Managing App and Desktop Solutions with Citrix XenDesktop 7

Citrix Course CXD-203-4I

Managing App and Desktop Solutions with Citrix XenDesktop 7

Citrix Course CXD-203-4I
November 2013
Version 4.0

Table of Contents

Notices

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

Citrix Systems, Inc.

851 West Cypress Creek Road

Fort Lauderdale, FL 33309 USA

http://www.citrix.com

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

Mark	Owner
Citrix®, Citrix Provisioning Services™, Citrix Receiver™, ®, ICA®, NetScaler®, XenCenter®, XenDesktop®, XenServer®	Citrix Systems, Inc.
Active Directory®, Hyper-V®, Microsoft®, SQL Server®, Windows PowerShell®, Windows Server®, Office®, App-V®	Microsoft
VMware®, vSphere®	VMware, Inc.
Vyatta®	Brocade

Other product and company names mentioned herein might be the service marks, trademarks or registered trademarks of their respective owners in the United States and other countries.

Credits

Instructional Designers	Jeremy Boehl, Orlando A. Martínez, John Spina
Lab Environment Developer:	Andrew Garfield, Evin Safdia
Graphic Artists:	Andres Mungarrieta, Joshua Jack, Tyler Fromma
Managers:	Gina Alesse, Nathan Jackson, Brad Moczik
Editor:	Kathryn Morris
Subject Matter Experts:	Rob Blincoe, Kimberly Ferrie, Allen Furmanski, Michael Korth, Cris Lau, Mark Simmons, Stacy Scott, Elisabeth Teixeira, Nick Thomas, Daniel Wipperfürth

Connect with Citrix Education

Become a part of the Citrix Education community today! Stay connected with us, get the latest updates on our offerings, and let us know how we are doing.

- Facebook - Become a fan of Citrix Education
- Twitter - Follow @CitrixEducation
- LinkedIn - Join the Citrix Education group

Visit *http://training.citrix.com*to find more information on training, certifications, and exams.

To submit feedback about this course use the following web form link:
https://podio.com/webforms/4962770/390059

Module 1

Understanding the Architecture of a XenDesktop Solution

1

Understanding the Architecture of a XenDesktop Solution

Citrix XenDesktop 7 delivers Windows applications and desktops as secure mobile services. With XenDesktop, IT can mobilize the business, while reducing costs by centralizing control and security for intellectual property. Users can self-select applications from an easy-to-use application store that is accessible from tablets, smartphones, PCs, Macs, and thin clients.

HDX technologies enable XenDesktop to deliver a user experience that is optimized for different user devices, as well as network conditions. XenDesktop is built on an architecture that offers simple, powerful configuration and operations management and cloud-style automation and scalability.

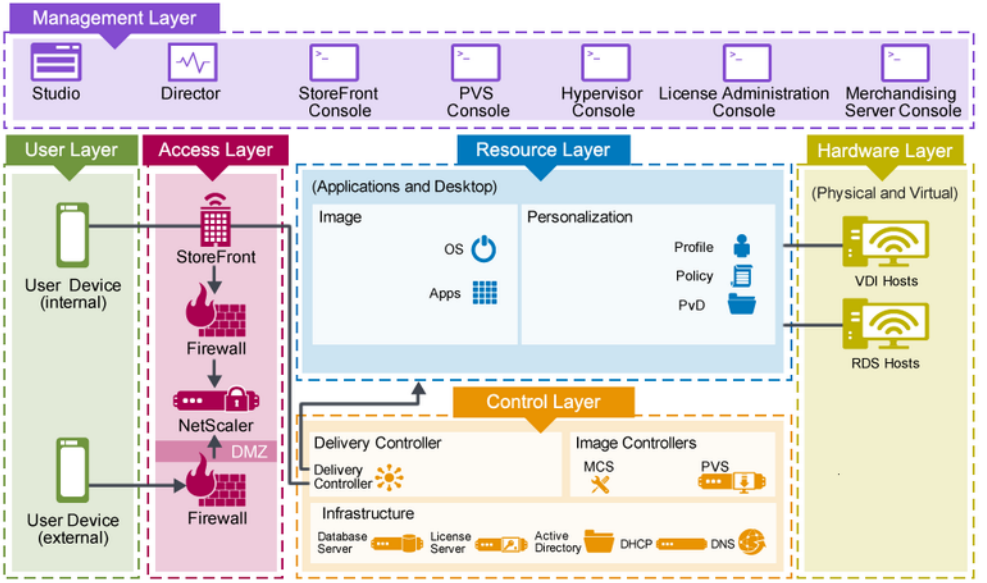
At the end of this module you will be able to:

- Identify the architecture and components of a XenDesktop 7 solution.
- Explain the role of:
  - Citrix Receiver
  - Citrix NetScaler
  - Citrix StoreFront
  - Delivery Controller
  - Machine Creation Services (MCS)
  - Citrix Provisioning Services (PVS)
  - Hypervisor
  - Virtual Delivery Agent (VDA)
  - Citrix Profile management
- Discuss the responsibilities of the different XenDesktop components.

Module timing: Approximately 2 hours

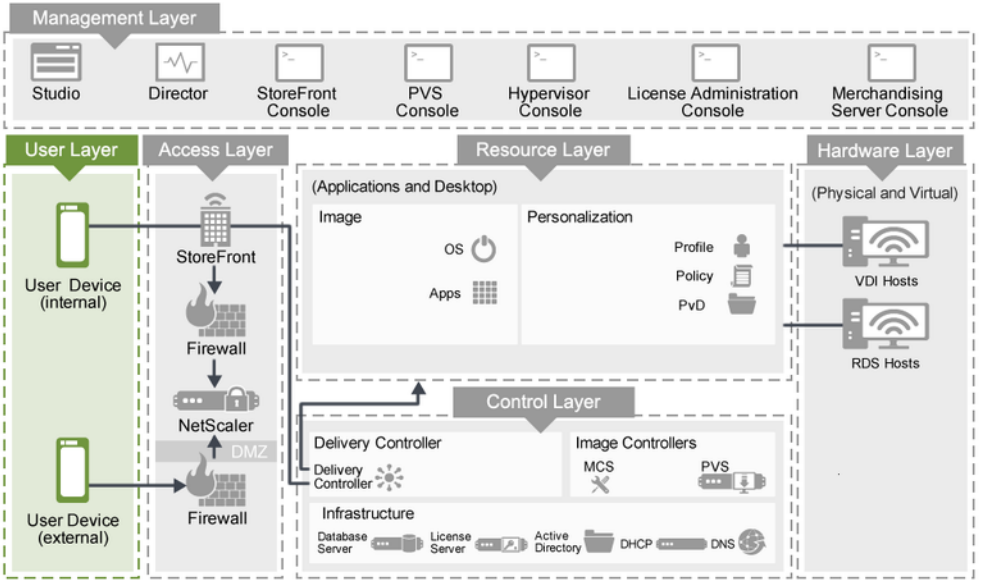
XenDesktop Architecture Overview

During this module we will explore the components that comprise a XenDesktop solution. The following diagram depicts a XenDesktop solution and the associated components.



User Layer

The user layer contains Citrix Receiver, regardless of whether the end user is connecting from an internal or external device.



Citrix Receiver

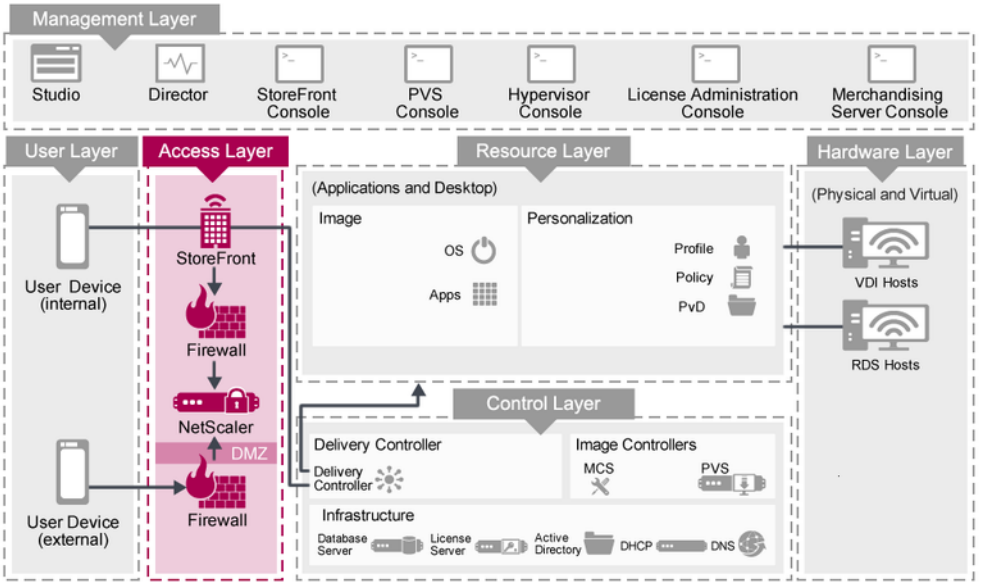
Installed on end-user devices, Citrix Receiver provides end users with quick, secure, self-service access to documents, applications, and desktops from any end-user device including smartphones, tablets, and PCs. Receiver provides on-demand access to Windows, Web, and Software as a Service (SaaS) applications.

Access Layer

The access layer contains the components that provide end-user access to the environment: Citrix NetScaler and StoreFront. The NetScaler provides secure access and intelligent load balancing for StoreFront, Delivery Controller, and related infrastructure.

Internal end-user devices connect from the user layer to the access layer using Citrix StoreFront.

In a Citrix-recommended implementation, external end-user devices connect first through Citrix NetScaler - and often a firewall and perimeter network - and then through StoreFront to access resources.



Citrix NetScaler

NetScaler is an integrated web application delivery controller that slashes server and bandwidth requirements, cutting the costs of delivering enterprise applications. NetScaler functions as an application accelerator through caching and HTTP compression. It also provides advanced management using layer-4 through layer-7 load balancing and content switching functions. NetScaler also includes application security using a web application firewall. NetScaler offloads applications and web servers to ensure application availability, increased security through SSL, and server consolidation. It reduces the cost of ownership of web application delivery and optimizes the end-user experience.

Citrix StoreFront

Citrix StoreFront delivers a powerful, self-service Windows applications store to provide a single, simple, and consistent aggregation point for all IT user services. Users may subscribe to applications, desktops, or data services from any device and have access to those services, even when already in use, from any other device for a seamless and simple experience.

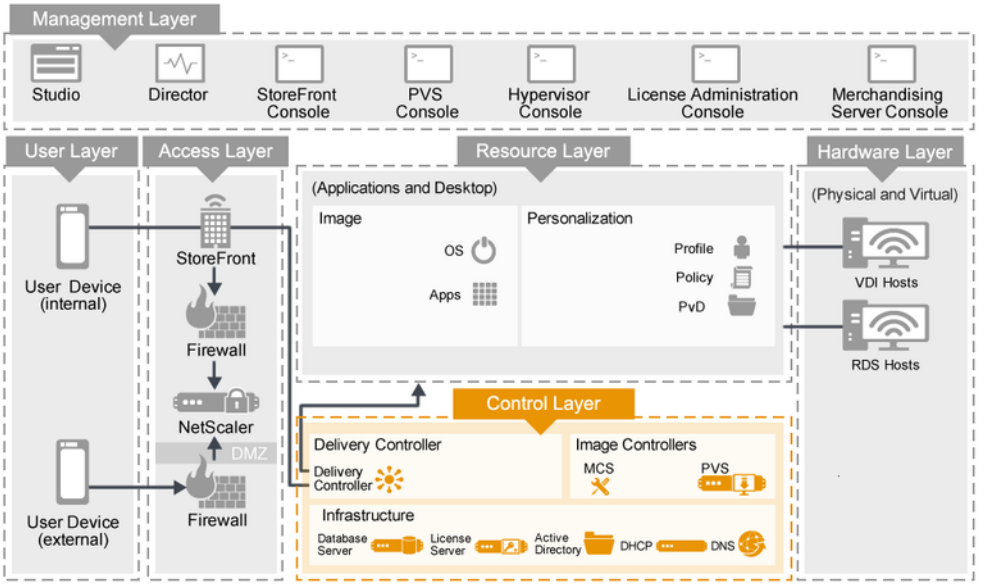
StoreFront requires 2 GB of memory. StoreFront 2.0 is the minimum version supported with XenDesktop 7. For more information about StoreFront requirements, see Citrix eDocs at *http://edocs.citrix.com*.

Discussion Question

What type of solution are you using for external access?

Control Layer

The control layer is home for the various controllers and infrastructure components required for managing and delivering virtual desktops. Within the control layer, decisions surrounding the management and maintenance of the overall solution are addressed. The control layer is comprised of access controllers, delivery controllers, and infrastructure controllers. Once a user connection moves past the access layer, Citrix StoreFront communicates with the Delivery Controller in the control layer.



Delivery Controller

Installed on servers in the datacenter, the Delivery Controller consists of services that communicate with the hypervisor to distribute applications and desktops, authenticate and manage end-user access, and broker connections between end users and their virtual desktops and applications. The Controller manages the state of the desktops, starting and stopping them based on demand and administrative configuration. Additionally, all XenDesktop 7 editions allow you to install profile management to manage end-user personalization settings in virtualized or physical Windows environments. Each site has one or more delivery controllers.

Supported operating systems for the Delivery Controller include:

- Windows Server 2012, Standard and Datacenter Editions.
- Windows Server 2008 R2 SP1, Standard, Enterprise, and Datacenter Editions.

Requirements for the Delivery Controller include:

- 100 MB of disk space.

- Microsoft .NET Framework 3.5 SP1 (required on Windows Server 2008 R2 only).
- Microsoft .NET 4.0.
- Windows PowerShell 2.0 or 3.0.
- Visual C++ 2005, 2008 SP1, and 2010 Redistributable packages. The installer deploys these automatically.

Machine Creation Services

Machine Creation Services (MCS) are a collection of services that run on the Delivery Controller to generate multiple clone-like machines from a single virtual machine serving as the primary image. The Machine Creation Service communicates with the hypervisor and creates the desired number of machines using storage-based snapshot technologies, while the Citrix AD Identity Service generates the computer accounts within Active Directory.

New to XenDesktop 7 is the ability of MCS to now generate server-based operating systems as well as desktops.

Citrix Provisioning Services

Citrix Provisioning Services uses network-based streaming technology to deliver the operating system for both single-user virtual-desktops and multi-user server-based resources. Citrix Provisioning Services allows a single vDisk to be used to deliver a consistent virtual desktop across the environment and to simplify image management and maintenance.

When using Provisioning Services with XenDesktop 7, the minimum supported Provisioning Services version is 7.0.

Hypervisor

A hypervisor is a thin layer of software that allows you to share physical resources of a device amongst multiple virtual machines. XenDesktop supports several hypervisors, including:

- Citrix XenServer
- Microsoft Hyper-V using Microsoft System Center Virtual Machine Manager (SCVMM)
- VMware ESX using VMware vCenter

After the authentication process is completed, the Delivery Controller contacts the Microsoft SQL database to discover the machines and applications available to the user.

These machines can be either physical or virtual. If the machines are virtual, then they reside within the hypervisor. Every machine physical or virtual must have the Virtual Delivery Agent installed.

Virtual Delivery Agent (VDA)

The Virtual Delivery Agent (VDA) must be installed on any server or workstation-based operating system that will be used to deliver applications or desktops to the user. The VDA enables connections for desktops and applications, installs special profile management and printing services, and extends the applicable group policy settings.

The VDA for Windows Desktop OS supports Windows 8 and Windows 7 SP1 machines.

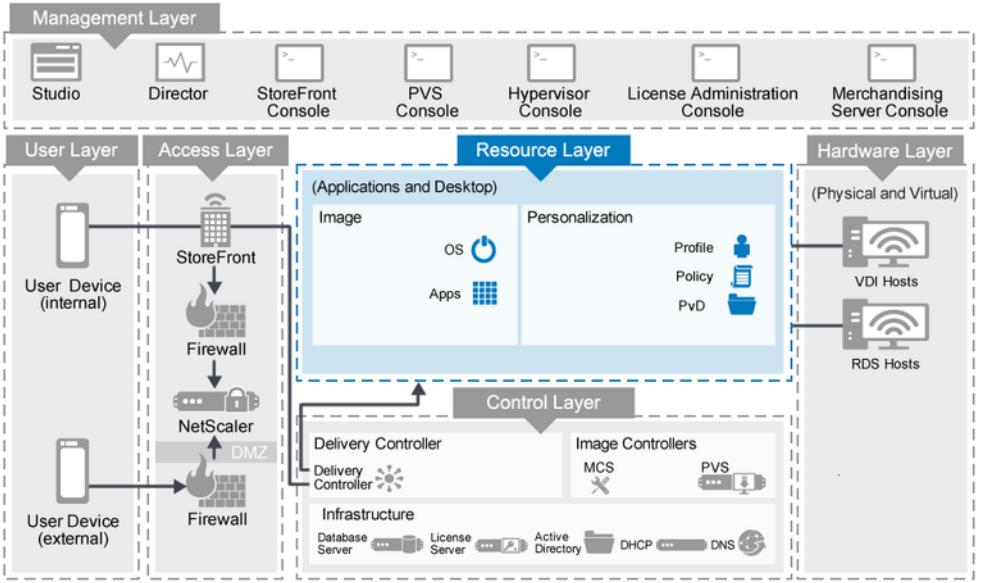
The VDA for Windows Server OS supports Windows 2012 and Windows 2008 R2 SP1 machines.

Discussion Question

What are the benefits of hosting virtual machines within a hypervisor as opposed to physical machines? What hypervisor does your organization use?

Resource Layer

The resource layer contains the end-user's virtual desktop and applications and is subdivided into three components: applications, operating system image, and personalization, which contain the user profile, policies, and personal vDisk.



Applications

You can choose to install applications on Server OS or Desktop OS machines in your XenDesktop environment in order to deliver them to end-user devices.

Operating System Image

Virtual desktop delivery with XenDesktop involves delivering an image of an operating system (such as Windows 7) to the end user.

Citrix Profile Management

Citrix Profile management provides an easy, reliable, and high-performance way to manage end-user personalization settings in virtualized or physical Windows environments. Citrix Profile management allows end users to customize their virtual and physical desktops, applications, and server settings. Managed through Citrix policies or GPOs, Profile management can provide a

central point of configuration and control to give a consistent experience regardless of which machine hosts the end-user session.

Policies

Citrix policies are the most efficient method of controlling connection, security, and bandwidth settings. You can create policies for specific groups of end users, devices, or connection types. Each policy can contain multiple settings and different settings from policies can be merged. Any conflicts between settings are resolved using a system of priorities.

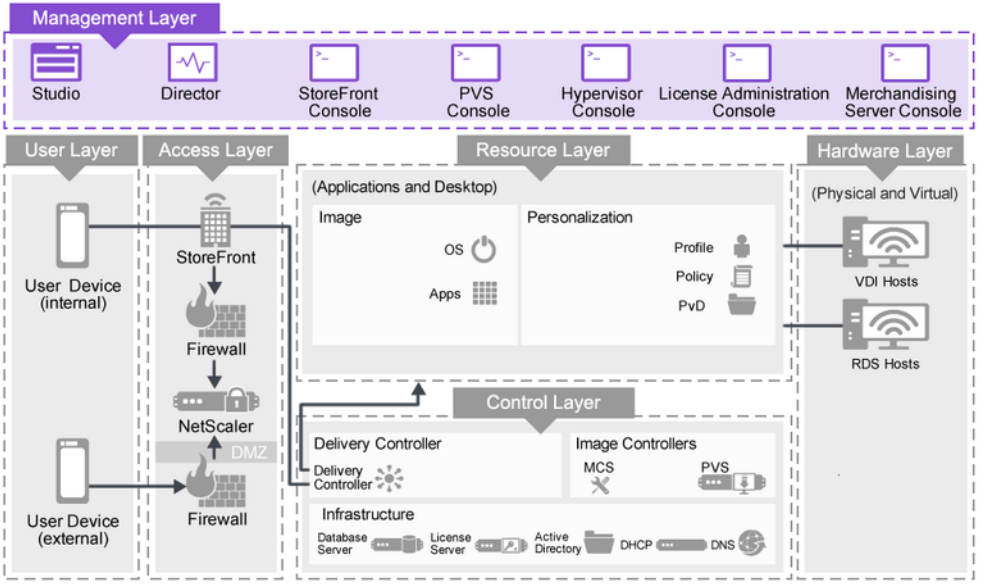
Personal vDisk

The personal vDisk feature in XenDesktop retains the single image management of pooled and streamed desktops while allowing people to install applications and change their desktop settings.

Management Layer

The management layer contains all of the consoles and utilities used to configure and manage the XenDesktop components including:

- Studio
- Director
- StoreFront Console
- Provisioning Services Console
- Hypervisor console
- License Administration Console
- Merchandising Server Console
- Optional third-party consoles



Citrix Studio

Citrix Studio is the management console that enables you to configure and manage your deployment, eliminating the need for separate management consoles for managing delivery of applications and desktops. Studio provides various wizards to guide you through the process of setting up your environment, creating your workloads to host applications and desktops, and assigning applications and desktops to end users.

Supported operating systems for Studio include:

- Windows 8 Professional and Enterprise Editions.
- Windows 7 Professional, Enterprise, and Ultimate Editions.
- Windows Server 2012, Standard and Datacenter Editions.
- Windows Server 2008 R2 SP1, Standard, Enterprise, and Datacenter Editions.

Requirements for Studio include:

- 75 MB of disk space.
- Microsoft .NET Framework 3.5 SP1 (required on Windows Server 2008 R2 only).
- Microsoft Management Console 3.0.
- Windows PowerShell 2.0 or 3.0.

Citrix Director

Citrix Director is a web-based tool that enables IT support and Help Desk teams to monitor a XenDesktop environment, troubleshoot issues before they become system critical, and perform support tasks for end users.

Supported operating systems for Director include:

- Windows Server 2012, Standard and Datacenter Editions.
- Windows Server 2008 R2 SP1, Standard, Enterprise, and Datacenter Editions.

Requirements for Director include:

- 50 MB of disk space.
- Microsoft .NET Framework 4.0.
- Microsoft Internet Information Services (IIS) 7.0 and ASP.NET 2.0. If these are not already installed, you are prompted for the Windows Server installation media, then they are installed for you.

Supported browsers for viewing Director include:

- Internet Explorer 9 and 10

Compatibility mode in Internet Explorer 10 is not supported.

- Firefox
- Chrome

Discussion Question

Which tools does your organization use (or plan to use) for monitoring your XenDesktop environment?

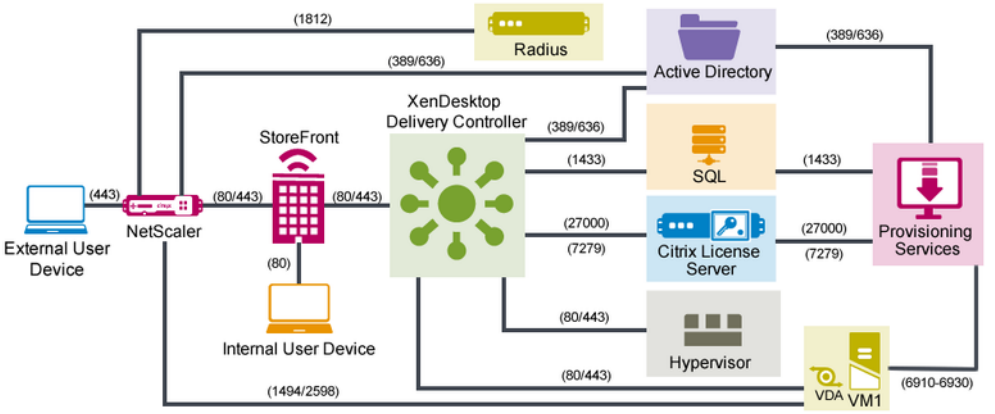
XenDesktop Site

A Site is the name you give to a product deployment. It comprises the controllers and the other core components and virtual delivery agents, host connections (if used), plus the machine catalogs and Delivery Groups you create and manage. A Site does not necessarily correspond to geographical location, although it can. The site is defined in a SQL database that needs to be available at all times to each Delivery Controller within the deployment.

Ports

The following is a summary of the ports used by the components we have discussed throughout this module.

For more information about the ports used in a XenDesktop environment, see Citrix article CTX101810 at *http://support.citrix.com*.



Reinforcement Exercise: XenDesktop 7 Components

In this module you learned how to:

- Identify the architecture and components of a XenDesktop 7 solution.
- Explain the role of:
  - Citrix Receiver
  - Citrix StoreFront
  - Citrix NetScaler
  - Delivery Controller
  - Machine Creation Services
  - Citrix Provisioning Services
  - Hypervisor
  - Virtual Delivery Agent
  - Citrix Profile management
- Describe the responsibilities of the different XenDesktop management consoles.

Directions: Match the term to its function within XenDesktop 7.

Time to complete: Approximately 5 minutes

Choices

A. Citrix Receiver	E. Citrix StoreFront	I. Citrix Provisioning Services
B. Citrix NetScaler	F. Delivery Controller	J. Machine Creation Services
C. Hypervisor	G. Virtual Delivery Agent	K. Citrix Profile management
D. Personal vDisk	H. Citrix Studio	L. Citrix Director

1. Provides end users with quick, secure, self-service access to documents, applications, and desktops from any end-user device.
2. A Web-based tool that enabled IT support to monitor a XenDesktop environment, troubleshoot issues, and perform support tasks for end users.
3. A management console that enables you to configure and manage your XenDesktop implementation.
4. A feature in XenDesktop that allows end users to install applications and change their desktop settings, while retaining the single image management of pooled and streamed desktops.

5. Allows you to manage end-user personalization settings in a virtualized or physical Windows environment.
6. A thin layer of software that allows you to share physical resources of a device amongst several virtual machines.
7. Enables virtual machines to register with a Delivery Controller.
8. Uses a vDisk image to provision virtual machines.
9. Communicates with the hypervisor to distribute applications and desktops, authenticates and manages end-user access, and brokers connections between end users and their virtual desktops and applications.
10. A collection of services that run on the Delivery Controller to generate clone-like machines from a single virtual machine serving as the primary image.
11. A self-service, Windows application store that provides a single aggregation point for all IT user services.
12. Functions as an application accelerator and also provides advanced management using load balancing, content switching, and application security.

Module 2

Managing Licenses and Delegating Administration

2

Managing Licenses and Delegating Administration

Citrix XenDesktop now offers four editions. Similar to previous releases of XenDesktop, this release includes Platinum, Enterprise, and VDI edition licenses that may be purchased as user or device, or concurrent licenses. In addition, XenDesktop now offers a new App edition license for all hosted shared application and desktop workloads.

Delegated administration in XenDesktop consists of administrators, roles, and scopes. Administrators are individual Active Directory users or groups. Each administrator can have one or more roles assigned. The role outlines the permissions granted to the administrator. Roles can be customized, which allows for a detailed view of specific actions and tasks that an administrator can complete within the Studio console. Scopes represent collections of objects such as Delivery Groups. Objects can belong to multiple scopes and administrators can be assigned to multiple scopes as well.

After completing this module you will be able to:

- Describe how Citrix Studio is used to manage licensing.
- Manage licensing.
- Manage delegated administration.
- Monitor configuration logs.
- Generate configuration log reports.

Module timing: Approximately 2.5 hours

Managing Licenses in Studio

Studio is the primary management console for XenDesktop that enables you to configure and manage your deployment, eliminating the need for separate management consoles for managing delivery of applications and desktops. Studio provides various wizards to guide you through the process of setting up your environment, creating your workloads to host applications and desktops, and assigning applications and desktops to end users. The console also includes PowerShell functionality. Most administration tasks can be completed within the console, while only some advanced configuration tasks require the explicit use of PowerShell.

The console can be used to configure machine catalogs, Delivery Groups, policies (including HDX policies), logging, administrators, delegated administration, licensing, and profile management.

You can use Studio to manage and track licensing, provided the license server is in the same domain as Studio, or in a trusted domain. You must possess full-administrative permissions on the licensing server to carry out the tasks described below, except for viewing license information. To only view license information, a XenDesktop administrator needs the read-only permission.

Discussion Question

Which licensing model are you currently using? What would you require in a XenDesktop environment? How would your licenses be consumed if you switched from named to concurrent?

Types of Licenses

XenDesktop offers four license editions:

- Platinum
- Enterprise
- Apps
- VDI

For more information about the features and entitlements of each edition, visit *https://www.citrix.com/go/products/xendesktop/feature-matrix*

Downloading, Allocating, and Importing a License File

Although you can use Studio for license administration, Citrix also provides a web-based License Administration Console. These consoles can be used interchangeably; however, the License Administration Console is used during the deployment of XenDesktop, prior to the installation of Studio. This exercise will show you an example of the License Administration Console.

To Access Your Exercise

1. Go to *http://training.citrix.com/voucher*.
2. Log on with your Citrix account. If you do not have a Citrix account, click **Create new account** to create a new one now.

For the registration process to work, or to retrieve a forgotten password, you will need to access your email address. Use your mobile device if necessary.

3. Type your voucher code and click **Redeem Voucher**.
4. Browse to the CXD-203 course to redeem your voucher and click **Redeem Voucher**. The course will be added to your My Training, where it will be available for launch.
5. Go to training.citrix.com > My Training.
6. Select **CXD-203**.
7. Select the **Resources** tab.
8. Click **CXD-203 Student Resources**.
9. Click **Launch**.
10. Navigate to the **Exercises** page.
11. Click the + next to Module 2.
12. Select **Downloading, Allocating, and Importing License Files.**

Once the exercise launches, use the following procedure to complete the exercise.

To Download, Allocate, and Import a License File

1. Open an Internet browser and go to *http://www.citrix.com*.

   The exercise will begin at *http://www.citrix.com*. Proceed to next step.

2. Click **My Account (Log In)**.
3. Click **Create Account**.
4. Click **Create Customer Account**.

5. Specify your information to create an account.

   Type your company information into the field.

6. Click **Continue** on page 1 of the registration.
7. Create a new Login ID and Password.

   Type **Admin1** as the Login ID and **Password1** as the password.

8. Click **Continue** on page 2 of the registration.
9. Click **Activate and Allocate Licenses**.
10. Click **Single Allocation**.
11. Type the license code.

    Type **CTXLF-12345-67890-12345-67890**.

12. Click **Continue** on the license code page.
13. Click **Continue** on the Host Name Warning page.
14. Type the case-sensitive Host ID.

    Type **LS-1**.

15. Type the license quantity.

    Type **5**.

16. Click **Continue** on the Configure page.
17. Verify that the information is correct and click **Confirm**.
18. Click **OK** within the dialog box.
19. Click **Save** on the download dialog box**.**
20. Select a location to save the license file.

    Leave as the default **Downloads** folder.

21. Click **Save** on the Save As window.
22. Click **Close** on the Download Complete window.
23. Click **Log Out**.
24. Close the browser window.
25. Click **Start** at the Windows desktop.
26. Type **Citrix License Administration** and press **Enter**.
27. Click **Citrix License Administration.**
28. Click **Administration** within the License Administration Console.

29. Log on as an administrator.

    Type **CCH\Admin1** as the User Name and **Password1** as the password and then click **Submit**.

30. Click **Vendor Daemon Configuration**.
31. Click **Import License**.
32. Click **Browse** and locate the recently downloaded license file.

    Select **FID_309f.lic**.

33. Click **Open**.
34. Click **Import License**.
35. Click **OK** upon completion.
36. Click **Dashboard**.
37. Click **Citrix XenDesktop Enterprise | Concurrent** to view the allocated licenses.
38. Close the License Administration Console browser window to complete the exercise.

The exercise is now complete.

Discussion Question

What are some of the different ways you can download, allocate, and monitor a Citrix license file?

Adding a License Administrator

The license server is pre-configured in the lab environment. To experience adding a license administrator, we have provided an Adding a License Administrator exercise in the Student Resource Kit for the CXD-203 Managing App and Desktop Solutions with Citrix XenDesktop 7 course. You will be able to use the steps in this course to complete the exercise in the Student Resource Kit.

Follow these steps to open the Adding a License Administrator exercise in the Student Resource Kit:

1. Go to page 4 of the Student Resource Kit.
2. Click the + sign to the left of the Module 2 heading.
3. Click **Adding a License Administrator** and then click the **Play** button.

To Add a License Administrator

1. Log on to your licensing server as an administrator.

   Proceed to the next step.

2. Click **Start** on the bottom left hand corner of Windows.
3. Type **Citrix License Administration** at the Windows Start screen and press **Enter**.
4. Click **Citrix License Administration** to open the license console.
5. Click **Administration** to log on.
6. Type your username and password and click **Submit**.

   Type **CCH\Admin1** into the User Name field and **Password1** into the password field and click **Submit**.

7. Click **User Configuration** and then click **New User**.
8. Select the role of the new user.

   Select **Domain Administrator**.

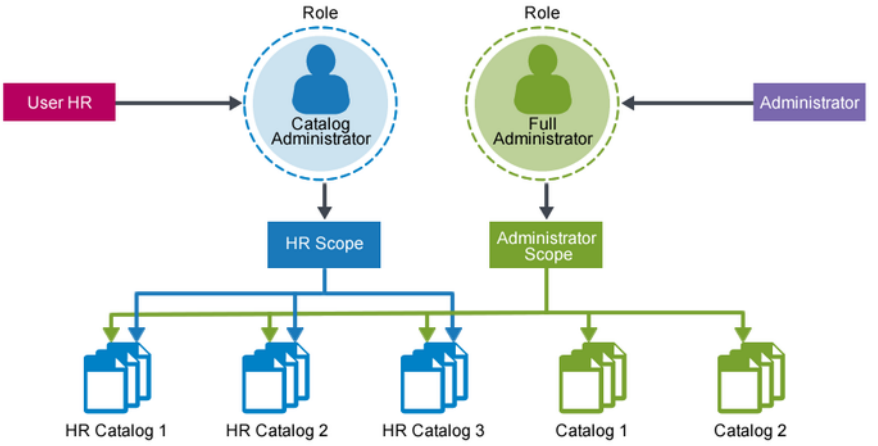
9. Specify the user name of the user you would like to add as a license administrator and click **Save**.

   Type **CCH\Admin2** and then click **Save**.

10. Click **Log Out**.

Managing Delegated Administration

The delegated administration model offers the flexibility to match how your organization wants to delegate administration activities, using role- and object-based control. Delegated administration accommodates deployments of all sizes and allows you to configure more permission detail as your deployment grows in complexity. Delegated administration uses three concepts: administrators, roles, and scopes.

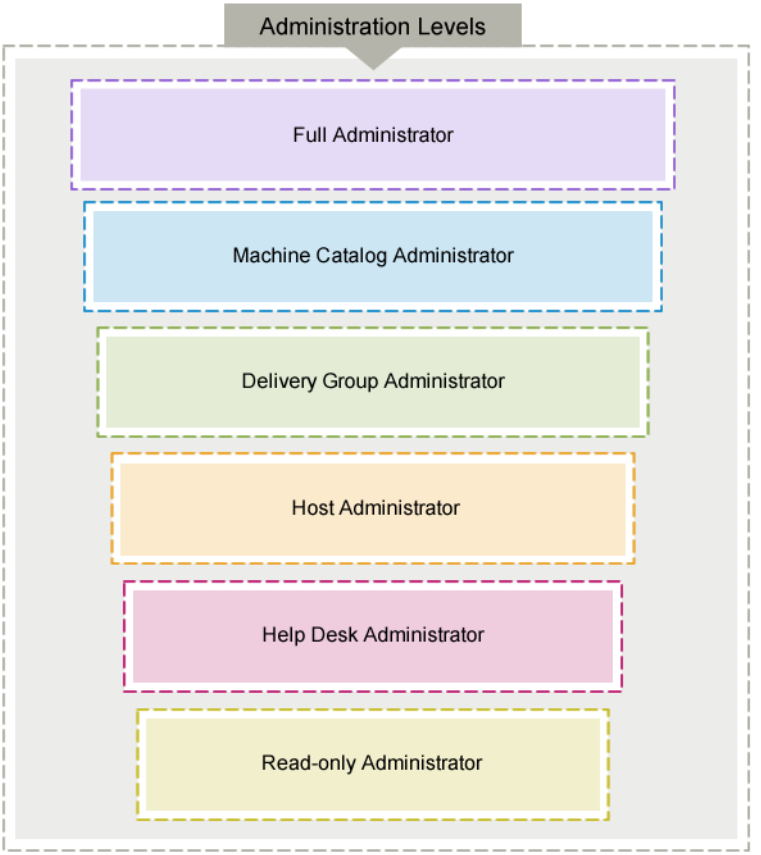


No specific Active Directory permissions are required for delegated administration. Standard domain users will work fine.

Administrators

An administrator represents an individual person or a group of people identified by their Active Directory account. Each administrator is associated with one or more role and scope pairs, which allows organizations to delegate responsibility based on the administrator's role and function.

Roles



Roles represent a job function, with defined permissions. XenDesktop has the following built-in roles:

- Full administrator: Can perform all tasks and operations. A Full Administrator is always combined with the All scope.
- Machine Catalog administrator: Can create and manage machine catalogs and provision the machines into them. This role can manage base images and install software, but cannot assign applications or desktops to end users.
- Delivery Group administrator: Can deliver applications, desktops, and machines; can also manage the associated sessions and application and desktop configurations such as policies and power management settings.
- Host administrator: Can manage host connections and their associated resource settings. Cannot deliver machines, applications, or desktops to end users.

- Help Desk administrator: Can view Delivery Groups, and manage their sessions and machines. Can see the machine catalog and host information for the Delivery Groups being monitored, and can also perform session management and machine power management operations for the machines in those Delivery Groups.
- Read-only administrator: Can read all objects in specified scopes as well as global information, but cannot change anything.

Scopes

Scopes represent a collection of objects. Scopes are used to group objects in a way that is relevant to your organization. Objects can be in more than one scope; you can think of objects being labeled with one or more scopes. There is one built-in scope: 'All,' which always contains all objects. The Full Administrator role is always paired with the All scope.

To Add an Administrator

1. Log on to a machine that has Citrix Studio installed on it.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Click **Administrators** in the left pane.
4. Click the **Administrators** tab in the middle pane. A list of existing administrators appears.
5. Click **Create Administrator** in the Actions pane.
6. Click **Browse** and type the name of the administrator that you would like to add.

   Enter **CCH\Admin2**.

7. Click **Check Names** to validate the administrator name and then click **OK**.
8. Select a scope to specify the objects the administrator can access and click **Next**.

   Select **All** in the scope field and click **Next**.

9. Select a role for the new administrator and click **Next**.

   Select **Full Administrator** and click **Next**.

10. Verify that the configuration is correct and that **Enable Administrator** is selected.
11. Click **Finish** to create the administrator.

To Create a Custom Scope Using Studio

1. Log on to a machine that has Citrix Studio installed on it.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Click **Administrators** in the left pane.
4. Click the **Scopes** tab in the middle pane. A list of existing scopes appears.
5. Click **Create Scope** in the Actions pane.
6. Type a name and description for the scope.

   a. Type **Notepad App Administrators** for the name of the scope.
   b. Type **Able to support the Notepad App** for the description of the scope.

7. Select the objects you want to add to the new scope.

   a. Expand **Delivery Groups** and select **Notepad Application Servers**.
   b. Select **Machine Catalogs**.

8. Click **Save**.

To Edit a Custom Scope

1. Log on to a machine that has Citrix Studio installed on it.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Click **Administrators** in the left pane.
4. Click the **Scopes** tab in the middle pane. A list of existing scopes appears.
5. Select the scope that you would like to edit.

   Select **Notepad App Administrators**.

6. Click **Edit Scope** in the Actions pane. The edit scope window appears.
7. Make the necessary changes to the scope.

   Deselect **Machine Catalogs** from the objects list.

8. Click **Save**.

To Create a Custom Role

1. Log on to a machine that has Citrix Studio installed on it.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Click **Administrators** in the left pane.
4. Click the **Roles** tab in the middle pane. A list of existing roles appears.
5. Click **Create Role** in the Actions pane.
6. Type a name and description for the role.

   a. Type **Hosted Application Administrator** for the name of the role.
   b. Type **Can Add, Edit, and Delete Hosted Applications** for the description

7. Select the object type, and then select the permissions that you want the role to have.

   a. Expand **Delivery Groups** and select **Manage**.
   b. Select the following options:
      - **Add Application to Delivery Group**
      - **Create Application**
      - **Delete Application**
      - **Edit Application Properties**
      - **Enable/disable maintenance mode of an Application**
      - **Remove Application from Delivery Group**

8. Click **Save**.
9. Verify that you have created the role with appropriate permissions.

   Select **Hosted Application Administrator** and look over the details at the bottom of the pane.

To Edit a Custom Role

1. Log on to a machine that has Citrix Studio installed on it.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Click **Administrators** in the left pane.
4. Click the **Roles** tab in the middle pane. A list of existing roles appears.

5. Select the role you would like to edit.

   Select **Hosted Application Administrator**.

6. Click **Edit Role** in the Actions pane.
7. Edit the permissions as needed.

   a. Expand **Delivery Groups**.
   b. Select **Change users assigned to an application**.

8. Click **Save**.

To Edit an Administrator's Permissions

1. Log on to a machine that has Citrix Studio installed on it.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Click **Administrators** in the left pane.
4. Click the **Administrators** tab in the middle pane. A list of existing administrators appears.
5. Select the administrator you want to edit.

   Select the **CCH\NotepadAdmin** administrator account to edit.

6. Click **Edit Administrator** in the Actions pane. The details of that administrator appear.
7. Click **Edit.** The Edit Administrator window opens.

You have to select a scope before the Edit button is enabled.

8. Select a new scope.

   Select **Notepad App Administrators**.

9. Click **Role** and select a new role.

   Select **Hosted Application Administrator**.

10. Click **OK** to save the change.
11. Click **OK** to finalize the administrator edits.

Running a Delegated Administration Report

The resultant set of permissions (RSOP) HTML report shows the role/scope pairs associated with an administrator and lists the individual permissions for each type of object - Delivery Groups and machine catalogs, for example.

To Run a Delegated Administration Report

1. Log on to a machine that has Citrix Studio installed on it.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Click **Administrators** in the left pane.
4. Click **Create Report**.
5. Type the user or group name you want to select.

   Type **CCH\NotepadAdmin.**

6. Click **Check Names** and click **OK**.
7. Type a file name for the report and click **Save.**

   a. Click **Documents**.
   b. Type **RSOP_NotepadAdmin** as the report name and click **Save**. Make note of where it is saved.

8. Open the RSOP_NotepadAdmin report to view the delegated administration rights for NotepadAdmin.

Discussion Question

When would you typically run a delegated administration report? Why?

Using PowerShell

Everything that is accomplished in the Studio console can also be accomplished using PowerShell. As such, you can use PowerShell cmdlets to create new administrators, apply roles and scopes, and track the rights and status of each administrator.

Every action performed within Studio is launched as a PowerShell statement in the background. You can see the actions that you have performed by clicking the top node labeled Citrix Studio (CCH) in the left pane of Studio, and selecting the PowerShell tab in the middle pane. To use Citrix-specific commands on your own, either start PowerShell and add the required snap-ins or

click Launch PowerShell in the bottom right corner of the middle pane of Studio to start a PowerShell console with pre-loaded Citrix snap-ins.

For example, to add a new administrator, you can use the New-AdminAdministrator cmdlet. To apply a role and scope to the new administrator, you can use the Add-AdminRight cmdlet. If you would like to get a list of the rights and status of each administrator account in the site, you can use the Get-AdminAdministrator.

For more information about the available PowerShell cmdlets, see Citrix eDocs at *http://edocs.citrix.com*.

Discussion Question

How would the use of delegated administration change with the size of your XenDesktop deployment?

Monitoring Configuration Logs

Configuration logging captures Site configuration changes and administrative activities to the database. You can use the logged content to:

- Diagnose and troubleshoot problems after configuration changes have been made.
- Assist change management and track configuration changes.
- Report administrative activities.

More specifically, configuration logging tracks configuration changes and administrative activities initiated from Studio, Director, and PowerShell scripts. A few examples include:

- Creating or editing a host
- Adding an end user to a Delivery Group
- Adding an administrator
- Changing delegated administrator roles

Changes made through the registry, direct access of the database, or from sources other than Studio, Director, or PowerShell are not logged.

By default, the Configuration Logging feature is enabled and uses the database that is created when you create the Site (the Site Configuration Database). Citrix strongly recommends that you change the location of the database used for Configuration Logging as soon as possible after creating a Site for three reasons:

1. The backup strategy for the Configuration Logging Database is likely to differ from the backup strategy for the Site Configuration Database.
2. The volume of data collected for Configuration Logging could adversely affect the space available to the Site Configuration database.
3. Having a separate database splits the single point of failure for the databases.

To Display Configuration Log Content

1. Log on to a machine that has Citrix Studio installed on it.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Select **Logging** in the left pane. The configuration log content is displayed in the center pane.
4. Click the **Today** drop-down menu to view the different options available for filtering by time.

To Generate Configuration Log Reports

1. Log on to a machine that has Citrix Studio installed on it.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Select **Logging** in the left pane.
4. Click **Create Custom Report** in the Actions pane.
5. Select a date range for the report by selecting a predefined interval or specifying a custom time frame.

   Select **Last 7 days** and click **Next**.

6. Select the report format.

   Select **HTML**.

7. Browse to the location where the report should be saved.

   Click **Browse**, select **My Documents** as the location and click **OK**.

8. Click **Next**.
9. Review your selections on the Summary page and click **Finish**.
10. Open the reports from `C:\Users\Admin1\Documents` and review the changes that have been made over the last seven days.

Two reports are created for you; one is a summary of the changes, while the other provides more detail about the changes made in the environment.

To Change the Configuration Log Settings

1. Log on to a machine that has Citrix Studio installed on it.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Select **Logging** in the left pane.
4. Click **Preferences** in the Action pane. The Logging Preferences window opens.
5. Ensure that Enable is selected and edit the settings as necessary.

   Deselect **Allow changes when the database is disconnected**.

An important option available in the Logging Preferences window is the ability to change the logging database or the location of the database. For more information about changing the logging database and its location, see Citrix eDocs at *http://edocs.citrix.com/*.

6. Click **OK** to finish changing the settings.

Discussion Question

What are some use cases for the CSV output of the configuration logs?

Troubleshooting: Managing Licenses and Delegated Administration

Issue	Resolution
An administrator account that was created does not have the appropriate authority.	Verify what role was assigned and reassign a new role with the correct permissions. 1. Open Studio. 2. Click **Configuration**. 3. Click **Administrators**. 4. Click the **Administrators** tab in the center pane. 5. Choose the administrator name that does not have the correct authority. 6. Click **Edit Administrator** in the right pane. 7. Choose a role that appears in the details pane and click **Edit**. 8. In the Edit Administrator window, click **Role**. 9. Click **View permissions** next to the selected option. 10. Verify that these are the correct permissions. 11. Click **Cancel**. 12. If the permissions were incorrect, choose the appropriate role and click **Apply**. 13. If the permissions were correct, click **Cancel** and click **Add** to add an additional role to this administrator. • Verify that the administrator is not set for read-only access.

Issue	Resolution
An administrator is unable to access Studio.	Verify that the Administrator is Enabled. 1. Open Studio. 2. Click **Configuration**. 3. Click **Administrators**. 4. Click the **Administrators** tab in the center pane. 5. Choose the administrator name that cannot access Studio. 6. Click **Edit Administrator** in the right pane. • Ensure the **Enable Administrator** checkbox is checked.
A delegated administrator cannot shadow an end user.	Verify the following: • Remote assistance is enabled on the virtual desktop. • The administrator is authorized to launch a remote assistance session on the virtual desktop. • The Microsoft Remote Assistance client is installed on the system running Director. • Director is accessed through Internet Explorer 7 or 8 and ActiveX is enabled.

Reinforcement Exercise: Configuring Roles and Scopes

During this exercise, you will not be given step-by-step instructions for performing the task. Instead, you are asked to use what you have learned to complete it. This exercise is designed to take your newly gained knowledge and determine if you can apply it to perform a task you have never done before. In most instances the default value/choice will be the best choice, but we encourage you to explore and try different options. If you have a question or need help, ask the instructor or a fellow student for assistance.

In this module, you learned how to:

- Describe how Citrix Studio is used to manage licensing.
- Manage licensing.
- Manage delegated administration.
- Monitor configuration logs.
- Generate configuration log reports.

Time to complete: Approximately 20 minutes

CCH wants you to implement a design for their HelpDesk organization. The design calls for the first tier support to be able to manage requests regarding the hosted applications that CCH will be using. They want the tier-2 staff to be able to handle requests for all types of company resources due to their additional experience and training.

Your objective is to configure the appropriate roles and scopes in order to achieve the following delegation:

AD Group	Scope	Role
Helpdesk	All	Read Only Administrator
Helpdesk-Apps	Notepad App Administrators	Help Desk Administrator
Helpdesk-Tier2	All	Help Desk Administrator

Module 3

Managing and Monitoring the Hypervisor

3

Managing and Monitoring the Hypervisor

Virtualization enables multiple virtual machines to run on a single physical server. Each virtual machine is completely isolated from other virtual machines and is decoupled from the underlying host by a thin layer of software known as a hypervisor.

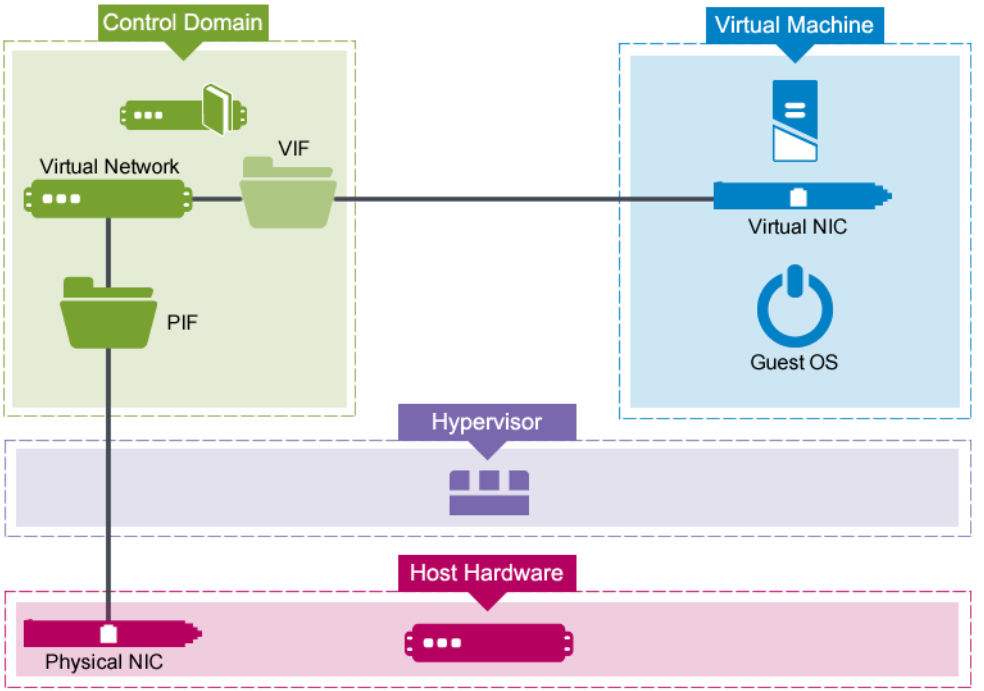
XenDesktop has an open architecture, which allows it to manage virtual desktops hosted on several different hypervisors. This module will discuss tasks that can be done with each hypervisor that is supported by XenDesktop. However, the tasks will be described using Citrix XenServer. Although the steps may differ within each hypervisor, the overall task will have the same end result.

After completing this module, you will be able to:

- Describe the communication process between the host hardware, hypervisor, control domain, and virtual machine.
- Create, copy, and manage virtual machines.
- Create snapshots and revert virtual machines to prior states.
- Manage resources allocated to virtual machines and templates.
- Configure and customize alerts within the hypervisor.

Module timing: Approximately 3 hours

Architecture Overview



The following components are combined to virtualize server and desktop hardware so that multiple operating systems can share devices like hard drives and network cards.

- **Host Hardware** - The bare-metal machine in which the hypervisor lays and whose resources are used and distributed throughout a virtualized environment. This hardware contains the physical server components including memory, CPU, and disk drives.
- **Hypervisor** - A thin layer of software that gives each virtual machine a dedicated view of the hardware. The hypervisor provides an abstraction layer that allows each physical server to run one or more virtual machines, effectively decoupling the operating system and its applications from the underlying hardware.
- **Control Domain** - Manages the network - and storage - I/O of all virtual machines.
- **Virtual Machines** - Virtual machines that appear to end users as separate computers, each with its own network identity, user authorization, authentication capabilities, operating system version, configuration, applications, and data. The machine shares physical resources with other virtual machines and is portable because the virtual machine is abstracted from physical hardware.
- **Guest Operating System** - The operating system that is installed on a virtual machine.
- **Physical Interface (PIF)** - A driver-like representation within the control domain that corresponds to an actual network interface card in the host machine.

- **Virtual Interface (VIF)** - A virtualized representation of a computer network interface. A virtual machine connects to a virtual interface to provide network connectivity to other virtual machines and the physical network.
- **Virtual Network Interface Card (Virtual NIC)** - A driver-like program that allows a virtual machine's guest OS to connect to a virtual network.
- **Physical Network Interface Card (Physical NIC)** - A physical network card that is installed on the host hardware.
- **Virtual Network** - The software representation of a network switch within the control domain. Virtual machines communicate with other network nodes using the virtual network to which they are connected.

The hypervisor works by virtualizing the hardware. Hardware virtualization abstracts system components, such as hard drives, resources, and ports, and allocates them to the virtualized servers running on the system. These virtualized servers are known as virtual machines, which run operating systems and applications that are known as guest software.

The hypervisors that are supported by XenDesktop 7 are:

- XenServer
  - XenServer 6.2
  - XenServer 6.1
  - XenServer 6.0.2
- Hyper-V and System Center Virtual Machine Manager (SCVMM)
  - Any version of Hyper-V that can register with SCVMM 2012 and SCVMM 2012 SP1, including Microsoft Hyper-V Server 2008 R2 SP1 and Microsoft Hyper-V Server 2012
- VMware vSphere
  - VMware vSphere 5.1 Update 1
  - VMware vSphere 5.0 Update 2

When using a hypervisor to host your XenDesktop virtual machines, ensure that the proper tools are installed. For example, XenServer tools must be installed in order to properly manage virtual machines within XenServer and to gain maximum performance from the virtual machines. Without XenServer Tools, you cannot:

- Restart a virtual machine.
- Suspend a virtual machine.
- Migrate a running virtual machine using XenMotion.
- Adjust dynamically the number of virtual CPUs assigned to a running Linux virtual machine; Windows virtual machines require a restart for this to take effect.
- Dynamically adjust the memory of the virtual machines to compensate for overload situations.
- View virtual machine performance data in XenCenter.
- Create quiesced snapshots or snapshots with memory.
- Revert to snapshots.

Creating a Virtual Machine from an ISO

You will create a new virtual machine template in your virtualized environment from an ISO file. This is analogous to installing an operating system onto a computer through the DVD drive. You will then prepare the virtual machine for copying and turn it into a template.

Creating a Virtual Machine

You will create virtual machines that can be deployed to end users or used as server machines. This can be done for many reasons including proper allocation of resources, replacing physical boxes with virtual machines, host different operating systems, and end-of-life replacement. Virtual machines also never leave the datacenter, which offers a much higher level of security and simplifies administration and management.

To Create a Virtual Machine Using XenCenter

1. Open the XenCenter console.
2. Click the **New VM** button at the top of the console.
3. Select a template, operating system, or snapshot for the new virtual machine.

   Select **Windows 7 (32-bit)**.
4. Click **Next**.
5. Name the virtual machine.

   Type **Win7**.
6. Select the ISO to use to perform the initial installation of the operating system.

   Select **Windows_7_32bit.iso** from the Install from ISO library or DVD drive drop-down menu.
7. Click **Next** two times.
8. Select the number of vCPUs and memory to allocate to the virtual machine.

   Select **1 vCPU** and **1024 MB** for memory.
9. Click **Next**.
10. Select the storage to be allocated to the virtual machine and add additional storage if necessary.

    Select **Local storage on xenserver_1** and then click **Next**.
11. Configure the networking on the new virtual machine.

    Leave the default settings and then click **Next**.

12. Ensure that **Start the new VM automatically** is selected, verify the configuration settings for the new virtual machine, and then click **Finish**.

To Install a Windows OS onto a Virtual Machine

1. Select the virtual machine in the XenCenter console and then click **Console**.

   Select the **Win7** virtual machine and then click **Console**.

2. Select the language, time and currency format and keyboard settings for your area and then click **Next**.
3. Click **Install now**.
4. Read and respond to the licensing terms.

   Select **I accept the license terms** and then click **Next**.

5. Select **Custom (advanced)**.
6. Adjust the drive options and then click **Next**.

   Ensured that **Disk 0 Unallocated Space** is selected and then click **Next**.

7. Allow for the installation to complete and then restart the virtual machine.

The virtual machine may restart several times to complete the installation.

8. Type a user name in the Type a user name field and then click **Next**.

   Type **TempUser** as the user name and then click **Next**.

9. Specify a password and hint for your account and then click **Next**.

   a. Type **Password1** in the Type a password and Retype your password fields.
   b. Type **Regular** in the Type a password hint field and then click **Next**.

10. Select the desired update settings.

    Select **Ask me later**.

11. Review your time and date settings to ensure that they are correct and then click **Next**.

    Click **Next**.

12. Select the current location of the computer.

    Click **Work network**.

13. Allow Windows to finalize your settings and then log on using the account you created previously.

Installing XenServer Tools

XenServer Tools provides high performance Windows drivers and a management agent, enhancing disk and network performance for XenServer virtual machines. XenServer Tools must be installed for each virtual machine in order to be able to use the xe CLI or XenCenter. Virtual machine performance will be significantly lowered unless the tools are installed.

Running a virtual machine without installing the XenServer Tools is not a supported configuration.

To Install XenServer Tools on a Virtual Machine

1. Select **xs-tools.iso** in the DVD Drive 1 field at the top of the console screen.
2. Wait a few moments for the AutoPlay screen to appear and then click **Run xensetup.exe**.

   Select **Yes** in the User Account Control screen, if it appears.
3. Read and respond to the license agreement terms.

   Select **I accept the terms of the License Agreement** and then click **Next**.
4. Click **Install**.
5. Wait while the installation completes.
6. Ensure that **Reboot now** is selected and then click **Finish**.
7. Wait while the virtual machine restarts.
8. Click **Eject** to eject the ISO from the virtual machine.

Generalizing the Virtual Machine

Citrix recommends that you generalize a virtual machine before creating a template from it. This is done to eliminate the possibility of virtual machines created from the template conflicting with one another. On a Windows operating system, the tool to do this is called Sysprep and is bundled with all versions of Windows from Vista forward.

This process is only required if you plan to make a template from the virtual machine.

To Generalize the Virtual Machine

1. Log on to the virtual machine that will be generalized.
    a. Select the **Win7** virtual machine in XenCenter.
    b. Click **Console**.
    c. Log on using the **TempUser** and **Password1** credentials.
2. Browse to and run the Sysprep executable.
    a. Click the **Windows Explorer** icon in the taskbar and then click **Computer**.
    b. Browse to `C:\Windows\Sysprep32\sysprep` and then double-click **sysprep**.
3. Configure the System Cleanup Action and Shutdown Option and then run the Sysprep process.
    a. Select **Generalize**.
    b. Select **Shutdown** from the Shutdown Options and click **OK**.
4. Wait while the Sysprep process completes and the virtual machine shuts down.

Creating a Template

With the virtual machine properly prepared and generalized, the template can be created in XenServer.

This process is only required if you plan to make a template from the virtual machine.

To Create a Template from a Virtual Machine

1. Select the virtual machine that will be converted to a template.
    Select the **Win7** virtual machine in XenCenter.
2. Right-click the virtual machine, click **Convert to Template**, and then click **Convert**.
    a. Right-click **Win7** and then click **Convert to Template.**
    b. Click **Convert**.
3. Rename the virtual machine to fit with your naming scheme.
    a. Right-click **Win7** and then select **Properties**.
    b. Type **Win7_template** in the Name field and then click **OK**.

Managing Virtual Machines within a Hypervisor

You will manage your virtualized environment and virtual machines within your hypervisor. Virtual machines can be created by building an image or by using a previously made template that contains all the configuration settings necessary to create an instance of a specific virtual machine.

Creating a Virtual Machine

You will create virtual machines that can be deployed to end users or used as server machines. This can be done for many reasons including proper allocation of resources, replacing physical boxes with virtual machines, host different operating systems, and end-of-life replacement. Virtual machines also never leave the datacenter, which offers a much higher level of security and simplifies administration and management.

To Create a Virtual Machine Using XenCenter

1. Open the XenCenter console.
2. Click the **New VM** button at the top of the console.
3. Select a template, operating system, or snapshot for the new virtual machine.

   Select **Win8_template**.
4. Click **Next**.
5. Name the virtual machine.

   Type **EndPoint-Internal**.
6. Click **Next** three times to use the default settings.
7. Specify the number of vCPUs and memory to allocate to the virtual machine.

   Select **1** vCPU and **1024** MB for memory.
8. Click **Next**.
9. Select the storage to be allocated to the virtual machine and then add additional storage, if necessary.

   Select **NFS virtual disk storage** and then click **Next**.
10. Configure the networking on the new virtual machine.

    Accept the default networking settings and then click **Next**.
11. Deselect **Start the new VM automatically**, verify the configuration settings for the new virtual machine, and then click **Finish**.

It is important to ensure that you deselect the option to start the new virtual machine automatically for this exercise to complete successfully. If this option was not deselected prior to clicking Finish, you must delete the virtual machine and recreate it using the steps in this procedure.

Taking a Snapshot

A snapshot is an image of a virtual machine that preserves the current settings and data at the point in time in which the snapshot is taken. Taking snapshots allows an administrator to restore a virtual machine if for any reason it fails.

To Take a Snapshot in XenCenter

1. Select the virtual machine of which you would like to take a snapshot.

   Select the **EndPoint-Internal** virtual machine.

2. Select the **Snapshots** tab.
3. Click **Take Snapshot**.
4. Type a name for the snapshot.

   Type **Sysprepped** in the Name field.

5. Click **Take Snapshot**. The new snapshot will appear in seconds.

Discussion Question

What are some of the concerns associated with having too many snapshots in your environment?

Restoring a Virtual Machine From Sysprep

When virtual machines are generalized by Sysprep, they are not usable until they are brought out of the generalized state.

To Restore a Virtual Machine from Sysprep

1. Start the virtual machine that will be restored from Sysprep.

   Double-click the **EndPoint-Internal** virtual machine to start it.

2. Select the **Console** tab for the virtual machine.

   Click **EndPoint-Internal** and select the **Console** tab.

3. Wait while the virtual machine starts. This may take a few minutes.
4. Read and respond to the license terms.

   Select **I accept the license terms for using Windows** and then click **Accept**.

5. Type a name for the computer in the PC name field and then click **Next**.

   Type **EP-E** in the PC name field and then click **Next**.

6. Specify which settings to use for the computer.

Click **Use express settings**.

7. Specify how you want to sign in to the computer.

   Select **Sign in without a Microsoft Account** and then click **Local account.**

8. Specify a username, password and password hint information for the new local account and then click **Finish**.

   a. Type **TempUser** in the User name field.
   b. Type **Password1** in the Password and Reenter password fields.
   c. Type **First Password** in the Password hint field.
   d. Click **Finish**.

9. Wait while the virtual machine completes its setup and the Start screen appears.

Copying a Virtual Machine

One of the benefits of creating virtual machines is that they can be easily copied. You will do this at times to have a complete backup of a virtual machine, troubleshoot, or test applications prior to installing them on the live machine, for fault tolerance and providing the ability to roll back in the event of problems, or to repurpose the machine for other needs within the environment.

To Copy a Virtual Machine using XenCenter

1. Shut down the virtual machine you would like to copy.

   Shut down **EndPoint-Internal** if it is currently on.

2. Right-click the virtual machine you would like to copy.

   Right-click **EndPoint-Internal**.

3. Select **Copy VM**.
4. Type a name in the Name field for the copied virtual machine.

   Type **EndPoint-External**.

5. Select **Fast clone**.
6. Click **Copy**.
7. Select the copied virtual machine and then click **Start** to verify that it was successfully copied.

   Select the **EndPoint-External** virtual machine and then click **Start**.

Discussion Question

What would happen if you turn on both the copied and the original virtual machines without performing a sysprep?

Reverting to a Snapshot

If a snapshot has been taken, you can easily revert to the snapshot, which will return the virtual machine to the particular state at the time the snapshot was taken. You also have the option to take a new snapshot of the current virtual machine state before reverting back to the earlier snapshot, allowing you to easily restore the virtual machine to its current state if needed.

To Revert to a Snapshot in XenCenter

1. Select the virtual machine that you would like to revert to an earlier version.

   Select the **EndPoint-Internal** virtual machine in XenCenter.

2. Select the **Snapshots** tab.
3. Select the snapshot to which you would like to revert.

   Select **Sysprepped**.

4. Click **Revert To**.
5. Select the **Snapshot the virtual machine's current state and then revert** checkbox if you would like a snapshot of the current state.

   Deselect the **Snapshot the virtual machine's current state and then revert** checkbox so that a snapshot is not taken of the current state.

6. Click **Yes** to revert to the earlier snapshot.
7. Start the virtual machine to go through setup.

   Double-click the **EndPoint-Internal** virtual machine in XenCenter to start it.

Discussion Question

Are both the EndPoint-Internal and EndPoint-External virtual machines currently unique even though one was directly copied from the other? Why or why not?

Adjusting Virtual Machine or Template Resources

When managing a virtualized environment, it is important to use and allocate your resources wisely to maximize efficiency. Administrators who create virtual machines and templates within a hypervisor must be aware of storage capacity, available memory, network resources, and processing power.

Adding Storage to a Virtual Machine or Template

As with managing memory, occasionally end users require additional storage. With the appropriate resources, you can easily add storage to a virtual machine or a template.

To Add Storage to a Virtual Machine or Template in XenCenter

1. Select the virtual machine or template to which you would like to add storage.
    a. Select the **ProvisioningServicesHost-1** virtual machine.
    b. Click **Start**.
    c. Click the **Console** tab and allow the virtual machine to start.
    d. Log on as the **CCH\Admin1** user using **Password1** as the password.
2. Select the **Storage** tab.
3. Click **Add**.
4. Type a name for the new virtual disk in the Name field.

    Type **vDisk Storage**.
5. Select the size of the disk.

    Type **40** and then select **GB**.
6. Select the location of the storage.

    Select **Local storage on xenserver_1**.
7. Click **Add**.
8. Click the **Console** tab and click the **Server Manager** icon.
9. Click the **Tools** menu and then select **Computer Management**.
10. Select **Disk Management** in the left pane.
11. Click **OK** on the Initialize Disk window, if it appears. The new disk will appear.
12. Right-click **Unallocated** next to Disk 1.

13. Select **New Simple Volume**.
14. Click **Next** in the New Simple Volume Wizard.
15. Select the volume size.

    Use the default settings and click **Next**.

16. Assign a drive letter or path to the disk.

    Verify that **E** is selected in the Assign the following drive letter field and then click **Next**.

17. Specify the format partition information.

    Type **Store** in the Volume label field and then click **Next**.

18. Click **Finish**.
19. View the mounted disk.

    Click **File Explorer** and click **Computer**.

20. Ensure the disk has the correct permissions.

    a. Right-click **Store (E:)** and click **Properties**.
    b. Click **Security** and click **Edit**.
    c. Click **Add** type **CCH\Network Service** and click **OK**.
    d. Select **Network Service** and click **Allow** next to Full Control.
    e. Click **OK**.

Adjusting the Storage Allocated to a Virtual Machine

You may find at times that your environment is running low on storage. Before deciding to purchase additional storage hardware, check whether storage allocations are appropriate for end-user needs in the environment. For example, if some of your power users need additional hard disk space to store their files or if your file server needs additional space than originally planned, you can easily adjust your disks.

To Adjust the Storage Allocated to a Virtual Machine in XenCenter

1. Shut down the virtual machine or template to which you would like to make changes.

    a. Select the **ProvisioningServicesHost-1** virtual machine and then click **Shutdown**.
    b. Wait for the virtual machine to shut down.

2. Select the **Storage** tab in XenCenter.

3. Double-click the storage device that you would like to adjust.

   Double-click **vDisk Storage**.

4. Click **Size and Location** in the left pane.
5. Specify a size for the storage you would like to allocate to this disk.

   Type **50** GB in the Size field.

6. Click **OK**.
7. Verify that the size of the storage has increased on the Storage tab in XenCenter.
8. Log on to the virtual machine using your domain administrator credentials.

   a. Select the **ProvisioningServicesHost-1** virtual machine and then click **Start**.
   b. Wait while the virtual machine starts.
   c. Log on using the **CCH\Admin1** and **Password1** credentials.

9. Click the **Console** tab and click the **Server Manager** icon in the taskbar.
10. Click the **Tools** menu and then select **Computer Management**.
11. Select **Disk Management** in the left pane.
12. Right-click **Store** and select **Extend Volume**.
13. Click **Next** twice in the Extend Volume Wizard and then click **Finish**.

Adjusting the Memory Allocated to a Virtual Machine or Template

If you are encountering issues regarding memory within your environment, whether the environment is running low on resources or end users require more memory to use programs that are resource intensive, you will need to manage the memory allocation appropriately.

To Adjust Virtual Machine or Template Memory Allocations in XenCenter

1. Shut down the virtual machine you on which you would like to reallocate memory. Skip this step if you are adjusting a template.

   The **EndPoint-External** virtual machine should already be shut down.

2. Select the virtual machine or template that you would like to make changes to.

   Select the **EndPoint-External** virtual machine.

3. Select the **Memory** tab.
4. Click **Edit**.

5. Select either **Set a fixed memory of** and type the preferred memory you would like allocated to this virtual machine or select **Automatically allocate memory within this range** and type the minimum and maximum limits.

   Select **Set a fixed memory of** and type **1536** in the MB field.

6. Click **OK**.

Adjusting vCPUs Allocated to a Virtual Machine or Template

Another resource that can be a limiting factor within an environment is the processing power available to virtual machines. Although each vCPU must be allocated strategically, XenCenter allows you to set priority of vCPUs giving you more options when distributing processors across the environment.

To Adjust the vCPUs Allocated to a Virtual Machine or Template in XenCenter

1. Shut down the virtual machine you would like to allocate or reallocate vCPUs. Skip this step if you are adjusting a template.

   The **EndPoint-External** virtual machine should already be shut down.

2. Select the virtual machine or template that you would like to make changes to.

   Select the **EndPoint-External** virtual machine.

3. Select the **General** tab.
4. Click **Properties**.
5. Select **CPU** in the left pane.
6. Type the number of vCPUs for this virtual machine or template.

   Type **2**.

7. Click **OK**.

To Remove a Virtual NIC in XenCenter

1. Select the virtual machine or template from which you want to remove a virtual NIC.

   Select the **EndPoint-External** virtual machine.

2. Select the **Networking** tab.

3. Select the virtual NIC you would like to remove.

   Select **Device 0**.

4. Click **Remove Interface**.
5. Click **Yes** in the Delete Network Interface message.

Adding a Virtual NIC

Additional NICs are needed when virtual machines are required to be associated with networks other than networks they are currently associated with. When you install an interface into the virtual machine it links it to the relevant network, allocates it a MAC address, and also provides the option to complete a Quality of Service (QoS) settings value. The virtual machine now hosts a presence on the network and can communicate with other machines also associated with this network.

To Add a Virtual NIC in XenCenter

1. Select the virtual machine or template on which you would like to add a virtual NIC.

   Select the **EndPoint-External** virtual machine.

2. Select the **Networking** tab.
3. Click **Add Interface**.
4. Select the network to be added.

   Select **DMZ (10.29.0.x)**.

5. Select **Auto-generate a MAC address** or type a specific address in the Use this MAC address field.

   Select **Auto-generate a MAC address**.

6. Click **Add**.

To Adjust a Virtual NIC in XenCenter

1. Select the virtual machine or template on which you would like to adjust the virtual NIC settings.

   Select the **EndPoint-External** virtual machine.

2. Select the **Networking** tab.
3. Select the virtual NIC you would like to adjust.

   Select **Device 0**, which is currently connected to the DMZ (10.29.0.x) Network.

4. Click **Properties**.
5. Select **Enable a QoS limit of** and type the desired limit.

   Type **1024**.

6. Click **OK**.

To Activate or Deactivate a Virtual NIC in XenCenter

1. Double-click the virtual machine or template on which you would like to activate or deactivate a virtual NIC.

   Double-click the **EndPoint-External** virtual machine to start it. Please wait for the virtual machine to start to the log on screen before continuing.

2. Select the **Networking** tab.
3. Select the virtual NIC you would like to activate or deactivate.

   Select **Device 0**.

4. Click **Deactivate** or **Activate**.

   a. Click **Deactivate**.
   b. Click **Activate** to activate the virtual NIC again.

Discussion Question

Your environment is running low on memory and storage. What are some options available to you in order to resolve these issues?

Configuring and Customizing Alerts

To simplify monitoring of your environment, hypervisors allows you to configure events and alerts. These events and alerts raise awareness when resources reach a pre-determined level.

To Configure and Customize Alerts in XenCenter

1. Select the server or virtual machine on which you would like to configure the alert.

   Select the **Controller-1** virtual machine.

2. Select the **General** tab.
3. Click **Properties**.
4. Click **Alerts**.
5. Select one or more of the available options:
   - Select the **Generate CPU usage alerts** checkbox and then set the CPU usage and time that will trigger an alert.
   - Select the **Generate network usage alerts** checkbox and then set the network I/O usage and time threshold that will trigger an alert.
   - Select the **Generate disk usage alerts** checkbox and set the disk I/O usage and time threshold that will trigger an alert.
   - Type the number of minutes in the **Alert repeat interval** box at the top of the screen to configure the frequency of the alerts.
6. Click **OK**.
7. Click **System Alerts** on the top right within XenCenter to view any alerts.

Discussion Question

A subset of end users in your environment is having difficulty launching and utilizing their virtual machines. These end users are also noticing degradation in graphical performance with their AutoCAD software. How can you track these issues? What are some common causes of these issues?

Troubleshooting: Managing and Monitoring Hypervisors

Issue	Resolution
Memory statistics are not displayed for a virtual machine.	Confirm that the necessary hypervisor tools are installed on the virtual machine.
XenServer - Disk space is not reclaimed after deleting a snapshot.	XenServer 5.5 Update 1 and later 1. Retrieve the UUID of the VM (virtual machine) 2. Run coalesce-leaf-u<UUID of virtual machine>. This command suspends the virtual machine, initiates the reclamation process, and resumes the virtual machine.  For more information about how to reclaim disk space from deleted XenServer snapshots, see Citrix article CTX123400 at *http://support.citrix.com*.
Hyper-V - Virtual machines are missing from the Hyper-V Management Console.	Configure real-time scanning within anti-virus software to exclude: • Default and custom virtual machine configuration directories • Default and custom virtual hard disk drive directories • Snapshot directories • Vmms.exe and Vmwp.exe files

Reinforcement Exercise 1: Creating a Virtual Machine Template

During this exercise, you will not be given step-by-step instructions for performing the task. Instead, you are asked to use what you have learned to complete it. This exercise is designed to take your newly-acquired knowledge and determine if you can apply it to perform a task you have never done before. In most instances the default value will be the best choice, but we encourage you to explore and try different options. If you have a question or need help, ask the instructor or a fellow student for assistance.

In this module, you learned how to:

- Describe the communication process between the host hardware, hypervisor, control domain, and virtual machine.
- Create, copy, and manage virtual machines.
- Create snapshots and revert virtual machines to a prior state.
- Manage resources allocated to virtual machines and templates.
- Configure and customize alerts within the hypervisor.

Time to complete: Approximately 45 minutes

Recently you became part of the server virtualization team at CCH. Your first task within this new role is to create a new virtual machine image, which will be used later as a new master image for a XenDesktop machine catalog.

To complete your objective:

- Create a new Windows Server 2012 Standard (with GUI) base image from the Windows 2012 installation DVD and name the virtual machine Win2012_template in XenCenter.
  - If your version of XenServer does not have the Windows Serve 2012 diskless virtual machine template built-in, use the Windows Server 2008 R2 (64-bit) template instead.
- Install XenServer tools on the image in order to improve performance and management control.
- Assign the following attributes:
  - 1 virtual CPU
  - 2048 MB memory
  - 30 GB drive on local storage
  - Internal Network
- Sysprep the operating system.
- Convert the virtual machine into a template.

As the operating system is installing you can feel free to move onto Reinforcement Exercise 2 in this module, and then return once this installation is completed to perform the rest of the steps.

Reinforcement Exercise 2: Completing the Setup Process After a Sysprep

During this exercise, you will not be given step-by-step instructions for performing the task. Instead, you are asked to use what you have learned to complete it. This exercise is designed to take your newly-acquired knowledge and determine if you can apply it to perform a task you have never done before. In most instances the default value will be the best choice, but we encourage you to explore and try different options. If you have a question or need help, ask the instructor or a fellow student for assistance.

Time to complete: Approximately 15 minutes

You recently started the EndPoint-Internal virtual machine from a generalized (sysprepped) template. In order to make use of this virtual machine you must complete the setup process.

To complete your objective:

- Complete the setup process on the EndPoint-Internal virtual machine
- Change the hostname of the virtual machine to EP-I.
- Create a new local user called TempUser2 with a password of Password1.
- Join the virtual machine to the cch.local domain.
- Enable Remote Desktop access (without network level authentication) to the virtual machine and grant access to CCH\Domain Users.

Module 4

Managing Desktops and Applications

4

Managing Desktops and Applications

Collections of identical virtual machines or physical computers are managed as a single entity called a machine catalog. The machines within these machine catalogs are configured to run either a Windows Desktop operating system (OS) or a Windows Server OS. For end users who want to access their office machine remotely, there is also an option for Remote PC Access when creating machine catalogs.

In order to deliver desktops and applications to specific end users, you allocate machines from the catalog to end users through Delivery Groups. Delivery Groups provide desktops, applications, or a combination of the two, to one or more end users. Delivery Groups provide a flexible way of allocating machines and applications to end users. In a Delivery Group, you can:

- Use machines from multiple catalogs.
- Allocate a user to multiple machines.
- Allocate multiple end users to one machine.

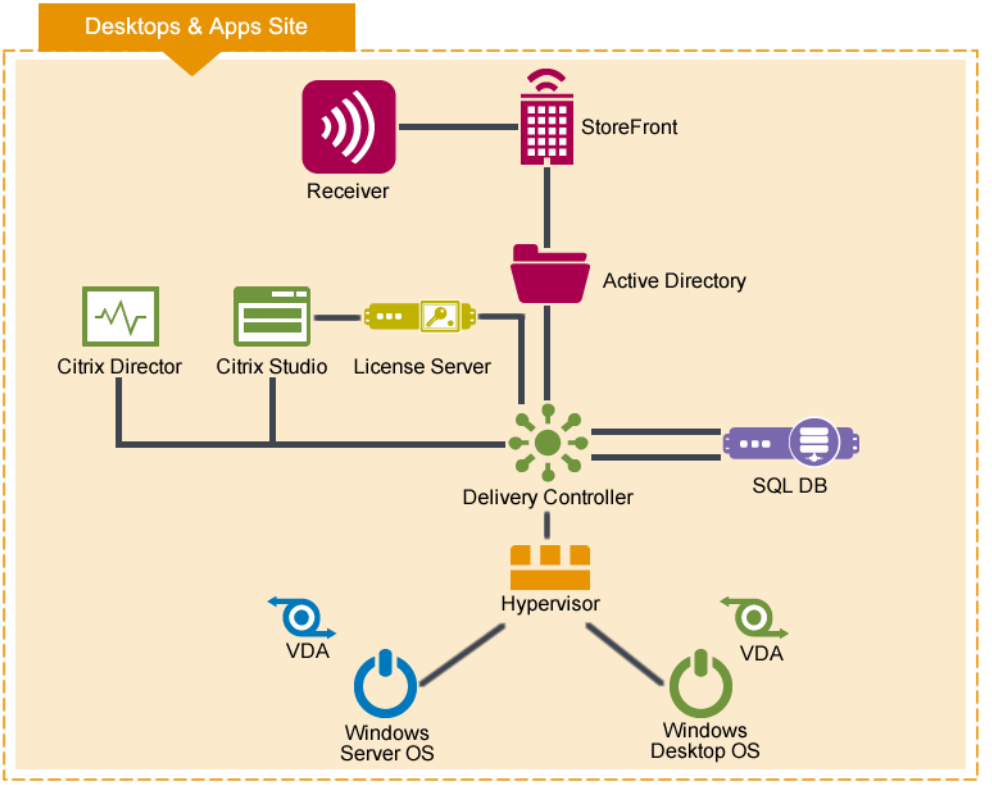
After completing this module you will be able to:

- Describe the XenDesktop 7 infrastructure for delivering desktops and applications.
- Describe the role of the Delivery Controller.
- Create and manage machine catalogs.
- Manage Delivery Groups.

Module timing: Approximately 4.5 hours

Architecture Overview

The following diagram depicts the functions and communications of the Delivery Controller within a XenDesktop deployment.



The Delivery Controller communicates with StoreFront to present resources to end users connected with Citrix Receiver.

Supported operating systems include:

- Windows Server 2012 (Standard and Datacenter Editions)
- Windows Server 2008 R2 SP1 (Standard, Enterprise, and Datacenter Editions)

Requirements include:

- 100 MB disk space
- Windows PowerShell 2.0 or 3.0
- Visual C++ 2005, 2008 SP1, and 2010
- Microsoft .NET 3.5 SP1 (required on Windows Server 2008 R2 only)
- Microsoft .NET 4.0

The SQL Server database presents information about the site to the Controllers. Supported database editions include:

- SQL Server 2012 SP1
- SQL Server 2008 R2 SP2

Windows authentication is required for connections between the Controller and the SQL Server database.

The Delivery Controller contacts the hypervisor to confirm availability of the virtual machines and applications that will be presented to an end user.

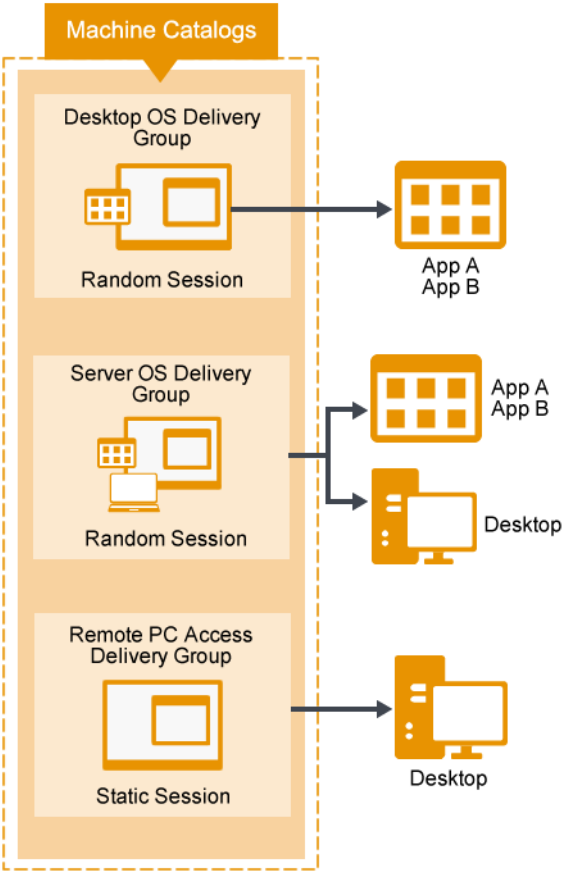
The Delivery Controller communicates with Active Directory to validate end-user credentials.

Studio and Director communicate with the Delivery Controller to manage and configure the site.

Once an end-user's session has connected to a StoreFront server, the Delivery Controller can present the end user with a list of resources from the physical network or from a supported hypervisor.

Managing Machine Catalogs

A machine catalog is a collection of virtual machines or physical computers managed as a single entity. Machine catalogs specify the virtual machines or computers available to host applications or desktops, the Active Directory computer accounts assigned to those virtual machines or computers, and in some cases, the master image that is copied to create the virtual machines. Virtual machines within machine catalogs are organized into Delivery Groups that deliver the same set of desktops and applications to groups of end users.



To Create New Resource Settings

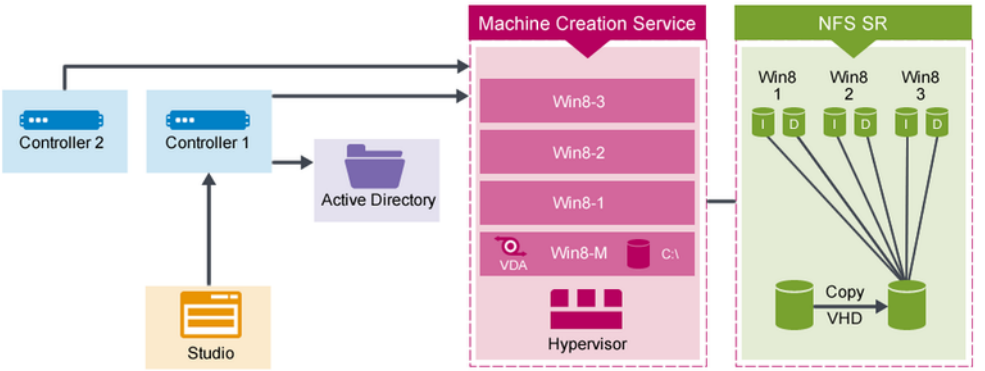
Perform these steps in order to create new resource settings. The new resource settings will allow you to create machine catalogs in the lab environment.

1. Log on to the **StudentManagementConsole-1** virtual machine and open Citrix Studio.

2. Expand the **Configuration** node in Studio.
3. Select the **Hosting** node.
4. Click **Add Connection and Resources** in the Actions pane.
5. Select **Use an existing connection** and then select **XenServer**.
6. Click **Next**.
7. Select **Internal** and then click **Next**.
8. Deselect **NFS virtual disk storage**.
9. Select **Local** within the Storage drop-down menu and then verify that **Local storage on xenserver_1** is selected.
10. Click **Next**.
11. Type **CCH Resource Settings** in the Resource Name field.
12. Click **Finish**.

Machine Creation Services

Machine Creation Services (MCS) is a collection of services that work together to create virtual desktops from a master desktop image on demand, optimizing storage utilization and providing a pristine virtual desktop to end users every time they log on.



Discussion Question

What are some use cases for Machine Creation Services? Are those use cases different for Provisioning Services?

Creating a Machine Catalog

Collections of identical virtual machines or physical computers are managed as a single entity called a machine catalog. If you are not provisioning through Machine Creation Services or Provisioning Services, Citrix recommends that you use Microsoft System Center Configuration Manager or another third-party application to make sure that the machines in the catalog are consistent.

The machines within these machine catalogs are configured to run either a Windows Desktop OS or a Windows Server OS. For end users who need to remotely access their office machine, you can select Remote PC Access for those machine catalogs.

You should create a new machine catalog whenever the desktop needs of your end users deviate from those being used in the environment. For example, all of the end users are currently provided with a Windows 8 desktop, but some of your end users require a Windows 7 desktop.

Here, we will explore two of the three options that are available to you when creating a machine catalog in Studio. First, we begin with a Server OS machine catalog.

Creating a Machine Catalog for Windows Server

Server OS machine catalogs provide a Windows Server environment and provide standard desktops and applications that are shared by a large number of end users. These machine catalogs provide desktops and applications that are:

- Allocated to end users on a per-session, first-come first-served basis
- Deployed on standardized machines

Typically, end users who need a Server OS machine:

- Are task workers who require standardized virtual desktops and applications, such as call center operators and retail workers
- Do not need to or are not permitted to install applications on their desktops

With these types of end users, you want to:

- Optimize hardware use by providing only the number of desktops that are required at any one time rather than assigning each user a specific desktop
- Maintain control over desktops and increase security by preventing end users from making permanent changes
- Minimize desktop management costs by providing a locked-down standardized environment for your end users

Installing the Virtual Delivery Agent (VDA)

The Virtual Delivery Agent (VDA) has to be present on the virtual or physical machines to which your end users will be connecting. It enables the machines to register with Controllers and manages the HDX connection between the machines and the end-user devices.

There are two kinds of VDA: VDA for Desktop OS and VDA for Server OS.

To Install and Configure the VDA

1. Log on to the virtual machine that you will use as the Master Image using domain administrator credentials.

   Start the **Win2012-Master** virtual machine and then log on with the **CCH\Admin1** and **Password1** credentials.

2. Insert the XenDesktop 7 installation media into the DVD drive in XenCenter.

   Select **Citrix_XenDesktop_7.iso** in the DVD Drive 1 field.

The XenDesktop 7 installer should automatically run. If it does not, simply go to the Desktop on your Win2012-Master virtual machine and open File Explorer > Computer. Double-click the CD Drive (D:) XenDesktop to launch the installer.

3. Click **Start** in the XenDesktop 7 installer.
4. Click **Virtual Delivery Agent for Windows Server OS**.
5. Select the appropriate configuration option.

   Select **Create a Master Image** and then click **Next**.

This option is selected because we are installing the VDA on a master image. For more information about optimizing XenDesktop machines, see Citrix article CTX125874 at *http://support.citrix.com*.

6. Select the core components to install.

   Verify that **Citrix Receiver** is selected and then click **Next**.

7. Choose your Delivery Controller configuration.

   a. Select **Do it manually**, type **c-1.cch.local** and then click **Add**.
   b. Enter the second Controller address, enter **c-2.cch.local** and click **Add**.

8. Click **Next**.
9. Select the features you would like to include in the installation.

   Select all features and then click **Next**.

10. Choose how you will configure your firewall rules.

    Select **Automatically** and then click **Next**.

These are the default ports used by the Controller. If you need to use different ports, select Manually and configure the respective ports after the installation completes.

11. Review the Installation Settings Summary and then click **Install** if the settings are correct.
12. Click **Finish** when the installation is complete. Windows configuration will continue and the virtual machine will be restarted.
13. Shut down the **Win2012-Master** virtual machine once the process is complete.
14. Eject the **Citrix_XenDesktop_7.iso** from the virtual machine.

To Create a Server OS Machine Catalog

1. Log on to a machine that has Citrix Studio installed on it.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Select the **Machine Catalogs** node in Studio.
4. Click **Create Machine Catalog** in the Actions pane.

The Machine Catalogs node is not visible until you have completed one of the initial configuration tasks presented when you first start Studio.

5. Click **Next**.
6. Select the type of machine catalog you want to create and then click **Next**.

   Select **Windows Server OS**.

7. Select the type of infrastructure that will deliver desktops and applications.

   Select **Virtual machines**.

8. Select the machine image management method.

   Select **Machine Creation Services (MCS)**.

9. Click **Next**.
10. Select the master image that you want to use and then click **Next**.

    Select **Win2012-Master**.

Ensure that the Win2012-Master virtual machine is turned off before continuing.

11. Select the number of virtual machines you would like to create and their resources.

    Select **1** virtual machine, with **1** Virtual CPU, and **1024** MB of memory, and then click **Next**.

12. Add computer accounts on the Active Directory Computer Accounts page.

    a. Select **Create new Active Directory accounts**.
    b. Select the **CCH Virtual Desktops > Servers** organizational unit.
    c. Specify the account-naming scheme as **HostedApps-#** and then click **Next**.

13. Define the scopes for the machine catalog on the Scopes page.

    Select **All** and then click **Next**.

14. Add a name and description before creating the machine catalog on the Summary page.

    Type **HostedApps** as the name of the machine catalog, leave the description blank, and then click **Finish**.

Creating a Machine Catalog for Windows Desktop

Desktop OS machine catalogs provide a Windows desktop environment and provide desktops and applications that are assigned to individual users.

Typically, end users who need a Desktop OS machine:

- Are task or knowledge workers who require personalized desktops of which they can take ownership
- Are mobile workers who want to access the same desktop from a variety of devices over different networks
- Need to install their own applications on their desktops

With these types of end users, you want to:

1. Standardize certain aspects of end users' desktops through the use of a common template
2. Deliver end users' desktops to any device regardless of hardware capability
3. Reduce desktop management costs while still providing your end users with a personalized desktop experience

To Install and Configure the VDA

1. Start the virtual machine that will become the master image for the Desktop OS machines.

   Start the **Win8-Master** virtual machine.

2. Log on to the virtual machine using domain administrator credentials.

   Log on using the **CCH\Admin1** and **Password1** credentials to log on to the Win8-Master-PvD virtual machine.

3. Attach the XenDesktop 7 media to the virtual machine.

   Select **Citrix_XenDesktop_7.iso** from the DVD Drive 1 field.

4. Start the XenDesktop 7 installer.

   a. Click **Desktop** and then click the **Windows Explorer** icon.
   b. Click **Computer** and then double-click **CD Drive (D:) XenDesktop**.

5. Click **Start** in the XenDesktop 7 installer.
6. Click **Virtual Delivery Agent for Windows Desktop OS**.
7. Select the appropriate configuration option.

   Select **Create a Master Image** and then click **Next**.

This option is selected because we are installing the VDA to a master image. For more information about optimizing XenDesktop machines, see Citrix article CTX125874 at *http://support.citrix.com*.

8. Determine which Virtual Delivery Agent to install.

   Select **No, install the standard VDA** and then click **Next**.

9. Select the necessary core components to install.

   Verify that **Citrix Receiver** is selected and then click **Next**.

10. Choose your Delivery Controller configuration.

    a. Select **Do it manually**, type **c-1.cch.local** and then click **Add**.
    b. Type **c-2.cch.local** and then click **Add**.

11. Click **Next**.
12. Select the features you would like to include in the installation.

    Select **Personal vDisk**, ensure that all other features are selected and then click **Next**.

13. Choose how you will configure your firewall rules.

    Select **Automatically** and then click **Next**.

These are the default ports used by the Controller. If you need to use different ports, select Manually and then configure the respective ports after the installation completes.

14. Review the Installation Settings Summary and then click **Install** if the settings are correct.
15. Click **Finish** when the installation is complete and allow the virtual machine to restart.
16. Log on to the virtual machine on which you want to run the inventory updater for Personal vDisk using domain administrator credentials.

    Log on to the **Win8-Master** virtual machine using the **CCH\Admin1** and **Password1** credentials.

17. Type **Update personal vDisk** on the Windows Start screen and then click **Update personal vDisk**.
18. Wait for the process to complete and shut down the virtual machine.

To Create a Desktop OS Machine Catalog

1. Log on to a machine that has Citrix Studio installed on it.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Select the **Machine Catalogs** node.
4. Click **Create Machine Catalog**.
5. Click **Next**.
6. Select the type of machine catalog you want to create.

   Select **Windows Desktop OS** and then click **Next**.

7. Select the type of infrastructure that will deliver desktops and applications.

   Select **Virtual machines**.

8. Select the machine image management method.

   Select **Machine Creation Services (MCS)**.

9. Click **Next**.
10. Select the appropriate desktop experience for your end users.

    Select **I want users to connect to the same (static) desktop each time they log on** and then select **Yes, save changes on a separate Personal vDisk**.

11. Select the master image you want to use.

    Select **Win8-Master** and then click **Next**.

12. Specify the number of virtual machines you would like to create and their configuration.

    Select::

    a. **2** as the number of virtual machines needed
    b. **1** Virtual CPU
    c. **1024** Memory (MB)
    d. **24** Personal vDisk size (GB)
    e. **P** Personal vDisk drive letter

13. Click **Next**.
14. Add computer accounts on the Active Directory Computer Accounts page.

    a. Select **Create new Active Directory accounts**.
    b. Select the **CCH Virtual Desktops > Desktops** organizational unit.
    c. Type **UserDesktop-##** in the Account naming scheme field and then click **Next**.

15. Define the scopes for the machine catalog on the Scopes page.

    Select **All** and then click **Next**.

16. Add a name and description before creating the machine catalog on the Summary page.

    a. Type **UserDesktops** as the machine catalog name.
    b. Type **Standard Windows 8 Desktops** as the description and then click **Finish**.

Discussion Question

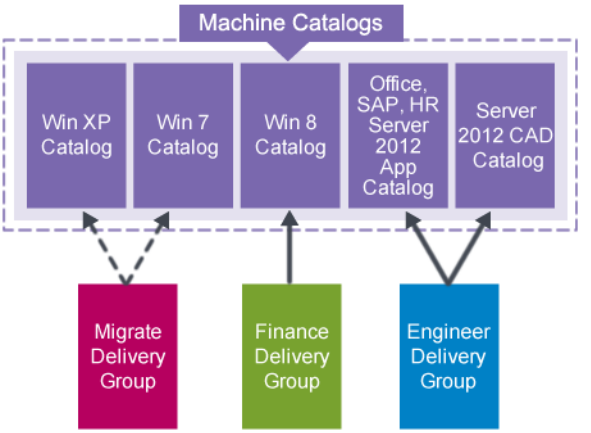
What are some reasons for creating a Server OS machine catalog as opposed to creating a Desktop OS machine catalog?

Managing Delivery Groups

Delivery Groups are a grouping of end users who require access to a common set of applications or desktop resources, and require the same end-user experience across those resources. A Delivery Group can access different machine catalogs as long as the machine catalogs consist of similar machine types. For example, end users assigned to the Engineer Delivery Group can access the hosted applications on the Server 2012 App Catalog as well as the CAD application hosted on the Server 2012 CAD Catalog; the desktop and the applications are delivered with a consistent end-user experience from a single Delivery Group.

In Studio, you cannot create mixed Delivery Groups from machine catalogs with different machine types. Machine catalog characteristics must match if you want to put the machines into a single group. For example, you cannot mix machines from Server OS machine catalogs with Desktop OS machine catalogs.

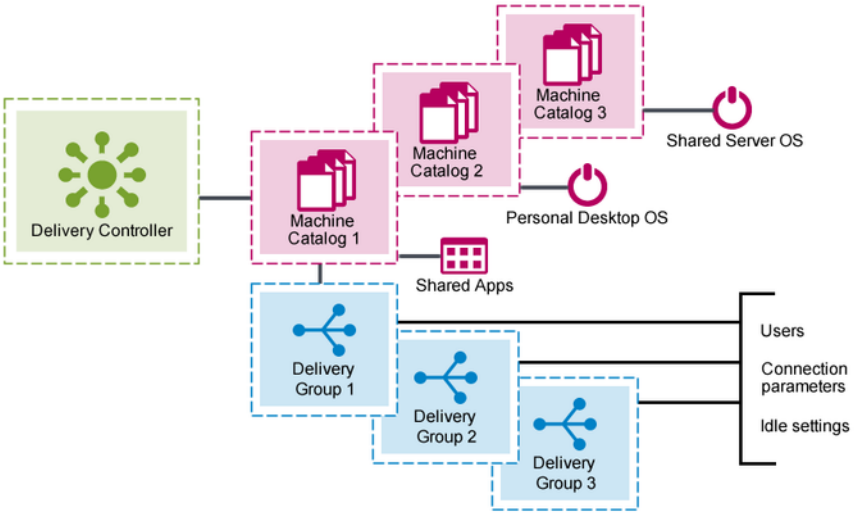
Defining the end-user experience in the Delivery Group means that you do not need to duplicate or maintain these settings across multiple pools of resources, and the backend resources can be changed without affecting the end-user experience.



You can create Delivery Groups for specific teams, departments, or types of end users. With Delivery Groups, you can:

- Specify groups of end users who access desktops, applications, or desktops and applications.
- Add end users and groups of users.

In order for end users to access resources from a machine catalog, a Delivery Group is required. When creating a Delivery Group, you will need to specify the end users, groups, applications, the desktop settings to match the end-user needs and the power management options for the desktops in the group.



To Create a Delivery Group for User Desktops

1. Log on to a machine that has Citrix Studio installed on it.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Select the **Delivery Groups** node.
4. Click **Create Delivery Group**.
5. Click **Next**.
6. Select a machine catalog for the Delivery Group and then specify the number of machines the group will consume from the machine catalog.

   Select the **UserDesktops** machine catalog and then specify **2** machines.

7. Click **Next**.
8. Select the type of resource that you want to deliver to your end users on the Delivery Type page.

   Select **Desktops**.

9. Click **Next**.

10. Add the user accounts and user groups that can access the resource.

    a. Click **Add users**, type **CCH\HR** and then click **OK**.
    b. Select **HR** and then click **OK**.
    c. Click **OK**.

11. Click **Next**.
12. Add your StoreFront server settings to automatically configure Citrix Receiver.

    Select **Manually, using a StoreFront server address that I will provide later** and then click **Next**.

13. Select the scope to assign to this Delivery Group.

    Use the default settings and then click **Next**.

14. Verify that all of the details on the Summary page are correct and then specify a Delivery Group name and display name.

    Type **HR Desktops** as the Delivery Group name and **HR Desktop** as the display name.

15. Click **Finish**.

To Create a Delivery Group for Application Delivery

1. Log on to a machine that has Citrix Studio installed on it.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Select the **Delivery Groups** node.
4. Click **Create Delivery Group**.
5. Click **Next**.
6. Select a machine catalog for the Delivery Group, and then specify the number of machines the group will consume from the machine catalog.

   Select the **HostedApps** machine catalog, and then add **1** machine.

7. Click **Next**.
8. Select the type of resource that you want to deliver to your end users on the Delivery Type page.

   Select **Applications**.

9. Click **Next**.

10. Add the user accounts and user groups that can access the resource.

    Click **Add users**, type **CCH\Domain Users**, click **Check Names**, and then click **OK**.

11. Click **Next**.
12. Select applications from the display on the Applications page, if the Delivery Group will provide applications.

It may take a few moments for the list of applications to populate. In the background, XenDesktop is starting the machine assigned to this catalog to inventory the applications available for publishing, and then populates this list.

    Select **WordPad** and **Calculator**, and then click **Next**.

13. Select the scope to assign to this Delivery Group.

    Use the default settings and then click **Next**.

14. Verify that all of the details on the Summary page are correct and then specify a Delivery Group name.

    Type **Hosted Applications** as the delivery group name.

15. Click **Finish**.

Discussion Question

How would you handle a request that asks you to provide access to a Windows 8 machine catalog and a Server 2012 machine catalog for one group of users?

To Add Machines to a Machine Catalog

1. Log on to a machine that has Citrix Studio installed on it.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Select the **Machine Catalogs** node and then select the machine catalog you want to add machines to.

   Select the **UserDesktops** machine catalog.

4. Click **Add Machines** in the Actions pane.
5. Specify the number of virtual machines that you want to add then click **Next**.

   Add **1** machine.

6. Ensure that the current Active Directory settings are correct for your environment.

   Use the default settings and then click **Next**.

7. Click **Finish**.

Studio creates the machine as a background process so that you can continue to work. Because XenDesktop creates virtual machines sequentially, this can be a lengthy process when you add a large number of machines to a machine catalog. Machine creation continues to completion even if you close Studio.

To Perform an Update to the Master Image Virtual Machine

It may be necessary to update desktops in a machine catalog when installing applications, when installing hotfixes or service packs into the base operating system, or when making any significant change to the original image.

1. Start the Master Image virtual machine and then log on using the domain administrator credentials.

   Start the **Win8-Master** virtual machine and then log on using the **CCH\Admin1** and **Password1** credentials.

2. Perform the desired changes.

    a. Type **\\DC-1\Share** in the Start screen and then press **Enter**.
    b. Double-click **Firefox Setup** and click **Run**.
    c. Ensure that **Standard** is selected and click **Next**.
    d. Click **Install** and then allow the installation to complete.
    e. Click **Finish**.

3. Update the Personal vDisk inventory on the virtual machine.

    a. Type **Update** into the Start screen and click **Update Personal vDisk.**
    b. Allow for the process to complete and shut down the virtual machine.

To Update the Desktops in a Machine Catalog

1. Log on to a machine that has Citrix Studio installed on it.

    Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Select the **Machine Catalogs** node in Studio and then select a machine catalog that you would like to update.

    Select the **UserDesktops** machine catalog.

4. Click **Update Machines**.
5. Select the delivery groups to be affected and then click **Next**.

    Select **HR Desktops** and then click **Next**.

6. Select the host and updated master image that you want to use and then click **Next**.

    Select the **Win8-Master** virtual machine image and then click **Next**.

7. Select the appropriate rollout strategy.

    Select **Immediately**.

    It is safe to roll out the changes immediately in the lab environment because there are no users currently logged in. This is likely not the case in a production scenario.

8. Click **Next**.
9. Verify that the details are correct and then click **Finish**.

Managing Computer Accounts

You can remove Active Directory computer accounts from Desktop OS and Server OS machine catalogs, and Organizational Units (OUs) from Remote PC Access machine catalogs in order to make unused accounts available for use in other machine catalogs. Similarly, you can attach additional accounts to a machine catalog so that when more machines are added to the machine catalog, the computer accounts are already in place.

To Manage Active Directory Accounts

1. Log on to a machine that has Citrix Studio installed on it.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Select the **Machine Catalogs** node.
4. Select a machine catalog in the center pane.

   Select the **AppServers** machine catalog.

5. Click **Manage AD Accounts**.
6. Click **Add**.
7. Type the object names to select and then click **Check Names**.

   Type **AppServer03;AppServer04** and then click **Check Names**.

8. Click **OK**.
9. Decide whether to reset the account password or to give them all the same password and then click **OK**.

   Select **Reset all account passwords** to negotiate new passwords for the pre-created computer accounts and then click **OK**.

10. Click **Close**.

Managing Power for Machines in a Desktop OS Delivery Group

Full and partial machine power management is available for Delivery Group machines. However, this only applies to Desktop OS machines. For Server OS machines, you can manage power settings by using reboot schedules.

To Manage Power for a Machine in a Delivery Group

1. Log on to a machine that has Citrix Studio installed on it.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Select the **Delivery Groups** node and then select the Delivery Group that you wish to control.

   Select **HR Desktops**.

4. Click **Edit Delivery Group** in the Actions pane.
5. Click **Power Management** in the left pane.
6. Edit the power management settings for the Delivery Group.

   a. Select **Weekdays** in Power on/off machines field.
   b. Type **30** machine for **When logged off** and select the action **Shutdown**.
   c. Set the hours as **6:00am to 9:00pm** for **During peak hours**.

7. Click **OK**.

There is a difference between power managing Desktop OS machines and Server OS machines in a Delivery Group. With Server OS machines, you can configure the restart schedule.

To Reallocate Machines in a Delivery Group

1. Log on to a machine that has Citrix Studio installed on it.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Select the **Delivery Groups** node.
4. Select the Delivery Group containing the machines you want to reallocate and then select **Edit Delivery Group**.

   Select **HR Desktops** and then select **Edit Delivery Group**.

5. Select the **Users** in the left pane and then add or remove the users and groups who can access any machines in the group.

You can use an import list to specify the users and groups who can access any existing or physical machines.

Click **Add users**.

6. Specify the users or groups you would like to add and then click **Check Names**.

   Type **CCH\Admin1** and then click **Check Names**.

7. Click **OK** twice.

Discussion Question

What is the time zone setting in the basic settings of a Delivery Group used for? What could be a reason to set two Delivery Groups to different time zones?

To Shut Down and Restart Desktops

1. Log on to a machine that has Citrix Studio installed on it.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Select the **Delivery Groups** node.
4. Select the Delivery Group containing the machines you want to shut down and then click **View Machines**.

   Select **HR Desktops** and then click **View Machines**.

5. Select the machine and then select the appropriate power management action from the Actions pane. Depending on the state of the machine, some of these options are not available:
   a. Force shutdown - Forcibly turns of the machine and refreshes the list of machines.
   b. Restart - Tells the machine operating system to shut down and start the machine again.
   c. Suspend - Pauses the machine without shutting it down and refreshes the list of machines.
   d. Shut down - Requests that the machine's operating system shut down.

   Select a machine that lists the power state as Off and then click **Start**.

6. Click **Yes**.

Discussion Question

You have been told by a Helpdesk administrator that an end user is experiencing problems when trying to launch an application. After investigating, you realize that the problem only happens on one server and only happens with new connections. How can you solve the problem?

Deleting Resources

From time to time existing resources may need to be deleted or reallocated to better fit the needs of your organization. The modularity of the XenDesktop design allow for objects to be reallocated or deleted in a very granular fashion to fit objectives.

Enabling and Disabling Maintenance Mode

Putting a machine in maintenance mode lets you perform administrative tasks on the associated image, such as applying updates and upgrade using image management tools.

User connectivity is affected as follows when in maintenance mode:

- With Server OS machines, end users can connect to existing sessions but cannot start new sessions.
- With Desktop OS and Remote PC Access machines, end users cannot connect or reconnect, once the machine is in maintenance mode. If the user is already connected, they will stay connected until they either disconnect or log off.

Machines are available for user connections when you take them out of maintenance mode.

To Enable and Disable Maintenance Mode

1. Log on to a machine that has Citrix Studio installed on it.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Select the **Delivery Groups** node.
4. Select the Delivery Group that you need to service and then click **View Machines** to locate individual machines.

   Select **Notepad Application Servers**.

5. Select the machine or Delivery Group and then click **Turn On Maintenance Mode**.

Select **AppServer-01.cch.local** and then click **Turn On Maintenance Mode**.

6. Click **Yes**.

Removing Desktops from Delivery Groups

Removing a machine deletes it from a Delivery Group but does not delete the associated virtual machine from the machine catalog on which the group is based. Therefore, the machines are available for assignment to other Delivery Groups.

You can only remove machines while in maintenance mode. Putting the machine in maintenance mode temporarily prevents end users from connecting to the machine while you are removing it.

Machines may contain personal data. Manage this activity appropriately, especially if the machine is allocated to another end user - for example, if you need to reimage the virtual machine.

To Remove Desktops from Delivery Groups

1. Log on to a machine that has Citrix Studio installed on it.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Select the **Delivery Groups** node.
4. Select a Delivery Group and then click **View Machines**.

   Select **Notepad Application Servers** and then click **View Machines**.

5. Select the machine and put it in maintenance mode.

   Select **AppServer-01.cch.local**. This machine should already be in maintenance mode.

6. Make sure the machine is shut down.
7. Click **Remove from Delivery Group**.
8. Click **Yes**.

Deleting a Delivery Group

There are Delivery Groups for desktops and for applications. There may be potential scenarios wherein you would need to move machines to another Delivery Group and then delete the leftover Delivery Group. This involves putting the Delivery Group into maintenance mode.

To Delete a Delivery Group

1. Log on to a machine that has Citrix Studio installed on it.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Click **Delivery Groups** and then select the Delivery Group to delete.

   Click **Delivery Groups** and then select the **Notepad Application Servers** Delivery Group.

4. Click **Delete Delivery Group** and then click **Yes**.

Deleting Machines from a Machine Catalog

When you delete a machine, end users can no longer access it, and the machine is deleted from the machine catalog. Before deleting the machine, make sure all user data is backed up. No end users can be logged on the machine that you want to delete. Put the machine in maintenance mode to stop end users from connecting to the machine.

If you want to delete the machine but retain the virtual machine it was created from and its associated Active Directory account, remove the machine from the Delivery Group. Do not delete the machine.

To Delete Machines from a Machine Catalog

1. Log on to a machine that has Citrix Studio installed on it.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Select **Machine Catalogs** in Citrix Studio and then select the catalog containing the machine to be deleted.

   Select **Machine Catalogs** and then select the **AppServers** machine catalog.

4. Click **View Machines** to view the machines associated with the machine catalog.
5. Select the machines to delete and then click **Delete**.

   Select **AppServer-01.cch.local** and then click **Delete**.

6. Select the Delete Options that fits the use case and then click **Next**.
   a. Select **Remove the virtual machines from the Catalog and delete the virtual machines**.

b. Select **Remove the accounts from the Catalog and delete them from Active Directory**.

c. Click **Next**.

7. Click **Finish**.

To Delete a Machine Catalog

1. Log on to a machine that has Citrix Studio installed on it.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Select **Machine Catalogs** in Citrix Studio and then select the catalog to be destroyed.

   Select **Machine Catalogs** and then select the **AppServers** machine catalog.

4. Click **Delete Machine Catalog**.
5. Click **Finish**.

Troubleshooting: Managing Desktops and Applications

Issue	Resolution
An administrator is unable to update desktops in a machine catalog.	Verify that the administrator has the appropriate permissions.
Unable to remove a machine from a machine catalog.	Verify that the machine is in maintenance mode prior to removal.
When creating an application in Studio, the desired application does not appear.	Verify that the application is installed on the application server/host.
Not all end users have access to a newly created application.	Verify that the application has been assigned to all of the required Delivery Groups. Verify that the application is enabled.
You are unable to power manage a machine.	Verify that the machine is a virtual machine. Physical machines cannot be power-managed through XenDesktop.
Users logon time is taking longer than usual.	Ensure that the power management settings for a Delivery Group are appropriate for the end users. Verify that different time zones are taken into consideration. 1. Choose the Delivery Group in which you would like to verify the time zone. 2. Click **Edit Delivery Group**. 3. Click **End user settings**. 4. Verify the time zone.
You are unable to reallocate a machine within a Delivery Group.	Ensure that the machine was not created using Provisioning Services, as they are unable to be reallocated.
Users in a Delivery Group are unable to access their applications or desktops.	Verify that maintenance mode is not enabled.

Reinforcement Exercise: Delivering Server Desktops

During this exercise, you will not be given step-by-step instructions for performing the task. Instead, you are asked to use what you have learned to complete it. This exercise is designed to take your newly-acquired knowledge and determine if you can apply it to perform a task you have never done before. In most instances the default value will be the best choice, but we encourage you to explore and try different options. If you have a question or need help, ask the instructor or a fellow student for assistance.

In this module, you have learned how to:

- Describe the XenDesktop 7 infrastructure for delivering desktops and applications.
- Describe the role of the Delivery Controller.
- Create and manage machine catalogs.
- Manage Delivery Groups.

Time to complete: Approximately 30 minutes

Your manager has asked you to publish a Server Desktop to all of the domain administrators on the network. As there are only a few domain administrators at CCH, you believe that a single server will easily fit this objective.

In order to deliver these desktops, you decide to use an existing machine catalog called HostedApps because it can fit your needs quickly. However, there are no more machines available in that catalog, so you will have to create them.

To complete your objective:

- Add one additional machine to the HostedApps machine catalog.
  - Use the default memory and processor resources.
  - Add the machine to the CCH Virtual Desktops > Servers organization unit.
  - Use the naming scheme ServerDesktop-#
- Add a new Delivery Group called ServerDesktops.
- Publish the desktops only to the CCH\Domain Admins group.

Module 5

Managing StoreFront and External Access

5

Managing StoreFront and External Access

Citrix StoreFront authenticates end users to XenDesktop sites, enumerating and aggregating available desktops and applications into stores that end users access through Citrix Receiver for Android, iOS, OSX, Linux, Windows, Win8/RT, or Receiver for Web sites. StoreFront is the successor to Web Interface and has been built on a modern, more flexible and powerful framework that enables StoreFront to provide next generation features, such as:

- A unified StoreFront that delivers SaaS & native mobile applications and XenDesktop resources.
- Simplified Account Provisioning, which enables end users to connect to assigned desktops and applications by simply entering their email or a server address, or by opening a Provisioning File in Receiver.
- Access from any Receiver with a consistent user experience, including automatic fallback to an HTML 5 client if a native client is not available locally and cannot be installed.
- Synchronization of resource subscriptions across all platforms and devices (Follow-me Apps & Data).

After completing this module you will be able to:

- Discuss StoreFront components and the communication that takes place within its architecture.
- Create, add, hide, and remove stores within StoreFront.
- Manage authentication services.
- Control the resources that are made available through stores.
- Manage Citrix Receiver updates.

Module timing: Approximately 3 hours

StoreFront Architectural Overview

StoreFront is a front-end Web server responsible for aggregating resources from different locations and presenting end users with a list of resources, including desktops and applications. When an end user subscribes to a resource, the presentation and home page display of that resource are customizable.

When planning your StoreFront deployment, consider the following recommendations:

- Citrix recommends hosting StoreFront on a dedicated instance of IIS. Installing other Web applications on the same IIS instance as StoreFront could have security implications for the overall StoreFront infrastructure.
- In a production environment, Citrix recommends using HTTPS to secure communications between StoreFront and end-users' devices. To use HTTPS, StoreFront requires that the IIS instance hosting the authentication service and associated stores is configured for HTTPS. In the absence of the appropriate IIS configuration, StoreFront uses HTTP for communications.
- StoreFront servers must reside within the same Microsoft Active Directory forest as the XenDesktop servers hosting end-users' resources. All the StoreFront servers in a group must reside within the same domain. To enable smart card and user certificate authentication, end-users' accounts must be configured within the Active Directory forest containing the StoreFront servers.
- Consider implementing multiple StoreFront servers to ensure high availability if the primary server hosting StoreFront fails.
- Configure the external load balancer to fail over between the servers to ensure users have uninterrupted access to their applications and desktops.

StoreFront Components

StoreFront consists of several components and are described in the following section:

- **StoreFront Server** - The StoreFront server records details of end-user application subscriptions locally along with associated shortcut names and locations. When an end user accesses a store, the application synchronization feature automatically updates the subscribed applications on the end-user device to match the configuration stored on the StoreFront server. The credentials are later retrieved by the Store Service to authenticate to XenDesktop, ensuring that end users have a consistent experience across all devices.

StoreFront requires a minimum of 2 GB of storage space on the StoreFront server.

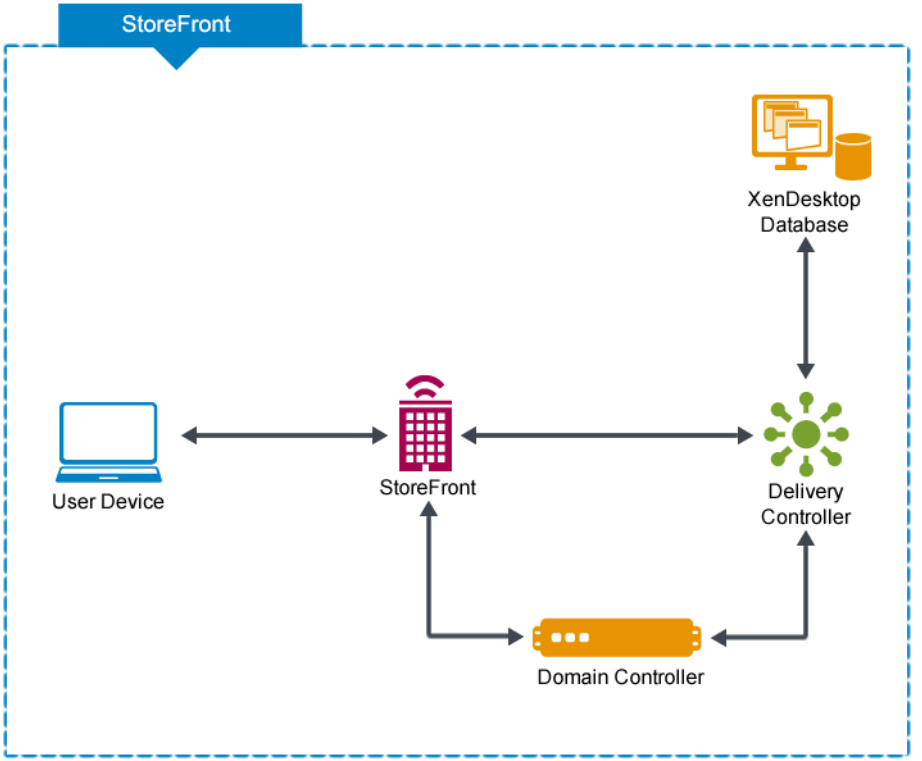
- **Authentication Service** - The StoreFront authentication service authenticates end users to XenDesktop sites. When an end-user's credentials have been validated, the authentication

service handles all subsequent interactions to ensure that the user only needs to log on once. The credentials are stored using built-in Windows security features.

- **Store** - The store retrieves end-user credentials from the authentication service to authenticate end users to the components providing the resources. The store also enumerates and aggregates the resources currently available from XenDesktop sites and the Delivery Controller (SaaS applications). End users access the store through Citrix Receiver or a Receiver for Web site.
- **Receiver for Web site** - This site enables end users to access stores through a Web page. Furthermore, this site can verify the version of Receiver installed locally on the end-user device and guide the end user through an upgrade or installation procedure if required. In scenarios where Receiver cannot be locally installed, an HTML 5-based Receiver will be used.

StoreFront Communication

This graphic explains the flow of communication between the components and StoreFront.



1. An end user enters a username and password into Receiver, which is then sent to the StoreFront server. End users may skip this step if pass-through authentication is configured.
2. The authentication service of StoreFront retrieves the end-user credentials and validates them with a domain controller. The StoreFront server must be a member of the same Active Directory forest as the end-user account and the accessed resources.
3. StoreFront retrieves the end-user's application subscriptions locally and loads them into memory.
4. StoreFront forwards the end-user credentials as part of an XML query to the XenDesktop Delivery Controller.
5. The Delivery Controller validates the end-user credentials with a domain controller.
6. After a successful validation, the Delivery Controller checks which resources have been published for this end user within its SQL Server database.
7. The Delivery Controller sends an XML response to StoreFront, which contains all resources available for the end user from the XenDesktop site.
8. StoreFront sends the list of available resources including the existing subscriptions to Citrix Receiver or displays them in the Receiver for Web site.

Discussion Question

Where is the physical location of the StoreFront server on your network?

What advantages does StoreFront offer in place of Web Interface?

StoreFront Management Console

After the initial configuration of StoreFront, other tasks that enable you to manage your deployment become available in the StoreFront management console. This console gives you the following access:

- **Stores** - Create, configure, and manage stores.
- **Receiver for Web** - Create and configure a Web-based point of access for end users.
- **Citrix NetScaler Gateway** - Configure NetScaler connection settings.
- **Server Groups** - Customize StoreFront server groups.
- **Beacons** - Manage beacon points for external and internal access.
- **Authentication** - Configure the authentication process for the StoreFront site.

Creating a New Store

StoreFront allows you to create as many stores as needed for a particular group of end users or to group together a specific set of resources. To create a store, you must identify and configure communications with the servers providing the resources that you want to make available in the store. You will then have the option to configure remote access through NetScaler.

To Create and Add a New Store

1. Log on to the primary StoreFront server using domain administrator credentials.

   Log on to the **StoreFrontServer-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Open Citrix StoreFront.
3. Select the **Stores** node.
4. Click **Create Store**.
5. Specify the store name.

   Type **Store**.

6. Click **Next**.
7. Click **Add** on the Delivery Controllers page.
8. Type a name for the Delivery Controller.

   Type **Delivery Controller**.

9. Select **XenDesktop** as the type of Delivery Controller.
10. Click **Add**.
11. Type the name or IP address of a Delivery Controller in the environment.

    Type **C-1.cch.local**.

12. Click **OK**.
13. Click **Add**.
14. Type the name or IP address of a Delivery Controller in the environment.

    Type **C-2.cch.local**.

15. Click **OK**.
16. Select the types of connections that StoreFront will use to communicate with the Delivery Controllers from the Transport type list.

    Select **HTTP**.

17. Specify the port for StoreFront to use for connections to the XenDesktop site.

    Verify that **80** is specified in the Port field..

18. Click **OK**.
19. Click **Next**.
20. Specify whether and how end users connecting from public networks can access the store through NetScaler on the Remote Access page.

    Select **None**.

If it is not already enabled, the pass-through from NetScaler authentication method is automatically enabled when you configure remote access to the store through NetScaler. End users authenticate to NetScaler and are automatically logged on when they access their stores.

21. Click **Create**.
22. Click **Finish**.

Hiding a Store

Hiding a store will prevent end users from adding stores to their accounts when they configure Citrix Receiver through email-based account discovery. By default, when you create a store it is presented as an option for end users to add within Citrix Receiver when they discover the StoreFront server hosting the store. Hiding the store does not make it inaccessible; instead end users must configure Citrix Receiver with connection details for the store, either manually using a setup URL, or with a provisioning file.

To Hide a Store

1. Log on to the StoreFront virtual machine using domain administrator credentials.

   Log on to the **StoreFrontServer-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Open Citrix StoreFront.
3. Select the **Stores** node.
4. Select the store you would like to hide.

   Select **CCH**.

5. Click **Hide Store**.
6. Click **Hide**.

Discussion Question

What is the impact of a StoreFront server failure on the end user?

Managing Authentication

The management of authentication within StoreFront is necessary to allow end users access to XenDesktop applications and desktops. StoreFront will then handle all interactions to ensure that end users only need to log on once.

Configuring Authentication

You can enable or disable end-user authentication methods set up when the authentication service was created by selecting an authentication method within the StoreFront management console. If end users are having difficulty accessing the store or Receiver for Web site, you may need to review their authentication settings.

To Configure Authentication Methods

1. Log on to the StoreFront virtual machine using domain administrator credentials.

   Log on to the **StoreFrontServer-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Open Citrix StoreFront.
3. Select the **Authentication** node.
4. Click **Add/Remove Methods** within the Actions pane.
5. Specify the access methods that you want to enable or disable for your end users.

   Select the following methods:

   - **User name and password**
   - **Domain pass-through**
   - **Pass-through from NetScaler Gateway**

6. Click **OK**.

Discussion Question

What authentication methods have you used? What are the benefits of each?

Enabling End Users to Change Their Passwords

You can perform this task to enable end users accessing stores with explicit domain credentials to reset their expired passwords when logging on. When this setting is enabled, end users who cannot

log on because their passwords have expired are redirected to the Change Password dialog box. StoreFront then contacts the domain controller to reset the end-user password.

To Enable End Users to Change Expired Passwords

1. Log on to the StoreFront virtual machine using domain administrator credentials.

   Log on to the **StoreFrontServer-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Open Citrix StoreFront.
3. Select the **Authentication** node.
4. Click **Manage Password Options** in the Actions pane.
5. Select the appropriate option.

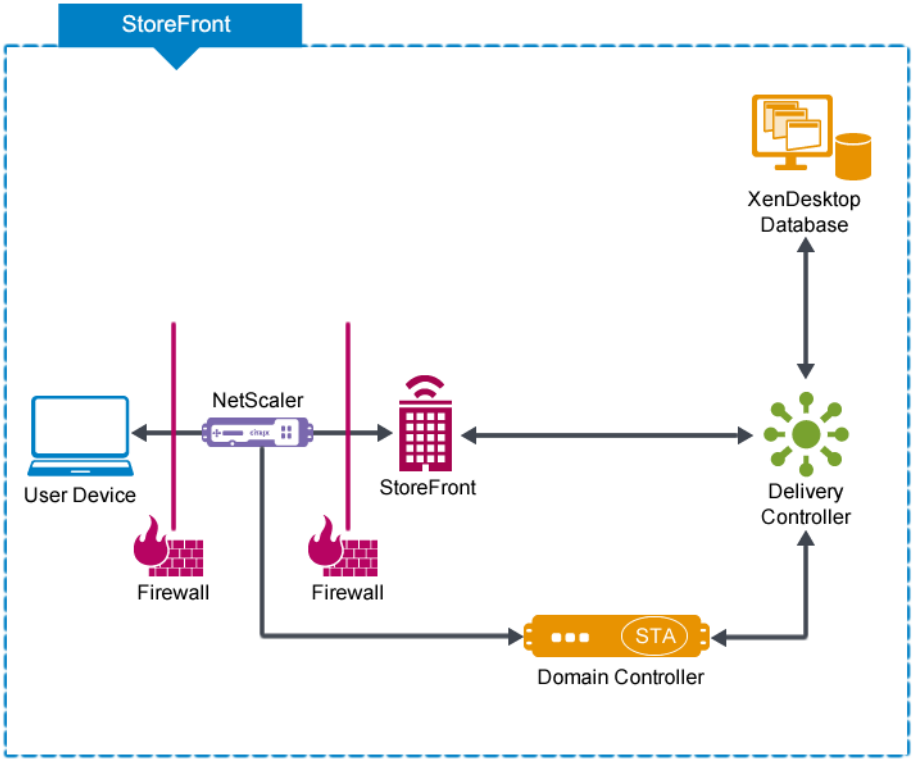
   Select **At any time**.

6. Click **OK**.

Enabling Remote Access to the Store

One of the methods available to secure connections established in a XenDesktop environment is to use a Citrix NetScaler. NetScaler is a physical or virtual appliance that acts as a single point of connectivity, routing all sessions through the appliance in order to provide a secure remote VPN or HTTPS link.

The NetScaler allows you to apply application-level policies and action controls to control access to resources within the environment. The following diagram describes the communication between StoreFront and NetScaler.



1. The end user enters their username and password, which is then sent to the NetScaler.
2. The NetScaler appliance authenticates the end user through the domain controller.
3. If the end user was successfully authenticated, credentials are passed through to the StoreFront server.

4. StoreFront retrieves the end-user's application subscriptions locally and loads them into memory.
5. StoreFront forwards the end-user credentials as part of a XML query to the Delivery Controller.
6. The Delivery Controller validates the end-user credentials with a domain controller.
7. After a successful validation the Delivery Controller verifies which resources have been published to this end user within its database.
8. The Delivery Controller sends an XML response to StoreFront, which contains all resources available for the end user from the XenDesktop site.
9. StoreFront sends the list of available resources including the existing subscriptions to Receiver.
10. Upon launching an application or desktop, the StoreFront server communicates with the Secure Ticket Authority (STA) located on the Delivery Controller.
11. The STA generates a token that is sent back to the StoreFront server.
12. Using the token information, the StoreFront server then generates the ICA file and delivers it to the end-user device.
13. The end-user device then launches the ICA file which directs the session to the NetScaler.
14. The NetScaler validates the token through Secure Ticket Authority (STA) on the Delivery Controller.
15. If the token is valid, the NetScaler retrieves the application or desktop address and launches a session.

To Enable Remote Access to a Store

1. Log on to the StoreFront virtual machine using domain administrator credentials.

   Log on to the **StoreFrontServer-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Open Citrix StoreFront.
3. Select the **Stores** node.
4. Select the store in which you would like to enable remote access.

   Select **Store**.

5. Click **Enable Remote Access**.
6. Select the type of remote access you would like to apply.

   Select **No VPN tunnel**.

7. Click **Add** to add NetScaler appliances.
8. Type a display name for the appliance.

   Type **NS-1**.

9. Type the NetScaler Gateway URL into the NetScaler Gateway URL field.

   Type ***https://access.cch.local***.

10. Change the version to the appropriate option.

    Select **10.0 (Build 69.4) or later**.

11. Select the appropriate logon type.

    Select **Domain**.

12. Type the callback URL.

    Type ***https://access.cch.local***.

13. Click **Next**.
14. Click **Add** on the Secure Ticket Authority window.
15. Type the Secure Ticket Authority (STA) URL.

    Type ***https://C-1.cch.local***.

16. Click **OK**.
17. Click **Create**.
18. Select the default appliance.

    Select **NS-1**.

19. Click **OK**.

Configuring the NetScaler with a Secure Ticket Authority (STA)

For the NetScaler to validate the integrity of the token generated by the STA, you must configure NetScaler with the addresses of the appropriate STAs.

To configure the NetScaler with a STA:

To Configure the NetScaler with a STA

1. Log on to the management system using domain administrator credentials.

Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Open **Firefox** and access the NetScaler Configuration utility.
    a. Double-click **Firefox** on the desktop.
    b. Type **10.29.0.12**.
    c. Press **Enter** to access the NetScaler Configuration utility
3. Log on to the NetScaler appliance.

    Log on with the **nsroot** and **Password1** credentials.
4. Click the **Configuration** tab and then select the **Access Gateway** node in the left pane.
5. Select the **Virtual Servers** node.
6. Double-click **STA Servers**.
7. Click the **Published Applications** tab.
8. Click **Add** in the Secure Ticket Authority pane.
9. Type the URL of the STA.

    Type ***https://C-1.cch.local***.
10. Click **Create**.
11. Click **OK**.

Creating Endpoint Analysis Policies

NetScaler allows the creation of pre-authentication policies to determine if an end-user device is allowed to log on to through the gateway. A pre-authentication policy will either allow or disallow an end user to log on based on the result of the endpoint analysis scan.

To Create Endpoint Analysis Policies

1. Log on to the management system using domain administrator credentials.

Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Open **Firefox** and access the NetScaler Configuration utility.
    a. Double-click **Firefox** on the desktop.
    b. Type **10.29.0.12**.
    c. Press **Enter** to access the NetScaler Configuration utility.
3. Select the **Access Gateway** node within the NetScaler Configuration utility.
4. Expand the **Policies** node.
5. Select **Pre-Authentication**.
6. Click **Add**.
7. Type a name for the policy.

    Type **deny_AVG** in the Name field.

8. Click **New** next to the Request Profile drop-down list box.
9. Specify a name for the profile.

    Type **deny_logon** in the Name field.

10. Select the appropriate action.

    Select **DENY** in the Action field.

11. Click **Create**.
12. Select **Add** below the Expression box.
13. Select the appropriate expression type.

    Select **Client Security** in the Expression Type field.

14. Select the component for your policy.

    Select **Anti-Virus** in the Component field.

15. Type the name of the file, process, operating system, etc. in the Name field.

    Type **AVG.exe** in the Name field.

16. Select **Version** in the Qualifier field.
17. Select the appropriate operator.

    Select == in the Operator field.

18. Type a value for the version.

    Type **2.0** in the Value field.

19. Click **OK**.
20. Click **Create**.
21. Click **Close**.
22. Click **Global Bindings** to link the policy.
23. Click **Insert Policy**.
24. Select the appropriate policy to apply.

    Select **deny_AVG**.

25. Click **OK** to apply.

Discussion Question

Which types of Endpoint Analysis scans would benefit your environment?

Managing Delivery Controllers

After creating a store within StoreFront, you may need to add other controllers. Adding controllers alleviates the issue of having a single point of failure. There may also be times in which you want to modify or remove existing Delivery Controllers that are available to a particular store.

Adding Delivery Controllers

StoreFront has the capability to aggregate several independent infrastructures, such XenApp farms or additional XenDesktop sites, to seamlessly present all available resources from each available infrastructure to users in a single location.

To Add Delivery Controllers

1. Log on to the StoreFront virtual machine using domain administrator credentials.

Log on to the **StoreFrontServer-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Open Citrix StoreFront.
3. Select the **Stores** node in the StoreFront console.
4. Select a store in the center pane.

   Select **Store**.

5. Click **Manage Delivery Controllers** in the Actions pane.
6. Click **Add** to include desktops and applications from another site, farm, or virtual appliance in the store.
7. Specify a name to help identify the deployment in the Display name field.

   Type **XenApp 6.5 Farm** in the Display name field.

8. Indicate whether the resources that you want to make available are provided by XenDesktop, XenApp, AppController, or VDI-in-a-Box.

   Select **XenApp**.

9. Click **Add**, type the name or IP address of Delivery Controllers running the Citrix XML Service and then click **OK**.

   Type **xenapp-1.cch.local** and then click **OK**.

The resource added in this step, "xenapp-1.cch.local" does not exist in this lab environment. It is being used for illustrative purposes only.

10. Select the type of connection in Transport type.

    Select **HTTP**.

If you are using certificates to secure connections between StoreFront and XenDesktop sites, ensure that the server names you specify in the Servers list match exactly (including the case) the names on the certificates for the servers.

11. Click **OK** twice.

To Remove Delivery Controllers

1. Log on to the StoreFront virtual machine using domain administrator credentials.

Log on to the **StoreFrontServer-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Open Citrix StoreFront.
3. Select the **Stores** node.
4. Select a store to delete in the results pane.

   Select **Store**.

5. Click **Manage Delivery Controllers** in the Actions pane.
6. Select a Delivery Controller and then click **Remove** to stop StoreFront from contacting that Delivery Controller or server when enumerating the resources that are available.

   Select **XenApp 6.5 Farm** and then click **Remove**.

7. Click **OK**.

Discussion Question

How can StoreFront help you transition from previous versions of Citrix products?

Managing Receiver Updates

In order for end users to have the most updated version of Receiver, it is important to specify the mechanism for the delivery of these updates. This procedure will offer options on how to manage these updates and allow end users to have full functionality of stores.

To Manage Receiver Updates

1. Log on to the StoreFront virtual machine using domain administrator credentials.

Log on to the **StoreFrontServer-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Open Citrix StoreFront.
3. Select the **Stores** node.
4. Select the store for you want to manage Receiver updates.

   Select **Store**.

5. Click **Manage Citrix Receiver Updates** in the Actions pane.
6. Specify how end users accessing the store receive plug-in updates for their Citrix Receiver.

   Select **Citrix (citrix.com)**.

7. Select the Citrix Update Options and then click **OK**.

   Select **Secure Access Plug-in** and then click **OK**.

Removing a Store

If an existing store is being replaced or is no longer usable for a particular group or user, it may be necessary to remove the store. When a store is removed, any associated Receiver for Web sites are also deleted.

To Remove a Store

1. Log on to the StoreFront virtual machine using domain administrator credentials.

Log on to the **StoreFrontServer-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Open Citrix StoreFront.

3. Select the **Stores** node.
4. Select the store that you want to remove.

   Select **CCH**.

5. Click **Remove Store**.
6. Click **Remove**.

Discussion Question

How does the propagation process work if you have a deployment of two StoreFront servers?

Troubleshooting: Managing StoreFront

Issue	Resolution
Receiver for Windows end users cannot log on to stores using pass-through authentication, even though the domain pass-through authentication method is enabled in the StoreFront authentication service.	To resolve this issue, run the command `Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $True` from a Windows PowerShell command prompt on the server hosting the XenDesktop connection broker.

StoreFront supports Windows event logging for the authentication service, stores, and Receiver for Web sites. Any events that are generated are written to the StoreFront Application log, which can be viewed using the Event Viewer under either Applications and Services Logs > Citrix Delivery Services or Windows Logs > Application. For more information about event logging, see Citrix eDocs at *http://edocs.citrix.com*.

Reinforcement Exercise: Create and Configure a New Store

During this exercise, you will not be given step-by-step instructions for performing the task. Instead, you are asked to use what you have learned to complete it. This exercise is designed to take your newly-acquired knowledge and determine if you can apply it to perform a task you have never done before. In most instances the default value will be the best choice, but we encourage you to explore and try different options. If you have a question or need help, ask the instructor or a fellow student for assistance.

In this module, you learned how to:

- Discuss StoreFront components and the communication that takes place within its architecture.
- Create, add, hide, and remove stores within StoreFront.
- Manage authentication services.
- Control the resources that are made available through stores.
- Manage Citrix Receiver updates.

Time to complete: Approximately 30 minutes

CCH has a legacy Web Interface server that has been decommissioned and is waiting to be replaced with a Citrix StoreFront server. The StoreFront server will initially be used for your internal CCH users of Receiver to access desktops and applications. Eventually, the design will incorporate a StoreFront site that is being rolled out externally and used across the business.

Your objective is to:

- Create a new store called CCH.
- Add both of the XenDesktop Delivery Controllers that exist in the environment.
- Allow access to XenDesktop using a HTTP connection only.
- Configure the store to be the default store to ensure that users of earlier Citrix client-side software will be able to access the store.
- Perform the following tests from the EndPoint-Internal virtual machine using the CCH\HRUser1 and Password1 credentials.
    - Confirm that you can successfully access your StoreFront site via a Web browser.
        - Install Citrix Receiver onto the virtual machine through the Web browser.
    - Confirm that you can connect to the store through Receiver.
    - Confirm that end users can view their allocated applications and subscriptions.

Module 6

Managing Policies and Profiles

6

Managing Policies and Profiles

Policies are the most efficient method of controlling connection, security, and bandwidth settings. You can create policies for specific groups of end users, devices, or connection types. Each policy can contain multiple settings. For example, you can configure settings to:

- Control sound quality for end-user devices.
- Allow end users to access the Documents folder on their local end-user device.
- Allow or prevent remote end users from being able to save to their hard drives from within a session.
- Allow or prevent end users from accessing the Windows clipboard.
- Monitor CPU usage, HDX (ICA) latency, and profile load time.

Citrix policies can be managed through Group Policy in Microsoft Windows or within the Citrix Studio console in XenDesktop. The console or tool you use depends on whether you have the appropriate permissions to manage Group Policy, where policies will be stored, and how policies will be maintained.

You can also use Citrix policies to accommodate your end users' varying needs. With policies you can apply different profile behavior to the machines in each Delivery Group. For example, one Delivery Group might require Citrix mandatory profiles, whose template is stored in one network location, but another Delivery Group might require Citrix roaming profiles stored in another location with several redirected folders.

Citrix Profile management provides you with an easy, reliable, and high-performance way to manage end-user personalization settings in a virtualized or physical Windows environment. Citrix Profile management requires minimal infrastructure and administration, and provides end users with fast logons and logoffs. Whichever profile solution you choose, you can access diagnostic information for and troubleshoot end-user profiles.

For more information about profile solutions, see Citrix eDocs at *http://edocs.citrix.com*.

After completing this module, you will be able to:

- Create, apply, and edit a policy in Studio and as a Group Policy Object (GPO).
- Prioritize policies in Studio and within Active Directory GPOs.
- Use, import, and export a user policy template within Studio and Active Directory.
- Run and obtain a resultant set of policy (RSOP) report.
- Configure folder redirection and streaming user profiles.
- Manage profile settings using Citrix policies.
- Resolve conflicting profiles.

Module timing: Approximately 5 hours

Creating Policies Using Studio

If you do not have the necessary permissions to manage Group Policy, or if filtering mechanisms such as SmartAccess are required, use Studio to create policies for your site. Policies created using Studio are stored in the site database and updates are pushed to the end-user session either when the machine registers with the broker or when an end user connects to the relevant resource.

Before you create a policy, decide which group of end users or devices you want it to affect. You may want to create a policy based on end-user job function, connection type, end-user device, or geographic location.

Unfiltered Policy

You have the option of creating policies that can be assigned to all objects in a site, or using the pre-created unfiltered policy. Unfiltered policies are created by default upon the installation of XenDesktop. By default, unfiltered policies apply to all objects and sessions within the site, allowing you to configure global, organization-based settings within one policy. If you want policies to impact specific groups or end users or objects, you can use policy filters to apply these settings. The pre-created unfiltered policies cannot be deleted.

Using a Policy Template in Studio

Templates can help you save time when administering a large environment and are also useful for establishing standards that multiple administrators can use.

You can create templates from either an existing template or an existing policy. Several computer policy templates already exist for specific purposes. New policies can be created from these templates and modified as needed or you can choose to create your own custom policy templates. The new template is then populated with the same settings as the original template or policy. Any assignments specified in the original policy are not included in the template.

To Create a New Template

1. Log on to the machine that has Citrix Studio installed.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Select **Policy** in the left pane of Studio and then select the **Templates** tab.

If the Welcome screen for Citrix Policies appears, select Don't show this again and then click Close.

4. Select the template that you want to implement and then create a new policy from it.

   Select **High Definition User Experience** and then click **Create Policy from Template** in the Actions pane.

5. Use the recommended settings and then click **Next**.
6. Select how you would like to apply the policy and then click **Next**.

   a. Click **Assign** to the right of the User or Group option.
   b. Type **CCH\RemoteEmployees** in the User or group name field.
   c. Click **+** and then type **CCH\LocalEmployees** in the new User or group name field.
   d. Select **Deny** in the Mode menu of the new entry and then click **OK**.
   e. Click **Next**.

7. Type a policy name and then click **Finish**.

   Type **User Experience Enhancements for Remote Employees** and then click **Finish**.

To Create a Policy Using Studio

1. Log on to the machine that has Citrix Studio.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Select **Policy** in the left pane of Studio.
4. Click **Create Policy** in the Actions pane. The New Policy wizard opens.
5. Add and configure individual policy settings, as required and then click **OK**.

   a. Select **Desktop UI** from the All Settings menu
   b. Click **Select** to the right of the **Menu animation** setting.
   c. Select **Prohibited** and then click **OK**.
   a. Click **Select** to the right of the View window contents while dragging setting.
   b. Select **Prohibited** and then click **OK**.

6. Click **Next**.
7. Assign the policy to a particular user or group or assign to it all objects within the site and then click **OK**.

   a. Click **Assign** to the right of the **Delivery Group** object.
   b. Select **HR Desktops** from the Delivery Group field and then click **OK**.

8. Click **Next**.
9. Enter a unique name for the new policy or accept the default name that is generated automatically.

   Type **Disabled Desktop UI Elements** as the policy name.

10. Click **Finish** to create the policy.

Applying a Policy Using Studio

When you assign a policy to certain end users and machine objects, that policy is applied to connections according to specific criteria or rules. If no assignments are added, the policy is applied to all connections. You can add as many assignments as you want to a policy, based on a combination of criteria.

You must add at least one assignment to a policy for that policy to be applied correctly. If you do not add any assignments, policy settings are applied to all user sessions, unless those policy settings are overridden by settings in a policy with a higher priority.

Citrix recommends that you apply policies to groups rather than individual end users. If you apply policies to groups, assignments are updated automatically when you add or remove end users from the group.

To Apply a Policy

1. Log on to the machine that has Citrix Studio installed.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Select **Policy** in the left pane of Studio.
4. Click the **Policies** tab and then select an existing policy or create a new policy.

   Select the **Disabled Desktop UI Elements** policy.

5. Click **Edit Policy** in the Actions pane to open the Policy Wizard.
6. Configure policy settings, if necessary and then click **Next**.

   Click **Next**.

7. Click **Assign** or **Edit** for each user or machine object to which you want to assign the policy.

    a. Select **Edit** to the right of the **Delivery Group** object.
    b. Click **+** and then select **Hosted Applications** from the Delivery Group field.
    c. Click **OK**.

8. Click **Next** to use the existing assignment settings and then click **Finish** to complete editing the policy.

Editing a Policy Using Studio

If you want to apply another policy setting, consider editing the existing policy and configuring the appropriate options instead of creating an additional policy. Avoid creating a new policy solely to enable a specific setting or to exclude the policy from applying to certain end users.

To edit a policy:

To Edit a Policy

1. Log on to the machine that has Citrix Studio installed.

    Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Select **Policy** in the left pane of Studio.
4. Click the **Policies** tab and then select an existing policy or create a new policy.

    Click the **Policies** tab and then select the **Disabled Desktop UI Elements** policy.

5. Click **Edit Policy** in the right pane to open the Policy Wizard.
6. Add or edit the policy settings and then click **OK**.

    a. Select **Desktop UI** from the All Settings menu.
    b. Click **Select** to the right of the **Desktop wallpaper** setting.
    c. Select **Prohibited** and then click **OK**.

7. Click **Next**.
8. Adjust user and machine assignments, if necessary and then click **Next**.

    Click **Next**.

9. Click **Finish**.

Prioritizing Policies Using Studio

When creating policies for a site, you may encounter a situation in which specific end users require exceptions to the current policy. This action is taken by creating policies and prioritizing them.

Prioritizing policies allows you to define the precedence of policies when they contain conflicting settings. You prioritize policies by giving them different priority numbers. By default, new policies are given the lowest priority. If policy settings conflict, a policy with a higher priority overrides a policy with a lower priority.

To Prioritize a Policy

1. Log on to the machine that has Citrix Studio installed.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Select **Policy** in the left pane of Studio.
4. Click the **Policies** tab and then select an existing policy.

   Click **Policies** and then select the **Disabled Desktop UI Elements** policy.

5. Click **Higher Priority** or **Lower Priority** in the right pane to change the policy to a higher or lower priority, as necessary.

   Select **Higher Priority** for the Disabled Desktop UI Elements policy.

Discussion Question

What type of policy should you configure if you need to create specific settings and want them applied globally across your organization?

What if there are end users or objects that should not be affected by these policy settings?

To Create a Computer Template in Studio

1. Log on to the machine that has Citrix Studio installed.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Select **Policy** in the left pane of Studio and then select the **Policies** tab.

4. Select the policy you would like to use as a template.

   Select the **Disabled Desktop UI Elements** policy that you previously configured.

5. Right-click the policy and select **Save as Template**.
6. Verify the settings, click **Unselect** to the right of any settings that you want to exclude from the template, and then click **Next**.

   Click **Next**.

7. Type a name for the template and a description.

   Type **Disabled Desktop UI Elements** without a description.

8. Click **Finish**. The new template appears on the Templates tab of Studio.

Exporting a Policy Template Using Studio

Exporting a policy template allows you to create backups of your template files to aid in the recovery of policy configurations. It also allows you to supply policy configurations from your site to aid Citrix Support in troubleshooting issues.

You can also export policies created in Studio into Group Policy Objects.

To Export a Policy Template

1. Log on to the machine that has Citrix Studio installed.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Select **Policy** in the left pane of Studio.
4. Click the **Templates** tab and then select the template you want to export.

   Click the **Templates** tab and then select **Disabled Desktop UI Elements** in the Custom templates field.

5. Click **Export Template**. The Export Template dialog box appears.
6. Select the location where you want to save the template and then click **Save**. A .gpt file is created in the location you specified.

   Type **\\DC-1\Share\Policies** in the Address field of the Export Template window and then click **Save**.

Importing a Policy Template Using Studio

Policy templates are local to the computer on which you are running the console to manage your site. You can transfer policy configurations between environments, including other sites that you manage on the computer running the console.

You can transfer templates by importing or exporting them. Importing a policy template allows you to implement policy configurations from servers in other sites, or policy configurations created by Citrix Support to resolve issues in your site.

To Import a Policy Template

1. Log on to the machine that has Citrix Studio installed.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

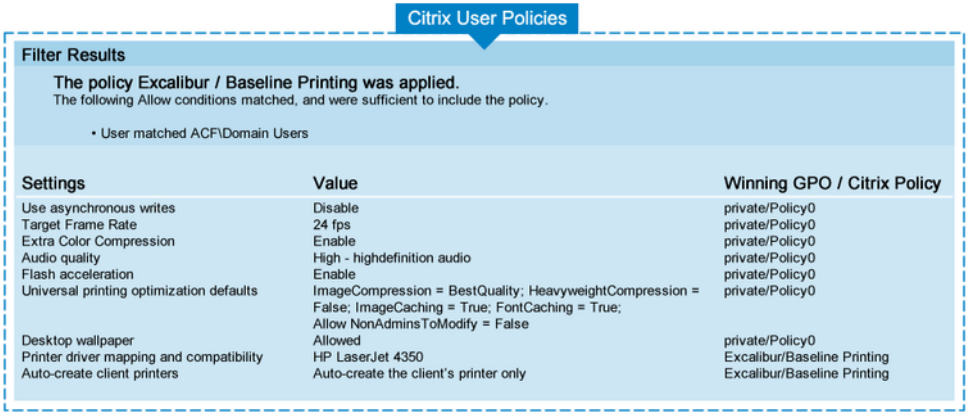
2. Double-click **Citrix Studio** on the desktop to open it.
3. Select **Policy** in the left pane of Studio.
4. Click the **Templates** tab and click **Import Template**.
5. Find the policy to import, click **Open**, and then click **Yes**.

   a. Browse to the **\\DC-1\Share\Polices** folder and select **USB Security.gpt**.
   b. Click **Open**.
   c. Click **Yes**.

Obtaining the Resultant Set of Policy Using Studio

Sometimes a connection does not respond as expected because several policies may apply. If a higher priority policy also applies to a connection, it can override the settings you configured in the original policy. You can determine how final policy settings are merged for a connection by calculating the resultant set of policy (RSOP).

When you run policy modeling from Studio as a domain user, you will see Citrix policies that have been configured within Active Directory as well as within the Studio console.



To Obtain the RSOP

1. Log on to the machine that has Citrix Studio.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** with **Password1** credentials.

2. Open Studio.
3. Select **Policy** in the left pane of Studio.
4. Click the **Modeling** tab.
5. Click **Launch Modeling Wizard** in the Actions pane. The Modeling Wizard opens.
6. Click **Next** to continue.
7. Select the domain controller and then click **Next**.

   Click **Next**.

8. Select **Container** or **User** and then browse to the specific object about which you want to run a report.

   Select **Container** under User Information and then click **Browse**.

9. Select the container or user and then click **OK**.

   Select **CCH** and then click **OK**.

10. Select another **Container** or **User** and then browse to the specific object about which you want to run a report.

    Select **Container** under Computer Information and then click **Browse**.

11. Select the container or user and then click **OK**.

    Select **CCH** and click **OK**.

12. Click **Next**.
13. Specify the filter evidence information and then click **Next**.

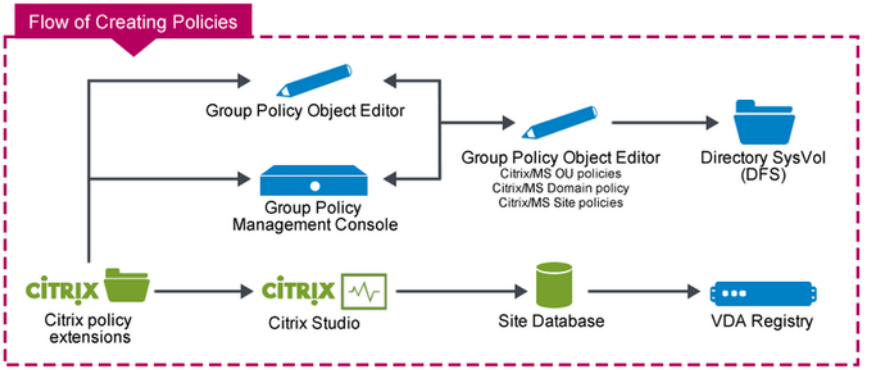
    a. Type **EP-Int** in the Client name field.
    b. Select **Skip to the final page of the wizard without collecting additional data** in the Filter Evidence page and then click **Next**.

14. Click **Run** on the Summary of Selections page to run the report.
15. Click **Close**.
16. Click **View Modeling Report** in the Actions pane.

Creating Policies Using Group Policy

If your network environment includes Active Directory and you have the appropriate permissions to manage Group Policy, you may want to use the Group Policy Management Console to create policies for your site. Using Active Directory group policy allows you to manage both Windows policies and Citrix policies in the same location and minimizes the administrative tools required for policy management.

The settings you configure affect the GPOs that you specify through the Group Policy Management Console (GPMC). Policies created using Group Policy are stored on the domain controller and updates are pushed to the virtual desktop at regular intervals as part of the GPO refresh policy.



The following is a description of the policy flow depicted in the graphic.

1. Citrix policy extensions are installed on the same machine where GPOs will be created or managed. These extensions add a Citrix node in the Microsoft GPO Editor and GPMC consoles for managing machines and end users.

In general, Citrix does not recommend installing policy extensions on domain controllers.

2. Local and domain policies are created
    a. Active Directory group policies are created and assigned using GPMC or GPO Editor. These policies are applied at the OU, Domain and site level of Active Directory. Citrix policies are created in exactly the same manner as Microsoft policies.
    b. Local site policies are created using the Citrix Studio Management Console. The settings are stored in the site database and propagated to the registry of the VDAs. Upon next restart or logon, policies are implemented.

3. Active Directory Group Policies take precedence over local system policies. If you do not have access to Active Directory, site policies can be used to accomplish all of the same tasks.
4. Policies are stored in a Directory file structure or System Volume (SysVol) on Domain Controllers only.
    a. Microsoft policy GUID folders are created in SysVol and hold ADM/X files
    b. Citrix policies at Active Directory level stored in SysVol as GPF/X files (XML files) that are parsed by Citrix Client-side extensions

Citrix settings are stored in the site database as metadata and propagated to servers as GPF/X files stored in Windows directory. These settings are applied to the VDA registry of each VDA configured.

Discussion Question

Where do you manage policies in your organization? Why do you choose one method over another?

Creating and Applying a Group Policy Object

The same criteria for creating a policy using Studio applies to creating a GPO. You may want to create a policy based on user job function, connection type, end-user device, or geographic location.

To Create a GPO

1. Log on to the machine that has the Group Policy Management Console and Citrix Studio installed.

    Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Open the Group Policy Management Console from the Start menu of the virtual machine.

    a. Click **Start**, type **Administrative Tools**, and then press **Enter**.
    b. Double-click **Group Policy Management**.

3. Right-click an organizational unit in the left pane and then select **Create a GPO in this domain, and Link it here** to open the New GPO window.

    a. Expand the **Forest: CCH.local** > **Domains** > **CCH.local** nodes.
    b. Right-click **CCH Virtual Desktops** and then select **Create a GPO in this domain, and Link it here** to open the New GPO window.

4. Type a name for the new Group Policy Object.

   Type **VDA Settings**.

5. Click **OK**. The new GPO appears in the console tree.

Editing a Group Policy Object

By default, only domain administrators, enterprise administrators, and members of the Group Policy creator owners group can edit GPOs.

Citrix recommends not editing the Default Domain Controllers Policy GPO or the Default Domain Policy GPO.

To Edit a Policy

1. Log on to the machine that has the Group Policy Management Console and Citrix Studio installed.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Open the Group Policy Management Console from the Start menu of the virtual machine.

   a. Click **Start**, type **Administrative Tools**, and then press **Enter**.
   b. Double-click **Group Policy Management**.

3. Select the organizational unit in the left pane of the Group Policy Management Console that contains the policy that you want to edit.

   Select **CCH Virtual Desktops**.

4. Right-click the GPO you would like to edit and then click **Edit**.

   Right-click the **VDA Settings** GPO in the right pane and then click **Edit**.

5. Expand the **Computer Configuration** node.
6. Expand **Policies** and then select **Citrix Policies** to open the Citrix Computer Policy window.
7. Create or edit an existing policy.

   Click **Edit** in the Policies tab.

8. Add or edit the settings within the policy and then click **OK**.

    a. Select the **Settings** tab.
    b. Select **Virtual Delivery Agent Settings** from the Categories menu.
    c. Click **Add** to the right of the Controllers setting.
    d. Type **c-1.cch.local c-2.cch.local** and then click **OK**.

Separate the FQDNs for the Controllers with a space.

9. Click **OK**.
10. Close the Group Policy Management Editor.

Using a User Template with Group Policy

Policy templates are displayed on the Templates tab in Group Policy Editor. Computer templates are displayed when you are working with Computer policies. User templates are displayed when you are working with user policies.

To Use a User Template

1. Log on to the machine that has the Group Policy Management Console and Citrix Studio installed.

    Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Open the Group Policy Management Console from the Start menu of the virtual machine.

    a. Click **Start**, type **Administrative Tools**, and then press **Enter**.
    b. Double-click **Group Policy Management**.

3. Select the organizational unit in the left pane of the Group Policy Management Console.

    a. Click **CCH.local > CCH Users**.
    b. Right-click **CCH Users** and then select **Create a GPO in this domain, and Link it here**.
    c. Type **WAN Optimization** and then click **OK**.

4. Right-click the GPO you would like to edit and then click **Edit**.

    Right-click the **WAN Optimization** GPO from the linked Group Policy Objects tab in the right pane and then click **Edit**.

5. Expand **User Configuration**.
6. Select **Policies**.
7. Double-click **Citrix Policies**.
8. Click the **Templates** tab.
9. Select the template from which you want to create a new template.

   Select **Optimized for WAN**.

10. Click **New Policy** to open the New Policy Wizard opens.
11. Type a name for the new template.

    Type **Remote Users** in the Name field.

12. Click **Next** two times to accept the default settings.
13. Configure when the policy is applied.

    a. Click **Add** to the right the Client IP address filter.
    b. Click **Add**.
    c. Select **Deny** from the Mode menu.
    d. Type **192.168.1.1-192.168.255.255** in the Client IP address field.
    e. Type **Policy applies to every user without an IP in this range** in the Comment field and then click **OK**.
    f. Click **OK**.

14. Click **Next**.
15. Click **Create**.
16. Close the Group Policy Management Editor.

Discussion Question

How does denying a policy to all users with an IP address of 192.168.1.1-192.168.255.255 apply it to all employees working remotely?

Importing a Policy Template with Group Policy

Built-in templates are created and updated by Citrix. You cannot modify or delete these templates. However, you can modify templates that you import through Studio or the Group Policy Editor.

To Import a Policy Template

1. Log on to the machine that has the Group Policy Management Console and Citrix Studio installed.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Open the Group Policy Management Console from the Start menu of the virtual machine.

   a. Click **Start**, type **Administrative Tools**, and then press **Enter**.
   b. Double-click **Group Policy Management**.

3. Select the organizational unit in the left pane of the Group Policy Management Console.

   Expand the **CCH.local** > **CCH users** organizational unit.

4. Right-click the GPO you would like to edit and then click **Edit**.

   Right-click **WAN Optimization** GPO from the linked Group Policy Objects tab in the right pane and then click **Edit**.

5. Expand **User Configuration**.
6. Select **Policies**.
7. Double-click **Citrix Policies** in the right pane.
8. Click **Templates** tab.
9. Select **Actions** and then select **Import** from the Actions menu.
10. Select the template that you want to import and then click **Yes**.

    a. Type **\\DC-1\Share\Policies** in the Address field of the Import Template window, press **Enter**, and then double-click **USB Security.gpt**.
    b. Click **Yes** in the Import Template message.

11. Close the Group Policy Editor.

Exporting a Policy Template with Group Policy

Exporting a policy template allows you to create backups of your template files to aid in the recovery of policy configurations. It also allows you to supply policy configurations from your site to aid Citrix Support in troubleshooting issues.

To Export a Policy Template

1. Log on to the machine that has the Group Policy Management Console and Citrix Studio installed.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Open the Group Policy Management Console from the Start menu of the virtual machine.

   a. Click **Start**, type **Administrative Tools**, and then press **Enter**.
   b. Double-click **Group Policy Management**.

3. Select the organizational unit in the left pane of the Group Policy Management Console.

   Select **CCH Virtual Desktops**.

4. Right-click the GPO you would like to edit and then click **Edit**.

   Right-click the **VDA Settings** GPO from the linked Group Policy Objects tab in the right pane and click **Edit**.

5. Expand **Computer Configuration**.
6. Select **Policies**.
7. Double-click **Citrix Policies** in the right pane.
8. Click **Templates**.
9. Select the template that you want to export.

   Select **High Server Scalability**.

10. Select **Actions** and then select **Export** from the Actions menu.
11. Select the location where you would like to export the file to and then click **OK.**

    a. Type **\\DC-1\Share\Policies** in the Address field of the Import Template window and then press **Enter**.
    b. Click **Save**.

12. Close the Group Policy Editor.

Prioritizing a Policy Using Group Policy

With the tree-based structure of Active Directory, policies can be created and enforced at any level in the tree structure. It is important to understand how the aggregation of policies, known as policy precedence, flows in order to understand how a resultant set of policies is created.

Any policy setting that is disabled takes precedence over a lower-ranked setting that is enabled. Policy settings that are not configured are ignored.

If you are using Active Directory, policy settings are updated when Active Directory re-evaluates policies at regular 90 minute intervals and when a user logs on.

To Change the Priority of a Policy

1. Log on to the machine that has the Group Policy Management Console and Citrix Studio installed.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Open the Group Policy Management Console from the Start menu of the virtual machine.

   a. Click **Start**, type **Administrative Tools**, and then press **Enter**.
   b. Double-click **Group Policy Management**.

3. Browse to the OU containing the policies you want to prioritize.

   Expand the **Forest: CCH.local** > **Domains** > **CCH.local** > **CCH Users** nodes in the left pane.

4. Select the **Linked Group Policy Objects** tab in the right pane.
5. Select a policy in the Group Policy Editor for which you want to change the priority.

   Select **WAN Optimization**.

6. Use the arrows on the left side of the Linked Group Policy Object tab to raise and lower the priority of the policy.

You will not be able change the priority of the policy because only one policy exists for the OU.

Discussion Question

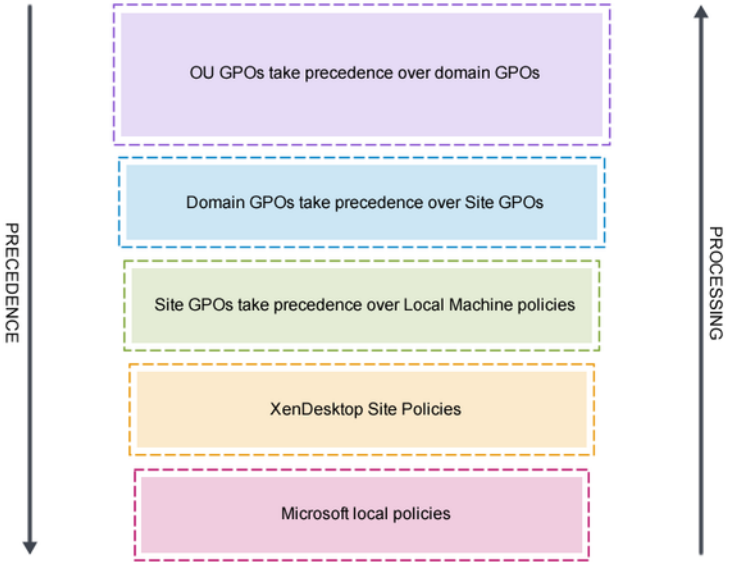
You have created and applied a new policy. You configured the policy with client removable drives set to disabled. The policy contains a filter that has been set to allow for the Accounting group. Some employees from the Engineering group are now asking the Support team why they are unable to access their client drives. What could be causing this issue? How can you fix the issue?

Policy Precedence (Studio vs. Group Policy Objects)

Policies can be created using Studio or using GPOs. Prior to creating policies, you should evaluate whether policies should be managed and stored in Studio or by using GPOs.

Citrix recommends managing and storing policies using GPOs if you have the appropriate permissions in Active Directory.

In situations where policies exist that have been created using both Studio and GPOs, Group Policy-based settings take precedence over policies stored within the site database.



Obtaining the Resultant Set of Policy Using Group Policy Objects

If you run the Citrix Group Policy Modeling Wizard or Group Policy Results tool from the Group Policy Management Console, site policy settings created using Studio are not included in the RSOP.

To ensure that you obtain the most comprehensive RSOP, Citrix recommends launching the Citrix Group Policy Modeling wizard from Studio, unless you create policies using only the Group Policy Management Console.

Troubleshooting: Managing Policies

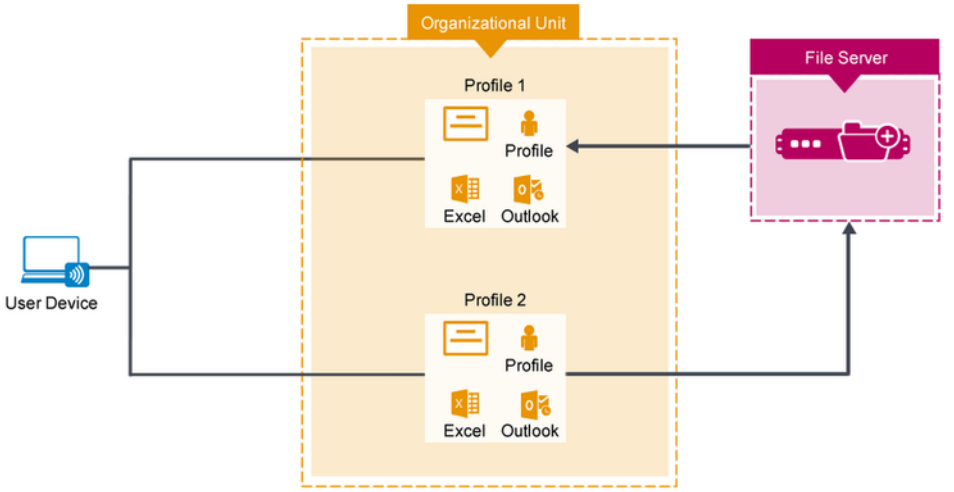
Issue	Resolution
A new policy is not functioning properly.	• Ensure that the policy is enabled. • Verify that it is assigned to the appropriate end users, groups, OUs, and/or domains. • Verify that there are no Active Directory policies that supersede the policy built in Studio. • Check the prioritization of the policies. • Ensure that the correct policy settings have been chosen to achieve the desired results.
Unable to modify or delete a template.	Verify that the administrator attempting to make this change has the authority to do so.  Built-in templates can be used as a model for other templates, but cannot be modified or deleted.
Loopback policy issues.	For information about loopback policy issues, see *http://technet.microsoft.com* Web site.
Unable to find the appropriate policy settings.	Use the Search field to narrow the results as you search for settings.

Managing End-User Profiles

In a virtualized environment where end users can get to their desktops and applications from practically any location or device, profile management technology will ensure that end users are getting a consistent experience every time. When end users log on to their virtual desktop or launch a virtual application, they want to see everything just as they left it, with their own personal settings, shortcuts, toolbars, templates, desktop wallpapers, and favorites. The more complex and varied the user access scenarios, the more challenging it becomes for IT to manage these end-user profiles.

Profile management ensures that the end user's personal settings are applied to the end user's virtual desktop and applications, regardless of the location or device. Profile management is incorporated into Studio and gives you an easy, reliable way to manage the settings in Windows environments to ensure consistent experience by maintaining a single profile that follows an end user. It auto-consolidates and optimizes end-user profiles to minimize management and storage requirements and requires minimal administration, support and infrastructure, while providing end users with improved logon and logoff experiences.

The steps below discuss how Citrix Profile management delivers a profile to a user device.



1. An end user starts a session for a machine with profile management enabled.
2. The Citrix Profile management service determines if the end user is a member of the processed group defined in the profile management policies. If the end user is a member of the group, the service attempts to load the end user's profile from the store. If the end user is not part of the group a Microsoft profile is assigned.
3. If the end user is a member of the processed group, Citrix Profile management verifies that the user store contains the profile. If a profile is not found in the store, the service migrates the end user's Microsoft profile to the store or creates a new one from a template specified in the policy.

4. A local profile that is managed by Citrix Profile management is streamed from the store to the virtual machine.
5. Profile management monitors the end user's profile and logs any changes back to the end user's profile store.

Profile management addresses end-user profile deficiencies in environments where simultaneous domain logons by the same end user introduces complexities and consistency issues to the profile. For example, if an end user starts sessions on two different virtual resources based on a roaming profile, the profile of the session that terminates last overwrites the profile of the first session. This problem, known as "last writer wins", discards any personalization settings that the end user has made in the first session.

You can prevent this by using separate profiles for each resource silo. However, this results in increased administration overhead and storage capacity requirements. Another drawback is that end users will experience different settings depending on the resource silo they access.

Profile management optimizes profiles in an easy and reliable way. At interim stages and at logoff, registry changes, as well as files and folders in the profile, are saved to the user store for each end user. If a file already exists, it is overwritten if it has an earlier timestamp. This helps safeguard application settings for mobile end users who experience network disruption and end users who access resources from different operating systems.

Alternatives to using Citrix Profile management exist, including Environment manager from AppSense and RES PowerFuse.

By default, Citrix Profile management is installed silently on master images when you install the VDA.

Configuring Folder Redirection

Client folder redirection changes the way that some of the files and folders within an end user's profile are accessible from their current logon destination, such as their virtual desktop. Folders that are frequently used, like "My Documents" and "Desktop" can be redirected to a network share outside of the roaming profile share so they are not copied over the network at every logon and logoff. This will also improve logon times as profiles will be smaller in size reducing the volume of network utilization required.

To Configure Folder Redirection

1. Log on to the machine that has Citrix Studio installed.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Select the **Policy** node in the left pane of Studio and then click the **Policies** tab.
4. Click **Create Policy** in the Actions pane.
5. Select **Profile Management** > **Basic Settings** from the All Settings menu.
6. Click **Select** to the right of the Enable Profile Management setting.
7. Select **Enable** and click **OK**.
8. Select **Folder Redirection** in the All Settings drop-down menu.
9. Configure the folders you want to redirect.

   a. Click **Select** to the right of the Documents path setting.
   b. Click **Enabled** and then type **\\DC-1\UPM$\%USERNAME%**.
   c. Click **OK**.
   d. Repeat the previous three steps for the Downloads path setting.

10. Click **Next**.
11. Click **Assign** to assign the policy to the appropriate user and machine objects and then click **OK**.

    Click **Assign** to the right of Delivery Group, select **HR Desktops** in the Delivery Group drop-down menu, and click **OK**.

12. Click **Next**.
13. Type the policy name and then click **Finish**.

    Type **Folder Redirection for HR Desktops** and then click **Finish**.

Managing Profile Settings Using Citrix Policies

Within Citrix policies, you have the option to customize and configure policy settings at a detailed level. Using policy filters, profile configuration settings can be associated with Delivery Groups, Delivery Group Types, Organizational Units, or Tags.

To Manage Profile Settings Using Citrix Policies

1. Log on to the machine that has Citrix Studio installed.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Select the **Policy** node in the left pane.
4. Select the **Policies** tab and then click **Folder Redirection for HR Desktops** policy.
5. Click **Edit Policy** in the Actions pane.
6. Select the appropriate setting in the drop-down field.

   Select **Profile handling**.

7. Click **Select** next to the settings that you would like to edit.

   Click **Select** to the right of the Delay before deleting cached profiles setting.

8. Make the necessary changes within the setting and then click **OK**.

Type **5** in the Value field and then click **OK**.

9. Click **Select** next to any other setting you would like to edit.

Click **Select** to the right of the Delete locally cached profiles on logoff setting.

10. Make the necessary changes within the setting and then click **OK**.

Click **Enabled** and then click **OK**.

11. Click **Next** twice and then click **Finish**.

Resolving Conflicting Profiles

Citrix Profile management has a feature that detects conflicting profiles between end users' Windows profile and Citrix profiles. When an end user is having difficulties with the desktop or applications, yet all policies and profiles appear to be correct, you should verify that there are no conflicting policies. You can use the steps below to address any profile conflicts.

To Resolve Conflicting Profiles

1. Log on to the machine that has Citrix Studio installed.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Click the **Policy** node and then click the **Policies** tab to display the list of policies in the center pane.
4. Select the profile policy that you would like to change.

   Select the **Folder Redirection for HR Desktops** policy.

5. Click **Edit Policy** in the Actions pane and determine which policy setting to add or delete from the policy.

If you know one or two words of a policy setting, you can use the Search field to find the setting.

   Type **Local profile** in the Search field.

6. Click **Select** to the right of the Local profile conflict handling setting.
7. Select the appropriate option in the Value field and then click **OK**.

   Select **Delete local profile** and then click **OK**.

8. Click **Next** twice and then click **Finish**.

Streaming End-User Profiles

To improve logon performance and enhance an end user's experience, profiles can be streamed. With profile streaming end users' profiles are synchronized on the local computer only when they are needed. Registry entries are cached immediately, but files and folders are only cached when accessed by end users.

To Stream End-User Profiles

1. Log on to the machine that has Citrix Studio installed.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Double-click **Citrix Studio** on the desktop to open it.
3. Click the **Policy** node and then click the **Policies** tab to display the list of policies.
4. Select the particular policy that you would like to edit and then right-click **Edit**.

   Select **Folder Redirection for HR Desktops** and then right-click **Edit**.

5. Select **Profile Management** in the All Settings field.
6. Click **Select** to the right of the Profile streaming setting.
7. Select **Enabled**.
8. Click **OK**.
9. Click **Next** twice and click **Finish**.

Discussion Question

What other settings are available within policies for customizing user profiles would be valuable within your environment? Why?

Troubleshooting: Profile Management

Issue	Resolution
Folder redirection is not working properly.	• Ensure that the redirection location is properly configured and that no characters are missing from the paths when utilizing variables. • View the "Configuring Folder Redirection" task within this module.
Profile definition is not affecting the relevant end users.	• Verify that the profile has been assigned to the appropriate Delivery Group. • Verify the profile policies are applied to the relevant filters. • Ensure conflicting policies have been configured with the appropriate priorities.
End user's Desktop settings, document history and download data is not being retained.	• Verify that the relevant Common Folders have been selected within the profile.

Reinforcement Exercise 1: Working with Policies

During these exercises, you will not be given step-by-step instructions for performing the tasks. Instead, you are asked to use what you have just learned to complete them. These exercises are designed to take your newly acquired knowledge determine if you can perform a task you have never done before. In most instances the default value will be the best choice, but we encourage you to explore and try things out. If you have a question or need help, ask the instructor or a fellow student for assistance.

In this module, you learned how to:

- Create, apply and edit a policy in Studio and as a Group Policy Object (GPO).
- Prioritize policies within Studio and with Active Directory GPOs.
- Use, import, and export a user policy template within Studio and Active Directory.
- Run and obtain a resultant set of policy (RSOP) report.
- Configure folder redirection and streaming user profiles.
- Manage profile settings using Citrix policies.
- Resolve conflicting profiles.

Time to complete: Approximately 15 minutes

The CCH Engineering team's IDE and programming tools will eventually be hosted on a desktop provided by XenDesktop 7. Since they have access to the source code, the company's intellectual property, management wants you to put some policies in place that may make it more difficult for the source code to be taken outside company systems.

Your objective is to put a group policy object in place to put some safeguards in place to limit how the Engineering team can transfer this kind of data.

To complete your objective:

- Create a group policy object called "Safeguards Against Data Theft" that is applied to the Engineering organizational unit.
- Add the following settings to the Citrix User Policies:
  - Disable client clipboard redirection
  - Disable client drive redirection
  - Disable USB device redirection

Reinforcement Exercise 2: Working with Profiles

During these exercises, you will not be given step-by-step instructions for performing the tasks. Instead, you are asked to use what you have just learned to complete them. These exercises are designed to take your newly acquired knowledge determine if you can perform a task you have never done before. In most instances the default value will be the best choice, but we encourage you to explore and try things out. If you have a question or need help, ask the instructor or a fellow student for assistance.

Time to complete: Approximately 15 minutes

The Engineering team needs only specific parts of their profiles to be redirected to a central location. Management has asked you to implement Folder Redirection for the Documents, AppData(Roaming) folders.

Your objective is to create a Citrix policy within Studio to enable the folder redirection required for the team and then apply the policy to the Engineering team.

To complete the objective:

- Create a Citrix policy in Studio called "Folder Redirection for Engineering".
- Add the following settings to the policy:
  - Enable AppData(Roaming) Path and set to \\dc-1\UPM$\%USERNAME%\AppData\Roaming.
  - Enable Documents Path and set to \\dc-1\UPM$\%USERNAME%.
- Apply the policy to the Engineering organizational unit.

Module 7

Managing and Monitoring Sessions, Sites, and End Users with Director

7

Managing and Monitoring Sessions, Sites, and End Users with Director

Managing end users and their sessions is a common administrative task. When end users experience difficulty accessing their applications or desktops, they will require troubleshooting assistance from the administrator in order to resolve the session issues.

Another important administrative task is the monitoring of your XenDesktop environment and the troubleshooting of issues before they become system critical. Director enables support teams to obtain an overview of the entire XenDesktop site, including real-time machine issues, usage metrics, and host and controller information. With this data, you can proactively monitor and troubleshoot system issues.

After completing this module, you will be able to:

- Monitor sessions and sites using the Dashboard within Director.
- Monitor and manage end-user sessions within Director.
- Monitor historical trends within Director.

Module timing: Approximately 3 hours

Director Overview

Director is a Web-based tool that enables IT Support and Helpdesk teams to monitor a XenDesktop environment, troubleshoot issues before they become system critical, and perform support tasks for end users.

Director allows you to search for a particular end user and display activity associated with that end user, such as:

- Finding the status of the end user's applications and processes
- Ending unresponsive applications or processes
- Restarting an end user's machine
- Disconnecting end-user sessions
- Shadowing an end-user session

Director provides an overview of the key aspects of a deployment, such as the status of connections, sessions, and the site infrastructure. Meaningful performance metrics and graphs are displayed, together with information about the health of the hypervisors and Controllers. Information is updated every minute. If issues occur, details appear automatically about the number and type of failures that have occurred. You can view more detailed information -- for example, to display all the end users affected and the associated machines.

In preparation for the exercises in this module, you will need to log on as an end user and begin a session that you can use Director to monitor in subsequent procedures.

To Monitor an End-User Session

1. Log on to an internal endpoint using domain user credentials.

Log on to the **EndPoint-Internal** virtual machine using the **CCH\HRUser1** and **Password1** credentials.

2. Launch **Internet Explorer** and then browse to the URL for the Receiver for Web site.

    a. Click **Internet Explorer** on the Start screen.

    b. Type ***https://sfs-1.cch.local/Citrix/StoreWeb*** in the Address field and then press **Enter**.

Citrix Receiver must be installed on the endpoint before an end user can access resources. If you do not install Citrix Receiver, an .ICA file will be downloaded to the endpoint. You will not be able to open the .ICA file, because Receiver is not installed on the endpoint.

3. Log on to Citrix Receiver using the domain user credentials.

   Log on using the **CCH\HRUser1** and **Password1** credentials.

4. Click **Save** and then click **Run** in the messages that appear at the bottom of the screen.
5. Click **Apps** at the bottom of the Receiver window and then click the + sign to add an application.
6. Click **All Apps** and then select an application to start.

   Click **All Apps** and then click **WordPad**.

7. Launch the newly added application.

   Click **WordPad** to launch the application.

8. Click **Save** and then click **Open** in the messages that appear at the bottom of the screen.
9. Click **Desktops** at the bottom of the Receiver window.
10. Launch a desktop.

    Click **HR Desktop** to launch the desktop.

11. Click **Save** and then click **Open** in the messages that appear at the bottom of the screen.

To Access Director

1. Log on to a computer within the same network as your Controller using domain administrator credentials.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Open a browser window.

Double-click **Mozilla Firefox** on the desktop.

3. Type the URL for Director using the following format, ***http://server/Director*** and then press **Enter**.

   Type ***http://C-1.cch.local/Director*** in the Web browser and then press **Enter**.

4. Type your domain user name.

   Type **Admin1** in the User name field.

5. Type your password.

   Type **Password1** in the Password field.

6. Type the domain you would like to connect to.

   Type **CCH** in the Domain field.

7. Click **Log on**.

Monitoring within the Director Dashboard

The Director Dashboard is the opening page of Director and shows basic information regarding your environment including:

- Infrastructure
- Sessions Connected
- Average Logon Duration

The Dashboard will give you a general overview of the current status of the environment and allow you to quickly view unusual and irregular activity.

Monitoring Infrastructure

From the Infrastructure panel in Director, you can monitor the health status of your XenDesktop site components, as well as view performance alerts. This panel lists all servers with alerts in alphabetical order.

The columns list different states for each server. A green check represents that everything is working properly; an alert or error represents a warning or failure of an infrastructure component. The panel lets you monitor the current status of the following entities:

- Hosts
- Delivery Controllers
- Services
- Database
- License Server
- Configuration Logging Database
- Monitoring Database

To Monitor the Infrastructure

1. Log on to Director (*http://server/Director*) using domain administrator credentials.

a. Type ***http://C-1.cch.local/Director*** in a Web browser on the **StudentManagementConsole-1** virtual machine and then press **Enter**.

b. Log on using the **Admin1**, **Password1** and **CCH** credentials.

2. Scroll the Dashboard to view the Infrastructure panel of Director.

If the Infrastructure panel is not available, click Trends at the top of the Director window and then click Dashboard again.

3. Ensure that no alerts exist. If a performance alert is indicated, click the alerts in the Infrastructure panel to read more information.

Monitoring Connected Sessions

The Dashboard shows information for Sessions Connected, which provides you with a real-time view of end users connected to the environment, including an option to view historical trends.

To Monitor Connected Sessions

1. Log on to Director (*http://server/Director*) using domain administrator credentials.

   a. Type ***http://C-1.cch.local/Director*** in a Web browser on the **StudentManagementConsole-1** virtual machine and then press **Enter**.
   b. Log on using the **Admin1**, **Password1** and **CCH** credentials.

2. Click the number above the Sessions Connected text on the Dashboard.

   Click **2** to view information about the two connected sessions.

Instead of clicking on the number of end users, you also have the option of clicking View Historical Trend in the Sessions Connected graph on the Dashboard if you would like to view information about the past number of concurrent sessions.

Monitoring Logon Duration Averages

From the Average Logon Duration panel within the Dashboard, you can view logon data for end users across a site. This panel provides data to determine where any patterns are affecting logon times.

The logon duration chart displays two types of information at each data point: The average logon duration and the number of logons. When you hover over the chart, a red line appears at the cursor to highlight that point in time and display a dialog box showing both the values of logon duration and logons at the same time.

To Monitor Logon Duration Averages

1. Log on to Director (*http://server/Director*) using domain administrator credentials.

a. Type ***http://C-1.cch.local/Director*** in a Web browser on the **StudentManagementConsole-1** virtual machine and then press **Enter**.

b. Log on using the **Admin1**, **Password1** and **CCH** credentials.

2. Scroll the Dashboard to view the Average Logon Duration panel in Director.
3. Point your cursor at the chart and view the logon duration and logon information at the same time.
4. Click **Trends** at the top of the Director screen to view logon performance data across a site beyond the last 60 minutes.
5. Select the Delivery Group that you want to view logon trend information about.

   Select **All** in the Delivery Group field.

6. Select a time period for which you want to view logon trend information.

   Select **Last 7 days** in the Time period field.

7. Click **Apply** to view the logon data for the Delivery Groups and time period selected.
8. Click **Dashboard** at the top of the Director window to return to the Dashboard.

Monitoring Machine and End-User Connection Failures

If there were Machine or User Connection failures in the previous 60 minutes, additional panels appear on the Dashboard automatically.

The large number on the left of the panel indicates the total number of failures for that type. If you click the large number, the Filters page opens and displays all the individual failures in this instance. Click the User Connection Failures number to see a list of these end users whose connections failed, so that you can troubleshoot and resolve the cause of these failures.

The list and graph on the right displays data for each type of failure. If a particular category has more than one failure during the last 60 minutes, it is expanded by default. These panels stay open even when you fix the failures, but you can click the tab to collapse them.

End-user connection failures can be categorized as follows:

- Client Connection Failures - Virtual machine unavailable, connection not established
- Machine failures - End user connection failures resulting from machine failures
- Unavailable capacity - Desktop OS machine or Server OS machine session is not available due to maximum capacity reached
- No License Available - Failure to acquire a license for this user

To Monitor End-User Connection Failures

1. Log on to Director (*http://server/Director*) using domain administrator credentials.

a. Type ***http://C-1.cch.local/Director*** in a Web browser on the **StudentManagementConsole-1** virtual machine and then press **Enter**.
b. Log on using the **Admin1**, **Password1** and **CCH** credentials.

2. Click the **User Connection Failures** link at the top of the Dashboard to view information about connection failures.

The number of end-user connection failures is listed to the right of the link. If the link is green, there are no failures identified.

3. Click the **Failed Desktop OS Machines** link at the top of the Dashboard to view information about failed Desktop OS machine connections.

The number of failed Desktop OS connections is listed to the right of the link. If the link is green, there are no failures identified.

4. Click the **Failed Server OS Machines** link at the top of the Dashboard to view information about failed Server OS machine connections.

The number of failed Server OS connections is listed to the right of the link. If the link is green, there are no failures identified.

5. Click **View Historical Trend** below any of the graphs to view additional information.
6. Click **Dashboard** at the top of the Director window to return to the Dashboard.

Monitoring and Managing End-User Sessions

You can easily monitor and manage end-user sessions within Director. Common monitoring tasks include:

- Viewing end-user sessions
- Searching for end-user sessions
- Monitoring end-user applications
- Monitoring machine processes
- Managing an end user's machine power status
- Enabling or disabling maintenance mode
- Disconnecting and logging off end users
- Shadowing end users
- Sending messages to end users
- Monitoring HDX channels
- Resetting end user profiles

These tasks may also be helpful for Helpdesk representatives to troubleshoot and resolve issues prior to escalation.

Viewing End-User Sessions

There are multiple ways to view sessions within Director. The steps below will be beneficial when you would like to search for groups of users or filter with specific requirements.

To View End-User Sessions

1. Log on to Director (*http://server/Director*) using domain administrator credentials.

   a. Type ***http://C-1.cch.local/Director*** in a Web browser on the **StudentManagementConsole-1** virtual machine and then press **Enter**.
   b. Log on using the **Admin1**, **Password1** and **CCH** credentials.

2. Click **Filters** at the top of the Director window.
3. Select **Sessions** > **All Sessions**.

The page displays information about all of the sessions currently running in the environment. You can reduce the number of sessions displayed using the Filter by fields. For example, you may want to view current sessions that exist by a particular Delivery Group, OS, machine catalog, etc.

4. Select one or more user sessions to enable the Session Control and Send Message functions for the selected user sessions.

   Select the **HRUser1** session that is running on the Hosted Apps-1 machine.

5. Click **Dashboard** at the top of the Director window to return to the Dashboard.

Searching for an End User

In order to search for a specific end user and have the ability to perform all management tasks, you should use the Search users field.

To search for an end user:

To Search for an End User

1. Log on to Director (*http://server/Director*) using domain administrator credentials.

   a. Type ***http://C-1.cch.local/Director*** in a Web browser on the **StudentManagementConsole-1** virtual machine and then press **Enter**.
   b. Log on using the **Admin1**, **Password1** and **CCH** credentials.

2. Scroll to the right within any page in Director to access the Search users field.
3. Type a specific end user's account name or a partial account name in the Search users field and then press **Enter** to locate information about matching end-user sessions.

   Type **HRUser1** into the Search users field and then press **Enter**.

4. Select the appropriate end user to open the Activity Manager for that user.

   Select **HRUser1** and then verify that Details appears below the Search users field..

This step is only necessary if a "fuzzy" search was performed using the Search users field.

Monitoring End-User Applications

You can monitor end-user applications by performing the following tasks:

- View local and hosted applications for currently connected machines.
- View applications on all machines to which the end user has access.
- Stop an application.

To Monitor End-User Applications

1. Log on to Director (*http://server/Director*) using domain administrator credentials.

a. Type ***http://C-1.cch.local/Director*** in a Web browser on the **StudentManagementConsole-1** virtual machine and then press **Enter**.

b. Log on using the **Admin1**, **Password1** and **CCH** credentials.

2. Scroll to the right within any page in Director to access the Search users field.
3. Type a specific end user's account name or a partial account name in the Search users field and then press **Enter** to locate information about matching end user's sessions.

   Type **HRUser1** into the Search users field and then press **Enter**.

4. Click **Activity Manager** below the Search users field to view the Activity Manager.

If Details is displayed below the Search users field, then the Activity Manager screen is already displayed. The Activity Manager screen is white and the Details screen is black.

5. Click the **Applications** tab menu in the Activity Manager to view a list of the applications and hosted applications being run by the selected end user.

Monitoring End-User Machine Processes

When an end user calls the Helpdesk about a slow desktop machine, you can monitor the status of the processes on that machine without needing to start a Remote Assistance session and shadow the end user.

One resolution for a process problem is to stop the process. If the process is successfully stopped, it disappears from the list of processes. If the process problems continue, you can escalate by restarting the machine or by resetting the end user's profile.

To Monitor End-User Machine Processes

1. Log on to Director (*http://server/Director*) using domain administrator credentials.

a. Type ***http://C-1.cch.local/Director*** in a Web browser on the **StudentManagementConsole-1** virtual machine and then press **Enter**.
b. Log on using the **Admin1**, **Password1** and **CCH** credentials.

2. Scroll to the right within any page in Director to access the Search users field.
3. Search for an end-user session and then click **Activity Manager** under the Search users field.

Type **HRUser1** in the Search users field, press **Enter**, and then click **Activity Manager**.

If Details is displayed below the Search users field, then the Activity Manager screen is already displayed. The Activity Manager screen is white and the Details screen is black.

4. Click the **Processes** tab in the Activity Manager.
5. Select the process to be stopped, click **End Process** and then select **Yes** to confirm the action.

Do not end any processes.

Managing an End User's Machine Power Status

Director gives you the ability to restart, shutdown, or suspend virtual machines within the environment.

To Manage an End User's Machine Power Status

1. Log on to Director (*http://server/Director*) using domain administrator credentials.

a. Type ***http://C-1.cch.local/Director*** in a Web browser on the **StudentManagementConsole-1** virtual machine and then press **Enter**.
b. Log on using the **Admin1**, **Password1** and **CCH** credentials.

2. Scroll to the right within any page in Director to access the Search users field.
3. Search for an end-user session and then click **Details** below the Search users field.

Type **HRUser1** in the Search users field, press **Enter**, and then click **Details**.

If Activity Manager is displayed below the Search users field, then the Details screen is already displayed. The Activity Manager screen is white and the Details screen is black.

4. Click **Power Control** under Machine Details on the page.
5. Select the appropriate action to take on the machine.

The following power controls are available:

- Restart
- Force Restart
- Shutdown
- Force Shutdown
- Suspend
- Resume
- Start

Do not select any of the available actions at this time.

Enabling or Disabling Maintenance Mode

Maintenance mode prevents end users from launching a session to specified desktops or Delivery Groups. If an end user has a connection, maintenance mode will not be enabled until the session is disconnected.

To Enable or Disable Maintenance Mode

1. Log on to Director (*http://server/Director*) using domain administrator credentials.

a. Type ***http://C-1.cch.local/Director*** in a Web browser on the **StudentManagementConsole-1** virtual machine and then press **Enter**.

b. Log on using the **Admin1**, **Password1** and **CCH** credentials.

2. Scroll to the right within any page in Director to access the Search users field.
3. Search for an end-user session that you would like to put in maintenance mode and then click **Details**.

   Type **HRUser1** in the Search users field, press **Enter**, and then click **Details**.

If Activity Manager is displayed below the Search users field, then the Details Manager screen is already displayed. The Activity Manager screen is white and the Details screen is black.

4. Ensure that the appropriate desktop or application connection for the end user is displayed.

   Click the machine switcher icon (Computer display icon) at the top of the Activity Manager page and then select the **WordPad** resource from the drop-down menu.

The machine switcher icon is only available when the selected end user has multiple sessions running.

5. Drag the **Maintenance mode** slider under Machine Details to the left or right to change the mode.

   Ensure that maintenance mode is set to **Off** before continuing.

Resetting an End-User Profile

Resetting a profile allows you to manage end-user settings stored within their Citrix-based profile or Microsoft roaming-based profile. When a profile is reset, and end user's folders and files are saved and copied to the new profile. All other profile properties are reset to default, including registry, applications, and personalization settings.

To Reset an End-User Profile

1. Log on to Director (*http://server/Director*) using domain administrator credentials.

   a. Type ***http://C-1.cch.local/Director*** in a Web browser on the **StudentManagementConsole-1** virtual machine and then press **Enter**.
   b. Log on using the **Admin1**, **Password1** and **CCH** credentials.

2. Scroll to the right within any page in Director to access the Search users field.
3. Search for an end-user session whose profile you want to reset and then click **Details** below the Search users field.

   Type **HRUser1** in the Search users field, press **Enter** and then click **Details**.

If Activity Manager is displayed below the Search users field, then the Details screen is already displayed. The Activity Manager screen is white and the Details screen is black.

4. Ensure that the appropriate desktop or application connection for the user is displayed.

   Click the machine switcher icon (Computer display icon) at the top of the Activity Manager page and then select the **WordPad** resource from the drop-down menu.

The machine switcher icon is only available when the selected end user has multiple sessions running.

5. Scroll the Details page down until you reach the Personalization panel.

6. Click **Reset Profile** in the Personalization panel of the Details page.

Discussion Question

Can you provide examples of when Director would be useful within your organization?

Monitoring HDX Channels

Monitor the status of the HDX channels within the user session in the HDX panel of the User Details page. The HDX channels monitor allows you to view the status and current configuration of end user's specific HDX channels within their session, greatly assisting in the diagnostic of connections and performance concerns. Detailed information can be gathered around numerous HDX parameters including Audio and Media Stream, Thinwire, USB utilities, and Flash.

To Monitor HDX Channels

1. Log on to Director (*http://server/Director*) using domain administrator credentials.

a. Type ***http://C-1.cch.local/Director*** in a Web browser on the **StudentManagementConsole-1** virtual machine and then press **Enter**.

b. Log on using the **Admin1**, **Password1** and **CCH** credentials.

2. Scroll to the right within any page in Director to access the Search users field.
3. Search for an end-user session whose HDX details you want to view and then click **Details** below the Search users field.

   Type **HRUser1** in the Search users field, press **Enter**, and then click **Details**.

If Activity Manager appears instead of Details, you are already on the Details page.

4. Ensure that the appropriate desktop or application connection for the user is displayed.

   Click the machine switcher icon (Computer display icon) at the top of the Details page and then select the **WordPad** resource from the drop-down menu.

The machine switcher icon is only available when the selected end user has multiple sessions running.

5. Scroll down to the Personalization panel on the Details page.
6. View the information specified below the HDX heading.

7. Click an HDX channel preceded by a red circle or triangle to view error information for an HDX channel.

    a. Click **Smart Cards** to view error information.
    b. Click the **X** to close the window.
    c. Click **Audio** to view warning information.
    d. Click the **X** to close the window.

8. Click an HDX channel preceded by a green checkmark to view information for an HDX channel that has no current alerts.

    a. Click **Adobe Flash** to view information about the channel.
    b. Click the **X** to close the window.

9. Click **Download System Report** to export HDX channel information for the session to an .XML file.
10. Save the file to a location of your choice or open the file.

    a. Select **Open with** and then click **OK** to view the HDX channel information.
    b. Click **X** in the Internet Explorer tab containing the HDX information to close the file.

Sending a Message to an End User

You can send messages to end users (or as a group message) to inform them about desktop maintenance or to communicate individually. For example, you may want to tell end users to log off before critical maintenance is about to take place to ensure they save their work, preventing loss of data.

To Send a Message to an End User

1. Log on to Director (*http://server/Director*) using domain administrator credentials.

    a. Type ***http://C-1.cch.local/Director*** in a Web browser on the **StudentManagementConsole-1** virtual machine and then press **Enter**.
    b. Log on using the **Admin1**, **Password1** and **CCH** credentials.

2. Scroll to the right within any page in Director to access the Search users field.
3. Search for an end-user session whose HDX details you want to view and then click **Details** below the Search users field.

    Type **HRUser1** in the Search users field, press **Enter**, and then click **Details**.

If Activity Manager appears instead of Details, you are already on the Details page.

4. Ensure that the appropriate desktop or application connection for the end user is displayed.

   Click the machine switcher icon (Computer display icon) at the top of the Details page and then select the **WordPad** resource from the drop-down menu.

The machine switcher icon is only available when the selected end user has multiple sessions running.

5. Scroll the page to the right to view the Session Details pane.
6. Click the **Send Message** button.
7. Type a message you would like to send the end user.

   Type **Thank you for contacting the Helpdesk. Your issue should now be resolved.**

8. Click **Send** and then verify that the message was successfully sent.

   a. Click **Send**.
   b. Switch to the **EndPoint-Internal** virtual machine and then click **OK** on the message to close it.
   c. Switch back to the **StudentManagementConsole-1** virtual machine.

The selected end user must have an active session running in order to receive the message. If the end user is disconnected or the session has timed out, the end user will not receive the message.

Shadowing an End-User Session

Director allows you to shadow a XenDesktop session while assisting an end user. When shadowing, you are using the Microsoft Remote Assistance client, which allows you to view and work on the virtual machine of an end user whom you are assisting. You can also request that the end user allow you to share control of the keyboard and mouse.

The Microsoft Remote Assistance client must be installed on the system running Director, usually the Helpdesk Agent's desktop. In addition, remote assistance must be enabled on the virtual desktop, either through the Virtual Delivery Agent Installation Wizard or through an Active Directory GPO. By default, only local administrators on the virtual desktop, including domain administrators, can launch a shadowing session. To provide shadowing access to Helpdesk administrators, you must configure an Active Directory GPO to add those administrators as remote assistance users.

To Shadow an End-User Session

1. Log on to Director (*http://server/Director*) using domain administrator credentials.

   a. Type ***http://C-1.cch.local/Director*** in a Web browser on the **StudentManagementConsole-1** virtual machine and then press **Enter**.
   b. Log on using the **Admin1**, **Password1** and **CCH** credentials.

2. Scroll to the right within any page in Director to access the Search users field.
3. Search for an end-user session that you want to shadow and then click **Details** below the Search users field.

   Type **HRUser1** in the Search users field, press **Enter**, and then click **Details**.

If Activity Manager appears instead of Details, you are already on the Details page.

4. Scroll the page to the right to view the Session Details pane.
5. Click the **Shadow** button.
6. Click **OK** in the Opening Invite.msrcincident dialog box and wait for the end user to accept your invitation.

   a. Click **OK** in the message on the **StudentManagementConsole-1** VM running Director to start the Shadowing session.
   b. Switch to the **Endpoint-Internal** machine and click **Yes** in the "Would you like to allow HelpAssistant to connect to your computer" message.

If the end user does not respond within 120 seconds, the connection will fail. If the user does not respond, click **OK** in the Windows Remote Assistance message, on the system running Director, to end the shadowing request.

7. Click **Request control** at the top of the Windows Remote Assistance window on the system running Director to ask the end user to allow you to take control of the keyboard and mouse in the session.

   a. Click **Request control** from the Windows Remote Assistance window on the system running Director.
   b. Switch to the **EndPoint-Internal** virtual machine.
   c. Click **Yes** on the Windows Remote Assistance screen to allow Admin1 to share control.
   d. Switch back to the **StudentManagementConsole-1** virtual machine.

8. Assist the end user from the system running Director and then close the Windows Remote Assistance window to end the shadowing session.

   Click the **X** in the small or full screen Windows Remote Assistance window.

The end user could also end the shadowing session by clicking the X in the Windows Remote Assistance window displayed on the endpoint. If the administrator ends the shadowing session closing the small Windows Remote Assistance window, they must close the full screen Windows Remote Assistance window separately.

Disconnecting an End-User Session

Disconnecting a session will break the connection that the end user has with their virtual desktop or application, however, the desktop or application will continue to run. When creating a new user session, the end user will have the ability to resume their work where they were interrupted. This is valuable when an end user has difficulty during a session, and may have unsaved work.

To Disconnect an End-User Session

1. Log on to Director (*http://server/Director*) using domain administrator credentials.

   a. Type ***http://C-1.cch.local/Director*** in a Web browser on the **StudentManagementConsole-1** virtual machine and then press **Enter**.
   b. Log on using the **Admin1**, **Password1** and **CCH** credentials.

2. Scroll to the right within any page in Director to access the Search users field.
3. Search for an end-user whose session that you want to disconnect and then click **Details** below the Search users field.

   Type **HRUser1** in the Search users field, press **Enter**, and then click **Details**.

If Activity Manager appears instead of Details, you are already on the Details page.

4. Ensure that the appropriate desktop or application connection for the end user is displayed.

   Click the machine switcher icon (Computer display icon) at the top of the page and then select the **WordPad** resource from the drop-down menu.

The machine switcher icon is only available when the selected end user has multiple sessions running.

5. Scroll the Details page to the right and then click **Session Control**.
6. Click **Disconnect** to disconnect the selected session.
7. Verify that the state of the session has changed to Disconnected.

Logging an End User Off

Unlike disconnecting an end-user session, logging an end user off will completely log the end user off the desktop or application, therefore leading to a loss of data. Once an end user is logged off of a desktop, it will become available to other end users.

To Log an End User Off

1. Log on to Director (*http://server/Director*) using domain administrator credentials.

a. Type ***http://C-1.cch.local/Director*** in a Web browser on the **StudentManagementConsole-1** virtual machine and then press **Enter**.
b. Log on using the **Admin1**, **Password1** and **CCH** credentials.

2. Scroll to the right within any page in Director to access the Search users field.
3. Search for an end user whose session that you want to log off and then click **Details** below the Search users field.

   Type **HRUser1** in the Search users field, press **Enter**, and then click **Details**.

If Activity Manager appears instead of Details, you are already on the Details page.

4. Ensure that the appropriate desktop or application connection for the user is displayed.

   Click the machine switcher icon (Computer display icon) at the top of the page and then select the **WordPad** resource from the drop-down menu.

If Activity Manager appears instead of Details, you are already on the Details page.

The machine switcher icon is not visible if the selected end user only has a single connection running.

5. Scroll the Details page to the right and then click **Session Control**.
6. Click **Log Off** to log the end user off the session.

Wait while the end user is logged off. Do not click Log Off again, doing so will result in an error being displayed. After the end user is logged off the session, the session details will disappear from the Details pane.

Discussion Question

What is the difference between disconnecting a session and logging a session off?

Monitoring Historical Trends

In Director, use the Trends page to access historical trend information for sessions, connection failures, machine failures, logon performance, and load evaluation for each site. To locate the information, on the Dashboard or Filters page, click Trends.

Each graph shows trend data for a specified period of time (the default is previous 24 hours) and for specified Delivery Groups (default: all groups). You can also view data for a single point in time by pointing your cursor to that location. Click the refresh icon at any time to update the data.

You can save the graph to a PDF file or save the data to a CSV file so that you can reuse the data in other applications. When the data is exported, you can view more detailed information that was not visible within the graph, assisting with the analysis of historical trends.

To Monitor Historical Trends

1. Log on to Director (*http://server/Director*) using domain administrator credentials.

   a. Type ***http://C-1.cch.local/Director*** in a Web browser on the **StudentManagementConsole-1** virtual machine and then press **Enter**.
   b. Log on using the **Admin1**, **Password1** and **CCH** credentials.

2. Click **Trends** at the top of the Director window.
3. Select the appropriate tab according to the type of trend analysis you would like to perform.

   Select the **Logon Performance** tab.

4. Select specific filters to view only important information that is relative to your analysis.

   a. Select **All** in the Delivery Group field.
   b. Select **Last 24 hours** in the Time period field.

5. Click **Apply**.
6. Review the information for specific trends.

Troubleshooting: Managing Sites, Sessions, and End Users with Director

Issue	Resolution
An error dialog is received during configuration with Citrix Studio.	If an error dialog box is received while configuring XenDesktop in Citrix Studio, a descriptive message will display that may help you self-diagnose the issue. If you are unable to address the issue based on the descriptive error message, you can select the option in Studio: "I need help from Citrix to solve this problem." When this option is selected, the Citrix Tools as a Service (TaaS) system searches an error reporting web service maintained by the Citrix TaaS team. If the service locates a matching Knowledge Base (KB) article that specifically addresses the problem, it displays the article. If no match is found, you are directed to a web page where you can send details to Citrix and search Citrix Support forums.  For more information about TaaS, access your Student Resource Kit (SRK).
Unable to shadow an end-user session in Director.	1. Ensure that the end user has an active session. 2. Verify that remote assistance is enabled on the virtual desktop. 3. Verify that the administrator has the correct permissions to shadow end users within Director. 4. Verify that the device you are trying to shadow accepts connections on port 3389.
The HDX Panel is not available in the administrator's Director.	Verify that the end user's machine is connected using HDX. If the end user is not connected using HDX, then the panel will not be available.

Issue	Resolution
Usage graphs are not displayed in the dashboard.	Ensure that the latest version of Flash is installed on the system running Director.
An error is displayed when running Real-Time reports.	Citrix Director requires that WinRM 1.1 or later be installed and enabled on the desktop machine.  Citrix recommends upgrading to WinRM 2.0 - based on operating system compatibility.

Reinforcement Exercise: Using Director

During this exercise, you will not be given step-by-step instructions for performing the task. Instead, you are asked to use what you have learned to complete it. This exercise is designed to take your newly-acquired knowledge and determine if you can apply it to perform a task you have never done before. In most instances the default value will be the best choice, but we encourage you to explore and try different options. If you have a question or need help, ask the instructor or a fellow student for assistance.

In this module, you learned how to:

- Monitor using the Dashboard within Director.
- Monitor and manage end-user sessions within Director.
- Monitor historical trends within Director.

Time to complete: Approximately 30 minutes

As a prerequisite for this exercise, perform the following:

- Log on to the EndPoint-Internal virtual machine using the HRUser1 and Password1 credentials.
- Log on to StoreFront (https://sfs-1.cch.local/Citrix/StoreWeb) using the HRUser1 and Password1 credentials.
- Launch the HR Desktop.

You want to explore some more of the options that Director can offer CCH.

To complete your objective:

- Use Director to restart the machine used by the HRUser1 user.
- View the results of issuing the command:
  - Watch the virtual machine restart in Citrix XenCenter.
  - View the results on the EndPoint-Internal virtual machine.
- On the EndPoint-Internal virtual machine log on again to HR Desktop using the CCH\HRUser1 credentials once the machine has finished restarting.
- Reset the Personal vDisk of the HR Desktop for the CCH\HRUser1.

Module 8

Managing Printing

8

Managing Printing

Printing is a very important aspect of every Citrix infrastructure, but it is not well understood and a common cause of issues. XenDesktop offers a variety of features to enable you to successfully integrate printing in almost every scenario. Choosing the most appropriate printing configuration for your organization helps to simplify administration and improve the end-user experience. In order to successfully design a printing infrastructure it is vital to understand the available technologies as well as their benefits and limitations.

After completing this module, you will be able to:

- Manage printers using policies.
- Add session printers.
- Map and install printer drivers.
- Customize and optimize printing performance.
- Manage the Universal Print Server.

Module timing: Approximately 3 hours

Managing Printing

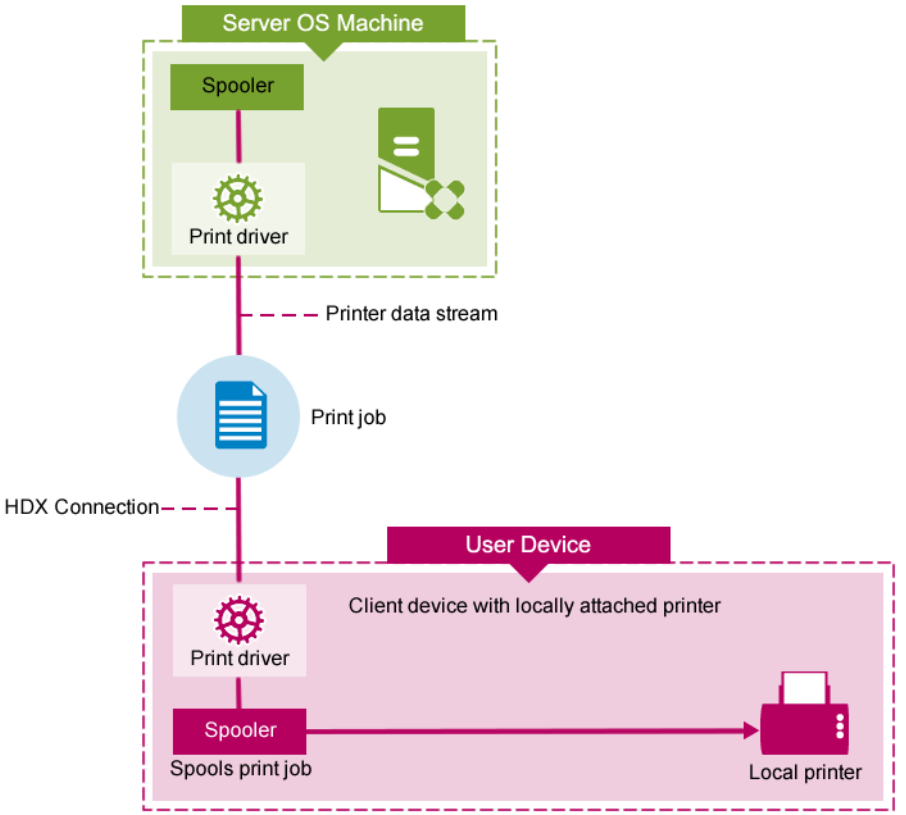
Managing printing in a XenDesktop environment is a multistage process:

- Plan your printing architecture, including analyzing your business needs, your existing printing infrastructure, how your end users and applications interact with printing today, and which printing management model best applies to your environment.
- Configure your printing environment, including creating the policies necessary to deploy your printing design.
- Test a pilot printing configuration before deploying it to end users.
- Maintain your Citrix printing environment, including updating policies when new employees or servers are added and maintaining drivers on your XenDesktop machines.
- Troubleshoot issues that may arise in your printing environment.

Default Printing Behavior

By default, if you do not configure any policy rules, XenDesktop printing behavior is as follows:

- All printers configured on the end-user device are created automatically at the beginning of each session. This behavior is equivalent to configuring the Citrix policy setting Auto-create client printers with the Auto-create all client printers option.
- XenDesktop routes all print jobs queued to printers locally attached to end-user devices as client print jobs.
- XenDesktop routes all print jobs queued to network printers directly from Server OS machines. If XenDesktop cannot route the jobs over the network, it will route them through the end-user device as a redirected client print job.
- XenDesktop uses the Windows version of the printer. If the printer driver is not available, XenDesktop attempts to install the driver from the Windows operating system. If the driver is not available in Windows, it uses a Citrix Universal Printer Driver.
- The Universal Print Server is disabled.



Configuring Client Printing

XenDesktop policies specify the client printers that are made available for end-user sessions. You can control the number and type of printers that are made available, along with customizing printer settings and options.

Within client-based printing policies, you can configure options such as client printer auto-creation, client printer redirection, printer property retention, print mapping, and other settings.

Modifying Client Printer Auto-Creation

Client printer auto-creation settings allow you to specify client printing behavior from the auto-creation of default printers to auto-creation of local non-network client printers only.

During printer auto-creation, if a new local printer connected to a end-user device is detected, the server hosting the published application is checked for the required printer driver. By default, if a Windows-native driver is not available, the Universal printer driver is used. This setting overrides default client printer auto-creation settings. This setting takes effect only if the Client printer redirection setting is present and set to Allowed.

To Modify Client Printer Auto-Creation Behavior

1. Log on to a virtual machine that has Citrix Studio and the Group Policy Management feature installed using domain administrator credentials.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Click **Start** and then click **Group Policy Management** to open the Group Policy Management Console.
3. Select the organizational unit to which you want to apply the policy.

   Expand **Forest: CCH.local** > **Domains** > **CCH.local** > **CCH Users** > **Human Resources**.

4. Right-click the OU and then click **Create a GPO in this domain, and Link it here**.

   Right-click **Human Resources** and then click **Create a GPO in this domain, and Link it here**.

5. Type a name for the new Group Policy Object and then click **OK**.

   Type **Print Settings** in the Name field and then click **OK**.

6. Click the OU containing the policy, right-click the GPO to which you want to add settings in the Linked Group Policy Objects tab and then click **Edit**.

   Click the **Human Resources** OU, right-click **Print Settings** in the Linked Group Policy Objects tab, and then click **Edit**.

7. Expand **User Configuration** > **Policies** > **Citrix Policies** nodes.
8. Click **Edit** in the right pane to add settings to the unfiltered Citrix User Policy.

If you select Edit, you are adding new settings to the Unfiltered policy. If you select New, you are creating a new policy and can filter that policy to determine to which objects the policy will apply.

9. Select the **Settings** tab to view the available settings.
10. Select a category of settings in the Categories field.

    Select **Printing** > **Client Printers**.

If you know the name of the category or a word in the name of the setting, you can search for the setting using the Search field. For example, you could search for Printing or Client Printers, or auto-create.

11. Click **Add** to the right of the desired setting.

Click **Add** to the right of the Auto-create client printers setting.

12. Select the desired value for the setting in the Value field and then click **OK**.

    Select **Auto-create the client's default printer only** and then click **OK**.

13. Click **OK**.
14. Close the Group Policy Management Editor.
15. Expand the **Group Policy Object** OU in the left pane and drag the policy to another OU to which you also want to apply that policy.

    a. Expand the **Group Policy Objects** OU, select the **Print Settings** policy, and drag it to the **CCH Users > Engineering** OU.

    b. Click **OK** in the Group Policy Management message.

This step is only necessary if you want to apply an existing policy to another OU.

Discussion Question

In your environment, you have attempted to configure printer auto-creation. You notice however that when a Windows-native driver is not available, the Universal print driver is not being used. What could be the problem?

Adding Session Printers

By default, network printers on the end-user device are created automatically at the beginning of sessions. XenDesktop enables you to reduce the number of network printers that are enumerated and mapped by specifying the network printers to be created within each session.

Network printers created within the session printers setting can vary according to where the session was initiated by filtering on objects such as subnets. This feature enables you to control the assignment of network printers so that the most appropriate printer is presented to the end-user, based on the location of the end-user device (also known as Proximity Printing).

To Add Session Printers

1. Ensure that the Print Server is running.

Double-click the **UniversalPrintServer-1** virtual machine in XenCenter to start it and wait for the logon screen to appear.

2. Log on to a virtual machine that has Citrix Studio and the Group Policy Management feature installed using domain administrator credentials.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

3. Click **Start** and then click **Group Policy Management** to open the Group Policy Management Console.
4. Select the organizational unit to which you want to apply the policy.

   Expand **Forest: CCH.local** > **Domains** > **CCH.local** > **CCH Users**.

5. Right-click the OU and then click **Create a GPO in this domain, and Link it here**.

   Right-click **CCH Users** and then click **Create a GPO in this domain, and Link it here**.

6. Type a name for the new Group Policy Object and then click **OK**.

   Type **Session Printers** in the Name field and then click **OK**.

7. Click the OU containing the newly created policy, right-click the GPO to which you want to add settings in the Linked Group Policy Objects tab, and then click **Edit**.

   Click **CCH Users**, right-click **Session Printers** in the Linked Group Policy Objects tab and then click **Edit**.

8. Expand **User Configuration** > **Policies** > **Citrix Policies**.
9. Click **New** in the right pane to launch the New Policy wizard.

If you select Edit, you are adding new settings to the Unfiltered policy. If you select New, you are creating a new policy and can filter that policy to determine to which objects the policy will apply.

You are creating a new policy so that filters can be applied at a later time should you decide to enable proximity printing.

10. Type a name for the new policy or leave the field blank and then click **Next**.

    Type **Citrix Session Printers** in the Name field and then click **Next**.

11. Type a setting name or a word contained in the setting to filter the Settings list.

    Type **Session** or **Printers** in the Search field.

You could also scroll through the categories of settings in the Categories field to find the required setting.

12. Click **Add** to the right of the desired setting.

    Click **Add** to the right of the Session printers setting.

13. Click **Add** in the Add Setting screen.
14. Click **Browse**, go to the location where the network printers are defined, and then click **OK**.

    a. Click **Browse**.
    b. Expand **Entire Network > Microsoft Windows Network** > **CCH** > **UPS-1**.
    c. Click **Accounting** to add the Accounting printer.
    d. Click **OK** twice.

You could also type the UNC path to the printer directly into the Printer UNC path field and then click OK.

15. Click **OK** after all desired network printers are added to the Session printers list.
16. Click **Next** to go to the Filters screen.

17. Configure any necessary filters and then click **Next**.

    Click **Next**.

You will not be adding any filters at this time. If you wanted to enable proximity printing, you could assign session printers to end users based on the Client IP address filter. Session printers are an optimal configuration for scenarios where users roam between locations using the same device (i.e. laptop) or where thin clients are used because they do not have the ability to connect to network-based printers directly.

18. Click **Create**.
19. Close the Group Policy Management Editor.

Managing Printer Drivers

There are three options for managing printer driver usage within XenDesktop policies:

- Automatic installation of in-box printer drivers
- Universal Printer Driver preference
- Universal Printer Driver usage

Using these features, you can control the way end-user sessions use specific printer drivers as well as configure the Citrix Universal Printer driver settings.

Automatic Installation of In-Box Printer Drivers

You have the ability to control the automatic installation of Windows-native printer drivers. If it is necessary to ensure consistency across Server OS machines and virtual desktops, this can be achieved by disabling the policy setting through Citrix or Microsoft policies.

To Configure the Automatic Installation of Printer Drivers

1. Log on to a virtual machine that has Citrix Studio and the Group Policy Management feature installed using domain administrator credentials.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Click **Start** and then click **Group Policy Management** to open the Group Policy Management Console.
3. Select the organizational unit to which you want to apply the policy.

   Expand **Forest: CCH.local** > **Domains** > **CCH.local** > **CCH Users**.

4. Right-click the OU and then click **Create a GPO in this domain, and Link it here**.

   Right-click **CCH Users** and then click **Create a GPO in this domain, and Link it here**.

5. Type a name for the new Group Policy Object and then click **OK**.

   Type **Disable Auto-Install of Printer Drivers** in the Name field and then click **OK**.

6. Click the OU containing the newly created policy, right-click the GPO to which you want to add settings in the Linked Group Policy Objects tab, and then click **Edit**.

   Click **CCH Users**, right-click **Disable Auto-Install of Printer Drivers** in the Linked Group Policy Objects tab and then click **Edit**.

7. Expand **User Configuration** > **Policies** > **Citrix Policies**.
8. Select **Edit** to add settings to the unfiltered Citrix User Policy.

9. Select the **Settings** tab to view the available settings.
10. Type a setting name or a word contained in the setting to filter the Settings list.

    Type **Automatic** or **Printers** in the Search field.

You could also scroll through the categories of settings in the Categories field to find the required setting.

11. Click **Add** to the right of the desired setting.

    Click **Add** to the right of the Automatic installation of in-box printer drivers setting.

12. Select the appropriate value for the setting and then click **OK**.

    Select **Disabled** and then click **OK**.

13. Click **OK**.

While you added multiple settings to the unfiltered Citrix User Policy in previous procedures, the reason that you do not see them now is because they were applied to a different OU in the environment.

14. Close the Group Policy Management Editor.

Configuring Printer Driver Mapping and Compatibility

Each client provides information about client-side printers during logon, including the printer driver name. During client printer auto-creation, Windows server printer driver names are selected; these names correspond to the printer model names provided by the client. The auto-creation process then uses identified, available printer drivers to construct redirected client print queues.

When you define these rules, you can allow or prevent printers to be created with the specific driver. Additionally, you can allow created printers to use only the Universal Printer Driver.

You can add a driver mapping, edit an existing mapping, or override custom settings.

To Configure Printer Driver Mapping and Compatibility

1. Log on to a virtual machine that has Citrix Studio and the Group Policy Management feature installed using domain administrator credentials.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Click **Start** and then click **Group Policy Management** to open the Group Policy Management Console.

3. Browse to the OU containing the Group Policy Objects.

   Expand **Forest: CCH.local** > **Domains** > **CCH.local** > **Group Policy Objects**.

4. Right-click the policy to which you want to add new settings and then click **Edit**.

   Right-click the **Print Settings** policy and then click **Edit**.

5. Expand **User Configuration** > **Policies** > **Citrix Policies**.
6. Select **Edit** to add settings to the unfiltered Citrix User Policy.

If you select Edit, you are adding new settings to the Unfiltered policy. If you select New, you are creating a new policy and can filter that policy to determine to which objects the policy will apply.

7. Select the **Settings** tab to view the available settings.
8. Type a setting name or a word contained in the setting to filter the Settings list.

   Type **Mapping** or **Printer** in the Search field.

You could also scroll through the categories of settings in the Categories field to find the required setting.

9. Click **Add** to the right of the desired setting.

   Click **Add** to the right of the Printer driver mapping and compatibility setting.

10. Specify the desired values for the setting.

    a. Click **Add** to configure driver mapping.
    b. Type **HP PhotoSmart D-110**.
    c. Select **Replace with**.
    d. Type **HP PhotoSmart 220X** in the Replace with field.
    e. Click **OK**.

You could also click the Find Driver button to search for the desired printer driver. If you have printer drivers already configured, you can use those drivers.

11. Click **OK** twice after all settings have been configured.

The new setting in the unfiltered policy is displayed in the Active Settings pane of the Group Policy Management Editor.

12. Close the Group Policy Management Editor.

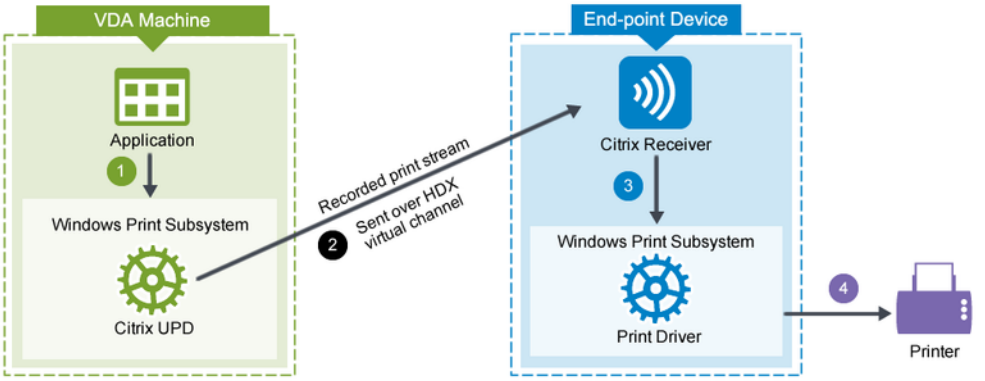
Universal Printer Driver (UPD)

To simplify printing in XenDesktop environments, Citrix recommends the use of the Citrix Universal Printer Driver (UPD). The Universal Printer Driver is a device-independent driver that supports any print device and thus simplifies administration by reducing the number of drivers required. The Universal Printer Driver supports advanced printer functionality, such as stapling and sorting, and does not limit color depth.

The UPD consists of two components:

- **Server component**: On a XenDesktop-based virtual desktop, the Citrix UPD is installed as part of the XenDesktop VDA installation. When a print job is initiated, this driver records the output of the application and sends it, without any modification, to the end-user device with the ICA/HDX connection.
- **Client component**: The client component of the Citrix UPD is installed as part of the Citrix Receiver installation. It receives the incoming print stream for the virtual desktop and forwards it to the local printing subsystem where the print job is rendered using the device-specific printer driver.

The following diagram shows the UPD components and a typical work flow for a printer locally attached to a device.



Controlling Universal Printing Behavior

Universal Printing behavior is controlled by configuring policies to optimize processing, print quality, and compression limit settings. Using these features you can streamline items such as the transfer of printer traffic and the spooling process.

Optimizing Printing Performance

To optimize printing performance, use the Universal Print Server and Universal Printer Driver. The following policies control printing optimization and compression:

- Universal printing optimization defaults
  - Desired image quality
  - Enable heavyweight compression
  - Image and Font caching
  - Allow non-administrators to modify these settings
- Universal printing image compression limit
- Universal printing print quality limit
- Printer redirection bandwidth limit
- Printer redirection bandwidth limit percent

To Configure Printing Optimization

1. Log on to a virtual machine that has Citrix Studio and the Group Policy Management feature installed using domain administrator credentials.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Click **Start** and then click **Group Policy Management** to open the Group Policy Management Console.
3. Browse to the OU to which you want to apply the policy.

   Expand **Forest: CCH.local** > **Domains** > **CCH.local** > **CCH Virtual Desktop**.

4. Right-click the OU and then click **Create a GPO in this domain, and Link it here**.

Right-click the **CCH Users** and then click **Create a GPO in this domain, and Link it here**.

5. Type a name for the new policy and then click **OK**.

Type **Printer Optimizations** in the Name field and then click **OK**.

6. Right-click the policy in the Linked Group Policy Objects tab and then click **Edit**.

   Right-click the **Printer Optimizations** policy and then click **Edit**.

7. Expand **User Configuration** > **Policies** > **Citrix Policies**.
8. Select **Edit** to add settings to the unfiltered Citrix User Policy.

If you select Edit, you are adding new settings to the Unfiltered policy. If you select New, you are creating a new policy and can filter that policy to determine to which objects the policy will apply.

9. Select the **Settings** tab to view the available settings.
10. Type a setting name or a word contained in the setting to filter the Settings list.

    Type **Universal** or **Printing** in the Search field.

You could also scroll through the categories of settings in the Categories field to find the required setting.

11. Click **Add** to the right of the desired setting.

    Click **Add** to the right of the Universal printing optimization defaults setting.

12. Specify the desired values for the setting.

    Select **Reduced quality (maximum compression)** in the Desired image quality field, select the **Enable heavy weight compression** and then click **OK**.

13. Click **Add** to the right of the desired setting.

    Click **Add** to the right of the Universal printing print quality limit setting.

14. Select the desired option from the Value field.

    Select **Medium resolution (600 DPI)**.

15. Click **OK** twice after all settings have been configured.

The new settings in the unfiltered policy are displayed in the Active Settings pane of the Group Policy Management Editor.

While you added multiple settings to the unfiltered Citrix User Policy in previous procedures, the reason that you do not see them now is because they were applied to a different OU in the environment.

16. Close the Group Policy Management Editor.

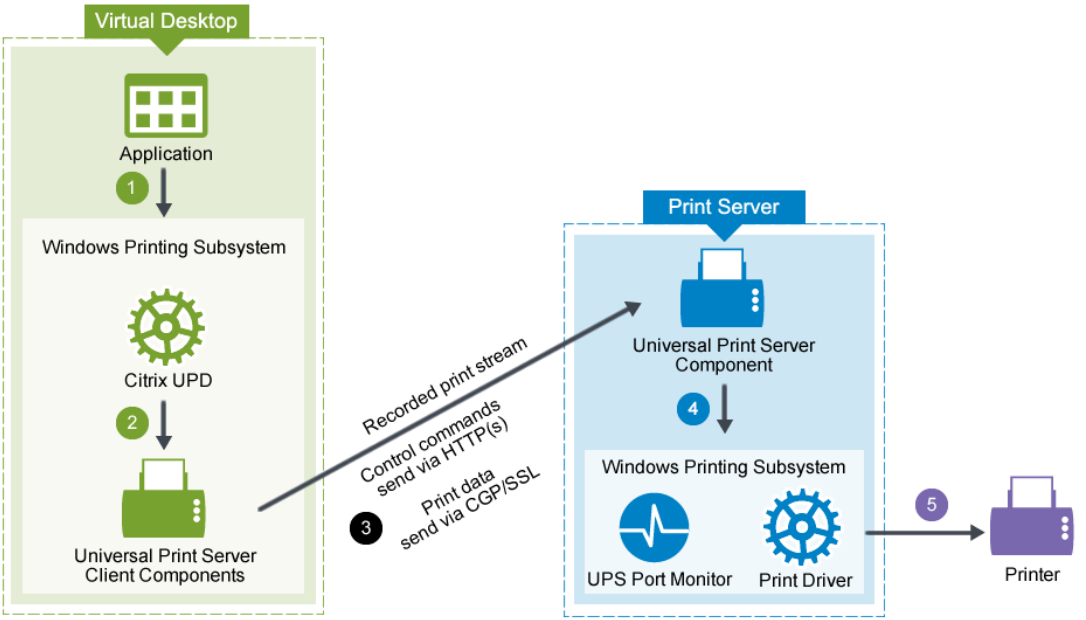
Discussion Question

Users are experiencing substantial network latency when attempting to print high quality images used for marketing campaigns. What polices should be adjusted or implemented to resolve this? Which policies would you want to avoid?

Setting Up and Managing the Universal Print Server

The Universal Print Server provides universal printing support for network printers. The Universal Print Server uses the Universal Printer Driver, which is installed with XenDesktop.

Citrix recommends the Citrix Universal Print Server for remote print server scenarios. The Universal Print Server transfers the print job over the network in an optimized and compressed format, thus minimizing network use and improving the end-user experience.



To Set Up and Manage the Universal Print Server

1. Log on to a virtual machine that has Citrix Studio and the Group Policy Management feature installed using domain administrator credentials.

   Log on to the **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Click **Start** and then click **Group Policy Management** to open the Group Policy Management Console.
3. Browse to the OU to which you want to apply the policy.

   Expand **Forest: CCH.local** > **Domains** > **CCH.local** > **CCH Virtual Desktop**.

4. Right-click the OU and then click **Create a GPO in this domain, and Link it here**.

Right-click the **CCH Virtual Desktop** and then click **Create a GPO in this domain, and Link it here**.

5. Type a name for the new policy and then click **OK**.

Type **Universal Printing** in the Name field and then click **OK**.

6. Right-click the policy in the Linked Group Policy Objects tab and then click **Edit**.

   Right-click the **Universal Printing** policy and then click **Edit**.

7. Expand **Computer Configuration** > **Policies** > **Citrix Policies**.

Ensure that you select Computer Configuration in this step.

8. Select **Edit** to add settings to the unfiltered Citrix User Policy.

If you select Edit, you are adding new settings to the Unfiltered policy. If you select New, you are creating a new policy and can filter that policy to determine to which objects the policy will apply.

9. Select the **Settings** tab to view the available settings.
10. Type a setting name or a word contained in the setting to filter the Settings list.

    Type **Print Server** in the Search field.

You could also scroll through the categories of settings in the Categories field to find the required setting.

11. Click **Add** to the right of the desired setting.

    Click **Add** to the right of the Universal Print Server enable setting.

12. Click **OK** to continue.

13. Specify the desired values for the setting and then click **OK**.

    Select **Enabled with fallback to Windows' native remote printing** in the Value field and then click **OK**.

14. Click **OK** twice after all settings have been configured.

The new settings in the unfiltered policy are displayed in the Active Settings pane of the Group Policy Management Editor. While you added multiple settings to the unfiltered Citrix User Policy in the previous procedure, the reason that you do not see them now is because this policy setting is a Citrix Computer Policy rather than a Citrix User Policy.

15. Close the Group Policy Management Editor.

Troubleshooting: Managing Printing

Issue	Resolution
Cannot update printer drivers.	Citrix recommends that you never update a printer driver. Always uninstall a driver, restart the print server, and install the replacement driver. This helps ensure consistency and decreases the chance that issues with existing drivers are transferred to the updated drivers.
Printers that are no longer used or no longer exist are being created.	Verify that all unused drivers are uninstalled to prevent this.
The Universal Print Server does not appear.	• Verify that the Universal Print Server is enabled. • Ensure that the operating system is Windows Server 2008 or later.

Module 9

Managing Provisioning Services

9

Managing Provisioning Services

Provisioning Services takes a different approach from traditional imaging solutions by fundamentally changing the relationship between hardware and the software that runs on it, enabling organizations to reduce the number of images that they manage, and simultaneously providing the efficiencies of a centralized management with the benefits of distributed processing.

After completing this module, you will be able to:

- Describe the basic architecture and communication flow of Provisioning Services.
- Describe the differences between Machine Creation Services and Provisioning Services.
- Manage vDisks and target devices for a Provisioning Services implementation.
- Manage vDisk updates.

Module timing: Approximately 5 hours

Citrix Provisioning Services

Provisioning Services provides the ability to provision the operating system of a computer and re-provision it in real time. Administrators can choose from a one-to-one relationship between the Provisioning Services host and the target device or a one-to-many relationship, starting multiple target devices from a single shared-disk image. In doing so, you can completely eliminate the need to manage and update individual systems, allowing changes made to one disk to be deployed to multiple target devices simultaneously.

Provisioning Services is based on software-streaming technology. After installing and configuring Provisioning Services components, a vDisk is created from the hard drive of a device by taking a snapshot of the operating system and application image, and then storing that image as a VHD file on the network.

vDisks can exist on a Provisioning Services host, file share, or in larger deployments, on a storage system with which the Provisioning Services host can communicate, such as iSCSI, NFS, and CIFS. vDisks can be assigned to a single target device in private image mode, or to multiple target devices in standard image mode.

Machine Creation Services or Provisioning Services

Citrix XenDesktop contains improvements to both the Machine Creation Services (MCS) and Provisioning Services (PVS) features.

XenDesktop sites can now be deployed and managed from within Studio. Sites can also be provisioned using the MCS linked-clone delivery model. MCS allows new machine catalogs containing virtual desktops and Server OS machines to be created with ease.

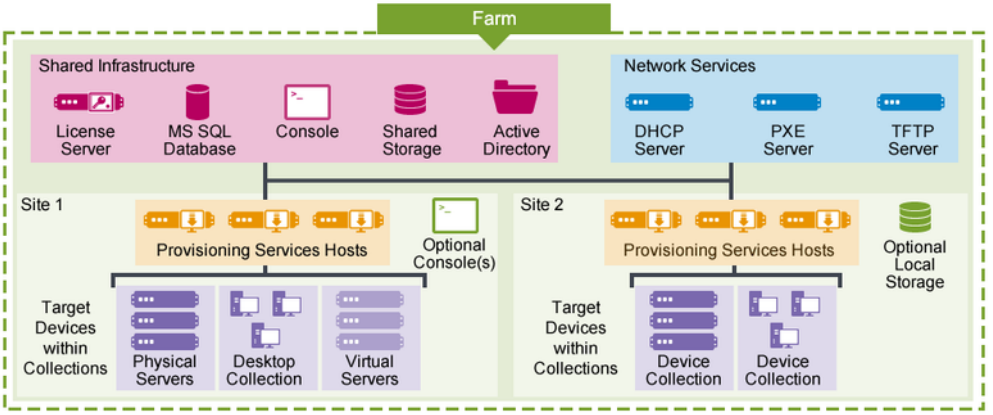
The Machine Creation Services model provides many of the same single-image management benefits of Provisioning Services, but works directly on the storage managed by your hypervisor, so there is no need for PXE or to build out a Provisioning Services deployment.

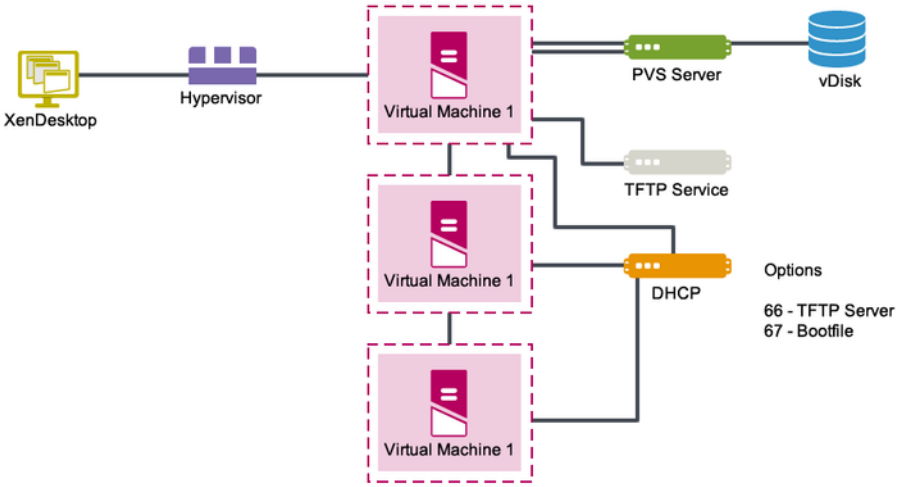
Provisioning Services provides enhanced image management capabilities and storage I/O optimizations beneficial in larger, more complex environments. Provisioning Services can provide a centralized image library for mixed environments where multiple XenDesktop sites are used.

Your implementation may require you to migrate your virtual machines from Machine Creation Services to Provisioning Services. This will allow you to use the machines that you created using Machine Creation Services and deploy and manage those using Provisioning Services.

When possible, Citrix recommends reducing complexity by using either Provisioning Services or Machine Creation Services, but not both. For more information about using Machine Creation Services or Provisioning Services, see the Citrix blog "PVS vs. MCS Revisited" at *http://blogs.citrix.com/2013/08/12/pvs-vs-mcs-revisited/*.

Provisioning Services Overview and Architecture





When a target device is turned on, it is set to start from the network and to communicate with a Provisioning Services host. The target device downloads the startup file from a TFTP server, and then the target device starts up. Based on the device start up configuration settings, the appropriate vDisk is located, and then mounted by a Provisioning Services host. The software on that vDisk is streamed to the target device, as needed.

Instead of immediately pulling all the vDisk content down to the target device, the data is brought across the network in real time, as needed. The Provisioning Services host provides blocks of data from the vDisk as they are requested by the operating system, in the same way that the operating system would normally request them from its hard drive. This approach allows a target device to load a completely new operating system and software from the vDisk in the time it takes to restart. This approach dramatically decreases the amount of network bandwidth required by traditional disk imaging tools; making it possible to support a larger number of target devices on your network without impacting overall network performance, although a dedicated storage network could be required for larger implementations.

Discussion Question

What are the components that comprise a Provisioning Services farm? What would happen if the SQL database of the Provisioning Services farm failed?

Navigating the Provisioning Services Console

The Provisioning Services Console is used for viewing and managing sites, servers, connections, and performing tasks such as assigning vDisk to target devices, managing stores, creating device collections and more.

To Navigate the Provisioning Services Console

1. Ensure that your Provisioning Services servers are started.

   Start the **ProvisioningServicesHost-1** virtual machine in XenCenter and wait for it to start before continuing to the next step.

2. Log on to a virtual machine that has the Provisioning Services Console installed using domain administrator credentials.

   Start the **StudentManagementConsole-1** virtual machine and log on using the **CCH\Admin1** and **Password1** credentials.

3. Click the **Provisioning Services Console** icon on the Start screen.

The Provisioning Services Console has also been added as a shortcut on the desktop of the StudentManagementConsole-1 virtual machine.

4. Specify the hostname name of the Provisioning Services server in the Name field and then click **Connect**.

   Type **PVS-1** in the Name field and then click **Connect**.

5. Double-click the farm node in the left pane of the Provisioning Services Console to expand it.

   Double-click **CCH (pvs-1)**.

You could also expand a node by clicking the arrow to the left of the node.

6. Double-click the **Sites** node in the left pane of the Provisioning Services Console to expand it.

The Sites node can contain multiple sites. Each site contains the servers, vDisk pools, device collections, and settings for the resources defined in that site. In our lab environment, you will only have a single site available.

7. Double-click a site in the Sites node to reveal its contents.

   Double-click the **Miami** site.

8. Double-click the **Servers** node in the left pane of the Provisioning Services Console to expand it and view information about the Provisioning Services servers in the implementation.

Notice that the **PVS-1** virtual machine is currently online and in an UP state.

9. Double-click the **Device Collections** node in the left pane of the Provisioning Services Console to expand it and view the collections that are currently defined.
10. Double-click the **Stores** node in the left pane of the Provisioning Services Console to view the stores that are currently defined.

The names of the Sites, Device Collections, and Stores can be changed by right-clicking the node and selecting Properties.

To Create a vDisk File

1. Log on to a virtual machine that has the Provisioning Services Console installed using domain administrator credentials.

   Start the **StudentManagementConsole-1** virtual machine and log on using the **CCH\Admin1** and **Password1** credentials.

2. Click the **Provisioning Services Console** icon on the Start screen and then click **Connect**.

If this is the first time the user has opened the Provisioning Services Console on a system, you must specify the NetBIOS name of the Provisioning Services server in the Name field and then click **Connect** to connect to the server.

3. Browse to the **vDisk Pool** node in the Provisioning Services Console.

   Double-click **CCH (PVS-1)** > **Sites** > **Miami** > **vDisk Pool**.

4. Right-click the **vDisk Pool** node and then select **Create vDisk**.

vDisks are displayed in the Details pane when a site vDisk pool is selected or when a store in the farm is selected.

5. Type a name for the vDisk in the Filename field.

   Type **Windows8** in the Filename field.

6. Specify the size in GB that you want to assign the new vDisk.

   Type **20** in the Size field.

7. Specify the type of vDisk to create.

   Select **Dynamic** in the Type field.

8. Click **Create vDisk**.
9. Verify that the new vDisk appears in the right pane for the vDisk Pool node.

Discussion Question

Why would you create a vDisk and for what purpose?

To Create a Provisioning Services Master Virtual Machine

1. Right-click a template in XenCenter and then click **Quick Create**.

   Right-click the **Win8_template** in XenCenter and then click **Quick Create**.

2. Right-click the newly created virtual machine and then click **Properties**.

   Right-click **Win8_template (1)** and then click **Properties**.

3. Type a new name for the virtual machine in the Name field and then click **OK**.

   Type **Win8-Master (PVS)** as the name and then click **OK**.

4. Click the **Console** tab in XenCenter for the newly created virtual machine and wait for the VM to start.
5. Read and respond to the license terms.

   Select **I accept the license terms for using Windows** and then click **Accept**.

6. Type a name for the computer in the PC name field and then click **Next**.

   Type **Win8-PVS** in the PC name field and then click **Next**.

7. Specify which settings to use for the computer.

Click **Use express settings**.

8. Specify how you want to sign in to the computer.

   Select **Sign in without a Microsoft Account** and then click **Local account.**

9. Specify a username, password and password hint information for the new local account and then click **Finish**.

   a. Type **TempUser2** in the User name field.
   b. Type **Password1** in the Password and Reenter password fields.
   c. Type **First Password** in the Password hint field.
   d. Click **Finish**.

10. Wait while the virtual machine completes its setup and the Start screen appears.
11. Type **Computer** at the Start screen, right-click **Computer**, and then select **Properties**.
12. Click **Change settings** and then click **Change**.
13. Select **Domain**, type the name of the domain into the Domain field, and then click **OK**.

    Select **Domain**, type **CCH.local** and then click **OK**.

14. Type the credentials of a domain administrator into the User name and Password fields and then click **OK**.

    Type **CCH\Admin1** in the User name field, **Password1** in the Password field and then click **OK**.

15. Click **OK** in the ComputerName/Domain Changes message.
16. Click **OK** in the Restart message.
17. Click **Close** in the System Properties screen.
18. Click **Restart Now** in the Microsoft Windows message.

To Install the Virtual Delivery Agent (VDA)

1. Log on to the virtual machine that will be used as the Master Target Device for Provisioning Services using domain administrator credentials.

    Log on to the **Win8-Master (PVS)** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Insert the XenDesktop 7 installation media into the DVD drive.

    Select **Citrix_XenDesktop_7.iso** in the DVD Drive 1 field.

3. Click **Desktop** on the Start screen and then click the **File Explorer** icon.
4. Click **Computer** and then double-click **CD Drive (D:) XenDesktop**.
5. Click **Start** on the XenDesktop 7 Installation screen.
6. Click **Virtual Delivery Agent for Windows Desktop OS**.
7. Determine how you want the Virtual Delivery Agent to be configured on the virtual machine and then click **Next**.

    Select **Create a Master Image** and then click **Next**.

This option is selected because we are installing the VDA on a Master Image. For more information about optimizing XenDesktop machines, see Citrix article CTX125874 at *http://support.citrix.com*.

8. Determine which Virtual Delivery Agent to install on the virtual machine and then click **Next**.

    Select **No, install the standard VDA** and then click **Next**.

9. Select the core components to install during the Virtual Delivery Agent installation and then click **Next**.

    Verify that **Citrix Receiver** is selected and then click **Next**.

10. Determine how the Delivery Controllers in the environment will be identified and then click **Next**.

    a. Select **Do it manually**, type **c-1.cch.local** and then click **Add**.
    b. Type **c-2.cch.local** and then click **Add**.
    c. Click **Next**.

11. Select the features to install and then click **Next**.

    Verify that all features except Personal vDisk are selected and then click **Next**.

12. Determine how the firewall rules will be configured and then click **Next**.

    Select **Automatically** and then click **Next**.

These are the default ports used by the Controller. If you need to use different ports, select **Manually** and then configure the respective ports after the installation completes.

13. Review the prerequisites and the components selected for installation on the Summary screen and then click **Install**.
14. Click **Finish** when the installation is completed.

The virtual machine will restart automatically after the prerequisites and components are installed.

15. Wait while the virtual machine restarts.

Do not shut down the virtual machine or eject the installation media until the virtual machine restarts successfully. If the installation of the VDA or the restart of the virtual machine is interrupted, vDisks created from the Master Target Device will not register with XenDesktop.

16. Eject the installation media from the DVD drive.

    Click **Eject** to the right of the DVD Drive 1 field to eject the installation media.

To Prepare the Master Image for Provisioning Services

1. Click the **Console** tab of the virtual machine that will become the Master Target Device and then log on to the virtual machine using domain administrator credentials.

    a. Click the **Console** tab of the Win8-Master (PVS) virtual machine.
    b. Log on using the **CCH\Admin1** and **Password1** credentials.

2. Insert the Provisioning Services DVD into the DVD drive.

   Select the **Citrix_ProvisioningServices_7.ISO** in the DVD Drive 1 field.

3. Click **Desktop** on the Start screen and then click the **File Explorer** icon in the taskbar.
4. Click **Computer** and then double-click the **CD Drive (D:) PVS_70** to start the installation program.
5. Click **Target Device Installation** to view the target device installation options.
6. Click **Target Device Installation** to begin the installation of the Target Device software on the virtual machine.
7. Click **Next** on the Welcome screen.
8. Read and respond to the license agreement.

   Select **I accept the terms in the license agreement** and then click **Next**.

9. Specify the account being used to install the software and then click **Next**.

   Verify that **TempUser2** is specified in the User Name field and then click **Next**.

10. Specify where the Target Device software should be installed on the virtual machine and then click **Next**.

    Click **Next** to accept the default folder location.

11. Click **Install**.
12. Determine if the Imaging Wizard will be launched by the Target Device Installation program or separately and then click **Finish**.

    Deselect **Launch Imaging Wizard** and then click **Finish**.

The Imaging Wizard software is installed on the Master Target Device virtual machine and can be started from the Start screen on that virtual machine.

13. Click **Yes** in the Restart message to restart the Master Target Device virtual machine.
14. Wait while the Master Target Device virtual machine restarts.
15. Eject the Provisioning Services DVD from the DVD drive.

    Click **Eject** to the right of the DVD Drive 1 field to eject the installation media.

Creating the Master vDisk Image Using the Imaging Wizard

You can use the Provisioning Services Imaging Wizard to automatically create the base vDisk or populate an existing vDisk with an image from a master target device. The Imaging Wizard prompts for information that allows for connecting to the farm as well as information to set the appropriate credentials and licensing information to apply to this particular vDisk.

To Create the Master vDisk

1. Log on to the Master Target Device virtual machine using domain administrator credentials.

   Log on to the **Win8-Master (PVS)** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Click the **General** tab in XenCenter.

   Click the **General** tab in XenCenter for the Win8-Master (PVS) virtual machine.

3. Click **Properties** and then click **Boot Options**.
4. Select **Network** and then click **Move Up** until Network is at the top of the list and then click **OK**.

This will force the target device to boot from the network rather than from a hard drive or a DVD drive.

5. Click the **Console** tab.
6. Type **Imaging Wizard** on the Start screen and then press **Enter**.
7. Click **Next** in the Imaging Wizard Welcome screen.
8. Type the hostname of the Provisioning Services virtual machine into the Server field and then click **Next**.

   Type **PVS-1** and then click **Next**.

9. Determine if a new vDisk will be created or an existing vDisk will be used and then click **Next**.

a. Select **Use existing vDisk**.
b. Select **Store\Windows8** in the vDisk name field.
c. Click **Next**.

You created the Windows 8 vDisk in a previous procedure.

10. Select the Volume Licensing method to be used with the vDisk and then click **Next**.

    Select **Key Management Service (KMS)** and then click **Next**.

11. Specify the size for each volume and then click **Next**.

    Click **Next** to accept the default volume size.

12. Type a name for the target device and then click **Next**.

    Type **Windows8-Master** and then click **Next**.

In the lab environment:

- **Win8-Master (PVS)** is the Master Target Device used to create the vDisk and the target device.
- **Windows8-Master** is the target device that will be stored in the Device Collections node of the Provisioning Services Console.
- **Windows8** is the vDisk and is stored in the Stores node of the Provisioning Services Console.

13. Click **Optimize for Provisioning Services**, determine which optimizations should be implemented and then click **OK**.

    Click **Optimize for Provisioning Services**, verify that all optimizations are selected and then click **OK**.

14. Click **Finish**.
15. Click **Yes** in the Reboot now message and then wait for the virtual machine to restart.
16. Log on to the virtual machine using domain administrator credentials.

    Log on to the **Win8-Master (PVS)** virtual machine using the **CCH\Admin1** and **Password1** credentials.

17. Wait while the XenConvert process completes and then click **Finish**.

This will take approximately 20 minutes in the lab environment based on the size selected for the vDisk.

18. Shut down the Master Target Device virtual machine.

    Shut down the **Win8-Master (PVS)** virtual machine.

Creating the Provisioning Services Target Devices

Within the Provisioning Services Console you can manually create target devices or you can configure Provisioning Services to automatically add a target device, allowing unknown devices to self-register within the Provisioning Services farm.

To Create the Provisioning Services Target Devices

1. Log on to a virtual machine that has the Provisioning Services Console installed using domain administrator credentials.

   Start the **StudentManagementConsole-1** virtual machine and log on using the **CCH\Admin1** and **Password1** credentials.

2. Click the **Provisioning Services Console** icon on the Start screen and then click **Connect**.

If this is the first time the user has opened the Provisioning Services Console on a system, you must specify the NetBIOS name of the Provisioning Services server in the Name field and then click **Connect** to connect to the server.

3. Browse to the **Device Collections** node in the Provisioning Services Console.

   Double-click **CCH (PVS-1)** > **Sites** > **Miami** > **Device Collections**.

4. Configure the target device to start from the vDisk.

   a. Click the **Windows 8** collection.
   b. Right-click the **Windows8-Master** target device in the right pane and then click **Properties**.
   c. Select the **General** tab, select **vDisk** in the Boot from field, and then click **OK**.

If the Boot from field does not appear, ensure that you selected the target device in the right pane in Step 4.b and not the collection in the left pane.

5. Select the **vDisk Pool** node and then change the properties of the vDisk to **Standard Image** access mode.

   a. Select the **vDisk Pool** node in the left pane of the Provisioning Services Console.
   b. Right-click the **Windows8** vDisk in the right pane and then click **Properties**.
   c. Select **Standard Image (multi-device, read-only access)** in the Access mode field. and then click **OK**.

6. Select the device collection, right-click the target device, and then click **Auto-Add Wizard**.

   Select the **Device Collections** > **Windows8** node, right-click the **Windows8-Master** target device in the right pane, and then click **Auto-Add Wizard.**

7. Click **Next** on the Welcome screen.
8. Select **Enable auto-add** and then click **Next**.
9. Select the site in the Site field and then click **Next**.

   Select **Miami** in the Site field and then click **Next**.

10. Select the collection that you want to add the new devices to and then click **Next**.

    Select **Windows8** in the Collection field and then click **Next**.

11. Select the template that will be used to provide the newly added target devices with their properties and then click **Next**.

Select **Windows8-Master** in the Template field and then click **Next**.

12. Specify a naming scheme to use for the new devices and then click **Next**.

a. Type **Windows8-** in the Prefix field.
b. Select **3** in the Length field.
c. Select **Zero fill**.
d. Click **Next**.

13. Click **Finish**.
14. Create a diskless virtual machine in XenCenter and set it to boot from the network.

a. Click **New VM** in XenCenter, select the **Windows 7 (64-bit)** and then click **Next**.
b. Type **Windows 8 (PVS)** in the Name field and then click **Next**.
c. Select **Boot from network** and then click **Next**.
d. Click **Next**, type **2048** into the Memory field and then click **Next**.
e. Click **Next** to use the defaults for Storage.
f. Click **Next** to use the defaults for Networking.
g. Deselect **Start the new VM automatically** and then click **Finish**.

If your version of XenCenter has a built-in Windows 8 template, this may be used instead of the Windows 7 template.

15. Convert the virtual machine into a template.

Right-click **Windows 8 (PVS)** in XenCenter, click **Convert to Template** and then click **Convert**.

16. Create new virtual machines from the newly created template.

a. Right-click **Windows 8 (PVS)** in XenCenter and then click **Quick Create** to create a new virtual machine named Windows 8 (PVS) (1).
b. Right-click **Windows 8 (PVS)** in XenCenter and then click **Quick Create** to create a new virtual machine named Windows 8 (PVS) (2).
c. Right-click **Windows 8 (PVS)** in XenCenter and then click **Quick Create** to create a new virtual machine named Windows 8 (PVS) (3).

17. Verify that each of the virtual machines starts properly using Provisioning Services.

    a. Select **Windows 8 (PVS) (1)** in XenCenter and click **Console**.
    b. Verify that the virtual machine starts and that Start screen is displayed.
    c. Select **Windows 8 (PVS) (2)** in XenCenter and click **Console**.
    d. Verify that the virtual machine starts and that Start screen is displayed.
    e. Select **Windows 8 (PVS) (3)** in XenCenter and click **Console**.
    f. Verify that the virtual machine starts and that Start screen is displayed.

18. Click **Action** > **Refresh** in the Provisioning Services Console.
19. Verify that the new virtual machines have been added to the device collection as target devices.

    Click the **Windows 8** device collection and verify that **Windows8-001**, **Windows8-002**, and **Windows8-003** appear.

20. Create Active Directory accounts for each new machine.

    a. Click the **Windows8** device collection node in the Provisioning Services Console.
    b. Press and hold the **Shift** key and then select the **Windows8-001**, **Windows8-002**, and **Windows8-003** devices.
    c. Right-click **Windows8-001** and then click **Active Directory > Create Machine Account**.
    d. Select **CCH Virtual Desktops/Desktops** from the Organization unit menu and then click **Create Account**.
    e. Click **Close**.

Discussion Question

What is the purpose of the Master Target Device and the target device within Provisioning Services?

To Create a New Machine Catalog

1. Log on to a virtual machine hosting Citrix Studio using domain administrator credentials.

   Log on to **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Right-click **Machine Catalogs** in the left pane and then click **Create Machine Catalog**.
3. Click **Next** in the Getting Started screen.
4. Determine what type of resource you want to create and then click **Next**.

   Select **Windows Desktop OS** in the Operating System and Hardware screen and click **Next**.

5. Determine the type of infrastructure that will be used.

Select **Virtual machines**.

6. Select **Provisioning Services (PVS)** as the image management technology and then click **Next**.
7. Specify whether end users will be provided with a random desktop or a static desktop.

   Select **I want users to connect to a random desktop each time they log on** and then click **Next**.

8. Type the IP address or NetBIOS name of the Provisioning Services server into the Provisioning Services server address field and then click **Connect**.

   Type **PVS-1** and then click **Connect**.

9. Select the collection that houses the target devices and then click **Next**.

   Double-click **Miami**, select **Windows 8** and then click **Next**.

10. Specify the scope and then click **Next**.

    Verify that **All** is selected and then click **Next**.

11. Specify a name for the catalog and then click **Finish**.

    Type **Windows 8 PVS** in the machine catalog name field and then click **Finish**.

To Assign a Machine Catalog to a Delivery Group

1. Log on to the virtual machine hosting Citrix Studio using domain administrator credentials.

   Log on to **StudentManagementConsole-1** virtual machine using the **CCH\Admin1** and **Password1** credentials.

2. Select **Delivery Groups** in the left pane and then click **Create Delivery Group** in the right pane.

If the Create Delivery Group option is not available, make sure the Delivery Group tab is selected in the center pane.

3. Click **Next** in the Getting Started screen.
4. Select a machine catalog, determine the number of machines in the catalog that is Delivery Group will consume, and then click **Next**.

   Select **Windows 8 PVS**, type **3** in the number of machines to add field, and then click **Next**.

5. Select the resource to deliver in the Delivery Type screen and then click **Next**.

   Select **Desktops** and then click **Next**.

The choices include:

- **Desktops:** Allows you to provide end users with a desktop.
- **Applications:** Allows you to publish applications found on the master image, applications provided on an App-V server, or applications located on other network locations. You can also edit the properties of those applications.
- **Desktops and Applications:** Provides a combination of the previous two choices. This choice is only available for Server OS operating systems.

6. Click the **Add users** button to specify which end users can access the desktops.
7. Type the name of the end user or group, click **Check Names** and then click **OK**.

   Type **CCH\Domain Users** in the Enter the object names to select field, click **Check Names** and then click **OK**.

8. Verify that the appropriate end users and groups appear in the Assign users field and then click **Next**.

   Verify that **CCH\Domain Users** appears and then click **Next**.

9. Determine how Receiver will be configured on the machines and click **Next**.

   Select **Manually, using a StoreFront server address that I will provide later** and then click **Next**.

10. Type a name for the Delivery Group that administrators will see in the Delivery Group name field.

    Type **Windows 8 for All Users**.

11. Type a name for the Delivery Group that end users will see in the Display name field.

    Type **Windows 8**.

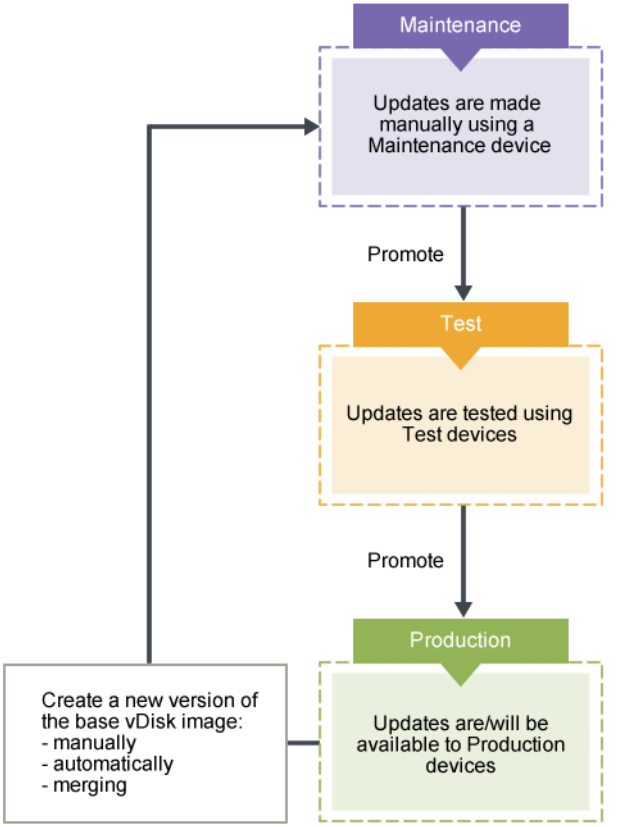
12. Click **Finish**.

Discussion Question

Upon assigning machine catalogs to a Delivery Group, users of the Delivery Group are unable to access their desktops or applications. What can be the cause of this issue?

Updating vDisks

A vDisk update allows you to deliver new versions of a vDisk to all branch offices without creating and imaging an entirely new vDisk. Another advantage or performing a vDisk update rather than creating a new vDisk is that target devices do not need to be reconfigured to use a new vDisk. A vDisk update can be used to add or remove third-party software applications or files to or from a vDisk. Enabling vDisk updates requires configuring settings in the properties of both the server and the vDisk.



To Update a vDisk

1. Log on to a virtual machine that has the Provisioning Services Console installed using domain administrator credentials.

   Start the **StudentManagementConsole-1** virtual machine and then log on using the **CCH\Admin1** and **Password1** credentials.

2. Click the **Provisioning Services Console** icon on the Start screen and then click **Connect**.

If this is the first time the user has opened the Provisioning Services Console on a system, you must specify the NetBIOS name of the Provisioning Services server in the Name field and then click **Connect** to connect to the server.

3. Browse to a site in the Provisioning Services Console.

   Double-click **CCH (PVS-1)** > **Sites** > **Miami**.

4. Click the **vDisk Pool** node, right-click a vDisk in the right pane, and then click **Versions**.

   Click **vDisk Pool**, right-click **Windows8** in the right pane, and then click **Versions**

5. Click **New** and then click **Done**.
6. Click the **Device Collections** node and then click on the device collection that contains a device that uses the targeted vDisk.

   Click **Device Collections** > **Windows 8**.

7. Right-click a target device and then click **Properties**.

   Right-click **Windows8-001** and then click **Properties**.

8. Select **Maintenance** in the Type field and then click **OK**.
9. Right-click the virtual machine associated with the target device that you put in Maintenance mode and then start or restart the virtual machine.

   Right-click the **Windows 8 (PVS) (1)** virtual machine in XenCenter and then select **Reboot**.

10. Wait while the virtual machine restarts and then select the target device that you put in Maintenance mode from the Boot Menu in the console of the virtual machine.

    Type **1** in the console of the Windows 8 (PVS) (1) virtual machine and then press **Enter**.

11. Make the desired changes to the virtual machine.

    Perform the following changes to the virtual machine:

    a. Log on to the **Windows 8 (PVS) (1)** virtual machine using the **CCH\Admin1** and **Password1** credentials.
    b. Type **\\DC-1\Share** in the Start screen and then press **Enter**.
    c. Double-click **Firefox Setup** and then click **Run**.
    d. Ensure that **Standard** is selected and click **Next**.
    e. Click **Install** and then allow the installation to complete.
    f. Deselect **Launch Firefox now** and click **Finish**.

12. Right-click the virtual machine in XenCenter, click **Shut Down** and then click **Yes** in the Shut Down virtual machine message.

    Right-click the **Windows 8 (PVS) (1)** virtual machine in XenCenter, click **Shut Down**, and then click **Yes** in the Shut Down virtual machine message.

Promoting Updated Versions

An updated version of the vDisk is not available to production devices until it is promoted to production. The updated promotion stages include maintenance, test, and production. Each time a new version is created, the Access setting is automatically set to maintenance to allow maintenance devices to make updates. After updates are complete, this version can be promoted from maintenance to test to allow for testing by test devices, or directly to production, for use by all target devices.

To Promote Updated vDisk Versions

1. Log on to a virtual machine that has the Provisioning Services Console installed using domain administrator credentials.

   Start the **StudentManagementConsole-1** virtual machine and then log on using the **CCH\Admin1** and **Password1** credentials.

2. Click the **Provisioning Services Console** icon on the Start screen and then click **Connect**.
3. Click the **vDisk Pool** node, right-click a vDisk in the right pane, and then click **Versions**.

   Click **vDisk Pool**, right-click **Windows8** in the right pane, and then click **Versions**

4. Select the latest version of the vDisk and then click **Promote** to promote the updated version of the vDisk.

   Select version **1** and then click **Promote**.

5. Select the version access and availability time frame and then click **OK**.

   Select **Production**, select **Immediate**, and then click **OK**.

6. Start or restart a target device

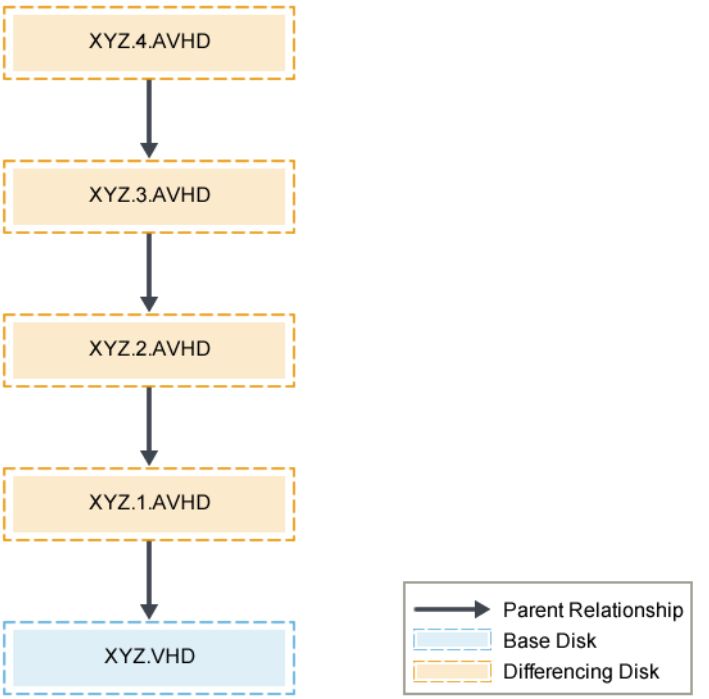
Restart the **Windows 8 (PVS) (2)** virtual machine, log on as the **CCH\Admin1** user, and ensure that Firefox is now present.

Discussion Question

What are the benefits of updating and merging a vDisk over traditional re-creation of images?

VHD Chain of Differencing Disks

A vDisk consists of a VHD base image file, any associated files, and if applicable, a chain of referenced VHD differencing disks. Differencing disks are created to capture the changes made to the base disk image, leaving the original base disk unchanged. Each differencing disk that is associated with a base disk represents a different version.



vDisk versions are created and managed using the vDisk versions dialog box and by performing vDisk versioning tasks. Each time a vDisk is put into maintenance mode a new version of the VHD differencing disk is created and the file name is numerically incremented.

Merging VHD Differencing Disks

Merging VHD differencing disk files can save disk space and increase performance, depending on the merge method selected. Merge methods include merging to a new base image or merging to a consolidated differencing disk.

A merge can only occur when no Maintenance version exists for this vDisk or when the vDisk is in Private Image mode. A merge starts from the top of the chain down to a base disk. A starting disk cannot be specified for the merge.

Merging to a new base image is recommended when performance is more important than disk space, because a new base disk is created for every merge performed.

Merging to a consolidated differencing disk is recommended when disk storage is limited or when the bandwidth between remote locations is limited, which makes copying large images impractical.

To Merge VHD Differencing Disks

1. Log on to a virtual machine that has the Provisioning Services Console installed using domain administrator credentials.

   Start the **StudentManagementConsole-1** virtual machine and then log on using the **CCH\Admin1** and **Password1** credentials.

2. Click the **Provisioning Services Console** icon on the Start screen and then click **Connect**.
3. Click the **vDisk Pool** node, right-click a vDisk in the right pane, and then click **Versions**.

   Click **vDisk Pool**, right-click **Windows8** in the right pane, and then click **Versions**.

4. Click **Merge** to open the Merge window.
5. Select the type of merge version you want to create and the merge version access type.

   Select **Merged Base** and then select **Maintenance**.

6. Click **OK** to begin the merge process.

Troubleshooting: Provisioning Services

Issue	Resolution
Streamed Services stops running.	Set the service to automatically restart on failure.
End-user machine is not receiving an IP address (DCHP issues).	Verify that DHCP is accessible on the subnet. Ensure that the client device is BIOS is configured to start from the network. You need to adjust the BIOS device startup order for the virtual machine. It is hypervisor-specific.
Machine cannot obtain ARDBP32.bin.	Ensure the settings in DHCP (67) are pointing to the correct file. Verify that the boot file is present on the PVS machine. Ensure that the TFTP service running to point to the relevant boot file.
When starting up a target device using Boot Device Manager (BDM), the static address assigned in the boot file is not what is reflected when the target device fully starts.	Place the target device in Private image mode and change the network adapter to use any statically assigned IP address. Avoid using DHCP unless it is preferred, in which case you must specify DHCP in the BDM file when running the BDM wizard.  For more information about BDM, see Citrix article CTX125066 at *http://support.citrix.com.*
After updating a Provisioning Services vDisk that has Personal vDisk enabled, a blue screen of death (BSOD) appears with a STOP error indicating a corrupt file.	There are corrupt files or directories on the Personal vDisk. Detaching the personal vDisk from the virtual machine allows it to start.  For more information about this error, see Citrix article CTX138150 at *http://support.citrix.com.*

Reinforcement Exercise: Provisioning Services

During this exercise, you will not be given step-by-step instructions for performing the task. Instead, you are asked to use what you have just learned to complete it. This exercise is designed to take your newly-acquired knowledge and determine if you can perform a task you have never done before. In most instances the default value will be the best choice, but we encourage you to explore and try things out. If you have a question or need help, ask the instructor or a fellow student for assistance.

In this module, you learned how to:

- Describe the differences between Machine Creation Services and Provisioning Services.
- Describe the basic architecture and communication flow of Provisioning Services.
- Manage vDisks and target devices for a Provisioning Services implementation.
- Manage vDisk updates.

Time to complete: Approximately 90 minutes

You already have a Provisioning Services host installed. Using the Provisioning Services host, you have been asked to complete the following tasks:

- Create a new Master virtual machine of Windows 2012 for use on Provisioning Services using the Win2012_template.
  - Install the VDA and PVS tools.
  - Join the virtual machine to the domain.
  - Install Firefox from the \\dc-1\Share.
- Create a new 20 GB vDisk in the vDisk pool for Windows 2012.
- Create a new Device collection for Windows 2012.
- Use the Imaging Tools to copy the master onto a vDisk.
- Create two new virtual machines that start from this vDisk.
- Create a new machine catalog with two virtual machines.
  - Name the machine catalog "Windows 2012 (PVS)".
- Create a new Delivery Group named "Hosted Firefox".
  - Publish Firefox to CCH\Domain Users.

851 West Cypress Creek Road Fort Lauderdale, FL 33309 USA (954) 267 3000 www.citrix.com

Rheinweg 9 8200 Schaffhausen Switzerland +41 (0) 52 63577 00 www.citrix.com