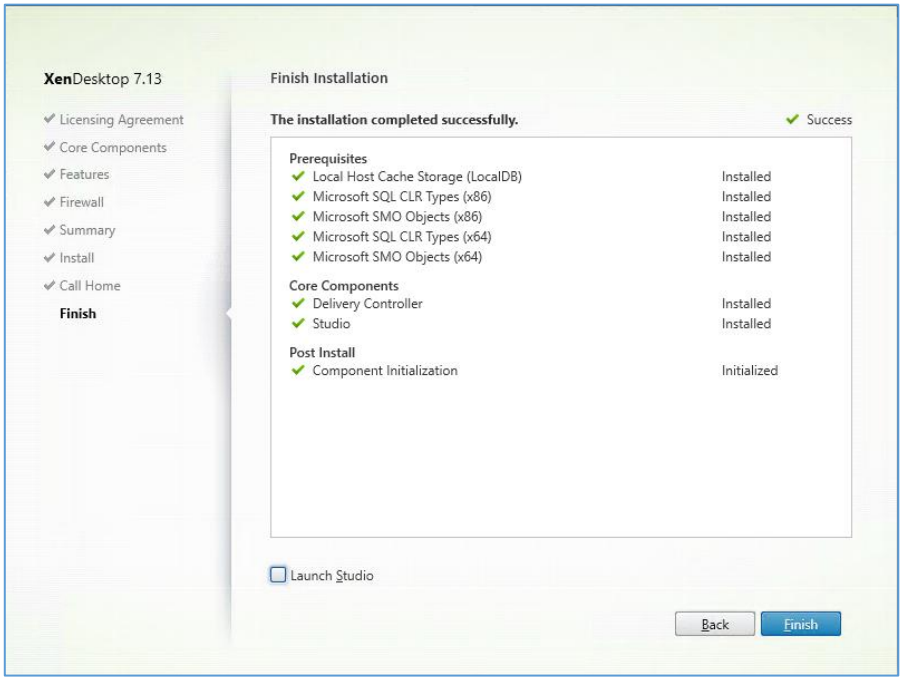


11. If prompted for reboot click **Close** to let the machine reboot and resume the installation.

    Note: You can switch to XenCenter to monitor the reboot status for NYC-XDC-002. Using Remote Desktop Connection Manager, connect back to NYC-XDC-002 and wait for the installer to resume setup.

12. On Call Home Screen, Select **I do not want to participate in Call Home** and click **Next**.



13.	When the installation has completed, uncheck **Launch Studio**.  Click **Finish**.
14.	Using **XenCenter** eject the XenApp and XenDesktop installation media from **NYC-XDC-002**. To eject the installation media ISO, select **NYC-XDC-002** in the left pane of XenCenter. In the right pane, select the **Console** tab and click **Eject** to remove **XenApp_and_XenDesktop_7_13.iso** from the DVD Drive 1. **Note**: The Eject option can be difficult to see. It is an underlined word to the right side of the DVD Drive 1 drop-down menu.
15.	Using XenCenter right-click **NYC-XDC-002** and choose **Reboot** and then click **OK**.

Key Takeaways:

- The installation Wizard can rapidly deploy all components required for a proof of concept deployment, including a database engine.
- The installation Wizard will install any pre-requisites needed.
- Citrix recommends keeping the different roles separated in a production environment.

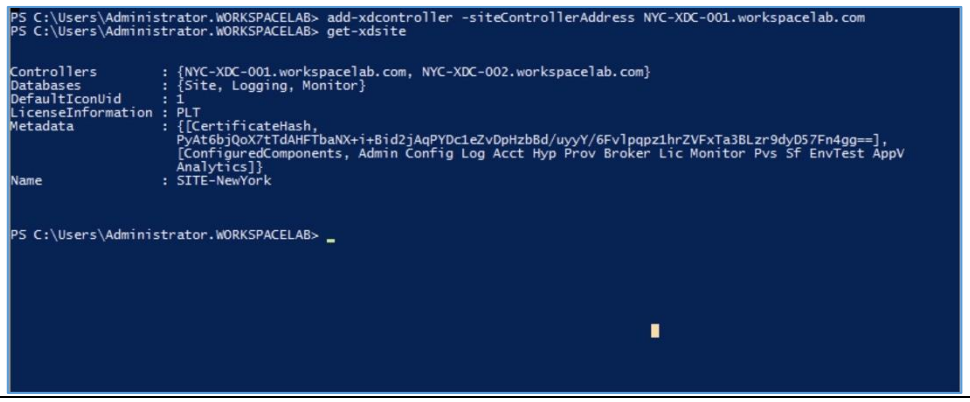
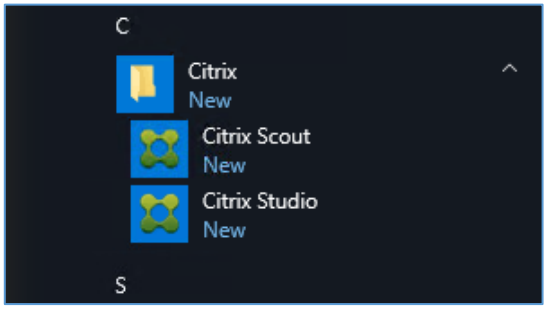
Exercise 11-2: Join the Second Delivery Controller to the Site

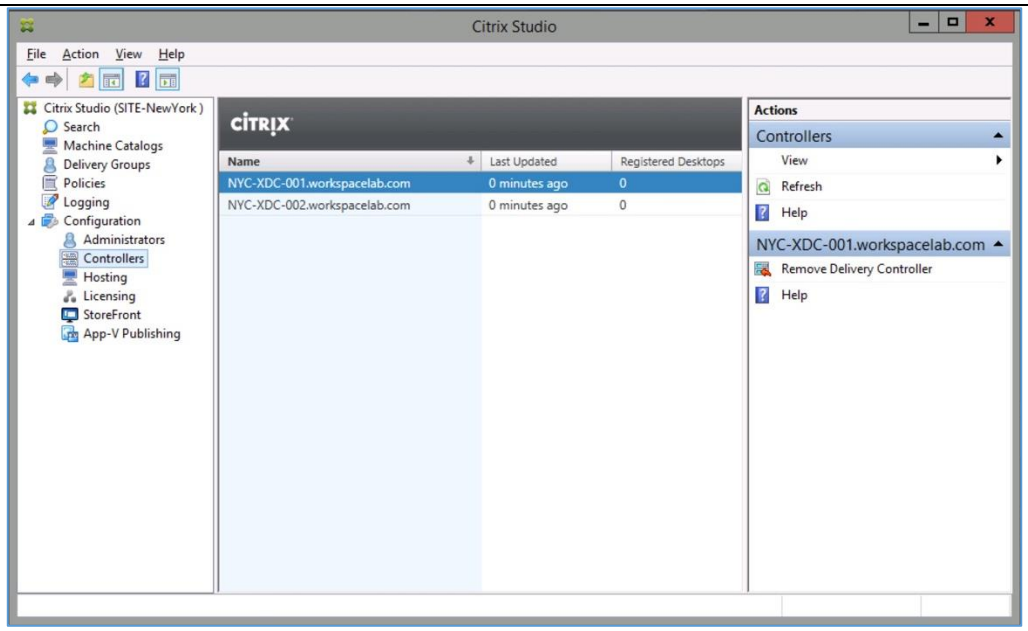
There is more than one method to join this second Delivery Controller to the Citrix Site. One method uses Power Shell and the other uses Studio. Both methods are valid in this environment and by Citrix. You must choose either Option 1 or Option 2. You will be unable to perform the steps for both options.

Scenario:

Your task is to join this second Delivery Controller to the Citrix Site.

Option 1: Step-by-Step using Power Shell

Step	Action
1.	Using the Remote Desktop Connection Manager, connect to **NYC-XDC-002**. To log on to NYC-XDC-002, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password.
2.	Launch **Windows PowerShell** from the **Start** Menu or by clicking the icon in the taskbar.
3.	Type **asnp Citrix*** and press **Enter** to add the Citrix cmdlets.
4.	Type **add-xdcontroller -siteControllerAddress NYC-XDC-001.workspacelab.com** and press **Enter**. **Note:** This process of joining the site takes approximately 2 to 3 minutes.
5.	Type **Get-XDSite** and press **Enter**. Verify that both Delivery Controllers are listed. 
6.	Click **Start** and then expand the Citrix folder.  Click **Citrix Studio**.
7.	Click **Configuration** > **Controllers** and verify both Delivery Controllers are listed.

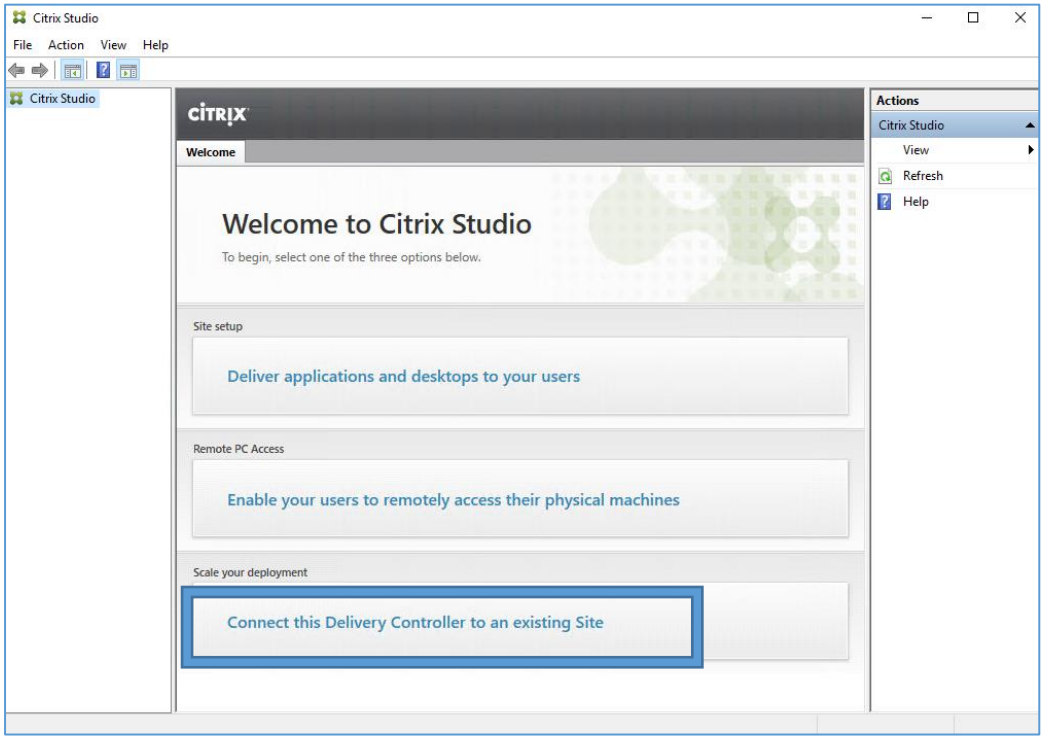
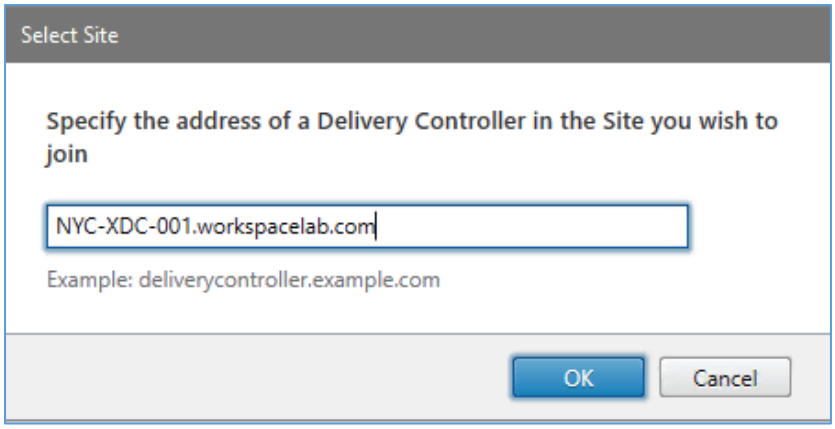
	 **Note**: For smaller environments and POCs, try to administer the site consistently from one Delivery Controller or even an Admin Server with Citrix Studio installed. For larger environments, you should consider deploying Studio as a published application resource.

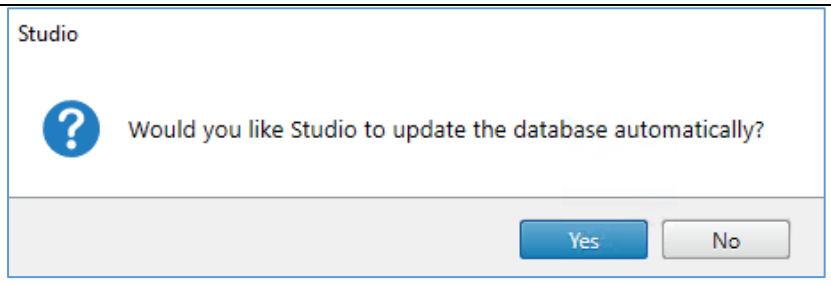
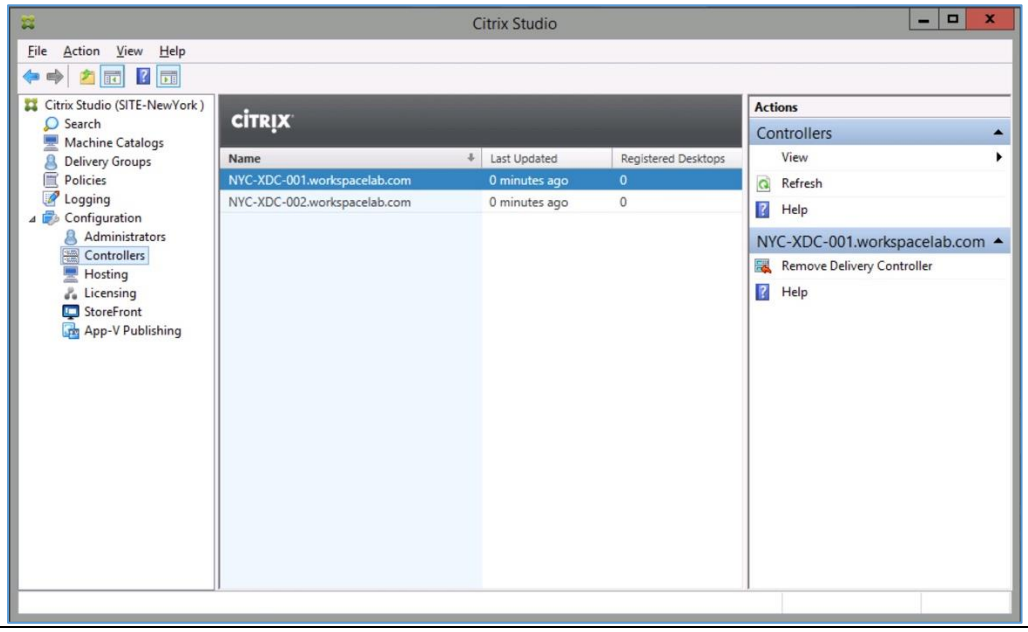
Key Takeaways:

- When a new XenDesktop controller is built, you can add it to the existing XenDesktop site using the PowerShell command Add-XDController.
- Because Add-XDController command does not return the execution status, it is a good practice to verify the site configuration using the Get-XDSite command. The expected result is to have both Delivery Controllers listed in the site configuration.
- In order to remove the Delivery Controller, you need to execute the Remove-XDController –ControllerName NYC-XDC-002 –AdminAddress NYC-XDC_001 command, where ControllerName is the controller you want to remove and AdminAddress is the name of the controller to which the PowerShell command will connect.

Option 2: Step-by-Step using Studio

Step	Action
1.	Using the Remote Desktop Connection Manager, confirm you are still connected to **NYC-XDC-002**. **Note:** In a previous exercise, you had logged on to **NYC-XDC-002** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-XDC-002**, right-click this machine and choose **Connect server**.

2.	Using Studio, click **Connect this Delivery Controller to an existing Site**. 
3.	Type **NYC-XDC-001.workspacelab.com** in the Select Site field.  Click **OK**.
4.	Click **Yes** on the dialog box asking if you would like Studio to update the database automatically.

	
5.	Using Studio, expand **Citrix Studio (SITE-NewYork)** > **Configuration** and select **Controllers**. Confirm that both Delivery Controllers are listed. 

Key Takeaways:

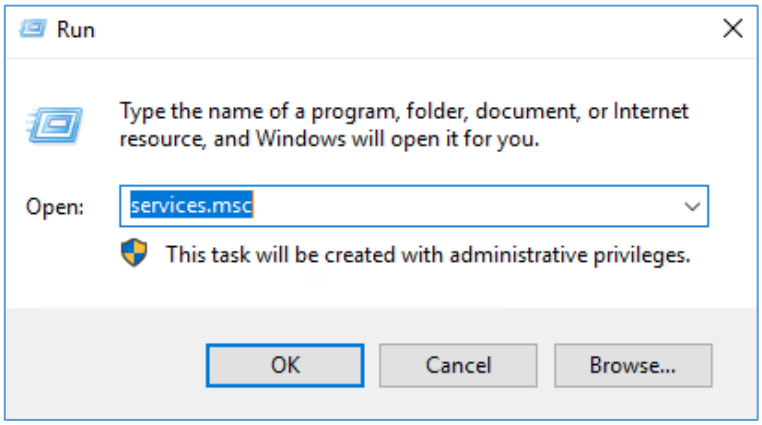
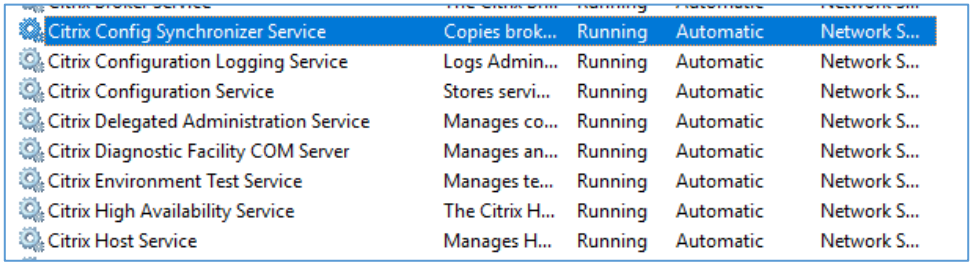
- The list of available Controllers can be viewed from within Citrix Studio by expanding Configuration and selecting the Controllers node.

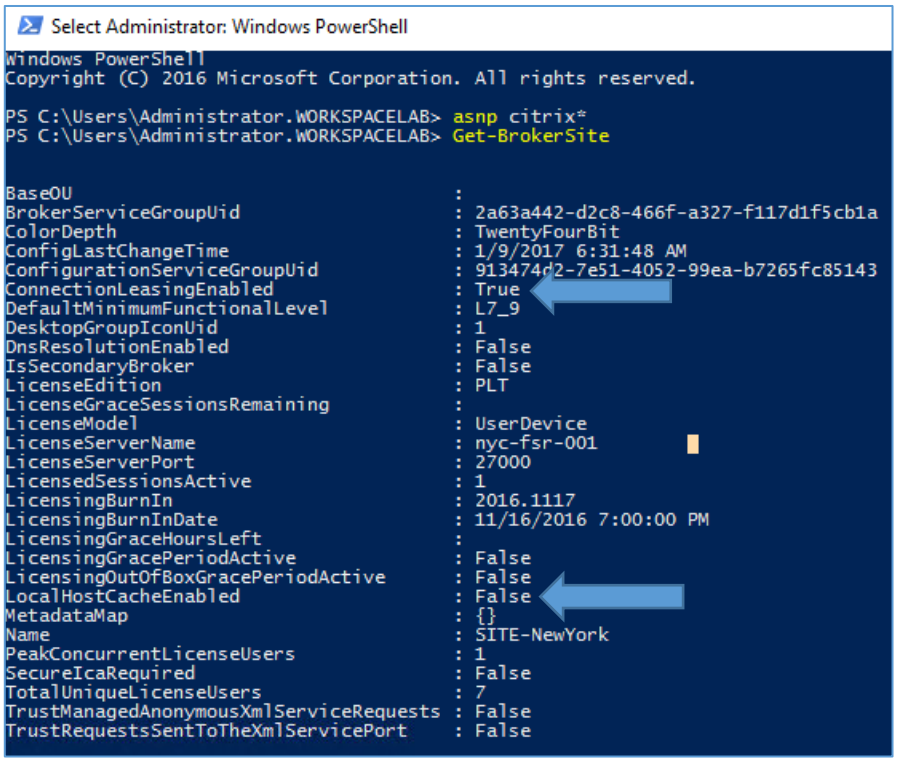
Exercise 11-3: Configure and Test Local Host Cache

Scenario:

The Citrix Lead Architect has expressed concerns that new users might not be able to broker sessions in the unlikely event that the SQL server becomes unavailable. You have been tasked to investigate the limitations of connection leasing and evaluate the Local Host Cache feature in order to select the best solution for the production environment.

Step	Action
1.	Using the Remote Desktop Connection Manager, connect to **NYC-XDC-001**.

	To log on to NYC-XDC-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password.
2.	Open the **services console** on NYC-XDC-001 and check the new services that are introduced (HA service and CSS service). Right-click on **Start** and select **Run**. Type **services.msc** and click **OK**.  Look for **Citrix Config Synchronizer Service** and **Citrix High Availability Service**.  **Note:** The Citrix Config Synchronizer Service is responsible for keeping the LocalDB in sync with the content of the primary datastore. The Citrix High Availability Service is the secondary broker. When the controller loses contact with the primary datastore, the primary Broker Service stops responding and hands over the brokering responsibilities to Citrix HA Service, which relies on the data stored in LocalDB.
3.	Launch **Windows PowerShell** from the Start Menu. Type **asnp citrix*** and press **Enter**. This command will load Citrix modules to the PowerShell window. Type **get-brokersite** and press enter, to verify that connection leasing is enabled and LHC is disabled.



Note: By default, local host cache is disabled and connection leasing is enabled.

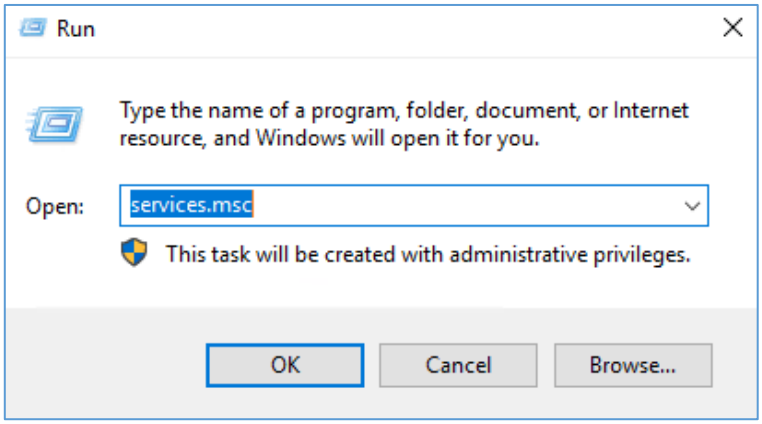
4. Log on to the SQL server to stop the service **SQL Server(MSSQLSERVER)**.

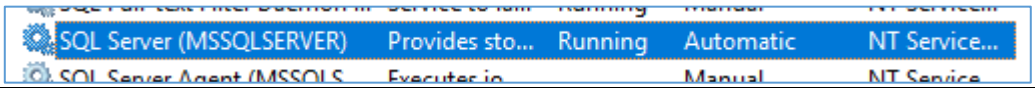
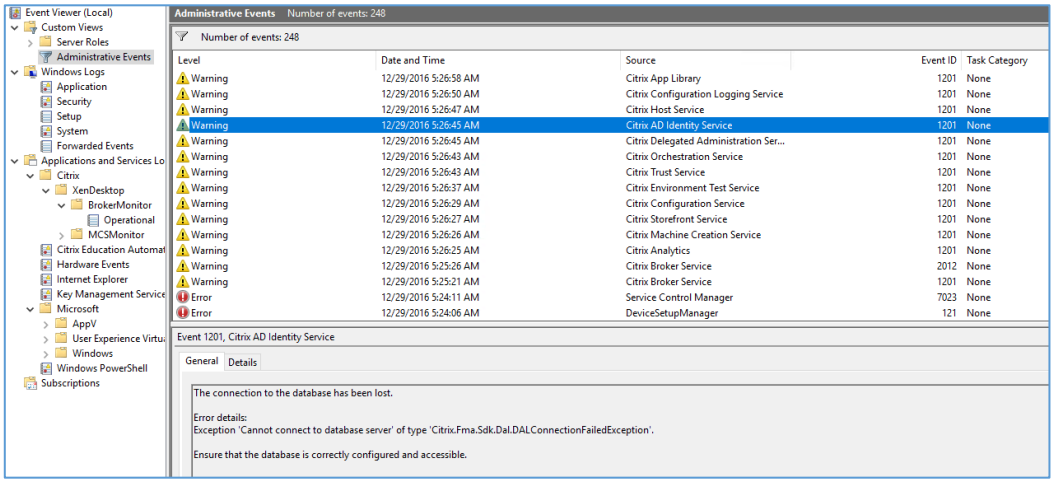
   Using the Remote Desktop Connection Manager, confirm you are still connected to **NYC-SQL-001**.

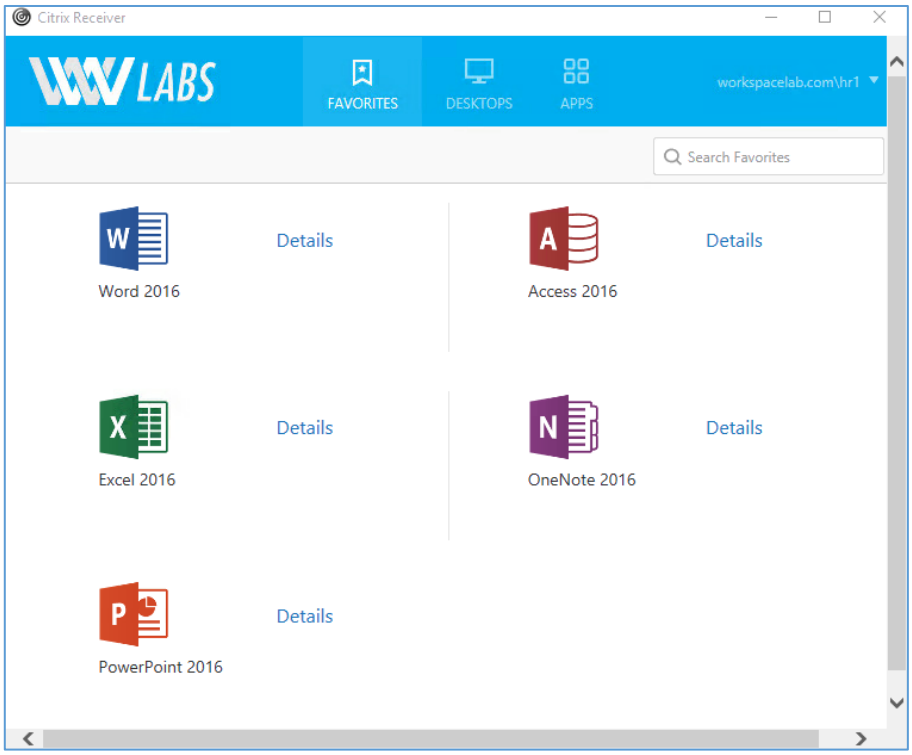
   Note: Use the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password.

5. Open the services console on NYC-SQL-001 and stop the service **SQL Server(MSSQLSERVER)**.

   Right-click **Start** and select **Run**. Type **services.msc** and click **OK**.



6.	Look for the service **SQL Server (MSSQLSERVER)**, right-click and select **Stop**. 
7.	Switch back to **NYC-XDC-001**. Right-click **Start** and select **Event Viewer**. Browse to **Custom Views** > **Administrative Events**.  Look for **event ID 1201 database connection is lost**.
8.	Switch to **NYC-WRK-001** and log on to Citrix Receiver using the HR1 user account. Log on to **Citrix Receiver** using the following credentials: User name: **HR1** Password: **Password1**
9.	Launch **Word 2016**.

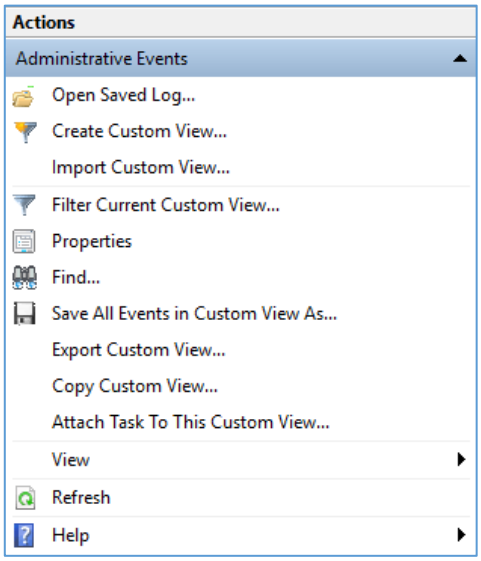


Application launches successfully.

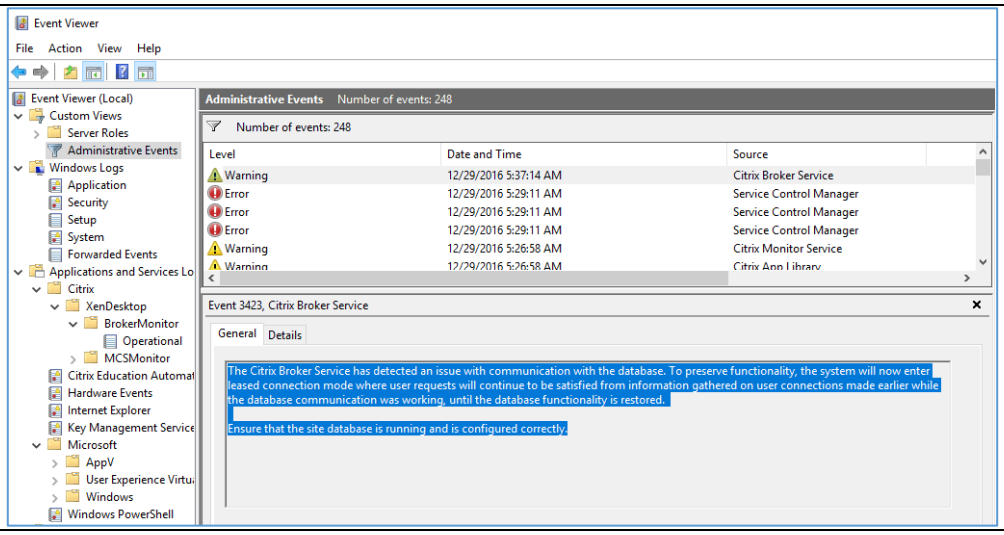
10. Switch back to **NYC-XDC-001**.

Verify you are viewing **Custom Views** > **Administrative Events**.

On the right pane, under Actions, click **Refresh**.



Look for **Event ID :3423 db** connection is lost and system has entered into **lease mode**.



11. Switch back to **NYC-WRK-001**.

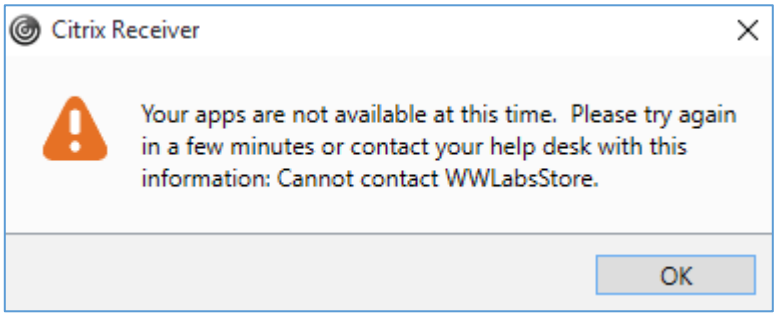
Close **Word 2016**.

Log off the Store. Click **HR1** and **Log Off**.

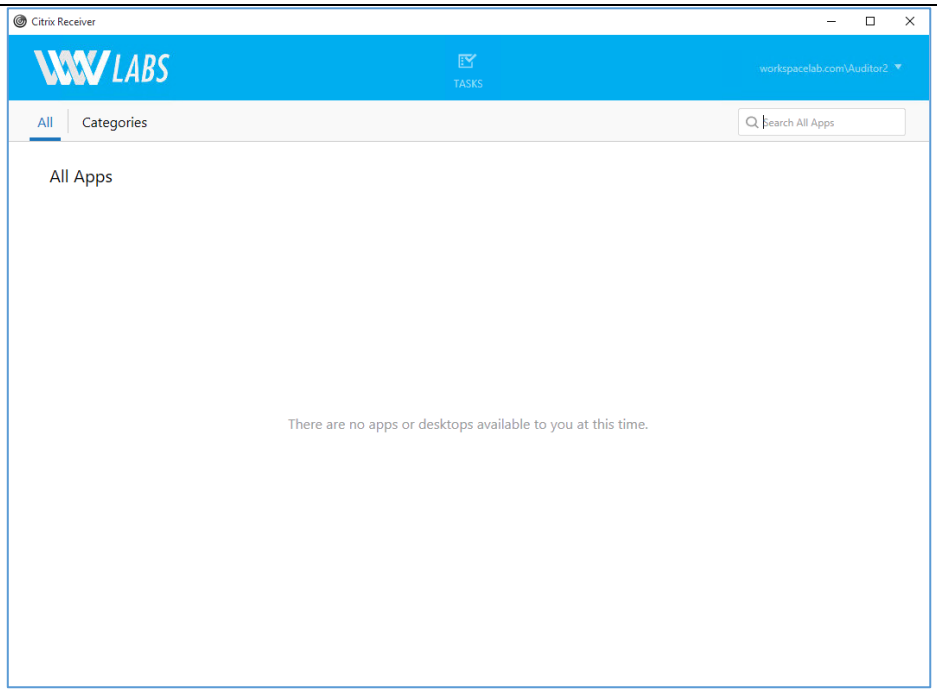
Click Refresh Apps to log on to **Citrix Receiver** using the following credentials:

User name: **Auditor2**
Password: **Password1**

User **Auditor2** gets an error.



Note: Auditor2 has access to the same applications but is not able to see any published applications.

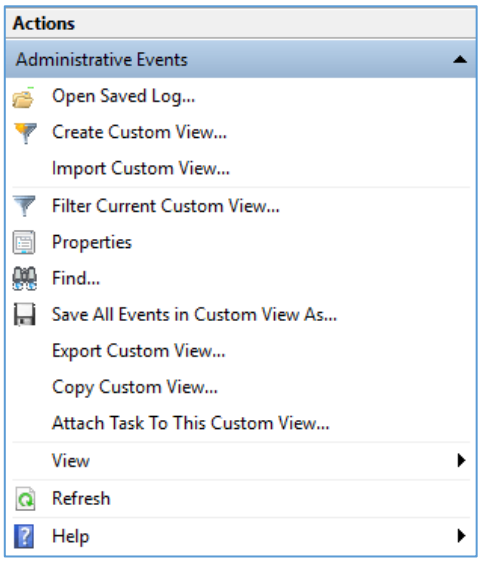


Note: With Connection Leasing, a user who has not connected to the store in the last 2 weeks will not be able to see his applications because the lease is maintained only for a period of 2 weeks.

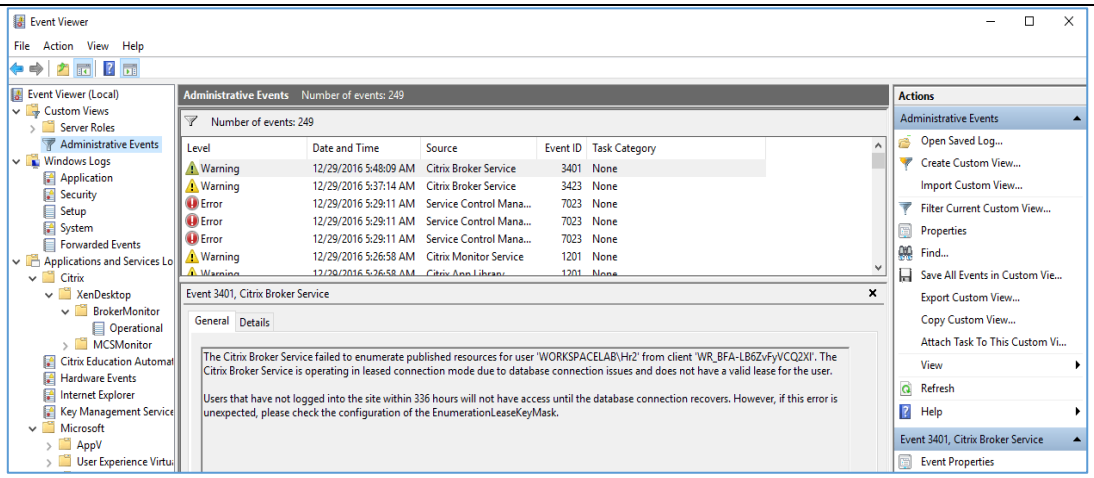
12. Switch to **NYC-XDC-001**.

Verify you are viewing **Custom Views** > **Administrative Events**.

On the right pane, under Actions, click **Refresh**.



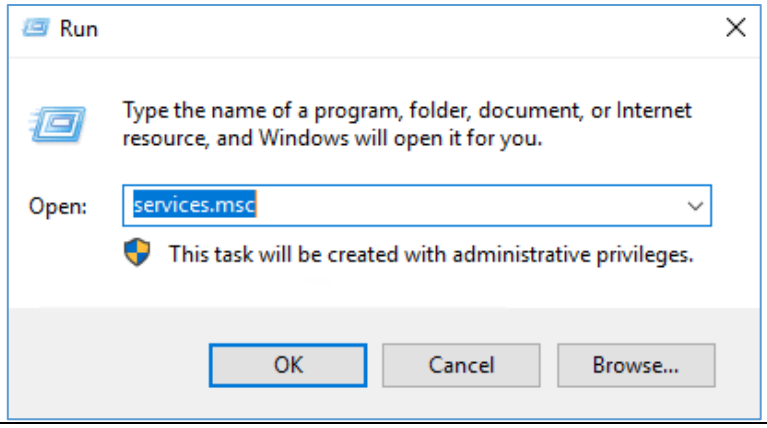
Look for **Event ID 3401**.



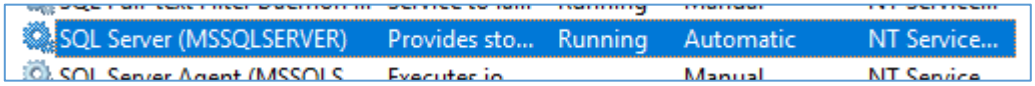
Event logs on broker will show **Event ID 3401: The Citrix Broker Service is operating in leased connection mode due to database connection issues and does not have a valid lease for the user**.

13. Switch to **NYC-SQL-001** and start the SQL Server Service.

    Right-click **Start** and select **Run.** Type **services.msc** and click **OK**.



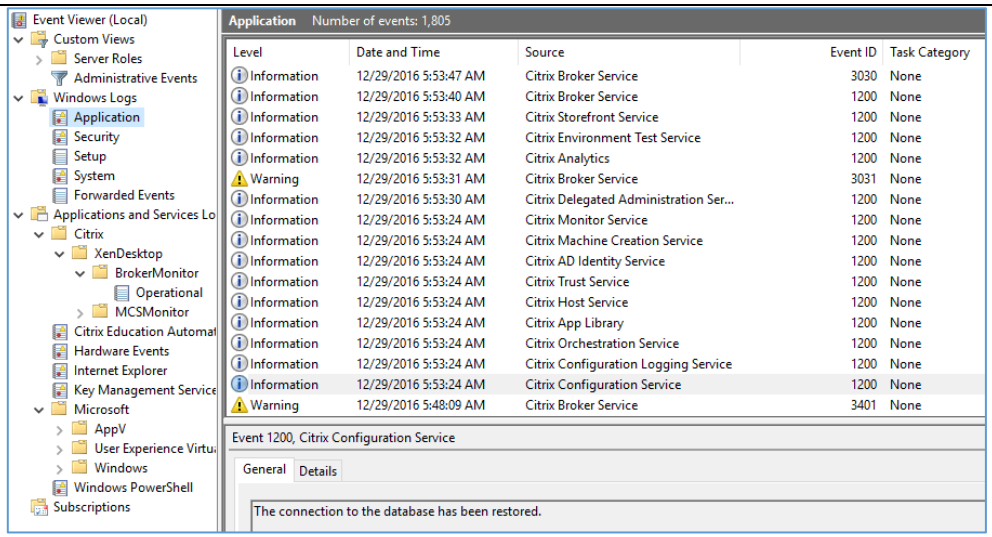
14. Look for the **SQL Server (MSSQLSERVER)** service, right-click on it and select **Start**.



15. Switch to **NYC-XDC-001**.

    Navigate to **Windows Logs** > **Application**.

    Look **for Event ID 1200**. **NYC-SRV-001**



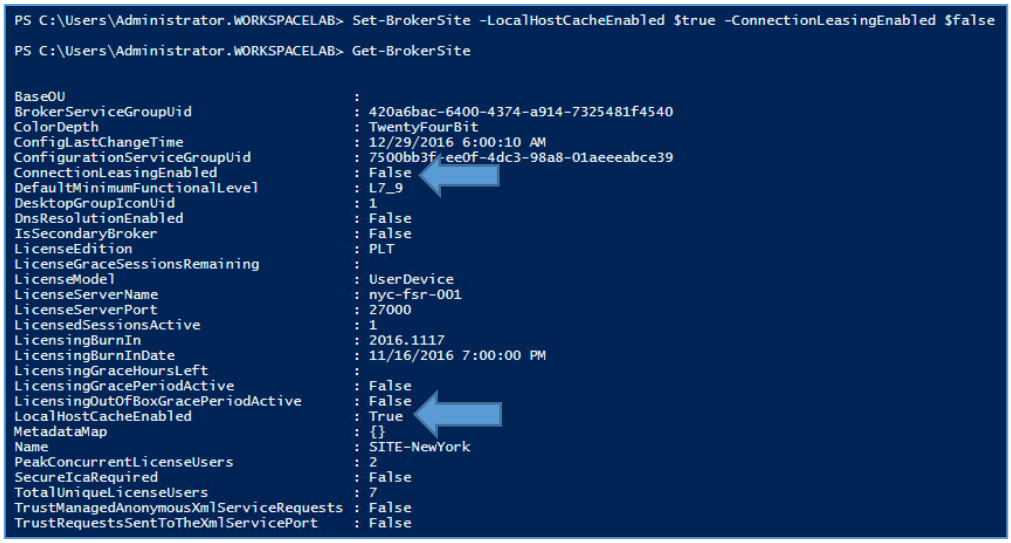
This validates that the XenDesktop Service instances have established a connection with the database successfully.

16. Switch to the **PowerShell** window.

Note: If PowerShell was closed in a previous exercise, ensure to run the ASNP Citrix* command to add the Citrix cmdlets again.

17. Enable LHC by running the command: **Set-BrokerSite -LocalHostCacheEnabled $true -ConnectionLeasingEnabled $false**

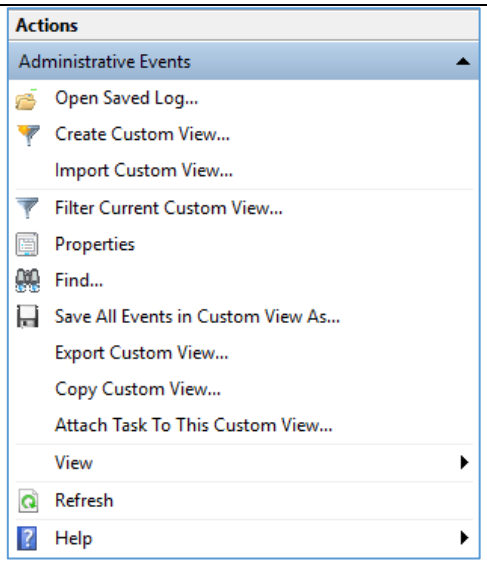
To validate the configuration, type **Get-BrokerSite** and press **Enter**.



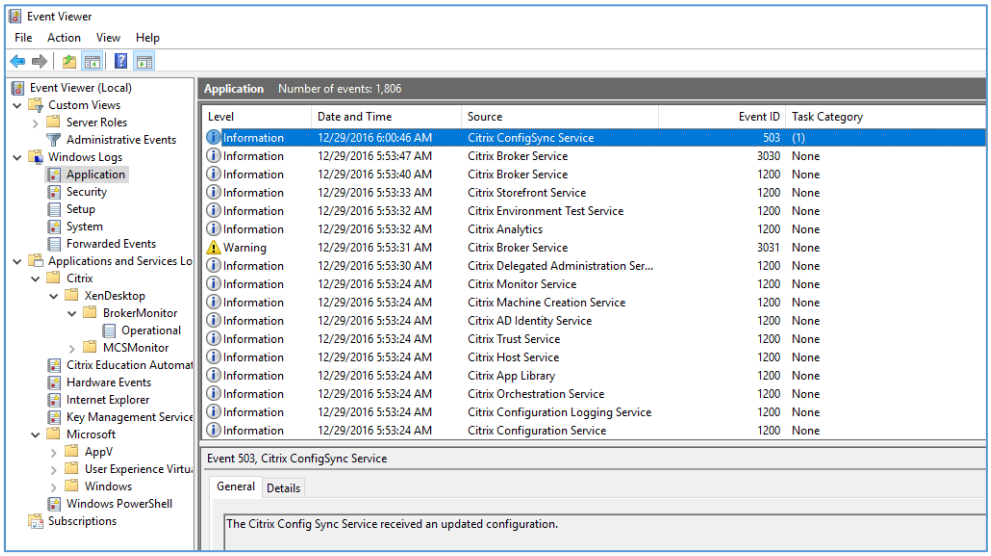
18. Switch to the Event Viewer window.

Verify you are viewing **Windows Logs** > **Application**.

On the right pane, under Actions, click **Refresh**.



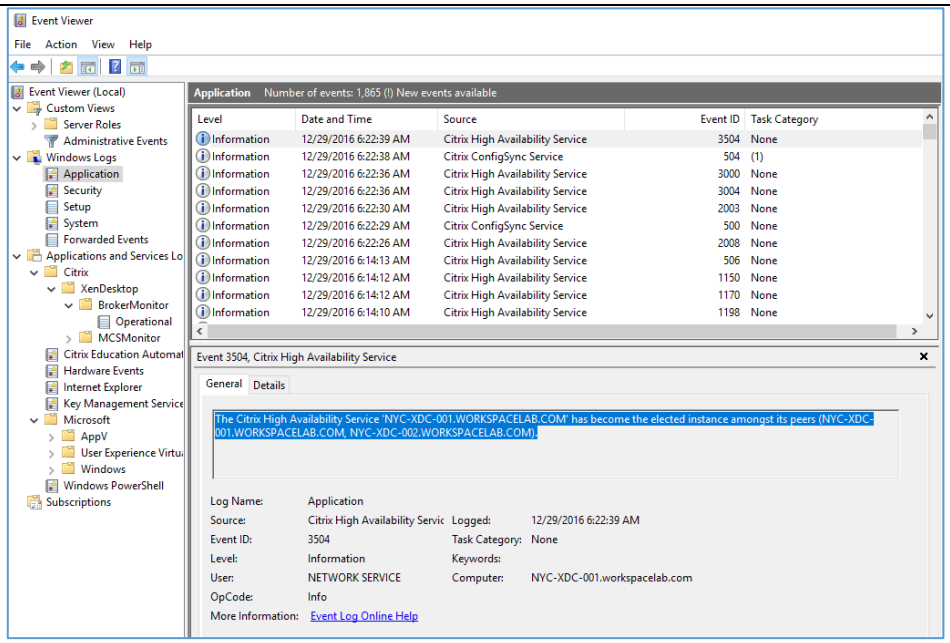
Look for event **ID 503**

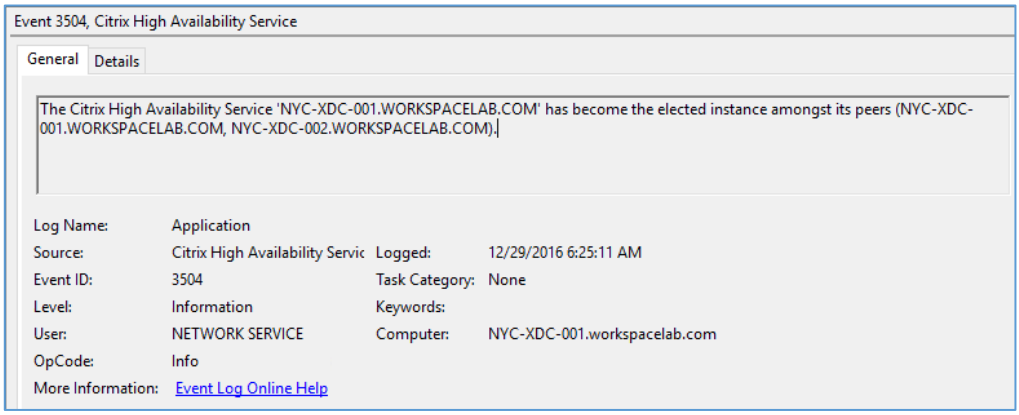


Note: It might take 30 seconds for this event to appear, click refresh until it appears.

19. Controllers are elected based on alphabetical and numerical order. Notice how the *001* broker server is elected. Election takes place while the Site database is active.

    Look for **Event ID 3504**.

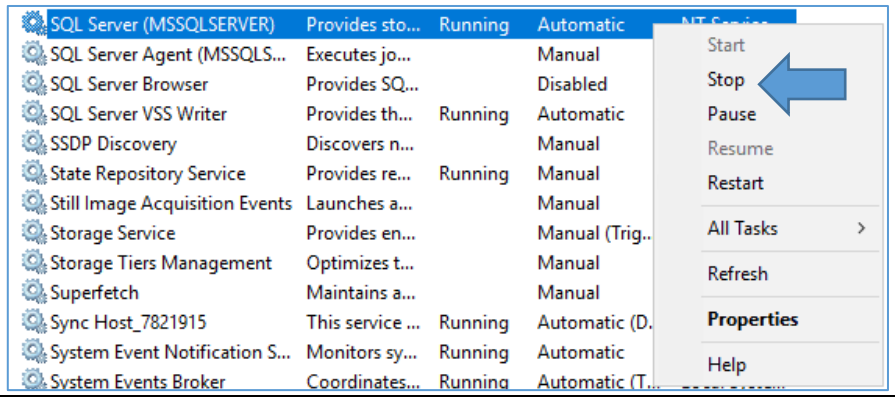




This event might take up to 10 minutes to show up from the time when LHC was enabled in the PowerShell window. Do not proceed with the exercises until this event has been verified.

Note: If election process takes longer than 10 minutes, reboot NYC-XDC-002 to force the election of NYC-XDC-001.

20. Switch to **NYC-SQL-001** and **Stop** the **SQL Server (MSSQLSERVER)** service using the services.msc console.

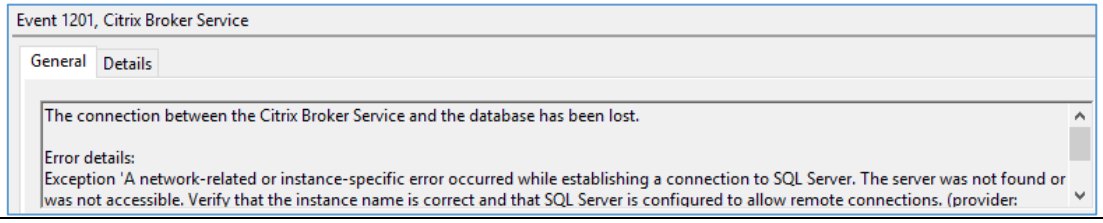


21. Switch to **NYC-XDC-001** and check the event logs.

Verify you are viewing **Custom Views** > **Administrative Events**.

Within the **Event Viewer**, from the Action pane on the right, select **Refresh**.

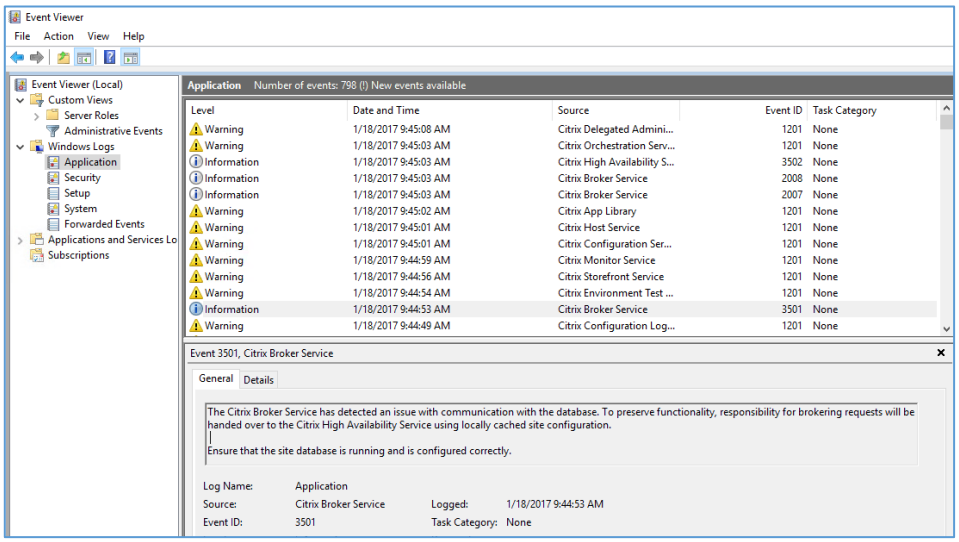
Look for Event ID **1201**.



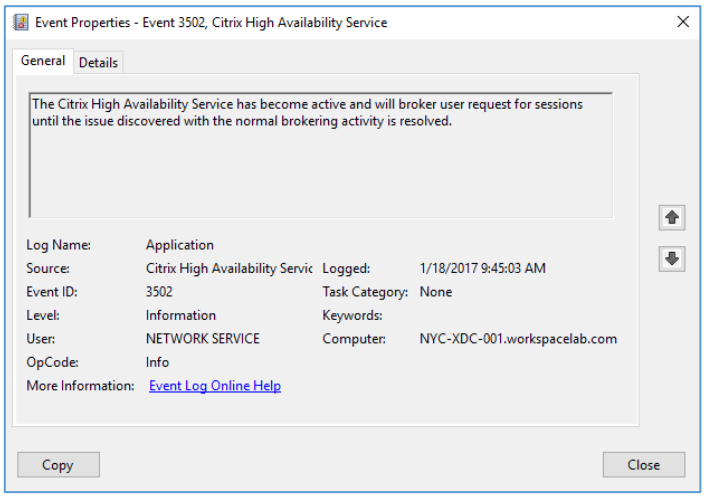
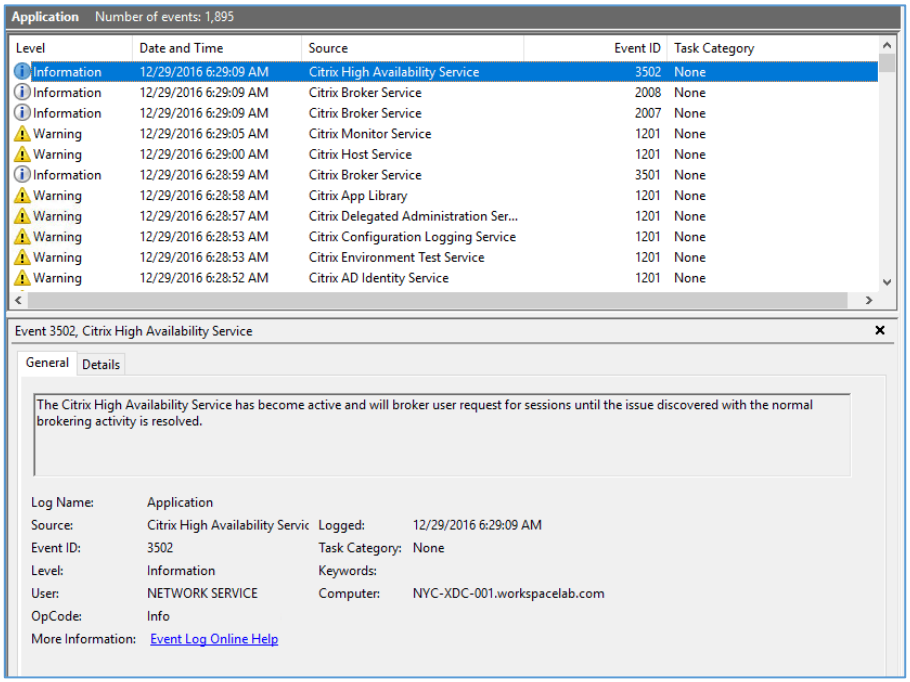
22. Switch the view within Event Viewer to the **Application** events view.

Within the **Event Viewer**, from Action pane on the right, select **Refresh**.

Wait for a minute and click **Refresh** again. Look for Event ID **3501**.



Note: After around 1 minute, the Citrix Broker Service hands operations over to the Citrix High Availability Service and we are now operating in Local Host Cache mode.

23.	Wait for a minute and click **Refresh** again. Look for **Event ID 3502**.  **Note:** With Event ID 3502 the Citrix Availability Service reports it has become active and will broker user requests until the SQL database is back online. 
24.	Switch to NYC-WRK-001, and log on to Citrix Receiver using Auditor2. User name: **Auditor2** Password: **Password1** Application enumeration is successful for Auditor2 user who has never logged on before.
25.	**Launch** the application **Word 2016**. Application launches successfully.
26.	Close **Word 2016** and exit **Citrix Receiver**.
27.	Switch to **NYC-SQL-001** and **Start** the **SQL Server (MSSQLSERVER) Service**.

28.	Log off from **NYC-SQL-001**.

Key Takeaways:

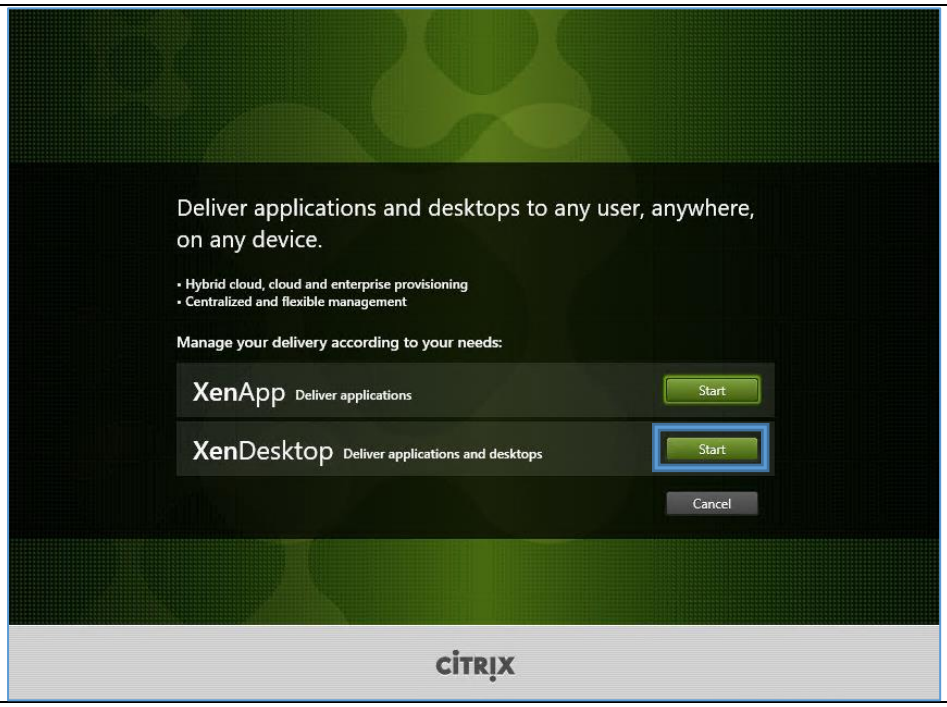
- Local Host Cache is installed automatically during the Controller installation; however, it is not enabled by default.
- Use PowerShell to enable Local Host Cache and disable Connection Leasing at the same time.
- Local Host Cache is a much more resilient feature than Connection Leasing but it does not negate the need for a highly available SQL installation.

Exercise 11-4: Install the Second StoreFront Server

Scenario:

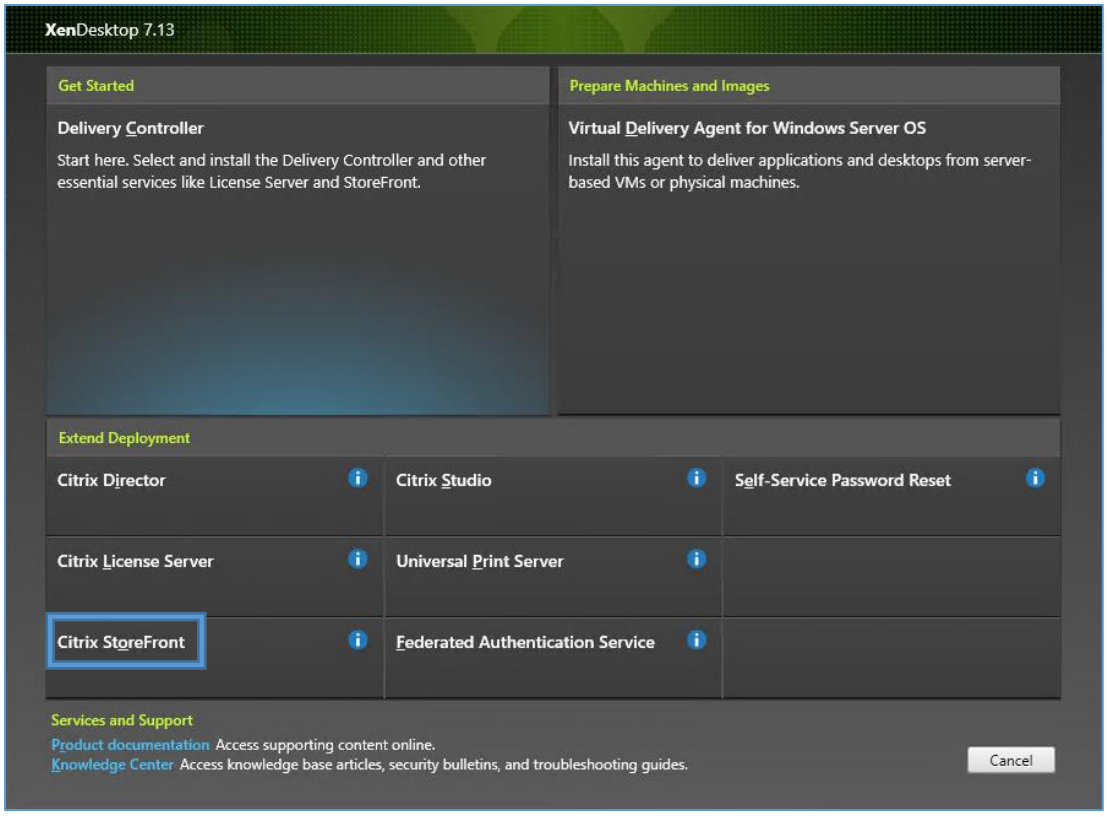
Your task is to install a Second StoreFront Server that will be used to join the StoreFront Server Group.

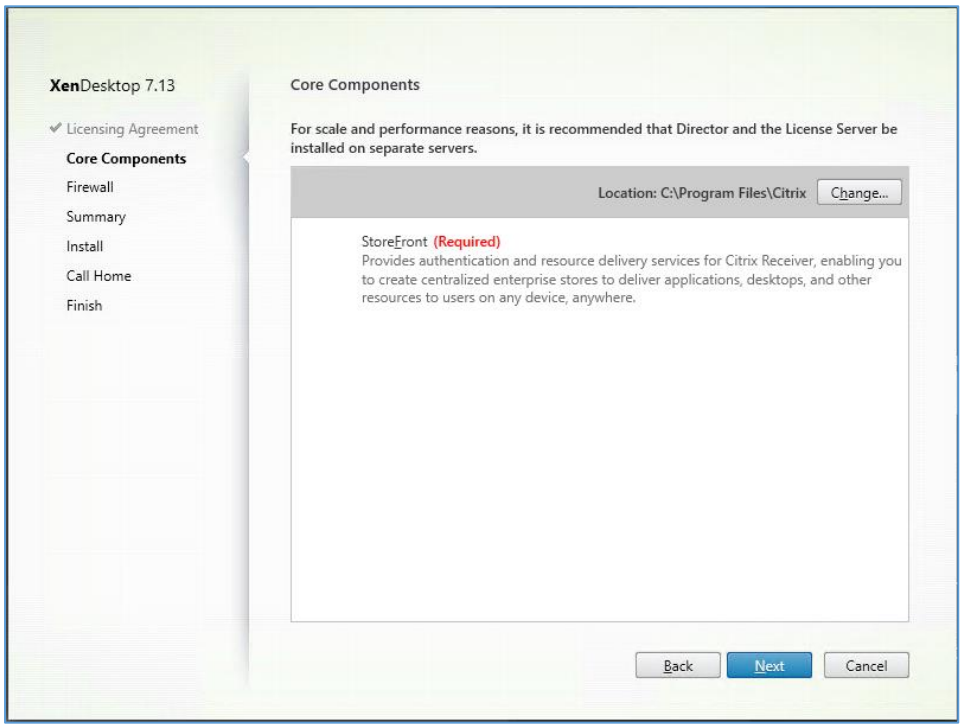
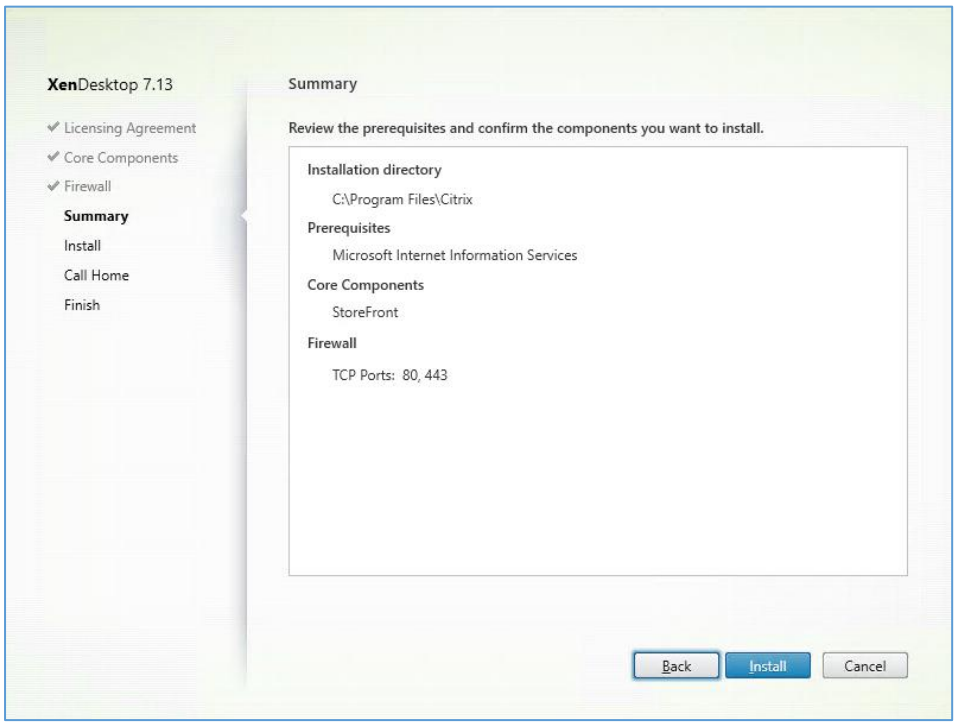
Step	Action
1.	Using **XenCenter** mount the XenApp and XenDesktop installation media ISO to **NYC-STF-002**. To mount the installation media ISO, select **NYC-STF-002** in the left pane of the XenCenter. In the right pane, select the **Console** tab. Using the **DVD Drive 1:** drop-down menu select **XenApp_and_XenDesktop_7_13.iso**. **Note**: If there are no ISOs listed in the **DVD Drive 1:** drop-down menu, then the Local ISO Storage Repository (SR) that contains the ISO library may need to be re-scanned. In the left pane of **XenCenter** select the **Local ISO SR XS**. In the right pane select the **Storage** tab and click on the **Rescan** button. This task may need to be repeated later in the course. **Note:** If the above rescan of the **Local ISO SR XS** does not show the specific ISO for installation: XenApp_and_XenDesktop_7_13.iso, then please tell your instructor.
2.	Using the Remote Desktop Connection Manager, connect to **NYC-STF-002**. To log on to NYC-STF-002, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password.
3.	Launch the **File Explorer** application from the Windows Taskbar or Start Menu. Double-click the **green Citrix logo** next to **CD Drive** under Devices and drives.
4.	On the Deliver applications and desktops to any user, anywhere, on any device screen, click **Start** next to the XenDesktop option.

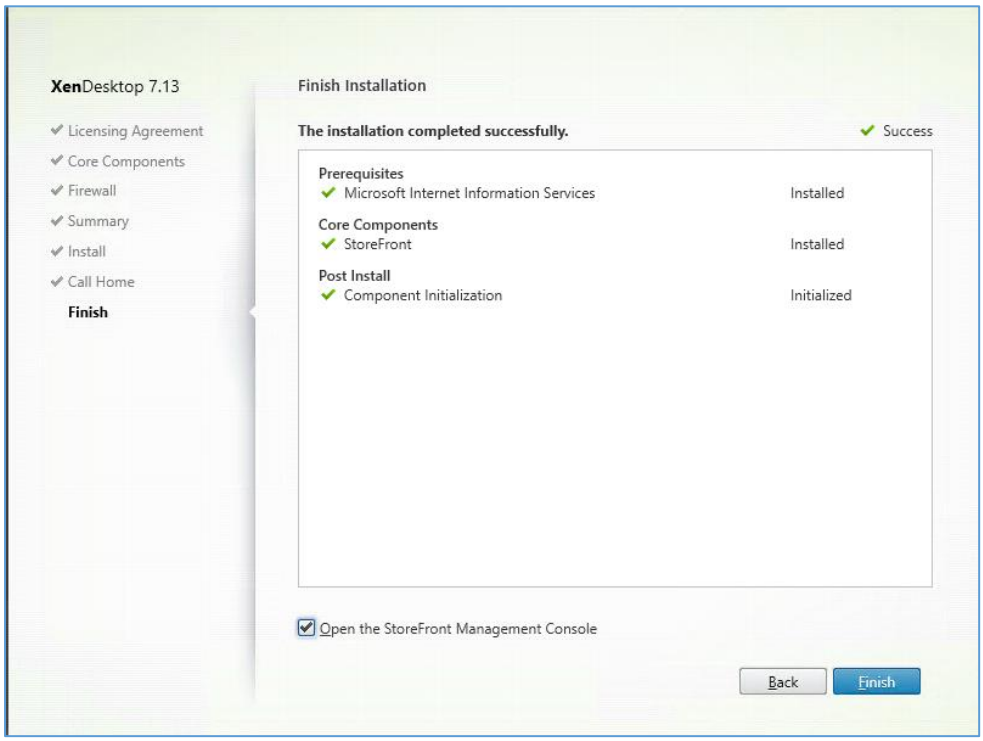
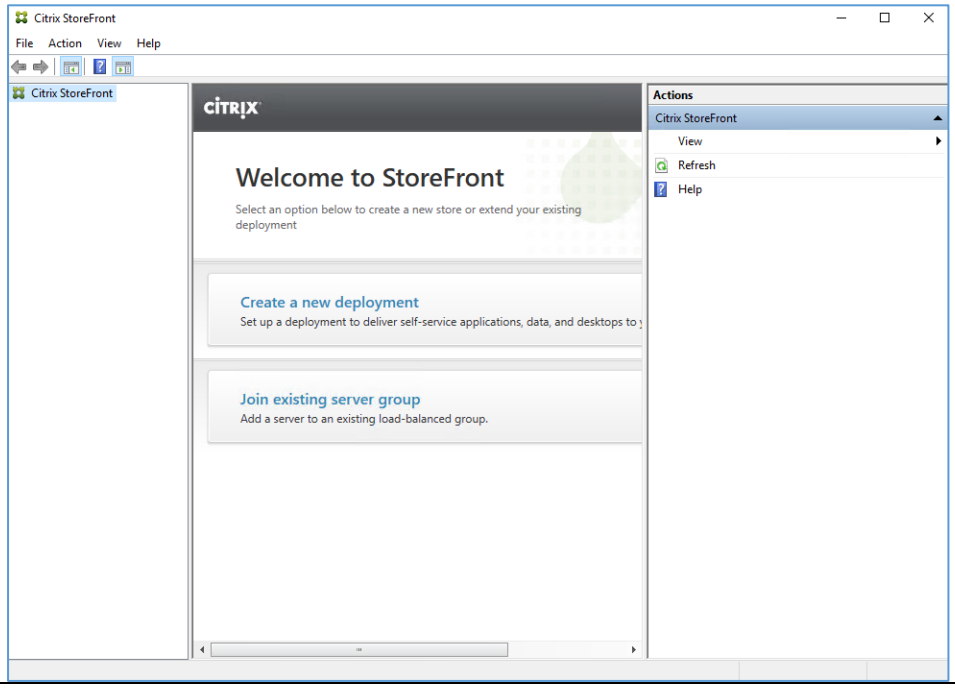


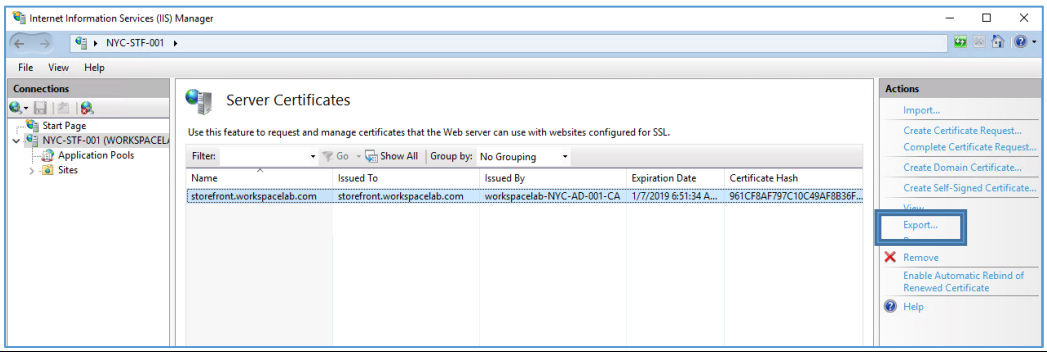
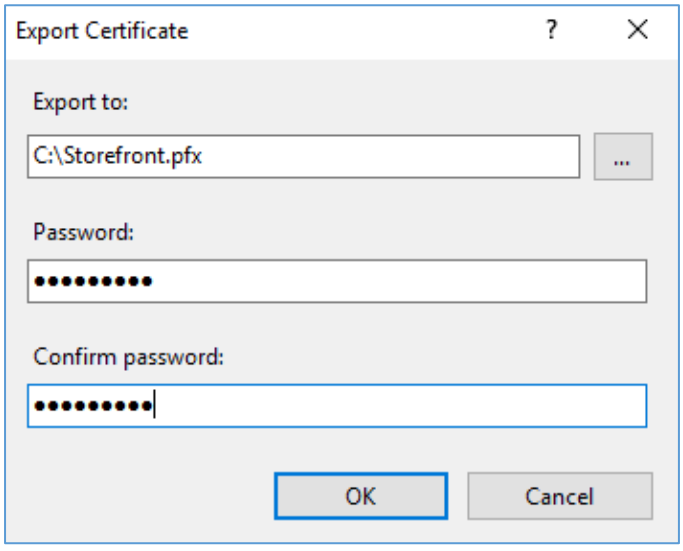
5. The wizard will now display all possible installation options that are compatible with the Operating System of the machine that you are on.

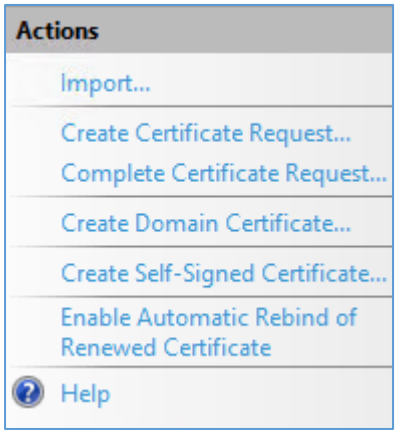
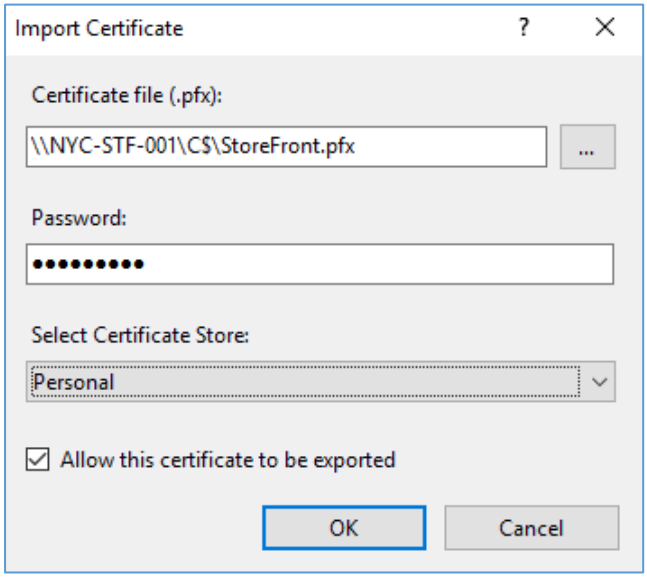
   Select **Citrix StoreFront**.

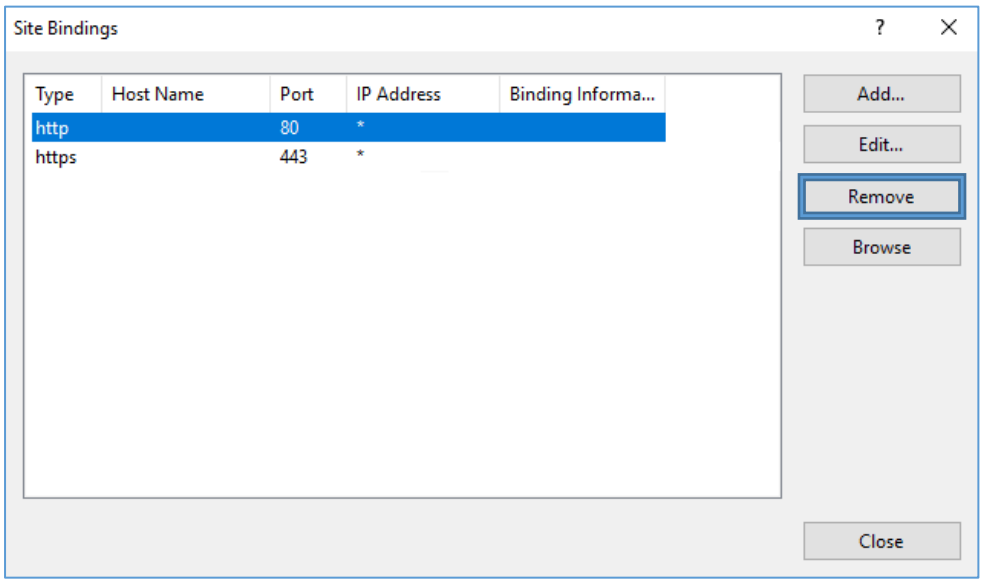


6.	Review the License Agreement page. If you agree, respond to the Software License Agreement and then click **Next**.
7.	On the Core Components page, leave the default location and click **Next**. 
8.	On the Firewall page, leave the default **Automatically** option selected and click **Next**.
9.	On the Summary page, review the summary and click **Install**. 

10.	The installation process will take a few minutes. After the installation has completed, on the Call Home page click, **I do not want to participate in Call Home** and click **Next**.
11.	On Finish Installation page, click **Finish**.  Wait for the StoreFront console to open. 
12.	Using the Remote Desktop Connection Manager, switch to **NYC-STF-001**. To log on to NYC-STF-001, right-click this machine and choose **Connect server**.

	Note: The following credentials are used to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password.
13.	Click **Start** > Windows **Administrative Tools** > **Internet Information Services (IIS) Manager**. **Note**: Internet Information Services (IIS) Manager can also be launched from Server Manager. Click the **Server Manager** icon in the Windows Taskbar > click **Tools** > then click **Internet Information Services (IIS) Manager**.
14.	Expand **NYC-STF-001 (WORKSPACELAB\Administrator)**. **Note**: If the Internet Information Manager (IIS) dialog box appears, select **Do not show this message again** and click **No** on the Internet Information Manager (IIS) dialog box. This dialog box will take you to http://www.microsoft.com/web/downloads/platform.aspx and provide information about IIS.
15.	In the middle pane, double-click **Server Certificates**.
16.	Within the Server Certificates pane highlight **storefront.workspacelab.com** and click **Export**. 
17.	In the Export Certificate Dialog box configure the following: Export to: **C:\StoreFront.pfx** Password: **Password1** Confirm Password: **Password1**  Click **OK**. Close **IIS Manager**.

18.	Using the Remote Desktop Connection Manager, switch to **NYC-STF-002**. To log on to NYC-STF-002, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password.
19.	Click **Start** > **Windows Administrative Tools** > **Internet Information Services (IIS) Manager**.
20.	Expand **NYC-STF-002 (WORKSPACELAB\Administrator)**. **Note**: If the Internet Information Services (IIS) Manager dialog box appears, select **Do not show this message** and click **No** on the Internet Information Services (IIS) Manager dialog box. This dialog box will take you to http://www.microsoft.com/web/downloads/platform.aspx and provide information about IIS.
21.	In the middle pane, double-click **Server Certificates**.
22.	Within the Server Certificates pane, click **Import**. 
23.	In the Import Certificate dialog box configure the following: Certificate file (.pfx): **\\NYC-STF-001\C$\StoreFront.pfx** Password: **Password1** Select Certificate Store: **Personal** 

	Note: Do not browse to the Certificate file, just enter in the text. Click **OK**.
24.	Expand **NYC-STF-002 (WORKSPACELAB\Administrator)** > **Sites** and click on **Default Web Site**.
25.	On the right pane under Actions, click **Bindings**.
26.	On the Site Bindings dialog box click **Add**.
27.	Change the Type field to be **https**.
28.	On the SSL certificate drop-down list select **storefront.workspacelab.com**.
29.	Click **View** and notice that this is the certificate created on Exercise 5-3. Click **OK**.
30.	On the Add Site Binding dialog box click **OK**.
31.	In the Site Bindings dialog box, select the **http** binding and click **Remove**.  Click **Yes** to confirm the removal of the binding and click **Close** to close the Site Bindings dialog box.

Key Takeaways:

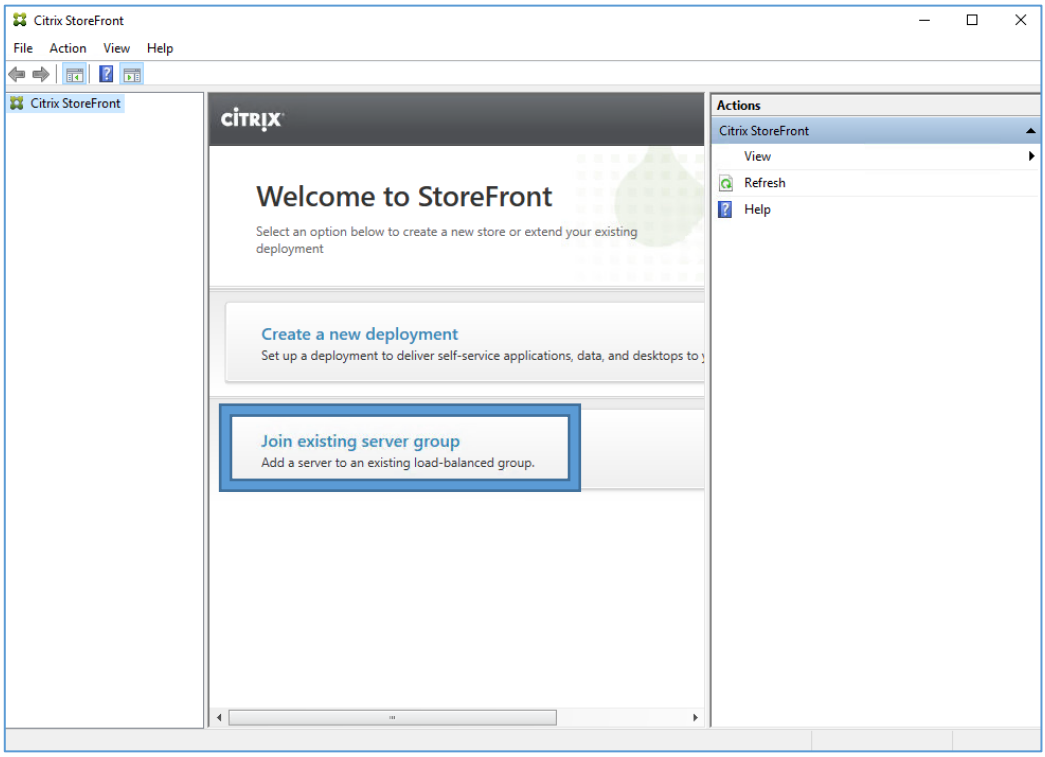
- Installing the Second StoreFront Server is the same steps as installing the first StoreFront Server. The Server is joined in a future exercise.
- The Storefront installation requires IIS and installs this component automatically if needed.
- To achieve LTSR compliance, ensure the correct StoreFront version (including required updates) are installed.

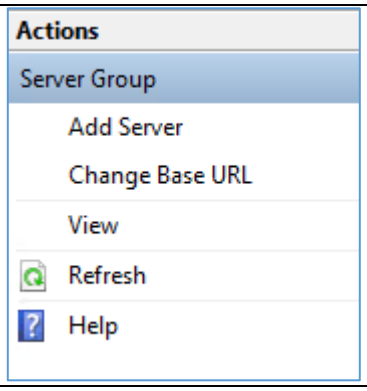
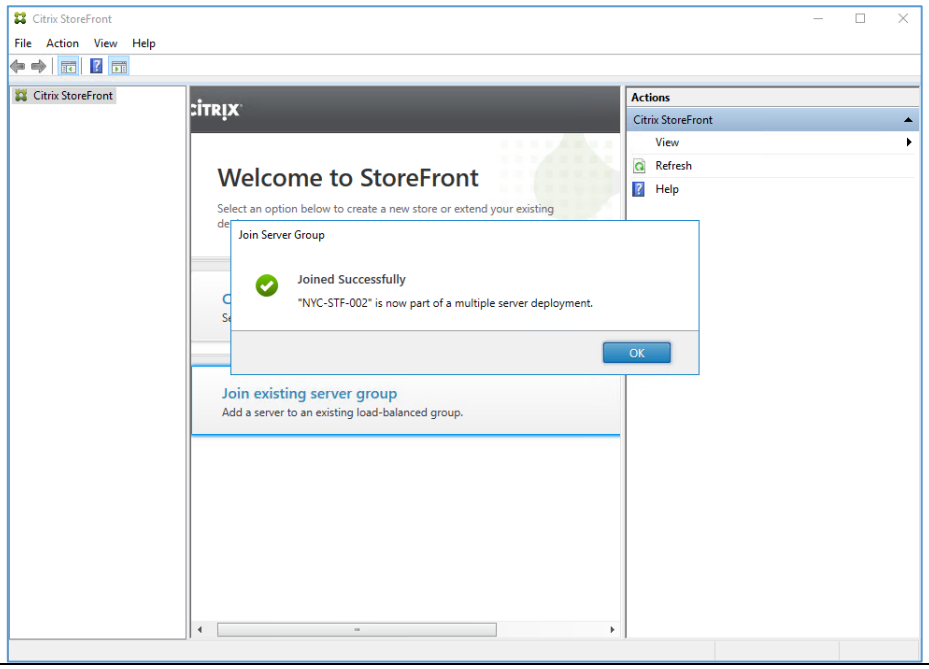
Exercise 11-5: Join the Second StoreFront Server to the Server Group

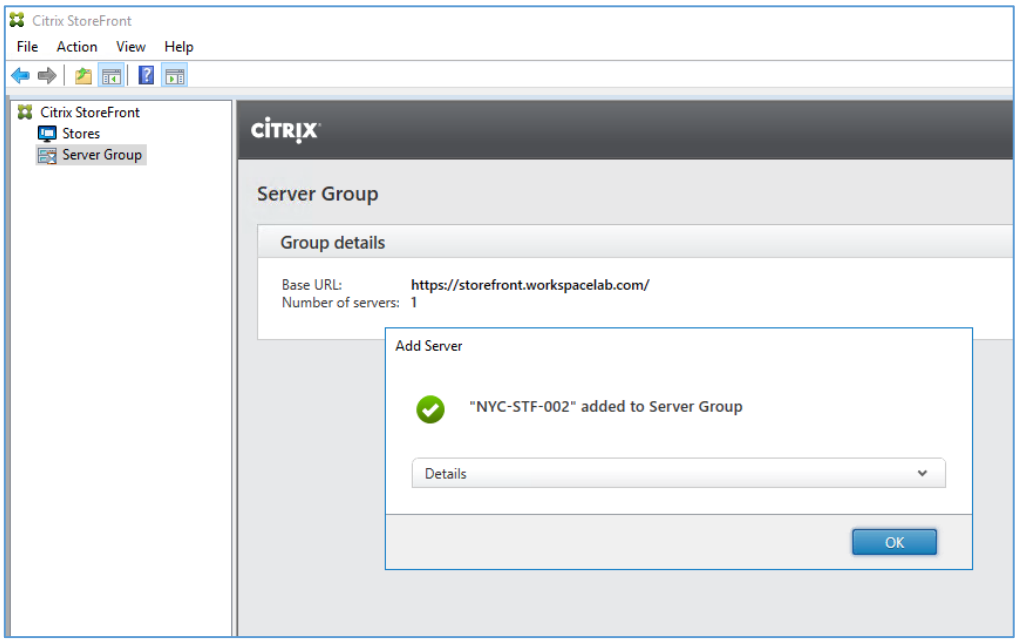
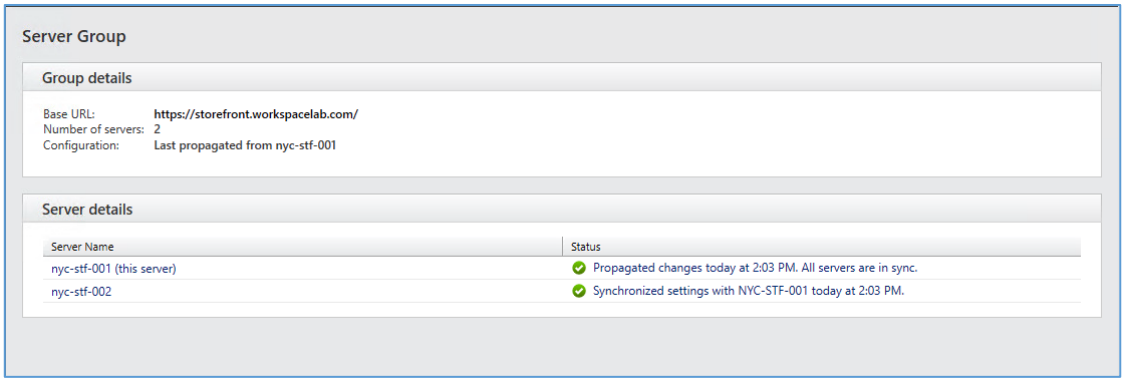
Scenario:

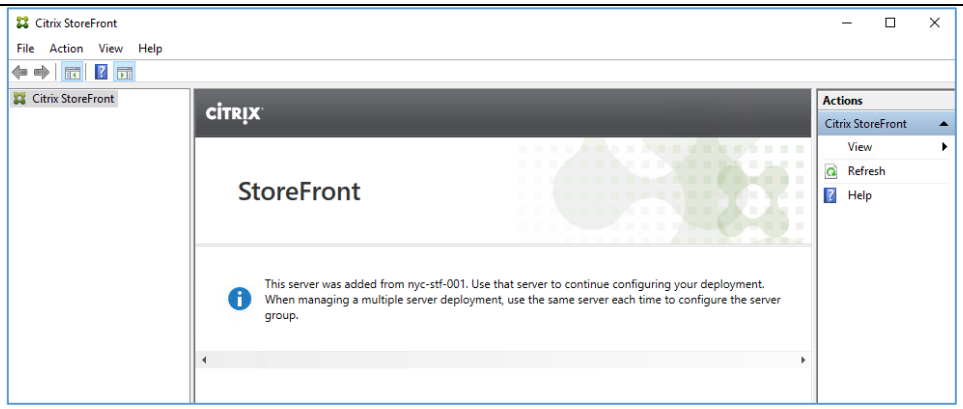
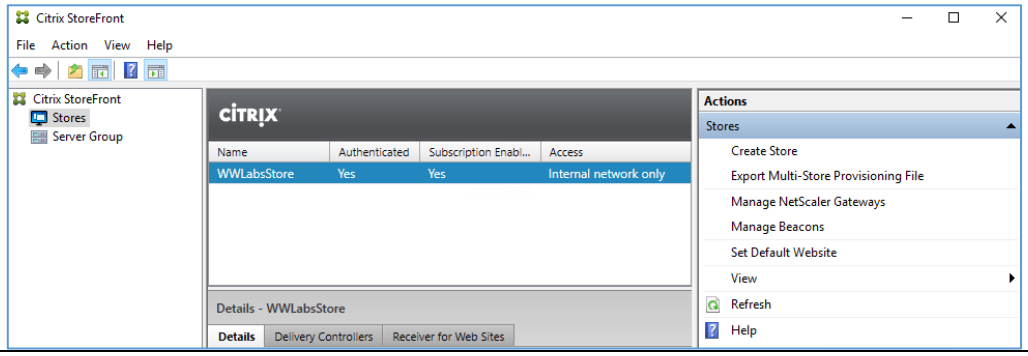
To complete the StoreFront redundancy, you have been tasked to join the second StoreFront server to the Server Group.

Step	Action
1.	Using the Remote Desktop Connection Manager, connect to **NYC-STF-002**.

	To log on to NYC-STF-002, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password.
2.	Use the StoreFront Management Console to join NYC-STF-002 to the existing server group. In the StoreFront console, click **Join existing server group**.  **Note**: The **StoreFront Management Console** was launched in a previous exercise. If the console was closed in a previous exercise, then click **Start** > **Citrix** > and click **Citrix StoreFront**.
3.	Using the Remote Desktop Connection Manager, connect to **NYC-STF-001**. To log on to NYC-STF-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password.
4.	Using the StoreFront Management Console, in the left pane click **Server Group**. In the right pane, click **Add Server**.

	
5.	An **Authorizing server** and an **Authorization code** displays on the screen. Write the code and the server name down.
6.	Using the Remote Desktop Connection Manager, switch back to **NYC-STF-002**. **Note:** In a previous exercise, you had logged on to **NYC-STF-002** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-STF-002**, right-click this machine and choose **Connect server**.
7.	Enter the **Authorizing server** and **Authorization code** from NYC-STF-001. Click **Join**. When successful click **OK** on the Join Server Group dialog box. 
8.	Using the Remote Desktop Connection Manager, switch back to **NYC-STF-001**. **Note:** In a previous exercise, you had logged on to **NYC-STF-001** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password.

	Note: If your Remote Desktop Connection session disconnected, log on to **NYC-STF-001**, right-click this machine and choose **Connect server**.
9.	On NYC-STF-001, click **OK** on the Add Server dialog box.   **Note**: In the event that the Add Server dialog box indicates that there was an error, review the Event Viewer on NYC-STF-001. If there is an Event 31 Citrix Configuration Replication Service error, then review the details tab of the error. An Event 31 error most likely means that access to the path for Citrix Receiver was denied. If this is the case, use the directory path in the contents of the error to copy receiver.exe from NYC-STF-001 to NYC-STF-002.
10.	Switch to **NYC-STF-002**, notice the message in the StoreFront console. This message is very important and is only shown the first time you open up the console on a secondary StoreFront server. Avoid editing the store from multiple StoreFront servers. Always use a single StoreFront server to make changes because failing to do so could lead to configuration replication problems or even store corruption.

	 On NYC-STF-002, click **Refresh** in the Actions pane.
11.	On the left pane click **Stores** and confirm that the WWLabsStore store is displayed. 

Key Takeaways:

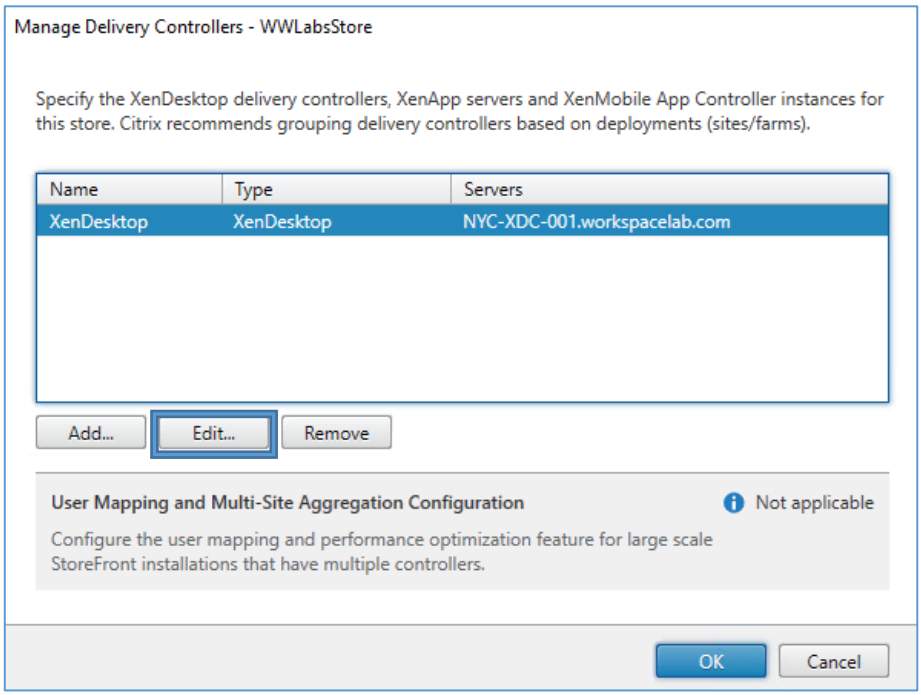
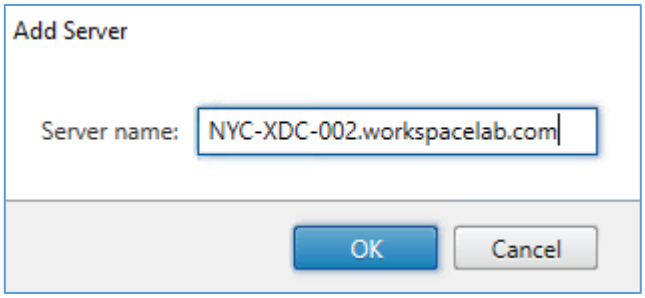
- When joining one StoreFront Server to a group, it is required to have access to both servers.
- The primary StoreFront Server version needs to be the same as the second StoreFront Server.
- Authorization server and Authorization code is required when joining a newly installed StoreFront server to the Server group.

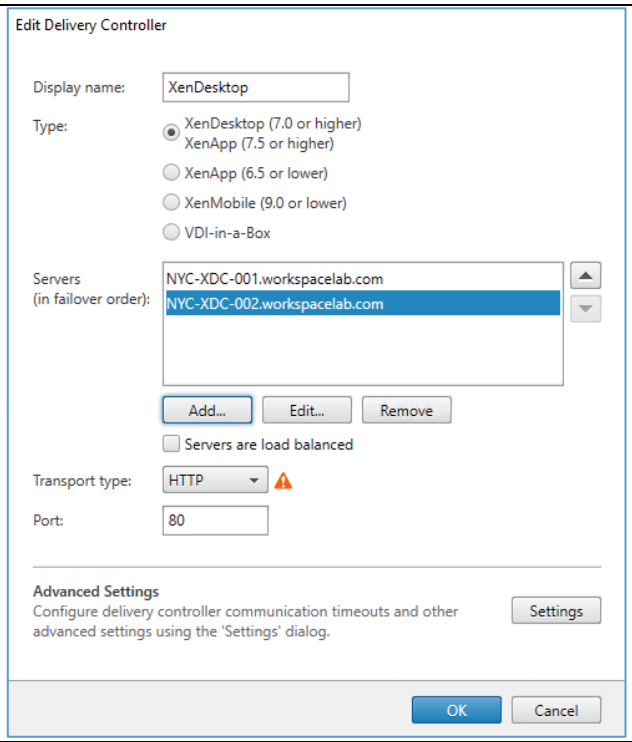
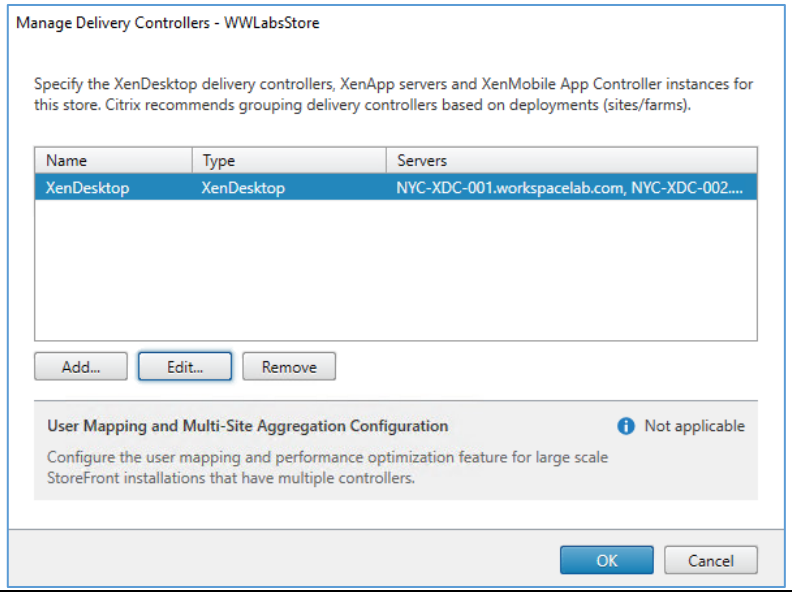
Exercise 11-6: Edit the Store to Add the Second Delivery Controller

Scenario:

Your task is to finalize the redundancy in the Site by adding a Second Delivery Controller.

Step	Action
1.	Using the Remote Desktop Connection Manager, confirm you are still connected to **NYC-STF-001**. **Note:** In a previous exercise, you had logged on to **NYC-STF-001** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-STF-001**, right-click this machine and choose **Connect server**.
2.	Using the StoreFront Management Console, on the left pane click **Stores**.

	Make sure that **WWLabsStore** is selected. On the right pane, click **Manage Delivery Controllers**. **Note**: The **StoreFront Management Console** was launched in a previous exercise. If the console was closed in a previous exercise, then click **Start** > **Citrix** > and click **Citrix StoreFront**.
3.	On the Manage Delivery Controllers dialog box, click **Edit**. 
4.	Click **Add** under the Servers section, type **NYC-XDC-002.workspacelab.com** and click **OK**. 
5.	On the Edit Delivery Controller window, de-select the checkbox **Servers are load balanced** and then click **OK**.

	
6.	On the Manage Delivery Controllers window, click **OK**. 
7.	Using the StoreFront Management Console, in the left pane click **Server Group**. Click **Propagate Changes** from the Actions pane. On the Propagate Changes dialog box, click **Yes**. Click **OK** once the action completes.

Key Takeaways:

- When adding a second controller to the StoreFront store, the existing Delivery Controller configuration is used and the new server is added to it.
- The FQDN of the Delivery Controller is used but it is not required if communication is on port 80.

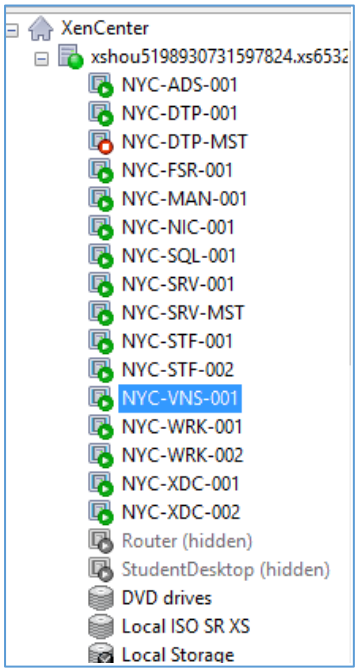
Exercise 11-7: Configuring Load Balancing of the StoreFront Servers

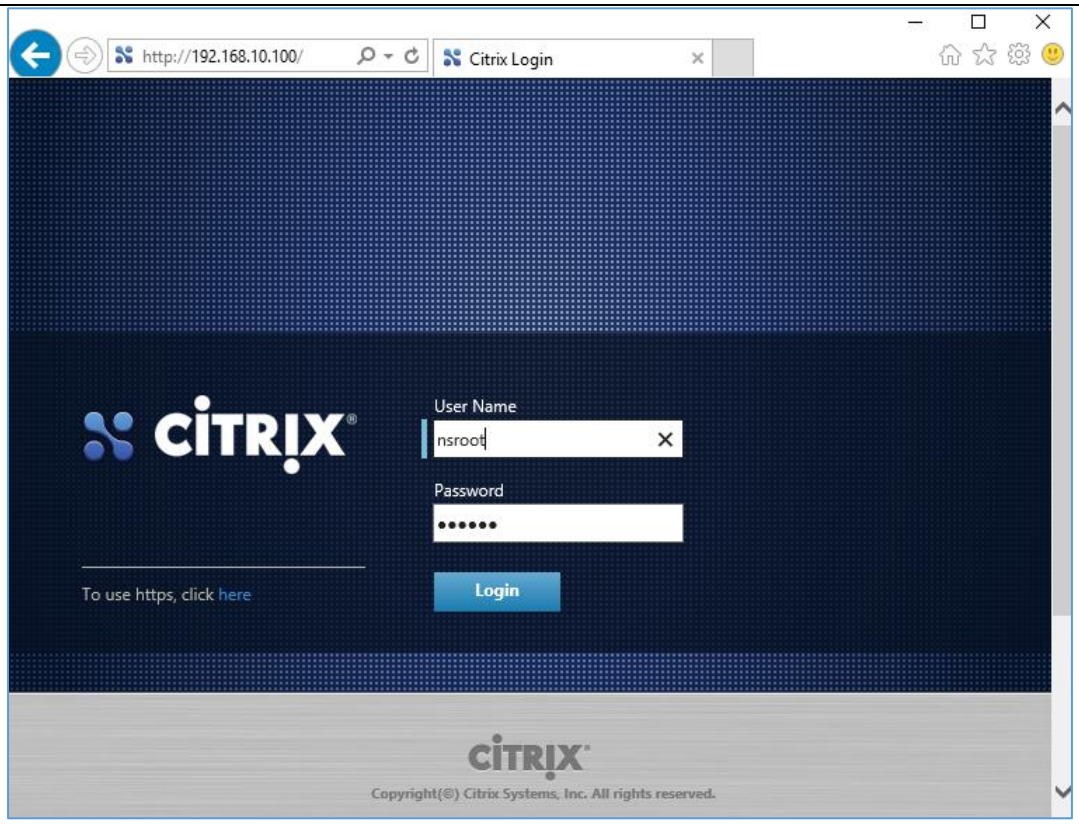
Scenario:

The Citrix NetScaler is an appliance that, among many features, can be used to perform load balancing. Your Lead Citrix Architect has pre-configured a NetScaler in this environment. This configuration includes a wild card certificate.

Your task is to configure the load balancing of the StoreFront Servers using NetScaler.

Note: This course is focused on XenApp and XenDesktop components. In an effort to meet Citrix Leading Practices the NetScaler is introduced here as a load balancer. There is a lot more to NetScaler and NetScaler. For more information, consider follow-up training with the CNS-222 course. Ask you Citrix Instructor for more information.

Step	Action
1.	In the left pane of **XenCenter**, ensure **NYC-VNS-001** and **NYC-NIC-001** are started. 
2.	From the Student Desktop browse to the NetScaler Console. To access the NetScaler Console open **Internet Explorer** and navigate to **http://192.168.10.100**.

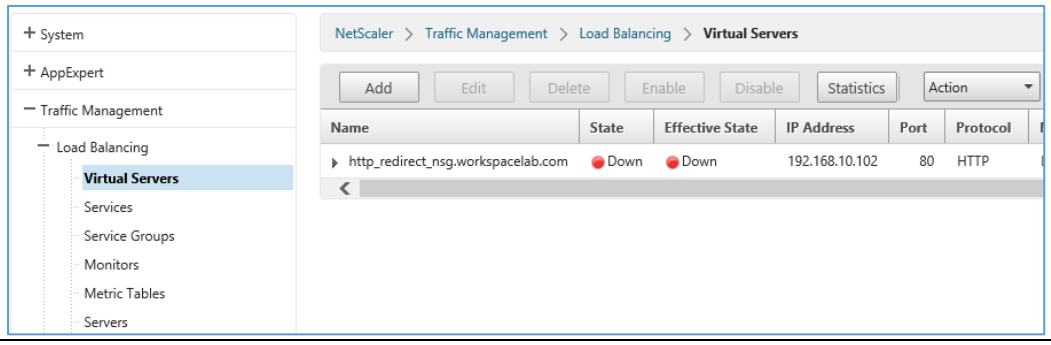


Log on with the following credentials:

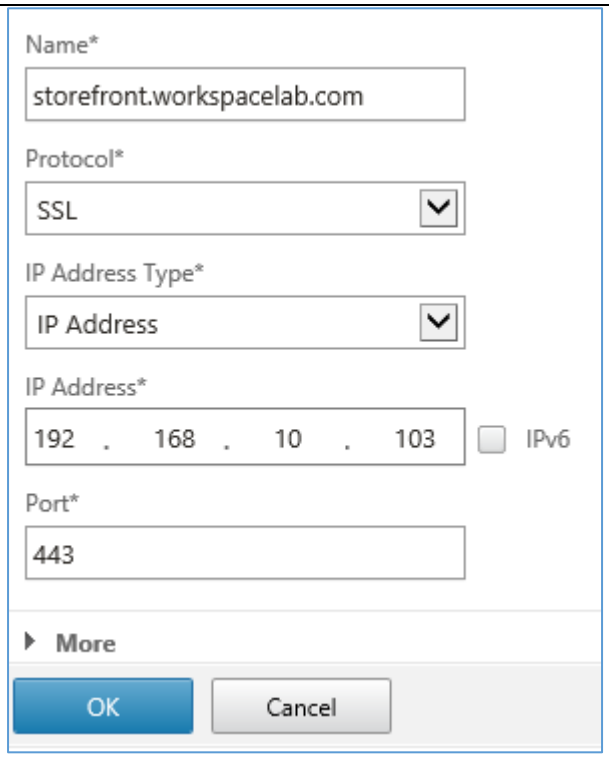
User Name: **nsroot**
Password: **nsroot**

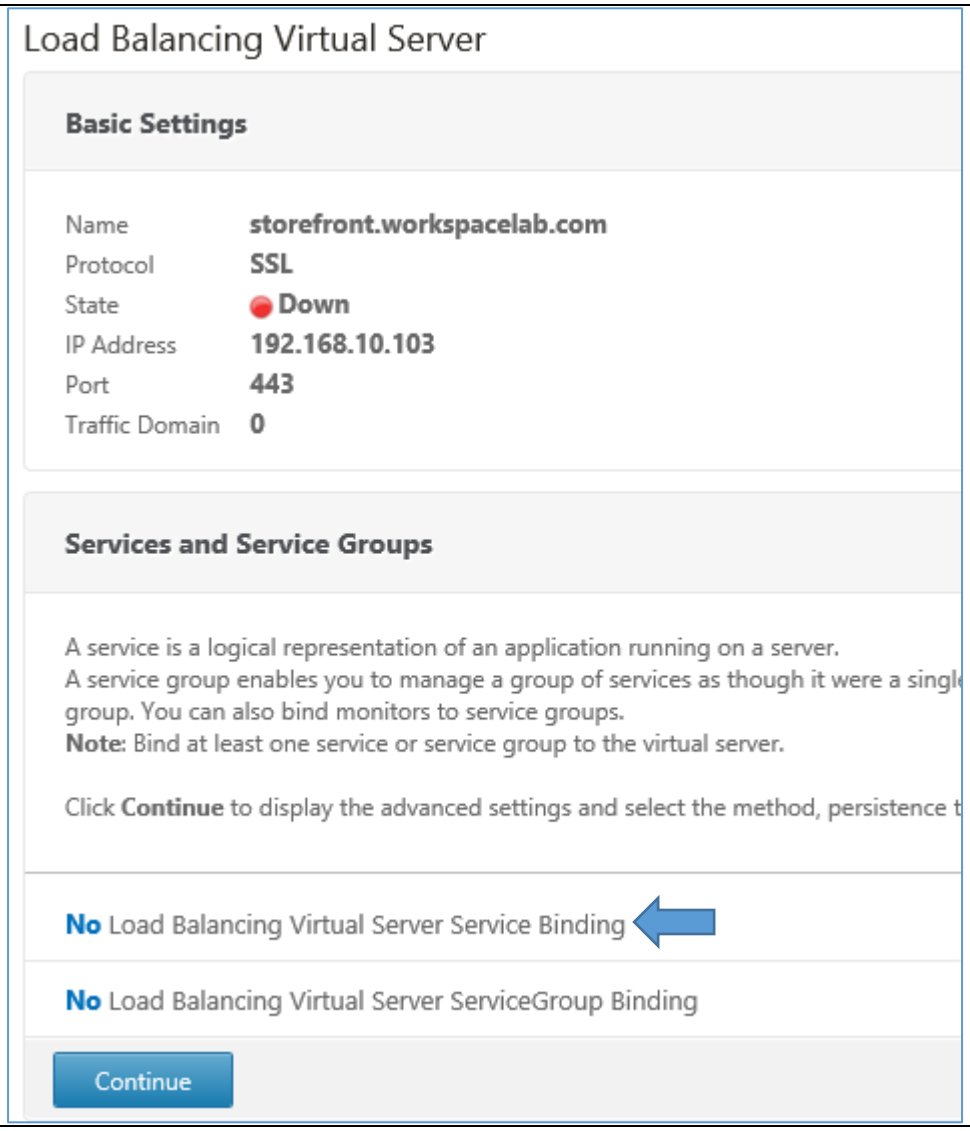
Note: The Citrix NetScaler is a Citrix appliance that you have been tasked to use as your load balancer.

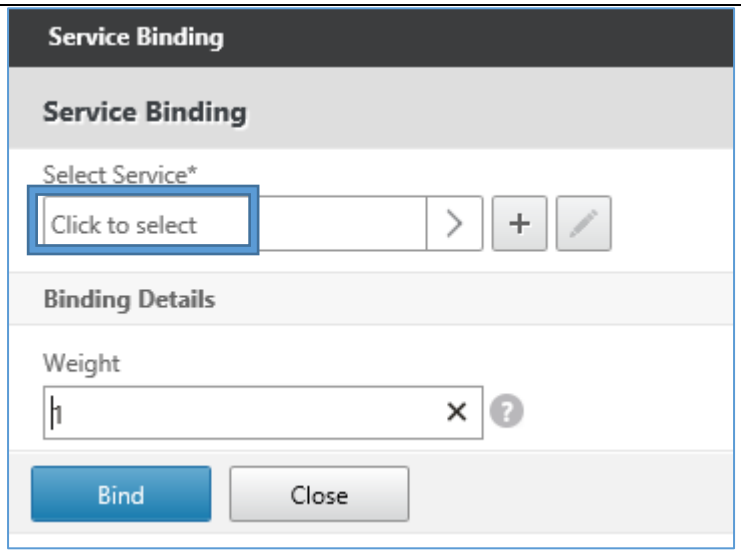
3. On the left pane expand **Traffic Management** > **Load Balancing** > and select **Virtual Servers**.



4. In the middle pane, click **Add** to add a new Virtual Server. Enter the following details:
   - Name: **storefront.workspacelab.com**
   - Protocol: **SSL**
   - IP Address Type: **IP Address**
   - IP Address: **192.168.10.103**
   - Port: **443**

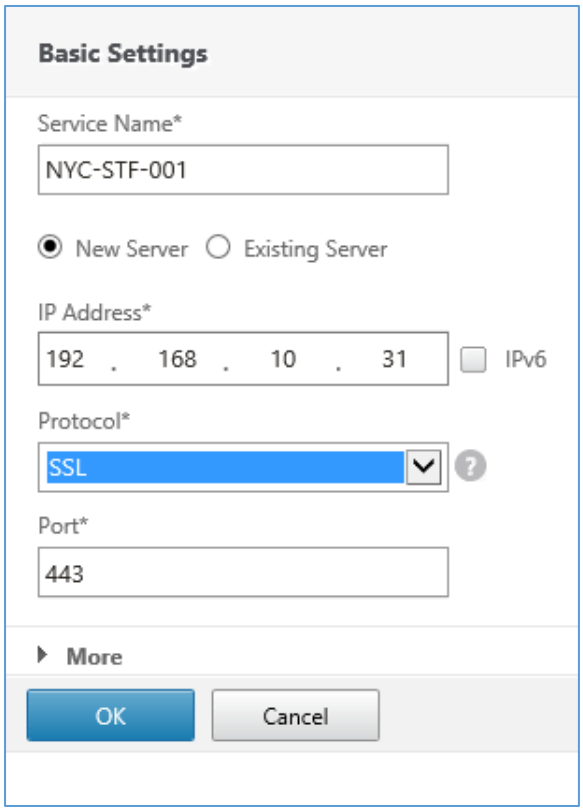
	 Click **OK**.
5.	Under Services and Service Groups, click **No Load Balancing Virtual Server Service Binding**.

	
6.	Click on **Click to select** under Select Service.

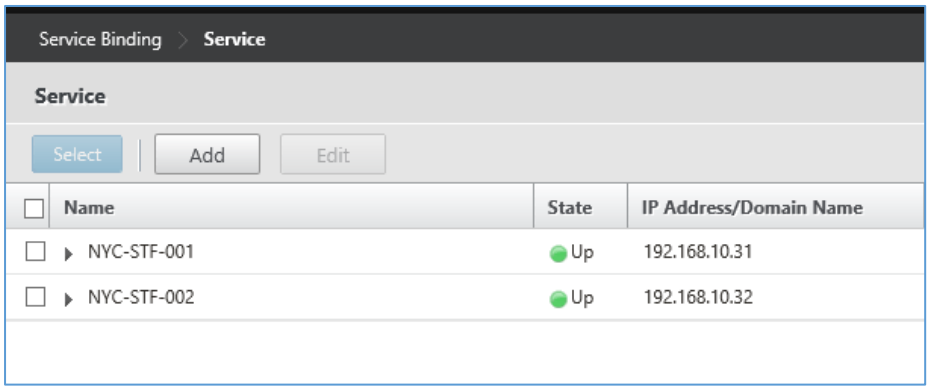
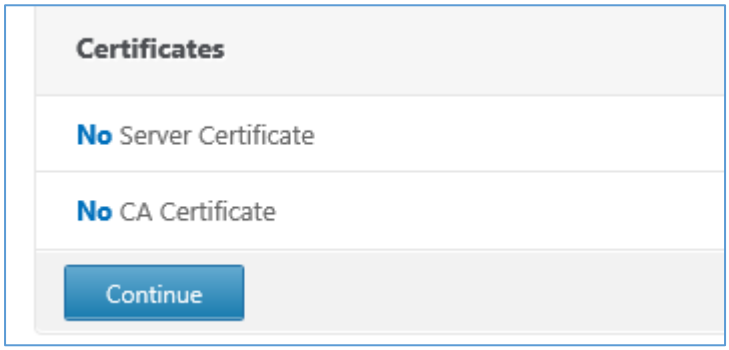


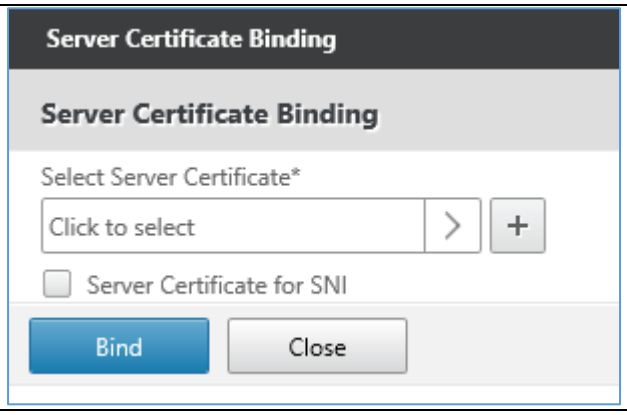
7. Click **Add** in order to define the first StoreFront Server that the load balancing VIP will use. Enter the following values:

- Service Name: **NYC-STF-001**
- Radio button: **New Server**
- IP Address: **192.168.10.31**
- Protocol: **SSL**
- Port: **443**

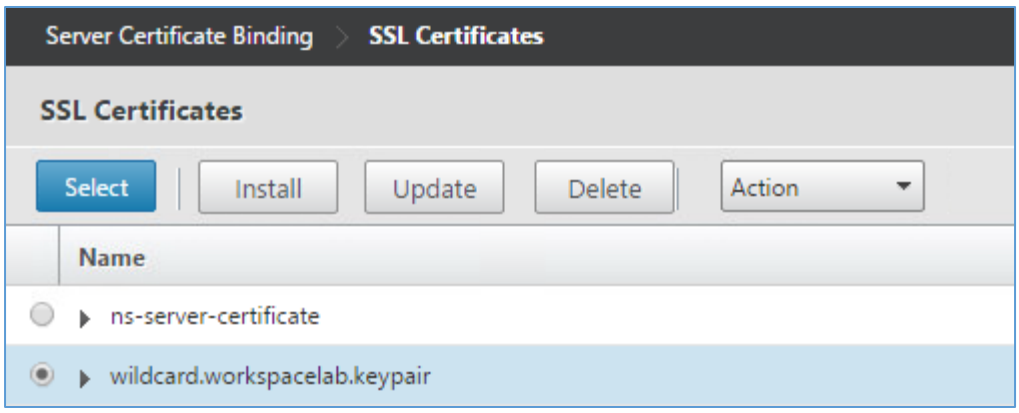


Click **OK**. Scroll down and click **Done**.

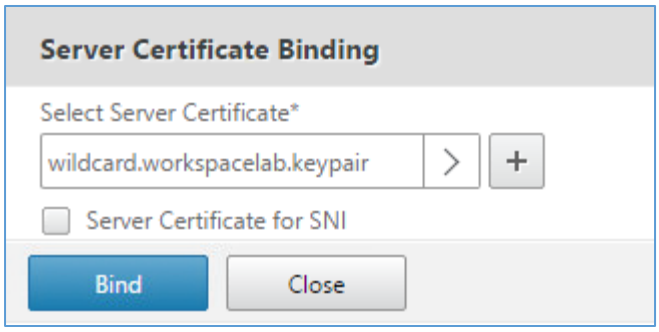
8.	On the Service page, click **Add** to define the second StoreFront Server that the load balancing VIP will use. Enter the following values: • Service Name: **NYC-STF-002** • Radio button: **New Server** • IP Address: **192.168.10.32** • Protocol: **SSL** • Port: **443** Click **OK**. Scroll down and click **Done**.
9.	On the Service page, make sure both Services are selected and click **Select**. 
10.	On the Service Binding page, click **Bind**.
11.	On the Load Balancing Virtual Server page, click **Continue**.
12.	Under Certificates, click **No Server Certificate**. 
13.	On the Server Certificate Binding page, click on **Click to select** under Select Server Certificate.



14. Select the **wildcard.workspacelab.keypair** radio button. Click **Select**.

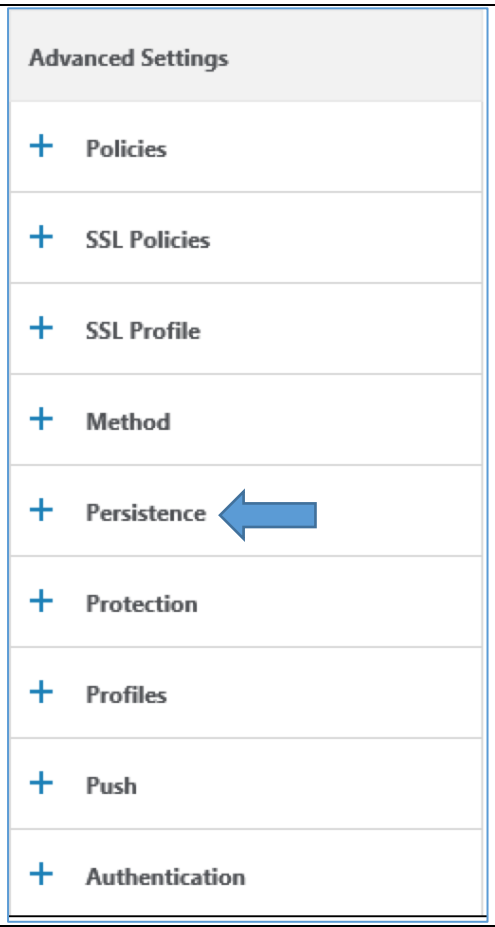
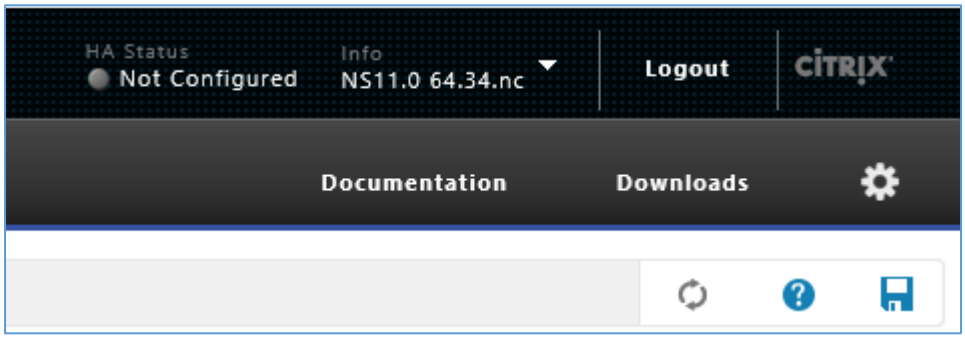


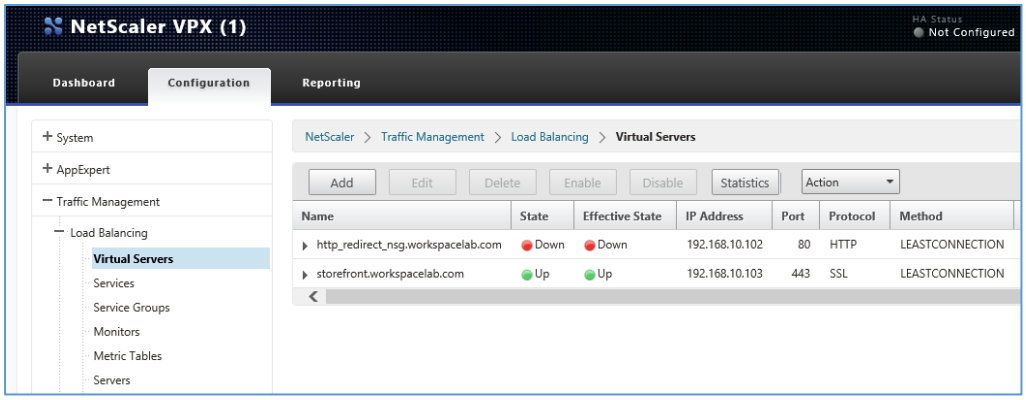
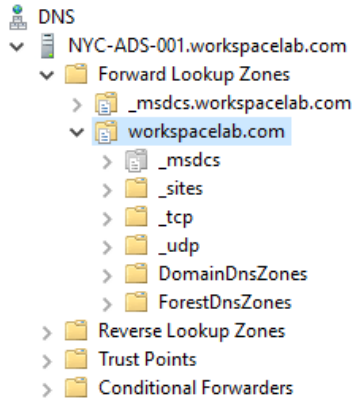
On the Service Certificate Binding page, click **Bind**.



Now click **Continue**.

15. Under **Advanced Settings** on the right, select **Persistence**.

	
16.	Select **SOURCEIP** from the drop-down menu. Set the Timeout (mins)* to **20** (this matches the StoreFront server). Click **OK**.
17.	On the Load Balancing Virtual Server page, scroll down and click **Done**.
18.	Save the running Configuration by clicking the **floppy disk icon** in the top right corner of the page.  Click **Yes** to confirm. **Note**: The NetScaler Appliance is a networking appliance; so it boots off a saved configuration. Any changes made to the configuration are immediately applied, but not saved. If you restart the NetScaler before saving the running configuration, you will lose all of your

	configuration changes, since either the last restart or the last time the running configuration was saved.
19.	On the Virtual Servers pane, verify that the state for the newly created virtual server shows as up.  **Note**: If the state is Down, click the **Refresh** button on the top right side of the console. **Note**: The **http_redirect** load balancer appearing as down was pre-created for this lab and it is down by default;do not attempt to bring this to an Up state.
20.	Using the Remote Desktop Connection Manager, connect to **NYC-ADS-001**. To log on to NYC-ADS-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password.
21.	Click **Start** > **Windows Administrative Tools** > **DNS**.
22.	Navigate the DNS Manager to the workspacelab DNS domain entries. Expand **NYC-ADS-001** > **Forward Lookup Zones** > **workspacelab.com**. 
23.	To load balance the Storefront Servers using the NetScaler Gateway, the DNS record for the StoreFront Server needs to point to the NetScaler Gateway Load Balancing VIP. Right-click the **storefront /Host (A)** record and click **Properties**. Change the IP address from **192.168.10.31** to **192.168.10.103**. Click **OK** to close out of the storefront Properties dialog box. The storefront Host (A) record should now display the updated IP address in DNS.

24.	Close the **DNS Manager** window. Log off **NYC-ADS-001**. To log off, right-click **Start** > choose **Shut down or sign out** > and click **Sign out**.

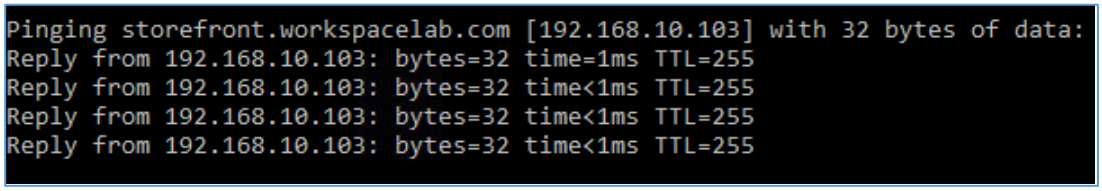
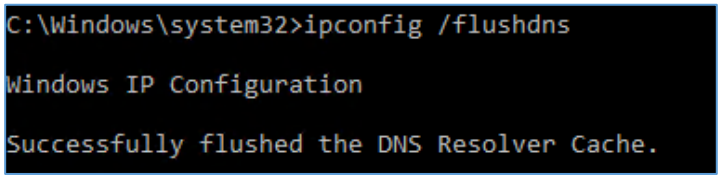
Key Takeaways:

- In order to lad balance StoreFront Servers, a minimum of two servers is required.
- A certificate is required to load balance StoreFront Servers using the NetScaler.

Exercise 11-8: Test the Load Balancing of the StoreFront Servers

Scenario:

Your task is to test the load balancing of the StoreFront Servers.

Step	Action
1.	Using the Remote Desktop Connection Manager, connect to **NYC-WRK-001**. To log on to NYC-WRK-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: user name: **WORKSPACELAB\HR1** with **Password1** as the password.
2.	Click **Start** and type **Command Prompt**. Right-click **Command Prompt** from the list and select **Run as administrator.** Type **ping storefront.workspacelab.com** and press **Enter**. **Note**: If you receive a User Account Control window, enter Username as Workspacelab\Administrator and Password as Password1, and click **Yes**.  Notice the output from the Command Prompt. **Note**: If the record is still pointing to 192.168.10.31 then run the following command: **ipconfig /flushdns**  Type **ping storefront.workspacelab.com** and press **Enter**. Notice, after flushing the DNS, the record now points to the new IP address 192.168.10.103. Close the **Command Prompt** after the command has completed successfully.
3.	Open **Internet Explorer** and browse to **https://storefront.workspacelab.com**. The Citrix NetScaler is now performing load balancing using both StoreFront servers.

4.	**Refresh** the Internet Explorer browser window to load balance between the StoreFront servers.

Key Takeaways:

- In order to use the NetScaler to load balance the StoreFront servers, an FQDN must be defined. In this scenario, the FQDN was already created to access the Load Balancing VIP on the NetScaler.
- One way to test load balancing of the StoreFront Servers is to turn a StoreFront Server off and make sure we can still access the StoreFront Store. You can also disable the service defined on the Load Balancing VIP on the NS.

Module 12: XenApp and XenDesktop Site Basic Network Security Considerations

Overview:

This module presents the integration of XenApp and XenDesktop with a Citrix NetScaler Gateway to perform as a network SSL Proxy in between the user endpoint devices and the StoreFront Server. This proxy provides secure connections outside of the network to apps and desktop resources.

Before you begin:

Estimated time to complete Module 12 lab exercises: 40 minutes

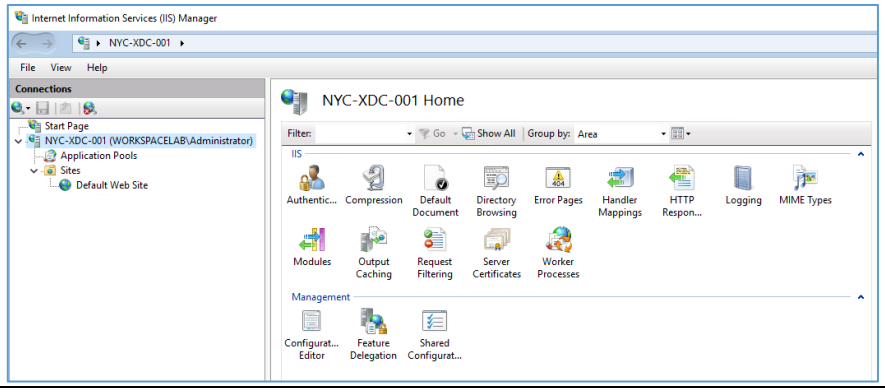
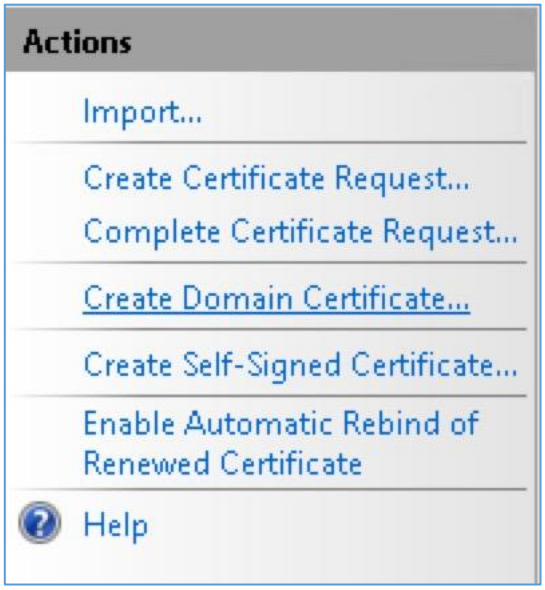
Exercise 12-1: Secure XML Traffic on NYC-XDC-001

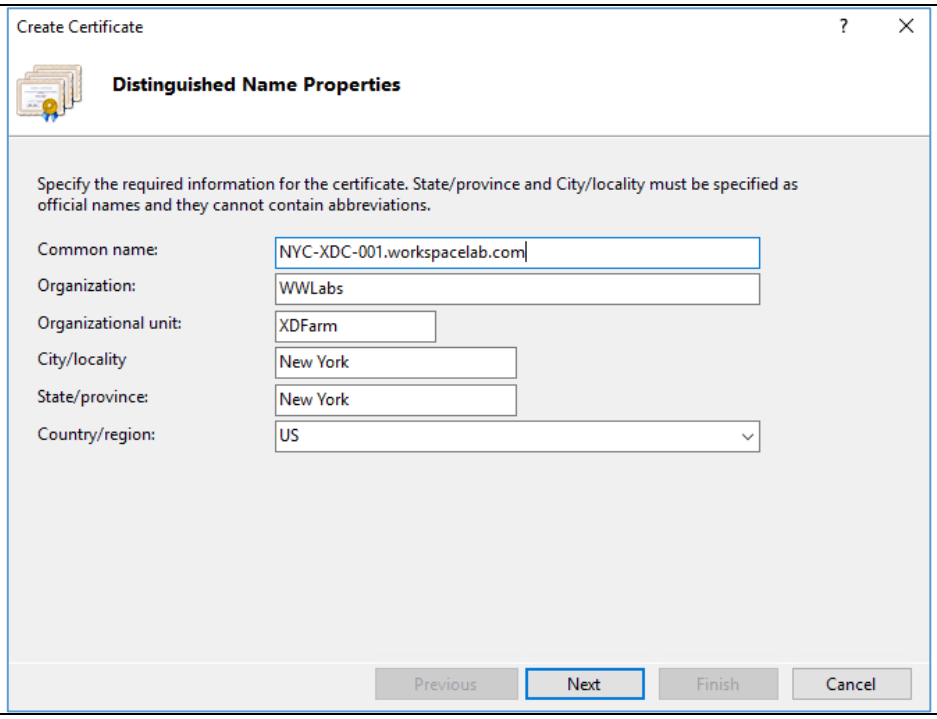
Scenario:

The Citrix XML Service is installed during the Delivery Controller installation. It's this service that the StoreFront servers use to communicate with the Site. The first step to address security to the XenApp and XenDesktop environment is to recognize that the XML service communication uses http clear text by default and that it is considered a Citrix Leading Practice to secure this XML traffic.

Your task is to secure XML traffic on the First Delivery Controller, NYC-XDC-001.

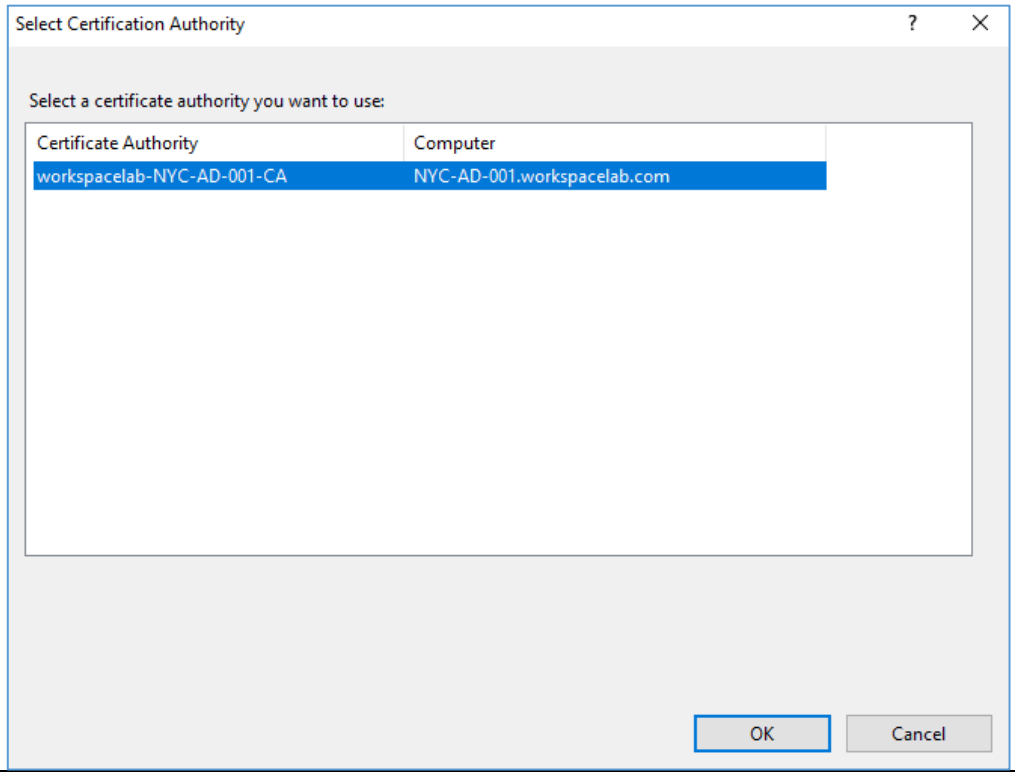
Step	Action
1.	The following VMs are required before beginning the exercises for this Module; all others may be powered down. To power manage your VMs, switch to XenCenter, right-click on the VM in the left pane and select Start or Shut Down. If prompted click Yes. • NYC-ADS-001 • NYC-SQL-001 • NYC-FSR-001 • NYC-VNS-001 • NYC-NIC-001 • NYC-XDC-001 • NYC-XDC-002 • NYC-STF-001 • NYC-STF-002 • NYC-SRV-001 • NYC-WRK-001 **Note**: These above VMs are listed in the start-up order.
2.	Using the Remote Desktop Connection Manager, confirm you are still connected to **NYC-XDC-001**. **Note:** In a previous exercise, you had logged on to **NYC-XDC-001** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-XDC-001**, right-click this machine and choose **Connect server**.

3.	Click **Start** > **Windows Administrative Tools** > **Internet Information Services (IIS) Manager**.
4.	Expand **NYC-XDC-001 (WORKSPACELAB\administrator)**. In the middle pane, double-click on **Server Certificates**. 
5.	On the right pane under Actions, click **Create Domain Certificate**.  Enter the following settings: • Common Name: **NYC-XDC-001.workspacelab.com** • Organization: **WWLabs** • Organizational unit: **XDFarm** • City/locality: **New York** • State/province: **New York** • Country/region: **US** Click **Next** to continue the Domain Certificate creation wizard.



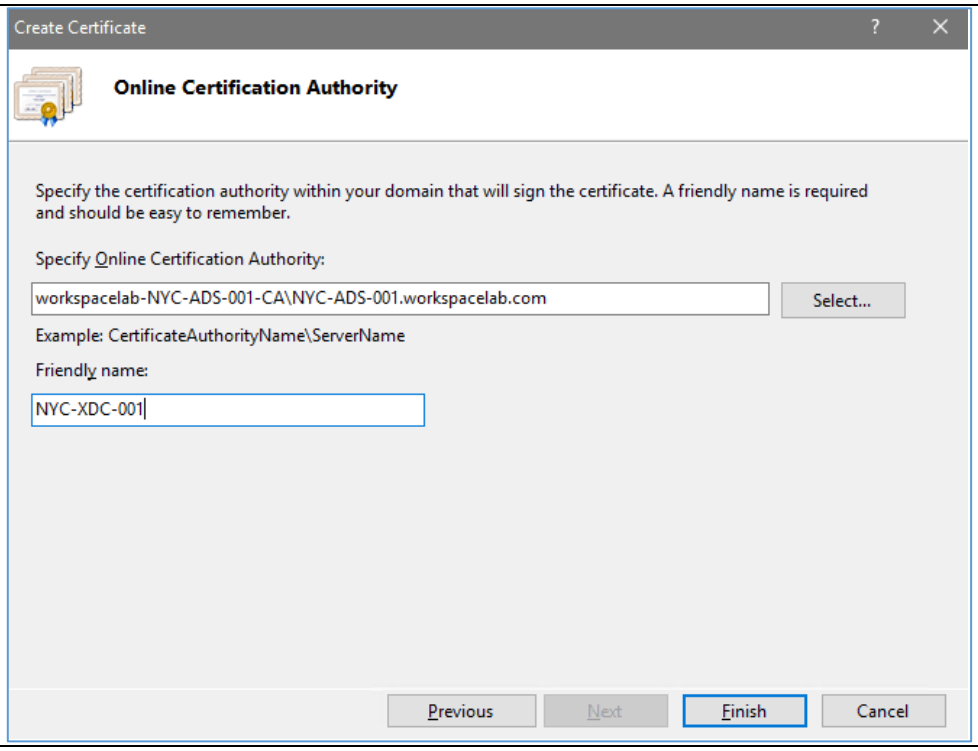
6. On the Online Certificate Authority page, click **Select** to the right of Specify Online Certification Authority.

7. On the Select Certification Authority select **workspacelab-NYC-ADS-001-CA** and click **OK**.

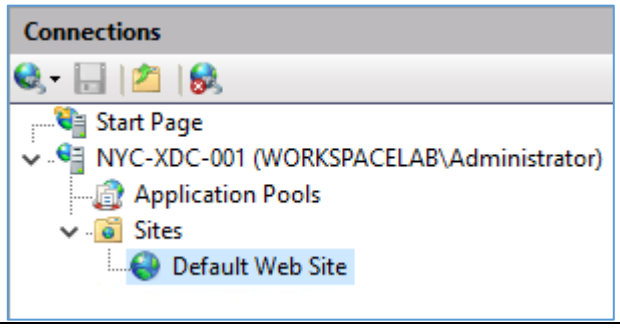


8. On the Friendly name field, type **NYC-XDC-001**.

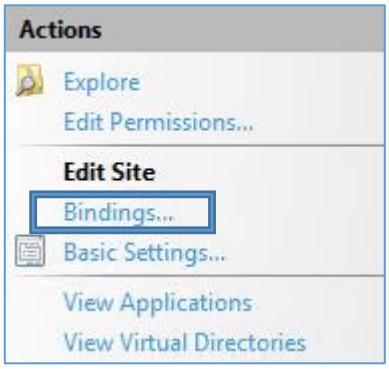
   Click **Finish** to create this Domain Certificate.



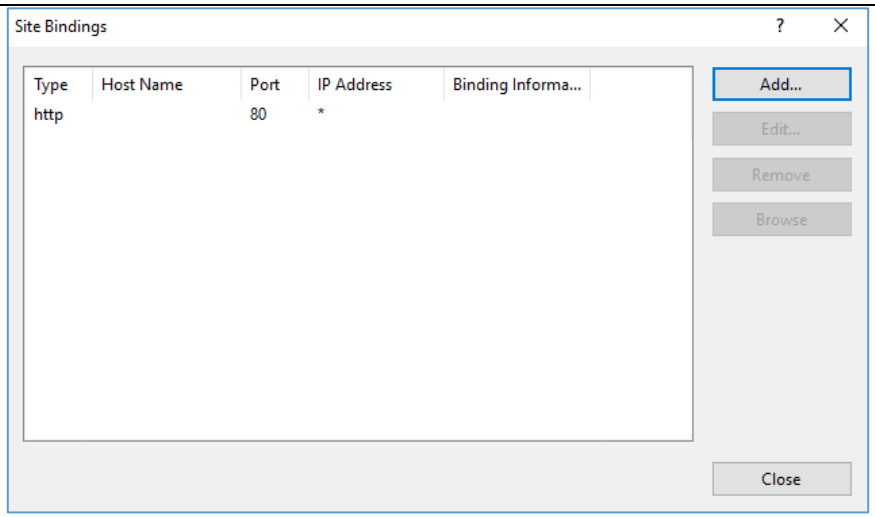
9. In IIS Manager expand **NYC-XDC-001 (WORKSPACELAB\administrator)** > **Sites** and click on **Default Web Site**.



10. On the right pane under Actions, click **Bindings**.



On the Site Bindings dialog box, click **Add**.

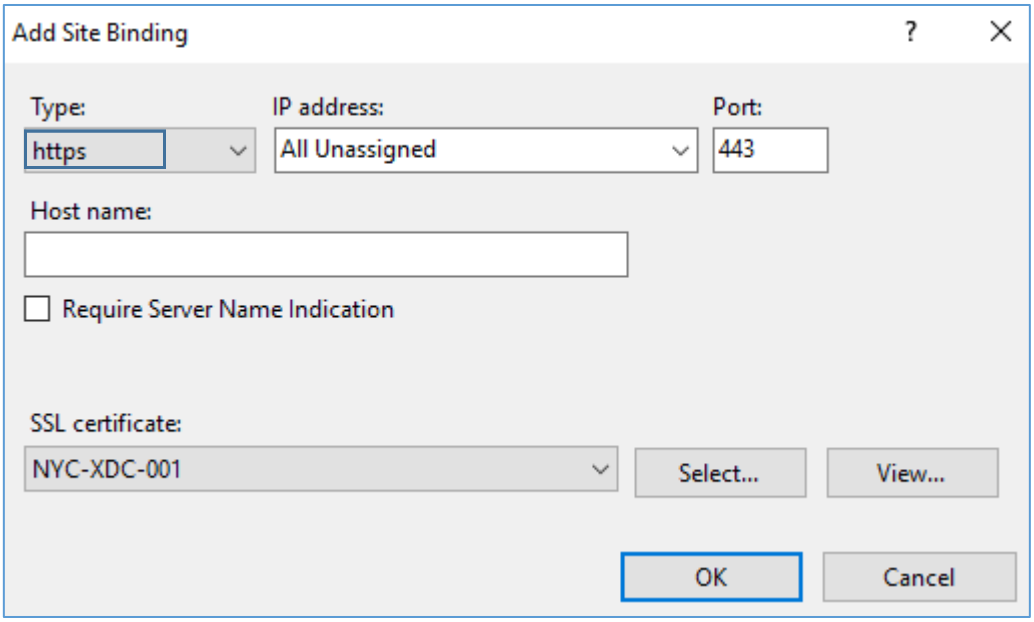


11. Change the Type field to be **https**.

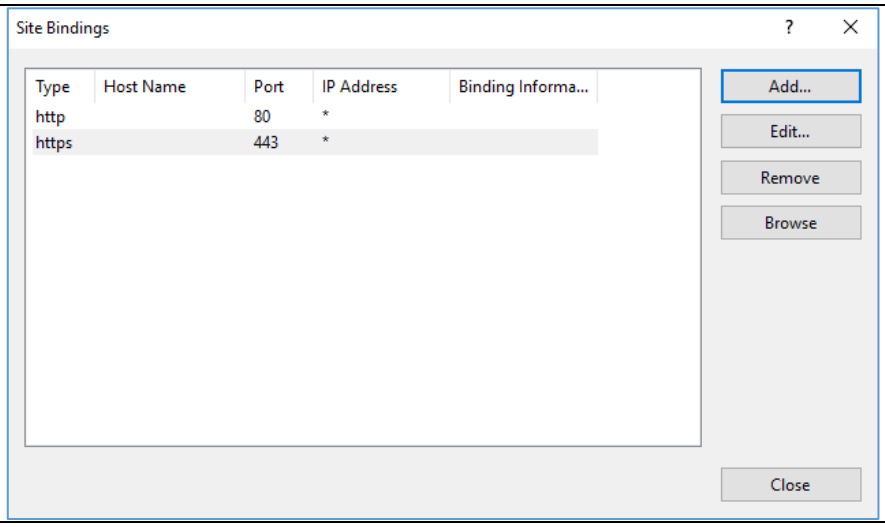
On the SSL certificate drop-down list, select **NYC-XDC-001**.

Click **View** and notice this is the certificate created at the beginning of this exercise.

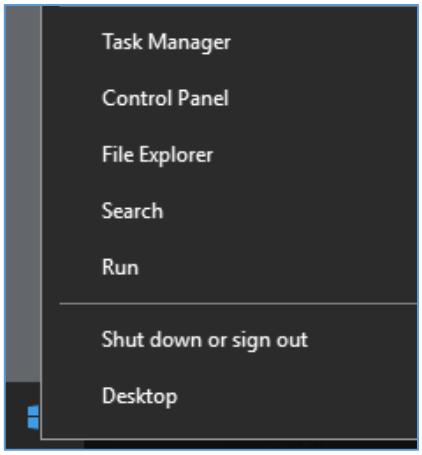
Click **OK** to close the Add Site Bindings window.



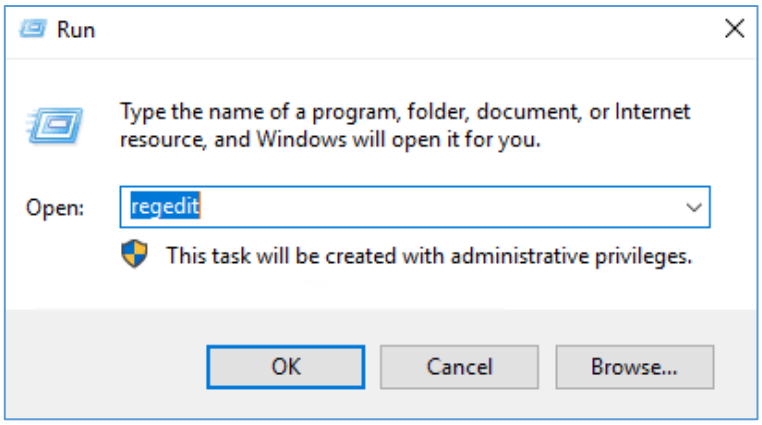
12. On the Site Bindings dialog box, click **Close**.



13. Open the Registry Editor by right-clicking **Start** and selecting **Run**.

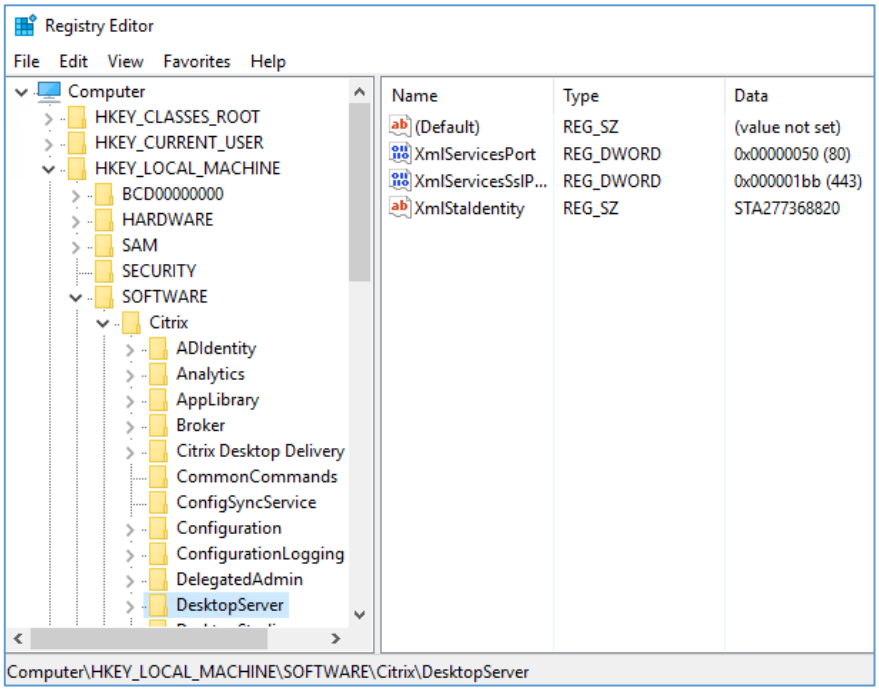


Type **regedit** and click **OK**.



Note: The command to open the Registry Editor is not case-sensitive. Typing Regedit or regedit will result in the same window opening up.

14. Browse to **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer**.

	Verify that the **XmlServicesSslPort** registry key exists with the correct value for SSL port. By default, it is set to **443**.  **Note**: The XML Service is a used as a data protocol running on the TCP/IP+HTTP transport protocol, which uses port 80 by default.
15.	**Close** the Registry Editor window. **Close** Internet Information Services (IIS) Manager.

Key Takeaways:

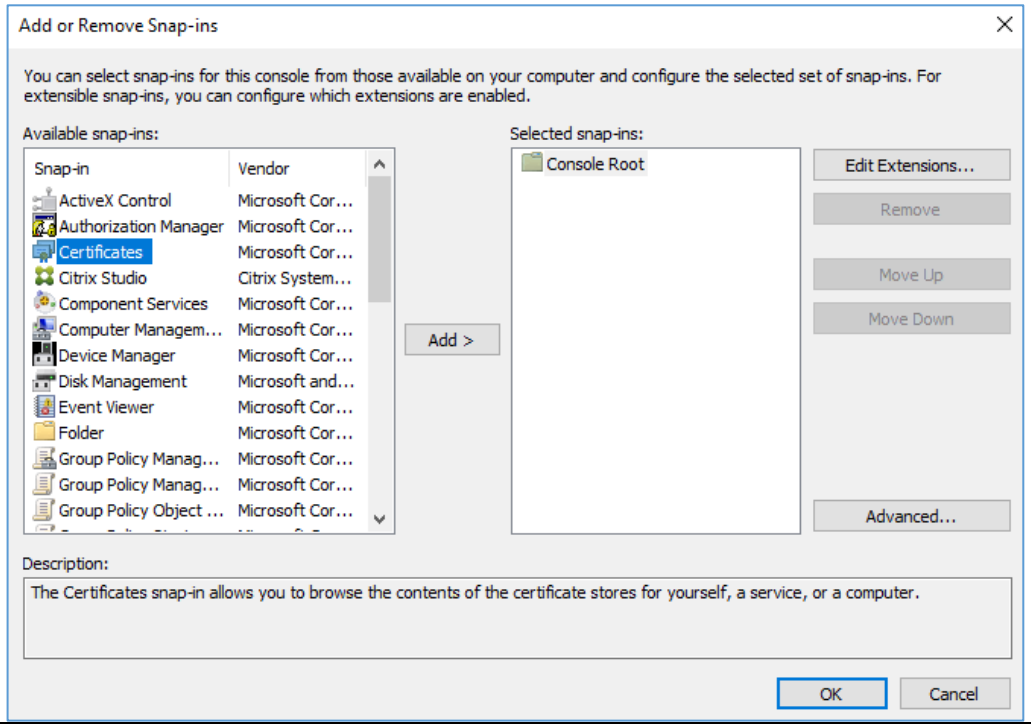
- Be sure to always import the PFX server certificates under the Delivery Controller Local Computer certificate store, and not the My user account.
- Securing XML traffic prevents attackers from cracking obfuscation and getting passwords, stealing resource set information and tickets, impersonating controller and intercepting authentication requests.
- A certificate is required to secure the XML port on the controller.
- For added security, the unsecured XML port should be disabled.

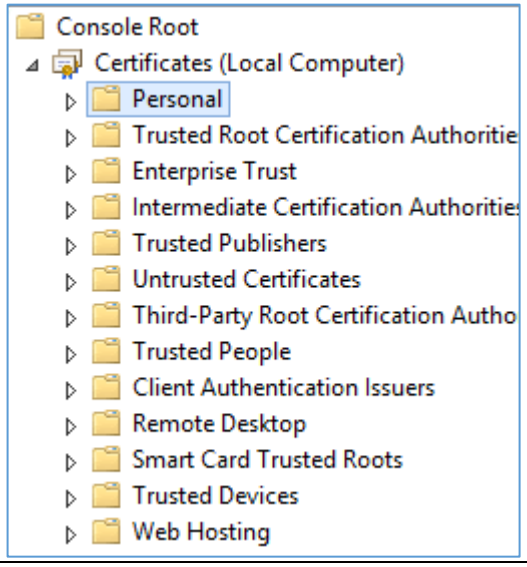
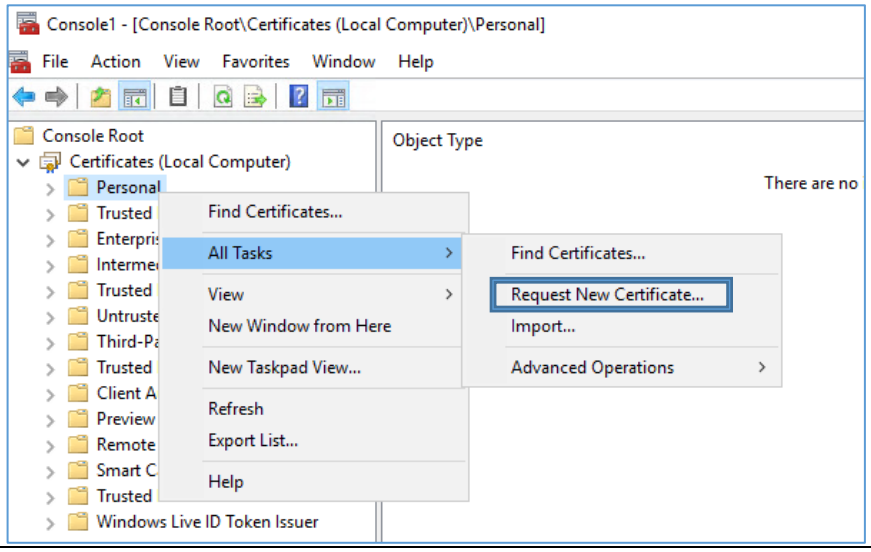
Exercise 12-2: Secure XML Traffic on NYC-XDC-002

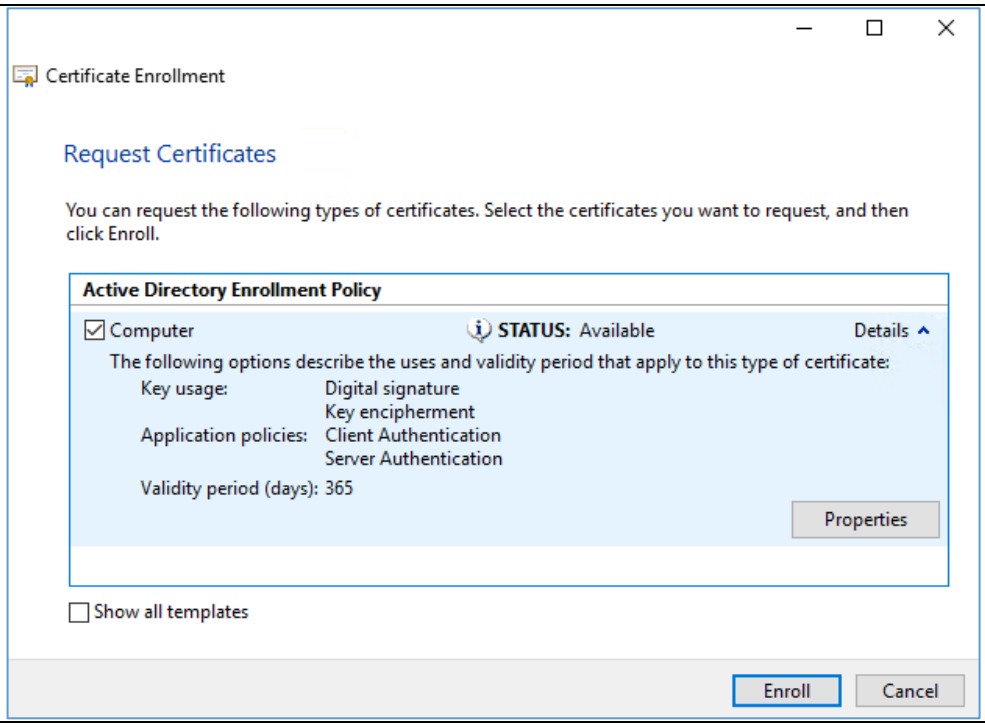
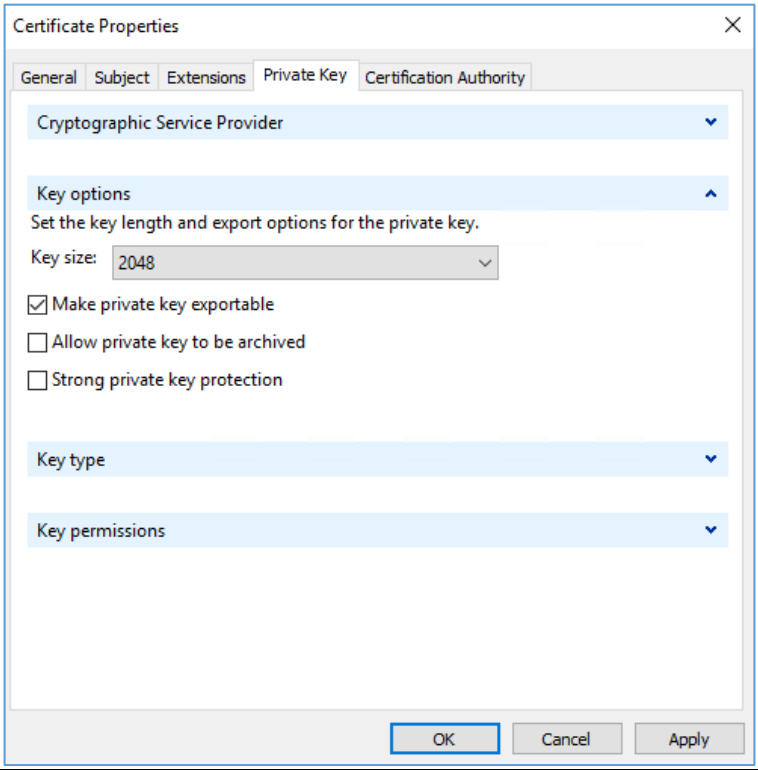
Scenario:

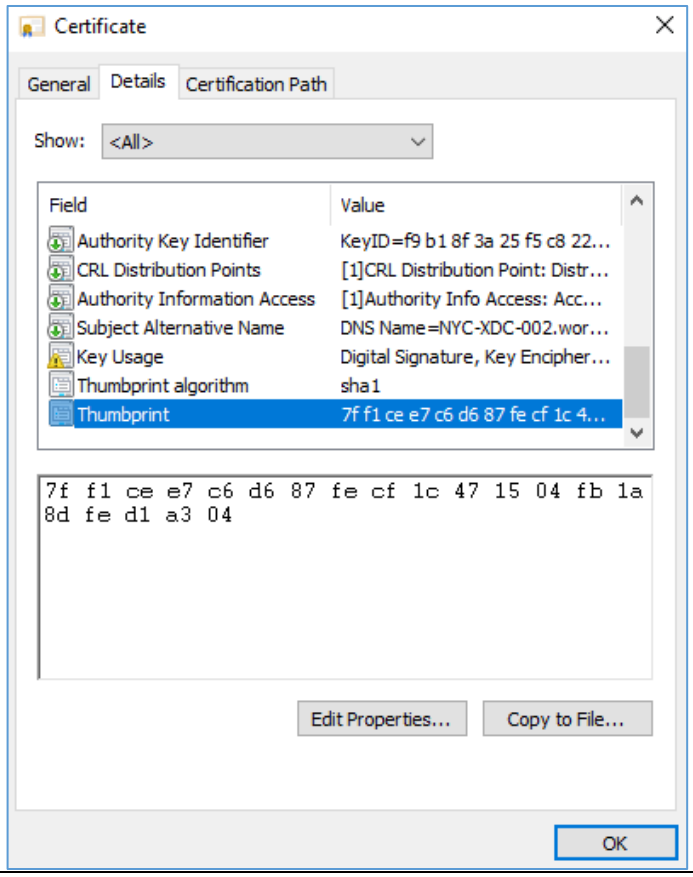
Your task is to secure XML traffic on the Second Delivery Controller, NYC-XDC-002.

Note: This exercise content is nearly identical to the steps in Exercise 12-1, the differences are that Exercise 12-2 is run against NYC-XDC-002 and that the steps in 12-2 are more advanced, because NYC-XDC-002 is setting up the scenario of not having IIS installed. These steps mainly target those who are in restrictive environments where IIS cannot be loaded on the Delivery Controllers. If these steps do not match your experience, or you do not wish to proceed through more advanced concepts, then return to Exercise 12-1 and re-run all of those steps only this time for NYC-XDC-002.

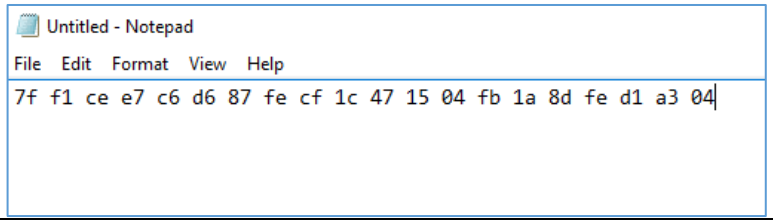
Step	Action
1.	Using the Remote Desktop Connection Manager, connect to **NYC-XDC-002**. To log on to NYC-XDC-002, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password.
2.	Right-click **Start** > click **Run** > type **MMC** and then press **Enter**.
3.	Click on **File** > **Add/Remove Snap-in**.
4.	Under Available snap-ins, click **Certificates** and click **Add**. 
5.	Select **Computer account**, click **Next**, and click **Finish**.
6.	Click **OK** on the Add or Remove Snap-ins dialog box.

7.	Expand **Certificates** and click **Personal**. 
8.	Right-click **Personal**, select **All Tasks**, and click **Request New Certificate**. 
9.	On the Certificate Enrollment Before you Begin window click **Next**.
10.	On the Certificate Enrollment Select Certificate Enrollment Policy click **Next**.
11.	On the Request Certificates window select **Computer**, click **Details** on the right, and click **Properties**.

	
12.	Click on the **Private Key** Tab, click the drop-down arrow for **Key options**, and select **Make private key exportable**. 
13.	Click **OK**, click **Enroll**, and click **Finish**.
14.	On the left pane expand **Personal** and click **Certificates**.
15.	Double-click the newly created certificate issued to **NYC-XDC-002.workspacelab.com**, click the **Details** tab and scroll down and select the **Thumbprint** field.

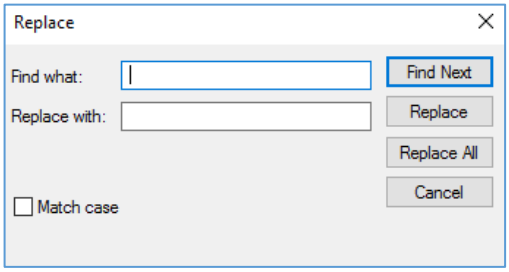


16. Highlight the Value details, copy the contents using the keyboard shortcut **CTRL + C** and paste into **Notepad** using the keyboard shortcut **CTRL + V**. The Value detail content will be used when binding the certificate to the XML service.

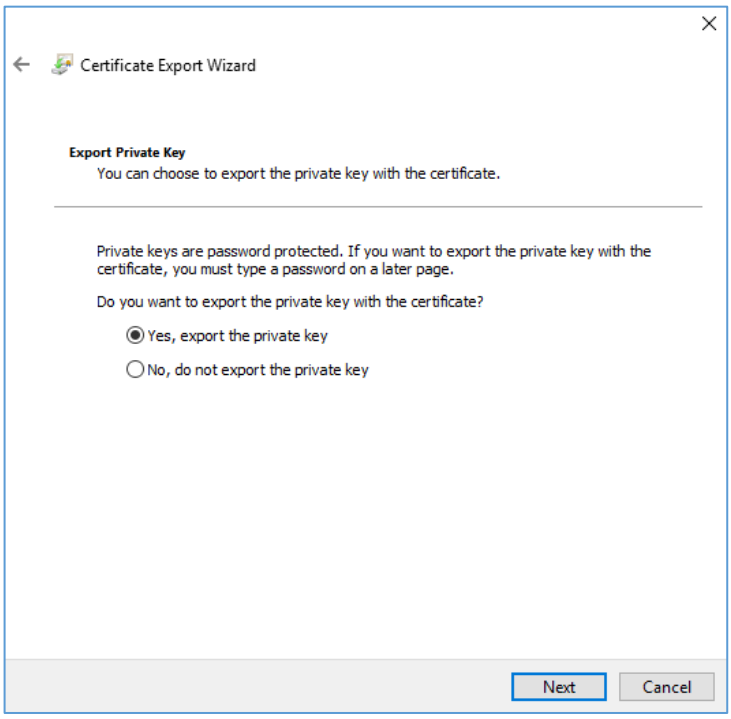
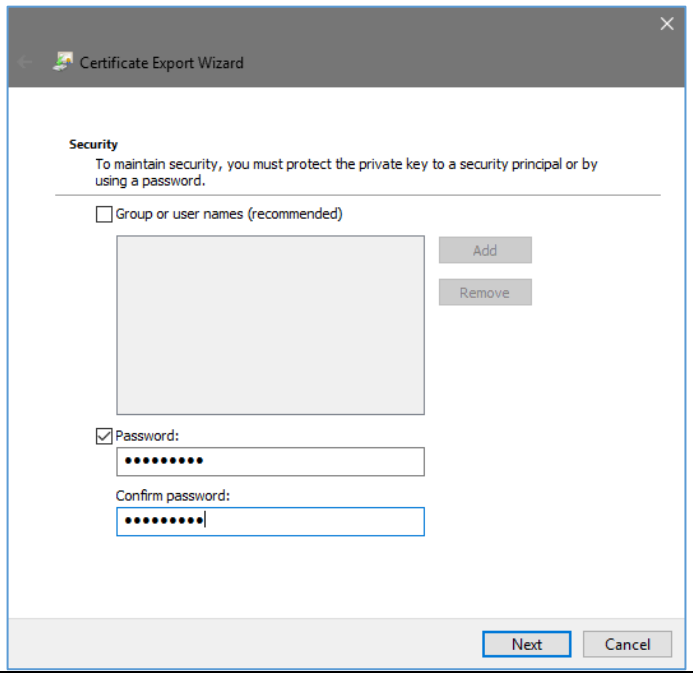


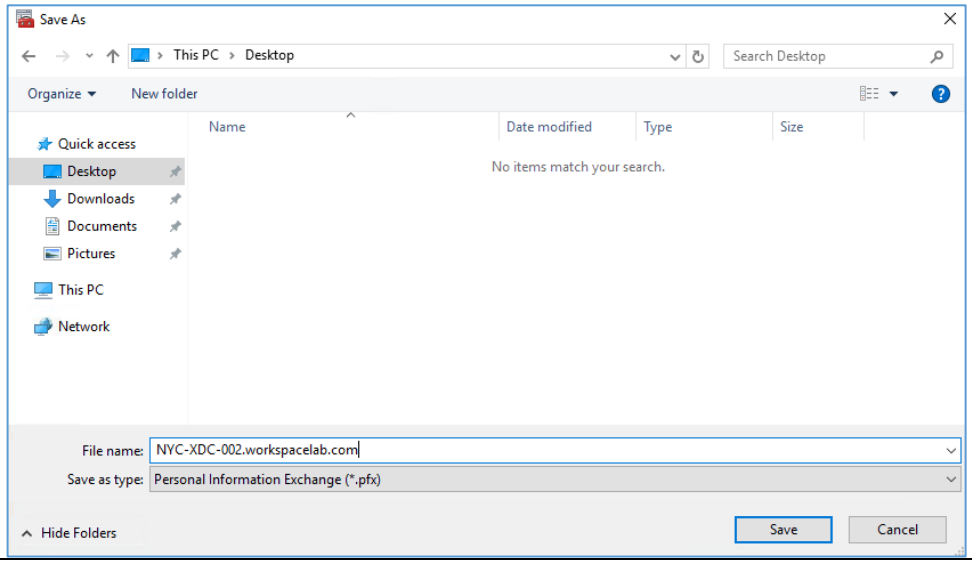
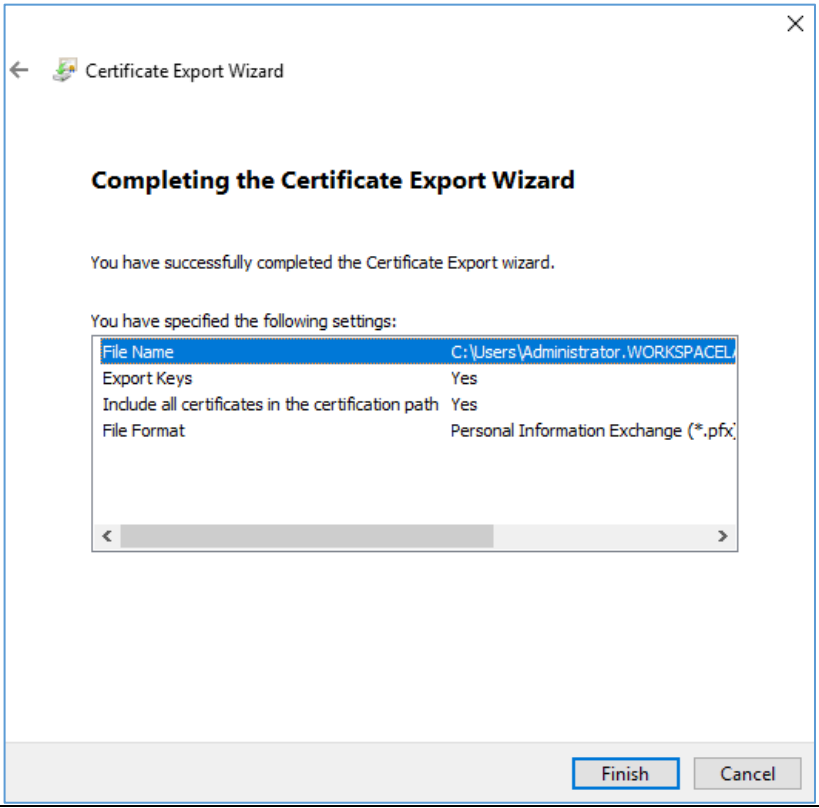
17. In Notepad click **Edit** > **Replace**.

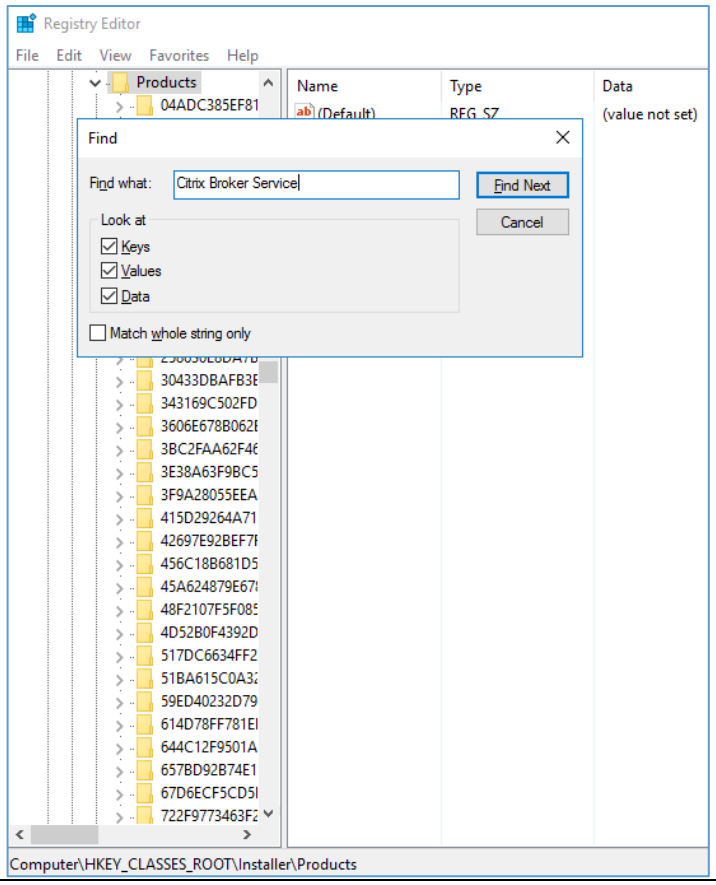
In the Find what field, left click inside the field and hit the **space bar** key on your keyboard one time.



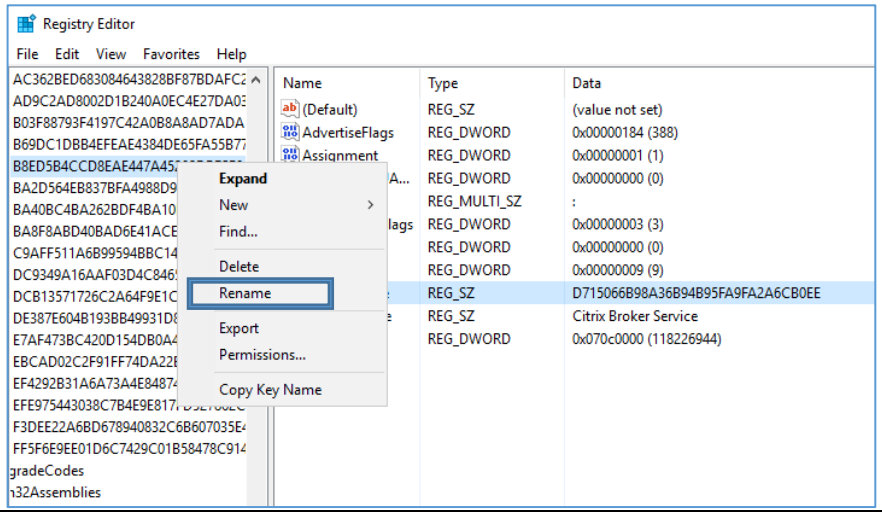
In the Replace with field, leave it blank.

	Click **Replace All** to replace all spaces with no character. Minimize **Notepad**.
18.	Click **Copy to File** on the Certificate.
19.	On the Certificate Export Wizard click **Next**.  Select the **Yes, export the private key** option and then click **Next** twice.
20.	On the Security page, select the **Password** checkbox and input **Password1** for both fields. Click **Next**. 

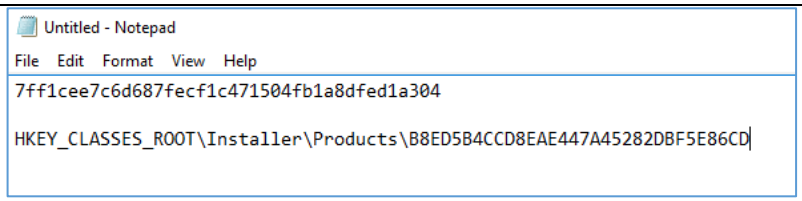
21.	On the File to Export click **Browse** next to File name. Click the **Desktop** location and in the File name field type **NYC-XDC-002.workspacelab.com**. Click **Save**. 
22.	Click **Next**. Click **Finish** and click **OK**. The certificate is now available on the Delivery Controller for binding in a future step. 
23.	Click **OK** to close the Certificate properties dialog box.
24.	Click **Start**, type **Regedit** and press **Enter**. Click the **HKEY_CLASSES_ROOT\Installer\Products** key and press **CTRL+F**. In the Find what field, enter **Citrix Broker Service** and click **Find Next**.



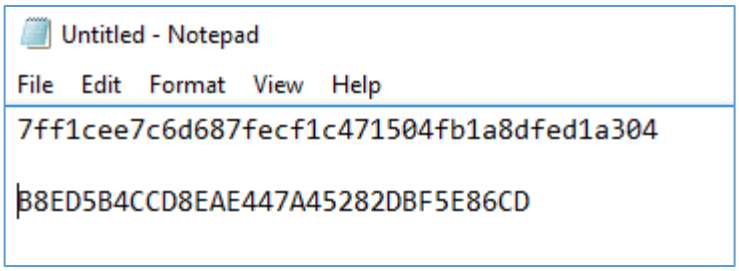
25. Right-click the key that contains **Citrix Broker Service** and click **Rename**. **Copy** the alphanumeric string.



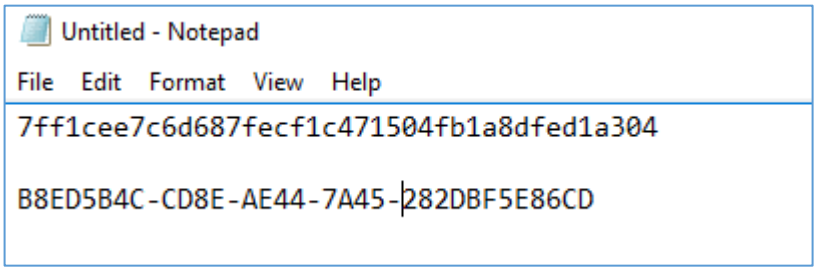
26. Open **Notepad** and **paste** the copied alphanumeric string.



27. If needed, Clear **HKEY_CLASSES_ROOT\INSTALLER\PRODUCTS**



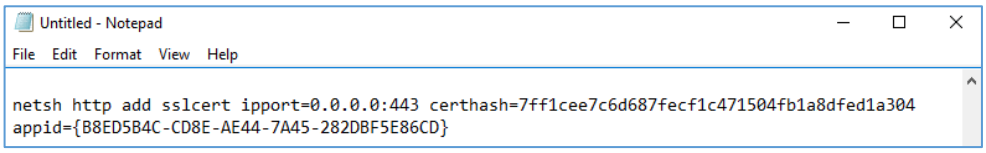
Add dashes after the 8th, 12th, 16th, and 20th characters so that the string is in the format: **B8ED5B4C-CD8E-AE44-7A45-282DBF5E86CD**



Note: B8ED5B4C-CD8E-AE44-7A45-282DBF5E86CD is just an example string and the actual string will be different in each environment.

28. In Notepad, copy the following command, replacing the values indicated with the certificate hash and the Citrix Broker Service GUID, which were obtained in Steps 17 and 27, respectively:

netsh http add sslcert ipport=0.0.0.0:443 certhash=PASTE_CERTIFICATE_HASH_FROM_STEP_17 appid={PASTE_BROKER_SERVICE_GUID_FROM_STEP_27}

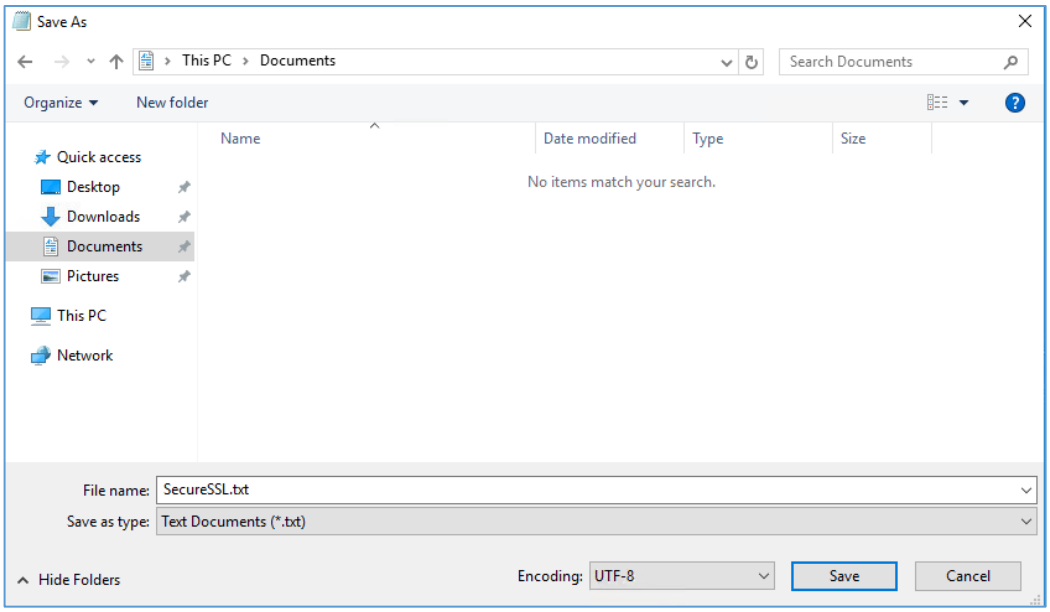


Note: Make sure the appid= field contains {} in between.

Example: netsh http add sslcert ipport=0.0.0.0:443 certhash=4dfadf447c0e401e82ff46d8092260e3ad8c6d30 appid={65763A9A-C9AA-AFE4-7A7D-CE4A8C3FCCE2}

29. Make sure to have a blank Notepad open containing only the command from Step 28.

Click **File** > **Save**. Expand **This PC**, click **Documents,** and type **SecureSSL.txt** as the File name.

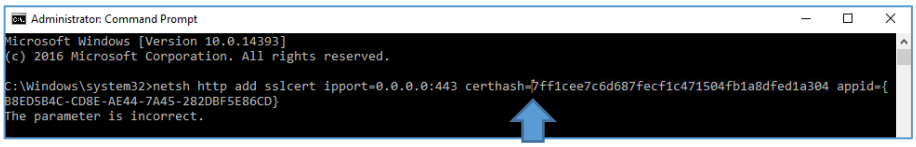


Click the Encoding drop-down list and select **UTF-8**. Click **Save**.

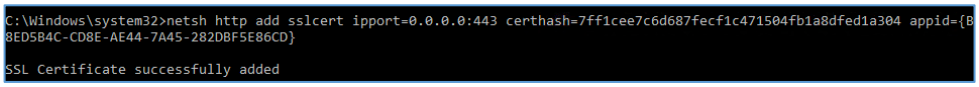
30. Right-click **Start** and click **Command Prompt (Admin)**.

Copy the command from **Notepad** and paste it in the **Administrator: command prompt** window.

Delete any **special characters** that appear in the pasted command and press **Enter**.



The command should return a message indicating that the SSL Certificate successfully added.



Note: The certificate has been successfully bound to port 443 on the Delivery Controller. In a future exercise, we will make sure to enable secure XML traffic by configuring StoreFront to use https.

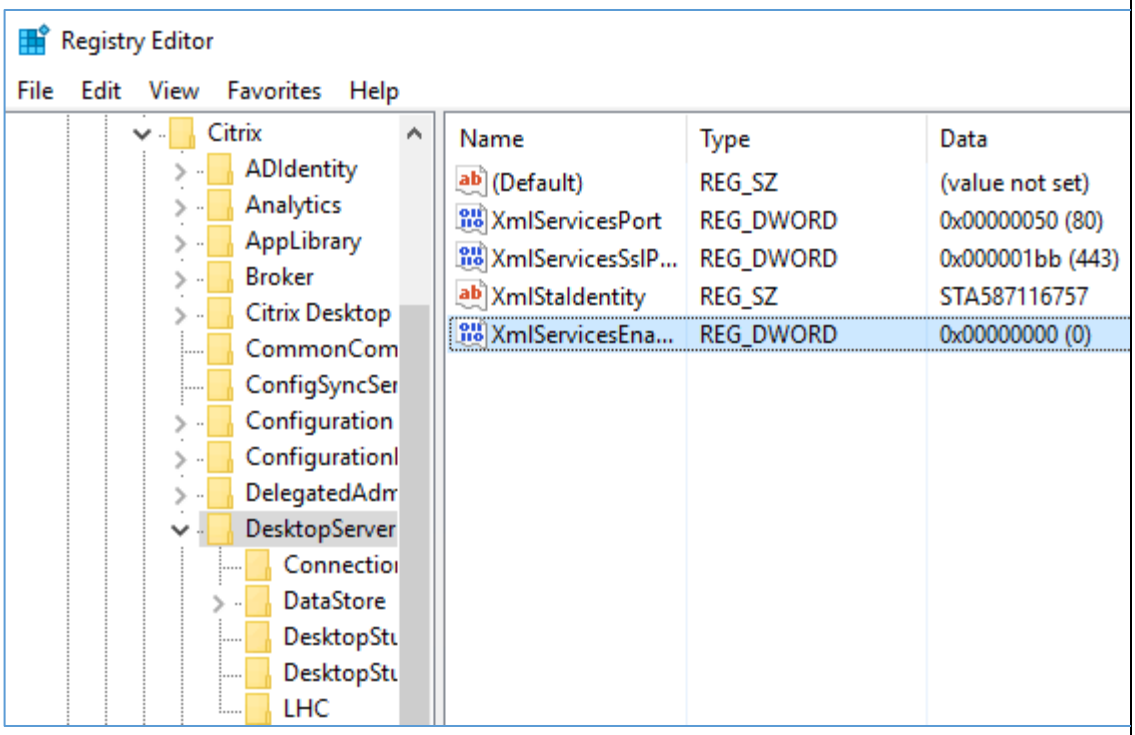
31. Now that NYC-XDC-002 has the XML service configured on HTTPS, you have been tasked to disable the non-SSL listener, so that the non-SSL port cannot be used; the XML Service will ignore HTTP traffic on the default port.

Click **Start**, type **Regedit**, and press **Enter**.

Browse to **HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer**

Right-click **DesktopServer** and select **New > DWORD (32-bit) Value**.

- Name: **XmlServicesEnableNonSsl**
- Value Data: **0**



Reboot **NYC-XDC-002**.

Key Takeaways:

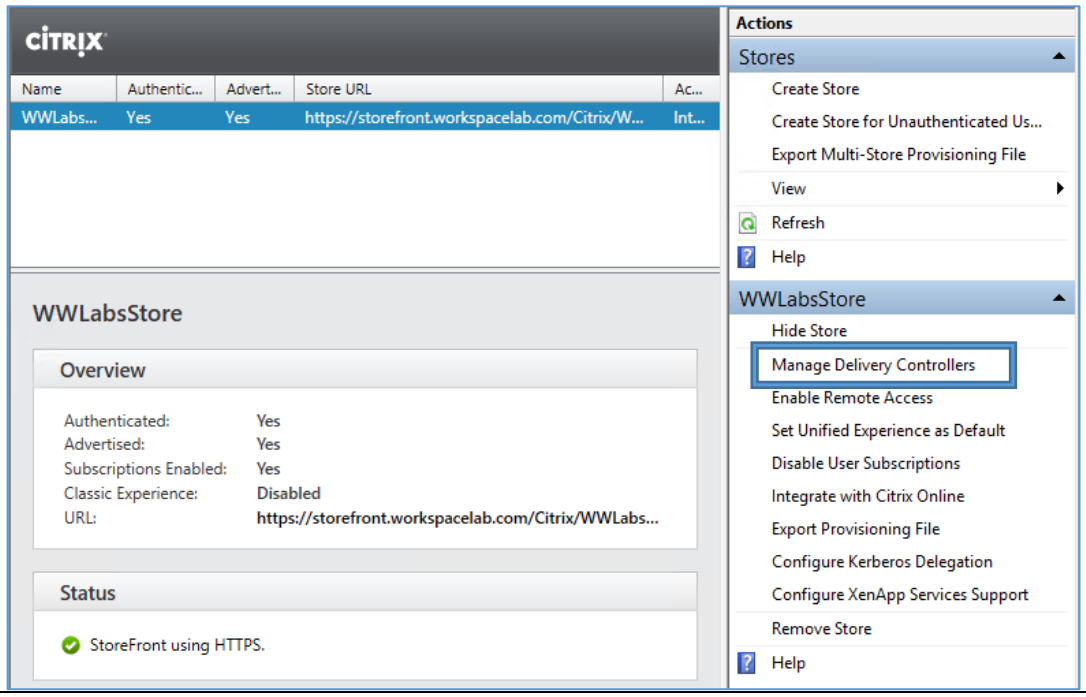
- After the Server Certificate is installed on XenDesktop Controller, register the SSL certificate for HTTPS on the server. To accomplish this, Windows has a built-in utility called netsh; this utility allows you to bind SSL certificates to a port configuration.
- Ensure to always import the PFX server certificates under the Delivery Controller Local Computer certificate store, and not My user account.
- Securing XML traffic prevents attackers from cracking obfuscation and getting passwords, stealing resource set information and tickets, impersonating controller and intercepting authentication requests.
- A certificate is required to secure the XML port on the controller.
- For added security, the unsecured XML port should be disabled.

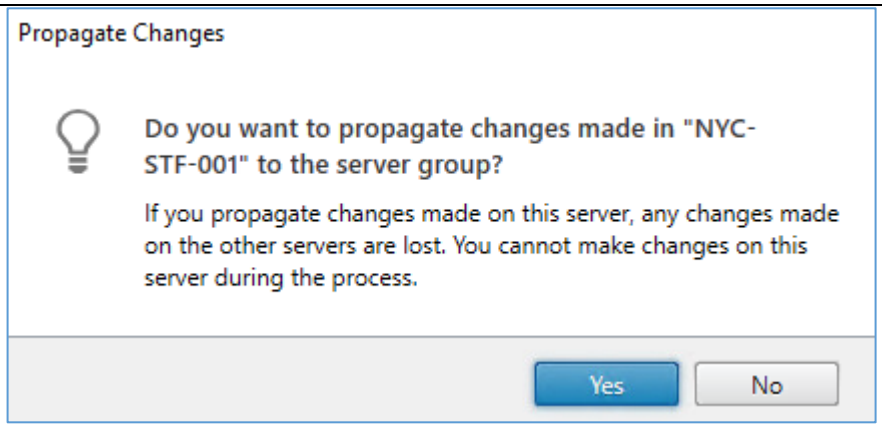
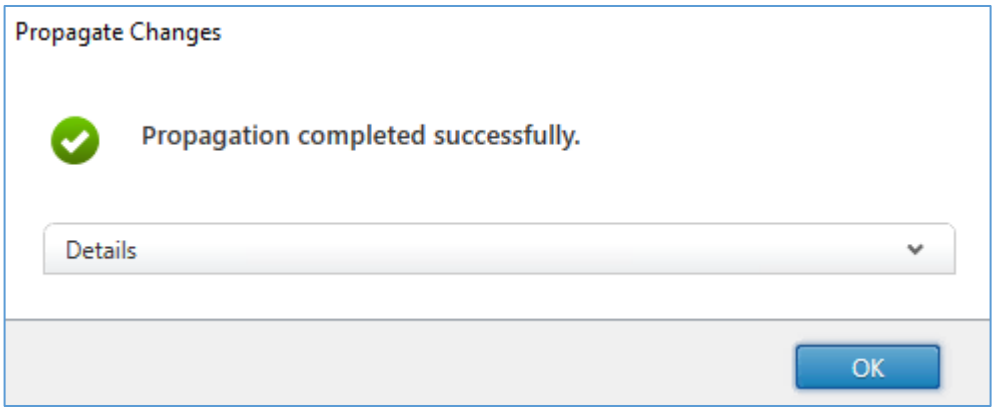
Exercise 12-3: Configure the Store to Use Secure XML Connections

Scenario:

After binding the certificates to the Delivery Controllers, your task is to configure the Store to use the secure XML connections.

Step	Action
1.	Using the Remote Desktop Connection Manager, confirm you are still connected to **NYC-STF-001**. **Note:** In a previous exercise, you had logged on to **NYC-STF-001** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password.

	Note: If your Remote Desktop Connection session disconnected, log on to **NYC-STF-001**, right-click this machine and choose **Connect server**.
2.	Using the StoreFront Management Console, in the left pane click **Stores**. Ensure the **WWLabsStore** store is selected. **Note**: If StoreFront was closed in a previous exercise, then click **Start** > **Citrix** > **Citrix StoreFront**.
3.	Click **Manage Delivery Controllers** from the Actions pane. 
4.	On the Manage Delivery Controllers dialog box, click **Edit**.
5.	On the **Edit Delivery Controller** window, ensure that both Delivery Controllers are listed using the Full Qualified Domain Name. Change Transport Type to **HTTPS** Ensure Port is **443** Click **OK**.
6.	On the **Manage Delivery Controllers** window, click **OK**.
7.	Using the StoreFront Management Console, in the left pane click **Server Group**. Click **Propagate Changes** from the Actions pane. On the Propagate Changes dialog box, click **Yes**.

	 **Note**: Propagating changes should be done every time a change has been made to the StoreFront configuration; this ensures that all StoreFront Servers have the most recent configuration set. Failing to do this might cause user interruptions or an inconsistent user experience.
8.	While the changes are propagating, click the drop-down list to view the details. Once the propagation has completed, click **OK** to close the Propagate Changes dialog box. 

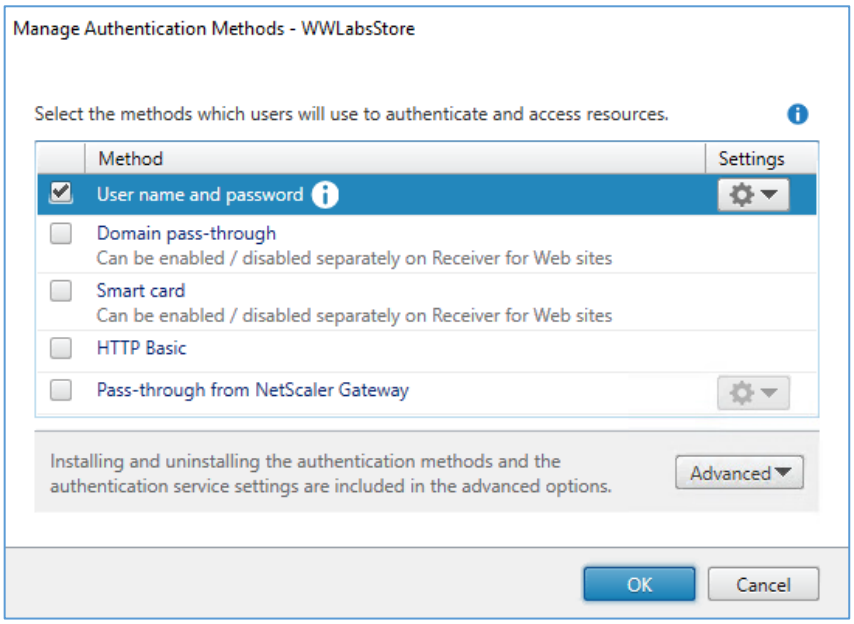
Key Takeaways:

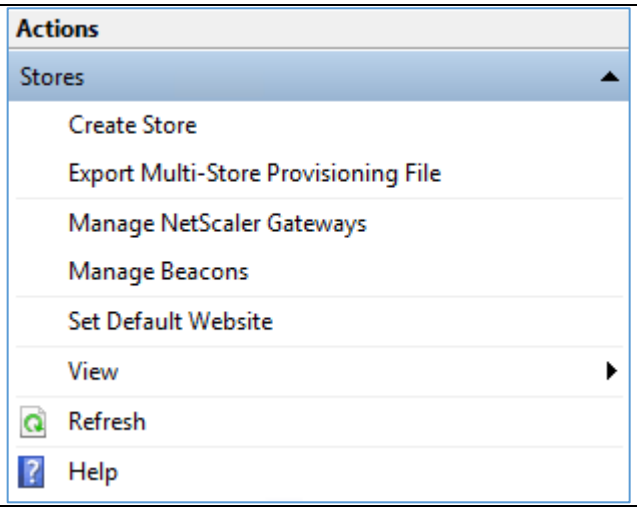
- Even though certificates are deployed on the Delivery Controllers, StoreFront has to be configured to use the secured connection; this is done by selecting HTTPS. The port can be any port that you chose, but it must match the port that you bound the certificate on the Delivery Controller.
- Remember to propagate changes every time you make a change to StoreFront; failing to do this task might leave users with an inconsistent user experience as they are load balanced from one StoreFront server to the next.

Exercise 12-4: Integrate StoreFront with the NetScaler Gateway

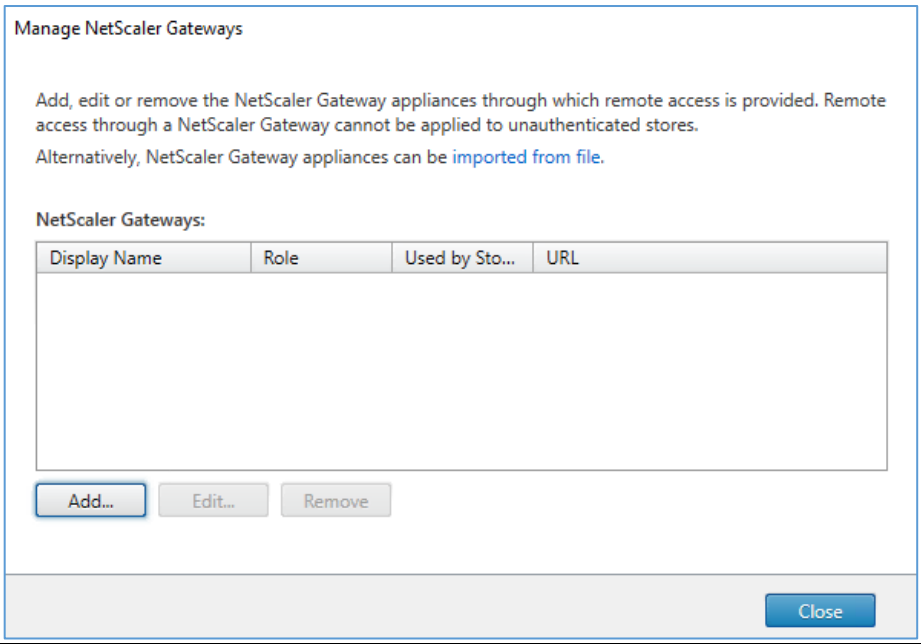
Scenario:

In a previous task, another Citrix Administrator configured the NetScaler Gateway.
Your task is to integrate StoreFront with NetScaler Gateway.

Step	Action
1.	Using the Remote Desktop Connection Manager, connect to **NYC-STF-001**. To log on to NYC-STF-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password.
2.	Using the StoreFront Management Console, configure authentication. In the left pane click **Stores.** Select **WWLabsStore** in the middle pane. In the right pane under WWLabsStore select **Manage Authentication Methods**.  Select **Pass-through from NetScaler Gateway** and click **OK**. **Note**: This enables pass-through from NetScaler Gateway authentication.
3.	Under the Actions pane on the right, click **Manage NetScaler Gateways**.

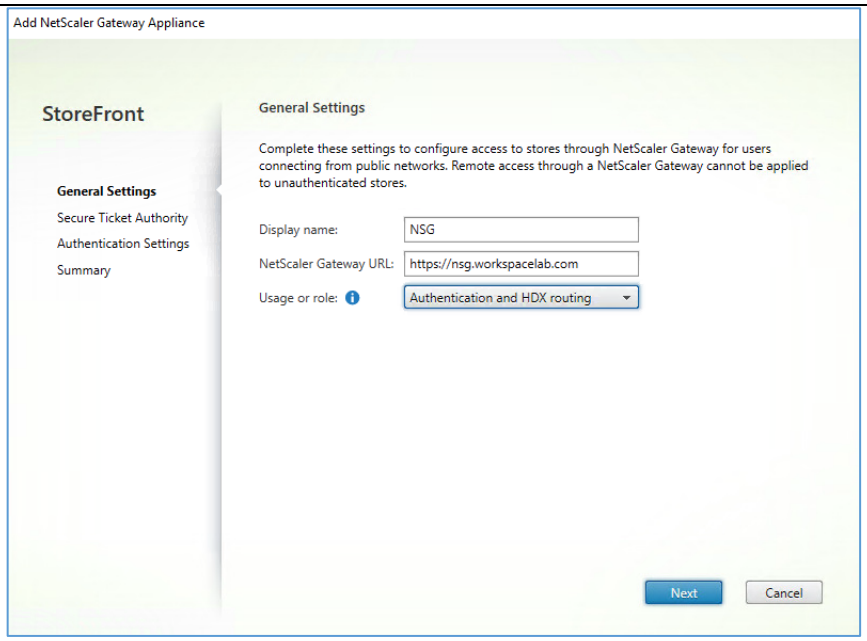


4. Click **Add**.



5. On the Add NetScaler Gateway Appliance window, configure the following settings:

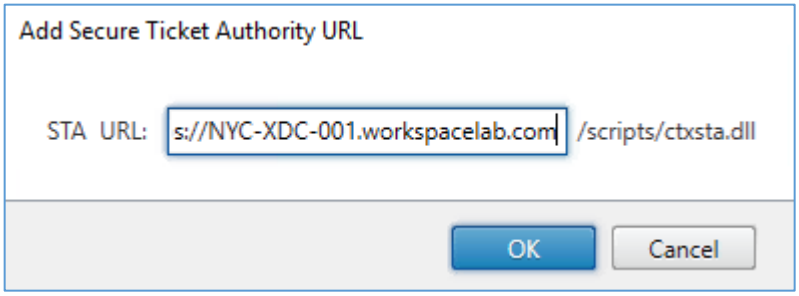
Display name: **NSG**
NetScaler Gateway URL: **https://nsg.workspacelab.com**
Usage or role: **Authentication and HDX Routing**



Click **Next**.

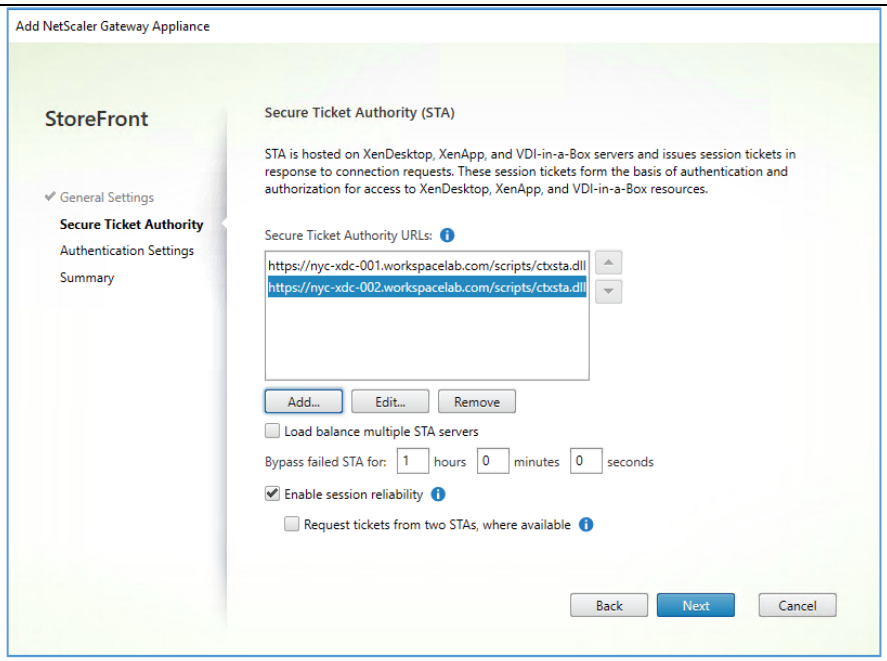
6. On the Secure Ticket Authority page, click **Add** under Secure Ticket Authority URLs.

   Type **https://NYC-XDC-001.workspacelab.com** and click **OK**.



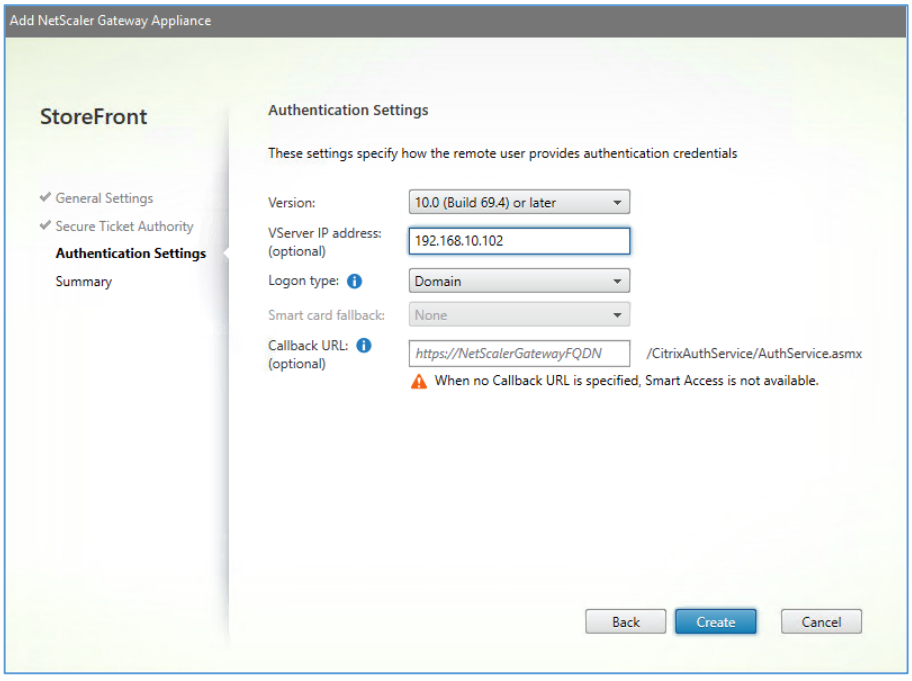
   Click **OK** and click **Add**.

   Click **Add** again, type **https://NYC-XDC-002.workspacelab.com** and click **OK**.



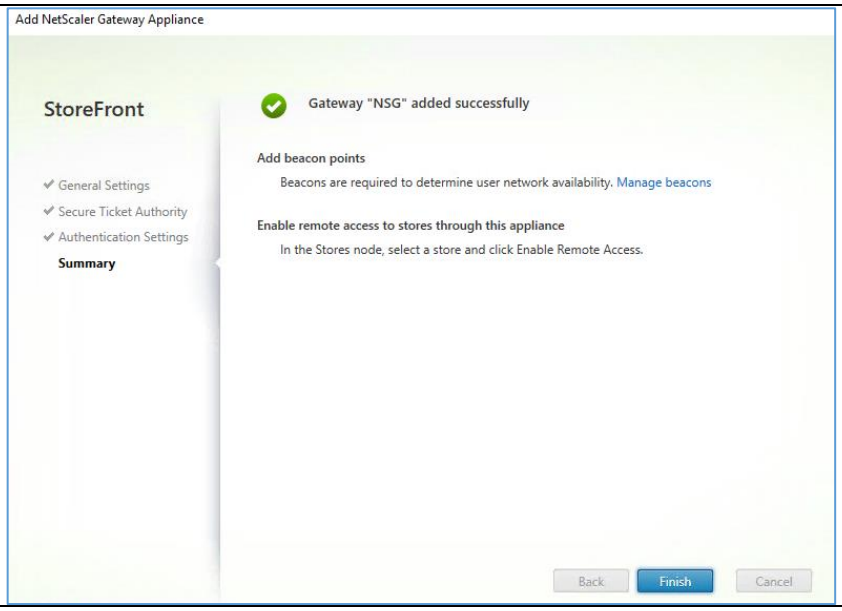
Click **Next**.

7. On the Authentication Settings page, key in the following information:
   - VServer IP address: **192.168.10.102**
   - Logon type: **Domain**



Click **Create**.

8. To finalize the Add NetScaler Gateway Appliance setting click **Finish**.

	
9.	Click **Close** on Manage NetScaler Gateways page.

Key Takeaways:

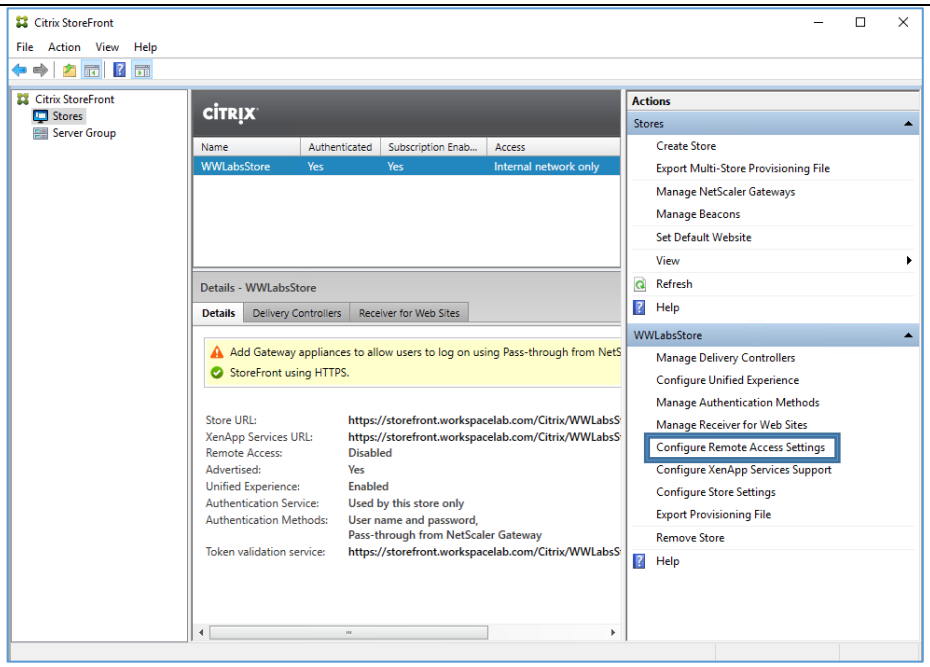
- Even though the NetScaler has been configured to connect to the StoreFront server, the StoreFront server needs to be configured to talk to the NetScaler.
- The StoreFront server needs to be able to talk to the NetScaler on the callback URL. One way to test this would be to open a browser on the StoreFront Server and access the callback URL. Make sure no certificate errors are present.
- The Controllers are used as the Secure Ticket Authorities. The function of the Secure Ticket Authorities is to allow a ticket exchange between the NetScaler and the server that will launch the application. This ticket exchange encrypts the IP address of the server that will launch the application or desktop.

Exercise 12-5: Enable Remote Access to the Store

Scenario:

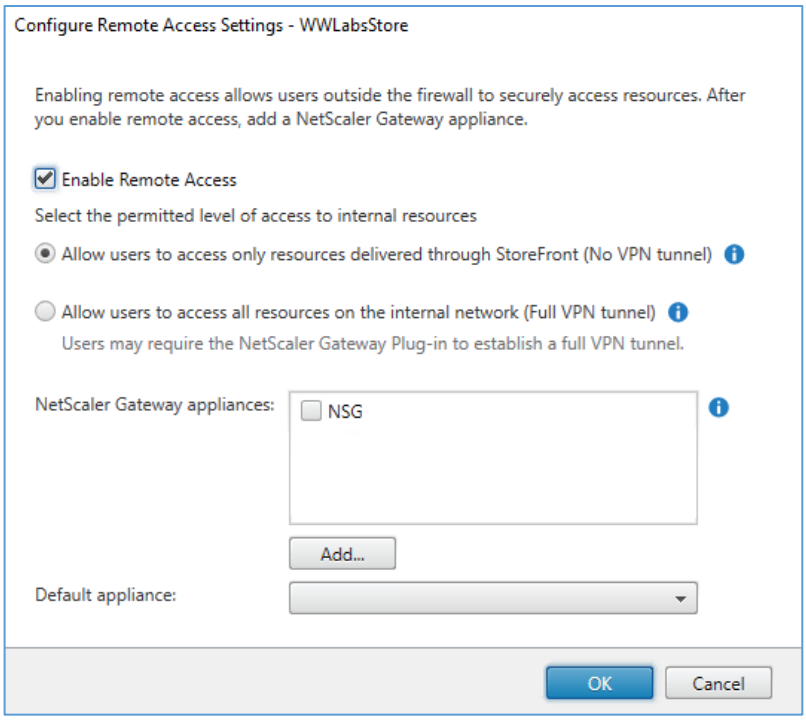
Your task is to enable remote access on the StoreFront Store.

Step	Action
1.	Using the Remote Desktop Connection Manager, confirm you are still connected to **NYC-STF-001**. **Note:** In a previous exercise, you had logged on to **NYC-STF-001** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-STF-001**, right-click this machine and choose **Connect server**.
2.	Using the StoreFront Management Console, in the left pane click **Stores**. Ensure the **WWLabsStore** store is selected.



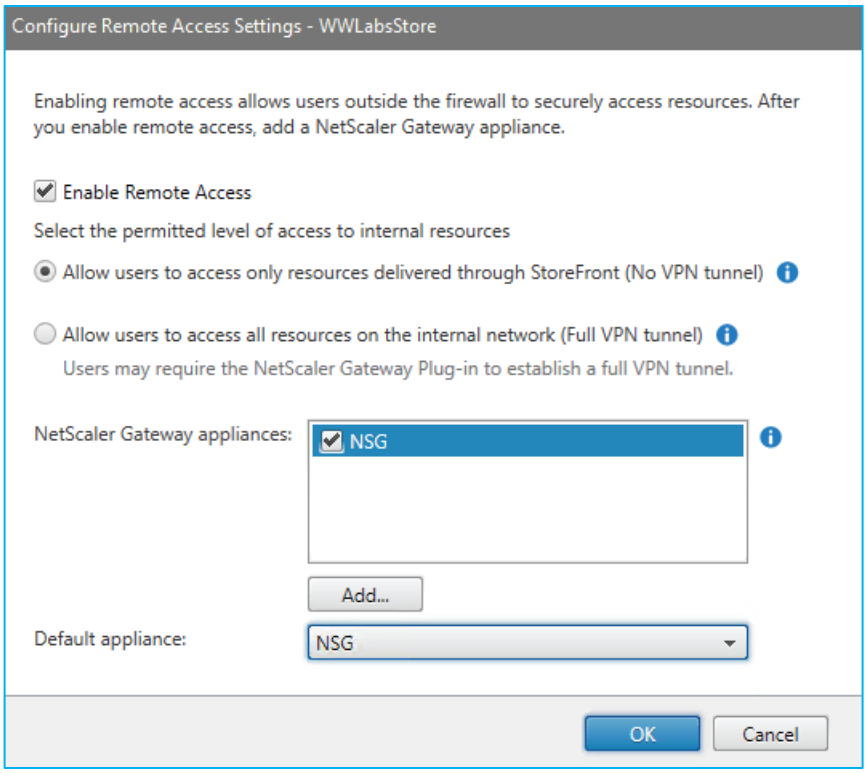
Under the WWLabsStore, select **Configure Remote Access Settings**.

3. On Configure Remote Access Settings – WWLabsStore, select the checkbox for **Enable Remote Access**.



Verify the **Allow users to access only resources delivered through StoreFront (No VPN tunnel)** radio button.

Check **NSG** in **NetScaler Gateway appliance** and make sure **NSG** is defined in the **Default appliance** drop-down list.

	 Click **OK**.

Key Takeaways:

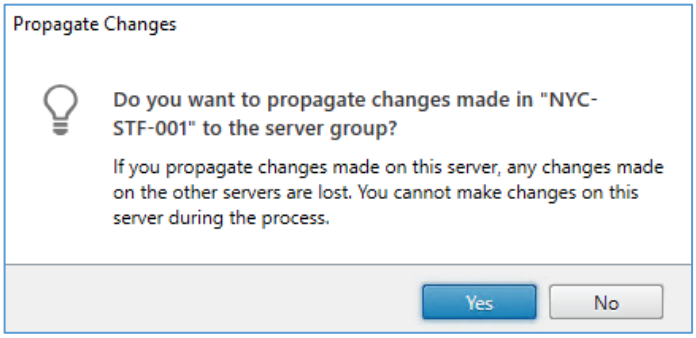
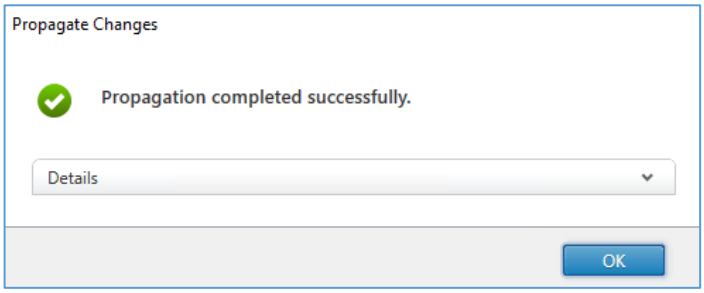
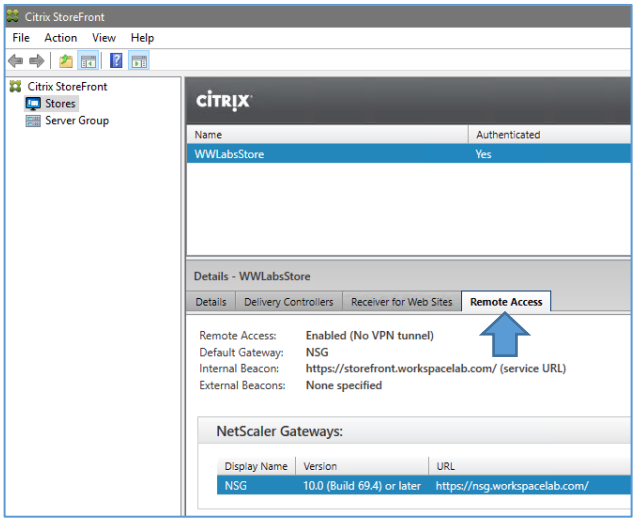
- Even though the StoreFront server is configured to talk to the NetScaler, it is still required to configure the StoreFront Store to use the newly added NetScaler Gateway configuration.
- Integration with NetScaler can be site specific.

Exercise 12-6: Propagate the StoreFront Settings to the Server Group

Scenario:

Your task is to propagate the StoreFront settings to the Server group.

Step	Action
1.	Using the Remote Desktop Connection Manager, confirm you are still connected to **NYC-STF-001**. **Note**: In a previous exercise, you had logged on to **NYC-STF-001** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-STF-001**, right-click this machine and choose **Connect server**.
2.	Using the StoreFront Management Console, in the left pane click **Server Group**. Click **Propagate Changes** from the Actions pane.

3.	On the Propagate Changes dialog box, click **Yes**.  While the changes are propagating, click the drop-down list to view the details. Once the changes are completed, click **OK** to close the Propagate Changes dialog box. 
4.	Using the Remote Desktop Connection Manager, switch to **NYC-STF-002**. To log on to NYC-STF-002, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password.
5.	Using the StoreFront Management Console, in the left pane click **Stores** and in the middle pane select **WWLabsStore**. Click **Remote Access** in the lower middle pane.  Verify pass-through from NetScaler Gateway is **enabled**.

	Verify **NSG** is set as the NetScaler Gateway appliance. **Note**: If you do not see the Pass-through from NetScaler Gateway listed, then perform a Refresh from the Actions pane.

Key Takeaways:

- When a change is made on one StoreFront server, a propagation needs to be made in order for the changes to take effect on the second StoreFront server.
- Propagation needs to be initiated on the server that has made the change.

Exercise 12-7: Test External Access through the NetScaler Gateway

Scenario:

Your task is to test external access through NetScaler Gateway.

Step	Action
1.	Using the Remote Desktop Connection Manager, connect to **NYC-WRK-001**. To log on to NYC-WRK-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: user name: **WORKSPACELAB\HR1** with **Password1** as the password.
2.	Open **Internet Explorer** and browse to **https://nsg.workspacelab.com**. The following credentials are used to make the connection: User name: **HR1** Password. **Password1**
3.	Launch the **Notepad** application from the **APPS** tab.
4.	From the system tray right-click **Citrix Receiver** and open up **Connection Center**. Select **NYC-SRV-001** within the Connection Center as this is the session host and choose properties. Click the session, and then click **Properties**. Review your session details to make sure the connection is using **256-bit TLSv1.2** as the Encryption level.
5.	Close **Connection Center** and **Notepad**. Log out **HR1** from the website.

Key Takeaways:

- Once the NetScaler is configured with a NetScaler Gateway VIP, so the StoreFront server and NetScaler can communicate with each other, we can then test external access.

Module 13: Monitoring the XenApp and XenDesktop Site

Overview:

This module presents how to install, configure and use Citrix Director to monitor your environment.

Before you begin:

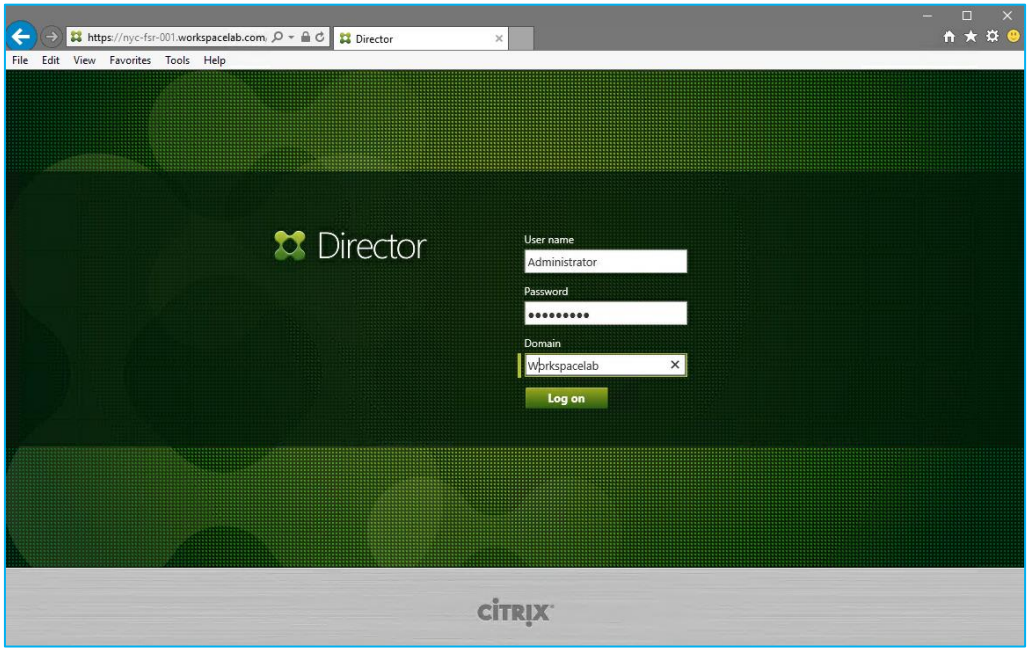
Estimated time to complete Module 13 lab exercises: 75 minutes

Exercise 13-1: Launch and Login to Citrix Director

Scenario:

Citrix Director was installed, configured and secured in a previous module. Your task is to launch and log on to Citrix Director.

Step	Action
1.	The following VMs are required before beginning the exercises for this Module; all others may be powered down. To power manage your VMs, switch to XenCenter, right-click on the VM in the left pane and select Start or Shut Down. If prompted click Yes. • NYC-ADS-001 • NYC-SQL-001 • NYC-FSR-001 • NYC-VNS-001 • NYC-NIC-001 • NYC-XDC-001 • NYC-XDC-002 • NYC-STF-001 • NYC-STF-002 • NYC-SRV-001 • NYC-WRK-001 **Note**: These above VMs are listed in the start-up order.
2.	Using the Remote Desktop Connection Manager, confirm you are still connected to **NYC-FSR-001**. **Note:** In a previous exercise, you had logged on to **NYC-FSR-001** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-FSR-001**, right-click this machine and choose **Connect server**.
3.	Click **Start** and open **Internet Explorer**. Browse to **https://nyc-fsr-001.workspacelab.com/Director/**
4.	Log on to **Citrix Director** with the following credentials: User name: **Administrator** Password: **Password1**

	Domain: **Workspacelab**  Click **Log on**. Spend a moment navigating the console. Then **Log Off** Director. Click **Administrator** > **Log Off**. **Note**: The log off is in the upper-right hand corner, using the arrow next to the name of the account logged in; in this this case, Administrator. **Note:** Following WW Labs Leading Practices, do not store your password for this site. On the dialog box at the bottom of Citrix Director, it asks *Would you like to store your password for localhos*t? Click **Not for this site.**

Key Takeaways:

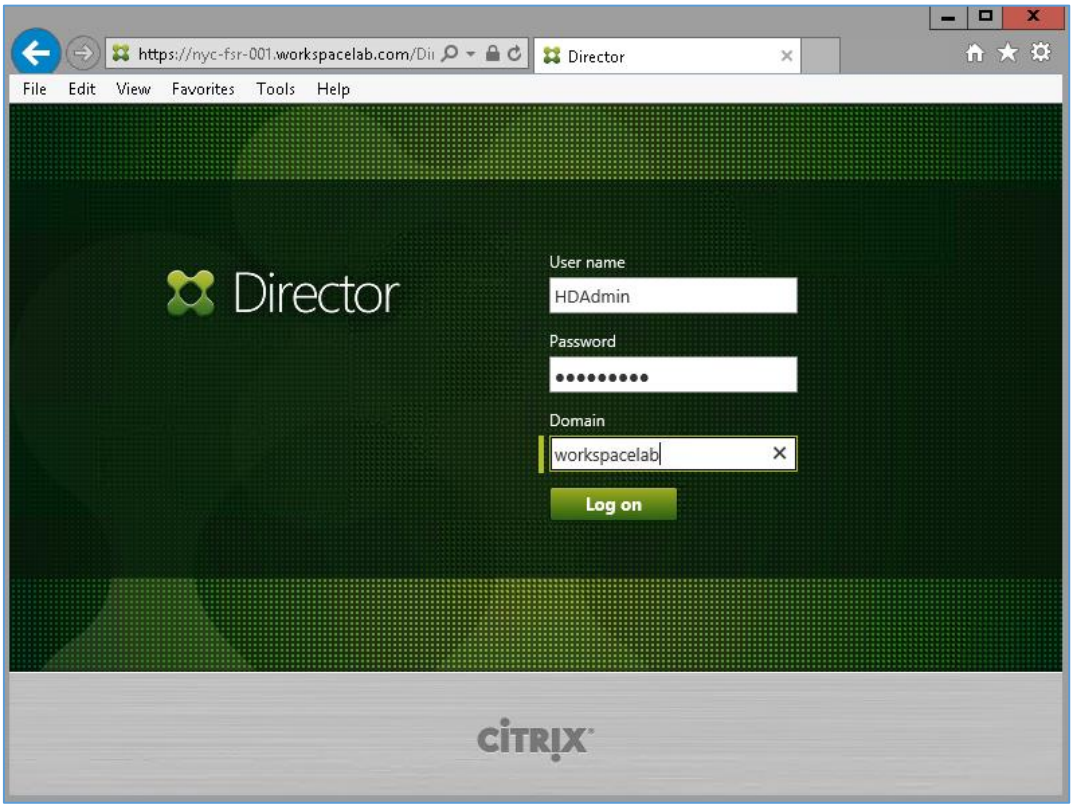
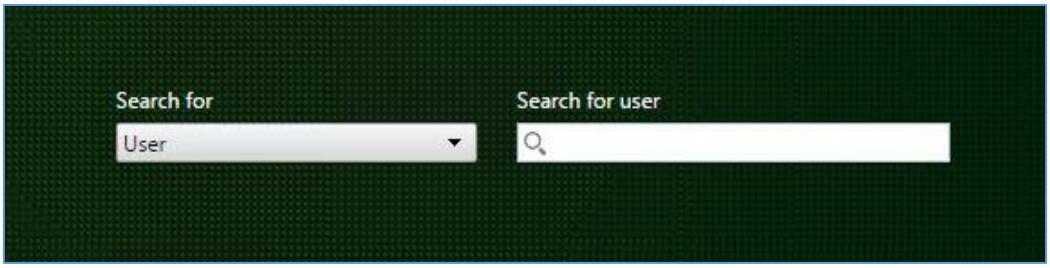
- Citrix Director is accessed from the Start Menu but it can also be accessed from a browser.

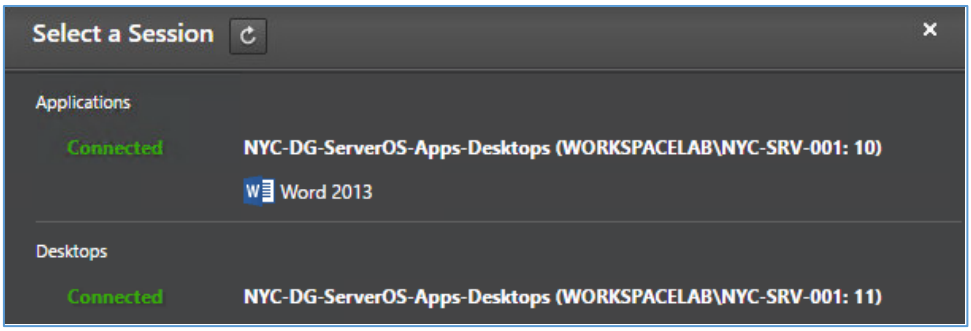
Exercise 13-2: Login to Citrix Director as a Delegated Help Desk Administrator

Scenario:

Your task to log on to Director as a Delegated Help Desk Administrator and search for a session, while taking notice of the differences in the console than from when you logged in last as a full administrator.

Step	Action
1.	Using the Remote Desktop Connection Manager, confirm you are still connected to **NYC-FSR-001**. **Note:** In a previous exercise, you had logged on to **NYC-FSR-001** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password.

	Note: If your Remote Desktop Connection session disconnected, log on to **NYC-FSR-001**, right-click this machine and choose **Connect server**.
2.	Log back in to Director using the following credentials: User name: **HDAdmin** Password: **Password1** Domain: **Workspacelab**  Click **Log on**. **Note**: Director was launched in a previous exercise. If Director was closed in a previous exercise, then click **Start** > **Internet Explorer** and browse to **https://nyc-fsr-001.workspacelab.com/Director/**.
3.	Notice that as a Help Desk delegated administrator you do not have access to the full dashboard of the Director, but rather your homepage is just the search field.  In the Search for user field type **HR1** and press **Enter**.
4.	View the session details for the user.

	 **Note:** This prompt appears only if the user has multiple sessions open. Select any active session**.** You may have different sessions open depending on your previous exercises. **Note**: If no sessions are open from previous exercises, connect to NYC-WRK-001, using the Workspacelab\HR1and Password1 credentials. Then, Launch Word 2016 and HR Desktop from the **https://storefront.workspacelab.com/Citrix/WWLabsStoreWeb/** site page. Then, Refresh the Director page tab on NYC-FSR-001.
5.	On the top right, click **HDAdmin** > **Log Off** Director.
6.	**Close** any running applications on NYC-WRK-001.

Key Takeaways:

- Delegated Help Desk Administrators account created with Citrix Studio can be used with Citrix Director to manage user sessions.

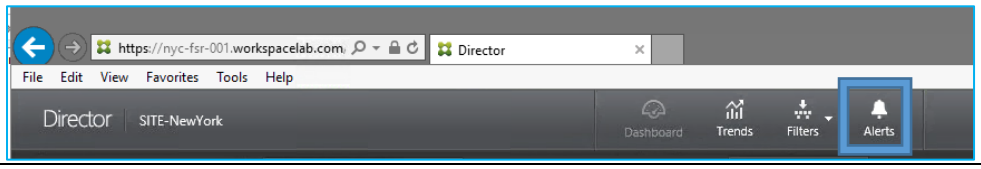
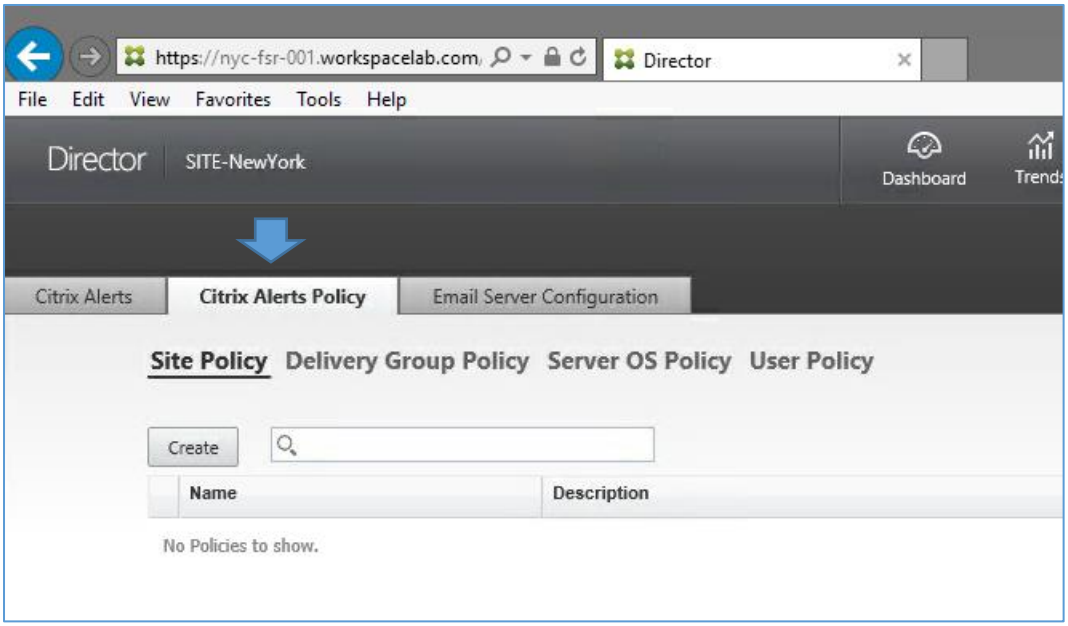
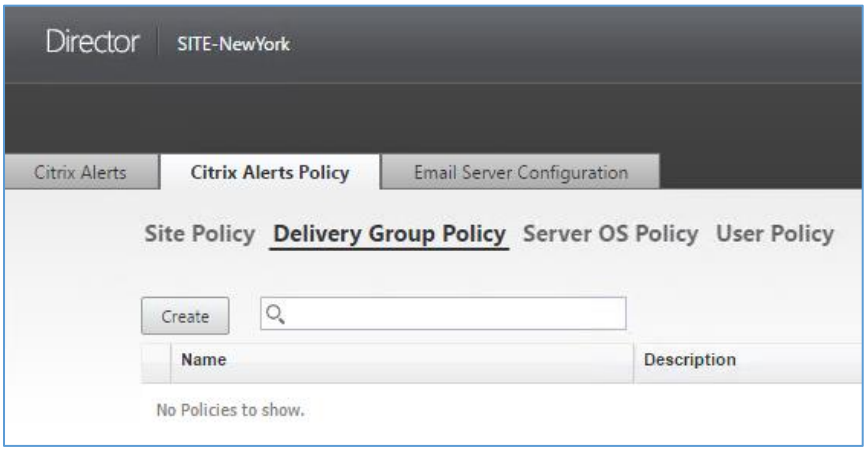
Exercise 13-3: Use Citrix Director to View Alerts

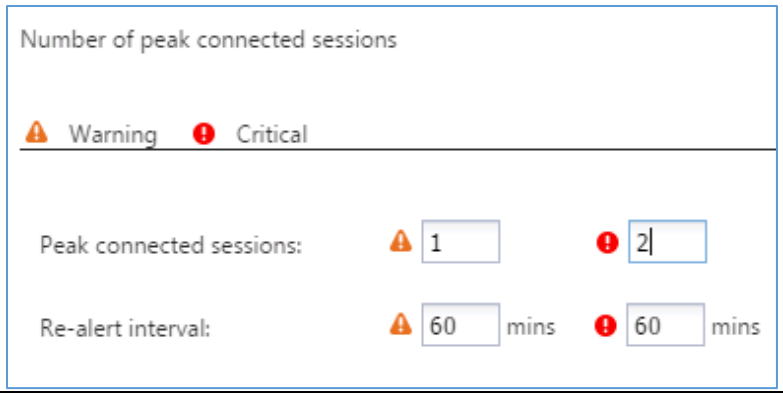
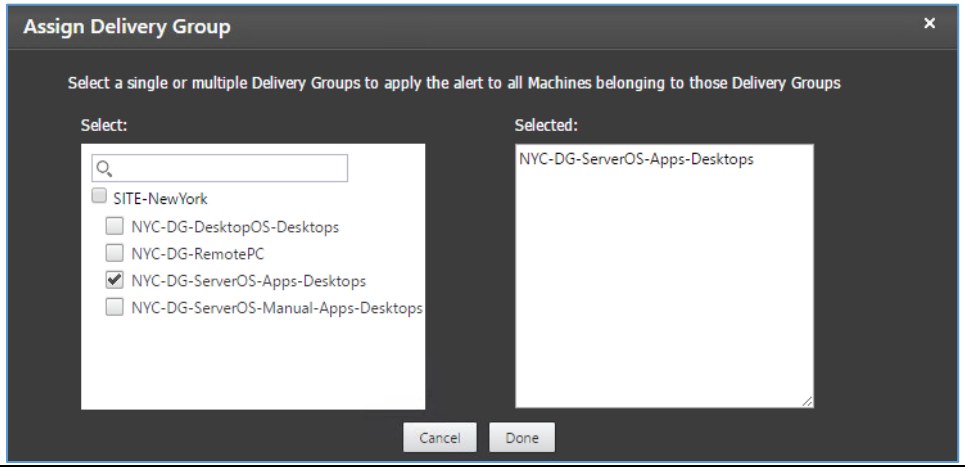
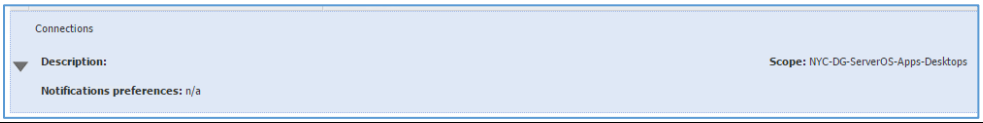
Scenario:

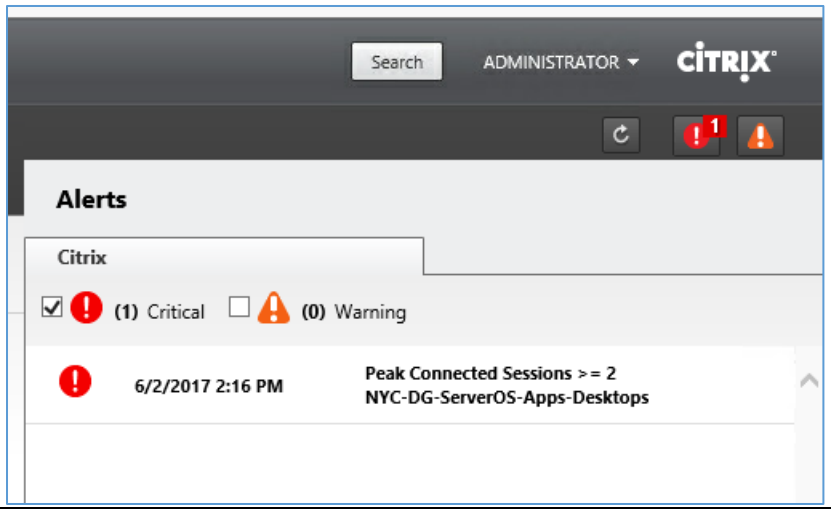
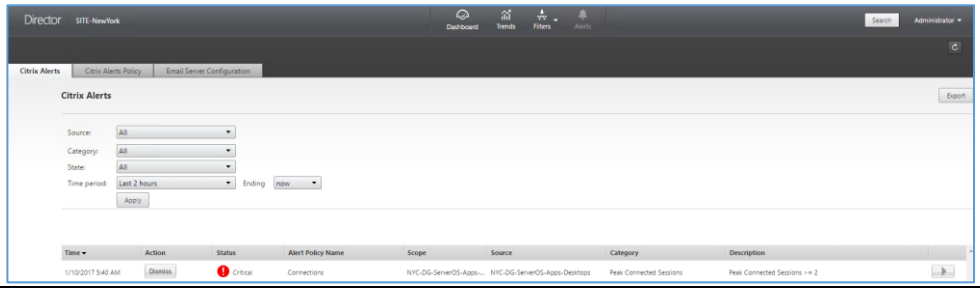
Another Citrix Administrator was tasked to monitor session counts during peak hours of the day. He noticed high session counts during peak hours and reported back to the WW Labs Citrix Administrator team.

The Citrix Administrator team has decided to pursue this trend and monitor more closely.
You have been tasked to set up alerts and notifications in real-time.

Step	Action
Create Alert	
1.	Using the Remote Desktop Connection Manager, connect to **NYC-FSR-001**. **Note:** The following credentials are used to make the connection: user name: **workspacelab\Administrator** with **Password1** as the password.
2.	Click **Start** > select **Internet Explorer** and navigate to **https://NYC-FSR-001.workspacelab.com/director**.
3.	Log on using the following credentials: User name: **Administrator** Password: **Password1**

Step	Action
	Domain: **Workspacelab**
4.	Select the **Alerts** button at the top of the Director page. 
5.	Select the **Citrix Alerts Policy** tab on the alerts page. 
6.	Select the **Delivery Group Policy** tab.  **Note**: You can create policies based on Delivery Group, Server or Site.
7.	Click **Create**.
8.	Type **Connections** in the Name of Alerts field.
9.	Select **Peak Connected Sessions** (default) from the Conditions list.
10.	Enter **1** in the **Warning** field and **2** in the **Critical** field.

Step	Action
	
11.	Click the **Assign** button under the Scope field.
12.	Check the box next to **NYC-DG-ServerOS-Apps-Desktops**. 
13.	Click **Done**.
14.	Click **Save**.
15.	Review the newly created **Connections** policy in Director. 
Triggering an Alert	
16.	Using the Remote Desktop Connection Manager, connect to **NYC-WRK-001**. **Note:** The following credentials are used to make the connection: user name: **workspacelab\HR1** with **Password1** as the password.
17.	Launch **Internet Explorer** from the Desktop and browse to **https://storefront.workspacelab.com/Citrix/WWLabsStoreWeb/** Log on with username: **HR1** and password: **Password1**.
18.	Launch **Excel 2016**.
19.	Launch **Google Chrome** from the desktop and browse to **https://storefront.workspacelab.com/Citrix/WWLabsStoreWeb/**.
20.	Log on as the **HR2** user with the following credentials: User name: **workspacelab\HR2**

Step	Action
	Password: **Password1**
21.	Launch **Excel 2016**.
22.	Using the Remote Desktop Connection Manager, switch back to **NYC-FSR-001** and refresh the Citrix Director **Alerts** page using the refresh arrow in the top right corner.
23.	Click the **Critical** and **Warning** notification icons in the top right corner of Director to review the information about the session connection limits that have been reached. 
24.	Select the **Citrix Alerts** tab from the Alerts page where you can review detailed information about the current alerts. 

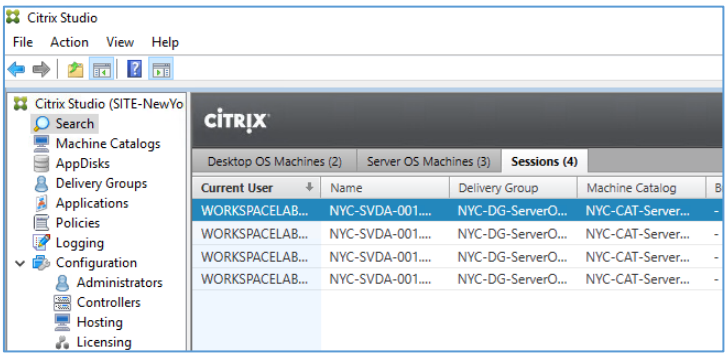
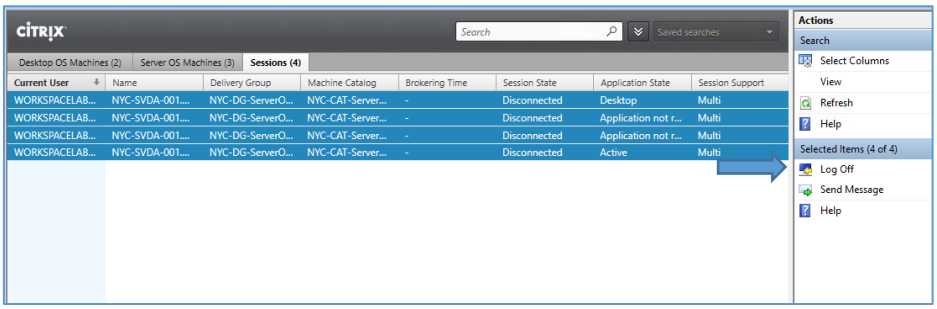
Takeaways:

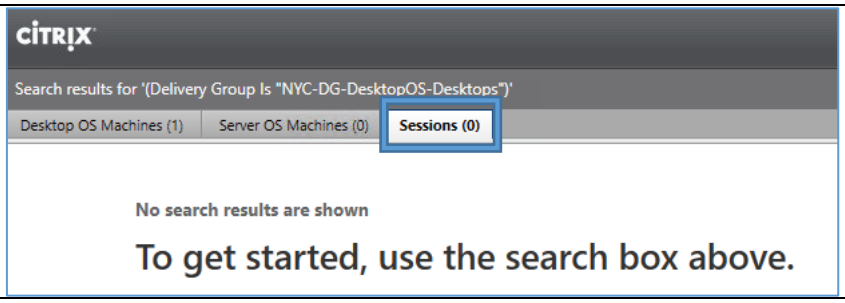
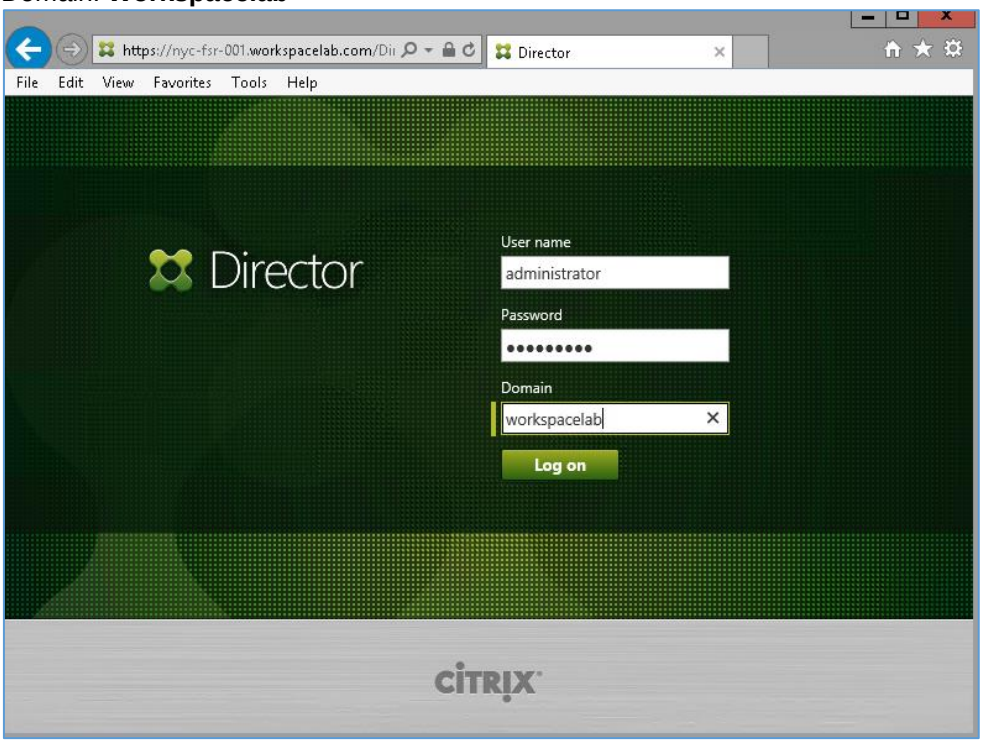
- You can configure email alerts to be sent to specific person(s) when session, connection or logon thresholds have been reached.
- Beginning with version 7.13, alerts can also trigger SNMP traps. SNMP integration is done through PowerShell using Set-MonitorNotificationSnmpServerConfiguration.
- You can create Citrix Alert policies for your infrastructure based on Delivery Group, Server or Site.
- Critical Alerts and Warnings can be reviewed and managed within Citrix Director under the Citrix Alerts tab.

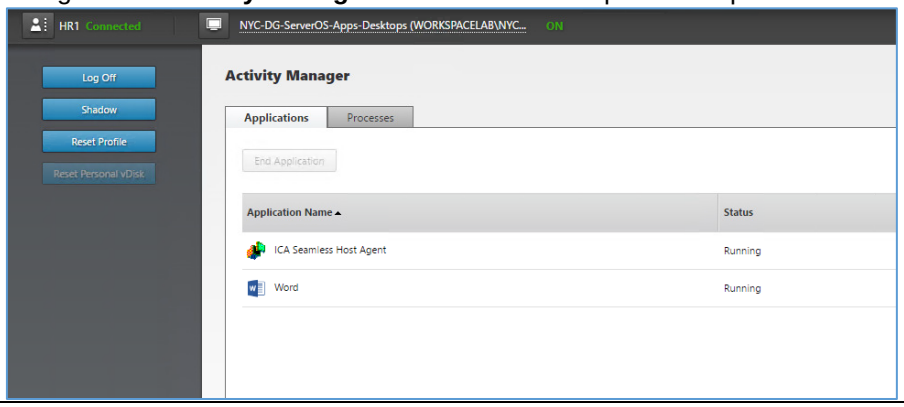
Exercise 13-4: View the Session Default View Page

Scenario:

Your task is to view the default page for Sessions.

Step	Action
1.	Using the Remote Desktop Connection Manager, switch back to **NYC-WRK-001**. **Note:** In a previous exercise, you had logged on to **NYC-WRK-001** using the following credentials to make the connection: user name: **WORKSPACELAB\HR1 with Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-WRK-001**, right-click this machine and choose **Connect server**.
2.	**Close** both **Excel 2016** sessions. **Log off** HR2 and HR1 users from Google Chrome and Internet Explorer. **Close** Google Chrome and Internet Explorer.
3.	Using the Remote Desktop Connection Manager, switch back to **NYC-XDC-001**.
4.	Using **Studio** navigate to **Search** and click **Sessions** in the center pane.  **Note**: Ensure that no filters are applied to the search.
5.	Select all sessions on the list and click **Log Off** in the Actions pane on the right to ensure all disconnected sessions are logged off.  **Note**: This is done to ensure that the output and results of the following exercises are consistent with the Exercise Workbook. If all sessions have been logged off, this screen shot may not match your Studio experience. To continue the Session count needs to be **0** as shown in the below screenshot.

	
6.	Using the Remote Desktop Connection Manager, switch back to **NYC-WRK-001**. Again, launch **Internet Explorer** from the desktop and browse to **https://storefront.workspacelab.com/Citrix/WWLabsStoreWeb/**
7.	Log on as the **HR1** user with the following credentials: User name: **HR1** Password: **Password1**
8.	Launch **Word 2016** and **HR Desktop**.
9.	Using the Remote Desktop Connection Manager, switch back to **NYC-FSR-001**. **Note:** In a previous exercise, you had logged on to **NYC-FSR-001** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-FSR-001**, right-click this machine and choose **Connect server**.
10.	Log back in to Director using the following credentials: User name: **Administrator** Password: **Password1** Domain: **Workspacelab**  Click **Log on**.

11.	On the top right of the Director console click **Search**. In the search for user field type **HR1** and press **Enter**.
12.	On the **Select a Session** pop up select **Word**.
13.	Navigate the **Activity Manager** for the user and explore the options available. 
14.	Click **Administrator** > **Log Off** Director.

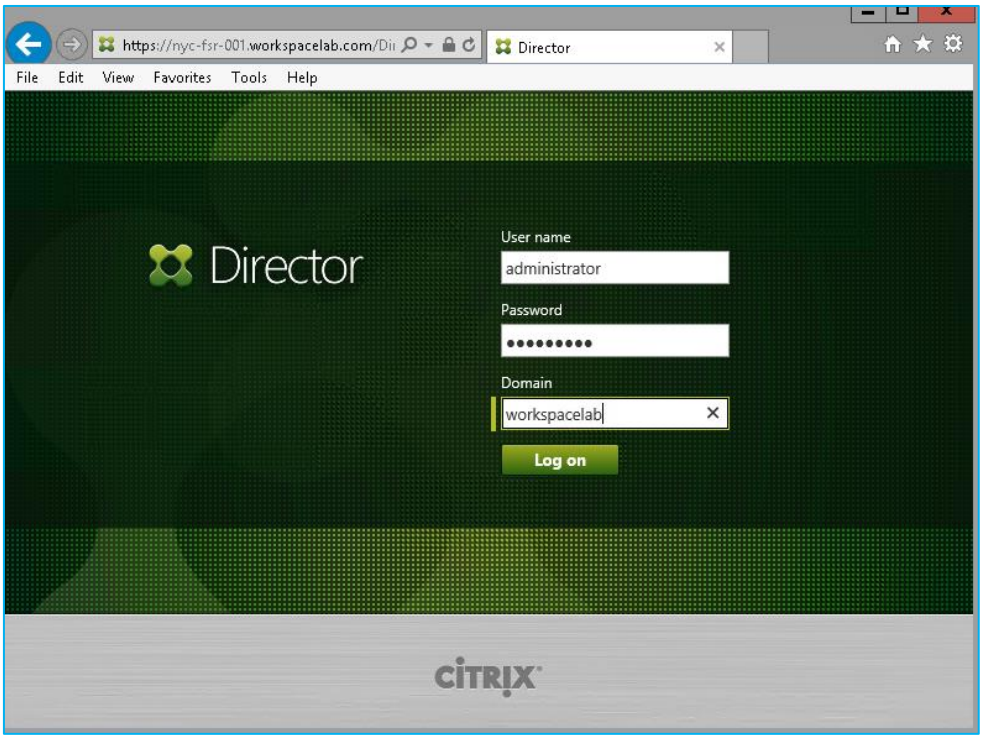
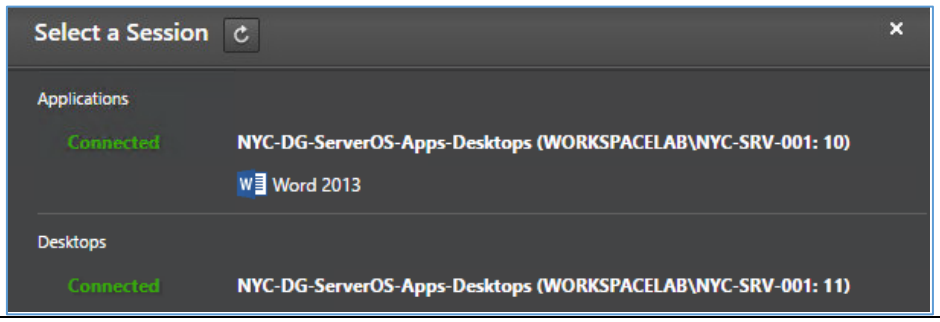
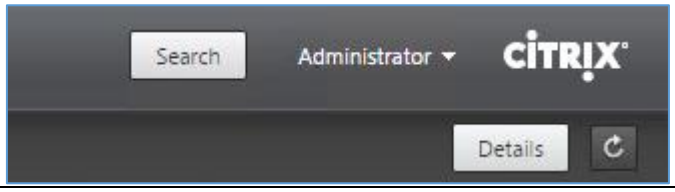
Key Takeaways:

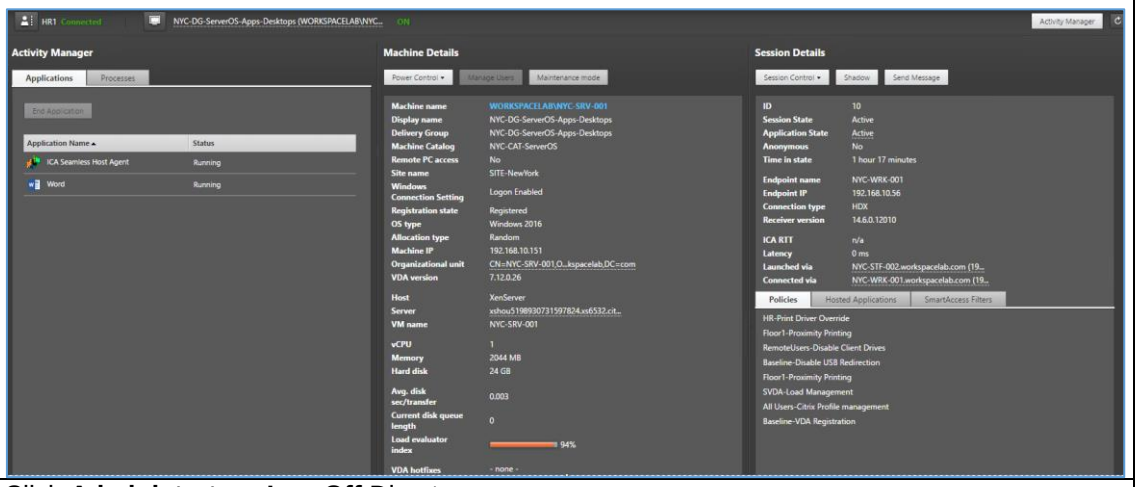
- To view the session default view page for a user, a search must be done to find the session the user has open.

Exercise 13-5: View the Session Details Page

In this exercise, you will learn to view the session details page.

Step	Action
1.	Using the Remote Desktop Connection Manager, confirm you are still connected to **NYC-WRK-001**. **Note:** In a previous exercise, you had logged on to **NYC-WRK-001** using the following credentials to make the connection: user name: **WORKSPACELAB\HR1** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-WRK-001**, right-click this machine and choose **Connect server**.
2.	Confirm you are still logged on to **Citrix Receiver** with the following credentials: User name: **HR1** Password: **Password1** Verify that the **HR Desktop** and **Microsoft Word** sessions are still running. **Note**: If needed, log back on to Citrix **Receiver** and re-launch the **HR Desktop** and **Microsoft Word** sessions.
3.	Using the Remote Desktop Connection Manager, switch back to **NYC-FSR-001**. **Note:** In a previous exercise, you had logged on to **NYC-FSR-001** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password.

	Note: If your Remote Desktop Connection session disconnected, log on to **NYC-FSR-001**, right-click this machine and choose **Connect server**.
4.	Log back in to Director using the following credentials: User name: **Administrator** Password: **Password1** Domain: **Workspacelab**  Click **Log on**.
5.	Click **Search** on the top right of the Director page, type **HR1**, and select **(WORKSPACELAB\HR1)**.
6.	When prompted to select a session, click on **Word 2016**. 
7.	Scroll to the right-hand side of the page, and click the **Details** button. 

8.	Explore the sections of the **Details** page. Depending on your screen resolution, you may need to scroll both directions. 
9.	Click **Administrator** >**Log Off** Director.

Key Takeaways:

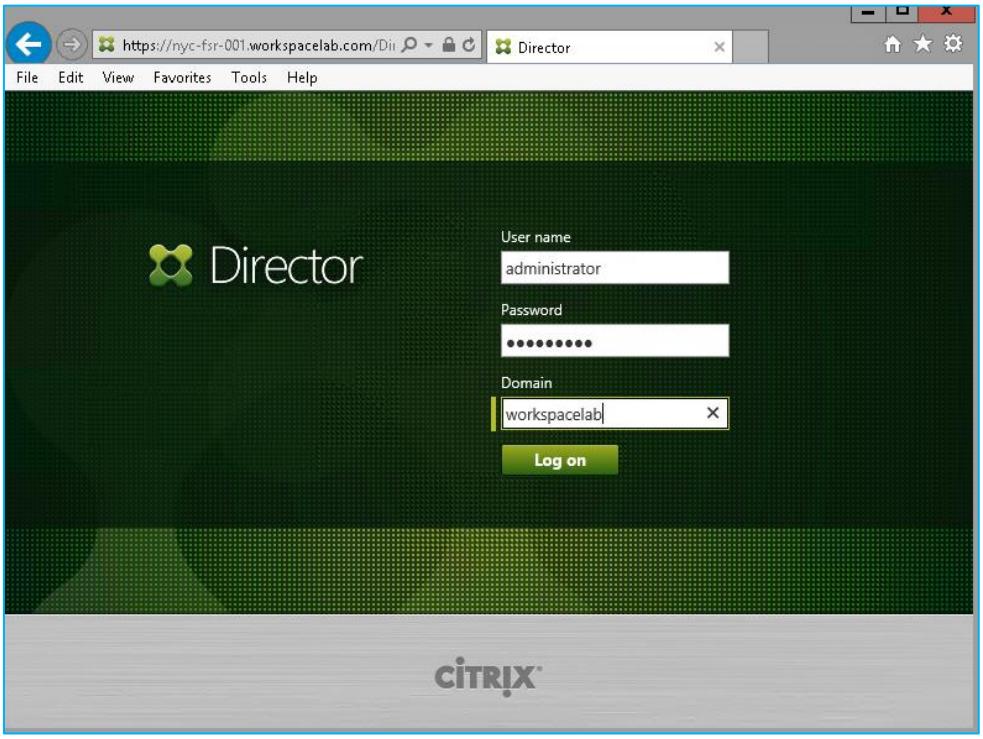
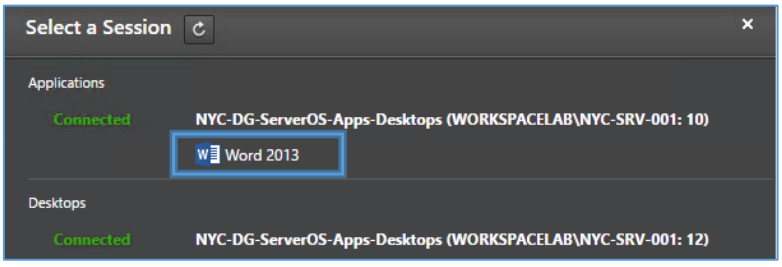
- To view the session details page for a user, a search must be done to find the session the user has open and then click the Details button.

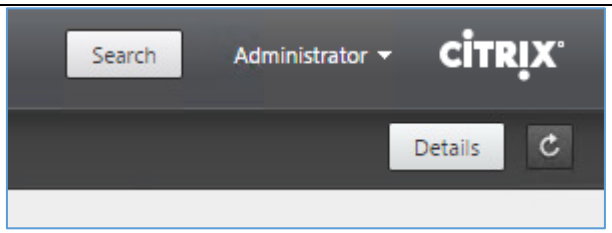
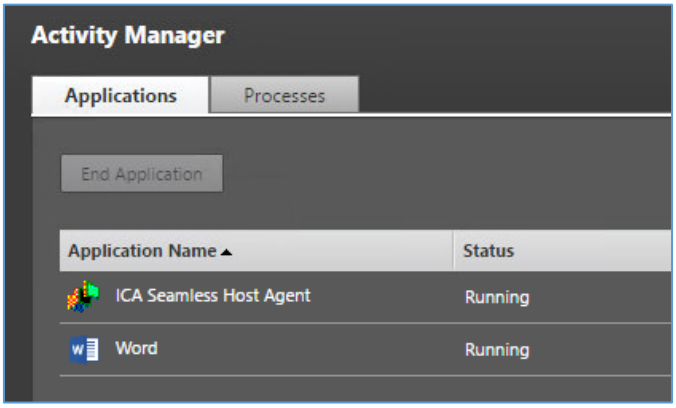
Exercise 13-6: Log Off a User Session

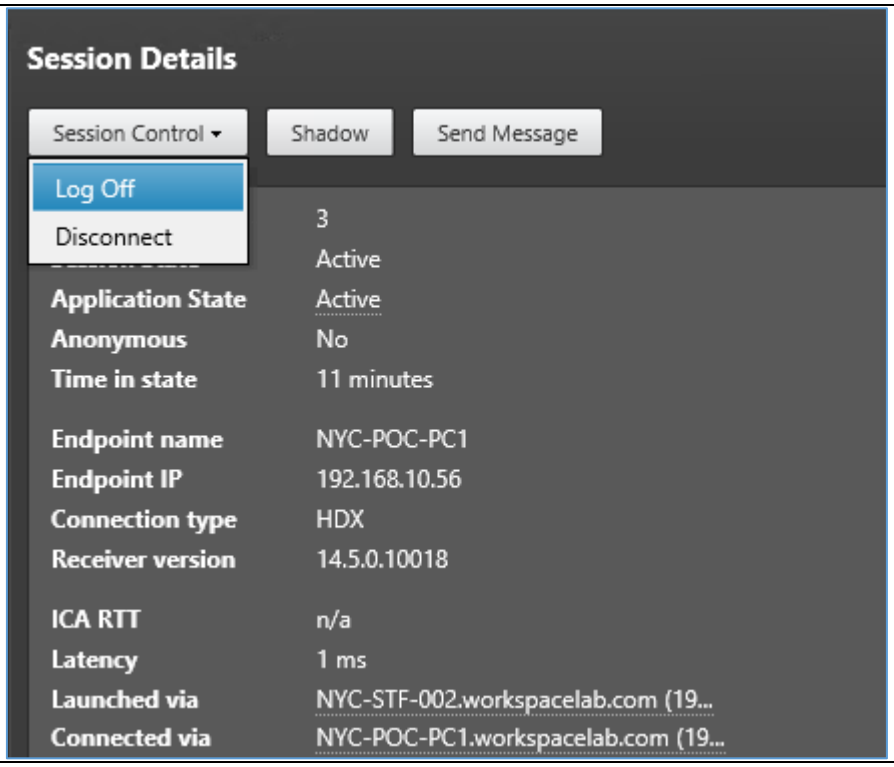
Scenario:

Your task is to log off a user session.

Step	Action
1.	Using the Remote Desktop Connection Manager, switch back to **NYC-WRK-001**. **Note:** In a previous exercise, you had logged on to **NYC-WRK-001** using the following credentials to make the connection: user name: **WORKSPACELAB\HR1** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-WRK-001**, right-click this machine and choose **Connect server**.
2.	Confirm you are still logged into **Citrix Receiver** with the following credentials: User name: **HR1** Password: **Password1** Verify that the **HR Desktop** and **Microsoft Word** sessions are still running. **Note**: If needed, log back on to **Citrix Receiver** and re-launch the **HR Desktop** and **Word 2016** session.
3.	Using the Remote Desktop Connection Manager, switch back to **NYC-FSR-001**. **Note:** In a previous exercise, you had logged on to **NYC-FSR-001** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password.

	Note: If your Remote Desktop Connection session disconnected, log on to **NYC-FSR-001**, right-click this machine and choose **Connect server**.
4.	Log back in to Director using the following credentials: User name: **Administrator** Password: **Password1** Domain: **Workspacelab**  Click **Log on**.
5.	Click **Search** on the top right of the Director page, type **HR1**, and select **(WORKSPACELAB\HR1)**.
6.	When prompted to select a session, click on **Word 2016**. 
7.	Scroll to the right-hand side of the page, and click the **Details** button.

	
8.	Ensure that the appropriate desktop or application connection for the user is displayed.  **Note**: If you wish to toggle between the sessions details for a user having multiple sessions, use the session icon. The session icon looks like a computer display at the top of the Details page. The session icon is only available when the selected end user has multiple sessions running.
9.	Scroll the Details page to the right and then click **Session Control**.

	
10.	Click **Log Off** to log the end user off the session.
11.	Wait for the logoff process to complete. Do not click Log Off again. Doing so will result in an error message. **Note**: Afterward, the session details will disappear from the Details pane.
12.	Click **Administrator** > **Log Off** Director.
13.	Using the Remote Desktop Connection Manager, switch back to **NYC-WRK-001**. **Note:** In a previous exercise, you had logged on to **NYC-WRK-001** using the following credentials to make the connection: user name: **WORKSPACELAB\HR1** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-WRK-001**, right-click this machine and choose **Connect server**.
14.	Verify that the **HR Desktop** session is still running. The **Microsoft Word** session should now be gone.

Key Takeaways:

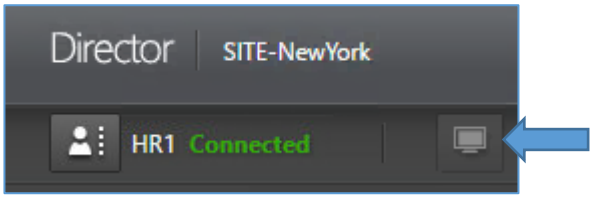
- The option to log off a user can be found in the details page by clicking Session Control.
- It is recommended to click Log off just once as possible errors will appear if multiple clicks are done.

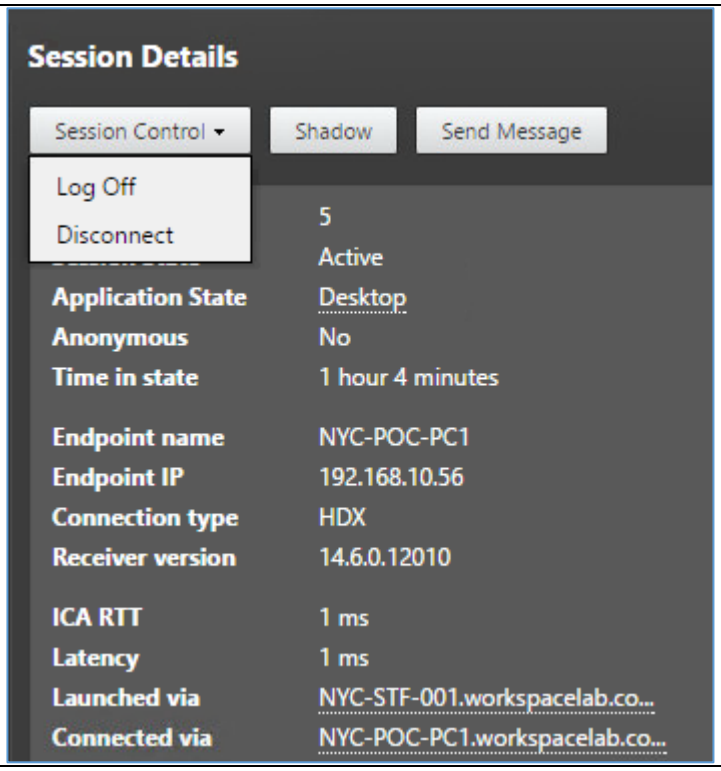
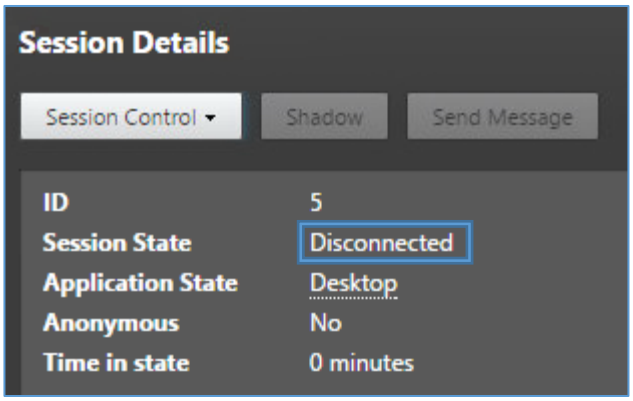
Exercise 13-7: Disconnect a User Session

Scenario:

Your task is to disconnect a user session.

Step	Action

1.	Using the Remote Desktop Connection Manager, switch back to **NYC-WRK-001**. **Note:** In a previous exercise, you had logged on to **NYC-WRK-001** using the following credentials to make the connection: user name: **WORKSPACELAB\HR1** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-WRK-001**, right-click this machine and choose **Connect server**.
2.	Confirm you are still logged on to **Citrix Receiver** with the following credentials: User name: **HR1** Password: **Password1** Your **HR Desktop** session should still be running. If this is not the case, re-launch the HR Desktop. **Note**: If needed, log back on to Citrix **Receiver**.
3.	Using the Remote Desktop Connection Manager, switch back to **NYC-FSR-001**. **Note:** In a previous exercise, you had logged into **NYC-FSR-001** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-FSR-001**, right-click this machine and choose **Connect server**.
4.	Log back in to Director using the following credentials: User name: **Administrator** Password: **Password1** Domain: **Workspacelab** Click **Log on**.
5.	Click **Search** on the top right of the Director page, type **HR1**, and select **(WORKSPACELAB\HR1)**.
6.	Scroll to the right-hand side of the page, and click the **Details** button.
7.	Confirm that the session selector is now **greyed out**; this is because the user only has one session running.  **Note**: The session icon is only available when the selected end user has multiple sessions running.
8.	Scroll the Details page to the right and then click **Session Control**.

	
9.	Click **Disconnect** to disconnect the selected session.
10.	Verify that the state of the session has changed to **Disconnected**.  **Note**: If needed, click the Refresh arrows in the top right side of the Director page.
11.	Click **Administrator** >**Log Off** Director.

Key Takeaways:

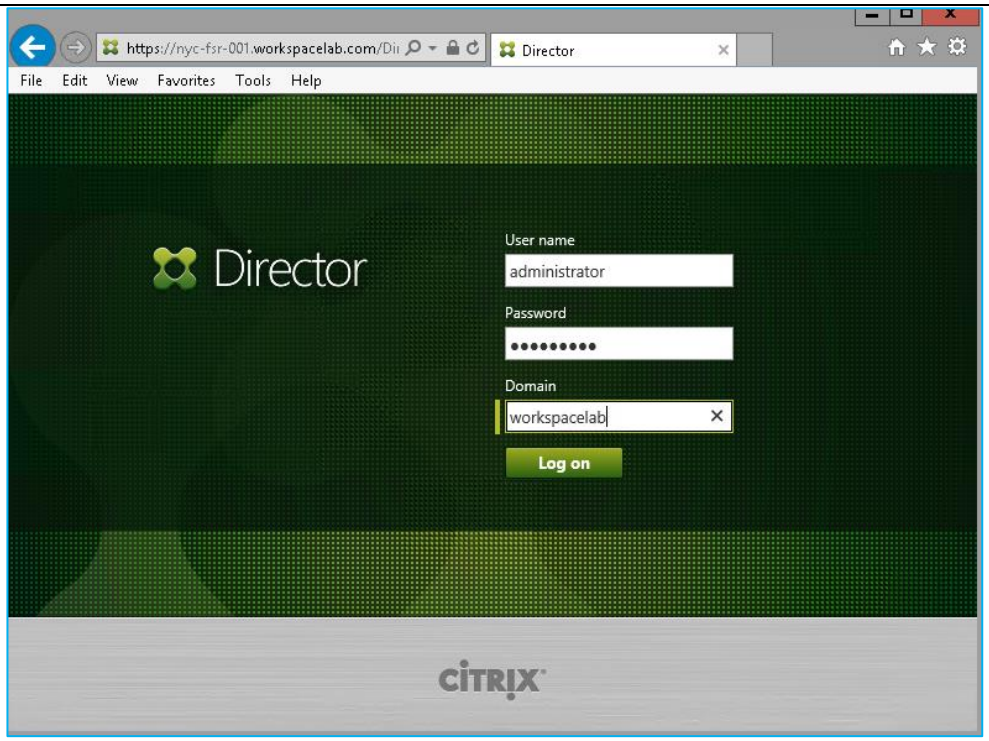
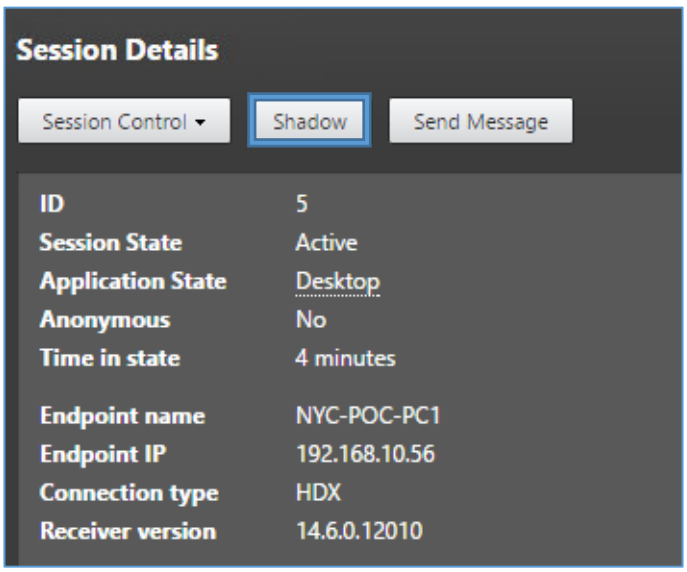
- To disconnect a user session, you need to search for the user and then view the details of the session.
- If you place a user session in a Disconnected state, the user can reconnect back to the disconnected session if policies allow it. By default, it is allowed.

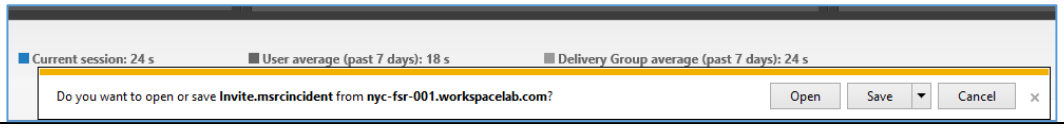
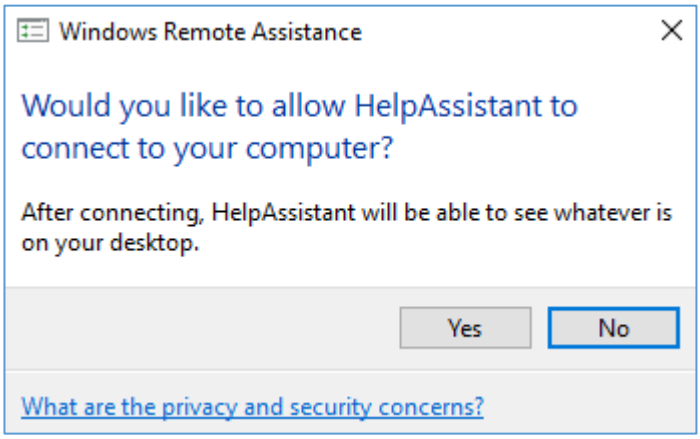
Exercise 13-8: Shadow a User Session

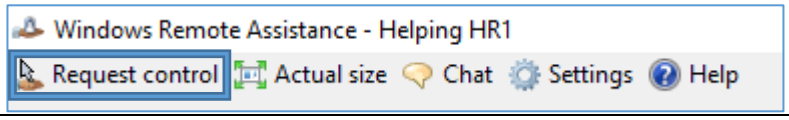
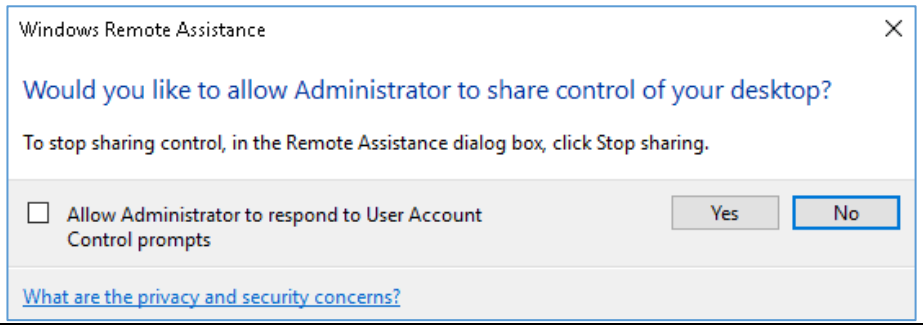
Scenario:

Your task is to shadow a user session.

Step	Action
1.	Using the Remote Desktop Connection Manager, switch back to **NYC-WRK-001**. **Note:** In a previous exercise, you had logged on to **NYC-WRK-001** using the following credentials to make the connection: user name: **WORKSPACELAB\HR1** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-WRK-001**, right-click this machine and choose **Connect server**.
2.	Confirm you are still logged on to **Citrix Receiver** with the following credentials: User name: **HR1** Password: **Password1** Your **HR Desktop** session was disconnected by the Administrator via Director in the previous task. To continue with this task, re-launch the HR Desktop. **Note**: A disconnected session continues to run on the machine that was hosting it. The disconnect action disconnects the Receiver to the session. By re-launching the HR Desktop, you are re-connecting to the existing session. **Note**: If needed, log back on to **Citrix Receiver**.
3.	Using the Remote Desktop Connection Manager, switch back to **NYC-FSR-001**. **Note:** In a previous exercise, you had logged on to **NYC-FSR-001** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-FSR-001**, right-click this machine and choose **Connect server**.
4.	Log back in to Director using the following credentials: User name: **Administrator** Password: **Password1** Domain: **Workspacelab**

	 Click **Log on**. **Note**: Director was launched in a previous exercise. If Director was closed in a previous exercise, then click the **Internet Explorer** icon on the desktop and browse to **https://nyc-fsr-001.workspacelab.com/Director**.
5.	Click **Search** on the top right of the Director page, type **HR1**, and select **(WORKSPACELAB\HR1)**.
6.	Scroll to the right-hand side of the page, and click the **Details** button.
7.	Click the **Shadow** button. 

	Note: If you receive an error here, it may be caused by a profile corruption within the Desktop session. Navigate back to NYC-WRK-001 and verify if the desktop session has a grey background image or a default Windows background. If you see a default Windows background, use Director to reset your profile, log off the desktop session, and start it again.
8.	Click **Open** in the Opening **Invite.msrcincident** dialog box and wait for the end user to accept your invitation. 
9.	Using the Remote Desktop Connection Manager, switch back to **NYC-WRK-001**. **Note:** In a previous exercise, you had logged on to **NYC-WRK-001** using the following credentials to make the connection: user name: **WORKSPACELAB\HR1** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-WRK-001**, right-click this machine and choose **Connect server**.
10.	Click **Yes** in the Would you like to allow HelpAssistant to connect to your computer message.  **Note**: If the end user does not respond within 120 seconds, the connection will fail. In such cases, the support administrator must click OK in the Windows Remote Assistance message on Director to end the shadowing request. **Note**: For the Shadow session to complete, the following conditions must be met: • The support administrator must run Director from a system in which the Remote Assistance Client is both installed and enabled. • The target Virtual Delivery Agent (VDA) system hosting the session to be shadowed must have remote assistance enabled. • The Remote Assistance network ports must be opened on the firewall (3389). • There must be a Citrix Policy allowing shadowing.
11.	Using the Remote Desktop Connection Manager, switch back to **NYC-FSR-001**. **Note:** In a previous exercise, you had logged on to **NYC-FSR-001** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-FSR-001**, right-click this machine and choose **Connect server**.

12.	Click **Request control** from the Windows Remote Assistance window on the system running Director. 
13.	Using the Remote Desktop Connection Manager, switch back to **NYC-WRK-001**. **Note:** In a previous exercise, you had logged on to **NYC-WRK-001** using the following credentials to make the connection: user name: **WORKSPACELAB\HR1** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-WRK-001**, right-click this machine and choose **Connect server**.
14.	Click **Yes** on the Windows Remote Assistance screen to allow Helpdesk Admin to share control. 
15.	Using the Remote Desktop Connection Manager, switch back to **NYC-FSR-001**. **Note:** In a previous exercise, you had logged on to **NYC-FSR-001** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-FSR-001**, right-click this machine and choose **Connect server**.
16.	Using the Director-launched Remote Assistance Shadowing window to interact with the user session.
17.	Close the Windows Remote Assistance window to end the shadowing session. Click the **X** in the small or full screen Windows Remote Assistance window.
18.	Click **Administrator** > **Log Off** Director.

Key Takeaways:

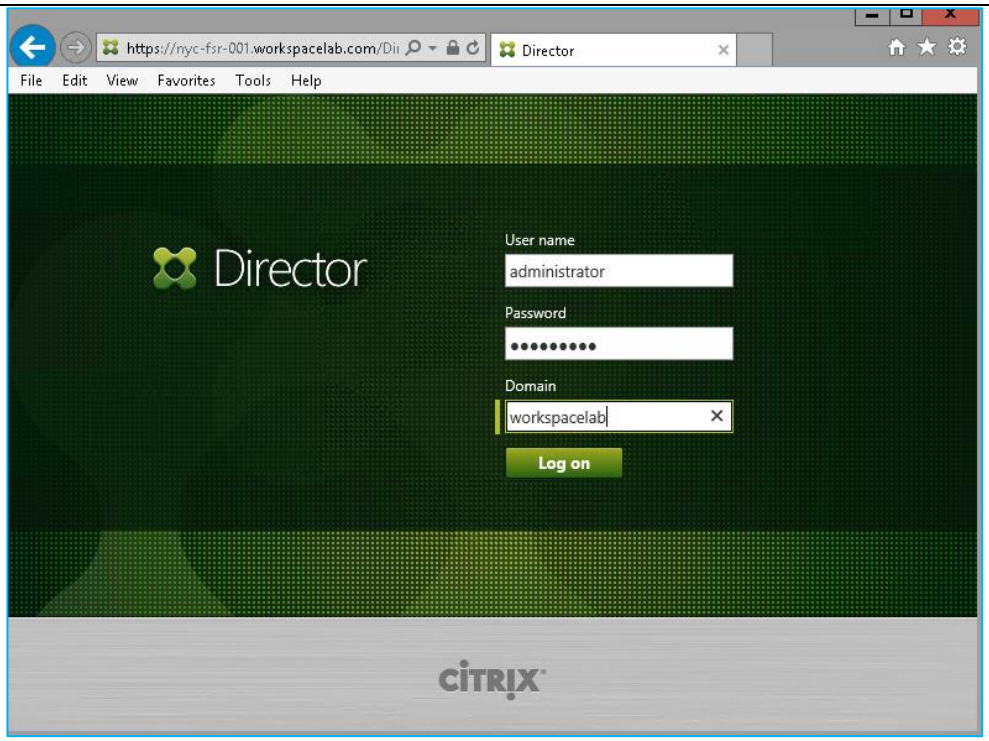
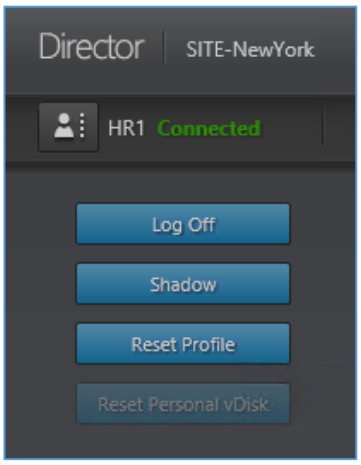
- The end user must accept the request to shadow his session.
- The end user could also end the shadowing session by clicking the X in the Windows Remote Assistance window displayed on the endpoint.
- If you end the shadowing session by closing the small Windows Remote Assistance window, you must close the full screen Windows Remote Assistance window separately.
- Shadowing a session is a great tool when troubleshooting user specific issues.

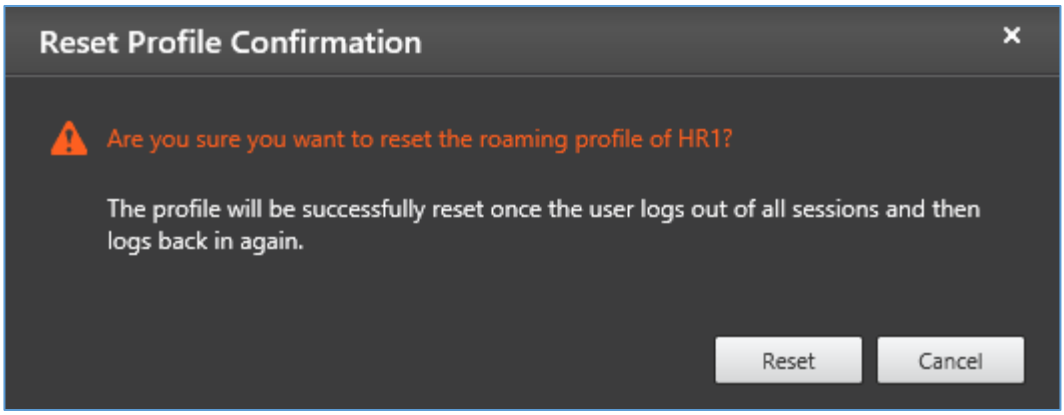
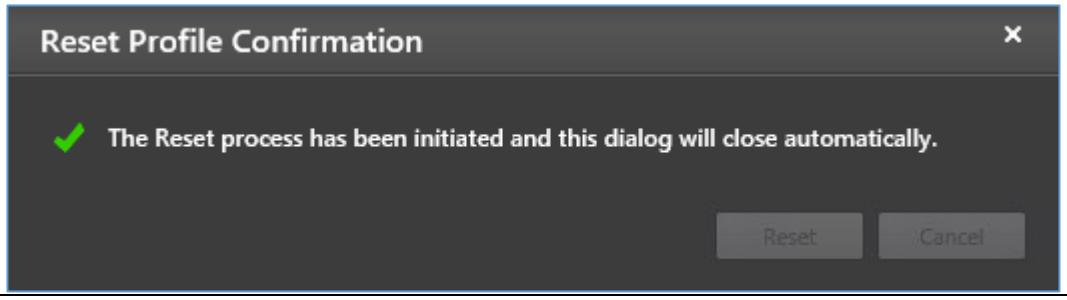
Exercise 13-9: Reset the User Profile

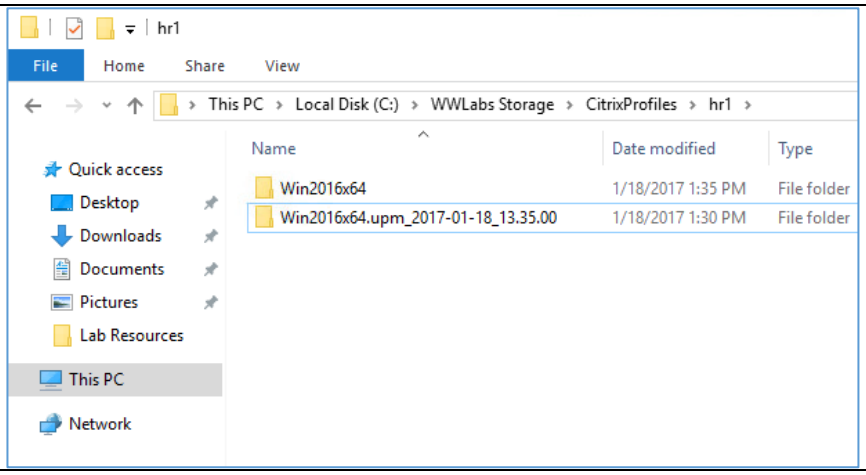
Scenario:

Your task is to reset a user profile using Citrix Director.

Step	Action
1.	Using the Remote Desktop Connection Manager, switch back to **NYC-WRK-001**. **Note:** In a previous exercise, you had logged on to **NYC-WRK-001** using the following credentials to make the connection: user name: **WORKSPACELAB\HR1** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-WRK-001**, right-click this machine and choose **Connect server**.
2.	Confirm you are still logged on to **Citrix Receiver** with the following credentials: User name: **HR1** Password: **Password1** Confirm the **HR Desktop** session is still running. **Note**: If needed, log back on to **Citrix Receiver** and re-launch the **HR Desktop** session.
3.	Using the Remote Desktop Connection Manager, switch back to **NYC-FSR-001**. **Note:** In a previous exercise, you had logged on to **NYC-FSR-001** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-FSR-001**, right-click this machine and choose **Connect server**.
4.	Log back in to Director using the following credentials: User name: **Administrator** Password: **Password1** Domain: **Workspacelab**

	 Click **Log on**. **Note**: Director was launched in a previous exercise. If Director was closed in a previous exercise, then click the **Internet Explorer** icon on the desktop and browse to **https://nyc-fsr-001.workspacelab.com/Director**.
5.	Click **Search** on the top right of the Director page, type **HR1**, and select **(WORKSPACELAB\HR1)**.
6.	Click the **Reset Profile** button on the left.  When prompted for confirmation click **Reset**.

	 **Note**: A Reset Profile Confirmation is displayed advising that The Reset process has been initiated. This dialog will close automatically.
7.	Acknowledge the **Reset Profile Confirmation**. 
8.	Using the Remote Desktop Connection Manager, switch back to **NYC-WRK-001**. Within the **HR Desktop**, right-click the **Start Menu** and select **Shut down or sign out > Sign out** to log off the session.
9.	Confirm you are still logged on to **Citrix Receiver** with the following credentials: User name: **HR1** Password: **Password1** Start the **HR Desktop** session again to complete the profile reset. **Note**: HR Desktop may take up to 5 minutes to start. **Note:** When resetting a profile through Director, UPM will rename the original profile during the next logon and create a new profile. This enables administrators to track when a profile was reset and recover files from the old profile.
10.	Using the Remote Desktop Connection Manager, switch back to **NYC-FSR-001**. Open **File Explorer** and navigate to: **C:\WWLabs Storage\CitrixProfiles\hr1**. Notice there are now two folders. The one with a date stamp in the folder name is the old profile that you just reset.

	
11.	Switch back to the Director browser window. Click **Administrator** > **Log Off** Director.

Key Takeaways:

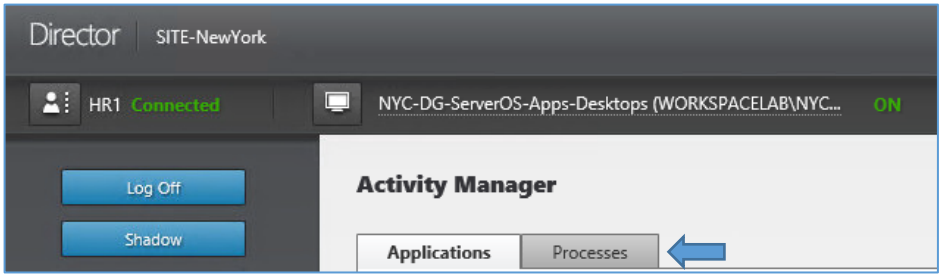
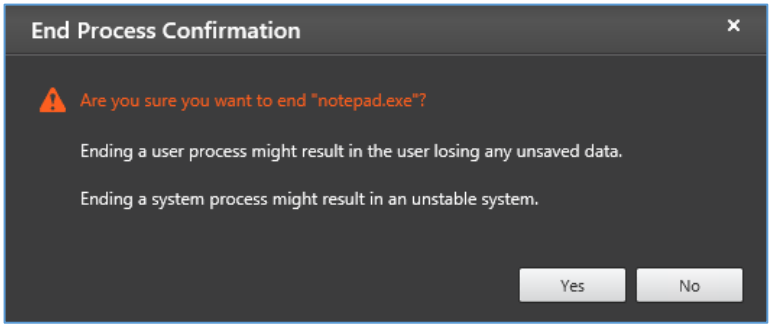
- When a profile is reset, although the user's folders and files are saved and copied to the new profile, most user profile data is deleted. For example, the registry is reset and application settings might be deleted.
- If the user has profiles on multiple platforms (such as Windows 8 and Windows 7), instruct the user to log back on first to the same desktop or app that the user reported as a problem. This enables the correct profile to be reset. If the profile is a Citrix user profile, the profile is already reset by the time the user's desktop appears. If the profile is a Microsoft roaming profile, the folder restoration might still be in progress for a brief time. The user must stay logged on until the restoration is complete.

Exercise 13-10: End a Process within a User Session

Scenario:

Your task is to kill a process for a user session from Citrix Director.

Step	Action
1.	Using the Remote Desktop Connection Manager, switch back to **NYC-WRK-001**. **Note:** In a previous exercise, you had logged on to **NYC-WRK-001** using the following credentials to make the connection: user name: **WORKSPACELAB\HR1** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-WRK-001**, right-click this machine and choose **Connect server**.
2.	Confirm you are still logged on to **Citrix Receiver** with the following credentials: User name: **HR1** Password: **Password1** Confirm the **HR Desktop** session is still running. **Note**: If needed, log back in to **Citrix Receiver** and re-launch the **HR Desktop** session.
3.	Inside the HR Desktop, open **Notepad** from the Start Menu. Click the **Start Menu** > **Windows Accessories** > **Notepad**.

4.	Using the Remote Desktop Connection Manager, switch back to **NYC-FSR-001**. **Note:** In a previous exercise, you had logged on to **NYC-FSR-001** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-FSR-001**, right-click this machine and choose **Connect server**.
5.	Log back in to Director using the following credentials: User name: **Administrator** Password: **Password1** Domain: **Workspacelab** Click **Log on**. **Note**: Director was launched in a previous exercise. If Director was closed in a previous exercise, then click the **Internet Explorer** icon on the desktop and browse to **https://nyc-fsr-001.workspacelab.com/Director**.
6.	Click **Search** on the top right of the Director page, type **HR1**, and select **(WORKSPACELAB\HR1)**.
7.	Click the **Processes** tab in the Activity Manager.  Find **notepad.exe** on the processes list, highlight the process and click **End Process**.  Click **Yes** to confirm ending the process. By clicking on **End Process** and selecting **Yes** to confirm the action, the selected process ends. This can be a helpful tool in troubleshooting and recovering a user's session that becomes unresponsive from a "hung" process. **Note:** Ending a system process or a Citrix process may cause the whole session to become unresponsive. Administrative care should be taken when ending processes, as it may lead to data loss or data corruption.

8.	Using the Remote Desktop Connection Manager, switch back to **NYC-WRK-001**. **Note:** In a previous exercise, you had logged on to **NYC-WRK-001** using the following credentials to make the connection: user name: **WORKSPACELAB\HR1** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-WRK-001**, right-click this machine and choose **Connect server**.
9.	Confirm the **HR Desktop** session is still running but the Notepad application inside the session has now been terminated.
10.	Using the Remote Desktop Connection Manager, switch back to **NYC-FSR-001**. **Note:** In a previous exercise, you had logged on to **NYC-FSR-001** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-FSR-001**, right-click this machine and choose **Connect server**.
11.	Click **Administrator** > **Log Off** Director.

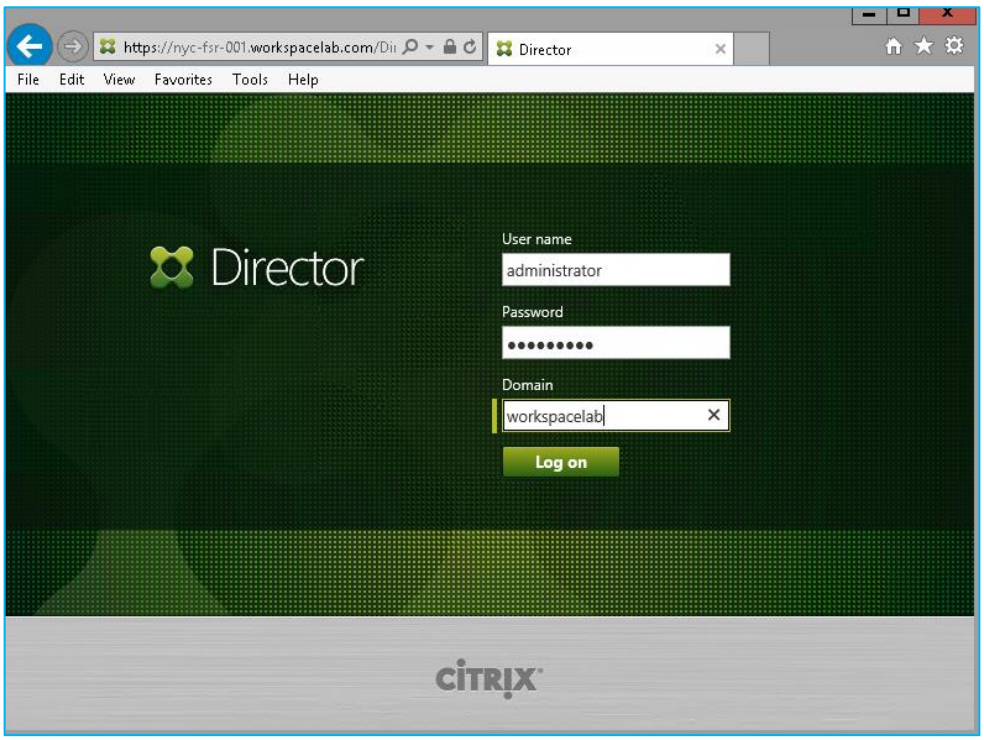
Key Takeaways:

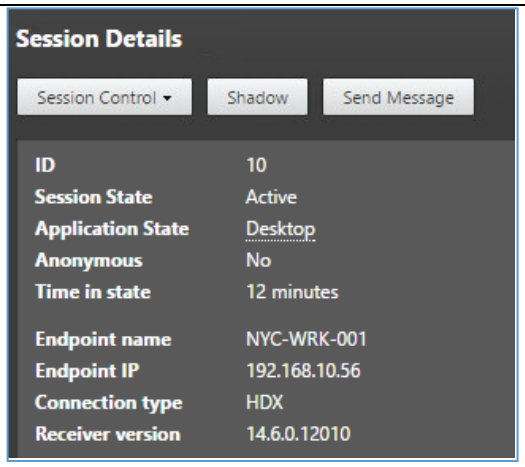
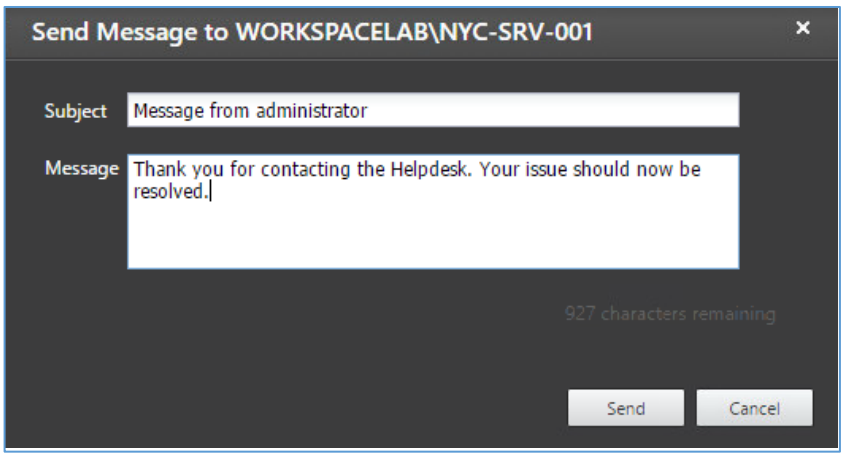
- Ending a user process will affect the functionality of the session, possibly logging the user off the current session.

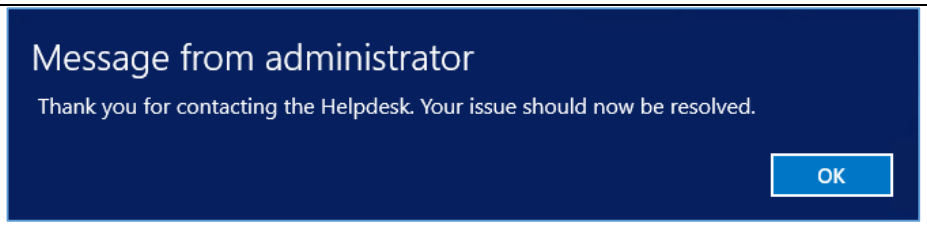
Exercise 13-11: Send a Message to a User Session

In this exercise, you will learn to send a message to a user session.

Step	Action
1.	Using the Remote Desktop Connection Manager, switch back to **NYC-WRK-001**. **Note:** In a previous exercise, you had logged on to **NYC-WRK-001** using the following credentials to make the connection: user name: **WORKSPACELAB\HR1** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-WRK-001**, right-click this machine and choose **Connect server**.
2.	Confirm you are still logged on to **Citrix Receiver** with the following credentials: User name: **HR1** Password: **Password1** Confirm the **HR Desktop** session is still running. **Note**: If needed, log back on to **Citrix Receiver** and re-launch the **HR Desktop** session.
3.	Using the Remote Desktop Connection Manager, switch back to **NYC-FSR-001**. **Note:** In a previous exercise, you had logged on to **NYC-FSR-001** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-FSR-001**, right-click this machine and choose **Connect server**.

4.	Log back in to Director using the following credentials: User name: **Administrator** Password: **Password1** Domain: **Workspacelab**  Click **Log on.** **Note**: Director was launched in a previous exercise. If Director was closed in a previous exercise, then click the **Internet Explorer** icon on the desktop and browse to **https://nyc-fsr-001.workspacelab.com/Director**.
5.	Click **Search** on the top right of the Director page, type **HR1**, and select **(WORKSPACELAB\HR1)**.
6.	Scroll to the right-hand side of the page, and click the **Details** button.
7.	Scroll the page to the right to view the Session Details pane.
8.	Click **Send Message**.

	 In the Message window, type **Thank you for contacting the Helpdesk. Your issue should now be resolved**.  Click **Send**. Acknowledge the message confirmation. **Note**: Citrix Leading Practice cannot stress enough to caution the Citrix Administrator using this Send Message feature to follow and comply with all company considerations and remain professional always. Citrix Administrators have lost their jobs over sending inappropriate messages.
9.	Using the Remote Desktop Connection Manager, switch back to **NYC-WRK-001**. **Note:** In a previous exercise, you had logged on to **NYC-WRK-001** using the following credentials to make the connection: user name: **WORKSPACELAB\HR1** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-WRK-001**, right-click this machine and choose **Connect server**.
10.	Click **OK** on the message to close it.

	 **Note**: Although we can send messages to both Active, Idle and Disconnected sessions, a user will likely only see the message when their session is in Active state.
11.	Within the **HR Desktop**, right-click the **Start Menu** and select **Shut down or sign out > Sign out** to log off the session. Log off HR1 from Receiver.
12.	Switch back to NYC-FSR-001. On the Internet Explorer window, click **Administrator** > **Log Off** Director.

Key Takeaways:

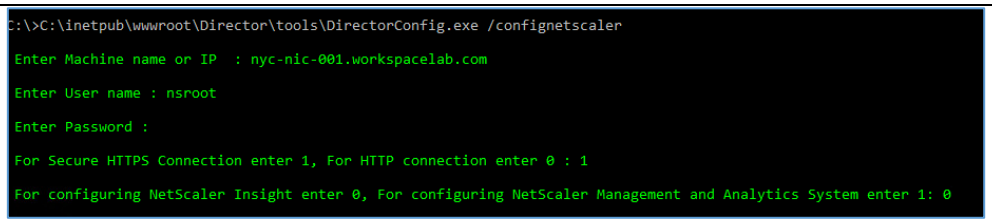
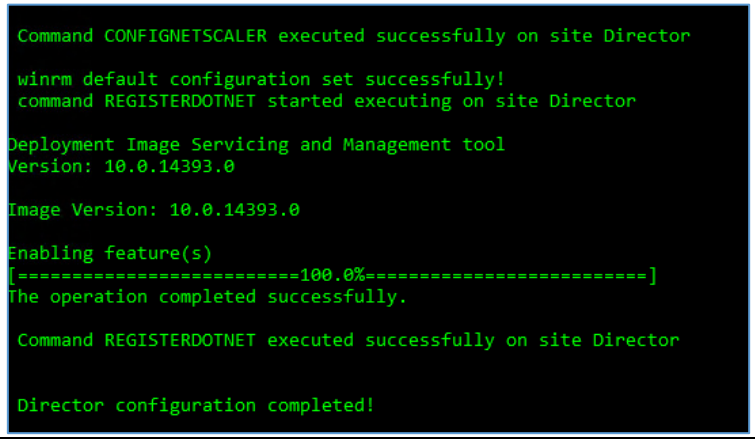
- Using Citrix Director is a great way to send important messages to users; such as advising that their issue has been resolved.

Exercise 13-12: Integrate HDX Insight with Director

Scenario:

The Citrix Lead Architect has recently introduced the features of HDX Insight to the rest of the Citrix team and every team member agrees that this will be a valuable add-on to the many features of Director. You have been tasked to configure HDX Insight and integrate it with Director.

Step	Action
1.	Using the Remote Desktop Connection Manager, switch back to **NYC-FSR-001**. **Note:** In a previous exercise, you had logged on to **NYC-FSR-001** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-FSR-001**, right-click this machine and choose **Connect server**.
2.	Right-click **Start** and select **Command Prompt (Admin)**. Enter in the following command and press **Enter**: ***C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configNetScaler*** `C:\Users\Administrator.WORKSPACELAB>C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configNetScaler`
3.	Enter the following information: • Enter Machine name: **NYC-NIC-001.workspacelab.com** • Enter User name: **nsroot** • Enter Password: **nsroot** • For HTTP connection enter: **1** • For configuring NetScaler Insight enter: **0**

	 **Note**: Both HTTP and HTTPS can be used to exchange data. For secure HTTPS connection enter 1.
4.	Once the command has run successfully, you will see the following on the command prompt: **Director configuration completed!** 
5.	**Close** the Command Prompt window.

Key Takeaways:

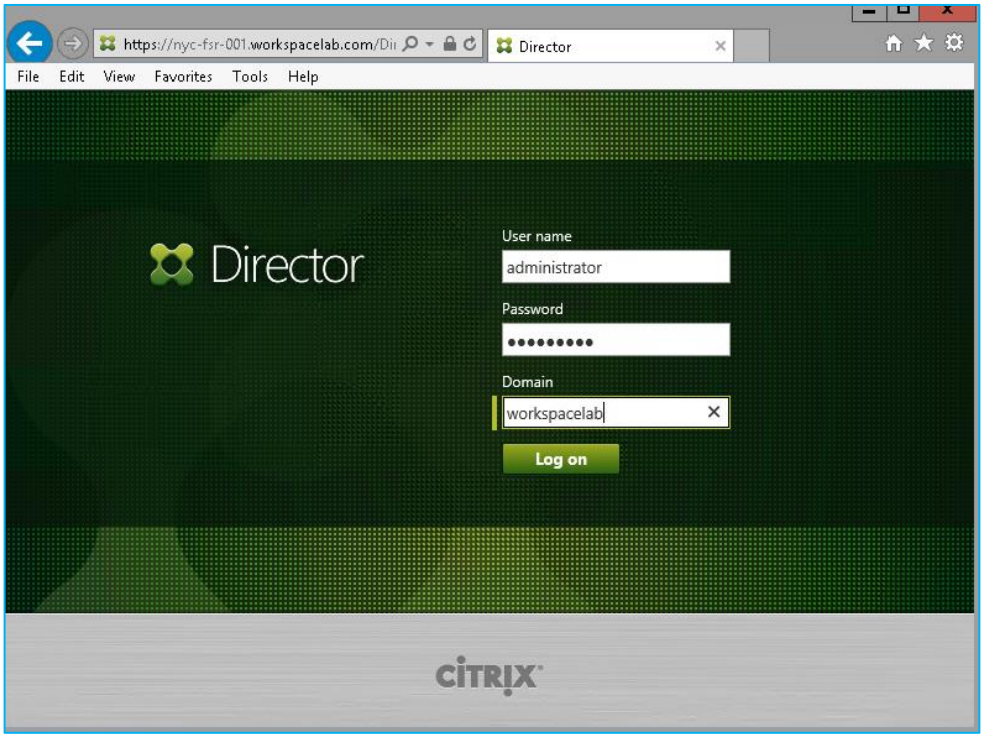
- Using HTTPS connection for both HDX Insight and Director is recommended for better security.
- If the Director logon is done via HTTPS, but HDX Insight is configured for HTTP connection, the connection is only partially encrypted. This is called webpage with mixed content.
- NetScaler HDX Insight must be v10.1 or above.
- XenDesktop VDA version 7.0 and above are supported by HDX Insight and NetScaler.

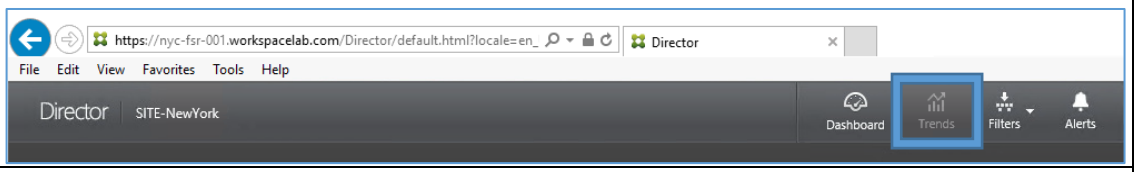
Exercise 13-13: View and Interact with the New Trends Page

Scenario:

Your task is to view the new network tab from the Trends page, after integration of NetScaler Insight Services has been done.

Step	Action
1.	Using the Remote Desktop Connection Manager, confirm you are still connected to **NYC-WRK-001**. **Note:** In a previous exercise, you had logged on to **NYC-WRK-001** using the following credentials to make the connection: user name: **WORKSPACELAB\HR1** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-WRK-001**, right-click this machine and choose **Connect server**.

2.	Open **Internet Explorer** and browse to **https://nsg.workspacelab.com**. Log on with the following credentials: User name: **HR1** Password: **Password1** Click the **APPS** tab and then launch the published **Notepad** application. **Note**: If an Internet Explorer message to store your password for the https://nsg.workspacelab.com, select Not for this site. **Note:** Tasks Tab is not available when user logs in via Access Gateway.
3.	Using the Remote Desktop Connection Manager, switch back to **NYC-FSR-001**. **Note:** In a previous exercise, you had logged on to **NYC-FSR-001** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-FSR-001**, right-click this machine and choose **Connect server**.
4.	Log back in to Director using the following credentials: User name: **Administrator** Password: **Password1** Domain: **Workspacelab**  Click **Log on**.

	Note: Director was launched in a previous exercise. If Director was closed in a previous exercise, then click the **Internet Explorer** icon on the desktop and browse to **https://nyc-fsr-001.workspacelab.com/Director**.
5.	On the top page of Director, click **Trends**. 
6.	Click the new **Network** tab.
7.	Review the new data provided by NetScaler Insight Center. Click the **Users**, **Applications** and **Desktops** to view the data.
8.	Click **Administrator** >**Log Off** Director.

Takeaways:

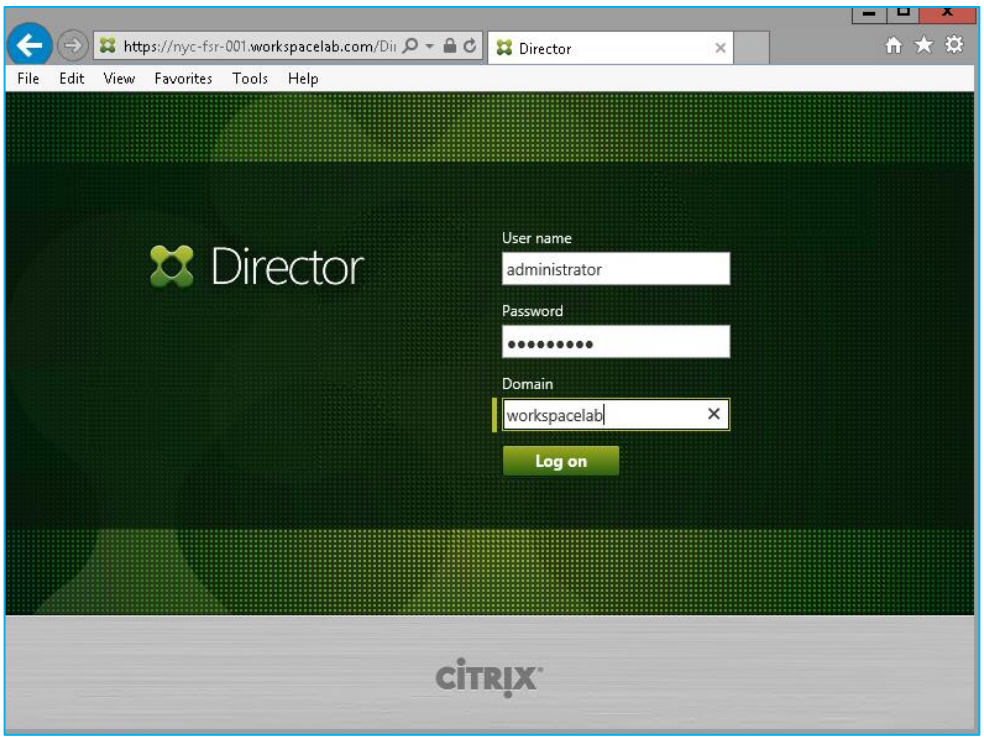
- The HDX Insight data on Director is displayed in two locations with different views; on the Trends view and the User Details view.
- In the Trends view, the HDX Insight data is available on Network tab. It gives the overview of the network details such as average bandwidth, latency, client jitter, ICA round trip time and additional network related details at the site level.
- The Network tab is enabled based on the XenDesktop license edition. The information shown from HDX Insight is based on the NetScaler license edition.

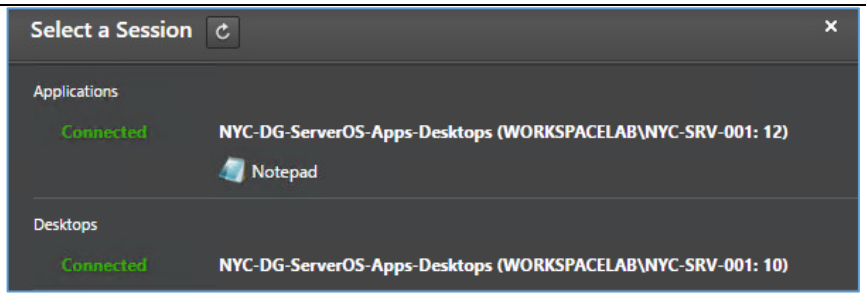
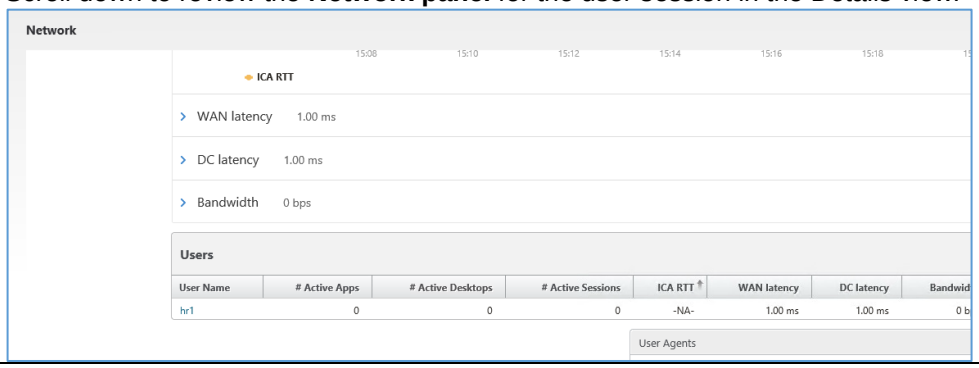
Exercise 13-14: View and Interact with the New User Details Page

Scenario:

Your task is to view the new network information section from the User Details page after integration of NetScaler Insight Services has been done.

Step	Action
1.	Using the Remote Desktop Connection Manager, switch back to **NYC-WRK-001**. **Note:** In a previous exercise, you had logged on to **NYC-WRK-001** using the following credentials to make the connection: user name: **WORKSPACELAB\HR1** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-WRK-001**, right-click this machine and choose **Connect server**.
2.	Verify that **Notepad** is still running, if not, launch Notepad again. Open **Internet Explorer** and browse to **https://nsg.workspacelab.com.** Log on with the following credentials: User name: **HR1** Password: **Password1** Launch the published **Notepad** application.

3.	Using the Remote Desktop Connection Manager, switch back to **NYC-FSR-001**. **Note:** In a previous exercise, you had logged on to **NYC-FSR-001** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-FSR-001**, right-click this machine and choose **Connect server**.
4.	Log back in to Director using the following credentials: User name: **Administrator** Password: **Password1** Domain: **Workspacelab**  Click **Log on**. **Note**: Director was launched in a previous exercise. If Director was closed in a previous exercise, then click the **Internet Explorer** icon on the desktop and browse to **https://nyc-fsr-001.workspacelab.com/Director**.
5.	Click **Search** on the top right of the Director page, type **HR1**, and select **(WORKSPACELAB\HR1)**.
6.	When prompted to select a session click on **Notepad**.

	
7.	Scroll to the right-hand side of the page, and click the **Details** button.
8.	Scroll down to review the **Network panel** for the user session in the Details view. 
9.	Click **Administrator** > **Log Off** Director.
10.	**Close** the running the Notepad application and logoff NetScaler page.

Key Takeaways:

- The HDX Insight data on Director is shown in two locations with different views; on the Trends view and the User Details view.
- To quickly analyze the network health, the chart provides a summary showing the average network metrics per time selection.
- The list of Users contains a list of users who have accessed the environment within the time selected. Metrics such as latency, number of application launches, ICA RTT, Bandwidth, and jitter are provided on a per user basis.
- Admins can drill down on a per user basis for network metrics relevant to that user.

Module 14: Troubleshooting

Overview:

This module presents an introduction to supporting the XenApp and XenDesktop Site with Citrix Supportability tools. Your Citrix Lead Architect, having reviewed your completed XenApp and XenDesktop POC deployment, has given you some final tasks to test some troubleshooting tools.

Before you begin:

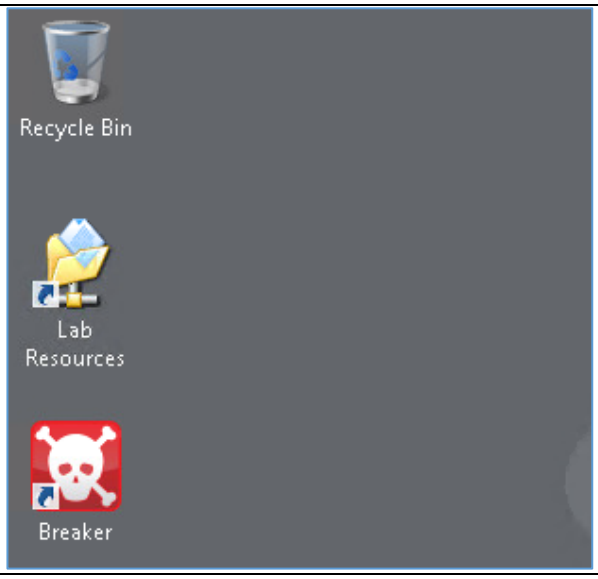
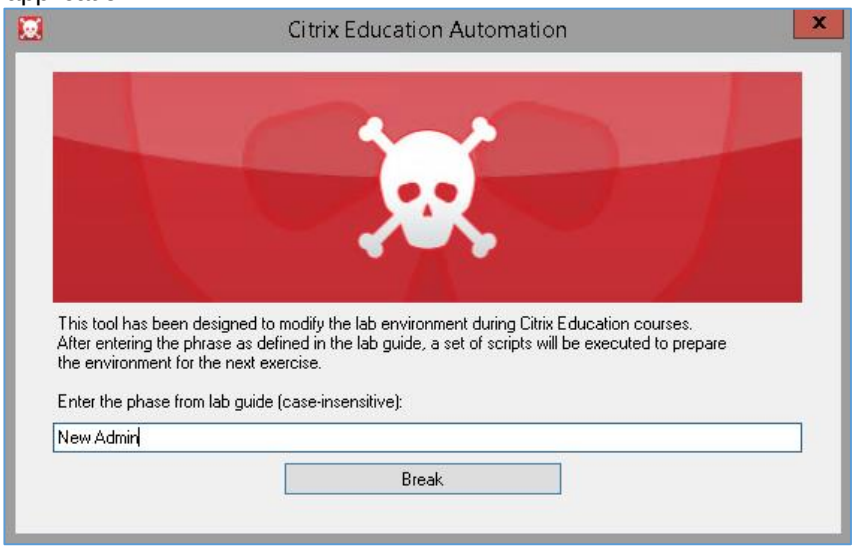
Estimated time to complete this lab: 60 minutes

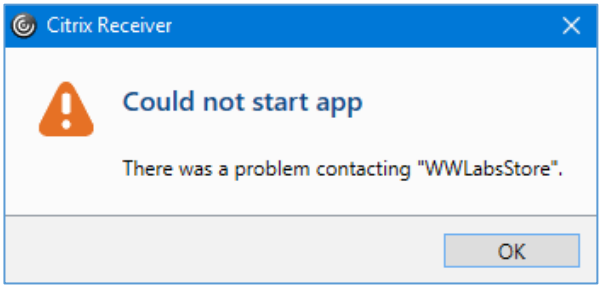
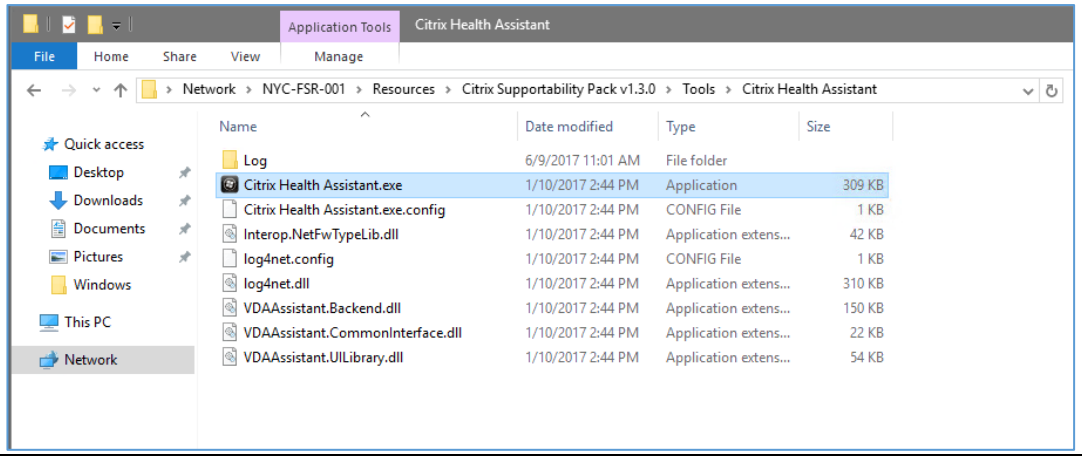
Exercise 14-1: Leverage the Citrix Supportability Pack and use the Citrix Health Assistant

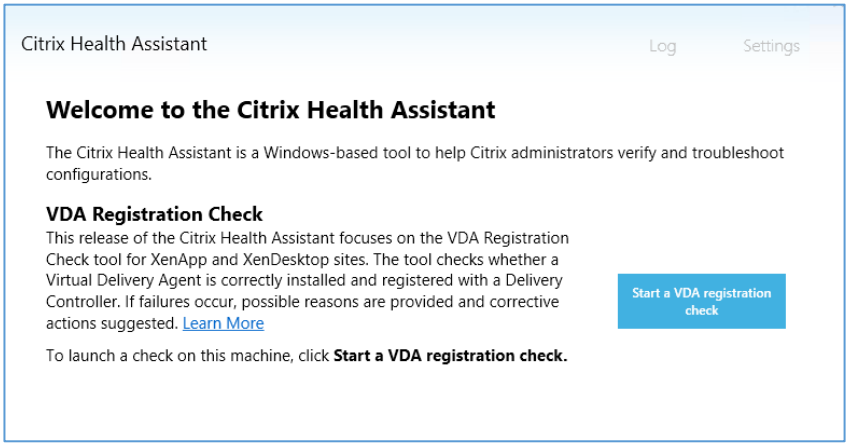
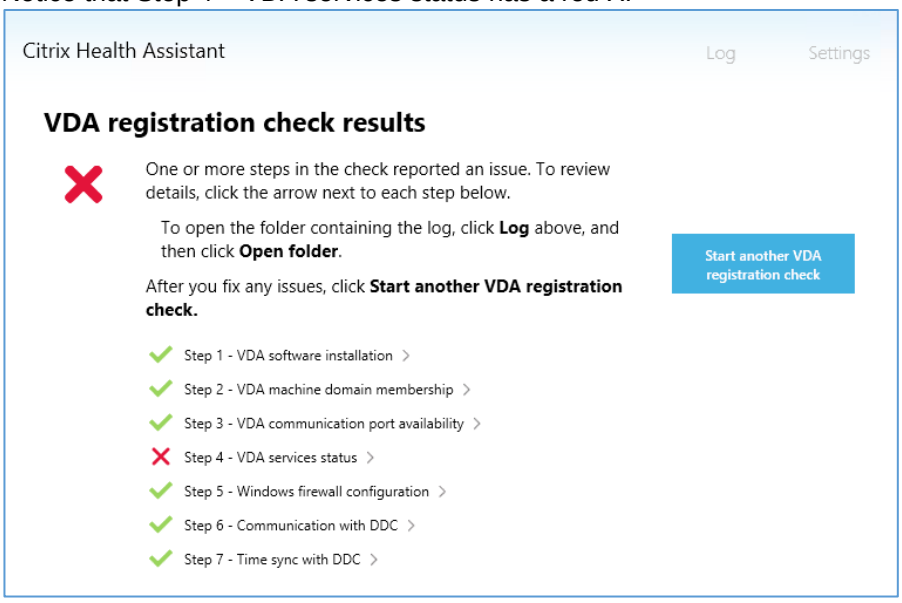
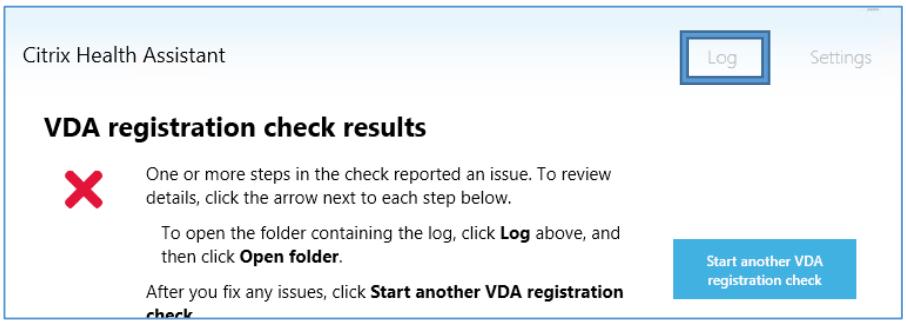
Scenario:

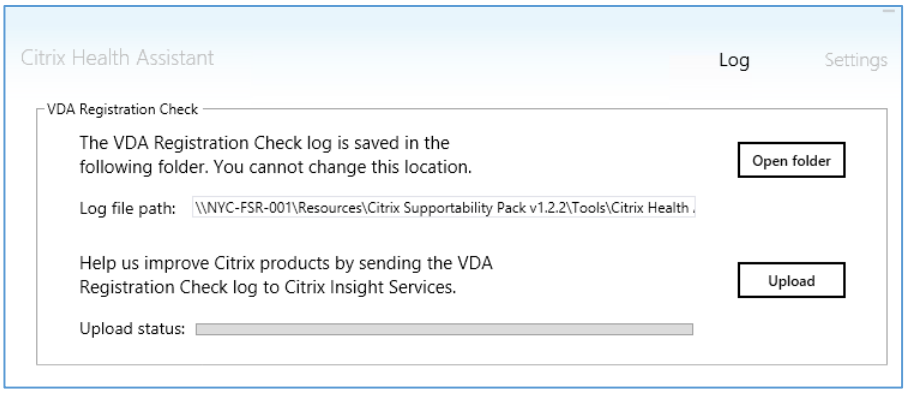
Your task is to run a pre-configure *Breaker App* in the environment which "breaks" something. Using the Citrix Health Assistant, you will then walk through steps to isolate the issue and fix what was "broken".

Step	Action
1.	The following VMs are required before beginning the exercises for this Module; all others may be powered down. To power manage your VMs, switch to XenCenter, right-click on the VM in the left pane and select Start or Shut Down. If prompted click Yes. • NYC-ADS-001 • NYC-SQL-001 • NYC-FSR-001 • NYC-VNS-001 • NYC-NIC-001 • NYC-XDC-001 • NYC-XDC-002 • NYC-STF-001 • NYC-STF-002 • NYC-SRV-001 • NYC-WRK-001 **Note**: These above VMs are listed in the start-up order.
2.	Using the Remote Desktop Connection Manager, connect to **NYC-XDC-001**. To log on to NYC-XDC-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password.
3.	Double-click the **Breaker** icon on your desktop.

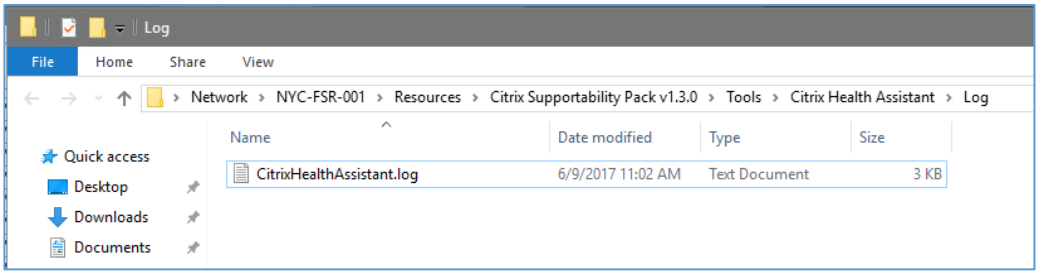
	
4.	Enter the following text **New Admin** and click on the **Break** button. Wait for confirmation that changes have been applied, and then click **OK** in the confirmation window. Then **close (X)** the Breaker application.  **Note:** Breaker is an application that is modifying the lab environment for the current lab exercise. Instead of a completely broken lab environment with multiple issues, you will start with a fully functional environment, and problems will be introduced one at a time.
5.	Using the Remote Desktop Connection Manager, connect to **NYC-WRK-001**. To log on to NYC-WRK-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: user name: **WORKSPACELAB\HR1** with **Password1** as the password.
6.	Log on to **Citrix Receiver** with the following credentials: User name: **HR1** Password: **Password1** Launch the **HR Desktop**

	HR Desktop **fails** to launch. Click **OK** on the error message.  **Note**: The error message appears after you are logged on. It may take few minutes for the error message to appear, while launching a published Desktop. You can log on to Receiver and enumerate your applications. You suspect the problem must be somewhere else; maybe the VDA registration?
7.	Log off **Citrix Receiver**. Click **HR1** and **Log Off**.
8.	Using the Remote Desktop Connection Manager, connect to **NYC-SRV-001**. To log on to NYC-SRV-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password.
9.	Right-click **Start** and select **Event Viewer**. Expand **Windows Logs** and review the **Application**, **Security**, and **System** event logs. Take note of any errors or warnings that come from Citrix and are close to the time that the breaker application was executed on step 3.
10.	From the desktop of **NYC-SRV-001** double-click the **Lab Resources** share. Browse to **\\NYC-FSR-001\Resources\Citrix Supportability Pack v1.3.0\Tools\Citrix Health Assistant** and double-click **Citrix Health Assistant.exe**. 

11.	Click **Start a VDA registration check**.  Notice that Step 4 – VDA services status has a red X.  To review the details, click the **arrow** next to Step 4. Service Citrix Desktop Service is not running.
12.	Click **Log** on the top right of the Citrix Health Assistant.  Click **Open folder** to view the Log.

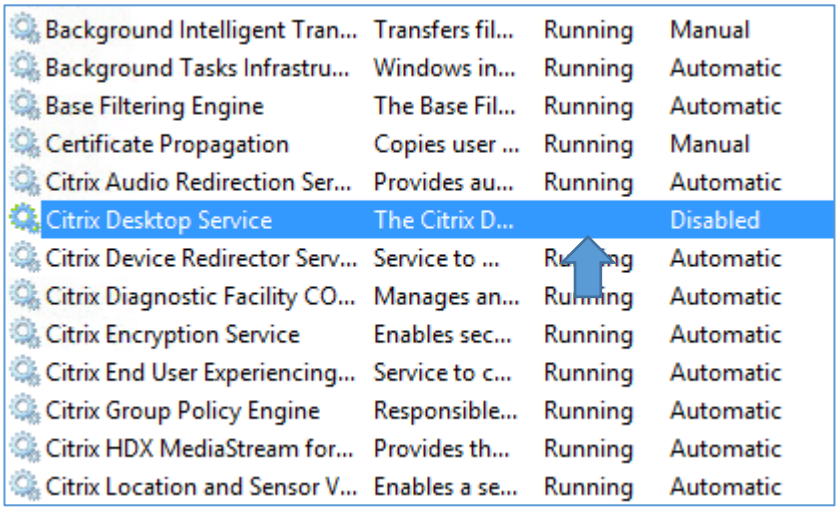


Double-click **CitrixHealthAssistant.log**.



13. From the NYC-SRV-001, click **Start** and type **Services.msc**. Then click **Services** from the list.

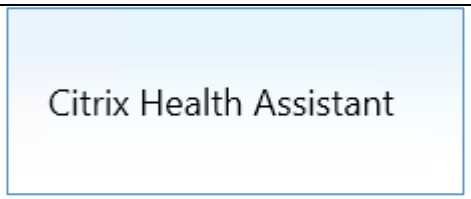
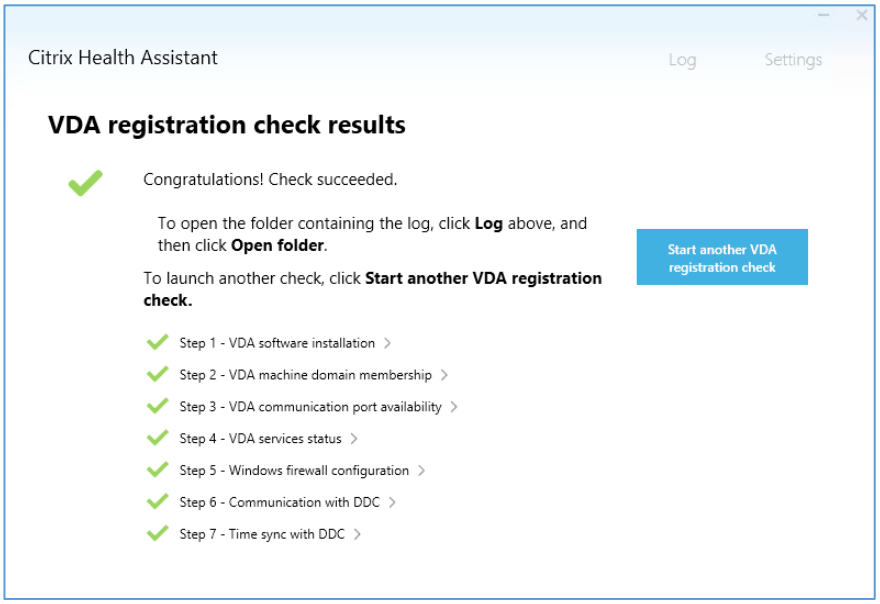
14. Locate the **Citrix Desktop Service**. Notice that this service is not running.



Right-click this service, select **Properties** and set the service Startup type to **Automatic**; click **OK**. Right-click the service again and click **Start**.

15. Return to the Citrix Health Assistant tool.

Click on the **Citrix Health Assistant** heading to return to the home page.

	 Click **Start another VDA registration check**.  Notice that all steps pass with a **green** check mark.
16.	Using the Remote Desktop Connection Manager, switch back to **NYC-WRK-001**. **Note:** In a previous exercise, you had logged on to **NYC-WRK-001** using the following credentials to make the connection: user name: **WORKSPACELAB\HR1** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-WRK-001**, right-click this machine and choose **Connect server**.
17.	Log on to **Citrix Receiver** with the following credentials: User name: **HR1** Password: **Password1** Launch the **HR Desktop**. The HR Desktop launches successfully. **Log off** the Desktop and then **Log Off** Receiver. **Note:** If the Desktop does not start in the first attempt, wait for a few seconds and try again. It takes a few seconds to re-register with the Delivery Controllers.

Key Takeaways:

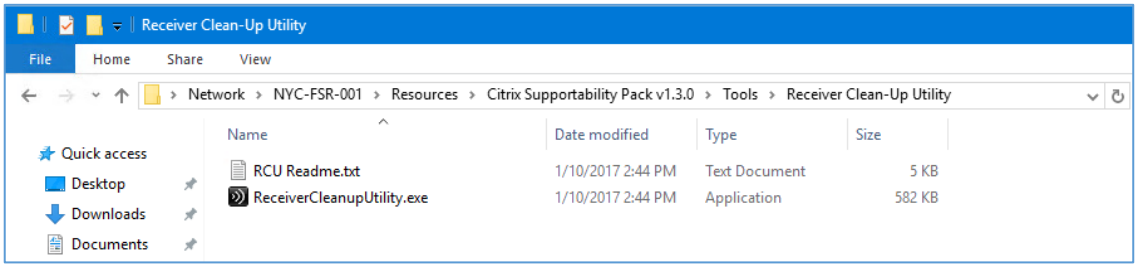
- The tool conducts the following health checks on a VDA, and reports results in the UI as well as in the log file:
    1. VDA software installation
    2. VDA machine domain membership verification
    3. VDA communication ports availability
    4. VDA services status
    5. Windows firewall configuration
    6. VDA communication with Delivery Controllers
    7. VDA time sync with each Delivery Controller
- Pre-requisites for the tool include Windows 7 or newer with .Net 3.5.1 or higher installed, and Citrix XenDesktop or XenApp 7.0 VDA or newer.

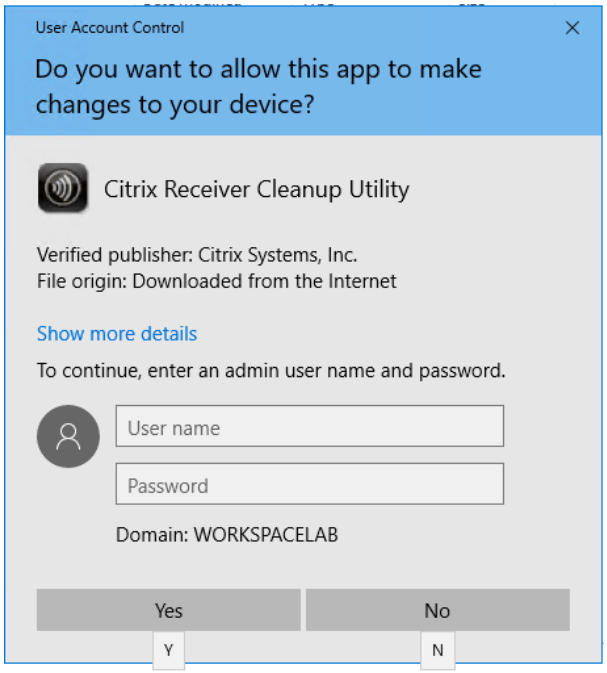
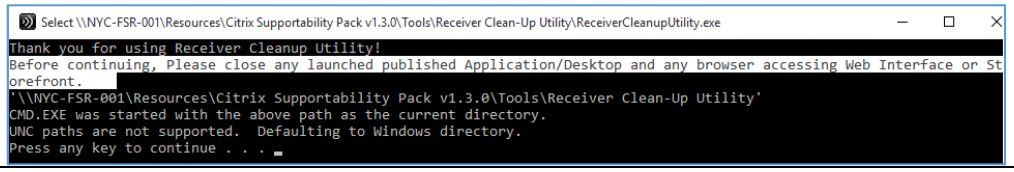
Exercise 14-2: Leverage the Citrix Supportability Pack and use the Citrix Receiver Clean-Up Utility

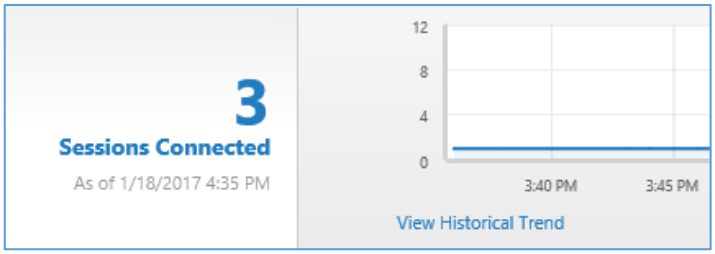
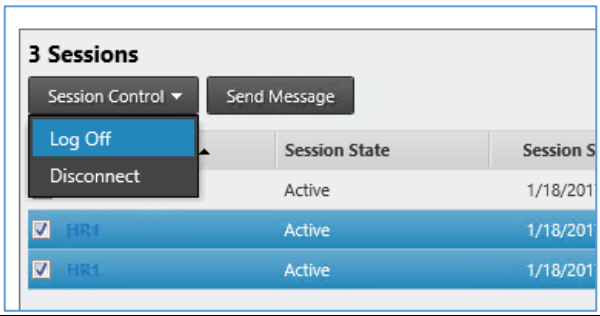
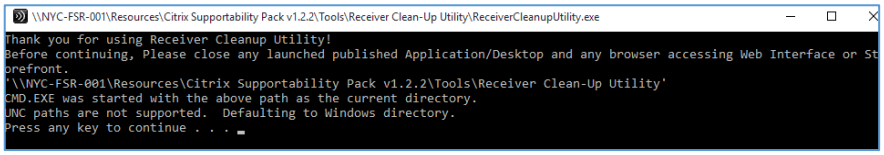
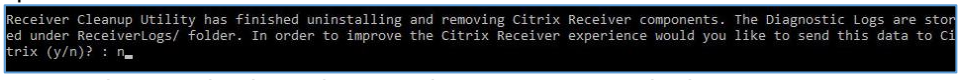
Scenario:

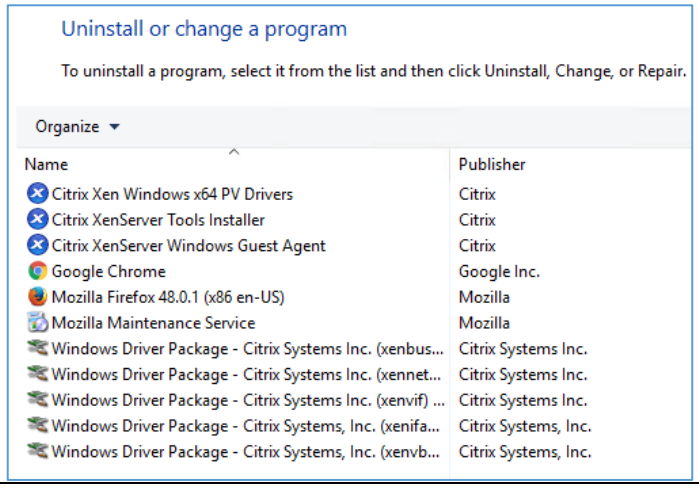
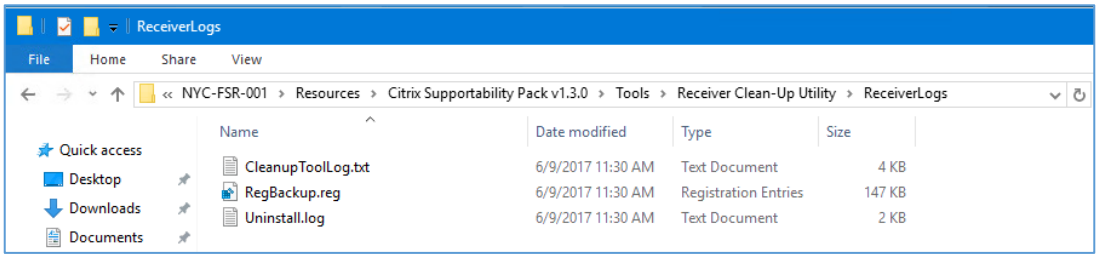
You are working with a user that is experiencing issues launching their Citrix resources. The user is successfully able to log on to StoreFront, but when they click on their HR Desktop, nothing happens. You verify that this user does not have the latest version of Receiver installed.

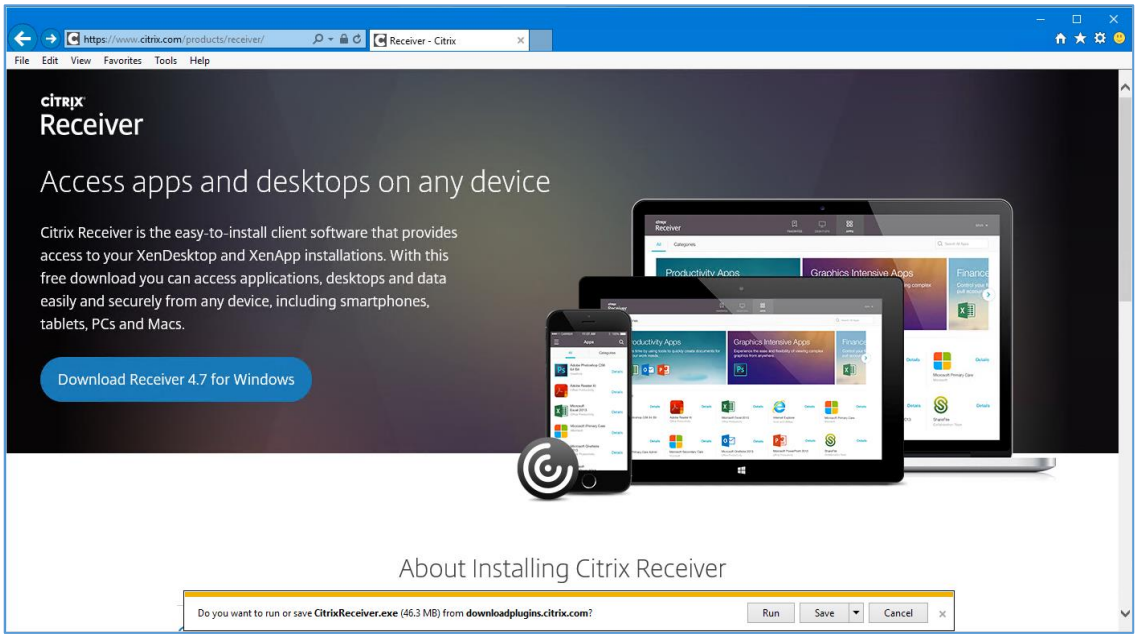
Your task is to help the user get the latest version of Citrix Receiver installed.

Step	Action
1.	Using the Remote Desktop Connection Manager, disconnect from **NYC-WRK-001** and then reconnect as **Administrator**. To log on to NYC-WRK-001 as Administrator, right-click this machine and choose **Connect Server as,** click the **Profile drop-down list** and select **WORKSPACELAB\Administrator.** Click **Connect**. **Note:** The following credentials are used to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password.
2.	Log on to **Citrix Receiver** with the following credentials: User name: **HR1** Password: **Password1** Launch the **HR Desktop**.
3.	On **NYC-WRK-001**, launch **File Explorer** and browse to **\\NYC-FSR-001\Resources\Citrix Supportability Pack v1.3.0\Tools\Receiver Clean-Up Utility**. Right-click **ReceiverCleanupUtility.exe** and select **Run as administrator**.  When prompted for User Account Control, use the following credentials:

	User name: **Administrator** Password: **Password1**  **Note:** The Receiver Clean-up Utility deletes all known locations within the file-system and the registry, without depending on a successful installation of any Receiver / online-plugin. This makes it usable even after canceled installation attempts resulting in corrupted installations of the product. For example, a blue-screen or power outage occurring during installation. Refer to **http://support.citrix.com/article/CTX325140** for a list of locations that the tool modifies.
4.	After starting the Clean-up Utility, you are asked to first quit all running published applications and close all Web Interface or StoreFront sessions, to ensure that the program you want to remove is not actually in use during removal. 
5.	Using the Remote Desktop Connection Manager, connect to **NYC-FSR-001**. To log on to NYC-FSR-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password.
6.	Click the **Internet Explorer** icon on the desktop and browse to **https://nyc-fsr-001.workspacelab.com/Director**. Log on to **Director** with the following credentials: User name: **Administrator** Password: **Password1**

	Domain: **Workspacelab** Click **Log on**.
7.	On the **Dashboard** click the blue number over **Sessions Connected**. 
8.	On the **Filters – All Connected Sessions** page, select all instances of **HR1** and then click **Session Control > Log Off**. 
9.	Using the Remote Desktop Connection Manager, switch back to **NYC-WRK-001**. **Note:** In a previous exercise, you had logged on to **NYC-WRK-001** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session disconnected, log on to **NYC-WRK-001**, right-click this machine and choose **Connect server**.
10.	Return to the **Clean-up Utility** task. Now that you have confirmed there are no active connections to session from NYC-WRK-001, follow the prompt on the screen: “Close all running remote sessions, if necessary, and then start the clean-up process by pressing **any key**.”  Once the clean-up process completes, you must decide if you want the log files of the removal operation to be sent to Citrix.  Answer the question by typing **N** and press **Enter** to submit your answer. Then **exit** the command window by pressing any key.

	Note: Citrix recommends customers to consider sending the data to Citrix to assist in making improvements to future versions of this product. You have reported this recommendation to the Citrix Lead Architect and he agrees to include this setting in the production environment scope, to be implemented following the results of this POC deployment.
11.	Right-click **Start** and select **Programs and Features**. Review the programs list to verify that the Citrix Receiver is no longer listed. 
12.	Open the **ReceiverCleanupUtility** folder and browse to the subfolder **ReceiverLogs**. Review the log files that the tool has created under the folder from which it was executed.  Notice that the **uninstall.log** file lists all actions from the tool, while the **RegBackup.reg** contains a backup of all modified registry keys. **Note**: The RegBackup.reg can be opened for review using Notepad. **Note**: There is no backup of the deleted files. If the Receiver Clean-up Utility is run again, the process will overwrite all log files in the directory, including the backup of the registry.
13.	Perform a **Reboot** of the **NYC-WRK-001** machine to finish any pending installation or uninstallation tasks before trying to install any new Receiver version. Using **XenCenter**, in the left pane select **NYC-WRK-001**, right-click and choose **Reboot**, and click **Yes** to confirm.
14.	Using the Remote Desktop Connection Manager, connect to **NYC-WRK-001**. To log on to NYC-WRK-001 as Administrator, right-click this machine and choose **Connect Server as,** click the **Profile drop-down list** and select **WORKSPACELAB\Administrator**. Click **Connect**. **Note:** The following credentials are used to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password.

15.	Download and install a fresh Citrix Receiver from the Citrix website. Launch **Internet Explorer** and browse to **https://www.citrix.com/go/receiver**.  Click on **Download Receiver 4.7 for Windows** to download the installation package. Execute the **CitrixReceiver.exe** by clicking the **Run** option at the bottom of the browser page to install the new version of Citrix Receiver on the machine. **Note:** You may also see Citrix Receiver 4.8 for Windows in this step, please proceed with it.
16.	Press **Start** on the Welcome screen of the Citrix Receiver Installation to proceed to the next page.
17.	Read the license agreement and if you agree, **Accept** the License Agreement and click **Next** to **Install**.
18.	When the installation has completed successfully, click **Finish** to close the Installer.
19.	Using **XenCenter** in the left pane select **NYC-WRK-001,** right-click and choose **Reboot**. Then select **Yes** to confirm the reboot. **Note**: Click **Close** on the Citrix Receiver Add Account window, if it displays after the reboot.

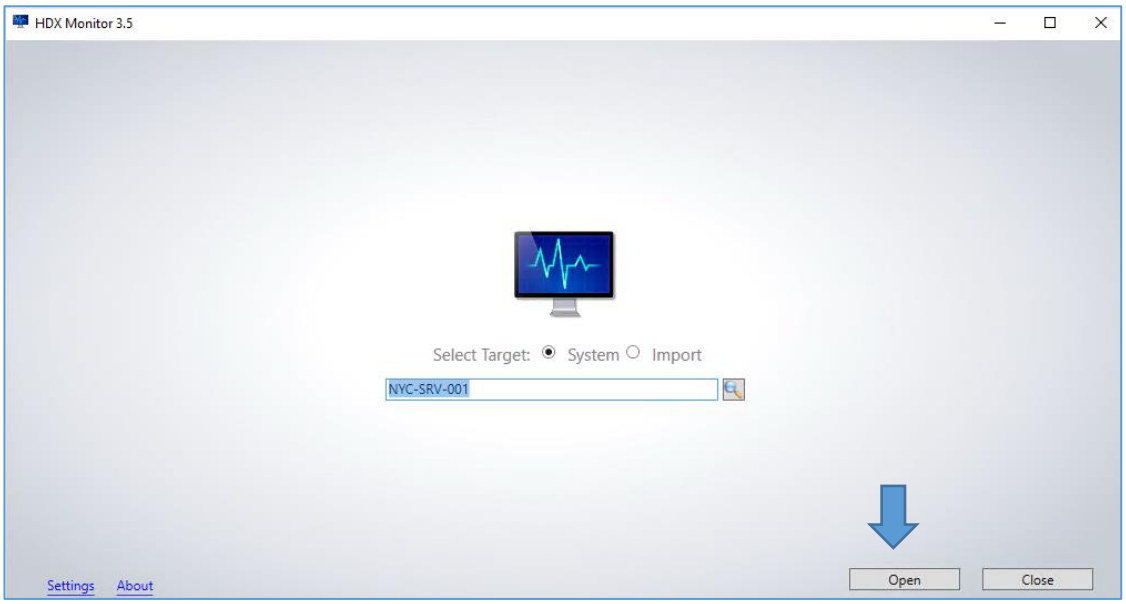
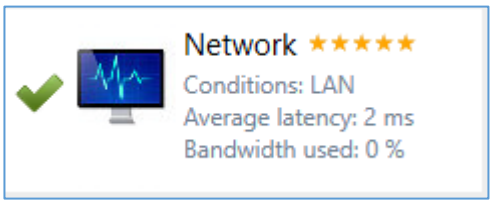
Key Takeaways:

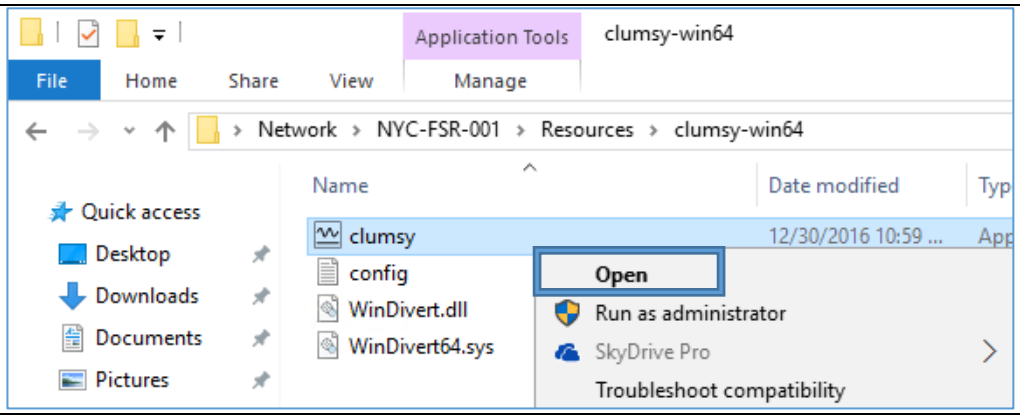
- The Receiver Clean-up utility can be used to help remove any files or registry entries left behind when an uninstall (or installation or upgrade) of the Citrix Receiver or plug-in fails to complete successfully.
- New Receiver versions can update certain older versions directly, while others require manual steps to be performed first.

Exercise 14-3: Leverage the Citrix Supportability Pack and use the HDX Monitor

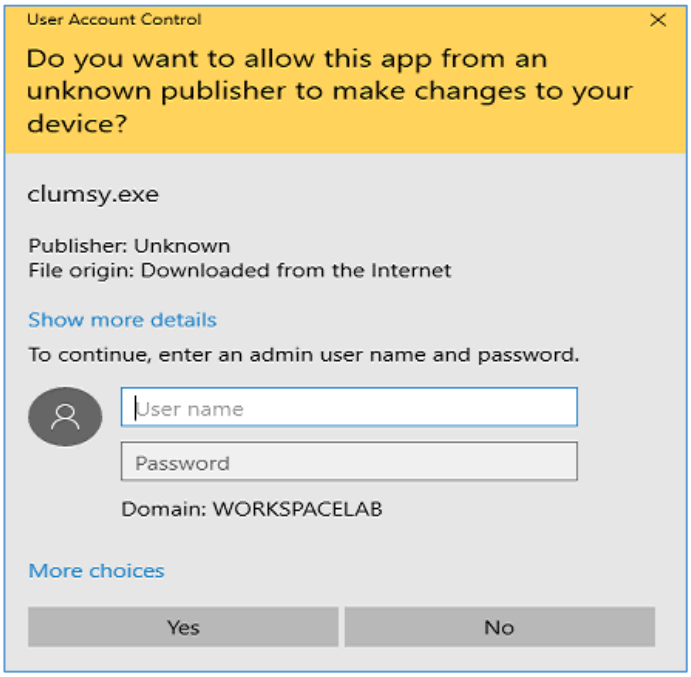
Scenario:

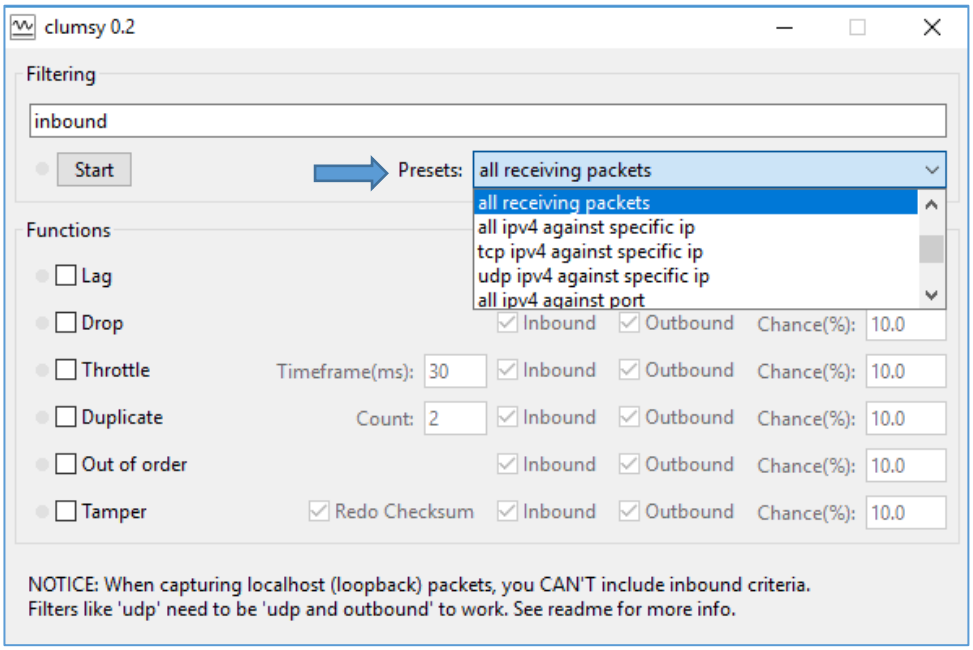
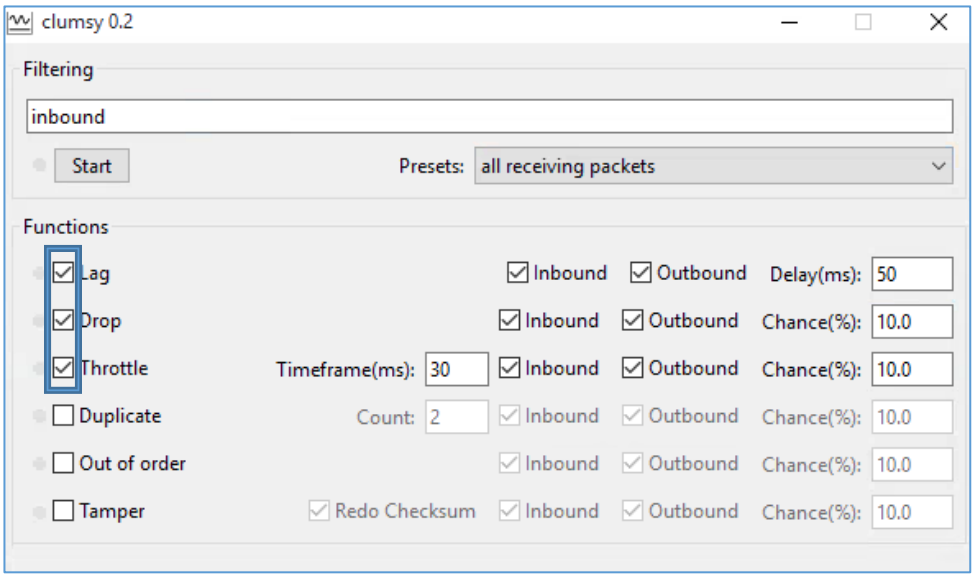
Your Citrix lead administrator has tasked you to test the HDX Monitor and report to him what the tool can be used for in terms of analyzing and troubleshooting user sessions.

Step	Action
1.	Using the Remote Desktop Connection Manager, connect to **NYC-WRK-001**. To log on to NYC-WRK-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: user name: **WORKSPACELAB\HR1** with **Password1** as the password.
2.	Click on the **Internet Explorer** icon on the desktop and browse to **https://storefront.workspacelab.com/Citrix/WWLabsStoreWeb/**.
3.	Log on as **HR1** and **Password1** and launch **HR Desktop**.
4.	From within the Hosted Desktop session, open **File Explorer** from the Taskbar. Browse to **\\NYC-FSR-001\Resources\HDX Monitor** . Double-click **Setup** to **launch** HDX monitor install wizard.
5.	On the Application Install - Security Warning, click **Install**.
6.	Verify that the **System** radio button is selected and click **Open**. 
7.	Look at the **Network** details to see the Condition and Average latency in the environment.  Network Shows: Condition: **LAN** and Average latency is low.
8.	To create network latency and to monitor it using HDX monitor, access **clumsy.exe** tool from **\\NYC-FSR-001\Resources\clumsy-win64**.
9.	Right-click the application and select **Open**.

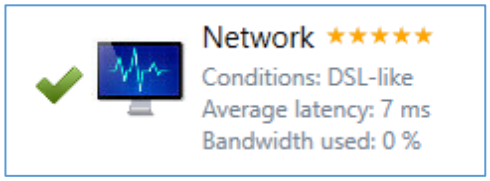


10. On the **User Account Control** warning message, log on with the following credentials: User name: **Administrator**, Password: **Password1** and click **Yes**.

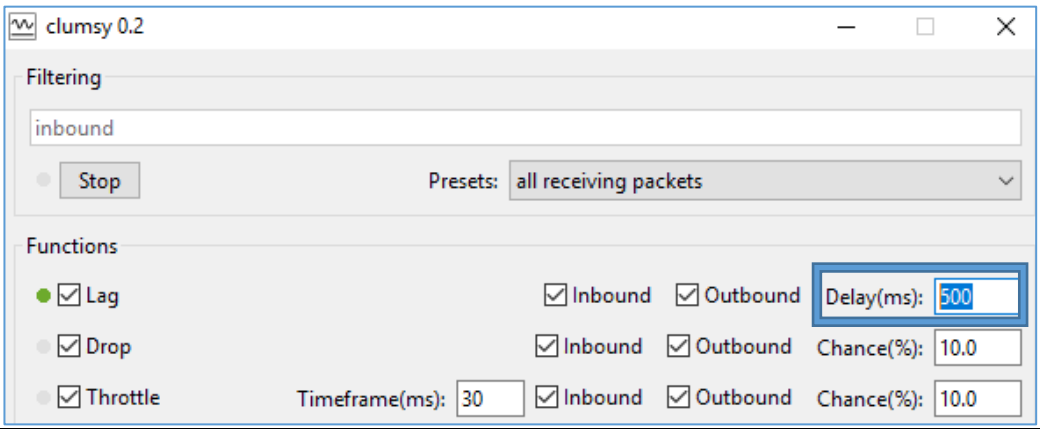


11.	Clear the existing filtering and select **all receiving packets** from the **Presets** drop-down. 
12.	Select **Lag**, **Drop** and **Throttle** check boxes, while keeping other settings as default.  Click **Start**.
13.	Switch to the HDX monitor window.

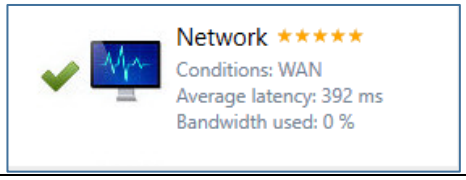
Now look at the HDX monitor network details again, and wait for few seconds to see that average latency increases, but network condition still says LAN.



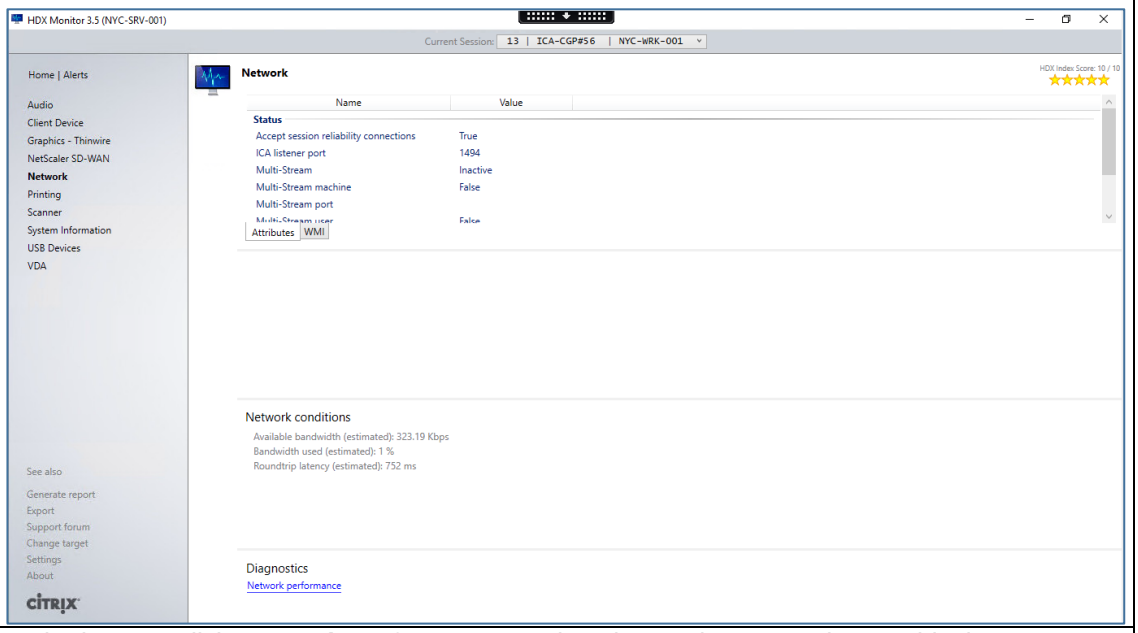
14. Now go back to Clumsy tool and increase the Delay for Lag to **500**.



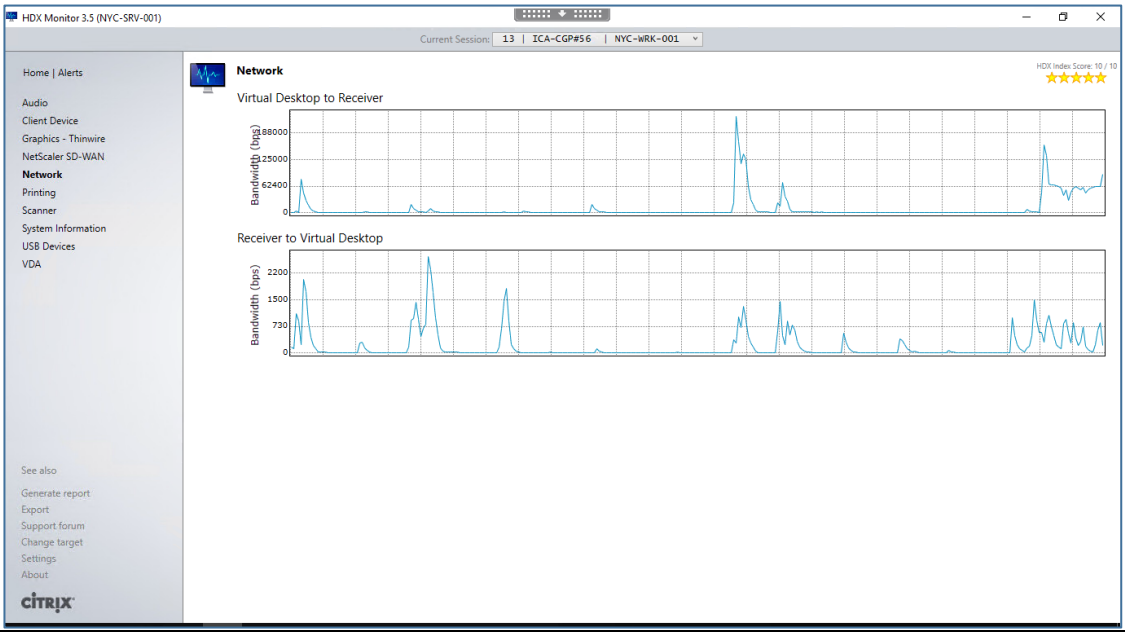
15. Wait for a few seconds and now monitor the network health and you will see that **Average latency** has increased considerably and **Condition** has changed to WAN.



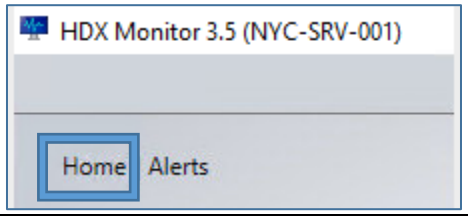
16. Click on **Network** and then look at the network attributes on which information is being collected (like ICA listener port, Multi-Stream etc).

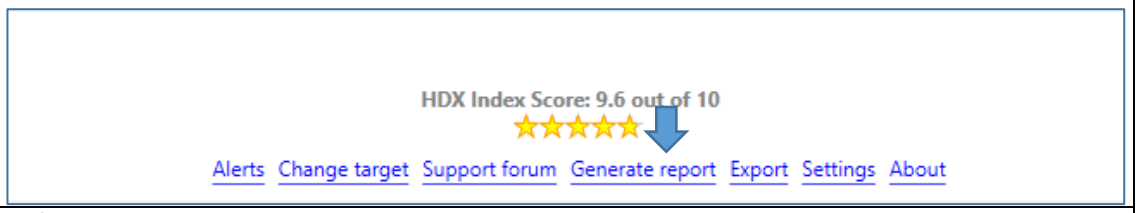
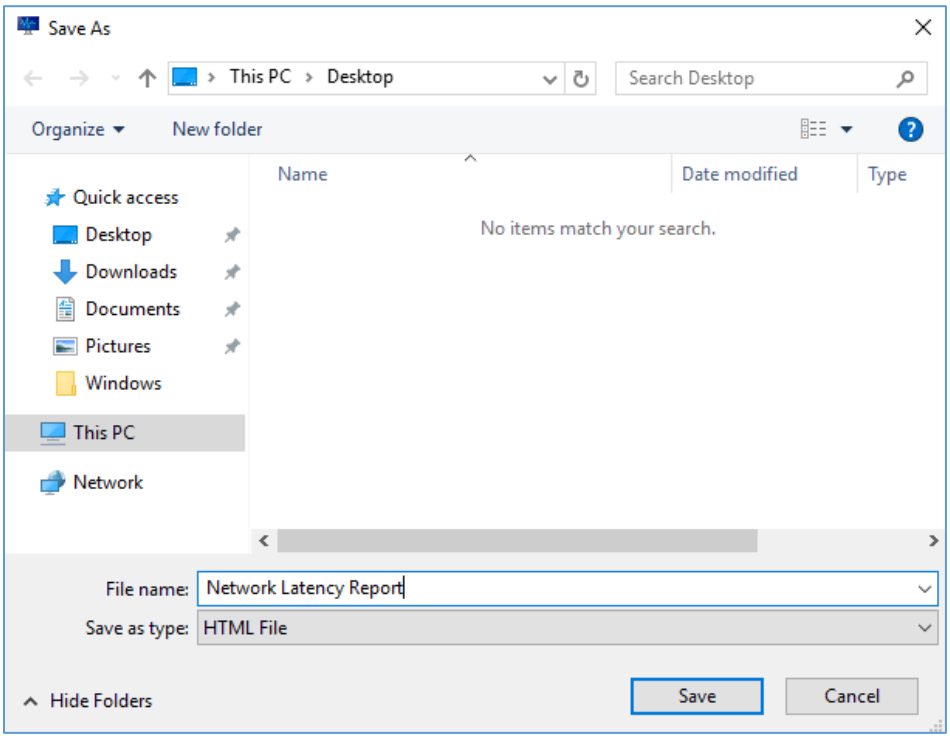


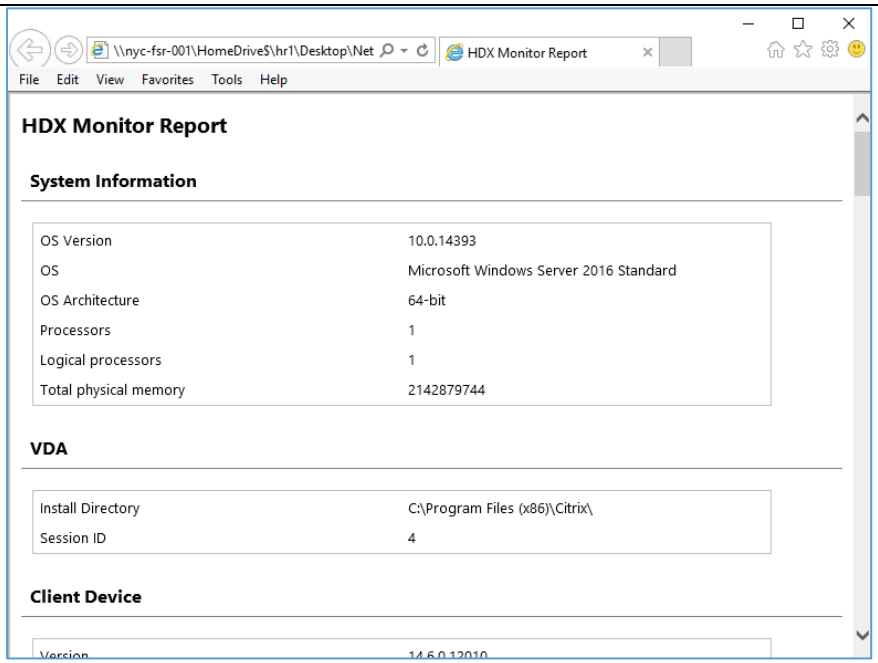
17. At the bottom, click **Network performance** under Diagnostics to see the graphical representation of the network condition.



18. Click **Home** to return to the Home screen of HDX monitor.

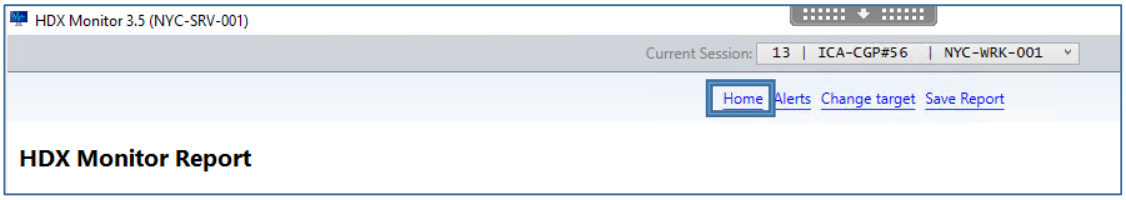


19.	To generate the report of the currently collected data, click **Generate report** at the bottom of HDX monitor screen. 
20.	Select **Save report**. Select **Desktop** and name the report **Network Latency Report**.  Click **Save**.
21.	Click **Stop** and then **Close** Clumsy 0.2 window. Double-click **Network Latency Report.html** on the Desktop and review the report.

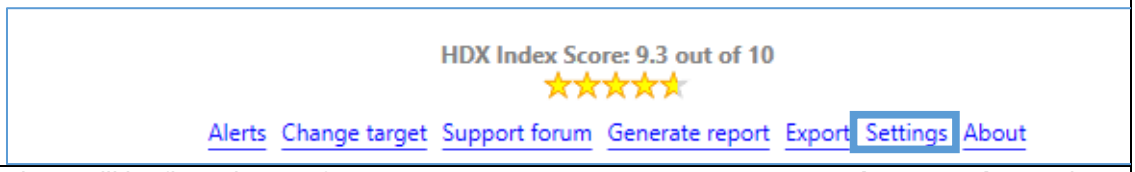


Close the browser to exit the report.

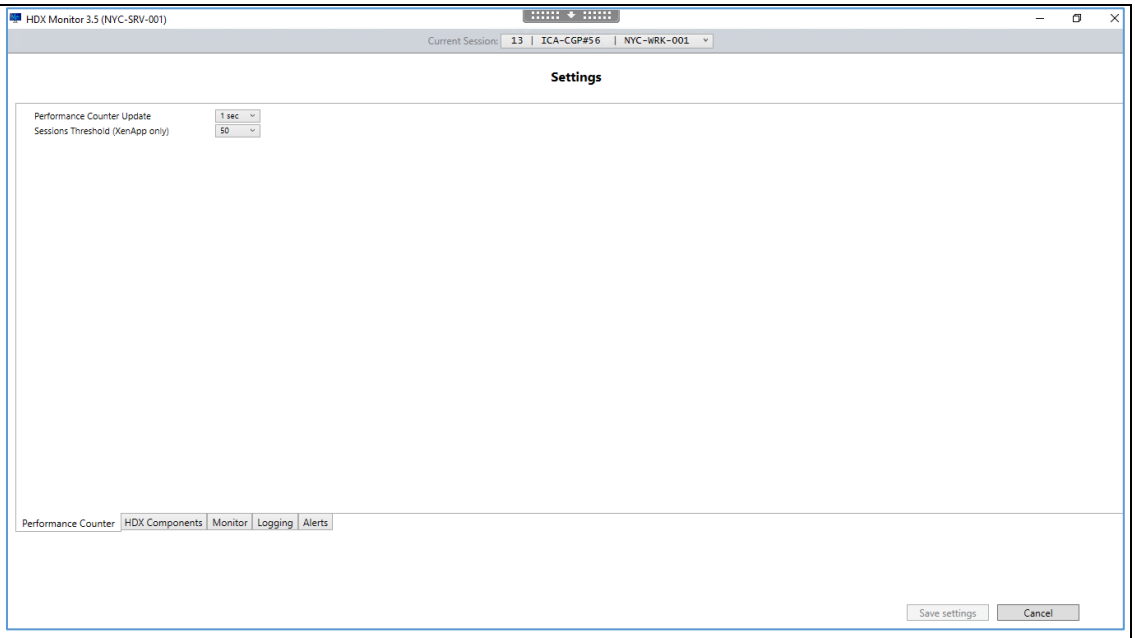
22. Switch to the **HDX Monitor** window and select **Home**.



Select **Settings** from bottom of the page



23. There will be five tabs: **Performance Counter, HDX Components, Monitor, Logging** and **Alerts**.

	 • **Performance Counter**: It will show the refresh rate at which data is pulled from the performance counters. • **HDX Components**: It will show all the components which are monitored and refresh interval rate. • **Monitor**: It provides an option to customize the protocol used to gather HDX monitor data. • **Alerts:** It will show the default Alerts that can be selected for Alert Monitoring. • **Logging:** It lets the user set a custom name for the log files gathered using HDX monitor.
24.	Click **Cancel** and return to home page. **Close** the HDX monitor.

Key Takeaways:

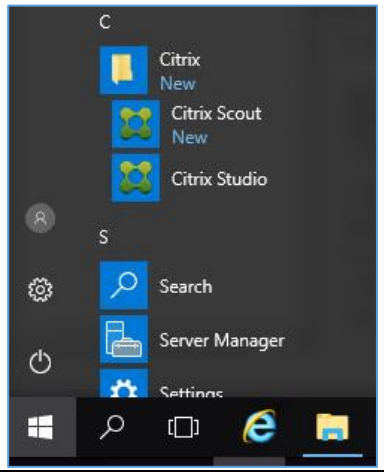
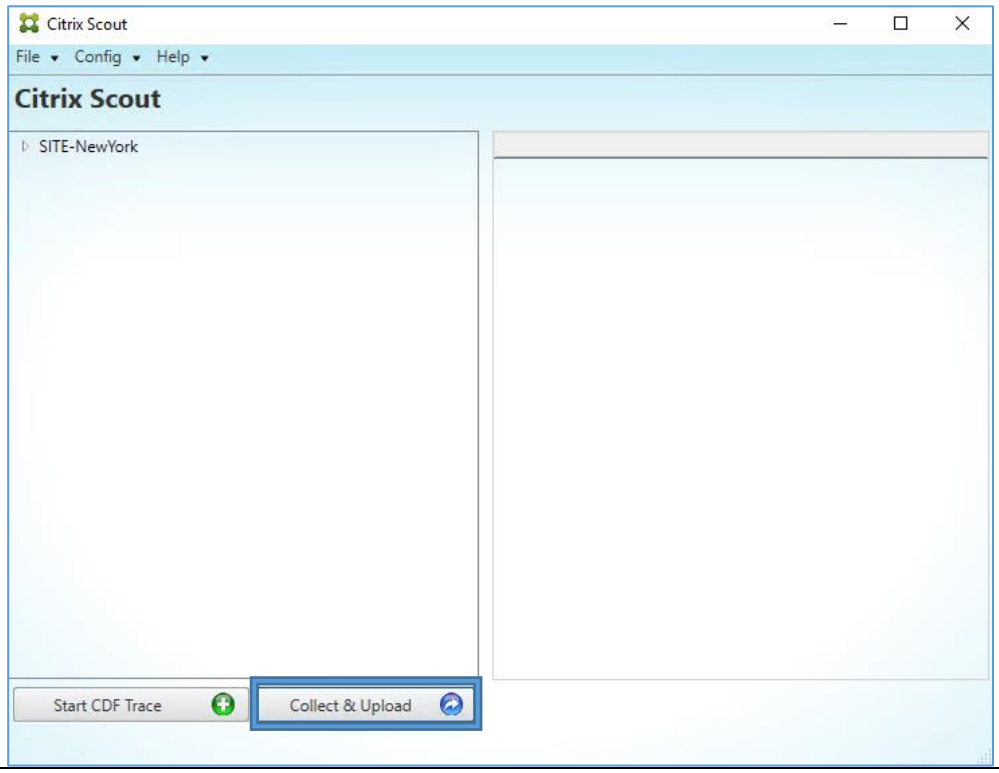
- HDX Monitor can provide insight into running session performance and capabilities in real-time.
- HDX Monitor is a great starting point for troubleshooting user experience issues that could be related to network latency or poor bandwidth.
- HDX Monitor provides reporting capabilities so findings can be analyzed at a later time.

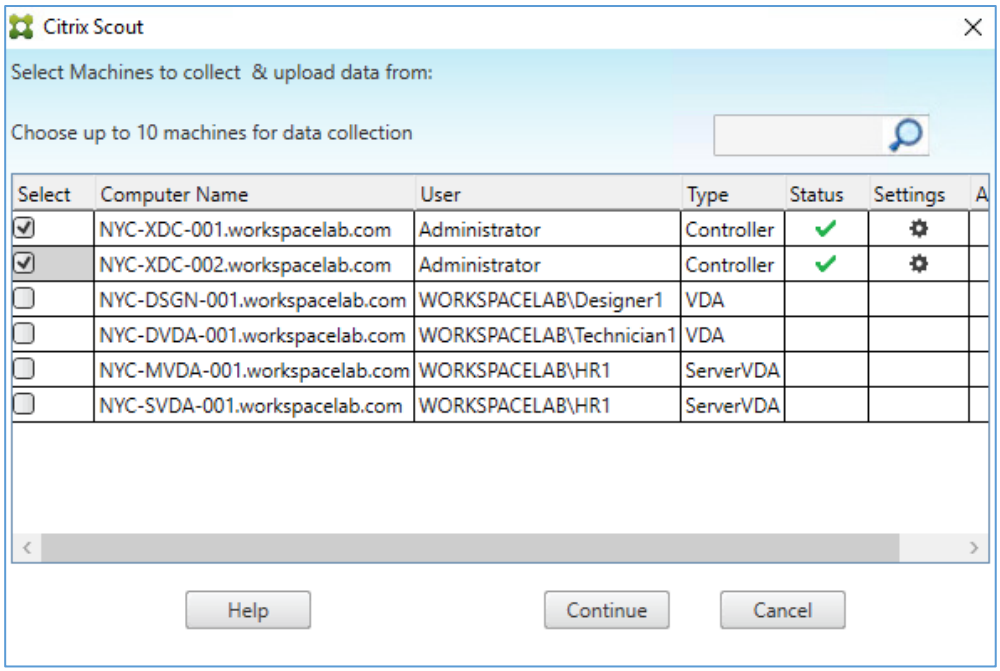
Exercise 14-4: Leverage the Citrix Supportability Pack and use the Scout Utility

Scenario:

The Citrix Lead Architect has tasked you to test the Scout Utility from the Citrix Supportability Pack, you decide to collect data from NYC-XDC-001 and NYC-XDC-002 and upload this set of data to Citrix Insight Services to evaluate how both tools can be used to assist in troubleshooting and support.

Note: This final exercise is optional.

Step	Action
1.	Using the Remote Desktop Connection Manager, connect to **NYC-XDC-001**. To log on to NYC-XDC-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password.
2.	On the Start menu, expand the Citrix folder and click **Citrix Scout**. 
3.	Click **Collect & Upload** on the bottom of the Scout tool. 
4.	Under Select, **enable** both NYC-XDC-001 and NYC-XDC-002 in the list to collect data from. The status column will have a green check mark.



Click **Continue**.

5. Once the tool has finished collecting data, it must be saved. On the Save As window click the **Desktop** and then click **Save**.

6. After the tool saves the zip file, you are asked to upload the file to the Citrix Insight Services site for analysis.

   Read the CIS information and if you agree with the Citrix Data Collection & Privacy Policy click **Continue**.

   Note: You can review the Privacy Policy by clicking on the section that states **Here** on the CIS dialog box.

7. To upload the data to CIS you will need to enter login information for My Citrix.

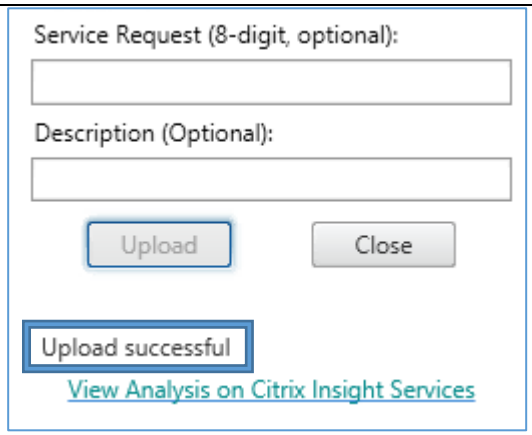
   Note: This login is the same login you used when accessing the Student Resource Kit (SRK) link to access this course via training.citrix.com and clicking on the My Training tab.

   Once the login details are defined click **Upload**.

   Note: On the first time an account uploads data, you will see a Data Collection dialog box. Read the Data Collection and Privacy policy and if you agree click **Agree**.

   Note: If you do not have the login details you can click **Don't have any** so you can create an account. Also, note that this exercise is optional and uploading data is not required.

8. You will see an Upload successful message at the bottom of the Upload to **https://cis.citrix.com** dialog box.

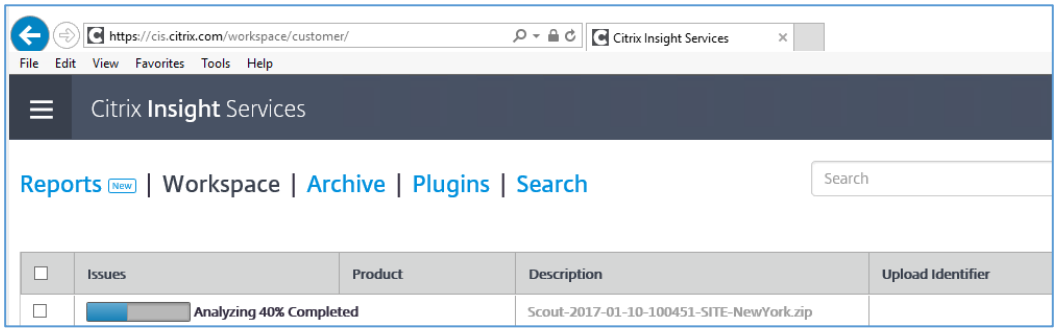


Under the Upload successful message, you can click **View Analysis on Citrix Insight Services**.

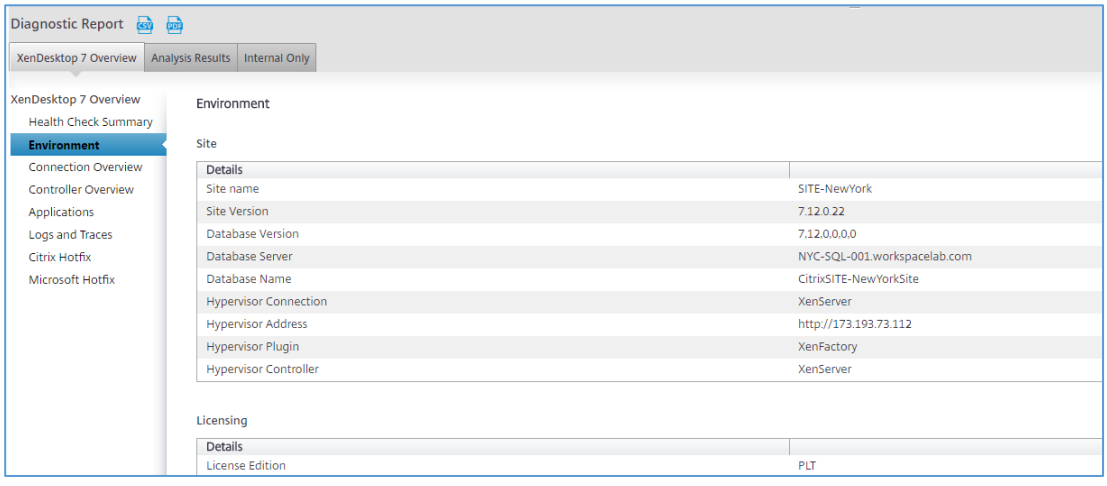
9. A browser window will open with a logon page for Citrix insight Services.

Log on with the same account information to review your uploaded data. Click on **Citrix insight Services > Diagnostics**.

Note: After logon you may see a Getting Started page, click **Get Started**.



Once the upload is finished, the Workspace page will show the results of the analysis.



Your screen may differ from the screen shot above, as not all environments will be the same.

	Note: The time it takes for the Citrix Insight Services to finish analyzing the uploaded data depends on the size of the data collected.

Key Takeaways:

- Run Citrix Scout from a single XenApp and XenDesktop Controller or VDA to capture key data points and CDF traces for selected computers; followed by secure and reliable upload of the data package to Citrix Technical Support.

Module 16: Provisioning Services Infrastructure.

Overview:

This module presents the steps to implement the initial Provisioning Services components to create a licensed Farm.

A Farm is the term used to represent the management scope of a Provisioning Services deployment. To create this Farm, we will address the following core tasks:

- Install the Provisioning Server role on a machine
- Configure a Provisioning Services Farm and create the Farm database
- Create and configure a shared vDisk Store

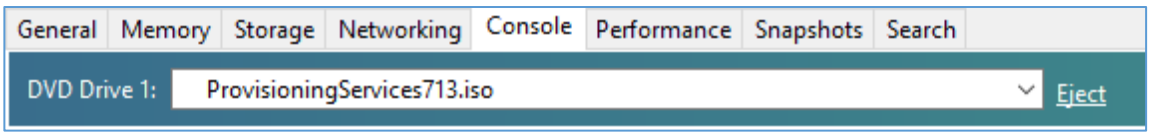
Before you begin:

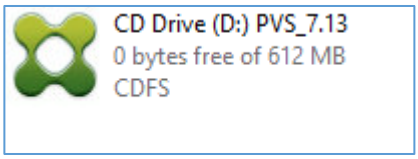
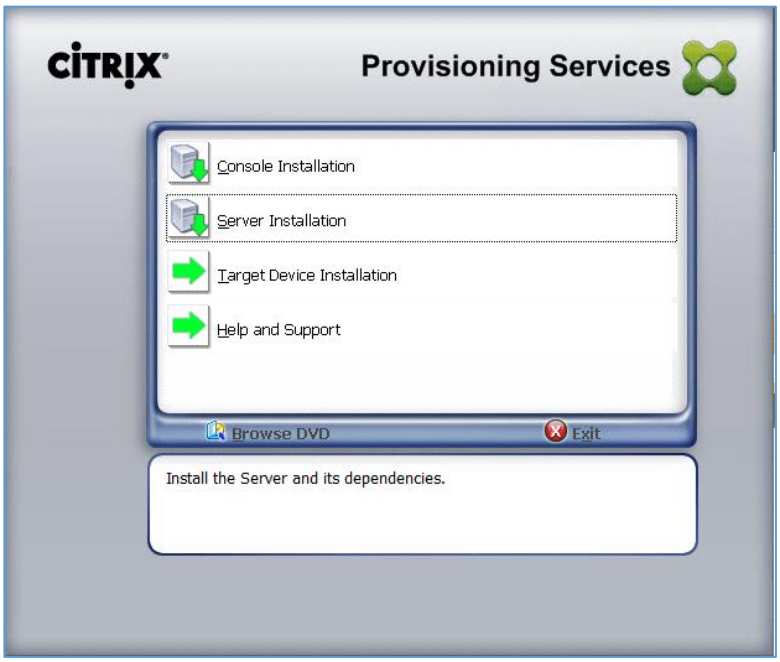
Estimated time to complete Module 16 lab exercises: 25 minutes

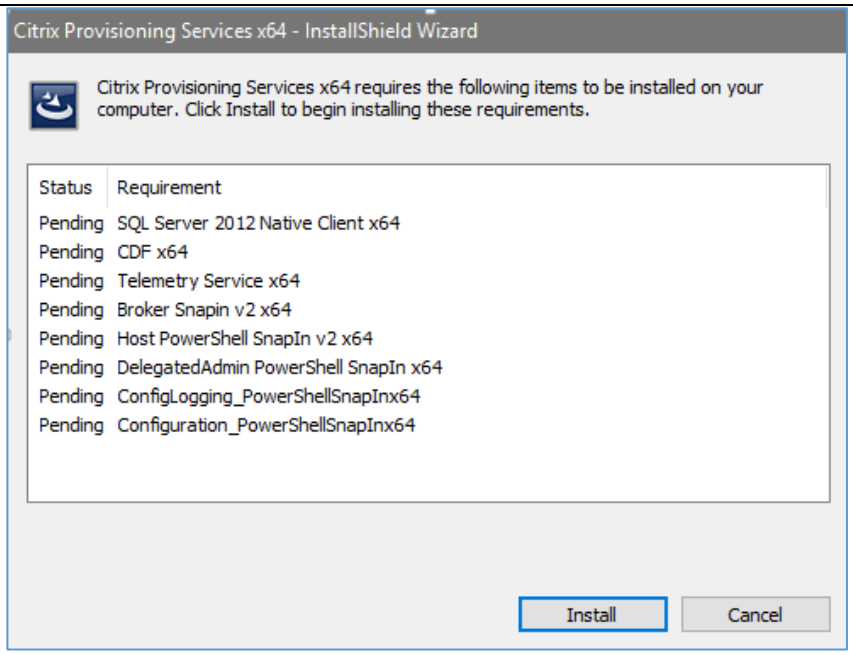
Exercise 16-1: Install Provisioning Services

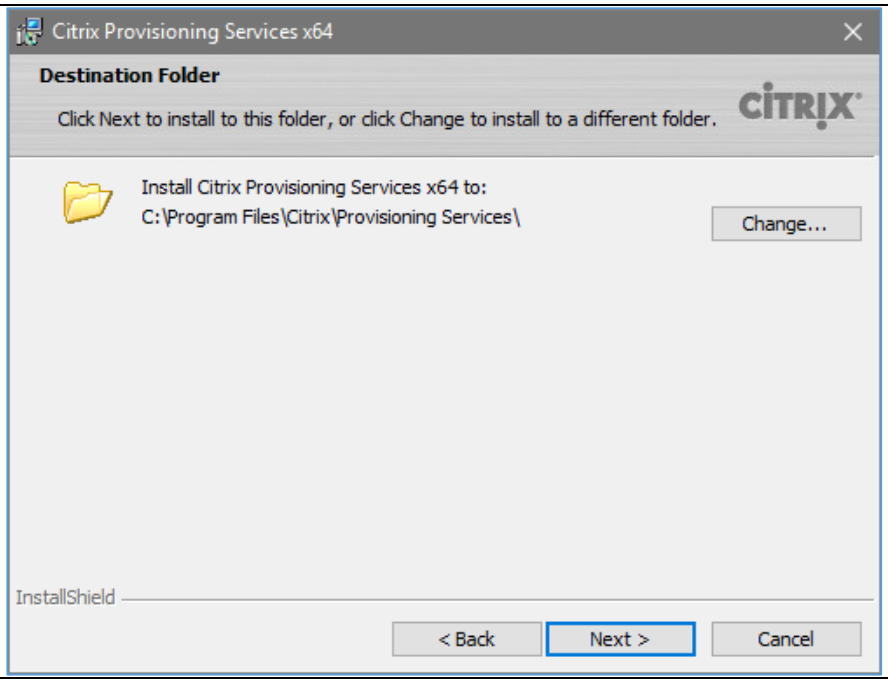
Scenario:

You are a Citrix Administrator at WW Labs, your Lead Citrix Architect has tasked you to deploy the Citrix Provisioning Services software and prerequisites to NYC-PVS-001. One of the junior team members have already configured Windows and joined the machine to the domain.

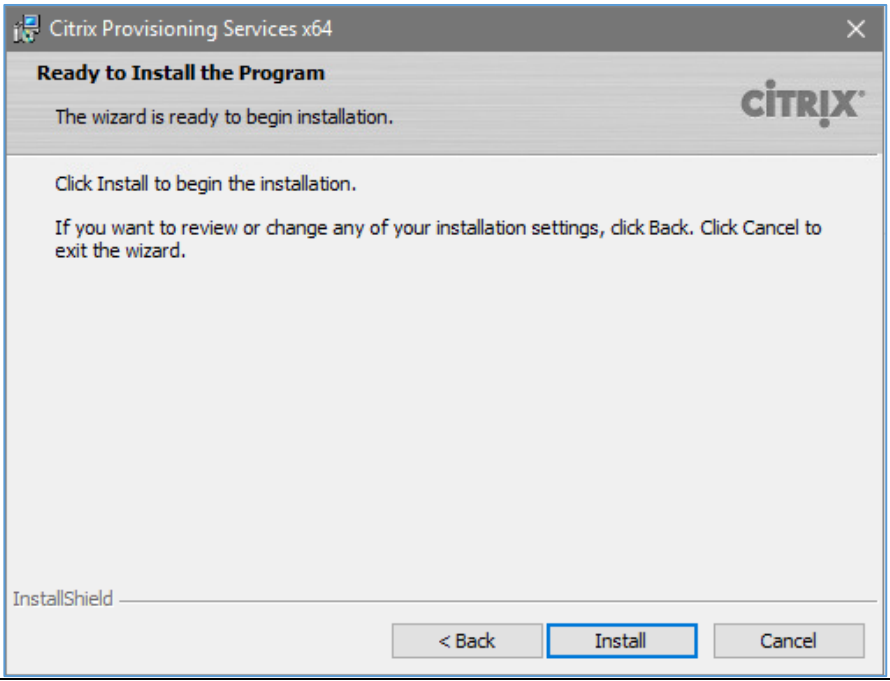
Step	Action
1.	The following VMs are required before beginning the exercises for this Module; all others may be powered down. To power manage your VMs, switch to XenCenter, right-click on the VM in the left pane and select Start or Shut Down. If prompted click Yes. • NYC-ADS-001 • NYC-SQL-001 • NYC-FSR-001 • NYC-PVS-001 **Note**: These above VMs are listed in the start-up order.
2.	Using **XenCenter**, mount the Provisioning Services installation media ISO to **NYC-PVS-001**. To mount the installation media ISO, select **NYC-PVS-001** in the left pane of XenCenter. In the right pane, select the **Console** tab. Using the **DVD-Drive 1:** drop-down menu, select **ProvisioningServices713.iso**.  **Note**: If there are no ISOs listed in the **DVD-Drive 1:** drop-down menu, then the Local ISO Storage Repository (SR) that contains the ISO library may need to be re-scanned. To perform the re-scan, select **Local ISO SR XS** from the left pane of XenCenter. Then, in the right pane select the Storage tab and click on the **Re-scan** button. This task may need to be repeated later in the course.

3.	Using the Remote Desktop Connection manager, connect to **NYC-PVS-001**. To login to **NYC-PVS-001,** right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the password.
4.	Click **File Explorer** in the taskbar. Click **This PC** and then double-click CD Drive (D:).  **Note**: If the main Provisioning Services menu screen does not launch after double-clicking the green Citrix logo, then double-click the **autorun.exe** file.
5.	Select **Server Installation** in the wizard window. 
6.	Click **Install** to begin the installation of Provisioning Services.

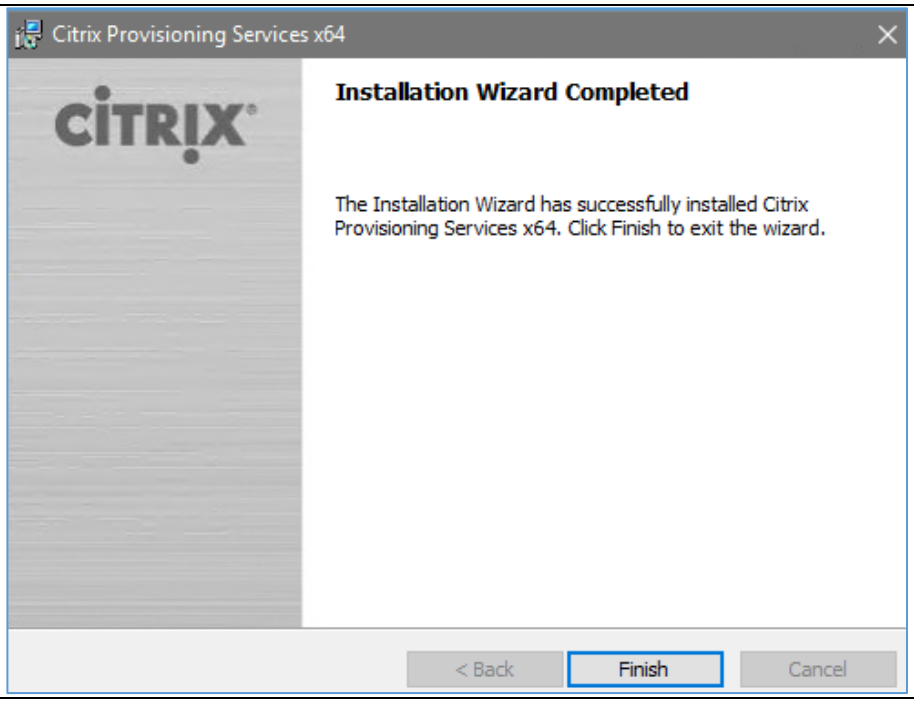
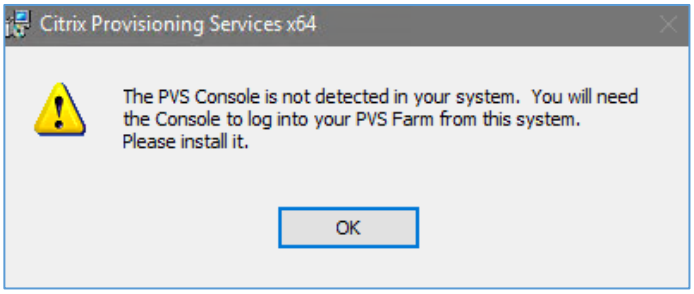
	
7.	Wait for the Citrix Provisioning Services wizard to appear and then click **Next**.
8.	Review the license agreement, and if you agree, select **I accept the terms in the license agreement** and then click **Next**.
9.	Click **Next** to accept the default information.
10.	Click **Next** to accept the default destination folder.

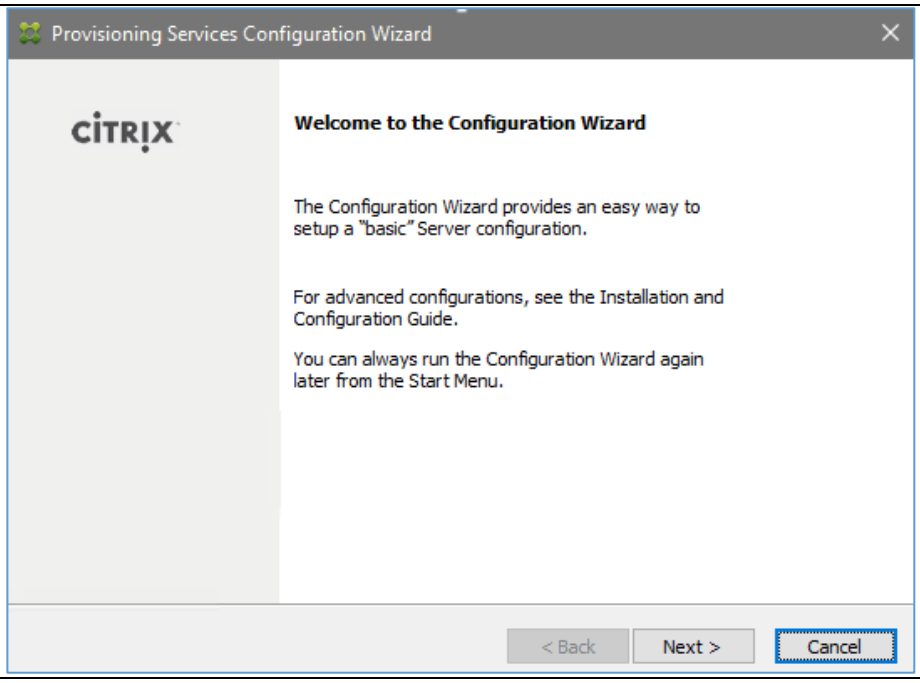
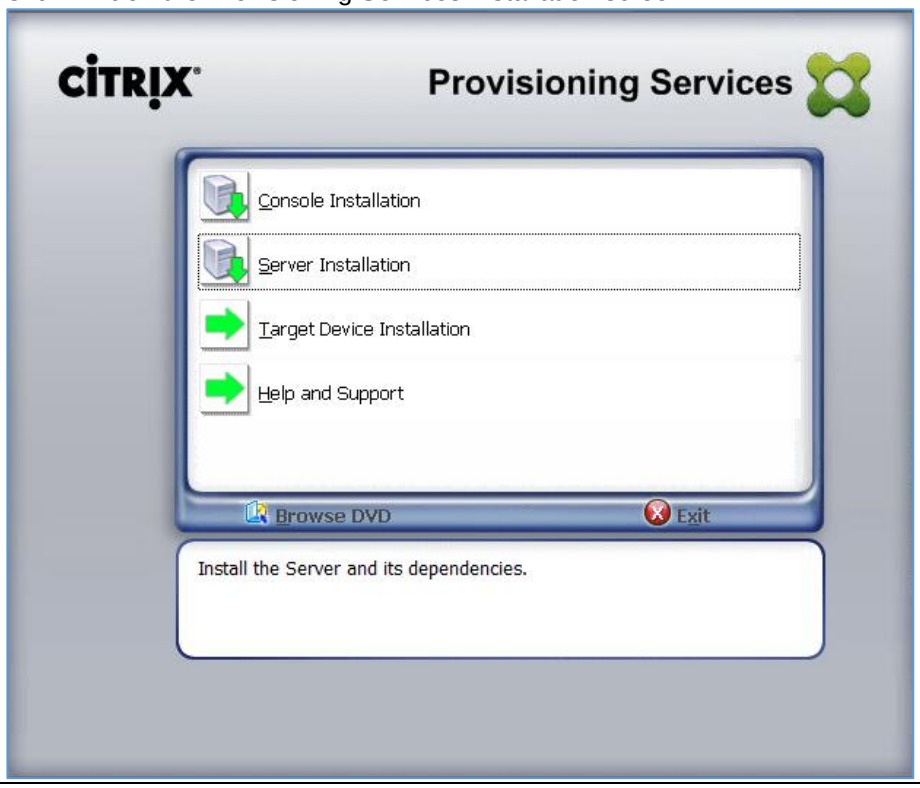


11. Click **Install** to begin the installation.



12. Click **Finish**.

	
13.	Click **OK** in the message concerning the PVS Console.  **Note:** The PVS Console is not installed yet. We will be installing it while configuring the Provisioning Services Farm.
14.	Click **Cancel** on the Provisioning Services Configuration Wizard screen.

	
15.	Click **Exit** on the Provisioning Services Installation screen. 
16.	Click **X** to close the Windows Explorer.

Key Takeaways:

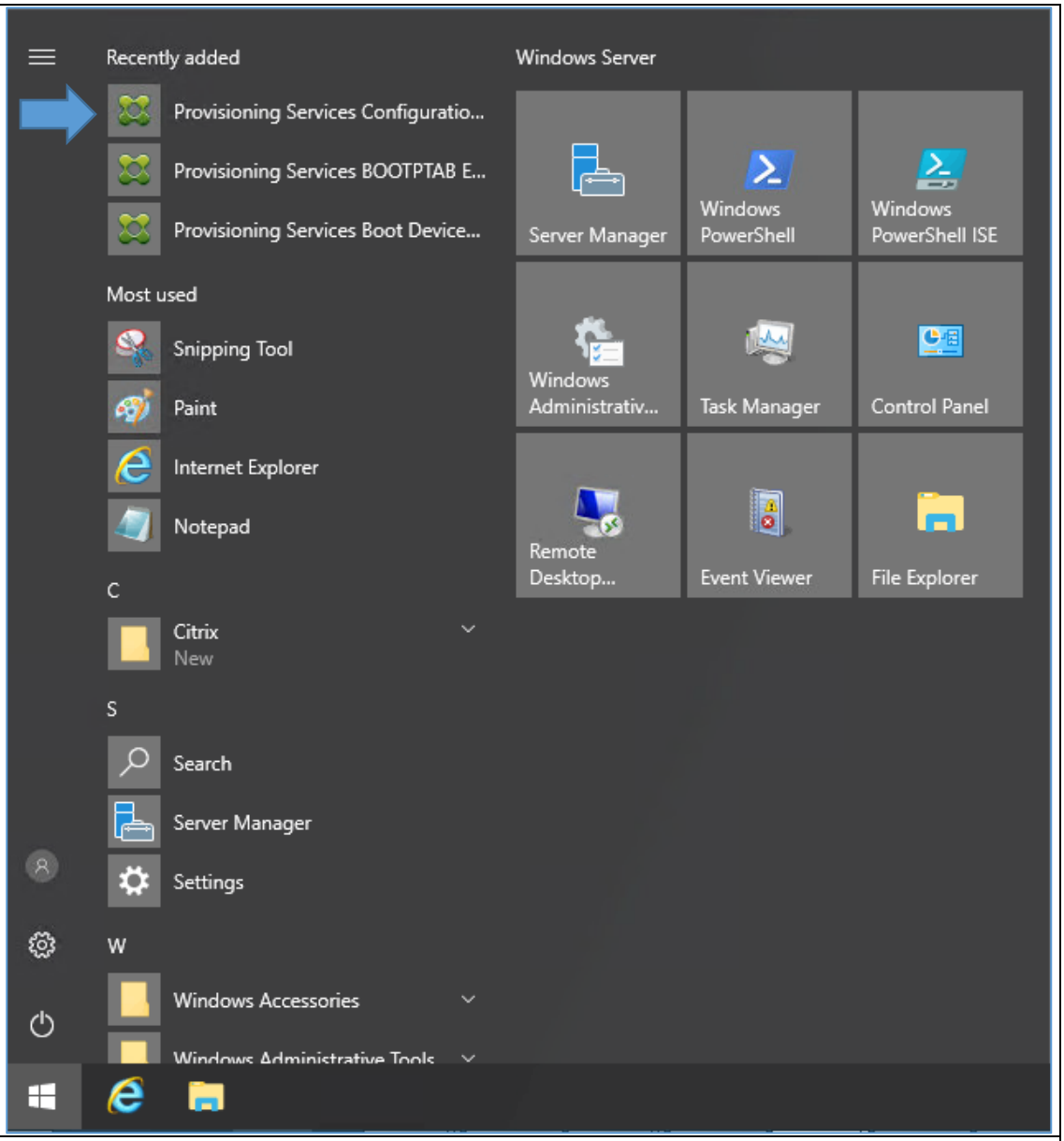
- Once a Provisioning Services server is installed, it must be configured first so as to be operational.
- Provisioning Services server install has only the server component and the services. The Provisioning Services console has to be installed so as to manage the farm.

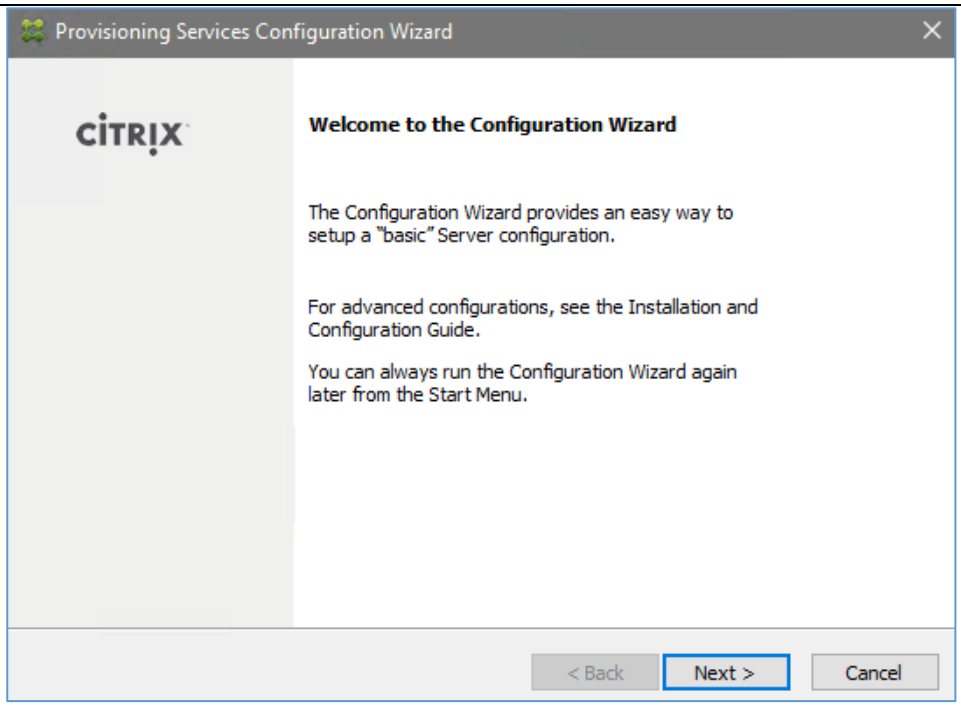
Exercise 16-2: Configure Provisioning Services Farm

Scenario:

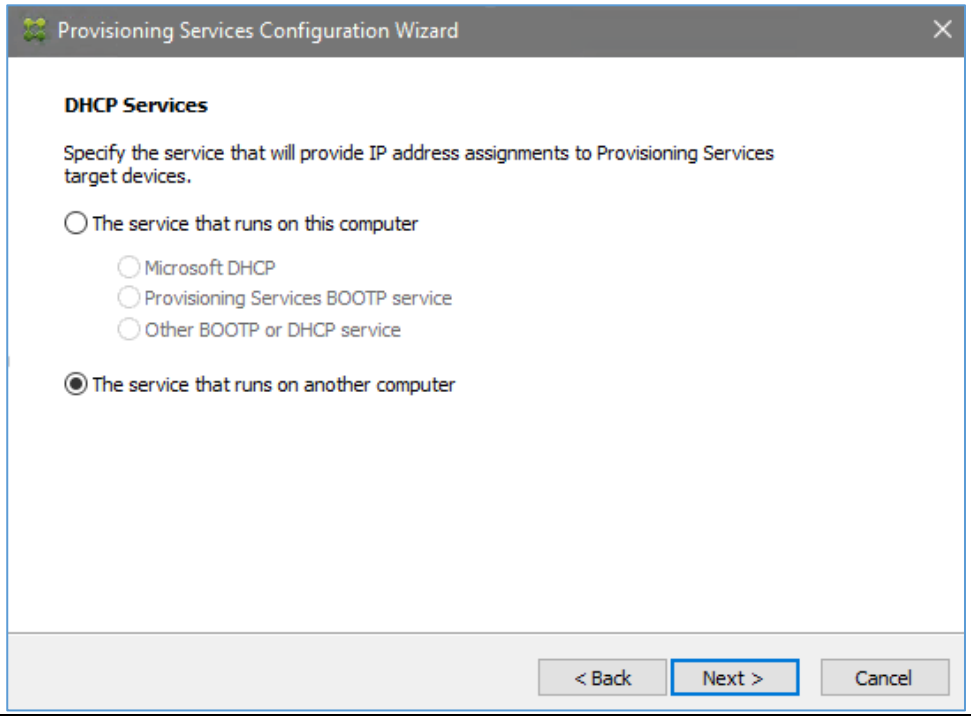
You are a Citrix Administrator at WW Labs, your Lead Citrix Architect has tasked you with starting the Citrix Provisioning Services Farm configuration using the Provisioning Services Configuration Wizard. Your instructions are to ensure PXE is enabled, a specific service account (Svc-PVS) is used to run the services and that the Provisioning Services database is automatically created on NYC-SQL-001 using the wizard. Further to these tasks, you notice that the Provisioning Services console has not yet been installed, so after highlighting this to the Lead Citrix Architect, he approves that you deploy the PVS Console to the NYC-PVS-001 server as well.

Step	Action
1.	Using the Remote Desktop Connection manager, confirm you are still connected to **NYC-PVS-001**. **Note:** In a previous exercise, you had logged into **NYC-PVS-001** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session is disconnected, log on to **NYC-PVS-001**, right-click this machine and choose **Connect server**. User name: **WORKSPACELAB\Administrator** with **Password1** as the Password.
2.	Click **Start** and double-click **Provisioning Services Configuration Wizard**.

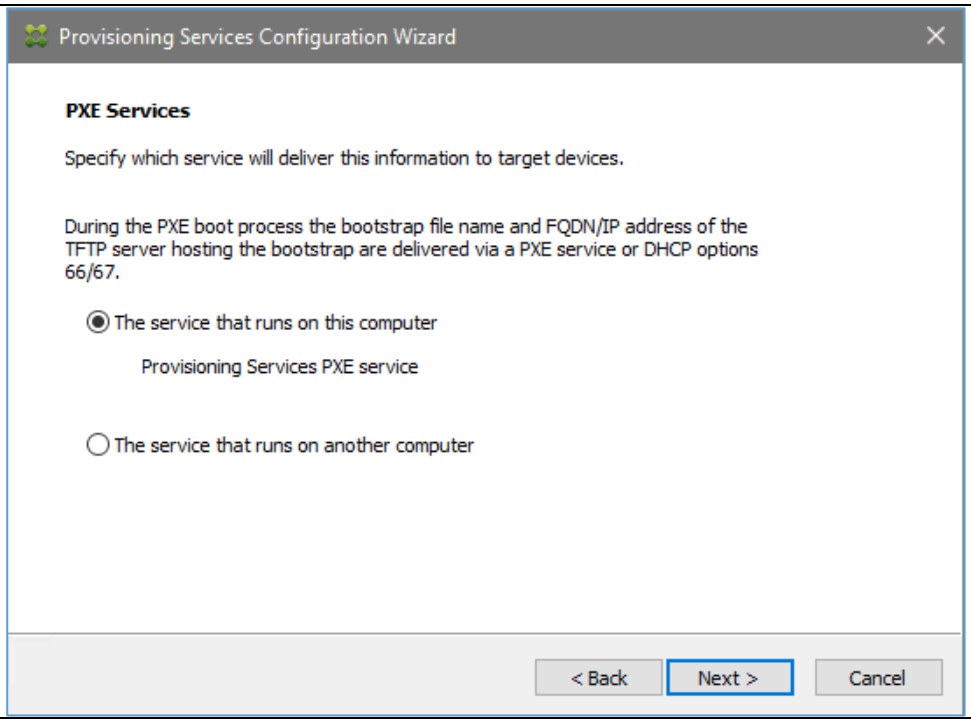
	
3.	Click **Next** in the **Provisioning Services Configuration Wizard** Welcome screen.



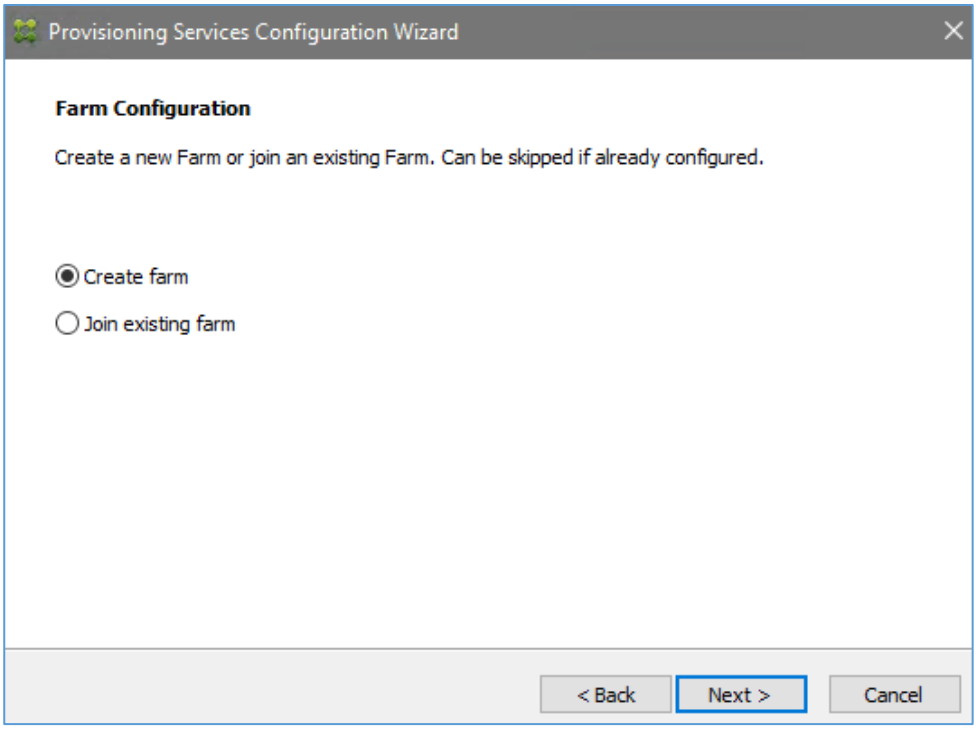
4. For **DHCP Services**, select **The service that runs on another computer** and then click **Next**.



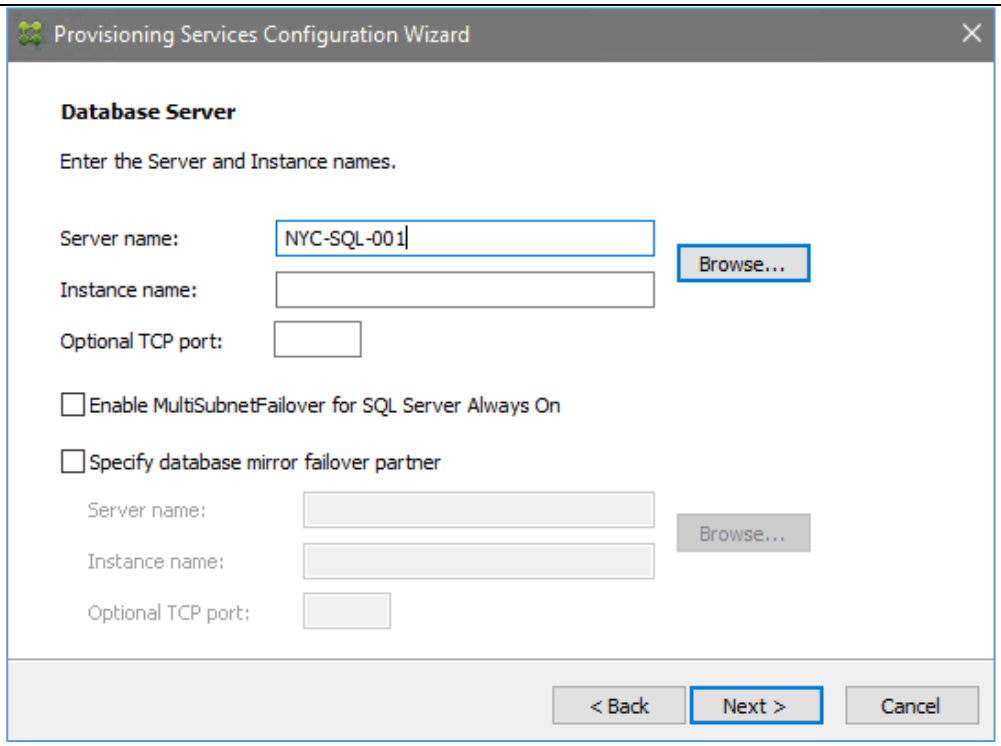
5. For **PXE Services**, select **The service that runs on this computer** and then click **Next**.

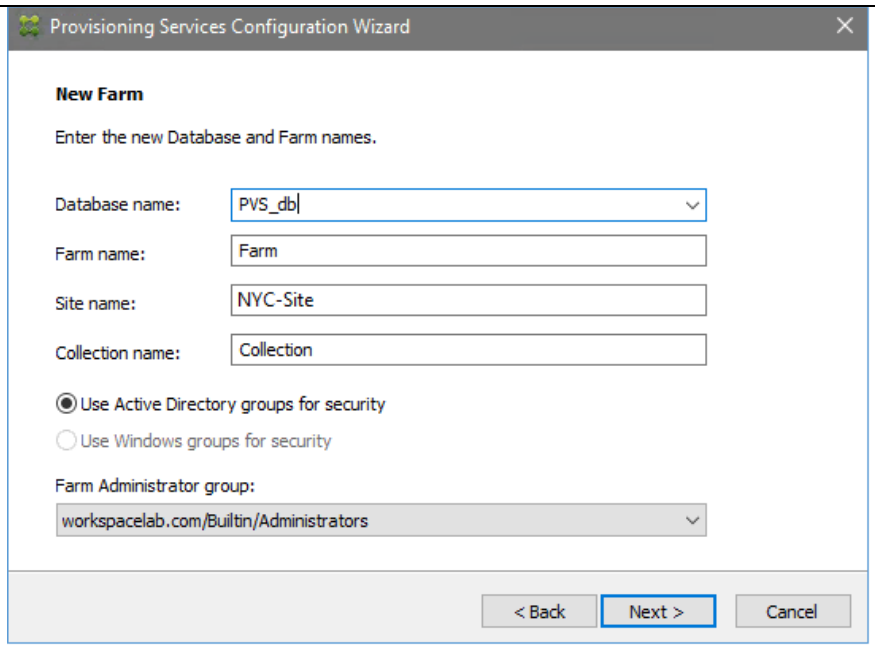


6. Select **Create farm** and then click **Next**.



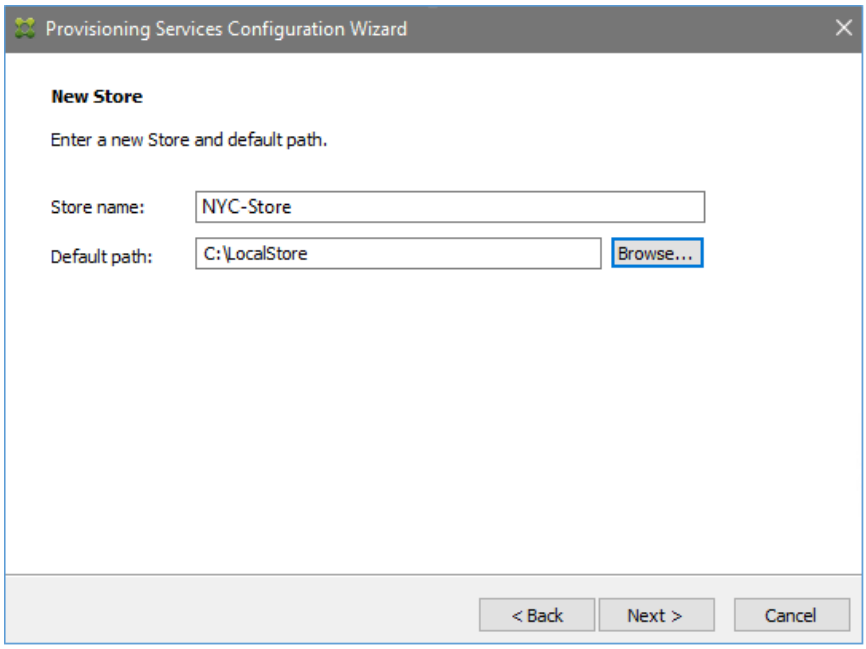
7. Type **NYC-SQL-001** in the Server name field and then click **Next**.

	
8.	Type **PVS_db** in the Database name field and then verify that **Farm** is specified in the Farm Name field. **Note:** The database named PVS_db would automatically be created provided we have the correct permissions to the database server. In case we do not have permissions to connect to the database remotely due to security constraints, we can also create the database manually (see **https://support.citrix.com/article/CTX134615)**.
9.	Verify that **NYC-Site** is specified in the Site name field and **Collection** is specified in the Collection name field.
10.	Verify that **Use Active Directory groups for security** and **Workspacelab.com/Builtin/Administrators** are selected, and then click **Next**.



11. Verify that **NYC-Store** is specified as the Store name.

12. Click **Browse** for default path and select **C:\LocalStore** and click **OK** and click **Next**.

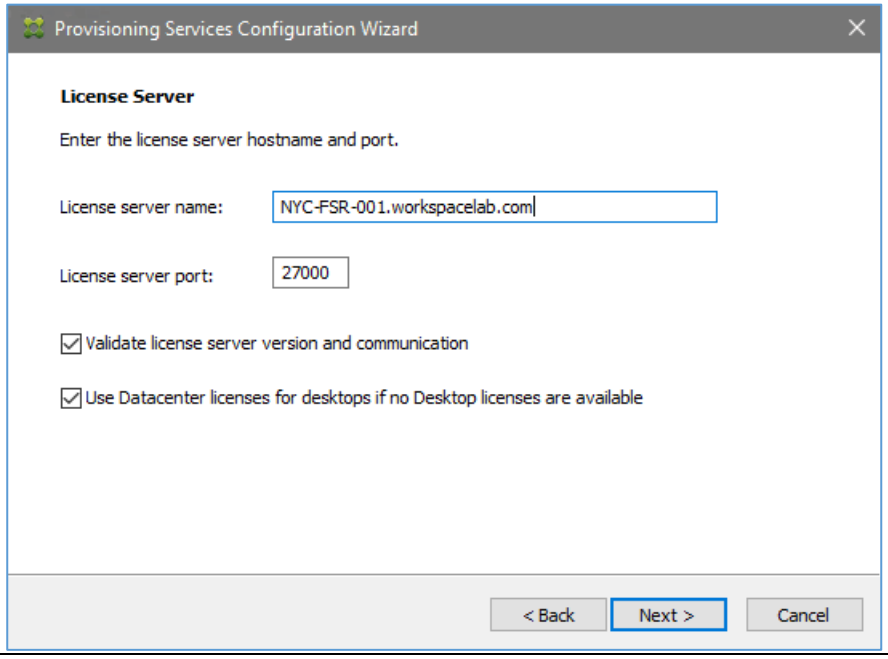
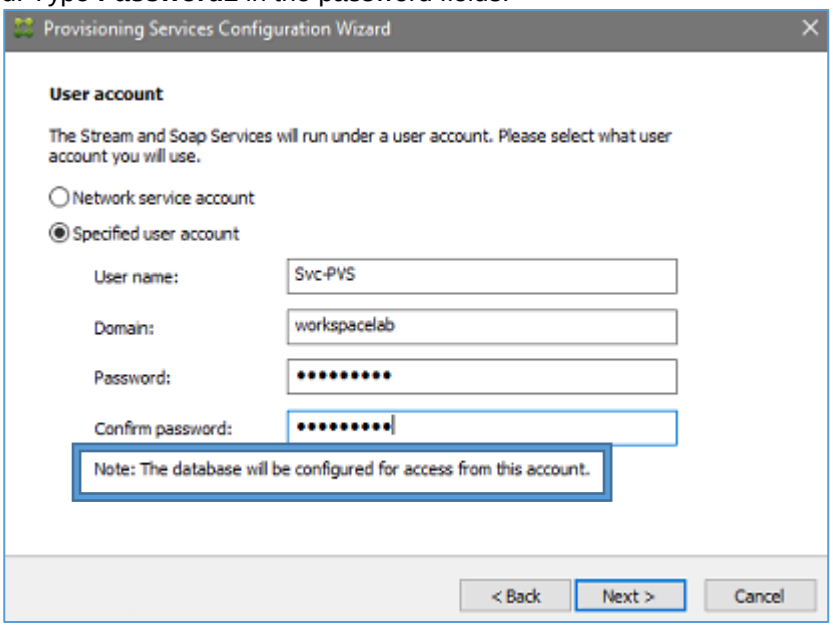


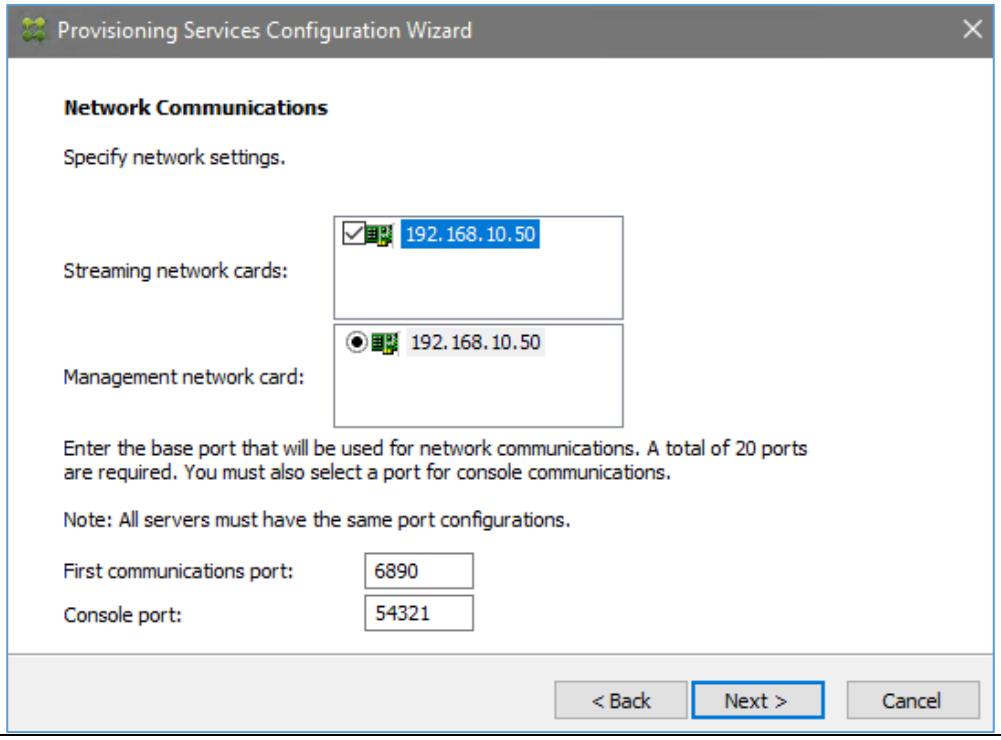
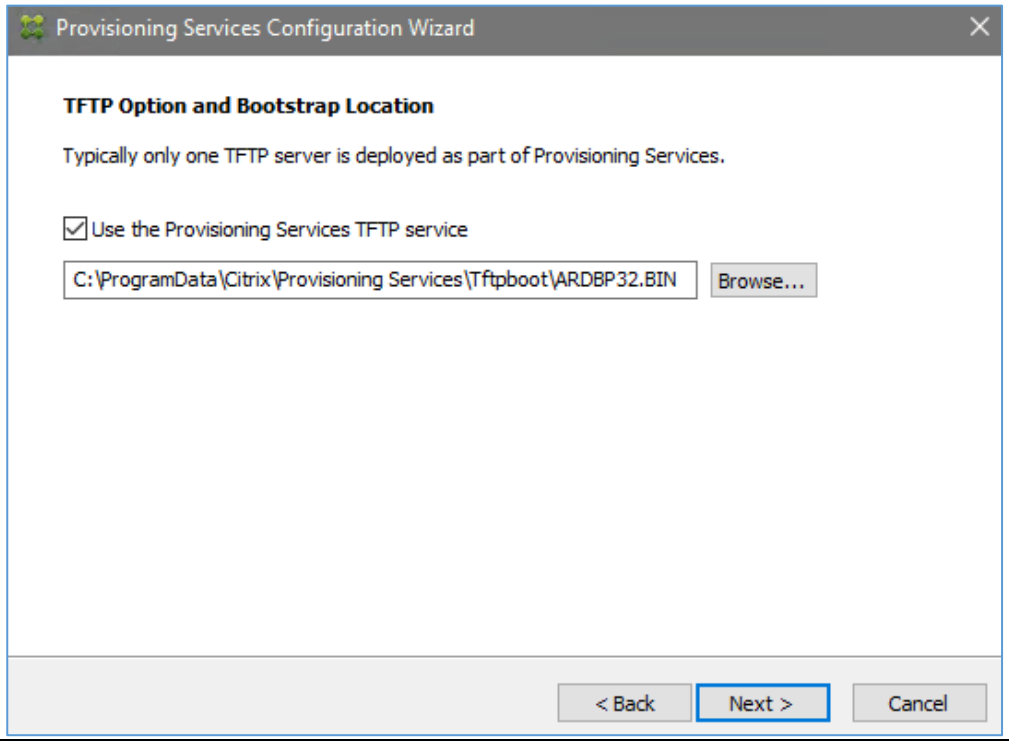
Note: A Local Store with full permissions to the service account has already been created for the lab environment. We would be creating a shared store in upcoming exercises.

13. Type **NYC-FSR-001.workspacelab.com** in the **License server name** field.

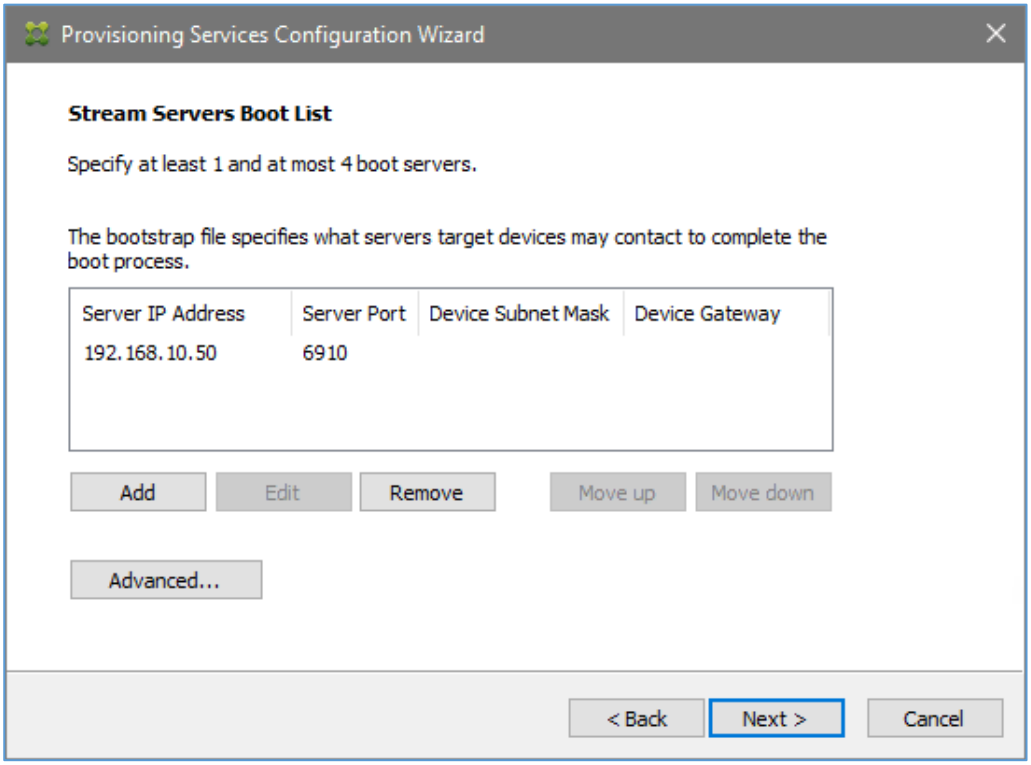
Note: If copying the license server name from lab guide, make sure there is no extra space at the end.

14. Verify **Validate license server version and communication** and **Use Datacenter licenses for desktops if no Desktop Licenses are available** are selected and then click **Next**.

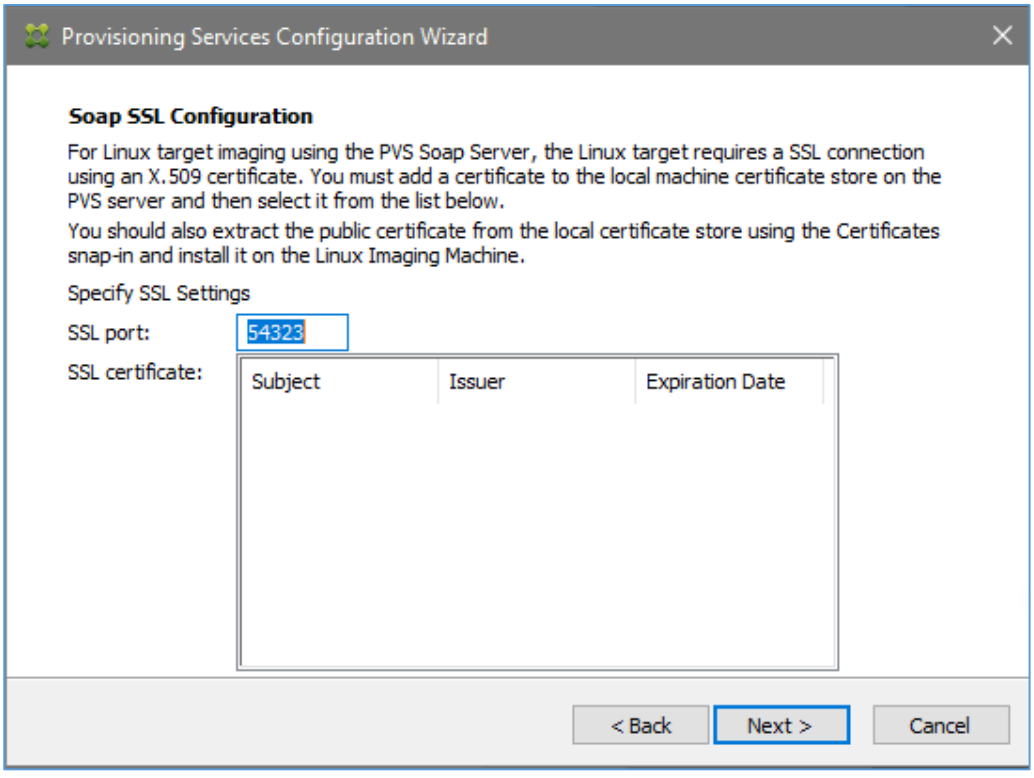
	Note: It will take a few seconds to validate the License Server. 
15.	Select the account to use for the Stream Services and SOAP Server and then click **Next**. a. Select **Specified user account**. b. Type **Svc-PVS** in the User name field. c. Type **workspacelab** in the Domain field. d. Type **Password1** in the password fields.  Click **Next**. **Note: Svc-PVS** Service account is already created for the Lab Environment. Once configured, stream and soap services will be running with this service account until changed manually. These are the two main services for PVS operations and they need permissions to access the vDisk store and database.

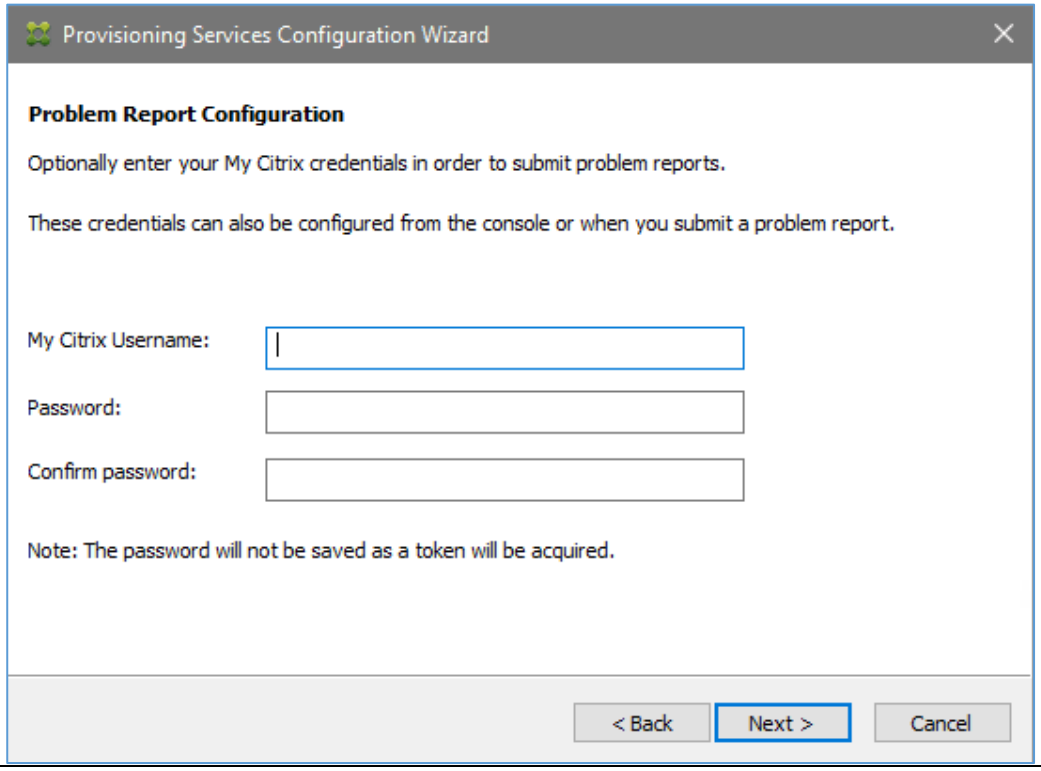
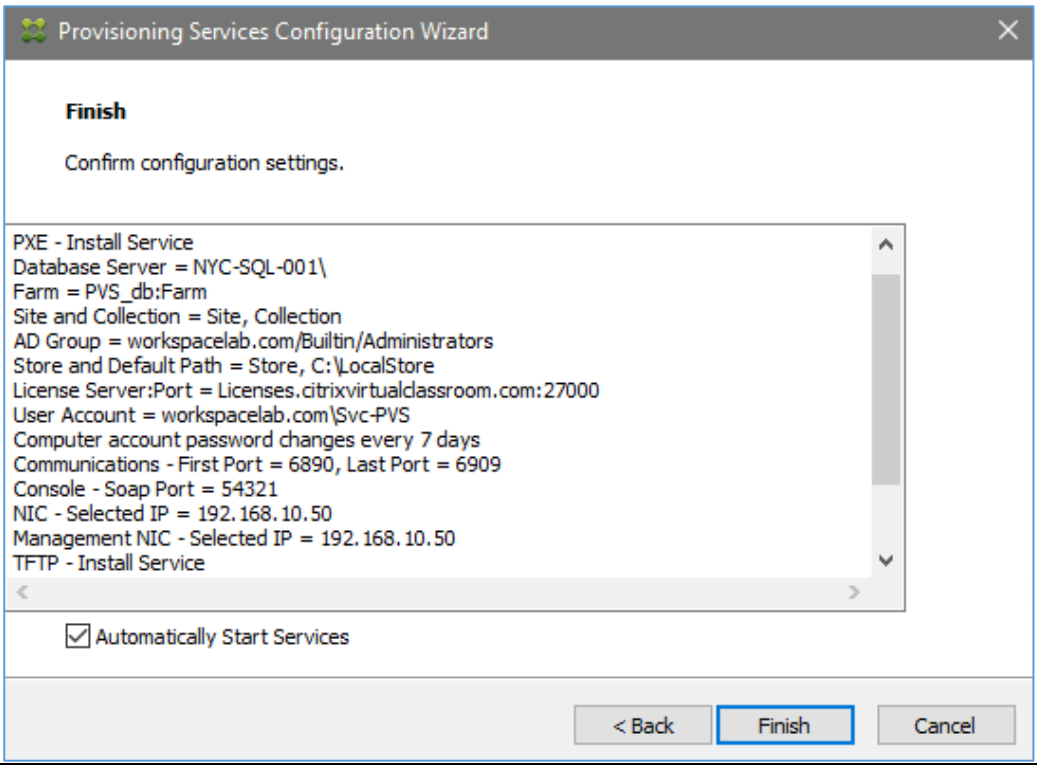
	Note: Login for the service account will automatically be added in the database.
16.	Verify that **Automate computer account password updates** is selected and then click **Next**.
17.	Verify that **6890** is specified as the first communications port, and that **54321** is specified as the Console port, and then click **Next**. 
18.	Select **Use the Provisioning Services TFTP service** and then click **Next**. 

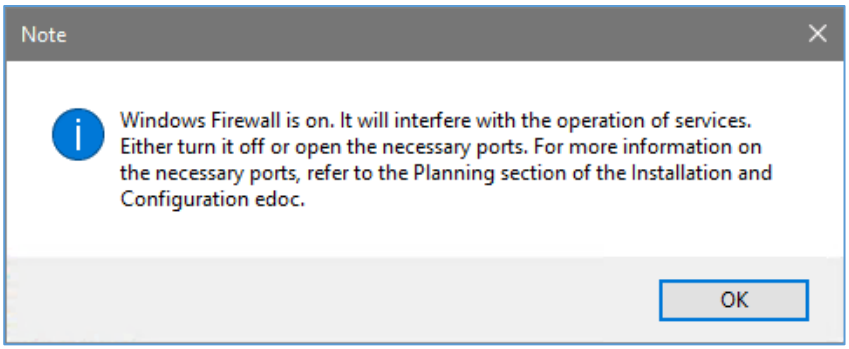
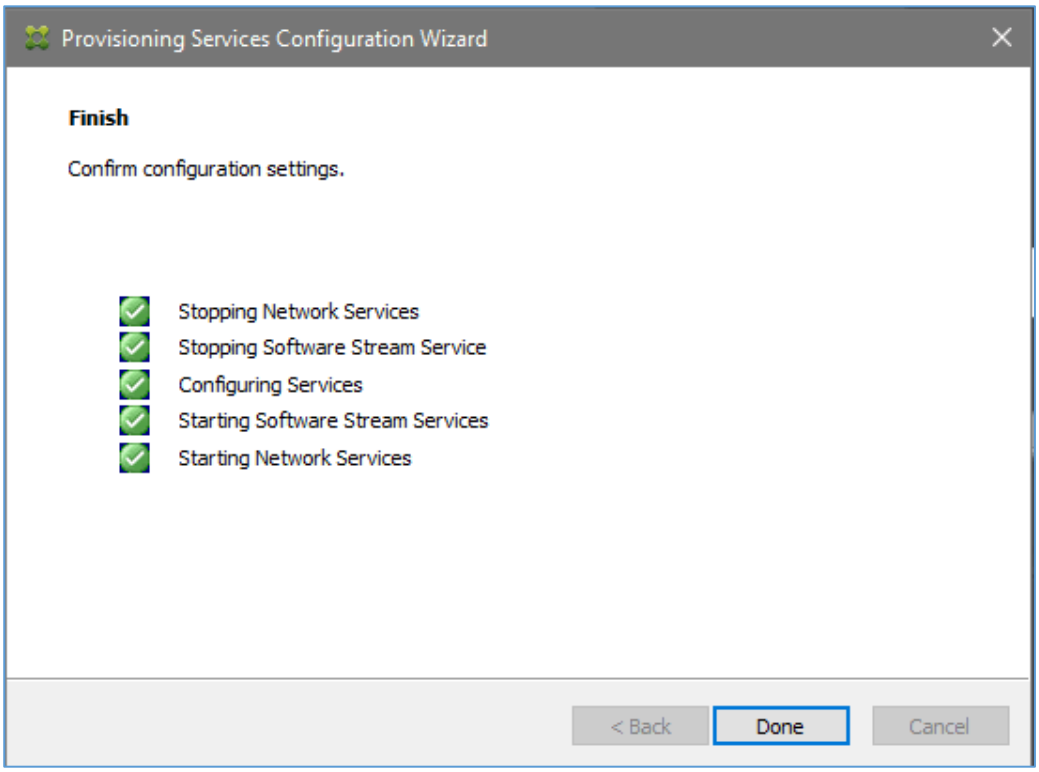
19. Click **Next** to accept the default **Stream Servers Boot list**.

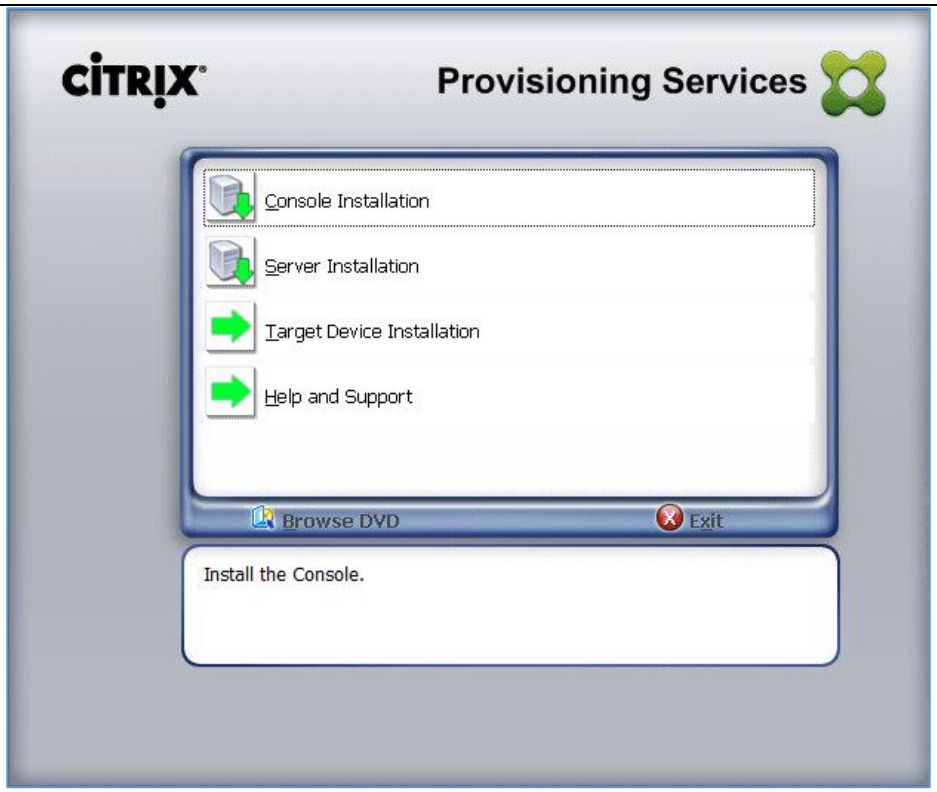


20. Click **Next** to accept the default **Soap SSL Configuration**.

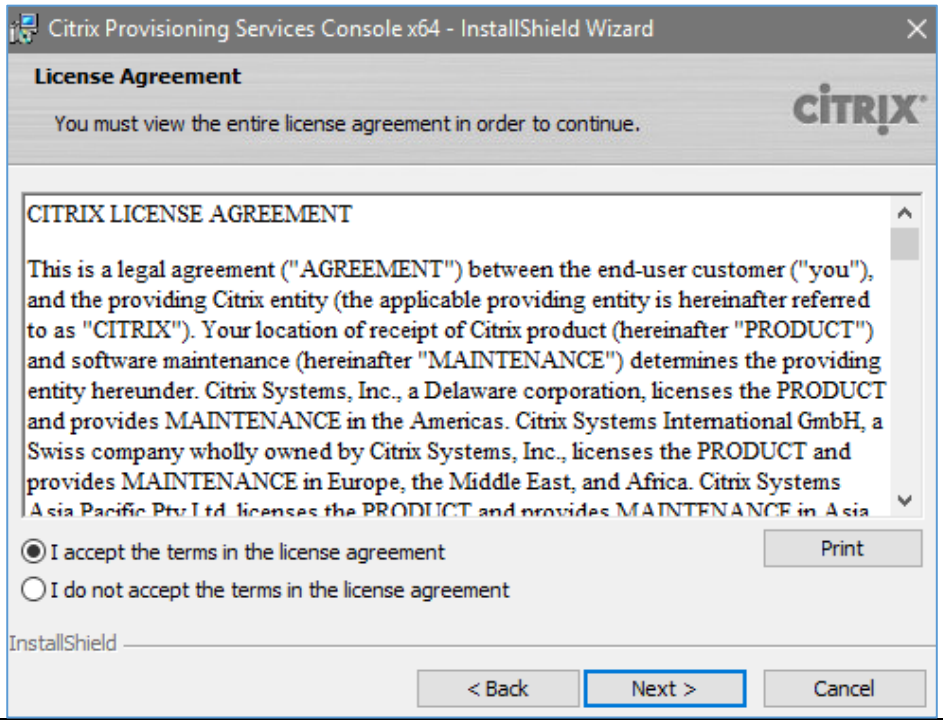


	Note: SSL Configuration is only for Linux target devices.
21.	Click **Next** to accept the default **Problem Report Configuration**. 
22.	Verify that **Automatically Start Services** is selected and then click **Finish**. 
23.	Click **OK** in the Windows Firewall message.

	
24.	Wait while the configuration completes and then click **Done**. 
25.	Click **File Explorer** in the taskbar. Click **This PC** and then double-click the **CD Drive (D:)**. **Note:** If the Provisioning Services main menu screen does not launch from double-clicking the green Citrix logo next to CD Drive under Devices and drives, then double-click the Autorun.exe file. **Note:** If DVD-drive is not seen, then verify that **ProvisioningServices713.iso** is inserted in **NYC-PVS-001** in XenCenter.
26.	Click **Console Installation** and then click **Next** on the Welcome page of the wizard.

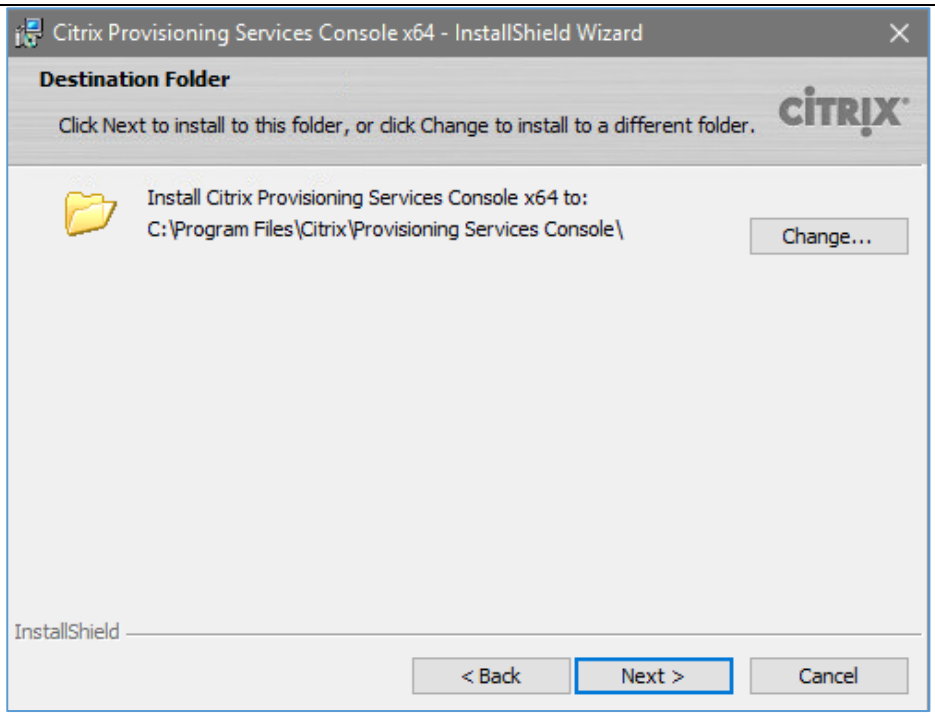


27. Select **I accept the terms of the license agreement** and then click **Next**.

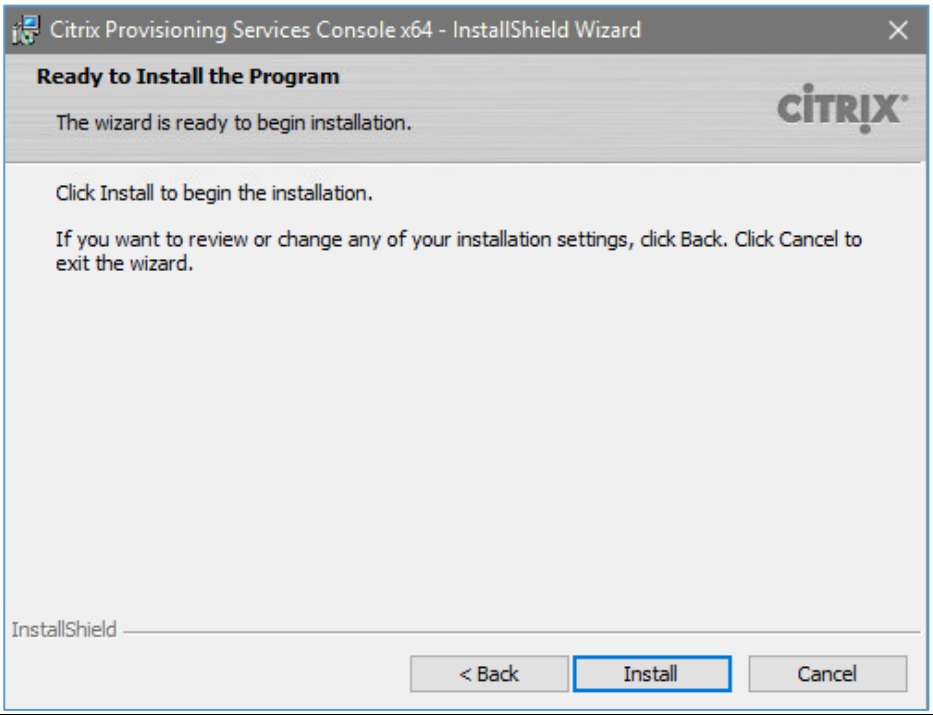


28. Click **Next** to accept the default information.

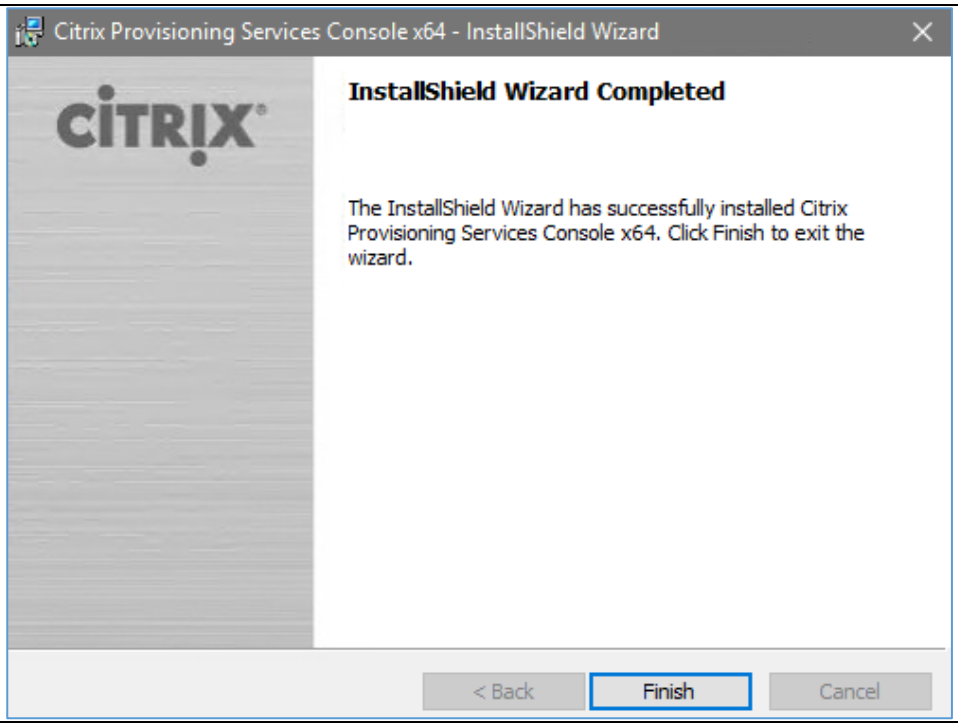
29. Click **Next** to accept the default destination folder.



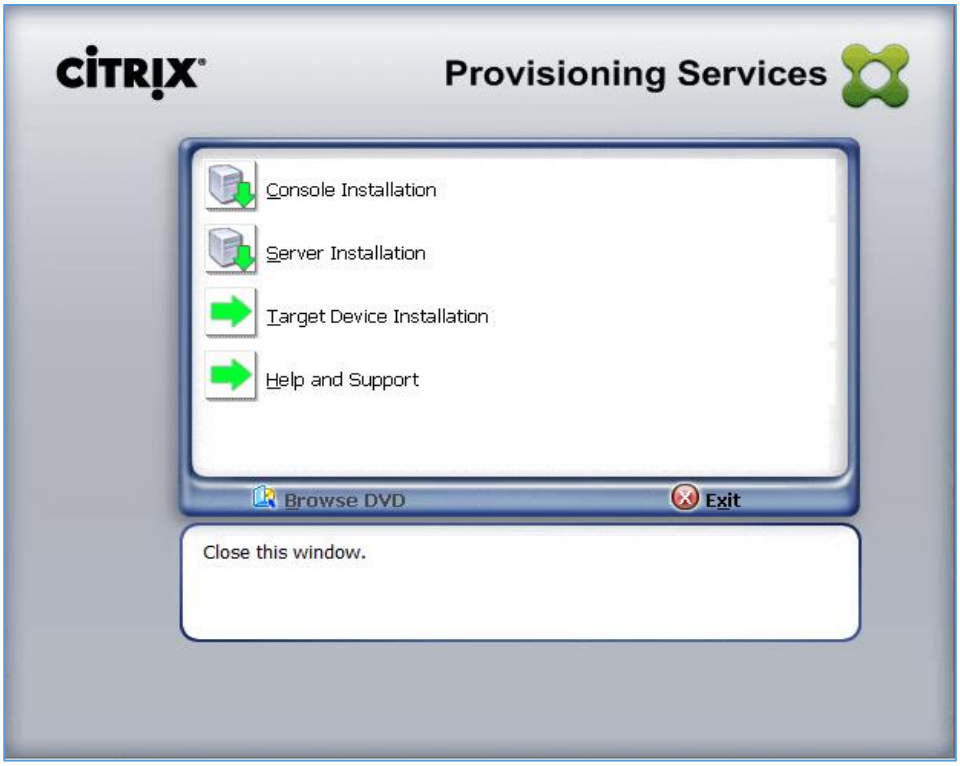
30. Click **Install** to begin the installation of the **Provisioning Services Console**.



31. Click **Finish**.



32. Click **Exit** and close File Explorer.



33.	Connect to **XenCenter** and click **Eject** to the right of the **DVD-Drive 1** field to eject the Provisioning Services media.

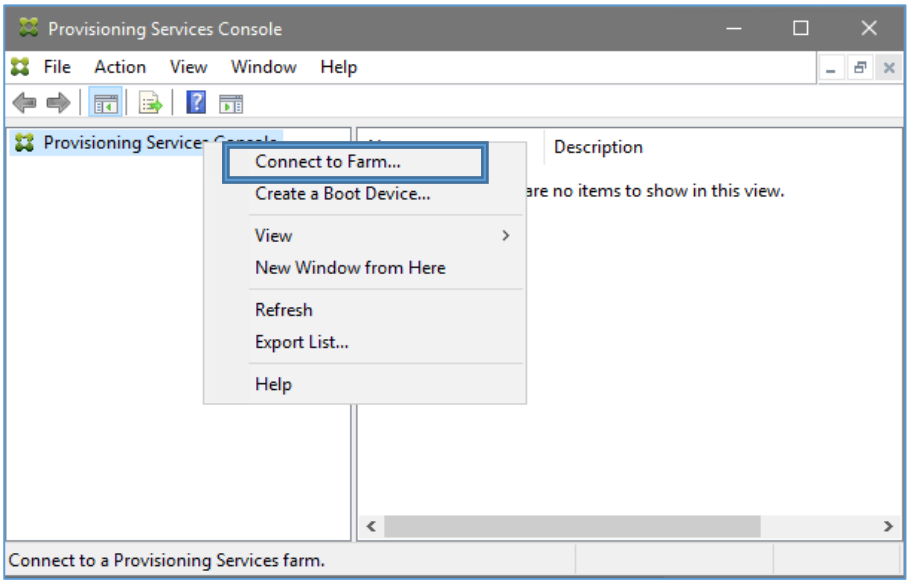
Key Takeaways:

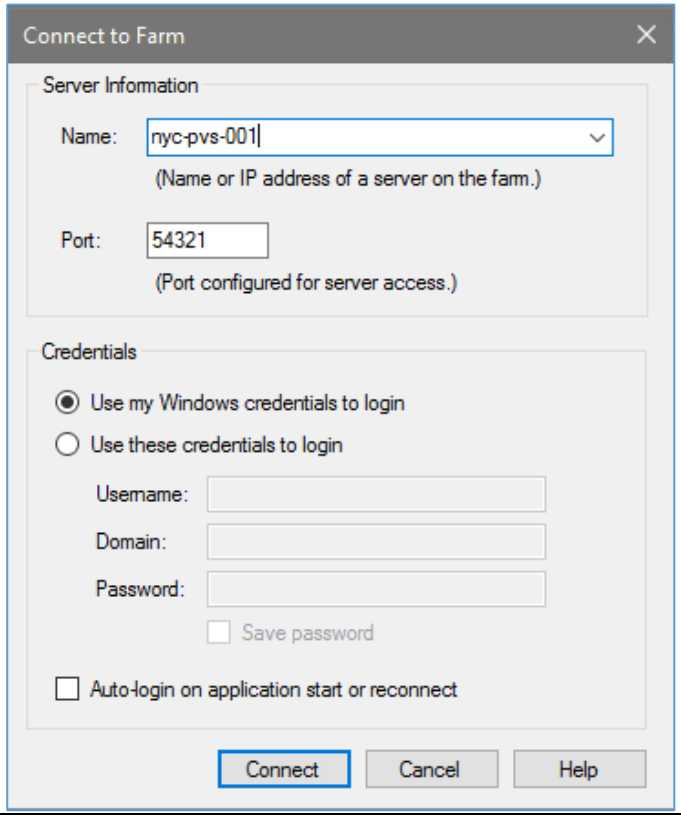
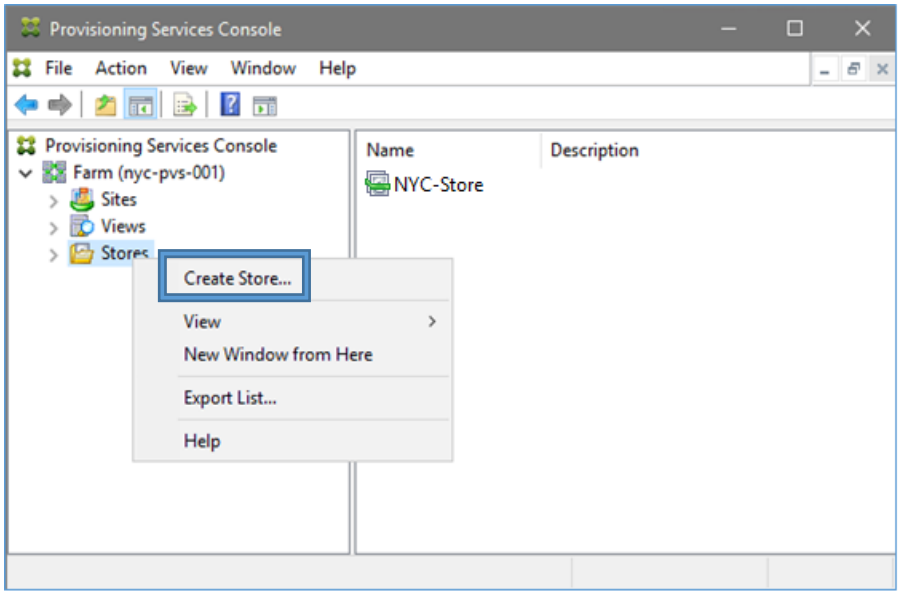
- In order for a Provisioning Services server to be operational it must first be configured.
- During the configuration, certain services are enabled or disabled depending in the design you chose.
- The services can be hosted in the context of Network Service or a custom service account.
- The account configured to run the services must have access to the vDisk store location and must be DB_owner on the database.
- The configuration wizard will automatically add the user to the database if a Netbios username is specified during configuration.
- If using a custom service account, this user should be added to the local administrators group on the PVS server.
- The PVS Console can be deployed on the PVS servers or a remote management computer.

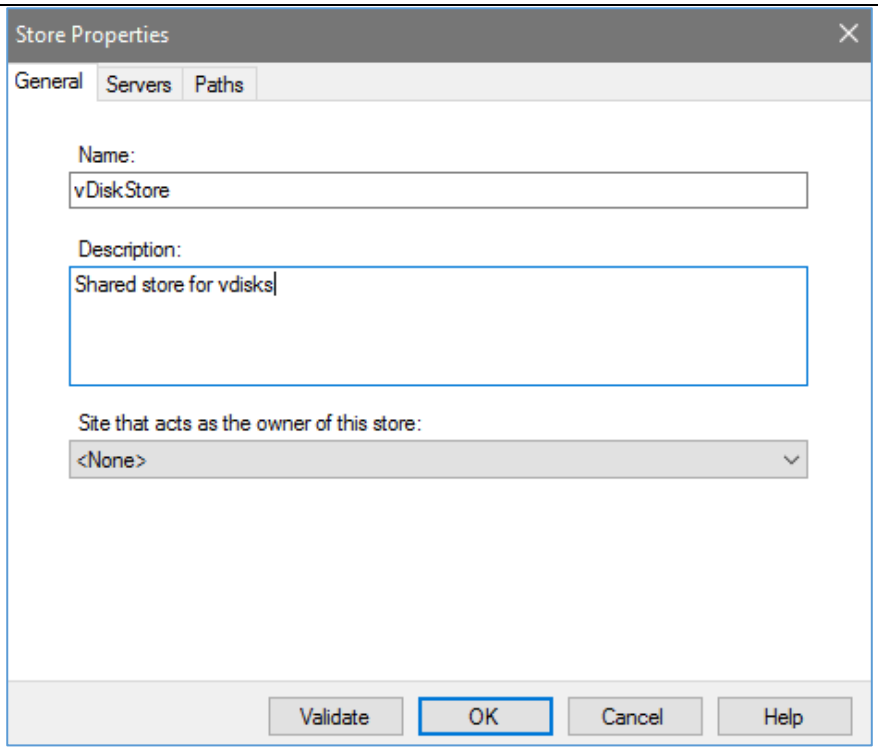
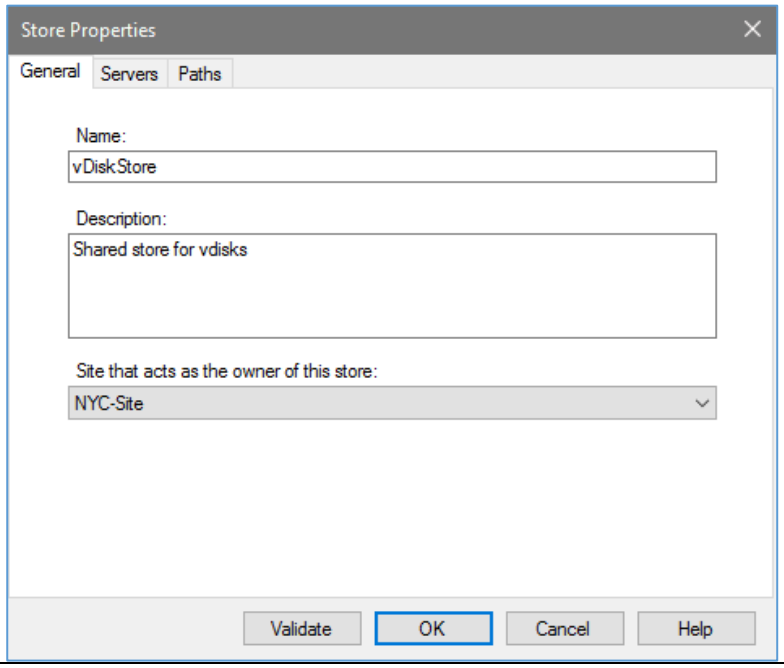
Exercise 16-3: Configure the Farm Store

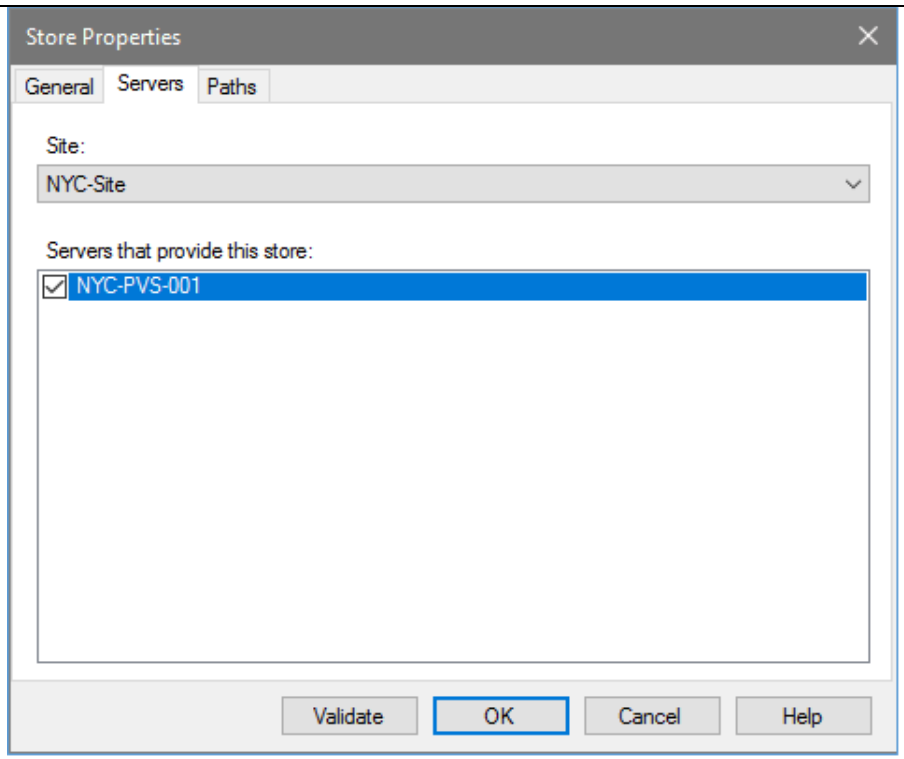
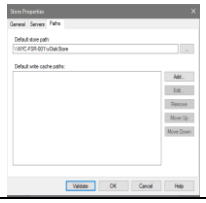
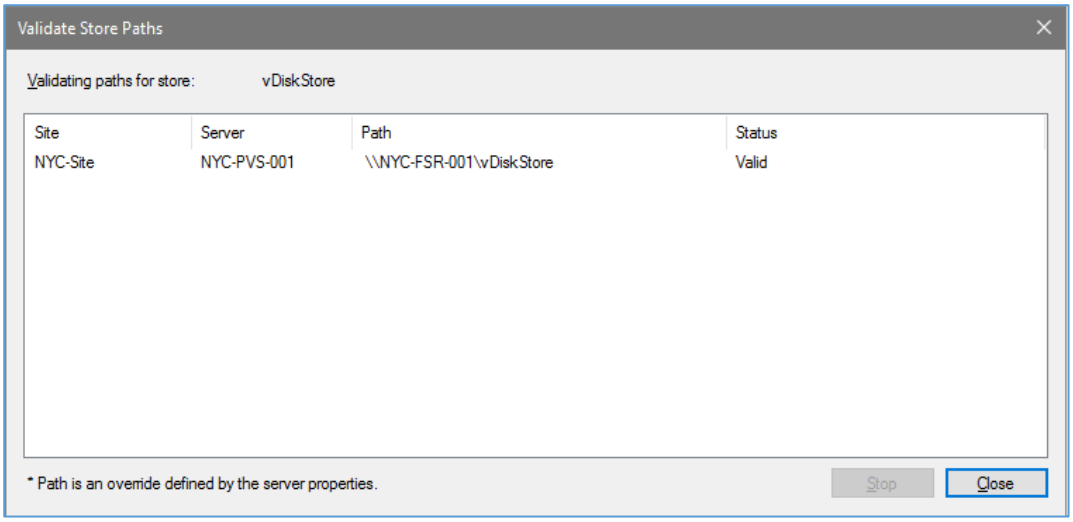
Scenario:

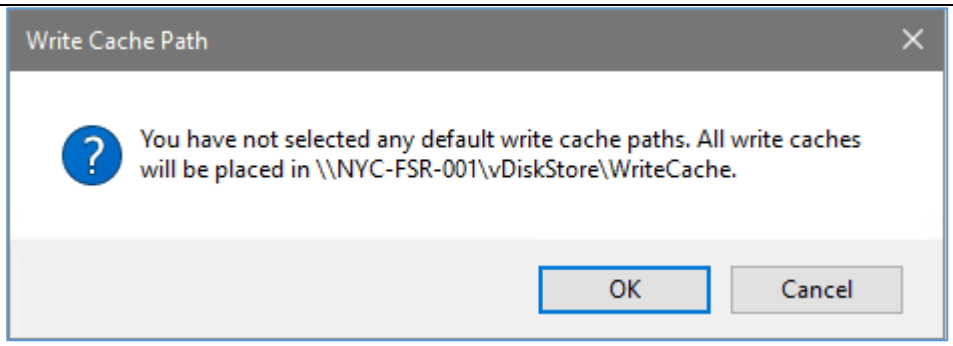
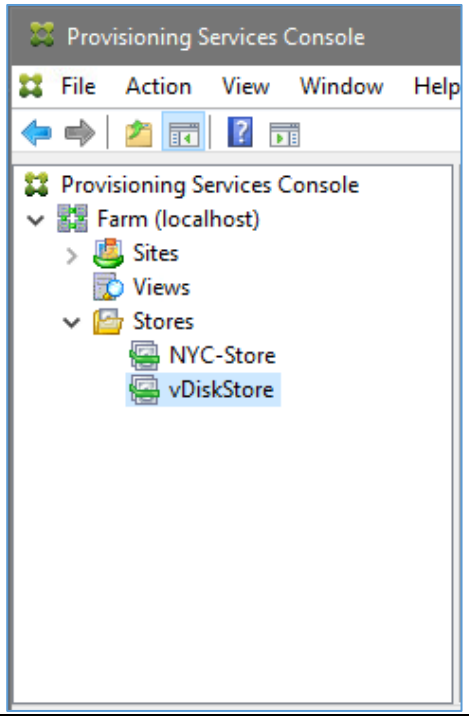
You are a Citrix Administrator at WW Labs, your Lead Citrix Architect has tasked you to configure Provisioning Services to use the new file share for storing vDisks during the POC.

Step	Action
1.	Using the Remote Desktop Connection manager, connect to **NYC-PVS-001**. To login **NYC-PVS-001** right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the Password.
2.	Click **Start** and click **Provisioning Services Console**.
3.	Right-click **Provisioning Services Console** in the left pane and select **Connect to Farm**. 

4.	Type **nyc-pvs-001** in Name section and then click **Connect**. 
5.	Browse to **Farm > Stores**.
6.	Right-click **Stores** and select **Create Store**. 
7.	In **General** Tab under Name, type **vDiskStore** and under Description, type **Shared store for vdisks**.

	
8.	Select **NYC-Site** from drop-down of **Site that acts as the owner of this store**. 
9.	Select **Servers** tab and select the checkbox corresponding to **NYC-PVS-001**.

	
10.	Select **Paths** tab and type **\\NYC-FSR-001\vDiskStore** under Default store path. 
11.	Click on **Validate**. Click on **Close** once status shows **Valid**. 
12.	Click **OK**.
13.	Click **OK** on **Write Cache Path** message.

	 **Note:** We have not selected any Write Cache Path because we will be caching on the target device hard disk. We will cover the write cache in upcoming exercises.
14.	Browse **Farm > Stores** and verify **vDiskStore** is created. 

Key Takeaways:

- The Store must be defined in the Provisioning Services console before any server can serve vDisks from the store.
- A Store can be served by a single PVS server or by multiple PVS servers in case you want high availability.
- When defining the vDisk store you also define the server side Write Cache location. By default, a folder named WriteCache is created under the Store location.

Module 17: Streaming the vDisk

Overview:

This module presents steps involved in creating a vDisk, including preparing the Master Target Device and imaging the Master image to a vDisk. Directly following the creation of one Server OS and one Desktop OS vDisk, some of the available vDisk boot options will be configured and tested.

Before you begin:

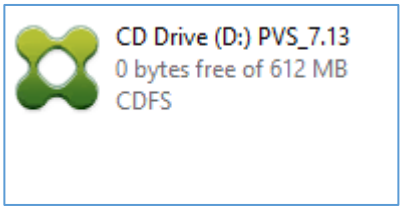
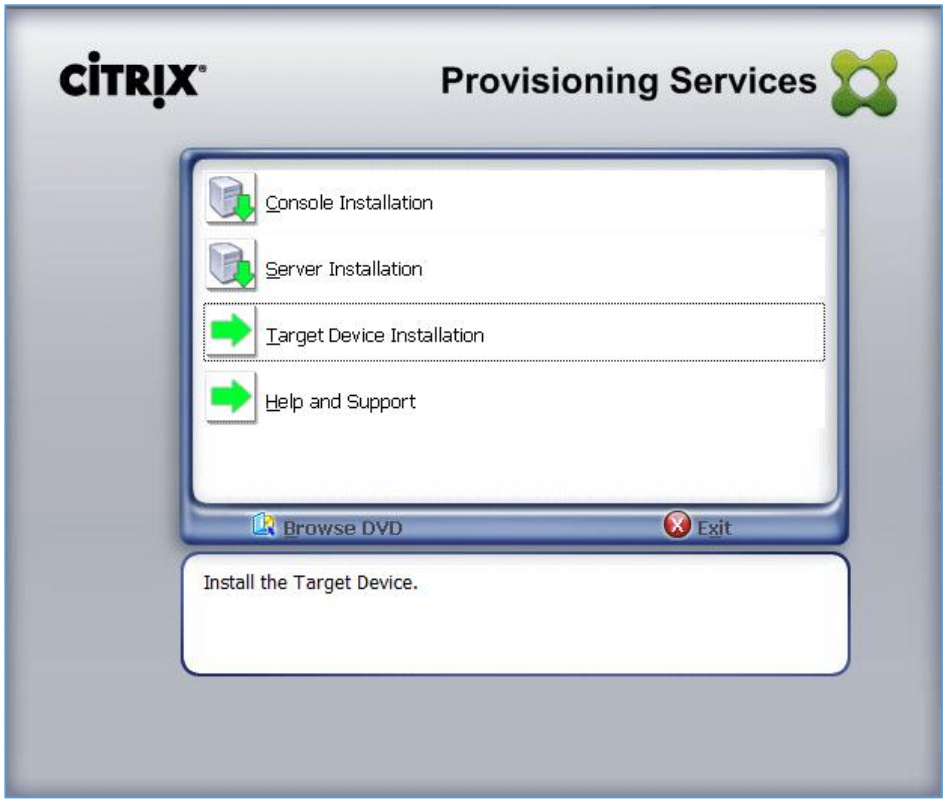
Estimated time to complete Module 17 lab exercises: 85 minutes

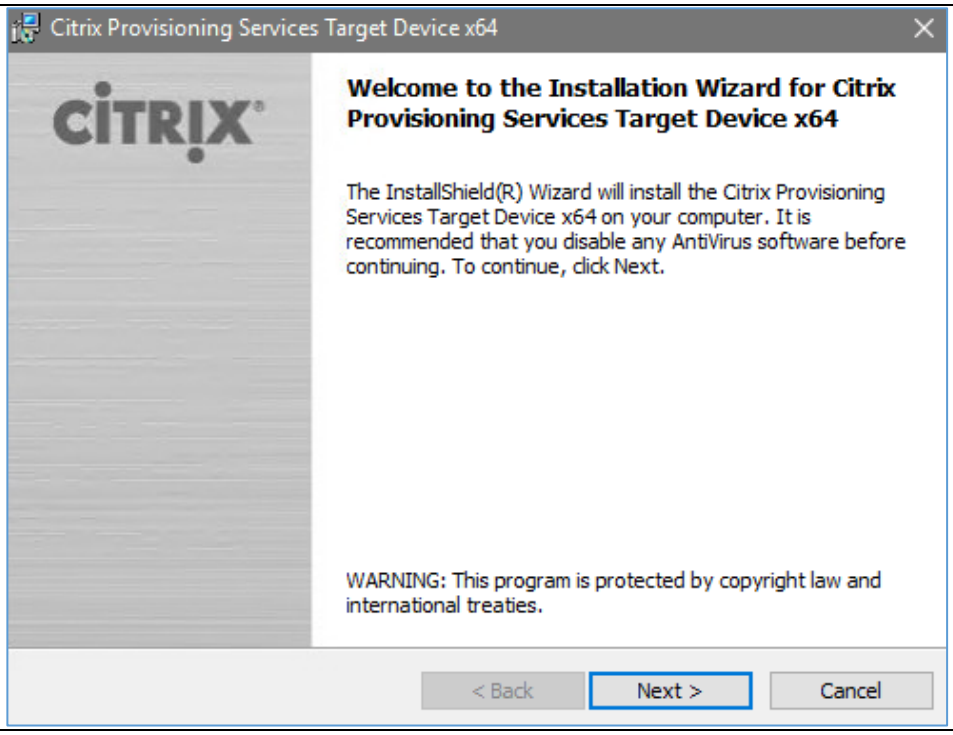
Exercise 17-1: Create vDisk for Server OS

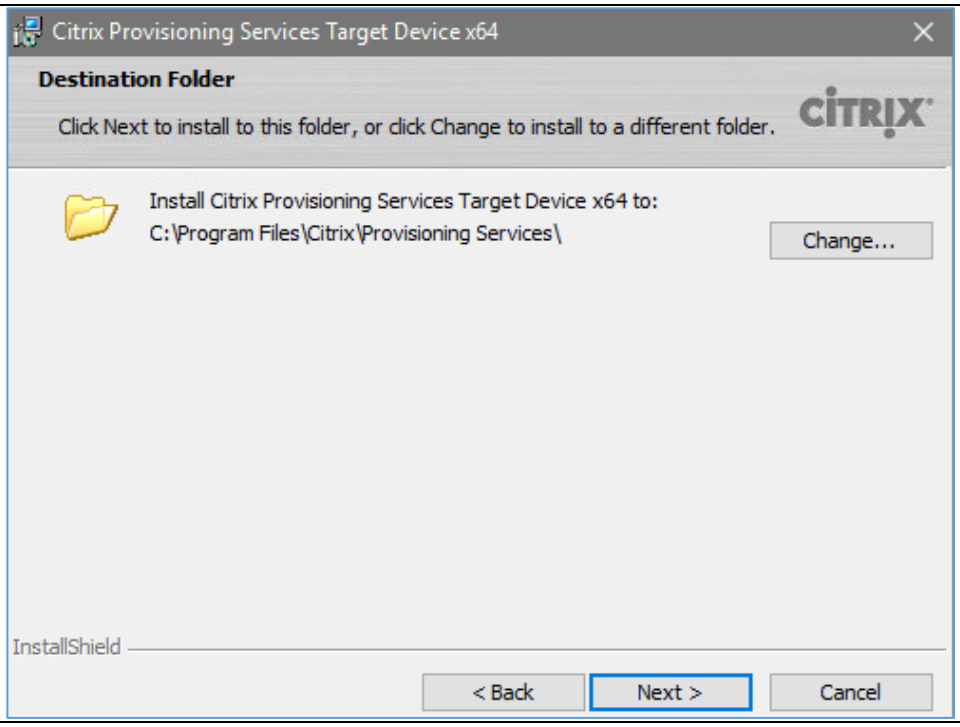
Scenario:

You are a Citrix Administrator at WW Labs, your Lead Citrix Architect has previously configured the VDA installation and has tasked you to install the Provisioning Services Target Device software and proceed with capturing the master image on to a Provisioning Services vDisk.

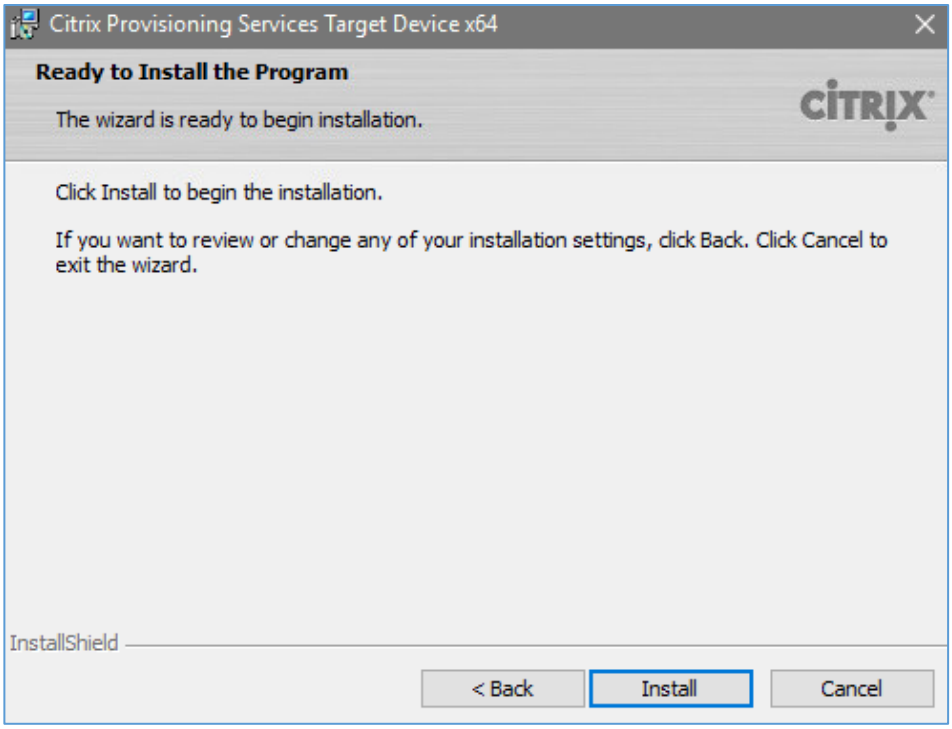
Step	Action
1.	The following VMs are required before beginning the exercises for this Module; all others may be powered down. To power manage your VMs, switch to XenCenter, right-click on the VM in the left pane and select Start or Shut Down. If prompted click Yes. • NYC-ADS-001 • NYC-SQL-001 • NYC-FSR-001 • NYC-PVS-001 • NYC-XDC-001 • PVS-SRV-MST • PVS-DTP-MST **Note**: These above VMs are listed in the start-up order.
2.	Using **XenCenter**, mount the **Provisioning Services** installation media ISO to **PVS-SRV-MST**. To mount the installation media ISO, select **PVS-SRV-MST** in the left pane of XenCenter. In the right pane, select the **Console** tab. Using the **DVD-Drive 1:** drop-down menu select

	ProvisioningServices713.iso. **Note**: If there are no ISOs listed in the **DVD-Drive 1:** drop-down menu, then the Local ISO SR that contains the ISO library may need to be re-scanned. In the left pane of **XenCenter** select the **Local ISO SR XS**. In the right pane select the **Storage** tab and click on the **Re-scan** button.
3.	Using the Remote Desktop Connection manager, connect to **PVS-SRV-MST**. User name: **WORKSPACELAB\Administrator** with **Password1** as the password.
4.	Launch the **File Explorer** application from the Windows Taskbar or Start Menu and double-click the green Citrix logo next to **CD drive** under Devices and drives.  **Note**: If the installation does not launch from double-clicking the green Citrix logo next to **CD drive** under Devices and drives, then right-click green Citrix logo and double-click on the **autorun.exe** file.
5.	Click **Target Device Installation** and then click **Target Device Installation** again. 
6.	Click **Next** on the welcome screen of the installation wizard.

	
7.	Review the License Agreement and if you agree select **I accept the terms in the license agreement** and then click **Next**.
8.	Click **Next** to accept the default selections on Customer Information window.
9.	Click **Next** to accept the default destination folder.

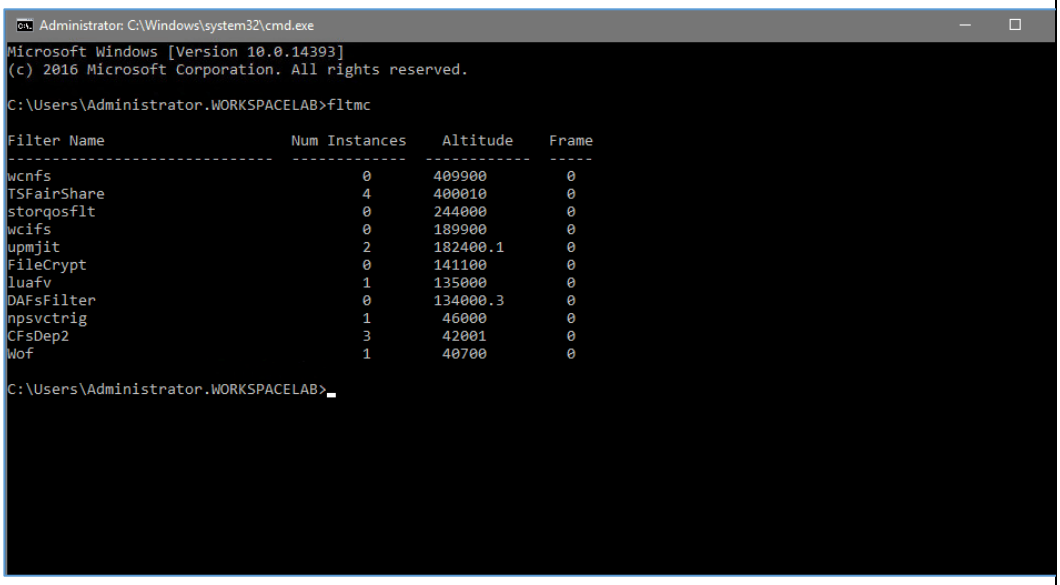


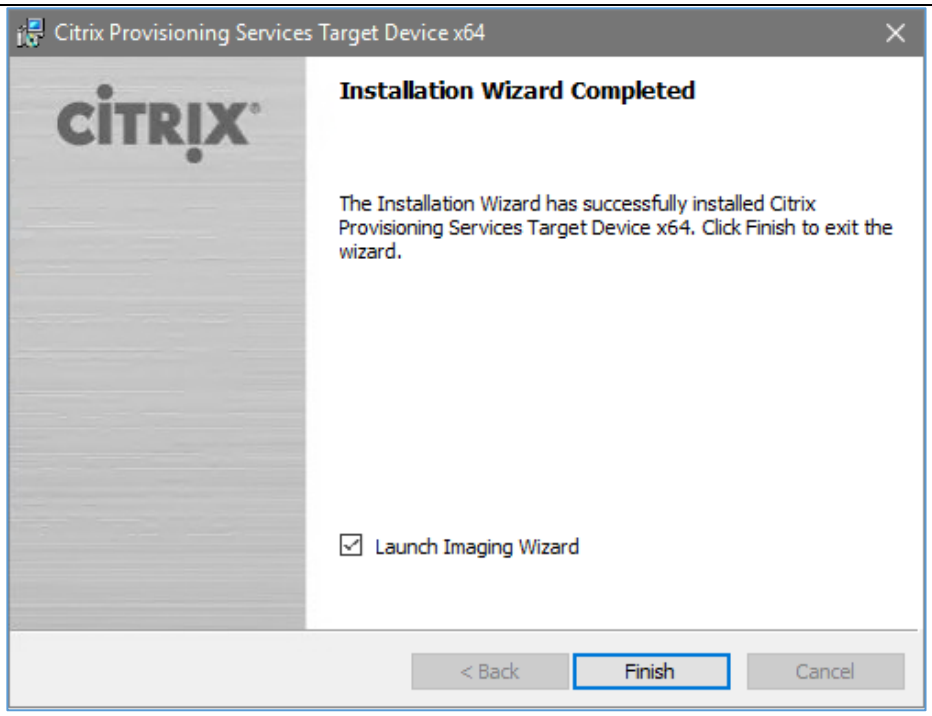
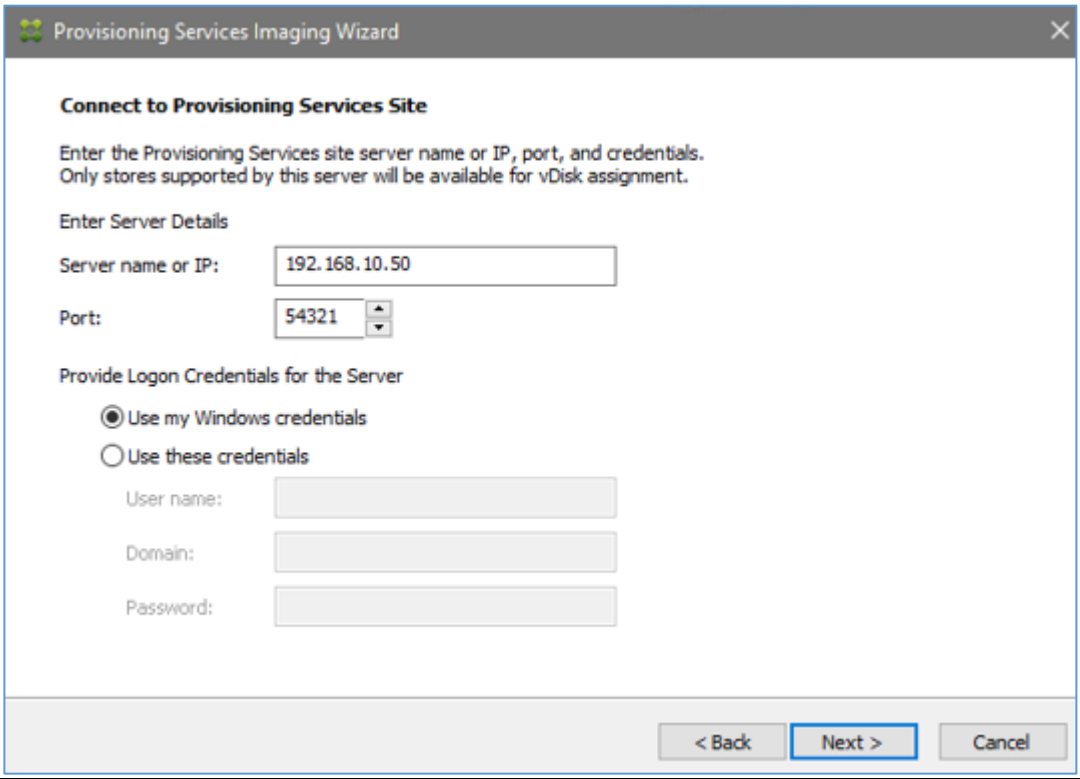
10. Click **Install** and wait while the installation completes.

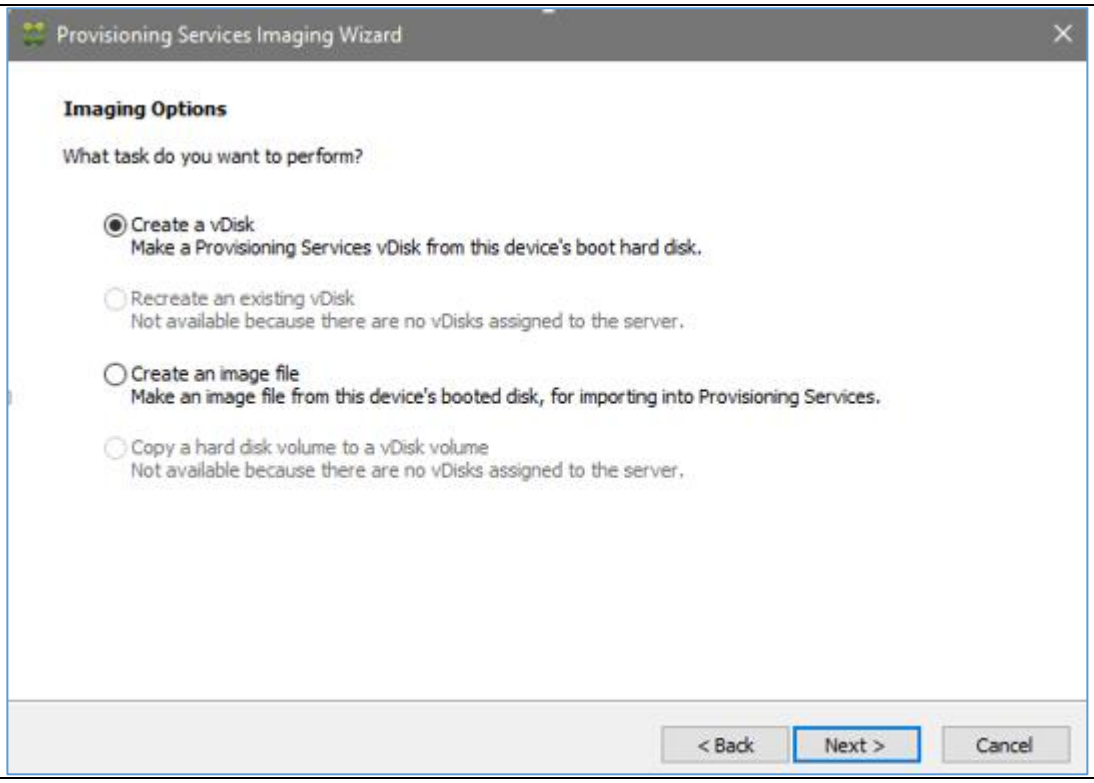


11. Before clicking finish in the installation wizard, verify that there are no third-party drivers like antivirus or malicious filter drivers.

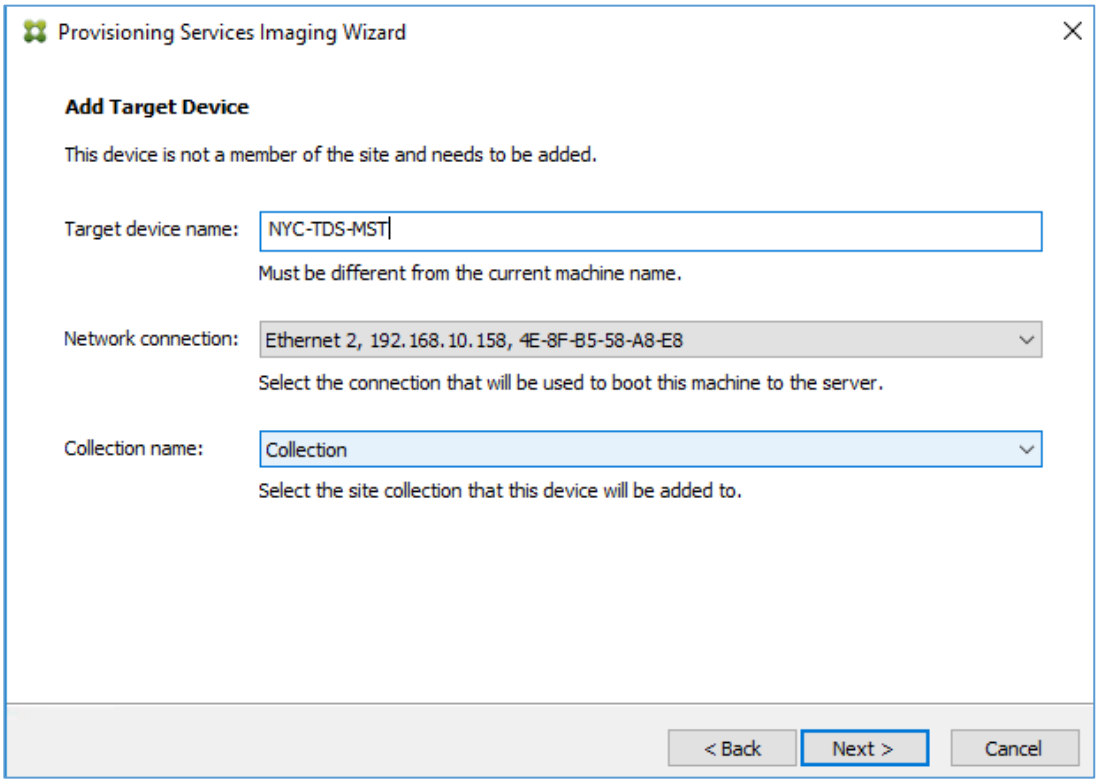
Right-click **Start** and select **Command Prompt**.

12.	Type **fltmc** and check that there are no 3rd Party Drivers on highest altitude. The drivers, 'luafv', 'FileInfo', 'CFsDep2' are displayed by default.  **Note:** Filter drivers sitting on highest altitude will load before PVS drivers and can affect the imaging process. The **Fltmc.exe** control program is a command-line utility for common mini filter driver management operations. In the above screenshot we see numerous filter drivers like **wcnfs, TSFairShare, storqosflt,** etc., which are loaded by Microsoft Windows and should not cause any issues. If any driver looks suspicious, it is advisable to study it and remove if it is not from a trusted source.
13.	Click **X** to close the **Command Prompt**.
14.	Go back to **Citrix Provisioning Services Target Device x64** screen: Verify that **Launch Imaging Wizard** is selected and then click **Finish**.

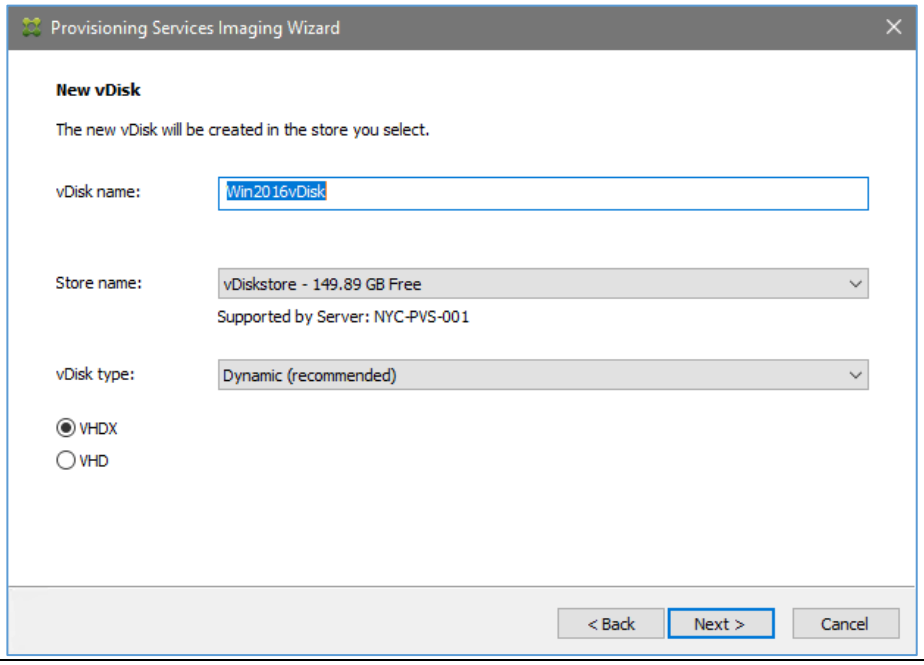
	
15.	Click **Next** on the welcome screen of the Imaging Wizard.
16.	Type **192.168.10.50** and then click **Next**. 
17.	Select **Create a vDisk** and then click **Next**.

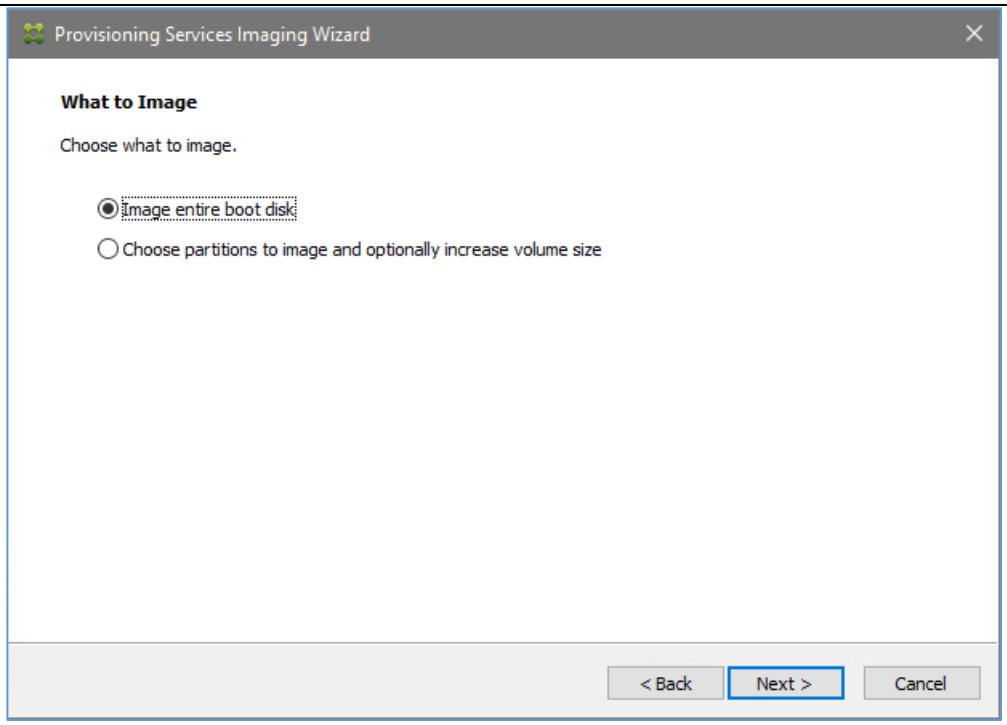


18. Type **NYC-TDS-MST** in the Target device name field and keeping everything else as default and click **Next**.



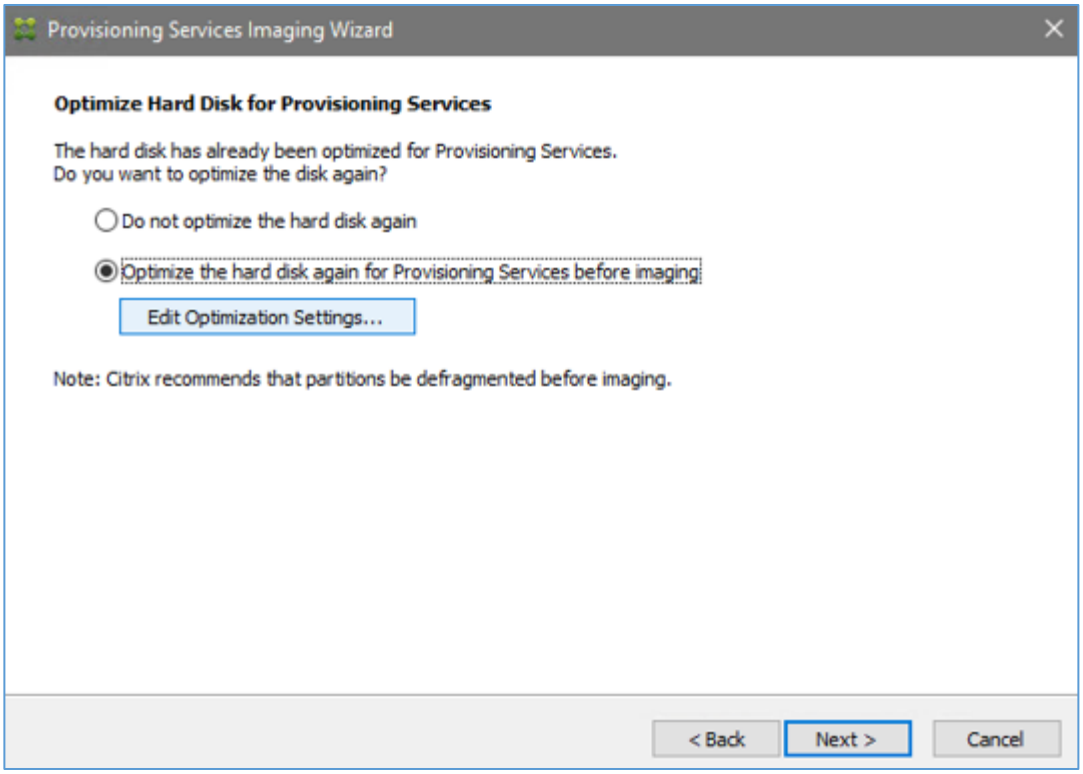
Note: The MAC address in the screesnhot will not match with the lab environment.

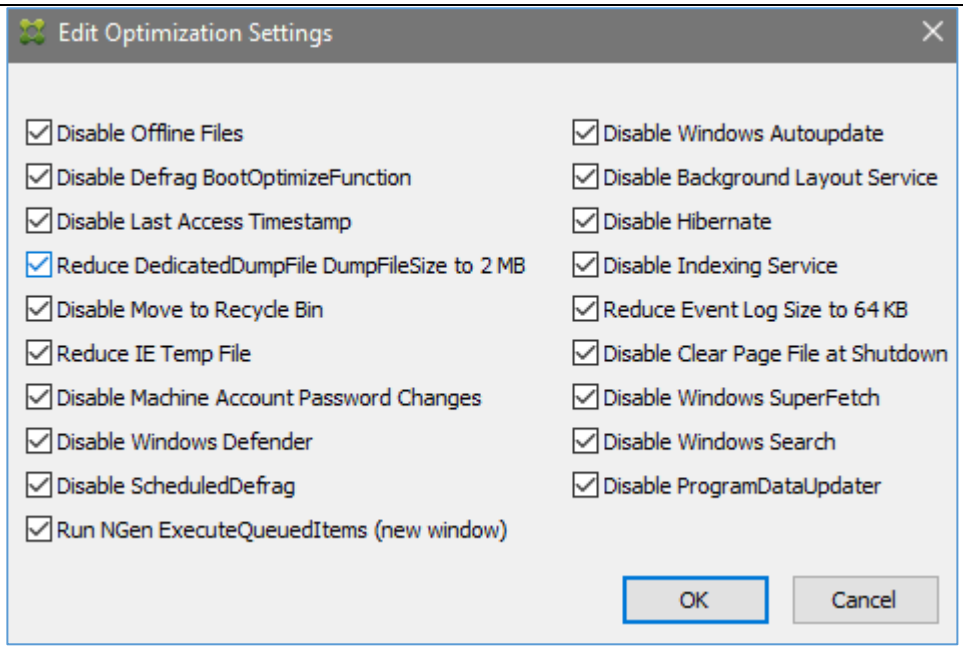
19.	Type **Win2016vDisk** in vDisk name. Select **vDiskStore** from the Store name drop-down. Select **Dynamic** as vDisk type Select **VHDX** format and then click **Next**. **Note:** The Fixed vDisk type allocates 100% of the space allocated for the vDisk immediately. The Dynamic vDisk type allocates space as it is needed. A Dynamic vDisk starts out small and then grows up to the maximum amount of space allocated as it is needed. VHDX is the new virtual hard disk format and has some important advantages over VHD in terms of capacity and performance. 
20.	Select **None** in the **Microsoft Volume Licensing** screen and then click **Next**.
21.	Select **Image entire boot disk** and then click **Next**. **Note:** There are not multiple boot partitions to select from. The second option can be used when we the Master Target Device has multiple partitions to choose from or when the volume size needs to be increased.



Click **Yes** in the confirmation message.

22. Select **Optimize the hard disk again for Provisioning Services before imaging** and click **Edit Optimization Settings**.

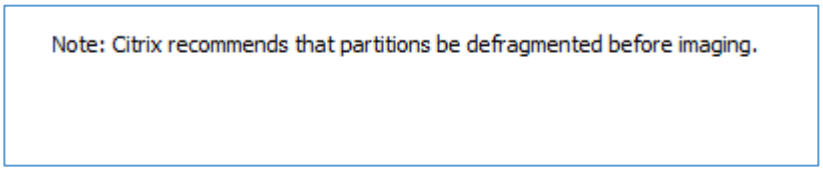




Note: It is recommended to go through all the default optimizations to verify if anything conflicts with company policies.

23. After reviewing the optimizations, click **OK** and then click **Next**.

Observe the note.

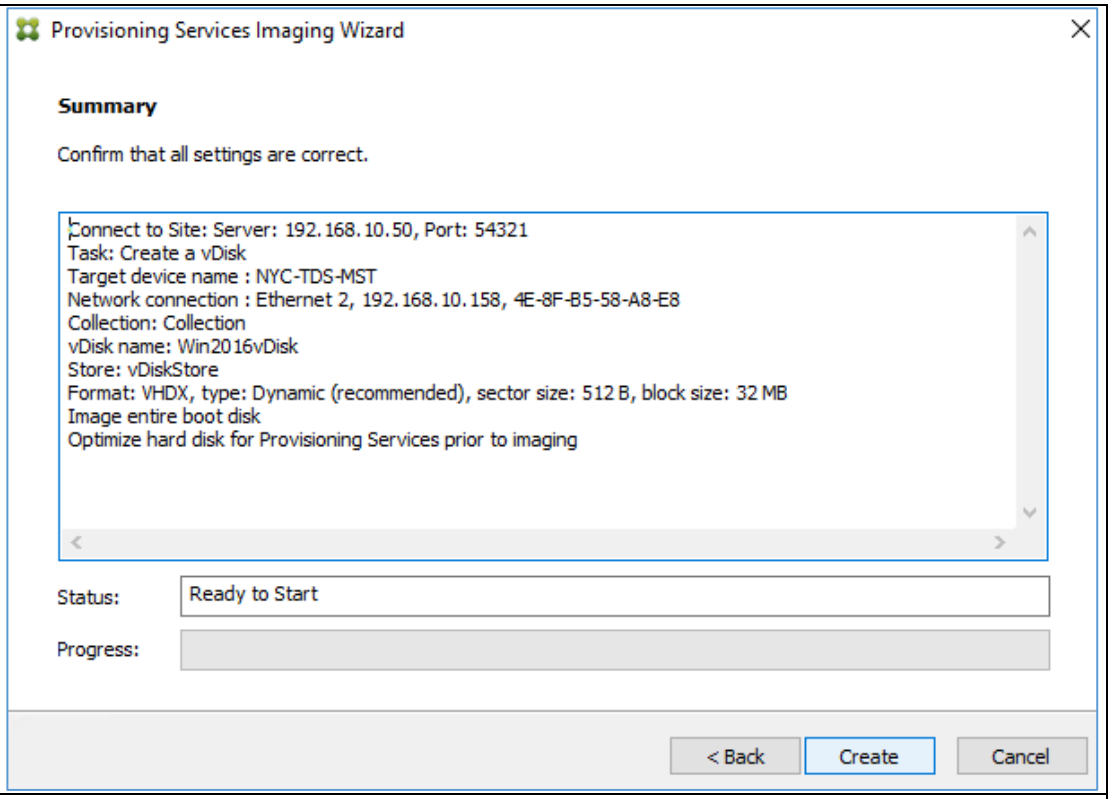


Click **Next**.

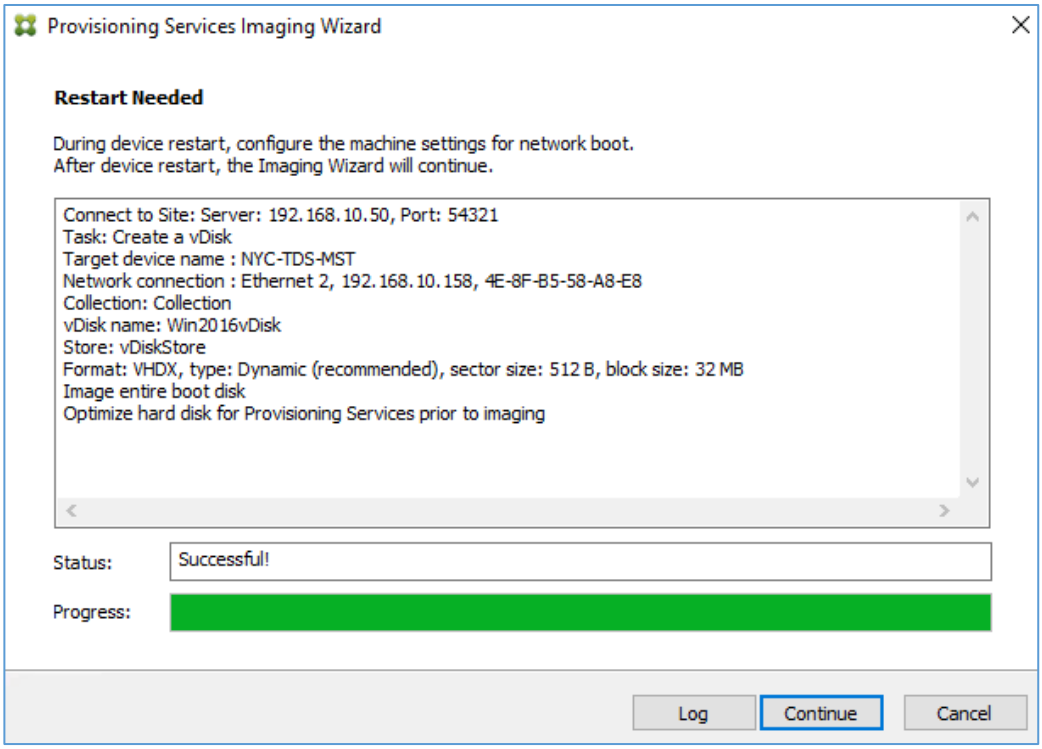
Note: The main advantage of using dynamic disks is that it reduces the amount of storage required for virtual disks. This leads to lower storage costs and allows for easier virtual disk management. However, over time, dynamic disks will grow as data is added to the virtual disk. When data is removed from the disk, the size of the virtual disk does not decrease. The virtual disk size remains at the largest amount of data size that was ever stored in the VHD(X).
In order to maintain the advantages of using dynamic disks, it is important to perform disk defragmentation, because files are constantly being written and deleted from a dynamic disk. This will move all of the data to the front of the disk, which will increase performance. Nothing has been added to vDisk at this time, so it does not require defragmentation.

Note: Please ignore if you do not see this note.

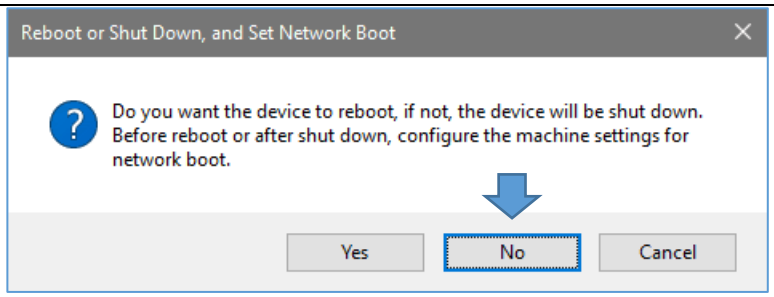
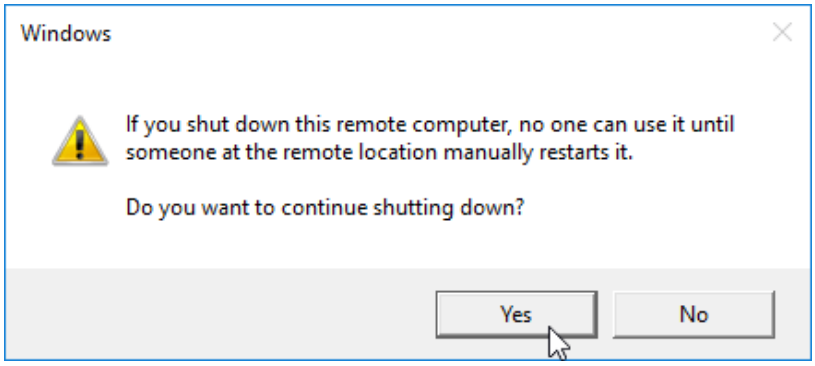
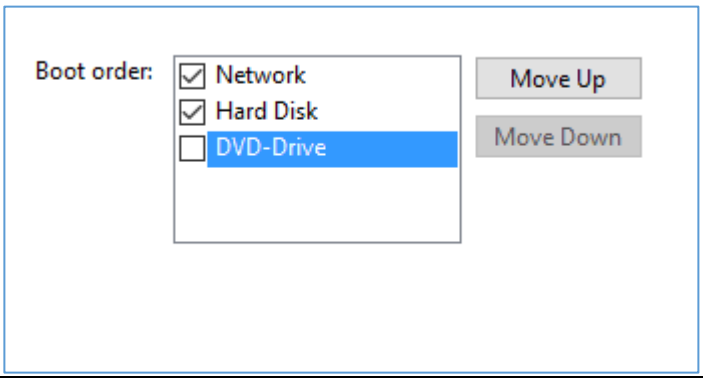
24. Verify the **Summary** and click **Create**.

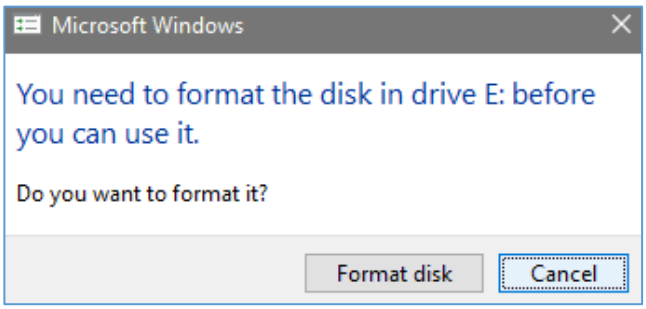
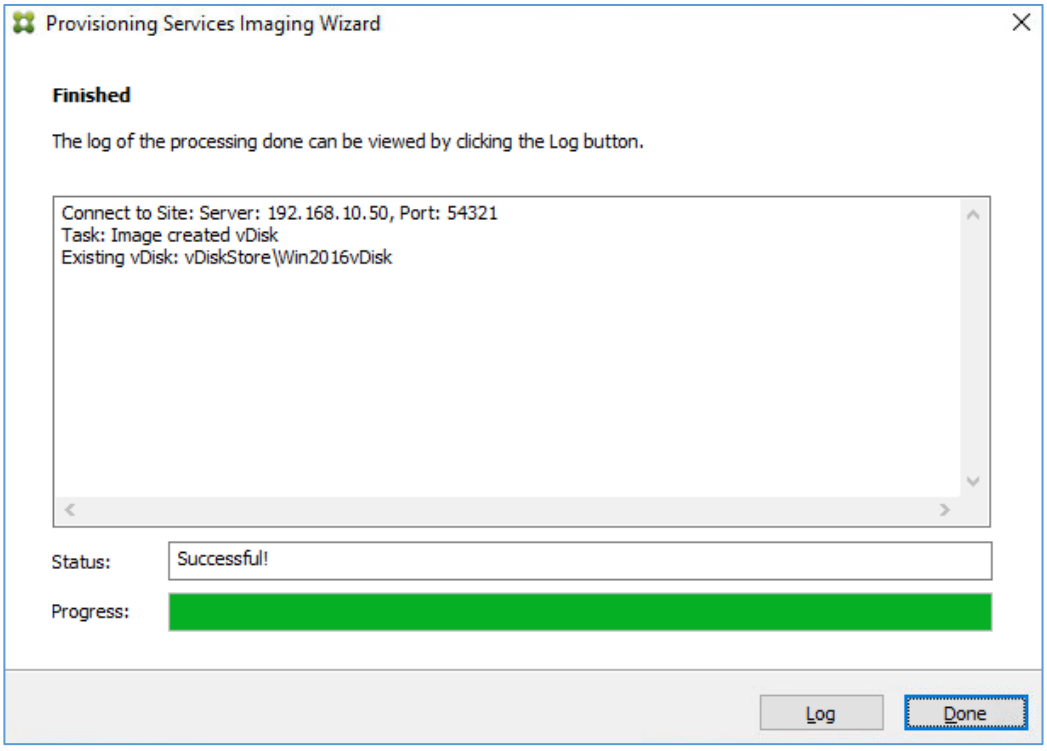


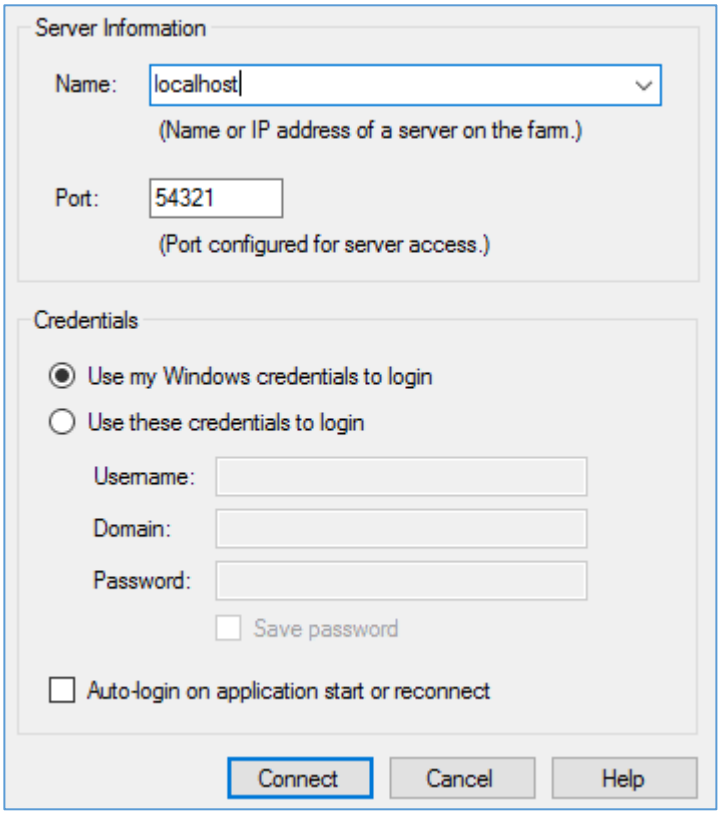
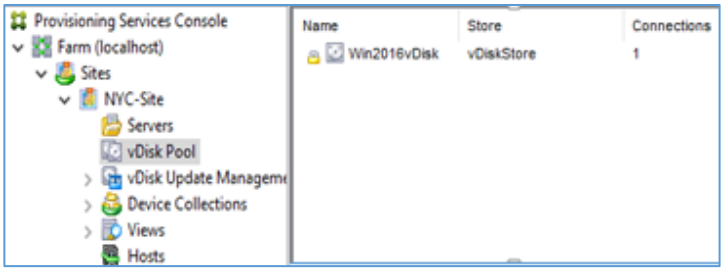
25. Verify **Status** message is **Successful** and click **Continue**.

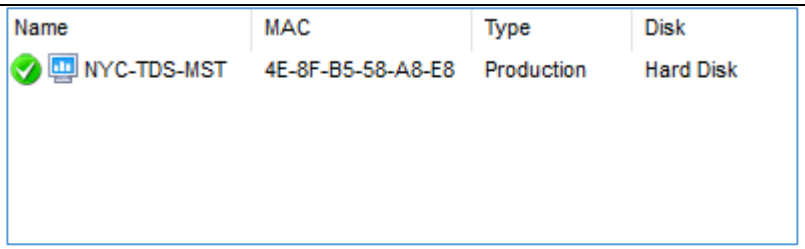
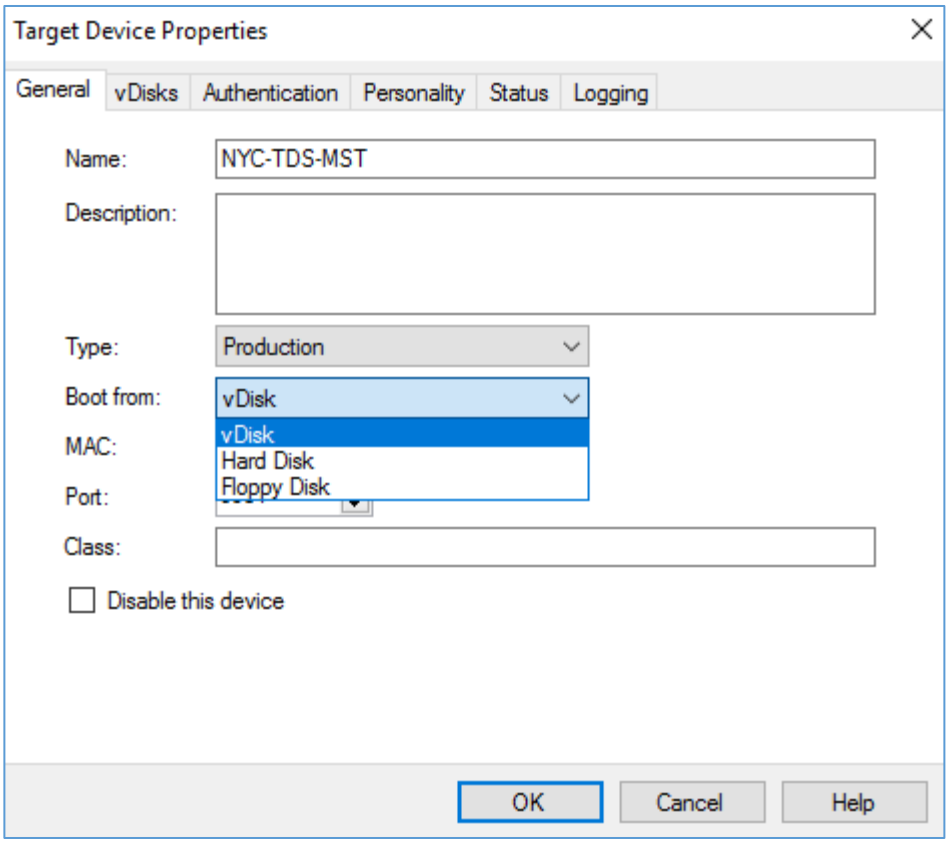


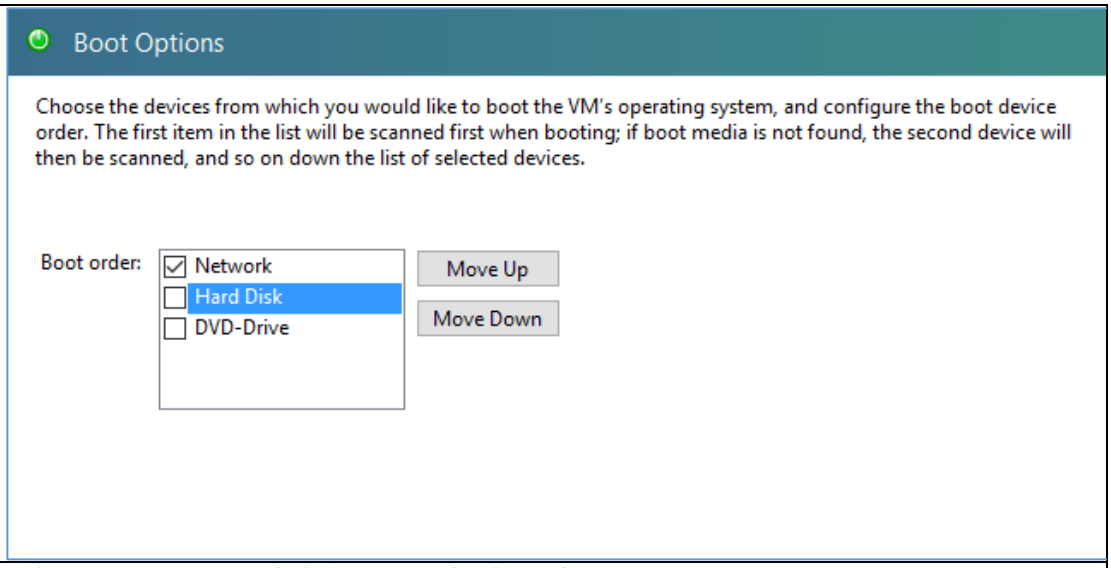
26. When asked to reboot, click **No** to shut down the machine. This gives you time to reconfigure the machine to boot from the network or ISO.

	
27.	Click **Yes** to shut down the machine. 
28.	Using **XenCenter,** eject the ProvisioningServices installation media from **PVS-SRV-MST**. To eject the installation media ISO, select **PVS-SRV-MST** in the left pane of XenCenter. In the right pane, select the **Console** tab and click **Eject** to remove **ProvisioningServices713.iso**.from the DVD-Drive 1. **Note**: The Eject option can be difficult to see. It is an underlined word to the right side of the DVD-Drive 1 drop-down menu.
29.	Click **PVS-SRV-MST** in XenCenter, click the **General** tab and then click **Properties** and select **Boot Options**.
30.	Click **Move Up** until the **Network** option is at the top of the list and **Hard Disk** is second, deselect **DVD-Drive** and click **OK**. 
31.	Right-click **PVS-SRV-MST** in left pane and select **Start**. **Note**: You may want to switch to XenCenter to monitor the progress. To do this, select **PVS-SRV-MST** in the left pane and the Console tab in the right pane.

32.	Once the machine finishes booting, using the Remote Desktop Connection manager, connect to **PVS-SRV-MST**. To login **PVS-SRV-MST** right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the Password.
33.	After you log on, you will see the Imaging Wizard progress window for the vDisk capture process. Do not restart the VM until the vDisk imaging process completes. **Note:** If prompted for **Format** of the disk, click cancel for both drive E: and drive F. 
34.	Click **Done** when **Status** shows successful.  **Note:** Please shut down all unneeded virtual machines while performing this exercise. The Imaging Process will take approximately 10-20 minutes.
35.	Using the Remote Desktop Connection manager, connect to **NYC-PVS-001**. To login to **NYC-PVS-001**, right-click this machine and choose **Connect server**.

	Note: The following credentials are used to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password.
36.	Click **Start** and click **Provisioning Services Console**. **Note**: Ignore if console is already open and jump to step 37.
37.	Type **localhost** and click **Connect**.  **Note**: We are typing localhost in name field, because Provisioning Services is installed locally on this server.
38.	Browse **Farm > Sites > NYC-Site > vDisk Pool** and verify **Win2016vDisk** is created.  **Note:** If vDisk is not seen, refresh the console.
39.	Browse **Farm > Sites > NYC-Site > Device Collections > Collection** and verify **NYC-TDS-MST** is created.

	 **Note:** If vDisk is not seen, refresh the console.
40.	Right-click **NYC-TDS-MST** and select **Properties**. Change **Boot from** drop-down menu to **vDisk**.  Click **OK**.
41.	Click **PVS-SRV-MST** in XenCenter and click the **General** tab, and then click **Properties** and select **Boot Options**.
42.	Uncheck **Hard Disk** and click **OK,** so the machine now boots from the vDisk over the network and does not use its hard disk.

	
43.	Select **PVS-SRV-MST** in left pane and select **Shut Down**.

Key Takeaways:

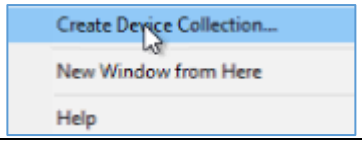
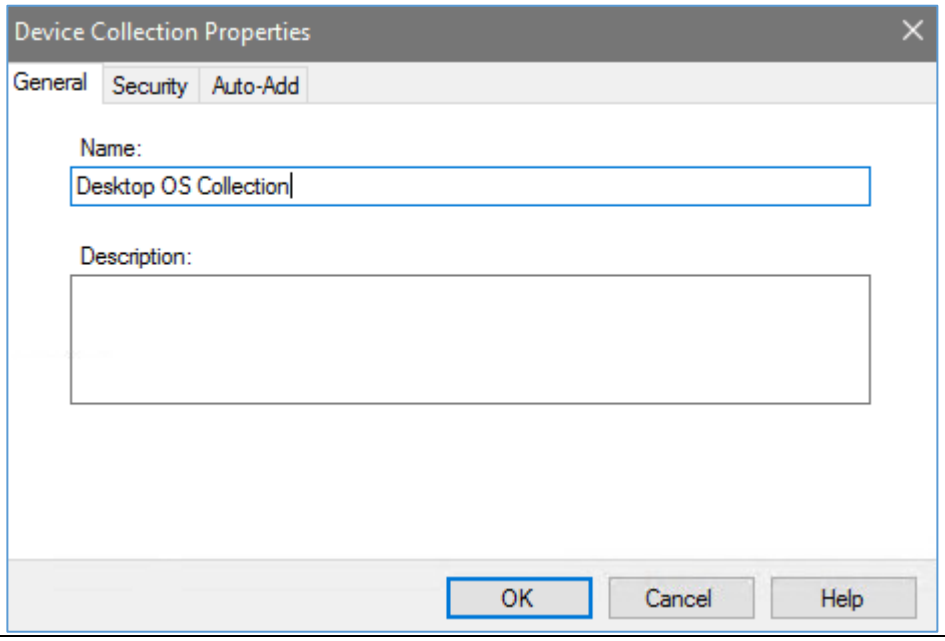
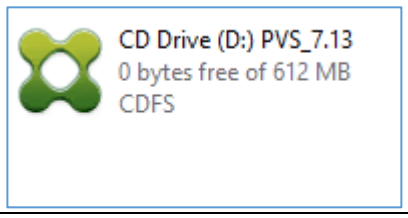
- The Provisioning Target Device Software is the component that allows a machine to attach a vDisk hosted on a Provisioning Services server and boot from the operating system hosted within the vDisk.
- The Imaging Wizard is installed by default with the Target Device Software.
- The Imaging Wizard can be used to capture the hard disk contents of a Master machine into a vDisk on the Provisioning Services server.
- Additionally, the Image Wizard can create a record for the Master machine in the PVS database, allowing the Master machine to boot via the network and attach the newly created vDisk.
- The Target Device software uses filter driver technology, so other similar 3rd party filter driver solutions should be carefully evaluated.

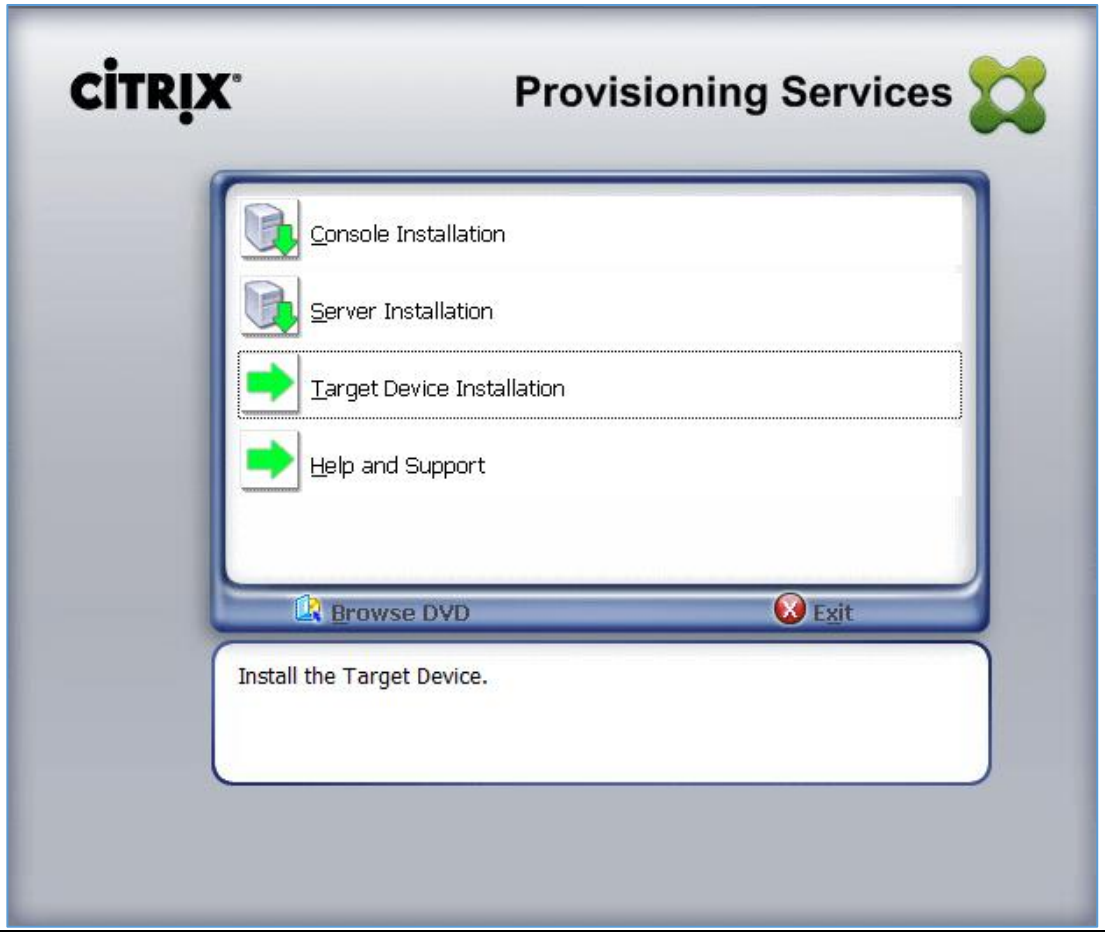
Exercise 17-2: Create VDisk for Desktop OS

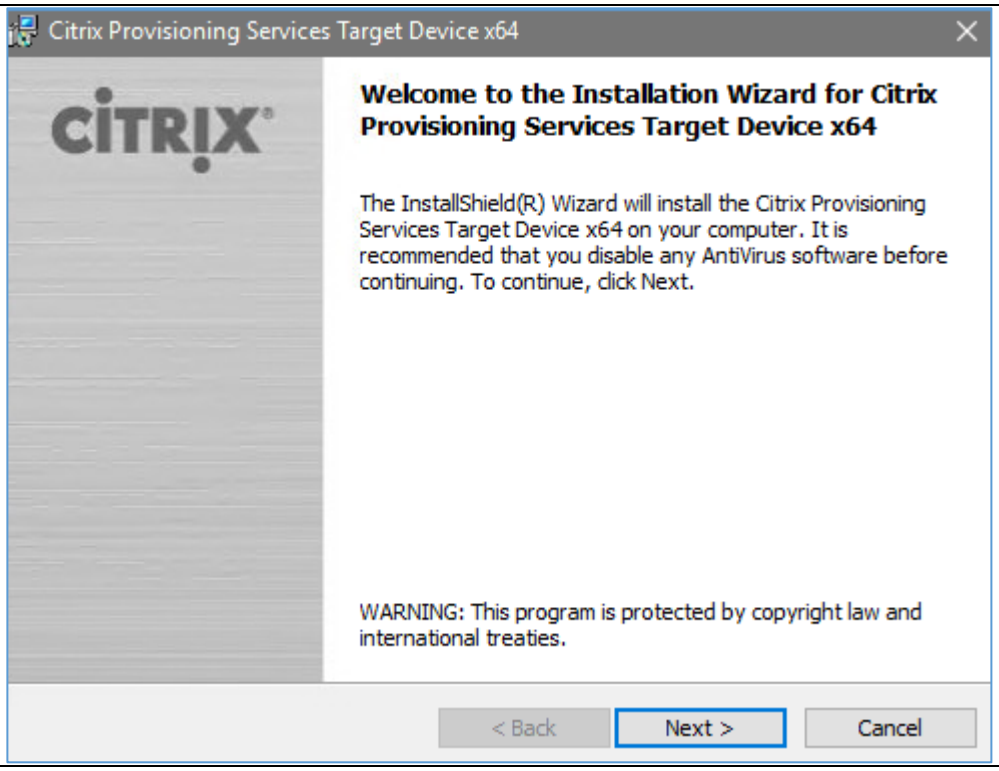
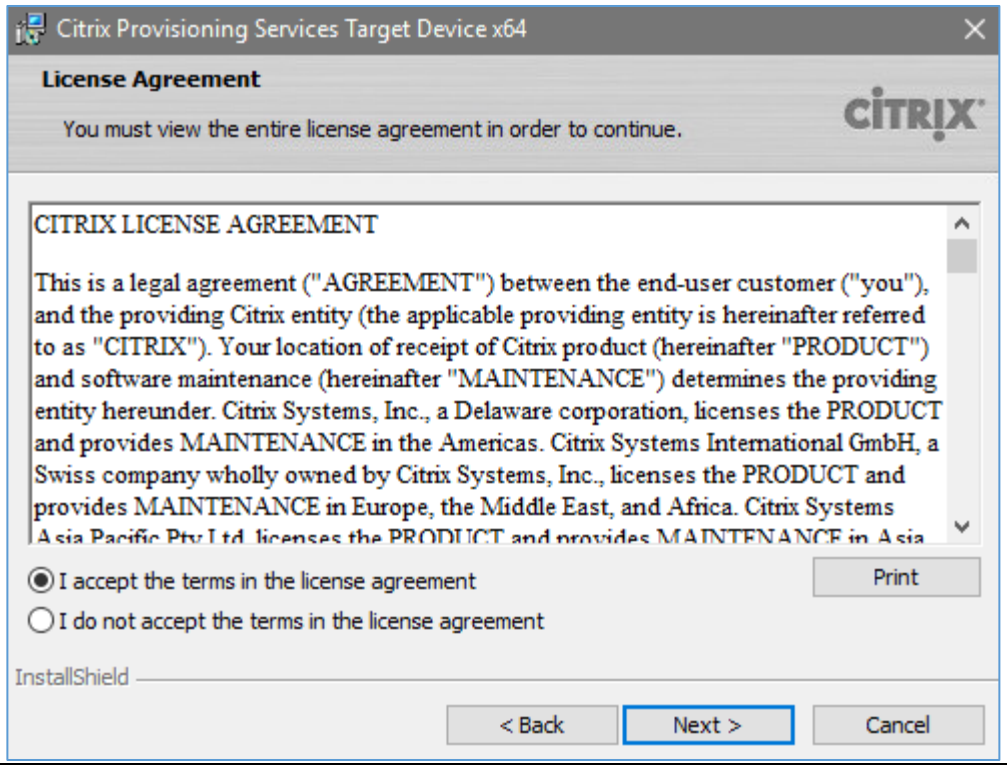
Scenario:

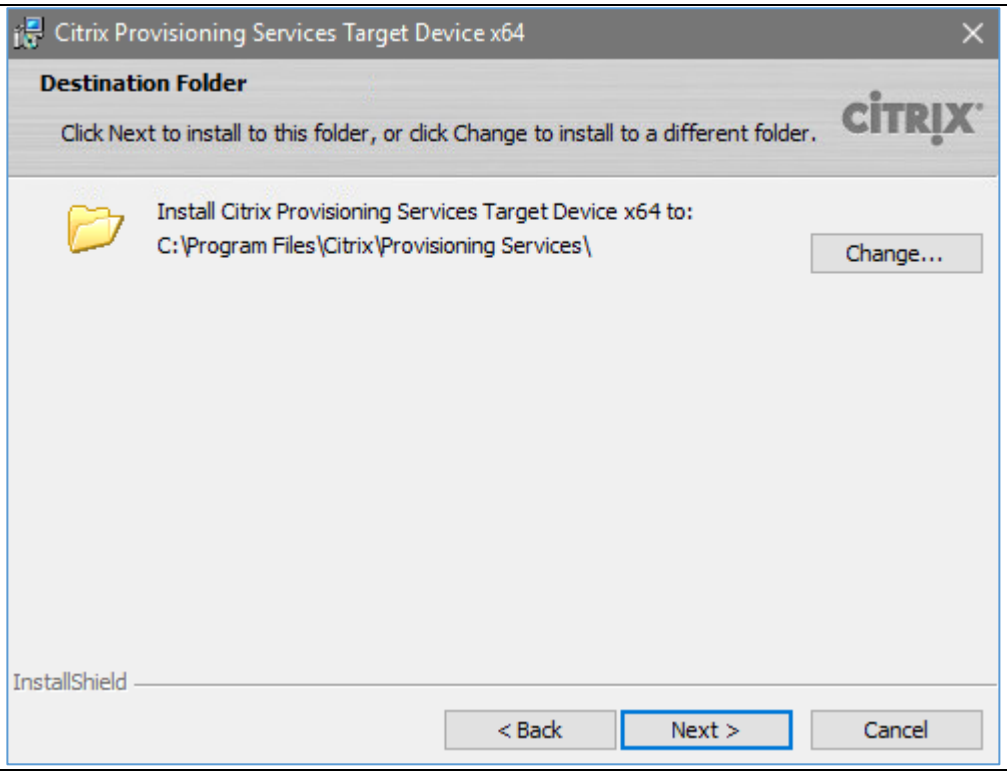
You are a Citrix Administrator at WW Labs, your Lead Citrix Architect has verified the VDA installation on Windows 10. Now your task is to capture the master image on to a new Provisioning Services vDisk.

Step	Action
1.	Using the Remote Desktop Connection manager, connect to **NYC-PVS-001**. To login **NYC-PVS-001** right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the Password.
2.	Click **Start** and click **Provisioning Services Console**. **Note:** Ignore if console is already open and jump to step 4.
3.	Type **Localhost** and click **Connect**.

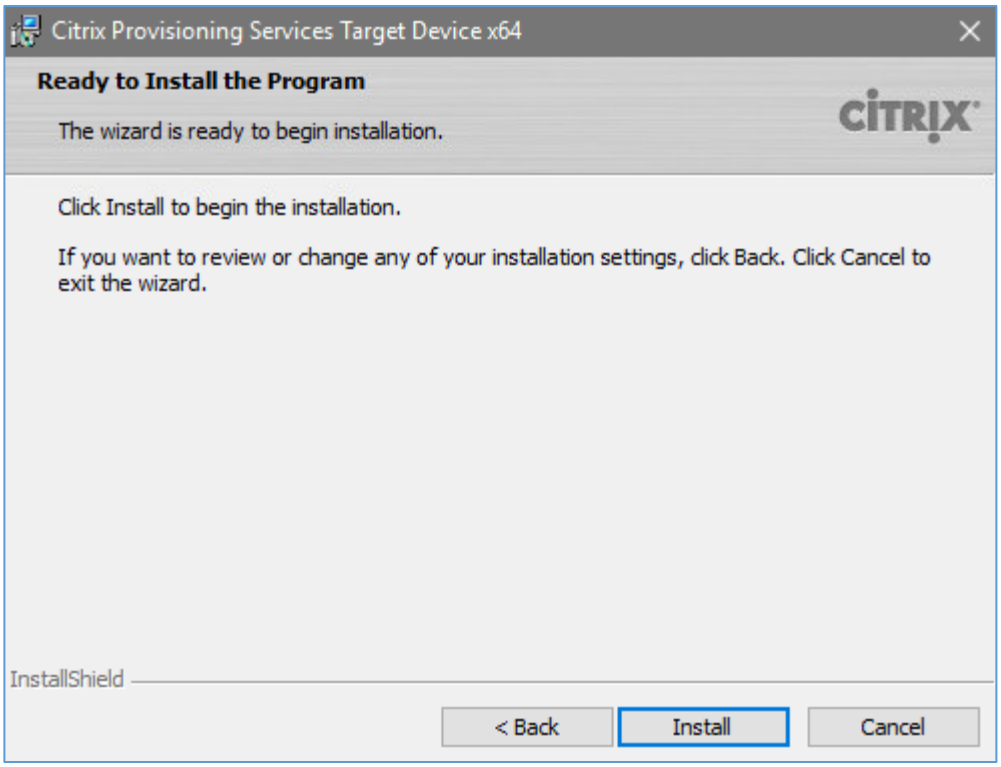
4.	Browse **Farm > Sites > NYC-Site > Device Collections**.
5.	Right-click **Device Collections** and select **Create Device Collection**. 
6.	Type **Desktop OS Collection** in the **Name** section and click **OK**. 
7.	Using **XenCenter** mount the **Provisioning Services** installation media ISO to **PVS-DTP-MST**. To mount the installation media ISO, select **PVS-DTP-MST** in the left pane of XenCenter. In the right pane, select the **Console** tab. Using the **DVD-Drive 1:** drop-down menu select **ProvisioningServices713.iso**. **Note**: If there are no ISOs listed in the **DVD-Drive 1:** drop-down menu, then the Local ISO SR that contains the ISO library may need to be re-scanned. In the left pane of **XenCenter** select the **Local ISO SR XS**. In the right pane select the **Storage** tab and click on the **Re-scan** button.
8.	Using the Remote Desktop Connection manager, connect to **PVS-DTP-MST**. To login **PVS-DTP-MST** right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the Password.
9.	Launch the **File Explorer** application from the Windows Taskbar or Start Menu and double-click the green Citrix logo next to **CD drive** under Devices and drives. 

	Note: If the installation does not launch from double-clicking the green Citrix logo next to **CD drive** under Devices and drives, then double-click on the **autorun.exe** file.
10.	Click **Target Device Installation** and then click **Target Device Installation** again. 
11.	Click **Next** on the Welcome screen of the Installation Wizard.

	
12.	Select **I accept the terms in the license agreement** and then click **Next**. 
13.	Click **Next** to accept the default selections.
14.	Click **Next** to accept the default destination folder.

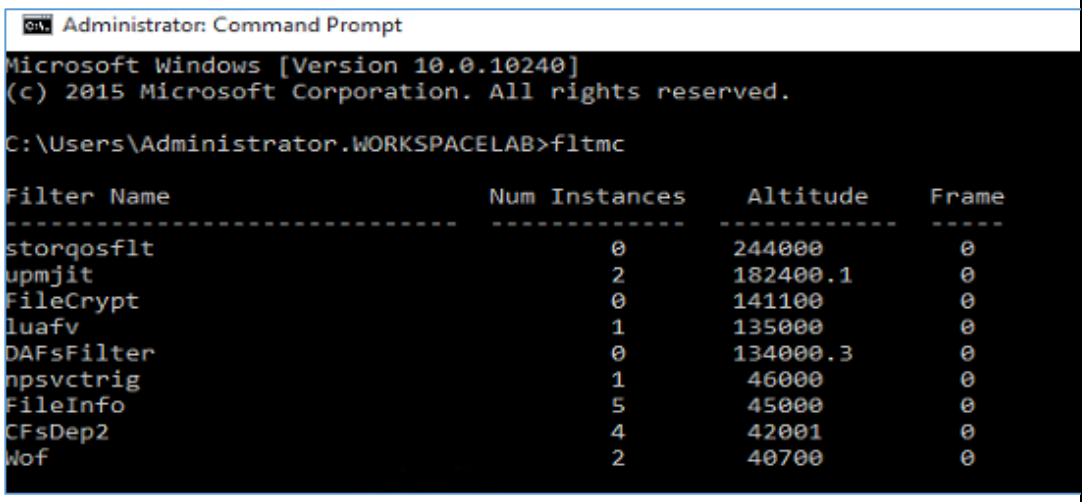


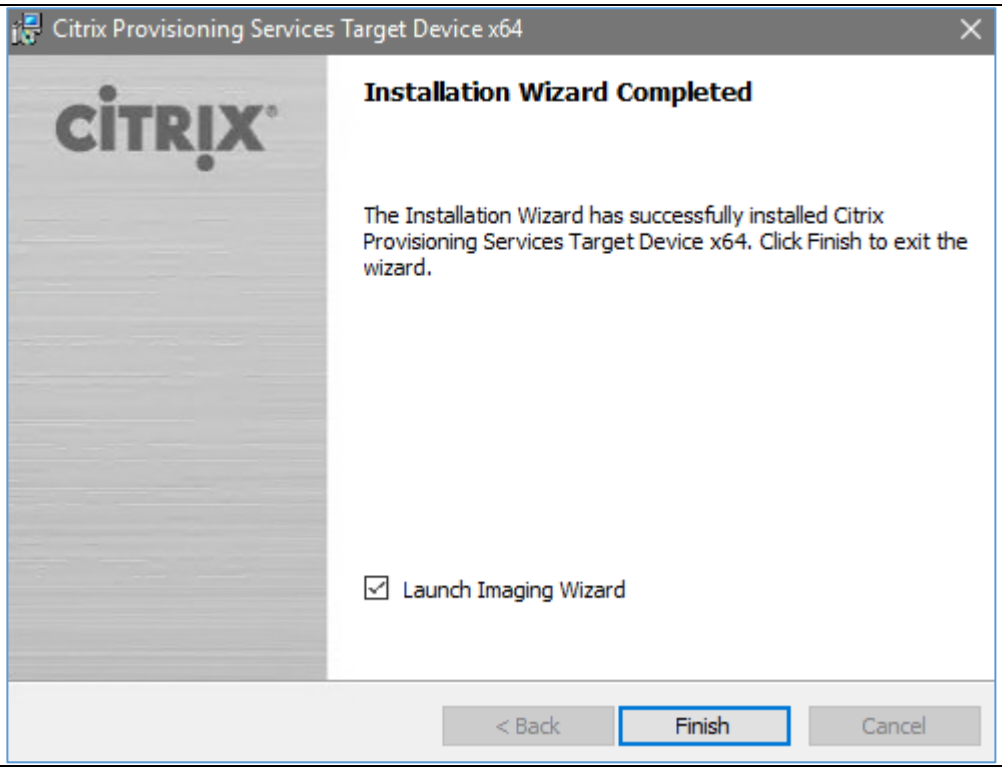
15. Click **Install** and wait while the installation completes.



16. Before clicking finish for installation Wizard, verify that there are not third-party drivers like antivirus or malicious filter drivers.

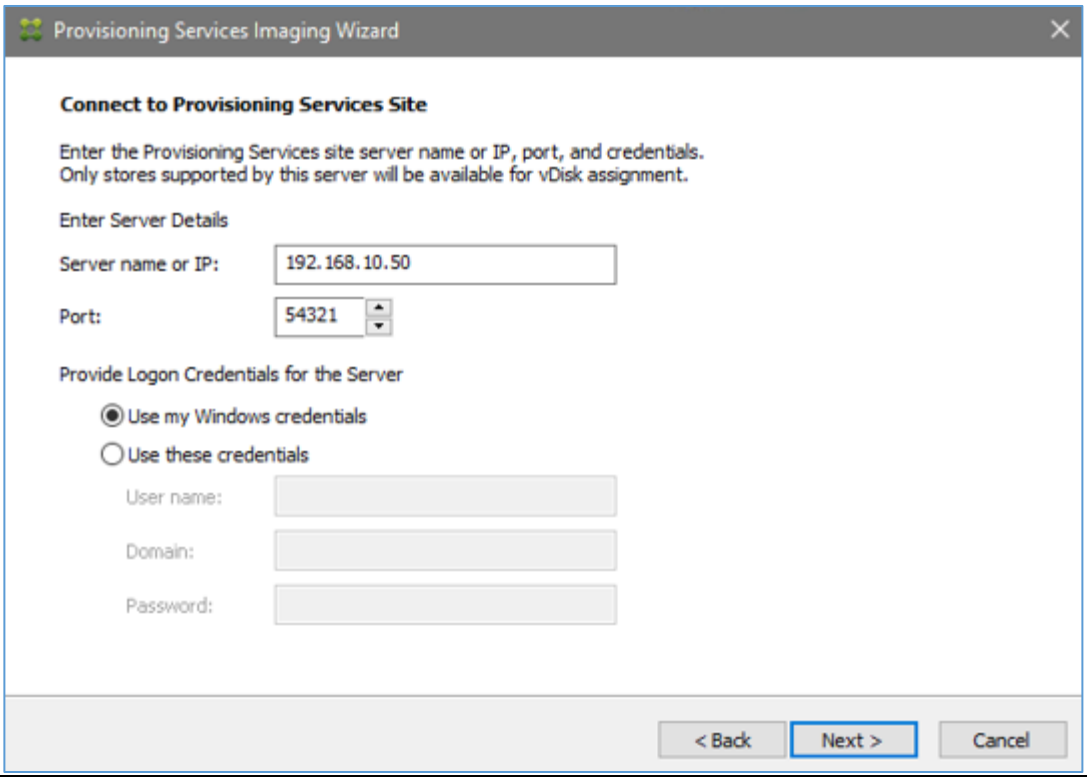
Right-click **Start** and select **Command Prompt**.

17.	Type **fltmc** and check that there is no 3rd Party Drivers on highest altitude. There should be 'luafv', 'FileInfo', 'CFsDep2' by default.  **Note:** Filter drivers sitting on highest altitude will load before PVS drivers and can affect the imaging process. **The Fltmc.exe** control program is a command-line utility for common minifilter driver management operations. Here in above screenshot we see filter drivers like **wcnfstorqosflt** which are loaded by **Microsoft Windows** and should not cause any issues. If we see any driver that looks to be suspicious, we should study about it and remove if it is not from a trusted source. **Note**: Drivers in screenshot might differ with respect to the lab environment.
18.	Click **X** to close the **Command Prompt**.
19.	Go back to Citrix Provisioning Services Target Device x64 screen: Verify that **Launch Imaging Wizard** is selected and then click **Finish**.

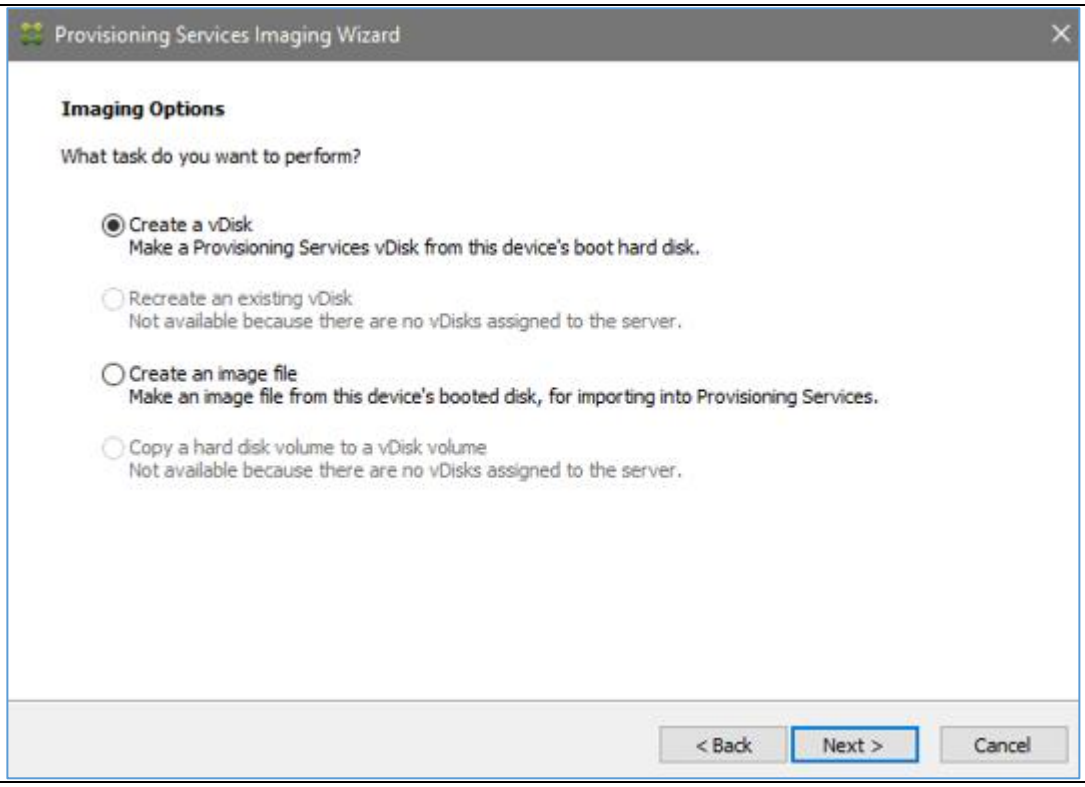


20. Click **Next** on the welcome screen of the Imaging Wizard.

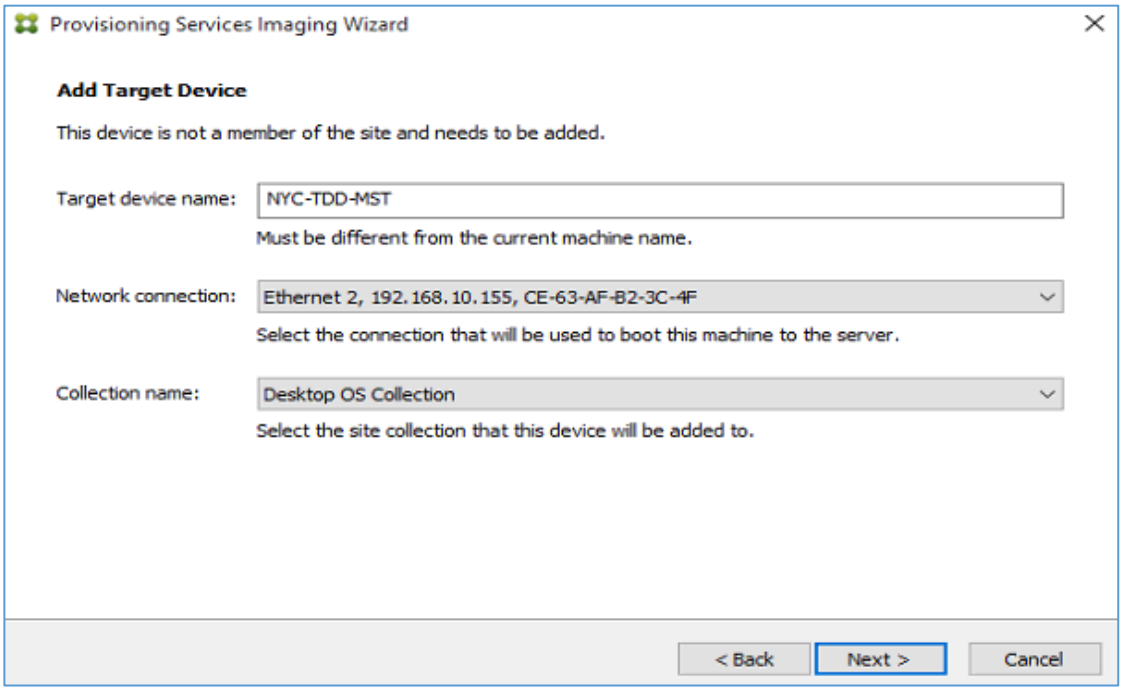
21. Type **192.168.10.50** and then click **Next**.



22. Select **Create a vDisk** and then click **Next**.

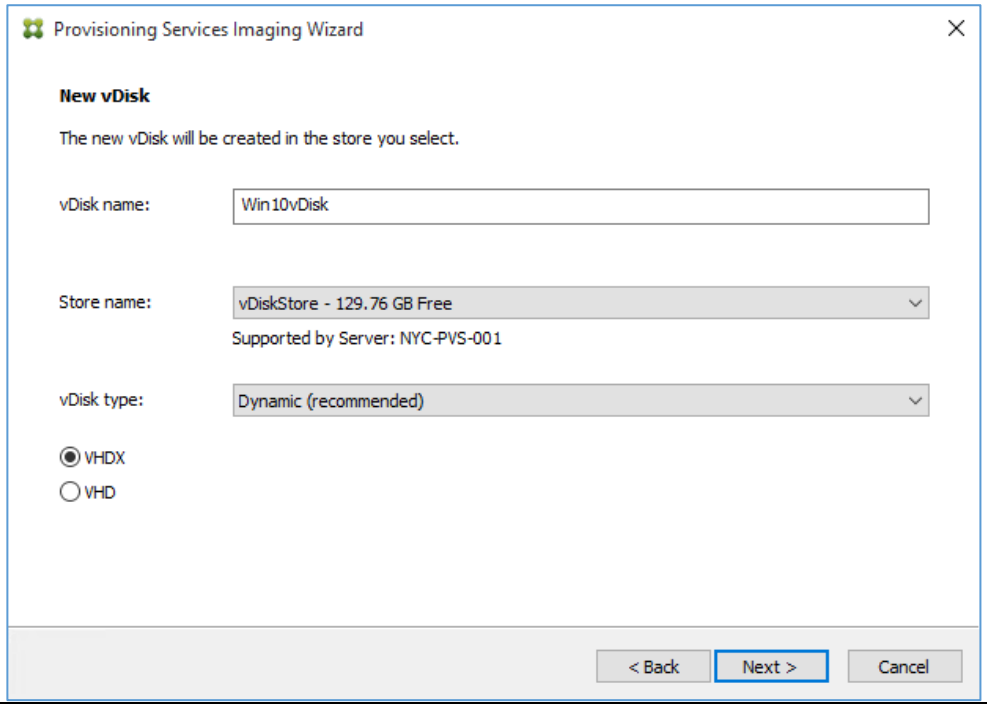


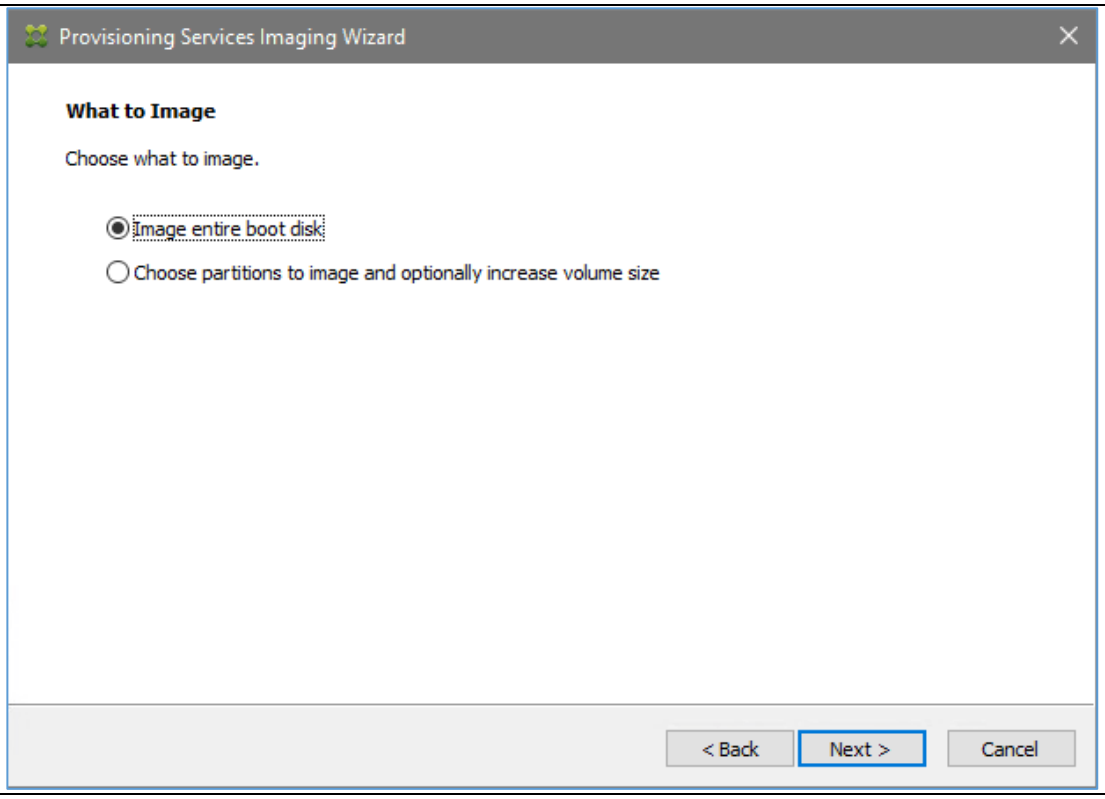
23. Type **NYC-TDD-MST** in Target device name and select **Desktop OS Collection** from **Collection name** drop-down and click **Next**.



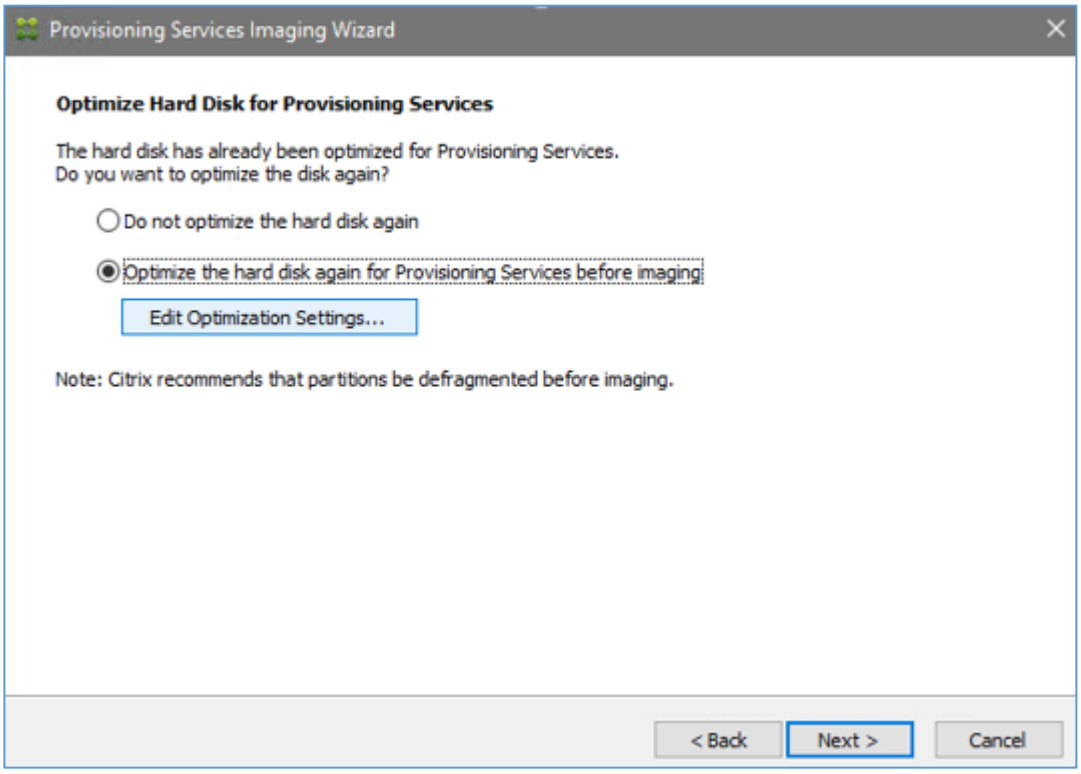
Note: MAC address will differ with respect to lab environment.

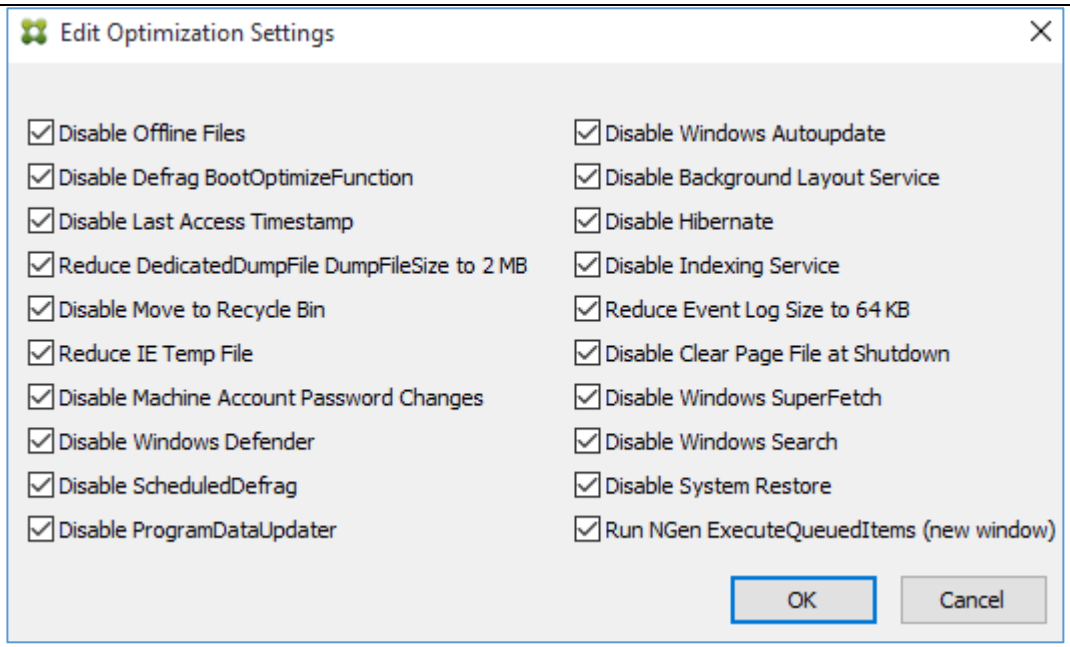
24. Type **Win10vDisk** in vDisk name.
Select **vDiskStore** from the Store name drop-down.
Select **Dynamic** as vDisk type.

	Select **VHDX** format and then click **Next**. **Note:** • The **Fixed vDisk** type allocates 100% of the space allocated for the vDisk immediately. The **Dynamic** vDisk type allocates space as it is needed. A Dynamic vDisk starts out small and then grows up to the maximum amount of space allocated as it is needed. • VHDX is the new Virtual hard disk format over legacy VHD format and some important advantages over VHD in terms of capacity and performance. 
25.	Select **None** in **Microsoft volume Licensing** and then click **Next**.
26.	Select **Image entire boot disk** and then click **Next**. **Note:** Second option can be used when we have multiple partitions to choose from or when we want to increase the volume size**.**



27. Select **Optimize the hard disk again for Provisioning before imaging** and click **Edit Optimization Settings**.

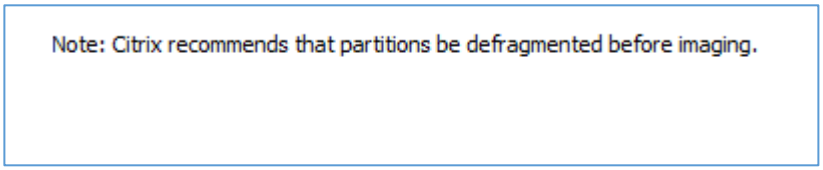




Note: It's good to go through all the default optimizations to verify if anything conflicts with the company's policies.

28. Click **OK** and then click **Next**.

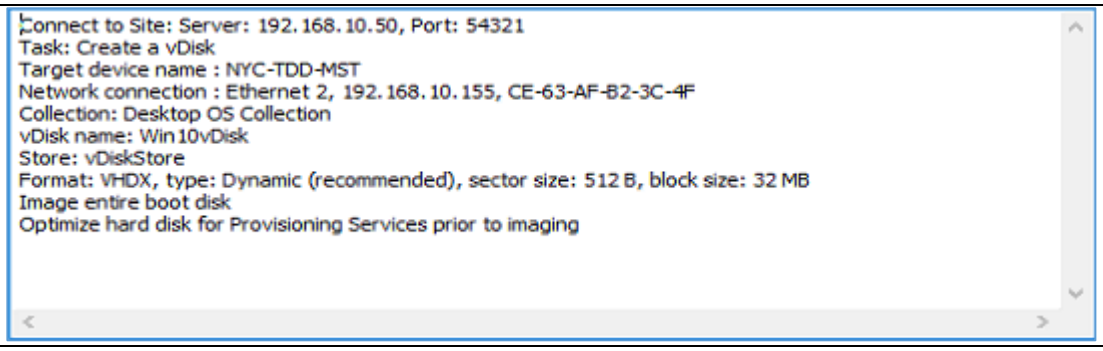
Note: Before clicking Next, look at the Note Specified.



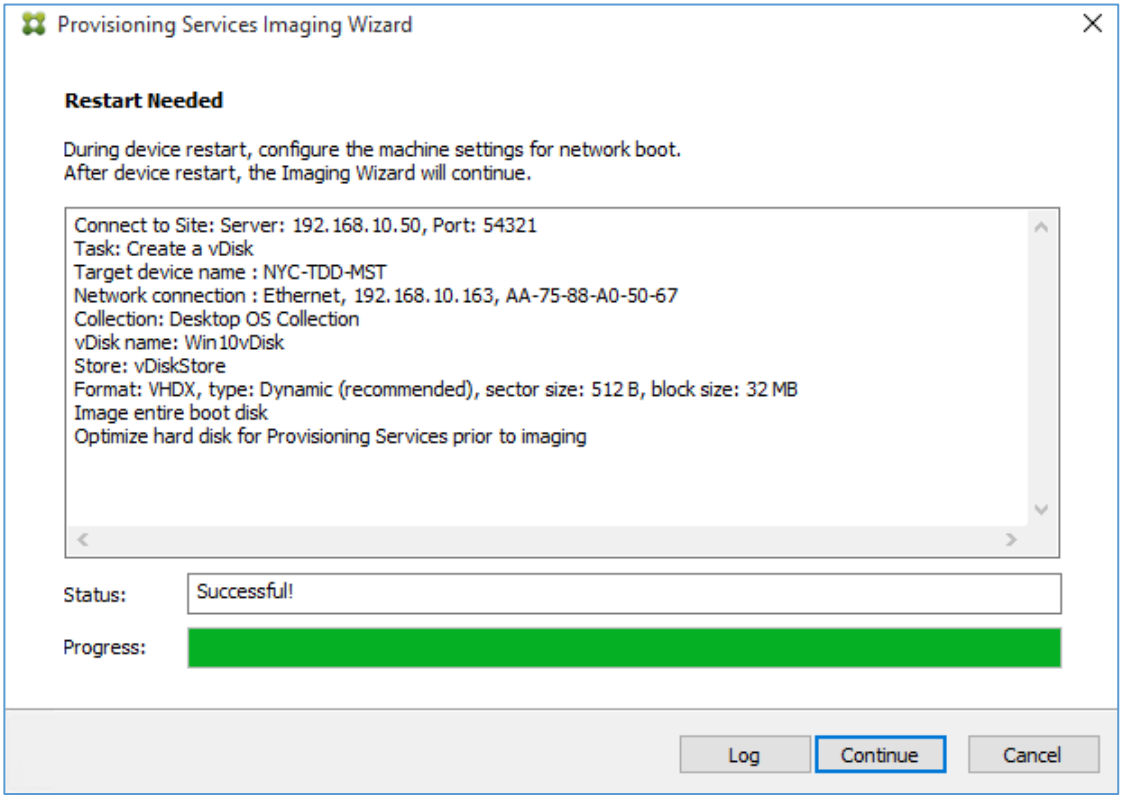
The main advantage of using dynamic disks is that it reduces the amount of storage required for virtual disks. This leads to lower storage costs and allows for easier virtual disk management. However, over time, dynamic disks will grow as data is added to the virtual disk. When data is removed from the disk, the size of the virtual disk does not decrease. The virtual disk size remains at the largest amount of data size that was ever stored in the VHD.
In order to maintain the advantages of using dynamic disks, it is important to perform **defragmentation.** Because, files are constantly being written and deleted from a dynamic disk, it is important to perform regular defragmentation of the virtual disk. This will move all the data to the front of the disk, which will increase performance.
As there is nothing we have added to vDisk at this time. We do not require defragmentation.

Note: Please ignore if you do not see this note.

29. Verify the **Summary** and click **Create**.

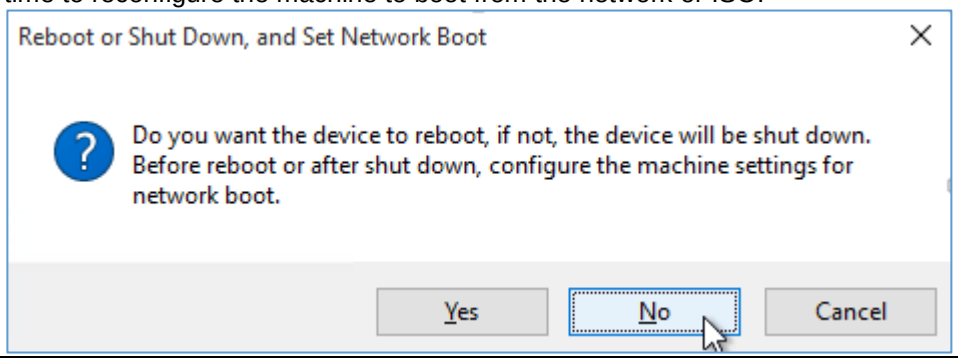


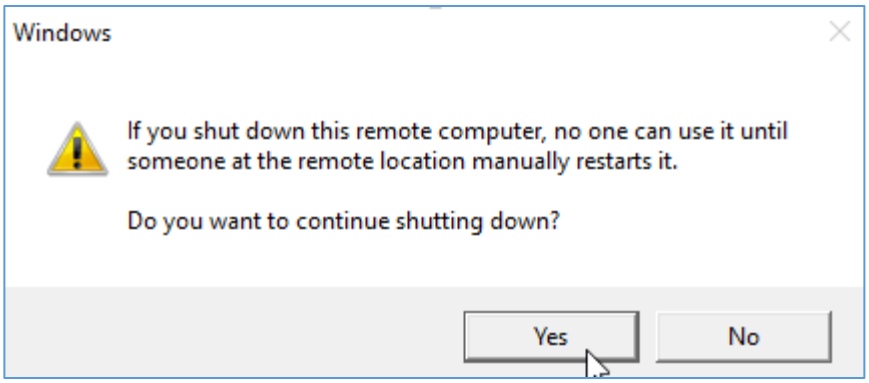
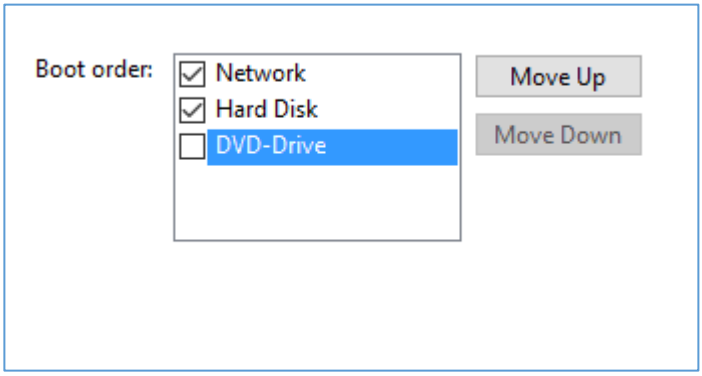
30. Verify **Status** is **Successful** and click **Continue**.

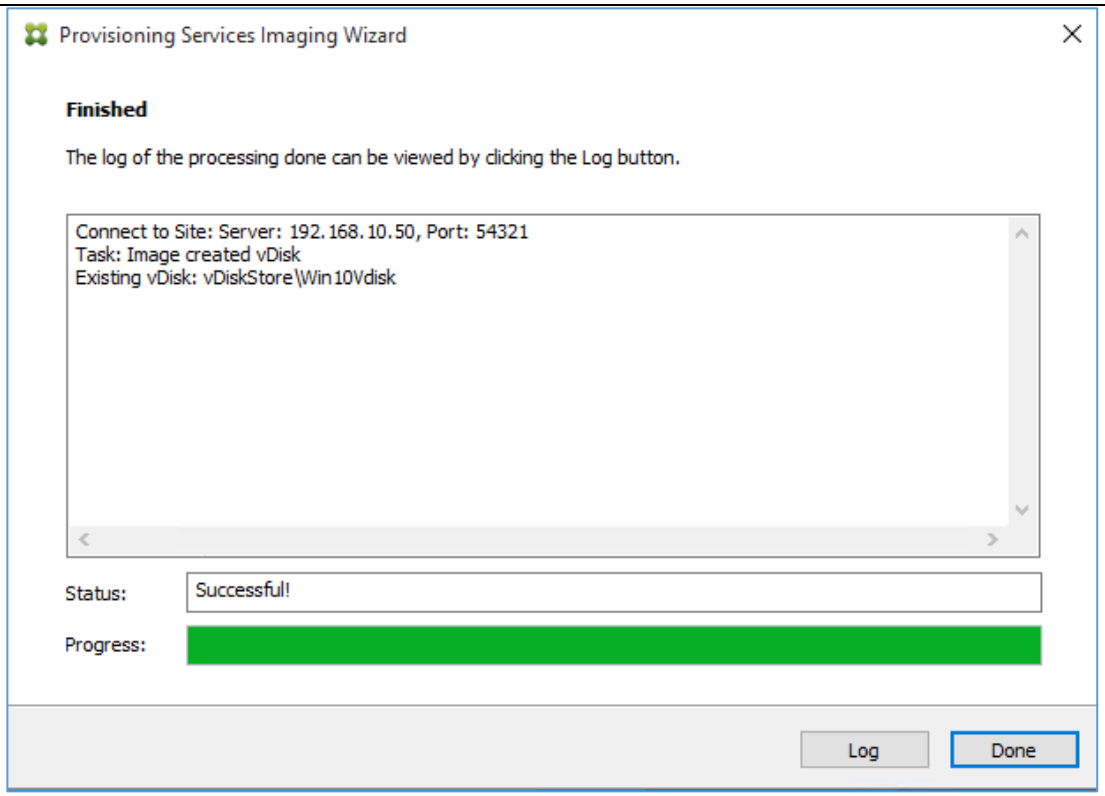
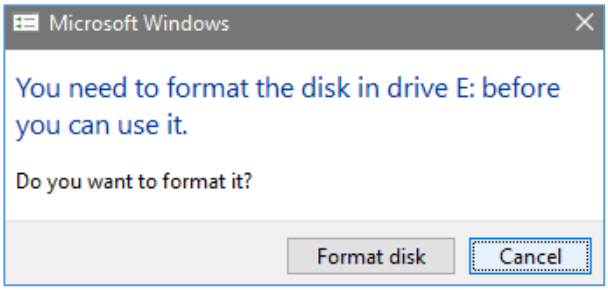


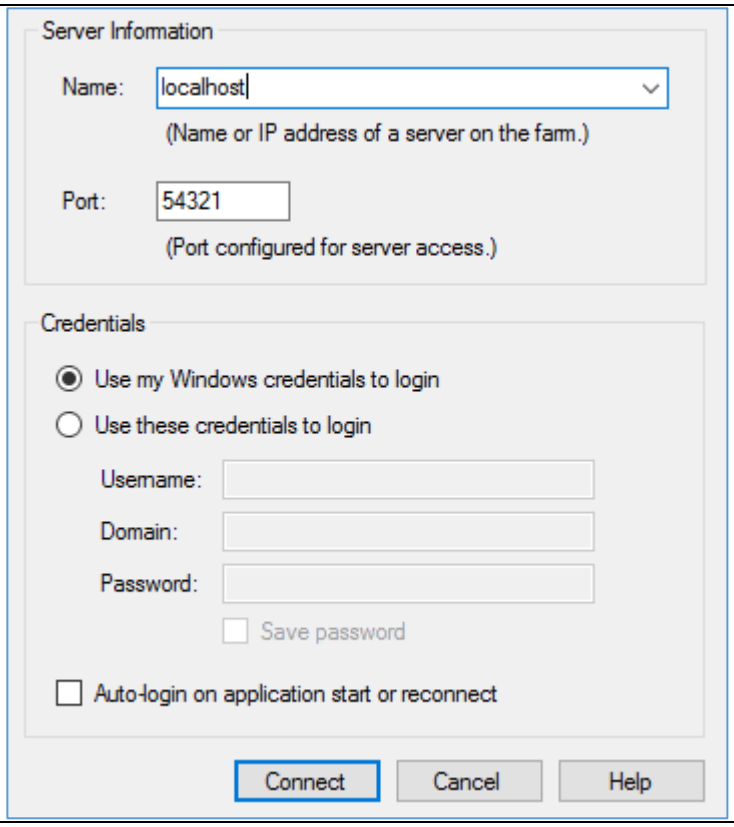
Note: IP address of the Master Target might differ with respect to lab environment.

31. When asked to reboot, click **No** to reboot and **Yes** to shut down the machine. This gives you time to reconfigure the machine to boot from the network or ISO.

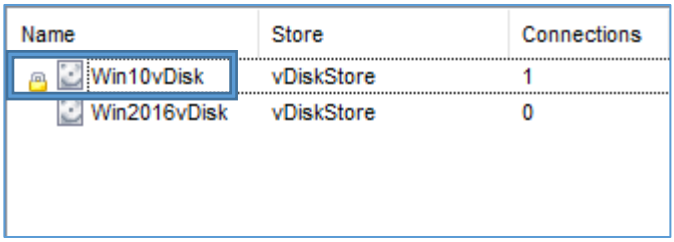


	
32.	Using **XenCenter** eject the Provisioning Services installation media from **PVS-DTP-MST**. To eject the installation media ISO, select **PVS-DTP-MST** in the left pane of XenCenter. In the right pane, select the **Console** tab and click **Eject** to remove **ProvisioningServices713.iso**. from the DVD-Drive 1. **Note**: The Eject option can be difficult to see. It is an underlined word to the right side of the DVD-Drive 1 drop-down menu.
33.	Select **PVS-DTP-MST** in XenCenter, click the **General** tab and then click **Properties.** Select **Boot Options**.
34.	Click **Move Up** until the **Network** option is at the top of the list and **Hard disk** at second. Deselect **DVD-Drive** and click **OK**. 
35.	Right-click **PVS-DTP-MST** in left pane and select **Start**. **Note**: You may want to switch to XenCenter to monitor the progress. To do this, select **PVS-DTP-MST** in the left pane and the Console tab in the right pane.
36.	Once the machine is UP. Using the Remote Desktop Connection manager, connect to **PVS-DTP-MST**. To login **PVS-DTP-MST** right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the Password.
37.	After you log on, you will see the Imaging Wizard progress window for the vDisk capture process. Do not restart the VM until the vDisk imaging process completes.
38.	Click **Done** when **Status** shows successful.

	 **Note:** Please shut down all unneeded virtual machines while performing this exercise. The Imaging Process will take approximately 10-20 minutes. **Note:** If prompted for Format of the disk, click **Cancel** for both drive E: and drive F. 
39.	Using the Remote Desktop Connection manager, connect to **NYC-PVS-001**. To login **NYC-PVS-001** right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the password.
40.	Click **Start** and click Provisioning Services Console. **Note**: Ignore if console is already open and jump to step 42.
41.	Type **Localhost** and click **Connect**.

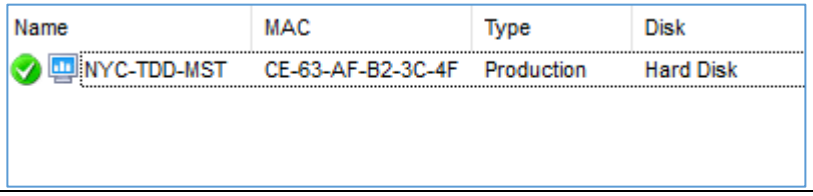


42. Browse **Farm > Sites > NYC-Site > vDisk Pool** and verify **Win10vDisk** is created.

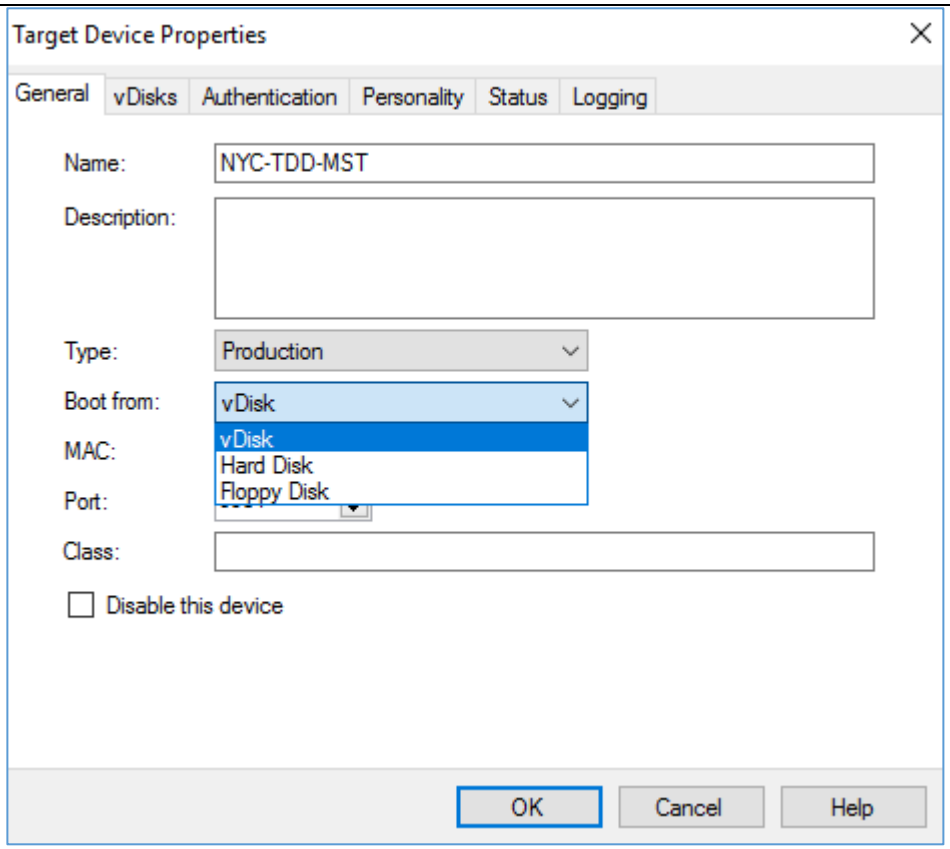
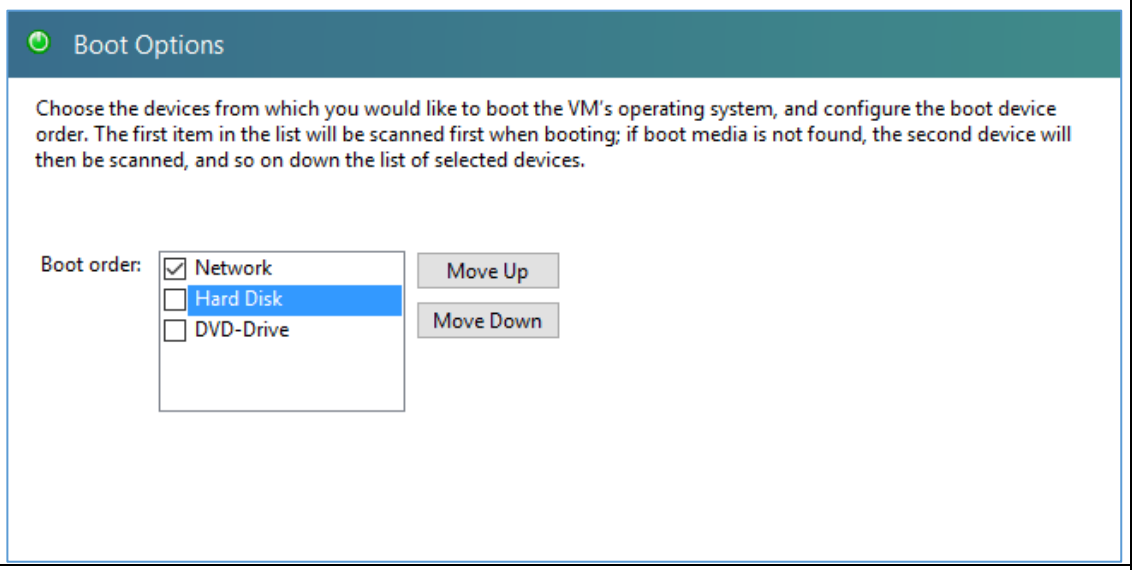


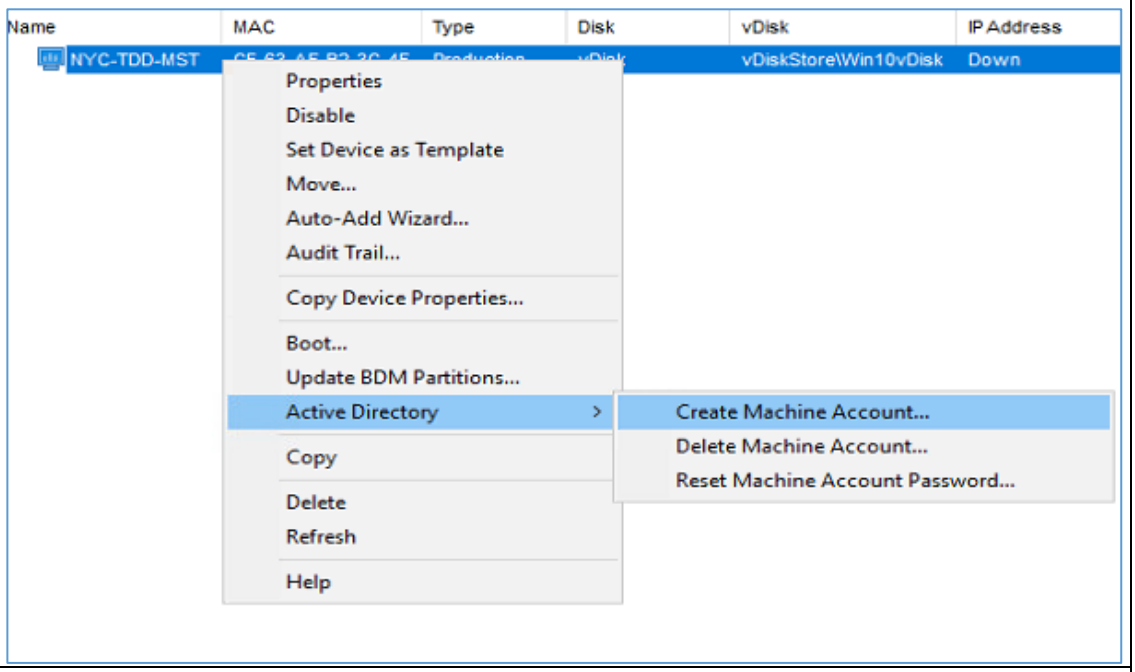
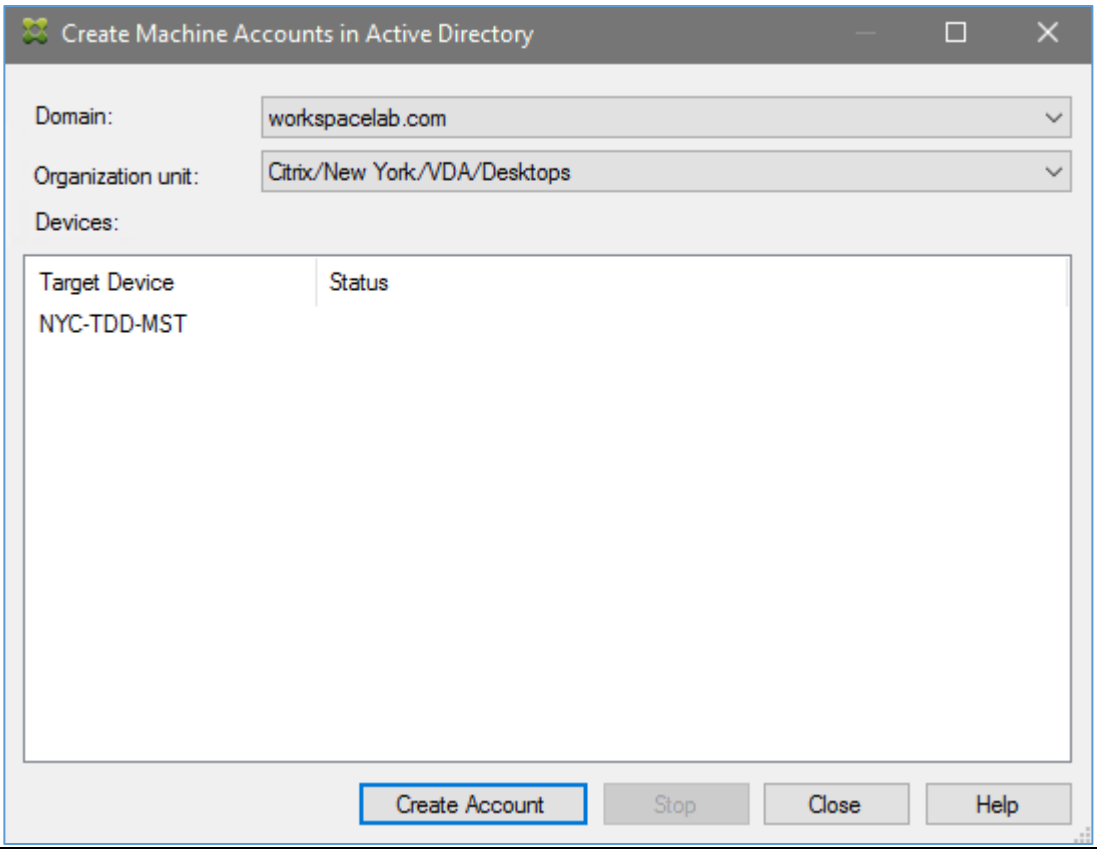
Note: Refresh the console, if vDisk is not seen.

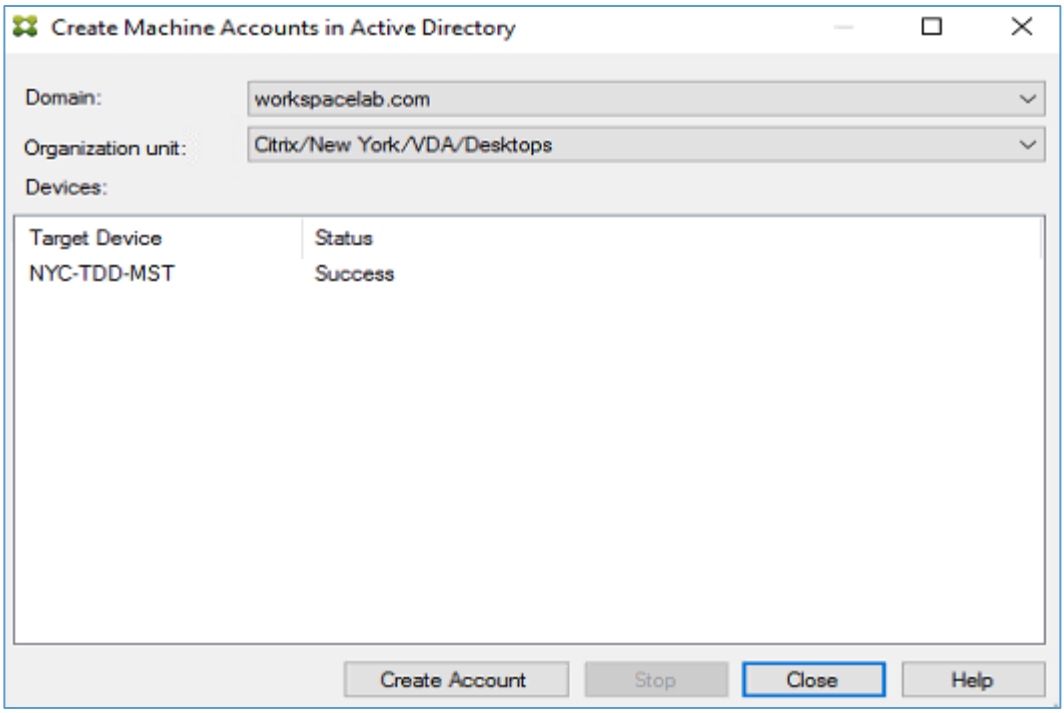
43. Browse **Farm > Sites > NYC-Site > Device Collections > Desktop OS Collection** and verify **NYC-TDD-MST** is created.



44. Right-click **NYC-TDD-MST** and select **Properties**. Change **Boot from** to **vDisk** and click **OK**.

	
45.	Select **PVS-DTP-MST** in XenCenter, click the **General** tab and then click **Properties** and select **Boot Options**.
46..	Uncheck **Hard Disk** and click **OK**. 
47.	Select **PVS-DTP-MST** in left pane and select **Shut Down**. **Note:** You may want to switch to XenCenter to monitor the progress. To do this, select PVS-DTP-MST in the left pane and the Console tab in the right pane.
48.	Connect back to **NYC-PVS-001 Provisioning Services Console** using remote desktop connection manager.

49.	Select **NYC-TDD-MST** under **Collections** and right-click select **Active Directory > Create Machine Account**. 
50.	Select **Citrix/New York/VDA/Desktops** from Organization unit drop-down. 
51.	Select **NYC-TDD-MST** and click **Create Account**.
52.	Click **Close** when status shows **Success**.



Note: Creating machine account from Provisioning services will create a machine account for the Target device in Active Directory that will be managed by Provisioning Services instead of the Domain Controller.

Key Takeaways:

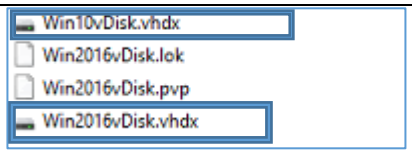
- FLTMC command to look at installed filter drivers.
- Target Device Software Installed.
- Imaging Wizard used to image the Hard disk of the machine into vDisk.
- Imaging Wizard creates the VDisk and also the Target device entry in the PVS Console.

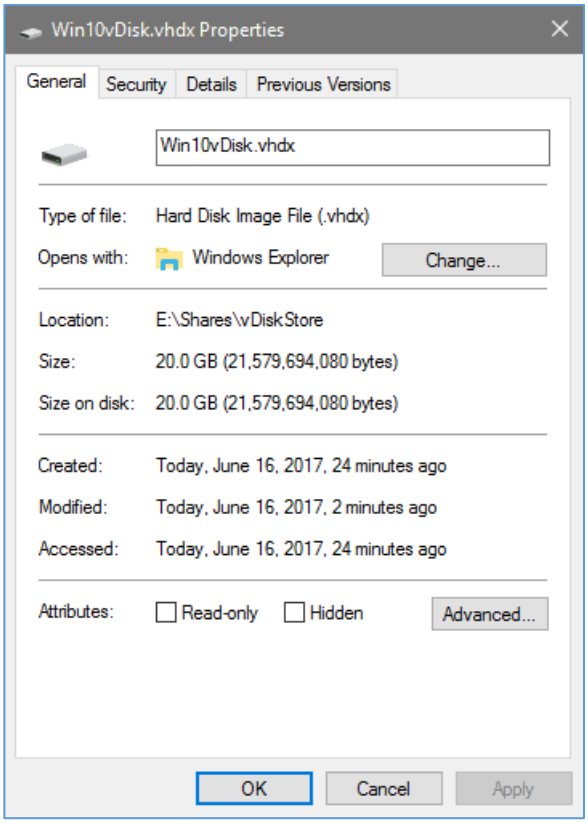
Exercise 17-3: Verify the Store via File Explorer

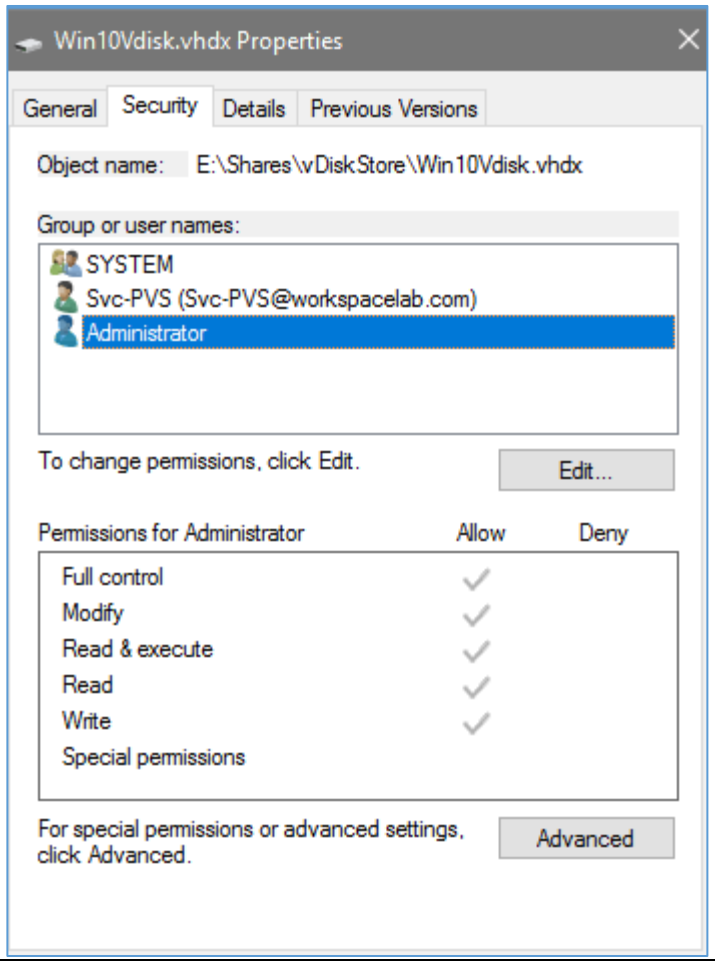
Scenario:

You are a Citrix Administrator at WW Labs, your Lead Citrix Architect has tasked you to verify that the appropriate vDisk files and permissions are visible in the Store.

Step	Action
1.	Using the Remote Desktop Connection manager, connect to **NYC-FSR-001**. To login to **NYC-FSR-001** right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the password.
2.	Launch the **File Explorer** and browse to **E:\Shares\vDiskStore**.
3.	Verify the two vDisks **Win10vDisk.vhdx** and **Win2016vDisk.vhdx** are created.

	
	
	Note: You will notice that three files are created for each vDisk.
	
	• The **.vhdx** file, which is the actual vDisk image.
	• The .**lok** file, which controls the read and write permissions for the vDisk and prevents disk corruption.
	• The **.pvp** file, which holds the vDisk properties information. Most of the settings configured for the vDisk are stored in this file such as:
	  ○ Class and type, which is used during an Auto Update.
	  ○ Build number, which is used in an auto update.
	  ○ Active Directory Switch, which is important to note that only the on/off switch is located here, no AD information such as the Machine Account Password hash key is located in this file.

4.	Select **Win10vDisk.vhdx**, right-click and select **Properties**.  **Note:** Size of the .vhdx file is 20.0GB, while the size of the disk attached to the PVS-DTP-MST is 50GB. This is because we selected Dynamic disk while creating the vDisk.
5.	Click on **Security** tab and verify the accounts that have permission to this .vhdx file.

	
6.	Click **OK** to close the **Properties** window.
7.	Click **X** to close the **File Explorer**.

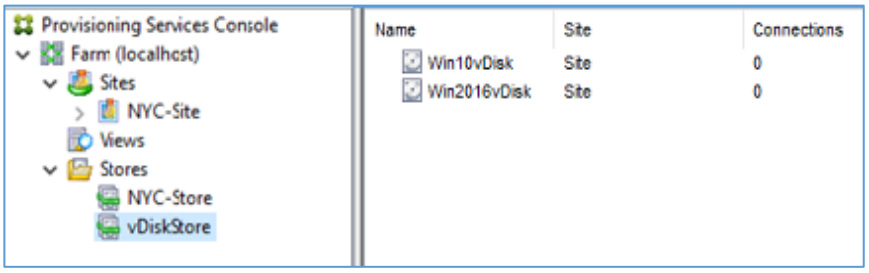
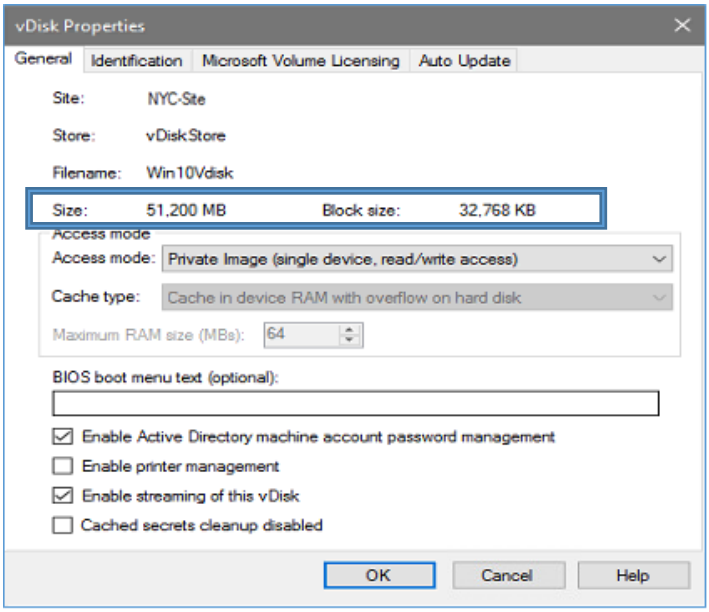
Key Takeaways:

- Each vDisk within the Provisioning Services Store comprises of 3 files; a VHDx containing all the image, a PVP file containing vDisk properties and a LOK file determining if the vDisk is currently in use.
- vDisks can be created as fixed or dynamic: fixed disks corresponds to thick provisioning while dynamic disks are thin provisioned.
- The vDisks automatically inherits the NTFS permissions from the folder where they were created.
- When copying vDisks between folders or different PVS systems, ensure that the NTFS permissions are set correctly.

Exercise 17-4: Verify the Store via PVS Console

Scenario:

You are a Citrix Administrator at WW Labs, your Lead Citrix Architect has tasked you to verify that the vDisks are also present within the Provisioning Services Console.

Step	Action
1.	Using the Remote Desktop Connection manager, confirm you are still connected to **NYC-PVS-001**. **Note:** In a previous exercise, you had logged into **NYC-PVS-001** using the following credentials to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session is disconnected, log on to **NYC-PVS-001**, right-click this machine and choose **Connect server**.
2.	Click **Start** and click **Provisioning Services Console**. **Note**: Ignore if console is already open and jump to step 4.
3.	Type **Localhost** and click **Connect**.
4.	Browse **Farm > Stores > vDiskStore** in the left pane.  **Note:** Refresh the console, if both vDisks are not listed.
5.	Select **Win10Vdisk** in the right pane. Right-click and select **Properties**.  **Note:** vDisk size is 51,200 MB with block size as 32,768 KB. 51,200 MB points to the actual disk size; unlike the .vhdx file seen in store which shows the actual occupied space in disk.
6.	Click **Cancel** and close the window.

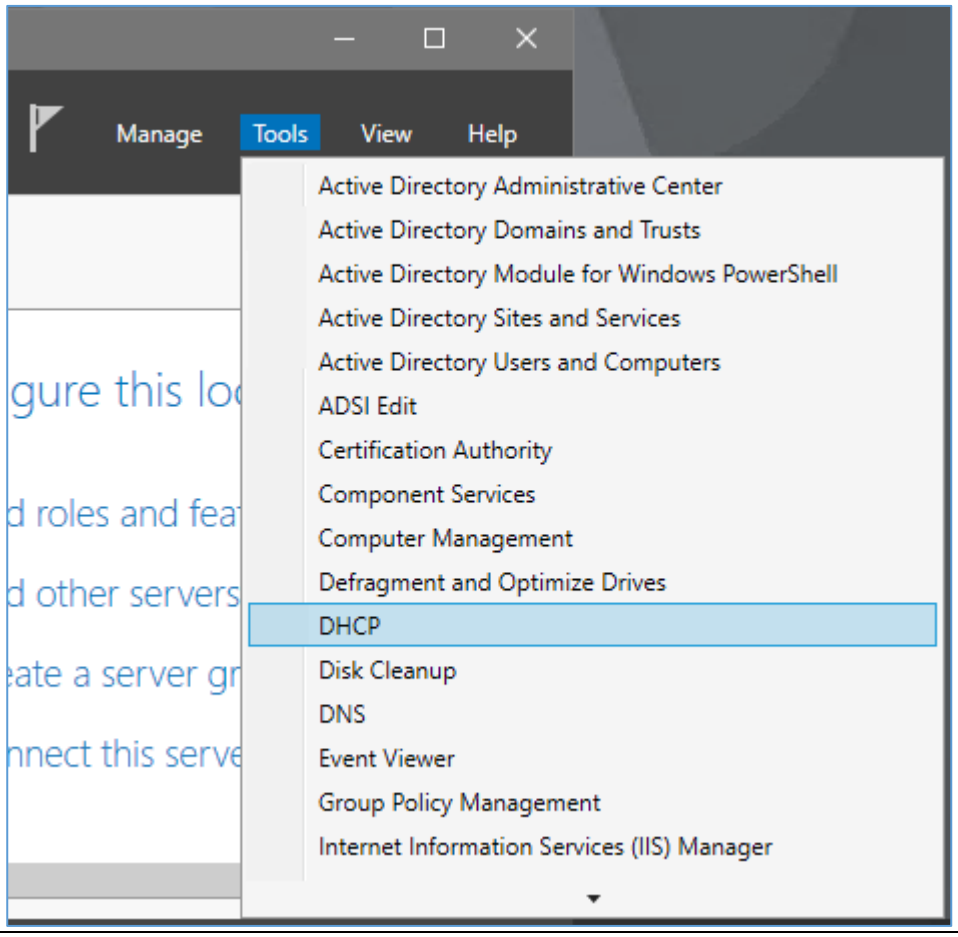
Key Takeaways:

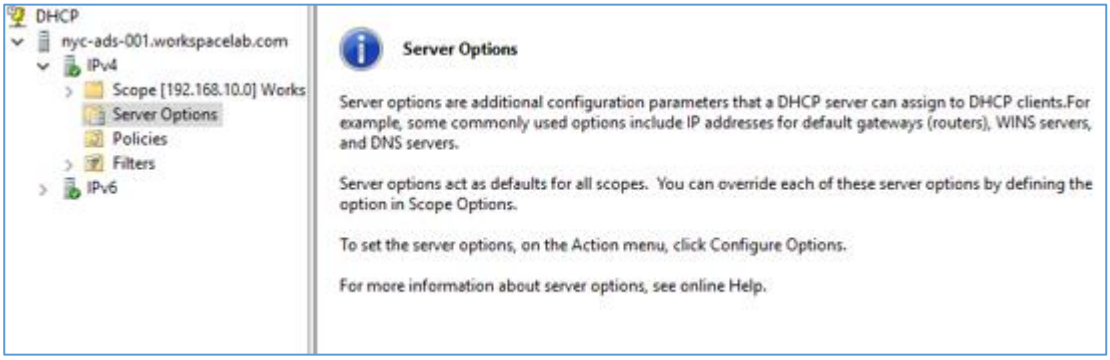
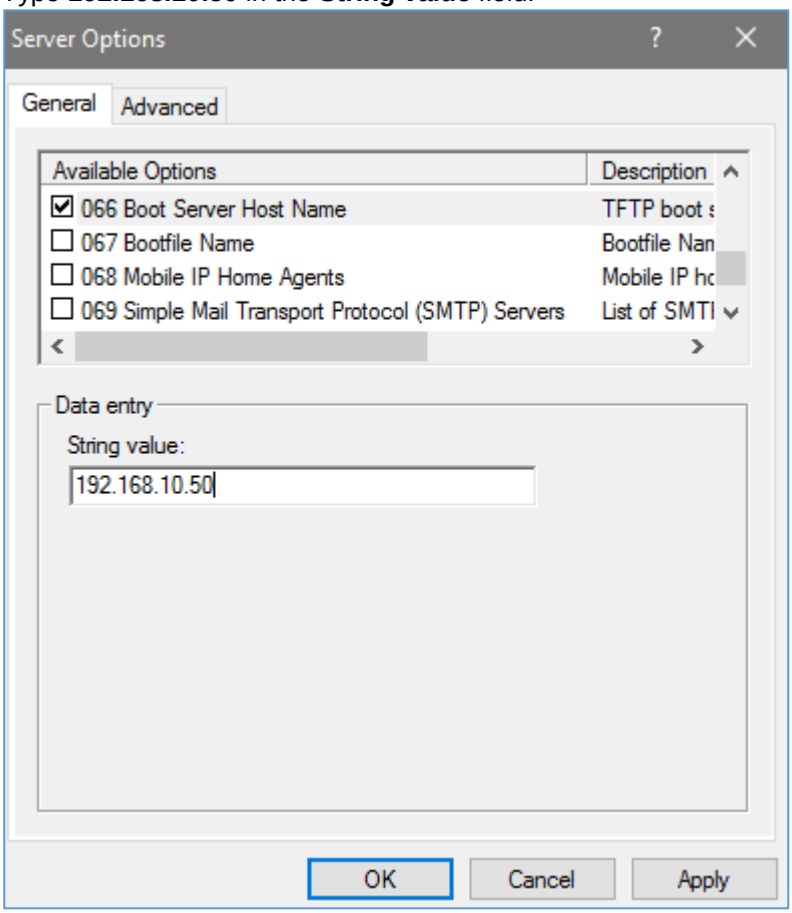
- The vDisk properties shown in the console are read from the PVP file.
- When inspecting the size and block size you can tell if the disk was created as dynamic or fixed.

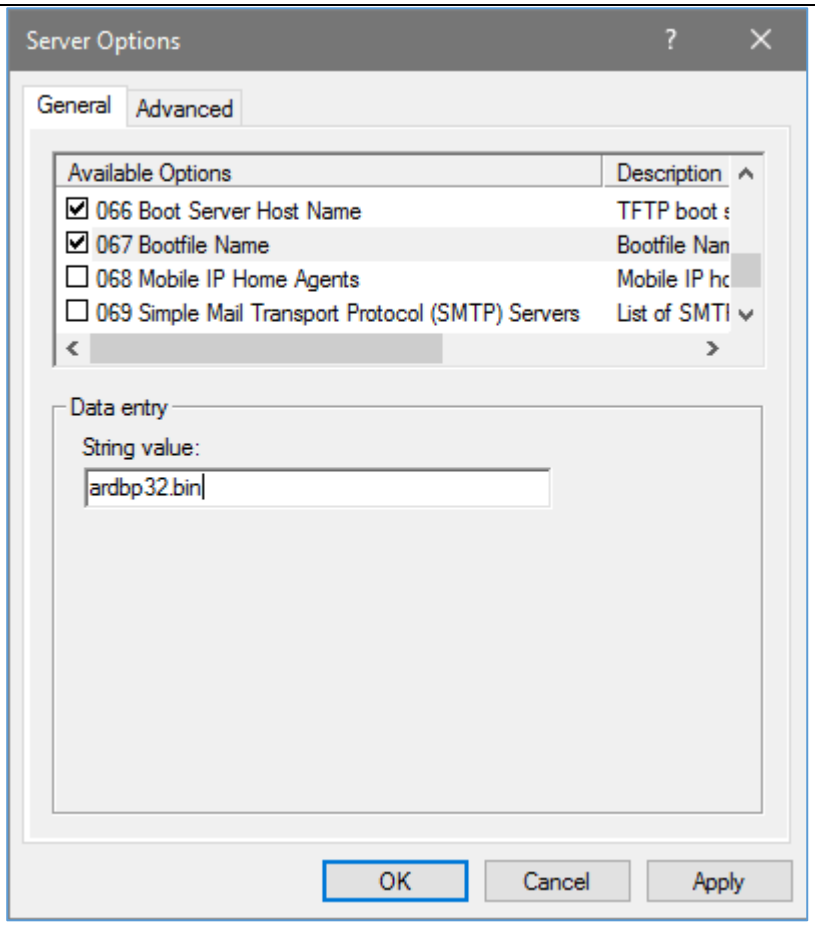
Exercise 17-5: Configure DHCP Options (66 and 67)

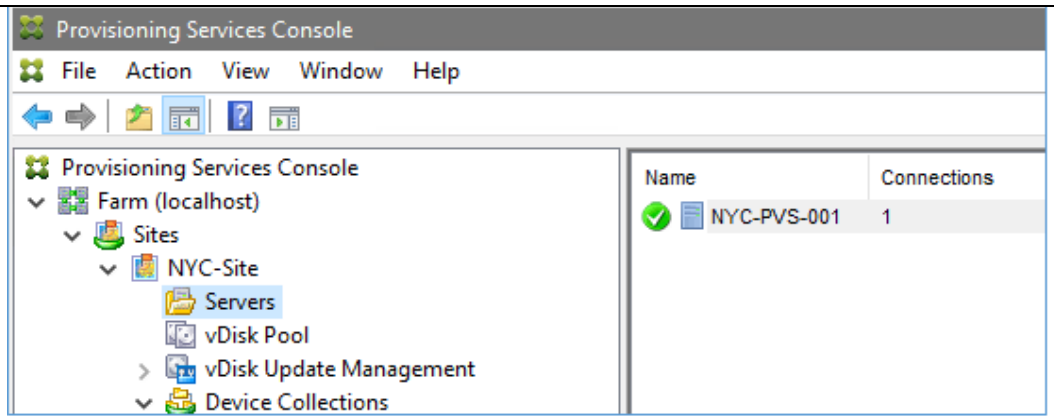
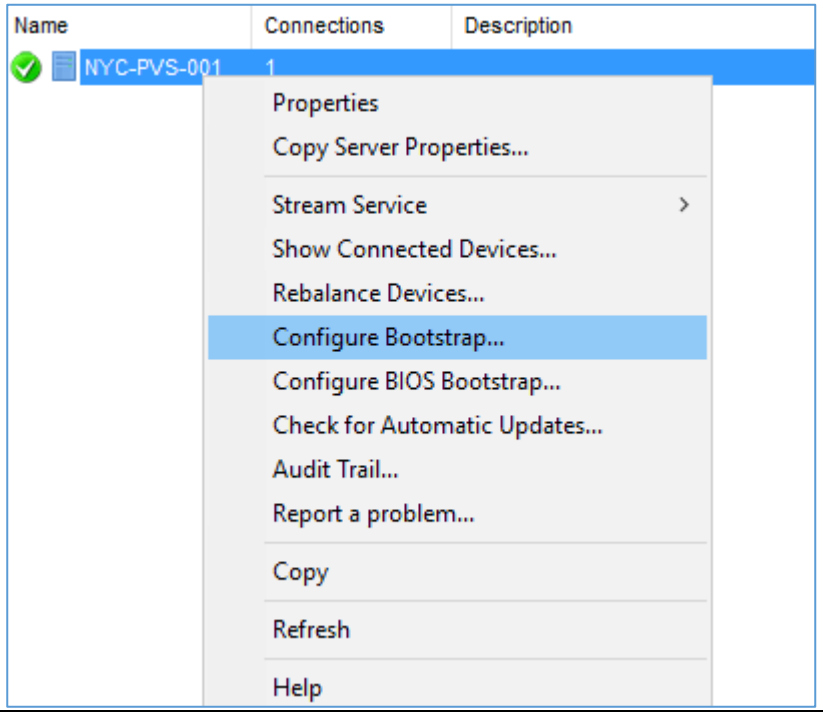
Scenario:

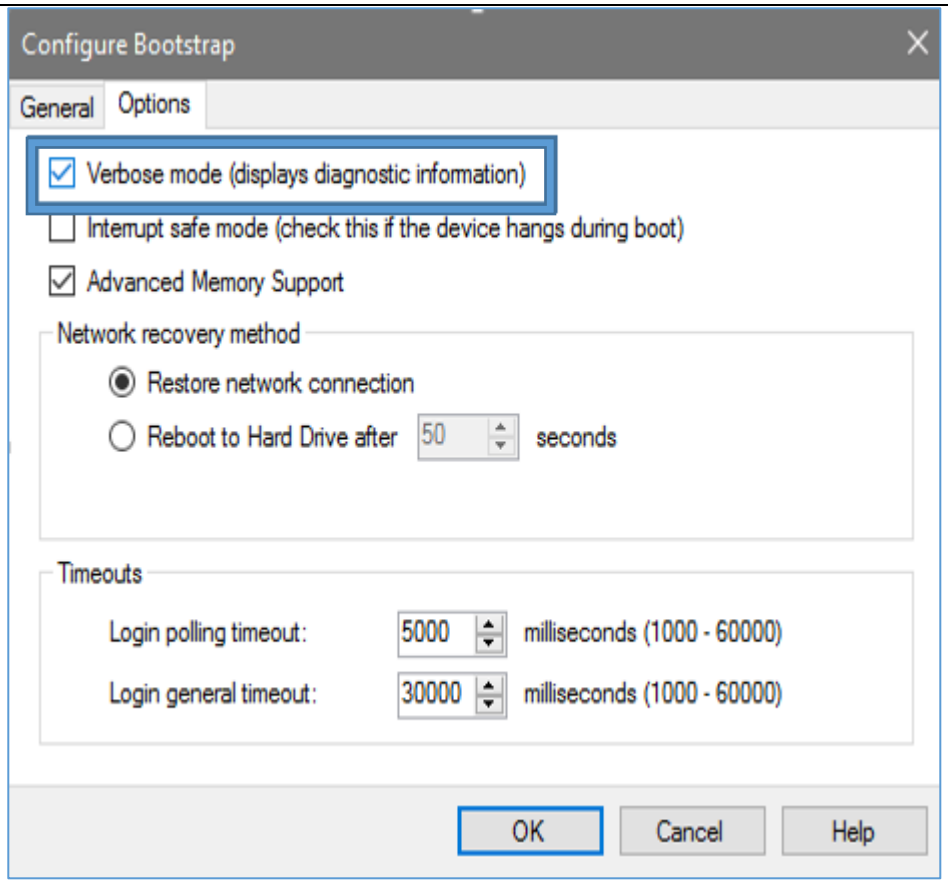
You are a Citrix Administrator at WW Labs, your Lead Citrix Architect has instructed you to ensure that even if PXE boot fails, the DHCP server will instruct the target devices to load the ARDBP32.bin bootstrap from the TFTP server hosted on the Provisioning Services Server. Your task is to configure options 66 and 67 on the DHCP scope.

Step	Action
1.	Using the Remote Desktop Connection manager, connect to **NYC-ADS-001**. To login to NYC-ADS-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the password.
2.	Select **Server Manager** from the task bar. Navigate to **Tools** and click **DHCP** to launch the **DHCP** console. 

3.	Browse **nyc-ads-001.workspacelab.com > IPv4 > Server Options**. 
4.	Right-click **Server Options** and then click **Configure Options**.
5.	Select **066 Boot Server Host Name** in the Available Options list on the General tab.
6.	Type **192.168.10.50** in the **String value** field.  **Note:** This is the IP address of the Provisioning Service server in our lab environment which will act as the TFTP server.
7.	Select **067 Bootfile Name** in the Available Options list on the General tab.
8.	Type **ARDBP32.BIN** in the **String value** field and then click **OK**.

	
9.	Close the **DHCP** console.
10.	Using the Remote Desktop Connection manager, confirm you are still connected to **NYC-PVS-001**. **Note:** In a previous exercise, you had logged into **NYC-PVS-001** using the following credentials to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session is disconnected, log on to **NYC-PVS-001**, right-click this machine and choose **Connect server**.
11.	Click **Start** and click **Provisioning Services Console**. Type **Localhost** and click **Connect**. **Note:** Ignore if console is already open.
12.	Browse **Farm > Sites > NYC-Site > Servers** in the left pane.

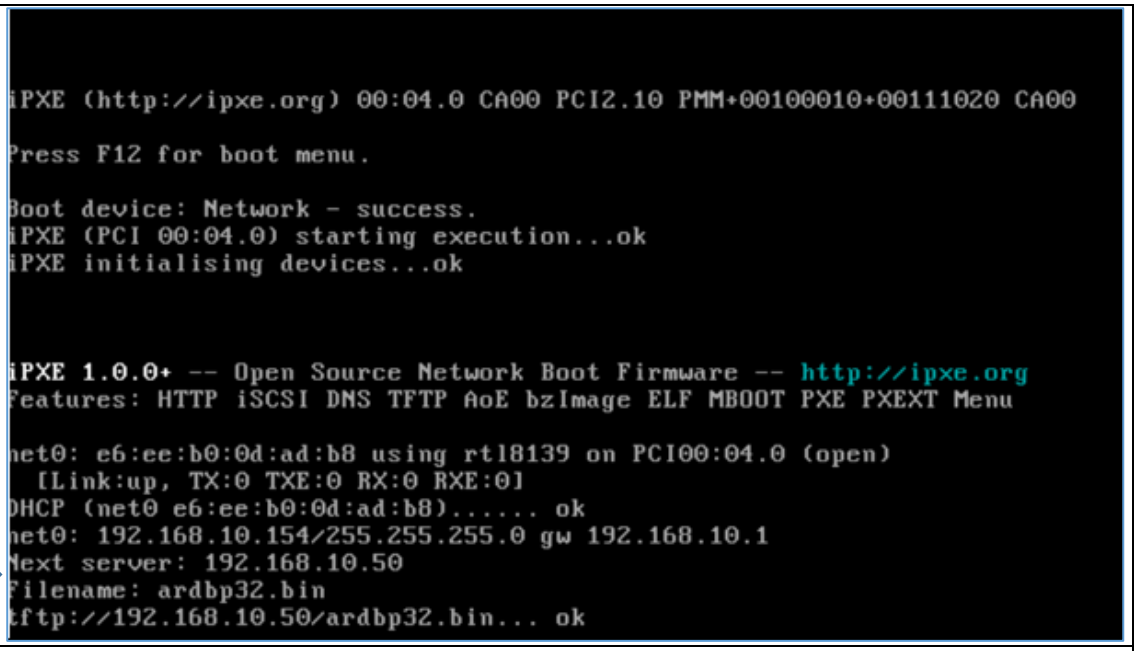
	
13.	Right-click **NYC-PVS-001** in the right pane and select **Configure Bootstrap**. 
14.	Select **Options** tab and check **Verbose mode** and click **OK**.



Note: Once Verbose mode is selected, we will be able to see all the diagnostic information in XenCenter when a target device is booted.

15. Select **PVS-DTP-MST** in XenCenter and click **Start**. Click **Console** tab in in the right pane and observe the following details:

- We see that the target device has gotten details from the DHCP server to connect to **192.168.10.50** and to obtain the **ardbp32.bin** file.
- A TFTP call is made to get the boot file.

	
16.	Monitor the state of the machine on XenCenter until it completes the boot process.
17.	Right-click **PVS-DTP-MST** in XenCenter and click **Shut Down**.

Key Takeaways:

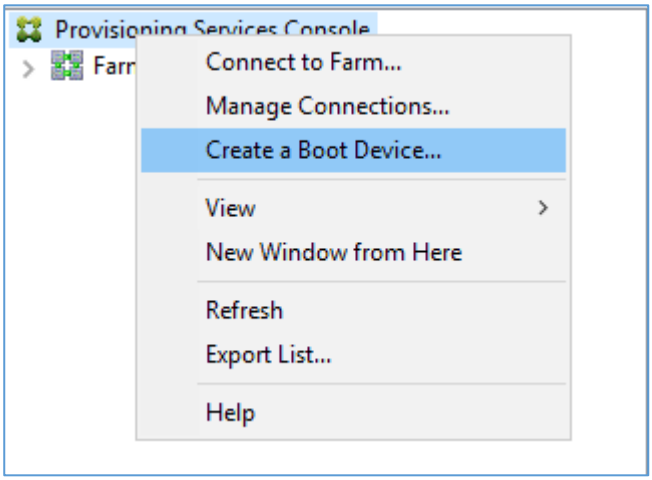
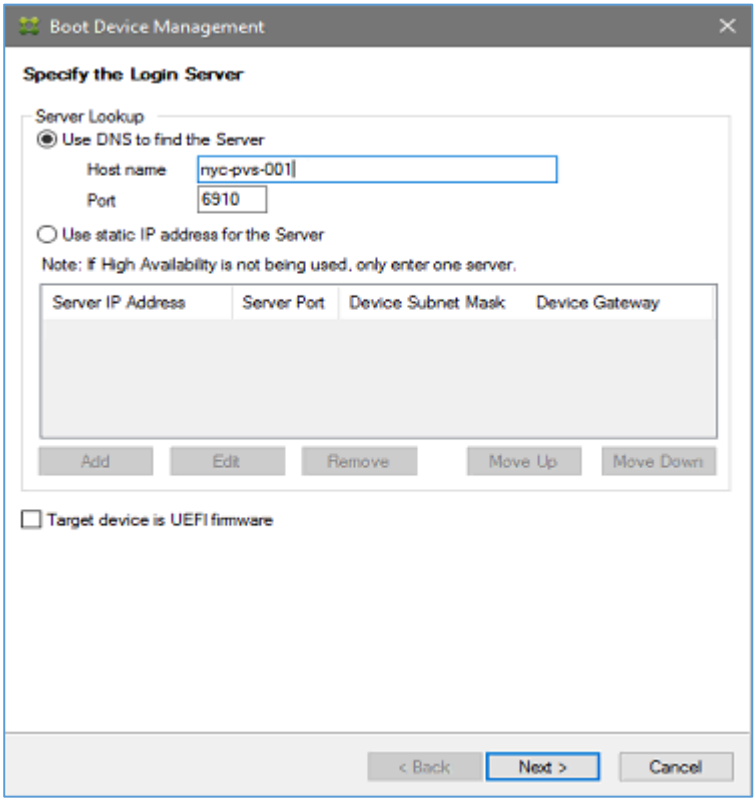
- The two main ways for a PVS Target Device to contact a PVS environment during boot are; either by doing a PXE broadcast to the whole network and wait for a PXE server to respond, or we can use DHCP options to direct the Target Devices to a specific TFTP server where they download the bootstrap.
- In the lab, both the PXE and the DHCP approach is now configured, however in a production environment you should select one or the other.
- Provisioning Services PXE should not be hosted on a vLAN or subnet where other PXE based environments are present.
- Enabling Verbose mode on the bootstrap will allow you to see additional diagnostic information during boot.

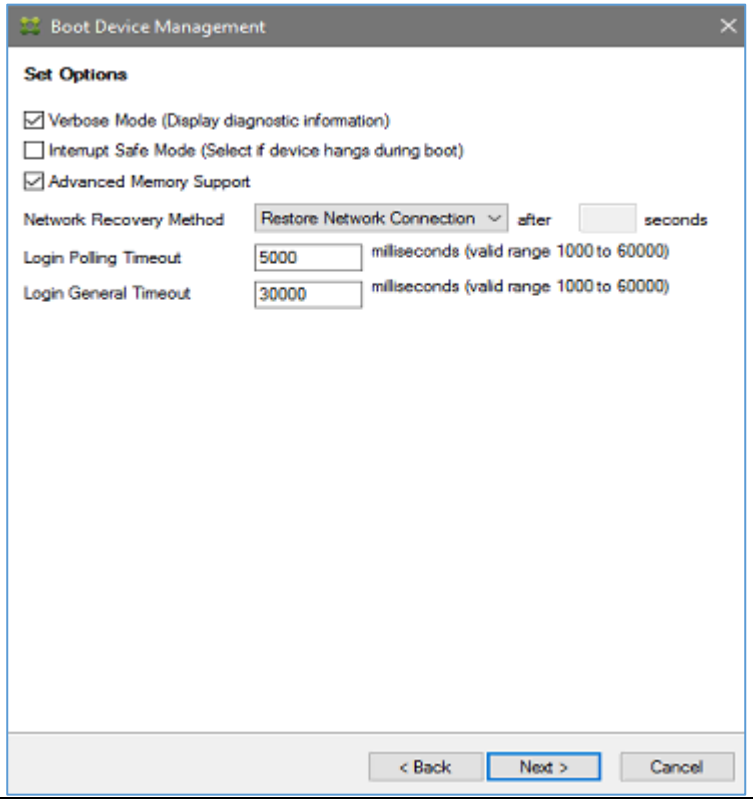
Exercice 17-6: Configure Boot ISO

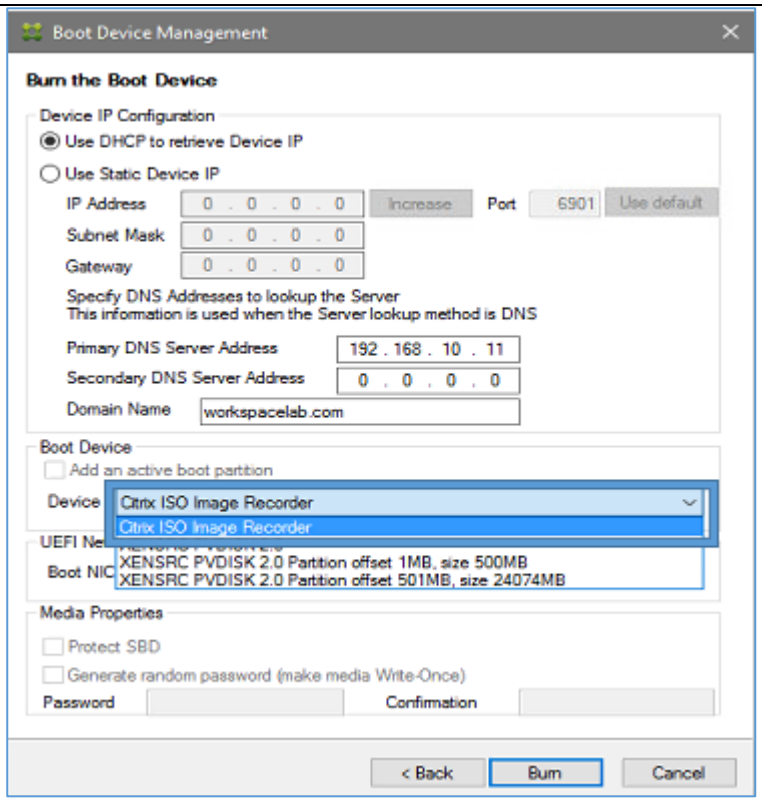
Scenario:

You are a Citrix Administrator at WW Labs, your Lead Citrix Architect has instructed to test the Boot Device Manager option. Your task will be to create a bootable ISO file that can reduce the need for reconfiguring the network to support booting provisioning target devices.

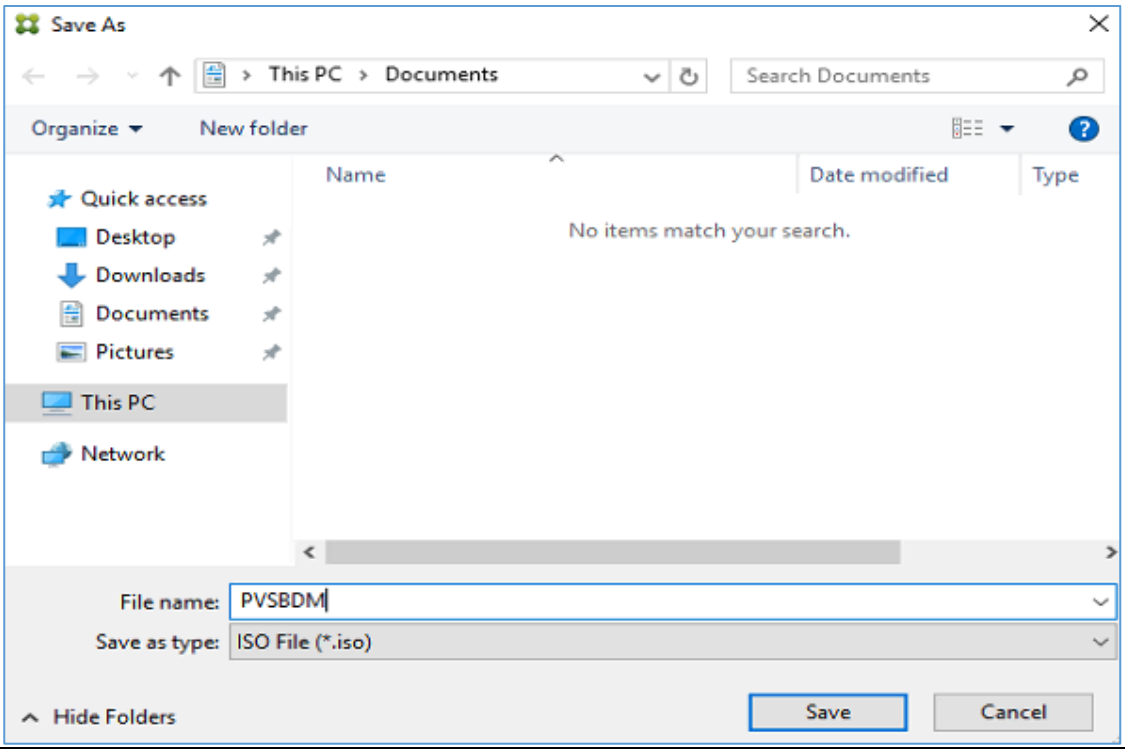
Step	Action
1.	Using the Remote Desktop Connection manager, confirm you are still connected to **NYC-PVS-001**. **Note:** In a previous exercise, you had logged into **NYC-PVS-001** using the following credentials to make the connection:

	User name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session is disconnected, log on to **NYC-PVS-001**, right-click this machine and choose **Connect server**.
2.	Click **Start** and click **Provisioning Services Console**. Type **Localhost** and click **Connect**.
3.	Right-click **Provisioning Services Console** and select **Create a Boot Device**. 
4.	Type **nyc-pvs-001** in host name section and click **Next**.  **Note:** We are specifying the DNS resolvable name of the PVS server that will be used as the login server for target devices. If we want to add multiple servers, select the other option to use a static IP address for the server and add a maximum of four login servers.

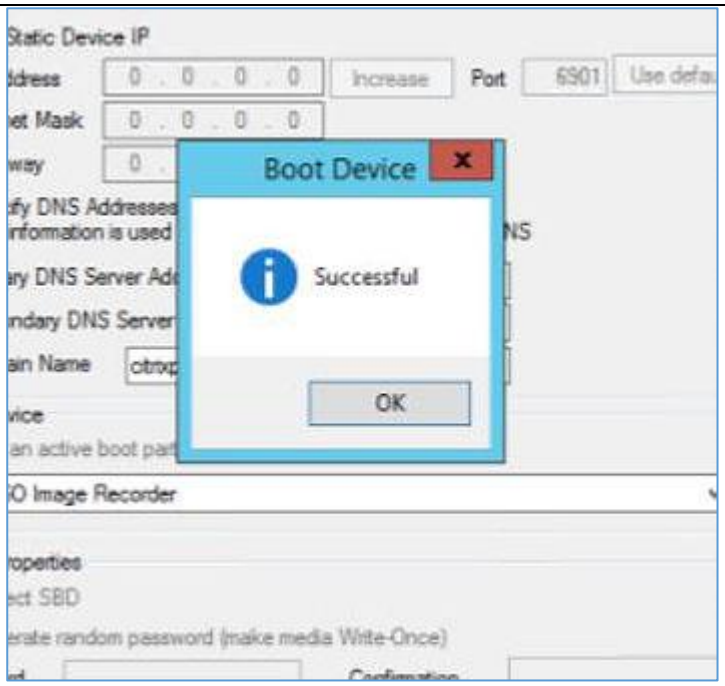
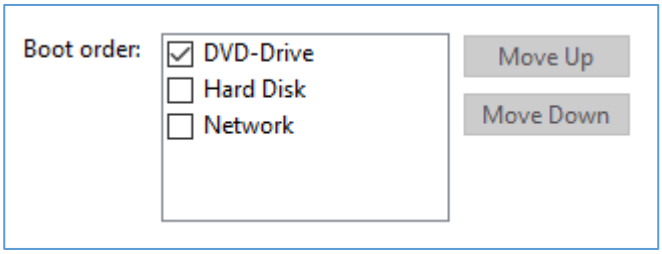
5.	Check **Verbose Mode** to display diagnostic information during boot and click **Next**. 
6.	Verify **Use DHCP to retrieve Device IP** is selected and complete other fields as: Primary DNS Server Address: **192.168.10.11** Domain Name: **workspacelab.com** Select **Citrix ISO Image Recorder** from the **Device** drop-down menu and click **Burn**. This will create an ISO file.

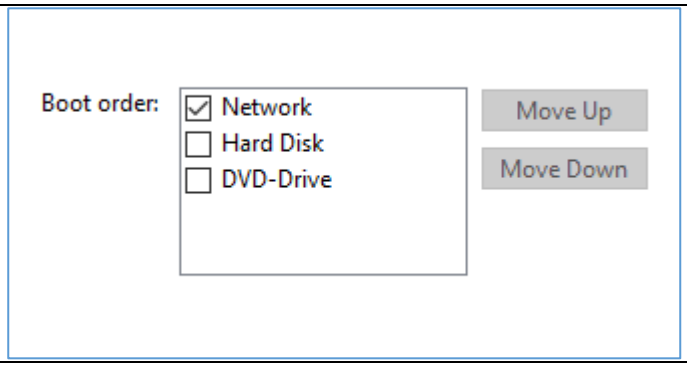


7. Specify a location to save the BDM ISO file. Type **PVSBDM** and click **Save**.



8. Click **OK** once the **Successful** message appears.

	 **Close** the Window. **Note:** Now depending on the environment we need to store the ISO in a highly available location that all PVS target VMs can access. **PVSBDM.iso** has already been copied on the **Local ISO SR XS** for the lab exercise.
9.	Select **PVS-DTP-MST** in XenCenter. In the right pane, click the **Console** tab. Using the **DVD-Drive 1:** drop-down menu select **PVSBDM.iso**. **Note**: If there are no ISOs listed in the **DVD-Drive 1:** drop-down menu, then the Local ISO SR that contains the ISO library may need to be re-scanned. In the left pane of **XenCenter**, select the **Local ISO SR XS**. In the right pane select, the **Storage** tab and click on the **Re-scan** button.
10.	Click **General** tab and then click **Properties** and select **Boot Options**.
11.	Move DVD-Drive to the top, uncheck other options and click **OK**.  Right-click **PVS-DTP-MST** in XenCenter and select **Start**. **Note:** This time the machine gets the boot information from the BDM ISO.
12.	Once the machine is up, right-click **PVS-DTP-MST** in XenCenter and select **Shut Down**.
13.	Click **Eject** to the right of the DVD-Drive 1 field to eject the PVSBDM.iso media.
14.	Click the **General** tab, click **Properties** and select **Boot Options**. Move **Network** back to the top, uncheck all other options, and click **OK**.



Key Takeaways:

- Boot Device Manager is an alternative method to booting PVS Target Devices.
- Instead of using the PXE or DHCP approach, the bootstrap can be hosted in an ISO or on a Virtual Disk attached to each Target Device.
- BDM is an easy approach if you are doing a POC or if you cannot enable network boot within your datacenter.

Module 18: Target Devices

Overview:

This module reinforces the concept of the way that production target devices handle disk data. To apply these concepts to the Provisioning Services deployment, different write cache locations will be configured for each of the vDisks. Additionally, you will redirect the event logs to an alternate storage location as an example of how certain data can be redirected to persist between target device reboots.

Before you begin:

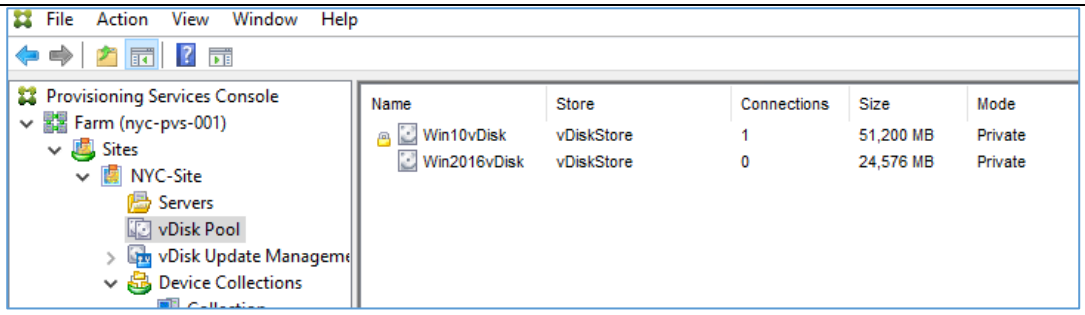
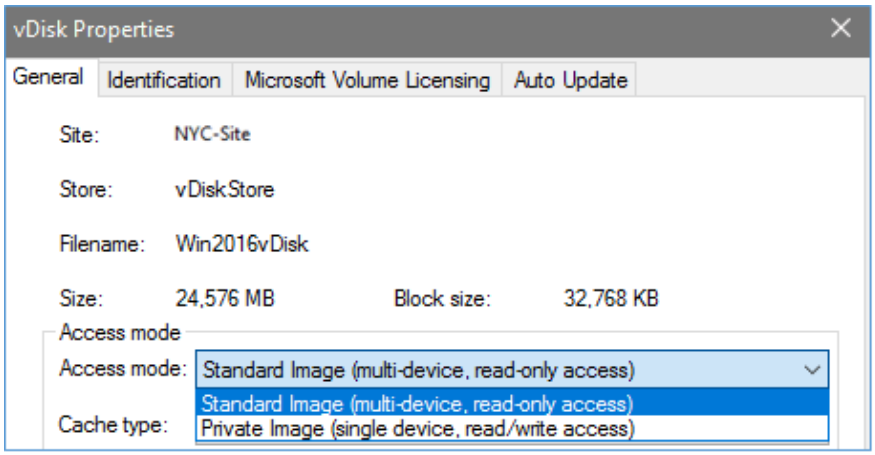
Estimated time to complete Module 18 lab exercises: 30 minutes

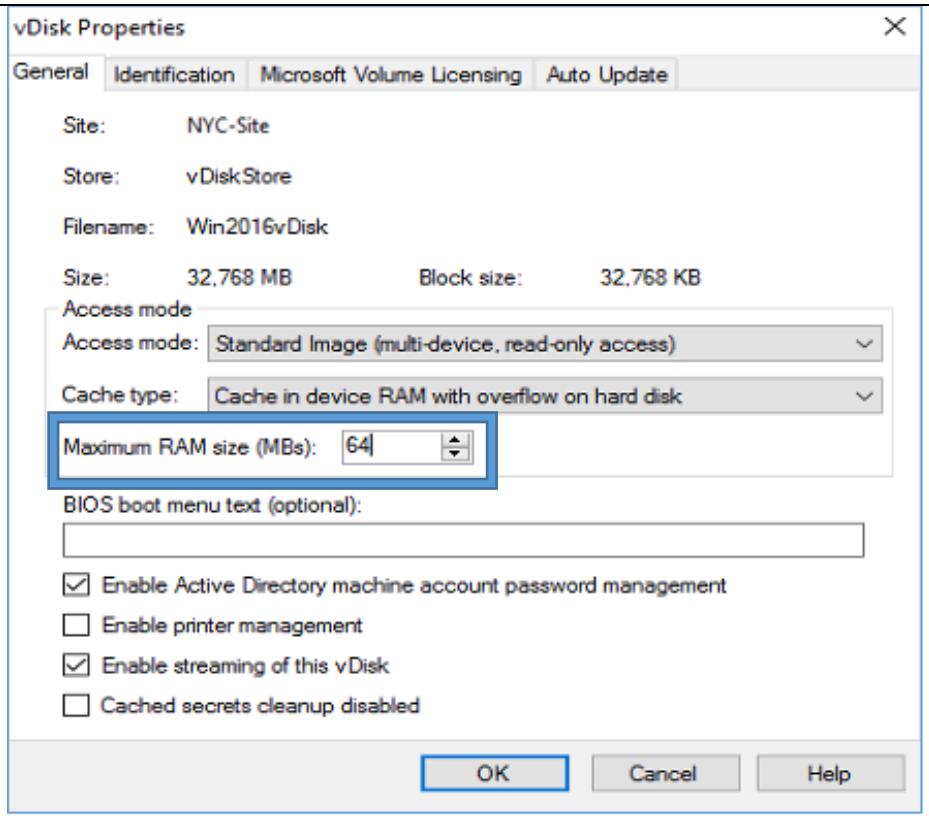
Exercise 18-1: Set the Write Cache location for the Server OS vDisk

Scenario:

You are a Citrix Administrator at WW Labs, your Lead Citrix Architect has instructed you to seal the Server OS vDisk and to ensure that all target devices streaming this vDisk will use RAM with overflow to disk for the write cache type.

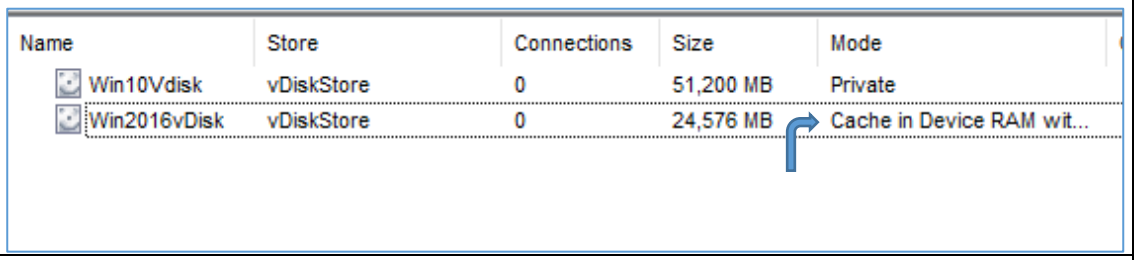
Step	Action
1.	The following VMs are required before beginning the exercises for this Module; all others may be powered down. To power manage your VMs, switch to XenCenter, right-click on the VM in the left pane and select Start or Shut Down. If prompted click Yes. • NYC-ADS-001 • NYC-SQL-001 • NYC-FSR-001 • NYC-PVS-001 • NYC-XDC-001 **Note**: These above VMs are listed in the start-up order.
2.	Using the Remote Desktop Connection manager, confirm you are still connected to **NYC-PVS-001**. **Note:** In a previous exercise, you had logged into **NYC-PVS-001** using the following credentials to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session is disconnected, log on to **NYC-PVS-001**, right-click this machine and choose **Connect server**.
3.	Click **Start** and click **Provisioning Services Console**. Type **Localhost** and click **Connect** **Note**: Ignore if console is already open.
4.	Browse **Farm > Sites > NYC-Site > vDisk Pool** in the left pane.

	
5.	Select **Win2016vDisk**. Right-click and select **Properties**.
6.	Using the Access mode drop-down menu, select **Standard Image (multi-device, read-only access)**. 
7.	Using the Cache type drop-down menu, select **Cache in device RAM with overflow on hard disk**. Verify Maximum RAM size (MBs) is **64** (By Default).



Note: Maximum RAM size specifies the max limit for RAM that the PVS target device driver can allocate from the non-paged pool for caching before moving the older disk writes to the hard disk cache overflow.

8. Click **OK** and verify on **Provisioning Services Console** that the mode is shown correctly.



9. Close the **Provisioning Services Console**.

Key Takeaways:

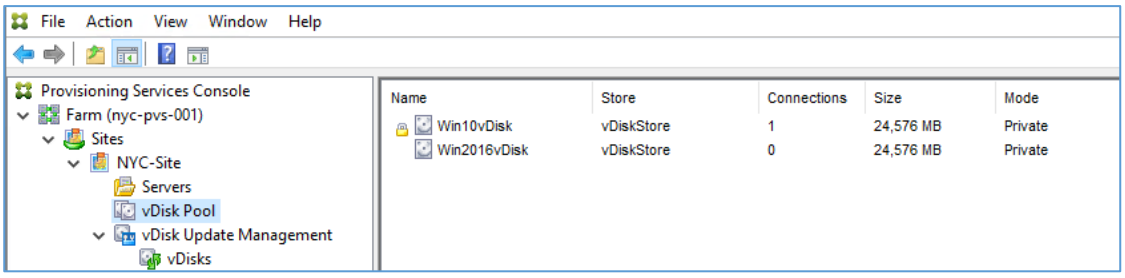
- A vDisk has two access modes: Standard Image and Private Image.
- Private Image means the image is open for changes and only one Target Device can use the image.
- Standard Image means the image is write protected and can be used by multiple Target Devices at one time.
- When Target Devices stream a write protected vDisk, the changes during runtime are stored in a temporary location called a Write Cache.
- The Write Cache can be hosted in the following places: Provisioning Server hard disk, Target Device RAM, Target Device hard disk or Target Device RAM with overflow on hard disk. Generally, the last option is preferred for most deployments.

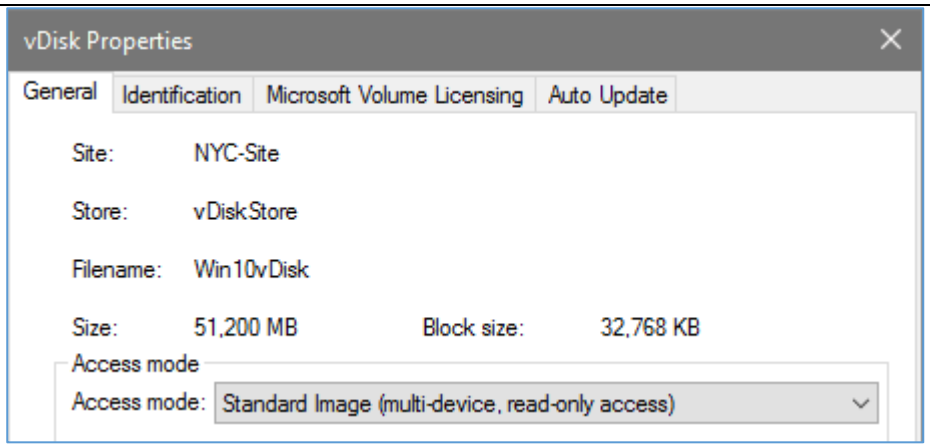
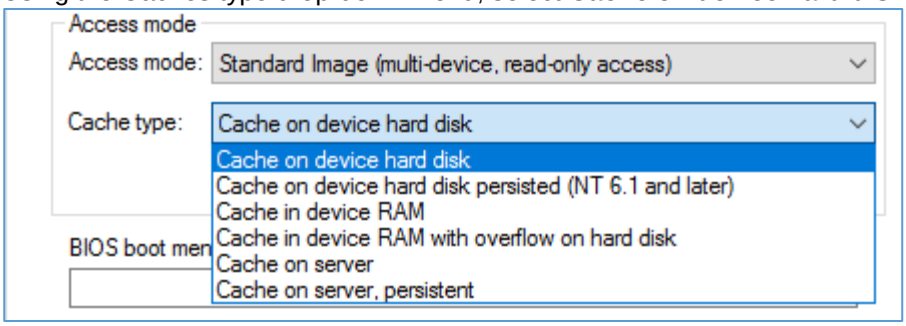
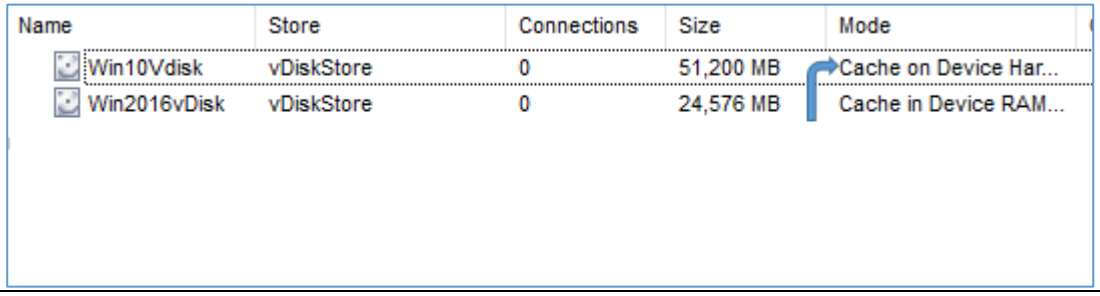
- The RAM will act as a write buffer to ensure that random reads and writes are processed quickly. When the RAM buffer is full, the least used blocks of data is written to the local write cache disk to accommodate newer data in the RAM cache. The process is very similar to the paging process in Windows.

Exercise 18-2: Set the Write Cache location for the Desktop OS vDisk

Scenario:

You are a Citrix Administrator at WW Labs, your Lead Citrix Architect has instructed you to seal the Desktop OS vDisk and to ensure that all target devices streaming this vDisk will use local disk for the write cache type.

Step	Action
1.	Using the Remote Desktop Connection manager, confirm you are still connected to **NYC-PVS-001**. **Note:** In a previous exercise, you had logged into **NYC-PVS-001** using the following credentials to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session is disconnected, log on to **NYC-PVS-001**, right-click this machine and choose **Connect server**.
2.	Click **Start** and click **Provisioning Services Console**. Type **Localhost** and click **Connect**. **Note**: Ignore if console is already open.
3.	Browse **Farm > Sites > NYC-Site > vDisk Pool** in the left pane.  **Note:** If vDisk shows a lock, refresh the console.
4.	Select **Win10VDisk** in the right pane, right-click and select **Properties**.
5.	Using the Access mode drop-down menu, select **Standard Image (multi-device, read-only access)**.

	
6.	Using the Caches type drop-down menu, select **Cache on device hard disk**. 
7.	Click **OK** and verify in the **Provisioning Services Console** that the mode is shown correctly. 
8.	Close the **Provisioning Services Console**.

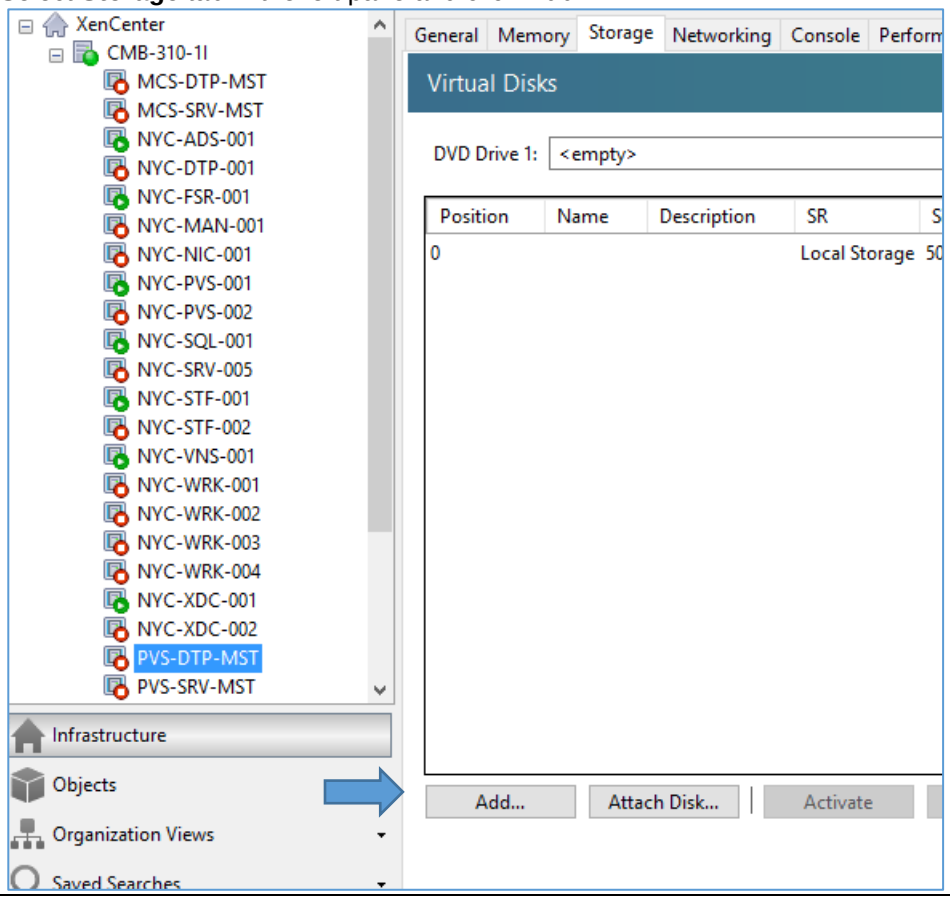
Key Takeaways:

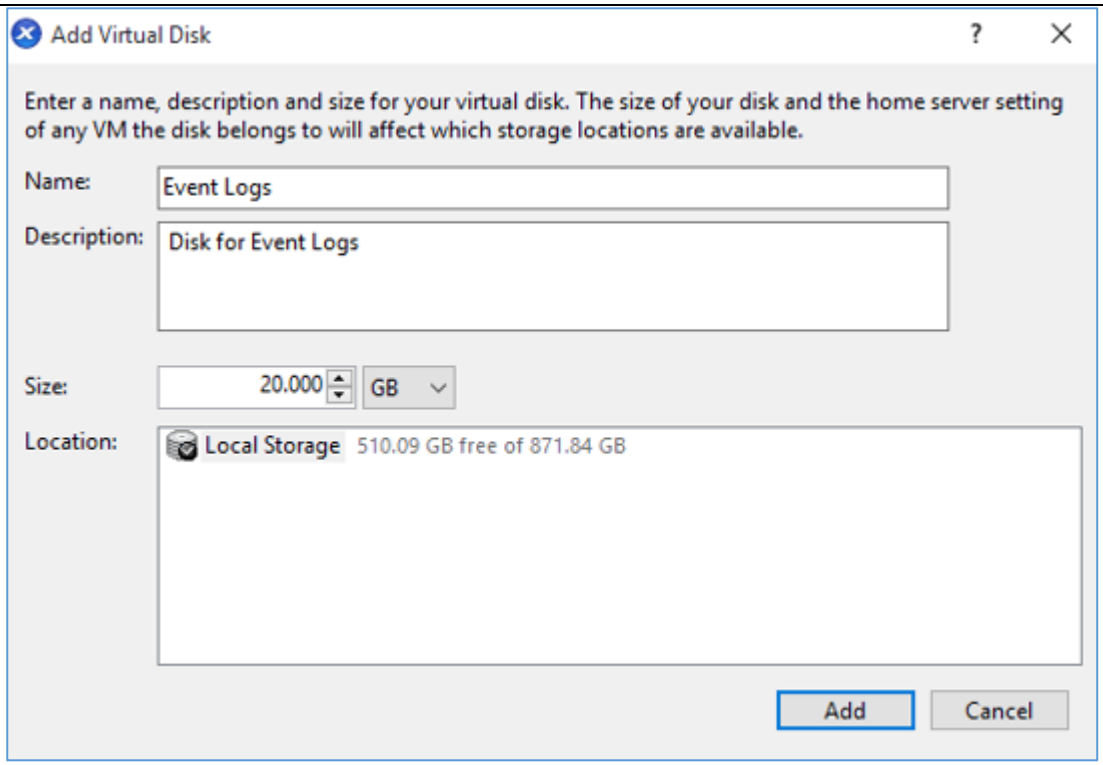
- Cache on device hard disk is another possible caching method available in Provisioning Services. When selecting this method, performance will depend entirely on the underlying storage subsystem of the Target Device.
- The Target Device must have a local hard disk attached containing a pre-formatted Basic Volume with a Windows NTFS file system that has at least 512MB of free space.
- The Write Cache will be contained within a hidden file on this hard disk and the file will automatically grow with every change made within the Target Device.
- When a Target Device using a standard mode vDisk is rebooted, the Write Cache is automatically reset and all changed will be lost.

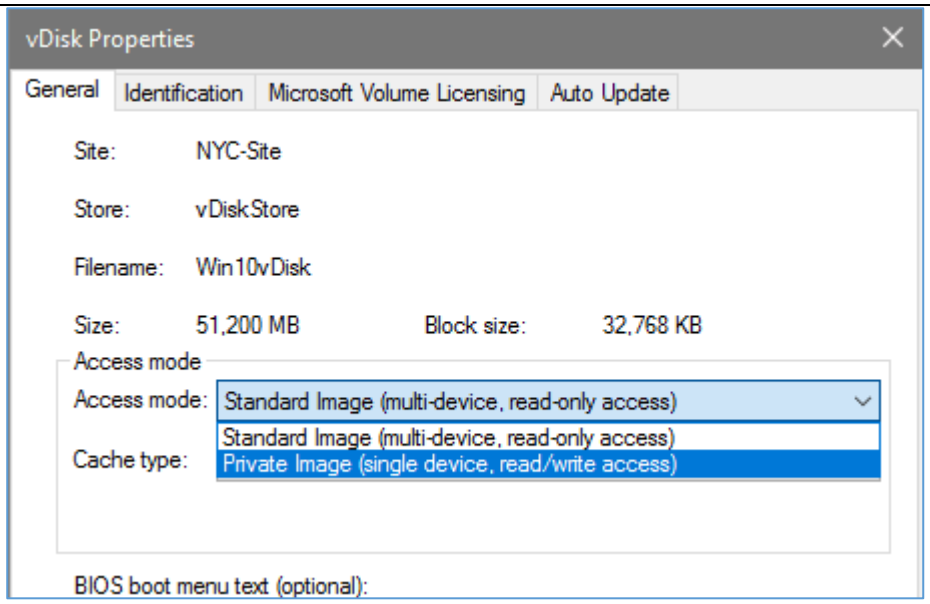
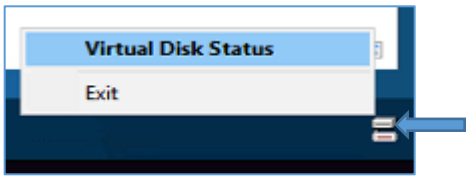
Exercise 18-3: Add a Persistent Drive and Redirect Event Logs

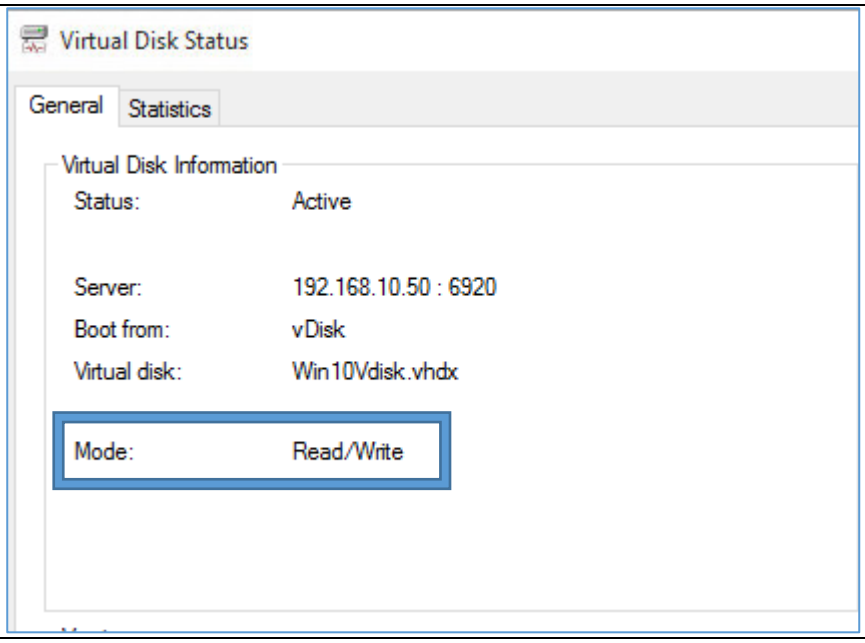
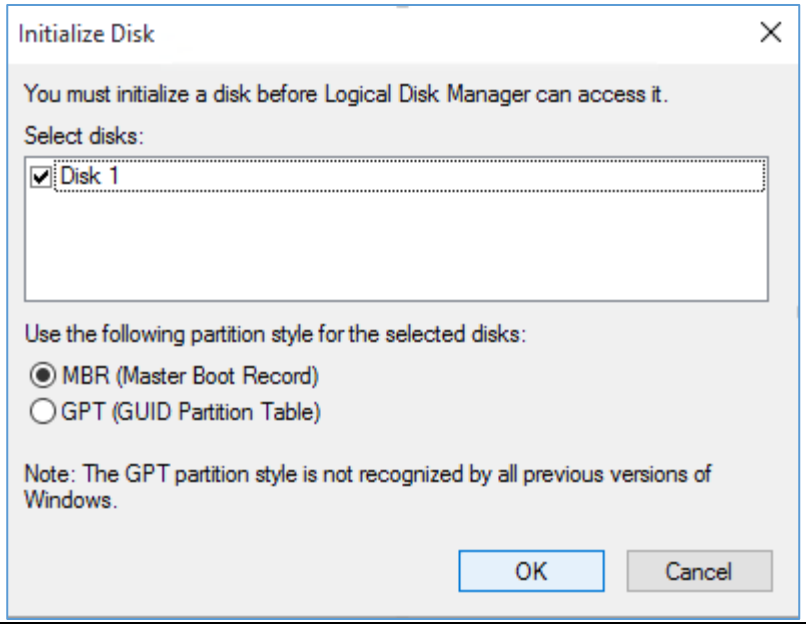
Scenario:

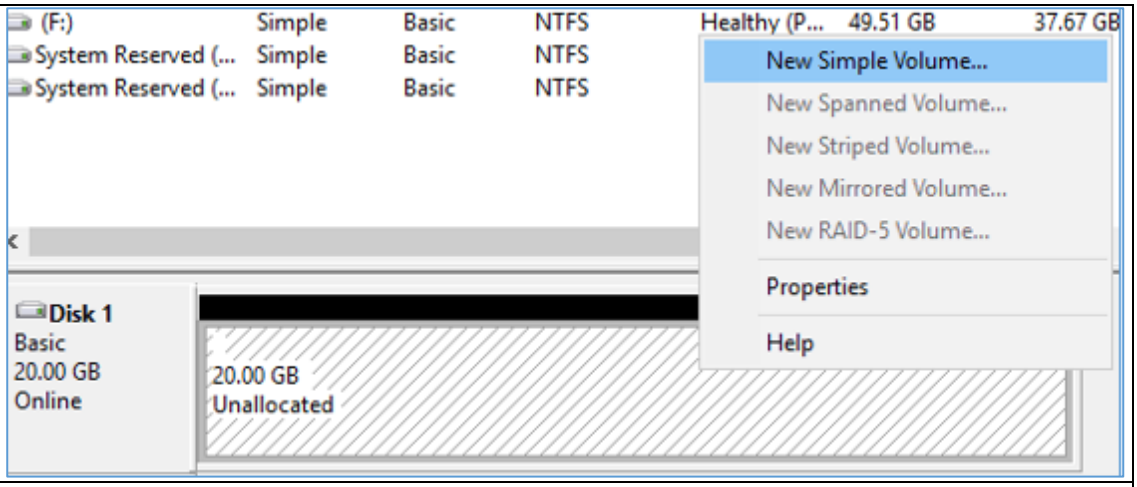
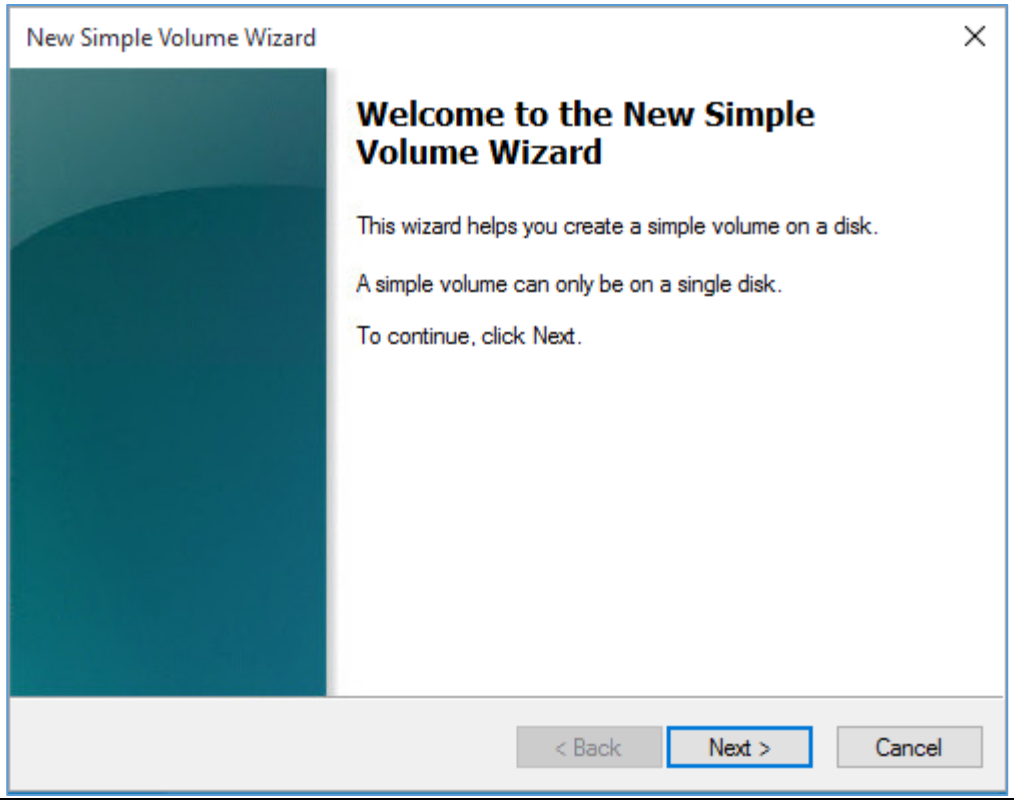
You are a Citrix Administrator at WW Labs, your Lead Citrix Architect has informed you about a new IT policy mandating that all non-persistent machines must save historical event log data. Your task is to redirect the event logs on the master target device to a persistent location, in order to comply with the new IT policy.

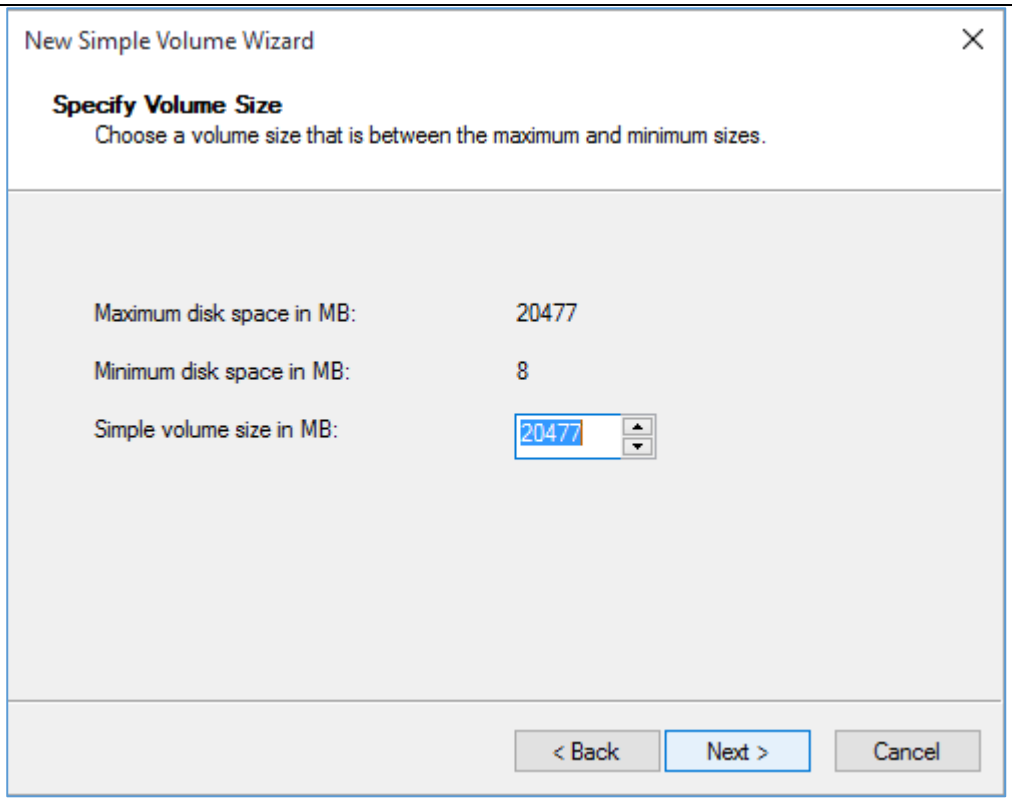
Step	Action
1.	Connect to XenCenter and select **PVS-DTP-MST**.
2.	Select **Storage** tab in the left pane and click **Add**. 
3.	In the Name field, type **Event Logs** and in the Description field type **Disk for Event Logs**. In the Size field enter **20GB**.

	 Click on **Add**.
4.	Using the Remote Desktop Connection manager, confirm you are still connected to **NYC-PVS-001**. **Note:** In a previous exercise, you had logged into **NYC-PVS-001** using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note**: If your Remote Desktop Connection session is disconnected, log on to **NYC-PVS-001**, right-click this machine and choose **Connect server**.
5.	Click **Start** and click **Provisioning Services Console**. Type **Localhost** and click **Connect**. **Note**: Ignore if console is already open.
6.	Browse **Farm > Sites > NYC-Site > vDisk Pool** in the left pane**.** Select **Win10Vdisk** in the right pane, right-click and select **Properties**.
7.	Using the Access mode drop-down menu, select **Private Image (single device, read/write access)**.

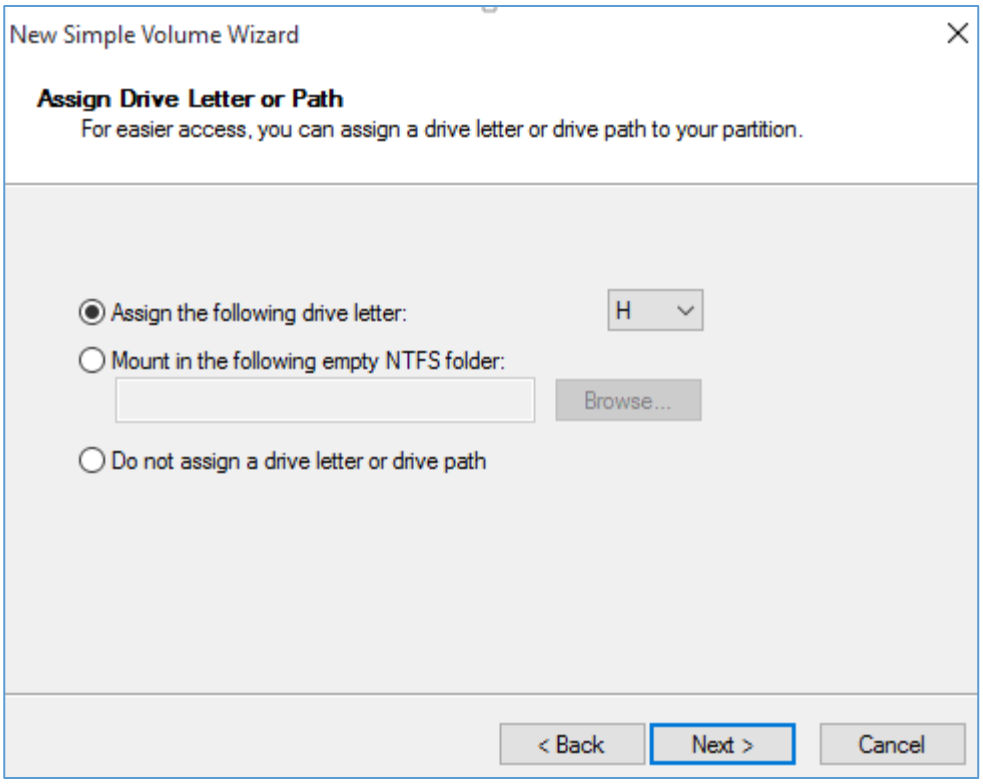
	 Click **OK**.
8.	Connect to XenCenter, select **PVS-DTP-MST** and click **Start**. Monitor the progress until machine has completed the boot process.
9.	Login to **PVS-DTP-MST** from XenCenter using **WORKSPACELAB\Administrator** with **Password1** as the password.
10.	Right-click the vDisk status tray icon in the right corner of the task bar and select **Virtual Disk Status.** 
11.	Verify that the **Mode** shows **Read/Write**. Click **X** to close the window.

	
12.	Right-click **Start** and select **Disk Management**.
13.	Click **OK** on the **Initialize Disk** window. 
14.	Select the recently added **20GB Disk1**. Right-click and select **New Simple Volume**.

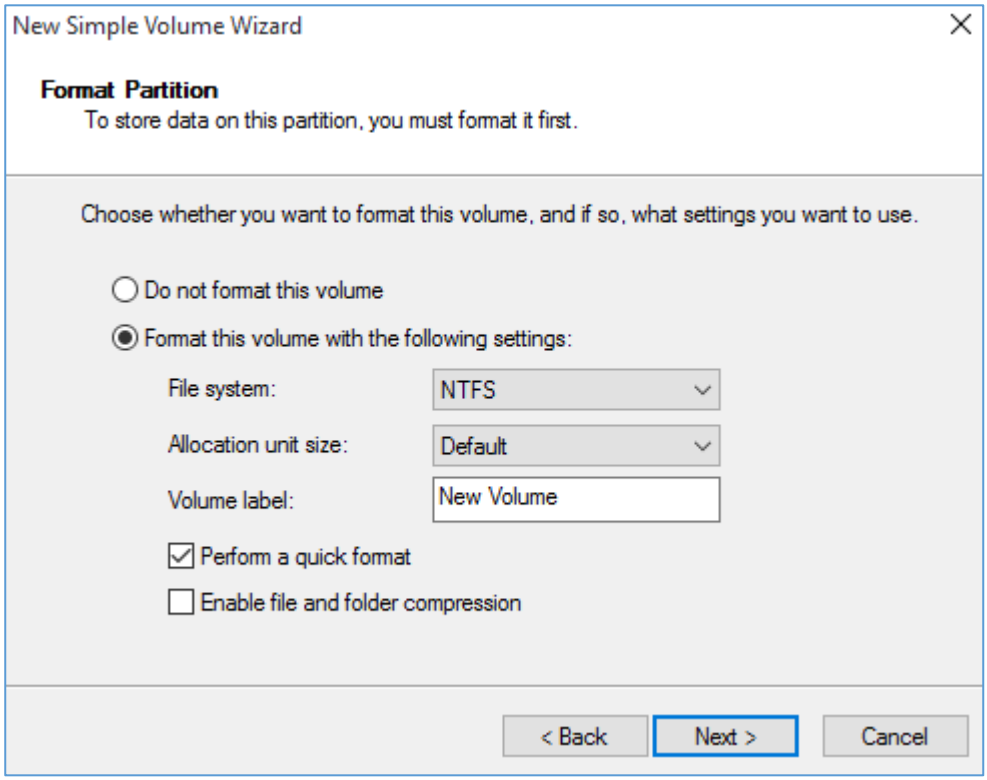
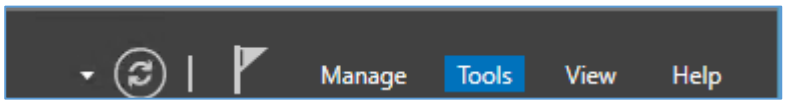
	
15.	Click **Next** on the Welcome to the New Simple Volume Wizard screen. 
16.	Click **Next** on the Specify Volume Size screen.

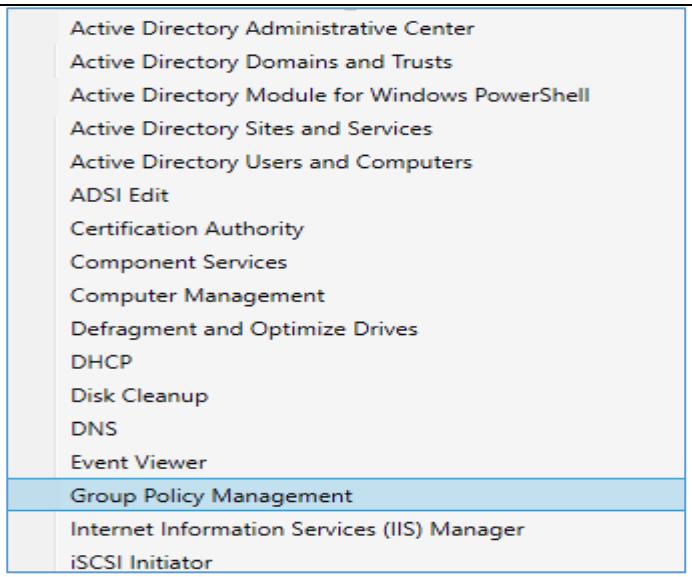
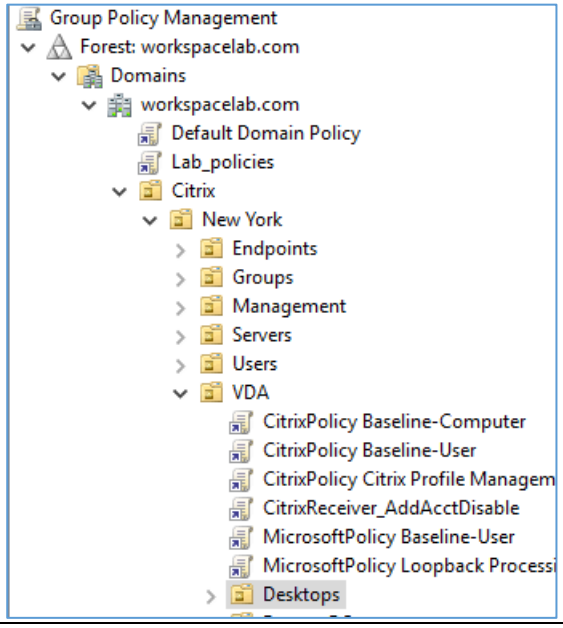


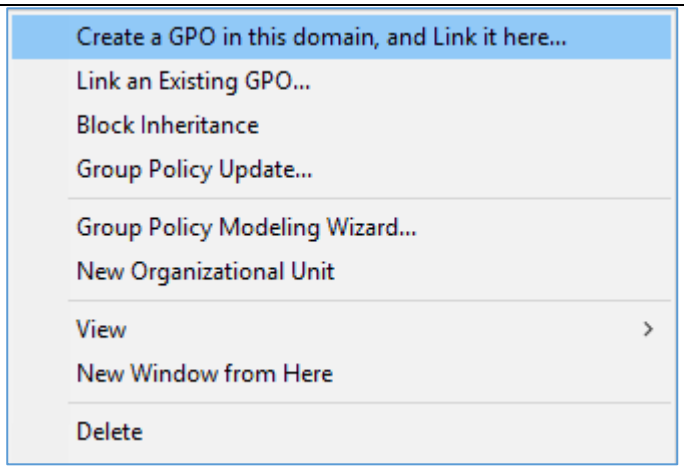
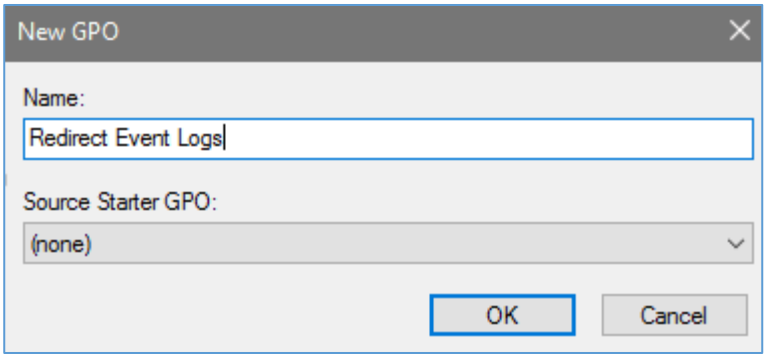
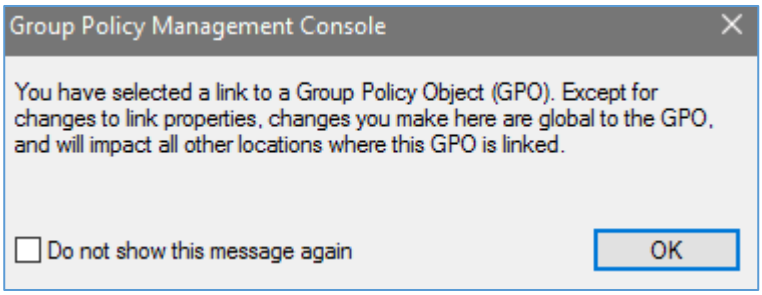
17. Verify **H** is selected from the Assign the following drive letter drop-down menu.

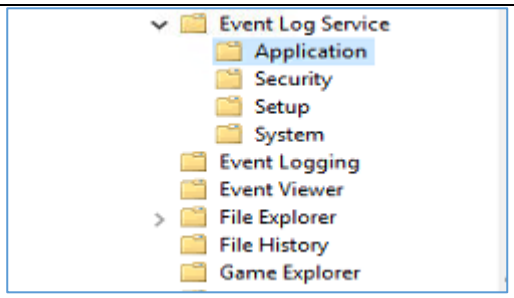
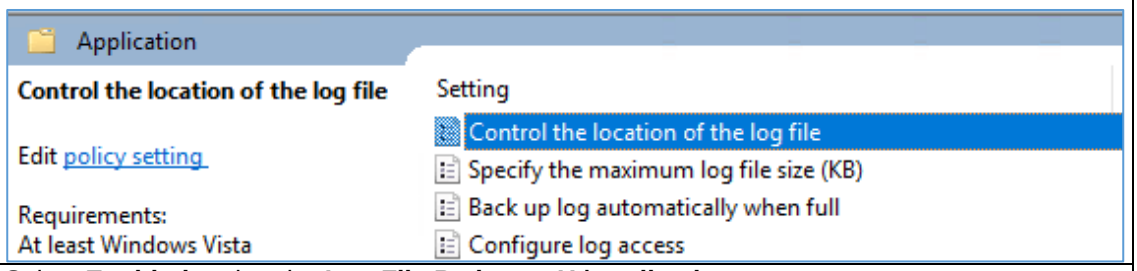
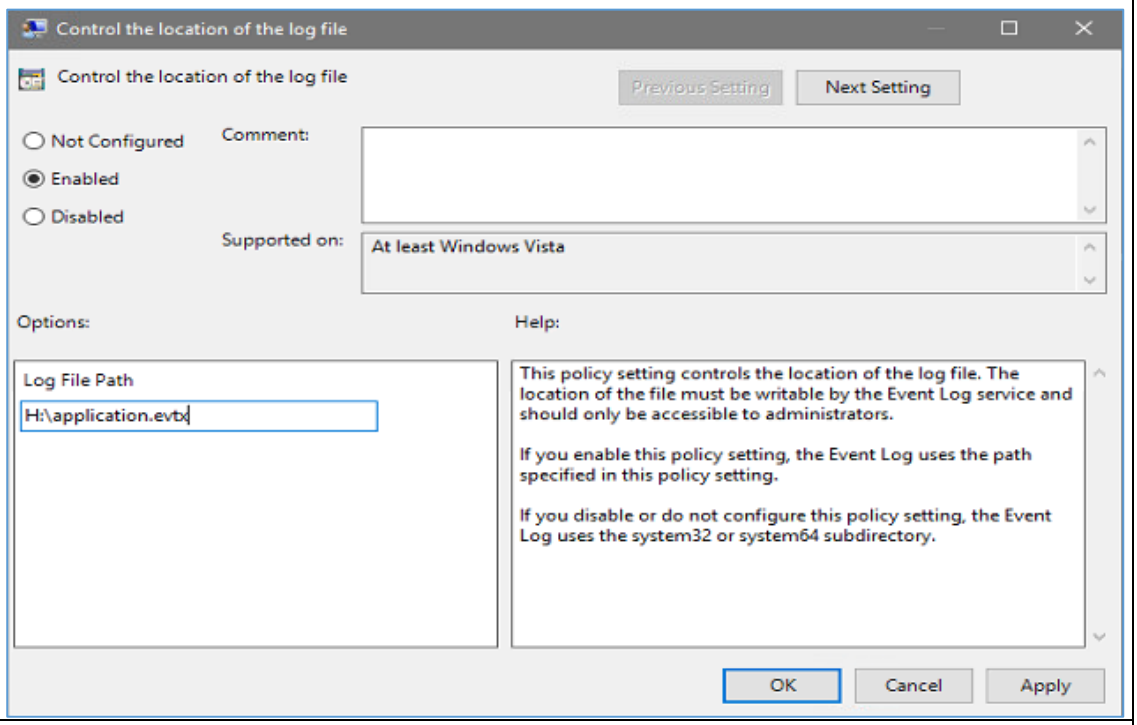


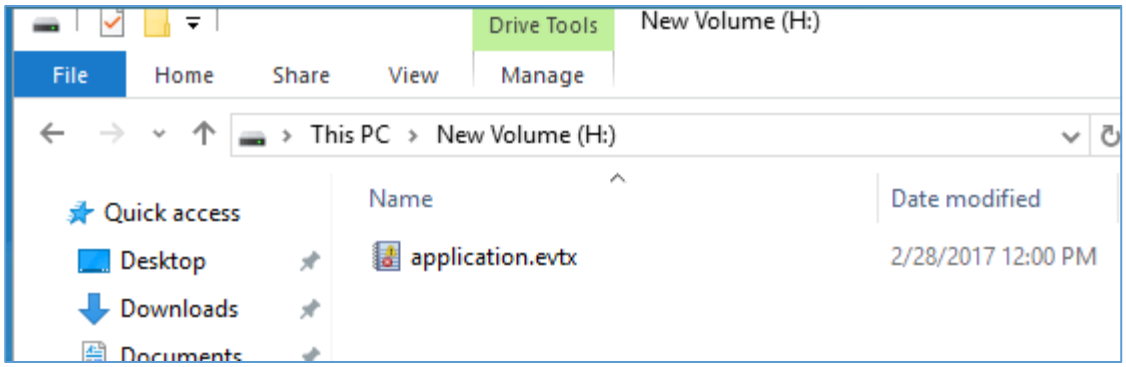
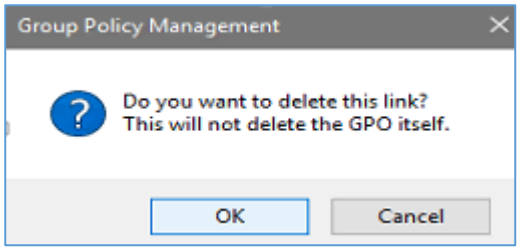
Click **Next**.

18.	Verify **Format this volume with the following settings** raio button is selected. Verify **Perform a quick format** is selected.  Click **Next**.
19.	Click **Finish** and close the **Disk Management console**.
20.	Connect to XenCenter and click **PVS-DTP-MST** and select **Shut Down**.
21.	Using the Remote Desktop Connection manager, connect to **NYC-ADS-001**. To login to NYC-ADS-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the password.
22.	Click **Server Manager** from the task bar. Click **Tools** and select **Group Policy Mangement**. 

	
23.	Browse **Forest:workspacelab.com > Domains > workspacelab.com > Citrix > New York > VDA > Desktops**. 
24.	Right-click **Desktops** and select **Create a GPO in this domain and Link it here**.

	
25.	Type **Redirect Event Logs** and click **OK**. 
26.	Expand **Desktops** and select the **Redirect Event Logs** GPO that was just created. Select **OK** on the Pop-Up message, if prompted. 
27.	Right-click **Redirect Event Logs** and select **Edit**.
28.	Browse to **Computer Configuration > Policies > Administrative Templates > Windows Components > Event Log Service**.
29.	Expand **Event Log Service** and select **Application** in the left pane.

	 **Note:** For this lab exercise we will be redirecting only the Application event logs. All other event logs can be redirected in the same manner.
30.	Double-click **Control the location of the log file** in the right pane. 
31.	Select **Enabled** and under **Log File Path** type **H:\application.evtx**. 
32.	Click **Apply** and **OK**.
33.	Close the **Group Policy Mangement Console**.
34.	Connect to XenCenter and click **PVS-DTP-MST** and select **Start**.
35.	Login to **PVS-DTP-MST** from XenCenter using **WORKSPACELAB\Administrator** with **Password1** as the password.
36.	Open File Explorer and browse to **This PC > H:** .
37.	Open the **H:** directory and notice that the Application event logs have been redirected.

	 Close the **File Explorer**. **Note**: If event logs are not redirected, reboot the machine to apply the Computer Policy.
38.	Shut Down **PVS-DTP-MST** from XenCenter.
39.	Using the Remote Desktop Connection manager, connect to **NYC-ADS-001**. To login to NYC-ADS-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password.
40.	Click **Server Manager** from the task bar. Click **Tools** and select **Group Policy Management**.
41.	Browse **Forest:workspacelab.com >Domains > workspacelab.com > Citrix > New York > VDA > Desktops**.
42.	Expand **Desktops** and right-click the **Redirect Event Logs** GPO that was recently created and select **Delete**. **Note:** We are deleting the GPO since we no longer need it in future exercises.
43.	Click **OK** on the message. 
44.	Close the **Group Policy Management Console**.

Key Takeaways:

- Target Devices reading their hard disk contents from a vDisk in standard image mode will write changes including any event log data to the write cache.
- It is a leading practice to redirect event logs and other data that you want to persist over reboots to a persistent location.
- Typically, every target device will have a local disk attached for hosting the write cache, this location is ideal for redirecting data that should persist over reboots, but event logs can also be redirected to a file server on the network.

Module 19: Integrating Provisioning Services with XenApp and XenDesktop

Overview:

This module presents the process used to integrate the Provisioning Services environment with a pre-existing XenApp and XenDesktop site. This is accomplished by creating a machine template, then using the XenDesktop Setup Wizard or the Streamed VM Wizard to create multiple target devices from that template. Following the target device creation, you will create Catalogs (as needed) and Delivery Groups to complete the resource delivery to the users.

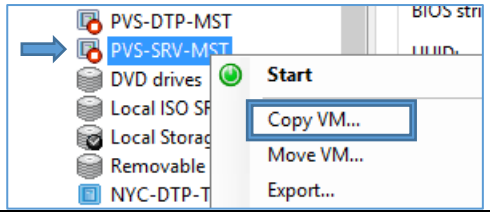
Before you begin:

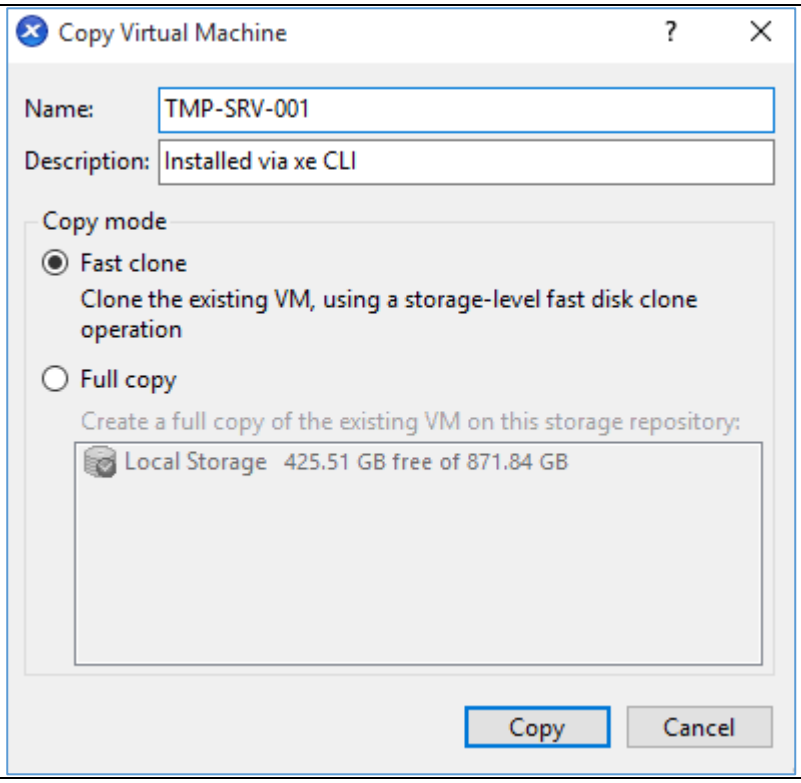
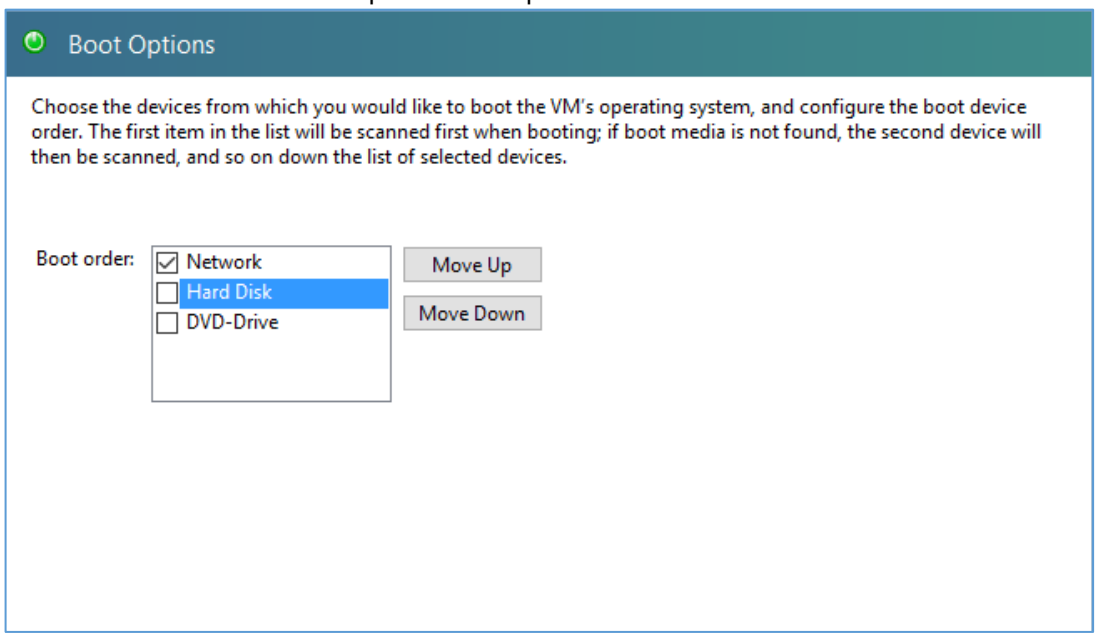
Estimated time to complete Module 19 lab exercises: 100 minutes

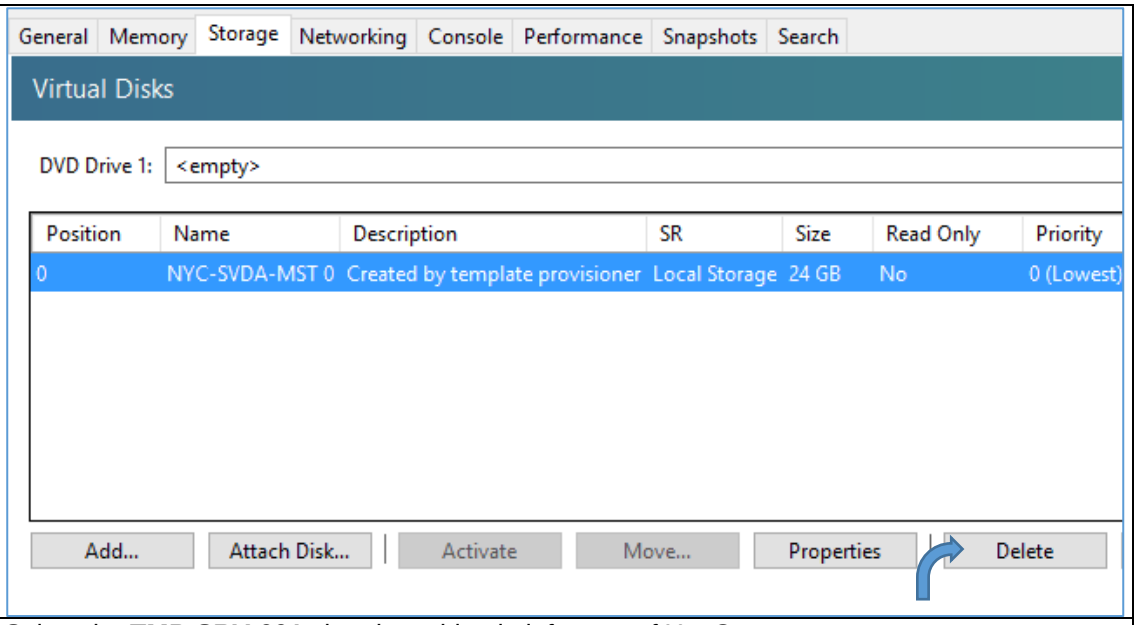
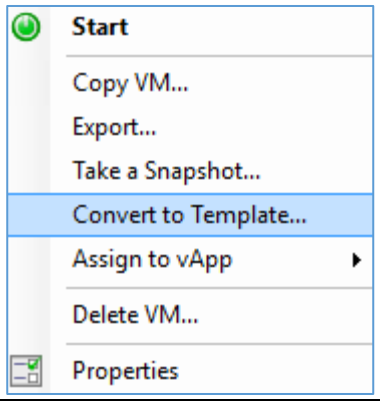
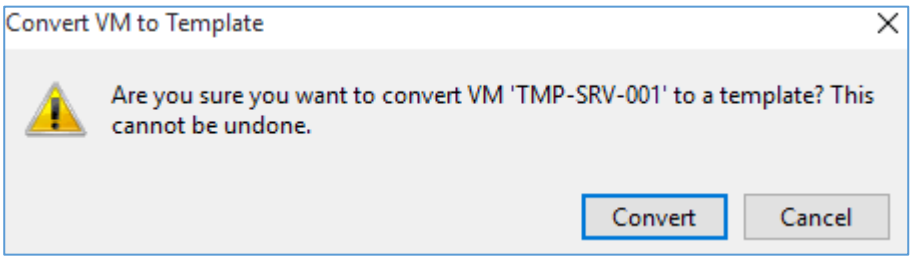
Exercise 19-1: Copy the Server OS Master and convert to a template

Scenario:

You are a Citrix Administrator at WW Labs, your Lead Citrix Architect has informed you that in order to use the built in wizards in Provisioning Services to deploy virtual machines, you must have a VM template, this template should match the VM configuration used to create the vDisk. Your task is to copy the Server Master VM, delete its hard disk associations and convert it to a template.

Step	Action
1.	The following VMs are required before beginning the exercises for this Module; all others may be powered down. To power manage your VMs, switch to XenCenter, right-click on the VM in the left pane and select Start or Shut Down. If prompted click Yes. • NYC-ADS-001 • NYC-SQL-001 • NYC-FSR-001 • NYC-PVS-001 • NYC-XDC-001 • NYC-VNS-001 • NYC-STF-001 • NYC-WRK-001 **Note**: These above VMs are listed in the start-up order.
2.	Connect to XenCenter and select **PVS-SRV-MST**. Right-click and select **Copy VM**. 
3.	In the Name field type **TMP-SRV-001** and click **Copy**.

	
4.	Select **TMP-SRV-001** VM in XenCenter.
5.	Click the **General** tab, click **Properties** and select **Boot Options**.
6.	Make sure **Network** is at the top and other options are unchecked.  Click **OK**.
7.	Click the **Storage** tab to remove the hard drive from the target device so you can use PXE or BDM to start and use a vDisk.
8.	Select the virtual disk, click **Delete** and then click **Yes** in the **Delete Virtual Disk** message.

	
9.	Select the **TMP-SRV-001** virtual machine in left pane of XenCenter.
10.	Right-click and select **Convert to Template**. 
11.	Click **Convert** on the warning message. 
12.	Scroll down in the XenCenter left pane and verify that the TMP-SRV-001 template has been created.

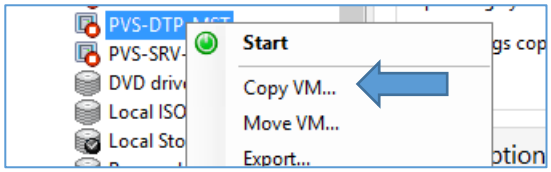
Key Takeaways:

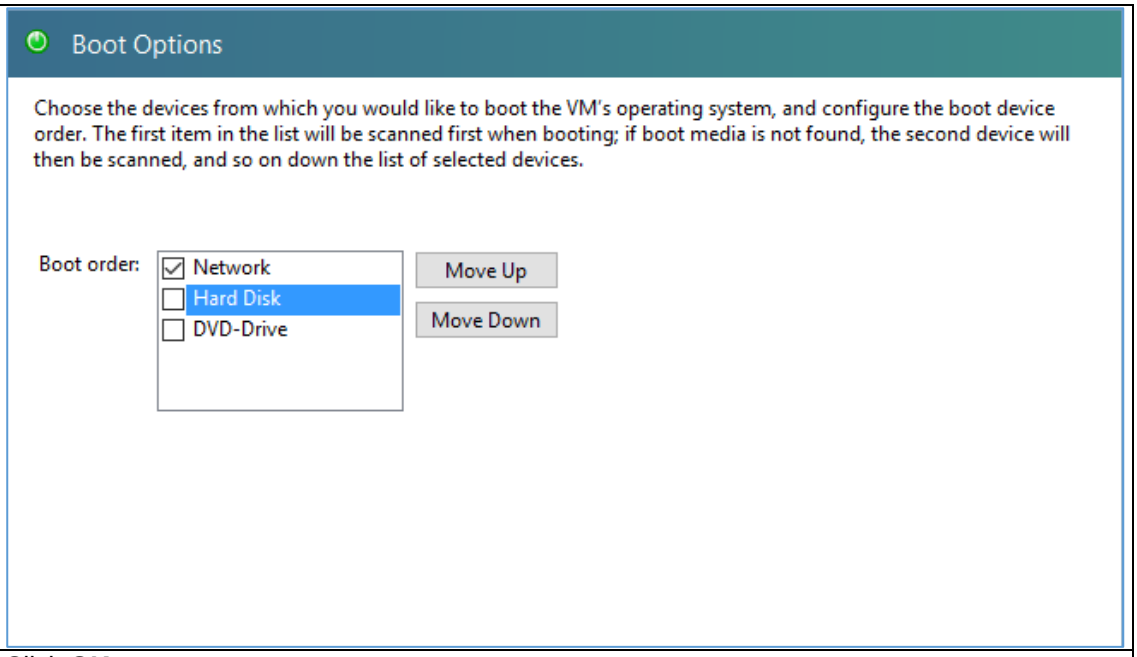
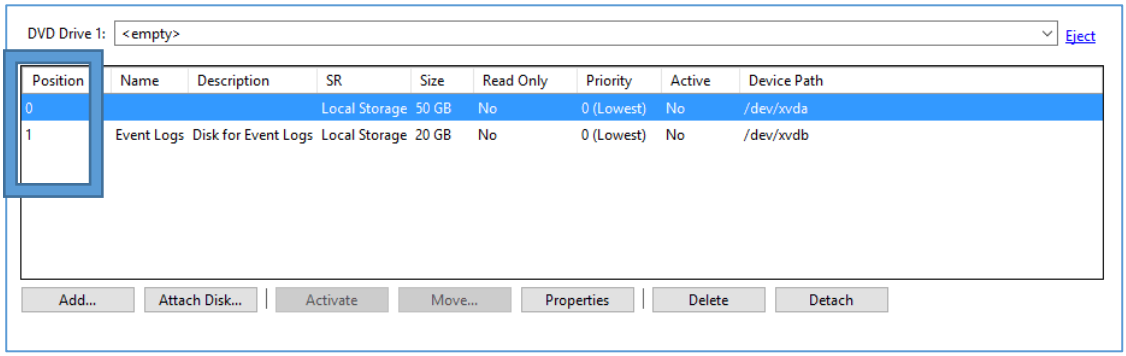
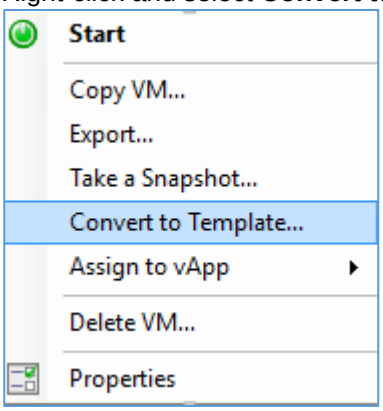
- In order to use the built in wizards in Provisioning Services to deploy virtual machines, a VM template is required.
- The VM template will define the virtual hardware in each VM created by the wizards.
- It is very important that the virtual hardware in the template match the virtual hardware used to build the corresponding image.
- The easiest way to ensure alignment between the master and the template is to copy the master, make the necessary adjustments and convert the copy to a template.
- The template does not need a local disk since the hard disk content is being streamed from PVS.

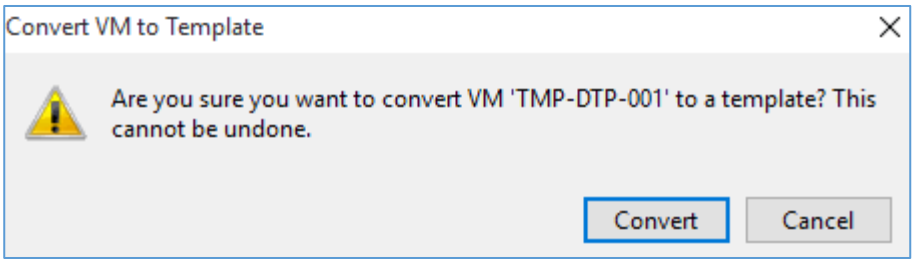
Exercise 19-2: Copy the Desktop OS Master and convert to a template

Scenario:

You are a Citrix Administrator at WW Labs, your Lead Citrix Architect has informed you that because the specifications on Server OS machines might differ from the Desktop OS machines, it is best to create a template for each machine type. Your task is to copy the Desktop Master VM, delete its hard disk associations and convert it to another template.

Step	Action
1.	Connect to XenCenter and select **PVS-DTP-MST**. Right-click and select **Copy VM**. 
2.	Type **TMP-DTP-001** and click **Copy**.
3.	Select **TMP-DTP-001** VM in XenCenter.
4.	Click the **General** tab, click **Properties** and select **Boot Options**.
5.	Make sure **Network** is at the top and other options are unchecked.

	
6.	Click **OK**.
7.	Click the **Storage** tab to remove the hard drive from the target device so you can use PXE or BDM to start and use a vDisk.
8.	Select both the virtual disk one by one and click **Delete** for both disks, and then click **Yes** in the **Delete Virtual Disk** message. 
9.	Select the **TMP-DTP-001** virtual machine in left pane of XenCenter.
10.	Right-click and select **Convert to Template**. 
11.	Click **Convert** on the warning message.

	
12.	Scroll down in the XenCenter left pane and verify that template has been created.

Key Takeaways:

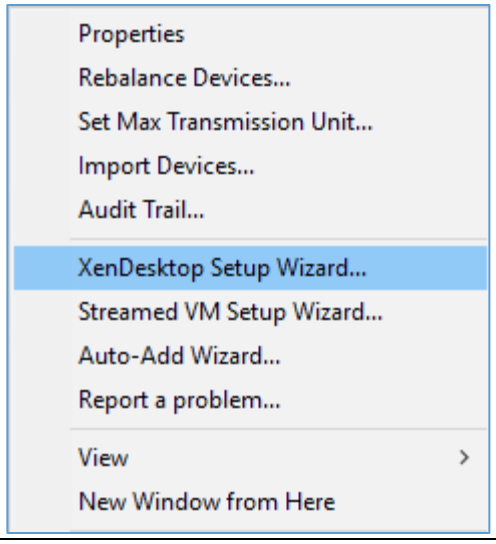
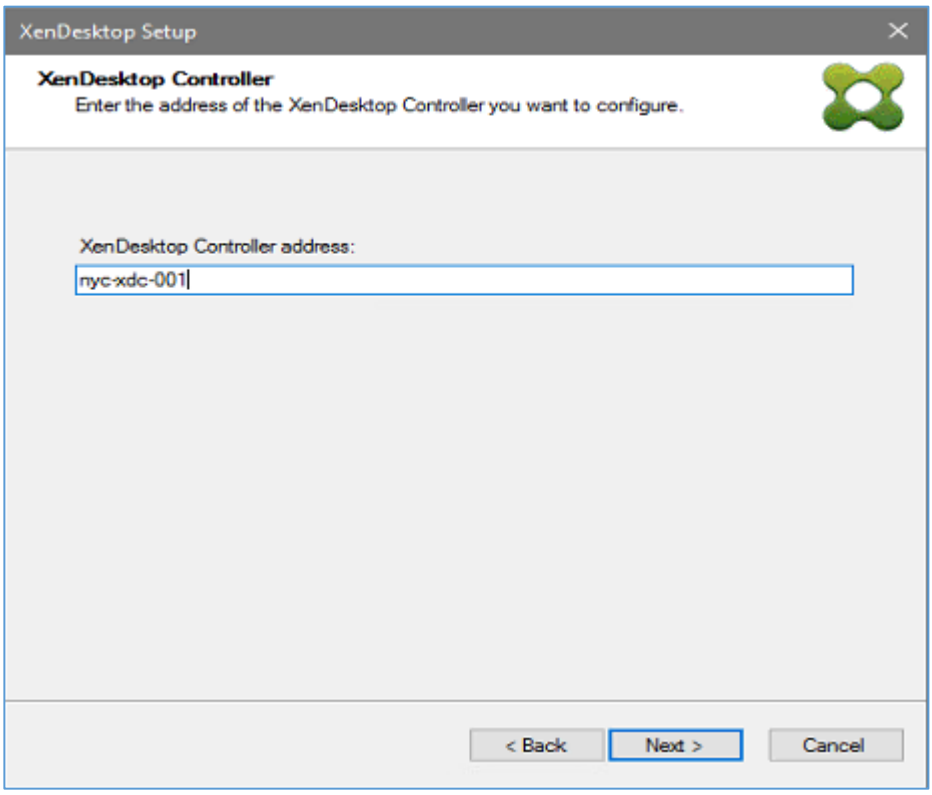
- In order to use the built in wizards in Provisioning Services to deploy virtual machines, a VM template is required.
- The VM template will define the virtual hardware in each VM created by the wizards.
- It is very important that the virtual hardware in the template match the virtual hardware used to build the corresponding image.
- The easiest way to ensure alignment between the master and the template is to copy the master, make the necessary adjustments and convert the copy to a template.
- The template does not need a local disk since the hard disk content is being streamed from PVS.

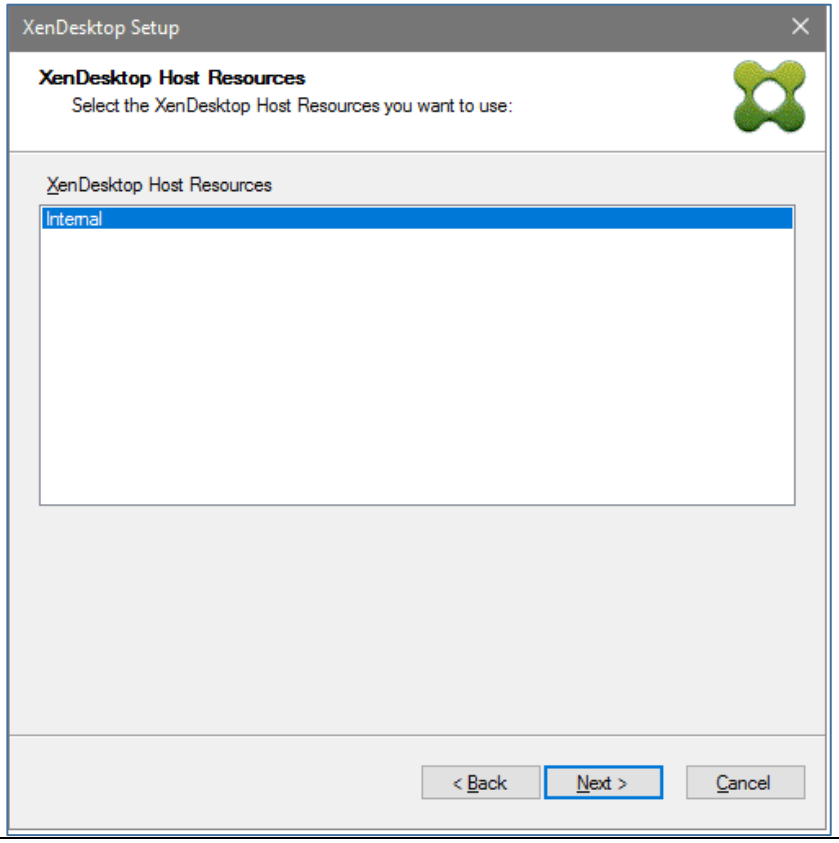
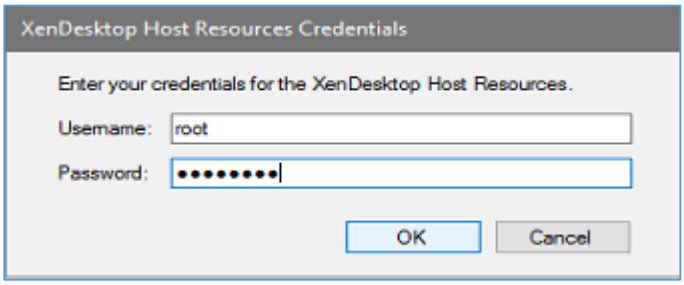
Exercise 19-3: XDSW for Server OS

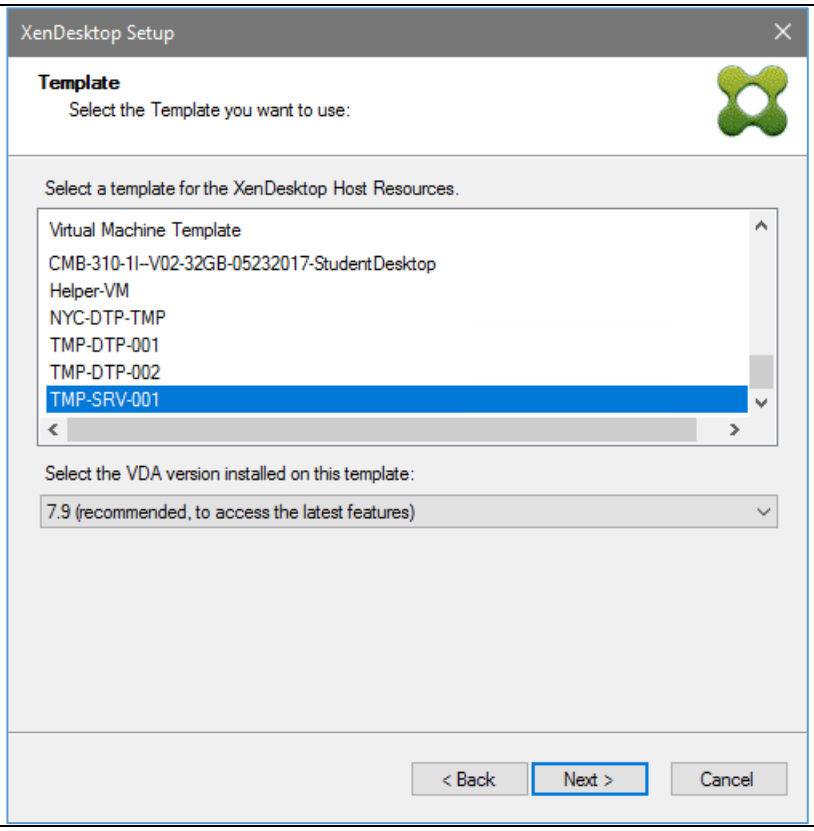
Scenario:

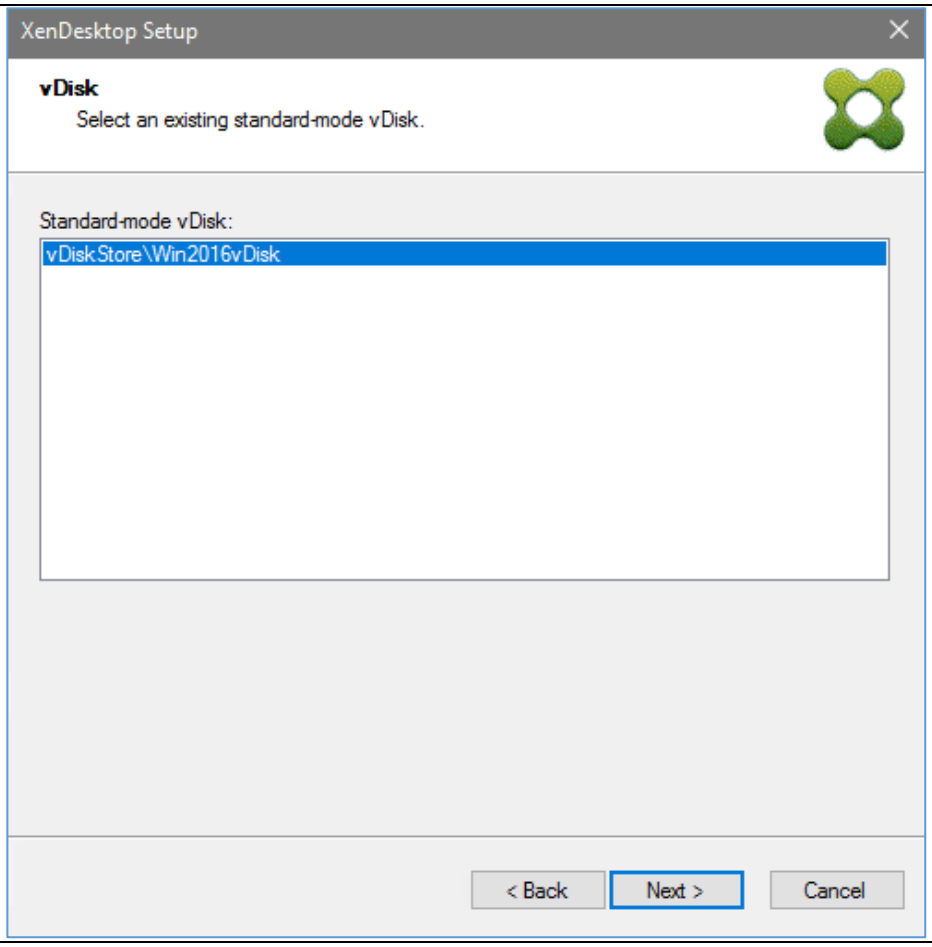
You are a Citrix Administrator at WW Labs; your Lead Citrix Architect has tasked you to test the XenDesktop Setup Wizard in Citrix Provisioning Services. Your task is to create one Server OS machine using the vDisk created in exercise 3-3 and the template created in exercise 5-1
You are a Citrix Administrator.

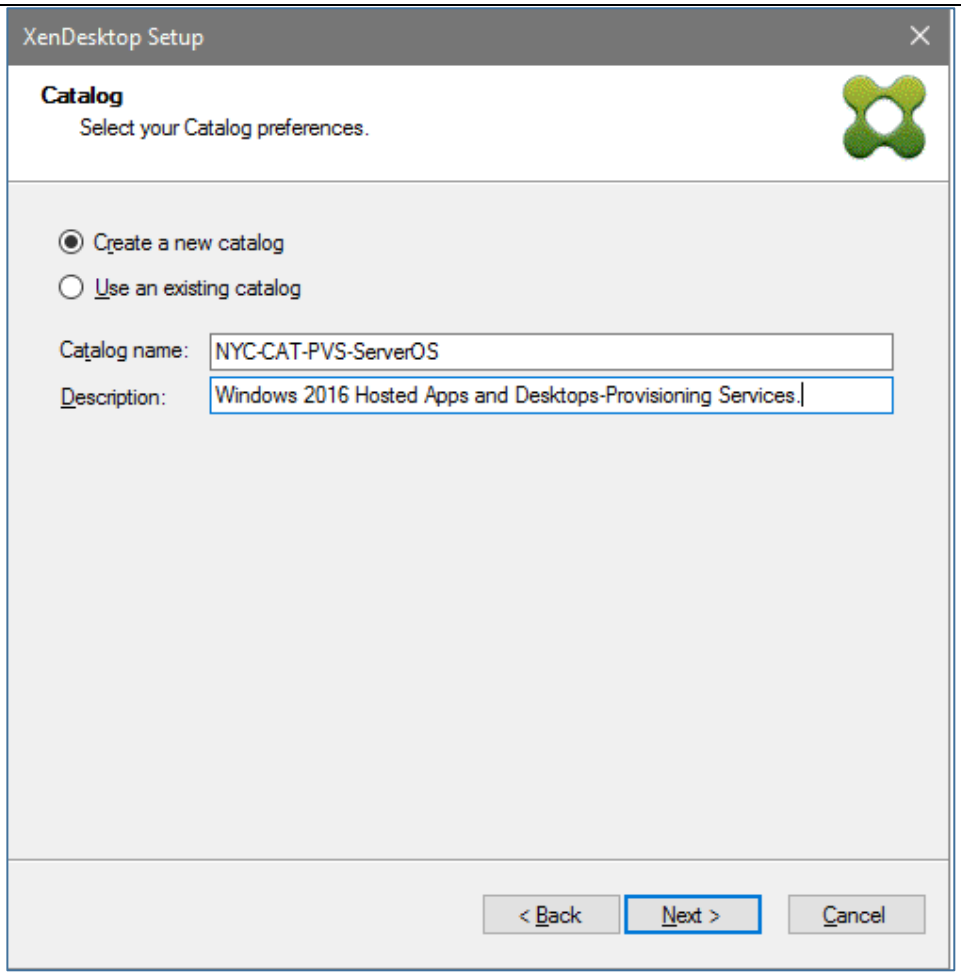
Step	Action
1.	Using the Remote Desktop Connection manager, connect to **NYC-XDC-001**. To login to **NYC-XDC-001** right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the password.
2.	Using the Remote Desktop Connection manager, confirm you are still connected to **NYC-PVS-001**. **Note:** In a previous exercise, you had logged into **NYC-PVS-001** using the following credentials to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the Password. **Note**: If your Remote Desktop Connection session is disconnected, log on to **NYC-PVS-001**, right-click this machine and choose **Connect server**.

3.	Click **Start** and click the **Provisioning Services Console**. Type **Localhost** and click **Connect**.
4.	Browse **Farm > Sites > NYC-Site**. Right-click **NYC-Site** and select **XenDesktop Setup Wizard**. 
5.	Click **Next** on the **Welcome** screen.
6.	In the XenDesktop Controller address field, type **nyc-xdc-001**.  Click **Next**. **Note:** The Delivery Controller is already configured for the lab environment.

7.	Verify **Internal** is selected in the **XenDesktop Host Resources** and click **Next**. 
8.	Verify **root** is pre-populated in the Username field. Take note of the XenServer hypervisor connection details discovered in Module 3, Exercise 5, Step 7 and type the password provided.  Click **OK**.
9.	Select **TMP-SRV-001** and click **Next**.

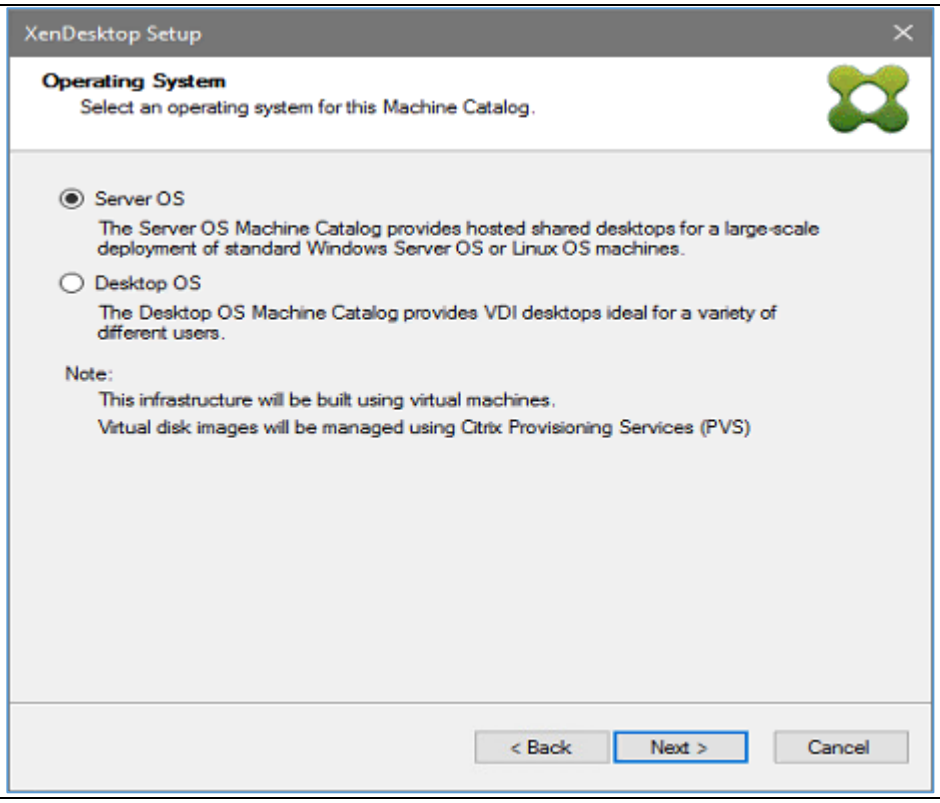
	
10.	Select **vDiskStore\Win2016vDisk** and click **Next**.

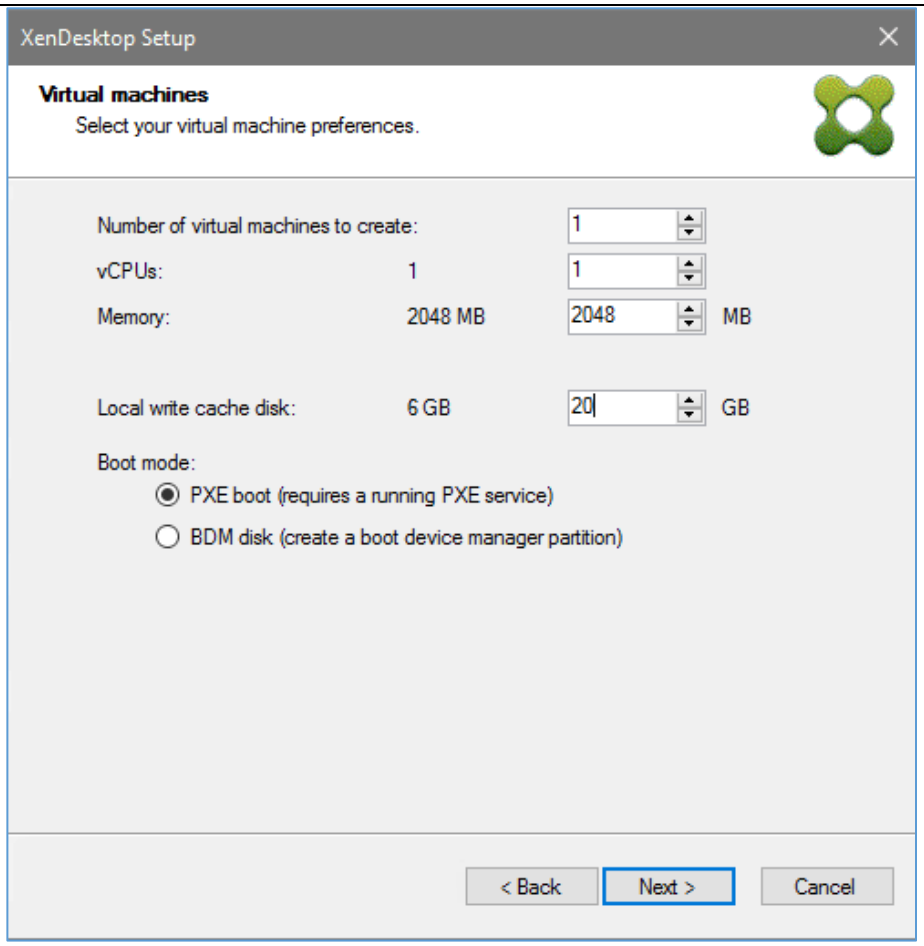
	
11.	Verify **Create a new catalog** is selected and then enter in the following: • Catalog name: **NYC-CAT-PVS-ServerOS** • Description: **Windows 2016 Hosted Apps and Desktops-Provisioning Services**.

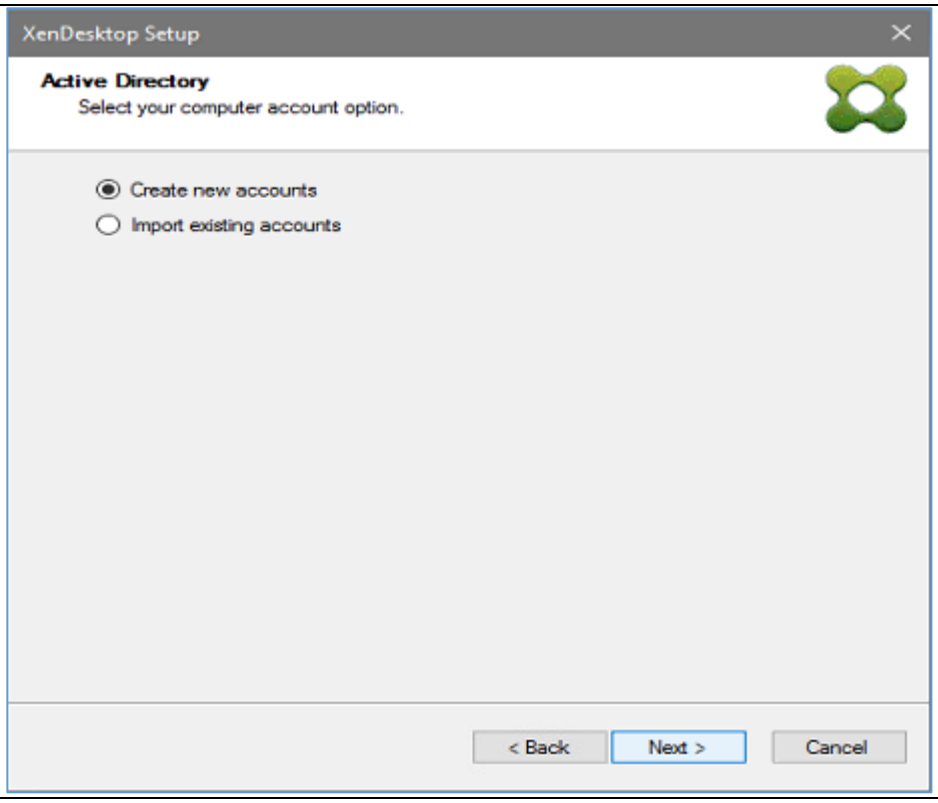


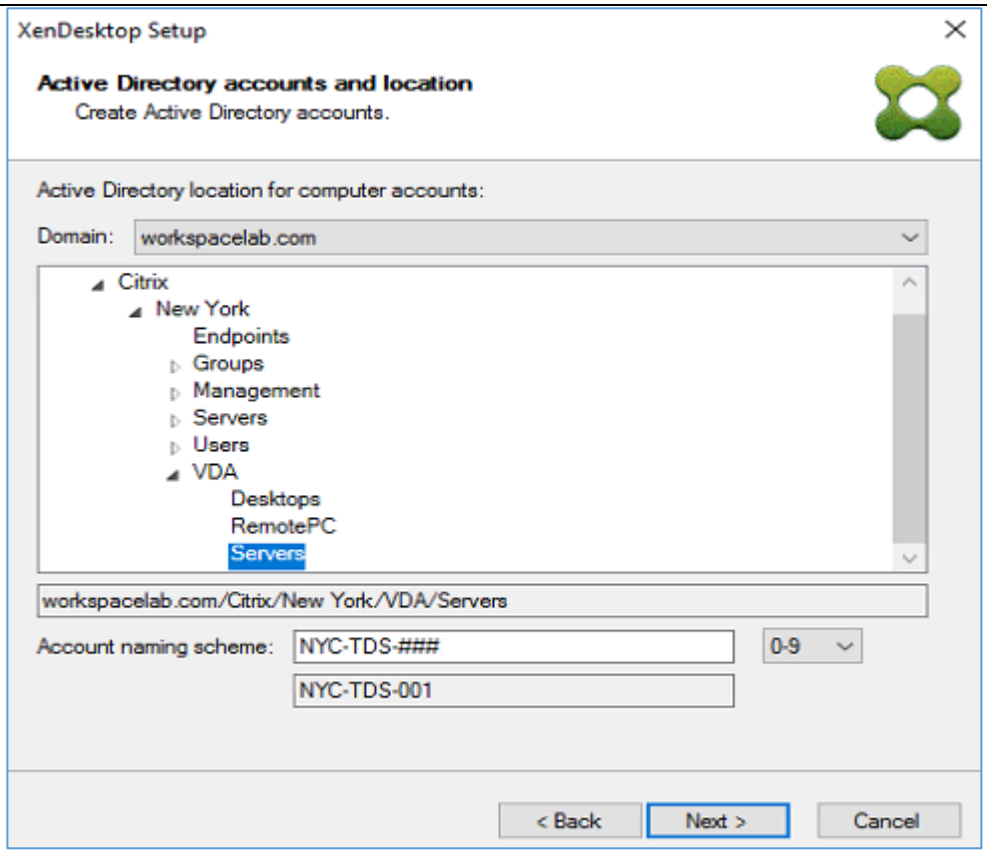
Click **Next**.

12. Select **Server OS** as the Operating System and click **Next**.

	
13.	Using the Local write cache disk field increase the size to **20** GB. Keep all other settings as default.

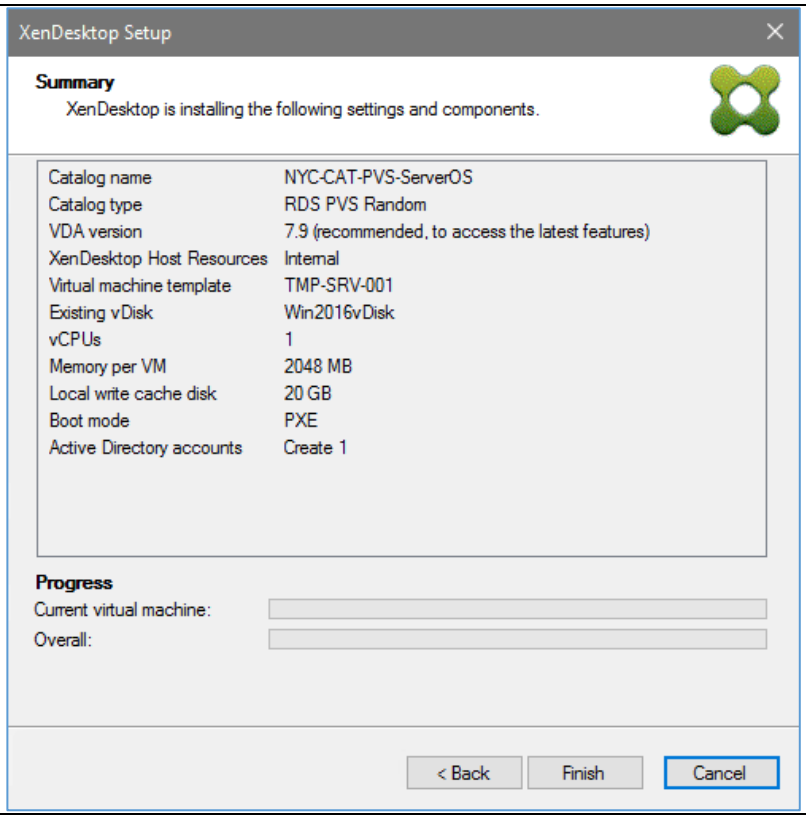
	 Click **Next**. **Note:** CPU and Memory values in the screenshot may differ with respect to the lab environment. **Note:** We are using DHCP options 66 and 67 to provide the boot file. One alternative to using DHCP is to create a Boot Device Partition to include the bootstrap file in a small virtual disk attached to each PVS target device VM. After using the XenDesktop setup wizard, each target device has an 8MB VHD file containing the bootstrap within its newly configured disk partition.
14.	On the Active Directory page, select **Create new accounts** and click **Next**.

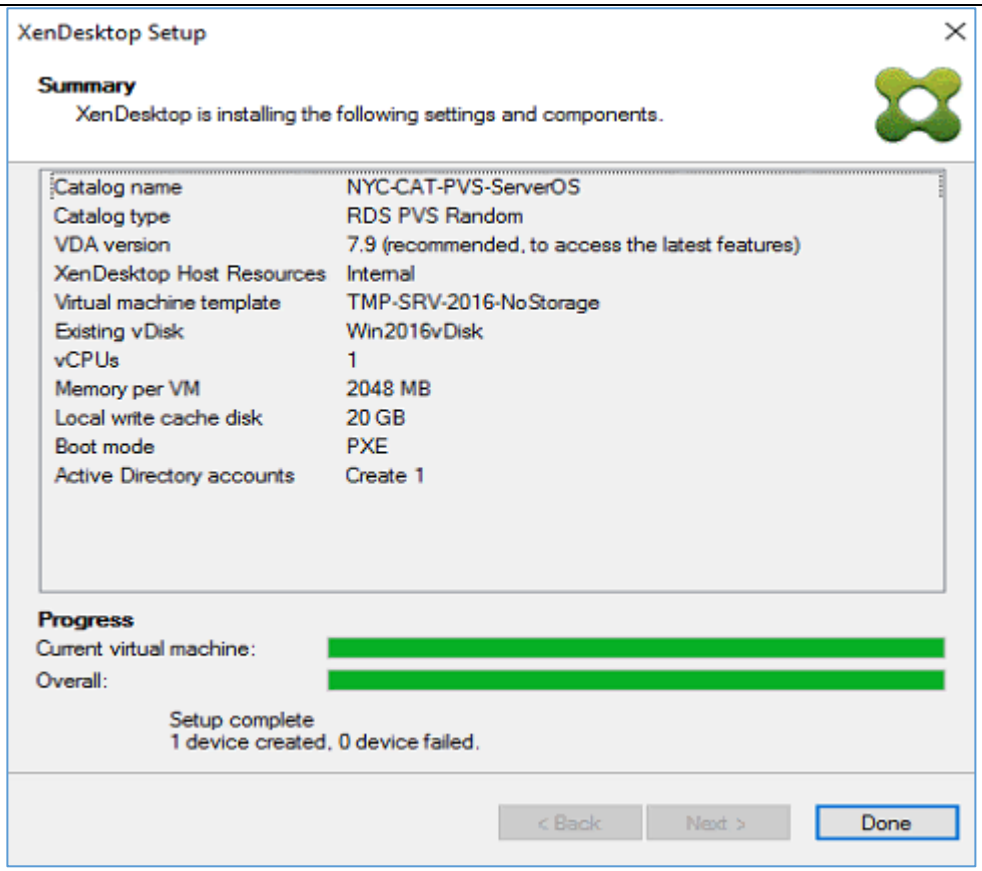
	
15.	Browse **Citrix > New York > VDA > Servers** and select the **Servers**. In the Account naming scheme field, type **NYC-TDS-###**.



Click **Next**.

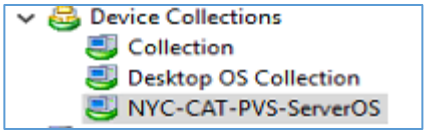
16. Verify the details in the **Summary** page and click **Finish**.

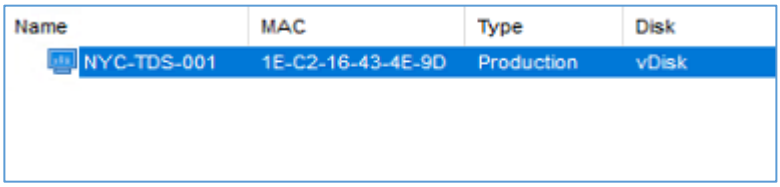
	
17.	Verify the progress completes successfully. Verify the text at the bottom of the screen reads: • Setup Complete • 1 device created, 0 device failed.



Click **Done**.

18. Refresh the **Provisioning Services console** and verify that a new Device Collection gets created in the left pane and that a new target device gets created in the right pane.





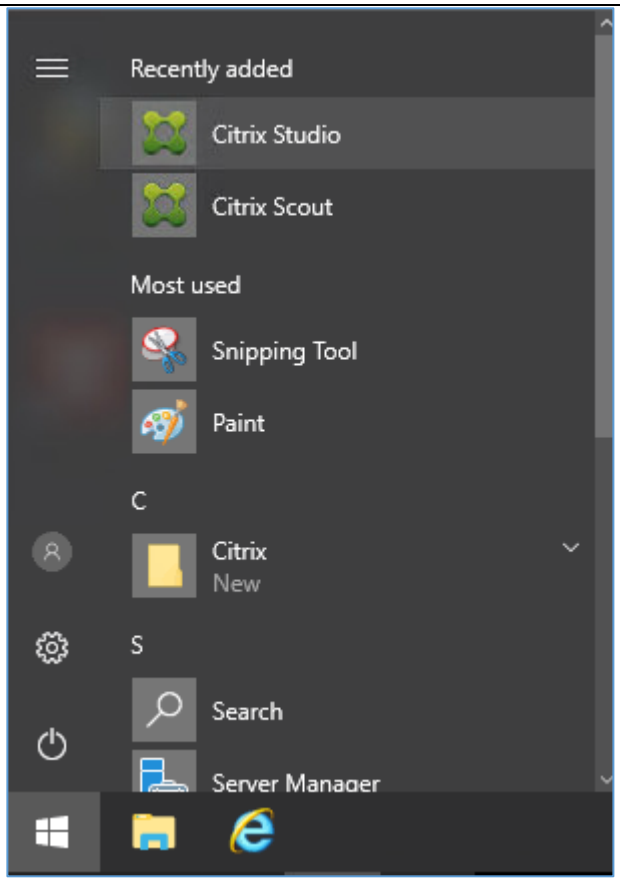
Close the **Provisioning Services Console**.

19. Using the Remote Desktop Connection manager, connect to **NYC-XDC-001**.

To login to **NYC-XDC-001**, right-click this machine and choose **Connect server**.

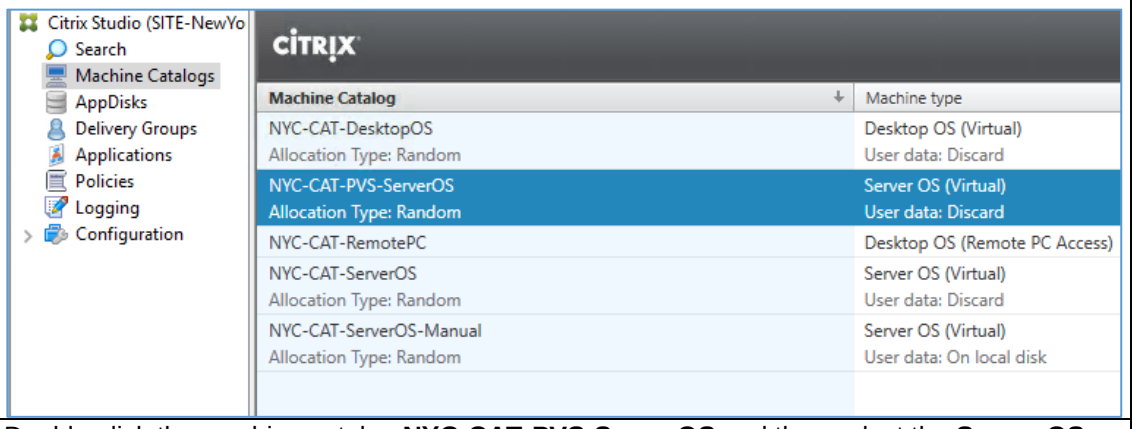
Note: The following credentials are used to make the connection:
User name: **WORKSPACELAB\Administrator** with **Password1** as the password.

20. Click **Start** and click **Citrix Studio**.

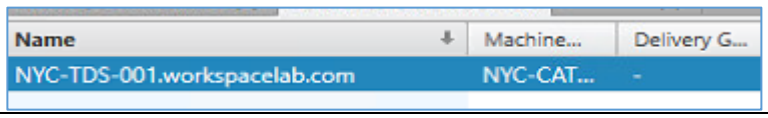


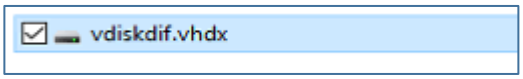
Note: Ignore this step if Studio is already open.

21. Click on **Machine Catalogs** in left pane. Verify that the expected machine catalog has been created in studio using the **XenDesktop Setup Wizard** from the Provisioning Services console.



22. Double-click the machine catalog **NYC-CAT-PVS-ServerOS** and then select the **Server OS Machines (1)** tab to verify that **NYC-TDS-001.workspacelab.com** machine is listed within the machine catalog.



23.	Close the **Citrix Studio**.
24.	Connect to **XenCenter** and select **NYC-TDS-001,** then right-click and select **Start**. Click **Console** tab and monitor the progress.
25.	Using the Remote Desktop Connection manager, connect to **NYC-TDS-001**. To login to **NYC-TDS-001** right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: User name: **WORKSPACELAB\ Administrator** with **Password1** as the Password.
26.	Open Windows **File Explorer** from the taskbar and browse to **This PC > WCDisk (D:)**. Double-click the **WCDisk** directory and verify that the **vdiskdif.vhdx** file was created for caching.  **Note:** The **VDiskdif.vhdx** cache file's size will not increase until 64 MB of memory from Non-Paged Pool gets used which we mentioned in Exercise 17-1.
27.	Close the **File Explorer**.
28.	Connect to XenCenter and Shut Down **NYC-TDS-001**.

Key Takeaways:

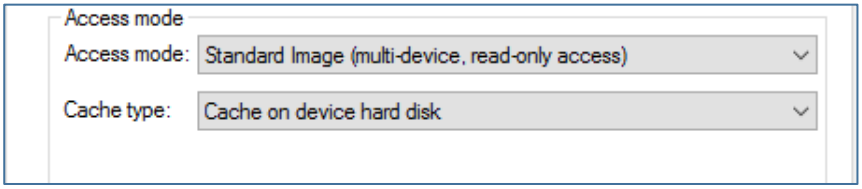
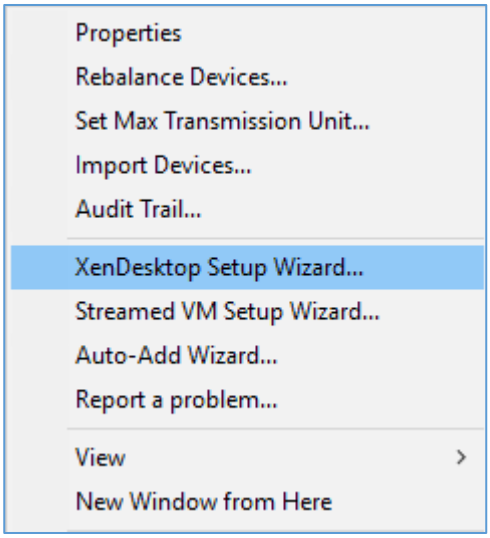
- The XenDesktop Setup Wizard is a built in wizard that can automate the process of creating Virtual Machines, Write Cache disks, Active Directory accounts, Machine Catalogs and Device Collections based on a vDisk and a VM template.

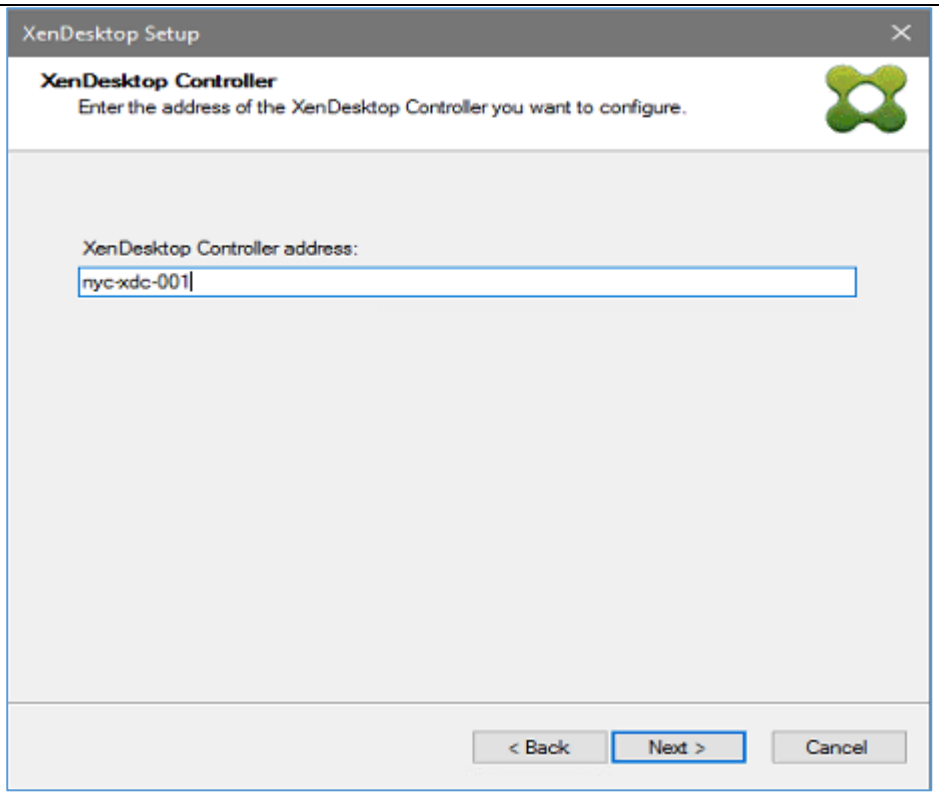
Exercise 19-4: XDSW Desktop OS

Scenario:

You are a Citrix Administrator at WW Labs, your Lead Citrix Architect has verified the Server OS machine you created in the previous exercise. Now he wants you to run the wizard again to provision a Desktop OS machine using the Win10 vDisk and the Desktop OS template. During the provisioning of Desktop OS target devices you will enable BDM disk, which will copy the bootstrap on to a local virtual disk, eliminating the need to do network boot.

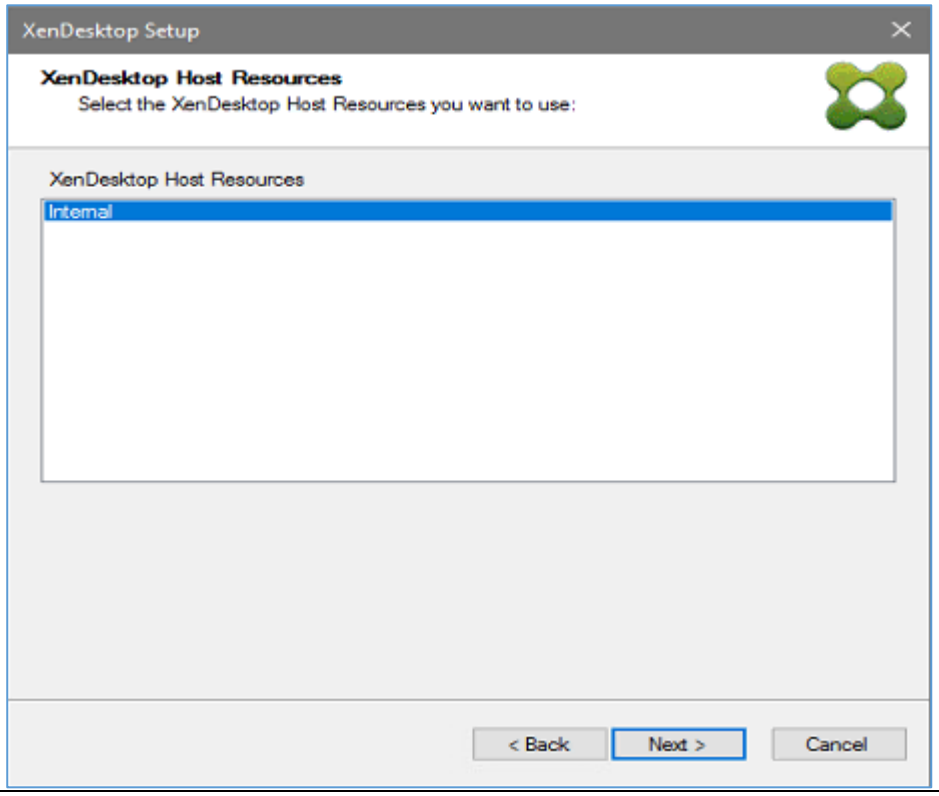
Step	Action
1.	Using the Remote Desktop Connection manager, confirm you are still connected to **NYC-PVS-001**. **Note:** In a previous exercise, you had logged into NYC-PVS-001 using the following credentials to make the connection: user name: **WORKSPACELAB\Administrator** with **Password1** as the password. **Note:** If your Remote Desktop Connection session is disconnected, log on to **NYC-PVS-001**, right-click this machine and choose **Connect server**.
2.	Click **Start** and click the **Provisioning Services** console. Type **Localhost** and click **Connect**. **Note**: Ignore this step if the console is already opened and connected to the farm.
3.	Browse **Farm > Sites > NYC-Site > vDisk Pool** in left pane and select **Win10vDisk** in right pane and right-click to select **Properties**.

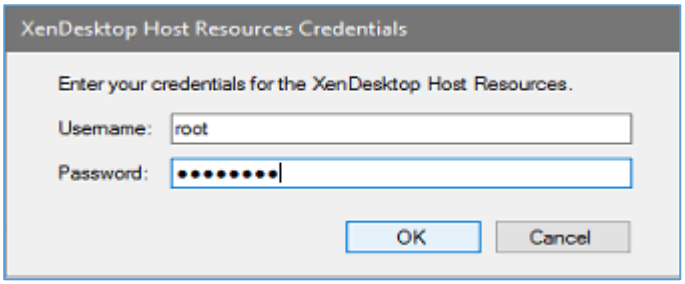
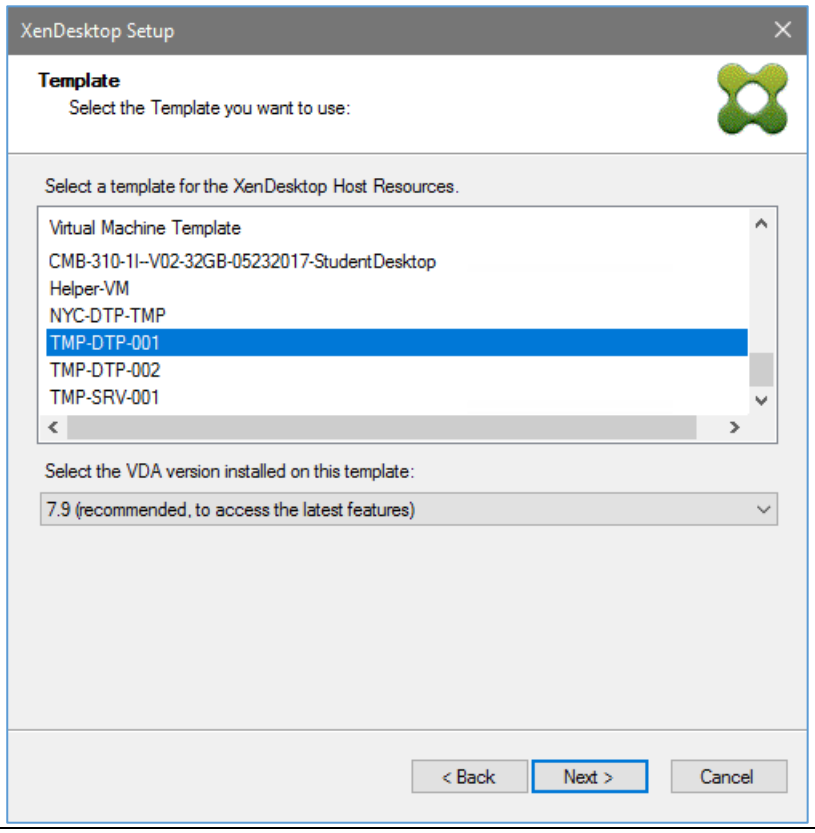
4.	Change the **Access mode** from **Private Image** mode to **Standard Image** with write **Cache on device hard disk** and then click **OK**.  **Note:** Refer exercise 18-2 to change the vDisk Mode. Ignore if vDisk is already in Standard Image mode.
5.	Browse **Farm > Sites > NYC-Site**. Right-click **NYC-Site** and select **XenDesktop Setup Wizard**. 
6.	Click **Next** on the Welcome screen.
7.	In the XenDesktop Controller address field, verify **nyc-xdc-001** is entered.

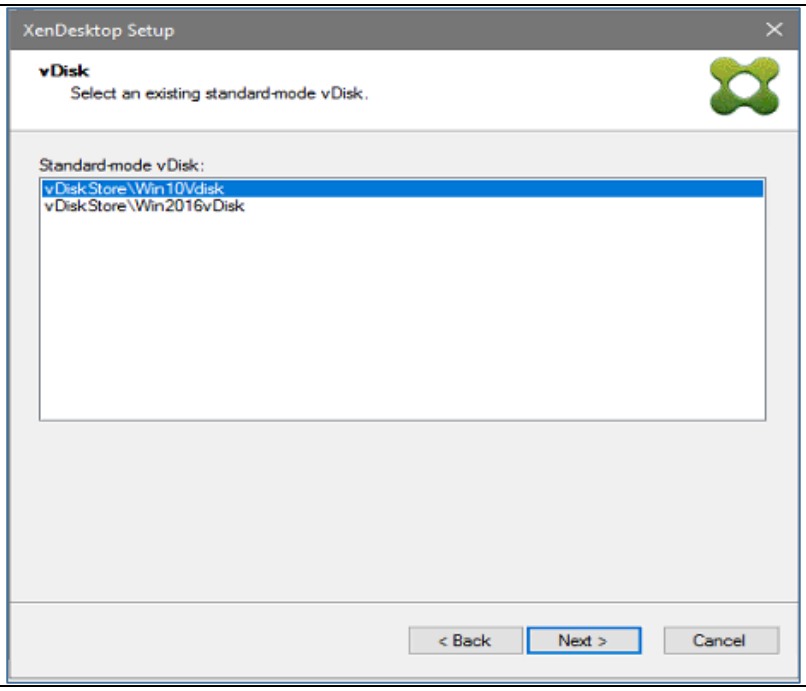


Click **Next**.

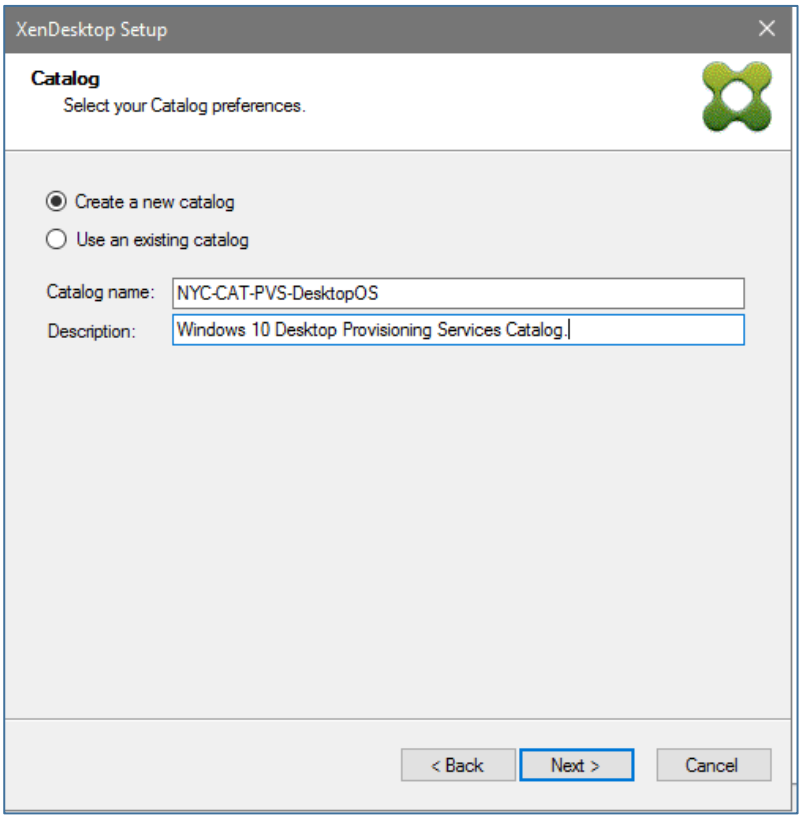
8. Verify **Internal** is selected in the **XenDesktop Host Resource** and click **Next**.



9.	Verify Root is pre-populated as Username. Take a note of the XenServer hypervisor connection details discovered in Exercise 5-3 and type the Password provided.  Click **OK**.
10.	Select **TMP-DTP-001** and click **Next**. 
11.	Select **vDiskStore\Win10VDisk** and click **Next**.

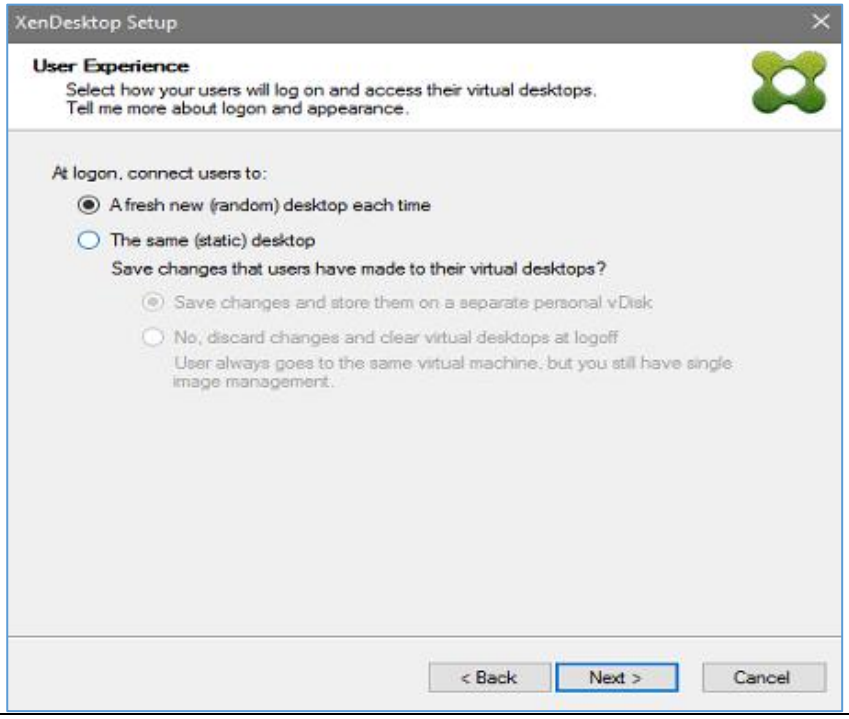
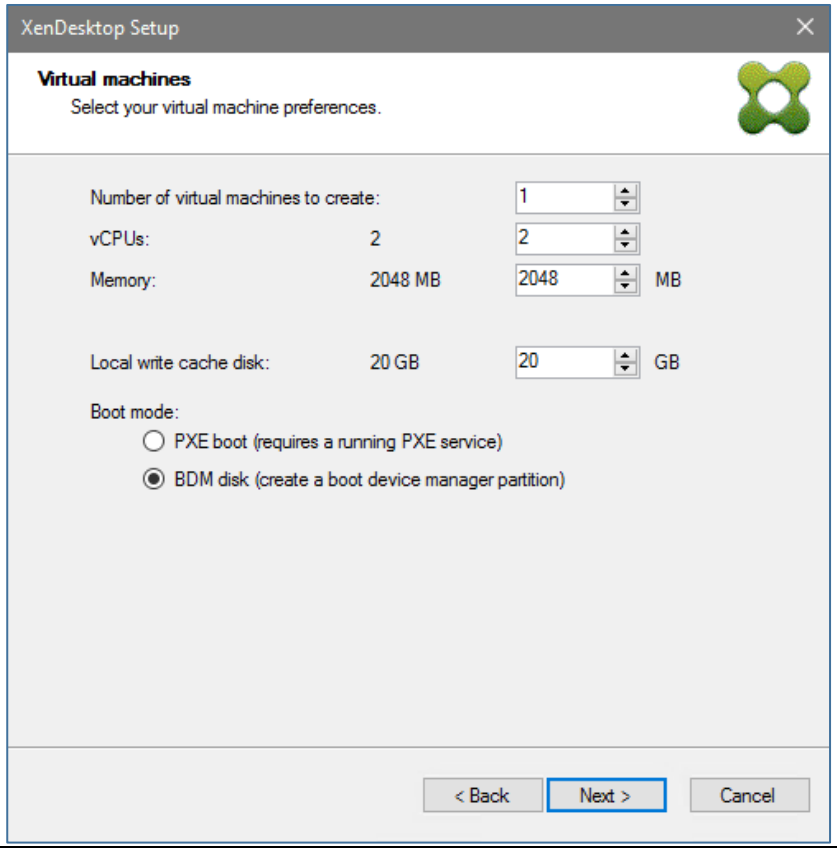


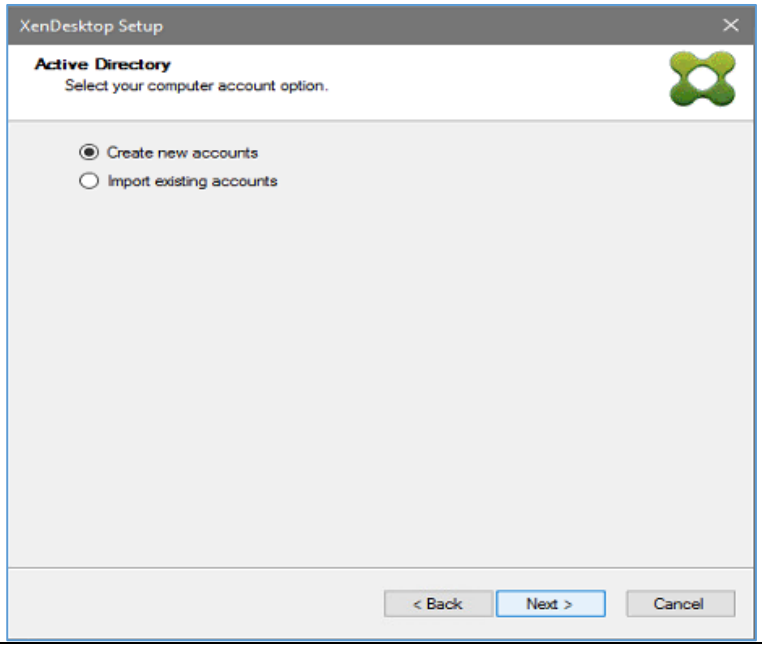
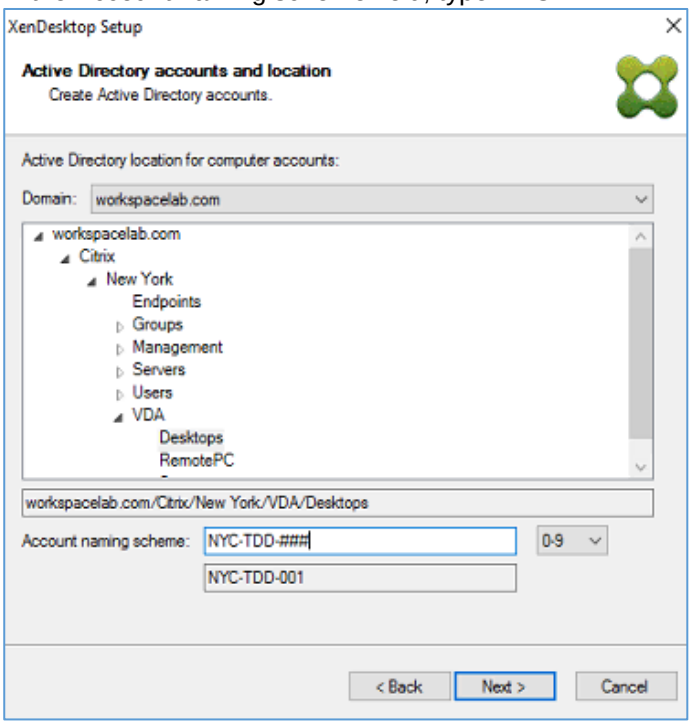
12. Verify **Create a new catalog** is selected and enter the following:
    - Catalog name: **NYC-CAT-PVS-DesktopOS**
    - Description: **Windows 10 Desktop Provisioning Services Catalog**.

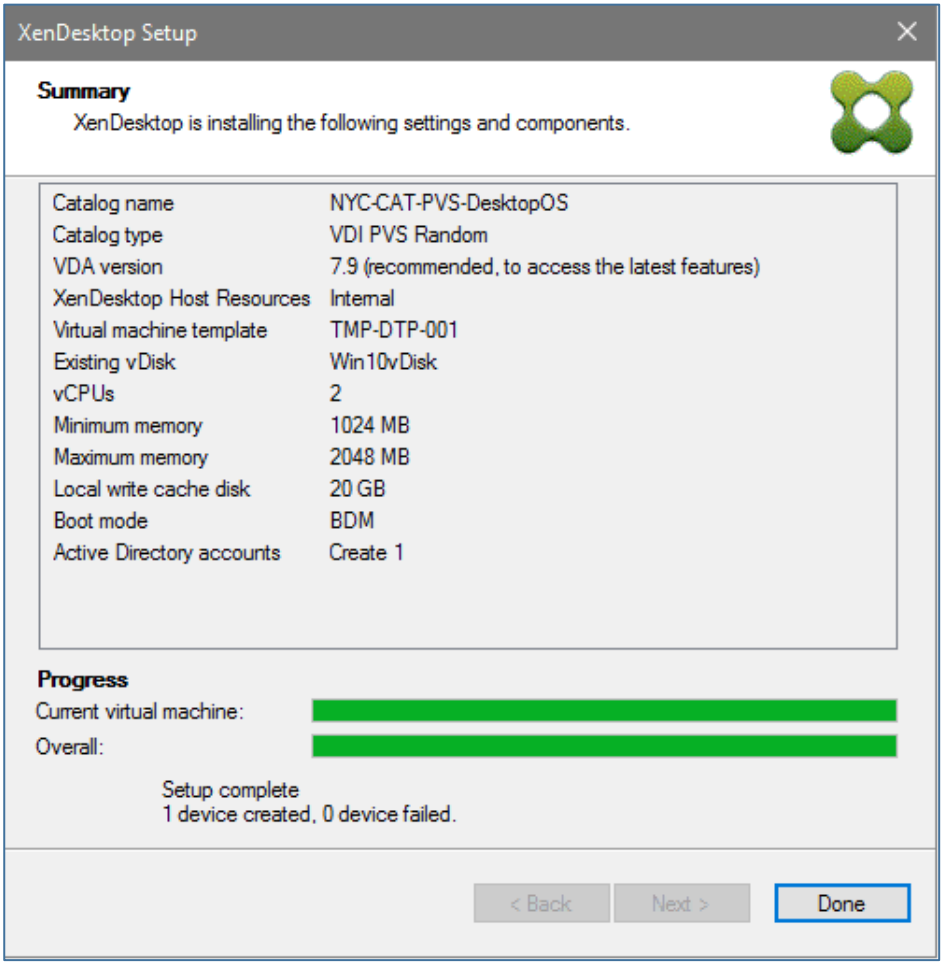


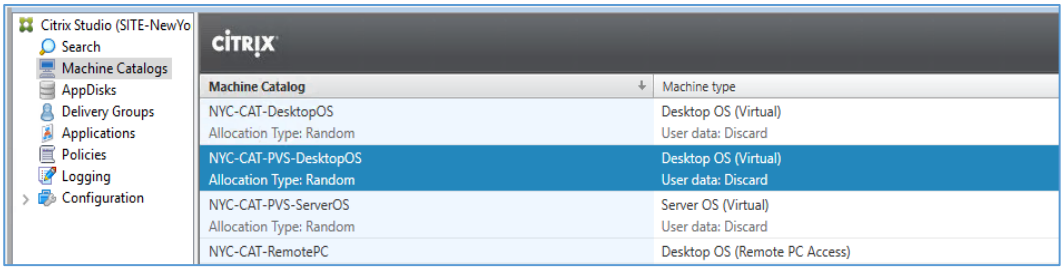
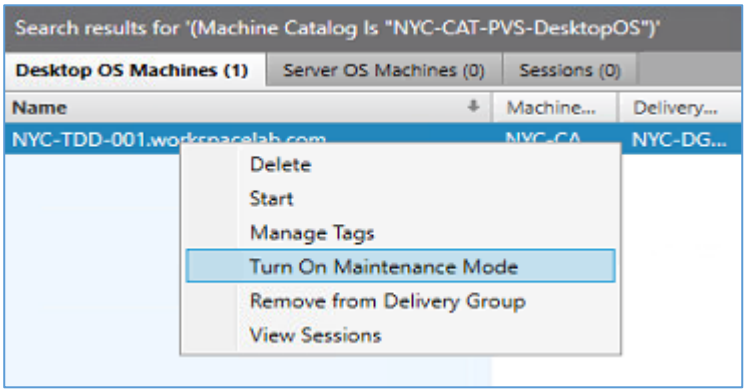
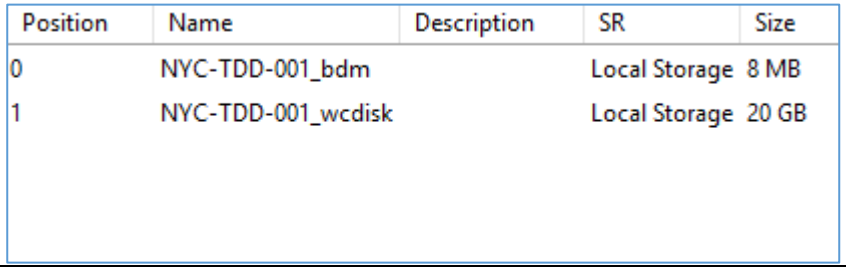
Click **Next**.

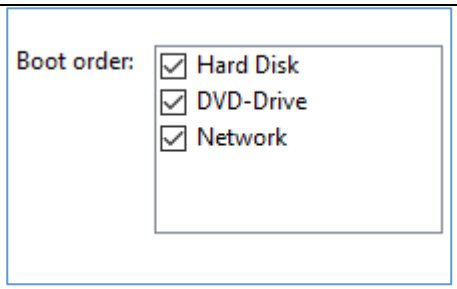
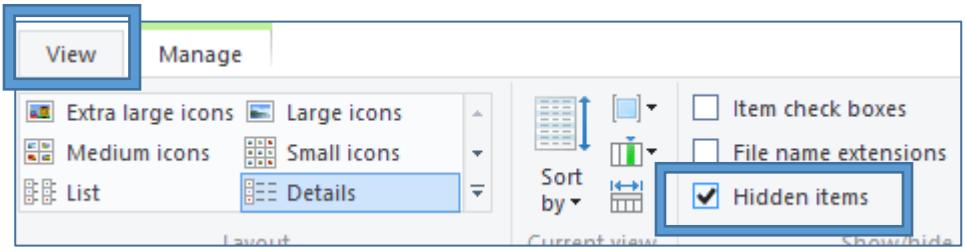
13. Select **Desktop OS** as the Operating System and click **Next**.

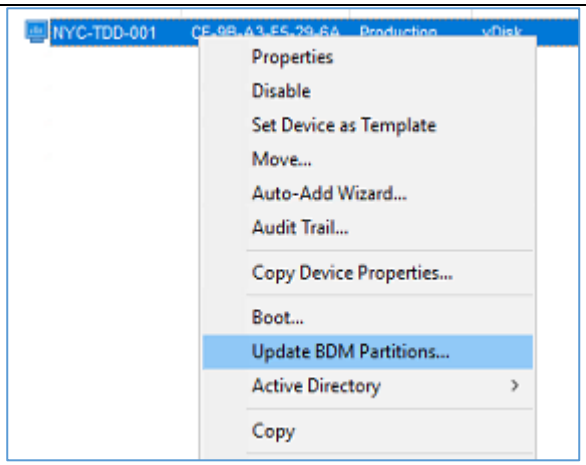
14.	Select **A fresh new (random) desktop each time** for User Experience and click **Next**. 
15.	Using the Local write cache disk field increase the size to **20** GB. Using the Boot Mode field select **BDM Disk**. Keep all other settings as default. 

	Click **Next**. **Note:** Memory and vCPUs values might differ with respect to the lab environment.
16.	On the Active Directory page, select **Create new accounts** and click **Next**. 
17.	Browse **Citrix > New York > VDA > Desktops** and select **Desktops** OU for creation of new accounts. In the Account naming scheme field, type **NYC-TDD-###**  Click **Next**.

18.	Verify the details in **Summary** and click **Finish**. 
19.	Verify the progress completes successfully. Verify the text at the bottom of the screen reads: • Setup Complete • 1 device created, 0 device failed Click **Done**.
20.	Refresh the **Provisioning Services** console and verify that a new Device Collection named **NYC-CAT-PVS-DesktopOS** gets created. **Note:** Select Device Collections and refresh if new Device Collection is not seen.
21.	Using the Remote Desktop Connection manager, connect to **NYC-XDC-001**. To login to **NYC-XDC-001**, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the Password.
22.	Click **Start** and click **Citrix Studio**. **Note:** Ignore if Studio is still open from previous exercise.

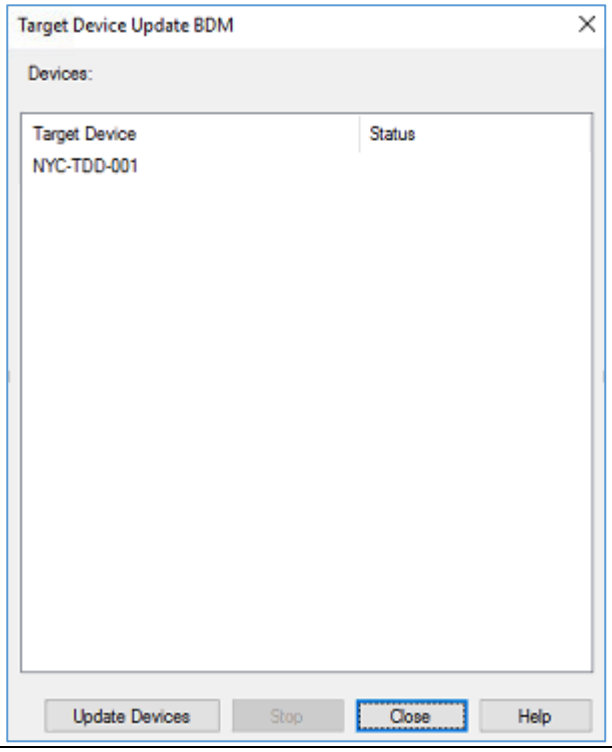
23.	Click on **Machine Catalogs** in left Pane. Verify that the expected Machine Catalog, **NYC-CAT-PVS-DesktopOS** has been created by the XenDesktop Setup Wizard from Provisioning Server. 
24.	Double-click the **NYC-CAT-PVS-DesktopOS** catalog and verify **NYC-TDD-001** machine is in there under the Desktop OS Machine (1).
25.	Right-click **NYC-TDD-001** and select **Turn On Maintenance Mode** and click **Yes** to confirm.  **Note: NYC-TDD-001** is put in Maintenance mode to avoid automatic Power ON by the Controller.
26.	Close the **Citrix Studio**.
27.	Connect to **XenCenter**, select **NYC-TDD-001** and select **Storage** tab in right pane. Notice an 8 MB bdm disk has been added and 20 GB cache disk. 
28.	Select **General** tab **Properties > Boot Options** and notice Hard disk is at the top to boot from the bdm disk.

	 Click **OK**.
29.	Right-click **NYC-TDD-001** and select **Start**. **Note:** Ignore this step if the machine is already booted up.
30.	Using the Remote Desktop Connection manager, connect to **NYC-TDD-001**. To login **NYC-TDD-001,** right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: User name: **WORKSPACELAB\ Administrator** with **Password1** as the Password.
31.	Open **File Explorer** from the taskbar and browse to **This PC > WCDisk**. Double-click **WCDisk** directory and see the **.vdiskcache** file is created for caching. **Note:** If cache file is not seen click **View** and check **Hidden items**.  **Note:** The vDiskcache file is a sparse file and therefore shows 0 bytes by default. Right-click and select properties to see the correct size.
32.	Close the **File Explorer**.
33.	Connect to XenCenter and Shut Down **NYC-TDD-001**. Monitor the console tab until machine is completely Shut Down.
34.	Using the Remote Desktop Connection manager, switch back to **NYC-PVS-001**.
35.	Expand **Device Collections** in Provisioning Console and select **NYC-CAT-PVS-DesktopOS**.
36.	In the right pane, right-click **NYC-TDD-001** and select **Update BDM Partitions**.



Note: This is a new feature in Provisioning Services from version 7.9 onwards. Now boot partitions can be updated automatically. After updating bootstrap information of Provisioning server, boot partitions can directly be upgraded using Update BDM Partitions. Target device needs to be Shut Down to make any update.

37. Click **Close**, as there is no update at this time.



Key Takeaways:

- The XenDesktop Setup Wizard is a built in wizard that can automate the process of creating Virtual Machines, Write Cache disks, Active Directory accounts, Machine Catalogs and Device Collections based on a vDisk and a VM template.
- The XenDesktop Setup Wizard can add a small BDM disk to each virtual machine, the BDM disk contains the bootstrap and can eliminate the need to support network boot in the datacenter.

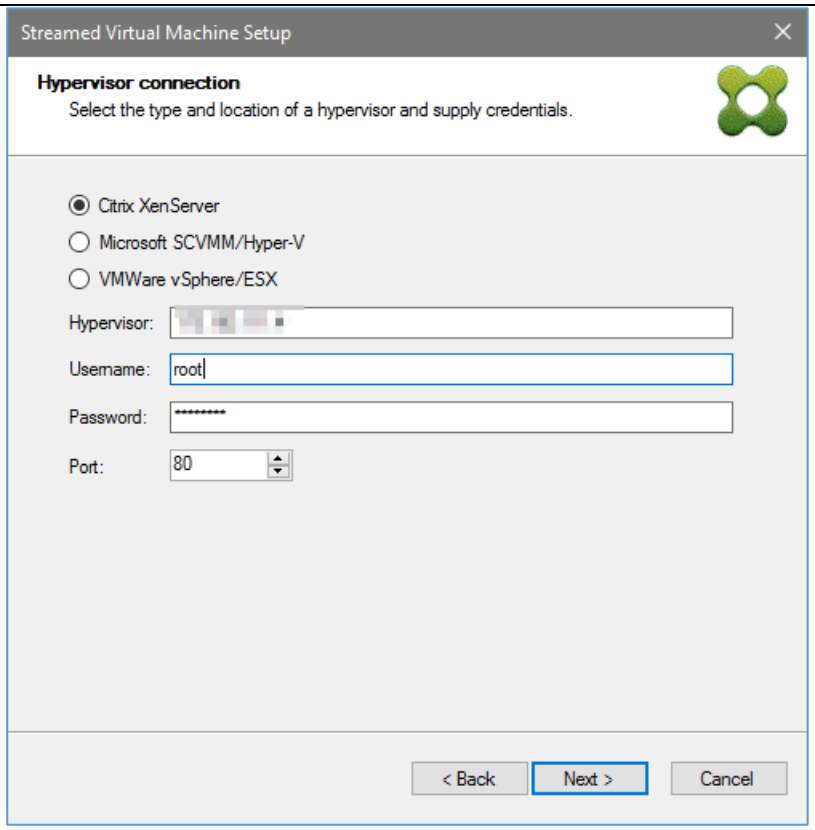
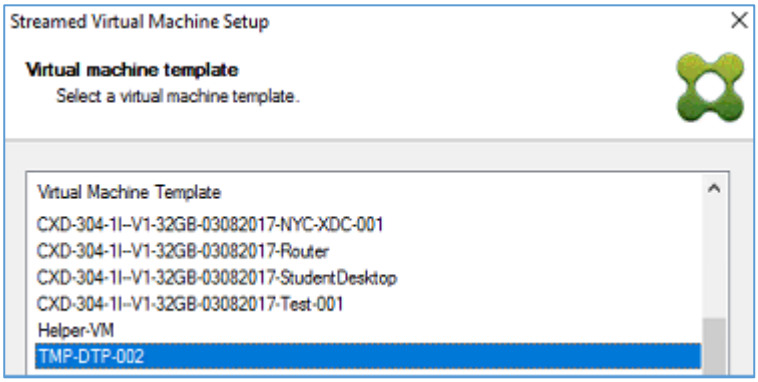
- The BDM partition must be updated whenever changes are made to the bootstrap, for this purpose a centralized update function has been built in to the PVS architecture.

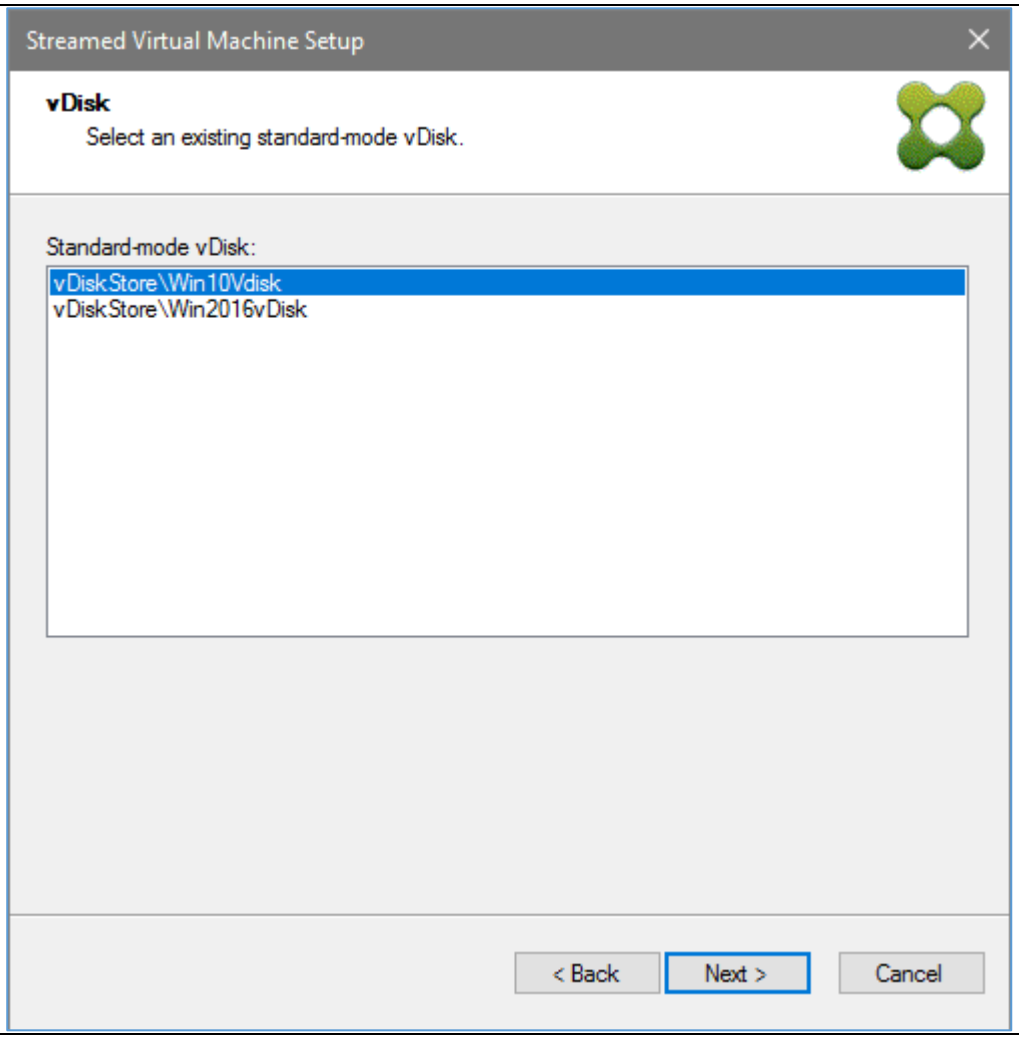
Exercise 19-5: Streamed VM Setup Wizard

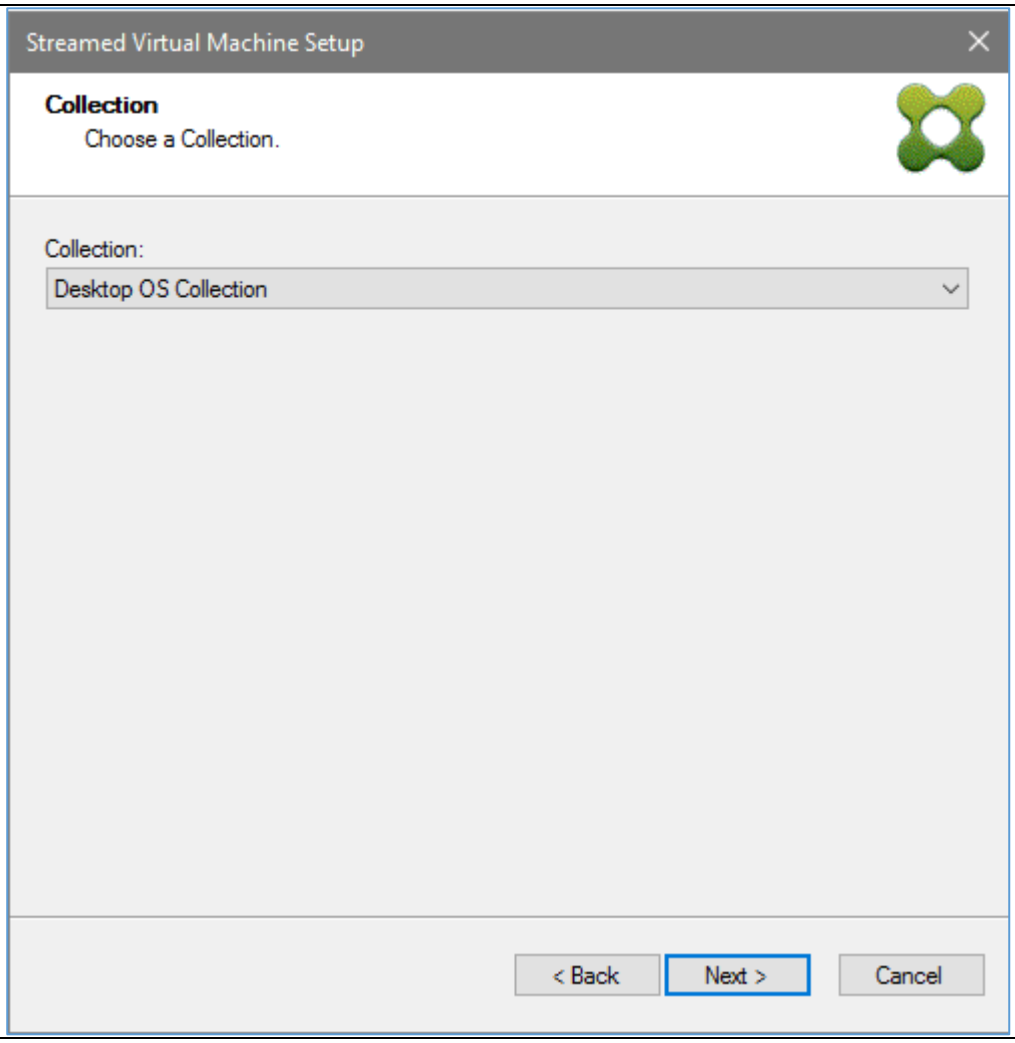
Scenario:

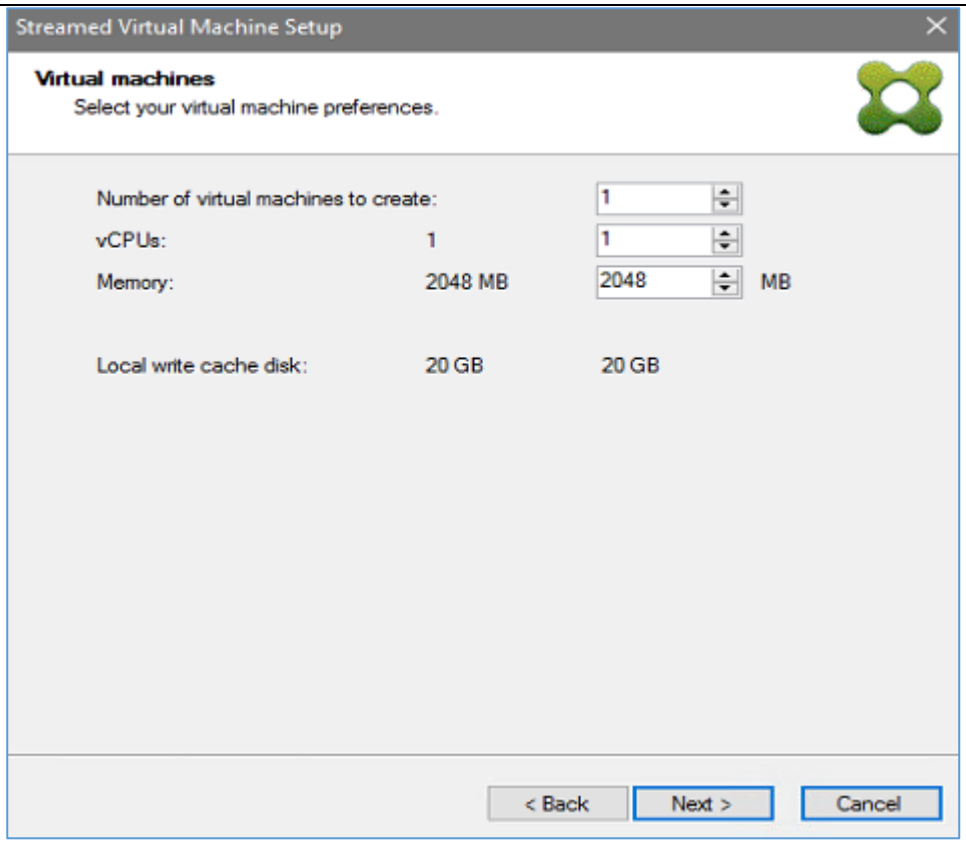
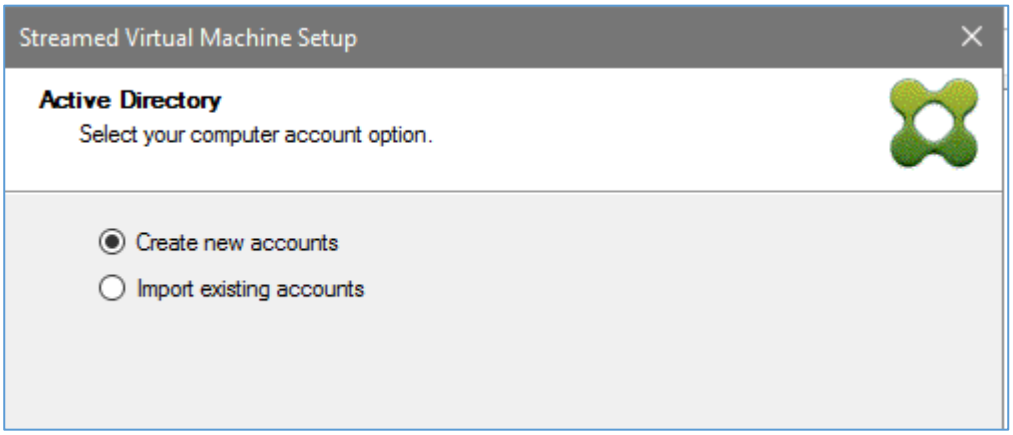
You are a Citrix Administrator at WW Labs, your Lead Citrix Architect has reported that there may be delays getting all necessary prerequisites in the production environment ready for use with the XenDesktop Setup Wizard. Therefore, he has instructed you to test the Steamed VM Wizard, and familiarize yourself with the differences in the two wizards.

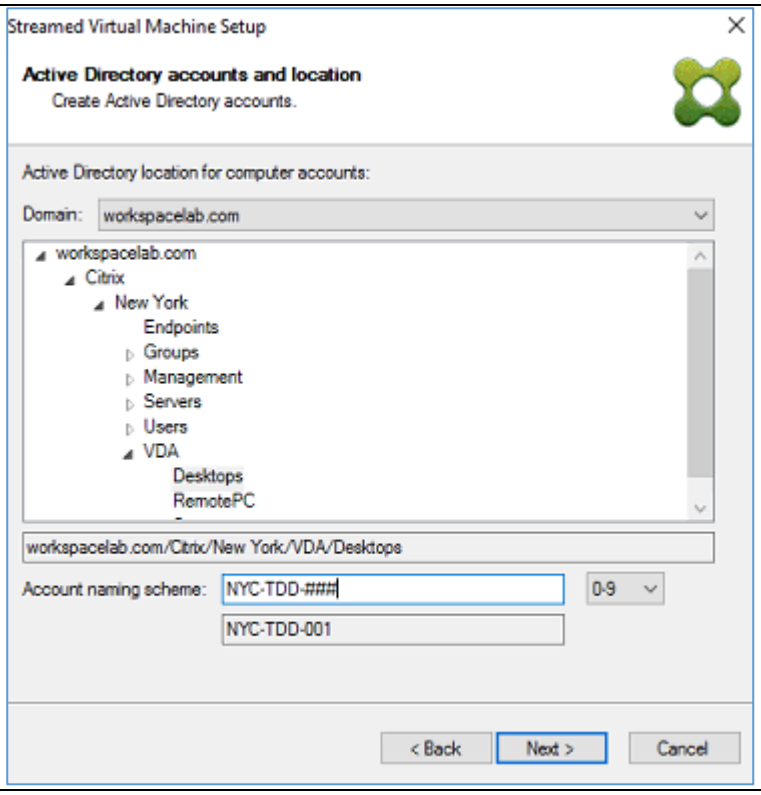
Step	Action
1.	Using the Remote Desktop Connection manager, confirm you are still connected to **NYC-PVS-001**. **Note:** In a previous exercise, you had logged into **NYC-PVS-001** using the following credentials to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the Password. **Note**: If your Remote Desktop Connection session is disconnected, log on to **NYC-PVS-001**, right-click this machine and choose **Connect server**.
2.	Click **Start** and click **Provisioning Services Console**. Type **Localhost** and click **Connect**. **Note:** Ignore this step if the console is already connected from a previous exercise.
3.	Browse **Farm > Sites > NYC-Site**. Right-click **NYC-Site** and select **Streamed VM Setup Wizard**. Click **Next** on the Welcome page.
4.	On **Hypervisor connection** page, select **Citrix XenServer**. Using the hypervisor connection details discovered in exercises 5-3 enter the following information: In the Hypervisor field: **<IP address of the XenServer Host>** Username: **root** Password: **<Password for the XenServer Host>**

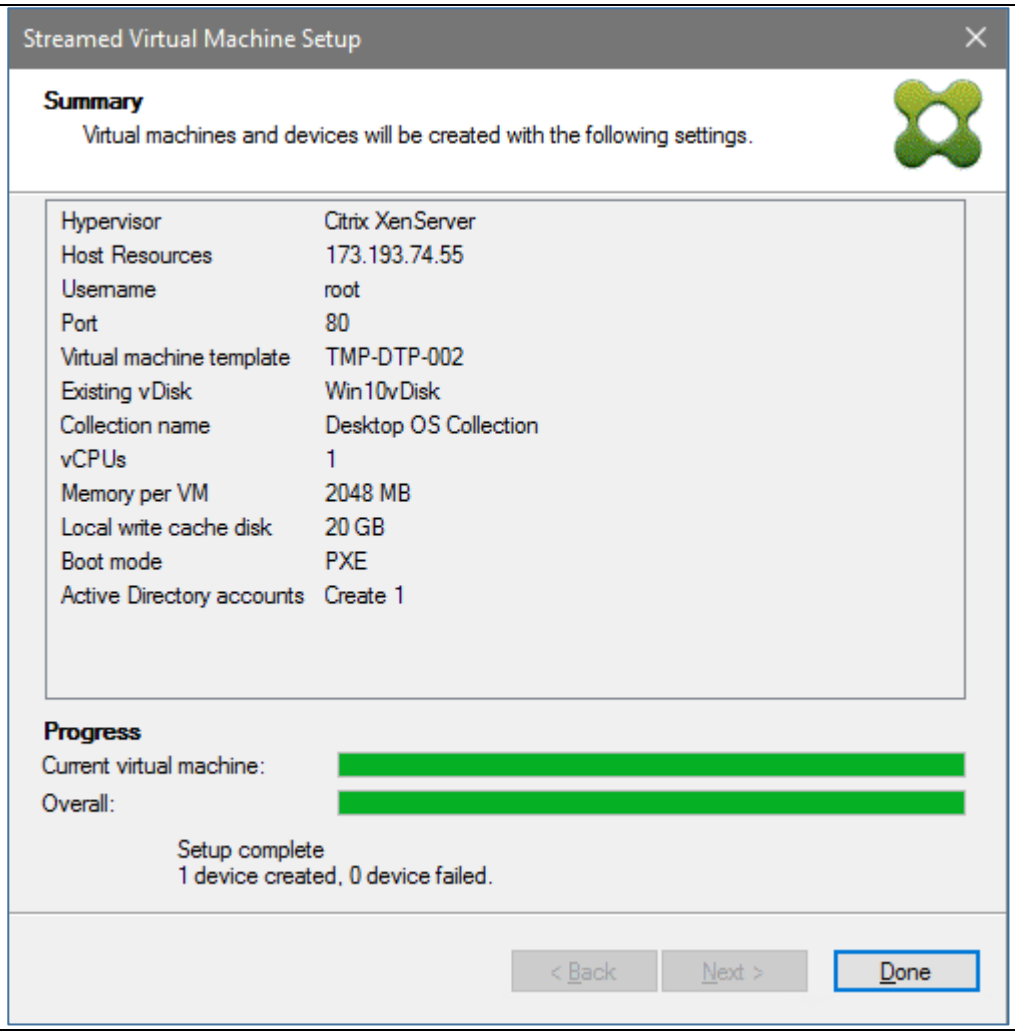
	 Click **Next**.
5.	Select the **TMP-DTP-002** template and click **Next**. 
6	Select **Win10Vdisk** and click **Next**.

	
7	In the Collection drop-down menu, select **Desktop OS Collection**. Click **Next**.

	
8	Verify the details as per below screenshot.

	 Click **Next**. **Note**: A 20 GB disk is manually attached to the template, unlike the XenDesktop Setup Wizard which automatically creates the disk for you.
9	Select **Create new accounts**.  Click **Next**.
10	Browse **workspacelab.com > Citrix > NewYork > VDA > Desktops**. Type **NYC-TDD-###** in the Account naming scheme and click **Next**.

	
11	Verify the Summary and click **Finish**.
12	Click **Done** when the setup completes.

	
13	Browse **Device Collections > Desktop OS Collection** and verify **NYC-TDD-002** is created. **Note:** Refresh the console if the device is not seen.

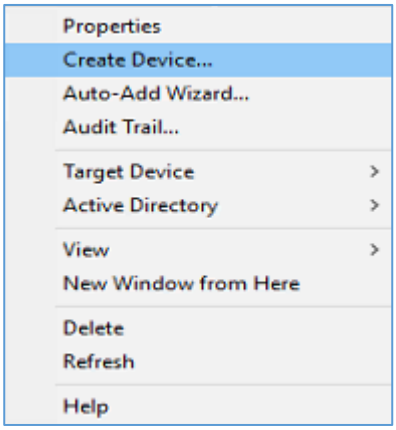
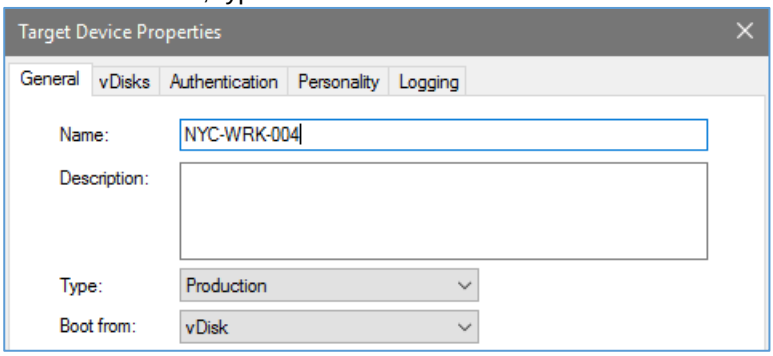
Key Takeaways:

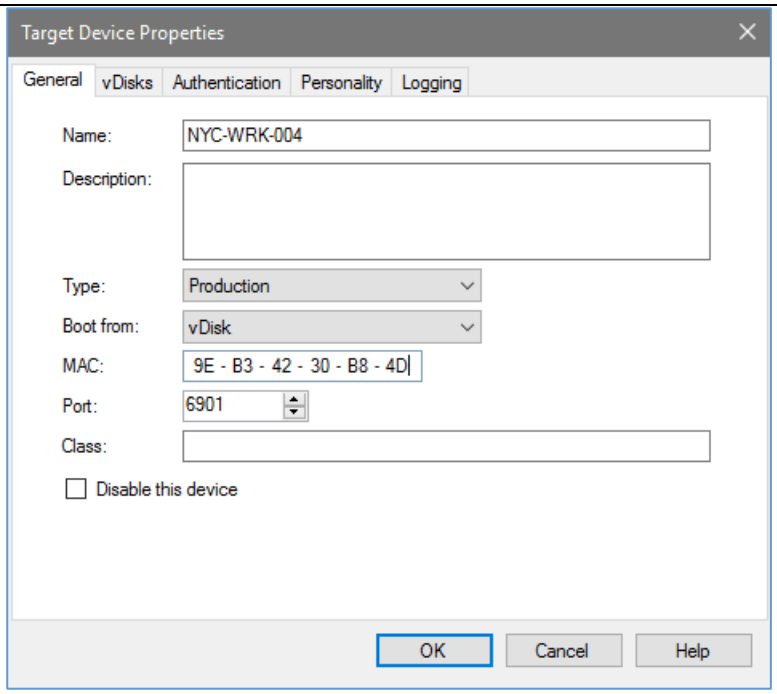
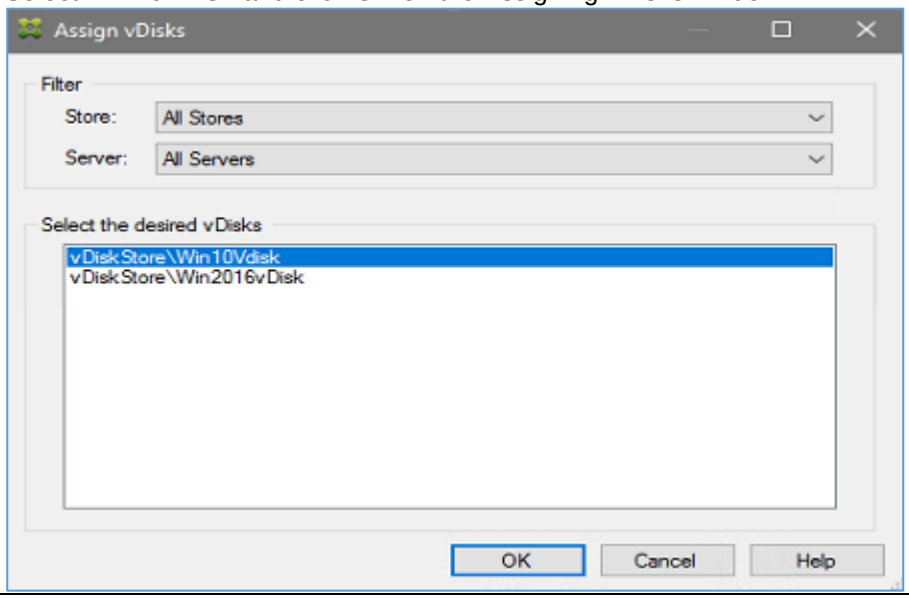
- Target Devices can be added to the PVS Farm manually.
- Each Target Device must have a unique name, MAC address and a vDisk assignment.
- Use the Provisioning Console to add the computer account to Active Directory.

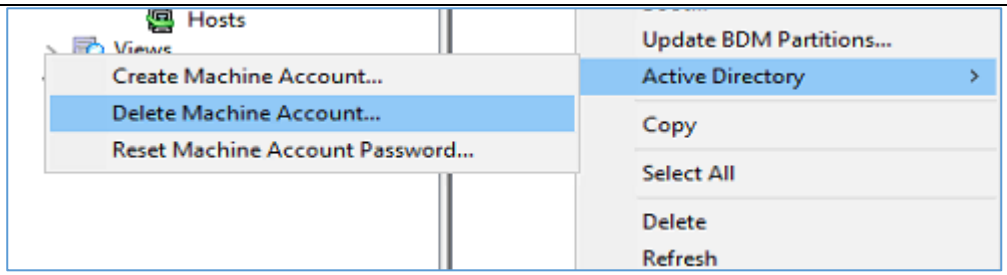
Exercise 19-6: Manually Adding Machines to the Device collection

Scenario:

You are a Citrix Administrator at WW Labs, another team member has previously created a Windows 10 machine for POC testing. Your Lead Citrix Architect has tasked you add this machine to the Windows 10 Device Collection, so it can be used to test and verify vDisk updates.

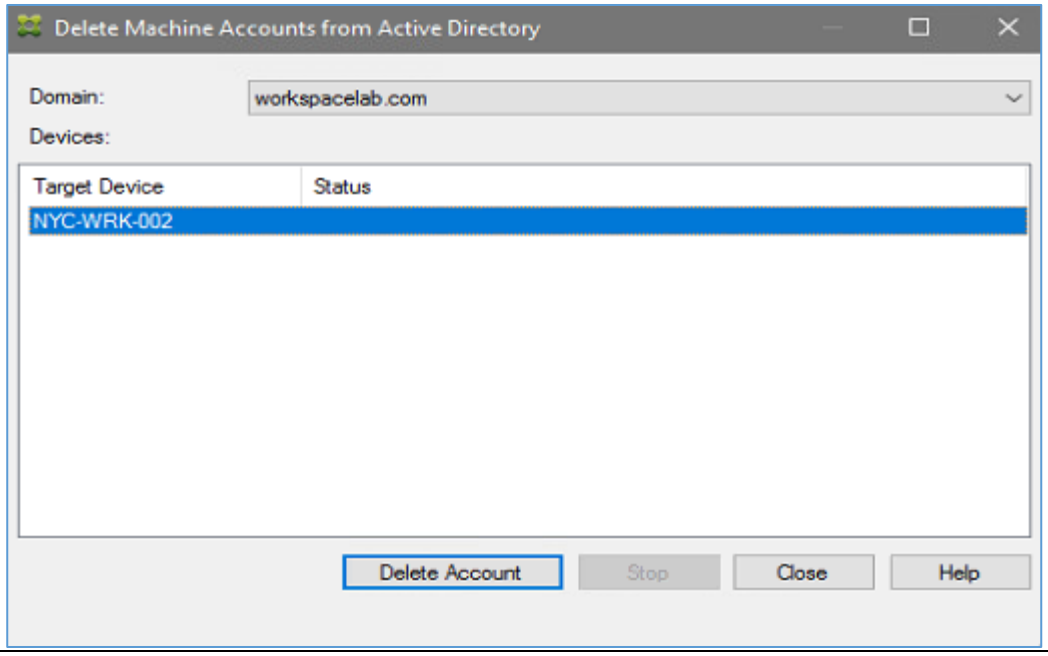
Step	Action
1.	Using the Remote Desktop Connection manager, confirm you are still connected to **NYC-PVS-001**. **Note:** In a previous exercise, you had logged into **NYC-PVS-001** using the following credentials to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the Password. **Note**: If your Remote Desktop Connection session is disconnected, log on to **NYC-PVS-001**, right-click this machine and choose **Connect server**.
2.	Click **Start** and click **Provisioning Services** console. Type **Localhost** and click **Connect**. **Note:** Ignore this step if already connected to the console from a previous exercise.
3.	Browse **Farm > Sites > NYC-Site > Device Collections > Desktop OS collection**.
4.	Right-click **Desktop OS Collection** and select **Create Device**. 
5.	In the Name field, type **NYC-WRK-004**.  **Note:** We already have a Windows 10 machine pre-created on the XenServer host for this lab environment. This machine will be added into an existing device collection this exercise.
6.	Connect to **XenCenter** and select **NYC-WRK-004**.
7.	Select the **Networking** tab in the right pane and note down the MAC address of the machine.
8.	Return back to the PVS console and fill in the MAC address of the device.

	 **Note:** The MAC address in the screenshot will differ with respect to the lab environment.
9.	Select the **vDisks** tab and click **Add**.
10.	Select **Win10vDisk** and click **OK** on the Assigning vDisks window. 
11.	Click **OK**.
12.	Select the **Desktop OS Collection** in the left pane and verify that the **NYC-WRK-004** machine appears in the right pane.
13.	Right-click **NYC-WRK-004** and select **Active Directory > Delete Machine Account**.



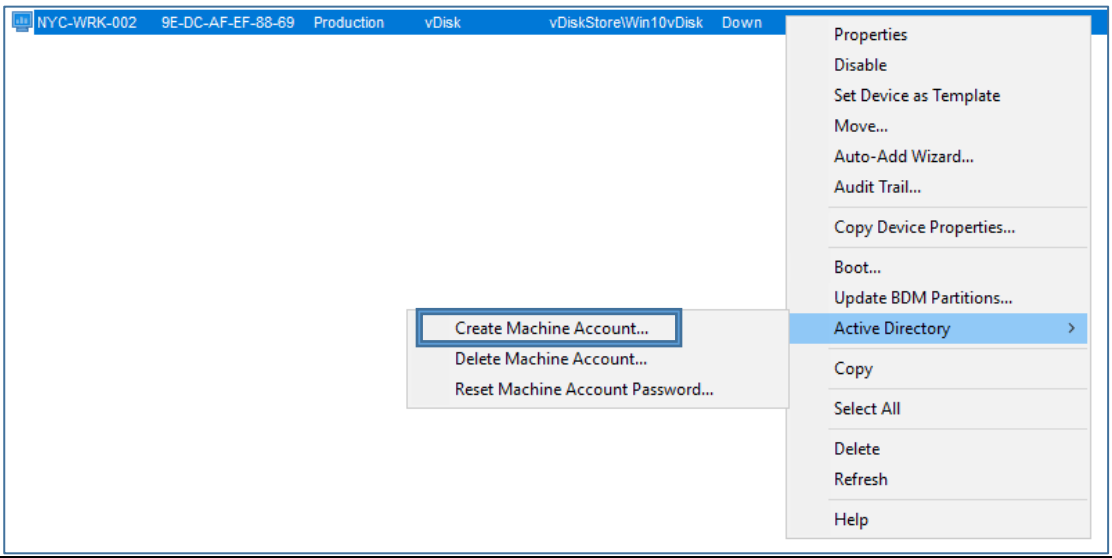
Note: Make sure the **NYC-WRK-004** machine is powered off before implementing this step, otherwise the feature will not function properly.

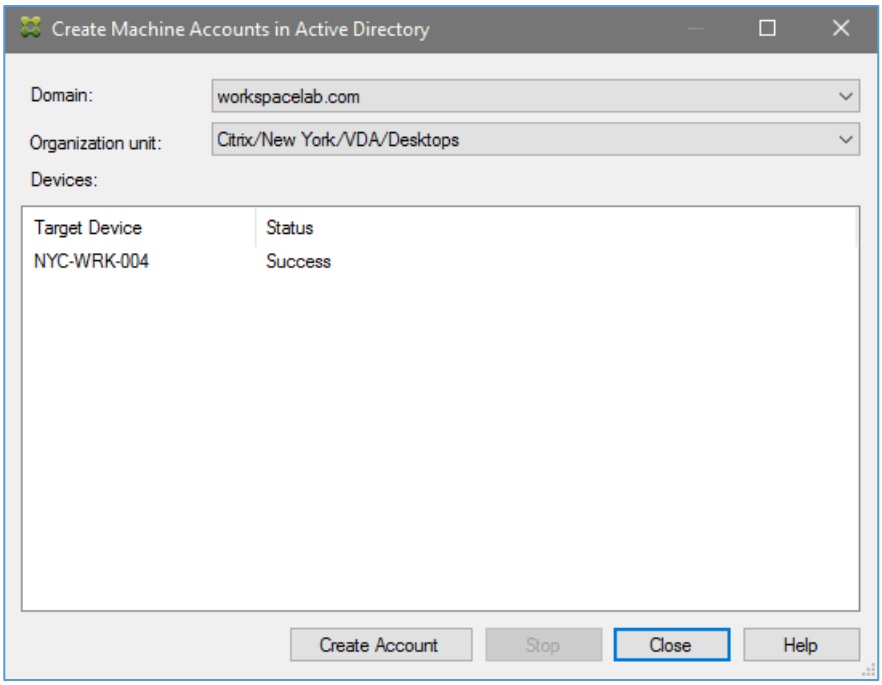
14. Select **NYC-WRK-004** and click **Delete Account**.



15. Click **Close** once the Status column shows **Success**.

16. Right-click **NYC-WRK-004** again and select **Active Directory > Create Machine Account**.



17.	Select **Citrix > New York > VDA > Desktops** as the Organizational Unit.
18.	Select **NYC-WRK-004** and click **Create Account**.  **Note:** Creating a machine account from Provisioning Services will create a machine account for the target device in Active Directory that will be managed by Provisioning Services instead of the Domain Controller.
19.	Verify that the Status shows **Success** and click **Close**.

Key Takeaways:

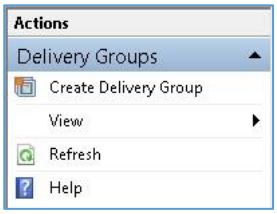
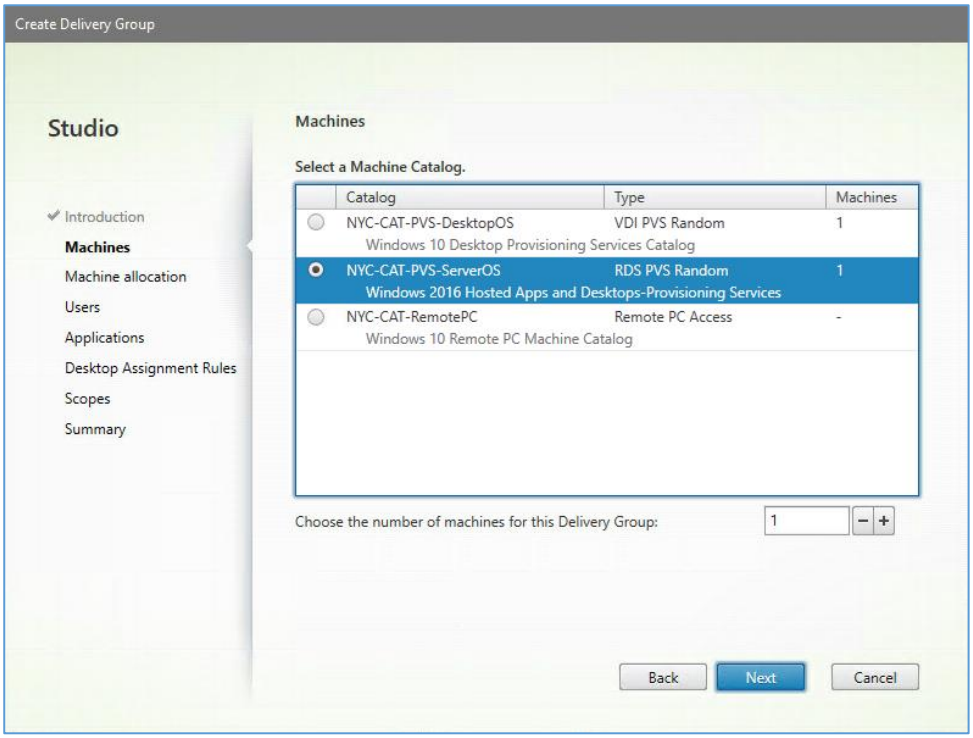
- The XenDesktop Setup Wizard will only create the Machine Catalogs; Delivery Groups must be created manually using Citrix Studio.
- The Server OS based Delivery Group publishes Microsoft Office to domain users.

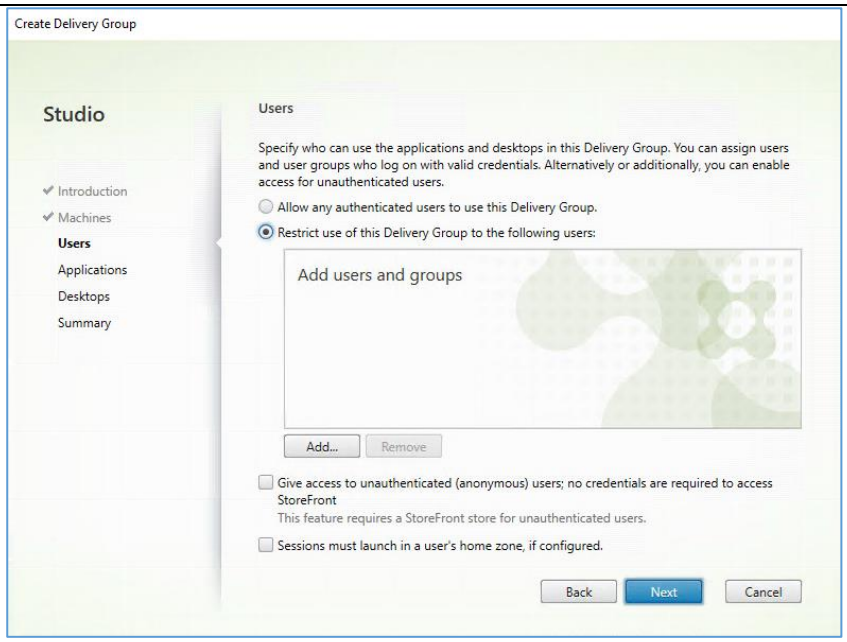
Exercise 19-7: Create a Delivery Group for Server OS

Scenario:

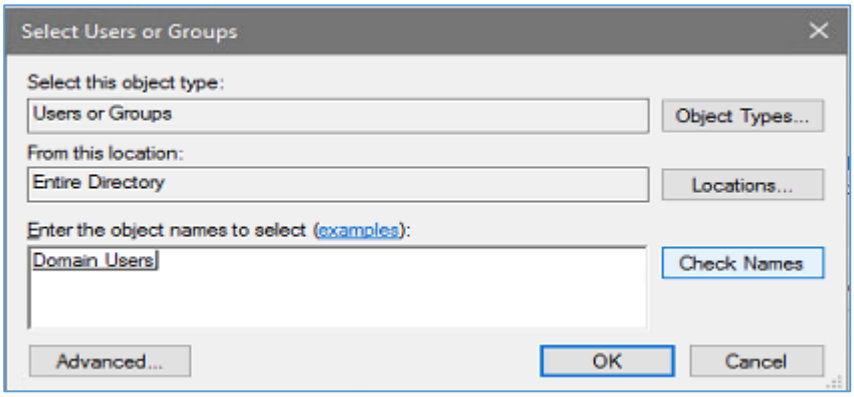
You are a Citrix Administrator at WW Labs, your Lead Citrix Architect has instructed you to create a new Delivery Group in Citrix Studio for testing purposes. Your task is to ensure that domain users has access to launch the Microsoft Office Publisher application from the Server OS machines.

Step	Action
1.	Using the Remote Desktop Connection manager, confirm you are still connected to **NYC-XDC-001**. **Note:** In a previous exercise, you had logged into **NYC-XDC-001** using the following credentials to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the Password. **Note**: If your Remote Desktop Connection session is disconnected, log on to **NYC-XDC-001**, right-click this machine and choose **Connect server**.
2.	Using Studio, expand **Citrix Studio (NYC)** and click **Delivery Groups**.

	On the right pane, click **Create Delivery Group**.  **Note**: Studio was launched in a previous exercise. If Studio was closed, then click **Start > Citrix > Citrix Studio**. **Note:** Click **Cancel** on End Snap-in window if prompted.
3.	On the Introduction page, click **Next** to continue the Delivery Group creation wizard. **Note:** Delivery Groups are collections of desktops and applications that are created from Machine Catalogs. Create Delivery Groups for specific teams, departments, or types of users, and base them on either a desktop or a server operating system. Make sure you have enough machines available in a suitable Catalog to create the Delivery Groups you need.
4.	On the Machines page, verify that the previously created Machine Catalogs are listed. Select the **NYC-CAT-PVS-ServerOS** Catalog. In the number of machines for this Delivery Group field, set the value to **1**.  Click **Next** to continue the Delivery Group creation wizard.
5.	On the Users page, select the **Restrict use of this Delivery Group to the following users:** Click the **Add** button under the Add users and group's box.



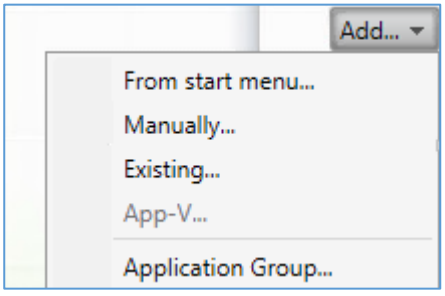
In the Select Users or Groups dialog box that appears, enter **Domain Users**.



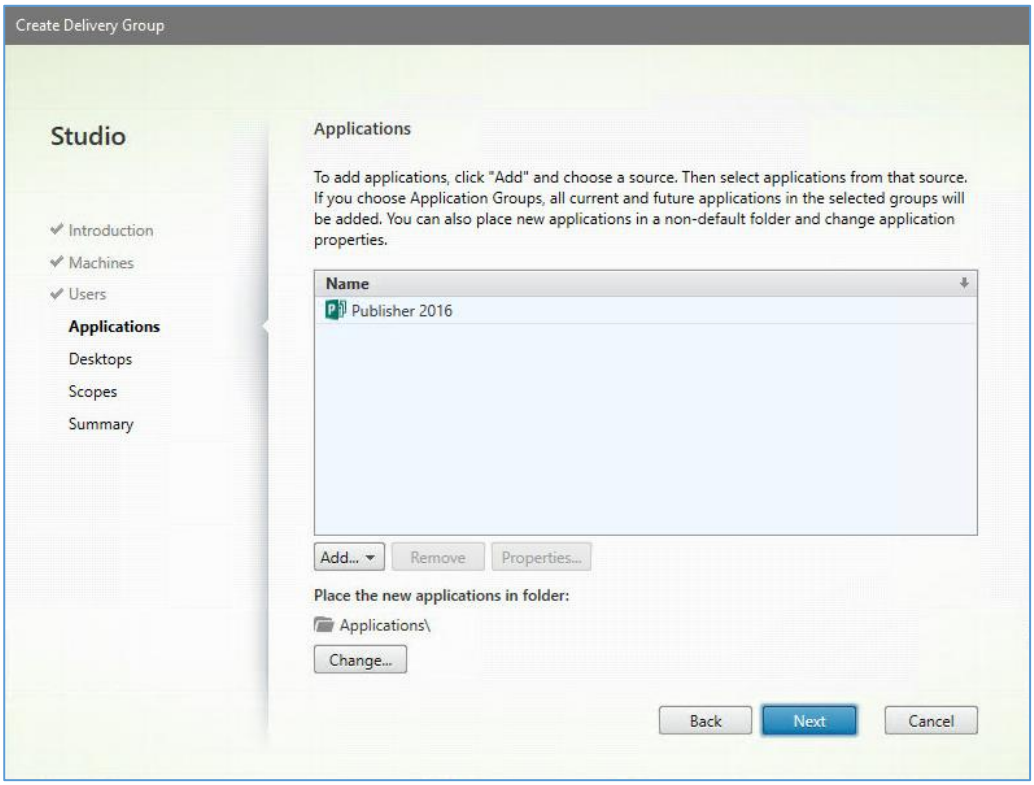
Click on the **Check Names** button and click **OK**.

Click **Next**.

6. On the Applications page, click on **Add** and select **From start menu**.



The wizard will begin the process of discovering applications found on **NYC-TDS-001**.

	Click the checkbox next to the following application: • Publisher 2016 Click **OK**. Click **Next** to continue the Delivery Group creation wizard.  **Note:** The applications can take a while to populate, because the NYC-TDS-001 machine may have been powered off in previous exercises to save on resource consumption. In order to return a list of the applications installed, the Delivery Controller has to call to the hypervisor hosting NYC-TDS-001 and have it powered on. Once powered on, the VDA will register with the Controller and send a list of installed applications to publish. **Note**: If this application list does not appear after five minutes, use XenCenter to verify that NYC-TDS-001 is powered on. **Note**: You can also add (create) applications manually, by providing the path to the executable, working directory, any optional command-line arguments and specifying a display name visible to users in Receiver and administrators in Studio.
7.	Click **Next** on the **Desktops** page.
8.	Click **Next** on the **Scopes** page.
9.	On the **Summary** page, verify the previously configured information and enter the following: • Delivery Group name: **NYC-DG-PVS-ServerOSApps** • Delivery Group description, used as label in Receiver (optional): **Windows 2016-Apps-Provisioning Services provisioned**. Click **Finish**.
10.	Verify that the **NYC-DG-PVS-ServerOSApps** Delivery Group is created in the console.

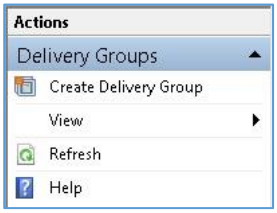
Key Takeaways:

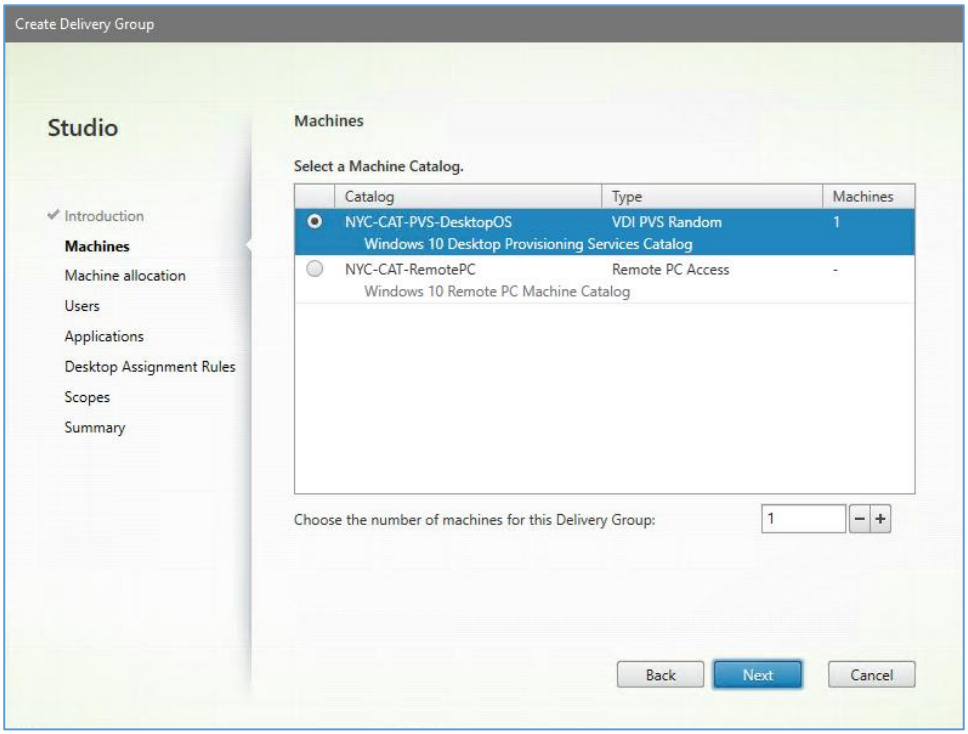
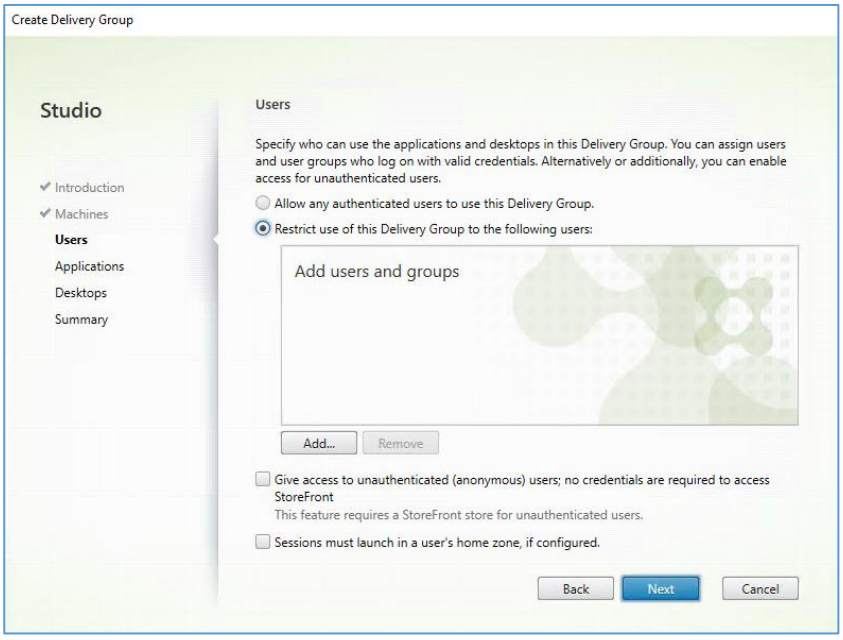
- The XenDesktop Setup Wizard will only create the Machine Catalogs; Delivery Groups must be created manually using Citrix Studio.
- The Server OS Application based Delivery Group publishes Applications from a Sever 2016 OS to domain users.
- The Servers provided in this Delivery Group are set to be shared between the configured users and will lose every change on reboot.

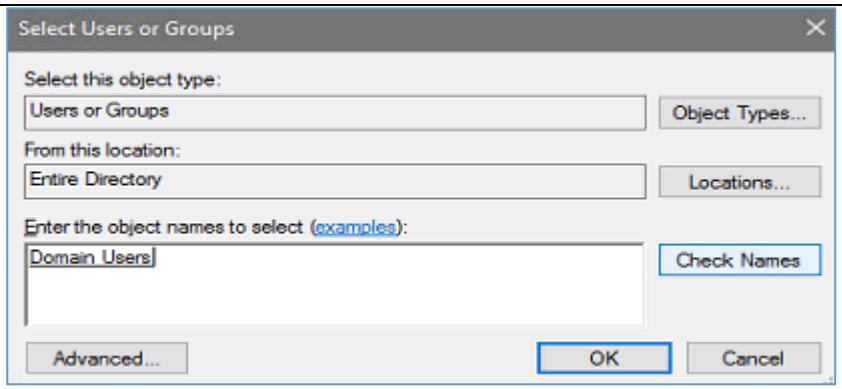
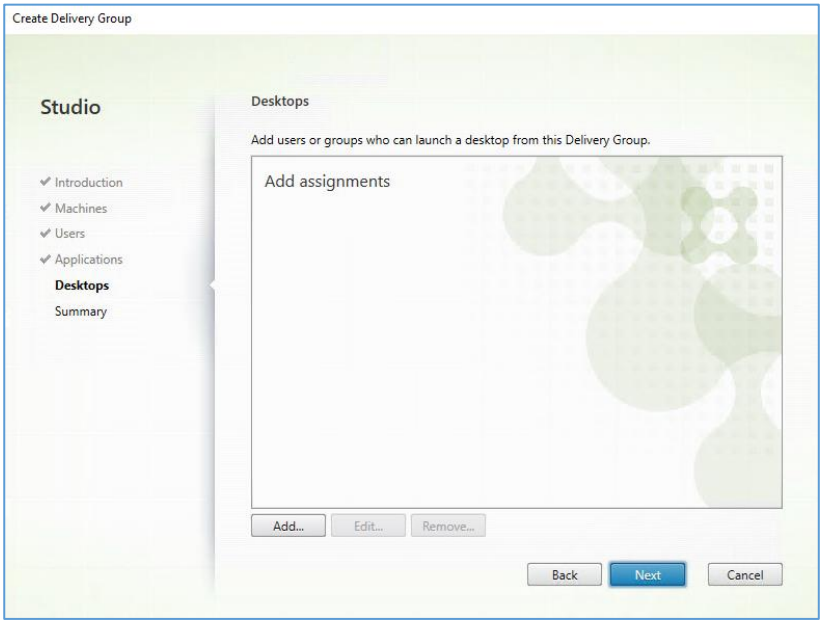
Exercise 19-8: Create a Delivery Group for Desktop OS

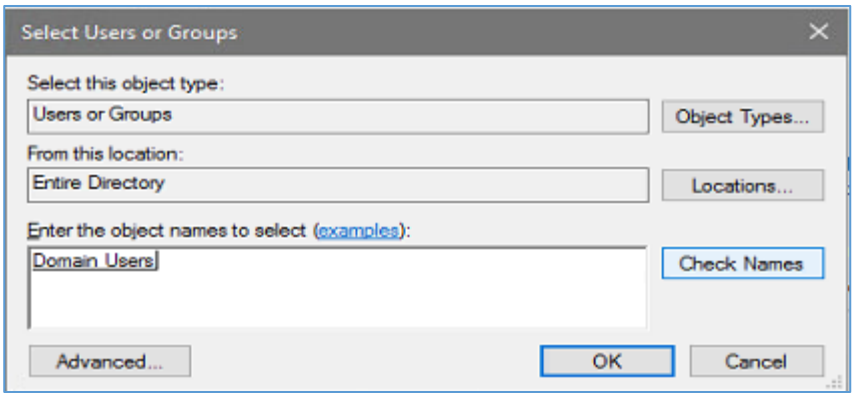
Scenario:

You are a Citrix Administrator at WW Labs, your Lead Citrix Architect has instructed you to create an additional Delivery Group in Citrix Studio for testing purposes. Your task is to ensure that domain users has access to launch s Windows 10 Desktop from the Desktop OS machines.

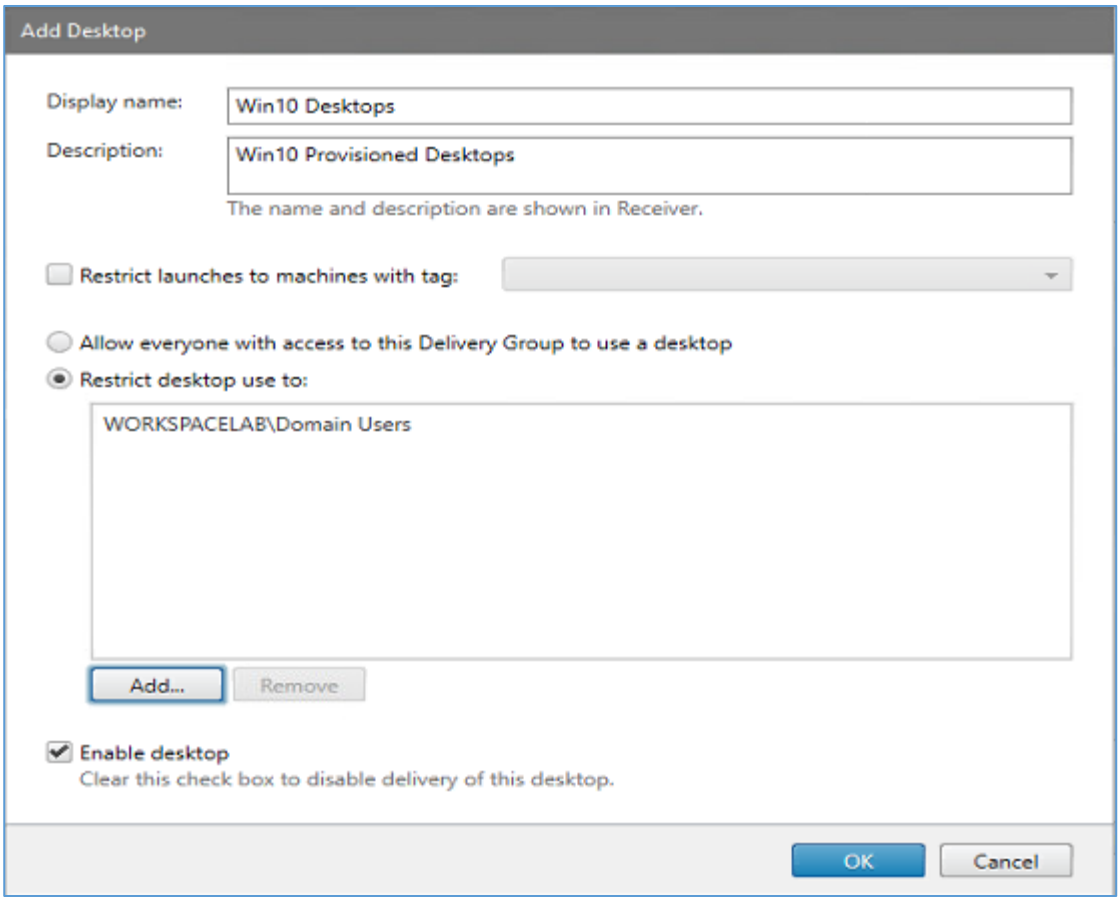
Step	Action
1.	Using the Remote Desktop Connection manager, confirm you are still connected to **NYC-XDC-001**. **Note:** In a previous exercise, you had logged into **NYC-XDC-001** using the following credentials to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the Password. **Note**: If your Remote Desktop Connection session is disconnected, log on to **NYC-XDC-001**, right-click this machine and choose **Connect server**.
2.	Using Studio, expand **Citrix Studio (NYC)** and click **Delivery Groups**. On the right pane, click **Create Delivery Group**.  **Note**: Studio was launched in a previous exercise. If Studio was closed, then click **Start > Citrix > Citrix Studio**.
3.	On the Introduction page, click **Next** to continue the Delivery Group creation wizard. **Note:** Delivery Groups are collections of desktops and applications that created from Machine Catalogs. Create Delivery Groups for specific teams, departments, or types of users, and base them on either a desktop or a server operation system. Make sure you have enough machines available in a suitable Catalog to create the Delivery Groups you need.
4.	On the Machines page, verify that the previously created Machine Catalogs are listed. Select **NYC-CAT-PVS-DesktopOS** Catalog.

	In the number of machines for this Delivery Group field, set the value to **1**.  Click **Next** to continue with the Delivery Group creation wizard.
5.	On the Users page, select **Restrict use of this Delivery Group to the following users:** click the **Add** button under the Add users and groups box.  In the Select Users or Groups dialog box that appears, enter **Domain Users**.

	 Click on the **Check Names** button and click **OK**. Click **Next**.
6.	On the Applications page, click **Next**.
7.	On the Desktops page, click **Add**.  On Add Desktop page, type the following information: Display Name: **Win10 Desktops** Description: **Win10 Provisioned Desktops for Domain Users** Select **Restrict desktop use to:** and click **Add**. On the Select Users or Groups window, type **Domain Users**.

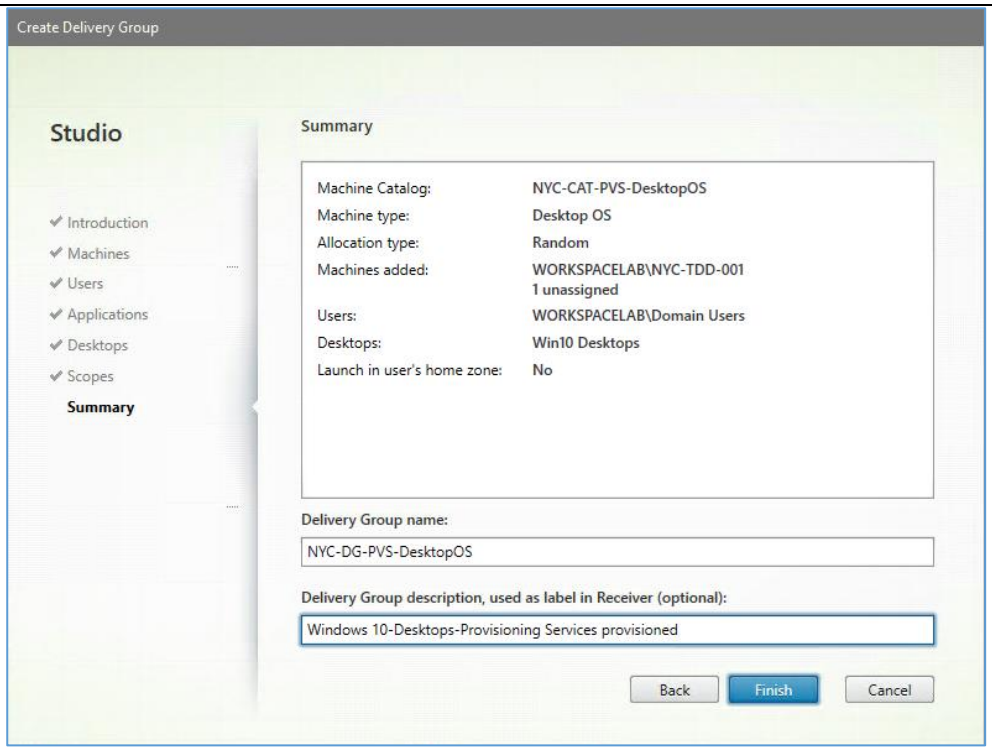


Click the **Check Names** button and click **OK**.



Click **OK** and click **Next**.

8.	On the **Scopes** page click **Next**.
9.	On the Summary page, verify the previously configured information and enter the following: • Delivery Group name: **NYC-DG-PVS-DesktopOS** • Delivery Group description, used as label in Receiver (optional): **Windows 10-Desktops-Provisioning Services provisioned** Click **Finish**.

	
10.	Verify that the **NYC-DG-PVS-DesktopOS** Delivery Group is created in the console.
11.	Close the **Studio**.

Key Takeaways:

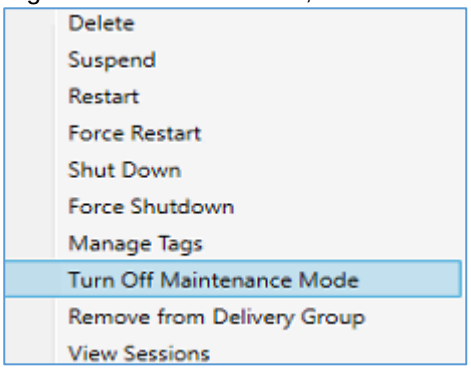
- The XenDesktop Setup Wizard will only create the Machine Catalogs; Delivery Groups must be created manually using Citrix Studio.
- The Desktop OS based Delivery Group publishes a Windows 10 Desktop to domain users.
- The desktops provided in this Delivery Group are set to be shared between the configured users and will lose every change on reboot; this option is referred to as Random non-persistent desktops.
- Other Deliver Group options include: Static non-persistent desktop and Static persistent, where users will receive the same desktop at each logon, changes will either be discarded or saved during reboot.

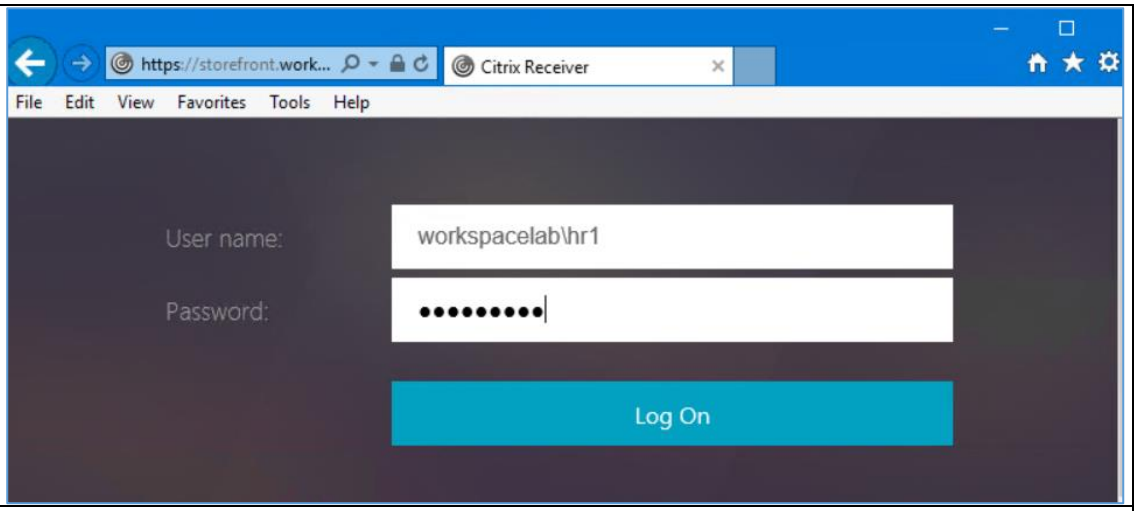
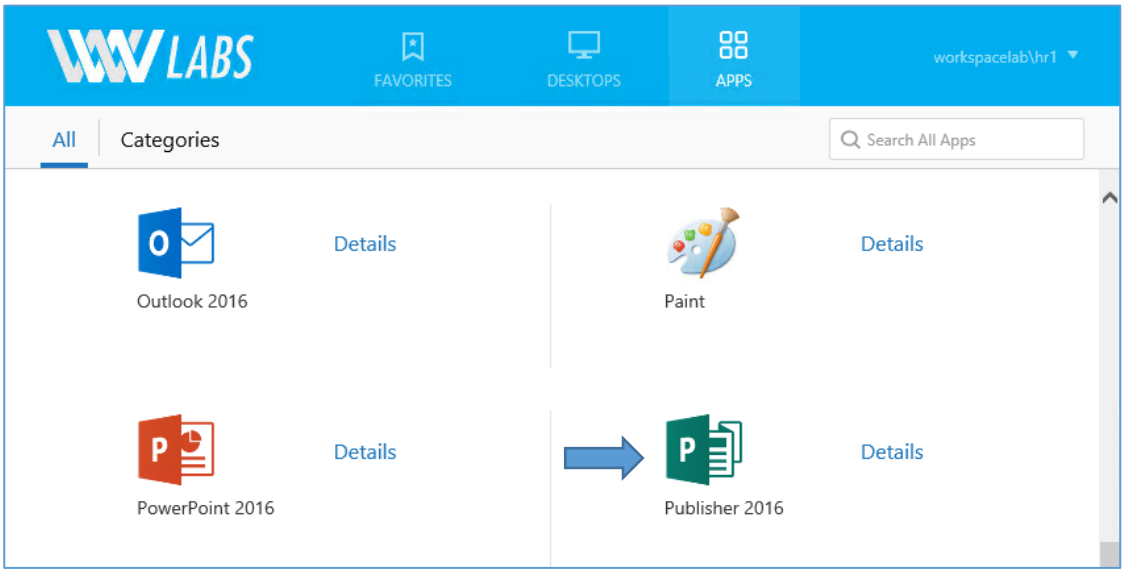
Exercise 19-9: Launch Published Application and Desktop

Scenario:

You are a Citrix Administrator at WW Labs, your Lead Citrix Architect has invited the CTO in for a demo of the POC environment. You task is to prove that you can now launch a HDX session running on a machine provisioned by Citrix Provisioning Services.

Step	Action
1.	Using the Remote Desktop Connection manager, connect to **NYC-XDC-001**. To login to NYC-XDC-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the Password.

2.	Click **Start** and click **Citrix Studio**. **Note:** Click **Cancel** on End Snap-in window if prompted.
3.	Click on **Machine Catalogs** in the left pane. Double-click **NYC-CAT-PVS-DesktopOS**.
4.	Right-click **NYC-TDD-001**, click **Turn Off Maintenance Mode** and click **Yes** to confirm.  **Note:** We would not be able to launch a desktop when maintenance mode is on.
5.	Connect to XenCenter and verify that **NYC-TDS-001** and **NYC-TDD-001** are powered on. If not, start both the machines and monitor them from XenCenter until they are up.
6.	Using the Remote Desktop Connection Manager, connect to NYC-WRK-001. To log on to NYC-WRK-001, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: • User name: Workspacelab\HR1 • Password: Password1
7.	Launch **Internet Explorer** and navigate to **https://storefront.workspacelab.com/Citrix/WWLabsStoreWeb/**. **Note:** Select the Switch to user name and password option if the log on window does not come directly.
8.	Log on using the following credentials: User name: **workspacelab\hr1** Password: **Password1**

	
9.	Click the **DESKTOPS** tab and launch the **Windows 10 desktop**. Verify that the desktop starts.
10.	From the Internet Explorer window that Win10 Desktops was launched from, click the **APPS** tab and launch **Publisher 2016**.  Interact with the desktop and the application sessions. When finished, close both sessions.
11.	Log off **Receiver for Web**.

	Click **WORKSPACELAB\hr1** and choose **Log Off**. Close the **Internet Explorer**.
12.	Connect to **NYC-XDC-001** using Remote Desktop Connection Manager.
13.	Click **Start** and click **Citrix Studio**. **Note**: Ignore if Studio is already open.
14.	Click on **Machine Catalogs** in left pane. Double-click **NYC-CAT-PVS-DesktopOS**.
15.	Right-click **NYC-TDD-001.workspacelab.com**, select **Turn On Maintenance Mode** and click **Yes** to confirm.
16.	Connect to XenCenter and shut down both **NYC-TDD-001** and **NYC-TDS-001**.

Key Takeaways:

- Users are able to launch virtual desktop sessions hosted on a Desktop OS VDA and published applications hosted on a Server OS VDA.
- Users cannot launch desktops or applications if the VDA machine is in Maintenance mode.

Module 20-1: Advanced Architecture

Overview:

This module presents the methods used to add redundancy to some of the core components in the Provisioning Services environment. To reinforce this, a second Provisioning Server will be installed and added to the existing Provisioning Services Farm. Additionally, the vDisk Store and TFTP service will be configured for redundancy.

Before you begin:

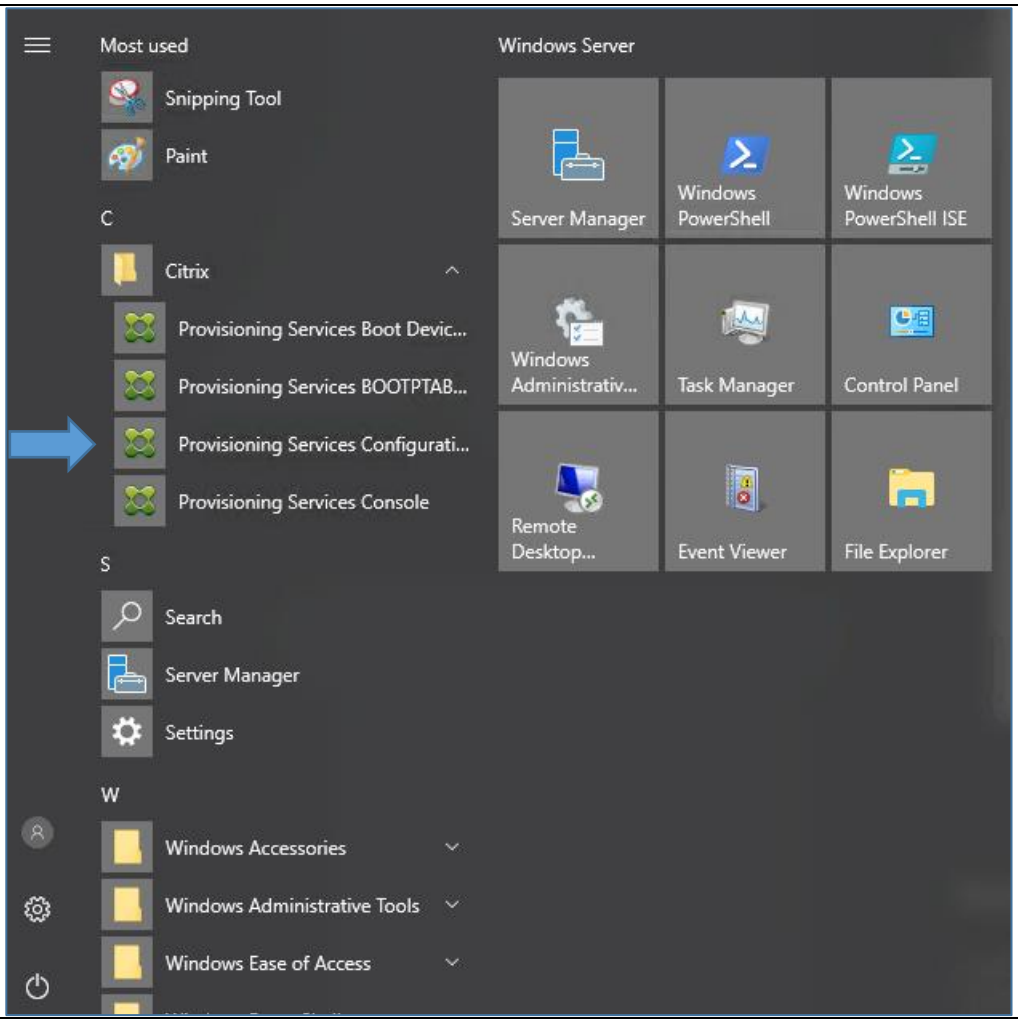
Estimated time to complete Module 20 lab exercises: 35 minutes.

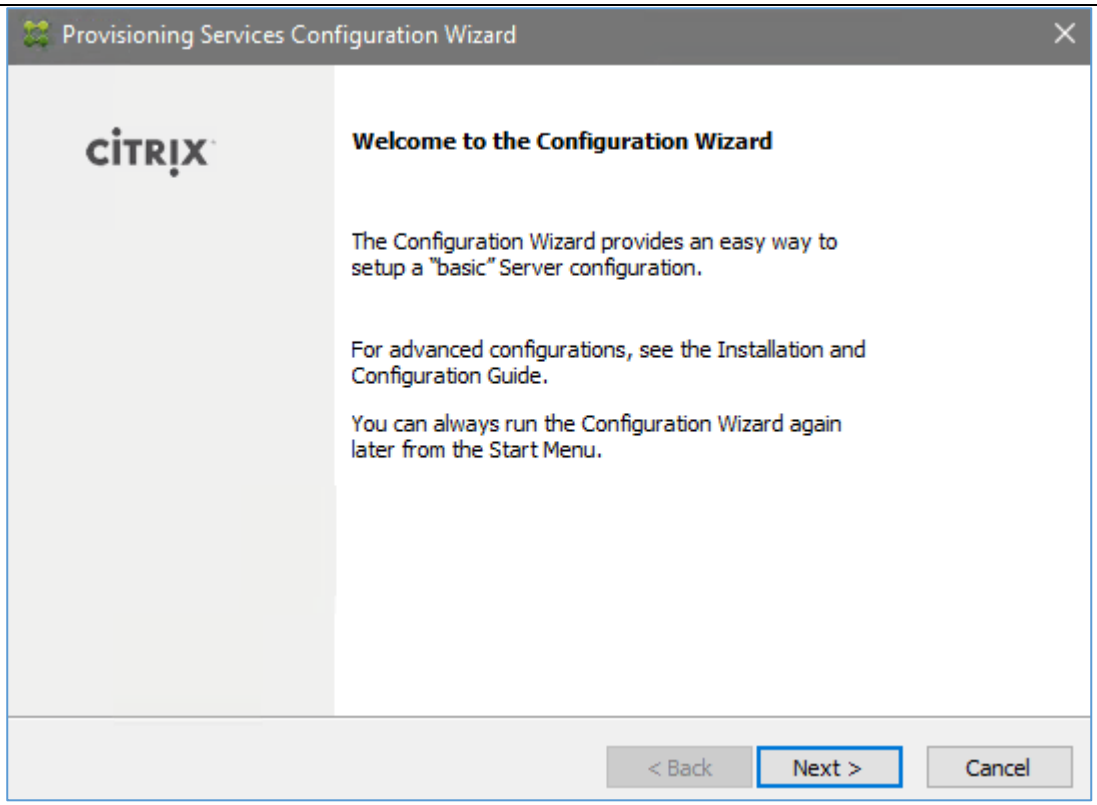
Exercise 20-1: Join Second PVS server to the Farm

Scenario:

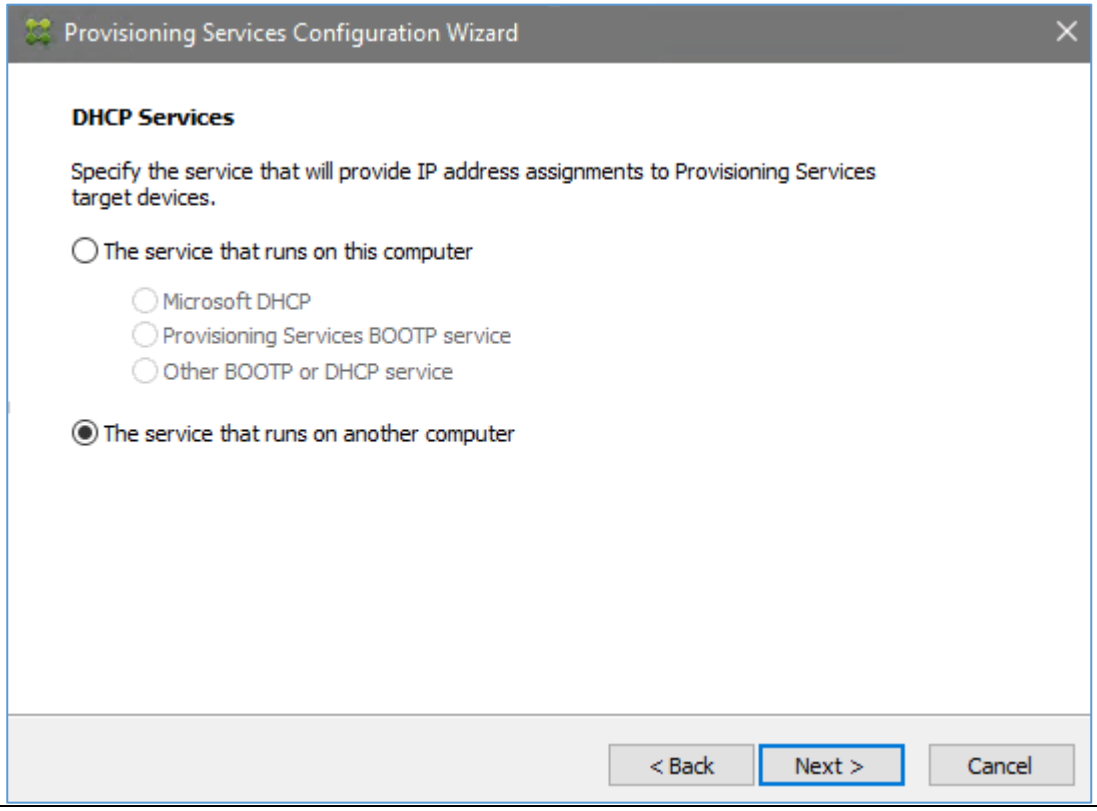
You are a Citrix Administrator at WW Labs, your Lead Citrix Architect has tasked you with joining a Provisioning Services Server to an existing farm.

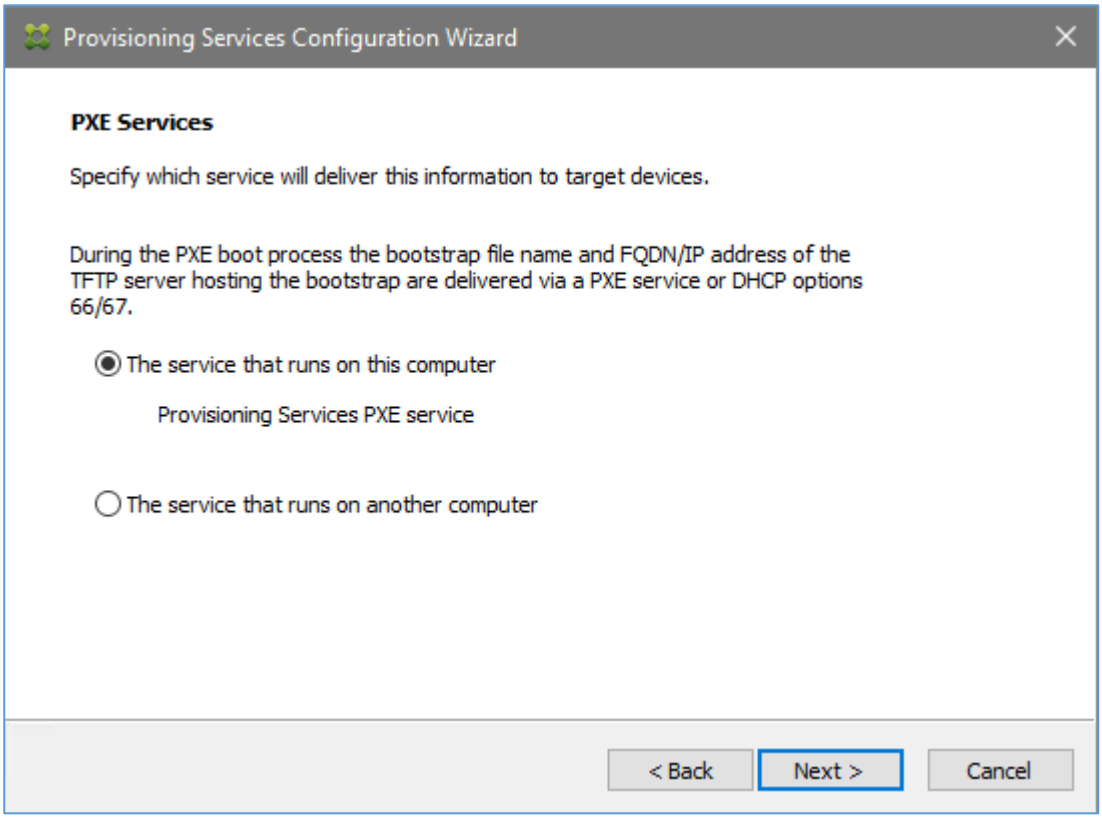
Step	Action
1.	The following VMs are required before beginning the exercises for this Module; all others may be powered down. To power manage your VMs, switch to XenCenter, right-click on the VM in the left pane and select Start or Shut Down. If prompted click Yes. • NYC-ADS-001 • NYC-SQL-001 • NYC-FSR-001 • NYC-PVS-001 • NYC-PVS-002 • NYC-VNS-001 **Note**: These above VMs are listed in the start-up order.
2.	Using the Remote Desktop Connection manager, connect to **NYC-PVS-002**. To login to **NYC-PVS-002**, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection User name: **WORKSPACELAB\Administrator** with **Password1** as the Password.
3.	Click **Start** and select **Provisioning Services Configuration Wizard**.

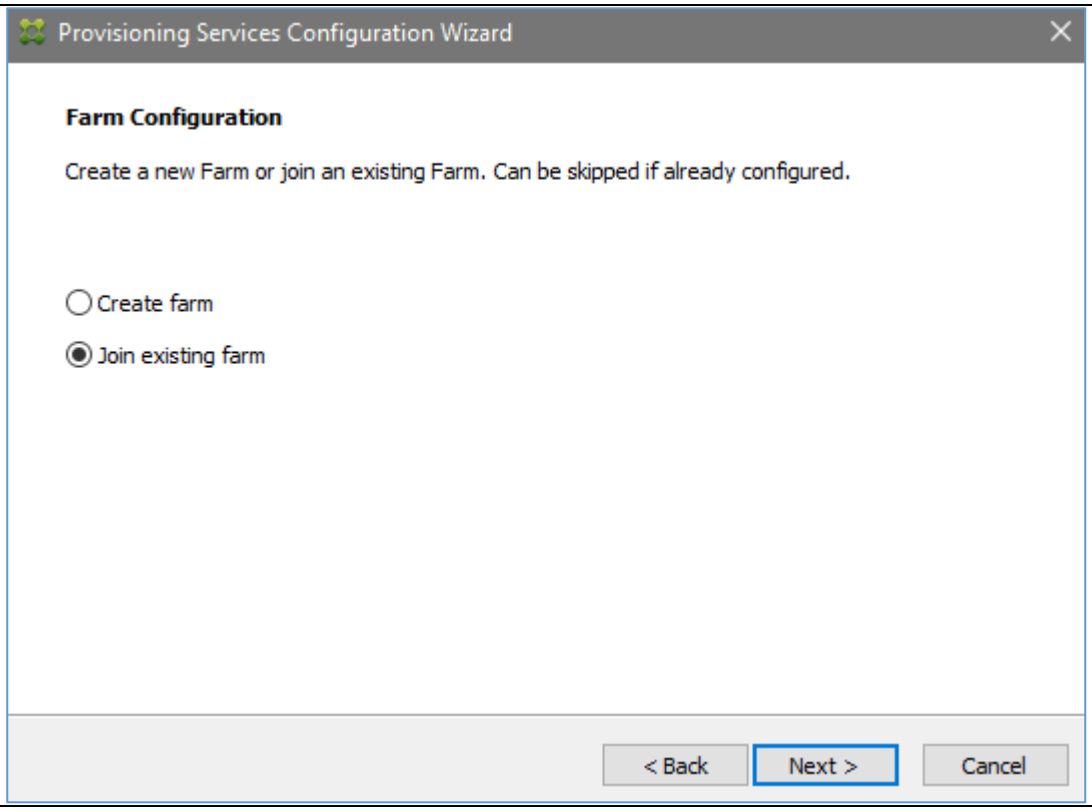
	
4.	Click **Next** in the **Provisioning Services Configuration Wizard** welcome screen.



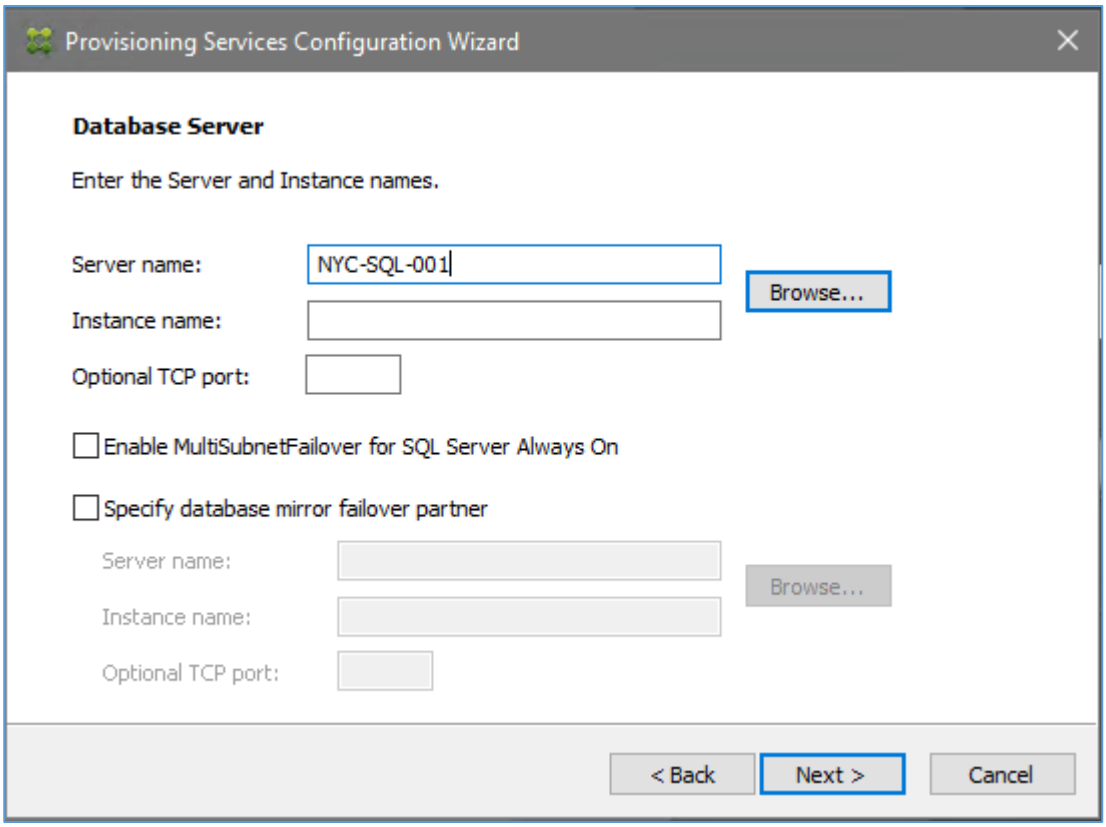
5. On the **DHCP Services** screen, select **The service that runs on another computer** and then click **Next**.

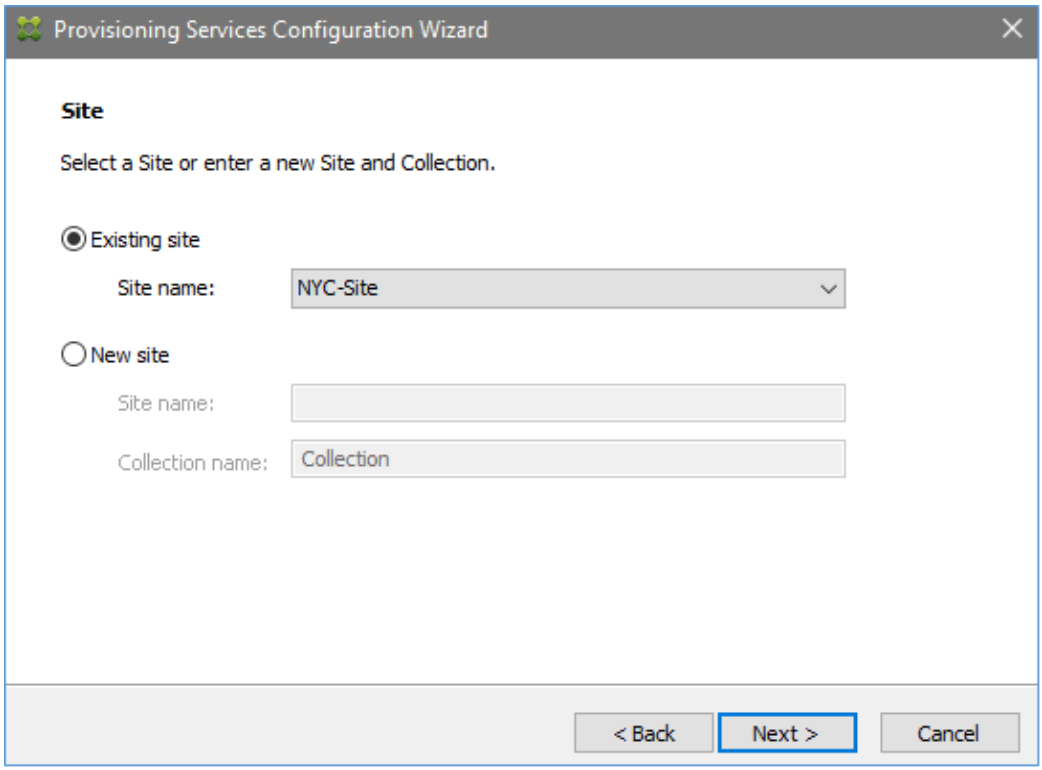


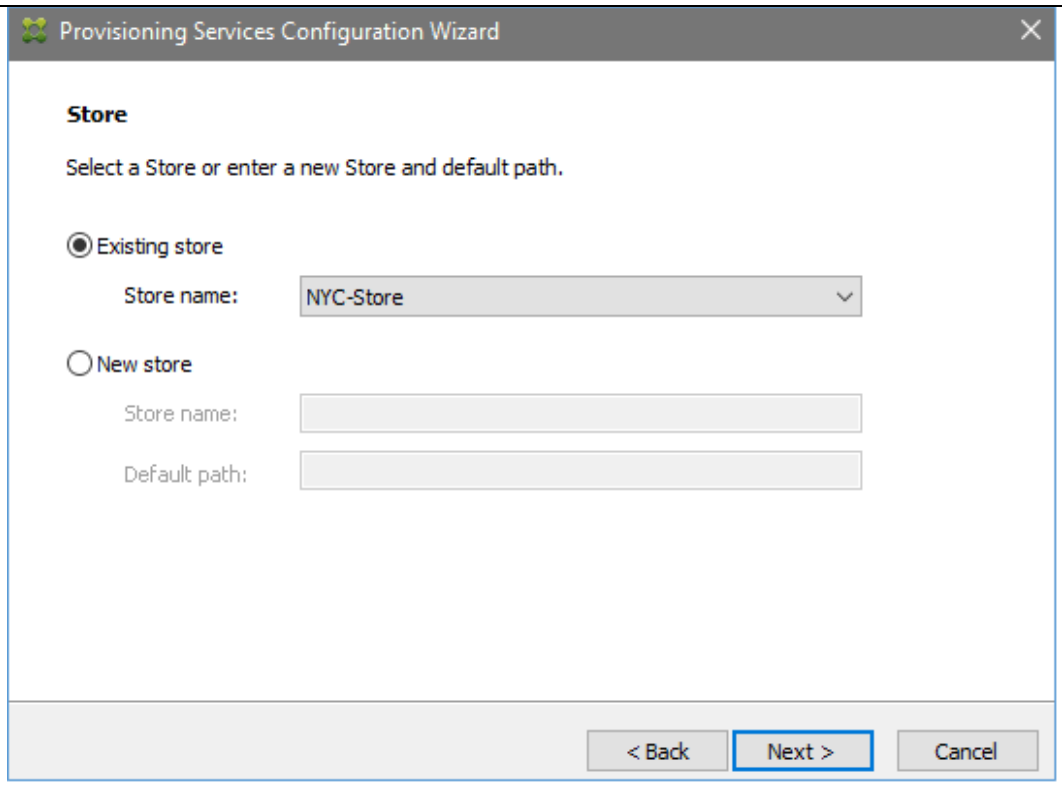
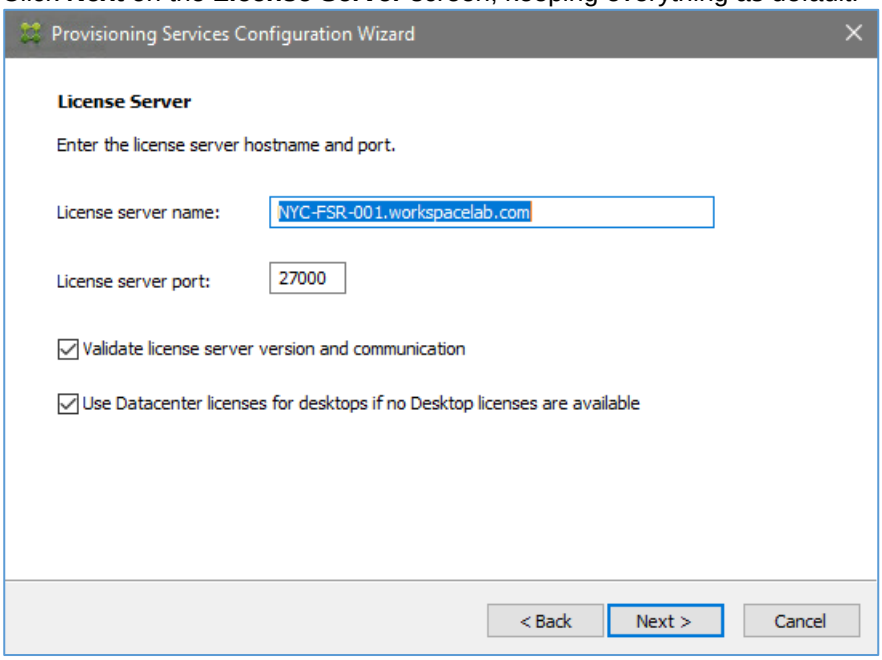
6.	On the **PXE Services** windows, select **The service that runs on this computer** and then click **Next**. 
7.	Select **Join existing farm** and then click **Next**.

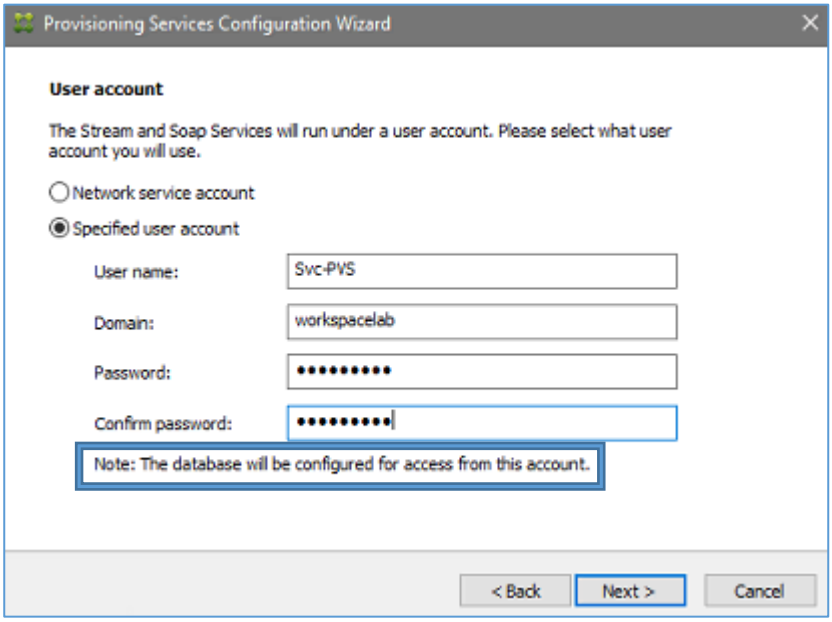


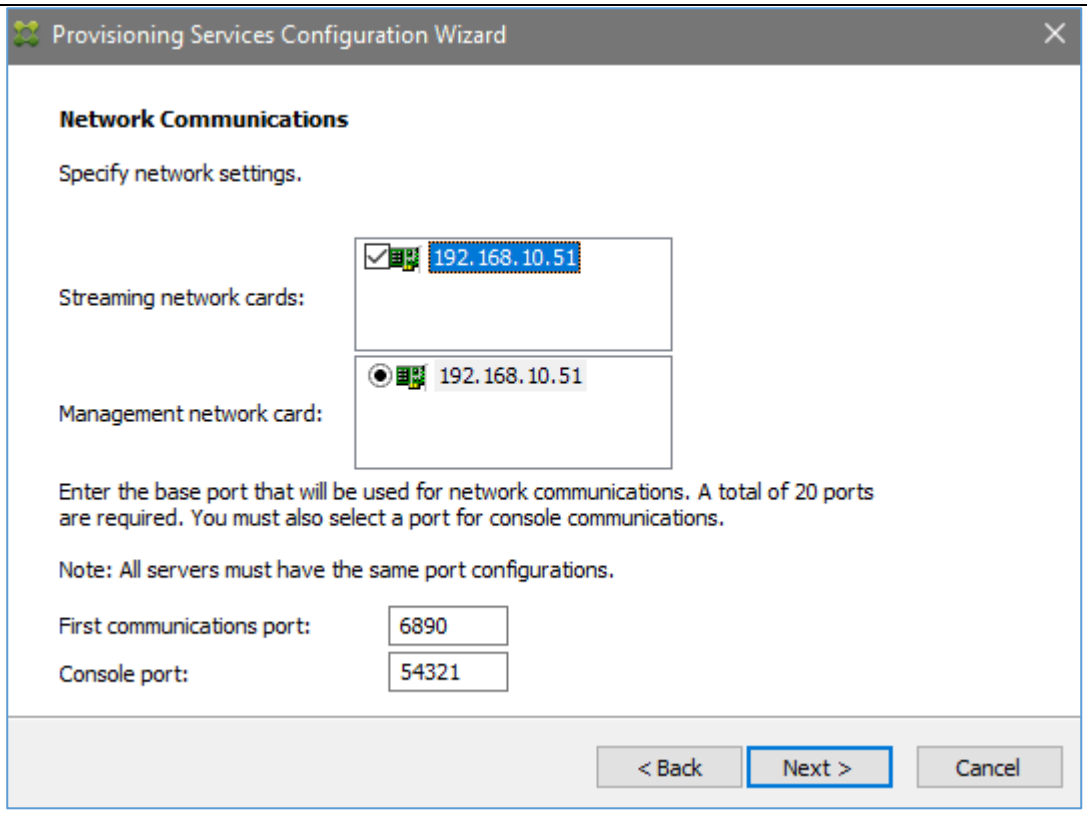
8. Type **NYC-SQL-001** in the Server name field and then click **Next**.



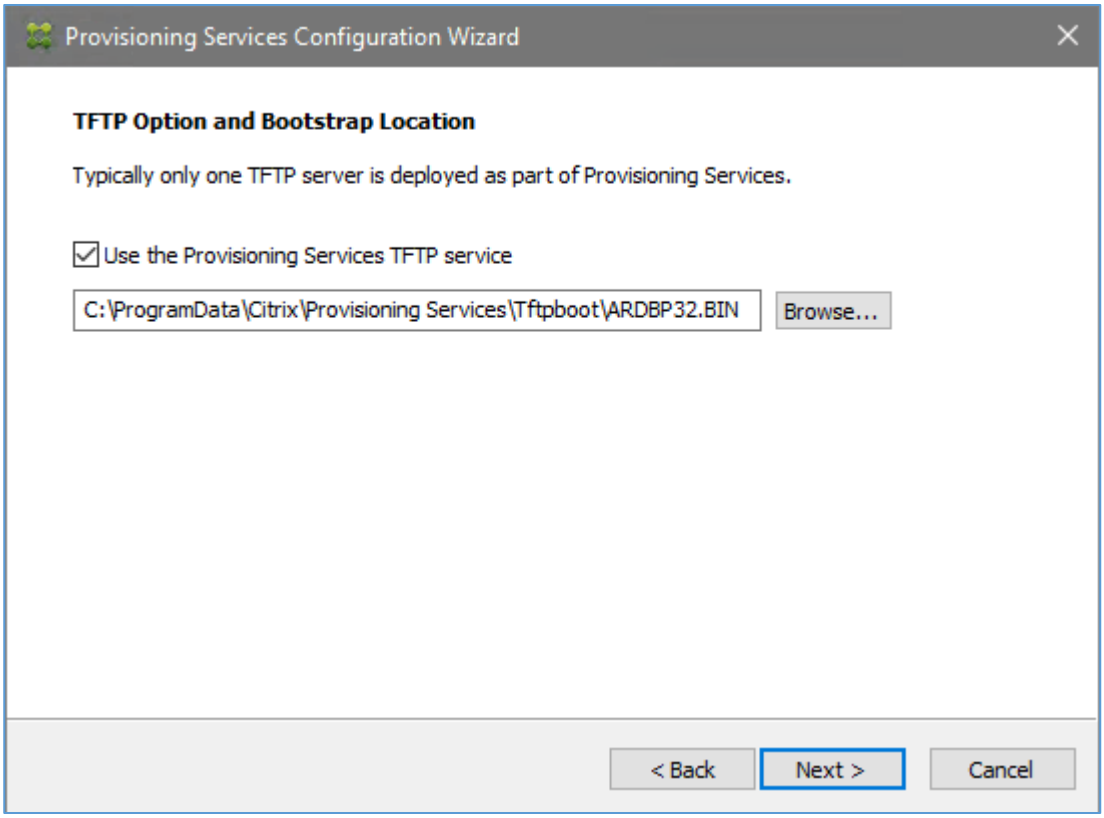
9.	Verify that **PVS_db:Farm** is listed as the database name in the Database Server page and click **Next**.
10.	Verify **Existing Site** is selected and the Site name is **NYC-Site**. Click **Next**. 
11.	Verify the **Existing Store** is selected and the Store name is **NYC-Store**. Click **Next**.

	
12.	Click **Next** on the **License Server** screen, keeping everything as default. 
13.	Select the account to use for the Stream Services and SOAP Server and then click **Next**. a. Select **Specified user account**. b. Type **Svc-PVS** in the User name field. c. Type **workspacelab** in the Domain field. d. Type **Password1** in the password fields.

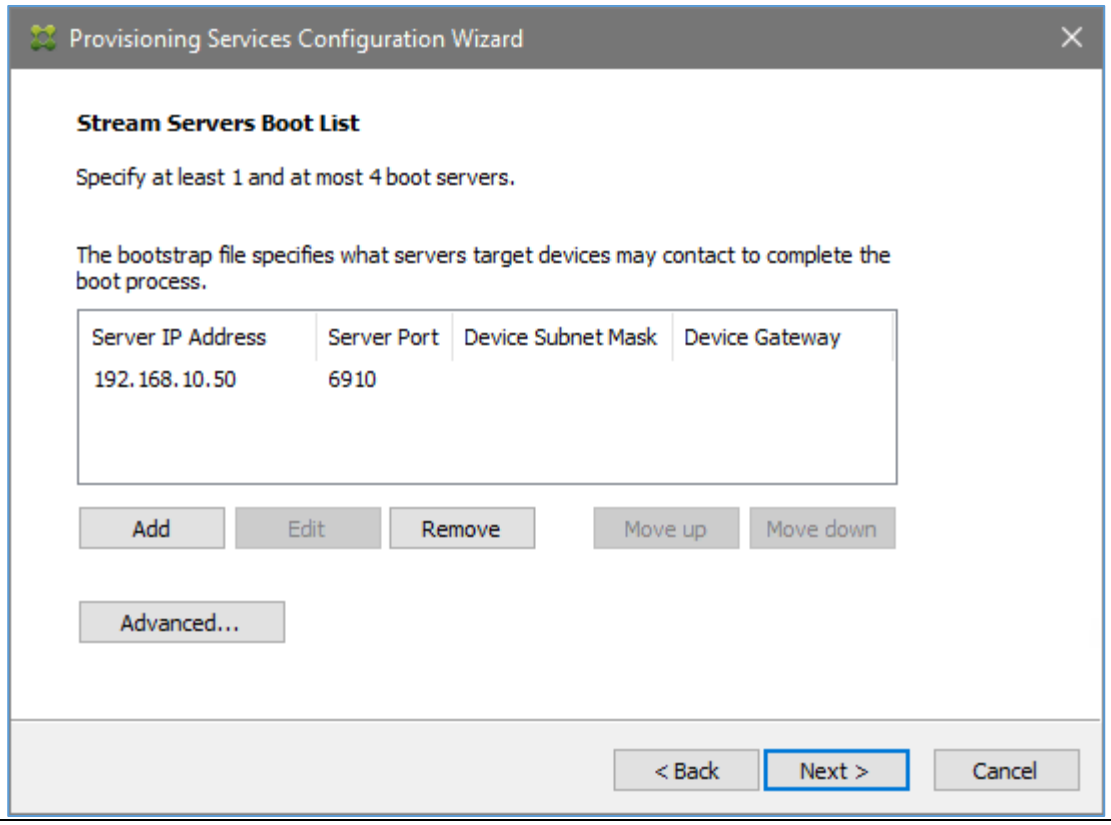
	e. Click **Next**.  **Note: Svc-PVS** Service account is already created for the Lab Environment. Once configured, stream and soap services will be running with this service account until changed manually. These are the two main services for PVS operations and they need permissions to access the vDisk store and database. **Note:** Login for the service account will automatically be added in the database.
14.	Verify that **Automate computer account password updates** is selected and then click **Next**.
15.	Verify that **6890** is specified as the First communications port, **54321** is specified as the Console port, and then click **Next**.



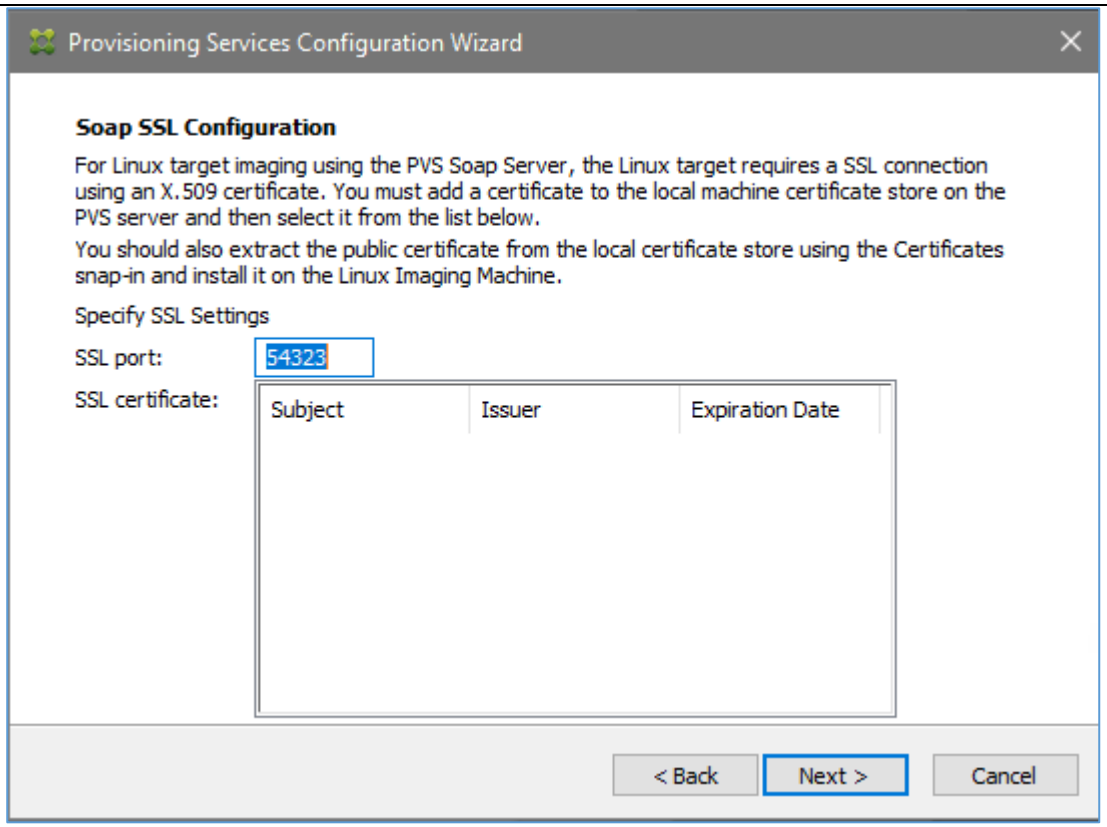
16. Select **Use the Provisioning Services TFTP service** and then click **Next**.



17. Click **Next** to accept the default **Stream Servers Boot List**.

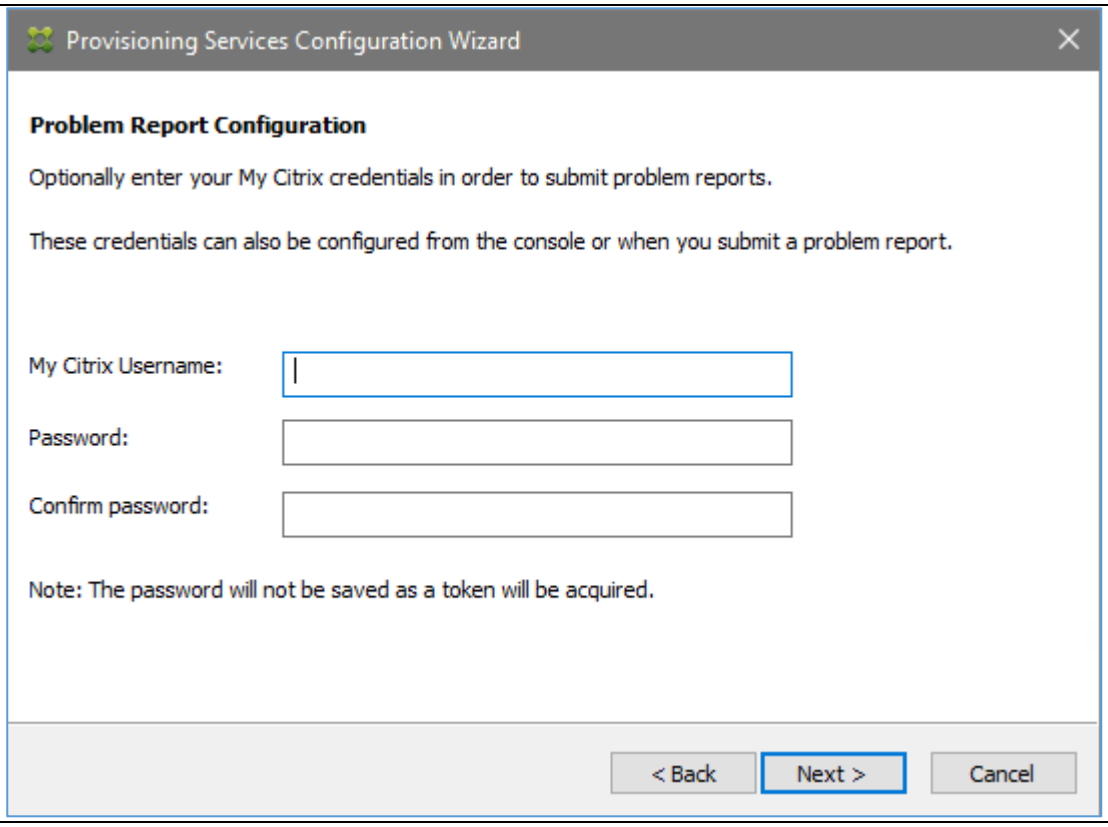


18. Click **Next** to accept the default **Soap SSL Configuration**.

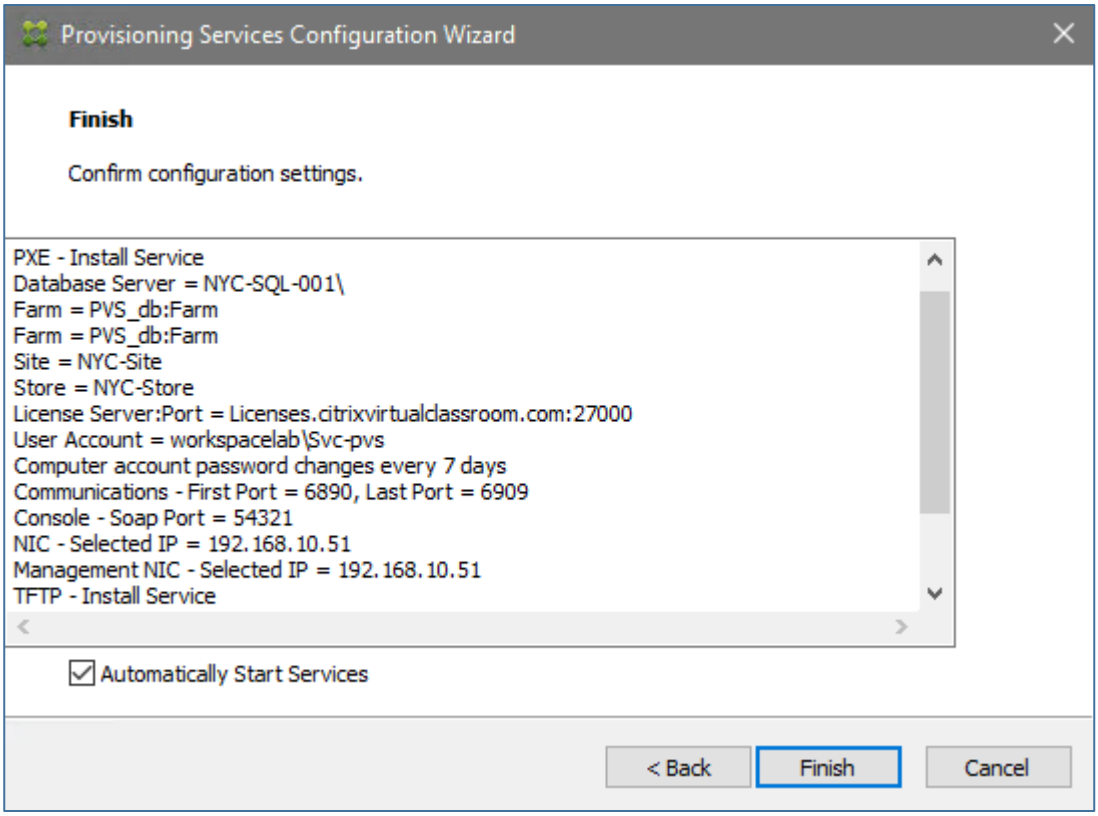


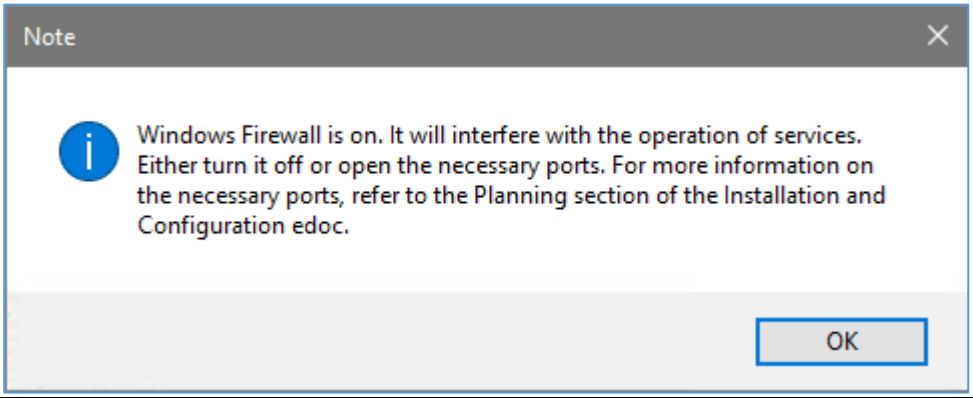
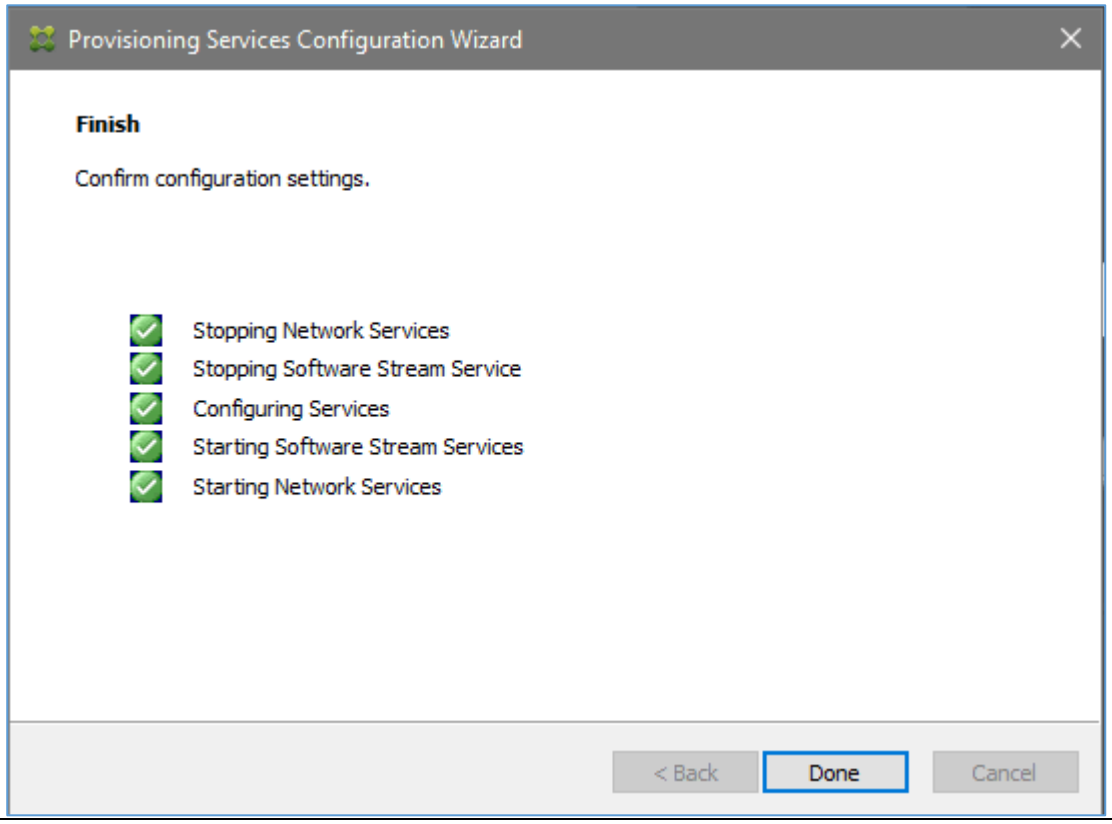
Note: SSL Configuration is only for Linux target devices.

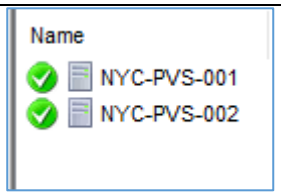
19. Click **Next** to accept the default **Problem Report Configuration**.



20. Verify that **Automatically Start Services** is selected and then click **Finish**.



21.	Click **OK** in the Windows Firewall pop-up window. 
22.	Wait while the configuration completes and then click **Done**. 
23.	Using the Remote Desktop Connection manager and connect to **NYC-PVS-001**. To login to **NYC-PVS-001**, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the password.
24.	Click **Start** and launch the **Provisioning Services Console**. Type **Localhost** and click **Connect**. **Note:** If the console is already open from the previous exercises ignore this step.
25.	Expand **Farm > Sites > NYC-Site > Servers** in the left pane and verify in right pane that we see two Provisioning Servers with a green check next to them.

	 **Note:** Refresh the console if both of the Provisioning Servers are not seen. It may take approximately 5 minutes for **NYC-PVS-002** to appear.

Key Takeaways:

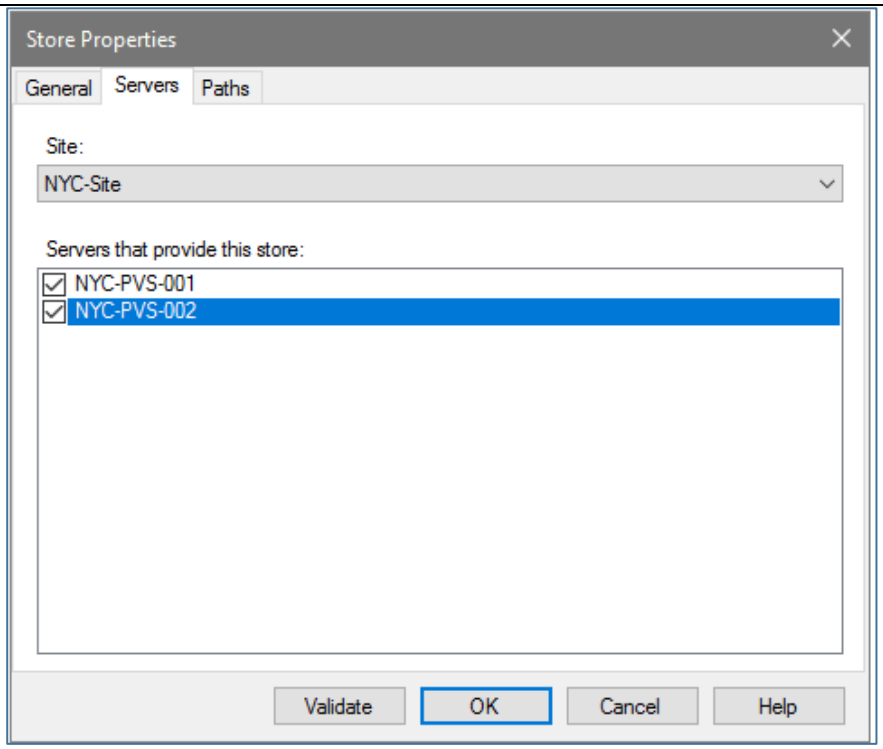
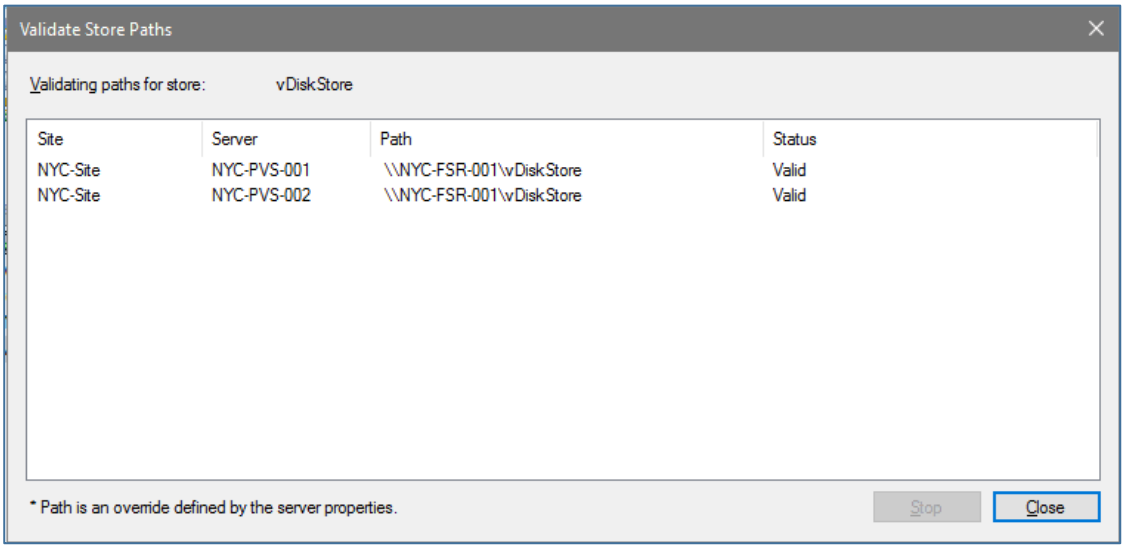
- Each Provisioning Services server must be joined to the farm in order to serve vDisks.
- When joining a new Provisioning Services server to a farm, you have the option to join an existing site or create a new site. You also have the option to join the existing Store or create a new Store.

Exercise 20-2: Reconfigure the Store for Redundancy

Scenario:

You are a Citrix Administrator at WW Labs, your Lead Citrix Architect has tasked you to ensure that both Provisioning Services servers now has the ability to stream vDisks from the vDiskStore hosted on the file server.

Step	Action
1.	Using the Remote Desktop Connection manager, confirm you are still connected to **NYC-PVS-001**. **Note:** In a previous exercise, you had logged into **NYC-PVS-001** using the following credentials to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the Password. **Note**: If your Remote Desktop Connection session is disconnected, log on to **NYC-PVS-001**, right-click this machine and choose **Connect server**.
2.	Click **Start** and launch the **Provisioning Services Console.** Type **Localhost** and click **Connect**. **Note:** If the console is already open from the previous exercise ignore this step.
3.	Browse **Farm > Stores > vDiskStore**.
4.	Right-click **vDiskStore** and select **Properties**. **Note:** A warning message may come if any of the target devices are is booted from the PVS environment. Click **Yes** on the Warning message.
5.	Select the **Servers** tab, check the **NYC-PVS-002** box**,** and verify both PVS servers are checked.

	
6.	Click on the **Paths** tab and click **Validate**.
7.	Wait for the status to read **Valid** for both servers and then click **Close**. 
8.	Click **OK**.

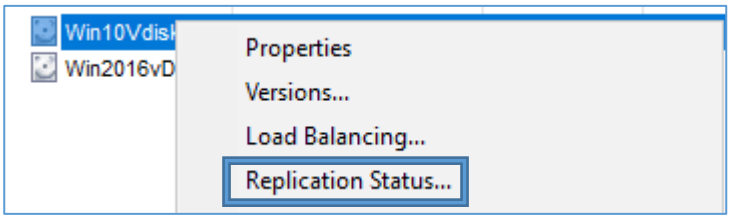
Key Takeaways:

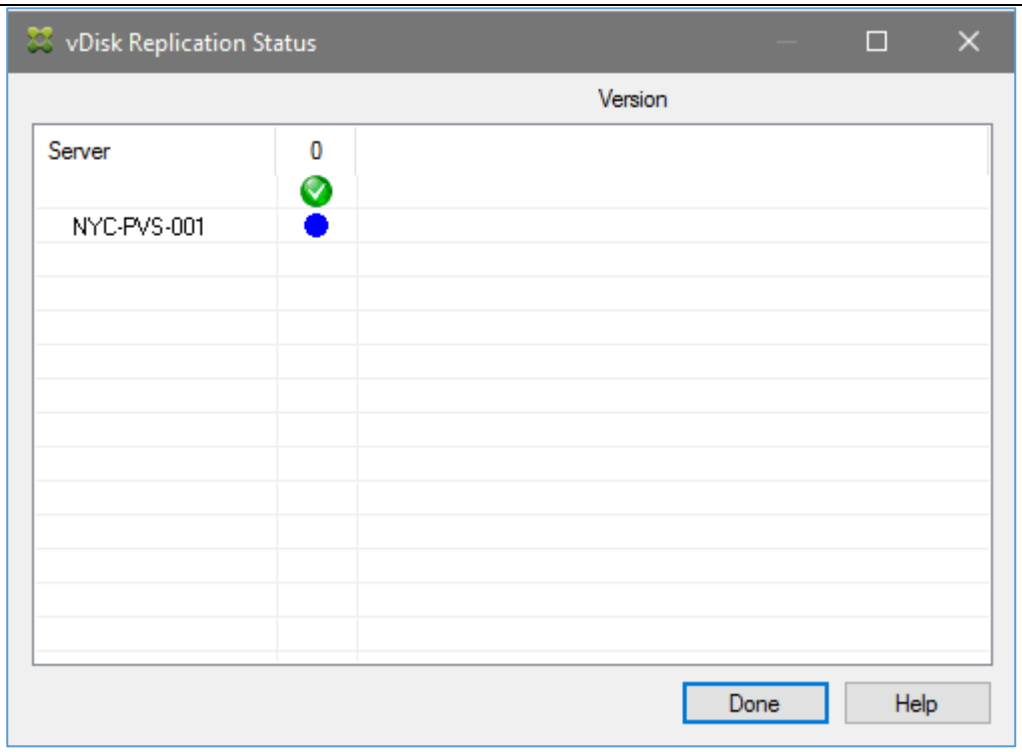
- After adding a new Provisioning Services host to a farm it is recommended to enable this server on all available stores and ensure that the server has a valid connection to the store.
- If a store is only served by a single Provisioning Services server, the vDisks hosted in this store are subject to single point of failure.

Exercise 20-4: Verify vDisk Replication

Scenario:

You are a Citrix Administrator at WW Labs, your Lead Citrix Architect has informed you that there is a vDisk replication monitor build in to the PVS Console. You task is to use this vDisk replication to verify if the Win10vDisk is currently being offered by both PVS servers.

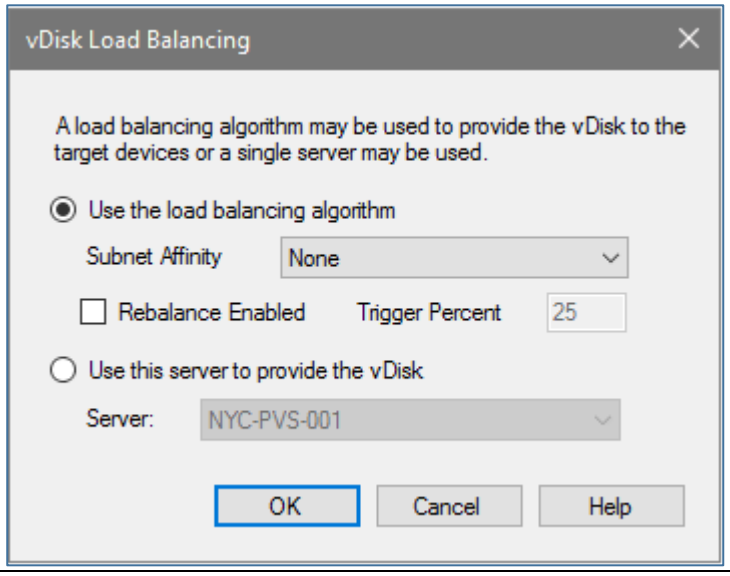
Step	Action
1.	Using the Remote Desktop Connection manager, confirm you are still connected to **NYC-PVS-001**. **Note:** In a previous exercise, you had logged into **NYC-PVS-001** using the following credentials to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the Password. **Note**: If your Remote Desktop Connection session is disconnected, log on to **NYC-PVS-001**, right-click this machine and choose **Connect server**.
2.	Click **Start** and launch the **Provisioning Services** console. Type **Localhost** and click **Connect**. **Note:** If the console is already open from the previous exercises ignore this step.
3.	Browse **Farm > Stores > vDiskStore**.
4.	Right-click **Win10Vdisk** in right pane and select **Replication Status**. 
5.	You will only see **NYC-PVS-001** and not **NYC-PVS-002**.

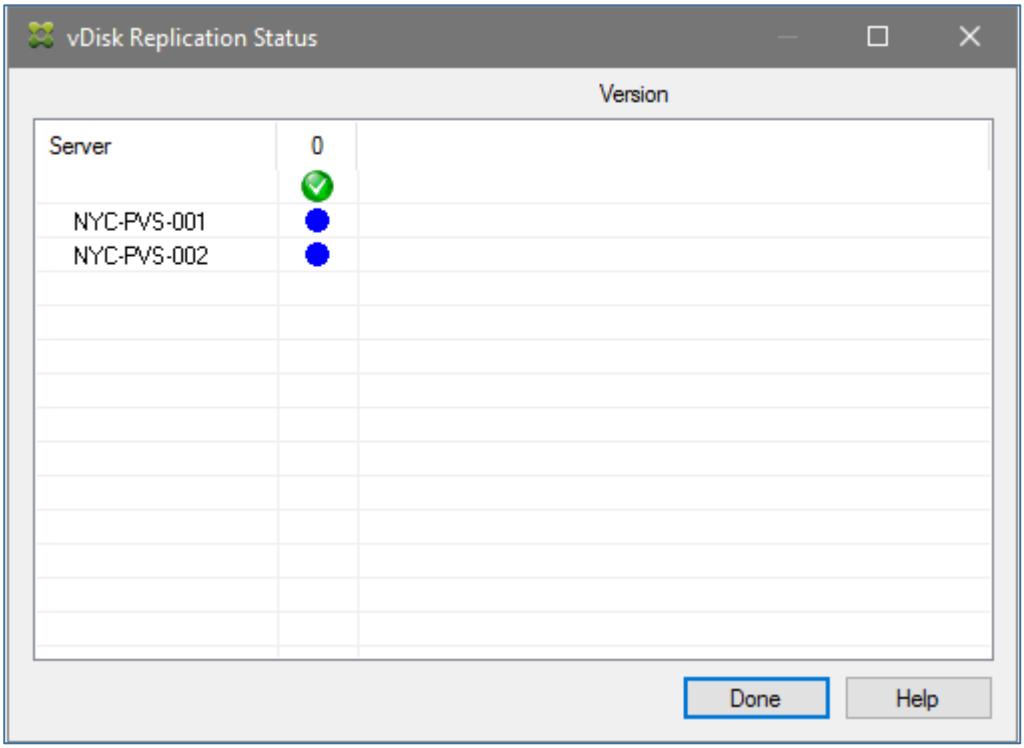


Click **Done**.

6. Right-click **Win10Vdisk** in right pane and select **Load Balancing**.

7. Select **Use the load balancing algorithm** and click **OK**.



8.	Right-click **Win10Vdisk** in right pane, select **Replication Status** and verify we see both the servers with **Blue Dots** showing that replication is good.  Click **Done**. **Note:** The vDisk store is a shared store for both NYC-PVS-001 and NYC-PVS-002, so we do not require any manual copy of vDisk and associated files. In case of local stores on Provisioning servers, we would need to copy files from one store to another; we will cover this process in the next exercise. **Note**: If either server does not display a blue dot, click done on the "vDisk Replication Status" window and repeat the step.

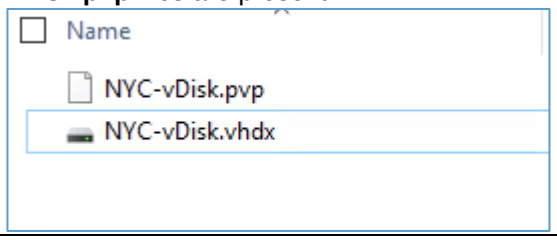
Key Takeaways:

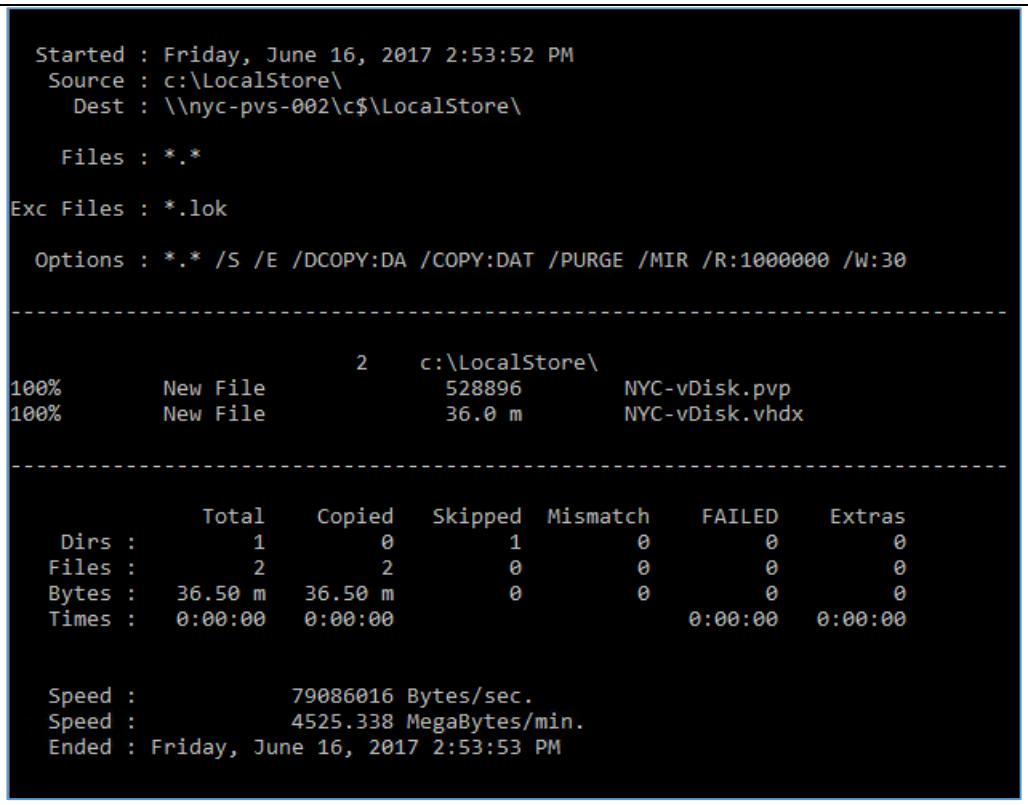
- On each vDisk you can configure whether the vDisk should be load balanced or served from only a specific Provisioning Services server.
- Under normal circumstances, the vDisk should always be load balanced to ensure high availability.
- When using distributed local stores and changing a vDisk to Private mode, you should ensure the vDisk is hosted from a single Provisioning Services server, otherwise you may not know which PVS server has the latest vDisk changes.
- Distributed local stores are presented in the next exercise.

Exercise 20-5: Copy a vDisk from One Store to Another

Scenario:

You are a Citrix Administrator at WW Labs, your Lead Citrix Architect has instructed you to ensure that the vDisks stored in the LocalStore folder on NYC-PVS-001 are replicated to NYC-PVS-002. Your task is to use RoboCopy to create a copy script that can be used as part of an automated process in production.

Step	Action
1.	Using the Remote Desktop Connection manager, connect to **NYC-PVS-001**. To login to **NYC-PVS-001**, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the Password.
2.	Open **File Explorer** and browse to **C:\LocalStore**. Verify that the **NYC-vDisk.vhdx** and **NYC-vDisk.pvp** files are present. 
3.	Using the Remote Desktop Connection manager, connect to **NYC-PVS-002**. To login to **NYC-PVS-002**, right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the Password.
4.	Open **File Explorer** and browse to **C:\LocalStore**. Verify that this directory is empty. Next, copy the files from the **NYC-PVS-001** local store to **NYC-PVS-002** local store using **Robocopy**. Switch back to **NYC-PVS-001** using Remote Desktop Connection manager. Right-click **Start** and select **Command Prompt (Admin).** Type the below command and press **Enter**: **Robocopy /MIR c:\LocalStore \\nyc-pvs-002\c$\LocalStore /XF *.lok** `C:\Windows\system32>Robocopy /MIR c:\LocalStore \\nyc-pvs-002\c$\LocalStore /XF *.lok` **Note**: Within the above line the **/MIR c:\LocalStore \\nyc-pvs-002\c$\LocalStore** portion tells robocopy to mirror the local vDisk store **(c:\LocalStore)** to the remote PVS server, while the last bit of the script **/XF *.lok** excludes any files with the .lok extension.
5.	Verify the copy starts and finishes without any errors.

	
6.	Switch back to **NYC-PVS-002** using Remote Desktop Connection manager. Open **File Explorer** and browse to **C:\Localstore**. Verify the files have been copied successfully.
7.	Right-click and delete the **NYC-vDisk.pvp** file. Switch back to **NYC-PVS-001** using Remote Desktop Connection manager. Browse to **C:\LocalStore** and delete **NYC-vDisk.pvp** file. **Note**: The .pvp files are being deleted from both stores because in the next exercise we will create a new .pvp file.

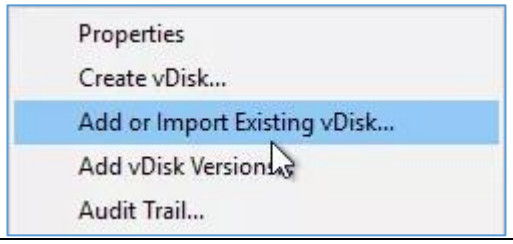
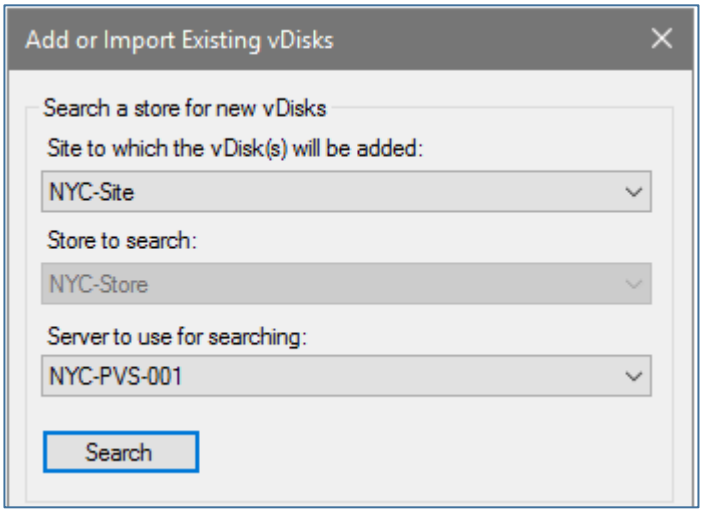
Key Takeaways:

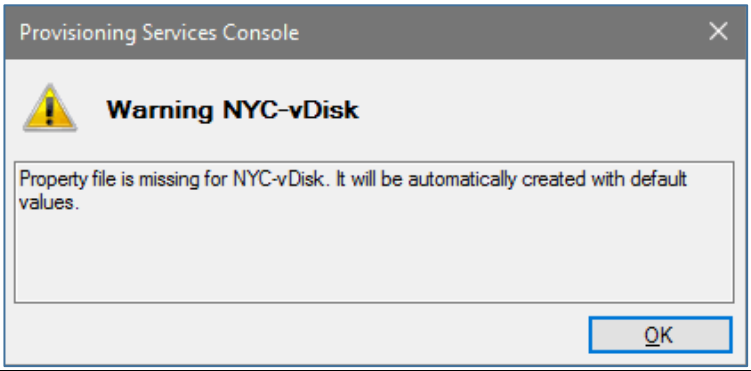
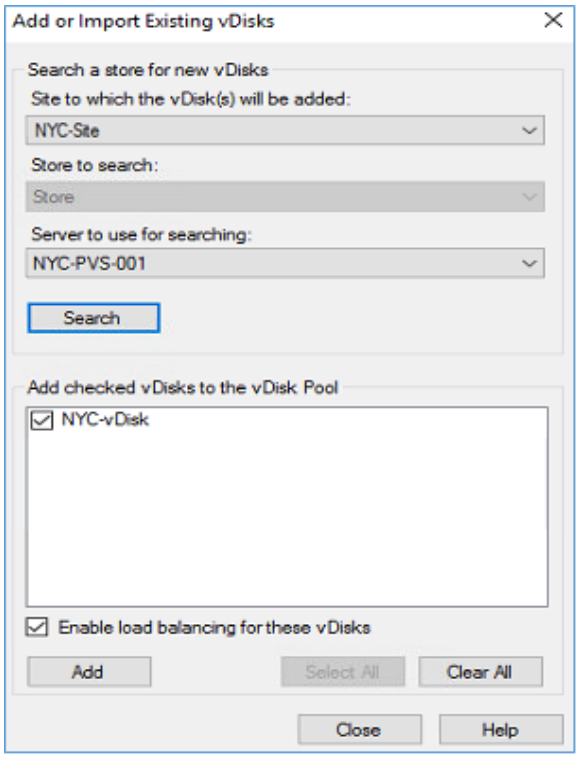
- Instead of hosting the vDisks on a centralized file server, customers can choose to have their vDisks hosted locally on each Provisioning Services server.
- This design removes the single point of failure in the file server and reduces the network traffic on the Provisioning Services server since the vDisk content is fetched locally rather than via the network.
- When choosing a distributed local store, it is important to have a process in place to ensure that all the vDisk content is replicated between the Provisioning Services servers – RoboCopy can be used to schedule a mirror action between multiple servers.

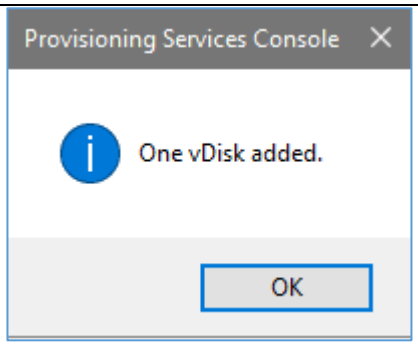
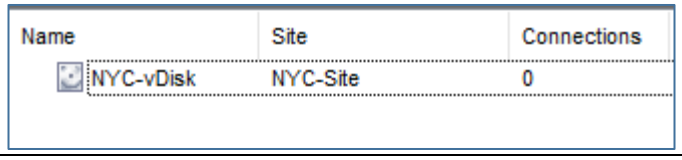
Exercise 20-6: Import a Pre-Existing vDisk and Create a New .pvp File

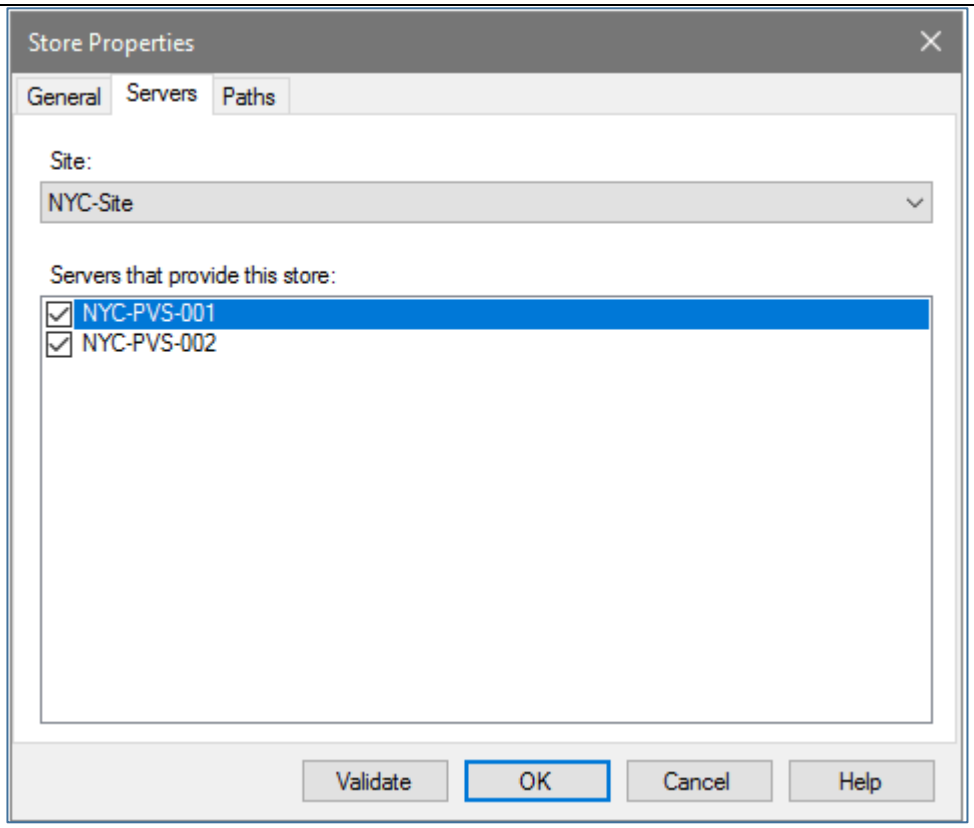
Scenario:

You are a Citrix Administrator at WW Labs. As part of the initial installation of Citrix Provisioning Services, you defined a vDisk store named Store. Your Lead Citrix Architect has now instructed you to import a pre-created vDisk located in the c:\LocalStore folder.

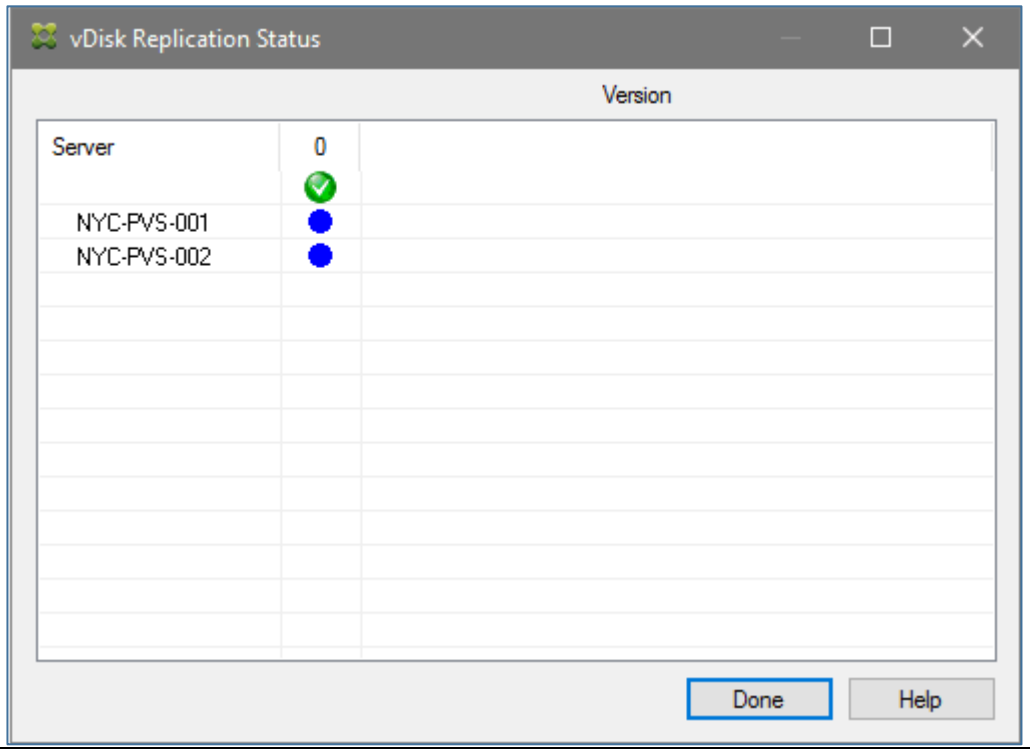
Step	Action
1.	Using the Remote Desktop Connection manager, confirm you are still connected to **NYC-PVS-001**. **Note:** In a previous exercise, you had logged into **NYC-PVS-001** using the following credentials to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the Password. **Note**: If your Remote Desktop Connection session is disconnected, log on to **NYC-PVS-001**, right-click this machine and choose **Connect server**.
2.	Click **Start** and launch **Provisioning Services** console. Type **Localhost** and click **Connect**. **Note:** If the console is already open from the previous exercises ignore this step.
3.	Browse **Farm > Stores > NYC-Store**. Right-click **NYC-Store** and select **Properties**. Click **X** on the Store Properties window. **Note:** A warning message may come if any of the target devices are booted from the PVS environment. Click **Yes** on the warning message.
4.	Right-click the **NYC-Store**, and click **Add or Import Existing vDisk**. 
5.	Click **Search**. 

6.	Click **OK** on the property file missing message. There is no .pvp file present PVS, so we will create a new .PVP file. 
7.	The new vDisk should be displayed in the Add checked vDisks to the vDisk Pool window. Verify **Enable load balancing for these vDisks** is checked and then click **Add**. 
8.	Click **OK**.

	 Click **Close**.
9.	Refresh the Provisioning Services Console by pressing **F5** and note that the **NYC-vDisk** is added. 
10.	Browse to **c:\LocalStore** and verify that the **NYC-vDisk.pvp** file has been created.
11.	Right-click **Start** and select **Command Prompt (Admin)** and type this command: **Robocopy /MIR c:\LocalStore \\nyc-pvs-002\c$\LocalStore /XF *.lok *.vhdx** **Note:** This command will copy only the .pvp file to **NYC-PVS-002** and will skip the .vhdx and .lok files.
12.	Close the **Command Prompt** Window.
13.	Switch to **NYC-PVS-002** and browse **c:\LocalStore** and verify that the **NYC-vDisk.pvp** file has been copied.
14.	Switch back to **NYC-PVS-001** using Remote Desktop Connection manager. Browse to **Farm > Sites > Stores > NYC-Store.** Right-click **NYC-Store** and select **Properties**.
15.	Click the **Servers** tab, verify both servers are checked, and click **OK**.



16. Click on **vDisk Pool** in the left pane of the console, right-click **NYC-vDisk** in the right pane and select **Replication Status**. Verify that replication is fine and click **Done**.



	Note: If either server does not display a blue dot, click done on the “vDisk Replication Status” window and repeat the step.
17.	Close the **Provisioning Services** console.

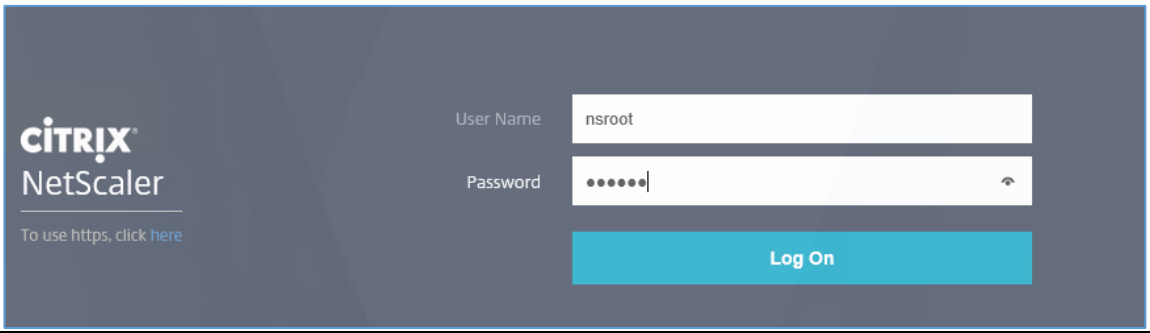
Key Takeaways:

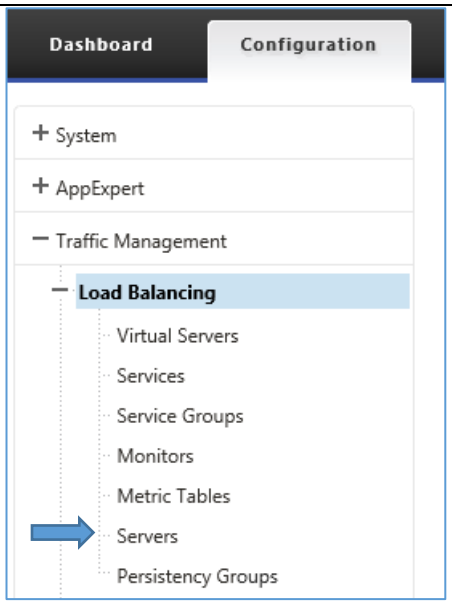
- vDisks can easily be imported into the Provisioning Services database using the console.
- When copying a vDisk between different environments avoid copying the PVP and LOK file.
- When importing a vDisk without a corresponding PVP file, a new PVP file containing default settings will be created.

Exercise 20-7: TFTP Load Balancing Configuration

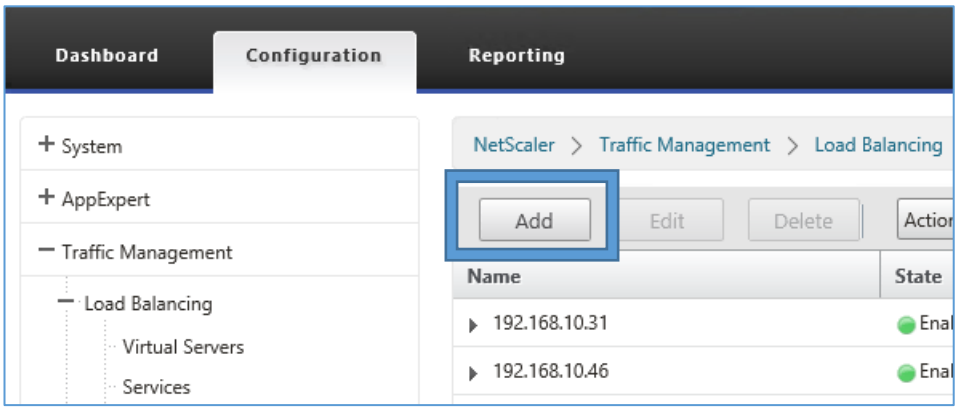
Scenario:

You are a Citrix Administrator at WW Labs, your Lead Citrix Architect has just reviewed the DHCP options you configured in a previous exercise. While reviewing the configuration he noticed that you only configured one PVS server in option 66. In the interest of reducing the single points of failure, your Lead Citrix Architect instructs you to investigate using the POC NetScaler to load balance the TFTP service hosted on each PVS server.

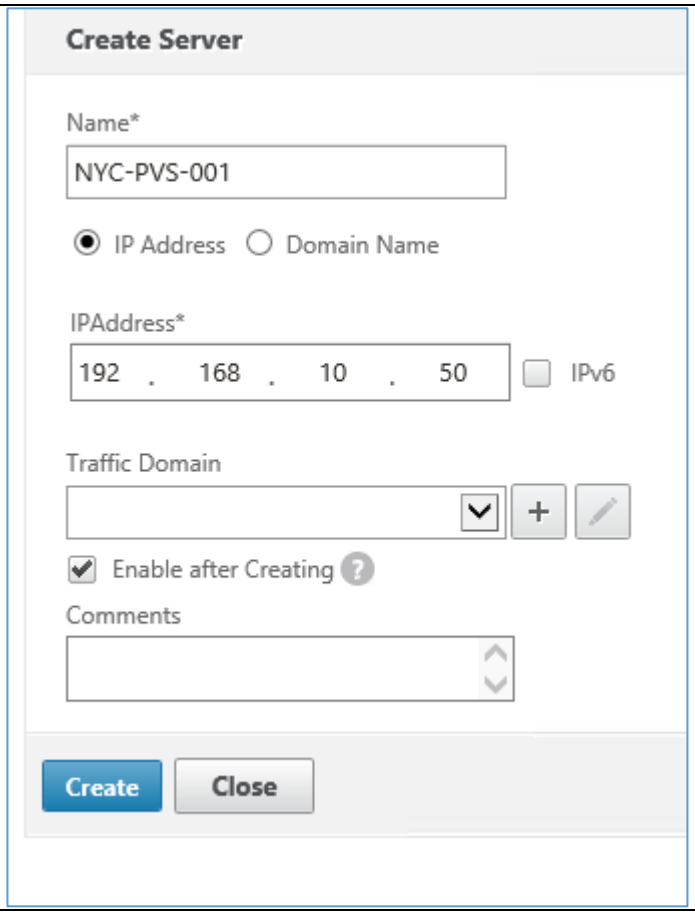
Step	Action
1.	Using the Remote Desktop Connection manager, switch back to **NYC-FSR-001**. **Note:** In a previous exercise, you had logged into **NYC-FSR-001** using the following credentials to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the Password. **Note**: If your Remote Desktop Connection session is disconnected, log on to **NYC-FSR-001**, right-click this machine and choose **Connect server**.
2.	Open **Internet Explorer** and navigate to **http://192.168.10.100/**. Log in to the NetScaler console with the following credentials: • User Name: **nsroot** • Password: **nsroot** 
3.	On the NetScaler console, navigate to **Configuration > Traffic Management > Load Balancing > Servers**.

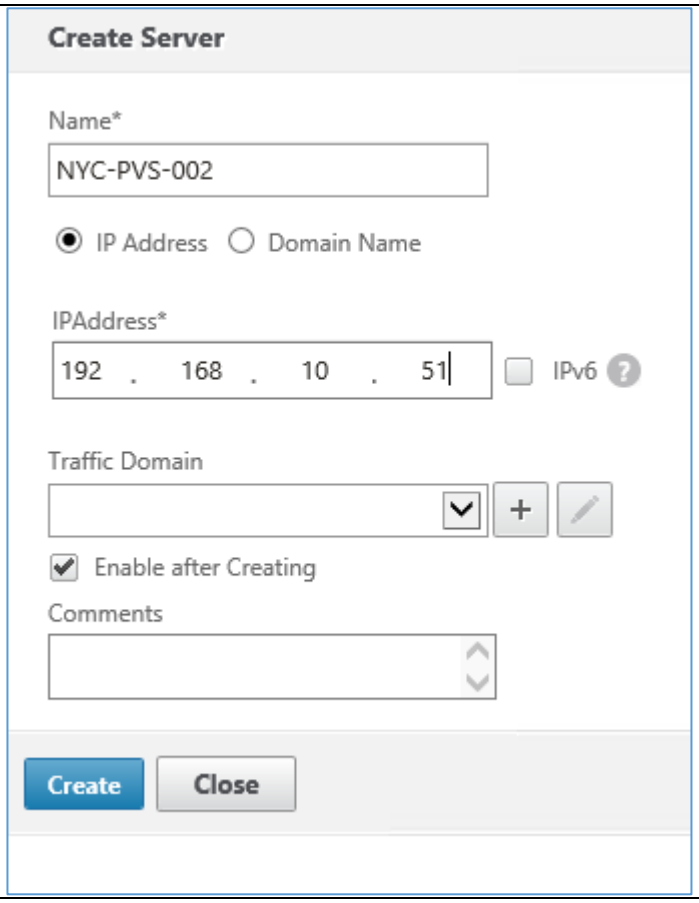
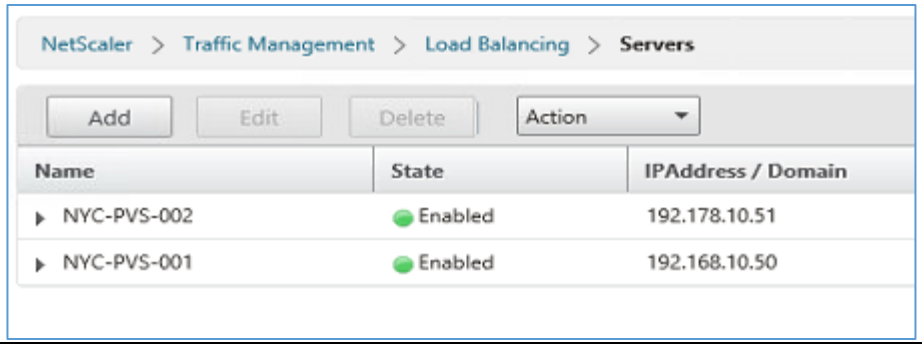


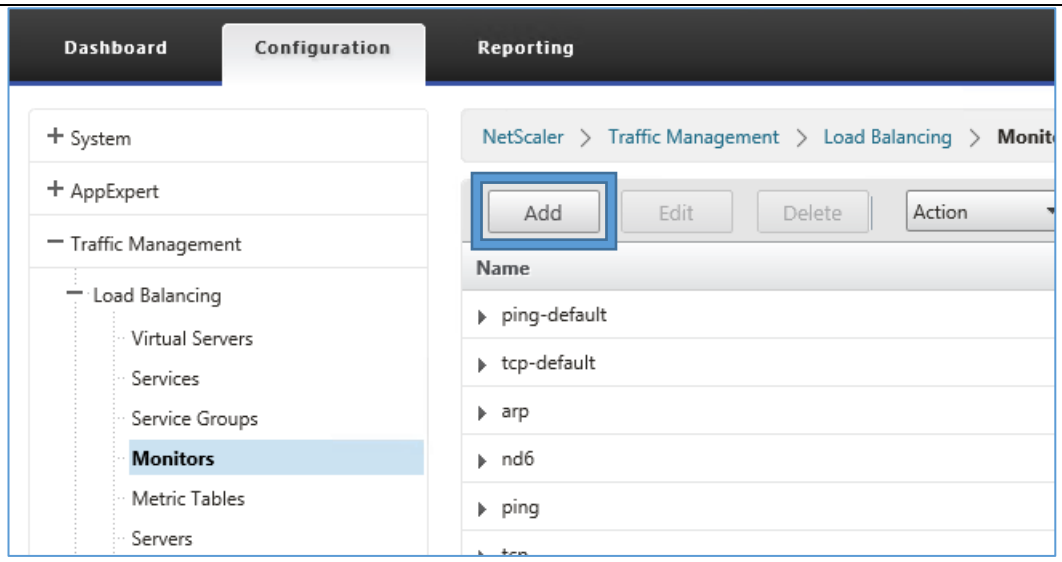
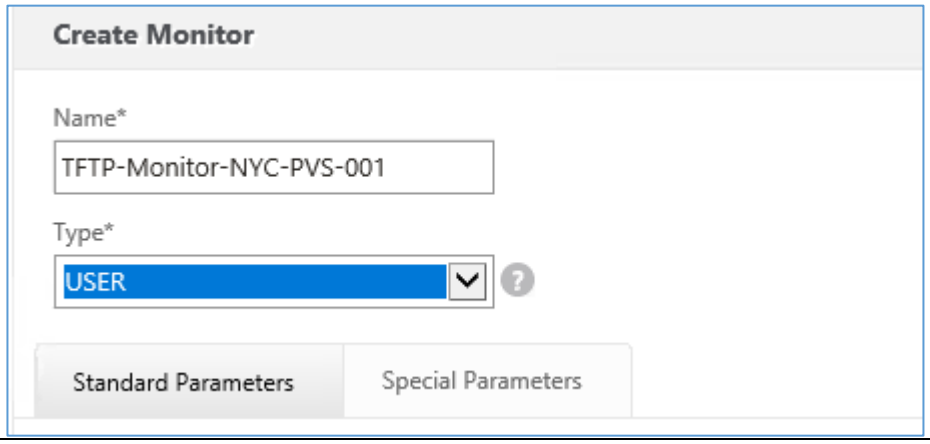
Select **Servers** in left pane and click **Add** in right pane.

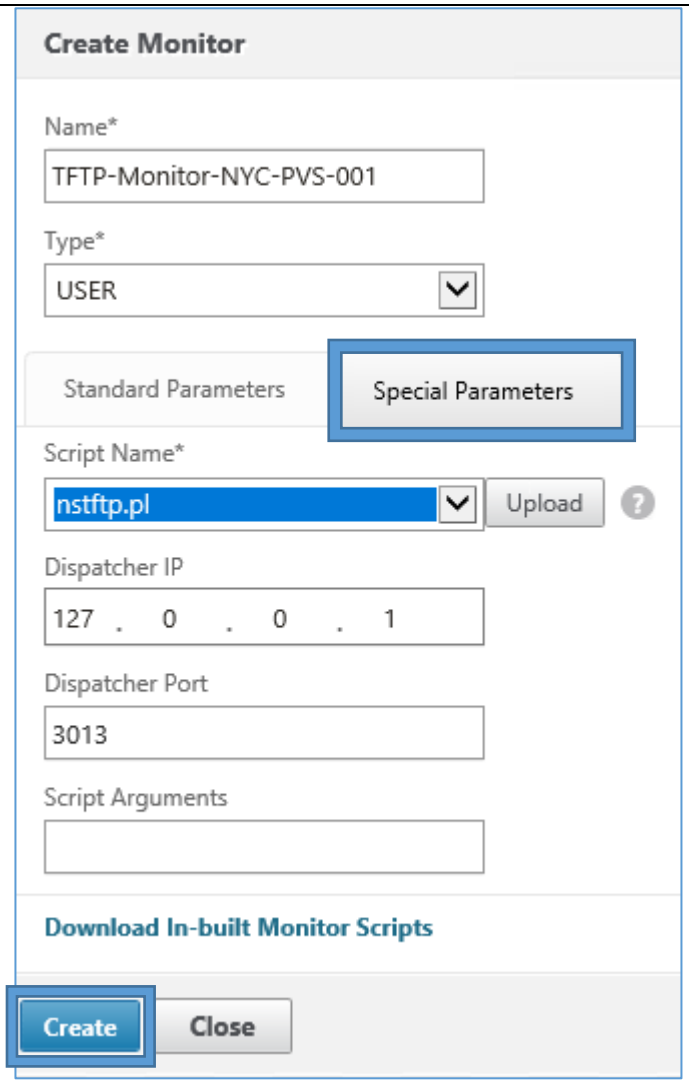


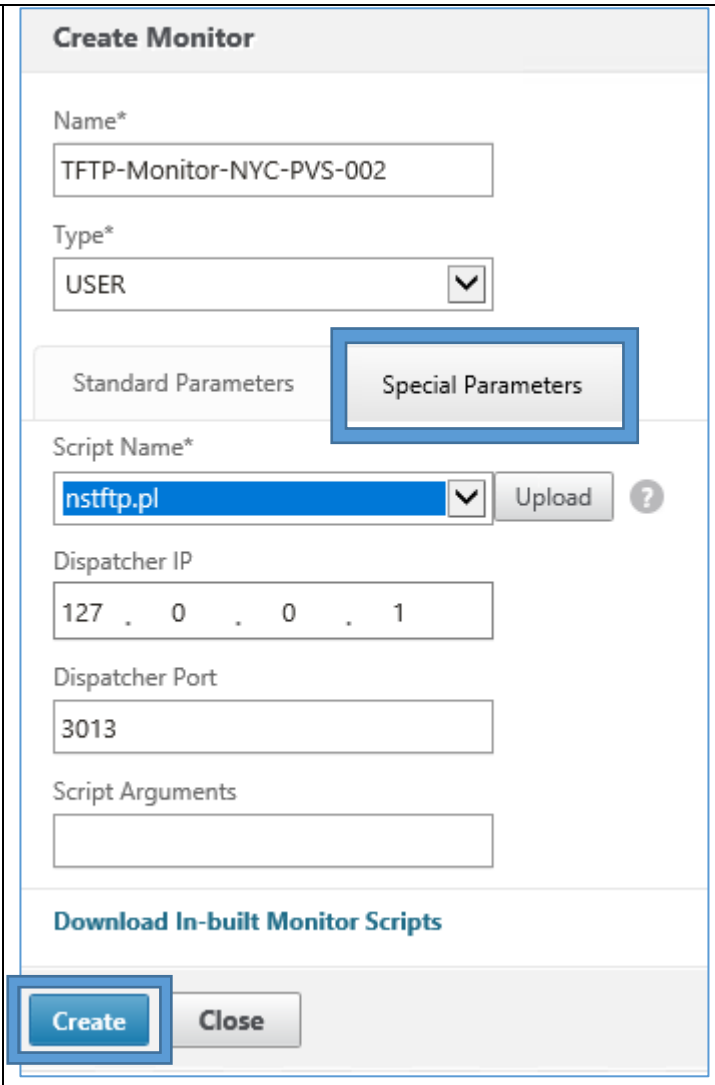
4. Enter the Name and IP address of your first PVS server (**NYC-PVS-001**) and click **Create**.

	
5.	Again click on **Add** under **Traffic Management > Load Balancing > Servers** tab, to add the second PVS Server **NYC-PVS-002**. Enter the Name and IP address of your second PVS server (**NYC-PVS-002**) and click **Create**.

	
6.	Verify that both servers are added. 
7.	Navigate to **Traffic Management > Load Balancing > Monitors**. Click **Add** in the right pane.

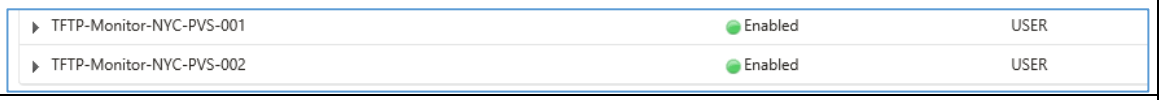
	
8.	In the Name field, type **TFTP-Monitor-NYC-PVS-001**. Using the Type drop-down select **USER**. 
9.	Click the **Special Parameters** tab and under **Script Name** select **nstftp.pl**.

	 Click **Create**.
10.	Navigate to **Traffic Management > Load Balancing > Monitors**. Click **Add** in the right pane to create a monitor for **NYC-PVS-002**. In the Name field, type **TFTP-Monitor-NYC-PVS-002**. Using the Type drop-down select **USER**. Click the **Special Parameters** tab and under **Script Name** select **nstftp.pl**.

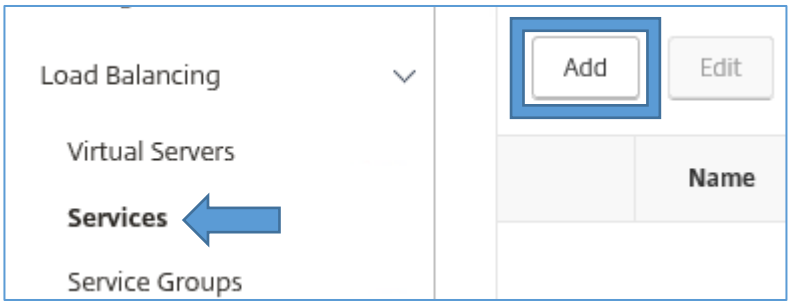


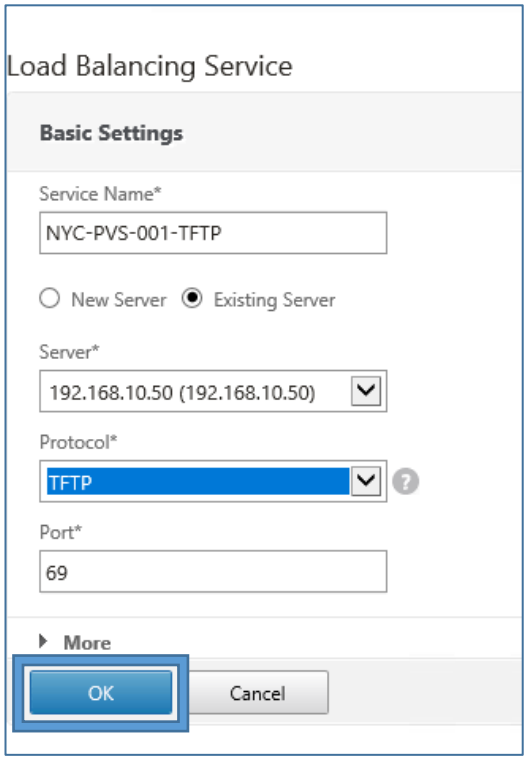
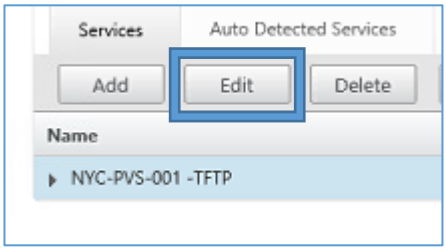
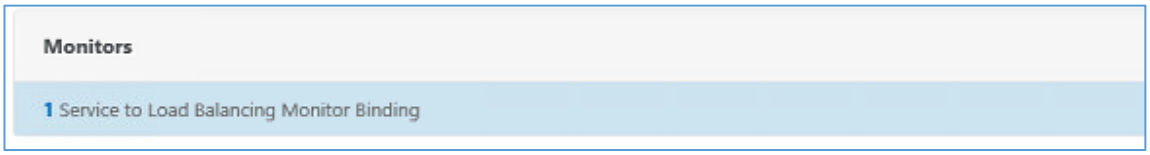
Click **Create**.

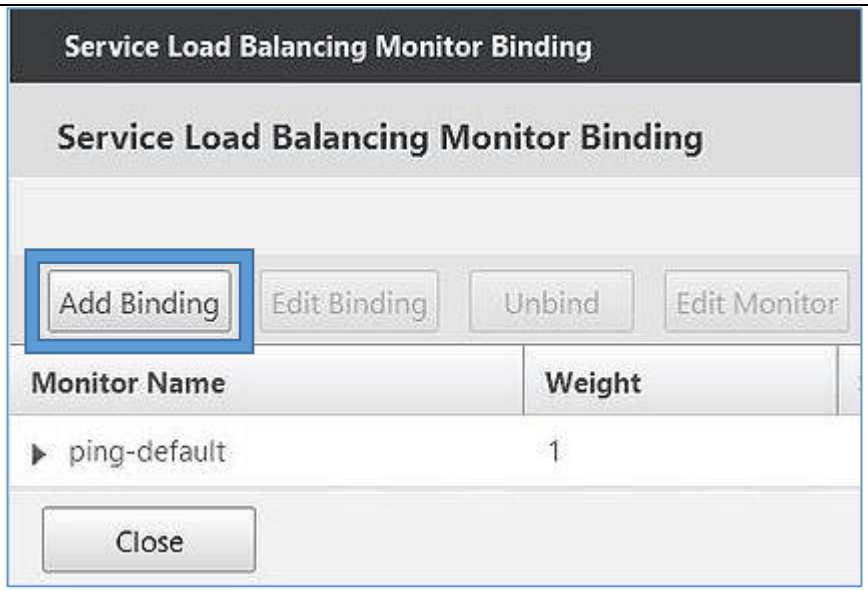
11. Once done verify the monitors are seen in Monitors view.



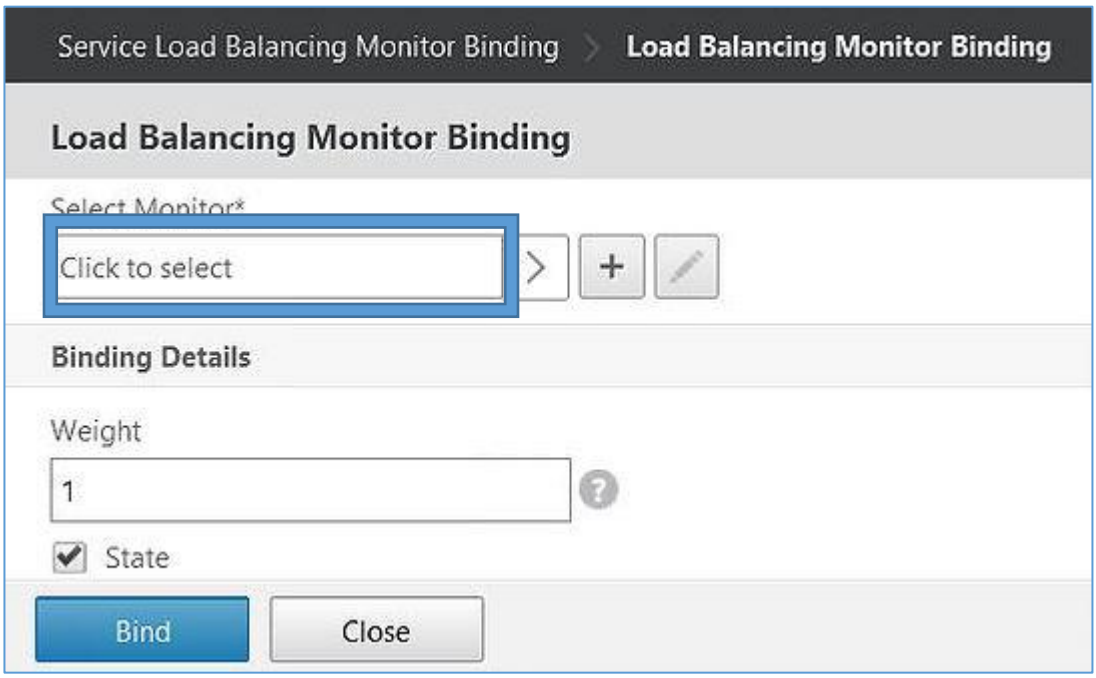
12. Navigate to **Traffic Management > Load Balancing > Services**. Click **Add** in the right pane.



13.	In the Service Name field, type **NYC-PVS-001-TFTP**. Select **Existing Server**. Point to an existing Provisioning Server by using the Server drop-down menu and choose NYC-PVS-001 **IP Address**. Specify the protocol using the Protocol drop-down menu and choose **TFTP**. In the Port field, type **69**. Click **OK**.  Scroll down and click **Done**.
14.	Select the Service just created and click **Edit**. 
15.	Scroll down and under Monitors select **1 Service to Load Balancing Monitor Binding**. 
16.	Click **Add Binding**.

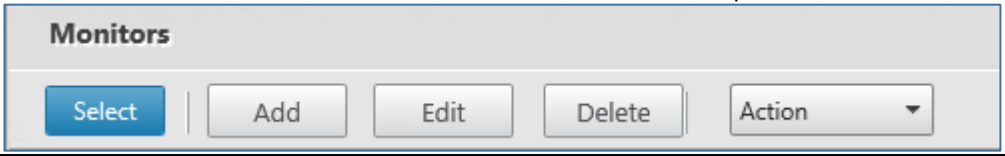


Click **Click to select**.

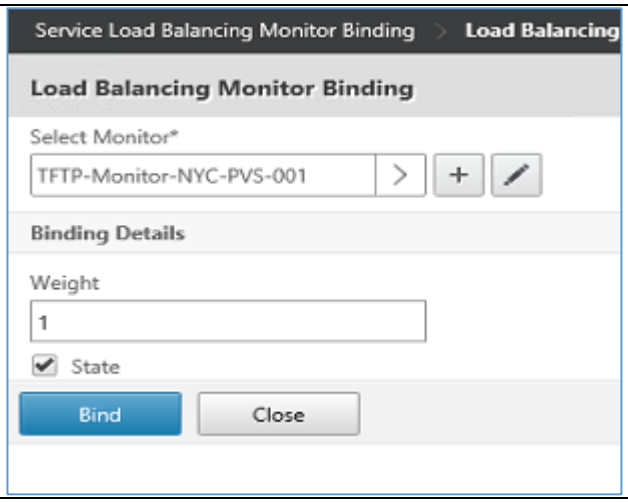
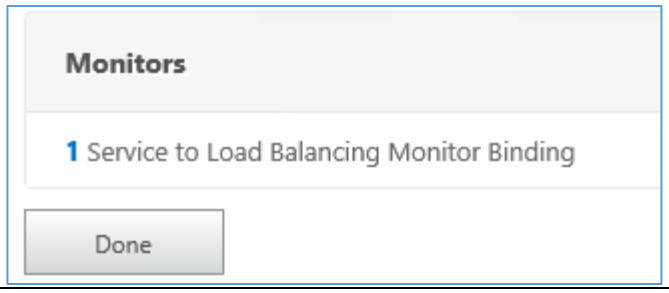
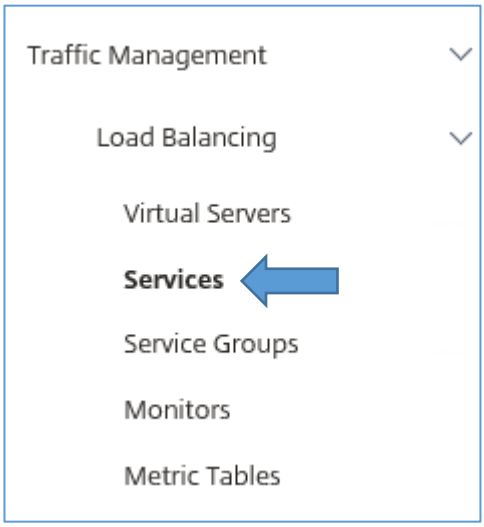


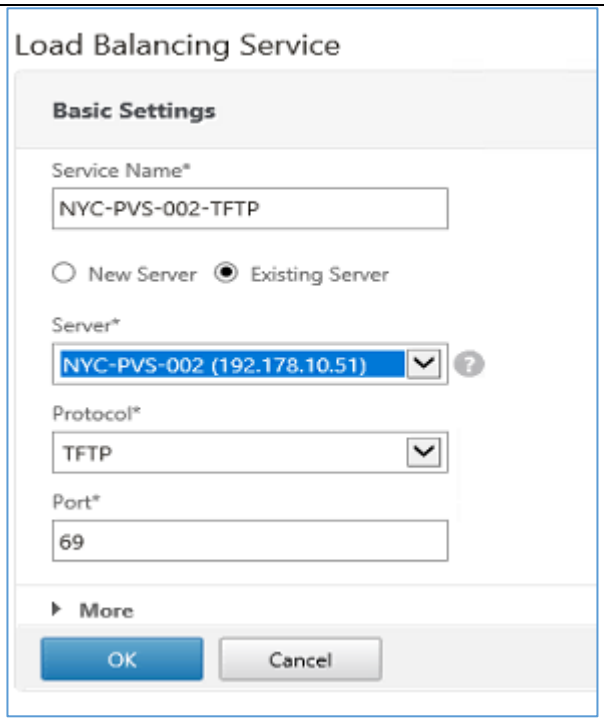
To create a service for **NYC-PVS-001,** attach the **TFTP-Monitor-NYC-PVS-001** monitor created earlier to this service.

17. Scroll down and select **TFTP-Monitor-NYC-PVS-001**. Scroll up and click **Select**.



18. Click **Bind**.

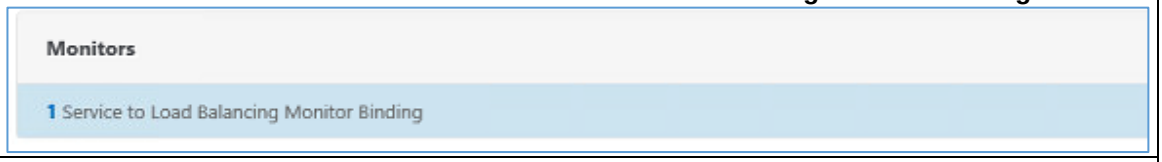
	
19.	The TFTP monitor probes **NYC-PVS-001** over UDP port 69. Click **Close**. Scroll down and click **Done**. 
20.	Next, we will repeat the process of creating a service, this time for the second PVS Server, by specifying a name, linking to the appropriate PVS server and specifying the protocol port. Navigate to **Traffic Management > Load Balancing > Services**. Click **Add** in right pane. 
21.	In the Service Name field, type **NYC-PVS-002-TFTP**. Select **Existing Server**. Point to an existing Provisioning Server by using the Server drop-down menu and choose NYC-PVS-002 **IP address**. Specify the protocol using the Protocol drop-down menu and choose **TFTP**. In the Port field, type **69**. Click **OK**.



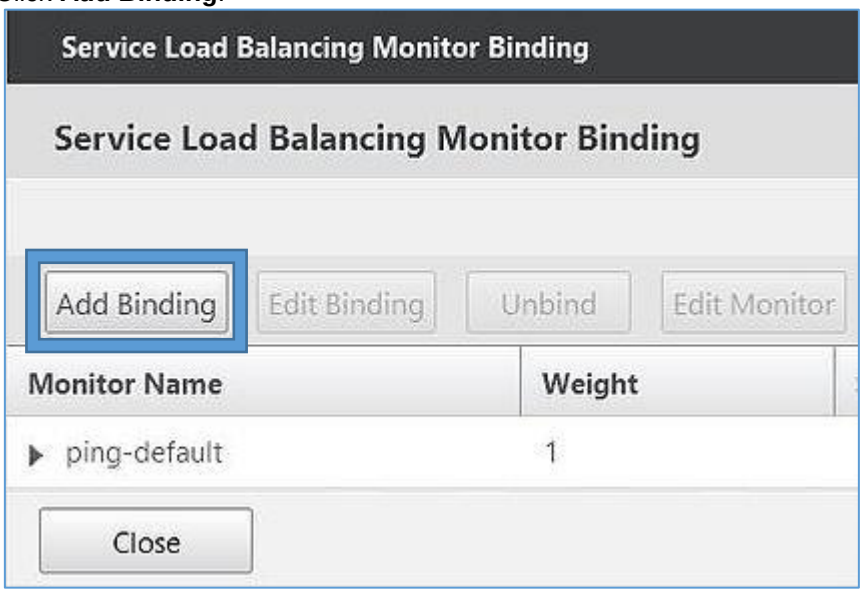
Scroll down and click **Done**.

22. Select the Service just created and click **Edit**.

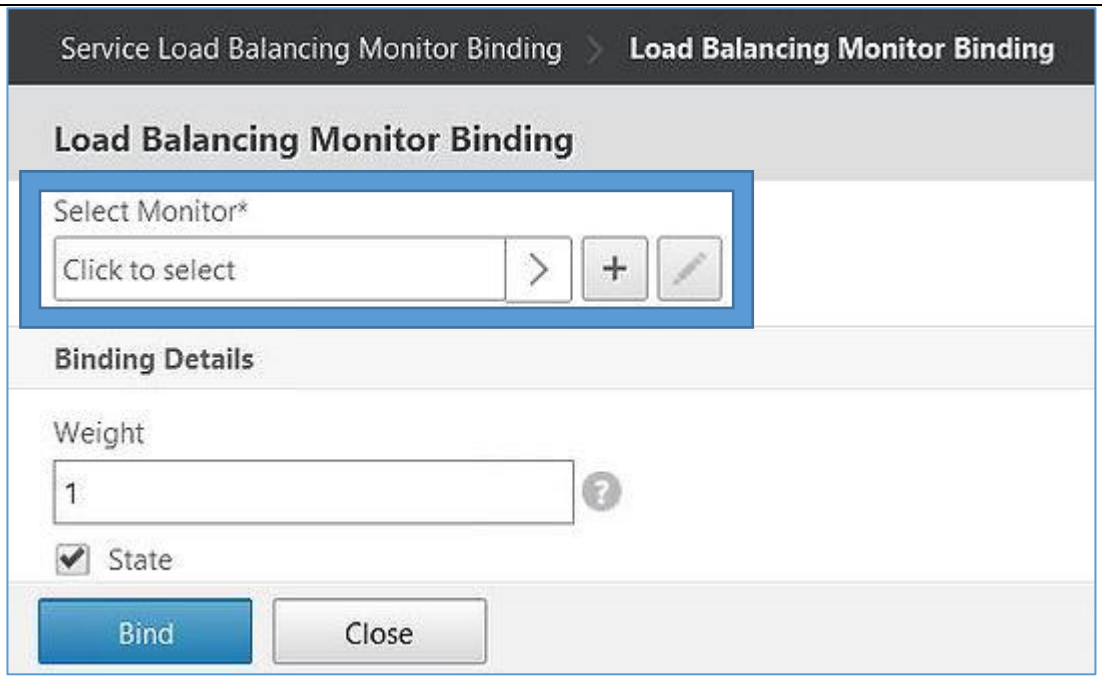
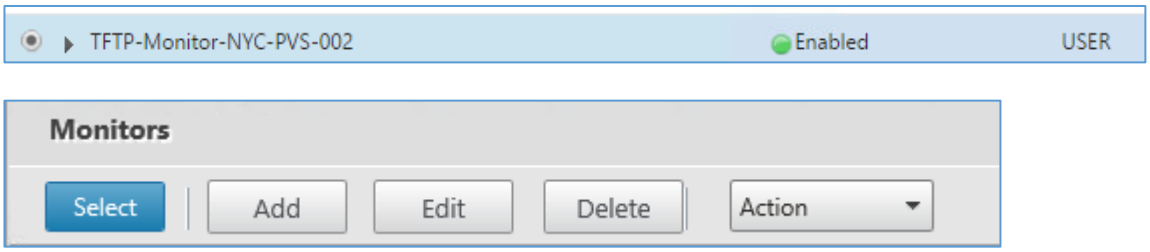
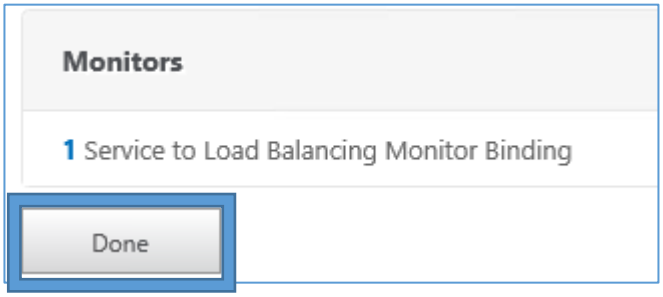
23. Scroll down and under Monitors select **1 Service to Load Balancing Monitor Binding**.

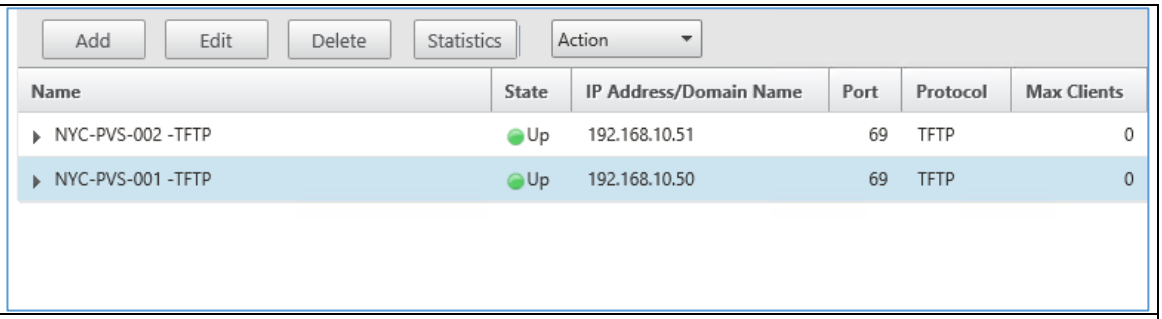
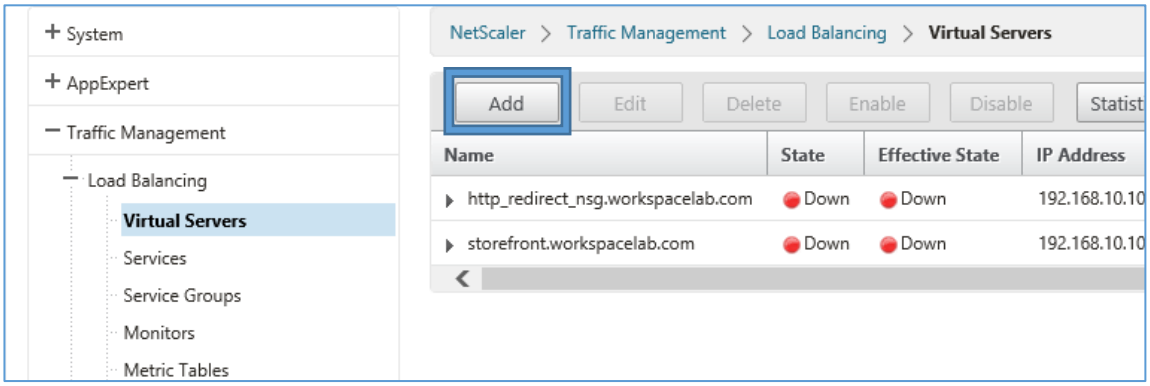


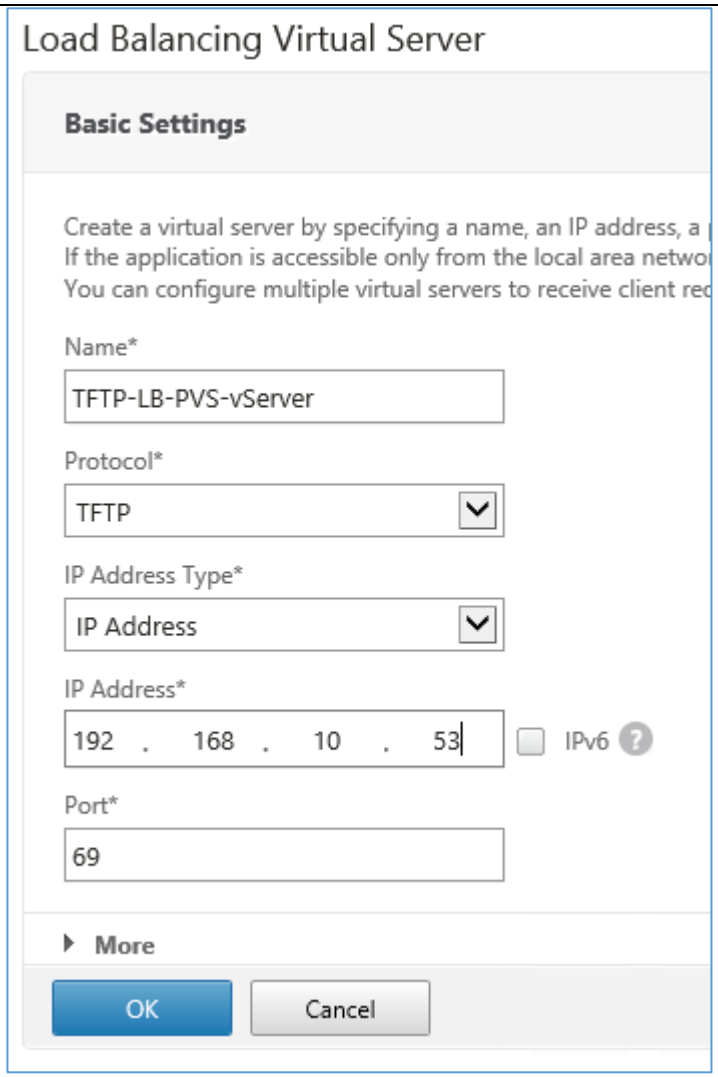
24. Click **Add Binding**.



Click **Click to select.**

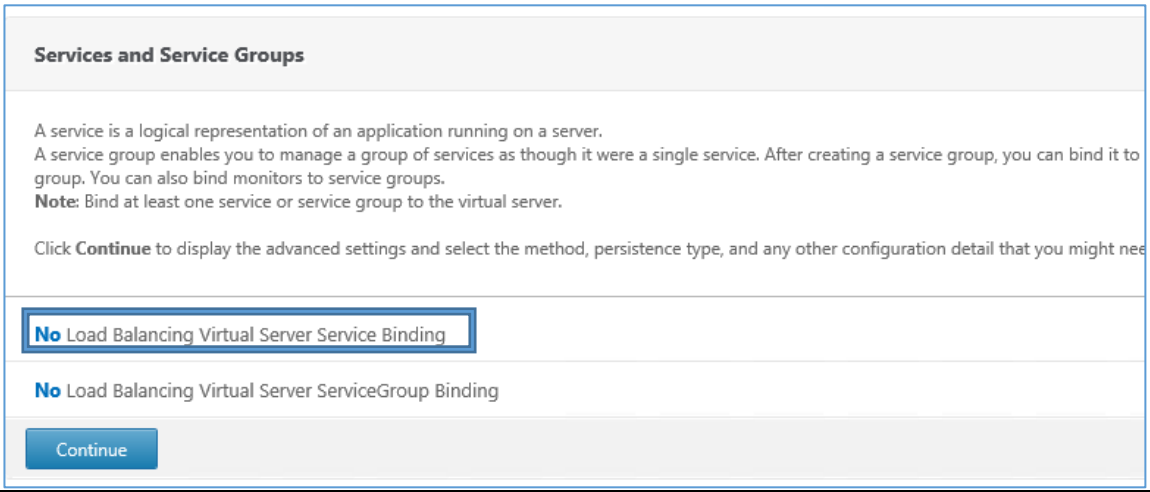
	 To create a service for **NYC-PVS-002** attach the **TFTP-Monitor-NYC-PVS-002** monitor created earlier to this service.
25.	Select **TFTP-Monitor-NYC-PVS-002**. Scroll up and click **Select**.  And click **Bind**.
26.	The TFTP monitor probes **NYC-PVS-002** over UDP port 69. Click **Close.** Scroll down and click **Done**. 
27.	Once both services are created, the services now appear in the Services view, with the State for both Up.

	
28.	Navigate to **Traffic Management > Load Balancing > Virtual Servers > Add**. 
29.	In the Name field, type **TFTP-LB-PVS-vServer**. Set the protocol using the Protocol drop-down menu and select **TFTP**. Verify the IP AddressType drop-down menu is set to **IP Address**. In the IP Address field, type **192.168.10.53**. In the Port field, type **69**.

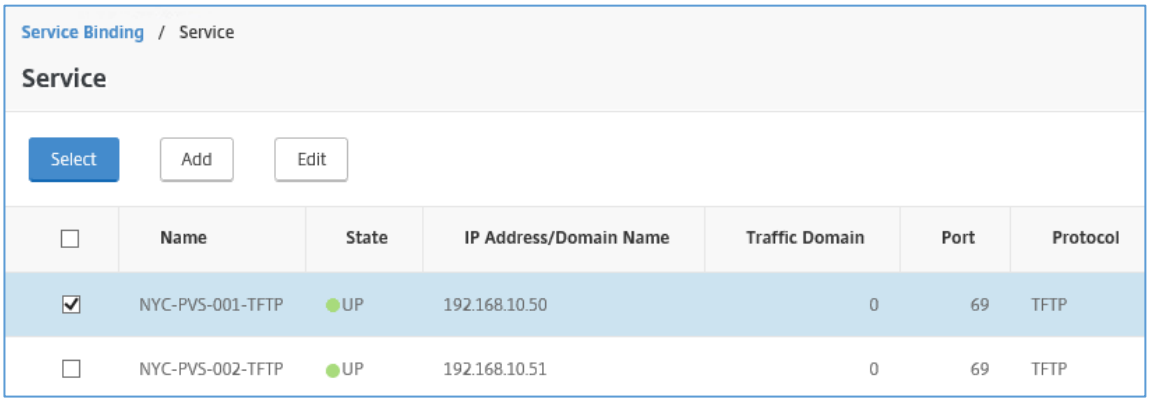


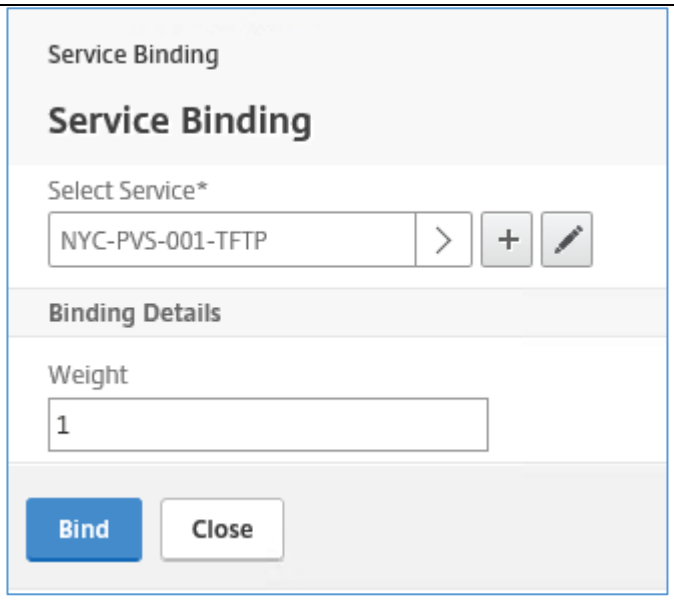
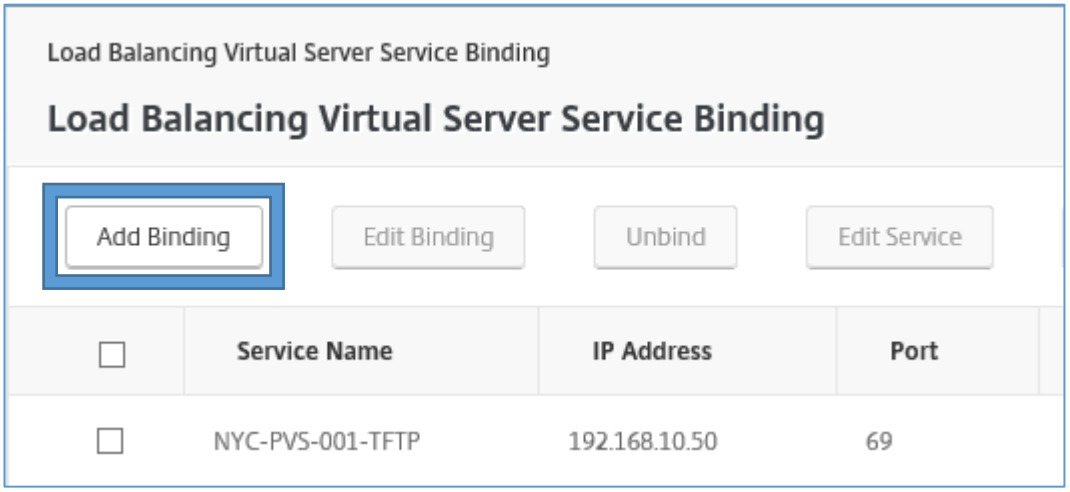
Click **OK**.

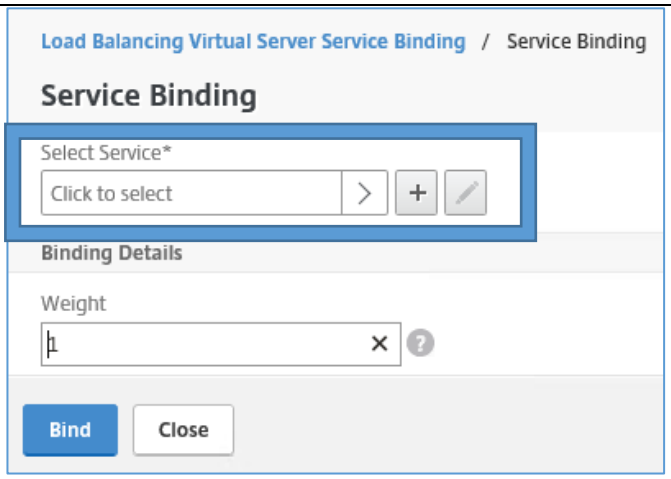
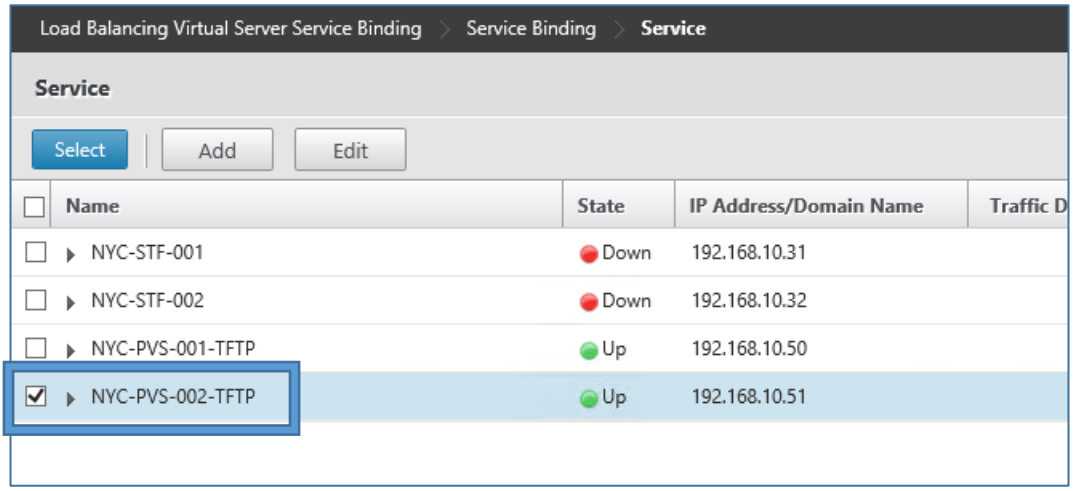
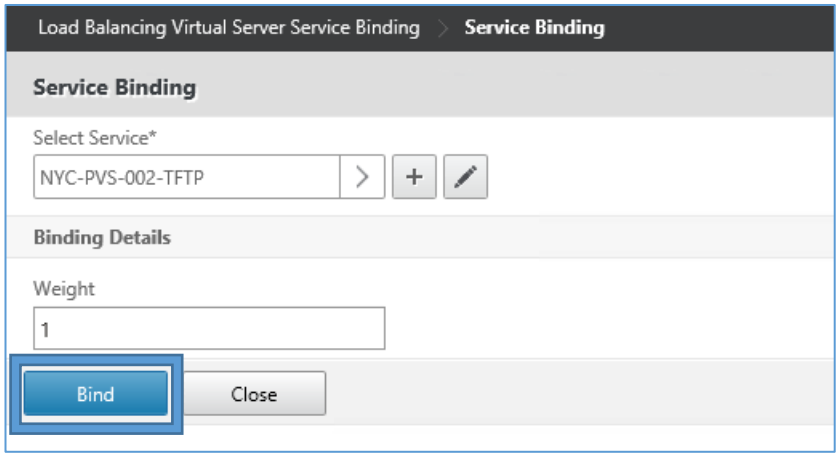
30. Scroll down and click on **No Load Balancing Virtual Server Service Binding**.

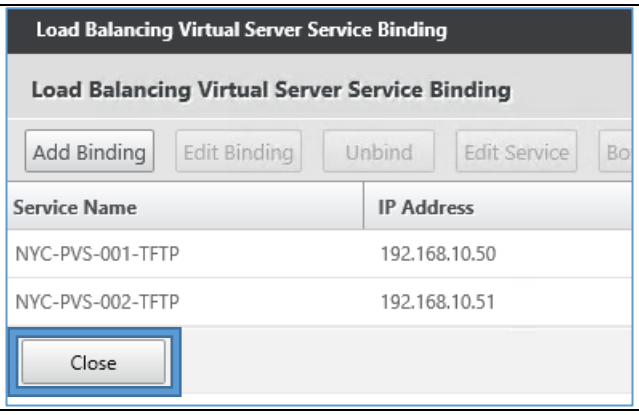


31. Click **Click to Select**.

32.	Select **NYC-PVS-001-FTP** service and click **Select**. 
33.	Click **Bind**.

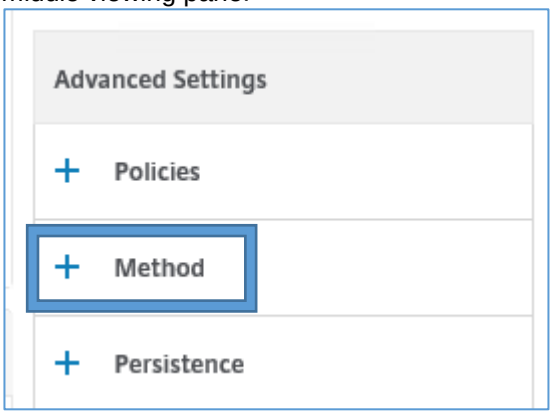
	
34.	Now click on **1 Load Balancing Virtual Server Service Binding**.
35.	On the **Load Balancing Virtual Server Service Binding** page, click **Add Binding**. 
36.	On the **Service Binding** option, click on **Click to select**.

	
37.	Check **NYC-PVS-002-TFTP** and click **Select**. 
38.	Click on **Bind**. 
39.	On the **Load Balancing Virtual Server Service Binding** option, click **Close**.

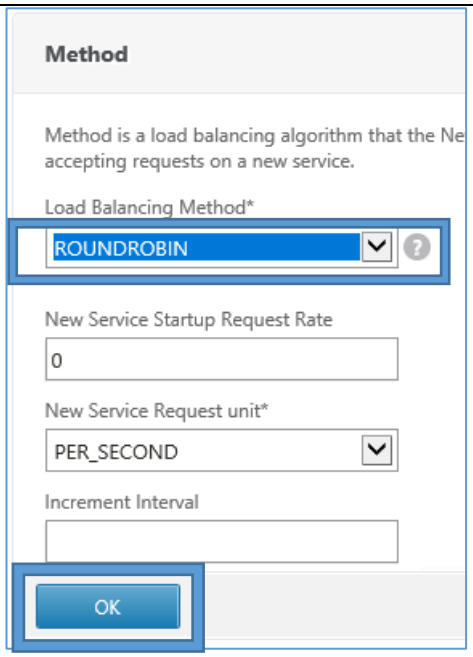


40. Click **Continue**.

41. Click on the **Method** box under **Advanced Settings** in the right pane to expand it out to the middle viewing pane.

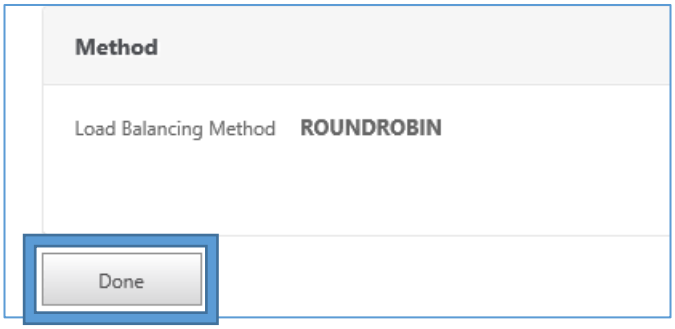


42. Under **Method**, set the **Load Balancing Method** using the drop-down menu and select **ROUNDROBIN**.

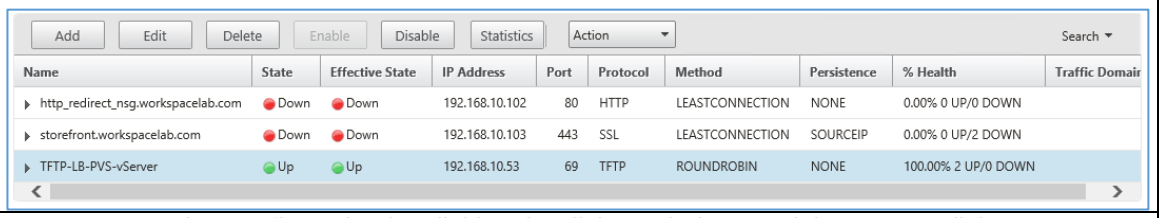


Click **OK**.

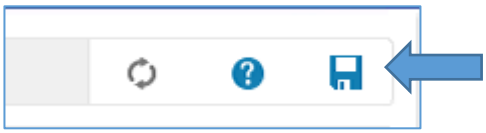
43. Scroll down and click **Done**.

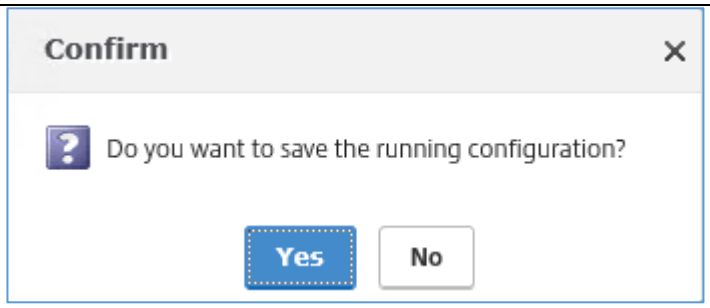


44. Verify the vServer appears in the up state.



45. Save your running configuration by clicking the disk symbol at top right corner. Click **Yes** to save the settings.





Log out from the NetScaler console.

Note: To complete the TFTP Load Balancing configuration, the newly created vServer must be specified in the DHCP options 66 and 67. However do not do this as we will be powering off the NetScaler in the upcoming lab module.

Option Name	Vendor	Value	Policy Name
066 Boot Server Host Name	Standard	192.168.10.53	None
067 Bootfile Name	Standard	ardbp32.bin	None

Key Takeaways:

- When using DHCP to supply the address of the TFTP server, only one host can be added in the DHCP options.
- NetScaler can be used to host a virtual server that load balances incoming TFTP requests and monitors the state of the TFTP services before forwarding the requests to one of the available TFTP servers.

Module 21: Supporting PVS

Overview:

The module presents several core management tasks that are performed within a Provisioning Services environment, including:

- Updating, promoting, rolling back, and merging vDisks by using versioning.
- Implementing delegated administration
- Enabling and using Provisioning Services auditing
- Using an alternative vDisk update method

Becoming familiar with these operations will assist you with maintaining and healthy and secure Provisioning Services environment after the initial installation and configuration has been completed.

Before you begin:

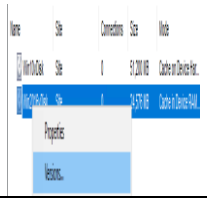
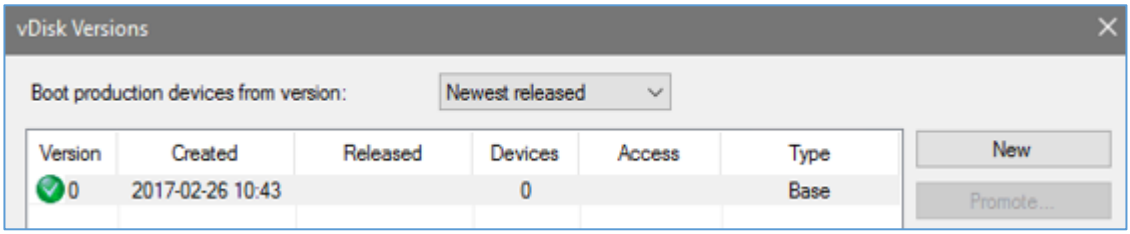
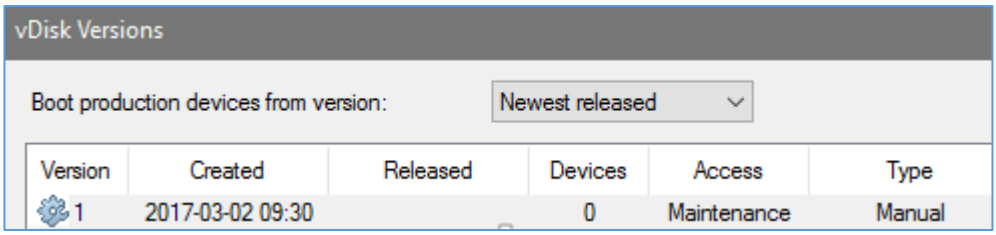
Estimated time to complete Module 21 lab exercises: 60 minutes

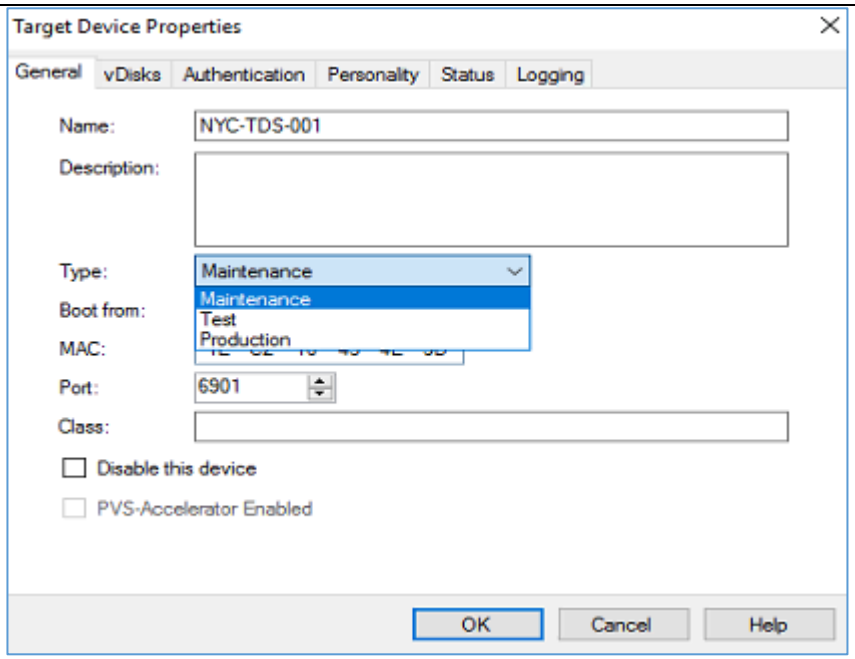
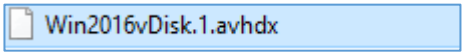
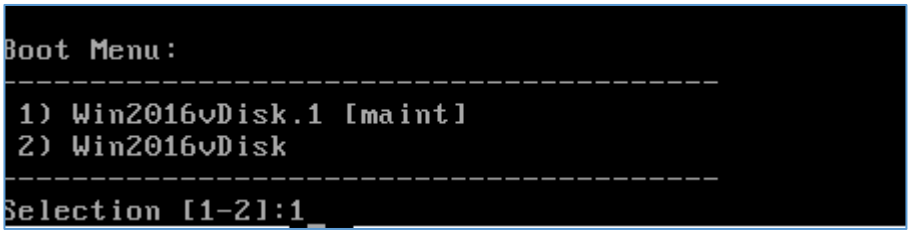
Exercise 21-1: Update the vDisk

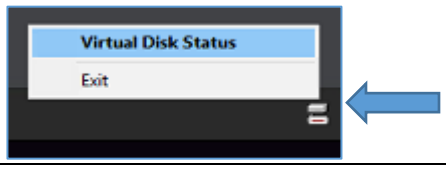
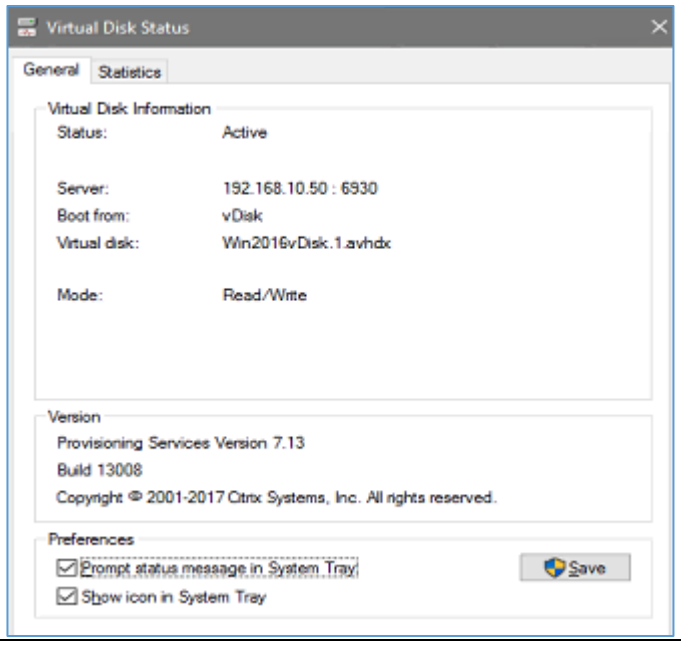
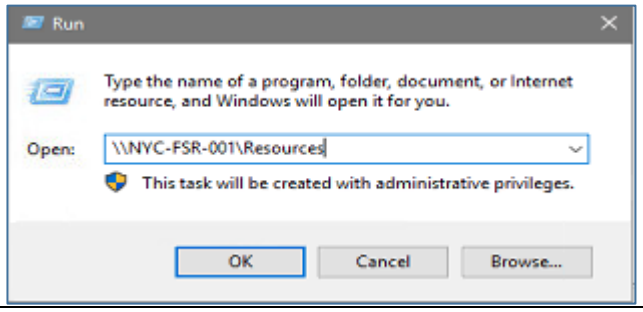
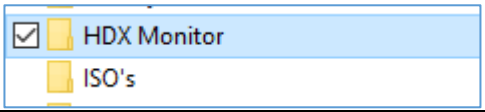
Scenario:

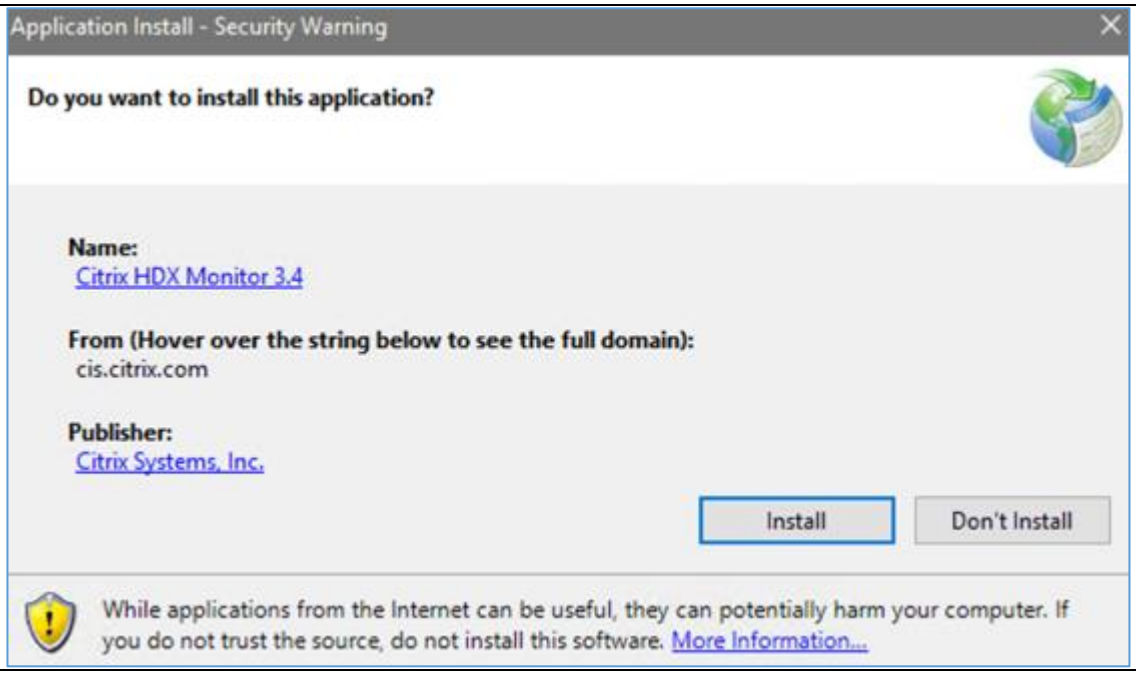
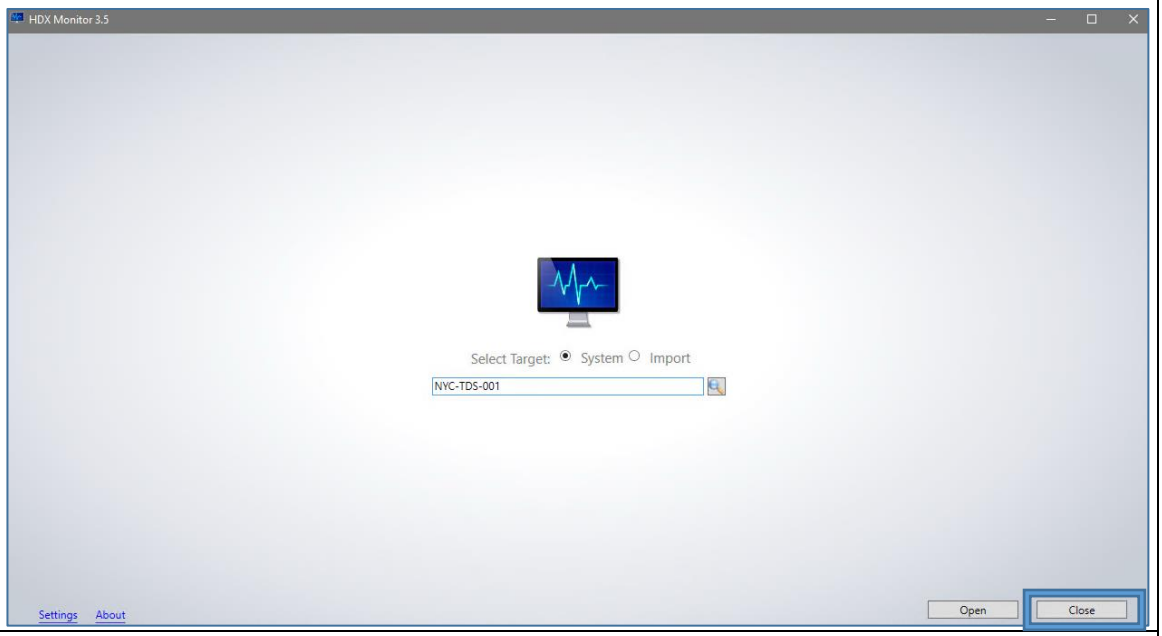
You are a Citrix Administrator at WW Labs, your Lead Citrix Architect has instructed you to install Citrix HDX Monitor on the Windows Server 2016 vDisk. You decide to use the versioning method to implement this change so that the test users can complete user acceptance testing, without delaying the project schedule.

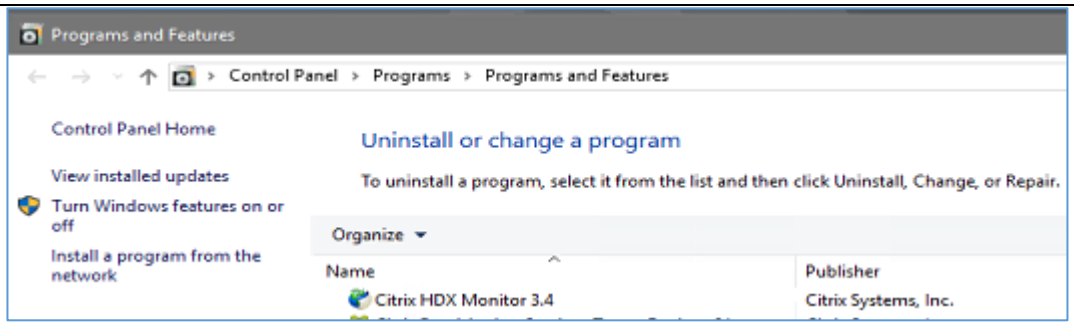
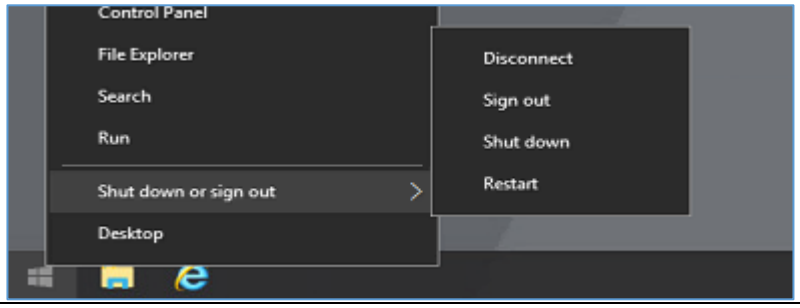
Step	Action
1.	The following VMs are required before beginning the exercises for this Module; all others may be powered down. To power manage your VMs, switch to XenCenter, right-click on the VM in the left pane and select Start or Shut Down. If prompted click Yes. • NYC-ADS-001 • NYC-SQL-001 • NYC-FSR-001 • NYC-PVS-001 • NYC-PVS-002 **Note**: These above VMs are listed in the start-up order.
2.	Using the Remote Desktop Connection manager, confirm you are still connected to **NYC-PVS-001**. **Note:** In a previous exercise, you had logged into **NYC-PVS-001** using the following credentials to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the Password. **Note**: If your Remote Desktop Connection session is disconnected, log on to **NYC-PVS-001**, right-click this machine and choose **Connect server**.
3.	Click **Start** and click **Provisioning Services Console**. Type **Localhost** and click **Connect**.

	Note: If the console is already open from the previous exercises ignore this step.
4.	Browse **Farm > Sites > Stores > VDiskStore** in the left pane.
5.	Select **Win2016vDisk** in the right pane. Right-click and select **Versions**. 
6.	Click **New** on the **vDisk Versions** screen. 
7.	Verify the new version gets created in **Maintenance Mode (Read/Write Mode)**. 
8.	Click **Done**.
9.	Expand **Device Collections > NYC-CAT-PVS-ServerOS** in left pane and select **NYC-TDS-001** in right pane.
10.	Right-click **NYC-TDS-001** and select **Properties**.
11.	In the **Type** drop-down menu select **Maintenance**.

	 Click **OK**.
12.	Using the Remote Desktop Connection manager, connect to **NYC-FSR-001**. To login to **NYC-FSR-001** right-click this machine and choose **Connect server**. **Note:** The following credentials are used to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the Password.
13.	Browse to **E:\Shares\vDiskStore** and verify that an **.avhdx** file was created.  **Note:** This file is the differential disk that gets created when creating a maintenance version using the Provisioning Services console; it contains the new changes that will be performed.
14.	Connect to XenCenter, select **NYC-TDS-001** and click **Start**.
15.	Click the **Console** tab in right pane and observe the machine boot progress. With the newly created maintenance version, the machine presented a Boot Menu to choose which vDisk version to boot from. Type **1** and press Enter to boot from the **Maintenance** version.  Monitor the machine until it finishes the boot process.
16.	Using the Remote Desktop Connection manager, connect to **NYC-TDS-001**. To login to **NYC-TDS-001** right-click this machine and choose **Connect server**.

	Note: The following credentials are used to make the connection: User name: **WORKSPACELAB\ Administrator** with **Password1** as the password.
17.	Right-click the **vDisk status tray** icon in right corner of the task bar and select **Virtual Disk Status**. 
18.	Verify the Mode says **Read/Write Mode** and the Virtual disk lists **Win2016vDisk.1.avhdx** and then close the window by clicking **X** at the top right corner. 
19.	Right-click **Start** and select **Run**.
20.	Type **\\NYC-FSR-001\Resources** and click **OK**. 
21.	Double-click the **HDX Monitor** folder. 
22.	Double-click **Setup.exe** and click **Install**.

	
23.	Click **Close** at the bottom right corner after installation completes. 
24.	Close the **File Explorer**.
25.	Right-click **Start** and select **Programs and Features** and verify **Citrix HDX Monitor 3.4** is installed.

	 Close the **Programs and Features** window.
26.	Right-click **Start**, select **Shut Down or sign out > Shut Down**. 

Key Takeaways:

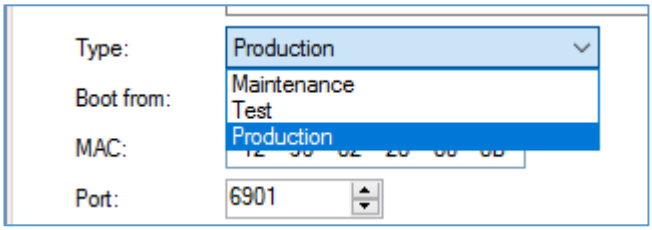
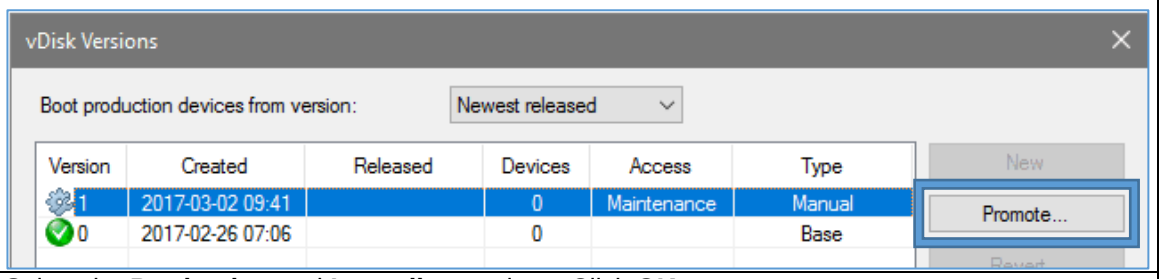
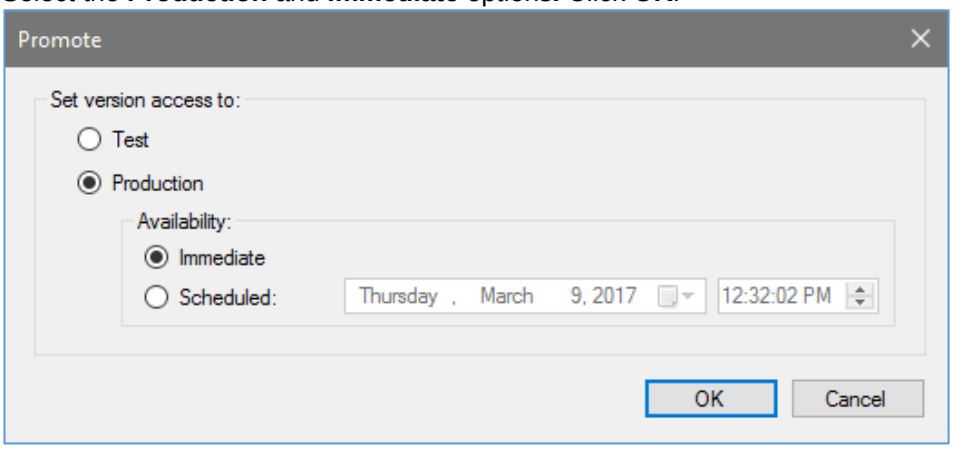
- Even when a vDisk is set to standard mode, we have a way to retain settings and changes; this method is called versions.
- Versions can be used to create delta vDisks linked to a base vDisk. The functionality works almost like snapshots in a hypervisor environment.
- A version or a delta vDisk is called aVHDx when looking browsing the store with a file explorer.
- A version can have 3 states: Maintenance which will allow changes, Test which will not retain changes but can be deployed to a limited set of Target Devices, and Production which is typically used when the changes has been made.
- Target Devices can also be linked to these 3 types of vDisks, meaning a Target Device can be configured to only boot from a certain type of vDisk.
- Only one vDisk version can be in maintenance mode at one time.

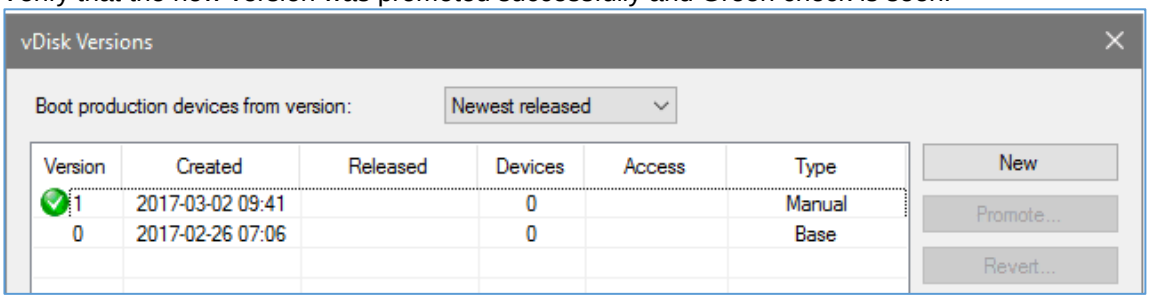
Exercise 21-2: Promote the vDisk

Scenario:

You are a Citrix Administrator at WW Labs, after adding the HDX Monitor to a new vDisk version, your Lead Citrix Architect has informed you that the user acceptance testing has completed, and you can promote the updated vDisk version to the target devices.

Step	Action
1.	Using the Remote Desktop Connection manager, confirm you are still connected to **NYC-PVS-001**.

	Note: In a previous exercise, you had logged into **NYC-PVS-001** using the following credentials to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the Password. **Note**: If your Remote Desktop Connection session is disconnected, log on to **NYC-PVS-001**, right-click this machine and choose **Connect server**.
2.	Click **Start** and launch the **Provisioning Services Console**. Type **Localhost** and click **Connect**. **Note:** If the console is already open from the previous exercises, ignore this step.
3.	Browse **Farm > Sites > NYC-Site > Device Collections**.
4.	Expand **Device Collections > NYC-CAT-PVS-ServerOS** in left pane and select **NYC-TDS-001** in the right pane.
5.	Right-click **NYC-TDS-001** and select **Properties**.
6.	Select drop-down next to **Type** and change from Maintenance to **Production**.  Click **OK**.
7.	Select **vDisk Pool** in the left pane and select **Win2016vDisk** in the right pane.
8.	Right-click **Win2016vDisk** and select **Versions**.
9.	Select the version in Maintenance mode and then click **Promote**. 
10.	Select the **Production** and **Immediate** options**.** Click **OK**. 

	Note: It may take some time to change the version from Maintenance to Production. The scheduled option can be selected to schedule when a maintenance vDisk version should be moved into production as per needed to comply with change control windows. **Note**: If a Snap-In Error appears, click Cancel. If the Provisioning Services Console closes, re-open again to verify that the new version has been promoted.
11.	Verify that the new version was promoted successfully and Green check is seen.  **Note:** Now all the target devices booting from this version will have the HDX Monitor software installed, proving that the vDisk was successfully updated.
12.	Click **Done**.

Key Takeaways:

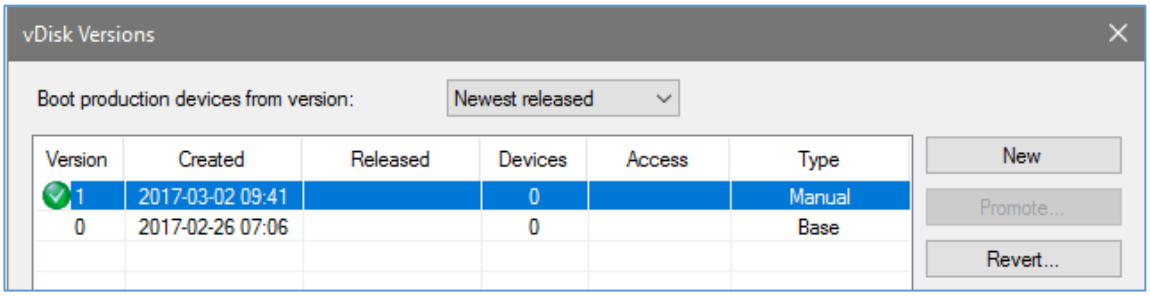
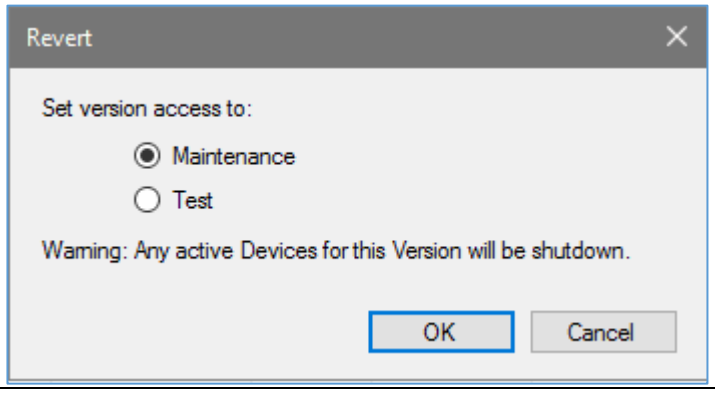
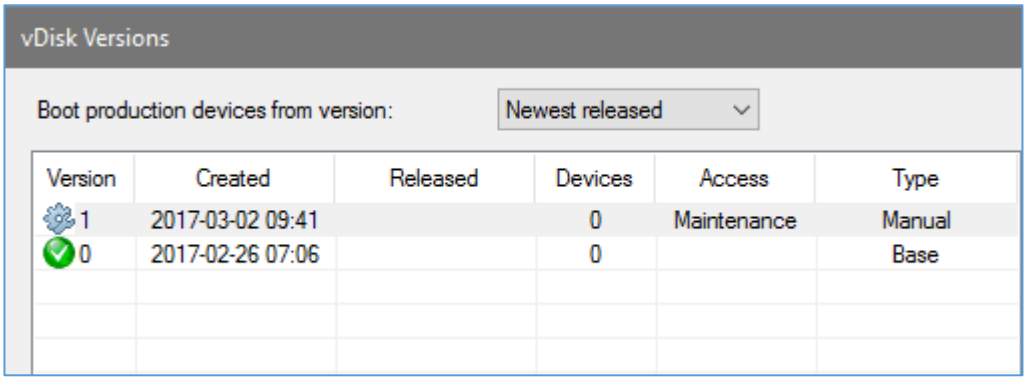
- It is always good to promote a vDisk to Test first and then to Production.
- Promote a vDisk directly to Production if you are confident that your updates won't cause any problems.
- Selecting Immediate while promoting a vDisk will not take effect until the Target Devices are rebooted.
- For Scheduled Promotion, the Target Devices must be rebooted after the scheduled date and time.

Exercise 21-3: Rollback the vDisk

Scenario:

You are a Citrix Administrator at WW Labs, your Lead Citrix Architect has instructed to test and verify the steps involved in rolling back a vDisk update. Your task is to ensure that the vDisk version containing HDX Monitor is no longer in production.

Step	Action
1.	Using the Remote Desktop Connection manager, confirm you are still connected to **NYC-PVS-001**. **Note:** In a previous exercise, you had logged into **NYC-PVS-001** using the following credentials to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the Password. **Note**: If your Remote Desktop Connection session is disconnected, log on to **NYC-PVS-001**, right-click this machine and choose **Connect server**.
2.	Click **Start** and launch **Provisioning Services Console**. Type **Localhost** and click **Connect**. **Note:** If the console is already open from the previous exercises, ignore this step.

3.	Browse **Farm > Sites > NYC-Site > vDisk Pool** in left pane and select **Win2016vDisk** in the right pane. **Note:** Make sure that the vDisk does not show a lock. The lock indicates there is a target device booted from the vDisk; shut down the target device and the lock will disappear. If there is no target device booting from the vDisk, right-click vDisk and select Mange Locks and Remove Locks.
4.	Right-click **Win2016vDisk** and select **Versions**.
5.	Select **Version 1** that we recently created and select **Revert**. 
6.	Select **Maintenance** and click **OK** to revert the version back to Maintenance mode to modify the changes previously made. 
7.	Verify **Maintenance** is again seen on the vDisk Versions screen to indicate the action revert is successful.  **Note:** The Production version is now reverted to **Maintenance** and if required, more changes can be done before promoting again.
8.	Click **Done**.

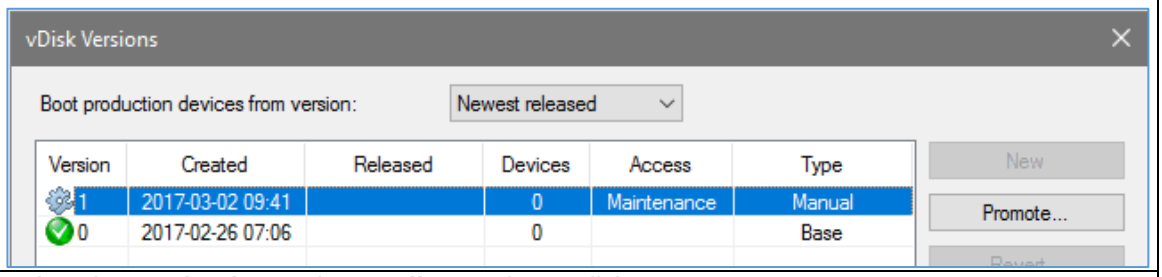
Key Takeaways:

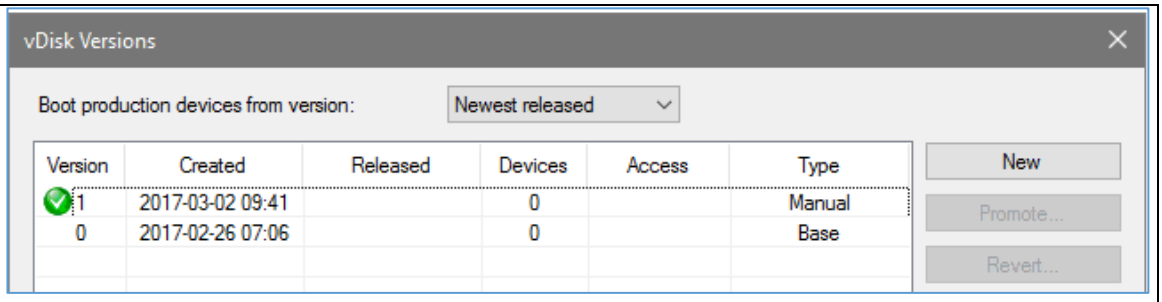
- An important benefit from using vDisks with Provisioning Services is the ability to quickly rollback a change.
- A vDisk can be rolled back to either Maintenance or Test mode.
- Changing the vDisk version back to Maintenance mode can only be done when the vDisk version is not in use.

Exercise 21-4: Merge the vDisk

Scenario:

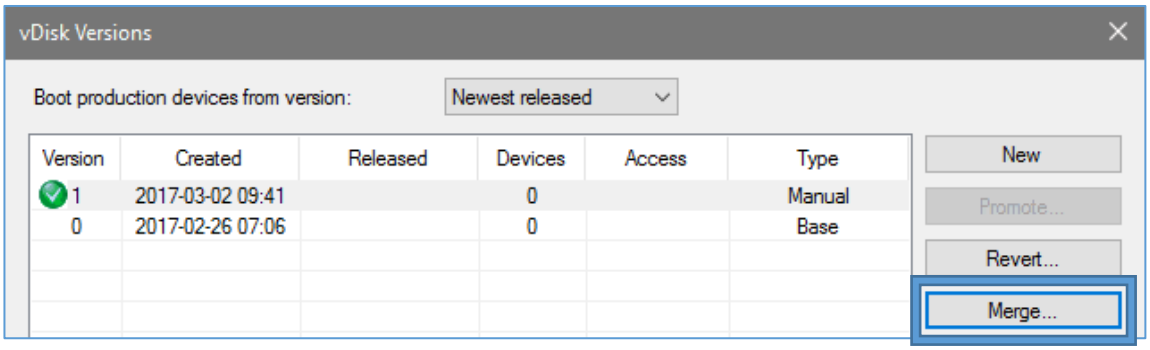
You are a Citrix Administrator at WW Labs, your Lead Citrix Architect has instructed you to merge the new vDisk version that was created to the base vDisk. That way, the new merged vDisk can be copied to a production file server in preparation for the production rollout.

Step	Action
1.	Using the Remote Desktop Connection manager, confirm you are still connected to **NYC-PVS-001**. **Note:** In a previous exercise, you had logged into **NYC-PVS-001** using the following credentials to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the Password. **Note**: If your Remote Desktop Connection session is disconnected, log on to **NYC-PVS-001**, right-click this machine and choose **Connect server**.
2.	Click **Start** and launch **Provisioning Services** console. Type **Localhost** and Click **Connect**. **Note:** If the console is already open from the previous exercises, ignore this step.
3.	Select the **vDisk Pool** in left pane and select **Win2016vDisk** in the right pane.
4.	Right-click **Win2016vDisk** and select **Versions**.
5.	Select the version in **Maintenance** mode and then click **Promote**. 
6.	Select the **Production** and **Immediate** options. Click **OK**. **Note:** If a Snap-In Error appears, click End Now-> click OK on Provisioning Servcies console , unhandled Exception messages and close the Provisioning Services console. Reopen the provisioning services console and connect to farm using localhost.
7.	Verify the new Version is promoted successfully and that the Green check is seen.



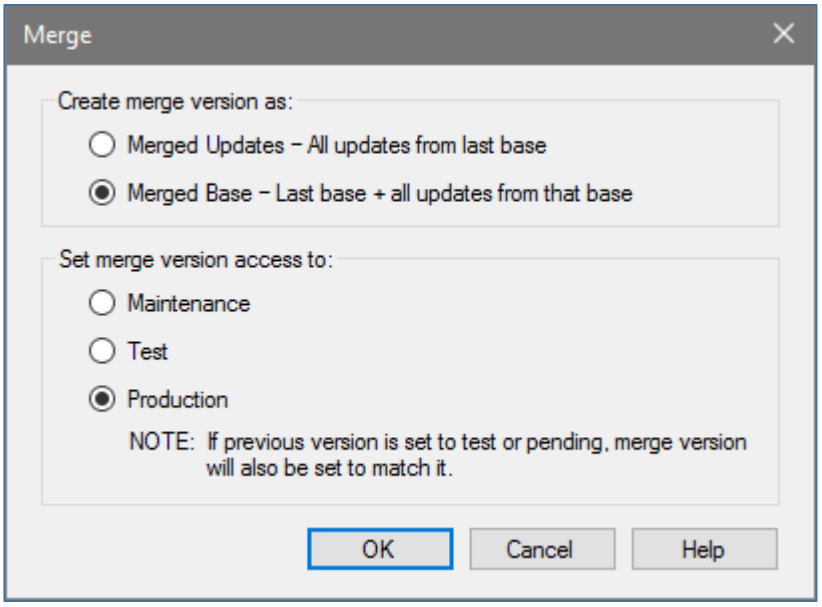
Note: If a Snap-In Error appears, click Cancel. If the Provisioning Services Console closes, re-open again to verify that the new version has been promoted.

8. Click **Merge**.



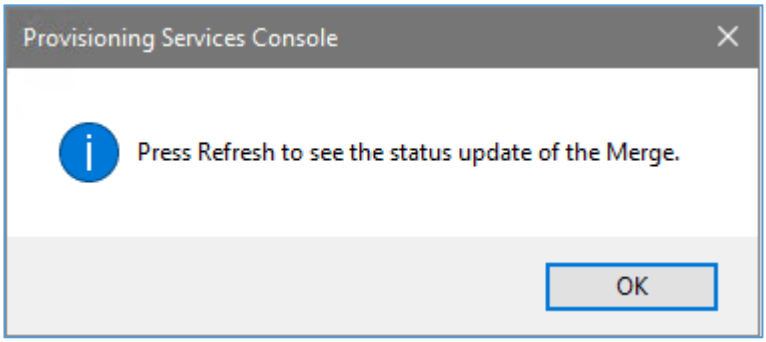
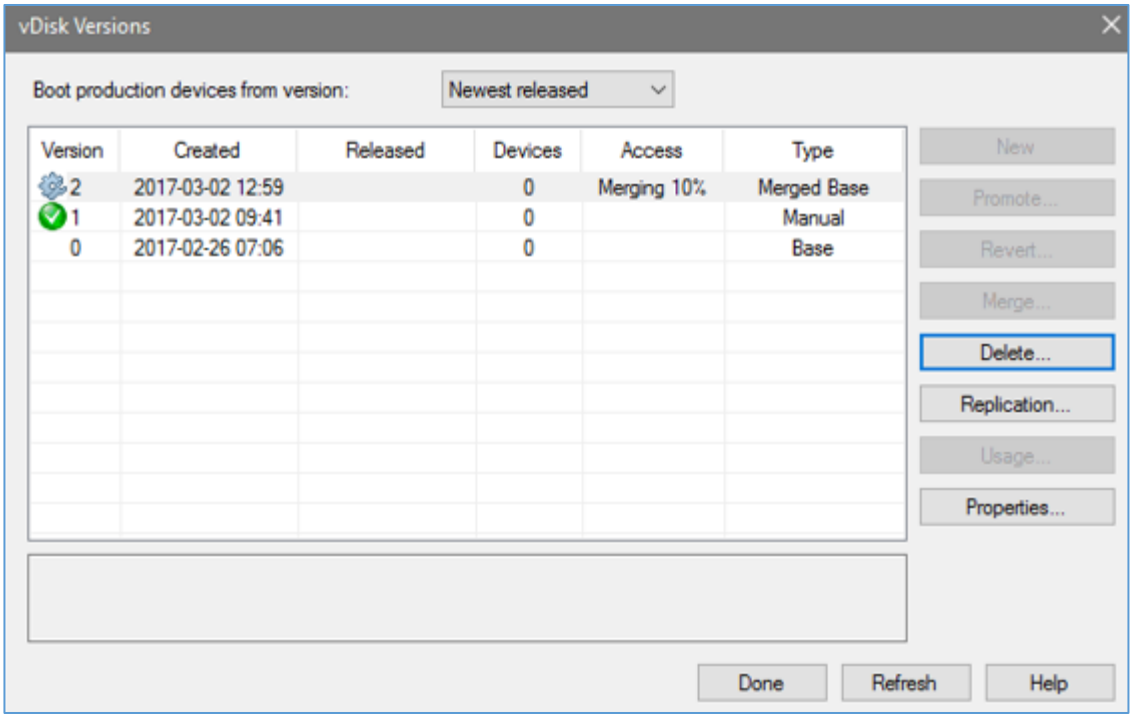
Note: If you receive any snap-in error, please click on **Cancel**.

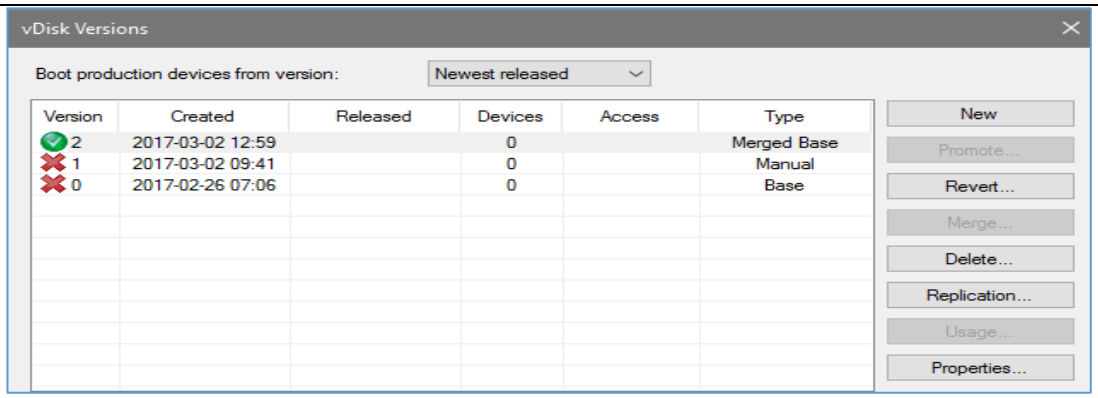
9. Select the **Merged Base – Last base + all updates from that base** and **Production** options.



Click **OK**.

Note: Using the Merged Base option, it will merge all the versions with the base vDisk into one base vDisk (.vhdx). If the Merged Updates option was chosen, it would merge all the versions into one consolidated version (.avhdx), keeping the base vDisk intact.

10.	Click **OK** on the **Provisioning Service Console** message and observe the **Merging %** under the Access column.   Continue to click the **Refresh** button every few seconds to observe the merging percentage changing. **Note:** The merge process will take approximately 5-10 minutes to complete.
11.	Once the merge is complete, the new base vDisk is created, the old versions and the old vDisk are marked with red X.

	 Click **Done**.
12.	The Merged Base process created a new .vhdx file. Connect to **NYC-FSR-001** using Remote Desktop Connection Manager. Browse to **E:\Shares\vDiskStore** and verify the new base disk is present now.
13.	Close the **File Explorer**.

Key Takeaways:

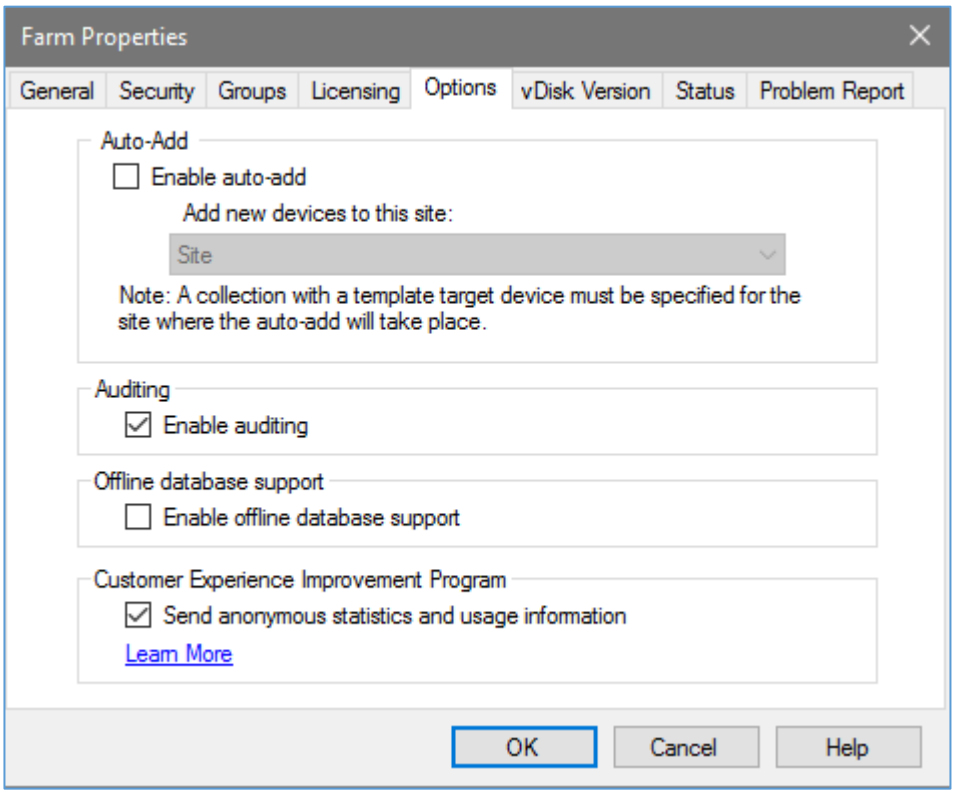
- Using vDisk versions is useful when deploying changes to an environment; however, as the chain if version grows, performance might start degrading. Citrix recommends keeping the number of versions below 5.
- The Merge functionality is used to reduce the number of active versions of a vDisk.
- A chain of vDisk versions can be merged to either a single version associated with the base vDisk, or all vDisk versions plus the base vDisk can be merged in to a new base vDisk.
- Merging to a complete base vDisk is useful when moving images between Provisioning Services environments since a vDisk chain cannot be imported.

Exercise 21-5: Enable Provisioning Service Auditing

Scenario:

You are a Citrix Administrator at WW Labs. The WW Labs CTO has announced new security guidelines for all IT systems: administrative changes must be logged and be available for review after any high severity incident. Your Lead Citrix Architect has tasked you to enable Auditing within the POC environment to show that Provisioning Services can meet this requirement.

Step	Action
1.	Using the Remote Desktop Connection manager, confirm you are still connected to **NYC-PVS-001**. **Note:** In a previous exercise, you had logged into **NYC-PVS-001** using the following credentials to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the Password.

	Note: If your Remote Desktop Connection session is disconnected, log on to **NYC-PVS-001**, right-click this machine and choose **Connect server**.
2.	Click **Start** and launch **Provisioning Services Console**. Type **Localhost** and click **Connect**.
3.	In the Console tree, right-click on the **Farm**, then select the **Properties** menu option. On the **Options** tab, under **Auditing**, check the **Enable auditing** check box.  Click **OK**. **Note:** If the Provisioning Services database is unavailable, no actions are recorded. The following managed objects within a Provisioning Services implementation are audited: • Farm • Site • Provisioning Servers • Collection • Device • Store • vDisks Only tasks performed from one of the following Provisioning Services utilities are recorded: • Console • MCLI • SOAP Server • PowerShell

Key Takeaways:

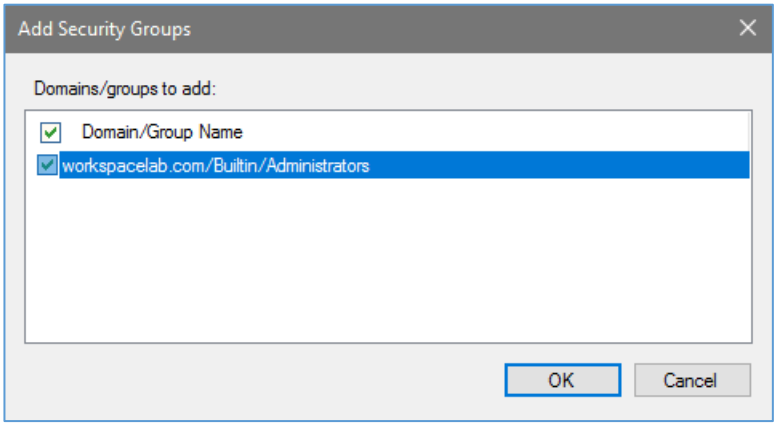
- In Provisioning Services, administrative auditing is not enabled by default.

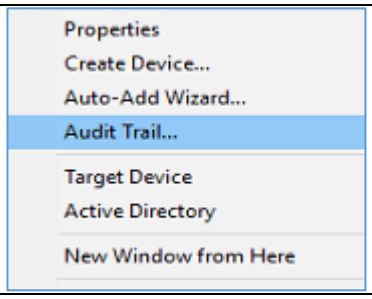
- Auditing is enabled within Farm properties.
- Audit events are saved in the Provisioning Services database.
- Audit events will not be tracked if the Provisioning Services database is offline.
- Auditing will track any change made through the Console, MCLI, PowerShell or using the SOAP Server.

Exercise 21-6: Use the Console to view Auditing

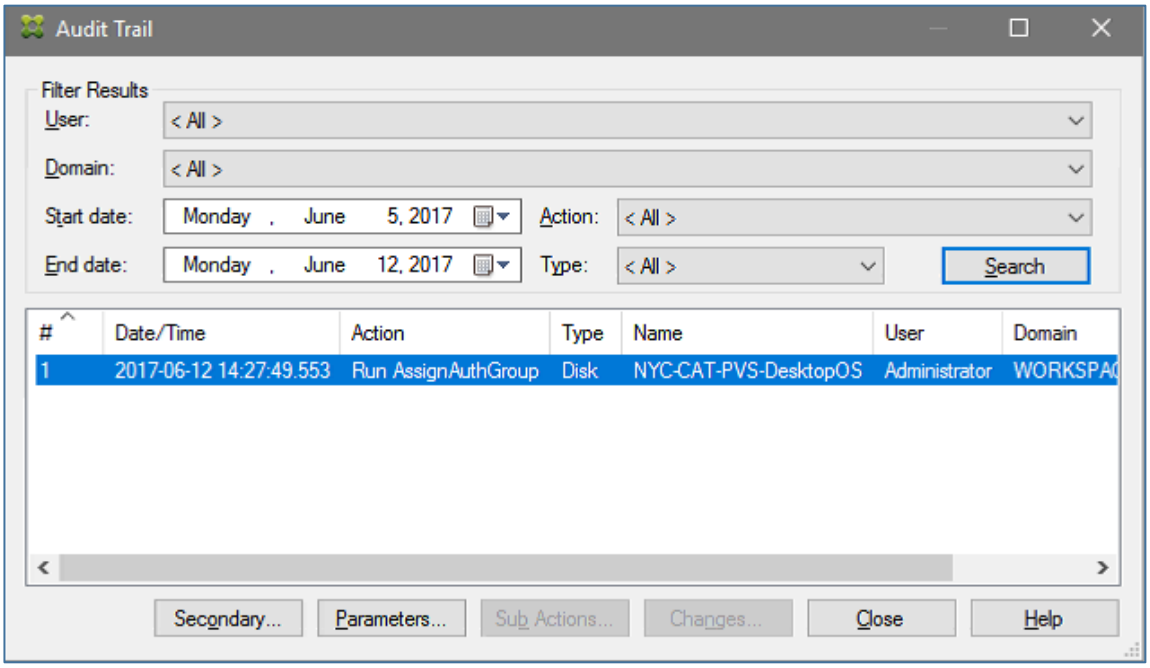
Scenario:

You are a Citrix Administrator at WW Labs, your Lead Citrix Architect has instructed you to prove that the auditing feature works. Your task is to open the audit trail for the Desktop OS Device Collection.

Step	Action
1.	Using the Remote Desktop Connection manager, confirm you are still connected to **NYC-PVS-001**. **Note:** In a previous exercise, you had logged into **NYC-PVS-001** using the following credentials to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the Password. **Note**: If your Remote Desktop Connection session is disconnected, log on to **NYC-PVS-001**, right-click this machine and choose **Connect server**.
2.	Click **Start** and launch **Provisioning Services Console**. Type **Localhost** and click **Connect**. **Note:** If the console is already open from the previous exercises, ignore this step.
3.	Browse **Farm > Sites > NYC-Site > Device Collections > Desktop OS Collection**.
4.	Right-click the **Desktop OS Collection** and select **Properties**. Select the **Security** tab. Click **Add** in the left pane.
5.	Select **Workspacelab.com/Builtin/Administrators** and click **OK** on Add Security Groups window.  **Note:** With auditing enabled in the previous exercise, a few administrative actions must be performed to generate entries in the audit trail.
6.	Click **OK**.
7.	Right-click the **Desktop OS Collection** and select **Audit trail**.



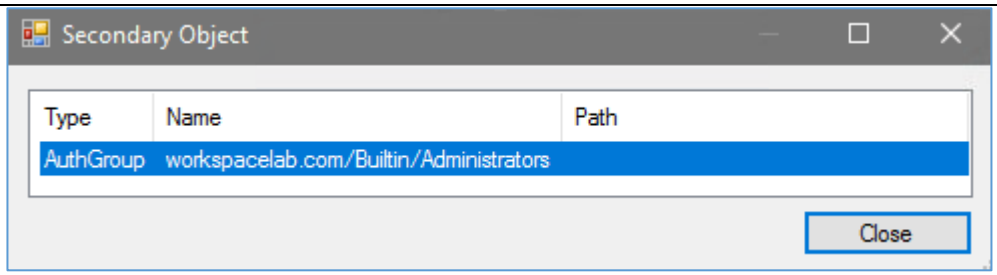
8. Notice the action just performed, adding the Administrator group in **Desktop OS Collection** Security, can be seen in the audit trail.



Note: Columns can be sorted in ascending and descending order by clicking on the column heading.

- The list # specifies the order the actions took place.
- The list Date/Time lists all audit actions that occurred within the Start date and End date filter criteria.
- The list Action identifies the name of the Provisioning Services action taken.
- The list Type identifies the type of action taken, which is based on the type of managed object for which the action was taken.
- The list Name identifies the name of the object within that object's type, for which the action was taken.
- The list User identifies the user's name that performed the action.
- The list Domain identifies the domain in which this user is a member.
- The list Path identifies the parent(s) or the managed object. For example, a Device will have a Site and Collection as parents.

9. Click **Secondary** tab and look at the changes that have just been made.

	 Click **Close** twice.

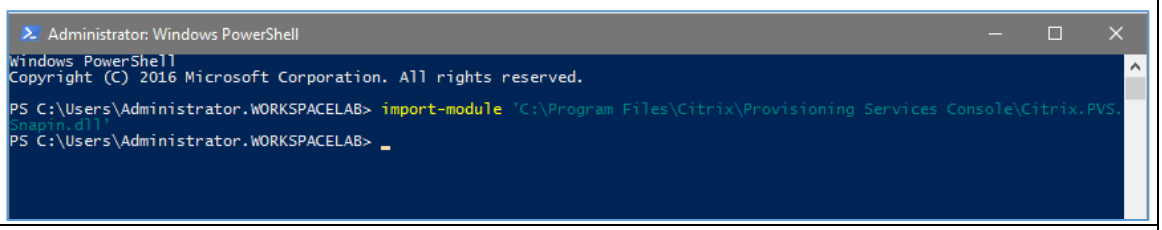
Key Takeaways:

- The audit log can be viewed by right-clicking an object and selecting Audit Trail.
- The Audit Trail window will allow you filter the result in many ways, making it easier to find relevant information.
- A search functionality is available to quickly find relevant events.

Exercise 21-7: Use PowerShell to view Auditing

Scenario:

The Citrix Architect is interested in potentially integrating Provisioning Services auditing with a 3rd party product that aggregates auditing data from different systems. The Architect asks your team to become familiar with the PowerShell programmer utility to retrieve auditing data in preparation to working with a developer involved with this effort.

Step	Action
1.	Using the Remote Desktop Connection manager, confirm you are still connected to **NYC-PVS-001**. **Note:** In a previous exercise, you had logged into **NYC-PVS-001** using the following credentials to make the connection: User name: **WORKSPACELAB\Administrator** with **Password1** as the Password. **Note**: If your Remote Desktop Connection session is disconnected, log on to **NYC-PVS-001**, right-click this machine and choose **Connect server**.
2.	Launch **PowerShel**l from the Task bar.
3.	Type the command below to import PVS PowerShell Snap-in: **import-module 'C:\Program Files\Citrix\Provisioning Services Console\Citrix.PVS.Snapin.dll'** 
4.	Type **Get-Module** to verify that the PVS Snap-in has been loaded.

```
PS C:\Users\Administrator.WORKSPACELAB> Get-Module

ModuleType Version    Name                                ExportedCommands
---------- -------    ----                                ----------------
Binary     7.13.0.... Citrix.PVS.Snapin                   {Clear-PvsConnection, Get-PvsADAccount,
```

5. To look at the audit trail of the device collection in which we made changes, type the following command:

   Get-PvsAuditTrail -SiteName NYC-site -CollectionName "Desktop OS Collection"

```
PS C:\Users\Administrator.WORKSPACELAB> Get-PvsAuditTrail -SiteName NYC-site -CollectionName "Desktop OS Collection"


AuditActionId : 7cbb223f-4334-49b9-a47f-f352c59e9c5f
Guid          : 7cbb223f-4334-49b9-a47f-f352c59e9c5f
Time          : 5/16/2017 2:58:52 AM
UserName      : Administrator
Domain        : WORKSPACELAB
Type          : 4
Action        : 2005
ObjectId      : 6309f4b4-ddfd-4136-a7e3-e8efb893890e
ObjectName    : Desktop OS Collection
Path          : NYC-Site
SiteId        : a6cb4a86-566e-4e58-823a-1480f5e43ba3
SubId         : 00000000-0000-0000-0000-000000000000
ParentId      : 00000000-0000-0000-0000-000000000000
RootId        : 00000000-0000-0000-0000-000000000000
Attachments   : 6


PS C:\Users\Administrator.WORKSPACELAB>
```

   The listed UserName is Administrator who has performed Action 2005 on ObjectName Desktop OS Collection.

   Note: The name of the action taken is a number that is converted to a string for display. Action 2005 means **(RunAssignAuthGroup)**.

   To know about which action value corresponds to which String Value refer to the following URL:
   - **https://docs.citrix.com/content/dam/docs/en-us/provisioning-services/7-12/downloads/PvsSnapInCommands_7_12_v2.pdf?_ga=1.33543101.22984942.1488288174**

6. Close the **PowerShell window**.

Key Takeaways:

- The Audit Trail window will allow you filter the result in many ways, making it easier to find relevant information.
- A search functionality is available to quickly find relevant events.