

OFFICIAL MICROSOFT LEARNING PRODUCT

6425B

**Lab Instructions and Answer Key:
Configuring and Troubleshooting
Windows Server® 2008 Active
Directory® Domain Services**

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The names of manufacturers, products, or URLs are provided for informational purposes only and Microsoft makes no representations and warranties, either expressed, implied, or statutory, regarding these manufacturers or the use of the products with any Microsoft technologies. The inclusion of a manufacturer or product does not imply endorsement of Microsoft of the manufacturer or product. Links may be provided to third party sites. Such sites are not under the control of Microsoft and Microsoft is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. Microsoft is not responsible for webcasting or any other form of transmission received from any linked site. Microsoft is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of Microsoft of the site or the products contained therein.

© 2009 Microsoft Corporation. All rights reserved.

Microsoft, Microsoft Press, Access, Active Directory, ActiveX, Convergence, Excel, Forefront, Hyper-V, Internet Explorer, MS, MSDN, MS-DOS, Outlook, PowerPoint, Segoe, SharePoint, SQL Server, Visio, Visual Basic, Visual Studio, Windows, Windows Live, Windows Mobile, Windows NT, Windows PowerShell, Windows Server and Windows Vista. are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.

Product Number: 6425B

Part Number: X16-23526

Released: 11/2009

Module 1

Lab Instructions: Introducing Active Directory Domain Services (AD DS)

Contents:

Exercise 1: Perform Post-Installation Configuration Tasks	3
Exercise 2: Install a New Windows Server 2008 Forest with the Windows Interface	6

Lab: Install an AD DS DC to Create a Single Domain Forest

- Exercise 1: Perform Post-Installation Configuration Tasks
- Exercise 2: Install a New Windows Server 2008 Forest with the Windows Interface

Logon information

Virtual machine	6425B-HQDC01-D
Logon user name	Administrator
Password	Pa\$\$w0rd

Estimated time: 15 minutes

Scenario

You have been hired to improve identity and access at Contoso, Ltd. The company currently has one server in a workgroup configuration. Employees connect to the server from their personal client computers. In anticipation of near-term growth, you have been tasked with improving the manageability and security of the company's resources. You decide to implement an AD DS domain and forest by promoting the server to a domain controller. You have just finished installing Windows Server 2008 from the installation DVD.

Exercise 1: Perform Post-Installation Configuration Tasks

In this exercise, you will prepare the server by performing post-installation configuration tasks.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Configure the display resolution.
3. Configure the time zone.
4. Change IP configuration.
5. Rename the server HQDC01.
6. Restart the server.

► Task 1: Prepare for the lab

- Start 6425B-HQDC01-D.
- Log on with username **Administrator** and password **Pa\$\$w0rd** (where the 0 is a zero).

► Task 2: Configure the display resolution

- Configure the display resolution to **1024 by 768**.

► Task 3: Configure the time zone

- Using the Initial Configuration Tasks window, change the time zone so that it is appropriate for your location.

► **Task 4: Change IP configuration**

- Using the Initial Configuration Tasks window, change the IP (IPv4) configuration to the following:
 - IP Address: **10.0.0.11**
 - Subnet Mask: **255.255.255.0**
 - Default Gateway: **10.0.0.1**
 - Preferred DNS Server: **10.0.0.11**

► **Task 5: Rename the server HQDC01**

- Using the Initial Configuration Tasks window, rename the server to **HQDC01**. Do not restart the server.

► **Task 6: Restart the server**

1. In the Initial Configuration Tasks window, note the **Add roles** and **Add features** links.

In the next exercise, you will use Server Manager to add roles and features to HQDC01. These links are another way to perform the same tasks.

By default, the Initial Configuration Tasks window will appear each time you log on to the server.

2. Select the **Do not show this window at logon** check box to prevent the window from appearing.

If you need to open the Initial Configuration Tasks window in the future, you do so by running the **Oobe.exe** command.

3. Click the **Close** button at the bottom of the window.

Server Manager appears.

Server Manager enables you to configure and administer the roles and features of a server running Windows Server 2008. You will use Server Manager in the next exercise.

At the bottom of the Server Manager window, a status message informs you, *Console cannot refresh until computer is restarted.*

4. Click the **Restart** link next to the status message.
You are prompted with the message *Do you want to restart now?*.
5. Click **Yes**.
The computer restarts.

Results: After this exercise, you will have a server named HQDC01 in the correct time zone, with display resolution of at least 1024 x 768, and with the IP configuration specified in Task 4.

Exercise 2: Install a New Windows Server 2008 Forest with the Windows Interface

Now that you have prepared the server with an appropriate name and IP configuration, you are ready to configure HQDC01 as a domain controller. In this exercise, you will add the AD DS role and create the forest and domain by promoting HQDC01 to be the first domain controller in the contoso.com forest.

The main tasks for this exercise are as follows:

1. Add the Active Directory Domain Services role to HQDC01.
2. Configure a new Windows Server 2008 forest named *contoso.com* with HQDC01 as the first domain controller.
3. Examine the default configuration of the contoso.com forest and domain.
4. Shut down the virtual machine.

► Task 1: Add the Active Directory Domain Services role to HQDC01

1. Log on to HQDC01 as **Administrator** with the password **Pa\$\$w0rd**.
2. Using Server Manager, add the role, **Active Directory Domain Services**. Accept all defaults.

► Task 2: Configure a new Windows Server 2008 forest named *contoso.com* with HQDC01 as the first domain controller

1. In Server Manager, expand the **Roles** node in the tree pane, and then select **Active Directory Domain Services**.
2. Click the **Run the Active Directory Domain Services Installation Wizard (dcpromo.exe)** link.

The Active Directory Domain Services Installation Wizard appears.

3. Click **Next**.
4. On the **Operating System Compatibility** page, review the warning about the default security settings for Windows Server 2008 domain controllers, and then click **Next**.
5. On the **Choose a Deployment Configuration** page, select **Create a new domain in a new forest**, and then click **Next**.

6. On the **Name the Forest Root Domain** page, type **contoso.com**, and then click **Next**.

The system performs a check to ensure that the DNS and NetBIOS names are not already in use on the network.

7. On the **Set Forest Functional Level** page, choose **Windows Server 2008**, and then click **Next**.

The Additional Domain Controller Options page appears.

Each of the functional levels is described in the Details box on the page. Choosing Windows Server 2008 forest functional level ensures that all domains in the forest operate at the Windows Server 2008 domain functional level, which enables several new features provided by Windows Server 2008.

In a production environment, you would choose Windows Server 2008 forest functional level when creating a new forest if you require the features provided by the Windows Server 2008 domain functional level and if you will not be adding any domain controllers running operating systems prior to Windows Server 2008.

DNS Server is selected by default. The Active Directory Domain Services Installation Wizard will create a DNS infrastructure during AD DS installation.

The first domain controller in a forest must be a global catalog server and cannot be a read-only domain controller (RODC).

8. Click **Next**.

A Static IP assignment warning appears.

Because discussion of IPv6 is beyond the scope of this training kit, you did not assign a static IPv6 address to the server in Exercise 2. You did assign a static IPv4 address in Exercise 1, and other labs in this course will use IPv4. You can therefore ignore this error in the context of the exercise.

9. Click **Yes, the computer will use a dynamically assigned IP address (not recommended)**.

A warning appears that informs you that a delegation for the DNS server cannot be created.

In the context of this exercise, you can ignore this error. Delegations of DNS domains will be discussed later in this course.

10. Click **Yes** to close the Active Directory Domain Services Installation Wizard warning message.

11. On the **Location for Database, Log Files, and SYSVOL** page, accept the default locations for the database file, the directory service log files, and the SYSVOL files, and then click **Next**.

The best practice in a production environment is to store these files on three separate volumes that do not contain applications or other files not related to AD DS. This best practice design improves performance and increases the efficiency of backup and restore.

12. On the **Directory Services Restore Mode Administrator Password** page, type **Pa\$\$w0rd** in both the **Password** and **Confirmed Password** boxes. Click **Next**.

In a production environment, you should use a very strong password for the Directory Services Restore Mode Administrator Password. Do not forget the password you assign to the Directory Services Restore Mode Administrator.

13. On the **Summary** page, review your selections.

If any settings are incorrect, click **Back** to make modifications.

14. Click **Next**.

Configuration of AD DS begins. After several minutes of configuration, the Completing the Active Directory Domain Services Installation Wizard page appears.

15. Click **Finish**.

16. Click **Restart Now**.

The computer restarts.

17. Continue with Task 3 (optional) or skip to Task 4.

► **Task 3: Examine the default configuration of the contoso.com forest and domain (OPTIONAL)**

1. Log on to HQDC01 as **Administrator** with the password **Pa\$\$w0rd**.
The Windows desktop appears and, after a moment, Server Manager opens.
2. Expand the **Roles** node in the tree pane, and expand the **Active Directory Domain Services** node.
3. Expand **Active Directory Users and Computers** and the **contoso.com** domain node.

4. Select the **Users** container in the tree.

The users and groups you see are available to any computer in the domain. For example, the domain's Administrator account can be used to log on to any computer in the domain, by default, and the Domain Users group is a member of the local Users group on each computer in the domain.

5. Select the **Builtin** container in the tree.

The groups you see are shared by and available to domain controllers, but not to member servers or workstations. For example, members of the Backup Operators group can perform backup and restore tasks on domain controllers only, and the Administrators group in the Builtin container represents the administrators of all domain controllers.

6. Select the **Computers** container in the tree.

It is empty. This is the default container for member servers and workstations.

7. Select the **Domain Controllers** organizational unit (OU) in the tree.

This is the OU into which domain controllers are placed. The computer object for HQDC01 appears in this OU.

► Task 4: Shut down the virtual machine

1. If you are not already logged on to HQDC01, log on to HQDC01 as **Administrator** with the password **Pa\$\$w0rd**.
2. Shut down HQDC01 and do not save any changes you made while doing this lab exercise.

Results: After this exercise, you will have a single-domain forest named contoso.com with a single domain controller named HQDC01.

Lab Review

After this lab you will have:

- Performed post installation tasks in naming a server HQDC01, configuring the correct time zone, with display resolution of at least 1024 x 768 and specifying its IP address information.
- Configured a single-domain forest named contoso.com with a single domain controller named HQDC01.

Module 2

Lab Instructions: Secure and Efficient Administration of Active Directory

Contents:

Lab A: Create and Run a Custom Administrative Console

Exercise 1: Perform Basic Administrative Tasks Using the Active Directory Users and Computers Snap-in 3

Exercise 2: Create a Custom Active Directory Administrative Console 5

Exercise 3: Perform Administrative Tasks with Least Privilege, Run As Administrator, and User Account Control 7

Exercise 4 (Advanced Optional): Advanced MMC Customization and Remote Administration 11

Lab B: Find Objects in Active Directory

Exercise 1: Find Objects in Active Directory 14

Exercise 2: Use Saved Queries 19

Exercise 3 (Advanced Optional): Explore Saved Queries 21

Lab C: Use DS Commands to Administer Active Directory

Exercise 1: Use DS Commands to Administer Active Directory 23

Lab A: Create and Run a Custom Administrative Console

- Exercise 1: Perform Basic Administrative Tasks Using the Active Directory Users and Computers Snap-in
- Exercise 2: Create a Custom Active Directory Administrative Console
- Exercise 3: Perform Administrative Tasks with Least Privilege, Run As Administrator, and User Account Control
- Exercise 4 (Advanced Optional): Advanced MMC Customization and Remote Administration

Logon information

Virtual machine	6425B-HQDC01-A
Logon user name	Pat.Coleman
Administrative user name	Pat.Coleman_Admin
Password	Pa\$\$w0rd

Estimated time: 20 minutes

Scenario

In this exercise, you are Pat Coleman, an Active Directory administrator at Contoso, Ltd. You are responsible for a variety of Active Directory support tasks, and you have found yourself constantly opening multiple consoles from the Administrative Tools folder in Control Panel. You have decided to build a single console that contains all of the snap-ins you require to do your work. Additionally, Contoso's IT security policy is changing, and you will no longer be permitted to log on to a system with credentials that have administrative privileges, unless there is an emergency. Instead, you are required to log on with nonprivileged credentials.

Exercise 1: Perform Basic Administrative Tasks Using the Active Directory Users and Computers Snap-in

In this exercise, you will perform basic administrative tasks in the Active Directory Users and Computers snap-in.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. View objects.
3. Refresh the view.
4. Create objects.
5. Configure object attributes.
6. View all object attributes.

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
Pat.Coleman_Admin is a member of Domain Admins.
Server Manager opens automatically.
3. Close Server Manager.
4. Open **D:\Labfiles\Lab02a**.
5. Right-click **Lab02a_Setup.bat**, and then click **Run as administrator**.
A User Account Control dialog box appears.
6. Click **Continue**.
7. The lab setup script runs. When it is complete, press any key to continue.
8. Close the Windows Explorer window, **Lab02a**.

► **Task 2: View objects**

1. Open **Active Directory Users and Computers** from the **Administrative Tools** folder.
2. Look at the objects in the **Employees** organizational unit (OU) inside the **User Accounts** OU.

► **Task 3: Refresh the view**

- Refresh the view of the **Employees** OU.

► **Task 4: Create objects**

- Create a new OU in the root of the domain called **6425B**.

► **Task 5: Configure object attributes**

1. Open the properties of the **Pat Coleman** user object in the **Employees** OU.
2. Change the **Office** attribute on the **General** tab to **Redmond**.

► **Task 6: View all object attributes**

1. Confirm that the **Attribute Editor** tab is not visible in the **Properties** dialog box of **Pat Coleman**, and that there is no input control for the **division** property on any of the tabs.
2. Turn on the view of **Advanced Features** for the Active Directory Users and Computers snap-in.
3. View the **Attribute Editor** for **Pat Coleman**.
4. Change Pat Coleman's **division** attribute to **6425B**.
5. Close Active Directory Users and Computers.

Results: After this exercise, you will have experienced the fundamentals of administration using the Active Directory Users and Computers snap-in.

Exercise 2: Create a Custom Active Directory Administrative Console

In this exercise, you will create a single, custom administrative console that contains all of the snap-ins you need to do your work.

The main tasks for this exercise are as follows:

1. Create a custom MMC console with the Active Directory Users and Computers snap-in.
2. Add other Active Directory snap-ins to the console.
3. Add the Active Directory Schema snap-in to a custom MMC console.
4. Manage snap-ins in a custom MMC console (optional).

► Task 1: Create a custom MMC console with the Active Directory Users and Computers snap-in

1. Launch an empty MMC console and maximize it.
2. Add the **Active Directory Users and Computers** snap-in.
3. Save the console. Create a new folder called **C:\AdminTools** and save the console in that folder as **MyConsole.msc**.

► Task 2: Add other Active Directory snap-ins to the console

1. Add the **Active Directory Sites and Services** and **Active Directory Domains and Trusts** snap-ins list to your console.
2. Rename the console root **Active Directory Administrative Tools**.
3. Save the console.

► **Task 3: Add the Active Directory Schema snap-in to a custom MMC console**

1. Confirm that Active Directory Schema is not listed as an available snap-in in the **Add or Remove Snap-ins** dialog box.

The Active Directory Schema snap-in is installed with the Active Directory Domain Services role, and with the RSAT, but it is not registered, so it does not appear.

2. In the **Start** menu, right-click **Command Prompt**, and then click **Run as administrator**.

3. In the command prompt, type the command **regsvr32.exe schmmgmt.dll**.

This command registers the dynamic link library (DLL) for the Active Directory Schema snap-in. This is necessary to do one time on a system before you can add the snap-in to a console.

4. Close the Command Prompt window.
5. Add the **Active Directory Schema** snap-in to the console.
6. Save the console.

► **Task 4: (Optional): Manage snap-ins in a custom MMC console**

- Open the **Add or Remove Snap-ins** dialog box and use the **Move Up**, **Move Down**, and **Remove** buttons to rearrange your console. For future Labs, you will need the console in the condition it was in at the end of Task 3, so *do not* save your changed console. Instead, close the console without saving changes.

Results: After this exercise, you will have a custom MMC console with the Active Directory Users and Computers, Active Directory Sites and Services, Active Directory Domains and Trusts, and Active Directory Schema snap-ins.

Exercise 3: Perform Administrative Tasks with Least Privilege, Run As Administrator, and User Account Control

In this exercise, you will perform administrative tasks while logged on with standard user credentials.

The main tasks for this exercise are as follows:

1. Log on with credentials that do not have administrative privileges.
2. Run Server Manager as an administrator.
3. Examine the credentials used by running processes.
4. Run the command prompt as an administrator.
5. Run Administrative Tools as an administrator.
6. Run a custom administrative console as an administrator.

► **Task 1: Log on with credentials that do not have administrative privileges**

1. Log off of HQDC01.
2. Log on to HQDC01 as **Pat.Coleman** with the password, **Pa\$\$w0rd**.
Pat.Coleman is a member of Domain Users and has no administrative privileges.

► **Task 2: Run Server Manager as an administrator**

1. Click the **Server Manager** icon in the **Quick Launch**, next to the **Start** button.

A User Account Control dialog box appears.

Because your user account is not a member of Administrators, the dialog box requires you to enter administrative credentials: a username and a password.

If you do not see the User Name and Password boxes, make sure that you are logged on as **Pat.Coleman** and *not* as **Pat.Coleman_Admin**.

2. In the **User name** box, type **Pat.Coleman_Admin**.
3. In the **Password** box, type **Pa\$\$w0rd** and press ENTER.

Server Manager opens.

► **Task 3: Examine the credentials used by running processes**

1. Right-click the taskbar and click **Task Manager**.
2. Click the **Processes** tab.
3. Click **Show processes from all users** and, in the **User Account Control** dialog box, authenticate as **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**

Task Manager can run without administrative credentials, but it will show only those processes running under the current user account. Therefore, the User Account Control dialog box includes an option to authenticate using the same credentials with which you are logged on: **Pat.Coleman**.

4. Click the **Processes** tab and sort by **User Name**.
5. Locate the processes being run as **Pat.Coleman** and **Pat.Coleman_Admin**.

Question: Which processes are running as **Pat.Coleman_Admin**? What applications do the processes represent?

► **Task 4: Run the command prompt as an administrator**

1. Click **Start**, then right-click **Command Prompt**, and then click **Run as administrator**.
2. In the **User Account Control** dialog box, authenticate as **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.

The Administrator: Command Prompt window appears.

3. Close the Command Prompt window.
4. Click **Start**, and in the **Start Search** box, type **cmd.exe**, and then press CTRL+SHIFT+ENTER.

In the Start Search box, the keyboard shortcut CTRL+SHIFT+ENTER runs the specified command as an administrator.

5. In the **User Account Control** dialog box, authenticate as **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.

The Administrator: Command Prompt window appears.

► **Task 5: Run administrative tools as an administrator**

1. Click the **Show Desktop** icon in the **Quick Launch**, next to the **Start** button.
2. Click **Start**, then point to **Administrative Tools**, then right-click **Active Directory Users and Computers**, and then click **Run as administrator**.
3. In the **User Account Control** dialog box, authenticate as **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.

► **Task 6: Run a custom administrative console as an administrator**

You are beginning to see that it can become tedious to run as an administrator each and every administrative tool that you require. One advantage of a custom administrative console is that you can launch the console, containing multiple snap-ins, with a single Run As Administrator command.

1. Close all open windows on your desktop.
2. Run **C:\AdminTools\MyConsole** with administrative credentials. In the **User Account Control** dialog box, authenticate as **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
3. Log off of HQDC01. Do not shut down or reset the virtual machine.

Results: After this exercise, you will have learned that by having a single, custom administrative console, you make it easier for yourself to work securely. You can log on to your computer with user (nonadministrative) credentials and run that single console as an administrator..

Exercise 4 (Advanced Optional): Advanced MMC Customization and Remote Administration

Advanced Optional exercises provide additional challenges for students who are able to complete lab exercises quickly. There are no answers in the Lab Answer Key.

The main tasks for this exercise are as follows:

1. Start SERVER01-A.
2. Start DESKTOP101-A.
3. Use the procedures described in this lesson to further customize your MMC console (C:\AdminTools\MyConsole.msc). Add a snap-in that provides administrative access to the Data share on SERVER01 (\\SERVER01\Data).
4. Using the procedures described in this lesson, create an Administrators Launch Pad with a task that opens the Command Prompt.
5. Add a task to the Administrators Launch Pad that allows you to shut down a computer remotely. There are no procedures listed for this task: You are on your own! Tip: Shutdown.exe.
6. Copy your console to D:\AdminTools. The D:\AdminTools folder is shared as \\HQDC01\AdminTools.
7. Log on to DESKTOP101 as Pat.Coleman with the password Pa\$\$w0rd, and create a shortcut to \\HQDC01\AdminTools\MyConsole.msc.
8. Configure the properties of the shortcut so that it always prompts for administrative credentials. There are no procedures listed for this task: You are on your own!
9. Run your custom console as an administrator.
10. Log off of DESKTOP101 and HQDC01. Do not shut down or reset the virtual machines.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in the Lab B.

Lab Review Questions

Question: Which snap-in are you most likely to use on a day-to-day basis to administer Active Directory?

Question: When you build a custom MMC console for administration in your enterprise, what snap-ins will you add?

Lab B: Find Objects in Active Directory

- Exercise 1: Find Objects in Active Directory
- Exercise 2: Use Saved Queries
- Exercise 3 (Advanced Optional): Explore Saved Queries

Logon information

Virtual machine	6425B-HQDC01-A
Logon user name	Pat.Coleman
Administrative user name	Pat.Coleman_Admin
Password	Pa\$\$w0rd

Estimated time: 20 minutes

Scenario

Contoso now spans five geographic sites around the world, with over 1000 employees. As your domain has become populated with so many objects, it has become more difficult to locate objects by browsing. You are tasked with defining best practices for locating objects in Active Directory for the rest of the team of administrators. You are also asked to monitor the health of certain types of accounts.

Exercise 1: Find Objects in Active Directory

In this exercise, you will use several tools and interfaces that make it easier for you to find an object in Active Directory.

The main tasks for this exercise are as follows:

1. Explore the behavior of the Select dialog box.
2. Control the view of objects in the Active Directory Users and Computers snap-in.
3. Use the Find command.
4. Determine where an object is located.

► Task 1: Explore the behavior of the Select dialog box



Important Note: The steps in this task guide you through using several important Active Directory Users and Computers interfaces. You can think of this task as a "tour" of the interfaces and their features. The specific changes you are making are less important than the experience you gain with the nuances of these interfaces. **Follow the exact steps listed** and don't worry about *what* you are doing; instead **focus on how you are doing it** and how the user interfaces behave.

The virtual machine should already be started and available after completing Lab A. However, if it is not, you should launch it complete the exercises in Lab A before continuing.

1. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd** and run your custom console, **C:\AdminTools\MyConsole.msc** as an administrator with username **Pat.Coleman_Admin** and password **Pa\$\$w0rd**. Alternately, run the pre-created console, **D:\AdminTools\ADConsole.msc** as an administrator.
2. In the console tree, expand the **Active Directory Users and Computers** snap-in, the **contoso.com** domain, and the **User Accounts** OU, and then click the **Employees** OU.
3. Right-click **Pat Coleman** and then click **Properties**.
4. Click the **Member Of** tab.

5. Click **Add**.
6. In the **Select** dialog box, type the name **Special**.
7. Click **OK**. The name is resolved to **Special Project**.
8. Click **OK** again to close the **Properties** dialog box.
9. In the console tree, expand the **Groups** OU, and then click the **Role** OU.
10. In the details pane, right-click the **Special Project** group and then click **Properties**.
11. Click the **Members** tab.
12. Click **Add**.

The Select Users, Contacts, Computers, or Groups dialog box appears.

13. Type **linda;joan**, and then click the **Check Names** button.

The Select dialog box resolves the names to Linda Mitchell and Joanna Rybka and underlines the names to indicate visually that the names are resolved.

14. Click **OK**.
15. Click **Add**.
16. Type **carole**, and then click **OK**.

The Select dialog box resolves the name to Carole Poland and closes. You see Carole Poland on the Members list.

When you click the OK button, a “Check Names” operation is performed prior to closing the dialog box. It is not necessary to click the Check Names button unless you want to check names and remain in the Select dialog box.

17. Click **Add**.
18. Type **tony;jeff**, and then click **OK**.

Because there are multiple users matching “tony,” the Multiple Names Found box appears.

19. Click **Tony Krijnen** and click **OK**.

Because there are multiple users matching “jeff,” the Multiple Names Found box appears.

20. Click **Jeff Ford** and click **OK**. Click **OK** to close the **Special Project Properties** dialog box.

Whenever there is more than one object that matches the information you enter, the check names operation will give you the opportunity to choose the correct object.

21. In the console tree, click the **Application** OU under the **Groups** OU.
22. In the details pane, right-click the **APP_Office** group and then click **Properties**.
23. Click the **Members** tab.
24. Click **Add**.
25. In the **Select** dialog box, type **DESKTOP101**.
26. Click **Check Names**.

A Name Not Found dialog box appears, indicating that the object you specified could not be resolved.

27. Click **Cancel** to close the **Name Not Found** box.
28. In the **Select** box, click **Object Types**.
29. Select the check box next to **Computers** and click **OK**.
30. Click **Check Names**.

The name will resolve now that the Select box is including computers in its resolution.

31. Click **OK**.
32. Click **OK** to close the **APP_Office Properties** dialog box.

► **Task 2: Control the view of objects in the Active Directory Users and Computers snap-in**

1. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.
2. Click the **View** menu, and then click **Add/Remove Columns**.
3. In the **Available Columns** list, click **Last Name**.

4. Click the **Add** button.
5. In the **Displayed columns** list, click **Last Name** and click **Move Up** two times.
6. In the **Displayed columns** list, click **Type** and click **Remove**.
7. Click **OK**.
8. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.
9. In the details pane, click the **Last Name** column header to sort alphabetically by last name.
10. Click the **View** menu, and then click **Add/Remove Columns**.
11. In the **Available Columns** list, click **Pre-Windows 2000 Logon**.
12. Click the **Add** button.
13. In the **Displayed columns** list, click **Pre-Windows 2000 Logon** and click **Move Up**.
14. Click **OK**.
15. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.

► **Task 3: Use the Find command**

1. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.
2. Click the **Find** button in the toolbar.
3. In the **Name** box, type **Dan**, and then click **Find Now**.
4. How many items were found? Look at the status bar, at the bottom of the Find Users, Contacts, and Groups window.
5. Click the **In** drop-down list, and then click **Entire Directory**.
6. Click **Find Now**.

7. How many items were found? Look at the status bar, at the bottom of the Find Users, Contacts, and Groups window.
8. Close the **Find Users, Contacts, and Groups** dialog box.

► **Task 4: Determine where an object is located**

1. Turn on the view of **Advanced Features** for the **Active Directory Users and Computers** snap-in.
2. Use the **Find** command to locate users in domain whose names begin with **Pat.Coleman**. You should see two results.
3. Use the properties of **Pat Coleman (Admin)** to determine where the user is located in Active Directory.

Results: After this exercise, you will have learned that there are several interfaces with which you perform searches against Active Directory, and you know how to control the view in the Active Directory Users and Computers snap-in.

Exercise 2: Use Saved Queries

In this exercise, you will create saved queries, with which administrative tasks can be more efficiently performed.

The main tasks for this exercise are as follows:

1. Create a saved query that displays all domain user accounts.
2. Create a saved query that shows all user accounts with non-expiring passwords.
3. Transfer a query to another computer.

► Task 1: Create a saved query that displays all domain user accounts

- Create a saved query called **All User Objects** that shows all users in the domain.

► Task 2: Create a saved query that shows all user accounts with non-expiring passwords

- Create a saved query called **Non-Expiring Passwords** that shows all users in the domain whose passwords do not expire.

Note that, for the purposes of maintaining a simple, single password for all users in this course, *all* user accounts are configured so that passwords do not expire. In a production environment, user accounts should not be configured with non-expiring passwords.

► **Task 3: Transfer a query to another computer**

1. Export the **Non-Expiring Passwords** query to C:\AdminTools\Query_NonExpPW.xml.
2. Delete the **Non-Expiring Passwords** query.
3. Import the C:\AdminTools\Query_NonExpPW.xml query.
4. Log off of HQDC01.

Results: After this exercise, you will have two saved queries. One, **All User Objects**, demonstrates that a saved query can create a virtualized view of your domain, allowing you to see objects that meet a set of criteria, regardless of which OU those objects are in. The second query, **Non-Expiring Passwords**, demonstrates that you can use saved queries to monitor the health of your environment.

Exercise 3 (Advanced Optional): Explore Saved Queries

Advanced Optional exercises provide additional challenges for students who are able to complete lab exercises quickly. There are no answers in the Lab Answer Key.

The main tasks for this exercise are as follows:

1. Run the pre-created console, D:\AdminTools\ADConsole.msc as an administrator and explore the console.
2. Examine the queries used in the Saved Queries node of the Active Directory Users and Computers snap-in.

Notice that administrators using this tool will rarely, if ever, need to "dive in" to the organizational unit structure underneath the contoso.com domain in the console tree. Almost all day-to-day administrative tasks can be performed with the views in Saved Queries.



Note: Do not shut down the virtual machine once you are finished with this lab as the settings you have configured here will be used in the Lab C.

Lab Review Questions

Question: In your work, what scenarios require you to search Active Directory?

Question: What types of saved queries could you create to help you perform your administrative tasks more efficiently?

Lab C: Use DS Commands to Administer Active Directory

- Exercise 1: Use DS Commands to Administer Active Directory

Logon information

Virtual machine	6425B-HQDC01-A
Logon user name	Pat.Coleman
Administrative user name	Pat.Coleman_Admin
Password	Pa\$\$w0rd

Estimated time: 15 minutes

Scenario

Contoso is growing, and changes need to be made to objects in Active Directory. You are an administrator of AD DS, and you know that it can be easier to create, delete, and modify objects using the command prompt than using Active Directory Users and Computers.

Exercise 1: Use DS Commands to Administer Active Directory

In this exercise, you will use DS commands to perform basic administrative tasks. Some of these tasks would be difficult or impossible to perform in the user interface of Active Directory Users and Computers.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Find objects with DSQuery.
3. Retrieve object attributes with DSGet.
4. Pipe DNs from DSQuery to other DS commands.
5. Pipe DNs from DSGet to DSMod (advanced, optional).

Remember that you can always type the command, followed by a `/?`, for help with the command. When a command works with a particular type of object, type *command objectType /?* for even more help.

► Task 1: Prepare for the lab

The virtual machine should already be started and available after completing Labs A and B. However, if it is not, you should launch it and complete the exercises Labs A and B before continuing.

1. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
2. Open **D:\Labfiles\Lab02c**.
3. Run **Lab02c_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
4. The lab setup script runs. When it is complete, press any key to continue.
5. Close the Windows Explorer window, **Lab02c**.

► Task 2: Find objects with DSQuery

1. Open Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Use **DSQuery** to find all users whose last names are **Mitchell**.

► **Task 3: Retrieve object attributes with DSGet**

1. From the command prompt, get the e-mail address of **Tony Krijnen**.

The distinguished name of Tony's user account is:

cn=Tony Krijnen,ou=Employees,ou=User Accounts,dc=contoso,dc=com

2. From the command prompt, list the members of the **Finance Managers** group.

The distinguished name of the Finance Managers group is:

cn=Finance Managers,ou=Role,ou=Groups,dc=contoso,dc=com

► **Task 4: Pipe DNs from DSQuery to other DS commands**

Scott and Linda Mitchell are joining the Special Project team. They are the only two employees with the last name Mitchell who work at Contoso. They work in the Vancouver office.

1. Using a single command, add the Mitchells to the Special Project group.

Perform this step without typing the DN of the Mitchells' user accounts.

The DN of the Special Project group is "**cn= Special Project,ou=Role,ou=Groups,dc=contoso,dc=com**"

If you receive an error that says "The specified name is already a member of the group," use Active Directory Users and Computers to remove Scott Mitchell and Linda Mitchell from the Special Project group, then try again.

You may receive an Access Denied error. What is causing this error, and what can you do to work around it?

2. Using a single command, retrieve the e-mail address of all users in the Vancouver office.

Users in the Vancouver office have the word Vancouver in the Description field.

If you receive a warning that your DSQuery has reached its limit, what can you do to ensure all results are returned?

3. Using a single command, change the **office** attribute of the Mitchells to **Vancouver**.

► **Task 5 (Advanced Optional): Pipe DNs from DSGet to DSMod**

Advanced Optional exercises provide additional challenges for students who are able to complete lab exercises quickly. There are no answers in the Lab Answer Key.

Contoso is relocating and centralizing the executive leadership from regional offices to the Seattle office.

- Using a single command, change the office attribute of all members of the Executives group to **Headquarters**. Do this without typing the DN of the Executives group.

► **Task 6 (Advanced Optional): DSQuery ***

Advanced Optional exercises provide additional challenges for students who are able to complete lab exercises quickly. There are no answers in the Lab Answer Key.

- Type **dsquery /?** and examine the syntax of **dsquery.exe** *. Notice that you can use this form of DSQuery to display an arbitrary set of attributes using the Schema-defined name for the attribute.

Results: After this exercise, the Mitchells will belong to the Special Project group. The **office** attribute of the Mitchells is set to Vancouver, and the members of the Executives group have their **office** attribute set to **Headquarters**. You've learned how to administer Active Directory from the command line with DS commands!



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: What can you do to avoid typing DNs of users, groups, or computers into DSGet, and other DS commands?

Question: How are wildcard searches with DSQuery different than searches performed with the Find command in Active Directory Users and Computers? In other words, what kind of search have you performed in this lab that would not have been possible using the basic interface of the Find command?

Module 3

Lab Instructions: Manage Users

Contents:

Lab A: Create and Administer User Accounts	
Exercise 1: Create User Accounts	3
Exercise 2: Administer User Accounts	5
Exercise 3 (Advanced Optional): Explore User Account Name Attributes	7
Lab B: Configure User Object Attributes	
Exercise 1: Examine User Object Attributes	9
Exercise 2: Manage User Object Attributes	12
Exercise 3: Create Users from a Template	14
Exercise 4 (Advanced Optional): Create Users with a Batch File	16
Lab C: Automate User Account Creation	
Exercise 1: Export and Import Users with CSVDE	19
Exercise 2: Import Users with LDIFDE	21

Lab A: Create and Administer User Accounts

- Exercise 1: Create User Accounts
- Exercise 2: Administer User Accounts
- Exercise 3 (Advanced Optional): Explore User Account Name Attributes

Logon information

Virtual machine	6425B-HQDC01-A
Logon user name	Pat.Coleman
Administrative user name	Pat.Coleman_Admin
Password	Pa\$\$w0rd

Estimated time: 15 minutes

Scenario

You are the administrator of Contoso, Ltd., an online university for adult education. Two new employees have been hired: Chris Mayo and Amy Strande. You must create accounts for these users. As time passes, Chris Mayo leaves the organization, and his account must be administered according to the company policy for user account lifecycle management.

Exercise 1: Create User Accounts

In this exercise, you will create user accounts with both the Active Directory Users and Computers snap-in and the command prompt.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Create a user account with Active Directory Users and Computers.
3. Create a user account with the DSAdd command.

► Task 1: Prepare for the lab

- Start 6425B-HQDC01-A.
- Log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.
- Run **D:\Labfiles\Lab03b\Lab03a_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.

► Task 2: Create a user account with Active Directory Users and Computers

- Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
- Create a user account for Chris Mayo in the **Employees** OU.
 - First Name: **Chris**
 - Last Name: **Mayo**
 - User Logon Name: **Chris.Mayo**
 - User Logon Name (Pre-Windows 2000): **Chris.Mayo**
 - Password: **Pa\$\$w0rd**
 - Specify that he must change the password at the next logon

► **Task 3: Create a user account with the DSAdd command**

- Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
- At the command prompt, create a user account for Amy Strande in the **Employees OU**.
 - First Name: **Amy**
 - Last Name: **Strande**
 - User Principal Name: **Amy.Strande@contoso.com**
 - User Logon Name (Pre-Windows 2000): **Amy.Strande**
 - Display Name: **Strande, Amy**
 - Description: **Vice President, IT**
- In **Active Directory Users and Computers**, open the properties of the user account you just created and confirm that the attributes were set correctly.

Results: After this exercise, you will have user accounts named Chris Mayo and Amy Strande in the Employees OU.

Exercise 2: Administer User Accounts

In this exercise, you will perform common tasks that support user accounts through their lifecycle in Active Directory.

The main tasks for this exercise are as follows:

1. Administer a user account.
2. Administer the lifecycle of a user account.

► Task 1: Administer a user account

The user account for Amy Strande is currently disabled, because no password was specified using the DSAdd command.

1. What parameter could you have used with the DSAdd command to specify a password?
2. In **Active Directory Users and Computers**, reset the password for **Amy Strande** to **Pa\$\$w0rd**, and specify that she must change the password at the next logon.
3. In **Active Directory Users and Computers**, enable Amy Strande's user account.
4. What command could have been used at the command prompt to reset the password, specify that the password must be changed at the next logon, and enable the account? Write the command, including all of the parameters.

Results: After this exercise, Amy Strande's account will be enabled.

► Task 2: Administer the lifecycle of a user account

1. Contoso's policy for user account lifecycle management states the following:
 - When a user leaves the organization for any reason, including leave of absence, the user's account must be disabled immediately and moved to the Disabled Accounts OU.
 - Sixty days after the termination of a user, the user's account must be deleted.
2. Chris Mayo has left Contoso, Ltd. Disable his account and move it to the Disabled Accounts OU.

3. It has been 60 days since you disabled Chris Mayo and company procedures specify that after 60 days, a disabled user account must be deleted. Delete the user account for Chris Mayo.
4. Log off of HQDC01.

Results: After this exercise, Chris Mayo's account will have been deleted.



Note: Do not shut down the virtual machine once you are finished with this lab as the settings you have configured here will be used in the Lab B.

Exercise 3 (Advanced Optional): Explore User Account Name Attributes

Advanced Optional exercises provide additional challenges for students who are able to complete lab exercises quickly. There are no answers in the Lab Answer Key.

The main tasks for this exercise are as follows:

1. Create a sample user account. In the **Full Name** box, type the user's name using the format *LastName, FirstName*.
2. Look at the display of the user in the Active Directory Users and Computers details pane. You should see the user listed as *LastName, FirstName*.
3. In the properties of the user object, click the **Attribute Editor** tab and examine the actual value of the cn attribute.
4. Use the Active Directory Schema snap-in to examine the sAMAccountName attribute. What is its schema-defined length limit?
5. Attempt to create a user with a 30-character name in the **User logon name (pre-Windows 2000)** box. Experiment to determine the maximum length of the sAMAccountName attribute. Active Directory restricts the sAMAccountName attribute for user objects to a length that is significantly shorter than the schema-defined length.

Lab Review Questions

Question: In this lab, which attribute(s) can be modified when you are creating a user account with the command prompt that cannot be modified when creating a user account with Active Directory Users and Computers?

Question: What happens when you create a user account that has a password that does not meet the requirements of the domain?

Lab B: Configure User Object Attributes

- Exercise 1: Examine User Object Attributes
- Exercise 2: Manage User Object Attributes
- Exercise 3: Create Users from a Template
- Exercise 4 (Advanced Optional): Create Users with a Batch File

Logon information

Virtual machine	6425B-HQDC01-A
Logon user name	Pat.Coleman
Administrative user name	Pat.Coleman_Admin
Password	Pa\$\$w0rd

Estimated time: 15 minutes

Scenario

You are the administrator of Contoso, Ltd., an online university for adult education. Changes in the Sales department require you to modify attributes of Sales users. Additionally, you decide to make it easier to create new accounts for salespeople by preparing a user account template.

Exercise 1: Examine User Object Attributes

In this exercise, you will examine the attributes of a user object.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Explore the properties of an Active Directory user object.
3. Explore all attributes of an Active Directory user object.
4. Analyze the naming and display of user object attributes.

► Task 1: Prepare for the lab

The virtual machine should already be started and available after completing Lab A. However, if it is not, you should launch it complete the exercises in Lab A before continuing.

- Start 6425B-HQDC01-A.
- Log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.
- Run **D:\Labfiles\Lab03b\Lab03b_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.

► Task 2: Explore the properties of an Active Directory user object

- Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
- Open the properties of **Tony Krijnen** in the **Employees** OU.
- In this sample contoso.com domain, attributes have been configured on the **General**, **Address**, **Account** and **Organization** tabs. Examine each of these tabs, then close the **Properties** dialog box.

► Task 3: Explore all attributes of an Active Directory user object

- Enable the **Advanced Features** view of the **Active Directory Users and Computers** snap-in.
- Examine the **Attribute Editor** tab of Tony Krijnen's **Properties** dialog box.

► **Task 4: Analyze the naming and display of user object attributes**

- For each of the following attributes in the **Tony Krijnen Properties** dialog box, identify the corresponding attribute name on the **Attribute Editor** tab:

Properties dialog box tab	Property name	Attribute name as shown on the Attribute Editor tab
General	First name	
General	Last name	
General	Display name	
General	Description	
General	Office	
General	Telephone number	
General	E-mail	
Address	Street	
Address	City	
Address	ZIP/Postal Code	
Address	Country	
Organization	Job Title	
Organization	Department	
Organization	Company	

Questions:

1. Use the Attribute Editor tab to answer the following questions.
 - Does the employeeID attribute, shown on the Attribute Editor tab, show up on a normal tab of the Properties dialog box? If so, which one? What about carLicense?
 - Looking at the Attribute Editor tab, what is the distinguished name (DN) of Tony Krijnen's object?
 - Looking at the Attribute Editor tab, what is Tony's user principal name (UPN)? On which other tab does the attribute appear, and how is it labeled and displayed?
2. Thought questions: Try to answer the following questions. However, it is possible that you may not come up with an answer. That is OK. Once you've tried to think of an answer, you can look at the Lab Answer Key.
 - Why might the sn attribute be named sn?
 - What is the use of the c attribute?

Exercise 2: Manage User Object Attributes

In this exercise, you will manage the attributes of user objects.

The main tasks for this exercise are as follows:

1. Modify the attributes of multiple user objects.
2. Manage user attributes from the command prompt.

► Task 1: Modify the attributes of multiple user objects

A special Marketing Task Force has been established by Ariane Berthier, the Vice President of Marketing. Members of the task force are being relocated to Headquarters and will report directly to Ariane.

- Select the following users in the **Employees** OU: **Adam Barr**, **Adrian Lannin**, **Ajay Manchepalli**, **Ajay Solanki**, **Allan Guinot**, **Anav Silverman** and **András Tóth**.
- Configure the following properties for the users:
 - Office: **Headquarters**.
 - Description: **Marketing Task Force**.
 - Manager: **Ariane Berthier**.
- After changing the attributes, open the properties of Adam Barr and examine the attributes you just changed.
- The **Manager** attribute is a linked attribute. The other side of the link is the **Direct Reports** attribute. Open the properties of Ariane Berthier and examine the **Direct Reports**.

► Task 2: Manage user attributes from the command prompt

- Open the Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
- Use the DS commands to list the e-mail addresses of all users in the Marketing Task Force.



Tip: Users in the Marketing Task Force share a common Description property.

- Use the DS commands to configure the home folder for all users in the Marketing Task Force, so that they each have a U: drive that maps to `\\FILE01\TaskForceUsers\username`, where *username* is each user's unique logon name.
- In **Active Directory Users and Computers**, confirm that the changes you made were applied correctly by examining the properties of **Adam Barr**.

Exercise 3: Create Users from a Template

In this exercise, you will create a user account template and then generate a new user account based on that template.

The main tasks for this exercise are as follows:

1. Create a user account template for Sales.
2. Create a new user account based on a template.

► Task 1: Create a user account template for Sales

- In the **Employees** OU, create a template account for new sales people with the following properties:
 - First Name and Last Name: blank.
 - Full Name: **_Sales User** (note the underscore at the beginning of the name).
 - User Logon Name: **Template.Sales**.
 - Password: **Pa\$\$w0rd**.
 - User must change password at next logon.
 - Account is disabled.
 - Member of: Sales.
 - Department: Sales.
 - Company: Contoso, Ltd.
 - Manager: **Anibal Sousa**.
 - Account Expires: **last day of the current year**.

► Task 2: Create a new user account based on a template

- In the **Employees** OU, create an account for a new sales person based on the **_Sales User** template. The account should have the following properties:
 - First Name: **Rob**.
 - Last Name: **Young**.
 - User logon name: **Rob.Young**.

- Password: **Pa\$\$w0rd**.
- Account is enabled.

Results: After this exercise, you will have a user account named Rob Young in the Employees OU. The account will have all of the attributes you configured for the _Sales User template.

Exercise 4 (Advanced Optional): Create Users with a Batch File

Advanced Optional exercises provide additional challenges for students who are able to complete lab exercises quickly. There are no answers in the Lab Answer Key.

The main tasks for this exercise are as follows:

1. Create a script called `User_Provision.bat` that uses `DSAdd` to provision a user in the Employees OU. The goal is to be able to run the script with two parameters: first name and last name. The batch file should take these two parameters and create a user account with the following attributes:
 - The first name and last name as defined in the parameters in the command line.
 - The name in the format *FirstName LastName*.
 - The `sAMAccountName` in the format *FirstName.LastName*.
 - The `userPrincipalName` in the format *FirstName.LastName@contoso.com*.
 - The e-mail address in the same format as the UPN.
 - The `displayName` in the format *LastName, FirstName*.
 - An initial password of **Pa\$\$w0rd** that the user must change at first logon.



Tip: when you run a batch script with parameters, the batch script can refer to the first parameter as `%1` and the second parameter as `%2`.

2. Run the Command Prompt with administrative credentials and test the script to create a sample user account. Confirm that the user is created successfully and all attributes are populated according to the specifications shown above.
3. Compare your results to `D:\Labfiles\Lab03b\User_Provision.bat`.



Note: Do not shut down the virtual machine once you are finished with this lab as the settings you have configured here will be used in the Lab C.

Lab Review Questions

Question: What options have you learned for modifying attributes of new and existing users?

Question: What are the advantages and disadvantages of each?

Lab C: Automate User Account Creation

- Exercise 1: Export and Import Users with CSVDE
- Exercise 2: Import Users with LDIFDE

Logon information

Virtual machine	6425B-HQDC01-A
Logon user name	Pat.Coleman
Administrative user name	Pat.Coleman_Admin
Password	Pa\$\$w0rd

Estimated time: 15 minutes

Scenario

You are the administrator of Contoso, Ltd., an online university for adult education. You are hiring several new employees. The Human Resources department has provided you with extracts from their database, in both comma-delimited text format and in LDIF format. You want to import those data files to create user accounts for the new hires.

Exercise 1: Export and Import Users with CSVDE

In this exercise, you will use the CSVDE command to export user attributes and to create new user accounts from a comma-delimited text file.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Export users with CSVDE.
3. Import users with CSVDE.

► Task 1: Prepare for the lab

The virtual machine should already be started and available after completing Labs A and B. However, if it is not, you should launch it complete the exercises in Labs A and B before continuing.

- Start 6425B-HQDC01-A.
- Log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.
- Run **D:\Labfiles\Lab03c\Lab03c_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.

► Task 2: Export users with CSVDE

- Open the Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
- Type the following command:

```
csvde -f D:\Labfiles\Lab03c\UsersNamedApril.csv -r "(name=April*)"
-l DN,objectClass,sAMAccountName,sn,givenName,userPrincipalName
```

and then press ENTER.

- Open **D:\Labfiles\Lab03c\UsersNamedApril.csv** in Notepad.
- Examine the file, and then close it.

► **Task 3: Import users with CSVDE**

- Open **D:\Labfiles\Lab03c\NewUsers.csv** with Notepad. Examine the information about the users listed in the file.
- Type the following command:

```
csvde -i -f D:\Labfiles\Lab03c\NewUsers.csv -k
```

and then press ENTER.

The two users are imported.

- Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**. Confirm that the users were created successfully.
 - If you have had the Active Directory Users and Computers snap-in open during this exercise, you might have to refresh your view to see the newly created accounts.
- Examine the accounts to confirm that first name, last name, user principal name, and pre-Windows 2000 logon name are populated according to the instructions in NewUsers.txt.
- Reset the passwords of the two accounts to **Pa\$\$w0rd**.
- Enable the two accounts.
- Close NewUsers.csv.

Exercise 2: Import Users with LDIFDE

Like CSVDE, LDIFDE can be used to import users. The LDIF file format, however, is not a typical delimited text file. In this exercise, you will use LDIFDE to import two users.

The main tasks for this exercise are as follows:

- Import users with LDIFDE.

► Task 1: Import users with LDIFDE

- Open `D:\Labfiles\Lab03c\NewUsers.ldf` with Notepad. Examine the information about the users listed in the file.
- Type the following command:

```
ldifde -i -f D:\Labfiles\Lab03c\NewUsers.ldf -k
```

then press ENTER.

The two users are imported.

- In **Active Directory Users and Computers**, confirm that the users were created successfully.
 - If you have had the Active Directory Users and Computers snap-in open during this exercise, you might have to refresh your view to see the newly created accounts.
- Examine the accounts to confirm that user properties are populated according to the instructions in `NewUsers.ldf`.
- Reset the passwords of the two accounts to **Pa\$\$w0rd**.
- Enable the two accounts.
- Close `NewUsers.ldf`.
- Log off HQDC01.

Results: After this exercise, you will have imported accounts for Lisa Andres, David Jones, Bobby Moore and Bonnie Kearney.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Question

Question: What scenarios lend themselves to importing users with CSVDE and LDIFDE?

Module 4

Lab Instructions: Manage Groups

Contents:

Lab A: Administer Groups	
Exercise 1: Implement Role-Based Management Using Groups	3
Exercise 2: Manage Group Membership from the Command Prompt	6
Exercise 3 (Advanced Optional): Explore Group Membership Reporting Tools	8
Exercise 4 (Advanced Optional): Understand "Account Unknown" Permissions	9
Lab B: Best Practices for Group Management	
Exercise 1: Implement Best Practices for Group Management	11
Exercise 2 (Advanced Optional): Maintain Shadow Group Membership	13

Lab A: Administer Groups

- Exercise 1: Implement Role-Based Management Using Groups
- Exercise 2: Manage Group Membership from the Command Prompt
- Exercise 3 (Advanced Optional): Explore Group Membership Reporting Tools
- Exercise 4 (Advanced Optional): Understand "Account Unknown" Permissions

Logon information

Virtual machine	6425B-HQDC01-A
Logon user name	Pat.Coleman
Administrative user name	Pat.Coleman_Admin
Password	Pa\$\$w0rd

Estimated time: 15 minutes

Scenario

In order to improve the manageability of resource access at Contoso, Ltd., you have decided to implement role-based management. The first application of role-based management will be to manage who can access the folders containing Sales information. You must create groups that manage access to that sensitive information. Business rules are that Sales and Marketing employees, as well as a team of Consultants, should be able to read the Sales folders. Additionally, Bobby Moore requires Read access. Finally, you have been asked to discover a way to produce a list of group members, including those who are in nested groups; and a list of a user's group membership, including indirect or nested membership.

Exercise 1: Implement Role-Based Management Using Groups

In this exercise, you will implement role-based management using groups and the best practice group nesting strategy, IGDLA. You will create different scopes and types using both the Active Directory Users and Computers snap-in and command-line tools.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Create role groups with Active Directory Users and Computers.
3. Create role groups with DSAdd.
4. Add users to the role group.
5. Implement a role hierarchy in which Sales Managers are also part of the Sales role.
6. Create a resource access management group.
7. Assign permissions to the resource access management group.
8. Define which roles and users have access to a resource.

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A.
2. Log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Run **D:\Labfiles\Lab04a\Lab04a_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.

► Task 2: Create role groups with Active Directory Users and Computers

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Create global security groups called **Sales** and **Consultants** in the **Groups\Role** OU.

► **Task 3: Create a group with DSAdd**

1. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Using the **DSAdd** command, create a global security group named **Auditors** in the **Groups\Role** OU.
3. In **Active Directory Users and Computers**, confirm that the object has been created.

► **Task 4: Add users to the role group**

1. Add **Tony Krijnen** to the **Sales** group using the **Members** tab of the **Sales** group.
2. Add **Linda Mitchell** to the **Sales** group by right-clicking **Linda Mitchell** and choosing **Add to a group**.

► **Task 5: Implement a role hierarchy in which Sales Managers are also part of the Sales role**

- Add the **Sales Managers** group as a member of the **Sales** group by using the **Member Of** tab of the **Sales Managers** group.

► **Task 6: Create a resource access management group**

- Create a domain local security group named **ACL_Sales Folders_Read** in the **Groups\Access** OU.

► **Task 7: Assign permissions to the resource access management group**

1. Create a folder in **D:\Data** named **Sales**.
2. Right-click the **Sales** folder, then click **Properties**, and then click the **Security** tab.
3. Click **Edit**, and then click **Add**.
4. Type **ACL_** and press **ENTER**.

Notice that when you use a prefix for group names, such as the **ACL_** prefix for resource access groups, you can find them quickly.

5. Click **ACL_Sales Folders_Read**, and then click **OK**.
6. Confirm that the group has been given Read & Execute permission.
7. Click **OK** to close each open dialog box.

► **Task 8: Define which roles and users have access to a resource**

- Add **Sales**, **Consultants**, **Auditors**, and **Bobby Moore** to the **ACL_Sales Folders_Read** group.

Results: After this exercise, you will have a simple role-based management implementation to manage Read access to the Sales folder.

Exercise 2: Manage Group Membership from the Command Prompt

In this exercise, you will manage group membership from the command prompt using commands such as DSGet and DSMod.

The main tasks for this exercise are as follows:

1. Modify group membership with DSMod.
2. Retrieve group membership with DSGet.

► Task 1: Modify group membership with DSMod

1. Switch to the command prompt. Type the following command on one line, and then press ENTER.

```
dsmod group "CN=Auditors,OU=Role,OU=Groups,DC=contoso,DC=com" -  
addmbr "CN=Mike Danseglio,OU=Employees,OU=User Accounts,  
DC=contoso,DC=com" "CN=Finance Managers,OU=Role,  
OU=Groups,DC=contoso,DC=com"
```

2. In **Active Directory Users and Computers**, confirm that the membership of the **Auditors** group includes **Mike Danseglio** and the **Finance Managers** group.

► Task 2: Retrieve group membership with DSGet

1. Switch to the command prompt.
2. List the direct members of the **Auditors** group by typing the following command, and then pressing ENTER:

```
dsget group "CN=Auditors,OU=Role,OU=Groups,DC=contoso,DC=com"  
-members
```

3. List the full list of members of the **Auditors** group by typing the following command, and then pressing ENTER:

```
dsget group "CN=Auditors,OU=Role,OU=Groups,DC=contoso,DC=com"  
-members -expand
```


4. List the full list of members of the **ACL_Sales Folders_Read** group by typing the following command, and then pressing ENTER:

```
dsget group "CN=ACL_Sales Folders_Read,OU=Access,  
OU=Groups,DC=contoso,DC=com" -members -expand
```

5. List the direct group membership of **Mike Danseglio** by typing the following command, and then pressing ENTER:

```
dsget user "CN=Mike Danseglio,OU=Employees,OU=User Accounts,  
DC=contoso,DC=com" -memberof
```

6. List the full group membership of **Mike Danseglio** by typing the following command on one line, and then pressing ENTER:

```
dsget user "CN=Mike Danseglio,OU=Employees,OU=User Accounts,  
DC=contoso,DC=com" -memberof -expand
```

Results: After this exercise, you will have a simple role-based management implementation to manage Read access to the Sales folder.

Exercise 3 (Advanced Optional): Explore Group Membership Reporting Tools

Advanced Optional exercises provide additional challenges for students who are able to complete lab exercises quickly. There are no answers in the Lab Answer Key.

The main tasks for this exercise are as follows:

1. Open **D:\AdminTools\Members_Report.hta**. Enter the name of a group, and then click **Report**.
2. Open **D:\AdminTools\MemberOf_Report.hta**. Enter the name of a user, computer, or group, and then click **Report**.

Exercise 4 (Advanced Optional): Understand "Account Unknown" Permissions

Advanced Optional exercises provide additional challenges for students who are able to complete lab exercises quickly. There are no answers in the Lab Answer Key.

The main tasks for this exercise are as follows:

1. In the **Role** OU, create a global security group named **Test**.
2. Give the group **Read & Execute** permission to the **D:\Data\Sales** folder.
3. Delete the group named **Test**.
4. Examine the **Security** tab of the Sales folder's properties dialog box. If you still see the Test group listed, Windows Explorer may be caching the mapping of the SID to the group name. Log off, log on, and check again.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in the Lab B.

Lab Review Questions

Question: Describe the purpose of global groups in terms of role-based management.

Question: What types of objects can be members of global groups?

Question: Describe the purpose of domain local groups in terms of role-based management of resource access.

Question: What types of objects can be members of domain local groups?

Question: If you have implemented role-based management and are asked to report who can read the Sales folders, what command would you use to do so?

Lab B: Best Practices for Group Management

- Exercise 1: Implement best practices for group management

Logon information

Virtual machine	6425B-HQDC01-A
Logon user name	Pat.Coleman
Administrative user name	Pat.Coleman_Admin
Password	Pa\$\$w0rd

Estimated time: 15 minutes

Scenario

Your implementation of role-based management at Contoso has been highly successful. As the number of groups in the domain has increased, you've come to realize that it is important to document groups thoroughly and to prevent administrators from accidentally deleting a group. Finally, you want to allow the business owners of resources to manage access to those resources by delegating to those owners the right to modify the membership of appropriate groups.

Exercise 1: Implement Best Practices for Group Management

In this exercise, you will perform the following tasks to document, delegate, and secure groups:

1. Prepare for the lab.
2. Create a well-documented group.
3. Protect a group from accidental deletion.
4. Delegate group membership management.
5. Validate the delegation of group membership management.

► Task 1: Prepare for the lab

The virtual machine should already be started and available after completing Lab A. However, if it is not, you should launch it and complete the exercises in Lab A before continuing.

1. Start 6425B-HQDC01-A.
2. Log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 2: Create a well-documented group

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the properties of the **ACL_Sales Folders_Read** group, configure the following:
 - A **Description** that summarizes the resource management rule represented by the group: **Sales Folders (READ)**
 - In the **Notes** box, type the following paths to represent the folders that have permissions assigned to this group:
\\contoso\teams\Sales (READ)
\\file02\data\Sales (READ)
\\file03\news\Sales (READ)

► **Task 3: Protect a group from accidental deletion**

1. Enable the **Advanced Features** view of the **Active Directory Users and Computers** snap-in.
2. Protect the **ACL_Sales Folders_Read** group from being accidentally deleted.
3. Attempt to delete the group. Confirm that the attempt to delete the group is denied.

► **Task 4: Delegate group membership management**

- Configure the **Managed By** attribute of **Auditors** to refer to **Mike Danseglio**.

► **Task 5: Validate the delegation of group membership management**

1. Log off of HQDC01, then log on with username **Mike.Danseglio** and password **Pa\$\$w0rd**.
2. Open the **Network** window and use **Search Active Directory** to locate the **Auditors** group.
3. Add the **Executives** group to the **Auditors** group.
4. Log off HQDC01.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Exercise 2 (Advanced Optional): Maintain Shadow Group Membership

Advanced Optional exercises provide additional challenges for students who are able to complete lab exercises quickly. There are no answers in the Lab Answer Key.

The main tasks for this exercise are as follows:

1. Confirm that a global security group called **Administrative Identities** exists in the **Groups\Role** OU.

This will be a shadow group that contains accounts in the Admin Identities OU.

2. Create a batch script that uses DSQuery, DSGet, and DSMod to synchronize the group's membership with the users in the Admin Identities OU.

The script will be run at regular intervals to keep the group's membership synchronized with the Admin Identities OU. The script must account for new users added to the OU, and for users removed from the OU.

3. Test the script by performing the following steps using administrative credentials:
 - a. Run the script.
 - b. Confirm that the membership of the Administrative Identities group is the same as the contents of the Admin Identities OU.
 - c. Create a new user account in the Admin Identities OU.
 - d. Run the script.
 - e. Confirm that the group contains the newly added user.
 - f. Disable the new user account and move the user into the Disabled Accounts OU.
 - g. Run the script.
 - h. Confirm that the group no longer contains the user.
4. Time permitting, create a Scheduled Task that runs the script once every minute. Repeat the test sequence, but instead of running the script, allow the scheduled task to run.

You can compare your batch script with
D:\Labfiles\Lab04b\Shadow_Group.bat.

Note that the DS Commands achieve the goal of maintaining a shadow group, but they do not do so particularly efficiently. Removing all members and re-adding all members generates a larger-than-necessary amount of replication traffic, particularly for a large shadow group with hundreds or thousands of members. You can use a scripting language, such as VBScript or Windows PowerShell, to create a more efficient script that updates, rather than replaces, group membership to account for changes. See the *Windows Administration Resource Kit: Productivity Solutions for IT Professionals* by Dan Holme (Microsoft Press, 2008) for a sample script.

Lab Review Questions

Question: What are some benefits of using the Description and Notes fields of a group?

Question: What are the advantages and disadvantages of delegating group membership?

Module 5

Lab Instructions: Support Computer Accounts

Contents:

Lab A: Create Computers and Joining the Domain	
Exercise 1: Join a Computer to the Domain with the Windows® Interface	3
Exercise 2: Secure Computer Joins	6
Exercise 3: Manage Computer Account Creation with Best Practices	8
Lab B: Administer Computer Objects and Accounts	
Exercise 1: Administer Computer Objects Through Their Life Cycle	11
Exercise 2: Administer and Troubleshooting Computer Accounts	14

Lab A: Create Computers and Join the Domain

- Exercise 1: Join a Computer to the Domain with the Windows Interface
- Exercise 2: Secure Computer Joins
- Exercise 3: Manage Computer Account Creation with Best Practices

Logon information

Virtual machine	6425B-HQDC01-A	6425B-SERVER01-B
Logon user name	Pat.Coleman	
Administrative user name	Pat.Coleman_Admin	Administrator
Password	Pa\$\$w0rd	Pa\$\$w0rd

Estimated time: 20 minutes

Scenario

You are an administrator for Contoso, Ltd. During a security audit, it was identified that there is no control over the creation of new computer accounts: both clients and servers are being added to the domain with no assurance that process is being followed. In fact, a number of computer accounts were discovered in the Computers container. These computer objects were for active computer accounts, but the computers had not been created in or moved to the correct OUs within the Client Computers or Servers OUs according to standard procedures. You've been tasked with improving the procedures.

Exercise 1: Join a Computer to the Domain with the Windows® Interface

In this exercise, you will join a computer to the domain using the Windows interface, and then you will remove the machine from the domain.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Identify and correct a DNS configuration error.
3. Join SERVER01 to the domain.
4. Verify the location of the SERVER01 account.
5. Remove SERVER01 from the domain.
6. Delete the SERVER01 account.

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A and 6425B-SERVER01-B.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Open **D:\Labfiles\Lab05a**.
4. Run **Lab05a_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
5. The lab setup script runs. When it is complete, press any key to continue.
6. Close the Windows Explorer window, **Lab05a**.
7. Start 6425B-SERVER01-B.

► Task 2: Identify and correct a DNS configuration error

1. Log on to SERVER01 as **Administrator** with the password **Pa\$\$w0rd**.
2. Open **System Properties** using one of the following methods:
 - Click **Start**, then right-click **Computer**, and then click **Properties**.
 - Open **System** from **Control Panel**.
 - Press the WINDOWS LOGO key and the PAUSE key.

3. Attempt to join the computer to the domain **contoso.com**, being sure to use *the fully qualified domain name (contoso.com)* rather than the NetBIOS name for the domain (contoso).

Doing so tests that DNS is configured correctly on the client for locating the domain.

4. Change the DNS Server configuration on the client to **10.0.0.11**.

Question: Why might the join have succeeded if you had used the domain name **contoso** instead of **contoso.com**? What might go wrong after the domain was successfully joined with DNS but incorrectly configured?

► **Task 3: Join SERVER01 to the domain**

1. Join SERVER01 to the domain. When prompted for domain credentials, enter the username **Aaron.Painter** and the password **Pa\$\$w0rd**.

Note that Aaron.Painter is a standard user in the contoso.com domain. He has no special rights or permissions, and yet he is able to join a computer to the domain. He does have to be logged on to the computer with an account that is a member of the computer's Administrators group.

2. Allow the system to restart.

► **Task 4: Verify the location of the SERVER01 account**

1. On HQDC01, run Active Directory Users and Computers as an administrator, with the username **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Locate the SERVER01 account.

Question: In which OU or container does the account exist?

► **Task 5: Remove SERVER01 from the domain**

1. Log on to SERVER01 as Administrator with the password **Pa\$\$w0rd**.
2. Change SERVER01's domain/workgroup membership to a workgroup named **WORKGROUP**.
3. Restart the server.

► **Task 6: Delete the SERVER01 account**

Question: On HQDC01, refresh the view of the Computers container and examine the SERVER01 account. What is its status?

Question: You were not prompted for domain credentials in Task 5, and yet a change was made to the domain: the computer account was reset and disabled. What credentials were used to do this? What credentials were used to change the workgroup/domain membership of SERVER01?

- Delete SERVER01's account.

Results: After this exercise, you will be familiar with typical legacy practices used to join computers to a domain.

Exercise 2: Secure Computer Joins

In this exercise, you will implement best practices to secure the joining of machines to the domain.

The main tasks for this exercise are as follows:

1. Redirect the default computer container.
2. Restrict unmanaged domain joins.
3. Validate the effectiveness of ms-DS-MachineAccountQuota.

► Task 1: Redirect the default computer container

1. Run a command prompt as an administrator with the username **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Use the **RedirCmp** command to redirect the default computers container to the **New Computers** OU in the **contoso.com** domain.

► Task 2: Restrict unmanaged domain joins

1. Run the ADSI Edit console as an administrator with the username **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Connect to the domain and, in the properties of the domain, change the **ms-DS-MachineAccountQuota** to zero (0).

► Task 3: Validate the effectiveness of ms-DS-MachineAccountQuota

- Log on to SERVER01 as **Administrator** and attempt to join **SERVER01** to the **contoso.com** domain just as you did in Exercise 1. When prompted for domain credentials, enter the username **Aaron.Painter** and the password **Pa\$\$w0rd**.

In the Exercise 1, Aaron Painter was able to join the domain. Now, he is unable to join the domain.

Question: What message do you receive when a user is no longer able to create a computer object because of the ms-DS-MachineAccountQuota?

Results: After this exercise, the container for creating computer accounts will be redirected to the New Computers OU, and users will be restricted from joining computers to the domain without explicit permissions to do so.

Exercise 3: Manage Computer Account Creation with Best Practices

In this exercise, you will implement several best practices for creating computer accounts and joining machines to the domain.

The main tasks for this exercise are as follows:

1. Prestage a computer account.
2. Join a computer remotely to a prestaged account using NetDom.

► Task 1: Prestage a computer account

1. Run **Active Directory Users and Computers** as an administrator with the username **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. In the **Servers\File** OU, create a new computer object for **SERVER01** and give the **AD_Server_Deploy** group permission to join the computer to the domain.

► Task 2: Join a computer remotely to a prestaged account using NetDom

In this task, you will join **SERVER01** to the domain *remotely*, using credentials that are in the local Administrators group of **SERVER01** and domain credentials that are in the **AD_Server_Deploy** group.

1. Run the command prompt as an administrator, with the username **Aaron.Painter_Admin** and the password **Pa\$\$word**.

Note that **Aaron.Painter_Admin** is not an administrator, *per se*. The Run as an administrator command allows you to launch a process with any credentials, as long as those credentials have sufficient privilege to launch the process itself.
2. Type the command **whoami /groups** to list the group memberships of the current account (**Aaron.Painter_Admin**). Note that the user is a member of **AD_Server_Deploy** and is not a member of any other administrative group.
3. Using the **NetDom** command, join **SERVER01** to the domain. Use the local Administrator account credentials for **SERVER01** and the domain credentials for **Aaron.Painter_Admin**, who is a member of **AD_Server_Deploy** and therefore has permission to join the computer to the domain. Configure the server to reboot automatically in 5 seconds.

Type the following command, and then press ENTER:

```
netdom join SERVER01 /domain:contoso.com  
/UserO:Administrator /Password0:*  
/UserD:CONTOSO\Aaron.Painter_Admin /PasswordD:*  
/REBoot:5
```



Note: SERVER01 has firewall exceptions configured ports 135, 139, and for Network Discovery (NB-Name-In). These exceptions allow NetDom Join to be used to remotely join SERVER01 to the domain.

4. The server restarts.

Results: After this exercise, SERVER01 will be joined to the domain with an account in the Servers\File OU.



Important: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in the Lab B.

Lab Review Questions

Question: What did you learn about the pros and cons of various approaches to creating computer accounts in an AD DS domain?

Question: What are the two credentials that are necessary for any computer to join a domain?

Lab B: Administer Computer Objects and Accounts

- Exercise 1: Administer Computer Objects Through Their Life cycle
- Exercise 2: Administer and Troubleshooting Computer Accounts

Logon information

Virtual machine	6425B-HQDC01-A	6425B-SERVER01-B
Logon user name	Pat.Coleman	Pat.Coleman
Administrative user name	Pat.Coleman_Admin	Administrator
Password	Pa\$\$w0rd	Pa\$\$w0rd

Estimated time: 15 minutes

Scenario

You are an administrator for Contoso, Ltd. During a security audit, a number of computer accounts were discovered. Those computers no longer exist in the domain. You've been tasked with improving the management of computer accounts, and identifying best practices for administering the entire life cycle of a computer account.

Exercise 1: Administer Computer Objects Through Their Life Cycle

In this exercise, you will configure common attributes of computer objects, including description and ManagedBy. You will also manage the group membership of computers and move computers between OUs.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Configure computer object attributes.
3. Add computers to software management groups.
4. Move a computer between OUs.
5. Disable, enable and delete computers.

► Task 1: Prepare for the lab

The virtual Machines should already be started and available after completing Lab A. However, if they are not, you should complete steps 1 to 3 below and then step through exercises 1 to 3 in Lab A before continuing. You will be unable to successfully complete Lab B unless you have completed Lab A.

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Start 6425B-SERVER01-B.

► Task 2: Configure computer object attributes

1. On HQDC01, run **Active Directory Users and Computers** as an administrator, with the username **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. In the **Client Computers\SEA OU**, use the **Managed By** tab of computer objects to assign **LNO8538** to **Linda Mitchell** and **LOT9179** to **Scott Mitchell**.
3. Because Scott and Linda Mitchell will occasionally use each other's computer, use multiselect to change the description of both **LNO8538** and **LOT9179** to **Scott and Linda Mitchell**.

► **Task 3: Add computers to software management groups**

Microsoft Office Project is required on both Scott's and Linda's computers. Contoso uses security groups as collections for scoping the deployment of software. You will add each of their computers to the group APP_Project using two different methods.

1. In the **Client Computers\SEA OU**, right-click **LOT9179**, and then click **Add to a group**.

2. Type **APP_** and press ENTER.

The Multiple Items Found dialog box appears.

3. Click **APP_Project** and click **OK**.

A message appears: "The Add to Group operation was successfully completed."

4. Click **OK**.

5. In the console tree, expand the **Groups OU**, and then click **Application**.

6. Right-click **APP_Project**, and then click **Properties**.

7. Click the **Members** tab.

8. Click **Add**.

9. Type **LNO8538** and press ENTER.

The Name Not Found dialog box appears.

By default, the Select Users, Computers, or Groups interface does not search for computer objects.

10. Click **Object Types**.

11. Select the check box next to **Computers**, and then click **OK**.

12. Click **OK** to close the **Name Not Found** dialog box.

Both computers can now be seen on the Members tab.

13. Click **OK**.

► **Task 4: Move a computer between OUs**

Scott and Linda are relocating to the Vancouver office. You will move their computers to the new OU using two different methods.

1. In the **Client Computers\SEA OU**, click **LOT9179**.
2. Drag **LOT9179** into the **VAN OU**, visible in the console tree.
A message appears that reminds you to be careful about moving objects in Active Directory.
3. Click **Yes**.
4. Right-click **LNO8538**, and then click **Move**.
The Move dialog box appears.
5. In the console tree, expand **Client Computers**, and then click **VAN**.
6. Click **OK**.

► **Task 5: Disable, enable, and delete computers**

1. In the **Client Computers\SEA OU**, disable, then enable the account for **DEP6152**.
2. Delete the account for **DEP6152**.

Exercise 2: Administer and Troubleshooting Computer Accounts

In this exercise, you will administer and troubleshoot computer accounts and the secure channel.

The main tasks for this exercise are as follows:

1. Reset a computer account.
2. Experience a secure channel problem.
3. Reset the secure channel.

► Task 1: Reset a computer account

Recently, Scott Mitchell's computer required reinstallation. Contoso's naming convention is that the name of a computer object is its asset tag, assigned by the IT inventory team. Because Scott reinstalled his computer on the same piece of hardware, the computer name is the same: LOT9179. He now wants to join the machine to the domain, but there is already an account for LOT9179, and the account is a member of groups that ensure the correct software (including Microsoft Office Project) and configuration are applied to the system. Therefore, it is important that the account not be deleted, so that group memberships can be retained.

- In the **Client Computers\VAN OU**, reset the account for **LOT9179**.

You could now join Scott's reinstalled computer to the domain.

► Task 2: Experience a secure channel problem

1. Demonstrate that you can log on successfully to SERVER01 as **Pat.Coleman** with the password **Pa\$\$w0rd**. After the desktop appears, log off.
2. To "break" the secure channel, use Active Directory Users and Computers on HQDC01 to reset the account for SERVER01.
3. Attempt to log on to SERVER01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 3: Reset the secure channel

To solve a broken trust relationship between a domain member and the domain, you can reset the computer's account, then move the computer into a workgroup, and then rejoin the domain.

- Reset the computer account for SERVER01.

After resetting the secure channel, you could move SERVER01 into a workgroup, and then rejoin the domain. It will join its reset account, thereby retaining its group memberships. Do not perform that step at this time.

Results: After this exercise, you will have a user account named Chris Mayo in the Employees OU.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Question

Question: What insights did you gain into the issues and procedures regarding computer accounts and administering computer accounts through their life cycle?

Module 6

Lab Instructions: Implement a Group Policy Infrastructure

Contents:

Lab A: Implement Group Policy	
Exercise 1: Create, Edit, and Link Group Policy Objects	3
Lab B: Manage Settings and GPOs	
Exercise 1: Use Filtering and Commenting	7
Exercise 2: Manage Administrative Templates	9
Lab C: Manage Group Policy Scope	
Exercise 1: Configure GPO Scope with Links	14
Exercise 2: Configure GPO Scope with Filtering	17
Exercise 3: Configure Loopback Processing	19
Lab D: Troubleshoot Policy Application	
Exercise 1: Perform RSoP Analysis	22
Exercise 2: Use the Group Policy Modeling Wizard	25
Exercise 3: View Policy Events	28

Lab A: Implement Group Policy

- Exercise 1: Create, Edit, and Link Group Policy Objects

Logon information

Virtual machine	6425B-HQDC01-A	6425B-Desktop101-A
Logon user name	Pat.Coleman	Pat.Coleman
Administrative user name	Pat.Coleman_Admin	
Password	Pa\$\$w0rd	Pa\$\$w0rd

Estimated time: 30 minutes

Scenario

You are responsible for managing change and configuration at Contoso, Ltd. Contoso corporate IT security policies specify that computers cannot be left unattended and logged onto for more than 10 minutes. You will therefore configure the screen-saver timeout and password-protected screen-saver policy settings. Additionally, you will lock down access to registry editing tools.

Exercise 1: Create, Edit, and Link Group Policy Objects

In this exercise, you will create a GPO that implements a setting mandated by the corporate security policy of Contoso, Ltd., and scope the setting to all users and computers in the domain. You will then experience the effect of the GPO. Any remaining time can be used exploring settings that are made available within a Group Policy object.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Create a GPO.
3. Edit the settings of a GPO.
4. Scope a GPO with a GPO link.
5. View the effects of Group Policy application.
6. Explore GPO settings.

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Start 6425B-DESKTOP101-A but do not log on to the system.

► Task 2: Create a GPO

1. Run **Group Policy Management** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Create a **Group Policy** object named **CONTOSO Standards** in the **Group Policy** objects container.

► Task 3: Edit the settings of a GPO

1. Edit the **CONTOSO Standards** GPO.
2. Navigate to the **User Configuration, Policies, Administrative Templates, System** folder.
3. Prevent users from running **Registry Editor** and **regedit /s**.

4. Navigate to the **User Configuration, Policies, Administrative Templates, Control Panel, Display** folder.
5. Examine the explanatory text for the **Screen Saver** timeout policy setting.
6. Configure the **Screen Saver** timeout policy to **600** seconds.
7. Enable the **Password protect the screen saver** policy setting.

► **Task 4: Scope a GPO with a GPO link**

- Link the **CONTOSO Standards** GPO to the **contoso.com** domain.

► **Task 5: View the effects of Group Policy application**

1. Log on to DESKTOP101 as **Pat.Coleman**.
2. Attempt to change the **Screen Saver** timeout and password protection. You will be prevented from doing so by Group Policy.
3. Attempt to run **Registry Editor**. You will be prevented from doing so by Group Policy.

► **Task 6: Explore GPO settings**

- On HQDC01, edit the **CONTOSO Standards** GPO and spend time exploring the settings that are available in a GPO. Do not make any changes.

Results: After this exercise, you will have a GPO named **CONTOSO Standards** that configures password-protected screen saver, screen-saver timeout, and registry editing tool restrictions..



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs.

Lab Review Questions

Question: What policy settings are already being deployed using Group Policy in your organization?

Question: What policy settings did you discover that you might want to implement in your organization?

Lab B: Manage Settings and GPOs

- Exercise 1: Use Filtering and Commenting
- Exercise 2: Manage Administrative Templates

Logon information

Virtual machine	6425B-HQDC01-A
Logon user name	Pat.Coleman
Administrative user name	Pat.Coleman_Admin
Password	Pa\$\$w0rd

Estimated time: 30 minutes

Scenario

You were recently hired as the domain administrator for Contoso, Ltd., replacing the previous administrator, who retired. You are not certain what policy settings have been configured, so you decide to locate and document GPOs and policy settings. You also discover that the company has not leveraged either the functionality or the manageability of administrative templates.

Exercise 1: Use Filtering and Commenting

In this exercise, you will use the new commenting and filtering features of Group Policy to locate and document policy settings.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Search and filter policy settings.
3. Document GPOs and settings with comments.

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 2: Search and filter policy settings

1. In the **User Configuration\Policies\Administrative Templates** folder, filter the view to show only policy settings that contain the phrase **screen saver**. Spend a few moments examining those settings.
2. Filter the view to show only configured policy settings. Spend a few moments examining those settings.
3. Turn off the filter from **Administrative Templates**.

► **Task 3: Document GPOs and settings with comments**

1. Edit the comment to the **CONTOSO Standards** GPO and add the following comment to the GPO: **Contoso corporate standard policies. Settings are scoped to all users and computers in the domain. Person responsible for this GPO: *your name*.**

This comment appears on the Details tab of the GPO in the GPMC.

2. Add the following comment to the screen saver policy setting: **Corporate IT Security Policy implemented with this policy in combination with Password Protect the Screen Saver.**
3. Add the following comment to the **Password Protect the Screen Saver** policy setting: **Corporate IT Security Policy implemented with this policy in combination with Screen Saver Timeout.**

Results: After this exercise, you will have added comments to your Group Policy object and settings..

Exercise 2: Manage Administrative Templates

Administrative templates provide the instructions with which the GPME creates a user interface to configure Administrative Templates policy settings and specify the registry changes that must be made based on those policy settings. In this exercise, you will examine and manage administrative templates. You will also create a central store of administrative templates to centralize the management of templates.

The main tasks for this exercise are as follows:

1. Explore the syntax of an Administrative Template.
2. Manage classic administrative templates (.ADM files).
3. Manage .ADMX and .ADML files.
4. Create the central store.

► Task 1: Explore the syntax of an administrative template

1. On HQDC01, click **Start**, then click **Run**, then type **%SystemRoot%\PolicyDefinitions** and press ENTER. The **PolicyDefinitions** folder opens.
2. Open the **en-us** folder or the folder for your region and language.
3. Double-click **ControlPanelDisplay.adml**.
4. Choose the **Select a program from a list of installed programs** option and click **OK**.
5. Select **Notepad** and click **OK**.
6. Click the **Format** menu and select **Word wrap**.
7. Search for the text **ScreenSaverIsSecure**.
This is a definition of a string variable called ScreenSaverIsSecure.
8. Note the text between the **<string>** and **</string>** tags.
9. Note the name of the variable on the following line, **ScreenSaverIsSecure_Help**, and the text between the **<string>** and **</string>** tags.
10. Close the file.
11. Navigate up to the **PolicyDefinitions** folder.

12. Double-click **ControlPanelDisplay.admx**.
13. Choose the **Select a program from a list of installed programs** option and click **OK**.
14. Select **Notepad** and click **OK**.
15. Search for the text, **ScreenSaverIsSecure**.
16. Examine the code in the file, also shown below:

```
<policy name="ScreenSaverIsSecure" class="User"
displayName="$(string.ScreenSaverIsSecure)"
explainText="$(string.ScreenSaverIsSecure_Help)"
key="Software\Policies\Microsoft\Windows\Control Panel\Desktop"
valueName="ScreenSaverIsSecure">
  <parentCategory ref="Display" />
  <supportedOn ref="windows:SUPPORTED_Win2kSP1" />
  <enabledValue>
    <string>1</string>
  </enabledValue>
  <disabledValue>
    <string>0</string>
  </disabledValue>
</policy>
```

17. Identify the parts of the template that define the following:
 - The name of the policy setting that appears in the GPME
 - The explanatory text for the policy setting
 - The registry key and value affected by the policy setting
 - The data put into the registry if the policy is enabled
 - The data put into the registry if the policy is disabled
18. Close the file, and then close Windows Explorer.

► **Task 2: Manage classic administrative templates (.ADM files)**

1. Open the GPME and, in the **User Configuration\Policies\Administrative Templates** folder, add the **office12.adm** template from **D:\Labfiles\Lab06b\Office 2007 Administrative Templates**.

Classic administrative templates (.ADM files) are provided primarily for enterprises that do not manage Group Policy with Windows Vista or Windows Server 2008 or later operating systems.

You should use a computer running the most recent version of Windows to manage Group Policy. By doing so, you will be able to view and modify all available policy settings, including those that apply to previous versions of Windows. If you have at least one computer running Windows Vista, Windows Server 2008, or later, you should use that computer to manage Group Policy, and then you will not need classic administrative templates (.ADM files) when .ADMX/.ADML files are available.

Note that the template format affects only the *management* of Group Policy. Settings will apply to versions of Windows as described in the Supported on or Requirements section of the policy setting properties.

2. Examine the settings exposed by this administrative template.
3. Remove the template.

► **Task 3: Manage .ADMX and .ADML files**

- Copy all .ADMX files and the **en-us** subfolder (or the appropriate subfolder for your language and region) from **D:\Labfiles\Lab06b\Office 2007 Administrative Templates** to **%SystemRoot%\PolicyDefinitions**. When you paste the files, you will be prompted for administrative credentials. Use the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
- Close and then re-open the GPME for **CONTOSO Standards**. In the console tree, expand **User Configuration\Policies\Administrative Templates**. Note the addition of Microsoft® Office 2007 policy setting folders.

► Task 4: Create the central store

1. In the GPME, select the **Administrative Templates** node underneath **User Configuration\Policies**, and note the heading in the details pane reports: **Policy definitions (ADMX files) retrieved from the local machine**.
2. Close the GPME.
3. Copy all .ADMX files from %systemroot%\PolicyDefinitions to \\contoso.com\SYSVOL\contoso.com\Policies\PolicyDefinitions.
4. Copy all .ADML files from %systemroot%\PolicyDefinitions\en-us (or the appropriate folder for your language and region) to \\contoso.com\SYSVOL\contoso.com\Policies\PolicyDefinitions\en-us (or the appropriate folder for your language and region).
5. Edit the **CONTOSO Standards** GPO and, in the GPME, select the **Administrative Templates** node underneath **User Configuration\Policies**, and note the heading in the details pane reports: **Policy definitions (ADMX files) retrieved from the central store**.

Results: After this exercise, you will have created a central store of administrative templates and added the Microsoft Office 2007 templates..



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs.

Lab Review Questions

Question: Describe the relationship between administrative template files (both .ADMX and .ADML files) and the GPME.

Question: When does an enterprise get a central store? What benefits does it provide?

Question: What are the advantages of managing Group Policy from a client running the latest version of Windows? Do settings you manage apply to previous versions of Windows?

Lab C: Manage Group Policy Scope

- Exercise 1: Configure GPO Scope with Links
- Exercise 2: Configure GPO Scope with Filtering
- Exercise 3: Configure Loopback Processing

Logon information

Virtual machine	6425B-HQDC01-A	6425B-DESKTOP101-A
Logon user name	Pat.Coleman	Do not Logon
Administrative user name	Pat.Coleman_Admin	
Password	Pa\$\$w0rd	

Estimated time: 30 minutes

Scenario

You are an administrator of the contoso.com domain. The CONTOSO Standards GPO, linked to the domain, configures a policy setting that requires a ten-minute screen saver timeout. An engineer reports that a critical application that performs lengthy calculations crashes when the screens saver starts, and the engineer has asked you to prevent the setting from applying to the team of engineers that uses the application every day. You have also been asked to configure conference room computers to use a 45-minute timeout, so that the screen saver does not launch during a meeting.

Exercise 1: Configure GPO Scope with Links

In this exercise, you will modify the scope of GPOs using GPO links, and you will explore inheritance, precedence, and the effects of Enforced links and Block Inheritance.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Create a GPO with a policy setting that takes precedence over a conflicting setting.
3. View the effect of an Enforced GPO link.
4. Apply Block Inheritance.

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Start 6425B-DESKTOP101-A but do not log on to the system.

► Task 2: Create a GPO with a policy setting that takes precedence over a conflicting setting

1. Run **Active Directory Users and Computers** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. In the **User Accounts\Employees** OU, create a sub-OU called **Engineers**, and then close Active Directory Users and Computers.
3. Run the Group Policy Management Console as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
4. Create a new GPO linked to the **Engineers** OU called **Engineering Application Override**.
5. Configure the **Screen saver** timeout policy setting to be disabled, and then close the GPME.

6. Select the **Engineers** OU, and then click the **Group Policy Inheritance** tab. Notice that the **Engineering Application Override** GPO has precedence over the **CONTOSO Standards** GPO.
7. The screen saver timeout policy setting you just configured in the **Engineering Application Override** GPO will be applied after the setting in the **CONTOSO Standards** GPO. Therefore, the new setting will overwrite the standards setting, and will "win." Screen saver timeout will be disabled for users within the scope of the **Engineering Application Override** GPO.

► **Task 3: View the effect of an Enforced GPO link**

1. In the GPMC console tree, select the **Domain Controllers** OU, and then click the **Group Policy Inheritance** tab.
2. Notice that the GPO named **6425B** has the highest precedence. Settings in this GPO will override any conflicting settings in any of the other GPOs.

The Default Domain Controllers GPO specifies, among other things, which groups are given the right to log on locally to domain controllers. To enhance the security of domain controllers, standard users are not given the right to log on locally. In order to allow a nonprivileged user account such as Pat.Coleman to log on to domain controllers in this course, the 6425B GPO gives Domain Users the right to log on locally to a computer. The 6425B GPO is linked to the domain, so its settings would normally be overridden by settings in the Default Domain Controllers GPO. Therefore, the 6425B GPO link to the domain is configured as Enforced. In this way, the conflict in user rights assignment between the two GPOs is "won" by the 6425B GPO.

► **Task 4: Apply Block Inheritance**

1. In the GPMC console, select the **Engineers** OU, and examine the precedence and inheritance of GPOs on the **Group Policy Inheritance** tab.
2. Block the inheritance of GPOs to the **Engineers** OU.

Question: What GPOs continue to apply to users in the Engineers OU? Where are those GPOs linked? Why did they continue to apply?

3. Turn off **Block Inheritance** from the **Engineers** OU.

Results: After this exercise, you will have created a GPO called Engineering Application Override, and linked it to the Engineers OU. You will also have an understanding of inheritance, precedence, and the effects of an Enforced link and Block Inheritance..

Exercise 2: Configure GPO Scope with Filtering

As time passes, you discover that only a small number of engineers require the screen saver timeout override that is currently applied to all users in the Engineers OU. In addition, you learn that a small number of users must be exempted from the screen saver timeout policy and other settings configured by the CONTOSO Standards GPO. You decide to use security filtering to manage the scope of the GPOs.

In this exercise, you will modify the scope of GPOs using filtering.

The main tasks for this exercise are as follows:

1. Configure policy application with security filtering.
2. Configure an exemption with security filtering.

► Task 1: Configure policy application with security filtering

1. Run **Active Directory Users and Computers** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. In the **Groups\Configuration** OU, create a global security group named **GPO_Engineering Application Override_Apply**.
3. In the GPMC console, select the **Engineering Application Override** GPO. Notice that in the **Security Filtering** section, the GPO applies by default to all authenticated users.
4. Configure the GPO to apply only to the **GPO_Engineering Application Override_Apply** group.

► **Task 2: Configure an exemption with security filtering**

1. Run **Active Directory Users and Computers** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. In the **Groups\Configuration** OU, create a global security group named **GPO_CONTOSO Standards_Exempt**.
3. In the GPMC console, select the **CONTOSO Standards** GPO. Notice that in the **Security Filtering** section, the GPO applies by default to all authenticated users.
4. Configure the GPO to deny **Apply Group Policy** permission to the **GPO_CONTOSO Standards_Exempt** group.

Results: After this exercise, you will have configured the Engineering Application Override GPO to apply only to the members of GPO_Engineering Application Override_Apply. You will have also configured a group with the Deny Apply Group Policy permission, which overrides the Allow permission. If any user requires exemption from the policies in the CONTOSO Standards GPO, you can simply add the computer to the group GPO_CONTOSO Standards_Exempt..

Exercise 3: Configure Loopback Processing

You have been asked to configure the screen saver timeout in conference rooms to 45 minutes, so that a screen saver does not appear in the middle of a meeting.

In this exercise, you will configure loopback GPO processing.

The main task for this exercise is as follows:

- Configure loopback processing.

► Task 1: Configure loopback processing

1. Create a new GPO named **Conference Room Policies** and link it to the **Kiosks\Conference Rooms** OU.
2. Confirm that the **Conference Room Policies** GPO is scoped to **Authenticated Users**.
3. Modify the **Screen Saver timeout** policy to launch the screen saver after 45 minutes. Modify the **User Group Policy loopback processing mode** policy setting to use **Merge** mode.

Results: After this exercise, you will have created a Conference Room Policies GPO that applies a 45-minute screen saver timeout to users when they log on to conference room computers..



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs.

Lab Review Questions

Question: Many organizations rely heavily on security group filtering to scope GPOs, rather than linking GPOs to specific OUs. In these organizations, GPOs are typically linked very high in the Active Directory logical structure: to the domain itself or to a first-level OU. What advantages are gained by using security group filtering rather than GPO links to manage the scope of the GPO?

Question: Why might it be useful to create an exemption group—a group that is denied the Apply Group Policy permission—for every GPO that you create?

Question: Do you use loopback policy processing in your organization? In what scenarios and for what policy settings can loopback policy processing add value?

Lab D: Troubleshoot Policy Application

- Exercise 1: Perform RSoP Analysis
- Exercise 2: Use the Group Policy Modeling Wizard
- Exercise 3: View Policy Events

Logon information

Virtual machine	6425B-HQDC01-A	6425B-DESKTOP101-A
Logon user name	Pat.Coleman	Pat.Coleman
Administrative user name	Pat.Coleman_Admin	
Password	Pa\$\$w0rd	Pa\$\$w0rd

Estimated time: 30 minutes

Scenario

You are responsible for administering and troubleshooting the Group Policy infrastructure at Contoso, Ltd. You want to evaluate the resultant set of policies for users in your environment in order to ensure that the Group Policy infrastructure is healthy, and that all policies are applied as they were intended.

Exercise 1: Perform RSoP Analysis

In this exercise, you will evaluate resultant set of policy using both the Group Policy Results Wizard and the GPResults command.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Refresh Group Policy.
3. Create a Group Policy results RSoP report.
4. Analyze RSoP with GPResults.

► Task 1: Prepare for the lab

The virtual machines should already be started and available after completing Labs A, B and C. However, if they are not, you should complete the below steps then step through the exercises in Labs A, B and C before continuing.

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Start 6425B-DESKTOP101-A.
4. Log on to DESKTOP101 as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 2: Refresh Group Policy

1. Run the command prompt as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Run the command **gpupdate /force**. After the command has completed, make a note of the current system time, which you will need to know for a task later in this lab.
3. Restart DESKTOP101 and wait for it to restart before proceeding with the next task.

► **Task 3: Create a Group Policy results RSoP report**

1. On HQDC01, run **Group Policy Management** console as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Use the **Group Policy Results Wizard** to run an RSoP report for **Pat.Coleman** on DESKTOP101.
3. Review the **Group Policy Summary** results. For both user and computer configuration, identify the time of the last policy refresh and the list of allowed and denied GPOs. Identify the components that were used to process policy settings.
4. Click the **Settings** tab. Review the settings that were applied during user and computer policy application, and identify the GPO from which the settings were obtained.
5. Click the **Policy Events** tab, and locate the event that logs the policy refresh you triggered with the **GPUpdate** command in Task 1.
6. Click the **Summary** tab, right-click the page, and choose **Save Report**. Save the report as an HTML file to drive D with a name of your choice. Then open the RSoP report from drive D.

► **Task 4: Analyze RSoP with GPREsults**

1. Log on to DESKTOP101 as **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Run the command prompt with administrative credentials.
3. Type **gpresult /r** and press ENTER.
RSoP summary results are displayed. The information is very similar to the Summary tab of the RSoP report produced by the Group Policy Results Wizard.
4. Type **gpresult /v** and press ENTER.
A more detailed RSoP report is produced. Notice that many of the Group Policy settings applied by the client are listed in this report.
5. Type **gpresult /z** and press ENTER.
The most detailed RSoP report is produced.

6. Type **gpresult /h:"%userprofile%\Desktop\RSOP.html"** and press ENTER.
An RSoP report is saved as an HTML file to your desktop.
7. Open the saved RSoP report from your desktop.
8. Compare the report, its information, and its formatting to the RSoP report you saved in the previous task.

Results: After this exercise, you will have learned how to do a resultant set of policy two ways, using a wizard and from the command line.

Exercise 2: Use the Group Policy Modeling Wizard

Before you roll out the Conference Room Policies GPO for production use, you want to evaluate the effect it will have on users who log on to conference room computers. In this exercise, you will use the Group Policy Modeling Wizard to model the resultant set of policies applied to a user, Mike Danseglio, if he were to log on to a conference room computer, DESKTOP101.

The main task for this exercise is as follows:

- Perform Group Policy results modeling.

► Task 1: Perform Group Policy results modeling

1. Switch to HQDC01.
2. In the Group Policy Management console tree, expand **Forest:Contoso.com**, and then click **Group Policy Modeling**.
3. Right-click **Group Policy Modeling**, and then click **Group Policy Modeling Wizard**.

The Group Policy Modeling Wizard appears.

4. Click **Next**.
5. On the **Domain Controller Selection** page, click **Next**.
6. On the **User And Computer Selection** page, in the **User Information** section, click the **User** option button, and then click **Browse**.

The Select User dialog box appears.

7. Type **Mike.Danseglio** and then press ENTER.
8. In the **Computer Information** section, click the **Computer** option button, and then click **Browse**.

The Select Computer dialog box appears.

9. Type **DESKTOP101** and then press ENTER.
10. Click **Next**.

11. On the **Advanced Simulation Options** page, select the **Loopback Processing** check box and then click **Merge**.

Even though the Conference Room Policies GPO specifies the loopback processing, you must instruct the Group Policy Modeling Wizard to consider loopback processing in its simulation.

12. Click **Next**.
13. On the **Alternate Active Directory Paths** page, click the **Browse** button next to **Computer location**.

The Choose Computer Container dialog box appears.

14. Expand **contoso.com** and **Kiosks**, and then click **Conference Rooms**.

You are simulating the effect of DESKTOP101 as a conference room computer.

15. Click **OK**.
16. Click **Next**.
17. On the **User Security Groups** page, click **Next**.
18. On the **Computer Security Groups** page, click **Next**.
19. On the **WMI Filters for Users** page, click **Next**.
20. On the **WMI Filters for Computers** page, click **Next**.
21. Review your settings on the **Summary of Selections** page, and then click **Next**.
22. Click **Finish**.
23. On the **Summary** tab, scroll to and expand, if necessary, **User Configuration**, **Group Policy Objects**, and **Applied GPOs**.
24. Will the **Conference Room Policies** GPO apply to Mike Danseglio as a User policy when he logs on to DESKTOP101 if DESKTOP101 is in the Conference Rooms OU?

If not, check the scope of the Conference Room Policies GPO. It should be linked to the Conference Rooms OU with security group filtering that applies the GPO to the Authenticated Users special identity. You can right-click the modeling query to rerun the query. If the GPO is still not applying, try deleting and re-building the Group Policy Modeling report, and be very careful to follow each step precisely.

25. Click the **Settings** tab.

26. Scroll to, and expand if necessary, **User Configuration, Policies, Administrative Templates** and **Control Panel/Display**.
27. Confirm that the screen saver timeout is 2700 seconds (45 minutes), the setting configured by the **Conference Room Policies** GPO that overrides the 10-minute standard configured by the **CONTOSO Standards** GPO.

Results: After this exercise, you will have used the Group Policy Modeling Wizard to confirm that the Conference Room Policies GPO will in fact apply its settings to users logging on to conference room computers..

Exercise 3: View Policy Events

As a client performs a policy refresh, Group Policy components log entries to the Windows event logs. In this exercise, you will locate and examine Group Policy-related events.

The main task for this exercise is as follows:

- View policy events.

► Task 1: View policy events

1. On DESKTOP101, where you are logged on as **Pat.Coleman_Admin**, run Event Viewer as an administrator.
2. Locate and review **Group Policy** events in the **System** log.
3. Locate and review **Group Policy** events in the **Application** log.
4. In the **Group Policy Operational** log, locate the first event related in the **Group Policy** refresh you initiated in Exercise 1, with the **GPUpdate** command. Review that event and the events that followed it.

Results: After this exercise, you will have identified Group Policy events in the event logs.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: In what situations have you used RSoP reports to troubleshoot Group Policy application in your organization?

Question: In what situations have you used, or could you anticipate using, Group Policy modeling?

Question: Have you ever diagnosed a Group Policy application problem based on events in one of the event logs?

Module 7

Lab Instructions: Manage Enterprise Security and Configuration with Group Policy Settings

Contents:

Lab A: Delegate the Support of Computers	
Exercise 1: Configure the Membership of Administrators by Using Restricted Groups Policies	3
Lab B: Manage Security Settings	
Exercise 1: Manage Local Security Settings	7
Exercise 2: Create a Security Template	10
Exercise 3: Use Security Configuration and Analysis	11
Exercise 4: Use the Security Configuration Wizard	15
Lab C: Manage Software with GPSI	
Exercise 1: Deploy Software with GPSI	20
Exercise 2: Upgrade Applications with GPSI	23
Lab D: Audit File System Access	
Exercise 1: Configure Permissions and Audit Settings	26
Exercise 2: Configure Audit Policy	28
Exercise 3: Examine Audit Events	29

Lab A: Delegate the Support of Computers

- **Exercise 1: Configure the Membership of Administrators by Using Restricted Groups Policies**

Logon information

Virtual machine	6425B-HQDC01-A	6425B-DESKTOP101-A
Logon user name	Pat.Coleman	Do not Logon
Administrative user name	Pat.Coleman_Admin	
Password	Pa\$\$w0rd	

Estimated time: 15 minutes

Scenario

You have been asked by the corporate security team to lock down the membership of the Administrators group on client computers. However, you need to provide the centralized help desk with the ability to perform support tasks for users throughout the organization. Additionally, you must empower the local site desktop support team to perform administrative tasks for client computers in that site.

Exercise 1: Configure the Membership of Administrators by Using Restricted Groups Policies

In this exercise, you will use Group Policy to delegate the membership of the Administrators group. You will first create a GPO with a restricted groups policy setting that ensures that the Help Desk group is a member of the Administrators group on all client systems. You will then create a GPO that adds the SEA Support group to Administrators on clients in the SEA OU. Finally, you will confirm that in the SEA OU, both the Help Desk and SEA Support groups are administrators.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Delegate the administration of all clients in the domain.
3. Create a Seattle Support group.
4. Delegate the administration of a subset of clients in the domain.
5. Confirm the cumulative application of Member Of policies.

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A.
2. Log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Start 6425B-DESKTOP101-A but do not log on to the system.

► Task 2: Delegate the administration of all clients in the domain

1. Run **Group Policy Management** as an administrator, with the username **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Create a **GPO** named **Corporate Help Desk**, scoped to all computers in the Client Computers OU.
3. Configure a **Restricted Groups** policy setting that ensures that the Help Desk group is a member of the Administrators group on all client systems.

► **Task 3: Create a Seattle Support group**

1. Run **Active Directory Users and Computers** as an administrator, with the username **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. In the **Groups\Role** OU, create a global security group called **SEA Support**.
3. Close Active Directory Users and Computers.

► **Task 4: Delegate the administration of a subset of clients in the domain**

1. In **Group Policy Management**, create a GPO named **Seattle Support**, scoped to all computers in the Client Computers\SEA OU.
2. Configure a **Restricted Groups** policy setting that ensures that the SEA Support group is a member of the Administrators group on all client systems in the SEA OU.

► **Task 5: Confirm the cumulative application of Member Of policies**

- Use **Group Policy Modeling** to confirm that a computer in the SEA OU will include both the Help Desk and SEA Support groups in its Administrators group.

Results: After this exercise, you will have created a Corporate Help Desk GPO that ensures that the Help Desk group is a member of the local Administrators group on all computers in the Client Computers OU. Additionally, you will have created a Seattle Support GPO that adds the Seattle Support group to the local Administrators group on all client computers in the SEA OU.



Important: Do not shut down the virtual machine once you are finished with this lab as the settings you have configured here will be used in subsequent labs.

Lab Review Question

Question: If you wanted to ensure that the *only* members of the local Administrators group on a client computer were the Help Desk in the site-specific Support group, and to remove any other members from the local Administrators group, how would you achieve that using only restricted groups policies?

Lab B: Manage Security Settings

- Exercise 1: Manage Local Security Settings
- Exercise 2: Create a Security Template
- Exercise 3: Use Security Configuration and Analysis
- Exercise 4: Use the Security Configuration Wizard

Logon information

Virtual machine	6425B-HQDC01-A
Logon user name	Pat.Coleman
Administrative user name	Pat.Coleman_Admin
Password	Pa\$\$w0rd

Estimated time: 30 minutes

Scenario

You are an administrator of the contoso.com domain. As part of your effort to secure the directory service, you want to establish a security configuration to apply to domain controllers that, among other things, specifies who can log on to domain controllers using Remote Desktop to perform administrative tasks.

Exercise 1: Manage Local Security Settings

In this exercise, you will create a group that allows you to manage who is allowed to log on to HQDC01, a domain controller, using Remote Desktop. You will do so by configuring security settings directly on HQDC01.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Enable Remote Desktop on HQDC01.
3. Create a global security group named SYS_DC Remote Desktop.
4. Add SYS_DC Remote Desktop to the Remote Desktop Users group.
5. Configure the Local Security Policy to allow remote desktop connections by SYS_DC Remote Desktop.
6. Revert the local security policy to its default setting.

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 2: Enable Remote Desktop on HQDC01

1. Run **Server Manager** as an administrator, with the username **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. In the **Server Summary** section, click **Configure Remote Desktop**, and then click **Allow connections only from computers running Remote Desktop with Network Level Authentication** (more secure).
3. Close Server Manager.

► Task 3: Create a global security group named SYS_DC Remote Desktop

1. Run **Active Directory Users and Computers** as an administrator, with the username **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. In the **Admins\Admin Groupsp\Server Delegation** OU, create a global security group named **SYS_DC Remote Desktop**.

► **Task 4: Add SYS_DC Remote Desktop to the Remote Desktop Users group**

To connect using Remote Desktop, a user must have the user logon right to log on through Terminal Services, which you will grant to the SYS_DC Remote Desktop group in the next task.

Additionally, the user must have permission to connect to the RDP-Tcp connection. By default, the Remote Desktop Users group and the Administrators group have permission to connect to the RDP-Tcp connection. Therefore, you should add the user (or the SYS_DC Remote Desktop group in this case) to the Remote Desktop Users group.

1. Add the **SYS_DC Remote Desktop** group to the **Remote Desktop Users** group, found in the **Builtin** container.
2. Close Active Directory Users and Computers.



Note: Instead of adding the group to Remote Desktop Users, you could add the SYS_DC Remote Desktop group to the access control list (ACL) of the RDP-Tcp connection, using the Terminal Services Configuration console. Right-click RDP-Tcp and choose Properties; then click the Security tab, click the Add button, and type SYS_DC Remote Desktop. Click OK twice to close the dialog boxes.

► **Task 5: Configure the Local Security Policy to allow Remote Desktop connections by SYS_DC Remote Desktop**

On a domain member (workstation or server), the Remote Desktop Users group has permission to connect to the RDP-Tcp connection and has the user right to log on through Terminal Services. Therefore, on a domain member server or workstation, the easiest way to manage both the user right and the permission on RDP-Tcp connection is to add a user or group directly to the Remote Desktop Users group.

Because HQDC01 is a domain controller, only Administrators has the right to log on with Terminal Services. Therefore, you must explicitly grant the SYS_DC Remote Desktop group the user logon right to log on through Terminal Services.

- Run **Local Security Policy** as an administrator, with the username **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
- Modify the configuration of the user rights policy setting, **Allow Log On Through Terminal Services**, and add **SYS_DC Remote Desktop**.

► **Task 6: Revert the local security policy to its default setting**

You will now revert the policy to its default in preparation for following Exercises.

1. Modify the configuration of the user rights policy setting, **Allow Log On Through Terminal Services**, and then remove **SYS_DC Remote Desktop**.
2. Close Local Security Policy.

Results: After this exercise, you should have configured each of the local settings necessary to allow SYS_DC Remote Desktop to log on to HQDC01 using remote desktop.

Exercise 2: Create a Security Template

In this exercise, you will create a security template that gives the SYS_DC Remote Desktop group the right to log on using Remote Desktop.

The main tasks for this exercise are as follows:

1. Create a custom MMC console with the Security Templates snap-in.
2. Create a security template.

► Task 1: Create a custom MMC console with the Security Templates snap-in

1. Run **mmc.exe** as an administrator, with the username **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Add the **Security Templates** snap-in.
3. Save the console as **D:\Security Management.msc**.

► Task 2: Create a security template

1. In the **Security Templates** snap-in, create a new security template named **DC Remote Desktop**.
2. Modify the configuration of the user rights policy setting, **Allow log on through Terminal Services**, and then add **SYS_DC Remote Desktop**.
3. Using a **Restricted Groups** setting, configure the template to give **SYS_DC Remote Desktop** to the **Remote Desktop Users** group.
4. Save the changes you made to the template.

Results: After this exercise, you will have configured a security template named DC Remote Desktop that adds the SYS_DC Remote Desktop group to the Remote Desktop Users group, and gives the SYS_DC Remote Desktop group the user logon right to log on through Terminal Services.

Exercise 3: Use Security Configuration and Analysis

In this exercise, you will analyze the configuration of HQDC01, using the DC Remote Desktop security template to identify discrepancies between the server's current configuration and the desired configuration defined in the template. You will then create a new security template.

The main tasks for this exercise are as follows:

1. Add the Security Configuration and Analysis snap-in to a custom console.
2. Create a security database and import a security template.
3. Analyze the configuration of a computer using the security database.
4. Configure security settings using a security database.

► **Task 1: Add the Security Configuration And Analysis snap-in to a custom console**

- Add the **Security Configuration and Analysis** snap-in to a custom console and save the change to the console.

► **Task 2: Create a security database and import a security template**

- Create a new security database called **HQDC01Test**.
- Import the **DC Remote Desktop** security template.

► **Task 3: Analyze the configuration of a computer by using the security database**

1. In the console tree, right-click **Security Configuration and Analysis**, and then click **Analyze Computer Now**.
2. Click **OK** to confirm the default path for the error log.
The snap-in performs the analysis.
3. In the console tree, expand **Security Configuration and Analysis** and **Local Policies**, and then click **User Rights Assignment**.

Notice that the Allow log on through Terminal Services policy is flagged with a red circle and an X. This indicates a discrepancy between the database setting and the computer setting.

4. Double-click **Allow log on through Terminal Services**.

Notice the discrepancies. The computer is not configured to allow the SYS_DC Remote Desktop Users group to log on through Terminal Services.

Notice also that the Computer setting currently allows Administrators to log on through Terminal Services. This is an important setting that should be incorporated into the database.

5. Confirm that the **Define this policy in the database** check box is selected.
6. Select the **Administrators** check box, under **Database Setting**.

This will add the right for Administrators to log on through Terminal Services to the database. It does not change the template, and it does not affect the current configuration of the computer.

7. Click **OK**.
8. In the console tree, select **Restricted Groups**.
9. In the details pane, double-click **CONTOSO\SYS_DC Remote Desktop**.
10. Click the **Member Of** tab.

Notice that the database specifies that the SYS_DC Remote Desktop group should be a member of Remote Desktop Users, but the computer is not currently in compliance with that setting.

11. Confirm that the **Define this group in the database** check box is selected.
12. Click **OK**.
13. Right-click **Security Configuration and Analysis**, and then click **Save**.

This saves the security database, which includes the settings imported from the template plus the change you made to allow Administrators to log on through Terminal Services.

The hint displayed in the status bar when you hover over the Save command suggests that you are saving the template. That is incorrect. You are saving the database.

14. Right-click **Security Configuration and Analysis**, and then click **Export Template**.

The Export Template To dialog box appears.

15. Select **DC Remote Desktop**, and then click **Save**.

You have now replaced the template created in Exercise 2 with the settings defined in the database of the Security Configuration and Analysis snap-in.

► **Task 4: Configure security settings by using a security database**

1. Close your Security Management console. If you are prompted to save your settings, click **Yes**.

Closing and reopening the console is necessary to refresh fully the settings shown in the Security Templates snap-in.

2. Run **D:\Security Management.msc** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.

3. In the console tree, expand **Security Templates**, **C:\Users\Pat.Coleman_Admin\Documents\Security\Templates**, **DC Remote Desktop**, **Local Policies**, and then click **User Rights Assignment**.

4. In the details pane, double-click **Allow log on through Terminal Services**.

Notice that both the Administrators and SYS_DC Remote Desktop groups are allowed to log on through Terminal Services in the security template.

5. Click **OK**.

6. Right-click **Security Configuration and Analysis**, and then click **Configure Computer Now**.

7. Click **OK** to confirm the error log path. The settings in the database are applied to the server. You will now confirm that the change to the user right was applied.

8. Run **Local Security Policy** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.

9. In the console tree expand **Local Policies**, and then click **User Rights Assignment**.

10. Double-click **Allow Log On Through Terminal Services**.

The Allow Log On Through Terminal Services Properties dialog box opens.

11. Confirm that both **Administrators** and **SYS_DC Remote Desktop** are listed.
The Local Security Policy console displays the actual, current settings of the server.
12. Close the Local Security Policy console.
13. Close your custom Security Management console.

Results: After this exercise, you will have created and applied a security template that gives the SYS_DC Remote Desktop the right to log on through Terminal Services, and adds the group as a member of the Remote Desktop Users group.

Exercise 4: Use the Security Configuration Wizard

In this exercise, you will use the Security Configuration Wizard to create a security policy for domain controllers in the contoso.com domain based on the configuration of HQDC01. You will then convert the security policy into a GPO, which could then be deployed to all domain controllers by using Group Policy.

The main tasks for this exercise are as follows:

1. Create a security policy.
2. Transform a security policy into a Group Policy object.

► Task 1: Create a security policy

1. Run the Security Configuration Wizard, in the Administrative Tools folder, with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. On the **Welcome to the Security Configuration Wizard** page, click **Next**.
3. On the **Configuration Action** page, select **Create a new security policy**, and then click **Next**.
4. On the **Select Server** page, accept the default server name, **HQDC01**, and click **Next**.
5. On the **Processing Security Configuration Database** page, you can optionally click **View Configuration Database** and explore the configuration that was discovered on HQDC01.
6. Click **Next**.
7. On the **Role Based Service Configuration** section introduction page, click **Next**.
8. On the **Select Server Roles** page, you can optionally explore the settings that were discovered on HQDC01, but do not change any settings. Click **Next**.
9. On the **Select Client Features** page, you can optionally explore the settings that were discovered on HQDC01, but do not change any settings. Click **Next**.
10. On the **Select Administration And Other Options** page, you can optionally explore the settings that were discovered on HQDC01, but do not change any settings. Click **Next**.

11. On the **Select Additional Services** page, you can optionally explore the settings that were discovered on HQDC01, but do not change any settings. Click **Next**.
12. On the **Handling Unspecified Services** page, do not change the default setting, **Do not change the startup mode of the service**. Click **Next**.
13. On the **Confirm Service Changes** page, in the **View** list, choose **All Services**.
14. Examine the settings in the **Current Startup Mode** column, which reflect service startup modes on HQDC01, and compare them to the settings in the **Policy Startup Mode** column.
15. In the **View** list, select **Changed Services**.
16. Click **Next**.
17. On the **Network Security** section introduction page, click **Next**.
18. On the **Network Security Rules** page, you can optionally examine the firewall rules derived from the configuration of HQDC01. Do not change any settings. Click **Next**.
19. On the **Registry Settings** section introduction page, click **Next**.
20. On each page of the **Registry Settings** section, examine the settings, but do not change any of them, then click **Next**. When the **Registry Settings Summary** page appears, examine the settings and click **Next**.
21. On the **Audit Policy** section introduction page, click **Next**.
22. On the **System Audit Policy** page, examine but do not change the settings. Click **Next**.
23. On the **Audit Policy Summary** page, examine the settings in the **Current Setting** and **Policy Setting** columns. Click **Next**.
24. On the **Save Security Policy** section introduction page, click **Next**.
25. In the **Security Policy File Name** text box, click at the end of the file path and type **DC Security Policy**.
26. Click the **Include Security Templates** button.
27. Click **Add**.

28. Browse to locate the **DC Remote Desktop** template created in Exercise 3, located in your Documents\Security\Templates folder. When you have located and selected the template, click **Open**.

Be careful that you add the Documents\Security\Templates\DC Remote Desktop.inf file and *not* the DC Security.inf default security template.

29. Click **OK** to close the **Include Security Templates** dialog box.
30. Click the **View Security Policy** button.

You are prompted to confirm the use of the ActiveX control.
31. Click **Yes**.
32. Examine the security policy. Notice that the DC Remote Desktop template is listed in the **Templates** section.
33. Close the window after you have examined the policy.
34. In the Security Configuration Wizard, click **Next**.
35. On the **Apply Security Policy** page, accept the **Apply Later** default setting, and then click **Next**.
36. Click **Finish**.

► **Task 2: Transform a security policy into a Group Policy object**

1. Run the Command Prompt as an administrator, with the username **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Type **cd c:\windows\security\msscw\policies**, and then press ENTER.
3. Type **scwcmd transform /?**, and then press ENTER.
4. Use the **scwcmd.exe** command to transform the security policy named "DC Security Policy.xml" to a GPO named "DC Security Policy".

5. Run **Group Policy Management** as an administrator, with the username **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
6. Examine the settings of the **DC Security Policy GPO**. Confirm that the **BUILTIN\Administrators** and **CONTOSO\SYS_DC Remote Desktop** groups are given the **Allow log on through Terminal Services** user right. Also confirm that the **CONTOSO\SYS_DC Remote Desktop** group is a member of **BUILTIN\Remote Desktop Users**.

Results: After this exercise, you will have used the Security Configuration Wizard to create a security policy named DC Security Policy, and transformed the security policy to a Group Policy object named DC Security Policy.



Important: Do not shut down the virtual machine once you are finished with this lab as the settings you have configured here will be used in subsequent labs

Lab Review Question

Question: Describe the relationship between security settings on a server, Local Group Policy, security templates, the database used in Security Configuration And Analysis, the security policy created by the Security Configuration Wizard, and domain-based Group Policy.

Lab C: Manage Software with GPSI

- Exercise 1: Deploy Software with GPSI
- Exercise 2: Upgrade Applications with GPSI

Logon information

Virtual machine	6425B-HQDC01-A	6425B-DESKTOP101-A	6425B-SERVER01-A
Logon user name	Pat.Coleman	Pat.Coleman	Do not Logon
Administrative user name	Pat.Coleman_Admin		
Password	Pa\$\$w0rd	Pa\$\$w0rd	

Estimated time: 15 minutes

Scenario

You are an administrator at Contoso, Ltd. Your developers require XML Notepad to edit XML files, and you want to automate the deployment and life cycle management of the application. You decide to use Group Policy Software Installation. Most applications are licensed per computer, so you will deploy XML Notepad to the developers' computers, rather than associating the application with their user accounts.

Exercise 1: Deploy Software with GPSI

In this exercise, you will use GPSI to deploy XML Notepad to computers including DESKTOP101.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Create a software distribution folder.
3. Create a software deployment GPO.
4. Deploy software to computers.
5. Confirm the successful deployment of software.

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A and log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.
2. Start 6425B-SERVER01-A but do not log on.
3. Wait for both SERVER01 to finish startup before continuing with the next task.

► Task 2: Create a software distribution folder

1. On HQDC01, run **Active Directory Users and Computers** as an administrator, with the username **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. In the **Groups\Application** OU, create a new global security group named **APP_XML Notepad**.
3. In the **Servers\File** OU, right-click **SERVER01**, and then click **Manage**.
4. Use the **Shared Folders** snap-in to create a new shared folder, **C:\Software**, with a share name of **Software**. Configure the NTFS permissions as described below:
 - System::Allow::Full Control
 - Administrators::Allow::Full Control

And configure the Share permission such that the Everyone group is allowed Full Control.

Security management best practice is to configure least privilege permissions in the ACL of the resource, which will apply to users regardless of how users connect to the resource, at which point you can use the Full Control permission on the SMB shared folder. The resultant access level will be the more restrictive permissions defined in the ACL of the folder.

5. Open the administrative share for the C drive on SERVER01 (\\SERVER01\\c\$) as **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
6. Inside the **Software** folder on SERVER01, create a folder called **XML Notepad**.
7. Add permission to the **XML Notepad** folder so that the **APP_XML Notepad** group is allowed **Read & Execute permission**.
8. Copy **XML Notepad.msi** from **D:\\Labfiles\\Lab07b** to **\\SERVER01\\c\$\\Software\\XML Notepad**.
9. Close any opened Windows Explorer windows.
10. Close the Computer Management console.

► **Task 3: Create a software deployment GPO**

1. Run **Group Policy Management** as an administrator, with the username **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. In the **Group Policy Objects** container, create a new GPO called **XML Notepad**. Edit that GPO.
3. Expand **Computer Configuration, Policies, Software Settings**, and then click **Software Installation**.
4. Right-click **Software Installation**, point to **New**, and then click **Package**.
5. In the **File name** text box, type the network path to the software distribution folder, **\\server01\\software\\XML Notepad**, and then press ENTER.
6. Select the Windows Installer package, **XmlNotepad.msi**; and then click **Open**.
After a few moments, the Deploy Software dialog box appears.
7. Click **Advanced**, and then click **OK**.
8. On the **General** tab, note that the name of the package includes the version, **XML Notepad 2007**.

9. Click the **Deployment** tab.

Note that when deploying software to computers, Assigned is the only option. Examine the options that would be available if you were assigning or publishing the application to users.

10. Select **Uninstall This Application When It Falls Out Of The Scope Of Management**.
11. Click **OK**.
12. Close the Group Policy Management Editor.
13. Scope the GPO to apply only to members of APP_XML Notepad, and not to Authenticated Users.
14. Link the GPO to the **Client Computers** OU.

► **Task 4: Deploy software to computers**

1. Add **DESKTOP101** to the **APP_XML Notepad** group.
2. Start 6425B-DESKTOP101-A, but do not log on.

► **Task 5: Confirm the successful deployment of software**

1. Log on to DESKTOP101 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
2. Confirm that **XML Notepad** installed successfully.



Note: When verifying the deployment of the xml notepad and it may take two startups to be successful. I.e. if you do not see Notepad installed restart the virtual machine. You may need to do this a couple of times.

Results: After this exercise, you will have deployed XML Notepad to DESKTOP101.

Exercise 2: Upgrade Applications with GPSI

In this exercise, you will simulate deploying an upgraded version of XML Notepad.

The main task for this exercise is as follows:

- Create an upgrade package using GPSI.

► Task 1: Create an upgrade package by using GPSI

1. Switch to HQDC01.
2. In the Group Policy Management console tree, right-click the **XML Notepad** GPO in the **Group Policy Objects** container, and then click **Edit**.
The Group Policy Management Editor opens.
3. In the console tree, expand **Computer Configuration, Policies, Software Settings**, and then click **Software Installation**.
4. Right-click **Software Installation**, point to **New**, and then click **Package**.
5. In the **File name** text box, type the network path to the software distribution folder, **\\server01\software\XML Notepad**, and then press ENTER.
This exercise will use the existing XmlNotepad.msi file as if it is an updated version of XML Notepad.
6. Select the Windows Installer package, **XmlNotepad.msi**, and then click **Open**.
The Deploy Software dialog box appears.
7. Click **Advanced**, and then click **OK**.
8. On the **General** tab, change the name of the package to suggest that it is the next version of the application. Type **XML Notepad 2010**.
9. Click the **Deployment** tab. Because you are deploying the application to computers, Assigned is the only deployment type option.
10. Click the **Upgrades** tab.
11. Click the **Add** button.
12. Click the **Current Group Policy Object (GPO)** option.
13. In the **Package to upgrade** list, select the package for the simulated earlier version, **XML Notepad 2007**.

14. Click the **Uninstall the existing package and then select then install the upgrade package** option.
15. Click **OK**.
16. Click **OK**.

If this were an actual upgrade, the new package would upgrade the previous version of the application as clients applied the XML Notepad GPO. Because this is only a simulation of an upgrade, you can remove the simulated upgrade package.

17. Right-click **XML Notepad 2010**, which you just created to simulate an upgrade, point to **All Tasks**, and then select **Remove**.
18. In the **Remove Software** dialog box, click **Immediately uninstall the software from users and computers**, and then click **OK**.

Results: After this exercise, you will have simulated an upgrade of XML Notepad by using GPSI.



Important: Do not shut down the virtual machine once you are finished with this lab as the settings you have configured here will be used in subsequent labs.

Lab Review Questions

Question: Consider the NTFS permissions you applied to the Software and XML Notepad folders on SERVER01. Explain why these least privilege permissions are preferred to the default permissions.

Question: Consider the methods used to scope the deployment of XML Notepad: Assigning the application to computers, filtering the GPO to apply to the APP_XML Notepad group that contains only computers, and linking the GPO to the Client Computers OU. Why is this approach advantageous for deploying most software? What would be the disadvantage of scoping software deployment to users rather than to computers?

Lab D: Audit File System Access

- Exercise 1: Configure Permissions and Audit Settings
- Exercise 2: Configure Audit Policy
- Exercise 3: Examine Audit Events

Logon information

Virtual machine	6425B-HQDC01-A	6425B-DESKTOP101-A	6425B-SERVER01-A
Logon user name	Pat.Coleman	Pat.Coleman and Mike.Danseglio	Pat.Coleman
Administrative user name	Pat.Coleman_Admin		Pat.Coleman_Admin
Password	Pa\$\$w0rd	Pa\$\$w0rd	Pa\$\$w0rd

Estimated time: 30 minutes

Scenario

In this Lab, you will configure auditing settings, enable audit policies for object access, and filter for specific events in the Security log. The business objective is to monitor a folder containing confidential data that should not be accessed by users in the Consultants group.

Exercise 1: Configure Permissions and Audit Settings

In this exercise, you will configure permissions on the Confidential Data folder to deny access to consultants. You will then enable auditing of attempts by consultants to access the folder.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Create and secure a shared folder.
3. Configure auditing settings on a folder.

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A and log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.
2. Start 6425B-SERVER01-A but do not log on.
3. Start 6425B-DESKTOP101-A but do not log on.
4. Wait for all virtual machines to complete startup before continuing to the next task.

► Task 2: Create and secure a shared folder

1. Switch to HQDC01.
2. Run **Active Directory Users and Computers** as an administrator, with the username **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
3. In the **Groups\Role** OU, create a new global security group named **Consultants**.
4. Add **Mike.Danseglio** to the **Consultants** group.
5. Create a new folder in **\\server01\c\$\data** called **Confidential Data**.
6. Configure NTFS permissions that deny the **Consultants** group all access to the folder.

► **Task 3: Configure auditing settings on a folder**

- Configure auditing settings on the **Confidential Data** folder to audit for any failed access by the Consultants group.

Exercise 2: Configure Audit Policy

In this exercise, you will enable auditing of file system access on file servers using Group Policy.

The main tasks for this exercise are as follows:

- Enable auditing of file system access using Group Policy.

► Task 1: Enable auditing of file system access by using Group Policy

1. Run **Group Policy Management** as an administrator, with the username **Pat.Coleman_Admin** and the password **Pa\$\$wOrd**.
2. Create a new GPO named **File Server Auditing**.
3. Configure the GPO to audit for failed object access.
4. Link the GPO to the Servers\File OU.

Results: After this exercise, you will have configured for auditing of failed access to file system objects on servers in the Servers\File OU.

Exercise 3: Examine Audit Events

In this exercise, you will generate audit failure events and then examine the resulting security event log messages.

The main tasks for this exercise are as follows:

1. Generate audit events.
2. Examine audit event log messages.

► Task 1: Generate audit events

1. Log on to SERVER01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
2. Run the Command Prompt as an administrator, with the username **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
3. Refresh **Group Policy** to apply the new auditing settings by executing the command **gpupdate.exe /force**.
4. Log off of SERVER01.
5. Log on to DESKTOP101 as **Mike.Danseglio** with the password **Pa\$\$w0rd**.
6. Attempt to open **\\server01\data\Confidential Data**. You will receive an Access Denied message.

► Task 2: Examine audit event log messages

1. Switch to SERVER01.
2. Run **Event Viewer** as an administrator, with the username **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
3. Locate the audit failure events related to Mike Danseglio's access to the **Confidential Data** folder.

Question: What is the Task Category for the event? What is the Event ID? What type of access was attempted?

Results: After this exercise, you will have validated the auditing of failed access to the Confidential Data folder by members of the Consultants group..



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: What are the three major steps required to configure auditing of file system and other object access?

Question: What systems should have auditing configured? Is there a reason not to audit all systems in your enterprise? What types of access should be audited, and by whom should they be audited? Is there a reason not to audit all access by all users?

Module 8

Lab Instructions: Secure Administration

Contents:

Lab A: Delegate Administration

Exercise 1: Delegate Permission to Create and Support User Accounts 3

Exercise 2: View Delegated Permissions 6

Exercise 3: Remove and Reset Permissions 8

Lab B: Audit Active Directory Changes

Exercise 1: Audit Changes to Active Directory by Using Default Audit Policy 11

Exercise 2: Audit Changes to Active Directory by Using Directory Service
Changes Auditing 13

Lab A: Delegate Administration

- Exercise 1: Delegate permission to create and support user accounts
- Exercise 2: View delegated permissions
- Exercise 3: Remove and reset permissions

Logon information

Virtual machine	6425B-HQDC01-A
Logon user name	Pat.Coleman
Administrative user name	Pat.Coleman_Admin
Password	Pa\$\$w0rd

Estimated time: 15 minutes

Scenario

The enterprise security team at Contoso has asked you to lock down the administrative permissions delegated to support personnel.

Exercise 1: Delegate Permission to Create and Support User Accounts

In this exercise, you will delegate to the help desk permission to unlock user accounts, reset passwords, and require users to change passwords at the next logon. This permission will scope only to standard user accounts and will not allow the help desk to change passwords of administrative accounts. You will also delegate permission to the User Account Admins group to create and delete user accounts, as well as full control over user accounts.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Create security groups for role-based management.
3. Delegate control of user support with the Delegation of Control Wizard.
4. Delegate permission to create and delete users with the Access Control List Editor interface.
5. Validate the implementation of delegation.

► Task 1: Prepare for the lab 1. Start 6425B-HQDC01-A

1. Log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.
2. Run **D:\Labfiles\Lab08a\Lab08a_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.

► Task 2: Create security groups for role-based management

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the **Groups\Role** OU, create the following role groups:
 - **Help Desk** (global security group)
 - **User Account Admins** (global security group)

3. Add the following users' *administrative accounts* to the **Help Desk** group. Be careful not to add the users' standard, non-privileged account.
 - **Aaron Painter**
 - **Elly Nkya**
 - **Julian Price**
 - **Holly Dickson**
4. Add the following users' *administrative accounts* to the **User Account Admins** group. Be careful not to add the users' standard, non-privileged account.
 - **Pat Coleman**
 - **April Meyer**
 - **Max Stevens**
5. In the **Admins\Admin Groups\AD Delegations** OU, create the following administrative access management groups:
 - **AD_User Accounts_Support** (domain local security group).
 - **AD_User Accounts_Full Control** (domain local security group).
6. Add the **Help Desk** as a member of **AD_User Accounts_Support**.
7. Add **User Account Admins** as a member of **AD_User Accounts_Full Control**.

► **Task 3: Delegate control of user support with the Delegation Of Control Wizard**

- Right-click the **User Accounts** OU and then click **Delegate Control**. Delegate to the **AD_User Accounts_Support** group the right to reset user passwords and force users to change passwords at next logon.

► **Task 4: Delegate permission to create and delete users with the Access Control List Editor interface**

1. Turn on the **Advanced Features** view of the **Active Directory Users and Computers** snap-in.
2. Right-click the **User Accounts** OU, and then click **Properties**. Click the **Security** tab, and then click **Advanced**.
3. Add permissions that give **AD_User Accounts_Full Control** the ability to create and delete users, and also gives the group full control over user objects. Be careful to limit the **Full Control** permission to user objects only.

► **Task 5: Validate the implementation of delegation**

1. Close Active Directory Users and Computers.
2. Run **Active Directory Users and Computers** as an administrator, with the username **Aaron.Painter_Admin** and the password **Pa\$\$w0rd**.
3. Confirm that you can reset the password for **Jeff Ford**, in the **Employees** OU, and that you can force him to change his password at the next logon.
4. Confirm that you cannot disable Jeff Ford's account.
5. Confirm that you cannot reset the password for **Pat Coleman (Admin)** in the **Admin Identities** OU.
6. Close Active Directory Users and Computers.
7. Run **Active Directory Users and Computers** as an administrator, with the username **April.Meyer_Admin** and the password **Pa\$\$w0rd**.
8. Confirm that you can create a user account in the **Employees** OU by creating an account with your own first and last name, the user name First.Last, and the password **Pa\$\$w0rd**.
9. Close Active Directory Users and Computers.

Results: After this exercise, you will have delegated to the help desk permission to unlock user accounts, reset passwords, and force users to change passwords at next logon, through the help desk's membership in the AD_User Accounts_Support group. You have also delegated full control of user objects to User Account Admins, through its membership in the AD_User Accounts_Full Control group. And you have tested both delegations to validate their functionality.

Exercise 2: View Delegated Permissions

In this exercise you will view, report, and evaluate the permissions that have been assigned to Active Directory objects.

The main tasks for this exercise are as follows:

1. View permissions in the Access Control List Editor interfaces.
2. Report permissions using DSACLs.
3. Evaluate effective permissions.

► Task 1: View permissions in the Access Control List Editor interfaces

1. Run **Active Directory Users and Computers** as an administrator, with the username **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Right-click the **User Accounts** OU, and then click **Properties**. Click the **Security** tab, and then click **Advanced**.
3. Sort so that permissions are displayed according to the group to which they are assigned.

Question: How many permission entries were created for the AD_User Accounts_Support group by the Delegation Of Control Wizard? Is it easy to tell what permissions were assigned in the Permission Entries list? List the permissions assigned to AD_User Accounts_Support.

► **Task 2: Report permissions using DSACLs**

- From the command prompt, use DSACLs to report the permissions assigned to the **User Accounts** OU. Type the command:

```
dsac1s "ou=User Accounts,dc=contoso,dc=com"
```

and then press ENTER.

Question: What permissions are reported for AD_User Accounts_Support by the DSACLs command?

► **Task 3: Evaluate effective permissions**

1. Right-click the **User Accounts** OU, and then click **Properties**. Click the **Security** tab, and then click **Advanced**.
2. Using the **Advanced Security Settings** dialog box, evaluate the **Effective Permissions** for **April.Meyer_Admin**. Locate the permissions that allow her to create and delete users.

Question: Do you see the Reset Password in this list?

3. In the **Employees** OU, right-click the user account for **Aaron Lee**, and then click **Properties**. Click the **Security** tab, and then click **Advanced**.
4. Using the **Advanced Security Settings** dialog box, evaluate the **Effective Permissions** for **Aaron.Painter_Admin**. Locate the permissions that allow him to reset the password for **Aaron Lee**.

Results: After this exercise, you will have confirmed that the permissions you assigned in the previous exercise were applied successfully.

Exercise 3: Remove and Reset Permissions

In this exercise, you will remove delegated permissions and will reset an OU to its schema-defined default ACL.

The main tasks for this exercise are as follows:

1. Remove permissions assigned to AD_User Accounts_Support.
2. Reset the User Accounts OU to its default permissions.

► **Task 1: Remove permissions assigned to AD_User Accounts_Support**

1. Right-click the **User Accounts** OU, and then click **Properties**. Click the **Security** tab, and then click **Advanced**.
2. Sort so that permissions are displayed according to the group to which they are assigned.
3. Remove the permissions assigned to **AD_User Accounts_Support**.

► **Task 2: Reset the User Accounts OU to its default permissions**

1. Right-click the **User Accounts** OU, and then click **Properties**. Click the **Security** tab, and then click **Advanced**.
2. Click **Restore defaults**, and then click **Apply**.

Question: What do you achieve by clicking Reset To Default? What permissions remain?

Results: After this exercise, you will have reset the permissions on the User Accounts OU to its schema-defined defaults.



Note: Do not shut down the virtual machine once you are finished with this lab as the settings you have configured here will be used in the subsequent lab.

Lab Review Questions

Question: How does Active Directory Users and Computers indicate to you that you do not have permissions to perform a particular administrative task?

Question: When you evaluated effective permissions for April Meyer on the User Accounts OU, why didn't you see permissions such as Reset Password in this list? Why did the permission appear when you evaluated effective permissions for Aaron Painter on Aaron Lee's user account?

Question: Does Windows make it easy to answer the questions, "Who can reset user passwords?" and "What can XXX do as an administrator?"

Question: What is the benefit of a two-tiered, role-based management group structure when assigning permissions in Active Directory?



Note: Role-based management is a big topic, and there are other aspects of role-based management, including discipline and auditing, that are required to ensure that the members of a group such as AD_User Accounts_Support have the permissions they are supposed to have, and no other permissions, and that no other users or groups have been delegated the same permissions.

Question: What is the danger of resetting the ACL of an OU back to its schema-defined default?

Lab B: Audit Active Directory Changes

- Exercise 1: Audit changes to Active Directory by using default audit policy
- Exercise 2: Audit changes to Active Directory by using Directory Service Changes auditing

Logon information

Virtual machine	6425B-HQDC01-A
Logon user name	Pat.Coleman
Administrative user name	Pat.Coleman_Admin
Password	Pa\$\$w0rd

Estimated time: 15 minutes

Scenario

The enterprise security team at Contoso has asked you to provide detailed reports regarding changes to the membership of security-sensitive groups, including Domain Admins. The reports must show the change that was made, who made the change, and when.

Exercise 1: Audit Changes to Active Directory by Using Default Audit Policy

In this exercise, you will see the Directory Service Access auditing that is enabled by default in Windows Server 2008 and Windows Server 2003.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Confirm that the Domain Admins group is configured to audit changes to its membership.
3. Make a change to the membership of Domain Admins.
4. Examine the events that were generated.

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 2: Confirm that the Domain Admins group is configured to audit changes to its membership

- Run **Active Directory Users and Computers** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
- Open the **Audit Settings** properties of the **Domain Admins** group.

Locate the entry that specifies the auditing of successful attempts to modify properties of the group such as membership.

Question: What is the Auditing Entry that achieves this goal?

► **Task 3: Make a change to the membership of Domain Admins**

- Add **Stuart Munson** (user logon name **Stuart.Munson**) to the **Domain Admins** group. Be sure to apply your change.
- Remove **Stuart Munson** from the **Domain Admins** group.
- Make a note of the time when you made the changes. That will make it easier to locate the audit entries in the event logs.

► **Task 4: Examine the events that were generated**

- Run **Event Viewer** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
- Open the **Security Log** and locate the events that were generated when you added and removed Stuart Munson.

Question: What is the Event ID of the event logged when you made your changes? What is the Task Category?

Question: Examine the information provided on the General tab. Can you identify the following in the event log entry?

- Who made the change?
- When the change was made?
- What object was changed?
- What type of access was performed?
- What attribute was changed? How is the changed attribute identified?
- What change was made to that attribute?

Results: After this exercise, you will have generated and examined Directory Service Access audit entries.

Exercise 2: Audit Changes to Active Directory by Using Directory Service Changes Auditing

In this exercise, you will implement the new Directory Services Changes auditing of Windows Server 2008 to reveal the details about changes to the Domain Admins group.

The main tasks for this exercise are as follows:

1. Enable Directory Services Changes auditing.
2. Make a change to the membership of Domain Admins.
3. Examine the events that were generated.

► Task 1: Enable Directory Services Changes auditing

- Run the command prompt as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
- Type the following command, and then press ENTER:

```
auditpol /set /subcategory:"directory service changes"  
/success:enable
```

► Task 2: Make a change to the membership of Domain Admins

- Add **Stuart Munson** (user logon name **Stuart.Munson**) to the **Domain Admins** group. Be sure to apply your change.
- Remove **Stuart Munson** from the **Domain Admins** group.
- Make a note of the time when you made the changes. That will make it easier to locate the audit entries in the event logs.

► Task 3: Examine the events that were generated

- Run **Event Viewer** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
- Open the **Security Log** and locate the new types of events that were generated when you added and removed Stuart Munson.

Question: What are the Event IDs of the event logged when you made your changes? What is the Task Category?

Question: Examine the information provided on the General tab. Can you identify the following in the event log entry?

- What type of change was made?
- Who made the change?
- What member was added or removed?
- What group was affected?
- When the change was made?

Results: After this exercise, you will have generated Directory Services Changes auditing entries.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: What details are captured by Directory Services Changes auditing that are not captured by Directory Service Access auditing?

Question: What types of administrative activities would you want to audit using Directory Services Changes auditing?

Module 9

Lab Instructions: Improve the Security of Authentication in an Active Directory Domain Services (AD DS) Domain

Contents:

Lab A: Configure Password and Account Lockout Policies	
Exercise 1: Configure the Domain's Password and Lockout Policies	3
Exercise 2: Configure Fine-Grained Password Policy	4
Lab B: Audit Authentication	
Exercise 1: Audit Authentication	9
Lab C: Configure Read-Only Domain Controllers	
Exercise 1: Install an RODC	13
Exercise 2: Configure Password Replication Policy	16
Exercise 3: Manage Credential Caching	18

Lab A: Configure Password and Account Lockout Policies

- Exercise 1: Configure the Domain's Password and Lockout Policies
- Exercise 2: Configure Fine-Grained Password Policy

Logon information

Virtual machine	6425B-HQDC01-A
Logon user name	Pat.Coleman
Administrative user name	Pat.Coleman_Admin
Password	Pa\$\$w0rd

Estimated time: 30 minutes

Scenario

Contoso's security team has tasked you with increasing the security and monitoring of authentication against the enterprise's AD DS domain. Specifically, you are to enforce a specified password policy for all user accounts, and a more stringent password policy for security sensitive, administrative accounts.

Exercise 1: Configure the Domain's Password and Lockout Policies

In this exercise, you will modify the Default Domain Policy GPO to implement a password and lockout policy for users in the contoso.com domain.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Configure the domain account policies.

► Task 1: Start the virtual machines and log on

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 2: Configure the domain account policies

1. Run **Group Policy Management** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Edit the **Default Domain Policy GPO**.
3. Configure the following password policy settings. Leave other settings at their default values.
 - **Maximum password age:** 90 Days
 - **Minimum password length:** 10 characters
5. Configure the following account lockout policy setting. Leave other settings at their default values.
 - **Account lockout threshold:** 5 Invalid Logon Attempts.
6. Close Group Policy Management Editor and Group Policy Management.

Results: After this exercise, you will have configured new settings for the domain account policies.

Exercise 2: Configure Fine-Grained Password Policy

In this exercise, you will create a PSO that applies a restrictive, fine-grained password policy to user accounts in the Domain Admins group. You will identify the PSO that controls the password and lockout policies for an individual user. Finally, you will delete the PSO that you created.

The main tasks for this exercise are as follows:

1. Create a PSO.
2. Link a PSO to a Group.
3. Identify the Resultant PSO for a User.
4. Delete a PSO.

► Task 1: Create a PSO

1. Click **Start**, point to **Administrative Tools**, right-click **ADSI Edit**, and choose **Run as administrator**.
2. Click **Use another account**.
3. In the **User name** box, type **Pat.Coleman_Admin**.
4. In the **Password** box, type **Pa\$\$w0rd**, and then press ENTER. ADSI Edit opens.
5. Right-click **ADSI Edit** and choose **Connect To**.
6. Accept all defaults. Click **OK**.
7. Click **Default Naming Context** in the console tree.
8. Expand **Default Naming Context**, and select **DC=contoso,DC=com**.
9. Expand **DC=contoso,DC=com**, and select **CN=System**.
10. Expand **CN=System**, and select **CN= Password Settings Container**.

All PSOs are created and stored in the Password Settings Container (PSC).

11. Right-click the **PSC** and choose **New, Object**. The **Create Objects** dialog box appears.

It prompts you to select the type of object to create. There is only one choice: *msDS-PasswordSettings*—the technical name for the object class referred to as a PSO.

12. Click **Next**. You are then prompted for the value for each attribute of a PSO. The attributes are similar to those found in the domain account policies.
13. Configure each attribute as indicated below. Click **Next** after each attribute.
 - *Common-Name*: **My Domain Admins PSO**. This is the friendly name of the PSO.
 - *msDS-PasswordSettingsPrecedence*: **1**. This PSO has the highest possible precedence.
 - *msDS-PasswordReversibleEncryptionEnabled*: **False**. The password is not stored using reversible encryption.
 - *msDS-PasswordHistoryLength*: **30**. The user cannot reuse any of the last 30 passwords.
 - *msDS-PasswordComplexityEnabled*: **True**. Password complexity rules are enforced.
 - *msDS-MinimumPasswordLength*: **15**. Passwords must be at least 15 characters long.
 - *msDS-MinimumPasswordAge*: **1:00:00:00**. A user cannot change his or her password within one day of a previous change. The format is d:hh:mm:ss (days, hours, minutes, seconds).
 - *msDS-MaximumPasswordAge*: **45:00:00:00**. The password must be changed every 45 days.
 - *msDS-LockoutThreshold*: **5**. Five invalid logons within the time frame specified by XXX (the next attribute) will result in account lockout.
 - *msDS-LockoutObservationWindow*: **0:01:00:00**. Five invalid logons (specified by the previous attribute) within one hour will result in account lockout.
 - *msDS-LockoutDuration*: **1:00:00:00**. An account, if locked out, will remain locked for one day, or until it is unlocked manually. A value of zero will result in the account remaining locked out until an administrator unlocks it.
14. Click **Finish**.
15. Close ADSI Edit.

► **Task 2: Link a PSO to a Group**

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **System** container.
If you do not see the System container, then click the View menu of the MMC console, and ensure that Advanced Features is selected.
3. In the console tree, click the **Password Settings Container**.
4. Right-click **My Domain Admins PSO**, and then click the **Attribute Editor** tab.
5. In the **Attributes** list, select **msDS-PSOAppliesTo**, and then click **Edit**.
The Multi-valued Distinguished Name With Security Principal Editor dialog box appears.
6. Click **Add Windows Account**.
The Select Users, Computers, or Groups dialog box appears.
7. Type **Domain Admins**, and then press ENTER.
8. Click **OK** twice to close the open dialog boxes.

► **Task 3: Identify the Resultant PSO for a user**

1. Run **Active Directory Users and Computers** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Open the **Attribute Editor** in the **Properties** dialog box for the account **Pat.Coleman_Admin**.
3. Click the **Filter** button and ensure that **Constructed** is selected.
The attribute you will locate in the next step is a constructed attribute, meaning that the resultant PSO is not a hard-coded attribute of a user; rather it is calculated by examining the PSOs linked to a user in real-time.

Question: What is the resultant PSO for Pat Coleman (Administrator)?

► **Task 4: Delete a PSO**

1. With **Advanced Features** enabled in the **View** menu of **Active Directory Users and Computers**, open the **System** container and the **Password Settings Container**.
2. Delete the PSO you created, My Domain Admins PSO.

Results: After this exercise, you should have created a PSO, applied it to Domain Admins and confirmed its application, and then deleted the PSO.



Note: Do not shut down the virtual machine once you are finished with this lab as the settings you have configured here will be used in subsequent labs in this module

Lab Review Questions

Question: Where should you define the default password and account lockout policies for user accounts in the domain?

Question: What are the best practices for managing PSOs in a domain?

Question: How can you define a unique password policy for all of the service accounts in the Service Accounts OU?

Lab B: Audit Authentication

- Exercise 1: Audit Authentication

Logon information

Virtual machine	6425B-HQDC01-A	6425B-SERVER01-A
Logon user name	Pat.Coleman	Pat.Coleman
Administrative user name	Pat.Coleman_Admin	Pat.Coleman_Admin
Password	Pa\$\$w0rd	Pa\$\$w0rd

Estimated time: 30 minutes

Scenario

Contoso's security team has tasked you with increasing the security and monitoring of authentication against the enterprise's AD DS domain. Specifically, you are to create an audit trail of logons.

Exercise 1: Audit Authentication

In this exercise, you will use Group Policy to enable auditing of both successful and unsuccessful logon activity by users in the contoso.com domain. You will then generate logon events and view the resulting entries in the event logs.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Configure auditing of account logon events.
3. Configure auditing of logon events.
4. Force a refresh Group Policy.
5. Generate account logon events.
6. Examine account logon events
7. Examine logon events

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Open **D:\Labfiles\Lab09b**.
4. Run **Lab09b_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.

► Task 2: Configure auditing of account logon events

1. Run **Group Policy Management** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Modify the **Default Domain Controllers Policy GPO** to enable auditing events for both successful and failed account logon events.
3. Close Group Policy Management Editor.

► **Task 3: Configure auditing of logon events**

1. Create a **Group Policy Object** (GPO) linked to the **Servers\Important Project OU**. Name the GPO **Server Lockdown Policy**.
2. Modify the **Server Lockdown Policy** to enable auditing events for both successful and failed account logon events.
3. Close Group Policy Management Editor and Group Policy Management.

► **Task 4: Force a refresh Group Policy**

1. Start SERVER01-A. As the computer starts, it will apply the changes you made to Group Policy.
2. On HQDC01, run the **Command Prompt** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**, and then run the command **gpupdate.exe /force**. Close the Command Prompt.

► **Task 5: Generate account logon events**

1. Log on to SERVER01 as **Pat.Coleman**, but enter an incorrect password.
2. After you have been denied logon, log on again with the correct password, **Pa\$\$w0rd**.

► **Task 6: Examine account logon events**

1. Run **Event Viewer** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Identify the failed and successful events in the **Security** log.

Question: What Event ID is associated with the account logon failure events? (Tip: Look for the earliest of a series of failure events at the time you logged on incorrectly to SERVER01.)

Question: What Event ID is associated with the successful account logon? (Tip: Look for the earliest of a series of events at the time you logged on incorrectly to SERVER01.)

► Task 7: Examine logon events

1. On SERVER01, run **Event Viewer** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Identify the failed and successful events in the Security Log.

Question: What Event ID is associated with the logon failure events? (Tip: Look for the earliest of a series of failure events at the time you logged on incorrectly to SERVER01.)

Question: What Event ID is associated with the successful logon? (Tip: Look for the earliest of a series of events at the time you logged on incorrectly to SERVER01.)

Results: After this exercise, you will have established and reviewed auditing for successful and failed logons to the domain and to servers in the Important Project OU.



Note: Do not shut down the virtual machine once you are finished with this lab as the settings you have configured here will be used in subsequent labs in this module

Lab Review Questions

Question: What would be the disadvantage of auditing all successful and failed logons on all machines in your domain?

Question: You have been asked to audit attempts to log on to desktops and laptops in the Finance division using local accounts such as Administrator. What type of audit policy do you set, and in what GPO(s)?

Lab C: Configure Read-Only Domain Controllers

- Exercise 1: Install an RODC
- Exercise 2: Configure Password Replication Policy
- Exercise 3: Manage Credential Caching

Logon information

Virtual machine	6425B-HQDC01-A	6425B-BRANCHDC01-A
Logon user name	Pat.Coleman	
Administrative user name	Pat.Coleman_Admin	Administrator
Password	Pa\$\$w0rd	Pa\$\$w0rd

Estimated time: 60 minutes

Scenario

Contoso's security team has tasked you with increasing the security and monitoring of authentication against the enterprise's AD DS domain. Specifically, you are to improve the security of domain controllers in branch offices.

Exercise 1: Install an RODC

In this exercise, you will configure the server BRANCHDC01 as an RODC in the distant branch office. In order to avoid travel costs, you decide to do the conversion remotely, with the assistance of Aaron Painter, the desktop support technician and only IT staff member at the branch. Aaron Painter has already installed a Windows Server 2008 computer named BRANCHDC01 as a server in a workgroup. You will stage a delegated installation of an RODC so that Aaron Painter can complete the installation.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Stage a delegated installation of an RODC.
3. Run the Active Directory Domain Services Installation Wizard on a workgroup server.

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Open **D:\Labfiles\Lab09c**.
4. Run **Lab09c_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
5. The lab setup script runs. When it is complete, press any key to continue.
6. Close the Windows Explorer window, **Lab09c**.

► Task 2: Stage a delegated installation of an RODC

1. Run **Active Directory Users and Computers** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Right-click the **Domain Controllers** OU, and then click **Pre-create Read only Domain Controller** account.

3. Step through the Active Directory Domain Services Installation Wizard, accepting all defaults. Use the computer name BRANCHDC01 and, on the **Delegation of RODC Installation and Administration** page, delegate installation to **Aaron.Painter_Admin**.

Note that when the wizard is complete, the server appears in the Domain Controllers OU with the DC Type column showing Unoccupied DC Account (Read-only, GC).

► **Task 3: Run the Active Directory Domain Services Installation Wizard on a workgroup server**

1. Start 6425B-BRANCHDC01-A.
2. Log on to BRANCHDC01 as **Administrator** with the password **Pa\$\$w0rd**.
3. Click **Start**, and then click **Run**.
4. Type **dcpromo**, and then press ENTER.

A window appears that informs you that the Active Directory Domain Services binaries are being installed. When installation is completed, the Active Directory Domain Services Installation Wizard appears.

5. Click **Next**.
6. On the **Operating System Compatibility** page, click **Next**.
7. On the **Choose A Deployment Configuration** page, click the **Existing forest** option, then click **Add a domain controller to an existing domain**, and then click **Next**.
8. On the **Network Credentials** page, type **contoso.com**.
9. Click the **Set** button.

A Windows Security dialog box appears.

10. In the **User Name** box, type **Aaron.Painter_Admin**.
11. In the **Password** box, type **Pa\$\$w0rd**, and then press ENTER.
12. Click **Next**.

13. On the **Select a Domain** page, select **contoso.com**, and then click **Next**.

A message appears to inform you that your credentials do not belong to the Domain Admins or Enterprise Admins groups. Because you have pre-staged and delegated administration of the RODC, you are able to proceed with the delegated credentials.

14. Click **Yes**.

A message appears to inform you that the account for BRANCHDC01 has been prestaged in Active Directory as an RODC.

15. Click **OK**.

A warning message appears that indicates the computer has a dynamically assigned IP address. BRANCHDC01 has a dynamically assigned IPv6 address. However, the server does have a fixed IPv4 address. IPv6 addresses are not being used in this course, so you can ignore this message.

16. Click **Yes, the computer will use a dynamically assigned IP address (not recommended)**.

17. On the **Location For Database, Log Files, And SYSVOL** page, click **Next**.

18. On the **Directory Services Restore Mode Administrator Password** page, type **Pa\$\$w0rd12345** in the **Password** and **Confirm Password** boxes, and then click **Next**.

In a production environment, you should assign a complex and secure password to the Directory Services Restore Mode Administrator account.

Also note that we modified the minimum password length in Lab A and as such need to meet the new minimum password length requirements.

19. On the **Summary** page, click **Next**.
20. In the progress window, select the **Reboot On Completion** check box. Active Directory Domain Services is installed on BRANCHDC01, the server reboots.

Results: After this exercise, you will have a new RODC named BRANCHDC01 in the contoso.com domain.

Exercise 2: Configure Password Replication Policy

In this exercise, you will configure domain-wide password replication policy and the password replication policy specific to BRANCHDC01.

The main tasks for this exercise are as follows:

1. Configure domain-wide password replication policy.
2. Create a group to manage password replication to the branch office RODC.
3. Configure password replication policy for the branch office RODC.
4. Evaluate resultant password replication policy.

► Task 1: Configure domain-wide password replication policy

- Who are the default members of Allowed RODC Password Replication Group?
- Who are the default members of Denied RODC Password Replication Group?
- Add the DNSAdmins group as a member of the Denied RODC Password Replication Group.
- Examine the password replication property for BRANCHDC01.
- What is the password replication policy for the Allowed RODC Password Replication Group? For the Denied RODC Password Replication Group?

► Task 2: Create a group to manage password replication to the branch office RODC

1. In the **Groups\Role OU**, create a new global security group called **Branch Office Users**.
2. Add the following users to the Branch Office Users group:
 - **Anav.Silverman**
 - **Chris.Gallagher**
 - **Christa.Geller**
 - **Daniel.Roth**

- ▶ **Task 3: Configure password replication policy for the branch office RODC**
 - Configure BRANCHDC01 so that it caches passwords for users in the **Branch Office Users** group.

- ▶ **Task 4: Evaluate resultant password replication policy**
 - Open the **Resultant Policy** for BRANCHDC01's password replication policy.

Question: What is the resultant policy for Chris.Gallagher?

Results: After this exercise, you will have configured the domain-wide password replication policy to prevent the replication of passwords of members of DNSAdmins to RODCs. You will have also configured the password replication policy for BRANCHDC01 to allow replication of passwords of members of Branch Office Users.

Exercise 3: Manage Credential Caching

In this exercise, you will monitor credential caching.

The main tasks for this exercise are as follows:

1. Monitor credential caching.
2. Pre-populate credential caching.

► Task 1: Monitor credential caching

1. Log on to BRANCHDC01 as **Chris.Gallagher** with the password **Pa\$\$w0rd**, and then log off.
2. Log on to BRANCHDC01 as **Mike.Danseglio** with the password **Pa\$\$w0rd**, and then log off.

The contoso.com domain used in this course includes a Group Policy object (named 6425B) that allows users to log on to domain controllers. In a production environment, it is not recommended to give users the right to log on to domain controllers.

3. On HQDC01, in **Active Directory Users and Computers**, examine the password replication policy for BRANCHDC01.

Question: What users' passwords are currently cached on BRANCHDC01?

Question: What users have been authenticated by BRANCHDC01?

► Task 2: Pre-populate credential caching

- In the password replication policy for BRANCHDC01, pre-populate the password for **Christa Geller**.

Results: After this exercise, you will have identified the accounts that have been cached on BRANCHDC01, or have been forwarded to another domain controller for authentication. You will have also prepopulated the cached credentials for Christa Geller.

Lab Review Questions

Question: Why should you ensure that the PRP for a branch office RODC has, in its Allow list, the accounts for the *computers* in the branch office as well as the users?

Question: What would be the most manageable way to ensure that computers in a branch are in the Allow list of the RODC's PRP?

Question: What are the pro's and con's of prepopulating the credentials for all users and computers in a branch office to that branch's RODC?

Module 10

Lab Instructions: Configure Domain Name System (DNS)

Contents:

Lab A: Install the DNS Service

Exercise 1: Add the DNS Server Role 3

Exercise 2: Configure Forward Lookup Zones and Resource Records 5

Lab B: Advanced Configuration of DNS

Exercise 1: Enable Scavenging of DNS Zones 8

Exercise 2: Create Reverse Lookup Zones 10

Exercise 3: Explore Domain Controller Location 12

Exercise 4: Configure Name Resolution for External Domains 13

Lab A: Install the DNS Service

- Exercise 1: Add the DNS Server Role
- Exercise 2: Configure Forward Lookup Zones and Resource Records

Logon information

Virtual machine	6425B-HQDC01-B	6425B-HQDC02-B
Logon user name	Do not log on	Pat.Coleman
Administrative user name		Pat.Coleman_Admin
Password		Pa\$\$w0rd

Estimated time: 30 minutes

Scenario

You are an administrator of Contoso, Ltd. You recently added a second domain controller to your enterprise, and you want to add redundancy to the DNS server hosting the domain's zone. Currently, the only DNS server for the contoso.com zone is HQDC01. You need to ensure that clients that resolve against the new DNS server, HQDC02, are able to access Internet Web sites. Additionally, you have been asked to configure a subdomain to support name resolution required for the testing of an application by the development team.

Exercise 1: Add the DNS Server Role

In this exercise, you will add the DNS server role to HQDC02, examine the domain zone that is automatically populated on the DNS server, and then configure HQDC02 to use itself as its primary DNS server.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Add the DNS server role.
3. Change the DNS server configuration of the DNS client.
4. Examine the domain forward lookup zone.
5. Configure forwarders for Internet name resolution.

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-B.
2. Wait for startup to complete.
3. Start 6425B-HQDC02-B.
4. Log on to HQDC02 as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 2: Add the DNS server role

1. On HQDC02, run Server Manager as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Add the DNS server role to HQDC02.
3. Close Server Manager.
4. Restart HQDC02. Then log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.

This is not necessary in a production environment, but it speeds the process of restarting services and replicating the DNS records to HQDC02 for the purposes of this exercise.

► **Task 3: Change the DNS server configuration of the DNS client**

1. Run the command prompt as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Type **netsh interface ipv4 set dnsserver "Local Area Connection" static 10.0.0.12 primary** and then press ENTER.
3. Type **netsh interface ipv4 add dnsserver "Local Area Connection" 10.0.0.11** and then press ENTER.

► **Task 4: Examine the domain forward lookup zone**

1. Run DNS Manager as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Examine the SOA, NS, and A records in the contoso.com forward lookup zone.

► **Task 5: Configure forwarders for Internet name resolution**

- Configure two forwarders for HQDC02: 192.168.200.12 and 192.168.200.13. Because these DNS servers do not actually exist, the Server FQDN will display either <Attempting to resolve> or <Unable to resolve>. In a production environment, you would configure forwarders to upstream DNS servers on the Internet, usually those provided by your Internet service provider (ISP).

Results: After this exercise, you will have added the DNS server role to HQDC02 and simulated the configuration of forwarders to resolve internet DNS names..

Exercise 2: Configure Forward Lookup Zones and Resource Records

In this exercise, you will add a forward lookup zone for the development domain at Contoso. You will then add a host and CNAME record to the zone and confirm that name resolution for the new zone is functioning.

The main tasks for this exercise are as follows:

1. Create a forward lookup zone.
2. Create Host and CNAME records.
3. Test name resolution.

► Task 1: Create a forward lookup zone

- Create a new forward lookup zone named **development.contoso.com**. The zone should be a primary zone, stored in Active Directory and replicated to all domain controllers in the contoso.com domain. Configure the zone so that it does not allow dynamic updates.



Note: In a production environment you would most likely just replicate to all DNS servers. However for the purposes of our lab we will replicate to all domain controllers to ensure quick and guaranteed replication.

► Task 2: Create Host and CNAME records

1. In the development.contoso.com zone, create a host (A) record for APPDEV01 with the IP address **10.0.0.24**.
2. Create a CNAME record, **www.development.contoso.com** that resolves to **appdev01.development.contoso.com**.

► Task 3: Test name resolution

- At the command prompt, type **nslookup www.development.contoso.com** and then press ENTER.

Examine the output of the command. What does the output tell you?

Results: After this exercise, you will have created a new forward lookup zone, development.contoso.com, with host and CNAME records, and verified that names in the zone can be resolved..



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in the next lab.

Lab Review Questions

Question: If you did not configure forwarders on HQDC02, what would be the result for clients that use HQDC02 as their primary DNS server?

Question: What would happen to clients' ability to resolve names in the development.contoso.com domain if you had chosen a stand-alone DNS zone, rather than an Active Directory-integrated zone? Why would this happen? What would you have to do to solve this problem?

Lab B: Advanced Configuration of DNS

- Exercise 1: Enable Scavenging of DNS Zones
- Exercise 2: Create Reverse Lookup Zones
- Exercise 3: Explore Domain Controller Location
- Exercise 4: Configure Name Resolution for External Domains

Logon information

Virtual machine	6425B-HQDC01-B	6425B-HQDC02-B	6425B-TSTDC01-A	6425B-BRANCHDC01-B
Logon user name	Do not Logon	Pat.Coleman	Sara.Davis	Do not Logon
Administrative user name		Pat.Coleman_Admin	Sara.Davis_Admin	
Password		Pa\$\$w0rd	Pa\$\$w0rd	

Estimated time: 60 minutes

Scenario

You are the DNS administrator at Contoso, Ltd. You want to improve the health and efficiency of your DNS infrastructure by enabling scavenging and by creating a reverse lookup zone for the domain. You also want to examine the records that enable clients to locate domain controllers. Finally, you are asked to configure name resolution between contoso.com and the domain of a partner company, tailspintoys.com.

Exercise 1: Enable Scavenging of DNS Zones

In this exercise, you will enable scavenging of DNS zones, in order to remove stale resource records.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Enable scavenging of a DNS zone.
3. Configure default scavenging settings.

► Task 1: Prepare for the lab

Some of the virtual machines should already be started and available after completing Lab A. However, if they are not, you should step through Exercises 1 and 2 in Lab A before continuing as there are dependencies between Lab A and Lab B.

1. Start 6425B-HQDC01-B.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Open **D:\Labfiles\Lab10b**.
4. Run **Lab10b_Setup.bat** with administrative credentials. Use the account **Administrator** with the password **Pa\$\$w0rd**.
5. The lab setup script runs. When it is complete, press any key to continue.
6. Close the Windows Explorer window, **Lab10b**.
7. Start 6425B-HQDC02-B.
8. Log on to HQDC02 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
9. Start 6425B-TSTDC01-A.
10. Log on to TSTDC01 as **Sara.Davis** with the password **Pa\$\$w0rd**.
11. Start 6425B-BRANCHDC01-B.
12. Wait for BRANCHDC01 to complete startup before continuing.

► **Task 2: Enable scavenging of a DNS zone**

1. On HQDC02, run DNS Manager as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Enable scavenging for the contoso.com zone. Accept the defaults for scavenging-related intervals.

► **Task 3: Configure default scavenging settings**

- Configure HQDC02 so that, by default, scavenging is enabled for all zones. Accept the defaults for scavenging-related intervals.

Results: After this exercise, you will have configured scavenging of the contoso.com domain and enabled scavenging as the default for all zones..

Exercise 2: Create Reverse Lookup Zones

In this exercise, you will create a reverse lookup zone for the contoso.com domain.

The main tasks for this exercise are as follows:

1. Create a reverse lookup zone.
2. Explore and verify the functionality of a reverse lookup zone.

► Task 1: Create a reverse lookup zone

- Create a reverse lookup zone for IPv4 network 10. Allow only secure dynamic updates, and replicate the zone to all domain controllers in the contoso.com domain.



Note: In a production environment you would most likely just replicate to all DNS servers. However for the purposes of our lab we will replicate to all domain controllers to ensure quick and guaranteed replication

► Task 2: Explore and verify the functionality of a reverse lookup zone

1. Run the command prompt as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Type **nslookup www.development.contoso.com**, and then press ENTER.
Note that the first section of the command output, which identifies the DNS server that was queried, indicates the IP address of the server but, next to Server, reports that the server is Unknown. That is because the nslookup.exe command cannot resolve the IP address to a name.
3. Switch to DNS Manager.
4. In the console tree, click the **10.in-addr.arpa** zone under **Reverse Lookup Zones**.
5. Examine the records in the zone.
6. Switch to the command prompt.
7. Type **ipconfig /registerdns**, and then press ENTER.
8. Switch to DNS Manager.
9. Right-click the **10.in-addr.arpa** zone, and then click **Refresh**.

10. Examine the resource records that have appeared.
11. Switch to the command prompt.
12. Type **nslookup www.development.contoso.com**, and then press ENTER.

Note that the DNS server that was queried at 10.0.0.12 is now resolved to its name.

Results: After this exercise, you will have created and experienced the functionality of a reverse lookup zone..

Exercise 3: Explore Domain Controller Location

In this exercise, you will examine the resource records that allow clients to locate domain controllers.

The main tasks for this exercise are as follows:

1. Explore `_tcp`.
2. Explore `_tcp.brancha._sites.contoso.com`.

► **Task 1: Explore `_tcp`**

- Examine the records in `_tcp.contoso.com`. What do the records represent?

► **Task 2: Explore `_tcp.brancha._sites.contoso.com`**

- Examine the records in `_tcp.brancha._sites.contoso.com`. What do the records represent?

Results: After this exercise, you will have examined the Service Locator (SRV) records in the `contoso.com` domain..

Exercise 4: Configure Name Resolution for External Domains

In this exercise, you will configure name resolution between two completely separate domains.

The main tasks for this exercise are as follows:

1. Configure a stub zone.
2. Configure a conditional forwarder.
3. Validate name resolution for external domains.

► Task 1: Configure a stub zone

- On HQDC02, create a stub zone for tailspintoys.com that refers to the IPv4 address **10.0.0.31** as the master server.

► Task 2: Configure a conditional forwarder

1. On TSTDC01, run DNS Management as an administrator, with the user name **Sara.Davis_Admin** and the password **Pa\$\$w0rd**.
2. Create a conditional forwarder for contoso.com that forwards to the IPv4 address **10.0.0.11**.

► Task 3: Validate name resolution for external domains

1. On TSTDC01, open a command prompt and type **nslookup www.development.contoso.com**, and then press ENTER. The command should return the address **10.0.0.24**.
2. Switch to DNS Manager and create a host (A) record for www.tailspintoys.com that resolves to **10.0.0.143**.
3. On HQDC02, open a command prompt and type **nslookup www.tailspintoys.com**, and then press ENTER. The command should return the address **10.0.0.143**.

Results: After this exercise, you will have configured DNS name resolution between the contoso.com and tailspintoys.com domains.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: In this lab, you used a stub zone and a conditional forwarder to provide name resolution between two distinct domains. What other options might you have chosen to use?

Module 11

Lab Instructions: Administer Active Directory® Domain Services (AD DS) Domain Controllers (DCs)

Contents:

Lab A: Install Domain Controllers

Exercise 1: Create an Additional DC with the Active Directory Domain Services Installation Wizard 3

Exercise 2: Add a Domain Controller from the Command Line 5

Exercise 3: Remove a Domain Controller 7

Exercise 4: Create a Domain Controller from Installation Media 8

Lab B: Install a Server Core DC

Exercise 1: Perform Post-Installation Configuration on Server Core 11

Exercise 2: Create a Domain Controller with Server Core 13

Lab C: Transfer Operations Master Roles

Exercise 1: Identify Operations Masters 16

Exercise 2: Transfer Operations Master Roles 18

Lab D: Configure DFS-R Replication of SYSVOL

Exercise 1: Observe the Replication of SYSVOL 21

Exercise 2: Prepare to Migrate to DFS-R 23

Exercise 3: Migrate SYSVOL Replication to DFS-R 25

Exercise 4: Verify DFS-R Replication of SYSVOL 31

Lab A: Install Domain Controllers

- Exercise 1: Create an Additional DC with the Active Directory Domain Services Installation Wizard
- Exercise 2: Add a Domain Controller from the Command Line
- Exercise 3: Remove a Domain Controller
- Exercise 4: Create a Domain Controller from Installation Media

Logon information

Virtual machine	6425B-HQDC01-A	6425B-HQDC02-A
Logon user name	Pat.Coleman	Administrator
Administrative user name	Pat.Coleman_Admin	Pat.Coleman_Admin
Password	Pa\$\$w0rd	Pa\$\$w0rd

Estimated time: 30 minutes

Scenario

You have been hired to replace the former administrator at Contoso, Ltd. The first thing you discover is that the domain has only one domain controller. You decide to add a second domain controller to provide fault tolerance for the directory service. You have already installed a new server named HQDC02.

Exercise 1: Create an Additional DC with the Active Directory Domain Services Installation Wizard

In this exercise, you will use the Active Directory Domain Services Installation Wizard (DCPromo.exe) to create an additional domain controller in the contoso.com domain. You will not complete the installation, however. Instead, you will save the settings as an answer file, which will be used in the next exercise.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Promote a domain controller using the Active Directory Domain Services Installation Wizard.

► Task 1: Prepare for the lab

- Start 6425B-HQDC01-A, and log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.
- Start 6425B-HQDC02-A, a workgroup server, and log on as the local **Administrator** with the password **Pa\$\$w0rd**.

► Task 2: Promote a domain controller using the Active Directory Domain Services Installation Wizard

- On HQDC02, run **DCPromo.exe**. Accept all of the defaults provided by the Active Directory Administration Wizard except those listed below:
 - Additional domain controller in an existing forest
 - Domain: **contoso.com**
 - Alternate credentials: **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
 - Select domain: **contoso.com**.
 - When a warning appears informing you that HQDC01 has a dynamically assigned IP address, click **Yes, the computer will use a dynamically assigned IP address**.
 - When a warning appears informing you that a DNS delegation could not be found, click **Yes**.
 - Directory Services Restore Mode Administrator Password: **Pa\$\$w0rd**

- On the **Summary** page, review your selections. If any settings are incorrect, click **Back** to make modifications.
- Export the settings to a file on your desktop called **AdditionalDC**.
- Cancel the installation of the domain controller on the **Summary** page. Do not continue with the Active Directory Domain Services Installation Wizard.

Results: After this exercise, you should have simulated promoting HQDC02 to a domain controller.

Exercise 2: Add a Domain Controller from the Command Line

In this exercise, you will examine the answer file you created in Exercise 1. You will use the installation options in the answer file to create a dcpromo.exe command line to install the additional domain controller.

The main tasks for this exercise are as follows:

1. Create the DCPromo command.
2. Execute the DCPromo command.

► Task 1: Create the DCPromo command

- Open the **AdditionalDC.txt** file you created in Exercise 1. Examine the answers in the file. Can you identify what some of the options mean?

Tip: Lines beginning with a semicolon are comments or inactive lines that have been commented out.

- Open a second instance of Notepad, as a new text file. Turn on word wrap. Position the windows so you can see both the blank text file and the AdditionalDC.txt file as a reference.
- In Notepad, type the dcpromo.exe command line just as you would do in a command prompt. Determine the command line to install the domain controller with the same options as those listed in the answer file. Parameters on the command line take the form /option:value whereas, in the answer file, they take the form option=value. Configure both the **Password** and **SafeModeAdminPassword** values as **Pa\$\$w0rd**. Instruct DCPromo to reboot when complete.
- As you will learn in Lab B, you can set the Password value to an asterisk (*) and you will be prompted to enter the password when you run the command.
- When you have created the command, open the **Exercise2.txt** file, found in the \\HQDC01\d\$\Labfiles\Lab11a folder. Compare the correct command in **Exercise2.txt** to the command you created in the previous step. Make any necessary corrections to your command.

► **Task 2: Execute the DCPromo command**

- Open the Command Prompt window.
- Switch to the Notepad file with the dcpromo.exe command you built in Task 1. Turn off word wrap, copy the command line you created and paste it into the command prompt window, then press ENTER to execute the command.

HQDC02 is promoted to a domain controller. This takes a few minutes.

Results: After this exercise, you should have promoted HQDC02 as an additional domain controller in the contoso.com domain and forest.

Exercise 3: Remove a Domain Controller

In this exercise, you will remove a domain controller from the contoso.com domain.

The main tasks for this exercise are as follows:

- Remove a domain controller.

► Task 1: Remove a domain controller

- After HQDC02 has restarted, log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.
- Run DCPromo as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**. Accept all defaults presented by the wizard, and configure the new Administrator password to be **Pa\$\$w0rd**. Restart the server when the process has completed.

Results: After this exercise, you should have demoted HQDC02 to a member server.

Exercise 4: Create a Domain Controller from Installation Media

You can reduce the amount of replication required to create a domain controller by promoting the domain controller, using the IFM option. IFM requires that you provide installation media, which is, in effect, a backup of Active Directory. In this exercise, you will create the installation media on HQDC01, transfer it to HQDC02, and then simulate the promotion of HQDC02 to a domain controller using the installation media.

The main tasks for this exercise are as follows:

1. Create installation media.
2. Promote a domain controller using installation media.

► Task 1: Create installation media

1. On HQDC01, run the Command Prompt as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Use **ntdsutil.exe** to create installation media in a folder named **C:\IFM**.

► Task 2: Promote a domain controller using installation media

1. Switch to HQDC02, and log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.
2. Copy the IFM folder from the HQDC01 drive C to drive C on HQDC02.
3. On HQDC02, run **DCPromo.exe**. Accept all of the defaults provided by the Active Directory Administration Domain Services Installation Wizard except those listed below:
 - Additional domain controller in an existing forest.
 - Domain: **contoso.com**.
 - User: **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
 - Select domain: **contoso.com**.
 - When a warning appears informing you that HQDC01 has a dynamically assigned IP address, click **Yes, the computer will use a dynamically assigned IP address**.

- When a warning appears informing you that a DNS delegation could not be found, click **Yes**.
- Install from Media: Replicate data from media stored at C:\IFM.
- After the Source Domain Controller page, cancel the wizard without completing the promotion.

Results: After this exercise, you should have created installation media on HQDC01 and simulated the promotion of HQDC02 to a domain controller using the installation media..



Note: Shut down HQDC02, but do not shut down HQDC01 as it will be used in Lab B.

Lab Review Questions

Question: Why would you choose to use an answer file, or a dcpromo.exe command line to install a domain controller rather than the Active Directory Domain Services Installation Wizard?

Question: In what situations does it make sense to create a domain controller using installation media?

Lab B: Install a Server Core DC

- Exercise 1: Perform Post-Installation Configuration on Server Core
- Exercise 2: Create a Domain Controller with Server Core

Logon information

Virtual machine	6425B-HQDC01-A	6425B-HQDC03-A
Logon user name	Do not log on	Administrator
Administrative user name		Pat.Coleman_Admin
Password		Pa\$\$wOrd

Estimated time: 30 minutes

Scenario

You are a domain administrator for Contoso, Ltd., and you want to add a domain controller to the AD DS environment. In order to enhance the security of the new DC, you plan to use Server Core. You have already installed Server Core on a new computer, and you are ready to configure the server as a domain controller.

Exercise 1: Perform Post-Installation Configuration on Server Core

In this exercise, you will perform post-installation configuration of the server to prepare it with the name and TCP/IP settings required for the remaining exercises in this Lab.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Perform post-installation configuration of Server Core.

► Task 1: Prepare for the Lab

The 6425B-HQDC01-A virtual machine should already be available after completing Lab A.

- Start 6425B-HQDC01-A, but do not log on.
- Start 6425B-HQDC03-A, but do not log on.

► Task 2: Perform post-installation configuration of Server Core

- Log on to HQDC03 as **Administrator** with the password **Pa\$\$w0rd**.
- Configure the IPv4 address and DNS server by typing each of the following commands:

```
netsh interface ipv4 set address name="Local Area Connection"  
source=static address=10.0.0.13 mask=255.255.255.0  
gateway=10.0.0.1
```

```
netsh interface ipv4 set dns name="Local Area Connection"  
source=static address=10.0.0.11 primary
```

- Confirm the IP configuration you entered previously with the command **ipconfig /all**.
- Rename the server by typing **netdom renamecomputer %computername% /newname:HQDC03**. You will be prompted to press **Y** to confirm the operation.
- Restart by typing **shutdown -r -t 0**.

- Log on as **Administrator** with the password **Pa\$\$w0rd**.
- Join the domain using the following command:

```
netdom join %computename% /domain:contoso.com  
/UserD:CONTOSO\Pat.Coleman_Admin /PasswordD:Pa$$w0rd  
/OU:"ou=servers,dc=contoso,dc=com"
```

- Restart by typing **shutdown -r -t 0**.

Results: After this exercise, you should have configured the Server Core installation as a member of the contoso.com domain named HQDC03.

Exercise 2: Create a Domain Controller with Server Core

In this exercise, you will add the DNS and AD DS roles to the Server Core installation.

The main tasks for this exercise are as follows:

1. Add the DNS Server role to Server Core.
2. Create a domain controller on Server Core with the `dcpromo.exe` command.

► Task 1: Add the DNS Server role to Server Core

- Log on to HQDC03 as **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
- Display available server roles by typing **oclist**. What is the package identifier for the DNS server role? What is its status?
- Type **ocsetup**, and then press ENTER. Surprise! There is a minor amount of GUI in Server Core. Click **OK** to close the window.
- Type **ocsetup DNS-Server-Core-Role**. Note that package identifiers are case sensitive.
- Type **oclist** and confirm that the DNS server role is installed.

► Task 2: Create a domain controller on Server Core with the `dcpromo.exe` command

- Make sure you are still logged on to HQDC03 as **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**
- Type **dcpromo.exe /?**, and then press ENTER. Review the usage information.
- Type **dcpromo.exe /?:Promotion**, and then press ENTER. Review the usage information.
- Type the following command to add and configure the AD DS role, and then press ENTER:

```
dcpromo /unattend /ReplicaOrNewDomain:replica  
/ReplicaDomainDNSName:contoso.com /ConfirmGC:Yes  
/UserName:CONTOSO\Pat.Coleman_Admin /Password:*  
/safeModeAdminPassword:Pa$$w0rd
```

- When prompted to enter network credentials, type **Pa\$\$w0rd**, and then click **OK**. The AD DS role will be installed and configured, and then the server will reboot.

Results: After this exercise, you should have promoted the Server Core server, HQDC03, to a domain controller in the contoso.com domain.



Note: You can shut down both virtual machines as different virtual machines are used in the next Lab.

Lab Review Questions

Question: Did you find the configuration of Server Core to be particularly difficult?

Question: What are the advantages of using Server Core for domain controllers?

Lab C: Transfer Operations Master Roles

- Exercise 1: Identify Operations Masters
- Exercise 2: Transfer Operations Master Roles

Logon information

Virtual machine	6425B-HQDC01-B	6425B-HQDC02-B
Logon user name	Pat.Coleman	Do not log on
Administrative user name	Pat.Coleman_Admin	
Password	Pa\$\$w0rd	

Estimated time: 30 minutes

Scenario

You are a domain administrator at Contoso, Ltd. One of the redundant power supplies has failed on HQDC01 and you must take the server offline for servicing. You want to ensure that AD DS operations are not interrupted while the server is offline.

Exercise 1: Identify Operations Masters

In this exercise, you will use both user interface and command-line tools to identify operations masters in the contoso.com domain.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Identify operations masters using the Active Directory administrative snap-ins.
3. Identify operations masters using NetDom.

► Task 1: Prepare for the lab

- Start 6425B-HQDC01-B and log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.
- Open **D:\Labfiles\Lab11c**.
- Run **Lab11c_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
- The lab setup script runs. When it is complete, press any key to continue.
- Close the Windows Explorer window, **Lab11c**.
- Start 6425B-HQDC02-B, but do not log on.

► Task 2: Identify operations masters using the Active Directory administrative snap-ins

- Run **Active Directory Users and Computers** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
- Use **Active Directory Users and Computers** to identify the operations master role token holders for RID, PDC and Infrastructure. Which DC holds those roles?
- Close Active Directory Users and Computers.
- Run **Active Directory Domains and Trusts** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
- Use **Active Directory Domains and Trusts** to identify the operations master role token holders for Domain Naming. Which DC holds this role?
- Close Active Directory Domains and Trusts.

- Run the Command Prompt as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
 - Type **regsvr32 schmmgmt.dll**, and then press ENTER.
 - Run **mmc.exe** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
 - Add the **Active Directory Schema** snap-in to the console.
 - Use **Active Directory Schema** to identify the operations master role token holders for Schema. Which DC holds this role?
 - Close the console. You do not need to save any changes.
- **Task 3: Identify operations masters using NetDom**
- Run the Command Prompt as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
 - Type the command **netdom query fsmo**, and press ENTER.

Results: After this exercise, you should have used both administrative snap-ins and NetDom to identify operations masters.

Exercise 2: Transfer Operations Master Roles

In this exercise, you will prepare to take the operations master offline by transferring its role to another domain controller. You will then simulate taking it offline, bringing it back online, and returning the operations master role.

The main tasks for this exercise are as follows:

1. Transfer the PDC role using the Active Directory Users And Computers snap-in.
2. Consider other roles before taking a domain controller offline.
3. Transfer the PDC role using NTDSUtil.

► Task 1: Transfer the PDC role using the Active Directory Users And Computers snap-in

- Run **Active Directory Users and Computers** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
- Connect to HQDC02.

Before transferring an operations master, you must connect to the domain controller to which the role will be transferred.

The root node of the snap-in indicates the domain controller to which you are connected: Active Directory Users And Computers [hqdc02.contoso.com].

- Transfer the PDC operations master role to HQDC02.

► Task 2: Consider other roles before taking a domain controller offline

You are preparing to take HQDC01 offline. You have just transferred the PDC operations role to HQDC02.

- List other operations master roles that must be transferred prior to taking HQDC01 offline?
- List other server roles that must be transferred prior to taking HQDC01 offline?

► Task 3: Transfer the PDC role using NTDSUtil

You have finished performing maintenance on HQDC01. You bring it back online.

Remember you cannot bring a domain controller back online if the RID, schema, or domain naming roles have been seized. But you can bring it back online if a role was transferred.

- Run the Command Prompt as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
- Use **NTDSUtil** to connect to HQDC01 and transfer the PDC role back to it.

Results: After this exercise, you should have transferred the PDC role to HQDC02 using the Active Directory Users And Computers snap-in, and then transferred it back to HQDC01 using NTDSUtil.



Note: You can shut down these virtual machines when finished with them as they will need to be restarted for the next lab.

Lab Review Questions

Question: If you transfer all roles before taking a domain controller offline, is it OK to bring the domain controller back online?

Question: If a domain controller fails and you seize roles to another domain controller, is it OK to bring the failed domain controller back online?

Lab D: Configure DFS-R Replication of SYSVOL

- Exercise 1: Observe the Replication of SYSVOL
- Exercise 2: Prepare to Migrate to DFS-R
- Exercise 3: Migrate SYSVOL Replication to DFS-R
- Exercise 4: Verify DFS-R Replication of SYSVOL

Logon information

Virtual machine	6425B-HQDC01-B	6425B-HQDC02-B
Logon user name	Pat.Coleman	Pat.Coleman
Administrative user name	Pat.Coleman_Admin	Pat.Coleman_Admin
Password	Pa\$\$w0rd	Pa\$\$w0rd

Estimated time: 30 minutes

Scenario

You are an administrator at Contoso. You have recently upgraded the last remaining Windows Server 2003 domain controller to Windows Server 2008, and you want to take advantage of the improved replication of SYSVOL using DFS-R.

Exercise 1: Observe the Replication of SYSVOL

In this exercise, you will observe SYSVOL replication with File Replication Service (FRS) by adding a logon script to the NETLOGON share and observing its replication to another domain controller.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Observe SYSVOL replication.

► Task 1: Prepare for the lab

- Shut down all VMs.
- Start 6425B-HQDC01-B, and log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.
- Open **D:\Labfiles\Lab11d**.
- Run **Lab11d_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
- The lab setup script runs. When it is complete, press any key to continue.
- Close the Windows Explorer window, **Lab11d**.
- Start 6425B-HQDC02-B, and log on as **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.

► Task 2: Observe SYSVOL replication

- On HQDC01, open **%SystemRoot%\ Sysvol\sysvol\contoso.com\Scripts**.
- Run Notepad as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
- Save a test file as **%SystemRoot%\ Sysvol\sysvol\contoso.com\Scripts \TestFRS.txt**.
- On HQDC02, open **%SystemRoot%\Sysvol\sysvol\contoso.com\Scripts \Scripts**.

- Confirm that **TestFRS.txt** has replicated to the HQDC02 Scripts folder.
If the file does not appear immediately, wait a few moments. It can take up to 15 minutes for replication to occur. You can, optionally, continue with Exercise 2. Before continuing even further with Exercise 3, check back to ensure that the file has replicated.
- After you have observed the replication, close the Windows Explorer window showing the Scripts folder on both HQDC01 and HQDC02.

Results: After this exercise, you should have observed the replication of a test file between the SYSVOL\Scripts folders of two domain controllers.

Exercise 2: Prepare to Migrate to DFS-R

Before you can migrate to DFS-R of SYSVOL, the domain must contain only Windows Server 2008 domain controllers, and the domain functional level must be raised to Windows Server 2008. In this exercise, you will confirm the fact that DFS-R migration is not supported in other domain functional levels. Then, you will raise the domain functional level to Windows Server 2008.

The main tasks for this exercise are as follows:

1. Confirm that the current domain functional level is lower than Windows Server 2008.
2. Confirm that DFS-R replication is not available at domain functional levels lower than Windows Server 2008.
3. Raise the domain functional level.
4. Confirm that DFS-R replication is available at Windows Server 2008 domain functional level.

► Task 1: Confirm that the current domain functional level is lower than Windows Server 2008

- On HQDC01, run **Active Directory Users and Computers** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
- Confirm that the current domain functional level is Windows Server 2003 but *do not raise the functional level*. Instead, cancel out of the dialog box.

► Task 2: Confirm that DFS-R replication is not available at domain functional levels lower than Windows Server 2008

- Run the Command Prompt as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
- Type **dfsrmig /getglobalstate**, and then press ENTER. A message appears informing you that dfsrmig is supported only on domains at the Windows Server 2008 functional level.

► **Task 3: Raise the domain functional level**

- In **Active Directory Users and Computers**, raise the domain functional level to **Windows Server 2008**.
- Close **Active Directory Users and Computers**.

► **Task 4: Confirm that DFS-R replication is available at Windows Server 2008 domain functional level**

- Switch to the command prompt. Type **dfsrmig /getglobalstate**, and then press ENTER. A message appears informing you that DFS-R migration has not yet been initialized.

Results: After this exercise, you should have raised the domain functional level to Windows Server 2008, and confirmed that by doing so you have made it possible to migrate SYSVOL replication to DFS-R.

Exercise 3: Migrate SYSVOL Replication to DFS-R

In this exercise, you will migrate the replication mechanism from FRS to DFS-R.

The main task for this exercise is as follows:

1. Migrate SYSVOL replication to DFS-R

► Task 1: Migrate SYSVOL replication to DFS-R

1. Switch to the Command Prompt
2. Type **dfsrmig /setglobalstate 0**, and then press ENTER.

The following message appears:

```
Current DFSR global state: 'Start'  
New DFSR global state: 'Start'  
Invalid state change requested.
```

The default global state is already 0, 'Start,' so your command is not valid. However, this does serve to initialize DFSR migration.

3. Type **dfsrmig /getglobalstate**, and then press ENTER.

The following message appears:

```
Current DFSR global state: 'Start'  
Succeeded.
```

4. Type **dfsrmig /getmigrationstate**, and then press ENTER.

The following message appears:

```
All Domain Controllers have migrated successfully to Global state  
( 'Start' ).  
Migration has reached a consistent state on all Domain  
Controllers.  
Succeeded.
```

5. Type **dfsrmig /setglobalstate 1**, and then press ENTER.

The following message appears:

```
Current DFSR global state: 'Start'
New DFSR global state: 'Prepared'

Migration will proceed to 'Prepared' state. DFSR service will
copy the contents of SYSVOL to SYSVOL_DFSR
folder.

If any DC is unable to start migration then try manual polling.
OR Run with option /CreateGlobalObjects.
Migration can start anytime between 15 min to 1 hour.
Succeeded.
```

6. Type **dfsrmig /getmigrationstate**, and then press ENTER.
A message appears that reflects the migration state of each domain controller. Migration can take up to 15 minutes.
7. Repeat this step until you receive the following message that indicates migration has progressed to the 'Prepared' state and is successful:

```
All Domain Controllers have migrated successfully to Global state
('Prepared').
Migration has reached a consistent state on all Domain
Controllers.
Succeeded.
```

When you receive the message just shown, continue to the next step.

During migration to the 'Prepared' state, you might see one of these messages:

```
The following Domain Controllers are not in sync with Global state
('Prepared'):
```

Domain Controller (Local Migration State) - DC Type
HQDC01 ('Start') - Primary DC
HQDC02 ('Start') - Writable DC

```
Migration has not yet reached a consistent state on all Domain
Controllers.
State information might be stale due to AD latency.
```

or

The following Domain Controllers are not in sync with Global state ('Prepared'):

Domain Controller (Local Migration State) - DC Type
=====

HQDC01 ('Start') - Primary DC
HQDC02 ('Waiting For Initial Sync') - Writable DC

Migration has not yet reached a consistent state on all Domain Controllers.
State information might be stale due to AD latency.

or

The following Domain Controllers are not in sync with Global state ('Prepared'):

Domain Controller (Local Migration State) - DC Type
=====

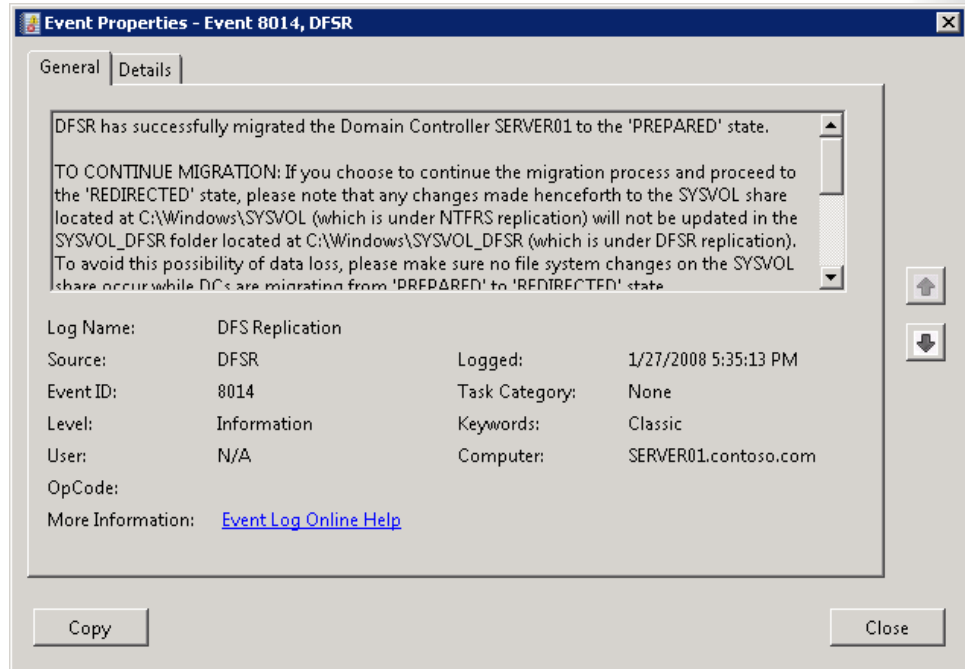
HQDC02 ('Waiting For Initial Sync') - Writable DC

Migration has not yet reached a consistent state on all Domain Controllers.
State information might be stale due to AD latency.

8. Click **Start**, point to **Administrative Tools**, right-click **Event Viewer**, and then choose **Run as administrator**.
9. Click **Use another account**.
10. In the **User name** box, type **Pat.Coleman_Admin**.
11. In the **Password** box, type **Pa\$\$w0rd**, and then press ENTER.
Event Viewer opens.
12. In the console tree, expand **Applications and Services Logs**, and select **DFS Replication**.

13. Locate the event with **Event ID 8014** and open its properties.

You should see the details shown in the following screen shot.



14. Close Event Viewer.
15. Switch to the Command Prompt.

16. Type **dfsrmig /setglobalstate 2**, and then press ENTER.

The following message appears:

```
Current DFSR global state: 'Prepared'
New DFSR global state: 'Redirected'

Migration will proceed to 'Redirected' state. The SYSVOL share
will be
changed to SYSVOL_DFSR folder.

If any changes have been made to the SYSVOL share during the state
transition from 'Prepared' to 'Redirected', please robocopy the
changes
from SYSVOL to SYSVOL_DFSR on any replicated RWDC.
Succeeded.
```

17. Type **dfsrmig /getmigrationstate**, and then press ENTER.

A message appears that reflects the migration state of each domain controller. Migration can take up to 15 minutes.

18. Repeat step 17 until you receive the following message that indicates migration has progressed to the 'Prepared' state and is successful:

```
All Domain Controllers have migrated successfully to Global state
('Redirected').
Migration has reached a consistent state on all Domain
Controllers.
Succeeded.
```

When you receive the message just shown, continue to the next task.

During migration, you might receive messages like the following:

```
The following Domain Controllers are not in sync with Global state
('Redirected'):

Domain Controller (Local Migration State) - DC Type
=====

HQDC02 ('Prepared') - Writable DC

Migration has not yet reached a consistent state on all Domain
Controllers.
State information might be stale due to AD latency.
```

Results: After this exercise, you should have migrated the replication of SYSVOL to DFS-R in the contoso.com domain.

Exercise 4: Verify DFS-R Replication of SYSVOL

In this exercise, you will verify that SYSVOL is being replicated by DFS-R.

The main tasks for this exercise are as follows:

1. Confirm the new location of SYSVOL.
2. Observe SYSVOL replication.

► Task 1: Confirm the new location of SYSVOL

- At the Command Prompt, type **net share**, and then press ENTER. Confirm that the NETLOGON share refers to the %SystemRoot%\SYSVOL_DFSR\Sysvol\contoso.com\Scripts folder, and that the SYSVOL share refers to the %SystemRoot%\SYSVOL_DFSR\Sysvol folder.

► Task 2: Observe SYSVOL replication

- On HQDC01, open %SystemRoot%\SYSVOL_DFSR\Sysvol\contoso.com\Scripts.

Note that the TestFRS.txt file created earlier is already in the Scripts folder. While the domain controllers were at the Prepared state, files were replicated between the legacy, FRS SYSVOL folder and the new, DFS-R SYSVOL folder.

- Run Notepad as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
- Save a test file as %SystemRoot%\SYSVOL_DFSR\Sysvol\contoso.com\Scripts\TestDFSR.txt.
- On HQDC02, open %SystemRoot%\SYSVOL_DFSR\Sysvol\contoso.com\Scripts.
- Confirm that the TestDFSR.txt file has replicated to the HQDC02 Scripts folder.

If the file does not appear immediately, wait a few moments.

Results: After this exercise, you should have observed the replication of a test file between the SYSVOL_DFSR Scripts folders of two domain controllers.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: What would you expect to be different between two enterprises, one which created its domain initially with Windows 2008 domain controllers, and one that migrated to Windows Server 2008 from Windows Server 2003?

Question: What must you be aware of while migrating from the Prepared to the Redirected state?

Module 12

Lab Instructions: Manage Sites and Active Directory Replication

Contents:

Lab A: Configure Sites and Subnets	
Exercise 1: Configure the Default Site	3
Exercise 2: Create Additional Sites	4
Exercise 3: Move Domain Controllers into Sites	5
Lab B: Configure the Global Catalog and Application Partitions	
Exercise 1: Configure a Global Catalog	7
Exercise 2: Configure Universal Group Membership Caching	8
Exercise 3: Examine DNS and Application Directory Partitions	9
Lab C: Configure Replication	
Exercise 1: Create a Connection Object	12
Exercise 2: Create Site Links	14
Exercise 3: Move Domain Controllers into Sites	15
Exercise 4: Designate a Preferred Bridgehead Server	16
Exercise 5: Configure Intersite Replication	17

Lab A: Configure Sites and Subnets

- Exercise 1: Configure the Default Site
- Exercise 2: Create Additional Sites

Logon information

Virtual machine	6425B-HQDC01-B	6425-HQDC02-B	6425B-HQDC03-B	6425B-BRANCHDC01-B
Logon user name	Pat.Coleman	Do not log on	Do not log on	Do not log on
Administrative user name	Pat.Coleman_Admin			
Password	Pa\$\$wOrd			

Estimated time: 30 minutes

Scenario

You are an administrator for Contoso, Ltd. You are preparing to improve the service localization and Active Directory replication of your enterprise. The previous administrator made no changes to the out-of-box configuration of sites and subnets. You want to begin the process of defining your physical topology in Active Directory.

Exercise 1: Configure the Default Site

In this exercise, you will rename the Default-First-Site-Name site and associate two subnets with the site.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Rename Default-First-Site-Name.
3. Create a subnet and associate it with a site.

► Task 1: Prepare for the lab

- Start 6425B-HQDC01-B, and log on as **Pat.Coleman** with the password **Pa\$\$w0rd**. This virtual machine may take several minutes to start.
- After logging on to HQDC01, start 6425B-HQDC02-B but do not log on.
- After HQDC02 has completed startup, start 6425B-HQDC03-B but do not log on.
- After HQDC03 has completed startup, start 6425B-BRANCHDC01-B, but do not log on.
- Wait for BRANCHDC01 to finish startup before continuing to the next task.

► Task 2: Rename Default-First-Site-Name

- Run **Active Directory Sites and Services** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
- Rename Default-First-Site-Name to **HEADQUARTERS**.

► Task 3: Create a subnet and associate it with a site

- Create two subnets: **10.0.0.0/24** and **10.0.1.0/24**, and associate each with the **HEADQUARTERS** site.

Results: After this exercise, you should have a site named HEADQUARTERS and two subnets (10.0.0.0/24 and 10.0.1.0/24) associated with the site.

Exercise 2: Create Additional Sites

In this exercise, you will create a second site and associate a subnet with it.

The main tasks for this exercise are as follows:

1. Create additional sites.
2. Create subnets and associate them with sites.

► Task 1: Create additional sites

- Create a site named **HQ-BUILDING-2**.
- Create a site named **BRANCHA**.

► Task 2: Create subnets and associate them with sites

- Create a subnet, **10.1.0.0/24**, and associate it with the **HQ-BUILDING-2** site.
- Create a subnet, **10.2.0.0/24**, and associate it with the **BRANCHA** site.

Results: After this exercise, you should have created 2 new sites, HQ-BUILDING-2 and BRANCHA, and associated them with the 10.1.0.0/24 and 10.2.0.0/24 subnets.

Exercise 3: Move Domain Controllers into Sites

► Task 1: Move domain controllers to new sites

- Move HQDC03 to the **HQ-BUILDING-2** site.
- Move BRANCHDC01 to the **BRANCHA** site.



Important: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs in this module.

Lab Review Questions

Question: You have a site with 50 subnets, each with a subnet address of 10.0.x.0/24, and you have no other 10.0.x.0 subnets, what could you do to make it easier to identify the 50 subnets and associate them with a site?

Question: Why is it important that all subnets are identified and associated with a site in a multisite enterprise?

Lab B: Configure the Global Catalog and Application Partitions

- Exercise 1: Configure a Global Catalog
- Exercise 2: Configure Universal Group Membership Caching
- Exercise 3: Examine DNS and Application Directory Partitions

Logon information

Virtual machine	6425B-HQDC01-B	6425-HQDC02-B	6425B-HQDC03-B	6425B-BRANCHDC01-B
Logon user name	Pat.Coleman	Do not log on	Do not log on	Do not log on
Administrative user name	Pat.Coleman_Admin			
Password	Pa\$\$w0rd			

Estimated time: 30 minutes

Scenario

You are the administrator of Contoso, Ltd. In your continued effort to improve the availability and resiliency of the directory service, you decide to configure additional global catalog servers and universal group membership caching. You are also curious about the relationship between Active Directory-integrated DNS zones and the DNS application partitions.

Exercise 1: Configure a Global Catalog

The first domain controller in a forest acts as a GC server. You might want to place GC servers in additional locations to support directory queries, logon, and applications such as Exchange Server. In this exercise, you will configure BRANCHDC01 to host a replica of the partial attribute set—the global catalog.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Configure a global catalog server.

► Task 1: Start and log on to the virtual machines

The virtual Machines should already be started and available after completing Lab A. However, if they are not, you should complete the below steps then step through Exercises 1 to 3 in Lab A before continuing.

1. Start 6425B-HQDC01-B, and log on as **Pat.Coleman** with the password **Pa\$\$w0rd**. This virtual machine may take several minutes to start.
2. After logging on to HQDC01, start 6425B-HQDC02-B but do not log on.
3. After HQDC02 has completed startup, start 6425B-HQDC03-B but do not log on.
4. After HQDC03 has completed startup, start 6425B-BRANCHDC01-B but do not log on.
5. Wait for BRANCHDC01 to finish startup before continuing to the next task.

► Task 2: Configure a global catalog server

1. Run **Active Directory Sites and Services** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Configure HQDC02 to be a global catalog server.
3. Confirm that BRANCHDC01 is a global catalog server.

Results: After this exercise, you should have configured HQDC02 to be a global catalog server and confirmed that BRANCHDC01 is already a global catalog server.

Exercise 2: Configure Universal Group Membership Caching

In sites without GC servers, user logon might be prevented if the site's domain controller is unable to contact a GC server in another site. To reduce the likelihood of this scenario, you can configure a site to cache the membership of universal groups. In this exercise, you will create a site to reflect a branch office and configure the site to cache universal group membership.

The main tasks for this exercise are as follows:

- Configure universal group membership caching.
-
- **Task 1: Configure universal group membership caching**
 - Configure the NTDS Site Settings of BRANCHA so that domain controllers cache universal group membership.

Results: After this exercise, you should have configured domain controllers in BRANCHA to cache universal group membership.

Exercise 3: Examine DNS and Application Directory Partitions

In this exercise, you will explore the DNS records related to replication and the DomainDnsZone application directory partition, using ADSI Edit.

The main tasks for this exercise are as follows:

1. Examine DNS records related to replication.
2. Examine the DNS application directory partition.

► Task 1: Examine DNS records related to replication

1. Run **DNS Manager** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Examine the service locator records in **_tcp.HEADQUARTERS._sites.contoso.com**
3. Examine the service locator records in **_tcp.BRANCHA._sites.contoso.com**.

► Task 2: Examine the DNS application directory partition

1. Click **Start>Administrative Tools >ADSI Edit** and enter administrative credentials when prompted. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, right-click **ADSI Edit**, and then click **Connect To**.
3. In the **Select a well known naming context** drop-down list, select **Configuration**.
4. Accept all other defaults. Click **OK**.
5. In the console tree, click **Configuration**, and then expand it.
6. In the console tree, click **CN=Configuration, DC=contoso, DC=com**, and then expand it.
7. In the console tree, click **CN=Partitions**.
8. Right-click **ADSI Edit**, and then click **Connect To**.
9. Click **Select or type a distinguished name or naming context**.
10. In the combo box, type **DC=DomainDnsZones,DC=contoso,DC=com**. Click **OK**.

11. In the console tree, click **Default Naming Context**, and then expand it.
12. Click on **DC=DomainDnsZones,DC=contoso,DC=com**, and then expand it.
13. Click on **CN=MicrosoftDNS**, and then expand it.
14. Click **DC=contoso.com**.
15. Examine the objects in this container. Compare the records to the DNS records you examined in the previous exercise.

Results: After this exercise, you should have explored the DNS records and the application directory partition for DNS in the contoso.com domain.



Important: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs in this module.

Lab Review Questions

Question: Describe the relationship between the records you viewed in ADSI Edit and the records you viewed in DNS Manager.

Question: When you examined the DNS records in `_tcp.BRANCHA._sites.contoso.com`, what domain controller was registering service locator records in the site? Explain why it did so.

Lab C: Configure Replication

- Exercise 1: Create a Connection Object
- Exercise 2: Create Site Links
- Exercise 3: Move Domain Controllers into Sites
- Exercise 4: Designate a Preferred Bridgehead Server
- Exercise 5: Configure Intersite Replication

Logon information

Virtual machine	6425B-HQDC01-B	6425-HQDC02-B	6425B-HQDC03-B	6425B-BRANCHDC01-B
Logon user name	Pat.Coleman	Do not log on	Do not log on	Do not log on
Administrative user name	Pat.Coleman_Admin			
Password	Pa\$\$w0rd			

Estimated time: 30 minutes

Scenario

You are the administrator of Contoso, Ltd. You want to optimize replication of AD DS by aligning replication with your network topology and domain controller roles and placement.

Exercise 1: Create a Connection Object

It is a best practice to configure direct replication between a domain controller that will be a standby operations master and the domain controller that is currently the operations master. Then, if the current operations master needs to be taken offline, the standby operations master is as up to date as possible with the operations master. In this exercise, you will create a connection object between HQDC01 and HQDC02, where HQDC02, the standby operations master, replicates from HQDC01, the current operations master.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Create a connection object.

► Task 1: Start and log on to the virtual machines

The virtual Machines should already be started and available after completing Labs A and B. However, if they are not, you should complete the below steps then step through Exercises 1 to 3 in Labs A and B before continuing.

- Start 6425B-HQDC01-B, and log on as **Pat.Coleman** with the password **Pa\$\$w0rd**. This virtual machine may take several minutes to start.
- After logging on to HQDC01, start 6425B-HQDC02-B but do not log on.
- After HQDC02 has completed startup, start 6425B-HQDC03-B but do not log on.
- After HQDC03 has completed startup, start BRANCHDC01-B but do not log on.
- Wait for BRANCHDC01 to finish startup before continuing to the next task.

► **Task 2: Create a connection object**

- Run **Active Directory Sites and Services** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
- In the console tree, expand **HEADQUARTERS, Servers**, and **HQDC02**, and then click the **NTDS Settings** node below **HQDC02**.
- Right-click **NTDS Settings** and click **New Active Directory Domain Services Connection**.
- In the **Find Active Directory Domain Controllers** dialog box, select **HQDC01**, and then click **OK**, and answer **Yes** to the warning message.
- In the **New Object – Connection** dialog box, type the name **HQDC01 - OPERATIONS MASTER**, and click **OK**.

Results: After this exercise, you should have created a connection object to replicate changes from HQDC01 to HQDC02.

Exercise 2: Create Site Links

In this exercise, you will create site links between the headquarters and the other sites, creating a hub-and-spoke replication topology.

The main tasks for this exercise are as follows:

- Create site links.

► Task 1: Create site links

- Rename the **DEFAULTSITELINK** to **HQ-HQB2**, and modify it so that it includes only the **HEADQUARTERS** and **HQ-BUILDING-2** sites.
- Create a new IP site link named **HQ-BRANCHA** that includes the **HEADQUARTERS** and **BRANCHA** sites.

Results: After this exercise, you should have two site links, one that links the **HEADQUARTERS** and **HQ-BUILDING-2** sites, and one that links **HEADQUARTERS** and **BRANCHA**.

Exercise 3: Move Domain Controllers into Sites

When you promote a domain controller, you can select the site for the DC and, by default, it will be in the site associated with the DC's IP address. If you modify sites and subnets after domain controllers are already in place, you must move the existing domain controllers into the correct sites. In this exercise, you will move domain controllers into the sites you have created in this module's Labs.

The main tasks for this exercise are as follows:

- Move domain controllers to new sites.

► Task 1: Move domain controllers to new sites

- Move BRANCHDC01 into the **BRANCHA** site.

Results: After this exercise, you should have moved BRANCHDC01 to the BRANCHA site.

Exercise 4: Designate a Preferred Bridgehead Server

You can designate a preferred bridgehead server that will handle replication to and from its site. This is useful when you want to assign the role to a domain controller in a site with greater system resources or when firewall considerations require that the role be assigned to a single, fixed system. In this exercise, you will designate a preferred bridgehead server for the site.

The main tasks for this exercise are as follows:

- Designate a preferred bridgehead server.
-
- ▶ **Task 1: Designate a preferred bridgehead server**
 - Configure HQDC02 as a preferred bridgehead server. When you do so, a lengthy warning message appears. Read the message. You will discuss it at the end of the Lab. Then click **OK**.

Results: After this exercise, you should have designated HQDC02 as a preferred bridgehead server.

Exercise 5: Configure Intersite Replication

After you have created site links and, optionally, designated bridgehead servers, you can continue to refine and control replication by configuring properties of the site link. In this exercise, you will reduce the intersite replication polling frequency, and you will increase the cost of a site link.

The main tasks for this exercise are as follows:

- Configure Intersite Replication.

► Task 1: Configure Intersite Replication

- Configure the replication interval for the **HQ-HQB2** site link to **15** minutes.
- Configure the replication interval for the **HQ-BRANCHA** site link to **15** minutes, and the cost to **200**.
- Examine the replication schedule for the **HQ-BRANCHA** site link. Experiment with configuring the schedule but click **Cancel** when you are finished.

Results: After this exercise, you should have configured the intersite replication interval to 15 minutes for all site links.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: Explain the warning message that appeared when you designated HQDC02 as a preferred bridgehead server.

Question: What are the advantages of reducing the intersite replication interval? What are the disadvantages?

Question: Is the procedure you performed in Exercise 2 enough to create a "hub and spoke" replication topology, which ensures that all changes from branches are replicated to the headquarters before being replicated to other branches? If not, what must still be done?

Module 13

Lab Instructions: Directory Service Continuity

Contents:

Lab A: Monitor Active Directory Events and Performance

Exercise 1: Monitor Real-Time Performance Using Task Manager and Resource Monitor 3

Exercise 2: Use Reliability Monitor and Event Viewer to Identify Performance-Related Events 6

Exercise 3: Monitor Events on Remote Computers with Event Subscriptions 9

Exercise 4: Attach Tasks to Event Logs and Events 11

Exercise 5: Monitor AD DS with Performance Monitor` 12

Exercise 6: Work with Data Collector Sets 14

Lab B: Manage the Active Directory Database

Exercise 1: Perform Database Maintenance 19

Exercise 2: Work with Snapshots and Recover a Deleted User 21

Lab C: Back Up and Restore Active Directory

Exercise 1: Back Up Active Directory 27

Exercise 2: Restore Active Directory and a Deleted OU 29

Lab A: Monitor Active Directory Events and Performance

- Exercise 1: Monitor Real-Time Performance Using Task Manager and Resource Monitor
- Exercise 2: Use Reliability Monitor and Event Viewer to Identify Performance-Related Events
- Exercise 3: Monitor Events on Remote Computers with Event Subscriptions
- Exercise 4: Attach Tasks to Event Logs and Events
- Exercise 5: Monitor AD DS with Performance Monitor
- Exercise 6: Work with Data Collector Sets

Logon information

Virtual machine	6425B-HQDC01-B	6425B-HQDC02-B
Logon user name	Pat.Coleman	Pat.Coleman
Administrative user name	Pat.Coleman_Admin	Pat.Coleman_Admin
Password	Pa\$\$w0rd	Pa\$\$w0rd

Estimated time: 60 minutes

Scenario

Last month, the only domain controller in the branch office failed, causing Contoso's call center to be offline for an entire day and costing the company a significant amount of money in lost revenue. You were hired to replace the administrator who had configured a critical location without redundant authentication or monitoring. This week, you are working to configure monitoring to ensure that performance and reliability can be watched on an ongoing basis for any signs of trouble.

Exercise 1: Monitor Real-Time Performance Using Task Manager and Resource Monitor

In this exercise, you will use Task Manager and Resource Monitor to examine real-time performance at a high level, which can help you to identify performance bottlenecks and processes or services that are consuming too many system resources.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Monitor real-time performance with Task Manager.
3. Monitor real-time performance with Resource Monitor.

► Task 1: Prepare for the lab

- Start 6425B-HQDC01-B and log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.
- Run **D:\Labfiles\Lab13a\Lab13a_Setup.bat** with administrative credentials. Use the account **Administrator** with the password **Pa\$\$w0rd**.
- The lab setup script runs. When it is complete, press any key to continue.
- Close the Windows Explorer window, **Lab13a**.
- Start 6425B-HQDC02-B.
- Log on to HQDC02 as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 2: Monitor real-time performance with Task Manager

1. On HQDC01, press CTRL+SHIFT+ESC to launch Task Manager.
2. Click the **Processes** tab and examine the commands available when you right-click **taskmgr.exe**. Examine the properties of a process by opening the **Properties** dialog box for **taskmgr.exe**.
3. Show processes from all users, which requires administrative credentials. Authenticate as **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
4. On the **Services** tab, stop and then start the **Dnscache** service.
5. Right-click the **Dnscache** service, and then click **Go to Process**.

Question: What process is hosting the DNS Client service?

6. Right-click the process and choose **Go to Service(s)**.

Question: The Services tab exposes a subset of the most-used functionality of which administrative snap-in?

7. Click the **Services** button. The **Services** console appears. Close the **Services** console.
8. Click the **Users** tab. This tab displays users who have either local (console) or remote desktop connections to the server.
9. Click the **Networking** tab.

This tab provides an overview of performance for each available network adapter.

10. Click the **Performance** tab.

This tab provides an overview of performance for CPU utilization and memory.

Question: Which major system component is *not* shown by task manager?

► **Task 3: Monitor real-time performance with Resource Monitor**

1. In Task Manager, on the **Performance** tab, click the **Resource Monitor** button.
If you are prompted for administrative credentials, use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Resource Monitor appears. Maximize the **Resource Monitor** window and close Task Manager.
3. Click the **CPU** graph. How much CPU utilization is being generated by Reliability and Performance Monitor itself?
4. Click the **CPU** graph again. The **CPU** section collapses.

5. Click the **Disk** graph. Which file is experiencing the most Read activity? Which process is causing the Read activity for that file? Which file is experiencing the most Write activity? Which process is causing the Write activity for that file?

To view the activity of the page file, click the File column label. If C:\pagefile.sys is not listed, open an application such as Server Manager, which should generate some paging activity.

Question: How many processes are reading from or writing to pagefile.sys?

Question: If the pagefile Read and Write activity is consistently high, what system component should be augmented?

6. Close Resource Manager. Click the **Start** button and run **perfmon** as an administrator with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.

Users, members of the Performance Monitor Users group, members of the Performance Log Users group, and members of the local Administrators group, are able to access increasing levels of functionality from WRPM.

The home view for the console is the Resource Overview, equivalent to Resource Monitor. Note that the console tree contains each of the WRPM snap-ins. Close Reliability and Performance Monitor.

7. Click the **Start** button and run **perfmon /res** as an **Administrator**, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**. This is an alternate way to open Resource Monitor, which you have opened from Task Manager, and which is the home view of the Reliability and Performance Monitor console. Close Resource Monitor.

Results: After this exercise, you will have used both Task Manager and Resource Monitor to monitor real-time performance of processes, services, and system components including disk, memory, network and CPU.

Exercise 2: Use Reliability Monitor and Event Viewer to Identify Performance-Related Events

In this exercise, you will use Reliability Monitor to examine stability-related events. You will then use Event Viewer to identify events related to performance and reliability, and you will learn how to work with custom views.

The main tasks for this exercise are as follows:

1. Monitor stability-related events with Reliability Monitor.
2. Identify role-related events with Server Manager.
3. Examine the event logs.
4. Create a custom view.
5. Export a custom view.
6. Import a custom view.

► Task 1: Monitor stability-related events with Reliability Monitor

1. Run **Server Manager** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Use Reliability Monitor to examine stability-related events that occurred on Sept 9, 2009.

► Task 2: Identify role-related events with Server Manager

1. In the root node of **Server Manager**, in the **Roles Summary** section, notice what icons appear next to the **ADDS** and **DNS Server** roles.
2. Click the link to the **ADDS** role in the **Roles Summary** section and examine the information in the **Events** section.
3. Click the **Filter Events** link in the **Events** section and remove **Information** events from the view.
4. Double-click an event to open its details, examine the event, and then close the event.
5. Note the information shown in the **System Services** section.

► Task 3: Examine the event logs

1. In the root of the Server Manager Event Viewer snap-in, in the **Summary of Administrative Events** section, expand the **Error** events summary. Double-click a summary row with **ActiveDirectory** as the source.
2. If you do not see a row in the summary with **ActiveDirectory** as the source, double-click another row in the **Error** events summary.

The Summary page events view opens in the details pane. This view "drills down" to show the events that were summarized on the row of the Error events summary.

Examine the logs in the Windows Logs and Applications and Services Logs nodes of the console tree.

Examine the events in the Administrative Events view. Right-click Administrative Events, and then click Properties. Note that the Description indicates that the view shows Critical, Error, and Warning events from all administrative logs. Click the Edit Filter button and note that this custom view cannot be modified—it is Read Only. Note also that it is difficult to know exactly which logs are being included in the Event Logs list. The information is truncated. Click the XML tab. Can you identify which logs are included using the information on the XML tab? In each XML Select element, what do you think Level refers to? Click Cancel twice to close the open dialog boxes.

► Task 4: Create a custom view

- In the **Custom Views** folder, create a custom view that displays **Critical**, **Warning**, and **Error** messages for the following logs: **DFS Replication**, **Directory Service**, and **DNS Server**. Name the log **Custom Directory Service Event View**.

► Task 5: Export a custom view

- Export the **Custom Directory Service Event View** as **D:\Data\DSEventView.xml**.

► **Task 6: Import a custom view**

1. On HQDC02, import the custom view `\\HQDC01\Data\DSEventView.xml` and name it **Custom Directory Service Event View**.
2. A **Query Error** message appears, because HQDC02 is not a DNS server and therefore has no **DNS Server** log. Click **OK**.

Results: After this exercise, you will have identified several places in Server Manager that expose events related to server roles and performance. You will also have created a custom view and imported that view to Event Viewer on another computer.

Exercise 3: Monitor Events on Remote Computers with Event Subscriptions

In this exercise, you will use the new event forwarding and subscription functionality of Windows Server 2008 to collect events from remote systems for centralized monitoring.

The main tasks for this exercise are as follows:

1. Configure computers to forward and collect events.
2. Create a subscription to collect events.
3. Generate events.
4. View forwarded events.

► Task 1: Configure computers to forward and collect events

1. On HQDC01, run the command prompt as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**. Type **wecutil qc**, then press ENTER, then press **Y**, then press ENTER to configure event collection.
2. On HQDC02, run the command prompt as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**. Type **winrm quickconfig**, then press ENTER, then press **Y**, then press ENTER to configure Windows Remote Management.

► Task 2: Create a subscription to collect events

1. On HQDC01, in the Server Manager Event Viewer snap-in, create a new subscription named **DC Services** that collects events from HQDC02. Configure the subscription to collect System log events with Event ID 7036. The subscription should use the user name **CONTOSO\Pat.Coleman_Admin**, and the password **Pa\$\$w0rd**. It should be configured to **Minimize Latency**. If Event Viewer messages appear when you complete the configuration, click **Yes**.
2. Confirm that in the **Subscriptions** folder, the new **DC Services** subscription shows a status of **Active**.

► **Task 3: Generate events**

- On HQDC02, at the command prompt, type **net stop dfsr** and press ENTER, then type **net start dfsr** and press ENTER.

► **Task 4: View forwarded events**

1. Switch to HQDC01.
2. In the Server Manager console tree, under **Event Viewer\Windows Logs**, click **Forwarded Events**.

Forwarded events may take several minutes to appear. If the events do not appear right away, wait a few minutes, start and stop the Distributed File System Replication (DFSR) service on HQDC02 again, then wait a few more minutes.

Results: After this exercise, you will have configured event subscriptions so that you can view events from HQDC02 on HQDC01.

Exercise 4: Attach Tasks to Event Logs and Events

In this exercise, you will invoke tasks when an event log is updated or when an event is generated.

The main tasks for this exercise are as follows:

1. Attach a task to an event log and to an event.
2. Prepare to view event viewer task messages.
3. Confirm that event viewer tasks are functioning.

► Task 1: Attach a task to an event log and to an event

1. On HQDC01, right-click the **Forwarded Events** event log and attach a task to the log. The task should display a message with the title, **Forwarded Event Received** and with the message, **A forwarded event was received**.
2. In the **Forwarded Events** event log, right-click one of the 7036 events and attach a task to the event. The task should display a message with the title, **DC Service Event** and with the message, **A service was started or stopped**.

► Task 2: Prepare to view event viewer task messages

When you choose to display a message in a task, because messages are displayed on the desktop of the user whose account is used to create the event viewer task (Pat.Coleman_Admin), you will need to log on interactively as Pat.Coleman_Admin to fully experience this simulation.

- Log off of HQDC01 and log on as **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.

► Task 3: Confirm that event viewer tasks are functioning

1. On HQDC02, at the Command Prompt, type **net stop dfsr** and press ENTER, then type **net start dfsr** and press ENTER.
2. On HQDC01, wait for the event viewer task messages to appear.

Results: After this exercise, you will have configured tasks to launch when an event is received in the Forwarded Events log and when a service is started or stopped on a remote machine.

Exercise 5: Monitor AD DS with Performance Monitor

In this exercise, you will use Performance Monitor to monitor the real-time performance of AD DS, to save performance counters, and to view a log of saved performance counters.

The main tasks for this exercise are as follows:

1. Configure Performance Monitor to monitor AD DS.
2. Create a Data Collector Set from Performance Monitor counters.
3. Start a Data Collector Set.
4. View a Data Collector Set report.

► Task 1: Configure Performance Monitor to monitor AD DS

1. On HQDC02, in Server Manager, open the **Performance Monitor** snap-in.
2. Add the following object performance counters:
 - **DirectoryServices\DRS Inbound Bytes Total/sec**
 - **DirectoryServices\DRS Outbound Bytes Total/sec**
 - **DirectoryServices\DS Threads In Use**
 - **DirectoryServices\DS Directory Reads/sec**
 - **DirectoryServices\DS Directory Writes/sec**
 - **DirectoryServices\DS Directory Searches/sec**
 - **Security System-Wide Statistics\Kerberos Authentications**
 - **DNS\UDP Query Received/sec**
3. Watch performance for a few moments. Then, in the counter list below the graph, select **UDP Query Received/sec**. Click the **Highlight** button in the toolbar to highlight that counter in the graph. Then click the **Highlight** button in the toolbar again to turn off the highlight.
4. Spend a few moments exploring the functionality of Performance Monitor. Do not add or remove counters, however.

► **Task 2: Create a Data Collector Set from Performance Monitor counters**

- Create a new Data Collector Set from the current view of Performance Monitor. Name the Data Collector Set **Custom ADDS Performance Counters**. Make a note of the default root directory in which the Data Collector Set will be saved.

► **Task 3: Start a Data Collector Set**

1. Click the **Data Collector Sets\User Defined** node, then right-click **Custom ADDS Performance Counters** and then click **Start**.
2. The **Custom ADDS Performance Counters** node is automatically selected. You can identify the individual data collectors in the Data Collector Set. In this case, only one data collector (the System Monitor Log performance counters) is contained in the Data Collector Set. You can also identify where the output from the data collector is being saved.
3. In the console tree, right-click the **Custom ADDS Performance Counters** data collector set, and then click **Stop**.

► **Task 4: View a Data Collector Set report**

- In the console tree, expand **Custom ADDS Performance Counters**, and then click **System Monitor Log.blg**. The graph of the log's performance counters is displayed.

Results: After this exercise, you will have created a Data Collector Set, allowed the Data Collector Set to run, and then viewed the data it contains.

Exercise 6: Work with Data Collector Sets

In this exercise, you will examine and run a Data Collector Set that is predefined when you add the AD DS role to a server. You will then create a custom Data Collector Set, configure its schedule and data management policies, run it, and examine its data.

The main tasks for this exercise are as follows:

1. Examine a predefined Data Collector Set.
2. Create a Data Collector Set.
3. Configure start conditions for a Data Collector Set.
4. Configure stop conditions for a Data Collector Set.
5. Configure data management for a data collector.
6. View the results of data collection.

► Task 1: Examine a predefined Data Collector Set

1. Select the **Active Directory Diagnostics** Data Collector Set under **Reliability and Performance\Data Collector Sets\System**. Notice what data collectors are part of the Data Collector Set.
2. Start the Data Collector Set.
3. Expand **Reports, System**, and **Active Directory Diagnostics**, and then click the report. The **Report Status** indicates that data is being collected for 300 seconds (five minutes). Wait five minutes or wait at least one minute, and then right-click **Active Directory Diagnostics** under **Data Collector Sets\System** and choose **Stop**.
4. Spend a few moments examining the sections of the report. Right-click the report and, using the **View** menu, examine the **Performance Monitor, Report**, and **Folder** views.
5. In the Folder view, double-click **Performance Counter** in the details pane. A new instance of WRPM is opened to display the log. The new instance may be minimized, in which case you can bring it to the front by clicking its button in the task bar. Examine the window, then close WPRM.

6. In the Server Manager console tree, select the **Performance Monitor** node. Click the **View Log Data** button, and configure the source for Performance Monitor to be **C:\PerfLogs\ADDS\report\Performance Counter**, where *report* is the same name as the report you just generated.

Note that no counters are immediately visible. Click the **Add** counter button, and add the following DirectoryServices object counters to the display: **DS Directory Reads/sec**, **DS Directory Searches/sec**, and **DSDirectoryWrites/sec**.

► Task 2: Create a Data Collector Set

1. In the Server Manager console tree, select the **User Defined** node underneath **Data Collector Sets**.
2. Create a new Data Collector Set named **Custom ADDS Diagnostics** using the predefined **Active Directory Diagnostics** Data Collector Set as a template. Save the new Data Collector Set in the **C:\ADDS Data Collector Sets** folder. Run the data collector set as **CONTOSO\Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.

In a production environment, the account you use should be a unique domain account. It must be a member of the Performance Log Users group and must have the Logon as a batch job user logon right. By default, the Performance Log Users group has this right, so you can simply create a domain account and make it a member of the group.

► Task 3: Configure start conditions for a Data Collector Set

- Configure the schedule for the new Data Collector Set to begin today, with an expiration date in one week. Configure the start time to a time five minutes from now. Make a note of the start time you configure. When prompted for credentials with which to run the scheduled task, use the user name **CONTOSO\Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.

► Task 4: Configure stop conditions for a Data Collector Set

- Configure the Stop Condition for the task to be an overall duration of two minutes. In a production environment, you would likely run a data collector for a longer period of time. Select the option to **Stop when all data collectors have finished**.

► **Task 5: Configure data management for a data collector**

- Configure the data manager resource policy to delete the oldest items and, every day, to copy cab files to \\hqdc01\ADDS_Diag_Reports. Ensure that **Create cab file** and **Delete data file** are selected. When prompted for credentials with which to run the scheduled task, use the user name **CONTOSO\Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.

► **Task 6: View the results of data collection**

1. Wait until the time that you configured as the start time for the Data Collector Set passes. Select the report under **Reports\User Defined\Custom ADDS Diagnostics** and note that the **Report Status** indicates that data is being collected for 120 seconds (two minutes). After data collection has completed, the **Report Status** indicates that the report is being generated.

Spend a few moments examining the report.

2. Right-click the report in the console tree, then point to **View**, and then select **Folder**. Double-click **Performance Counter** in the details pane.

A new instance of Reliability and Performance Monitor opens, with Performance Monitor displaying the logged data in the **Performance Counter** log. Spend a few moments examining the performance graph, and then close the window.

Results: After this exercise, you will have examined a predefined Data Collector Set, created a custom Data Collector Set, run the set on a schedule, and viewed its results.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs in this module.

Lab Review Questions

Question: In what situations do you currently use, or can you envision using, event subscriptions as a monitoring tool?

Question: To what events or performance counters would you consider attaching e-mail notifications or actions? Do you use notifications or actions currently in your enterprise monitoring?

Lab B: Manage the Active Directory Database

- Exercise 1: Perform Database Maintenance
- Exercise 2: Work with Snapshots and Recovering a Deleted User

Logon information

Virtual machine	6425B-HQDC01-B	6425B-HQDC02-B
Logon user name	Pat.Coleman	Pat.Coleman
Administrative user name	Pat.Coleman_Admin	Pat.Coleman_Admin
Password	Pa\$\$w0rd	Pa\$\$w0rd

Estimated time: 30 minutes

Scenario

You are the administrator of Contoso, Ltd., an online university. At the end of the semester, 65 days ago, you deleted 835 user accounts for students who have graduated or will no longer return to the program. You now want to compact your Active Directory database to reclaim the space released by that many deleted objects. Additionally, you were notified that yesterday, one user account, Adriana Giorgi, was deleted by accident. You want to recover that account with a snapshot you have scheduled to run each night at 1:00 a.m.

Exercise 1: Perform Database Maintenance

In this exercise, you will perform maintenance on the Active Directory database. To do so, you will need to stop the AD DS service and restart it when the maintenance is complete.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Prepare to compact the Active Directory database.
3. Stop the AD DS service.
4. Compact the Active Directory database.
5. Replace the Active Directory database with the compacted copy.
6. Verify the integrity of the compacted database.
7. Start the AD DS service.

► Task 1: Prepare for the lab

The virtual machines should already be started and available after completing Lab A. However, if they are not, you should complete the below steps.

1. Start 6425B-HQDC01-B and log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.
2. Start 6425B-HQDC02-B but do not log on.

► Task 2: Prepare to compact the Active Directory database

1. Run the command prompt as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. From the command prompt, create two folders: **D:\NTDSCompact** and **D:\NTDSOriginal**.

► Task 3: Stop the AD DS service

1. Run the **Services** console as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Stop the AD DS service.

► **Task 4: Compact the Active Directory database**

- Use **NTDSUtil** to activate the NTDS instance and to compact the database file to **D:\NTDSCompact**.

► **Task 5: Replace the Active Directory database with the compacted copy**

1. Move the old version of **NTDS.dit** and all *.log files from **%systemroot%\NTDS** to **D:\NTDSOriginal** to preserve them in the event that the compaction did not succeed or caused corruption.
2. Copy the compacted **NTDS.dit** from **D:\NTDSCompact** to **%systemroot%\NTDS\ntds.dit**.

► **Task 6: Verify the integrity of the compacted database**

- Use **NTDSUtil** to activate the NTDS instance, to perform an integrity check, and to perform a semantic database analysis in fixup mode.

► **Task 7: Start the AD DS service**

1. Switch to the **Services** console.
2. Start the AD DS service.
3. Close the **Services** console.

Results: After this exercise, you will have stopped AD DS, compacted the Active Directory database, performed integrity and semantic checking, and restarted AD DS.

Exercise 2: Work with Snapshots and Recover a Deleted User

In this exercise, you will create and mount an Active Directory snapshot, and you will use the information to help you repopulate attributes of a deleted user object.

The main tasks for this exercise are as follows:

1. Create a snapshot of Active Directory.
2. Make a change to Active Directory.
3. Mount an Active Directory snapshot and create a new instance.
4. Explore a snapshot with Active Directory Users and Computers.
5. Use LDP to restore a deleted object (OPTIONAL).

► Task 1: Create a snapshot of Active Directory

- From the elevated command prompt, type the following commands:

```
ntdsutil  
snapshot  
activate instance ntds  
create  
quit  
quit
```

The command returns a message indicating that the snapshot set was generated successfully. The GUID that is displayed is important for commands in later tasks. Make a note of the GUID or, alternatively, copy it to the Clipboard.

► Task 2: Make a change to Active Directory

1. Run Active Directory Users and Computers as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Delete **Adriana Giorgi's** account in the **User Accounts\Employees** organizational unit (OU).

► **Task 3: Mount an Active Directory snapshot and create a new instance**

1. From the elevated command prompt, type the following commands:

```
ntdsutil  
activate instance ntds  
snapshot  
list all
```

The command returns a list of all snapshots.

2. Type the following commands:

```
mount guid  
quit  
quit
```

where *guid* is the GUID of the snapshot you created.

3. Start an instance of Active Directory using the snapshot by typing the following command, all on one line.

```
dsamain -dbpath c:\$snap_datetime_volume$\windows\ntds\ntds.dit -  
ldapport 50000
```

Note that *datetime* will be a value that is unique for you. There should only be one folder on your drive C with a name that begins with *\$snap*.

A message indicates that Active Directory Domain Services startup is complete. Leave Dsamain.exe running. Do not close the command prompt.

► **Task 4: Explore a snapshot with Active Directory Users and Computers**

1. Switch to **Active Directory Users and Computers**. Right-click the root node of the snap-in and choose **Change Domain Controller**. Type the directory server name and port **HQDC01:50000**, and then press ENTER. Click **OK**.
2. Locate **Adriana Giorgi's** object in the **User Accounts\Employees** OU. Note that **Adriana Giorgi's** object is displayed because the snapshot was taken prior to deleting it.

► **Task 5 (Optional): Use LDP to restore a deleted object**

Restoring a deleted user account is a task that is not directly related to snapshots. You use the Ldp.exe command to reanimate objects from the Deleted Objects container of Active Directory. A deleted object is stripped of most of its attributes, so a snapshot can be helpful to examine attributes of the object prior to its deletion.

1. Click the **Start** button. In the **Start Search** box, type **LDP.exe** and press CTRL+SHIFT+ENTER, which executes the command as an administrator.
The User Account Control dialog box appears.
2. Click **Use another account**.
3. In **User name**, type **Pat.Coleman_Admin**.
4. In **Password**, type **Pa\$\$w0rd**, and then press ENTER.
LDP opens.
5. Click the **Connection** menu, then click **Connect**, and then click **OK**.
6. Click the **Connection** menu, then click **Bind**, and then click **OK**.
7. Click the **Options** menu, and then click **Controls**.
8. In the **Load Predefined** list, click **Return Deleted Objects**, and then click **OK**.
9. Click the **View** menu, then click **Tree**, and then click **OK**.
10. In the console tree, expand **DC=contoso,DC=com**, and then double-click **CN=Deleted Objects,DC=contoso,DC=com**.
11. Right-click **CN=Adriana Giorgi**, and then click **Modify**.
12. In the **Attribute** box, type **isDeleted**.
13. In the **Operation** section, click **Delete**.
14. Click the ENTER button.
15. In the **Attribute** box, type **distinguishedName**.
16. In the **Values** box, type **CN=Adriana Giorgi,OU=Employees,OU=User Accounts,DC=contoso,DC=com**.
17. In the **Operation** section, click **Replace**.
18. Click the ENTER button.
19. Select the **Extended** check box.

20. Click the **Run** button.
21. Click the **Close** button.
22. Close LDP.
23. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
24. In the console tree, expand the **contoso.com** domain, and the **User Accounts** OU, and then click the **Employees** OU.
25. Note that Adriana Giorgi's account is restored; however, all attributes are missing, including the description and the password. Because the password is missing, the account has been disabled.
26. Switch to the instance of Active Directory Users and Computers that is displaying the snapshot data.
27. Note that you can use the attributes contained in the snapshot to manually repopulate attributes in Active Directory.
28. Close both instances of Active Directory Users and Computers.

► **Task 6: Unmount an Active Directory snapshot**

1. In the command prompt, press CTRL+C to stop **DSAMain.exe**.
2. Type the following commands:

```
ntdsutil  
activate instance ntds  
snapshot  
unmount guid quit  
quit
```

where guid is the GUID of the snapshot.

Results: After this exercise, you will have created, mounted, and examined a snapshot of Active Directory and, optionally, restored a deleted user account.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs in this module.

Lab Review Questions

Question: In what other situations might it be useful to mount a snapshot of Active Directory?

Question: What are the disadvantages of restoring a deleted object with a tool such as LDP?

Lab C: Back Up and Restore Active Directory

- Exercise 1: Back up Active Directory
- Exercise 2: Restore Active Directory and a Deleted OU

Logon information

Virtual machine	6425B-HQDC01-B	6425B-HQDC02-B
Logon user name	Pat.Coleman	Pat.Coleman
Administrative user name	Pat.Coleman_Admin	Pat.Coleman_Admin
Password	Pa\$\$wOrd	Pa\$\$wOrd

Estimated time: 30 minutes

Scenario

As administrator of Contoso, it is your responsibility to ensure that the directory service is backed up. Today, you noticed that last night's backup did not run as scheduled. You therefore decided to perform an interactive backup. Shortly after the backup, a domain administrator accidentally deletes the Employees OU. Luckily, you are able to restore the OU with the backup you just made.

Exercise 1: Back Up Active Directory

In this exercise, you will install the Windows Server Backup feature, and then use it to schedule a backup of Active Directory. You also will perform an interactive backup of the system volume.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Install the Windows Server Backup feature.
3. Create a scheduled backup.
4. Perform an interactive backup.

► Task 1: Prepare for the lab

The virtual machines should already be started and available after completing Labs A and B. However, if they are not, you should complete the below steps.

1. Start 6425B-HQDC01-B and log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.
2. Start 6425B-HQDC02-B and log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 2: Install the Windows Server Backup feature

1. On HQDC01, run Server Manager as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Install all of the Windows Server Backup features.

► Task 3: Create a scheduled backup

1. Run **Windows Server Backup** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the Actions pane, click the **Backup Schedule** link.
The Backup Schedule Wizard appears.
3. On the **Getting Started** page, click **Next**.
4. On the **Select backup configuration** page, click **Custom**, and then click **Next**.

5. On the **Select backup items** page, clear the **6425B (D:)** drive check box, and then click **Next**.
6. On the **Specify backup time** page, select **Once a day**.
7. In the **Select time of day** list, select **12:00 am**.
8. Click **Next**.
9. On the **Select destination disk** page, click **Show All Available Disks**.
The Show All Available Disks dialog box appears.
10. Select the **Disk 1** check box, and then click **OK**.
11. On the **Select destination disk** page, select the **Disk 1** check box, and then click **Next**.
The Windows Server Backup dialog box appears, informing you that all data on the disk will be deleted.
12. Click **Yes** to continue.
13. On the **Label destination disk** page, click **Next**.
14. On the **Confirmation** page, click **Cancel** to avoid formatting drive D.

► **Task 4: Perform an interactive backup**

1. In the Windows Server Backup window, in the Actions pane, click **Backup Once**.
2. Configure the backup to use the following settings:
 - **Backup type:** Custom
 - **Backup items:** C: drive only with Enable system recovery
 - **Advanced option:** VSS full backup
3. The backup will take about 10 to 15 minutes to complete. When the backup is complete, close Windows Server Backup.

Results: After this exercise, you will have installed the Windows Server Backup feature and used it to schedule a backup of the AD DS information, and to perform an interactive backup.

Exercise 2: Restore Active Directory and a Deleted OU

In this exercise, you will perform an authoritative restore of the AD DS database. You will then verify that the data is restored successfully.

The main tasks are as follows:

1. Delete the Employees OU.
2. Restart in Directory Services Restore Mode (DSRM).
3. Restore System State data.
4. Mark the restored information as authoritative and restart the server.
5. Verify that the deleted data has been restored.

► Task 1: Delete the Employees OU

1. Run **Active Directory Users and Computers** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Delete the **Contractors** OU within the **User Accounts** OU.
3. On HQDC02, run **Active Directory Users and Computers** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
4. Verify that the domain controller has replicated the deletion of the **Contractors** OU.

► Task 2: Restart in Directory Services Restore Mode (DSRM)

1. On HQDC01, run the command prompt as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Type **bcdedit /set safeboot dsrepair** to configure the server to start in Directory Services Restore Mode (DSRM).
3. Restart HQDC01.

► **Task 3: Restore System State data**

1. Log on as **Administrator** using the password **Pa\$\$w0rd**.
2. Run the command prompt as an administrator.
3. Type **wbadmin get versions -backuptarget:D: -machine:HQDC01** to get the version information for the backup.
4. Restore the System State information by typing **wbadmin start systemstaterecovery -version:version -backuptarget:D: -machine:HQDC01**.
i.e. **wbadmin start systemstaterecovery -version:10/14/2009-01:11 -backuptarget:D: -machine:HQDC01**
The restore will take about 30-35 minutes.

► **Task 4: Mark the restored information as authoritative, and then restart the server**

1. At the command prompt, use NTDS to perform an authoritative restore of **"OU=Contractors,OU=User Accounts,DC=contoso,DC=com"**.
2. To restart the server normally after you perform the restore operation, type **bcdedit /deletevalue safeboot**, and then press ENTER.
3. Restart the server.

► **Task 5: Verify that the deleted data has been restored**

1. After the server restarts, log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.
2. Run Active Directory Users and Computers as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
3. On HQDC02, refresh the view of **Active Directory Users and Computers**. Verify that the **Contractors** OU has also been restored on this domain controller.

Results: After this exercise, you will have performed an authoritative restore of Active Directory data to recover from the accidental deletion of an OU.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: What type of domain controller and directory service backup plan do you have in place? What do you expect to put in place after having completed this lesson and this Lab?

Question: When you restore a deleted user (or an OU with user objects) using authoritative restore, will the objects be exactly the same as before? What attributes might not be the same?

Module 14

Lab Instructions: Manage Multiple Domains and Forests

Contents:

Lab A: Raise Domain and Forest Functional Levels

Exercise 1: Raise the Domain Functional Level to Windows Server 2003 3

Exercise 2: Raise the Forest Functional Level to Windows Server 2003 5

Exercise 3: Raise the Domain Functional Level to Windows Server 2008 7

Lab B: Administer a Trust Relationship

Exercise 1: Configure DNS 10

Exercise 2: Create a Trust Relationship 11

Exercise 3: Validate a Trust Relationship 12

Exercise 4: Assign Permissions to Trusted Identities 13

Exercise 5: Implement Selective Authentication 15

Lab A: Raise Domain and Forest Functional Levels

- Exercise 1: Raise the Domain Functional Level to Windows Server 2003
- Exercise 2: Raise the Forest Functional Level to Windows Server 2003
- Exercise 3: Raise the Domain Functional Level to Windows Server 2008

Logon information

Virtual machine	6425B-TSTDC01-A
Logon user name	Sara.Davis
Administrative user name	Sara.Davis_Admin
Password	Pa\$\$w0rd

Estimated time: 30 minutes

Scenario

You are the domain administrator of Tailspin Toys. A branch office was the last location with a Windows 2000 domain controller, and you have just upgraded it to Windows Server 2008. You want to take advantage of functionality provided by higher domain and forest functional levels.

Exercise 1: Raise the Domain Functional Level to Windows Server 2003

In this exercise, you will attempt to take advantage of capabilities supported at the Windows Server 2003 domain functional level. You will see that these capabilities are not supported at lower domain functional levels. You will then raise the domain functional level. Finally, you will test the advanced capabilities to verify that they are now supported.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Confirm that the current domain functional level is Windows 2000 Native.
3. Experience functionality not supported by the Windows 2000 Native domain functional level.
4. Raise the domain functional level to Windows Server 2003.
5. Verify functionality supported by the Windows Server 2003 domain functional level.

► Task 1: Prepare for the lab

- Start 6425B-TSTDC01-A and log on as **Sara.Davis** with the password **Pa\$\$w0rd**.

► Task 2: Confirm that the current domain functional level is Windows 2000 Native

1. On TSTDC01, run **Active Directory Domains and Trusts** as an administrator, with the user name **Sara.Davis_Admin** and the password **Pa\$\$w0rd**
2. Confirm that the current domain functional level is Windows 2000 Native, but *do not raise the functional level*. Instead, cancel out of the dialog box.

► **Task 3: Experience functionality not supported by the Windows 2000 Native domain functional level**

1. Run Command Prompt as an administrator, with the user name **Sara.Davis_Admin** and the password **Pa\$\$w0rd**.
2. Type **redircmp.exe "ou=Client Computers,dc=tailspintoys,dc=com"** and press ENTER. A message appears indicating that redirection was not successful. This is because the domain functional level is not at least Windows Server 2003.
3. Type **redirusr.exe "ou=User Accounts,dc=tailspintoys,dc=com"** and press ENTER. A message appears indicating that redirection was not successful. This is because the domain functional level is not at least Windows Server 2003.

► **Task 4: Raise the domain functional level to Windows Server 2003**

- In **Active Directory Domains and Trusts**, raise the domain functional level to Windows Server 2003.

► **Task 5: Verify functionality supported by Windows Server 2003 domain functional level**

1. Run the Command Prompt as an administrator, with the user name **Sara.Davis_Admin** and the password **Pa\$\$w0rd**.
2. Type **redircmp.exe "ou=Client Computers,dc=tailspintoys,dc=com"** and press ENTER. A message appears indicating that redirection was successful.
3. Type **redirusr.exe "ou=User Accounts,dc=tailspintoys,dc=com"** and press ENTER. A message appears indicating that redirection was successful.

Results: After this exercise, you will have raised the domain functional level to Windows Server 2003 and confirmed that new functionality is enabled.

Exercise 2: Raise the Forest Functional Level to Windows Server 2003

In this exercise, you will attempt to take advantage of capabilities supported at the Windows Server 2003 forest functional level. You will see that these capabilities are not supported at lower forest functional levels. You will then raise the forest functional level. Finally, you will test the advanced capabilities to verify that they are now supported.

The main tasks for this exercise are as follows:

1. Confirm that the current forest functional level is Windows 2000 Native.
2. Experience functionality not supported by the Windows 2000 Native forest functional level.
3. Raise the forest functional level to Windows Server 2003.
4. Verify functionality supported by the Windows Server 2003 forest functional level.

► Task 1: Confirm that the current forest functional level is Windows 2000 Native

1. On TSTDC01, run **Active Directory Domains and Trusts** as an administrator, with the user name **Sara.Davis_Admin** and the password **Pa\$\$w0rd**.
2. Confirm that the current domain functional level is Windows 2000 Native, but *do not raise the functional level*. Instead, cancel out of the dialog box.

► Task 2: Experience functionality not supported by the Windows 2000 Native forest functional level

1. Run **Active Directory Users and Computers** as an administrator, with the user name **Sara.Davis_Admin** and the password **Pa\$\$w0rd**.
2. Right-click the **Domain Controllers** OU and attempt to create a new Read-Only domain controller account. Accept all defaults in the Active Directory Domain Services Installation Wizard.

You are prevented from creating an RODC account, and you are informed that the forest functional level must be Windows Server 2003 or higher.

- ▶ **Task 3: Raise the forest functional level to Windows Server 2003**
 - In **Active Directory Domains and Trusts**, raise the forest functional level to Windows Server 2003.

- ▶ **Task 4: Verify functionality supported by the Windows Server 2003 forest functional level**
 - In **Active Directory Users and Computers**, create a Read-Only domain controller account named **TSTDC03** in the **Domain Controllers** OU. Accept all default values in the Active Directory Domain Services Installation Wizard.

Exercise 3: Raise the Domain Functional Level to Windows Server 2008

In this exercise, you will attempt to take advantage of capabilities supported at the Windows Server 2008 domain functional level. You will see that these capabilities are not supported at lower domain functional levels. You will then raise the domain functional level. Finally, you will test the advanced capabilities to verify that they are now supported.

The main tasks for this exercise are as follows:

1. Confirm that the current domain functional level is lower than Windows Server 2008.
2. Confirm that DFS-R is not available at domain functional levels lower than Windows Server 2008.
3. Raise the domain functional level.
4. Confirm that DFS-R replication is available at the Server 2008 domain functional level.

► Task 1: Confirm that the current domain functional level is lower than Windows Server 2008

1. On TSTD01, run **Active Directory Domains and Trusts** as an administrator, with the user name **Sara.Davis_Admin** and the password **Pa\$\$w0rd**.
2. Confirm that the current domain functional level is Windows Server 2003, but *do not raise the functional level*. Instead, cancel out of the dialog box.

► Task 2: Confirm that DFS-R replication is not available at domain functional levels lower than Windows Server 2008

1. Run the Command Prompt as an administrator, with the user name **Sara.Davis_Admin** and the password **Pa\$\$w0rd**.
2. Type **dfsrmig /getglobalstate** and press ENTER. A message appears informing you that dfsrmig is supported only on domains at the Windows Server 2008 functional level.

► **Task 3: Raise the domain functional level**

- In **Active Directory Domains and Trusts**, raise the domain functional level to Windows Server 2008.
- Close Active Directory Domains and Trusts.

► **Task 4: Confirm that DFS-R replication is available at the Windows Server 2008 domain functional level**

- Switch to the command prompt. Type `dfsrmig /getglobalstate` and then press ENTER. A message appears informing you that DFS-R migration has not yet been initialized. This indicates that the feature is now available, but has not yet been initialized.

Results: After this exercise, you will have raised the domain functional level to Windows Server 2008 and confirmed that new functionality is available.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs.

Lab Review Questions

Question: Can you raise the domain functional level to Windows Server 2008 when your Microsoft Exchange server is still running Windows Server 2003?

Question: Can you raise the domain functional level of a domain to Windows Server 2008 when other domains contain domain controllers running Windows Server 2003?

Lab B: Administer a Trust Relationship

- Exercise 1: Configure DNS
- Exercise 2: Create a Trust Relationship
- Exercise 3: Validate a Trust Relationship
- Exercise 4: Assign Permissions to Trusted Identities
- Exercise 5: Implement Selective Authentication

Logon information

Virtual machine	6425B-HQDC01-A	6425B-TSTDC01-A
Logon user name	Pat.Coleman	Sara.Davis
Administrative user name	Pat.Coleman_Admin	Sara.Davis_Admin
Password	Pa\$\$w0rd	Pa\$\$w0rd

Estimated time: 45 minutes

Scenario

Contoso, Ltd. is forming a partnership with Tailspin Toys. A team of product developers at Tailspin Toys requires access to a shared folder in the Contoso domain. You must configure your domain to support this business requirement. Additionally, the inexperienced domain administrator at Tailspin Toys requires assistance configuring the reciprocal side of the trust relationship.

Exercise 1: Configure DNS

It is important for DNS to be functioning properly before you create trust relationships. Each domain must be able to resolve names in the other domain. In Module 10, you learned how to configure name resolution. There are several ways to support name resolution between two forests. In this exercise, you will create a stub zone in the contoso.com domain for the tailspintoys.com domain and a conditional forwarder in the tailspintoys.com domain to resolve contoso.com.

The main tasks for this exercise are as follows:

1. Prepare for the lab.
2. Configure DNS in contoso.com.
3. Configure DNS in tailspintoys.com.

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A and log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.
2. Start 6425B-TSTDC01-A and log on as **Sara.Davis** with the password **Pa\$\$w0rd**.

► Task 2: Configure DNS in contoso.com

1. On HQDC01, run DNS Management as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Create a stub zone for tailspintoys.com that refers to the IPv4 address **10.0.0.31** as the master server.

► Task 3: Configure DNS in tailspintoys.com

1. On TSTDC01, run **DNS Management** as an administrator, with the user name **Sara.Davis_Admin** and the password **Pa\$\$w0rd**.
2. Create a conditional forwarder for contoso.com that forwards to the IPv4 address **10.0.0.11**.

Results: After this exercise, you will have configured DNS name resolution between the contoso.com and tailspintoys.com domains.

Exercise 2: Create a Trust Relationship

In this exercise, you will create the trust relationship to enable authentication of Tailspin Toys users in the Contoso domain.

The main tasks for this exercise are as follows:

1. Identify the trusted and trusting domains.
2. Initiate the trust in the trusted domain.
3. Complete the trust in the trusting domain.

► Task 1: Identify the trusted and trusting domains

- Users in tailspintoys.com require access to a shared folder in contoso.com. Answer the following questions:
 - Which domain is the trusting domain, and which is the trusted domain?
 - Which domain has an outgoing trust, and which has an incoming trust?

► Task 2: Initiate the trust in the trusted domain

1. On HQDC01, run **Active Directory Domains and Trusts** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
2. Create a one-way, outgoing external trust relationship with tailspintoys.com. Configure the trust to use domain-wide authentication, and to use **Pa\$\$w0rd** as the initial trust relationship password.

► Task 3: Complete the trust in the trusting domain

1. On TSTDC01, run **Active Directory Domains and Trusts** as an administrator, with the user name **Sara.Davis_Admin** and the password **Pa\$\$w0rd**.
2. Create a one-way, incoming external trust relationship with contoso.com. Configure the trust to use domain-wide authentication, and to use **Pa\$\$w0rd** as the initial trust relationship password.

Results: After this exercise, you will have established a trust relationship between the contoso.com and tailspintoys.com domains, in which contoso.com is the trusted domain.

Exercise 3: Validate a Trust Relationship

In the previous exercise, you had the opportunity to confirm the trust relationship. You can also confirm or validate an existing trust relationship. In this exercise, you will validate the trust between contoso.com and tailspintoys.com.

The main task for this exercise is as follows:

- Validate a trust relationship.

► Task 1: Validate a trust relationship

- On HQDC01, use **Active Directory Domains and Trusts** to validate the trust between contoso.com and tailspintoys.com.

Results: After this exercise, you will have validated the trust between contoso.com and tailspintoys.com.

Exercise 4: Assign Permissions to Trusted Identities

In this exercise, you will provide access to a shared folder in the Contoso domain to the product team from Tailspin Toys.

The main task for this exercise is as follows:

- Assign permissions to trusted groups.

► Task 1: Assign permissions to trusted groups

1. On TSTDC01, run **Active Directory Users and Computers** as an administrator, with the user name **Sara.Davis_Admin** and the password **Pa\$\$w0rd**.
2. In the **User Accounts** OU, create a user account for **Pat Coleman** with the user logon name **Pat.Coleman** and the password **Pa\$\$w0rd**. Configure the password so that it does not have to be changed at first logon.
3. In the **tailspintoys.com** domain, create an OU named **Groups**.
4. In the **Groups** OU, create a global security group named **Product Team**.
5. On HQDC01, run **Active Directory Users and Computers** as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa\$\$w0rd**.
6. In the **Groups\Role** OU, create a global security group named **Product Developers**.
7. In the **Groups\Access** OU, create a domain local group named **ACL_Product Information_Modify**.
8. Create a folder named **Product Information** on drive C of HQDC01.
9. Give the **ACL_Product Information_Modify** group **Modify** permission to the **Product Information** folder.

10. Open the properties of the **ACL_ Product Information _Modify** group. Add the **Contoso Product Developers** and the **Tailspin Toys Product Team** as members.

When you do so, a Windows Security dialog box appears. Because the trust is one-way, your user account as the administrator of contoso.com (Pat.Coleman_Admin) does not have permissions to read the directory of the tailspintoys.com domain. You must have an account in tailspintoys.com to read its directory. If the trust were a two-way trust, this message would not have appeared. Your standard user account in the tailspintoys.com domain will be used to provide you Read Access to the directory service.

In the **User Name** box, type **TAILSPINTOYS\Pat.Coleman**. In the **Password** box, type **Pa\$\$w0rd**.

11. Note that the two global groups from the two domains are now members of the domain local group in the contoso.com domain that has access to the Product Information folder.

Results: After this exercise, you will have assigned resource access permissions to the Product Information folder in the Contoso domain to groups in both the Contoso and Tailspin Toys domains.

Exercise 5: Implement Selective Authentication

In this exercise, you will restrict the ability of users from the tailspintoys.com domain to authenticate with computers in the contoso.com domain.

The main task for this exercise is as follows:

- Implement selective authentication.

► Task 1: Implement selective authentication

- On HQDC01, use **Active Directory Domains and Trusts** to enable selective authentication for the trust between contoso.com and tailspintoys.com.

With selective authentication enabled, users from a trusted domain cannot authenticate against computers in the trusting domain, even if they've been given permissions to a folder. Trusted users must also be given the **Allowed To Authenticate** permission on the computer itself.

- In **Active Directory Users and Computers**, ensure that **Advanced Features** are enabled. Then open the properties of HQDC01 and give the **TAILSPINTOYS\Product Team** the **Allowed to Authenticate** permission.

When you do so, a Windows Security dialog box appears. Because the trust is one-way, your user account as the administrator of contoso.com (Pat.Coleman_Admin) does not have permissions to read the directory of the tailspintoys.com domain. You must have an account in tailspintoys.com to read its directory. If the trust were a two-way trust, this message would not have appeared. Your standard user account in the tailspintoys.com domain will be used to provide you Read Access to the directory service.

In the **User Name** box, type **TAILSPINTOYS\Pat.Coleman**. In the **Password** box, type **Pa\$\$w0rd**.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: You have given the Research and Development group from Tailspin Toys Modify permission to the Product Information folder on HQDC01. However, of the ten users in the group, only one user (who happens to also be a member of the Product Team group) has access. The others cannot access the folder. What must be done?

Question: A user from Contoso attempts to access a shared folder in the Tailspin Toys domain and receives an Access Denied error. What must be done to provide access to the user?

Module 1

Lab Answer Key: Introducing Active Directory Domain Services (AD DS)

Contents:

Exercise 1: Perform Post-Installation Configuration Tasks	2
Exercise 2: Install a New Windows Server 2008 Forest with the Windows Interface	6

Lab: Install an AD DS DC to Create a Single Domain Forest

Exercise 1: Perform Post-Installation Configuration Tasks

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-D.
2. Press ALT+DELETE, which sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine guest.
3. With the user name of Administrator present, In **Password**, type **Pa\$\$w0rd**, then press ENTER or click the log on arrow.

The Windows desktop appears and, after a moment, the Initial Configuration Tasks window opens.

► Task 2: Configure the display resolution

1. Minimize (do not close) the Initial Configuration Tasks window.
2. Right-click the desktop and choose **Personalize**.
3. Click **Display Settings**.
4. Drag the **Resolution** slider to **1024 by 768**.
5. Click **OK**.

You are prompted with the message *Do you want to keep these display settings?*

6. Click **Yes**.
7. Close the Personalization window.

► **Task 3: Configure the time zone**

1. Maximize the Initial Configuration Tasks window.
2. In the Initial Configuration Tasks window, click the **Set time zone** link.
3. Click **Change time zone**.
4. From the **Time zone** drop-down list, select the time zone that is appropriate for your location, and then click **OK**.
5. Click **OK** again.

► **Task 4: Change IP configuration**

1. In the Initial Configuration Tasks window, click the **Configure networking** link.
The Network Connections window appears.
2. Right-click **Local Area Connection** and choose **Properties**.
The Local Area Connection Properties dialog box appears.
3. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
Note that Windows Server 2008 also provides native support for Internet Protocol Version 6 (TCP/IPv6).
4. Click **Use the following IP address**. Enter the following configuration:
 - IP Address: **10.0.0.11**
 - Subnet Mask: **255.255.255.0**
 - Default Gateway: **10.0.0.1**
 - Preferred DNS Server: **10.0.0.11**
5. Click **OK**, and then click **Close**.
6. Close the Network Connections window.

► **Task 5: Rename the server HQDC01**

1. In the Initial Configuration Tasks window, click the **Provide computer name and domain** link.

The System Properties dialog box appears.

2. Click **Change**.
3. In the **Computer name** box, type **HQDC01**. Click **OK**.

You are prompted with the message *You must restart your computer to apply these changes*.

4. Click **OK**.
5. Click **Close**.

You are prompted with the message *You must restart your computer to apply these changes*.

6. Click **Restart Later**. If you accidentally click **Restart Now**, wait for the server to restart, and then log on as **Administrator** with the password **Pa\$\$w0rd**.

► **Task 6: Restart the server**

1. In the Initial Configuration Tasks window, note the **Add roles** and **Add features** links.

In the next exercise, you will use Server Manager to add roles and features to HQDC01. These links are another way to perform the same tasks.

By default, the Initial Configuration Tasks window will appear each time you log on to the server.

2. Select the **Do not show this window at logon** check box to prevent the window from appearing.

If you need to open the Initial Configuration Tasks window in the future, you do so by running the Oobe.exe command.

3. Click the **Close** button at the bottom of the window.

Server Manager appears.

Server Manager enables you to configure and administer the roles and features of a server running Windows Server 2008. You will use Server Manager in the next exercise.

At the bottom of the Server Manager window, a status message informs you, *Console cannot refresh until computer is restarted.*

4. Click the **Restart** link next to the status message.

You are prompted with the message *Do you want to restart now?*

5. Click **Yes**.

The computer restarts.

Exercise 2: Install a New Windows Server 2008 Forest with the Windows Interface

► Task 1: Add the Active Directory Domain Services role to HQDC01

1. Log on to HQDC01 as **Administrator** with the password **Pa\$\$w0rd**.
The Windows desktop appears and, after a moment, Server Manager opens.
If Server Manager does not open, click the Server Manager link in the Quick Launch next to the Start button.
2. In the **Roles Summary** section of the Server Manager home page, click **Add Roles**.
The Add Roles Wizard appears.
3. Click **Next**.
4. On the **Select Server Roles** page, select the check box next to **Active Directory Domain Services**. Click **Next**.
5. On the **Active Directory Domain Services** page, click **Next**.
6. On the **Confirm Installation Selections** page, click **Install**.
The Installation Progress page reports the status of installation tasks.
7. On the **Installation Results** page, confirm the installation succeeded, and then click **Close**.

In the Roles Summary section of Server Manager's home page, you'll notice an error message indicated by a red circle with a white "x." You'll also notice a message in the Active Directory Domain Services section of the Roles page. Both of these links will take you to the Active Directory Domain Services role page of Server Manager. The message shown reminds you that it is necessary to run dcpromo.exe, which you will do in the next task.

► **Task 2: Configure a new Windows Server 2008 forest named contoso.com with HQDC01 as the first domain controller**

1. In Server Manager, expand the **Roles** node in the tree pane, and then click **Active Directory Domain Services**.
2. Click the **Run the Active Directory Domain Services Installation Wizard (dcpromo.exe)** link.

The Active Directory Domain Services Installation Wizard appears.

3. Click **Next**.
4. On the **Operating System Compatibility** page, review the warning about the default security settings for Windows Server 2008 domain controllers, and then click **Next**.
5. On the **Choose a Deployment Configuration** page, click **Create a new domain in a new forest**, and then click **Next**.
6. On the **Name the Forest Root Domain** page, type **contoso.com**, and then click **Next**.

The system performs a check to ensure that the DNS and NetBIOS names are not already in use on the network.

7. On the **Set Forest Functional Level** page, choose **Windows Server 2008**, and then click **Next**.

The Additional Domain Controller Options page appears.

Each of the functional levels is described in the Details box on the page. Choosing Windows Server 2008 forest functional level ensures that all domains in the forest operate at the Windows Server 2008 domain functional level, which enables several new features provided by Windows Server 2008.

In a production environment, you would choose Windows Server 2008 forest functional level when creating a new forest if you require the features provided by the Windows Server 2008 domain functional level and if you will not be adding any domain controllers running operating systems prior to Windows Server 2008.

DNS Server is selected by default. The Active Directory Domain Services Installation Wizard will create a DNS infrastructure during AD DS installation.

The first domain controller in a forest must be a global catalog server and cannot be a read-only domain controller (RODC).

8. Click **Next**.

A Static IP assignment warning appears.

Because discussion of IPv6 is beyond the scope of this training kit, you did not assign a static IPv6 address to the server in Exercise 2. You did assign a static IPv4 address in Exercise 1, and other labs in this course will use IPv4. You can therefore ignore this error in the context of the exercise.

9. Click **Yes, the computer will use a dynamically assigned IP address (not recommended)**.

A warning appears that informs you that a delegation for the DNS server cannot be created.

In the context of this exercise, you can ignore this error. Delegations of DNS domains will be discussed later in this course.

10. Click **Yes** to close the Active Directory Domain Services Installation Wizard warning message.

11. On the **Location for Database, Log Files, and SYSVOL** page, accept the default locations for the database file, the directory service log files, and the SYSVOL files, and then click **Next**.

The best practice in a production environment is to store these files on three separate volumes that do not contain applications or other files not related to AD DS. This best practice design improves performance and increases the efficiency of backup and restore.

12. On the **Directory Services Restore Mode Administrator Password** page, type a **Pa\$\$w0rd** in both the **Password** and **Confirmed Password** boxes. Click **Next**.

In a production environment, you should use a very strong password for the Directory Services Restore Mode Administrator Password. Do not forget the password you assign to the Directory Services Restore Mode Administrator.

13. On the **Summary** page, review your selections.

If any settings are incorrect, click **Back** to make modifications.

14. Click **Next**.

Configuration of AD DS begins. After several minutes of configuration, the Completing the Active Directory Domain Services Installation Wizard page appears.

15. Click **Finish**.
16. Click **Restart Now**.
The computer restarts.
17. Continue with Task 3 (optional) or skip to Task 4.

► **Task 3: Examine the default configuration of the contoso.com forest and domain (OPTIONAL)**

1. Log on to HQDC01 as **Administrator** with the password **Pa\$\$w0rd**.
The Windows desktop appears and, after a moment, Server Manager opens.
2. Expand the **Roles** node in the tree pane, and expand the **Active Directory Domain Services** node.
3. Expand **Active Directory Users and Computers** and the **contoso.com** domain node.
4. Click the **Users** container in the tree.
The users and groups you see are available to any computer in the domain. For example, the domain's Administrator account can be used to log on to any computer in the domain, by default, and the Domain Users group is a member of the local Users group on each computer in the domain.
5. Click the **Builtin** container in the tree.
The groups you see are shared by and available to domain controllers, but not to member servers or workstations. For example, members of the Backup Operators group can perform backup and restore tasks on domain controllers only, and the Administrators group in the Builtin container represents the administrators of all domain controllers.
6. Select the **Computers** container in the tree.
It is empty. This is the default container for member servers and workstations.
7. Select the **Domain Controllers** organizational unit (OU) in the tree.
This is the OU into which domain controllers are placed. The computer object for HQDC01 appears in this OU.

► **Task 4: Shut down the virtual machine**

1. If you are not already logged on to HQDC01, log on to HQDC01 as **Administrator** with the password **Pa\$\$w0rd**.
2. If you are not already logged on to HQDC01, log on to HQDC01 as **Administrator** with the password **Pa\$\$w0rd**.
The Windows desktop appears and, after a moment, Server Manager opens.
3. Shut down HQDC01 and discard changes you made while doing this lab exercise.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Module 2

Lab Answer Key: Secure and Efficient Administration of Active Directory

Contents:

Lab A: Create and Run a Custom Administrative Console

Exercise 1: Perform Basic Administrative Tasks Using the Active Directory Users and Computers Snap-in 3

Exercise 2: Create a Custom Active Directory Administrative Console 6

Exercise 3: Perform Administrative Tasks with Least Privilege, Run As Administrator, and User Account Control 9

Lab B: Find Objects in Active Directory

Exercise 1: Find Objects in Active Directory 15

Exercise 2: Use Saved Queries 19

Lab C: Use DS Commands to Administer Active Directory

Exercise 1: Use DS Commands to Administer Active Directory 23

Lab A: Create and Run a Custom Administrative Console

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows® desktop appears.

Exercise 1: Perform Basic Administrative Tasks Using the Active Directory Users and Computers Snap-in

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
Pat.Coleman_Admin is a member of Domain Admins.
Server Manager opens automatically.
3. Close **Server Manager**.
4. Open **D:\Labfiles\Lab02a**.
5. Right-click **Lab02a_Setup.bat**, and then click **Run as administrator**.
A User Account Control dialog box appears.
6. Click **Continue**.
7. The lab setup script runs. When it is complete, press any key to continue.
8. Close the Windows Explorer window, **Lab02a**.

► Task 2: View objects

1. Click **Start**, and then click **Control Panel**.
2. If **Control Panel** is in the **Classic** view, double-click **Administrative Tools**.
If **Control Panel** is in the **Category** view, click **System and Maintenance** and then click **Administrative Tools**.
3. Double-click **Active Directory Users and Computers**.
A User Account Control dialog box appears.
4. Click **Continue**.
5. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.

► **Task 3: Refresh the view**

1. In the console tree, click the **Employees** OU.
2. Click the **Refresh** button in the snap-in toolbar or press **F5**.

► **Task 4: Create objects**

1. In the console tree, right-click **contoso.com**, then point to **New**, and then click **Organizational Unit**.
2. In the **Name** box, type **6425B**, and then click **OK**.

► **Task 5: Configure object attributes**

1. In the console tree, click the **Employees** OU.
2. In the details pane, right-click **Pat Coleman**, and then click **Properties**.
3. Click the **General** tab.
4. In **Office**, replace the current value with **Redmond**.
5. Click **OK**.

► **Task 6: View all object attributes**

1. In the console tree, click the **Employees** OU.
2. In the details pane, right-click **Pat Coleman**, and then click **Properties**.
3. Confirm that the **Attribute Editor** tab is not visible, and that there is no input control for the **division** property on any of the tabs.
4. Close the **Properties** dialog box.
5. Click the **View** menu, and then select the **Advanced Features** option.
6. In the console tree, expand the **User Accounts** OU, and then click the **Employees** OU.
7. In the details pane, right-click **Pat Coleman**, and then click **Properties**.
8. Click the **Attribute Editor** tab.

9. Double-click the **division** attribute.
10. Enter **6425B** and then click **OK**.
11. Click **OK** to close the **Pat Coleman Properties** dialog box.
12. Close Active Directory Users and Computers.

Exercise 2: Create a Custom Active Directory Administrative Console

► Task 1: Create a custom MMC console with the Active Directory Users and Computers snap-in

1. Click **Start**, and in the **Start Search** box type **mmc.exe**, and then press **ENTER**.
A User Account Control dialog box appears.
2. Click **Continue**.
An empty MMC console appears. By default, the new console window is not maximized.
3. Maximize the MMC console.
4. Click the **File** menu, and then click **Add/Remove Snap-in**.
The Add or Remove Snap-ins dialog box appears.
5. In the **Available snap-ins** list, click **Active Directory Users and Computers**, and then click **Add**.
6. Click **OK** to close the **Add or Remove Snap-ins** dialog box.
7. Click the **File** menu, and then click **Save**.
8. In the **Save As** dialog box, browse to drive **C**.
9. Click the **Create New Folder** button on the toolbar and name the new folder **AdminTools**.
10. Open the new **AdminTools** folder.
11. In the **File name** box, type **MyConsole**.
12. Click **Save**.

► Task 2: Add other Active Directory snap-ins to the console

1. Click the **File** menu, and then click **Add/Remove Snap-in**.
The Add or Remove Snap-ins dialog box appears.
2. In the **Available snap-ins** list, click **Active Directory Sites and Services**, and then click **Add**.

3. In the **Available snap-ins** list, click **Active Directory Domains and Trusts**, and then click **Add**.
4. Click **OK** to close the **Add or Remove Snap-ins** dialog box.
5. In the console tree, right-click **Console Root**, and then click **Rename**.
6. Type **Active Directory Administrative Tools** and press ENTER.
7. Click the **File** menu, and then click **Save**.

► **Task 3: Add the Active Directory Schema snap-in to a custom MMC console**

1. Click the **File** menu, and then click **Add/Remove Snap-in**.
The Add or Remove Snap-ins dialog box appears.
2. In the **Add or Remove Snap-ins** dialog box, examine the **Available snap-ins** list. Note that **Active Directory Schema** is not available.

The Active Directory Schema snap-in is installed with the Active Directory Domain Services role, and with the Remote Server Administration Tools (RSAT), but it is not registered, so it does not appear.

3. Click **OK** to close the **Add or Remove Snap-ins** dialog box.
4. Click **Start**, then right-click **Command Prompt**, and then click **Run as administrator**.

A User Account Control dialog box appears.

5. Click **Continue**.

The Administrator: Command Prompt window appears.

6. In the command prompt, type the command **regsvr32.exe schmmgmt.dll**.

This command registers the dynamic link library (DLL) for the Active Directory Schema snap-in. This is necessary to do one time on a system before you can add the snap-in to a console.

A prompt appears that indicates the registration was successful.

7. Click **OK**.
8. Close the Command Prompt window.

9. Return to your customized MMC console. Click the **File** menu, and then click **Add/Remove Snap-in**.

The Add or Remove Snap-ins dialog box appears.

10. In the **Available snap-ins** list, click **Active Directory Schema**, and then click **Add**.
11. Click **OK** to close the **Add or Remove Snap-ins** dialog box.
12. Click the **File** menu, and then click **Save**.

► **Task 4: Manage snap-ins in a custom MMC console (optional)**

- Open the **Add or Remove Snap-ins** dialog box and use the **Move Up**, **Move Down**, and **Remove** buttons to rearrange your console. For future labs, you will need the console in the condition it was in at the end of Task 3, so do not save your changed console. Instead, close the console without saving changes.

Exercise 3: Perform Administrative Tasks with Least Privilege, Run As Administrator, and User Account Control

- ▶ **Task 1: Log on with credentials that do not have administrative privileges**
 1. Log off of HQDC01.
 2. Log on to HQDC01 as **Pat.Coleman** with the password, **Pa\$\$w0rd**.

Pat.Coleman is a member of Domain Users and has no administrative privileges.

- ▶ **Task 2: Run Server Manager as an administrator**
 1. Click the **Server Manager** icon in the **Quick Launch**, next to the **Start** button.

A User Account Control dialog box appears.

Because your user account is not a member of Administrators, the dialog box requires you to enter administrative credentials: a username and a password.

If you do not see the User Name and Password boxes, make sure that you are logged on as Pat.Coleman and *not* as Pat.Coleman_Admin.
 2. In the **User name** box, type **Pat.Coleman_Admin**.
 3. In the **Password** box, type **Pa\$\$w0rd** and press ENTER.

Server Manager opens.

- ▶ **Task 3: Examine the credentials used by running processes**
 1. Right-click the taskbar and click **Task Manager**.

Task Manager opens.
 2. Click the **Processes** tab.

3. Click **Show processes from all users**.

A User Account Control dialog box appears.

Task Manager can run without administrative credentials, but it will show only those processes running under the current user account. Therefore, the User Account Control dialog box includes an option to authenticate using the same credentials with which you are logged on: Pat.Coleman.

4. Click **Use another account**.
5. In the **User name** box, type **Pat.Coleman_Admin**.
6. In the **Password** box, type **Pa\$\$w0rd** and press ENTER.
Task Manager closes and re-opens using the new credentials.
7. If Task Manager opens in a minimized state, click Task Manager on the taskbar to restore the window.
8. Click the **Processes** tab.
9. Click the **User Name** column header to sort by username.
10. Expand the **User Name** column so that it is wide enough to see the full width of usernames.
11. Scroll down to see the processes being run as Pat.Coleman and Pat.Coleman_Admin.

Question: Which processes are running as Pat.Coleman_Admin? What applications do the processes represent?

Answer: Task Manager (taskmgr.exe) and Server Manager (which appears in the Processes list as mmc.exe) are running as Pat.Coleman_Admin.

► **Task 4: Run the command prompt as an administrator**

1. Click **Start**, then right-click **Command Prompt**, and then click **Run as administrator**.
A User Account Control dialog box appears.
2. Click **Use another account**.
3. In the **User name** box, type **Pat.Coleman_Admin**.

4. In the **Password** box, type **Pa\$\$w0rd** and press ENTER.
The Administrator: Command Prompt window appears.
5. Close the Command Prompt window.
6. Click **Start**, and in the **Start Search** box, type **cmd.exe**, and then press CTRL+SHIFT+ENTER.
In the Start Search box, the keyboard shortcut CTRL+SHIFT+ENTER runs the specified command as an administrator.
A User Account Control dialog box appears.
7. Click **Use another account**.
8. In the **User name** box, type **Pat.Coleman_Admin**.
9. In the **Password** box, type **Pa\$\$w0rd** and press ENTER.
The Administrator: Command Prompt window appears.

► **Task 5: Run administrative tools as an administrator**

1. Click the **Show Desktop** icon in the **Quick Launch**, next to the **Start** button.
2. Click **Start**, then point to **Administrative Tools**, then right-click **Active Directory Users and Computers**, and then click **Run as administrator**.
A User Account Control dialog box appears.
3. Click **Use another account**.
4. In the **User name** box, type **Pat.Coleman_Admin**.
5. In the **Password** box, type **Pa\$\$w0rd** and press ENTER.

► **Task 6: Run a custom administrative console as an administrator**

1. Close all open windows on your desktop.
2. Open the **C:\AdminTools** folder.
3. Right-click **MyConsole** and click **Run as administrator**.
A User Account Control dialog box appears.
4. Click **Use another account**.

5. In the **User name** box, type **Pat.Coleman_Admin**.
6. In the **Password** box, type **Pa\$\$w0rd** and press ENTER.
7. Log off of HQDC01. Do not shut down or reset the virtual machine.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in the Lab B.

Lab Review Questions

Question: Which snap-in are you most likely to use on a day-to-day basis to administer Active Directory?

Answer: The correct answer will be based on your own experience and situation.

Question: When you build a custom MMC console for administration in your enterprise, what snap-ins will you add?

Answer: The correct answer will be based on your own experience and situation.

Lab B: Find Objects in Active Directory

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the username.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

1. In **User Name**, type the username.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Find Objects in Active Directory

► Task 1: Explore the behavior of the Select dialog box



Important Note: The steps in this task guide you through using several important Active Directory Users and Computers interfaces. You can think of this task as a "tour" of the interfaces and their features. The specific changes you are making are less important than the experience you gain with the nuances of these interfaces. **Follow the exact steps listed** and don't worry about *what* you are doing; instead **focus on how you are doing it** and how the user interfaces behave.

The virtual machine should already be started and available after completing Lab A. However, if it is not, you should launch it complete the exercises in Lab A before continuing.

1. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
2. Run your custom console, **C:\AdminTools\MyConsole.msc** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
Alternately, run the pre-created console, **D:\AdminTools\ADConsole.msc** with administrative credentials.
3. In the console tree, expand the **Active Directory Users and Computers** snap-in, the **contoso.com** domain, and the **User Accounts** OU, and then click the **Employees** OU.
4. Right-click **Pat Coleman** and then click **Properties**.
5. Click the **Member Of** tab.
6. Click **Add**.
7. In the **Select** dialog box, type the name **Special**.
8. Click **OK**.
The name is resolved to Special Project.
9. Click **OK** again to close the **Properties** dialog box.
10. In the console tree, expand the **Groups** OU, and then click the **Role** OU.
11. In the details pane, right-click the **Special Project** group and then click **Properties**.

12. Click the **Members** tab.

13. Click **Add**.

The Select Users, Contacts, Computers, or Groups dialog box appears.

14. Type **linda;joan**, and then click the **Check Names** button.

The Select dialog box resolves the names to Linda Mitchell and Joanna Rybka and underlines the names to indicate visually that the names are resolved.

15. Click **OK**.

16. Click **Add**.

17. Type **carole**, and then click **OK**.

The Select dialog box resolves the name to Carole Poland and closes. You see Carole Poland on the Members list.

When you click the OK button, a “Check Names” operation is performed prior to closing the dialog box. It is not necessary to click the Check Names button unless you want to check names and remain in the Select dialog box.

18. Click **Add**.

19. Type **tony;jeff**, and then click **OK**.

Because there are multiple users matching “tony,” the Multiple Names Found box appears.

20. Click **Tony Krijnen** and then click **OK**.

Because there are multiple users matching “jeff,” the Multiple Names Found box appears.

21. Click **Jeff Ford** and then click **OK**. Click **OK** to close the **Special Project Properties** dialog box.

Whenever there is more than one object that matches the information you enter, the check names operation will give you the opportunity to choose the correct object.

22. In the console tree, click the **Application** OU under the **Groups** OU.

23. In the details pane, right-click the **APP_Office** group and then click **Properties**.

24. Click the **Members** tab.

25. Click **Add**.

26. In the **Select** dialog box, type **DESKTOP101**.

27. Click **Check Names**.

A Name Not Found dialog box appears, indicating that the object you specified could not be resolved.

28. Click **Cancel** to close the **Name Not Found** box.

29. In the **Select** dialog box, click **Object Types**.

30. Select the check box next to **Computers** and click **OK**.

31. Click **Check Names**.

The name will resolve now that the Select dialog box is including computers in its resolution.

32. Click **OK**.

33. Click **OK** to close the **APP_Office Properties** dialog box.

► **Task 2: Control the view of objects in the Active Directory Users and Computers snap-in**

1. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.
2. Click the **View** menu, and then click **Add/Remove Columns**.
3. In the **Available Columns** list, click **Last Name**, then click **Add**.
4. In the **Displayed columns** list, click **Last Name** and click **Move Up** two times.
5. In the **Displayed columns** list, click **Type** and click **Remove**.
6. Click **OK**.
7. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.
8. In the details pane, click the **Last Name** column header to sort alphabetically by last name.
9. Click the **View** menu, and then click **Add/Remove Columns**.

10. In the **Available Columns** list, click **Pre-Windows 2000 Logon**, and then click **Add**.
11. In the **Displayed columns** list, click **Pre-Windows 2000 Logon**, and then click **Move Up**.
12. Click **OK**.
13. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.

► **Task 3: Use the Find command**

1. In the console tree, click the **Employees** OU.
2. Click the **Find** button in the snap-in toolbar.
3. In the **Name** box, type **Dan** and then click **Find Now**.

Question: How many users are found?

Answer: There should be more than one user named Dan.

4. Close the **Find Users, Contacts, and Groups** dialog box.

► **Task 4: Determine where an object is located**

1. Click the **View** menu, and then select the **Advanced Features** option.
2. Click **Find**.
3. Click the **In** drop-down list, and then click **Entire Directory**.
4. In the **Name** box, type **Pat.Coleman**, and then click **Find Now**.
5. Double-click **Pat Coleman (Admin)**.

Question: Where is Pat's administrative account located?

Answer: In the Admin Identities OU inside the Admins OU.

Exercise 2: Use Saved Queries

► Task 1: Create a saved query that displays all domain user accounts

1. In the console tree, right-click **Saved Queries**, then point to **New**, and then click **Query**.
2. In the **New Query** dialog box, type **All User Objects** in the **Name** box.
3. Click **Define Query**.
4. From the **Name** drop-down list, choose **Has a value**. Click **OK** two times.

► Task 2: Create a saved query that shows all user accounts with non-expiring passwords

1. In the console tree, right-click **Saved Queries**, then point to **New**, and then click **Query**.
2. In the **New Query** dialog box, type **Non-Expiring Passwords** in the **Name** box.
3. Click **Define Query**.
4. Select the **Non expiring passwords** check box. Click **OK** two times.

Note that, for the purposes of maintaining a simple, single password for all users in this course, *all* user accounts are configured so that passwords do not expire. In a production environment, user accounts should not be configured with non-expiring passwords.

► Task 3: Transfer a query to another computer

1. In the console tree, right-click the **Non-Expiring Passwords** query, and then click **Export Query Definition**. The **Save As** dialog box appears.
2. In the **File name** box, type **C:\AdminTools\Query_NonExpPW.xml** and click **Save**.
3. Right-click the **Non-Expiring Passwords** query, and then click **Delete**.
A confirmation message appears.
4. Click **Yes** to confirm the deletion of the query.
5. Right-click **Saved Queries**, and then click **Import Query Definition**.

6. Double-click **Query_NonExpPW**.
The Edit Query dialog box appears.
7. Click **OK**.
8. Log off of HQDC01.



Note: Do not shut down the virtual machine once you are finished with this lab as the settings you have configured here will be used in the Lab C.

Lab Review Questions

Question: In your work, what scenarios require you to search Active Directory?

Answer: The correct answer will be based on your own experience and situation.

Question: What types of saved queries could you create to help you perform your administrative tasks more efficiently?

Answer: The correct answer will be based on your own experience and situation.

Lab C: Use DS Commands to Administer Active Directory

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.
This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.
2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.
A User Account Control (UAC) dialog box appears.
2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the username.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

1. In **User Name**, type the username.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Use DS Commands to Administer Active Directory

► Task 1: Prepare for the lab

The virtual machine should already be started and available after completing Lab A. However, if it is not, you should launch it complete the exercises in Lab A before continuing.

1. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
2. Open **D:\Labfiles\Lab02c**.
3. Run **Lab02c_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
4. The lab setup script runs. When it is complete, press any key to continue.
5. Close the Windows Explorer window, Lab02c.

► Task 2: Find objects with DSQuery

1. Open Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
The Administrator: Command Prompt window appears.
2. Type **dsquery user -name "*Mitchell"** and press ENTER.

► Task 3: Retrieve object attributes with DSGet

1. From the command prompt, get the e-mail address of Tony Krijnen.

```
dsget user "cn=Tony Krijnen,ou=Employees,ou=User  
Accounts,dc=contoso,dc=com" -email
```

2. From the command prompt, list the members of the Finance Managers group.
Do you know which attribute to use? Type "dsget group /?".

```
dsget group "cn=Finance  
Managers,ou=Role,ou=Groups,dc=contoso,dc=com" -members
```

► **Task 4: Pipe DNs from DSQuery to other DS commands**

Scott and Linda Mitchell are joining the Special Project team. They are the only two employees with the last name Mitchell who work at Contoso. They work in the Vancouver office.

1. Using a single command, add the Mitchells to the **Special Project** group.

Perform this step without typing the DN of the Mitchells' user accounts.

The DN of the Special Project group is "cn=Special Project,ou=Role,ou=Groups,dc=contoso,dc=com"

```
dsquery user -name "*Mitchell" | dsmod group "cn=Special Project,ou=Role,ou=Groups,dc=contoso,dc=com" -addmbr
```

If you receive an error that says, "The specified name is already a member of the group," use Active Directory Users and Computers to remove Scott Mitchell and Linda Mitchell from the Special Project group, then try again.

You may receive an Access Denied error. What is causing this error, and what can you do to work around it?

If you launched the command prompt without Run As Administrator, your user account (Pat.Coleman) does not have credentials to change the group membership.

2. Using a single command, retrieve the e-mail address of all users in the Vancouver office.

Users in the Vancouver office have the word **Vancouver** in the **Description** field.

If you don't know what attribute switch to use (-desc), type **dsquery user /?**.

```
dsquery user -desc "*Vancouver*"
```

If you receive a warning that your DSQuery has reached its limit, what can you do to ensure all results are returned?

```
dsquery user -desc "*Vancouver*" -limit 0
```

3. Using a single command, change the **office** attribute of the two users named Mitchell to **Vancouver**.

```
dsquery user -name "*Mitchell" | dsmod user -office "Vancouver"
```



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: What can you do to avoid typing DNs of users, groups, or computers into DSGet, and other DS commands?

Answer: Create command files or batch files of commonly used commands.

Question: How are wildcard searches with DSQuery different than searches performed with the Find command in Active Directory Users and Computers? In other words, what kind of search have you performed in this lab that would not have been possible using the basic interface of the Find command?

Answer: DSQuery offers flexible wildcard searches with the * wildcard. The Find command can only do “Starts With” queries.

Module 3

Lab Answer Key: Manage Users

Contents:

Lab A: Create and Administer User Accounts	
Exercise 1: Create User Accounts	4
Exercise 2: Administer User Accounts	6
Lab B: Configure User Object Attributes	
Exercise 1: Examine User Object Attributes	11
Exercise 2: Manage User Object Attributes	14
Exercise 3: Create Users from a Template	16
Lab C: Automate User Account Creation	
Exercise 1: Export and Import Users with CSVDE	19
Exercise 2: Import Users with LDIFDE	21

Lab A: Create and Administer User Accounts

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the username.

3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

1. In **User Name**, type the username.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Create User Accounts

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Open **D:\Labfiles\Lab03a**.
4. Run **Lab03a_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
5. The lab setup script runs. When it is complete, press any key to continue.
6. Close the Windows Explorer window, **Lab03a**.

► Task 2: Create a user account with Active Directory Users and Computers

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.
3. Right-click the **Employees** OU, then point to **New**, and then click **User**.
4. In **First name**, type the user's first name: **Chris**.
5. In **Last name**, type the user's last name: **Mayo**.
6. In **User logon name**, type the user's logon name: **Chris.Mayo**.
7. In the **User logon name (pre-Windows 2000)** text box, type the pre-Windows 2000 logon name: **Chris.Mayo**.
8. Click **Next**.
9. Type **Pa\$\$w0rd** in the **Password** and **Confirm password** boxes.

In a production environment, you should use a unique, strong password for each user account that you create, even for the temporary password assigned to a new user.

10. Select **User must change password at next login**.
11. Click **Next**.
12. Review the summary and click **Finish**.

► **Task 3: Create a user account with the DSAdd command**

1. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. If you are unsure which switches to use for the DSAdd command, type **dsadd user /?** and press ENTER.
3. Type the following command, and then press ENTER:

```
dsadd user "cn=Amy Strande,ou=Employees,ou=User  
Accounts,dc=contoso,dc=com" -samid Amy.Strande -upn  
Amy.Strande@contoso.com -fn Amy -ln Strande -display "Strande,  
Amy" -desc "Vice President, IT"
```

4. Switch to **Active Directory Users and Computers**.
5. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.
6. If Active Directory Users and Computers was already open prior to this task, click the **Refresh** button.
7. Right-click **Amy Strande** and then click **Properties**.
8. Examine the properties of the user account. Confirm that the attributes were set correctly, and then close the dialog box.

Exercise 2: Administer User Accounts

► Task 1: Administer a user account

The user account for Amy Strande is currently disabled, because no password was specified using the DSAdd command.

Question: What parameter could you have used with the DSAdd command to specify a password?

Answer: -pwd

1. Right-click **Amy Strande** and then click **Reset Password**.
2. In the **New password** and **Confirm password** boxes, type **Pa\$\$w0rd**.
3. Select the **User must change password at next logon** check box.
4. Click **OK**.
A message appears: "The password for Amy Strande has been changed."
5. Click **OK**.
6. Right-click **Amy Strande** and then click **Enable Account**.
A message appears: "Object Amy Strande has been enabled."
7. Click **OK**.

Question: What command could have been used at the command prompt to reset the password, specify that the password must be changed at the next logon, and enable the account? Write the command below, including all of the parameters.

Answer:

```
dsmod user "cn=Amy Strande,ou=Employees,ou=User  
Accounts,dc=contoso,dc=com" -pwd Pa$$w0rd -mustchpwd yes -disabled  
no
```

► Task 2: Administer the lifecycle of a user account

Contoso's policy for user account lifecycle management states the following:

- When a user leaves the organization for any reason, including leave of absence, the user's account must be disabled immediately and moved to the Disabled Accounts OU.
- Sixty days after the termination of a user, the user's account must be deleted.
 1. In console tree, click the **Employees** OU.
 2. Right-click **Chris Mayo**, and then click **Disable Account**.
A message appears: *Object Chris Mayo has been disabled.*
 3. Click **OK**.
 4. Right-click **Chris Mayo**, and then click **Move**.
 5. Click the **Disabled Accounts** OU, and then click **OK**.
 6. In the console tree, click the **Disabled Accounts** OU.
 7. Right-click **Chris Mayo** and then click **Delete**.
A prompt appears: "Are you sure you want to delete the User named 'Chris Mayo?'"
 8. Click **Yes**.
 9. Log off of HQDC01.



Note: Do not shut down the virtual machine once you are finished with this lab as the settings you have configured here will be used in the Lab B.

Lab Review Questions

Question: In this lab, which attribute(s) can be modified when you are creating a user account with the command prompt that cannot be modified when creating a user account with Active Directory Users and Computers?

Answer: Description, Display Name.

Question: What happens when you create a user account that has a password that does not meet the requirements of the domain?

Answer: The account is created, but it is disabled. It cannot be enabled until a password that meets the requirements of the domain is configured.

Lab B: Configure User Object Attributes

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears. Run an Application with Administrative Credentials

7. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

8. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the username.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

1. In **User Name**, type the username.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Examine User Object Attributes

► Task 1: Prepare for the lab

The virtual machine should already be started and available after completing Lab A. However, if it is not, you should launch it complete the exercises in Lab A before continuing

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Open **D:\Labfiles\Lab03b**.
4. Run **Lab03b_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
5. The lab setup script runs. When it is complete, press any key to continue.
6. Close the Windows Explorer window, **Lab03b**.

► Task 2: Explore the properties of an Active Directory user object

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.
3. Right-click **Tony Krijnen** and then click **Properties**.
4. Examine the **General**, **Address**, **Account** and **Organization** tabs.
5. Click **OK** to close the **Properties** dialog box.

► Task 3: Explore all attributes of an Active Directory user object

1. Click the **View** menu, and then select **Advanced Features**, so that the **Advanced Features** option is enabled.
2. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.
3. Right-click **Tony Krijnen** and then click **Properties**.
4. Click the **Attribute Editor** tab.

► **Task 4: Analyze the naming and display of user object attributes**

- For each of the following attributes in the **Tony Krijnen Properties** dialog box, identify the corresponding attribute name on the **Attribute Editor** tab:

Properties dialog box tab	Property name	Attribute name as shown on the Attribute Editor tab
General	First name	givenName
General	Last name	sn
General	Display name	displayName
General	Description	description
General	Office	physicalDeliveryOffice
General	Telephone number	telephoneNumber
General	E-mail	mail
Address	Street	streetAddress
Address	City	l
Address	Zip/Postal Code	postalCode
Address	Country	co
Organization	Job Title	title
Organization	Department	department
Organization	Company	company

Questions:

1. Use the Attribute Editor tab to answer the following questions.
 - Does the employeeID attribute, shown on the Attribute Editor tab, show up on a normal tab of the Properties dialog box? If so, which one? What about carLicense?
 - **Answer:** Neither employeeID nor carLicense appear on any other tab.
 - Looking at the Attribute Editor tab, what is the distinguished name (DN) of Tony Krijnen's object?
 - **Answer:**

`cn=Tony Krijnen,ou=Employees,ou=User Accounts,dc=contoso,dc=com`
 - Looking at the Attribute Editor tab, what is Tony's user principal name (UPN)? On which other tab does the attribute appear, and how is it labeled and displayed?
 - **Answer:** The Account tab shows the UPN as the User Logon Name. It is separated into two pieces: the logon name as a text box and the UPN suffix as a drop-down list.
2. Thought questions: Try to answer the following questions. However, it is possible that you may not come up with an answer. That is OK. Once you've tried to think of an answer, you can look at the Lab Answer Key.
 - Why might the sn attribute be named sn?
 - **Answer:** surname
 - What is the use of the c attribute?
 - **Answer:** The International Standards Organization (ISO) code for country

Exercise 2: Manage User Object Attributes

► Task 1: Modify the attributes of multiple user objects

1. In the Active Directory Users and Computers console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.
2. Click **Adam Barr**. Then, hold the CTRL key and click **Adrian Lannin**, **Ajay Manchepalli**, **Ajay Solanki**, **Allan Guinot**, **Anav Silverman** and **András Tóth**.
3. Right-click any one of the selected users and then click **Properties**.
4. Select **Description**, and then type **Marketing Task Force** in the text box.
5. Select **Office**, and then type **Headquarters** in the text box.
6. Click the **Organization** tab.
7. Select **Manager**, and then click the **Change** button.
8. Type **Ariane Berthier**, and then click **OK**.
9. Click **OK**.
10. Double-click **Adam Barr**.
11. Click the **General** tab.
12. Examine the properties that you changed.
13. Click the **Organization** tab.
14. Examine the **Manager** property that you changed.
15. Close the **Properties** dialog box for **Adam Barr**.
16. Double-click **Ariane Berthier**.
17. Click the **Organization** tab.
18. Examine the values shown in the **Direct Reports** list.
19. Close the properties of **Ariane Berthier**.

► **Task 2: Manage user attributes from the command prompt**

1. Open the Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.

2. Type the command:

```
dsquery user -desc "Marketing Task Force" | dsget user -email
```

and press ENTER.

3. Type the command:

```
dsquery user -desc "Marketing Task Force" | dsmod user -hmdir  
"\\FILE01\TaskForceUsers\%username%" -hmdirv U
```

and press ENTER.

4. In the Active Directory Users and Computers console tree, click the **Employees** OU.
5. In the details pane, right-click **Adam Barr**, and then click **Properties**.
6. Click the **Profile** tab.
7. Examine the **Home Folder** section, and then click **OK**.

Exercise 3: Create Users from a Template

► Task 1: Create a user account template for Sales

1. In the Active Directory Users and Computers console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.
2. Right-click the **Employees** OU, point to **New**, and then click **User**.
3. Leave the **First Name** box empty.
4. Leave the **Last Name** box empty.
5. In the **Full Name** box, type **_Sales User**.
6. In **User Logon Name**, type: **Template.Sales**.
7. In the **User Logon Name (Pre-Windows 2000)** text box, enter the pre-Windows 2000 logon name: **Template.Sales**.
8. Click **Next**.
9. Type **Pa\$\$w0rd** in the **Password** and **Confirm password** boxes.
10. Select **User must change password at next logon**.
11. Select **Account is disabled**.
12. Click **Next**.
13. Review the summary and click **Finish**.
14. Right-click **_Sales User** and then click **Properties**.
15. Click the **Member Of** tab.
16. Click **Add**.
17. Type **Sales** and click **OK**.
The Multiple Names Found dialog box appears.
18. Click **Sales** and click **OK**.
19. Click the **Organization** tab.
20. In **Department**, type **Sales**.
21. In **Company**, type **Contoso, Ltd**.
22. Click the **Change** button in the **Manager** section.

23. Type **Anibal Sousa** and click **OK**.
24. Click the **Account** tab.
25. In the **Account Expires** section, click **End Of**, and then select the last day of the current year.
26. Click **OK**.

► **Task 2: Create a new user account based on a template**

1. Right-click **_Sales User**, and then click **Copy**.
2. In **First Name**, type **Rob**.
3. In **Last Name**, type **Young**.
4. In **User logon name**, type **Rob.Young**.
5. Confirm that the **User logon name (pre-Windows 2000)** is **Rob.Young**, and then click **Next**.
6. In **Password** and **Confirm password**, type **Pa\$\$w0rd**.
7. Clear **Account is disabled**.
8. Click **Next**.
9. Review the summary, and then click **Finish**.
10. Log off HQDC01.



Note: Do not shut down the virtual machine once you are finished with this lab as the settings you have configured here will be used in the Lab C.

Lab Review Questions

Question: What options have you learned for modifying attributes of new and existing users?

Answer: Multi-selecting users and opening the Properties dialog box, using the DSMod command, and creating a user account based on a user account template

Question: What are the advantages and disadvantages of each?

Answer: Each option gives you the chance to configure a slightly different set of attributes. No option provides the opportunity to configure all of the available attributes for more than one user. For example, DSMod allows you to change users' descriptions, but you cannot configure the description of a new user based on a template--the description attribute is not copied. DSMod allows you to reset passwords for multiple users, but you cannot do that when you select multiple users in Active Directory Users and Computers.

Lab C: Automate User Account Creation

Exercise 1: Export and Import Users with Comma Separated Value Directory Exchange (CSVDE)

► Task 1: Prepare for the lab

The virtual machine should already be started and available after completing Labs A and B. However, if it is not, you should launch it complete the exercises in Labs A and B before continuing.

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Open **D:\Labfiles\Lab03c**.
4. Run **Lab03c_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
5. The lab setup script runs. When it is complete, press any key to continue.
6. Close the Windows Explorer window, **Lab03c**.

► Task 2: Export users with CSVDE

1. Open the **Command Prompt** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Type the following command:

```
csvde -f D:\LABFILES\LAB03C\UsersNamedApril.csv -r "(name=April*)"
-l DN,objectClass,sAMAccountName,sn,givenName,userPrincipalName
```

then press ENTER.

3. Right-click the file **D:\LABFILES\LAB03C\UsersNamedApril.csv**, and then click **Open**.

A message appears: "Windows cannot open this file."

4. Click **Select a program from a list of installed programs**, and then click **OK**.
5. Click **Notepad**, and then click **OK**.
6. Examine the file, and then close it.

► **Task 3: Import users with CSVDE**

1. Open **D:\LABFILES\LAB03C\NewUsers.csv** with Notepad.
2. Examine the information about the users listed in the file.
3. Switch to the command prompt.
4. Type the following command:

```
csvde -i -f D:\LABFILES\LAB03C\NewUsers.csv -k
```

and then press ENTER.

The two users are imported.

5. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
6. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.
7. Confirm that the users were created successfully.

If you have had the Active Directory Users and Computers snap-in open while importing the CSV file, you might have to refresh your view to see the newly created accounts.

8. Examine the accounts to confirm that first name, last name, user principal name, and pre-Windows 2000 logon name are populated according to the instructions in NewUsers.csv.
9. Right-click **Lisa Andrews** and then click **Reset Password**. In the **Password** and **Confirm Password** boxes, type **Pa\$\$w0rd**, and then click **OK**.
10. Right-click **Lisa Andrews** and then click **Enable Account**.
11. Right-click **David Jones** and then click **Reset Password**. In the **Password** and **Confirm Password** boxes, type **Pa\$\$w0rd**, and then click **OK**.
12. Right-click **David Jones** and then click **Enable Account**.
13. Close NewUsers.csv.

Exercise 2: Import Users with Lightweight Directory Access Protocol (LDAP) Data Interchange Format Directory Exchange (LDIFDE)

► Task 1: Import users with LDIFDE

1. Right-click the file **D:\LABFILES\LAB03C\NewUsers.ldf**, and then click **Open**.

A message appears: “Windows cannot open this file.”

2. Click **Select a program from a list of installed programs**, and then click **OK**.
3. Click **Notepad**, and then click **OK**.
4. Examine the information about the users listed in the file.
5. Switch to the command prompt.
6. Type the following command:

```
ldifde -i -f D:\LABFILES\LAB03C\NewUsers.ldf -k
```

and then press ENTER.

The two users are imported.

7. Switch to Active Directory Users and Computers.
8. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.
9. Confirm that the users were created successfully.

If you have had the Active Directory Users and Computers snap-in open while importing the CSV file, you might have to refresh your view to see the newly created accounts.

10. Examine the accounts to confirm that user properties are populated according to the instructions in NewUsers.ldf.
11. Right-click **Bobby Moore** and then click **Reset Password**. In the **Password** and **Confirm Password** boxes, type **Pa\$\$w0rd**, and then click **OK**.
12. Right-click **Bobby Moore** and then click **Enable Account**.
13. Right-click **Bonnie Kearney** and then click **Reset Password**. In the **Password** and **Confirm Password** boxes, type **Pa\$\$w0rd**, and then click **OK**.

14. Right-click **Bonnie Kearney** and then click **Enable Account**.
15. Close NewUsers.ldf.
16. Log off HQDC01.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Question

Question: What scenarios lend themselves to importing users with CSVDE and LDIFDE?

Answer: If you are importing a large quantity of users, CSVDE and LDIFDE add significant value. Also, CSVDE and LDIFDE give you the ability to configure most user attributes, unlike templates and DSAdd, which support a very limited number of attributes.

Module 4

Lab Answer Key: Manage Groups

Contents:

Lab A: Administer Groups

Exercise 1: Implement Role-Based Management Using Groups 4

Exercise 2: Manage Group Membership from the Command Prompt 8

Lab B: Best Practices for Group Management

Exercise 1: Implement Best Practices for Group Management 13

Lab A: Administer Groups

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.
This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.
2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.
A User Account Control (UAC) dialog box appears.
2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

- a. Click **Use Another Account**.
- b. In **User Name**, type the username.
- c. In **Password**, type the password.
- d. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

1. In **User Name**, type the username.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Implement Role-Based Management Using Groups

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Open **D:\Labfiles\Lab04a**.
4. Run **Lab04a_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
5. The lab setup script runs. When it is complete, press any key to continue.
6. Close the Windows Explorer window, **Lab04a**.

► Task 2: Create role groups with Active Directory Users and Computers

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **contoso.com** domain and the **Groups** OU, and then click the **Role** OU.
3. Right-click the **Role** OU, then point to **New**, and then click **Group**.
4. In the **Group name** box, type **Sales**.
5. Select the **Global** group scope and **Security** group type. Click **OK**.
6. Repeat steps 3 through 5 to create a global security group called **Consultants**.

► **Task 3: Create role groups with DSAdd**

1. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Type the following command on one line, and then press ENTER:

```
dsadd group "CN=Auditors,OU=Role,OU=Groups,DC=contoso,DC=com"  
-secgrp yes -scope g
```

3. In Active Directory Users and Computers, confirm that the group was created successfully in the **Role** OU, inside the **Groups** OU.
 - If the Active Directory Users and Computers snap-in was open prior to performing this task, refresh the view.

► **Task 4: Add users to the role group**

1. In the Active Directory Users and Computers console tree, click the **Role** OU.
2. Right-click the **Sales** group, and then click **Properties**.
3. Click the **Members** tab.
4. Click the **Add** button.
5. Type **Tony Krijnen** and click **OK**.
6. Click **OK** to close the **Properties** dialog box.
7. In the console tree, expand the **User Accounts** OU, and then click the **Employees** OU.
8. Right-click **Linda Mitchell**, and then click **Add to a group**.
9. Type **Sales** and press ENTER.

The **Multiple Names Found** box appears, because there are two groups with names that begin with *Sales*.

10. Click **Sales**, and then click **OK**.

A message appears: *The Add to Group operation was successfully completed.*

11. Click **OK**.

► **Task 5: Implement a role hierarchy in which Sales Managers are also part of the Sales role**

1. In the console tree, expand the **Groups** OU, and then click the **Role** OU.
2. Right-click the **Sales Managers** group, and then click **Properties**.
3. Click the **Member Of** tab.
4. Click the **Add** button.
5. Type **Sales** and click **OK**.

The Multiple Names Found box appears, because there are two groups with names that begin with *Sales*.

6. Click **Sales**, and then click **OK**.
7. Click **OK** to close the **Properties** dialog box.

► **Task 6: Create a resource access management group**

1. In the console tree, click the **Groups\Access** OU.
2. Right-click the **Access** OU, then point to **New**, and then click **Group**.
3. In the **Group Name** box, type **ACL_Sales Folders_Read**.
4. Select the **Domain local** group scope and **Security** group type. Click **OK**.

► **Task 7: Assign permissions to the resource access management group**

1. Create a folder in D:\Data named **Sales**. If you are prompted for credentials use username **Pat.Coleman_Admin** with password **Pa\$\$w0rd**.
2. Right-click the **Sales** folder, then click **Properties**, and then click the **Security** tab.
3. Click **Edit**, and then click **Add**.
4. Type **ACL_** and press ENTER.

Notice that when you use a prefix for group names, such as the ACL_ prefix for resource access groups, you can find them quickly.

5. Click **ACL_Sales Folders_Read**, and then click **OK**.
6. Confirm that the group has been given Read & Execute permission.
7. Click **OK** to close each open dialog box.

► **Task 8: Define which roles and users have access to a resource**

1. In the Active Directory users and Computers console tree, click the **Access OU**.
2. Right-click the **ACL_Sales Folders_Read** group, and then click **Properties**.
3. Click the **Members** tab.
4. Click **Add**.
5. Type **Sales;Consultants;Auditors** and click **OK**.
The Multiple Items Found box appears because there are two groups with names that start with *Sales*.
6. Click **Sales** and click **OK**.
7. Click **Add**.
8. Type **Bobby Moore** and click **OK**.
9. Click **OK** to close the **Properties** dialog box.

Exercise 2: Manage Group Membership from the Command Prompt

► Task 1: Modify group membership with DSMod

1. Switch to the command prompt. It should still be running with administrator credentials from the previous exercise.
2. Type the following command on one line, and then press ENTER.

```
dsmod group "CN=Auditors,OU=Role,OU=Groups,DC=contoso,DC=com"  
-addmbr "CN=Mike Danseglio,OU=Employees,OU=User Accounts,  
DC=contoso,DC=com" "CN=Finance Managers,OU=Role,  
OU=Groups,DC=contoso,DC=com"
```

3. In the Active Directory Users and Computers console tree, click the **Role** OU.
4. Right-click the **Auditors** group, and then click **Properties**.
5. Click the **Members** tab.
6. Confirm that Mike Danseglio and the Finance Managers group are members, and then close the **Properties** dialog box.

► Task 2: Retrieve group membership with DSGet

1. Switch to the command prompt.
2. List the direct members of the **Auditors** group by typing the following command, and then pressing ENTER:

```
dsget group "CN=Auditors,OU=Role,OU=Groups,DC=contoso,DC=com"  
-members
```

3. List the full list of members of the **Auditors** group by typing the following command, and then pressing ENTER:

```
dsget group "CN=Auditors,OU=Role,OU=Groups,DC=contoso,DC=com"  
-members -expand
```

4. List the full list of members of the **ACL_Sales Folders_Read** group by typing the following command, and then pressing ENTER:

```
dsget group "CN=ACL_Sales Folders_Read,OU=Access,  
OU=Groups,DC=contoso,DC=com" -members -expand
```

5. List the direct group membership of **Mike Danseglio** by typing the following command, and then pressing ENTER:

```
dsget user "CN=Mike Danseglio,OU=Employees,OU=User Accounts,  
DC=contoso,DC=com" -memberof
```

6. List the full group membership of **Mike Danseglio** by typing the following command on one line, and then pressing ENTER:

```
dsget user "CN=Mike Danseglio,OU=Employees,OU=User Accounts,  
DC=contoso,DC=com" -memberof -expand
```



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in the Lab B.

Lab Review Questions

Question: Describe the purpose of global groups in terms of role-based management.

Answer: Global groups are generally used to define roles.

Question: What types of objects can be members of global groups?

Answer: Global groups can include as members users and other roles (global groups) from the same domain.

Question: Describe the purpose of domain local groups in terms of role-based management of resource access.

Answer: Domain local groups are generally used to define a scope of management, such as managing a level of access to a resource.

Question: What types of objects can be members of domain local groups?

Answer: Domain local groups can contain roles (global groups) and individual users from any trusted domain in the same forest or an external forest, as well as other domain local groups in the same domain. Finally, domain local groups can contain universal groups from anywhere in the forest.

Question: If you have implemented role-based management and are asked to report who can read the Sales folders, what command would you use to do so?

Answer: You would use the DSGet command.

Lab B: Best Practices for Group Management

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the username.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

1. In **User Name**, type the username.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Implement Best Practices for Group Management

► Task 1: Prepare for the lab

1. The virtual machine should already be started and available after completing Lab A. However, if it is not, you should launch it and complete the exercises in Lab A before continuing.
2. Start 6425B-HQDC01-A.
3. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 2: Create a well-documented group

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **Groups** OU, and then click the **Access** OU.
3. Right-click the **ACL_Sales Folders_Read** group and then click **Properties**.
4. In the **Description** box, summarize the resource management rule represented by the group. Type **Sales Folders (READ)**.
5. In the **Notes** box, type the following paths to represent the folders that have permissions assigned to this group and click OK when finished:
\\contoso\teams\Sales (READ)
\\file02\data\Sales (READ)
\\file03\news\Sales (READ)

► Task 3: Protect a group from accidental deletion

1. Click the **View** menu, and then select **Advanced Features**, so that the Advanced Features option is enabled.
2. In the console tree, click the **Groups\Access** OU.
3. Right-click the **ACL_Sales Folders_Read** group, and then click **Properties**.
4. Click the **Object** tab.
5. Select the **Protect object from accidental deletion** check box and click **OK**.

6. Right-click **ACL_Sales Folders_Read**, and then click **Delete**.

A message appears asking if you are sure.

7. Click **Yes**.

A message appears: *You do not have sufficient privileges to delete ACL_Sales Folders_Read, or this object is protected from accidental deletion.*

8. Click **OK**.

► **Task 4: Delegate group membership management**

1. In the console tree, click the **Role** OU.
2. Right-click the **Auditors** group, and then click **Properties**.
3. Click the **Managed By** tab.
4. Click the **Change** button.
5. Type **Mike Danseglio** and click **OK**.
6. Select the **Manager can update membership list** check box. Click **OK**.

► **Task 5: Validate the delegation of group membership management**

1. Log off HQDC01.
2. Log on to HQDC01 with the username **Mike.Danseglio** and the password **Pa\$\$w0rd**.
3. Click **Start**, and then click **Network**.
4. Click **Search Active Directory**.
5. Type **Auditors**.
6. Click **Find Now**.
7. Double-click the **Auditors** group.
8. Click the **Add** button.
9. Type **Executives**, and then click **OK**.
10. Click **OK**.
11. Log off of HQDC01.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: What are some benefits of using the Description and Notes fields of a group?

Answer: Better documented groups are easier to find and understand, and are less likely to be misused for purposes other than their intended purpose.

Question: What are the advantages and disadvantages of delegating group membership?

Answer: Delegating group membership allows IT to get "out of the middle." In most organizations, when a user needs access to a resource, he or she contacts IT, IT contacts the business owner to get approval, and then IT adds the user to the groups. Delegating allows the request to go straight to the business owner, who can then make the change to the group.

Module 5

Lab Answer Key: Support Computer Accounts

Contents:

Lab A: Create Computers and Joining the Domain

Exercise 1: Join a Computer to the Domain with the Windows® Interface 4

Exercise 2: Secure Computer Joins 10

Exercise 3: Manage Computer Account Creation with Best Practices 13

Lab B: Administer Computer Objects and Accounts

Exercise 1: Administer Computer Objects Through Their Life Cycle 17

Exercise 2: Administer and Troubleshooting Computer Accounts 20

Lab A: Create Computers and Joining the Domain

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

- a. Click **Use Another Account**.
- b. In **User Name**, type the username.
- c. In **Password**, type the password.
- d. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

1. In **User Name**, type the username.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Join a Computer to the Domain with the Windows® Interface

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Open **D:\Labfiles\Lab05a**.
4. Run **Lab05a_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
5. The lab setup script runs. When it is complete, press any key to continue.
6. Close the Windows Explorer window, **Lab05a**.
7. Start 6425B-SERVER01-B.

► Task 2: Identify and correct a DNS configuration error

1. Log on to SERVER01 as **Administrator** with the password **Pa\$\$w0rd**.
2. Open **System Properties** using one of the following methods:
 - Click **Start**, then right-click **Computer**, and then click **Properties**.
 - Open **System** from **Control Panel**.
 - Press the WINDOWS LOGO key and the PAUSE key.
3. In the **Computer name, domain and workgroup settings** section, click **Change Settings**.

The System Properties dialog box appears.

4. On the **Computer Name** tab, click **Change**.
5. In the **Member Of** section, click **Domain**.
6. Type **contoso.com**.

Be sure to use the fully qualified domain name, contoso.com, not the NetBIOS name of the domain, contoso.

7. Click **OK**.

A dialog box appears, informing you that "An Active Directory® Domain Controller for the domain contoso.com could not be contacted."

8. Click **OK** to close the warning.
9. Click **Cancel** to close the **Computer Name/Domain Changes** dialog box, and **Cancel** again to close the **System Properties** dialog box.
10. Click **Start**, then right-click **Network**, and then click **Properties**.
The Network and Sharing Center opens.
11. Click the **View status** link next to **Local Area Connection**.
12. Click **Properties**.
The Local Area Connection Properties dialog box appears
13. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
14. In the **Preferred DNS server** box, type **10.0.0.11**, and then click **OK**.
15. Click the **Close** button two times.

Question: Why might the join have succeeded if you had used the domain name contoso instead of contoso.com? What might go wrong after the domain was successfully joined with DNS but incorrectly configured?

Answer: The use of the fully qualified name forced the name resolution process to use DNS, and because DNS failed, the domain join failed. The domain name "contoso" is a flat domain name that could be resolved through NetBIOS name resolution. Even though the domain join would be successful, the client would likely have problems locating domain controllers in other sites, and locating other resources in the domain. Performing the join with a fully qualified domain name ensures that DNS is functioning before joining the domain.

► **Task 3: Join SERVER01 to the domain**

1. Open **System Properties** using one of the following methods:
 - If it is still open from the previous tasks in this exercise, click its button on the task bar.
 - Click **Start**, then right-click **Computer**, and then click **Properties**.
 - Open **System** from **Control Panel**.
 - Press the WINDOWS LOGO key and the PAUSE key.

2. In the **Computer name, domain and workgroup settings** section, click **Change Settings**.

The System Properties dialog box appears.

3. On the **Computer Name** tab, click **Change**.
4. In the **Member Of** section, click **Domain**.
5. Type **contoso.com**.
6. Click **OK**.

A Windows Security dialog box appears.

7. In **User name**, type **Aaron.Painter**.
8. In **Password**, type **Pa\$\$w0rd**.
9. Click **OK**.

A message appears: "Welcome to the contoso.com domain."

Note that Aaron.Painter is a standard user in the contoso.com domain. He has no special rights or permissions, and yet he is able to join a computer to the domain. He does have to be logged on to the computer with an account that is a member of the computer's Administrators group.

10. Click **OK**.

A message appears informing you to restart.

11. Click **OK**.
12. Click **Close** to close the **System Properties** dialog box.
13. Click **Restart Now**.

► **Task 4: Verify the location of the SERVER01 account**

1. Switch to HQDC01.
2. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.

3. In the console tree, expand the **contoso.com** domain, and then click the **Computers** container.
4. Locate SERVER01 in the **Computers** container.

Question: In which OU or container does the account exist?

Answer: The Computers container

► **Task 5: Remove SERVER01 from the domain**

1. Log on to SERVER01 as **Administrator** with the password **Pa\$\$w0rd**.
2. Open **System Properties** using one of the following methods:
 - Click **Start**, then right-click **Computer**, and then click **Properties**.
 - Open **System** from **Control Panel**.
 - Press the WINDOWS LOGO key and the PAUSE key.
3. In the **Computer name, domain and workgroup settings** section, click **Change Settings**.

The System Properties dialog box appears.

4. On the **Computer Name** tab, click **Change**.
5. In the **Member Of** section, click **Workgroup**.
6. Type **WORKGROUP**.
7. Click **OK**.

A message appears: "Welcome to the WORKGROUP workgroup."

8. Click **OK**.

A message appears informing you to restart.

9. Click **OK**.
10. Click **Close** to close the **System Properties** dialog box.

Another message appears informing you to restart.
11. Click **Restart Now**.

► **Task 6: Delete the SERVER01 account**

1. Switch to HQDC01.
2. In the Active Directory Users and Computers console tree, click the **Computers** container, and then click the **Refresh** button on the snap-in toolbar.

Question: On HQDC01, refresh the view of the Computers container and examine the SERVER01 account. What is its status?

Answer: Disabled

Question: You were not prompted for domain credentials in Task 5, and yet a change was made to the domain: the computer account was reset and disabled. What credentials were used to do this? What credentials were used to change the workgroup/domain membership of SERVER01?

Answer: This is a tricky question! Domain credentials with appropriate permissions *are* required to make a change to the domain, such as resetting and disabling a computer account; and credentials that are in the local Administrators group on the client are required to change the computer's workgroup/domain membership.

You were logged on to SERVER01 as the local Administrator, so you were able to change the computer's workgroup/domain membership. Normally, you would have been prompted for domain credentials, but it just so happens that the local Administrator account's username, Administrator, and password, Pa\$\$w0rd, are identical to those of the domain Administrator account, which of course has permission to modify objects in the domain. Windows attempts to authenticate you behind the scenes, and only prompts you for domain credentials if that authentication fails. In this case, because of the similarity in credentials, you were actually authenticated as the domain's Administrator.

In a production environment, the domain's Administrator account should have a very long, complex, secure password that is *different* from the passwords used for domain member computer Administrator accounts.

3. Right-click SERVER01, and then click **Delete**.
You are prompted to confirm the deletion.
4. Click **Yes**.

Exercise 2: Secure Computer Joins

► Task 1: Redirect the default computer container

1. Still on HQDC01 run **Command Prompt** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Type the following command:

```
redircmp "OU=New Computers,DC=contoso,DC=com"
```

and then press ENTER.

The output of the command indicates that it completed successfully.

3. Close the Command Prompt window.

► Task 2: Restrict unmanaged domain joins

1. Run **ADSI Edit** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Right-click **ADSI Edit**, and then click **Connect To**.
The Connection Settings dialog box appears.
3. In the **Connection Point** section, click **Select A Well Known Naming Context**, and from the drop-down list choose **Default Naming Context**.
4. Click **OK**.
5. Click **Default naming context** in the console tree.
6. In the details pane, right-click the domain folder, **dc=contoso,dc=com**, and then click **Properties**.
7. Click **ms-DS-MachineAccountQuota** and click **Edit**.
8. Type **0**.
9. Click **OK**.
10. Click **OK** to close the **Attribute Editor**.
11. Close ADSI Edit.

► **Task 3: Validate the effectiveness of ms-DS-MachineAccountQuota**

1. Log on to SERVER01 as **Administrator** with the password **Pa\$\$w0rd**.
2. Open **System Properties** using one of the following methods:
 - Click **Start**, then right-click **Computer**, and then click **Properties**.
 - Open **System** from **Control Panel**.
 - Press the WINDOWS LOGO key and the PAUSE key.
3. In the **Computer name, domain and workgroup settings** section, click **Change Settings**.

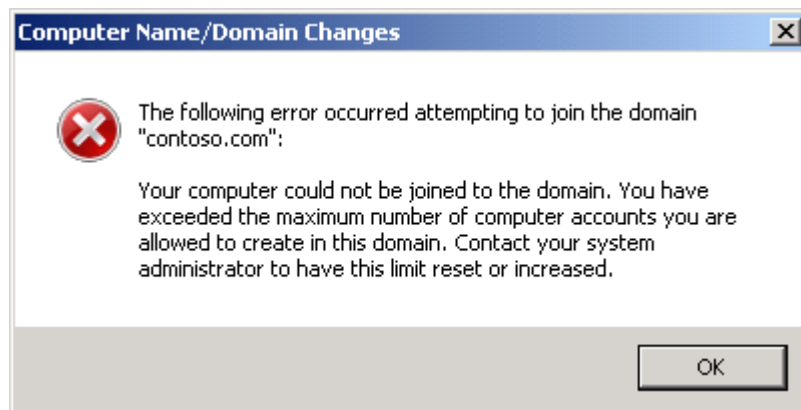
The System Properties dialog box appears.

4. On the **Computer Name** tab, click **Change**.
5. In the **Member Of** section, click **Domain**.
6. Type **contoso.com**.
7. Click **OK**.

A Windows Security dialog box appears.

8. In **User name**, type **Aaron.Painter**.
9. In **Password**, type **Pa\$\$w0rd**.
10. Click **OK**.

The message below appears:



11. Click **OK**.
12. Click **Cancel**.
13. Click **Cancel** to close the **System Properties** dialog box.

Exercise 3: Manage Computer Account Creation with Best Practices

► Task 1: Prestage a computer account

1. Switch to HQDC01.
2. In the Active Directory Users and Computers console tree, expand the **contoso.com** domain and the **Servers** OU, and then click the **File** OU.
3. Right-click the **File** OU, then point to **New**, and then click **Computer**.
The New Object - Computer dialog box appears.
4. In **Computer Name**, type **SERVER01**.
5. Click the **Change** button next to **User or Group**.
The Select User or Group dialog box appears.
6. Type **AD_Server_Deploy** and press ENTER.
7. Click **OK**.

► Task 2: Join a computer remotely to a prestaged account using NetDom

1. Run **Command Prompt** with administrative credentials. Use the account **Aaron.Painter_Admin** with the password **Pa\$\$w0rd**.
Aaron.Painter_Admin is a member of the **AD_Server_Deploy** group. In the previous task, you gave the group permission to join SERVER01 to the domain.
2. Type the command **whoami /groups** to list the group memberships of the current account (**Aaron.Painter_Admin**). Note that the user is a member of **AD_Server_Deploy** and is not a member of any other administrative group.

3. Type the following command on one line (the line can wrap), and then press ENTER:

```
netdom join SERVER01 /domain:contoso.com  
/UserO:Administrator /Password0:*  
/UserD:CONTOSO\Aaron.Painter_Admin /PasswordD:*  
/REBoot:5
```

You are prompted for the password associated with the domain user, CONTOSO\Aaron.Painter_Admin.

4. Type **Pa\$\$w0rd** and press ENTER.

You are prompted for the password associated with the object user, SERVER01\Administrator.

5. Type **Pa\$\$w0rd** and press ENTER.
6. The command completes successfully and SERVER01 restarts.
7. Log on to SERVER01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
This confirms that the server has successfully joined the domain.
8. Log off of SERVER01.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in the Lab B.

Lab B: Administer Computer Objects and Accounts

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the username.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

- a. In **User Name**, type the username.
- b. In **Password**, type the password.
- c. Press ENTER or click **OK**.

Exercise 1: Administer Computer Objects Through Their Life Cycle

► Task 1: Prepare for the lab

The virtual Machines should already be started and available after completing Lab A. However, if they are not, you should complete steps 1 to 3 below and then step through exercises 1 to 3 in Lab A before continuing. You will be unable to successfully complete Lab B unless you have completed Lab A.

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Start 6425B-SERVER01-B.

► Task 2: Configure computer object attributes

1. On HQDC01 run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **contoso.com** domain and the **Client Computers** OU, and then click **SEA**.
3. Right-click **LNO8538**, and then click **Properties**.
4. Click the **Managed By** tab.
5. Click the **Change** button.
6. Type **Linda Mitchell** and press ENTER.
Note that Linda's contact information is populated on the Managed By tab.
7. Click **OK** to close the computer **Properties** dialog box.
8. Repeat steps 3 through 8 to assign **LOT9179** to **Scott Mitchell**.
9. Click **LOT9179**.
10. Press and hold CTRL while you click **LNO8538**. You should now have both computers selected.

11. Right-click either of the highlighted items, **LNO8538** or **LOT9179**, and then click **Properties**.
12. Select the **Change the description text for all selected objects** check box.
13. Type **Scott and Linda Mitchell**.
14. Click **OK**.

► **Task 3: Add computers to software management groups**

1. In the console tree, click the **SEA** OU, then right-click **LOT9179** in the details pane, and then click **Add to a group**.
2. Type **APP_** and press ENTER.
The Multiple Items Found dialog box appears.
3. Click **APP_Project** and click **OK**.
A message appears: "The Add to Group operation was successfully completed."
4. Click **OK**.
5. In the console tree, expand the **Groups** OU, and then click **Application**.
6. Right-click **APP_Project**, and then click **Properties**.
7. Click the **Members** tab.
8. Click **Add**.
9. Type **LNO8538** and press ENTER.
The Name Not Found dialog box appears.
By default, the Select Users, Computers, or Groups interface does not search for computer objects.
10. Click **Object Types**.
11. Select the check box next to **Computers**, and then click **OK**.
12. Click **OK** to close the **Name Not Found** dialog box.
Both computers can now be seen on the **Members** tab.
13. Click **OK**.

► **Task 4: Move a computer between OUs**

1. In the **Client Computers\SEA OU**, click **LOT9179**.
2. Drag **LOT9179** into the **VAN OU**, visible in the console tree.
A message appears that reminds you to be careful about moving objects in Active Directory.
3. Click **Yes**.
4. Right-click **LNO8538**, and then click **Move**.
The Move dialog box appears.
5. Expand the **Client Computers** OU, and then click the **VAN OU**.
6. Click **OK**.

► **Task 5: Disable, enable, and delete computers**

1. In the **SEA OU**, right-click **DEP6152**, and then click **Disable Account**.
A confirmation message appears.
2. Click **Yes**.
A message appears: "Object DEP6152 has been disabled."
3. Click **OK**.
4. Right-click **DEP6152**, and then click **Enable Account**.
A message appears: "Object DEP6152 has been enabled."
5. Click **OK**.
6. Right-click **DEP6152**, and then click **Delete**.
A confirmation message appears.
7. Click **Yes**.

Exercise 2: Administer and Troubleshooting Computer Accounts

► Task 1: Reset a computer account

1. In the **VAN OU**, right-click **LOT9179**, and then click **Reset Account**.
A confirmation message appears.
2. Click **Yes**.
A message appears: "Account LOT9179 was successfully reset."
3. Click **OK**.

► Task 2: Experience a secure channel problem

1. Log on to **SERVER01** as **Pat.Coleman** with the password **Pa\$\$w0rd**.
2. Click **Start**, then point to the arrow next to the **Lock** icon, and then click **Log Off**.
3. Switch to **HQDC01**.
4. In the Active Directory Users and Computers console tree, expand the **Servers** OU, and then click the **File** OU.
5. Right-click **SERVER01**, and then click **Reset Account**.
Because **SERVER01** is currently joined to the domain correctly, this step effectively breaks the trust relationship by resetting the account password on the domain without involving or informing **SERVER01** itself. The computer therefore does not know its new password.
A confirmation message appears.
6. Click **Yes**.
A message appears: "Account **SERVER01** was successfully reset."
7. Click **OK**.
8. On **SERVER01**, attempt to log on as **Pat.Coleman** with the password **Pa\$\$w0rd**.
A message appears: "The trust relationship between this workstation and the primary domain failed."
9. Click **OK**.

► **Task 3: Reset the secure channel**

1. Switch to HQDC01.
2. In the Active Directory Users and Computers console tree, expand the **Servers** OU, and then click the **File** OU.
3. Right-click SERVER01, and then click **Reset Account**.

A confirmation message appears.

4. Click **Yes**.

A message appears: "Account SERVER01 was successfully reset."

5. Click **OK**.

After resetting the secure channel, you could move SERVER01 into a workgroup, and then rejoin the domain. It will join its reset account, thereby retaining its group memberships. Do not perform that step at this time.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Module 6

Lab Answer Key: Implement a Group Policy Infrastructure

Contents:

Lab A: Implement Group Policy	
Exercise 1: Create, Edit, and Link Group Policy Objects	4
Lab B: Manage Settings and GPOs	
Exercise 1: Use Filtering and Commenting	9
Exercise 2: Manage Administrative Templates	11
Lab C: Manage Group Policy Scope	
Exercise 1: Configure GPO Scope with Links	19
Exercise 2: Configure GPO Scope with Filtering	22
Exercise 3: Configure Loopback Processing	24
Lab D: Troubleshoot Policy Application	
Exercise 1: Perform RSoP Analysis	29
Exercise 2: Use the Group Policy Modeling Wizard	32
Exercise 3: View Policy Events	34

Lab A: Implement Group Policy

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the user name.
5. In **Password**, type the password.
6. Press ENTER or click the logon arrow.

The Windows® desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Perform the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to use another account:

- a. Click **Use Another Account**.
- b. In **User Name**, type the username.
- c. In **Password**, type the password.
- d. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

1. In **User Name**, type the username.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Create, Edit, and Link Group Policy Objects

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Start 6425B-DESKTOP101-A but do not log on to the system.

► Task 2: Create a GPO

1. Run **Group Policy Management** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand **Forest: contoso.com, Domains**, and **contoso.com**, and then click the **Group Policy Objects** container.
3. In the console tree, right-click the **Group Policy Objects** container, and then click **New**.
4. In **Name**: type **CONTOSO Standards**, and then click **OK**.

► Task 3: Edit the settings of a GPO

1. In the details pane of the Group Policy Management console (GPMC), right-click the **CONTOSO Standards** GPO, and then click **Edit**.
The Group Policy Management Editor (GPME) appears.
2. In the console tree, expand **User Configuration, Policies**, and **Administrative Templates**, and then click **System**.
3. Double-click the **Prevent access to registry editing tools** policy setting.
4. Click **Enabled**.
5. In the **Disable regedit from running silently?** drop-down list, select **Yes**.
6. Click **OK**.
7. In the console tree, expand **User Configuration, Policies, Administrative Templates**, and **Control Panel**, and then click **Display**.
8. In the details pane, click the **Screen Saver timeout** policy setting.
9. Note the explanatory text in the left margin of the console's details pane.

10. Double-click the **Screen Saver timeout** policy setting.
11. Review the explanatory text on the **Explain** tab.
12. Click the **Setting** tab and click **Enabled**.
13. In the **Seconds** box, type **600**, and click **OK**.
14. Double-click the **Password protect the screen saver** policy setting.
15. Click **Enabled**, and click **OK**.
16. Close the GPME.

Changes you make in the GPME are saved in real time. There is no Save command.

► **Task 4: Scope a GPO with a GPO link**

1. In the GPMC console tree, right-click the **contoso.com** domain, and then click **Link an Existing GPO**.
2. Select **CONTOSO Standards** and click **OK**.

► **Task 5: View the effects of Group Policy application**

1. Switch to DESKTOP101.
2. Log on to DESKTOP101 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Right-click the desktop, and then click **Personalize**.
4. Click **Screen Saver**.
5. Notice that the **Wait** control is disabled—you cannot change the timeout.
6. Notice that the **On resume, display logon screen** option is selected and disabled—you cannot disable password protection.
7. Click **OK** to close the **Screen Saver** dialog box.
8. Click **Start** and, in the **Start Search** box, type **regedit.exe**. Then press ENTER.
A message appears: "Registry editing has been disabled by your administrator."
9. Click **OK**.

► **Task 6: Explore GPO settings**

1. Switch to HQDC01.
2. Right-click the **CONTOSO Standards** GPO, and then click **Edit**.
3. Spend time exploring the settings that are available in a GPO. Do not make any changes.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs.

Lab Review Questions

Question: What policy settings are already being deployed using Group Policy in your organization?

Answer: The correct answer will be based on your own experience and situation.

Question: What policy settings did you discover that you might want to implement in your organization?

Answer: The correct answer will be based on your own experience and situation.

Lab B: Manage Settings and GPOs

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the logon arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Perform the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to use another account:

1. Click **Use Another Account**.
2. In **User Name**, type the username.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

1. In **User Name**, type the username.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Use Filtering and Commenting

► Task 1: Prepare for the lab

The virtual machine should already be started and available after completing Lab A. However, if it is not, you should complete the below steps then step through exercises 1 in Lab A before continuing.

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 2: Search and filter policy settings

1. Run **Group Policy Management** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand **Forest: contoso.com**, **Domains**, and **contoso.com**, and then click the **Group Policy Objects** container.
3. In the details pane, right-click the **CONTOSO Standards** GPO, and then click **Edit**.

The Group Policy Management Editor appears.

4. In the console tree, expand **User Configuration** and **Policies**, and then click **Administrative Templates**.
5. Right-click **Administrative Templates**, and then click **Filter Options**.
6. Select the **Enable Keyword Filters** check box.
7. In the **Filter for word(s)** text box, type **screen saver**.
8. In the drop-down list next to the text box, select **Exact**, and click **OK**.

Administrative Templates policy settings are filtered to show only those that contain the words *screen saver*.

9. Spend a few moments examining the settings that you have found.
10. In the console tree, right-click **Administrative Templates** under **User Configuration**, and then click **Filter Options**.
11. Clear the **Enable Keyword Filters** check box.

12. In the **Configured** drop-down list, select **Yes**, and then click **OK**.
Administrative Template policy settings are filtered to show only those that have been configured (enabled or disabled).
13. Spend a few moments examining those settings.
14. In the console tree, right-click **Administrative Templates** under **User Configuration** and clear the **Filter On** option.

► **Task 3: Document GPOs and settings with comments**

1. In the console tree of the Group Policy Management Editor, right-click the root node, **CONTOSO Standards**, and then click **Properties**.
2. Click the **Comment** tab.
3. Type **Contoso corporate standard policies. Settings are scoped to all users and computers in the domain. Person responsible for this GPO: your name.**
This comment appears on the Details tab of the GPO in the GPMC.
4. Click **OK**.
5. In the console tree, expand **User Configuration, Policies, Administrative Templates**, and **Control Panel**, and then click **Display**.
6. Double-click the **Screen Saver** policy setting.
7. Click the **Comment** tab.
8. Type **Corporate IT Security Policy implemented with this policy in combination with Password Protect the Screen Saver**, and click **OK**.
9. Double-click the **Password protect the screen saver** policy setting.
10. Click the **Comment** tab.
11. Type **Corporate IT Security Policy implemented with this policy in combination with Screen Saver Timeout**, and click **OK**.

Exercise 2: Manage Administrative Templates

► Task 1: Explore the syntax of an administrative template

1. Click **Start**, then click **Run**, then type `%SystemRoot%\PolicyDefinitions` and then press ENTER.

The PolicyDefinitions folder opens.

2. Open the **en-us** folder or the folder for your region and language.
3. Double-click **ControlPanelDisplay.adml**.
4. Click the **Select a program from a list of installed programs** option and click **OK**.
5. Click **Notepad** and click **OK**.
6. Click the **Format** menu and select the **Word wrap** option, so that it is enabled.
7. Search for the text **ScreenSaverIsSecure**.

This is a definition of a string variable called ScreenSaverIsSecure.

8. Note the text between the `<string>` and `</string>` tags.
9. Note the name of the variable on the following line, **ScreenSaverIsSecure_Help**, and the text between the `<string>` and `</string>` tags.
10. Close the file.
11. Navigate up to the **PolicyDefinitions** folder.
12. Double-click **ControlPanelDisplay.admx**.
13. Click the **Select a program from a list of installed programs** option and click **OK**.
14. Click **Notepad** and click **OK**.
15. Search for the text, **ScreenSaverIsSecure**.

16. Examine the code in the file, also shown below:

```
<policy name="ScreenSaverIsSecure" class="User"
displayName="$(string.ScreenSaverIsSecure)"
explainText="$(string.ScreenSaverIsSecure_Help)"
key="Software\Policies\Microsoft\Windows\Control Panel\Desktop"
valueName="ScreenSaverIsSecure">
  <parentCategory ref="Display" />
  <supportedOn ref="windows:SUPPORTED_Win2kSP1" />
  <enabledValue>
    <string>1</string>
  </enabledValue>
  <disabledValue>
    <string>0</string>
  </disabledValue>
</policy>
```

17. Identify the parts of the template that define the following:
- The name of the policy setting that appears in the GPME
 - **Answer:** \$(string.ScreenSaverIsSecure)
 - The explanatory text for the policy setting
 - **Answer:** \$(string.ScreenSaverIsSecure_Help)
 - The registry key and value affected by the policy setting
 - class="User" (HKCU)
 - key="Software\Policies\Microsoft\Windows\Control Panel\Desktop"
 - valueName="ScreenSaverIsSecure"
 - The data put into the registry if the policy is enabled
 - <enabledValue><string>1</string></enabledValue>
 - The data put into the registry if the policy is disabled
 - <disabledValue><string>0</string></disabledValue>
18. Close the file, and then close the Windows Explorer window, **PolicyDefinitions**.

► **Task 2: Manage classic administrative templates (.ADM files)**

1. Switch to the GPME.
2. In the console tree, expand **User Configuration** and **Policies**, and then click **Administrative Templates**.
3. Right-click **Administrative Templates**, and then click **Add/Remove Templates**.
4. Click **Add**.
5. Browse to **D:\Labfiles\Lab06b\Office 2007 Administrative Templates**.
6. Open the **ADM** folder and then the **en-us** folder.
7. Click **office12.adm** and click **Open**.
8. Click **Close**.

The Classic Administrative Templates (ADM) node appears in the Administrative Templates tree.

9. In the console tree, expand **Administrative Templates**, **Classic Administrative Templates (ADM)** and **Microsoft Office 2007 System**.

Classic administrative templates (.ADM files) are provided primarily for enterprises that do not manage Group Policy with Windows Vista® or Windows Server® 2008 or later operating systems.

You should use a computer running the most recent version of Windows to manage Group Policy. By doing so, you will be able to view and modify all available policy settings, including those that apply to previous versions of Windows. If you have at least one computer running Windows Vista, Windows Server 2008, or later, you should use that computer to manage Group Policy, and then you will not need classic administrative templates (.ADM files) when .ADMX/.ADML files are available.

Note that the template format affects only the *management* of Group Policy. Settings will apply to versions of Windows as described in the Supported on or Requirements section of the policy setting properties.

10. Right-click **Administrative Templates**, and then click **Add/Remove Templates**.
11. Click **office12**, and then click **Remove**.
12. Click **Close**.

► **Task 3: Manage .ADMX and .ADML files**

1. Click **Start**, click **Run**, and then type **D:\Labfiles\Lab06b\Office 2007 Administrative Templates** and press **ENTER**.
2. Open the **ADMX** folder.
3. Select all .ADMX files and the **en-us** folder, or the appropriate folder for your language and region, and then press **CTRL+C** to copy the files and the folder.
4. Click **Start**, click **Run**, and then type **%SystemRoot%\PolicyDefinitions** and press **ENTER**.
5. Press **CTRL+V** to paste the files and the folder.
You are prompted to merge the en-us folder.
6. Select the **Do this for all current items** check box, and then click **Yes**.
You are prompted for administrative permissions.
7. Select the **Do this for all current items** check box, and then click **Continue**. A **User Account Control** dialog box appears.
8. In **User name**, type **Pat.Coleman_Admin**.
9. In **Password**, type **Pa\$\$word**.
10. Click **OK**.
11. Close Windows Explorer.
12. Close the GPME.
13. In the GPMC console tree, right-click **CONTOSO Standards**, and then click **Edit**. The GPME appears.
14. In the console tree, expand **User Configuration** and **Policies**, and then click **Administrative Templates**.
15. Note the addition of Microsoft® Office 2007 policy setting folders.

► **Task 4: Create the central store**

1. In the GPME, click the **Administrative Templates** node underneath **User Configuration\Policies**.
2. In the details pane heading, note the message, **Policy definitions (ADMX files) retrieved from the local machine**.

3. Close the GPME.
4. Run the command prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
5. Type **md \\contoso.com\SYSVOL\contoso.com\Policies\PolicyDefinitions\en-us**, and then press ENTER.

If you are using another language or region, substitute *en-us* with the appropriate folder.

6. Type **xcopy %systemroot%\PolicyDefinitions\\contoso.com\SYSVOL\contoso.com\Policies\PolicyDefinitions**, and then press ENTER.

The .ADMX files are copied.

7. Type **xcopy %systemroot%\PolicyDefinitions\en-us\\contoso.com\SYSVOL\contoso.com\Policies\PolicyDefinitions\en-us**, and then press ENTER.

If you are using another language or region, substitute *en-us* with the appropriate folder.

The .ADML files are copied.

8. In the GPMC, right-click **CONTOSO Standards**, and then click **Edit**.
9. In the console tree, expand **User Configuration** and **Policies**, and then click **Administrative Templates**.
10. In the details pane heading, note the message, **Policy definitions (ADMX files) retrieved from the central store**.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs.

Lab Review Questions

Question: Describe the relationship between administrative template files (both .ADMX and .ADML files) and the GPME.

Answer: .ADMX files create the user interface for the GPME and determine the registry values that are applied when a policy setting is defined. .ADML files provide the language-specific elements (the text) in the user interface.

Question: When does an enterprise get a central store? What benefits does it provide?

Answer: A central store is manually created by adding a PolicyDefinitions folder to \\domain\sysvol\domain\Policies.

Question: What are the advantages of managing Group Policy from a client running the latest version of Windows? Do settings you manage apply to previous versions of Windows?

Answer: If you manage Group Policy with a client running the latest version of Windows, you will be able to use the latest administrative templates, and you will be able to view settings that apply to this and all previous versions of Windows. The policy settings you configure will apply not based on the version of Windows from which you manage Group Policy, but rather based on the versions of Windows to which the policy setting can apply.

Lab C: Manage Group Policy Scope

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the logon arrow.

The Windows desktop appears.

► Run an Application with Administrative Credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Perform the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to use another account:

1. Click **Use Another Account**.
2. In **User Name**, type the username.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

1. In **User Name**, type the username.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Configure GPO scope with links

► Task 1: Prepare for the lab

The virtual machines should already be started and available after completing Labs A and B. However, if they are not, you should complete the below steps then step through the exercises in Labs A and B before continuing.

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Start 6425B-DESKTOP101-A but do not log on to the system.

► Task 2: Create a GPO with a policy setting that takes precedence over a conflicting setting

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.
3. Right-click the **Employees** OU, point to **New**, and then click **Organizational unit**.
4. Type **Engineers**, and then click **OK**.
5. Close **Active Directory Users and Computers**.
6. Run the **Group Policy Management** console with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
The **Group Policy Management** console opens.
7. In the console tree, expand **Forest: contoso.com**, **Domains**, **contoso.com**, **User Accounts**, and **Employees**, and then click the **Engineers** OU.
8. Right-click the **Engineers** OU, and then click **Create a GPO in this domain and Link it here**.
9. Type **Engineering Application Override** and press **ENTER**.
10. Right-click the **Engineering Application Override** GPO, and then click **Edit**.
The **Group Policy Management Editor** appears.

11. In the console tree, expand **User Configuration, Policies, Administrative Templates**, and **Control Panel**, and then click **Display**.
12. Double-click the **Screen Saver timeout** policy setting.
13. Click **Disabled**, and click **OK**.
14. Close the GPME.
15. In the GPMC console tree, click the **Engineers OU**.
16. Click the **Group Policy Inheritance** tab.
17. Notice that the **Engineering Application Override** GPO has higher precedence than the **CONTOSO Standards** GPO.

The screen saver timeout policy setting you just configured in the Engineering Application Override GPO will be applied after the setting in the CONTOSO Standards GPO. Therefore, the new setting will overwrite the standards setting, and will "win." Screen saver timeout will be disabled for users within the scope of the Engineering Application Override GPO.

► **Task 3: View the effect of an enforced GPO link**

1. In the GPMC console tree, click the **Domain Controllers** OU, and then click the **Group Policy Inheritance** tab.
2. Notice that the GPO named **6425B** has the highest precedence. Settings in this GPO will override any conflicting settings in any of the other GPOs.

The Default Domain Controllers GPO specifies, among other things, which groups are given the right to log on locally to domain controllers. To enhance the security of domain controllers, standard users are not given the right to log on locally. In order to allow a nonprivileged user account such as Pat.Coleman to log on to domain controllers in this course, the 6425B GPO gives Domain Users the right to log on locally to a computer. The 6425B GPO is linked to the domain, so its settings would normally be overridden by settings in the Default Domain Controllers GPO. Therefore, the 6425B GPO link to the domain is configured as Enforced. In this way, the conflict in user rights assignment between the two GPOs is "won" by the 6425B GPO.

► **Task 4: Apply Block Inheritance**

1. In the GPMC console tree, click the **Engineers** OU, and then click the **Group Policy Inheritance** tab.
2. Examine the precedence and inheritance of GPOs.
3. Right-click the **Engineers** OU, and then click **Block Inheritance**.

Question: What GPOs continue to apply to users in the Engineers OU? Where are those GPOs linked? Why did they continue to apply?

Answer: The Engineering Application Override GPO, which is linked to the Engineers OU itself, and the 6425B GPO, linked to the domain, continue to apply. The 6425B GPO continues to apply to users in this OU because its link is Enforced.

4. Right-click the **Engineers** OU, and then clear **Block Inheritance**.

Exercise 2: Configure GPO Scope with Filtering

► Task 1: Configure policy application with security filtering

1. Switch to Active Directory Users and Computers.
2. In the console tree, expand the **contoso.com** domain and the **Groups** OU, and then click the **Configuration** OU.
3. Right-click the **Configuration** OU, then point to **New**, and then click **Group**.
4. Type **GPO_Engineering Application Override_Apply**, and then press ENTER.
5. Switch to the Group Policy Management console.
6. In the console tree, expand the **Engineers** OU, and then click the link of the **Engineering Application Override** GPO underneath the **Engineers** OU.
A message appears.
7. Read the message, then click **Do not show this message again**, and then click **OK**.
8. Notice in the **Security Filtering** section that the GPO applies by default to all authenticated users.
9. In the **Security Filtering** section, click **Authenticated Users**.
10. Click the **Remove** button. A confirmation prompt appears.
11. Click **OK**.
12. Click the **Add** button.
The Select User, Computer, or Group dialog box appears.
13. Type **GPO_Engineering Application Override_Apply** and press ENTER.

► Task 2: Configure an exemption with security filtering

1. Switch to Active Directory Users and Computers.
2. In the console tree, expand the **contoso.com** domain and the **Groups** OU, then click the **Configuration** OU.
3. Right-click the **Configuration** OU, then point to **New**, and then click **Group**.
4. Type **GPO_CONTOSO Standards_Exempt**, and then press ENTER.

5. Switch to the Group Policy Management console.
6. In the console tree, click the link of the **CONTOSO Standards** GPO to the **contoso.com** domain.
7. In the **Security Filtering** section, notice that the GPO applies by default to all authenticated users.
8. Click the **Delegation** tab.
9. Click the **Advanced** button.

The CONTOSO Standards Security Settings dialog box appears.
10. Click the **Add** button.

The Select User, Computer, or Group dialog box appears.
11. Type **GPO_CONTOSO Standards_Exempt** and press ENTER.
12. Click the check box below **Deny** and next to **Apply group policy**.
13. Click **OK**.

A warning message appears to remind you that deny permissions override allow permissions.
14. Click **Yes**.
15. Notice that the permission appears on the **Delegation** tab as **Custom**.

Exercise 3: Configure Loopback Processing

► Task 1: Configure loopback processing

1. In the GPMC console tree, expand the **Kiosks** OU, and then click the **Conference Rooms** OU.
2. Right-click the **Conference Rooms** OU and then click **Create a GPO in this domain, and Link it here**.
3. In **Name**, type **Conference Room Policies**, and then press ENTER.
4. In the console tree, expand **Conference Rooms**, and then click the **Conference Room Policies** GPO.
5. Click the **Scope** tab.
6. Confirm that the GPO is scoped to apply to **Authenticated Users**.
7. Right-click the **Conference Room Policies** GPO in the console tree, and then click **Edit**.

The Group Policy Management Editor appears.

8. In the GPME console tree, expand **User Configuration, Policies, Administrative Templates**, and then click **Control Panel**, and then click **Display**.
9. Double-click the **Screen Saver** timeout policy setting.
10. Click **Enabled**.
11. In the **Seconds** box, type **2700**, and click **OK**.
12. In the console tree, expand **Computer Configuration, Policies, Administrative Templates**, and then click **System**, and then click **Group Policy**.
13. Double-click the **User Group Policy loopback processing mode** policy setting.
14. Click **Enabled**.

15. In the **Mode** drop-down list, select **Merge**, and click **OK**.
16. Close the Group Policy Management Editor.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs.

Lab Review Questions

Question: Many organizations rely heavily on security group filtering to scope GPOs, rather than linking GPOs to specific OUs. In these organizations, GPOs are typically linked very high in the Active Directory® logical structure: to the domain itself or to a first-level OU. What advantages are gained by using security group filtering rather than GPO links to manage the scope of the GPO?

Answer: The fundamental problem of relying on OUs to scope the application of GPOs is that an OU is a fixed, inflexible structure within Active Directory, and that a single user or computer can only exist within one OU. As organizations get larger and more complex, configuration requirements are difficult to match in a one-to-one relationship with any container structure. With security groups, a user or computer can exist in as many groups as necessary, and can be added and removed easily without impacting the security or management of the user or computer account.

Question: Why might it be useful to create an exemption group—a group that is denied the Apply Group Policy permission—for every GPO that you create?

Answer: There are very few scenarios in which you can be guaranteed that all of the settings in a GPO will always need to apply to all users and computers within its scope. By having an exemption group, you will always be able to respond to situations in which a user or computer must be excluded. This can also help in troubleshooting compatibility and functionality problems. Sometimes, specific GPO settings can interfere with the functionality of an application. In order to test whether the application works on a "pure" installation of Windows, you might need to exclude the user or computer from the scope of GPOs, at least temporarily for testing.

Question: Do you use loopback policy processing in your organization? In what scenarios and for what policy settings can loopback policy processing add value?

Answer: Answers will vary. Scenarios including conference rooms, kiosks, virtual desktop infrastructures, and other "standard" environments should certainly be mentioned.

Lab D: Troubleshoot Policy Application

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the logon arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Perform the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to use another account:

1. Click **Use Another Account**.
2. In **User Name**, type the username.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

1. In **User Name**, type the username.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Perform RSoP Analysis

► Task 1: Prepare for the lab

The virtual machines should already be started and available after completing Labs A, B and C. However, if they are not, you should complete the below steps then step through the exercises in Labs A, B and C before continuing.

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Start 6425B-DESKTOP101-A.
4. Log on to DESKTOP101 as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 2: Refresh Group Policy

1. On the DESKTOP101 virtual machine run the command prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Type **gpupdate.exe /force**.
3. Wait for the command to complete.
4. Make a note of the current system time, which you will need to know for a task later in this lab.
5. Restart DESKTOP101.
6. Wait for DESKTOP101 to restart before proceeding with the next task. Do not log on to DESKTOP101.

► Task 3: Create a Group Policy results RSoP report

1. Switch to HQDC01.
2. Run **Group Policy Management** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
3. In the console tree, expand **Forest: contoso.com**, and then click **Group Policy Results**.
4. Right-click **Group Policy Results**, and click **Group Policy Results Wizard**.
5. On the **Welcome to the Group Policy Results Wizard** page, click **Next**.

6. On the **Computer Selection** page, click **Another computer**, and then type **DESKTOP101** in the text box. Click **Next**.
7. On the **User Selection** page, click **Display policy settings for**, then click **Select a specific user**, and then select **CONTOSO\Pat.Coleman**. Click **Next**.
8. On the **Summary Of Selections** page, review your settings, and then click **Next**.
9. Click **Finish**. The RSoP report appears in the details pane of the console.
10. If you are prompted by an Internet Explorer® security message that refers to **about:security_mmc.exe**, then click **Add**. In the **Trusted sites** dialog box, click **Add**, and then click **Close**.
11. Review the **Group Policy Summary** results. For both user and computer configuration, identify the time of the last policy refresh and the list of allowed and denied GPOs. Identify the components that were used to process policy settings.
12. Click the **Settings** tab. Review the settings that were applied during user and computer policy application and identify the GPO from which the settings were obtained.
13. Click the **Policy Events** tab and locate the event that logs the policy refresh you triggered with the **GPUpdate** command in Task 1.
14. Click the **Summary** tab, right-click the page, and then click **Save Report**.
15. Save the report as an HTML file to drive D with a name of your choice.
16. Open the saved RSoP report from drive D. Examine the RSoP report, and then close it.

► **Task 4: Analyze RSoP with GPResults**

1. Log on to DESKTOP101 as **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Run the command prompt with administrative credentials.
3. Type **gpresult /r** and press ENTER.

RSoP summary results are displayed.

The information is very similar to the Summary tab of the RSoP report produced by the Group Policy Results Wizard.

4. Type **gpresult /v** and press ENTER.
A more detailed RSoP report is produced.
Notice many of the Group Policy settings applied by the client are listed in this report.
5. Type **gpresult /z** and press ENTER.
The most detailed RSoP report is produced.
6. Type **gpresult /h:"%userprofile%\Desktop\RSOP.html"** and press ENTER.
An RSoP report is saved as an HTML file to your desktop.
7. Open the saved RSoP report from your desktop.
8. Compare the report, its information, and its formatting to the RSoP report you saved in the previous task.

Exercise 2: Use the Group Policy Modeling Wizard

► Task 1: Perform Group Policy results modeling

1. Switch to HQDC01.
2. In the Group Policy Management console tree, expand **Forest:Contoso.com**, and then click **Group Policy Modeling**.
3. Right-click **Group Policy Modeling**, and then click **Group Policy Modeling Wizard**.

The Group Policy Modeling Wizard appears.
4. Click **Next**.
5. On the **Domain Controller Selection** page, click **Next**.
6. On the **User And Computer Selection** page, in the **User Information** section, click the **User** option button, and then click **Browse**.

The Select User dialog box appears.
7. Type **Mike.Danseglio** and then press ENTER.
8. In the **Computer Information** section, click the **Computer** option button, and then click **Browse**.

The Select Computer dialog box appears.
9. Type **DESKTOP101** and then press ENTER.
10. Click **Next**.
11. On the **Advanced Simulation Options** page, select the **Loopback Processing** check box and then click **Merge**.

Even though the Conference Room Polices GPO specifies the loopback processing, you must instruct the Group Policy Modeling Wizard to consider loopback processing in its simulation.
12. Click **Next**.
13. On the **Alternate Active Directory Paths** page, click the **Browse** button next to **Computer location**.

The Choose Computer Container dialog box appears.
14. Expand **contoso.com** and **Kiosks**, and then click **Conference Rooms**.

You are simulating the effect of DESKTOP101 as a conference room computer.

15. Click **OK**.
16. Click **Next**.
17. On the **User Security Groups** page, click **Next**.
18. On the **Computer Security Groups** page, click **Next**.
19. On the **WMI Filters for Users** page, click **Next**.
20. On the **WMI Filters for Computers** page, click **Next**.
21. Review your settings on the **Summary of Selections** page, and then click **Next**.
22. Click **Finish**.
23. On the **Summary** tab, scroll to and expand, if necessary, **User Configuration, Group Policy Objects**, and **Applied GPOs**.
24. Will the **Conference Room Policies** GPO apply to Mike Danseglio as a User policy when he logs on to DESKTOP101 if DESKTOP101 is in the Conference Rooms OU?

If not, check the scope of the Conference Room Policies GPO. It should be linked to the Conference Rooms OU with security group filtering that applies the GPO to the Authenticated Users special identity. You can right-click the modeling query to rerun the query. If the GPO is still not applying, try deleting and re-building the Group Policy Modeling report, and be very careful to follow each step precisely.
25. Click the **Settings** tab.
26. Scroll to, and expand if necessary, **User Configuration, Policies, Administrative Templates** and **Control Panel/Display**.
27. Confirm that the screen saver timeout is 2700 seconds (45 minutes), the setting configured by the **Conference Room Policies** GPO that overrides the 10-minute standard configured by the **CONTOSO Standards** GPO.

Exercise 3: View Policy Events

► Task 1: View policy events

1. Switch to DESKTOP101.
2. Click **Start**, and then click **Control Panel**.
3. Click **System and Maintenance**.
4. Click **Administrative Tools**.
5. Double-click **Event Viewer**.

A User Account Control dialog box appears.

6. Click **Continue**.

Event Viewer opens.

7. In the console tree, expand **Windows Logs**, and then click the **System** log.
8. Locate events with **GroupPolicy** as the **Source**.

You can even click the Filter Current Log link in the Actions pane and then select GroupPolicy in the Event Sources drop-down list.

9. Review the information associated with **GroupPolicy** events.
10. In the console tree, click the **Application** log.
11. Sort the **Application** log by the **Source** column.
12. Review the events and identify the Group Policy events that have been entered in this log. Which events are related to Group Policy application, and which are related to the activities you have been performing to manage Group Policy?

Depending on how long the virtual machine has been running you may not have any Group Policy Events in the application log

13. In the console tree, expand **Applications and Services Logs, Microsoft, Windows**, and **GroupPolicy**, and then click **Operational**.
14. Locate the first event related in the **Group Policy** refresh you initiated in Exercise 1, with the **GPUpdate** command. Review that event and the events that followed it.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: In what situations have you used RSoP reports to troubleshoot Group Policy application in your organization?

Answer: The correct answer will be based on your own experience and situation.

Question: In what situations have you used, or could you anticipate using, Group Policy modeling?

Answer: The correct answer will be based on your own experience and situation.

Question: Have you ever diagnosed a Group Policy application problem based on events in one of the event logs?

Answer: The correct answer will be based on your own experience and situation.

Module 7

Lab Answer Key: Manage Enterprise Security and Configuration with Group Policy Settings

Contents:

Lab A: Delegate the Support of Computers	
Exercise 1: Configure the Membership of Administrators by Using Restricted Groups Policies	4
Lab B: Manage Security Settings	
Exercise 1: Manage Local Security Settings	10
Exercise 2: Create a Security Template	13
Exercise 3: Use Security Configuration and Analysis	15
Exercise 4: Use the Security Configuration Wizard	19
Lab C: Manage Software with GPSI	
Exercise 1: Deploy Software with GPSI	25
Exercise 2: Upgrade Applications with GPSI	31
Lab D: Audit File System Access	
Exercise 1: Configure Permissions and Audit Settings	37
Exercise 2: Configure Audit Policy	39
Exercise 3: Examine Audit Events	40

Lab A: Delegate the Support of Computers

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

3. Click **Use Another Account**.
4. In **User Name**, type the username.

5. In **Password**, type the password.

6. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

a. In **User Name**, type the username.

7. In **Password**, type the password.

8. Press ENTER or click **OK**.

Exercise 1: Configure the Membership of Administrators by Using Restricted Groups Policies

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Start 6425B-DESKTOP101-A but do not log on to the system.

► Task 2: Delegate the administration of all clients in the domain

1. On HQDC01 click **Start >Administrative Tools** and run **Group Policy Management** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **Forest:contoso.com, Domains and contoso.com**, and then click the **Group Policy Objects** container.
3. Right-click the **Group Policy Objects** container, and then click **New**.
4. In the **Name** box, type **Corporate Help Desk**, and then click **OK**.
5. In the details pane, right-click the **Corporate Help Desk**, and then click **Edit**.
The Group Policy Management Editor appears.
6. In the console tree, expand **Computer Configuration, Policies, Windows Settings, Security Settings**, and then click **Restricted Groups**.
7. Right-click **Restricted Groups**, and then click **Add Group**.
8. Click the **Browse** button.
The Select Groups dialog box appears.
9. Type **CONTOSO\Help Desk**, and then press ENTER.
10. Click **OK** to close the **Add Group** dialog box.
The CONTOSO\Help Desk Properties dialog box appears.
11. In the **This group is a member of** section, click the **Add** button.
The Group Membership dialog box appears.
12. Type **Administrators**, and then click **OK**.
13. Click **OK** again to close the **Properties** dialog box.

14. Close the **Group Policy Management Editor**.
15. In the **Group Policy Management** console tree, right-click the **Client Computers** OU, and then click **Link an Existing GPO**.
The Select GPO dialog box appears.
16. Select the **Corporate Help Desk** GPO, and then click **OK**.
17. Close the **Group Policy Management** console.

► **Task 3: Create a Seattle Support group**

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **contoso.com** domain and the **Groups** OU, and then click the **Role** OU.
3. Right-click **Role**, point to **New**, and then click **Group**.
4. In the **Group Name** box, type **SEA Support**, and then click **OK**.
5. Close Active Directory Users and Computers.

► **Task 4: Delegate the administration of a subset of clients in the domain**

1. In the Group Policy Management console tree, expand **Forest:contoso.com**, **Domains**, and **contoso.com**, and then click the **Group Policy Objects** container.
2. Right-click the **Group Policy Objects** container, and then click **New**.
3. In the **Name** box, type **Seattle Support**, and then click **OK**.
4. In the details pane, right-click **Seattle Support**, and then click **Edit**.
The Group Policy Management Editor appears.
5. In the console tree, expand **Computer Configuration**, **Policies**, **Windows Settings**, and **Security Settings**, and then click **Restricted Groups**.
6. Right-click **Restricted Groups**, and then click **Add Group**.
7. Click the **Browse** button.
The Select Groups dialog box appears.

8. Type **CONTOSO\SEA Support**, and then press ENTER.
9. Click **OK** to close the **Add Group** dialog box.
The **CONTOSO\SEA Support Properties** dialog box appears.
10. In the **This group is a member of** section, click the **Add** button.
The **Group Membership** dialog box appears.
11. Type **Administrators**, and then click **OK**.
12. Click **OK** again to close the **Properties** dialog box.
13. Close the **Group Policy Management Editor**.
14. In the **Group Policy Management** console tree, expand the **Client Computers** OU, and then click the **SEA** OU.
15. Right-click **SEA**, and then click **Link an Existing GPO**.
The **Select GPO** dialog box appears.
16. Select the **Seattle Support** GPO, and then click **OK**.

► **Task 5: Confirm the cumulative application of Member Of policies**

1. In the **Group Policy Management** console tree, expand **Forest:contoso.com**, and then click the **Group Policy Modeling** node.
2. Right-click the **Group Policy Modeling** node, and then click **Group Policy Modeling Wizard**. The **Group Policy Modeling Wizard** appears.
3. Click **Next**.
4. On the **Domain Controller Selection** page, click **Next**.
5. On the **User and Computer Selection** page, in the **Computer Information** section, click the **Browse** button next to **Container**.
6. Expand the **contoso** domain and the **Client Computers** OU, and then click the **SEA** OU.
7. Click **OK**.
8. Select the **Skip to the final page of this wizard without collecting additional data** check box. Click **Next**.
9. On the **Summary of Selections** page, click **Next**.
10. Click **Finish**. The **Group Policy Modeling** report appears.

11. Click the **Settings** tab.
12. Scroll to, and expand if necessary, **Computer Configuration, Policies, Windows Settings, Security Settings, and Restricted Groups**.
13. Confirm that you see both the **Help Desk** and **SEA Support** groups listed.

Restricted Groups policies using the This Group Is A Member Of setting are cumulative.

Notice that the report does not specify that the listed groups are members of the Administrators group in particular. This is a limitation of the Group Policy Modeling report. After the policy has been applied to a computer, the Group Policy Results report (RSoP) would specify that the groups are members of Administrators.



Note: Do not shut down the virtual machine once you are finished with this lab as the settings you have configured here will be used in subsequent labs.

Lab Review Questions

Question: If you wanted to ensure that the *only* members of the local Administrators group on a client computer were the Help Desk in the site-specific Support group, and to remove any other members from the local Administrators group, how would you achieve that using only restricted groups policies?

Answer: This is a bit of a tricky question, and requires some creative thinking. You can configure a Members policy setting for the Administrators group that adds the Administrator account. This would have the effect of cleaning out all other group members, and of course the Administrator account is already a member of the Administrator forest and cannot be removed. Then, you can configure restricted group policy settings for the Help Desk and the site-specific Support groups, as you did in the Lab. Alternately, you could use a Local Group preference configured to delete all member users and groups.

Lab B: Manage Security Settings

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press **ALT+DELETE**.
2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press **ENTER** or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.
A User Account Control (UAC) dialog box appears.
2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

- a. Click **Use Another Account**.
3. In **User Name**, type the username.
4. In **Password**, type the password.
5. Press **ENTER** or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

- a. In **User Name**, type the username.
6. In **Password**, type the password.
7. Press ENTER or click **OK**.

Exercise 1: Manage Local Security Settings

► Task 1: Prepare for the lab

The virtual Machine should already be started and available after completing Lab A. However, if it is not, you should complete the below steps.

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 2: Enable Remote Desktop on HQDC01

1. Click the **Server Manager** icon next to the Start button. The **User Account Control** dialog box appears.
2. In the **User name** box, type **Pat.Coleman_Admin**.
3. In the **Password** box, type **Pa\$\$w0rd**, and then press ENTER.
Server Manager opens.
4. In the **Server Summary** section, click **Configure Remote Desktop**.
The System Properties dialog box opens.
5. Click **Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)**.
6. Click **OK**.
7. Close **Server Manager**.

► Task 3: Create a global security group named SYS_DC Remote Desktop

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **contoso.com** domain, the **Admins** OU, and the **Admin Groups** OU, and then click the **Server Delegation** OU.
3. Right-click **Server Delegation**, point to **New**, and then click **Group**.
4. Type **SYS_DC Remote Desktop**, and then click **OK**.

► **Task 4: Add SYS_DC Remote Desktop to the Remote Desktop Users group**

In order to connect using remote desktop, a user must have the user logon right to log on through Terminal Services, which you will grant to the SYS_DC Remote Desktop group in the next task.

Additionally, the user must have permission to connect to the RDP-Tcp connection. By default, the Remote Desktop Users group and the Administrators group has permission to connect to the RDP-Tcp connection. Therefore, you should add the user (or the SYS_DC Remote Desktop group in this case) to the Remote Desktop Users group.

1. Still on HQDC01 in Active Directory Users and Computers, in the console tree, click **Builtin**.
2. In the details pane, double-click **Remote Desktop Users**.
3. Click the **Members** tab.
4. Click the **Add** button.

The Select Users, Contacts, Computers or Groups dialog box appears.

5. Type **SYS_DC Remote Desktop**, and then press ENTER.
6. Click **OK**.
7. Close Active Directory Users and Computers.



Note: Instead of adding the group to Remote Desktop Users, you could add the SYS_DC Remote Desktop group to the access control list (ACL) of the RDP-Tcp connection, using the Terminal Services Configuration console. Right-click RDP-Tcp, and then click Properties; then click the Security tab, click the Add button, and type SYS_DC Remote Desktop. Click OK twice to close the dialog boxes.

► **Task 5: Configure the Local Security Policy to allow Remote Desktop connections by SYS_DC Remote Desktop**

1. On HQDC01 go to **Start >Administrative Tools** and run **Local Security Policy** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand **Local Policies**, and then click **User Rights Assignment**.
3. Double-click **Allow log on through Terminal Services**.
The Allow log on through Terminal Services Properties dialog box opens.
4. Click **Add User or Group**.
The Select Users, Computers, Or Groups dialog box appears.
5. Type **SYS_DC Remote Desktop**, and then press ENTER.
6. Click **OK**.
7. Close the **Allow log on through Terminal Services** dialog box.

► **Task 6: Revert the local security policy to its default setting**

You will now revert the policy to its default in preparation for following Exercises.

1. Double-click **Allow log on through Terminal Services**.
The Allow Log On Through Terminal Services Properties dialog box opens.
2. Click **CONTOSO\SYS_DC Remote Desktop**.
3. Click **Remove**.
4. Click **OK**.
5. Close **Local Security Policy**.

Exercise 2: Create a Security Template

► Task 1: Create a custom MMC console with the Security Templates snap-in

1. Still on HQDC01, click **Start** and in the search box type **mmc.exe** and press ENTER, when prompted supply administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Click **File**, and then click **Add/Remove Snap-in**.
3. In the **Available snap-ins** list, select **Security Templates**, then click **Add**.
4. Click **OK**.
5. Click **File**, and then click **Save**.
The Save As dialog box appears.
6. Type **D:\Security Management**, and then press ENTER.

► Task 2: Create a security template

1. In the console tree, expand **Security Templates**.
2. Right-click **C:\Users\Pat.Coleman_Admin\Documents\Security\Templates**, and then click **New Template**.
3. Type **DC Remote Desktop**, and then click **OK**.
4. In the console tree, expand **C:\Users\Pat.Coleman_Admin\Documents\Security\Templates**, **DC Remote Desktop**, and **Local Policies**, and then click **User Rights Assignment**.
5. In the details pane, double-click **Allow log on through Terminal Services**.
The Allow log on through Terminal Services Properties dialog box appears.
6. Select **Define these policy settings in the template**.
7. Click **Add User or Group**.
The Add User or Group dialog box appears.
8. Click the **Browse** button.
The Select Users or Groups dialog box appears.

9. Type **SYS_DC Remote Desktop**, and then click **OK**.
10. Click **OK** to close the **Add User or Group** dialog box.
11. Click **OK** to close the Policy Properties dialog box.
12. In the console tree, click **Restricted Groups**.
13. Right-click **Restricted Groups**, and then click **Add Group**.
The Add Group dialog box appears.
14. Click the **Browse** button.
15. Type **SYS_DC Remote Desktop**, and then click **OK**.
16. Click **OK** again to close the **Add Group** dialog box.
The CONTOSO\SYS_DC Remote Desktop Properties dialog box appears.
17. In the **This group is a member of** section, click **Add Groups**.
The Group Membership dialog box appears.
18. Click the **Browse** button.
The Select Groups dialog box appears.
19. Type **Remote Desktop Users**, and then click **OK**.
20. Click **OK** to close the **Group Membership** dialog box.
21. Click **OK** to close the properties dialog box.
22. In the console tree, right-click **DC Remote Desktop**, and then click **Save**.

Exercise 3: Use Security Configuration and Analysis

► **Task 1: Add the Security Configuration and Analysis snap-in to a custom console**

1. Click **File**, and then click **Add/Remove Snap-in**.
2. In the **Available snap-ins** list, select **Security Configuration and Analysis**, then click the **Add** button.
3. Click **OK**.
4. On the **File** menu, click **Save**.

► **Task 2: Create a security database and import a security template**

1. In the console tree, click **Security Configuration and Analysis**.
2. Right-click **Security Configuration and Analysis**, and then click **Open Database**.
The Open database dialog box appears.
The Open Database command enables you to create a new security database.
3. Type **HQDC01Test**, and then click **Open**.
The Import Template dialog box appears.
4. Select the **DC Remote Desktop** template you created in Exercise 2, and then click **Open**.

► **Task 3: Analyze the configuration of a computer using the security database**

1. In the console tree, right-click **Security Configuration and Analysis**, and then click **Analyze Computer Now**.
2. Click **OK** to confirm the default path for the error log.
The snap-in performs the analysis.

3. In the console tree, expand **Security Configuration and Analysis** and **Local Policies**, and then click **User Rights Assignment**.

Notice that the Allow log on through Terminal Services policy is flagged with a red circle and an X. This indicates a discrepancy between the database setting and the computer setting.

4. Double-click **Allow log on through Terminal Services**.

Notice the discrepancies. The computer is not configured to allow the SYS_DC Remote Desktop Users group to log on through Terminal Services.

Notice also that the Computer setting currently allows Administrators to log on through Terminal Services. This is an important setting that should be incorporated into the database.

5. Confirm that the **Define this policy in the database** check box is selected.
6. Select the **Administrators** check box, under **Database Setting**.

This will add the right for Administrators to log on through Terminal Services to the database. It does not change the template, and it does not affect the current configuration of the computer.

7. Click **OK**.
8. In the console tree, select **Restricted Groups**.
9. In the details pane, double-click **CONTOSO\SYS_DC Remote Desktop**.
10. Click the **Member Of** tab.

Notice that the database specifies that the SYS_DC Remote Desktop group should be a member of Remote Desktop Users, but the computer is not currently in compliance with that setting.

11. Confirm that the **Define this group in the database** check box is selected.
12. Click **OK**.
13. Right-click **Security Configuration and Analysis**, and then click **Save**.

This saves the security database, which includes the settings imported from the template plus the change you made to allow Administrators to log on through Terminal Services.

The hint displayed in the status bar when you hover over the Save command suggests that you are saving the template. That is incorrect. You are saving the database.

14. Right-click **Security Configuration and Analysis**, and then click **Export Template**.

The Export Template To dialog box appears.

15. Select **DC Remote Desktop**, and then click **Save**.

You have now replaced the template created in Exercise 2 with the settings defined in the database of the Security Configuration and Analysis snap-in.

► **Task 4: Configure security settings by using a security database**

1. Close your Security Management console. If you are prompted to save your settings, click **Yes**.

Closing and reopening the console is necessary to refresh fully the settings shown in the Security Templates snap-in.

2. Run **D:\Security Management.msc** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
3. In the console tree, expand **Security Templates**, **C:\Users\Pat.Coleman_Admin\Documents\Security\Templates**, **DC Remote Desktop**, **Local Policies**, and then click **User Rights Assignment**.
4. In the details pane, double-click **Allow log on through Terminal Services**.

Notice that both the Administrators and SYS_DC Remote Desktop groups are allowed to log on through Terminal Services in the security template.

5. Click **OK**.
6. Right-click **Security Configuration and Analysis**, and then click **Configure Computer Now**.
7. Click **OK** to confirm the error log path. The settings in the database are applied to the server. You will now confirm that the change to the user right was applied.
8. Run **Local Security Policy** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
9. In the console tree expand **Local Policies**, and then click **User Rights Assignment**.
10. Double-click **Allow Log On Through Terminal Services**.

The Allow Log On Through Terminal Services Properties dialog box opens.

11. Confirm that both **Administrators** and **SYS_DC Remote Desktop** are listed.
The Local Security Policy console displays the actual, current settings of the server.
12. Close the **Local Security Policy** console.
13. Close your custom **Security Management** console.

Exercise 4: Use the Security Configuration Wizard

► Task 1: Create a security policy

1. Still on HQDC01 click **Start > Administrative Tools** and run the Security Configuration Wizard with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. On the **Welcome to the Security Configuration Wizard** page, click **Next**.
3. On the **Configuration Action** page, select **Create a new security policy**, and then click **Next**.
4. On the **Select Server** page, accept the default server name, **HQDC01**, and click **Next**.
5. On the **Processing Security Configuration Database** page, you can optionally click **View Configuration Database** and explore the configuration that was discovered on HQDC01.
6. Click **Next**.
7. On the **Role Based Service Configuration** section introduction page, click **Next**.
8. On the **Select Server Roles** page, you can optionally explore the settings that were discovered on HQDC01, but do not change any settings. Click **Next**.
9. On the **Select Client Features** page, you can optionally explore the settings that were discovered on HQDC01, but do not change any settings. Click **Next**.
10. On the **Select Administration And Other Options** page, you can optionally explore the settings that were discovered on HQDC01, but do not change any settings. Click **Next**.
11. On the **Select Additional Services** page, you can optionally explore the settings that were discovered on HQDC01, but do not change any settings. Click **Next**.
12. On the **Handling Unspecified Services** page, do not change the default setting, **Do not change the startup mode of the service**. Click **Next**.
13. On the **Confirm Service Changes** page, in the **View** list, choose **All Services**.
14. Examine the settings in the Current Startup Mode column, which reflect service startup modes on HQDC01, and compare them to the settings in the Policy Startup Mode column.

15. In the **View** list, select **Changed Services**.
16. Click **Next**.
17. On the **Network Security** section introduction page, click **Next**.
18. On the **Network Security Rules** page, you can optionally examine the firewall rules derived from the configuration of HQDC01. Do not change any settings. Click **Next**.
19. On the **Registry Settings** section introduction page, click **Next**.
20. On each page of the **Registry Settings** section, examine the settings, but do not change any of them, then click **Next**. Continue clicking **Next** at each page until you get to the **Registry Settings Summary** page appears, examine the settings and click **Next**.
21. On the **Audit Policy** section introduction page, click **Next**.
22. On the **System Audit Policy** page, examine but do not change the settings. Click **Next**.
23. On the **Audit Policy Summary** page, examine the settings in the **Current Setting** and **Policy Setting** columns. Click **Next**.
24. On the **Save Security Policy** section introduction page, click **Next**.
25. In the **Security Policy File Name** text box, click at the end of the file path and type **DC Security Policy**.
26. Click the **Include Security Templates** button.
27. Click **Add**.
28. Browse to locate the **DC Remote Desktop** template created in Exercise 3, located in the C:\Users\Pat.Coleman_Admin\Documents\Security\Templates folder. When you have located and selected the template, click **Open**.

Be careful that you add the Documents\Security\Templates\DC Remote Desktop.inf file and *not* the DC Security.inf default security template.
29. Click **OK** to close the **Include Security Templates** dialog box.
30. Click the **View Security Policy** button.

You are prompted to confirm the use of the ActiveX control.
31. Click **Yes**.
32. Examine the security policy. Notice that the DC Remote Desktop template is listed in the **Templates** section.

33. Close the window after you have examined the policy.
34. In the Security Configuration Wizard, click **Next**.
35. On the **Apply Security Policy** page, accept the **Apply Later** default setting, and then click **Next**.
36. Click **Finish**.

► **Task 2: Transform a security policy into a Group Policy object**

1. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Type **cd c:\windows\security\msscw\policies** and then press ENTER.
3. Type **scwcmd transform /?**, and then press ENTER.
4. Type **scwcmd transform /p:"DC Security Policy.xml" /g:"DC Security Policy"** and then press ENTER.
5. Run **Group Policy Management** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
6. In the console tree expand **Forest:contoso.com, Domains, contoso.com**, and **Group Policy Objects**, and then click **DC Security Policy**. This is the GPO created by the Scwcmd.exe command.
7. Click the **Settings** tab to examine the settings of the GPO.
8. Expand **Security Settings** and **Local Policies/User Rights Assignment**.
9. Confirm that the BUILTIN\Administrators and CONTOSO\SYS_DC Remote Desktop groups are given the **Allow log on through Terminal Services** user right.
10. Expand **Restricted Groups**.
11. Confirm that CONTOSO\SYS_DC Remote Desktop is a member of BUILTIN\Remote Desktop Users.

The GPO is not applied to DCs because it is not yet linked to the Domain Controllers OU. In this Lab, do not link the GPO to the domain, site, or any OU. In a production environment, you would spend more time examining, configuring, and testing security settings in the security policy before deploying it as a GPO to production domain controllers.



Note: Do not shut down the virtual machine once you are finished with this lab as the settings you have configured here will be used in subsequent labs.

Lab Review Question

Question: Describe the relationship between security settings on a server, Local Group Policy, security templates, the database used in Security Configuration and Analysis, the security policy created by the Security Configuration Wizard, and domain-based Group Policy.

Answer: Although some security settings can be modified directly—for example, file system ACLs or local group membership—many can only be configured directly on a system using Local Group Policy. Security templates allow you to create a security policy that can be easily transferred to another system and, using Security Configuration and Analysis, loaded into a database that can be used to analyze or configure a computer. The database used by Security Configuration and Analysis can be exported to a security template.

Security Configuration Wizard is a newer tool that enables the role-based configuration of services, network security settings, registry values, and audit policies. It creates an xml file that can incorporate a security template and that can then be applied to another system using the Security Configuration Wizard. The Security Configuration Wizard allows you to roll back a security policy if it does not produce the desired results. A security policy produced by the Security Configuration Wizard can be transformed into a domain-based Group Policy object that can then apply to multiple servers.

Lab C: Manage Software with GPSI

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.
This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.
2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.
A User Account Control (UAC) dialog box appears.
2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

- a. Click **Use Another Account**.
3. In **User Name**, type the username.
4. In **Password**, type the password.
5. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

- a. In **User Name**, type the username.
6. In **Password**, type the password.
7. Press ENTER or click **OK**.

Exercise 1: Deploy Software with GPSI

► Task 1: Prepare for the lab

The virtual Machines should already be started and available after completing the previous labs. However, if they are not, you should complete the below steps.

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Start 6425B-SERVER01-A but do not log on.
4. Wait for SERVER01 to finish startup before continuing with the next task.

► Task 2: Create a software distribution folder

1. Switch to HQDC01.
2. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
3. In the console tree, expand the **contoso.com** domain and the **Groups** OU, and then click the **Application** OU.
4. Right-click the **Application** OU, point to **New**, and then click **Group**.
5. Type **APP_XML Notepad**, and then press ENTER.
6. In the console tree, expand the **contoso.com** domain and the **Servers** OU, and then click the **File** OU.
7. In the details pane, right-click **SERVER01**, and then click **Manage**.
The Computer Management console opens, focused on SERVER01.
8. In the console tree, expand **System Tools** and **Shared Folders**, and then click **Shares**.
9. Right-click **Shares**, and then click **New Share**. The Create A Shared Folder Wizard appears.
10. Click **Next**.
11. In the **Folder Path** box, type **C:\Software**, and then click **Next**.
A message appears asking if you want to create the folder.
12. Click **Yes**.

13. Accept the default Share name, **Software**, and then click **Next**.
14. Click **Customize permissions**, and then click the **Custom** button.
15. Click the **Security** tab.
16. Click **Advanced**.

The Advanced Security Settings dialog box appears.
17. Click **Edit**.
18. Clear the option, **Include inheritable permissions from this object's parent**.

A dialog box appears asking if you want to Copy or Remove inherited permissions.
19. Click **Copy**.
20. Select the first permission assigned to the **Users** group, and then click **Remove**.
21. Select the remaining permission assigned to the **Users** group, and then click **Remove**.
22. Select the permission assigned to **Creator Owner**, and then click **Remove**.
23. Click **OK** two times to close the **Advanced Security Settings** dialog boxes.
24. In the **Customize Permissions** dialog box, click the **Share Permissions** tab.
25. Select the check box next to **Full Control** and below **Allow**.

Security management best practice is to configure least privilege permissions in the ACL of the resource, which will apply to users regardless of how users connect to the resource, at which point you can use the Full Control permission on the SMB shared folder. The resultant access level will be the more restrictive permissions defined in the ACL of the folder.
26. Click **OK**.
27. Click **Finish**.
28. Click **Finish** to close the wizard.
29. Click **Start**, click **Run**, type `\\SERVER01\c$`, and then press ENTER.

The Connect to SERVER01 dialog box appears.
30. In the **User name** box, type `CONTOSO\Pat.Coleman_Admin`.

31. In the **Password** box, type **Pa\$\$w0rd**, and then press ENTER.
A Windows Explorer window opens, focused on the root of the C drive on SERVER01.
32. Open the **Software** folder.
33. Click the **File** menu, point to **New**, and then click **Folder**.
A new folder is created and is in "rename mode."
34. Type **XML Notepad**, and then press ENTER.
35. Right-click the **XML Notepad** folder, and then click **Properties**.
36. Click the **Security** tab.
37. Click **Edit**.
38. Click **Add**. The **Select Users, Computers, or Groups** dialog box appears.
39. Type **APP_XML Notepad**, and then press ENTER.
The group is given the default, Read & Execute permission.
40. Click **OK** twice to close all open dialog boxes.
41. Open the **XML Notepad** folder.
42. Open the **D:\Labfiles\Lab07b** folder in a new window.
43. Right-click **XMLNotepad.msi**, and then click **Copy**.
44. Switch to the Windows Explorer window displaying **\\server01\c\$\Software\XML Notepad**.
45. Right-click in the empty details pane, and then click **Paste**.
XML Notepad is copied into the folder on SERVER01.
46. Close all open Windows Explorer windows.
47. Close the Computer Management console.

► **Task 3: Create a software deployment GPO**

1. Run **Group Policy Management** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand **Forest:contoso.com**, **Domains** and **contoso.com**, and then click the **Group Policy Objects** container.

3. Right-click the **Group Policy Objects** container, and then click **New**.
4. In the **Name** box, type **XML Notepad**, and then click **OK**.
5. Right-click the **XML Notepad** GPO, and then click **Edit**.
6. In the console tree, expand **Computer Configuration, Policies, and Software Settings**, and then click **Software Installation**.
7. Right-click **Software Installation**, point to **New**, and then click **Package**.
8. In the **File name** text box, type the network path to the software distribution folder, **\\server01\software\XML Notepad**, and then press ENTER.
9. Select the Windows Installer package, **XmlNotepad.msi**, and then click **Open**.
After a few moments, the Deploy Software dialog box appears.
10. Click **Advanced**, and then click **OK**.
The XML Notepad 2007 Properties dialog box appears.
11. On the **General** tab, note that the name of the package includes the version, XML Notepad 2007.
12. Click the **Deployment** tab.
Note that when deploying software to computers, Assigned is the only option. Examine the options that would be available if you were assigning or publishing the application to users.
13. Select **Uninstall this application when it falls out of the scope of management**.
14. Click **OK**.
15. Close **Group Policy Management Editor**.
16. In the Group Policy Management console tree, expand **Group Policy Objects**, and then click the **XML Notepad** GPO.
17. In the details pane, click the **Scope** tab.
18. In the **Security Filtering** section, select **Authenticated Users**, and then click **Remove**. You are prompted to confirm your choice.
19. Click **OK**.
20. Click the **Add** button.

The Select User, Computer or Group dialog box appears.

21. Type **APP_XML Notepad**, and press ENTER.
The GPO is now filtered to apply only to the APP_XML Notepad group. However, the GPO settings will not apply until it is linked to an OU, to a site, or to the domain.
22. In the console tree, right-click the **Client Computers** OU, and then click **Link an Existing GPO**.
23. Select **XML Notepad** from the Group Policy Objects list, and then click **OK**.

► **Task 4: Deploy software to computers**

1. Switch to **Active Directory Users and Computers**.
2. In the console tree, expand **Groups**, and then click the **Application** OU.
3. In the details pane, double-click **APP_XML Notepad**.
4. Click the **Members** tab.
5. Click the **Add** button.
6. Click the **Object Types** button.
7. Select **Computers**, and then click **OK**.
8. Type **DESKTOP101**, and then press ENTER.
9. Click **OK**.
10. Start 6425B-DESKTOP101-A, but do not log on.

► **Task 5: Confirm the successful deployment of software**

1. Switch to DESKTOP101.
2. Log on to DESKTOP101 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Click the **Start** button, and then click **All Programs**.
4. Open **XML Notepad**.

If XML Notepad is not installed, restart DESKTOP101 and repeat steps 2-4.



Note: When verifying the deployment of the xml notepad and it may take two startups to be successful. I.e. if you do not see Notepad installed restart the virtual machine. You may need to do this a couple of times.

Exercise 2: Upgrade Applications with GPSI

► Task 1: Create an upgrade package by using GPSI

1. Switch to HQDC01.
2. In the **Group Policy Management** console tree, right-click the **XML Notepad** GPO in the **Group Policy Objects** container, and then click **Edit**.
The Group Policy Management Editor opens.
3. In the console tree, expand **Computer Configuration, Policies, Software Settings**, and then click **Software Installation**.
4. Right-click **Software Installation**, point to **New**, and then click **Package**.
5. In the **File name** text box, type the network path to the software distribution folder, `\\server01\software\XML Notepad`, and then press ENTER.
This exercise will use the existing XmlNotepad.msi file as if it is an updated version of XML Notepad.
6. Select the Windows Installer package, **XmlNotepad.msi**, and then click **Open**.
The Deploy Software dialog box appears.
7. Click **Advanced**, and then click **OK**.
8. On the **General** tab, change the name of the package to suggest that it is the next version of the application. Type **XML Notepad 2010**.
9. Click the **Deployment** tab. Because you are deploying the application to computers, **Assigned** is the only deployment type option.
10. Click the **Upgrades** tab.
11. Click the **Add** button.
12. Click the **Current Group Policy Object (GPO)** option.
13. In the **Package to upgrade** list, select the package for the simulated earlier version, **XML Notepad 2007**.
14. Click the **Uninstall the existing package and then select then install the upgrade package** option.
15. Click **OK**.

16. Click **OK**.

If this were an actual upgrade, the new package would upgrade the previous version of the application as clients applied the XML Notepad GPO. Because this is only a simulation of an upgrade, you can remove the simulated upgrade package.

17. Right-click **XML Notepad 2010**, which you just created to simulate an upgrade, point to **All Tasks**, and then select **Remove**.
18. In the **Remove Software** dialog box, click **Immediately uninstall the software from users and computers**, and then click **OK**.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs.

Lab Review Questions

Question: Consider the NTFS permissions you applied to the Software and XML Notepad folders on SERVER01. Explain why these least privilege permissions are preferred to the default permissions.

Answer: The default permissions on a new NTFS folder include inherited permissions that are not least privilege. First, the USERS group is given the ability to add files and folders. In a software distribution folder, only administrators who need to add new applications should have the ability to add files and folders. Second, CREATOR OWNER special identity is given full control. This means that whoever adds a file or folder gets an explicit permission that allows full control, which may or may not be appropriate for each file and folder added to a software deployment point. Third, the USERS group is also given the ability to read all files and folders, which will allow them to install any software in the software distribution folder. Because most software is licensed per computer or per user, you can improve your compliance by allowing only a specified group to read the installation files for each application. The SOFTWARE folder (the root) gives access (full control) only to Administrators and System. The application subfolder, for example, XML Notepad, gives read access to a group that is allowed to install the application, for example, APP_XML Notepad. Those users can get to the subfolder even though they do not have access to the SOFTWARE folder. Windows allows all authenticated users the "traverse folders" privilege by default, which allows users to navigate to a specific subfolder to which they have access even if they do not have permission to a parent folder. The least privilege ACLs used in this Lab are a perfect example of the value of this user right.

Question: Consider the methods used to scope the deployment of XML Notepad: Assigning the application to computers, filtering the GPO to apply to the APP_XML Notepad group that contains only computers, and linking the GPO to the Client Computers OU. Why is this approach advantageous for deploying most software? What would be the disadvantage of scoping software deployment to users rather than to computers?

Answer: Most software is licensed per computer, so it is important to deploy such applications scoped to computers, rather than to users. The result is the same—the application is deployed to the computers of the users who require the application. If you were to deploy an application to users, it would "follow" the users to whatever computers they logged on to. For example, if a user logged on to a conference room computer or to a colleague's computer, the application would be installed on those computers as well. By scoping to a group of computers, and linking the GPO to a high-level OU (or even to the domain), it gives you maximum flexibility to deploy the application to whatever computers require it.

Lab D: Audit File System Access

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.
This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.
2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.
A User Account Control (UAC) dialog box appears.
2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

- a. Click **Use Another Account**.
3. In **User Name**, type the username.
4. In **Password**, type the password.
5. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

- a. In **User Name**, type the username.
6. In **Password**, type the password.
7. Press ENTER or click **OK**.

Exercise 1: Configure Permissions and Audit Settings

► Task 1: Prepare for the lab

The virtual Machines should already be started and available after completing the previous labs. However, if they are not, you should complete the below steps.

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Start 6425B-SERVER01-A but do not log on to the system.
4. Start 6425B-DESKTOP101-A but do not log on.
5. Wait for all virtual machines to complete startup before continuing to the next task.

► Task 2: Create and secure a shared folder

1. Switch to HQDC01.
2. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
3. In the console tree, expand the **contoso.com** domain and the **Groups** OU, and then click the **Role** OU.
4. Right-click the **Role** OU, point to **New**, and then click **Group**.
5. Type **Consultants**, and then press ENTER.
6. Double-click the **Consultants** group.
7. Click the **Members** tab.
8. Click the **Add** button.

The Select Users, Contacts, Computers, or Groups dialog box appears.

9. Type **Mike.Danseglio**, and then press ENTER.
10. Click **OK**.
11. Click **Start**, click **Run**, type **\\SERVER01\\c\$**, and then press ENTER.
The Connect to SERVER01 dialog box appears.
12. In the **User name** box, type **CONTOSO\Pat.Coleman_Admin**.

13. In the **Password** box, type **Pa\$\$w0rd**, and then press ENTER.

A Windows Explorer window opens, focused on the root of the C drive on SERVER01.

14. Open the **Data** folder.
15. Click the **File** menu, point to **New**, and then click **Folder**.
A new folder is created in "rename mode."
16. Type **Confidential Data**, and then press ENTER.
17. Right-click **Confidential Data**, and then click **Properties**.
18. Click the **Security** tab.
19. Click **Edit**.
20. Click **Add**.
21. Type **Consultants**, and then click **OK**.
22. Select the **Deny** check box for the **Full Control** permission.
23. Click **Apply**.
24. Click **Yes** to confirm the use of a Deny permission.
25. Click **OK** to close all open dialog boxes.

► **Task 3: Configure auditing settings on a folder**

1. Right-click **Confidential Data**, and then click **Properties**.
2. Click the **Security** tab.
3. Click **Advanced**.
4. Click the **Auditing** tab.
5. Click **Edit**.
6. Click **Add**.
7. Type **Consultants**, and then click **OK**.
8. In the **Auditing Entry** dialog box, select the check box under **Failed**, next to **Full Control**.
9. Click **OK** to close all open dialog boxes.

Exercise 2: Configure Audit Policy

► Task 1: Enable auditing of file system access by using Group Policy

1. Run **Group Policy Management** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand **Forest:contoso.com**, **Domains**, and **contoso.com**, and then click the **Group Policy Objects** container.
3. Right-click the **Group Policy Objects** container, and then click **New**.
4. In the **Name** box, type **File Server Auditing**, and then click **OK**.
5. Right-click the **File Server Auditing** GPO, and then click **Edit**.

The Group Policy Management Editor opens.

6. In the console tree, expand **Computer Configuration**, **Policies**, **Windows Settings**, **Security Settings**, and **Local Policies**, and then click **Audit Policy**.
7. Double-click **Audit object access**.
8. Select **Define these policy settings**.
9. Select the **Failure** check box.
10. Click **OK**.
11. Close **Group Policy Management Editor**.
12. In the GPM console tree, expand the **Servers** OU, and then click the **File** OU.
13. Right-click the **File** OU, and then click **Link an Existing GPO**.
The Select GPO dialog box appears.
14. Select **File Server Auditing**, and then click **OK**.

Exercise 3: Examine Audit Events

► Task 1: Generate audit events

1. Switch to SERVER01.
2. Log on to SERVER01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
4. Type **gpupdate.exe /force**, and then press ENTER.
5. Switch to DESKTOP101.
6. Log on to DESKTOP101 as **Mike.Danseglio** with the password **Pa\$\$w0rd**.
7. Click **Start**. In the **Start Search** box, type “**\\server01\data\Confidential Data**” and press ENTER.

A message appears to inform you that Windows cannot access
\\server01\data\Confidential Data.
8. Click **Cancel**.

► Task 2: Examine audit event log messages

1. Switch to SERVER01.
2. Run **Event Viewer** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
3. In the console tree, expand **Windows Logs**, and then click **Security**.
4. Locate the audit failure events related to Mike Danseglio's access to the Confidential Data folder.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: What are the three major steps required to configure auditing of file system and other object access?

Answer: 1) Configure auditing settings on the file/folder SACL. 2) Enable audit policy for object access, in a GPO scoped to the server. 3) Examine event log audit entries.

Question: What systems should have auditing configured? Is there a reason not to audit all systems in your enterprise? What types of access should be audited, and by whom should they be audited? Is there a reason not to audit all access by all users?

Answer: Auditing should reflect IT security and usage policies. Auditing not only puts a (small) burden on performance of a system, but also generates excessive “noise” that can make finding the “important” events even harder. What, who, and when auditing is performed should be aligned with why auditing is being performed—as driven by your business requirements.

Module 8

Lab Answer Key: Secure Administration

Contents:

Lab A: Delegate Administration

Exercise 1: Delegate Permission to Create and Support User Accounts 4

Exercise 2: View Delegated Permissions 10

Exercise 3: Remove and Reset Permissions 13

Lab B: Audit Active Directory Changes

Exercise 1: Audit Changes to Active Directory by Using Default Audit Policy 17

Exercise 2: Audit Changes to Active Directory by Using Directory Service
Changes Auditing 20

Lab A: Delegate Administration

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the username.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

1. In **User Name**, type the username.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Delegate Permission to Create and Support User Accounts

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Open **D:\Labfiles\Lab08a**.
4. Run **Lab08a_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
5. The lab setup script runs. When it is complete, press any key to continue.
6. Close the Windows Explorer window, **Lab08a**.

► Task 2: Create security groups for role-based management

1. On HQDC01 click **Start > Administrative Tools** and run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **contoso.com** domain and the **Groups** OU, and then click the **Role** OU.
3. Right-click the **Role** OU, then point to **New**, and then click **Group**.
4. In **Group name**, type **Help Desk**.
5. Confirm that **Group scope** is **global** and **Group type** is **Security**.
6. Click **OK**.
7. Repeat steps 3 through 5 to create a global security group named **User Account Admins**.
8. Right-click **Help Desk**, and then click **Properties**.
9. Click the **Members** tab.
10. Click the **Add** button.
11. Type **Aaron.Painter_Admin**; **Elly.Nkya_Admin**; **Julian.Price_Admin**; **Holly.Dickson_Admin**, and then press ENTER.
12. Click **OK** to close the group **Properties** dialog box.

13. Right-click **User Account Admins**, and then click **Properties**.
14. Click the **Members** tab.
15. Click the **Add** button.
16. Type **Pat.Coleman_Admin;April.Meyer_Admin;Max.Stevens_Admin**, and then press ENTER.
18. Click **OK** to close the group **Properties** dialog box.
19. In the console tree, expand the **Admins** OU and the **Admin Groups** OU, and then click **AD Delegation**.
20. Right-click **AD Delegation**, then point to **New**, and then click **Group**.
21. In **Group name**, type **AD_User Accounts_Support**.
22. In **Group scope**, click **Domain local**.
23. Confirm that **Group type** is **Security**.
24. Click **OK**.
25. Right-click **AD Delegation**, then point to **New**, and then click **Group**.
26. In **Group name**, type **AD_User Accounts_Full Control**.
27. In **Group scope**, click **Domain local**.
28. Confirm that **Group type** is **Security**.
29. Click **OK**.
30. Right-click **AD_User Accounts_Support**, and then click **Properties**.
31. Click the **Members** tab.
32. Click the **Add** button.
33. Type **Help Desk**, and then press ENTER.
34. Click **OK** to close the group **Properties** dialog box.
35. Right-click **AD_User Accounts_Full Control**, and then click **Properties**.
36. Click the **Members** tab.
37. Click the **Add** button.
38. Type **User Account Admins**, and then press ENTER.
39. Click **OK** to close the group **Properties** dialog box.

► **Task 3: Delegate control of user support with the Delegation of Control Wizard**

1. In the console tree, right-click the **User Accounts** OU, and then click **Delegate Control**.

The Welcome to the Delegation of Control Wizard appears.

2. Click **Next**.
3. On the **Users or Groups** page, click the **Add** button.
The Select Users, Computers, or Groups dialog box appears.
4. Type **AD_User Accounts_Support**, and then press ENTER.
5. Click **Next**.
6. On the **Tasks to Delegate** page, select the **Reset user passwords and force password change at next logon** check box.
7. Click **Next**.
8. On the **Completing the Delegation of Control Wizard** page, click **Finish**.

► **Task 4: Delegate permission to create and delete users with the Access Control List Editor interface**

1. Click the **View** menu, and then select **Advanced Features**, so that the Advanced Features option is enabled.
2. In the console tree, right-click the **User Accounts** OU, and then click **Properties**.

The User Accounts Properties dialog box appears.

3. Click the **Security** tab.
4. Click the **Advanced** button.
The Advanced Security Settings for User Accounts dialog box appears.
5. Click the **Add** button.
The Select User, Computer, or Group dialog box appears.
6. Type **AD_User Accounts_ Full Control** and press ENTER.
The Permission Entry for User Accounts dialog box appears.

7. In the **Apply to** list, select **This object and all descendant objects**.
8. In the **Permissions** list, select the **Allow** check box next to **Create User objects**.
9. In the **Permissions** list, select the **Allow** check box next to **Delete User objects**.
10. Click **OK**.
11. Click the **Add** button.
The Select User, Computer, or Group dialog box appears.
12. Type **AD_User Accounts_ Full Control** and press ENTER.
The Permission Entry for User Accounts dialog box appears.
13. In the **Apply to** list, select **Descendant User objects**.
14. In the **Permissions** list, select the **Allow** check box next to **Full control**.
15. Click **OK**.
16. Click **OK** to close each remaining open dialog box.

► **Task 5: Validate the implementation of delegation**

1. Close Active Directory Users and Computers.
2. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Aaron.Painter_Admin** with the password **Pa\$\$w0rd**.
3. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.
4. In the details pane, right-click **Jeff Ford**, and then click **Reset Password**.
The Reset Password dialog box appears.
5. In **New password**, type **Pa\$\$w0rd**.
6. In **Confirm password**, type **Pa\$\$w0rd**.
7. Notice that the **User must change password at next logon** check box is disabled.
8. Click **OK**.
A message appears: "The password for Jeff Ford has been changed."
9. Click **OK**.

10. Right-click **Jeff Ford**, and then click **Disable Account**. A message appears: "Windows cannot disable object Jeff Ford because: insufficient access rights to perform the operation."
11. Click **OK**.
12. In the console tree, expand the **contoso.com** domain and the **Admins** OU, and then click the **Admin Identities** OU.
13. In the details pane, right-click **Pat Coleman (Administrator)**, and then click **Reset Password**.
The Reset Password dialog box appears.
14. In **New password**, type **Pa\$\$w0rd**.
15. In **Confirm password**, type **Pa\$\$w0rd**.
16. Notice that the **User must change password at next logon** check box is disabled.
17. Click **OK**.

A message appears: "Windows cannot complete the password change for Pat Coleman (Administrator) because: Access is denied."

18. Close Active Directory Users and Computers.
19. Run **Active Directory Users and Computers** with administrative credentials. Use the account **April.Meyer_Admin** with the password **Pa\$\$w0rd**.
20. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click **Employees**.
21. Right-click **Employees**, then point to **New**, and then click **User**. The **New Object - User** dialog box appears.
22. In **First name**, type your first name.
23. In **Last name**, type your last name.
24. In **User logon name**, type a username for yourself following the naming standard **FirstName.LastName**.
25. Click **Next**.

Note that user logon names can be only 20 characters.

If you receive a message that indicates that another user account already exists with the same name, change your user logon name so that it is unique by adding **_6425** to the end.

26. In **Password**, type **Pa\$\$w0rd**.
27. In **Confirm password**, type **Pa\$\$w0rd**.
28. Click **Next**.
29. Click **Finish**.
30. Close Active Directory Users and Computers.

Exercise 2: View Delegated Permissions

► Task 1: View permissions in the Access Control List Editor interfaces

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **contoso.com** domain, and then click the **User Accounts** OU.
3. Right-click the **User Accounts** OU, and then click **Properties**.
The User Accounts Properties dialog box appears.
4. Click the **Security** tab.
If you do not see the Security tab, close the dialog box. Click the View menu of the MMC console, and ensure that Advanced Features is selected. Then open the properties of the object again.
5. Click the **Advanced** button.
The Advanced Security Settings for User Accounts dialog box appears.
6. Click the **Name** column heading, so that the **Name** column is sorted alphabetically.

Question: How many permission entries were created for the AD_User Accounts_Support group by the Delegation of Control Wizard? Is it easy to tell what permissions were assigned in the Permission Entries list? List the permissions assigned to AD_User Accounts_Support.

Answer: Two permission entries appear in the list. It is not easy to tell exactly what permissions were assigned in the list: one entry reports "Special" and the other entry reports nothing in the Permission column. Clicking Edit for the "Special" permission shows that it is Reset Password. Clicking Edit for the other permission shows that it is Read pwdLastSet and Write pwdLastSet.

7. Click **Cancel** to close all open dialog boxes.

► **Task 2: Report permissions using DSACLs**

1. Click **Start**, and then click **Command Prompt**.
2. Type the command **dscls "ou=User Accounts,dc=contoso,dc=com"** and then press ENTER.

Question: What permissions are reported for AD_User Accounts_Support by the DSACLs command?

Answer: DSACLs reports the following permissions for AD_User Accounts_Support:
SPECIAL ACCESS for pwdLastSet: WRITE PROPERTY and READ PROPERTY
Reset Password

► **Task 3: Evaluate effective permissions**

1. In the Active Directory Users and Computers console tree, expand the **contoso.com** domain and the **User Accounts** OU.
2. Right-click the **User Accounts** OU, and then click **Properties**.
The User Accounts Properties dialog box appears.
3. Click the **Security** tab.
4. Click the **Advanced** button.
The Advanced Security Settings for User Accounts dialog box appears.
5. Click the **Effective Permissions** tab.
6. Click the **Select** button.
The Select User, Computer, or Group dialog box appears.
7. Type **April.Meyer_Admin**, and then press ENTER.
8. Locate the permissions **Create User objects** and **Delete User objects**, approximately halfway down the **Effective permissions** list.

Question: Do you see the Reset Password permission in this list?

Answer: No. A Lab Review question at the end of this lab will address why the permission does not appear.

9. Click **Cancel** to close all open dialog boxes.
10. In the console tree, expand the **contoso.com** domain and the **User Accounts** OU, and then click the **Employees** OU.
11. In the details pane, right-click **Aaron Lee**, and then click **Properties**.
The Aaron Lee Properties dialog box appears.
12. Click the **Security** tab.
13. Click the **Advanced** button.
The Advanced Security Settings for Aaron Lee dialog box appears.
14. Click the **Effective Permissions** tab.
15. Click the **Select** button
The Select User, Computer, or Group dialog box appears.
16. Type **Aaron.Painter_Admin**, and then press ENTER.
17. Locate the **Reset Password** permission in the **Effective Permissions** list.
18. Click **Cancel** to close all open dialog boxes.

Exercise 3: Remove and Reset Permissions

► Task 1: Remove permissions assigned to AD_User Accounts_Support

1. In the console tree, expand the **contoso.com** domain, and then click the **User Accounts** OU.
2. Right-click the **User Accounts** OU, and then click **Properties**.
The User Accounts Properties dialog box appears.
3. Click the **Security** tab.
4. Click the **Advanced** button.
The Advanced Security Settings for User Accounts dialog box appears.
5. Click the **Name** column heading so that the **Name** column is sorted alphabetically.
6. Select the first permission assigned to **AD_User Accounts_Support**, and then click **Remove**.
7. Select the remaining permission assigned to **AD_User Accounts_Support**, and then click **Remove**.
8. Click **OK** to close the remaining open dialog boxes.

► Task 2: Reset the User Accounts OU to its default permissions

1. In the console tree, expand the **contoso.com** domain, and then click the **User Accounts** OU.
2. Right-click the **User Accounts** OU, and then click **Properties**.
The User Accounts Properties dialog box appears.
3. Click the **Security** tab.
4. Click the **Advanced** button.
The Advanced Security Settings for User Accounts dialog box appears.
5. Click **Restore defaults**, and then click **Apply**.



Note: Do not shut down the virtual machine once you are finished with this lab as the settings you have configured here will be used in the subsequent lab.

Question: What do you achieve by clicking Restore defaults? What permissions remain?

Answer: All custom, explicit permissions are removed. What remain are the default permissions explicitly assigned to any new OU object, as defined by the Active Directory Schema. In addition, permissions inherited from parent objects apply.

Lab B: Audit Active Directory Changes

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the username.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the username.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a username and password:

1. In **User Name**, type the username.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Audit Changes to Active Directory by Using Default Audit Policy

► Task 1: Prepare for the lab

The virtual Machines should already be started and available after completing Lab A. However, if they are not, you should complete the below steps then step through Exercises 1 to 3 in Lab A before continuing.

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 2: Confirm that the Domain Admins group is configured to audit changes to its membership

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **contoso.com** domain, and then click the **Users** container.
3. Right-click the **Domain Admins** group, and then click **Properties**.

The Domain Admins Properties dialog box appears.

4. Click the **Security** tab.

If you do not see the Security tab, close the dialog box. Click the View menu of the MMC console, and ensure that Advanced Features is selected. Then open the properties of the object again.

5. Click the **Advanced** button.

The Advanced Security Settings for Domain Admins dialog box appears.

6. Click the **Auditing** tab.
7. Select the first audit entry, for which the **Access** column is **Special**, and then click **Edit**.

The Auditing Entry for Domain Admins dialog box appears.

8. Locate the entry that specifies for auditing of successful attempts to modify properties of the group such as membership.

Question: What is the Auditing Entry that achieves this goal?

Answer: Successful attempts to Write all properties by the Everyone group.

9. Click **Cancel** to close each open dialog box.

► **Task 3: Make a change to the membership of Domain Admins**

1. Right-click the **Domain Admins** group, and then click **Properties**.
The Domain Admins Properties dialog box appears.
2. Click the **Members** tab.
3. Click **Add**.
4. Type **Stuart.Munson**, and press ENTER.
5. Click **Apply** to apply your change.
6. Select **Stuart Munson**.
7. Click **Remove**.
A message appears asking you to confirm the removal.
8. Click **Yes**.
9. Click **OK** to close the **Domain Admins Properties** dialog box.
10. Make a note of the time when you made the changes. That will make it easier to locate the audit entries in the event logs.

► **Task 4: Examine the events that were generated**

1. Run **Event Viewer** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand **Windows Logs**, and then click **Security**.
3. Scroll down to the events that took place at approximately the time that you made the changes to **Domain Admins**. You should see events that are *not* logon, logoff, or Kerberos (authentication) related.

Question: What is the Event ID of the event logged when you made your changes? What is the Task Category?

Answer: 4662. Directory Service Access.

Question: Examine the information provided on the General tab. Can you identify the following in the event log entry?

Who made the change?

When the change was made?

What object was changed?

What type of access was performed?

What attribute was changed? How is the changed attribute identified?

What change was made to that attribute?

Answer: You will be able to identify that a user (Pat.Coleman_Admin) accessed an object (Domain Admins) and used a Write Property access. The time of the change is shown. The property itself is displayed as a globally unique identifier (GUID)—you cannot readily identify that the Members property was changed. The event also does not detail the exact change that was made to the property.

Exercise 2: Audit Changes to Active Directory by Using Directory Service Changes Auditing

► Task 1: Enable Directory Services Changes auditing

1. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Type the following command, and then press ENTER:

```
auditpol /set /subcategory:"directory service changes"  
/success:enable
```

► Task 2: Make a change to the membership of Domain Admins

1. Switch to Active Directory Users and Computers.
2. In the console tree, expand the **contoso.com** domain, and then click the **Users** container.
3. Right-click the **Domain Admins** group, and then click **Properties**.
The Domain Admins Properties dialog box appears.
4. Click the **Members** tab.
5. Click **Add**.
6. Type **Stuart.Munson** and press ENTER.
7. Click **Apply** to apply your change.
8. Select **Stuart Munson**.
9. Click **Remove**.

A message appears asking you to confirm the removal.

10. Click **Yes**.
11. Click **OK** to close the **Domain Admins Properties** dialog box.
12. Make a note of the time when you made the changes. That will make it easier to locate the audit entries in the event logs.

► **Task 3: Examine the events that were generated**

1. Switch to Event Viewer.
2. In the console tree, expand **Windows Logs**, and then click **Security**.
3. Right-click **Security**, and then click **Refresh**.
4. Scroll down to the events that took place at approximately the time that you made the changes to Domain Admins. You should see events that are different than those you saw in the previous task.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Question: What are the Event IDs of the event logged when you made your changes? What is the Task Category?

Answer: Adding a member is event 4728. Removing a member is event 4729. Both events are in the Security Group Management Task Category.

Question: Examine the information provided on the General tab. Can you identify the following in the event log entry?

What type of change was made?

Who made the change?

What member was added or removed?

What group was affected?

When the change was made?

Answer: You can identify that a member was added or removed, that Pat.Coleman_Admin made the change, that Stuart Munson was the member that was added or removed, and the change was made to the Domain Admins group. The event metadata also shows when the change occurred.

Module 9

Lab Answer Key: Improve the Security of Authentication in an Active Directory Domain Services (AD DS) Domain

Contents:

Lab A: Configure Password and Account Lockout Policies

Exercise 1: Configure the Domain's Password and Lockout Policies 4

Exercise 2: Configure Fine-Grained Password Policy 6

Lab B: Audit Authentication

Exercise 1: Audit Authentication 12

Lab C: Configure Read-Only Domain Controllers

Exercise 1: Install an RODC 19

Exercise 2: Configure Password Replication Policy 22

Exercise 3: Manage Credential Caching 25

Lab A: Configure Password and Account Lockout Policies

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press **ALT+DELETE**.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the user name.
5. In **Password**, type the password.
6. Press **ENTER** or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the user name.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a user name and password:

1. In **User Name**, type the user name.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Configure the Domain's Password and Lockout Policies

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 2: Configure the domain account policies

1. Run **Group Policy Management** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand **Forest:contoso.com, Domains**, and **contoso.com**.
3. Right-click **Default Domain Policy** underneath the domain, contoso.com and click **Edit**.

You may be prompted with a reminder that you are changing the settings of a GPO. If so, click **OK**.

Group Policy Management Editor opens.

4. In the console tree, expand **Computer Configuration, Policies, Windows Settings, Security Settings**, and **Account Policies**, and then click **Password Policy**.
5. Double-click the following policy settings in the console details pane and configure the settings as indicated:
 - Maximum password age: **90** Days
 - Minimum password length: **10** characters
6. In the console tree, click **Account Lockout Policy**.
7. Double-click the **Account lockout threshold** policy setting and configure it for **5** Invalid Logon Attempts. Then click **OK**.

A Suggested Value Changes window appears.

8. Click **OK**.

The values for Account lockout duration and Reset account lockout counter after are automatically set to 30 minutes.

9. Close the Group Policy Management Editor window.
10. Close the Group Policy Management window.

Exercise 2: Configure Fine-Grained Password Policy

► Task 1: Create a PSO

1. Click **Start**, point to **Administrative Tools**, right-click **ADSI Edit**, and then click **Run as administrator**.
2. Click **Use another account**.
3. In the **User name** box, type **Pat.Coleman_Admin**.
4. In the **Password** box, type **Pa\$\$w0rd**, and then press ENTER. ADSI Edit opens.
5. Right-click **ADSI Edit**, and then click **Connect To**.
6. Accept all defaults. Click **OK**.
7. In the console tree, click **Default Naming Context**.
8. In the console tree, expand **Default Naming Context**, and then click **DC=contoso,DC=com**.
9. In the console tree, expand **DC=contoso,DC=com**, and then click **CN=System**.
10. In the console tree, expand **CN=System**, and then click **CN=Password Settings Container**.

All PSOs are created and stored in the Password Settings Container (PSC).

11. Right-click the **PSC**, point to **New**, and then click **Object**.

The Create Objects dialog box appears. It prompts you to select the type of object to create. There is only one choice: *msDS-PasswordSettings*—the technical name for the object class referred to as a PSO.

12. Click **Next**.

You are then prompted for the value for each attribute of a PSO. The attributes are similar to those found in the domain account policies.

13. Configure each attribute as indicated below. Click **Next** after each attribute.
 - **cn: My Domain Admins PSO**. This is the common name of the PSO.
 - **msDS-PasswordSettingsPrecedence: 1**. This PSO has the highest possible precedence.
 - **msDS-PasswordReversibleEncryptionEnabled: False**. The password is not stored using reversible encryption.

- *msDS-PasswordHistoryLength*: **30**. The user cannot reuse any of the last 30 passwords.
- *msDS-PasswordComplexityEnabled*: **True**. Password complexity rules are enforced.
- *msDS-MinimumPasswordLength*: **15**. Passwords must be at least 15 characters long.
- *msDS-MinimumPasswordAge*: **1:00:00:00**. A user cannot change his or her password within one day of a previous change. The format is d:hh:mm:ss (days, hours, minutes, seconds).
- *msDS-MaximumPasswordAge*: **45:00:00:00**. The password must be changed every 45 days.
- *msDS-LockoutThreshold*: **5**. Five invalid logons within the time frame specified by XXX (the next attribute) will result in account lockout.
- *msDS-LockoutObservationWindow*: **0:01:00:00**. Five invalid logons (specified by the previous attribute) within one hour will result in account lockout.
- *msDS-LockoutDuration*: **1:00:00:00**. An account, if locked out, will remain locked for one day, or until it is unlocked manually. A value of zero will result in the account remaining locked out until an administrator unlocks it.

14. Click **Finish**.

15. Close **ADSI Edit**.

► Task 2: Link a PSO to a Group

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **System** container.
If you do not see the System container, then click the View menu of the MMC console, and ensure that Advanced Features is selected.
3. In the console tree, click the **Password Settings Container**.
4. Right-click **My Domain Admins PSO**, click **Properties** and then click the **Attribute Editor** tab.

5. In the **Attributes** list, select **msDS-PSOAppliesTo**, and then click **Edit**.
The Multi-valued Distinguished Name With Security Principal Editor dialog box appears.
6. Click **Add Windows Account**.
The Select Users, Computers, or Groups dialog box appears.
7. Type **Domain Admins**, and then press ENTER.
8. Click **OK** twice to close the open dialog boxes.

► **Task 3: Identify the Resultant PSO for a user**

1. In the console tree, expand the **contoso.com** domain and the **Admins** OU, and then click the **Admin Identities** OU.
2. Right-click **Pat Coleman (Administrator)** and click **Properties**.
3. Click the **Attribute Editor** tab.
4. Click the **Filter** button, and click the **Constructed** option, so that it is selected.
The attribute you will locate in the next step is a constructed attribute, meaning that the resultant PSO is not a hard-coded attribute of a user; rather it is calculated by examining the PSOs linked to a user in real-time.

Question: What is the resultant PSO for Pat Coleman (Administrator)?

Answer: Open the value of the msDS-ResultantPSO attribute. The My Domain Admins PSO is the resultant PSO. It is displayed using its distinguished name (DN), CN=My Domain Admins PSO,CN=Password Settings Container,CN=System,DC=contoso,DC=com.

► Task 4: Delete a PSO

1. Close any open dialog boxes in Active Directory Users and Computers.
2. In the console tree, expand the **contoso.com** domain and the **System** container, and then click **Password Settings Container**.
3. Right-click **My Domain Admins PSO**, and then click **Delete**.
A confirmation prompt appears.
4. Click **Yes**.



Note: Do not shut down the virtual machine once you are finished with this lab as the settings you have configured here will be used in subsequent labs in this module.

Lab Review Questions

Question: Where should you define the default password and account lockout policies for user accounts in the domain?

Answer: Configure the baseline password and account lockout policies in the Default Domain Policy GPO.

Question: What are the best practices for managing PSOs in a domain?

Answer: Each PSO must fully define the appropriate password and account lockout policies, because PSOs do not "merge." Link PSOs to global groups, and not to individual user accounts. Ensure that each PSO has a unique precedence value.

Question: How can you define a unique password policy for all of the service accounts in the Service Accounts OU?

Answer: PSOs cannot be linked to an OU. You must create a global group that contains the accounts that are in the Service Accounts OU. You can then link a PSO to that group.

Lab B: Audit Authentication

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the user name.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the user name.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a user name and password:

1. In **User Name**, type the user name.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Audit Authentication

► Task 1: Prepare for the lab

The virtual Machine required to start this lab should already be started and available after completing Lab A. However, if it are not, you should complete the below steps and complete exercises 1 and 2 in Lab A.

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Open **D:\Labfiles\Lab09b**.
4. Run **Lab09b_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
5. The lab setup script runs. When it is complete, press any key to continue.
6. Close the Windows Explorer window, **Lab09b**.

► Task 2: Configure auditing of account logon events

1. Run **Group Policy Management** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand **Forest:contos.com**, **Domains**, **contoso.com**, and the **Domain Controllers** OU.
3. Right-click **Default Domain Controllers Policy**, and then click **Edit**.
The Group Policy Management Editor appears.
4. In the console tree, expand **Computer Configuration**, **Policies**, **Windows Settings**, **Security Settings**, and **Local Policies**, and then click **Audit Policy**.
5. Double-click **Audit account logon events**.
6. Select the **Define these policy settings** check box.
7. Select both the **Success** and **Failure** check boxes. Click **OK**.
8. Close the **Group Policy Management Editor**.

► **Task 3: Configure auditing of logon events**

1. In the **Group Policy Management** console tree, expand **Forest, Domains, contoso.com**, and the **Servers** OU, and then click the **Important Project** OU.
2. Right-click the **Important Project** OU and click **Create a GPO in this domain, and Link it here**.
3. In the **Name** box, type **Server Lockdown Policy**, and then click **OK**.
4. In the console tree, expand the **Important Project** OU.
5. In the console tree, right-click the link to the **Server Lockdown Policy** GPO, and then click **Edit**.

The Group Policy Management Editor appears.

5. In the console tree expand **Computer Configuration, Policies, Windows Settings, Security Settings**, and **Local Policies**, and then click **Audit Policy**.
6. Double-click **Audit logon events**.
7. Select the **Define these policy settings** check box.
8. Select both the **Success** and **Failure** check boxes. Click **OK**.
9. Close the **Group Policy Management Editor**.
10. Close **Group Policy Management**.

► **Task 4: Force a refresh Group Policy**

1. Start 6425B-SERVER01-A.

As the computer starts, it will apply the changes you made to Group Policy.

2. Switch to HQDC01.
3. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
3. Type **gpupdate.exe /force**.

This command causes HQDC01 to update its policies, at which time the new auditing settings take effect.

4. Close the Command Prompt window.

► **Task 5: Generate account logon events**

1. Switch to SERVER01.
2. Press ALT+DELETE, which sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine guest.
3. Click **Switch User**, and then click **Other User**.
4. In the **User name** box, type **Pat.Coleman**.
5. In the **Password** box, type **NotMyPassword**, and then press ENTER.
A message appears: *The user name or password is incorrect.*
6. Click **OK**.
7. In the **Password** box, type **Pa\$\$w0rd**, and then press ENTER.

► **Task 6: Examine account logon events**

1. Switch to HQDC01.
2. Run **Event Viewer** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
3. In the console tree, expand **Windows Logs**, and then click **Security**.
4. Look in the first column to identify failure events, then in the second column to see the date and time of the events. You should see only one Failure event at the time you logged on incorrectly.

Question: What Event ID is associated with the account logon failure events? (Tip: Look for the earliest of a series of failure events at the time you logged on incorrectly to SERVER01.)

Answer: 4771: Kerberos pre-authentication failed.

5. Look for the Kerberos Authentication event that happened after the incorrect logon. This should be a successful event generated when you logged on successfully.

Question: What Event ID is associated with the successful account logon? (Tip: Look for the earliest of a series of events at the time you logged on successfully to SERVER01.)

Answer: 4768: A Kerberos Authentication Ticket was requested.

► **Task 7: Examine logon events**

1. Switch to SERVER01.
2. Run **Event Viewer** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
3. In the console tree, expand **Windows Logs**, and then click **Security**.
4. Look in the first column to identify failure events, then in the second column to see the date and time of the events. You should see only one Failure event at the time you logged on incorrectly.

Question: What Event ID is associated with the logon failure events? (Tip: Look for the earliest of a series of failure events at the time you logged on incorrectly to SERVER01.)

Answer: 4625: An account failed to log on.

5. Look for the Logon event that happened after the incorrect logon. This should be a successful event generated when you logged on successfully.

Question: What Event ID is associated with the successful logon? (Tip: Look for the earliest of a series of events at the time you logged on successfully to SERVER01.)

Answer: 4624: An account was successfully logged on. Event 4648 is also registered. The information in the event indicates, "A logon was attempted using explicit credentials." This event shows the initiation of a logon, but it is Event 4624 that shows the logon actually succeeded.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs in this module.

Lab Review Questions

Question: What would be the disadvantage of auditing all successful and failed logons on all machines in your domain?

Answer: Such an audit policy would generate a tremendous amount of audit entries across every machine in your domain. Managing the security event logs and locating the events that indicate potential problems would be very difficult. It is best to align your audit policy with specific, narrowly-targeted auditing goals and requirements of your organization.

Question: You have been asked to audit attempts to log on to desktops and laptops in the Finance division using local accounts such as Administrator. What type of audit policy do you set, and in what GPO(s)?

Answer: You will need to enable auditing for successful and failed account logon events. But because the accounts you are interested in are local accounts, which are authenticated by the local security authority on each desktop and laptop, you will need to do so in a GPO that is scoped to apply to the desktops and laptops in the Finance division. The settings do not need to be scoped to domain controllers.

Lab C: Configure Read-Only Domain Controllers

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the user name.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the user name.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a user name and password:

1. In **User Name**, type the user name.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Install an RODC

► Task 1: Prepare for the lab

The virtual Machine required to start this lab should already be started and available after completing Lab A. However, if it are not, you should complete the below.

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Open **D:\Labfiles\Lab09c**.
4. Run **Lab09c_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
5. The lab setup script runs. When it is complete, press any key to continue.
6. Close the Windows Explorer window, **Lab09c**.

► Task 2: Stage a delegated installation of an RODC

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **contoso.com** domain, and then click the **Domain Controlllers** OU.
3. Right-click **Domain Controlllers** and click **Pre-create Read-only Domain Controller Account**.

The Active Directory Domain Services Installation Wizard appears.

4. Click **Next**.
5. On the **Operating System Compatibility** page, click **Next**.
6. On the **Network Credentials** page, click **Next**.
7. On the **Specify the Computer Name** page, type **BRANCHDC01**, and then click **Next**.
8. On the **Select a Site** page, click **Next**.

9. On the **Additional Domain Controller Options** page, click **Next**.

Note that the option, Read-only domain controller, is selected and cannot be unselected. That is because, of course, you launched the wizard by choosing to pre-create a read-only domain controller account.

10. On the **Delegation of RODC Installation and Administration** page, click the **Set** button.

The Select User or Computer dialog box appears.

11. Type **Aaron.Painter_Admin**, and then press ENTER.
12. Click **Next**.

13. Review your selections on the **Summary** page, and then click **Next**.

14. On the **Completing the Active Directory Domain Services Installation Wizard** page, click **Finish**.

Note that in the DC Type column, the new server is listed as an Unoccupied DC Account (Read-only, GC).

► **Task 3: Run the Active Directory Domain Services Installation Wizard on a workgroup server**

1. Start 6425B-BRANCHDC01-A.
2. Log on to BRANCHDC01 as **Administrator** with the password **Pa\$\$w0rd**.
3. Click **Start**, and then click **Run**.
4. Type **dcpromo**, and then press ENTER.

A window appears that informs you that the Active Directory Domain Services binaries are being installed. When installation is completed, the Active Directory Domain Services Installation Wizard appears.

5. Click **Next**.
6. On the **Operating System Compatibility** page, click **Next**.
7. On the **Choose A Deployment Configuration** page, click the **Existing forest** option, then click **Add a domain controller to an existing domain**, and then click **Next**.
8. On the **Network Credentials** page, type **contoso.com**.

9. Click the **Set** button.

A Windows Security dialog box appears.

10. In the **User Name** box, type **Aaron.Painter_Admin**.
11. In the **Password** box, type **Pa\$\$w0rd**, and then press ENTER.
12. Click **Next**.
13. On the **Select a Domain** page, select **contoso.com**, and then click **Next**.

A message appears to inform you that your credentials do not belong to the Domain Admins or Enterprise Admins groups. Because you have pre-staged and delegated administration of the RODC, you are able to proceed with the delegated credentials.

14. Click **Yes**.

A message appears to inform you that the account for BRANCHDC01 has been pre-staged in Active Directory as an RODC.

15. Click **OK**.

A warning message appears that indicates the computer has a dynamically assigned IP address. BRANCHDC01 has a dynamically assigned IPv6 address. However, the server does have a fixed IPv4 address. IPv6 addresses are not being used in this course, so you can ignore this message.

16. Click **Yes, the computer will use a dynamically assigned IP address (not recommended)**.
17. On the **Location For Database, Log Files, And SYSVOL** page, click **Next**.
18. On the **Directory Services Restore Mode Administrator Password** page, type **Pa\$\$w0rd12345** in the **Password** and **Confirm Password** boxes, and then click **Next**.

In a production environment, you should assign a complex and secure password to the Directory Services Restore Mode Administrator account.

Also note that we altered the domain password policy in Lab A and the directory services restore mode password (Pa\$\$w0rd) is no longer long enough. Therefore we need to add additional characters to meet the minimum required length

19. On the **Summary** page, click **Next**.
20. In the progress window, select the **Reboot On Completion** check box. Active Directory Domain Services is installed on BRANCHDC01, the server reboots.

Exercise 2: Configure Password Replication Policy

► Task 1: Configure domain-wide password replication policy

1. Switch to HQDC01.
2. In the **Active Directory Users and Computers** console tree, click the **Users** container.
3. Double-click **Allowed RODC Password Replication Group**.
4. Click the **Members** tab.
5. Examine the default membership of **Allowed RODC Password Replication Group**.

Question: Who are the default members of Allowed RODC Password Replication Group?

Answer: There are no members by default.

6. Click **OK**.
7. Double-click **Denied RODC Password Replication Group**.
8. Click the **Members** tab.

Question: Who are the default members of Denied RODC Password Replication Group?

Answer: Security-sensitive groups, including Cert Publishers, Domain Admins, Domain Controllers, Enterprise Admins, Group Policy Creator Owners, krbtgt, Read-Only Domain Controllers, and Schema Admins

9. Click the **Add** button.
The Select Users, Contacts, Computers, or Groups dialog box appears.
10. Type **DNSAdmins**, and then press ENTER.
11. Click **OK**.
12. In the console tree, click the **Domain Controllers** OU.
13. Right-click **BRANCHDC01** and click **Properties**.
14. Click the **Password Replication Policy** tab.

Question: What is the password replication policy for the Allowed RODC Password Replication Group? For the Denied RODC Password Replication Group?

Answer: Allow and Deny, respectively.

15. Click **OK** to close the dialog box.

► **Task 2: Create a group to manage password replication to the branch office RODC**

1. In **Active Directory Users and Computers** console tree, expand **Groups**, and then click the **Role** OU.
2. Right-click **Role**, point to **New**, and then click **Group**.
3. In the **Group name:** field, type **Branch Office Users**, and then click **OK**.
4. Right-click **Branch Office Users**, and then click **Properties**.
5. Click the **Members** tab, and then click the **Add** button.
6. Type **Anav.Silverman; Chris.Gallagher; Christa.Geller; Daniel.Roth**, and then click **OK**.
7. Click **OK** to close the **Branch Office Users Properties** dialog box.

► **Task 3: Configure password replication policy for the branch office RODC**

1. In the console tree, click the **Domain Controllers** OU.
2. Right-click **BRANCHDC01** and click **Properties**.
3. Click the **Password Replication Policy** tab.
4. Click the **Add** button.
5. Click **Allow passwords for the account to replicate to this RODC**, and then click **OK**.

The **Select Users, Computers, or Groups** dialog box appears.

6. Type **Branch Office Users**, and then press **ENTER**.
7. Click **OK** to close the **BRANCHDC01 Properties** dialog box.

► **Task 4: Evaluate resultant password replication policy**

1. Right-click **BRANCHDC01** and click **Properties**.
2. Click the **Password Replication Policy** tab.
3. Click the **Advanced** button.

The Advanced Password Replication Policy for BRANCHDC01 dialog box appears.

4. Click the **Resultant Policy** tab, and then click the **Add** button.
The Select Users or Computers dialog box appears.
5. Type **Chris.Gallagher**, and then press ENTER.

Question: What is the resultant policy for Chris.Gallagher?

Answer: Allow.

6. Click **Close**.
7. Click **OK** to close the **BRANCHDC01 Properties** dialog box.

Exercise 3: Manage Credential Caching

► Task 1: Monitor credential caching

1. Switch to BRANCHDC01.
2. Log on to BRANCHDC01 as **Chris.Gallagher** with the password **Pa\$\$w0rd**.
3. Click **Start**, point to the arrow next to the **Lock** button, and then click **Log Off**.
4. Log on to BRANCHDC01 as **Mike.Danseglio** with the password **Pa\$\$w0rd**.
5. Click **Start**, point to the arrow next to the **Lock** button, and then click **Log Off**.
6. Switch to HQDC01.
7. In the **Active Directory Users and Computers** console tree, click the **Domain Controllers** OU.
8. In the details pane, right-click **BRANCHDC01**, and then click **Properties**.
9. Click the **Password Replication Policy** tab.
10. Click the **Advanced** button.

The Advanced Password Replication Policy for BRANCHDC01 dialog box appears.

The Policy Usage tab is displaying Accounts whose passwords are stored on this Read-Only Domain Controller.

Question: What users' passwords are currently cached on BRANCHDC01?

Answer: The only user whose password is stored on BRANCHDC01 is Chris Gallagher. Additionally, passwords for the computer account of BRANCHDC01 itself, and the Kerberos service account, `krbtgt_xyz`, are cached.

11. From the drop-down list, select **Accounts that have been authenticated to this Read-only Domain Controller**.

Question: What users have been authenticated by BRANCHDC01?

Answer: Mike Danseglio and Chris Gallagher.

12. Click **Close**, and then click **OK**.

► **Task 2: Pre-populate credential caching**

1. In the **Active Directory Users and Computers** console tree, click the **Domain Controllers** OU.
2. In the details pane, right-click BRANCHDC01, and then click **Properties**.
3. Click the **Password Replication Policy** tab.
4. Click the **Advanced** button.
The Advanced Password Replication Policy for BRANCHDC01 dialog box appears.
5. Click the **Prepopulate Passwords** button.
The Select Users or Computers dialog box appears.
6. Type **Christa Geller**, and then click **OK**.
7. Click **Yes** to confirm that you want to send the credentials to the RODC.
A message appears: *Passwords for all accounts were successfully prepopulated.*
8. On the **Policy Usage** tab, select **Accounts whose passwords are stored on this Read-only Domain Controller**.
9. Locate the entry for **Christa Geller**. Christa's credentials are now cached on the RODC.
10. Click **Close**.
11. Click **OK**.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: Why should you ensure that the PRP for a branch office RODC has, in its Allow list, the accounts for the *computers* in the branch office as well as the users?

Answer: Computers must authenticate to the domain as well as users, so the logic is the same as with users: you want to improve authentication performance over the WAN and ensure that authentication can continue even if the WAN link is unavailable.

Question: What would be the most manageable way to ensure that computers in a branch are in the Allow list of the RODC's PRP?

Answer: Create a group for computers, for example Branch Office Computers.

Question: What are the pro's and con's of prepopulating the credentials for all users and computers in a branch office to that branch's RODC?

Answer: There is no clear-cut answer to this question. Use it to review the strategic role of an RODC. By prepopulating the credentials of users (and computers) in the branch RODC cache, you ensure that authentication performance is maximized (on the first logon—after that, the credential would have been cached because the users are on the Allow list anyway); and you ensure that, if the WAN link is unavailable on the first logon, users can authenticate. The disadvantage is that, should there be a breach of physical security on the RODC, those credentials are exposed even if the users have not yet logged on in the branch.

Module 10

Lab Answer Key: Configure Domain Name System (DNS)

Contents:

Lab A: Install the DNS Service

Exercise 1: Add the DNS Server Role 4

Exercise 2: Configure Forward Lookup Zones and Resource Records 7

Lab B: Advanced Configuration of DNS

Exercise 1: Enable Scavenging of DNS Zones 12

Exercise 2: Create Reverse Lookup Zones 14

Exercise 3: Explore Domain Controller Location 16

Exercise 4: Configure Name Resolution for External Domains 17

Lab A: Install the DNS Service

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.
This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.
2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the user name.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.
A User Account Control (UAC) dialog box appears.
2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the user name.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a user name and password:

1. In **User Name**, type the user name.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Add the DNS Server Role

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-B.
2. Wait for startup to complete.
3. Start 6425B-HQDC02-B.
4. Log on to HQDC02 as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 2: Add the DNS server role

1. On HQDC02, click the **Server Manager** icon next to the **Start** button.
The User Account Control dialog box appears.
2. In **User name**, type **Pat.Coleman_Admin**.
3. In **Password**, type **Pa\$\$w0rd**, and then press ENTER.
Server Manager opens.
4. In the details pane, under **Roles Summary**, click **Add Roles**.
The Add Roles Wizard appears.
5. On the **Before You Begin** page, click **Next**.
6. In the **Roles** list, click **DNS Server**, and then click **Next**.
7. Read the information on the **DNS Server** page, and then click **Next**.
8. On the **Confirm Installation Selections** page, verify that the DNS Server role will be installed, and then click **Install**.
9. On the **Installation Results** page, click **Close**.
10. Close Server Manager.
11. Restart HQDC02.

This is not necessary in a production environment, but it speeds the process of restarting services and replicating the DNS records to HQDC02 for the purposes of this exercise.

12. Log on to HQDC02 as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► **Task 3: Change the DNS server configuration of the DNS client**

1. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Type **netsh interface ipv4 set dnsserver "Local Area Connection" static 10.0.0.12 primary** and then press ENTER.
3. Type **netsh interface ipv4 add dnsserver "Local Area Connection" 10.0.0.11** and then press ENTER.

► **Task 4: Examine the domain forward lookup zone**

1. Run **DNS Manager** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.

DNS Manager is listed as DNS in the Administrative Tools folder.

DNS Manager opens.
2. In the console tree, expand **HQDC02** and **Forward Lookup Zones**, and then click **contoso.com**.
3. Examine the SOA, NS, and A records in the zone.

► **Task 5: Configure forwarders for Internet name resolution**

1. In the console tree, right-click **HQDC02**, and then click **Properties**.

The HQDC02 Properties dialog box appears.
2. Click the **Forwarders** tab.
3. Click the **Edit** button.

The **Edit Forwarders** dialog box appears.
4. Type **192.168.200.12** and press ENTER.
5. Type **192.168.200.13** and press ENTER.

6. Click **OK**.

Because these DNS servers do not actually exist, the Server FQDN will display either **<Attempting to resolve>** or **<Unable to resolve>**. In a production environment, you would configure forwarders to upstream DNS servers on the Internet, usually those provided by your Internet service provider (ISP).

7. Click **OK**.

Exercise 2: Configure Forward Lookup Zones and Resource Records

► Task 1: Create a forward lookup zone

1. In the console tree, right-click **Forward Lookup Zones**, and then click **New Zone**.
The New Zone Wizard appears.
2. Click **Next**.
3. On the **Zone Type** page, click **Primary zone** and ensure that the option **Store the zone in Active Directory** is selected, and then click **Next**.
4. On the **Active Directory Zone Replication Scope** page, click **To all domain controllers in this domain(for Windows 2000 compatability): contoso.com**, and then click **Next**.
5. On the **Zone Name** page, type **development.contoso.com**, and then click **Next**.
6. On the **Dynamic Update** page, click **Do not allow dynamic updates**, and then click **Next**.
7. On the **Completing the New Zone Wizard** page, click **Finish**.

► Task 2: Create Host and CNAME records

1. In the console tree, expand **HQDC02, Forward Lookup Zones**, and then click **development.contoso.com**.
2. Right-click **development.contoso.com**, and then click **New Host (A or AAAA)**.
The New Host dialog box appears.
3. In **Name**, type **APPDEV01**.
4. In **IP address**, type **10.0.0.24**.
5. Click **Add Host**.
A message appears informing you that the host record was completed successfully.
6. Click **OK**.

7. Click **Done**.
8. Right-click **development.contoso.com**, and then click **New Alias (CNAME)**.
The New Resource Record dialog box appears.
9. In **Alias name**, type **www**.
10. In **Fully qualified domain name (FQDN) for target host**, type **appdev01.development.contoso.com**, and click **OK**.

► **Task 3: Test name resolution**

1. Switch to the command prompt.
2. Type **nslookup www.development.contoso.com**, and then press ENTER.
3. Examine the output of the command. What does the output tell you?

The first section of output tells you which DNS server you queried. The timeout and Server: Unknown lines are the result of the fact that there is not a reverse lookup zone. The nslookup command attempts to resolve the name of the server based on its IP address, 10.0.0.12, and fails. The second section of output is the result of the query. Aliases shows the name you queried. Name shows the host name to which the CNAME (Alias) record resolved. And Address is the IP address of the host.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs.

Lab Review Questions

Question: If you did not configure forwarders on HQDC02, what would be the result for clients that use HQDC02 as their primary DNS server?

Answer: They could not resolve names other than those in the contoso.com domain (zone).

Question: What would happen to clients' ability to resolve names in the development.contoso.com domain if you had chosen a stand-alone DNS zone, rather than an Active Directory–integrated zone? Why would this happen? What would you have to do to solve this problem?

Answer: Clients who query the other DNS server would be unable to resolve names in the zone, because the server would not receive a replica of the zone. This could be solved by making the zone Active Directory–integrated, by hosting a secondary zone on the other DNS server, or by creating a stub zone that refers queries to the server hosting the development.contoso.com zone.

Lab B: Advanced Configuration of DNS

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the user name.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the user name.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a user name and password:

1. In **User Name**, type the user name.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Enable Scavenging of DNS Zones

► Task 1: Prepare for the lab

Some of the virtual machines should already be started and available after completing Lab A. However, if they are not, you should step through Exercises 1 and 2 in Lab A before continuing as there are dependencies between Lab A and Lab B.

1. Start 6425B-HQDC01-B.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Open **D:\Labfiles\Lab10b**.
4. Run **Lab10b_Setup.bat** with administrative credentials. Use the account **Administrator** with the password **Pa\$\$w0rd**.
5. The lab setup script runs. When it is complete, press any key to continue.
6. Close the Windows Explorer window, **Lab10b**.
7. Start 6425B-HQDC02-B.
8. Log on to HQDC02 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
9. Start 6425B-TSTDC01-A.
10. Log on to TSTDC01 as **Sara.Davis** with the password **Pa\$\$w0rd**.
11. Start 6425B-BRANCHDC01-B.
12. Wait for BRANCHDC01 to complete startup before continuing.

► Task 2: Enable scavenging of a DNS zone

1. Switch to HQDC02.
2. Run **DNS Management** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
3. In the console tree, expand **HQDC02** and **Forward Lookup Zones**, and then click **contoso.com**.
4. Right-click **contoso.com**, and then click **Properties**.
5. On the **General** tab, click the **Aging** button.

The Zone Aging/Scavenging Properties dialog box appears.

6. Select the **Scavenge stale resource records** check box.
7. Click **OK**.
8. Click **OK** to close the **contoso.com Properties** dialog box.

► **Task 3: Configure default scavenging settings**

1. In the console tree, right-click **HQDC02**, and then click **Set Aging/Scavenging for All Zones**.

The Server Aging/Scavenging Properties dialog box appears.

2. Select the **Scavenge stale resource records** check box.
3. Click **OK**.

The Server Aging/Scavenging Confirmation dialog box appears.

4. Select the **Apply these settings to the exiting Active Directory-integrated zones** check box.
5. Click **OK**.

Exercise 2: Create Reverse Lookup Zones

► Task 1: Create a reverse lookup zone

1. In the console tree, click **Reverse Lookup Zones**.
2. Right-click **Reverse Lookup Zones**, and then click **New Zone**.
The New Zone Wizard appears.
3. Click **Next**.
4. On the **Zone Type** page, click **Next**.
5. On the **Active Directory Zone Replication Scope** page, click **To all domain controllers in this domain(for Windows 2000 compatability: contoso.com)**. Click **Next**.
6. On the **Reverse Lookup Zone Name** page, click **IPv4 Reverse Lookup Zone**. Click **Next**.
7. On the **Reverse Lookup Zone Name** page, in **Network ID**, type **10**. Leave the other two octets empty. Click **Next**.
8. On the **Dynamic Update** page, click **Allow only secure dynamic updates**. Click **Next**.
9. On the **Completing the New Zone Wizard** page, click **Finish**.

► Task 2: Explore and verify the functionality of a reverse lookup zone

1. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Type **nslookup www.development.contoso.com**, and then press ENTER.
3. Note that the first section of the command output, which identifies the DNS server that was queried, indicates the IP address of the server but, next to **Server**, reports that the server is **Unknown**. That is because the nslookup.exe command cannot resolve the IP address to a name.
4. Switch to **DNS Manager**.
5. In the console tree, click the **10.in-addr.arpa** zone under **Reverse Lookup Zones**.

6. Examine the records in the zone.
7. Switch to the command prompt.
8. Type **ipconfig /registerdns**, and then press ENTER.
9. Switch to DNS Manager.
10. Right-click the **10.in-addr.arpa** zone, and then click **Refresh**.
11. Examine the resource records that have appeared.
12. Switch to the command prompt.
13. Type **nslookup www.development.contoso.com**, and then press ENTER.
14. Note that the first section of the command is now able to identify the server by both address *and* name.
15. Note that the DNS server that was queried at 10.0.0.12 is now resolved to its name.

Exercise 3: Explore Domain Controller Location

► Task 1: Explore _tcp

1. Switch to **DNS Manager**.
2. In the console tree, expand **HQDC02**, **Forward Lookup Zones**, and **contoso.com**, and then click the **_tcp** node.

Question: What do the resource records in the details pane represent?

Answer: The services offered by every domain controller in the contoso.com domain

► Task 2: Explore _tcp.brancha_sites.contoso.com

1. Switch to **DNS Manager**.
2. In the console tree, expand **HQDC02**, **Forward Lookup Zones**, **contoso.com**, **_sites**, **BRANCHA**, and then click the **_tcp** node.

Question: What do the resource records in the details pane represent?

Answer: The services offered by every domain controller that is located in, or is covering, the BRANCHA site.

Exercise 4: Configure Name Resolution for External Domains

► Task 1: Configure a stub zone

1. In the console tree, expand **HQDC02**, and then click **Forward Lookup Zones**.
2. Right-click **Forward Lookup Zones**, and then click **New Zone**.
The Welcome to the New Zone Wizard page appears.
3. Click **Next**.
The Zone Type page appears.
4. Click **Stub Zone**, and then click **Next**.
The Active Directory Zone Replication Scope page appears.
5. Click **Next**.
The Zone Name page appears.
6. Type **tailspintoys.com**, and then click **Next**.
The Master DNS Servers page appears.
7. Type **10.0.0.31** and press TAB.
8. Select the **Use the above servers to create a local list of master servers** check box.
9. Click **Next**, and then click **Finish**.

► Task 2: Configure a conditional forwarder

1. Switch to TSTDC01.
2. Run **DNS Management** with administrative credentials. Use the account **Sara.Davis_Admin** with the password **Pa\$\$w0rd**.
3. In the console tree, expand **TSTDC01**, and then click **Conditional Forwarders**.
4. Right-click the **Conditional Forwarders** folder, and then click **New Conditional Forwarder**.
5. In the **DNS Domain** box, type **contoso.com**.

6. Click **Click here to add an IP Address or DNS Name**, and type **10.0.0.11**.
7. Select the **Store this conditional forwarder in Active Directory, and replicate it as follows** check box.
8. Click **OK**.

► **Task 3: Validate name resolution for external domains**

1. Click **Start**, and then click **Command Prompt**.
2. Type **nslookup www.development.contoso.com**, and then press ENTER.
The command should return the address **10.0.0.24**.
3. Switch to DNS Manager.
4. In the console tree, expand **TSTDC01, Forward Lookup Zones**, and then click the **tailspintoys.com** zone.
5. Right-click **tailspintoys.com**, and then click **New Host (A or AAAA)**.
The New Host dialog box appears.
6. In **Name**, type **www**.
7. In **IP address**, type **10.0.0.143**.
8. Click **Add Host**.
A message appears informing you that the record was added successfully.
9. Click **OK**.
10. Click **Done**.
11. Switch to HQDC02.
12. Click **Start**, and then click **Command Prompt**.
13. Type **nslookup www.tailspintoys.com**, and then press ENTER.
The command should return the address **10.0.0.143**.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: In this lab, you used a stub zone and a conditional forwarder to provide name resolution between two distinct domains. What other options might you have chosen to use?

Answer: You could create a secondary zone in each domain that hosts a copy of the zone from the other. If the domains have delegations in the top-level .com domain, you could use root hints and standard DNS recursive queries to get them to resolve names in each other's domains.

Module 11

Lab Answer Key: Administer Active Directory® Domain Services (AD DS) Domain Controllers (DCs)

Contents:

Lab A: Install Domain Controllers

Exercise 1: Create an Additional DC with the Active Directory Domain Services Installation Wizard 4

Exercise 2: Add a Domain Controller from the Command Line 7

Exercise 3: Remove a Domain Controller 9

Exercise 4: Create a Domain Controller from Installation Media 10

Lab B: Install a Server Core DC

Exercise 1: Perform Post-Installation Configuration on Server Core 14

Exercise 2: Create a Domain Controller with Server Core 16

Lab C: Transfer Operations Master Roles

Exercise 1: Identify Operations Masters 18

Exercise 2: Transfer Operations Master Roles 22

Lab D: Configure DFS-R Replication of SYSVOL

Exercise 1: Observe the Replication of SYSVOL 25

Exercise 2: Prepare to Migrate to DFS-R 27

Exercise 3: Migrate SYSVOL Replication to DFS-R 29

Exercise 4: Verify DFS-R Replication of SYSVOL 34

Lab A: Install Domain Controllers

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the user name.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the user name.

3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a user name and password:

1. In **User Name**, type the user name.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Create an Additional DC with the Active Directory Domain Services Installation Wizard

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Start 6425B-HQDC02-A.
4. Log on to HQDC02 as **Administrator** with the password **Pa\$\$w0rd**.
The Windows desktop appears.

► Task 2: Promote a domain controller using the Active Directory Domain Services Installation Wizard

1. On HQDC02, click **Start**, then in the **Start Search** box, type **DCPromo.exe** and then press ENTER.

A message appears indicating that AD DS binaries are being installed. This takes several minutes.

The Active Directory Domain Services Installation Wizard appears.
2. On the **Welcome** page, click **Next**.
3. On the **Operating System Compatibility** page, review the warning about the default security settings for Windows Server 2008 domain controllers, and then click **Next**.
4. On the **Choose a Deployment Configuration** page, click **Existing forest**, then click **Add a domain controller to an existing domain**, and then click **Next**.
5. On the **Network Credentials** page, type **contoso.com** in the text box.
6. Click the **Set** button.
The Windows Security dialog box appears.
7. In the **User name** box, type **Pat.Coleman_Admin**.
8. In the **Password** box, type **Pa\$\$w0rd**, and then click **OK**.
9. Click **Next**.
10. On the **Select a Domain** page, select **contoso.com**, and then click **Next**.

11. On the **Select a Site** page, select **Default-First-Site-Name**, and then click **Next**.

The Additional Domain Controller Options page appears. DNS Server and Global Catalog are selected by default.

12. Click **Next**.

A Static IP assignment warning appears, informing you that the server has a dynamically assigned IP address.

HQDC02 has a fixed IPv4 address, and a dynamic IPv6 address. Because IPv6 is beyond the scope of this class, you can ignore this warning.

13. Click **Yes, the computer will use a dynamically assigned IP address (not recommended)**.

An Active Directory Domain Services Installation Wizard warning appears, informing you that a delegation could not be found.

The DNS configuration is correct in the sample contoso.com domain, so you can ignore this warning.

14. Click **Yes**.

15. On the **Location For Database, Log Files, And SYSVOL** page, accept the default locations for the database file, the directory service log files, and the SYSVOL files and click **Next**.

The best practice in a production environment is to store these files on three separate volumes that do not contain applications or other files not related to AD DS. This best practices design improves performance and increases the efficiency of backup and restore.

16. On the **Directory Services Restore Mode Administrator Password** page, type **Pa\$\$w0rd** in both the **Password** and **Confirm password** boxes. Click **Next**.

Do not forget the password you assigned to the Directory Services Restore Mode Administrator.

17. On the **Summary** page, review your selections.



Important: DO NOT CLICK NEXT.

If any settings are incorrect, click **Back** to make modifications.

18. Click **Export Settings**.
19. Click **Browse Folders**.

20. Click **Desktop**.
21. In the **File Name** box, type **AdditionalDC**, and then click **Save**.
A message appears, indicating that settings were saved successfully.
22. Click **OK**.
You will now cancel the domain controller installation and will, instead, promote the server to a domain controller in the next exercise.
23. On the **Active Directory Domain Services Installation Wizard Summary** page, click **Cancel**.
24. Click **Yes** to confirm that you are cancelling the installation of the DC.

Exercise 2: Add a Domain Controller from the Command Line

► Task 1: Create the DCPromo command

1. Open the **AdditionalDC.txt** file you created in Exercise 1.
2. Examine the answers in the file. Can you identify what some of the options mean?



Tip: Lines beginning with a semicolon are comments or inactive lines that have been commented out.

3. Click **Start**, and in the **Start Search** box, type **Notepad**. Then press ENTER. Notepad opens.
4. On the **Format** menu, click **Word Wrap**.
5. Position the blank Notepad window and the AdditionalDC.txt file so you can see both files.
6. In Notepad, type the dcpromo.exe command-line just as you would do in a command prompt. Determine the command-line to install the domain controller with the same options as those listed in the answer file. Options on the command-line take the form /option:value whereas, in the answer file, they take the form option=value. Configure both the **Password** and **SafeModeAdminPassword** values as **Pa\$\$w0rd**. Instruct DCPromo to reboot when complete.

Type on one line (with word wrap enabled):

```
dcpromo /unattend /ReplicaOrNewDomain:Replica  
/ReplicaDomainDNSName:contoso.com  
/SiteName:Default-First-Site-Name /InstallDNS:Yes /ConfirmGc:Yes  
/CreatedNSDelegation:No /UserDomain:contoso.com  
/UserName:contoso.com\Pat.Coleman_Admin /Password:Pa$$w0rd  
/DatabasePath:"C:\Windows\NTDS" /LogPath:"C:\Windows\NTDS"  
/SYSVOLPath:"C:\Windows\SYSVOL" /SafeModeAdminPassword:Pa$$w0rd  
/RebootOnCompletion:Yes
```

As you will learn in Lab B, you can set the Password value to an asterisk (*) and you will be prompted to enter the password when you run the command.

7. Open `\\HQDC01\d$\Labfiles\Lab11a\Exercise2.txt`.
8. Compare the correct command in the **Exercise2.txt** file to the command you created in the previous step. Make any necessary corrections to your command.

► **Task 2: Execute the DCPromo command**

1. Click **Start**, and then click Command Prompt.
The Command Prompt opens.
2. Switch to the Notepad window containing your `dcpromo.exe` command.
3. Click the **Format** menu, and then clear the **Word Wrap** option.
If word wrap is on, the command will not copy and paste correctly into the command prompt: Each line that is wrapped will be interpreted as a separate command.
4. Press CTRL+A. Then click the **Edit** menu, and then click **Copy**.
5. Switch to the Command Prompt window.
6. Right-click in the Command Prompt window, and then click **Paste**.
7. Press ENTER to execute the command.



Tip: If you encounter errors, it is probably because of a typo in your command. Compare what you have typed to the correct command, contained in `\\HQDC01\d$\Labfiles\Lab11a\Exercise2.txt`. Alternately, copy and paste the command from the `Exercise2.txt` file instead of using the command you created.

HQDC02 is promoted to a domain controller. This takes a few minutes.

The computer restarts when configuration is complete.

Exercise 3: Remove a Domain Controller

► Task 1: Remove a domain controller

1. Wait for HQDC02 to complete startup.
2. Log on to HQDC02 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
The Windows desktop appears.
3. Click the **Start** button, and then click **Run**.
4. Type **dcpromo.exe**, and then press ENTER.
The User Account Control dialog box appears.
5. In the **User name** box, type **Pat.Coleman_Admin**.
6. In the **Password** box, type **Pa\$\$w0rd**, and then press ENTER.
The Active Directory Domain Services Installation Wizard appears.
7. On the **Welcome** page, click **Next**.
A message appears, reminding you to make sure that this is not the last global catalog server in the forest.
8. Click **OK**.
9. On the **Delete the Domain** page, click **Next**.
10. On the **Administrator Password** page, type **Pa\$\$w0rd** in both the **Password** and **Confirm Password** boxes, and then click **Next**.
11. On the **Summary page**, click **Next**.
AD DS is removed from HQDC02.
12. Click **Finish**.
A message appears, prompting you to restart the server.
13. Click **Restart Now**.

Exercise 4: Create a Domain Controller from Installation Media

► Task 1: Create installation media

1. Switch to HQDC01.
2. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
3. Type **ntdsutil**, and then press ENTER.
4. Type **activate instance ntds**, and then press ENTER.
5. Type **ifm**, and then press ENTER.
6. Type **?**, and then press ENTER to list the commands available in IFM mode.
7. Type **create sysvol full c:\IFM**, and then press ENTER.

The installation media files are copied to c:\IFM.

When the process is complete, a message appears: *IFM media created successfully in c:\IFM*.

8. Type **quit**, and then press ENTER.
9. Type **quit**, and then press ENTER.

► Task 2: Promote a domain controller using installation media

1. Log on to HQDC02 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
The Windows desktop appears.
2. Click the **Start** button, and then click **Run**.
3. Type **\\HQDC01\c\$**, and then press ENTER.
The Connect to hqdc01.contoso.com dialog box appears.
4. In the **User name** box, type **CONTOSO\Pat.Coleman_Admin**.
5. In the **Password** box, type **Pa\$\$w0rd**, and then press ENTER.
A Windows Explorer window opens, showing the root of drive C on HQDC01.
6. Right-click the **IFM** folder and click **Copy**.
7. In the **Address** bar, type **C:**, and then press ENTER.

8. Right-click in an empty area of the details pane, and then click **Paste**.
The IFM folder is copied from HQDC01 to drive C.
9. Close the Windows Explorer window.
10. Click the **Start** button, and then click **Run**.
11. Type **dcpromo.exe**, and then press ENTER.
The User Account Control dialog box appears.
12. In the **User name** box, type **Pat.Coleman_Admin**.
13. In the **Password** box, type **Pa\$\$w0rd**, and then press ENTER.
The Active Directory Domain Services Installation Wizard appears.
14. On the **Welcome** page, select the **Use advanced mode installation** check box.
15. Click **Next**.
16. On the **Operating System Compatibility** page, review the warning about the default security settings for Windows Server® 2008 domain controllers, and then click **Next**.
17. On the **Choose a Deployment Configuration** page, click **Existing forest**, then click **Add a domain controller to an existing domain**, and then click **Next**.
18. On the **Network Credentials** page, type **contoso.com** in the text box.
19. Click **Next**.
20. On the **Select a Domain** page, select **contoso.com**, and then click **Next**.
21. On the **Select a Site** page, select **Default-First-Site-Name**, and then click **Next**.
The Additional Domain Controller Options page appears. DNS Server and Global Catalog are selected by default.
22. Click **Next**.
A Static IP assignment warning appears, informing you that the server has a dynamically assigned IP address.
HQDC01 has a fixed IPv4 address, and a dynamic IPv6 address. Because IPv6 is beyond the scope of this class, you can ignore this warning.

23. Click **Yes, the computer will use a dynamically assigned IP address (not recommended)**.

An Active Directory Domain Services Installation Wizard warning appears, informing you that a delegation could not be found.

The DNS configuration is correct in the sample contoso.com domain, so you can ignore this warning.

24. Click **Yes**.
25. On the **Install from Media** page, click **Replicate data from media at the following location**.
26. In the **Location** box, type **C:\IFM**, and then click **Next**.
27. On the **Source Domain Controller** page, click **Next**.

You will now cancel the domain controller installation.

28. Click **Cancel**.
29. Click **Yes** to confirm that you are cancelling the installation of the DC.
30. Shut down HQDC02. but do not shut down HQDC01 as it will be used in subsequent labs.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in Lab B.

Lab Review Questions

Question: Why would you choose to use an answer file, or a dcpromo.exe command-line to install a domain controller rather than the Active Directory Domain Services Installation Wizard?

Answer: Automation of installation. Consistency (always using the same options in a script versus hoping that an admin uses the correct options). Documentation (the script “documents” how the DC was installed). And, of course, in a Server Core installation.

Question: In what situations does it make sense to create a domain controller using installation media?

Answer: When the replication of Active Directory to the new domain controller will be problematic from a performance or network impact perspective.

Lab B: Install a Server Core DC

Exercise 1: Perform Post-Installation Configuration on Server Core

► Task 1: Prepare for the lab

The 6425B-HQDC01-A virtual machine should already be started and available after completing Lab A.

1. Start 6425B-HQDC01-A but do not log on.
2. Start 6425B-HQDC03-A but do not log on.

► Task 2: Perform post-installation configuration of Server Core

1. Log on to HQDC03 as **Administrator** with the password **Pa\$\$w0rd**.

The Command Prompt appears.

2. Type the following command, and then press ENTER:

```
netsh interface ipv4 set address name="Local Area Connection"  
source=static address=10.0.0.13 mask=255.255.255.0  
gateway=10.0.0.1
```

3. Type the following command, and then press ENTER:

```
netsh interface ipv4 set dns name="Local Area Connection"  
source=static address=10.0.0.11 primary
```

4. Type **ipconfig /all**, and then press ENTER.
5. Type the following command, and then press ENTER:

```
netdom renamecomputer %computername% /newname:HQDC03
```

You will be prompted to confirm the operation.

6. Press **Y** and then press ENTER.
7. Type **shutdown -r -t 0**, and then press ENTER.
The server restarts.
8. Wait for HQDC03 to restart.

9. Log on to HQDC03 as **Administrator** with the password **Pa\$\$w0rd**.
The Command Prompt appears.
10. Type the following command, and then press ENTER:

```
netdom join %computername% /domain:contoso.com  
/UserD:CONTOSO\Pat.Coleman_Admin /PasswordD:Pa$$w0rd  
/OU:"ou=servers,dc=contoso,dc=com"
```

11. Type **shutdown -r -t 0**, and then press ENTER.

Exercise 2: Create a Domain Controller with Server Core

► Task 1: Add the DNS Server role to Server Core

1. Wait for HQDC03 to restart.
2. Log on to HQDC03 as **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
3. Type **oclist**, and then press ENTER.

Question: What is the package identifier for the DNS server role?

Answer: DNS-Server-Core-Role.

Question: What is its status?

Answer: Not installed.

4. Type **ocsetup**, and then press ENTER.
The Windows Optional Component Setup dialog box appears.
Surprise! There is a minor amount of GUI in Server Core.
5. Click **OK**.
6. Type **ocsetup DNS-Server-Core-Role**, and then press ENTER.
Package identifiers are case sensitive.
7. Type **oclist**, and then press ENTER.
8. Confirm that DNS-Server-Core-Role shows a status of **Installed**.

► Task 2: Create a domain controller on Server Core with the **dcpromo.exe** command

1. Make sure you are still logged on to HQDC03 as **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**
2. Type **dcpromo.exe /?**, and then press ENTER.
3. Review the usage information.
4. Type **dcpromo.exe /?:Promotion**, and then press ENTER.

5. Review the usage information.
6. Type the following command to add and configure the AD DS role, and then press ENTER:

```
dcpromo /unattend /ReplicaOrNewDomain:replica  
/ReplicaDomainDNSName:contoso.com /ConfirmGC:Yes  
/UserName:CONTOSO\Pat.Coleman_Admin /Password:*  
/safeModeAdminPassword:Pa$$w0rd
```

7. When prompted to enter network credentials, type **Pa\$\$w0rd**, and then click **OK**.

The AD DS role is installed and configured, and the server reboots.



Note: You can shut down both virtual machines as different virtual machines are used in the next Lab.

Lab Review Questions

Question: Did you find the configuration of Server Core to be particularly difficult?

Answer: The correct answer will be based on your own experience and situation.

Question: What are the advantages of using Server Core for domain controllers?

Answer: Reduced system requirements, reduced attack surface (vulnerability) and therefore increased security.

Lab C: Transfer Operations Master Roles

Exercise 1: Identify Operations Masters

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-B.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Open **D:\Labfiles\Lab11c**.
4. Run **Lab11c_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
5. The lab setup script runs. When it is complete, press any key to continue.
6. Close the Windows Explorer window, **Lab11c**.
7. Start 6425B-HQDC02-B, but do not log on.
8. Wait for HQDC02 to complete startup before continuing.

► Task 2: Identify operations masters using the Active Directory administrative snap-ins

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, right-click the **contoso.com** domain, and then click **Operations Masters**.

The Operations Masters dialog box appears.

The tabs identify the domain controllers currently performing the single master operations roles for the domain: PDC emulator, RID master, and Infrastructure master.

3. Click the tab for each operations master.

Question: Which DC holds those roles?

Answer: HQDC01.contoso.com holds all three roles.

4. Click **Close**.
5. Close Active Directory Users and Computers.

6. Run **Active Directory Domains and Trusts** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
7. In the console tree, right-click the root node of the snap-in, **Active Directory Domains and Trusts**, and then click **Operations Master**.
The Operations Master dialog box appears.

Question: Which DC holds the domain naming operations master role?

Answer: HQDC01.contoso.com.

8. Click **Close**.
9. Close Active Directory Domains and Trusts.
The Active Directory Schema snap-in does not have a console of its own and cannot be added to a custom console until you have registered the snap-in.
10. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
11. Type **regsvr32 schmmgmt.dll**, and then press ENTER.
12. Click **OK** to close the message box that appears.
13. Click **Start** and, in the **Start Search** box, type **mmc.exe**, and then press ENTER.
The User Account Control dialog box appears.
14. Click **Use another account**.
15. In the **User name** box, type **Pat.Coleman_Admin**.
16. In the **Password** box, type **Pa\$\$w0rd**, and then press ENTER.
An empty MMC console appears.
17. Click the **File** menu, and then click **Add/Remove Snap-In**.
18. From the **Available snap-ins** list, select **Active Directory Schema**, click **Add**, and then click **OK**.
19. Click the root node of the snap-in, **Active Directory Schema**.
20. Right-click **Active Directory Schema**, and then click **Operations Master**.
The Change Schema Master dialog box appears.

Question: Which DC holds the schema master role?

Answer: HQDC01.contoso.com.

21. Click **Close**.
22. Close the console. You do not need to save any changes.

► **Task 3: Identify operations masters using NetDom**

1. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Type the command **netdom query fsmo**, and then press ENTER.
All operations master role holders are listed.

Exercise 2: Transfer Operations Master Roles

► Task 1: Transfer the PDC role using the Active Directory Users And Computers snap-in

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Right-click the **contoso.com** domain and click **Change Domain Controller**.
3. In the list of directory servers, select **HQDC02.contoso.com**, and then click **OK**.

Before transferring an operations master, you must connect to the domain controller to which the role will be transferred.

The root node of the snap-in indicates the domain controller to which you are connected: Active Directory Users and Computers [HQDC02.contoso.com].

4. Right-click the **contoso.com** domain and click **Operations Masters**.
5. Click the **PDC** tab.

The tab indicates that HQDC01.contoso.com currently holds the role token. HQDC02.contoso.com is listed in the second text box.

6. Click the **Change** button.

An Active Directory Domain Services dialog box prompts you to confirm the transfer of the operations master role.

7. Click **Yes**.

An Active Directory Domain Services dialog box confirms the role was successfully transferred.

8. Click **OK**, and then click **Close**.

At this point in a production environment, you would also transfer other FSMO roles held by HQDC01 to HQDC02 or other domain controllers. You would ensure that other roles performed by HQDC01 – DNS and global catalog, for example—were covered by other servers. Then you could take HQDC01 offline.

Remember that you cannot bring a domain controller back online if the RID, schema, or domain-naming roles have been seized. But you can bring it back online if a role was transferred.

► **Task 2: Consider other roles before taking a domain controller offline**

You are preparing to take HQDC01 offline. You have just transferred the PDC operations role to HQDC02.

Question: List other operations master roles that must be transferred prior to taking HQDC01 offline?

Answer: All other operations master roles held by HQDC01 should be transferred to HQDC02 or to other domain controllers prior to taking HQDC01 offline. Specifically, RID, Infrastructure, Domain Naming, and Schema master roles.

Question: List other server roles that must be transferred prior to taking HQDC01 offline?

Answer: You should consider other roles performed by HQDC01, such as DNS Server and global catalog. Ensure that these roles are covered by other servers or domain controllers prior to taking HQDC01 offline.

► **Task 3: Transfer the PDC role using NTDSUtil**

You have finished performing maintenance on **HQDC01**. You bring it back online.

1. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Type **ntdsutil**, and then press ENTER.
3. Type **roles**, and then press ENTER.
4. Type **connections**, and then press ENTER.
5. Type **connect to server HQDC01**, and then press ENTER.
6. Type **quit**, and then press ENTER.
7. Type **transfer PDC**, and then press ENTER.
The Role Transfer Confirmation dialog box appears.
8. Click **Yes**.



Note: You can shut down these virtual machines when finished with them as they will need to be restarted for the next lab.

Lab Review Questions

Question: If you transfer all roles before taking a domain controller offline, is it OK to bring the domain controller back online?

Answer: Yes

Question: If a domain controller fails and you seize roles to another domain controller, is it OK to bring the failed domain controller back online?

Answer: Only if the failed domain controller was the PDC emulator or infrastructure master. Schema, domain naming, and RID master role holders cannot be brought back online if the role was seized while the domain controller was offline. Instead, the failed domain controller must be demoted or, preferably, reinstalled entirely while offline. After the server is back online, it can be re-promoted to a domain controller and, at that time, the operations master role can be transferred gracefully to it.

Lab D: Configure DFS-R Replication of SYSVOL

Exercise 1: Observe the Replication of SYSVOL

► Task 1: Prepare for the lab

1. Shut down all VMs.
2. Start 6425B-HQDC01-B.
3. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
4. Open **D:\Labfiles\Lab11d**.
5. Run **Lab11d_Setup.bat** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
6. The lab setup script runs. When it is complete, press any key to continue.
7. Close the Windows Explorer window, **Lab11d**.
8. Start 6425B-HQDC02-B.
9. Log on to HQDC02 as **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.

► Task 2: Observe SYSVOL replication

1. Switch to HQDC01.
2. Click **Start**, and in the **Start Search** box, type **%SystemRoot%\Sysvol\Sysvol\contoso.com\Scripts**. Then press ENTER.
3. Run **Notepad** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
4. Click **File**, and then click **Save**.
5. In the **File name** box, type **%SystemRoot%\Sysvol\Sysvol\contoso.com\Scripts\TestFRS.txt**, and then press ENTER.
6. Close Notepad.
7. Confirm that you see the file, **TestFRS.txt**, in the Scripts folder.
8. Switch to HQDC02.

9. Click **Start**, and in the **Start Search** box type **%SystemRoot%\Sysvol\Sysvol\contoso.com\Scripts**. Then press ENTER.
10. Confirm that you see the file, **TestFRS.txt**, to the HQDC02 Scripts folder.
If the file does not appear immediately, wait a few moments. It can take up to 15 minutes for replication to occur. You can, optionally, continue with Exercise 2. Before continuing even further with Exercise 3, check back to ensure that the file has replicated.
11. After you have observed the replication, close the Windows Explorer window showing the Scripts folder on both HQDC01 and HQDC02.

Exercise 2: Prepare to Migrate to DFS-R

► Task 1: Confirm that the current domain functional level is lower than Windows Server 2008

1. Still on HQDC02 Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd** if prompted otherwise click **continue** on the **User Account Control** dialogue box.
2. In the console tree, right-click the **contoso.com** domain, and then click **Raise Domain Functional Level**.
The Raise Domain Functional Level dialog box appears.
3. Confirm that the **Current domain functional level** is **Windows Server 2003**.
4. Click **Cancel**. Do not make any change to the domain functional level.

► Task 2: Confirm that DFS-R replication is not available at domain functional levels lower than Windows Server 2008

1. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd** if prompted otherwise click **continue** on the **User Account Control** dialogue box.
2. Type **dfsrmig /getglobalstate**, and then press ENTER.
A message appears informing you that dfsrmig is supported only on domains at the Windows Server 2008 functional level.

► Task 3: Raise the domain functional level

1. Switch to **Active Directory Users and Computers**.
2. In the console tree, right-click the **contoso.com** domain, and then click **Raise Domain Functional Level**.
3. Confirm that the **Select an available domain functional level** list indicates **Windows Server 2008**.
4. Click **Raise**.

A message appears to remind you that the action cannot be reversed.

5. Click **OK** to confirm your change.

A message appears informing you that the functional level was raised successfully.

6. Click **OK**.
7. Close Active Directory Users and Computers.

► **Task 4: Confirm that DFS-R replication is available at Windows Server 2008 domain functional level**

1. Switch to the Command Prompt.
2. Type **dfsrmig /getglobalstate**, and then press ENTER.

A message appears informing you that DFS-R migration has not yet been initialized.

Exercise 3: Migrate SYSVOL Replication to DFS-R

► Task 1: Migrate SYSVOL replication to DFS-R

1. Switch to the Command Prompt
2. Type **dfsrmig /setglobalstate 0**, and then press ENTER.

The following message appears:

```
Current DFSR global state: 'Start'  
New DFSR global state: 'Start'  
Invalid state change requested.
```

The default global state is already 0, 'Start,' so your command is not valid. However, this does serve to initialize DFSR migration.

3. Type **dfsrmig /getglobalstate**, and then press ENTER.

The following message appears:

```
Current DFSR global state: 'Start'  
Succeeded.
```

4. Type **dfsrmig /getmigrationstate**, and then press ENTER.

The following message appears:

```
All Domain Controllers have migrated successfully to Global state  
( 'Start' ).  
Migration has reached a consistent state on all Domain  
Controllers.  
Succeeded.
```

5. Type **dfsrmig /setglobalstate 1**, and then press ENTER.

The following message appears:

```
Current DFSR global state: 'Start'
New DFSR global state: 'Prepared'

Migration will proceed to 'Prepared' state. DFSR service will
copy the contents of SYSVOL to SYSVOL_DFSR
folder.

If any DC is unable to start migration then try manual polling.
OR Run with option /CreateGlobalObjects.
Migration can start anytime between 15 min to 1 hour.
Succeeded.
```

6. Type **dfsrmig /getmigrationstate**, and then press ENTER.
A message appears that reflects the migration state of each domain controller. Migration can take up to 15 minutes.
7. Repeat this step until you receive the following message that indicates migration has progressed to the 'Prepared' state and is successful:

```
All Domain Controllers have migrated successfully to Global state
('Prepared').
Migration has reached a consistent state on all Domain
Controllers.
Succeeded.
```

When you receive the message just shown, continue to the next step.

During migration to the 'Prepared' state, you might see one of these messages:

```
The following Domain Controllers are not in sync with Global state
('Prepared'):
```

```
Domain Controller (Local Migration State) - DC Type
=====
```

```
HQDC01 ('Start') - Primary DC
HQDC02 ('Start') - Writable DC
```

```
Migration has not yet reached a consistent state on all Domain
Controllers.
State information might be stale due to AD latency.
```

or

The following Domain Controllers are not in sync with Global state ('Prepared'):

Domain Controller (Local Migration State) - DC Type
=====

HQDC01 ('Start') - Primary DC
HQDC02 ('Waiting For Initial Sync') - Writable DC

Migration has not yet reached a consistent state on all Domain Controllers.
State information might be stale due to AD latency.

or

The following Domain Controllers are not in sync with Global state ('Prepared'):

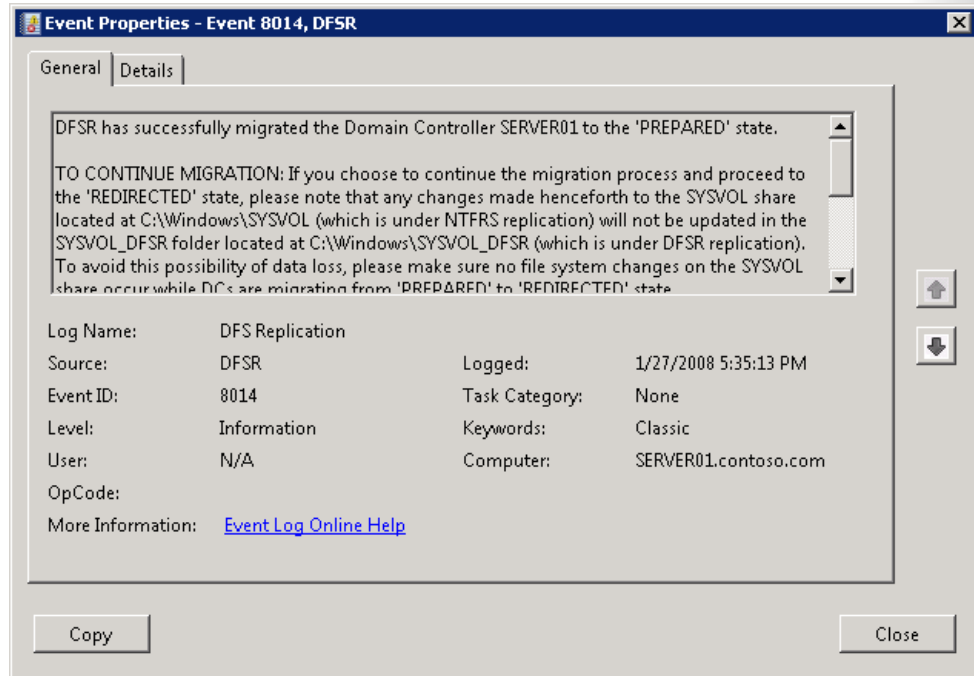
Domain Controller (Local Migration State) - DC Type
=====

HQDC02 ('Waiting For Initial Sync') - Writable DC

Migration has not yet reached a consistent state on all Domain Controllers.
State information might be stale due to AD latency.

8. Run **Event Viewer** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd** if prompted otherwise click **continue** on the **User Account Control** dialog box.
9. In the console tree, expand **Applications and Services Logs**, and then click **DFS Replication**.

10. Locate the event with **Event ID 8014** and open its properties.
You should see the details shown in the following screen shot.



11. Close **Event Viewer**.
12. Switch to the Command Prompt.

13. Type **dfsrmig /setglobalstate 2**, and then press ENTER.

The following message appears:

```
Current DFSR global state: 'Prepared'
New DFSR global state: 'Redirected'

Migration will proceed to 'Redirected' state. The SYSVOL share
will be
changed to SYSVOL_DFSR folder.

If any changes have been made to the SYSVOL share during the state
transition from 'Prepared' to 'Redirected', please robocopy the
changes
from SYSVOL to SYSVOL_DFSR on any replicated RWDC.
Succeeded.
```

14. Type **dfsrmig /getmigrationstate**, and then press ENTER.

A message appears that reflects the migration state of each domain controller. Migration can take up to 15 minutes.

15. Repeat step 14 until you receive the following message that indicates migration has progressed to the 'Prepared' state and is successful:

```
All Domain Controllers have migrated successfully to Global state
('Redirected').
Migration has reached a consistent state on all Domain
Controllers.
Succeeded.
```

When you receive the message just shown, continue to the next task.

During migration, you might receive messages like the following:

```
The following Domain Controllers are not in sync with Global state
('Redirected'):

Domain Controller (Local Migration State) - DC Type
=====

HQDC02 ('Prepared') - Writable DC

Migration has not yet reached a consistent state on all Domain
Controllers.
State information might be stale due to AD latency.
```

Exercise 4: Verify DFS-R Replication of SYSVOL

► Task 1: Confirm the new location of SYSVOL

1. Still on HQDC02, switch to the Command Prompt.
2. Type **net share**, and then press ENTER.
3. Confirm that the NETLOGON share refers to the %SystemRoot%\SYSVOL_DFSR\Sysvol\contoso.com\Scripts folder.
4. Confirm that the SYSVOL share refers to the %SystemRoot%\SYSVOL_DFSR\Sysvol folder.

► Task 2: Observe SYSVOL replication

1. Switch to HQDC01.
2. Click **Start**, and in the **Start Search** box, type %SystemRoot%\SYSVOL_DFSR\Sysvol\contoso.com\Scripts. Then press ENTER.

Note that the TestFRS.txt file created earlier is already in the Scripts folder. While the domain controllers were at the Prepared state, files were replicated between the legacy FRS SYSVOL folder and the new DFS-R SYSVOL folder.

3. Run **Notepad** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd** if prompted otherwise click **continue** on the **User Account Control** dialogue box.
4. Click **File**, and then click **Save**.
5. In the **File name** box, type %SystemRoot%\SYSVOL_DFSR\Sysvol\contoso.com\Scripts\TestDFSR, and then press ENTER.
6. Close Notepad.
7. Confirm that you see the file, TestDFSR.txt, in the Scripts folder.
8. Switch to HQDC02.

9. Click **Start**, and in the **Start Search** box, type `%SystemRoot%\SYSVOL_DFSR\Sysvol\contoso.com\Scripts`. Then press ENTER.
10. Confirm that you see the file, TestDFSR.txt, in the Scripts folder.
If the file does not appear immediately, wait a few moments.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: What would you expect to be different between two enterprises, one which created its domain initially with Windows 2008 domain controllers, and one that migrated to Windows Server 2008 from Windows Server 2003?

Answer: In a domain that was created with Windows 2008 in the first place, the SYSVOL share will refer to a folder named SYSVOL that is replicated with DFS-R. In a domain that was created with domain controllers prior to Windows 2008, SYSVOL will be replicated with FRS, until it has been migrated. After that point, the SYSVOL share will refer to a folder named SYSVOL_DFSR.

Question: What must you be aware of while migrating from the Prepared to the Redirected state?

Answer: While migrating from the Prepared to the Redirected state, any changes made to SYSVOL must be manually duplicated in SYSVOL_DFSR.

13. Type **dfsrmig /setglobalstate 2**, and then press ENTER.

The following message appears:

```
Current DFSR global state: 'Prepared'
New DFSR global state: 'Redirected'

Migration will proceed to 'Redirected' state. The SYSVOL share
will be
changed to SYSVOL_DFSR folder.

If any changes have been made to the SYSVOL share during the state
transition from 'Prepared' to 'Redirected', please robocopy the
changes
from SYSVOL to SYSVOL_DFSR on any replicated RWDC.
Succeeded.
```

14. Type **dfsrmig /getmigrationstate**, and then press ENTER.

A message appears that reflects the migration state of each domain controller. Migration can take up to 15 minutes.

15. Repeat step 14 until you receive the following message that indicates migration has progressed to the 'Prepared' state and is successful:

```
All Domain Controllers have migrated successfully to Global state
('Redirected').
Migration has reached a consistent state on all Domain
Controllers.
Succeeded.
```

When you receive the message just shown, continue to the next task.

During migration, you might receive messages like the following:

```
The following Domain Controllers are not in sync with Global state
('Redirected'):

Domain Controller (Local Migration State) - DC Type
=====

HQDC02 ('Prepared') - Writable DC

Migration has not yet reached a consistent state on all Domain
Controllers.
State information might be stale due to AD latency.
```


Exercise 4: Verify DFS-R Replication of SYSVOL

► Task 1: Confirm the new location of SYSVOL

1. Still on HQDC02, switch to the Command Prompt.
2. Type **net share**, and then press ENTER.
3. Confirm that the NETLOGON share refers to the %SystemRoot%\SYSVOL_DFSR\Sysvol\contoso.com\Scripts folder.
4. Confirm that the SYSVOL share refers to the %SystemRoot%\SYSVOL_DFSR\Sysvol folder.

► Task 2: Observe SYSVOL replication

1. Switch to HQDC01.
2. Click **Start**, and in the **Start Search** box, type %SystemRoot%\SYSVOL_DFSR\Sysvol\contoso.com\Scripts. Then press ENTER.

Note that the TestFRS.txt file created earlier is already in the Scripts folder. While the domain controllers were at the Prepared state, files were replicated between the legacy FRS SYSVOL folder and the new DFS-R SYSVOL folder.

3. Run **Notepad** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd** if prompted otherwise click **continue** on the **User Account Control** dialogue box.
4. Click **File**, and then click **Save**.
5. In the **File name** box, type %SystemRoot%\SYSVOL_DFSR\Sysvol\contoso.com\Scripts\TestDFSR, and then press ENTER.
6. Close Notepad.
7. Confirm that you see the file, TestDFSR.txt, in the Scripts folder.
8. Switch to HQDC02.

9. Click **Start**, and in the **Start Search** box, type `%SystemRoot%\SYSVOL_DFSR\Sysvol\contoso.com\Scripts`. Then press ENTER.
10. Confirm that you see the file, TestDFSR.txt, in the Scripts folder.
If the file does not appear immediately, wait a few moments.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: What would you expect to be different between two enterprises, one which created its domain initially with Windows 2008 domain controllers, and one that migrated to Windows Server 2008 from Windows Server 2003?

Answer: In a domain that was created with Windows 2008 in the first place, the SYSVOL share will refer to a folder named SYSVOL that is replicated with DFS-R. In a domain that was created with domain controllers prior to Windows 2008, SYSVOL will be replicated with FRS, until it has been migrated. After that point, the SYSVOL share will refer to a folder named SYSVOL_DFSR.

Question: What must you be aware of while migrating from the Prepared to the Redirected state?

Answer: While migrating from the Prepared to the Redirected state, any changes made to SYSVOL must be manually duplicated in SYSVOL_DFSR.

Module 12

Lab Answer Key: Manage Sites and Active Directory Replication

Contents:

Lab A: Configure Sites and Subnets	
Exercise 1: Configure the Default Site	4
Exercise 2: Create Additional Sites	6
Exercise 3: Move Domain Controllers into Sites	8
Lab B: Configure the Global Catalog and Application Partitions	
Exercise 1: Configure a Global Catalog	12
Exercise 2: Configure Universal Group Membership Caching	13
Exercise 3: Examine DNS and Application Directory Partitions	14
Lab C: Configure Replication	
Exercise 1: Create a Connection Object	18
Exercise 2: Create Site Links	20
Exercise 3: Move Domain Controllers into Sites	21
Exercise 4: Designate a Preferred Bridgehead Server	22
Exercise 5: Configure Intersite Replication	23

Lab A: Configure Sites and Subnets

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the user name.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the user name.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a user name and password:

1. In **User Name**, type the user name.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Configure the Default Site

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-B. This virtual machine may take several minutes to start.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Start 6425B-HQDC02-B but do not log on.
4. After HQDC02 has completed startup, start 6425B-HQDC03-B but do not log on.
5. After HQDC03 has completed startup, start 6425B-BRANCHDC01-B, but do not log on.
6. Wait for BRANCHDC01 to finish startup before continuing to the next task.

► Task 2: Rename Default-First-Site-Name

1. On HQDC01, run **Active Directory Sites and Services** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand **Sites**, and then click **Default-First-Site-Name**.
3. Right-click **Default-First-Site-Name** and click **Rename**.
4. Type **HEADQUARTERS**, and then press ENTER.

Because site names are registered in DNS, you should use DNS-compliant names that avoid special characters and spaces.

► Task 3: Create a subnet and associate it with a site

1. In the console tree, click **Subnets**.
2. Right-click **Subnets** and click **New Subnet**.
3. In the **Prefix** box, type **10.0.0.0/24**.
4. In the **Select a site object for this prefix** list, select **HEADQUARTERS**.
5. Click **OK**.
6. Right-click **10.0.0.0/24**, and then click **Properties**.

7. In the **Description** box, type **Server and back-end subnet**, and then click **OK**.
8. In the console tree, right-click **Subnets**, and then click **New Subnet**.
9. In the **Prefix** box, type **10.0.1.0/24**.
10. In the **Select a site object for this prefix** list, select **HEADQUARTERS**.
11. Click **OK**.
12. Right-click **10.0.1.0/24**, and then click **Properties**.
13. In the **Description** box, type **Client subnet**, and then click **OK**.

Exercise 2: Create Additional Sites

► Task 1: Create additional sites

1. In the console tree, right-click **Sites**, and then click **New Site**.
2. In the **Name** box, type **HQ-BUILDING-2**.
3. Select **DEFAULTIPSITELINK**.
4. Click **OK**.

An Active Directory Domain Services dialog box appears, explaining the steps required to complete the configuration of the site.

5. Click **OK**.
6. In the console tree, right-click **Sites**, and then click **New Site**.
7. In the **Name** box, type **BRANCHA**.
8. Select **DEFAULTIPSITELINK**.
9. Click **OK**.

► Task 2: Create subnets and associate them with sites

1. In the console tree, right-click **Subnets** and click **New Subnet**.
2. In the **Prefix** box, type **10.1.0.0/24**.
3. In the **Select a site object for this prefix** list, select **HQ-BUILDING-2**.
4. Click **OK**.
5. Right-click **10.1.0.0/24** and then click **Properties**.
6. In the **Description** box, type **Headquarters Building 2**.
7. In the **Site** drop-down list, select **HQ-BUILDING-2**.
8. Click **OK**.
9. In the console tree, right-click **Subnets** and click **New Subnet**.
10. In the **Prefix** box, type **10.2.0.0/24**.
11. In the **Select a site object for this prefix** list, select **BRANCHA**.

12. Click **OK**.
13. Right-click **10.2.0.0/24** and then click **Properties**.
14. In the **Description** box, type **Branch Office A**.
15. In the **Site** drop-down list, select **BRANCHA**.
16. Click **OK**.

Exercise 3: Move Domain Controllers into Sites

► Task 1: Move domain controllers to new sites

1. In the console tree, expand **HEADQUARTERS**, and then click the **Servers** node.
2. In the details pane, right-click **HQDC03** and click **Move**.
The Move Server dialog box appears.
3. Click **HQ-BUILDING-2**, and then click **OK**.
4. In the details pane, right-click **BRANCHDC01** and click **Move**.
The Move Server dialog box appears.
5. Click **BRANCHA**, and then click **OK**.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs.

Lab Review Questions

Question: You have a site with 50 subnets, each with a subnet address of 10.0.x.0/24, and you have no other 10.0.x.0 subnets, what could you do to make it easier to identify the 50 subnets and associate them with a site?

Answer: Define a single subnet, 10.0.0.0/16.

Question: Why is it important that all subnets are identified and associated with a site in a multisite enterprise?

Answer: Domain controller (and other service) location is made efficient by referring clients to the correct site, based on the client's IP address and the definition of subnets. If a client has an IP address that does not belong to a site, the client will query for all DCs in the domain, and that is not at all efficient. In fact, a single client can be performing actions against domain controllers in different sites, which (if those changes have not replicated yet) can lead to very strange results. It's very important that each client knows what site it's in, and that's achieved by ensuring that DCs can identify what site a client is in.

Lab B: Configure the Global Catalog and Application Partitions

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the user name.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the user name.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a user name and password:

1. In **User Name**, type the user name.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Configure a Global Catalog

► Task 1: Prepare for the lab

The virtual Machines should already be started and available after completing Lab A. However, if they are not, you should complete the below steps then step through Exercises 1 to 3 in Lab A before continuing.

1. Start 6425B-HQDC01-B. This virtual machine may take several minutes to start.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Start 6425B-HQDC02-B but do not log on.
4. After HQDC02 has completed startup, start 6425B-HQDC03-B but do not log on.
5. After HQDC03 has completed startup, start 6425B-BRANCHDC01-B, but do not log on.
6. Wait for BRANCHDC01 to finish startup before continuing to the next task.

► Task 2: Configure a global catalog server

1. On HQDC01, run **Active Directory Sites and Services** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand **HEADQUARTERS**, **Servers**, and HQDC02, and then click the **NTDS Settings** node below HQDC02.
3. Right-click the **NTDS Settings** node below HQDC02, and then click **Properties**.
4. Select the **Global catalog** check box, and then click **OK**.
5. Repeat steps 2 and 3 to confirm that BRANCHDC01 in the **BRANCHA** site is a global catalog server.

Exercise 2: Configure Universal Group Membership Caching

► Task 1: Configure universal group membership caching

1. In the console tree, click **BRANCHA**.
2. In the details pane, right-click **NTDS Site Settings** and click **Properties**.
3. Click the **Site Settings** tab.
4. Select the **Enable universal group membership caching** check box.
5. Click **OK**.

Exercise 3: Examine DNS and Application Directory Partitions

► Task 1: Examine DNS records related to replication

1. Run **DNS Manager** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand **HQDC01**, **Forward Lookup Zones**, **contoso.com**, **_sites**, and **HEADQUARTERS**, and then click **_tcp** under **HEADQUARTERS**.
3. Examine the service locator records.
4. In the console tree, expand **BRANCHA**, and then click **_tcp** under **BRANCHA**.
5. Examine the service locator records.

► Task 2: Examine the DNS application directory partition

1. Click **Start >Administrative Tools >ADSI Edit** and enter administrative credentials when prompted. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, right-click **ADSI Edit**, and then click **Connect To**.
3. In the **Select a well known naming context** drop-down list, select **Configuration**.
4. Accept all other defaults. Click **OK**.
5. In the console tree, click **Configuration**, and then expand it.
6. In the console tree, click **CN=Configuration, DC=contoso, DC=com**, and then expand it.
7. In the console tree, click **CN=Partitions**.
8. Right-click **ADSI Edit**, and then click **Connect To**.
9. Click **Select or type a distinguished name or naming context**.
10. In the combo box, type **DC=DomainDnsZones,DC=contoso,DC=com**. Click **OK**.
11. In the console tree, click **Default Naming Context**, and then expand it.
12. Click on **DC=DomainDnsZones,DC=contoso,DC=com**, and then expand it.
13. Click on **CN=MicrosoftDNS**, and then expand it.

14. Click **DC=contoso.com**.
15. Examine the objects in this container. Compare the records to the DNS records you examined in the previous exercise.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs.

Lab Review Questions

Question: Describe the relationship between the records you viewed in ADSI Edit and the records you viewed in DNS Manager.

Answer: Every record seen in DNS Manager's forward lookup zones has a corresponding record in the application directory partitions for DNS. However, the records as viewed in the application directory partition are flat. DNS Manager presents the records in a hierarchy.

Question: When you examined the DNS records in `_tcp.BRANCHA._sites.contoso.com`, what domain controller was registering service locator records in the site? Explain why it did so.

Answer: Answers will vary as to which DC covered BRANCHA. The site had no domain controllers, so a domain controller covers clients in the site by advertising itself using SRV records in the site.

Lab C: Configure Replication

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the user name.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the user name.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a user name and password:

1. In **User Name**, type the user name.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Create a Connection Object

► Task 1: Prepare for the lab

The virtual Machines should already be started and available after completing Labs A and B. However, if they are not, you should complete the below steps then step through Exercises 1 to 3 in Labs A and B before continuing.

1. Start 6425B-HQDC01-B.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. After logging on to HQDC01, start 6425B-HQDC02-B but do not log on.
4. After HQDC02 has completed startup, start 6425B-HQDC03-B but do not log on.
5. After HQDC03 has completed startup, start 6425B-BRANCHDC01-B but do not log on.
6. Wait for BRANCHDC01 to finish startup before continuing to the next task.

► Task 2: Create a connection object

1. Run **Active Directory Sites and Services** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand **HEADQUARTERS, Servers** and **HQDC02**, and then click the **NTDS Settings** node below HQDC02.
3. Right-click **NTDS Settings** and click **New Active Directory Domain Services Connection**.
4. In the **Find Active Directory Domain Controllers** dialog box, select HQDC01, and then click **OK**.

A warning appears asking if you want to create another connection.

Because the Knowledge Consistency Checker (KCC) has already created a connection from HQDC01 to HQDC02, you are asked if you want to create a duplicate connection. The direct connection that you create will be persistent, whereas connections that are automatically generated by the KCC may be changed. You want to ensure the connection is always maintained.

5. Click **Yes**.

6. In the **New Object – Connection** dialog box, type the name **HQDC01 - OPERATIONS MASTER**, and click **OK**.
7. Right-click the **HQDC01 - OPERATIONS MASTER** connection object under the NTDS settings object in the details pane, and then click **Properties**.

Question: Examine the properties of the connection object. Do not make any changes. What partitions are replicated from HQDC01? Is HQDC02 a GC server? How can you tell?

Answer: HQDC02 replicates the domain (contoso.com), Schema, and Configuration from HQDC01. It is also a global catalog server. The Partially Replicated Naming Context(s) property shows *All other domains*. This is another way of describing the forest's partial attribute set.

8. Click **OK** to close the **Properties** dialog box.

Exercise 2: Create Site Links

► Task 1: Create site links

1. In the **Active Directory Sites and Services** console tree, expand **Inter-Site Transports**, and then click **IP**.
2. In the details pane, right-click **DEFAULTIPSITELINK**, and then click **Rename**.
3. Type **HQ-HQB2**, and then press **ENTER**.
4. Double-click **HQ-HQB2**.
5. On the **General** tab, In the **Sites in this site link** list, click **BRANCHA**, and then click **Remove**. Click **OK**.
6. In the console tree, right-click **IP**, and then click **New Site Link**.
7. In the **Name** box, type **HQ-BRANCHA**.
8. In the **Sites not in this site link** list, click **HEADQUARTERS**, and then click **Add**.
9. In the **Sites not in this site link** list, click **BRANCHA**, and then click **Add**.
10. Click **OK**.

Exercise 3: Move Domain Controllers into Sites

► Task 1: Move domain controllers to new sites

1. In the console tree, expand **HEADQUARTERS**, and then click the **Servers** node.
2. In the details pane, right-click **BRANCHDC01** and click **Move**.
The Move Server dialog box appears.
3. Click **BRANCHA**, and then click **OK**.

Exercise 4: Designate a Preferred Bridgehead Server

► Task 1: Designate a preferred bridgehead server

1. In the console tree, expand **HEADQUARTERS**, **Servers**, and then click the **HQDC02** node.
2. Right-click **HQDC02** and click **Properties**.
3. In the **Transports available for inter-site data transfer** list, click **IP**.
4. Click **Add**, and then click **OK**.
A lengthy warning message appears.
5. Read the message. You will discuss it at the end of the lab.
6. Click **OK**.

Exercise 5: Configure Intersite Replication

► Task 1: Configure Intersite Replication

1. In the console tree, expand **Inter-Site Transports**, and then click the **IP** node.
2. In the details pane, double-click the **HQ-HQB2** site link.
3. In the **Replicate every** spin-box, type **15**, and then click **OK**.
4. In the details pane, double-click the **HQ-BRANCHA** site link.
5. In the **Replicate every** spin-box, type **15**.
6. Click the **Change Schedule** button.
7. Examine the **Schedule For HQ-BRANCHA** dialog box. Experiment with configuring the schedule but click **Cancel** when you are finished.
8. In the **Cost** spin-box, type **200**.
9. Click **OK**.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: Explain the warning message that appeared when you designated HQDC02 as a preferred bridgehead server.

Answer: A bridgehead server acts as the bridgehead only for Active Directory partitions that it contains. Because HQDC02 is not a DNS server, it does not host the ForestDnsZones or DomainDnsZones application partitions. The ISTG will continue to automatically designate another DC in the site as the bridgehead server for those two partitions. The warning message explained that the best practice is to designate bridgeheads for each partition. Ideally, the bridgehead server should host all partitions—in this case, including the DNS application partitions.

Question: What are the advantages of reducing the intersite replication interval? What are the disadvantages?

Answer: Convergence is improved. Changes made in one site are replicated more quickly to other sites. There are actually few, if any, disadvantages. If you consider that the same changes must replicate whether they wait 15 minutes or 3 hours to replicate, it's really a matter of timing of replication rather than quantity of replication. However, in some extreme situations, it's possible that allowing a smaller number of changes to happen more frequently might be less preferable than allowing a large number of changes to replicate less frequently.

Question: Is the procedure you performed in Exercise 2 enough to create a "hub and spoke" replication topology, which ensures that all changes from branches are replicated to the headquarters before being replicated to other branches? If not, what must still be done?

Answer: You must disable "Bridge all site links."

Module 13

Lab Answer Key: Directory Service Continuity

Contents:

Lab A: Monitor Active Directory Events and Performance

Exercise 1: Monitor Real-Time Performance Using Task Manager and Resource Monitor 4

Exercise 2: Use Reliability Monitor and Event Viewer to Identify Performance-Related Events 9

Exercise 3: Monitor Events on Remote Computers with Event Subscriptions 13

Exercise 4: Attach Tasks to Event Logs and Events 16

Exercise 5: Monitor AD DS with Performance Monitor` 18

Exercise 6: Work with Data Collector Sets 21

Lab B: Manage the Active Directory Database

Exercise 1: Perform Database Maintenance 29

Exercise 2: Work with Snapshots and Recover a Deleted User 32

Lab C: Back Up and Restore Active Directory

Exercise 1: Back Up Active Directory 39

Exercise 2: Restore Active Directory and a Deleted OU 42

Lab A: Monitor Active Directory Events and Performance

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the user name.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the user name.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a user name and password:

1. In **User Name**, type the user name.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Monitor Real-Time Performance Using Task Manager and Resource Monitor

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-B.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Open **D:\Labfiles\Lab13a**.
4. Run **Lab13a_Setup.bat** with administrative credentials. Use the account **Administrator** with the password **Pa\$\$w0rd**.
5. The lab setup script runs. When it is complete, press any key to continue.
6. Close the Windows Explorer window, **Lab13a**.
7. Start 6425B-HQDC02-B.
8. Log on to HQDC02 as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 2: Monitor real-time performance with Task Manager

1. Switch to HQDC01.
2. Press CTRL+SHIFT+ESC to launch Task Manager.
3. Click the **Processes** tab.
4. Right-click **taskmgr.exe** and examine the available commands. Then click **Properties**.

The Properties dialog box for the executable opens.

5. Close the **Properties** dialog box.
6. Click **Show processes from all users**.
7. Click **Use Another Account**.
8. In **User name**, type **Pat.Coleman_Admin**.

9. In **Password**, type **Pa\$\$w0rd**, and then press ENTER.

Task Manager re-opens with all processes displayed and with all administrative features enabled.

10. If you do not see Task Manager, it may be minimized or behind other windows. Click its icon in the task bar to make it visible.
11. Click the **Processes** tab.
12. Examine the full list of processes running on the system.
13. Click the **Services** tab.
14. Right-click **Dnscache**, and then click **Stop Service**.
15. Right-click **Dnscache**, and then click **Start Service**.
16. Right-click **Dnscache**, and then click **Go to Process**.

Question: What process is hosting the DNS Client service?

Answer: svchost.exe

17. Right-click the process, and then click **Go to Service(s)**.

Question: The Services tab exposes a subset of the most-used functionality of which administrative snap-in?

Answer: The Services snap-in

18. Click the **Services** button.
The Services console appears.
19. Close the **Services** console.
20. Click the **Users** tab.
This tab displays users who have either local (Console) or remote desktop connections to the server.
21. Click the **Networking** tab.
This tab provides an overview of performance for each available network adapter.
22. Click the **Performance** tab.
This tab provides an overview of performance for CPU utilization and Memory.

Question: Which major system component is *not* shown by task manager?

Answer: Disk

► **Task 3: Monitor real-time performance with Resource Monitor**

1. In Task Manager, on the **Performance** tab, click the **Resource Monitor** button.
If you are prompted for administrative credentials, use the account Pat.Coleman_Admin with the password Pa\$\$w0rd.
2. Resource Monitor appears. Maximize the Resource Monitor window and close Task Manager.
3. Click the **CPU** graph. The CPU section expands.

Question: How much CPU utilization is being generated by Reliability and Performance Monitor itself?

Answer: Answers will vary. Utilization will be higher at first, when the tool is opened, and will rise when views are changed. If a view is left alone, utilization drops.

5. Click the **CPU** graph. The **CPU** section collapses.
6. Click the **Disk** graph. The **Disk** section expands.

Questions: What file is experiencing the most Read activity? Which process is causing the Read activity for that file? Which file is experiencing the most Write activity? Which process is causing the Write activity for that file?

Answer: Answers will vary.

7. To view the activity of the page file, click the **File** column label.
8. If **C:\pagefile.sys** is not listed, open an application such as Server Manager with administrative credentials. Use the account **Pat.Coleman_admin** with the password **Pa\$\$w0rd**. This should generate some paging activity.

Questions: How many processes are reading from or writing to pagefile.sys?

Answer: Answers will vary.

Question: If the pagefile Read and Write activity is consistently high, what system component should be augmented?

Answer: Memory. Excessive paging causes disk activity, but paging itself is caused by insufficient RAM.

9. Close Resource Manager.
10. Click the **Start** button.
11. In the **Start Search** box, type **perfmon**, and then press ENTER.
The User Account Control dialog box appears.
12. Click **Use Another Account**.
13. In **User name**, type **Pat.Coleman_Admin**.
14. In **Password**, type **Pa\$\$w0rd**, and then press ENTER.

Users, members of the Performance Monitor Users group, members of the Performance Log Users group, and members of the local Administrators group, are able to access increasing levels of functionality from Windows Reliability and Performance Monitor (WRPM).

Reliability and Performance Monitor opens.

The home view for the console is the Resource Overview, equivalent to Resource Monitor.

Note that the console tree contains each of the WRPM snap-ins.

15. Close **Reliability and Performance Monitor**.
16. Click the **Start** button.
17. In the **Start Search** box, type **perfmon /res**, and then press ENTER.
The User Account Control dialog box appears.
18. In **User name**, type **Pat.Coleman_Admin**.

19. In **Password**, type **Pa\$\$w0rd**, and then press ENTER. The **Resource Monitor** opens.

This is an alternate way to open Resource Monitor, which you have opened from Task Manager, and which is the home view of the Reliability and Performance Monitor console.

20. Close **Resource Monitor**.

Exercise 2: Use Reliability Monitor and Event Viewer to Identify Performance-Related Events

► Task 1: Monitor stability-related events with Reliability Monitor

1. Click the **Server Manager** icon next to the **Start** button.
The User Account Control dialog box appears.
2. In **User name**, type **Pat.Coleman_Admin**.
3. In **Password**, type **Pa\$\$w0rd**, and then press ENTER.
Server Manager opens.
4. In the console tree, expand **Diagnostics, Reliability and Performance, Monitoring Tools**, and then click **Reliability Monitor**.
5. In the **System Stability Chart**, scroll to the left and right.
6. Click the **Information** icon in the **Software (Un) Installs** row on Sept 9, 2009.
7. Examine the events that affected system stability on Sept 9, 2009.

► Task 2: Identify role-related events with Server Manager

1. In the Server Manager console tree, click the root node, **Server Manager**.
2. In the details pane, scroll to the **Roles Summary** section.

Question: What icons appear next to the ADDS and DNS Server roles?

Answer: Answers will vary.

3. Click the link to the **Active Directory Domain Services** role in the **Roles Summary** section.
4. In the **Summary** section, examine the information shown in the **Events** section.
5. Click the **Filter Events** link in the **Events** section.
The Filter Events dialog box appears.

6. Clear the **Information** check box, and then click **OK**.
7. Double-click an event to open its details, examine the event, and then close the event.
8. Note the information shown in the **System Services** section.

► **Task 3: Examine the event logs**

1. In the Server Manager console tree, expand **Diagnostics** and **Event Viewer**, and then click **Event Viewer**.
The Event Viewer Overview and Summary view appears in the details pane.
2. In the **Summary of Administrative Events** section, click the plus sign (+) icon next to **Error** to expand the **Error** events summary.
3. Double-click a summary row with **ActiveDirectory** as the source.
If you do not see a row in the summary with ActiveDirectory as the source, double-click another row in the **Error** events summary.
The Summary page events view opens in the details pane.
This view "drills down" to show the events that were summarized on the row of the Error events summary.
4. In the console tree, expand **Windows Logs** and **Applications and Services Logs**.
5. Examine the logs contained in those nodes, and the types of events they display.
6. In the console tree, click the **Administrative Events** node underneath **Custom Views**.
7. Examine the events in the view.
8. Right-click **Administrative Events**, and then click **Properties**.
9. Note that the **Description** indicates that the view shows **Critical**, **Error** and **Warning** events from all administrative logs.
10. Click the **Edit Filter** button.
The Custom View Properties (Read Only) dialog box appears.
11. Note that this custom view cannot be modified—it is **Read Only**.

12. Note that it is difficult to know exactly which logs are being included in the **Event Logs** list. The information is truncated.
13. Click the **XML** tab.

Question: Can you identify which logs are included using the information on the XML tab?

Answer: Application, Security, System, DFS Replication, Directory Service, DNS Server, Hardware Events, Internet Explorer, Key Management Service, and Microsoft-Windows-TerminalServices-PnPDevices/Admin logs are included.

Question: In each XML Select element, what do you think Level refers to?

Answer: The Level refers to the event level: Warning, Error, or Critical events.

14. Click **Cancel** twice to close the open dialog boxes.

► **Task 4: Create a custom view**

1. In the console tree, click **Custom Views**.
2. Right-click **Custom Views**, and then click **Create Custom View**.
The **Create Custom View** dialog box appears.
3. In the **Event level** options, select **Critical**, **Warning**, and **Error**.
4. In the **Event logs** list, expand **Applications and Services Logs**, and then select **DFS Replication**, **Directory Service**, and **DNS Server**.
5. Click **OK**.
The **Save Filter to Custom View** dialog box appears.
6. In **Name**, type **Custom Directory Service Event View**, and then click **OK**.
7. In the console tree, right-click **Custom Directory Service Event View** and then examine the commands that are available for the view.

► **Task 5: Export a custom view**

1. In the console tree, right-click **Custom Directory Service Event View**, and then click **Export Custom View**.
The Save As dialog box appears.
2. In **File name**, type **D:\Data\DSEventView**, and then press ENTER.

► **Task 6: Import a custom view**

1. Switch to HQDC02.
2. Click the **Server Manager** icon next to the **Start** button.
The User Account Control dialog box appears.
3. In **User name**, type **Pat.Coleman_Admin**.
4. In **Password**, type **Pa\$\$w0rd**, and then press ENTER.
Server Manager opens.
5. In the console tree, expand **Diagnostics**, **Event Viewer**, and **Custom Views**, and then click **Custom Views**.
6. Right-click **Custom Views**, and then click **Import Custom View**.
The Import Custom View dialog box opens.
7. In **File Name**, type **\\HQDC01\Data\DSEventView.xml** and then press ENTER.
The Import Custom View File dialog box appears.
8. In **Name**, type **Custom Directory Service Event View**, and then click **OK**.
A Query Error message appears, because HQDC02 is not a Domain Name System (DNS) server and therefore has no DNS Server log.
9. Click **OK**.

Exercise 3: Monitor Events on Remote Computers with Event Subscriptions

► Task 1: Configure computers to forward and collect events

1. Switch to HQDC01 (the collector computer).
2. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
3. Type **wecutil qc** then press ENTER.
You are prompted to confirm the change.
4. Type **Y** and then press ENTER.
5. Switch to HQDC02 (the source computer).
6. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
7. Type **winrm quickconfig** and then press ENTER.
You are prompted to confirm the change.
8. Type **Y** and then press ENTER.

► Task 2: Create a subscription to collect events

1. Switch to HQDC01.
2. Switch to Server Manager.
3. In the console tree, under **Event Viewer**, click **Subscriptions**.
4. Right-click **Subscriptions** and click **Create Subscription**.
The Subscription Properties dialog box appears.
5. In **Subscription name**, type **DC Services**.
6. Ensure that **Collector initiated** is selected.
7. Click the **Select Computers** button.
The Computers dialog box appears.
8. Click the **Add Domain Computers** button.
The Select Computer dialog box appears.

9. Type **HQDC02**, and then click **OK**.
10. Click the **Test** button.

An Event Viewer message appears, indicating that the connectivity test succeeded.
11. Click **OK**.
12. Click **OK** to close the **Computers** dialog box.
13. Click the **Select Events** button.

The Query Filter dialog box opens.
14. Click the **Information** checkbox in the **Event Level:** section.
15. Click the **Event Logs** drop-down arrow.
16. Expand **Windows Logs**, and then select the **System** log.
17. Click in the **Includes/Excludes Event IDs** box.
18. Type **7036**, the Event ID associated with starting and stopping a service.
19. Click **OK**.
20. Click the **Advanced** button.

The Advanced Subscription Settings dialog box appears.
21. Click **Specific User**.
22. Click the **User and Password** button.

The Credentials for Subscription Source dialog box appears.
23. In **User name**, type **CONTOSO\Pat.Coleman_admin**.

We are using an account who is a member of the Domain Admins group for Lab purposes, but you should create a dedicated account to carry out this monitoring in a real world environment.
24. In **Password**, type **Pa\$\$w0rd**, and then press ENTER.
25. Click the **Minimize Latency** option, and then click **OK**.
26. Click **OK** to close the **Subscription Properties** dialog box.
27. If **Event Viewer** messages appear, click **Yes**.
28. Ensure that the **Status** column for the subscription indicates **Active**.

► **Task 3: Generate events**

1. Switch to HQDC02.
2. In the command prompt (running as an administrator), type **net stop dfsr**, and then press ENTER.
3. Type **net start dfsr**, and then press ENTER.

► **Task 4: View forwarded events**

1. Switch to HQDC01.
2. In the Server Manager console tree, under **Event Viewer\Windows Logs**, click **Forwarded Events**.

Forwarded events may take several minutes to appear. If the events do not appear right away, wait a few minutes, start and stop the Distributed File System Replication (DFSR) service on HQDC02 again, then wait a few more minutes.

Exercise 4: Attach Tasks to Event Logs and Events

► Task 1: Attach a task to an event log and to an event

1. Switch to HQDC01.
2. In the Server Manager console tree, under **Event Viewer\Windows Logs**, click **Forwarded Events**.
3. Right-click **Forwarded Events**, and then click **Attach a Task to this Log**, and then click **Next**.
4. On the **When a Specific Event is Logged** page, click **Next**.

You can invoke a task when an event matching specific criteria is logged, or when any event is added to a log. For each trigger, you can send an e-mail message, start a program, or display a message on the desktop. In a production environment, sending an e-mail message or starting a program that responds to the event are the most common tasks to invoke. In this lab, however, you will use the "display a message" task to demonstrate that, in fact, tasks are triggered.

5. On the **Action** page, click **Display a message**, and then click **Next**.
6. On the **Display a Message** page, in **Title**, type **Forwarded Event Received**.
7. In **Message**, type **A forwarded event was received**.
8. Click **Next**, and then click **Finish**.
9. Click **OK** to acknowledge the Event Viewer message.
10. In the details pane, right-click **one of the 7036** events, and then click **Attach Task to this Event**, and then click **Next**.
11. On the **When a Specific Event is Logged** page, click **Next**.
12. On the **Action** page, click **Display a message**, and then click **Next**.
13. On the **Display a Message** page, in **Title**, type **DC Service Event**.
14. In **Message**, type **A service was started or stopped**.
15. Click **Next**, and then click **Finish**.
16. Click **OK** to acknowledge the Event Viewer message.

17. In the console tree, expand **Configuration, Task Scheduler**, and then click **Event Viewer Tasks**.
18. Double-click the first event viewer task.
19. Explore the properties of the task that you created.

► **Task 2: Prepare to view event viewer task messages**

When you choose to display a message in a task, because messages are displayed on the desktop of the user whose account is used to create the event viewer task (Pat.Coleman_Admin), you will need to log on interactively as Pat.Coleman_Admin to fully experience this simulation.

1. Click the **Start** button, then click the arrow next to the **Lock** button, and then click **Log Off**.

The logon prompt appears.

2. Press ALT+DEL, which sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine guest.
3. Click **Switch User**.
4. Click **Other User**.
5. In **User name**, type **Pat.Coleman_Admin**.
6. In **Password**, type **Pa\$\$w0rd**, then press ENTER or click the log on arrow.

The Windows desktop appears.

► **Task 3: Confirm that event viewer tasks are functioning**

1. Switch to HQDC02.
2. In the command prompt (running as an administrator), type **net stop dfsr**, and then press ENTER.
3. Type **net start dfsr**, and then press ENTER.
4. Switch to HQDC01.
5. Wait for the event viewer task messages to appear.

Exercise 5: Monitor Active Directory Domain Services (AD DS) with Performance Monitor

► Task 1: Configure Performance Monitor to monitor AD DS

1. Switch to HQDC02.
2. In Server Manager's console tree, expand **Diagnostics, Reliability and Performance**, and **Monitoring Tools**, and then click **Performance Monitor**.
3. Click the **Add** button (the green plus sign) on the toolbar to add objects and counters.

The Add Counters dialog box appears.
4. In the **Available Counters** list, expand the **DirectoryServices** object.
5. Click the **DRA Inbound Bytes Total/sec** counter, and then click the **Add** button.
6. Repeat the previous step to add the following counters:
 - **DRA Outbound Bytes Total/sec**
 - **DS Threads In Use**
 - **DS Directory Reads/sec**
 - **DS Directory Writes/sec**
 - **DS Directory Searches/sec**
7. In the **Available Counters** list, expand the **Security System-Wide Statistics** object.
8. Select the **Kerberos Authentications** counter, and then click the **Add** button.
9. In the **Available Counters** list, expand the **DNS** object.
10. Select the **UDP Query Received/sec** counter, and then click the **Add** button.
11. Click **OK**.
12. Watch performance for a few moments.
13. In the counter list below the graph, select **UDP Query Received/sec**.

14. Click the **Highlight** button in the toolbar.

The selected counter is highlighted, making it easier to see that counter's performance.

15. Click the **Highlight** button in the toolbar again to turn off the highlight.
16. Spend a few moments exploring the functionality of Performance Monitor. Do not add or remove counters, however.

► **Task 2: Create a Data Collector Set from Performance Monitor counters**

1. In the console tree, right-click **Performance Monitor**, then point to **New**, and then click **Data Collector Set**.

The Create new Data Collector Set dialog box appears.

2. In **Name**, type **Custom ADDS Performance Counters**, and then click **Next**.
3. Make a note of the default root directory in which the data collector set will be saved, and then click **Next**.
4. Click **Finish**.

► **Task 3: Start a Data Collector Set**

1. In the console tree, expand **Data Collector Sets** and **User Defined**, and then click **User Defined**.

2. Right-click **Custom ADDS Performance Counters**, and then click **Start**.

The Custom ADDS Performance Counters node is automatically selected.

You can identify the individual data collectors in the Data Collector Set. In this case, only one data collector (the System Monitor Log performance counters) is contained in the data collector set.

You can also identify where the output from the data collector is being saved.

3. In the console tree, right-click the **Custom ADDS Performance Counters** data collector set, and then click **Stop**.

► **Task 4: View a Data Collector Set report**

- In the console tree, expand **Reports, User Defined, Custom ADDS Performance Counters**, and then click **System Monitor Log.blg**.

The graph of the log's performance counters is displayed.

Exercise 6: Work with Data Collector Sets

► Task 1: Examine a predefined Data Collector Set

1. Still on HQDC02 logged on as **contoso\Pat.Coleman** with password **Pa\$\$w0rd**.
2. In Server Manager's console tree, expand **Diagnostics, Reliability and Performance, Data Collector Sets, System**, and then click **Active Directory Diagnostics**.

Question: What data collectors are part of the Data Collector Set?

Answer: Event traces for NT Kernel and Active Directory, Configuration for AD Registry, and Performance Counters

3. Right-click **Active Directory Diagnostics**, and then click **Start**.
4. In the console tree, expand **Reports, System** and **Active Directory Diagnostics**, and then click the report, which will be named **yyyymmdd-xxxx** where **yyyy** is the current year, **mm** is the current date, **dd** is the current day, and **xxxx** is a four-digit incrementing serial number.

The Report Status indicates that data is being collected for 300 seconds (5 minutes).

5. Wait five minutes or at least one minute then right-click **Active Directory Diagnostics** under **Data Collector Sets\System**, and then click **Stop**.

The Report Status indicates that the report is being generated.

The report appears.

6. Spend a few moments examining the sections of the report.
7. Right-click the report, then point to **View**, and then click **Performance Monitor**.
8. Right-click the report, then point to **View**, and then click **Report**.
9. Right-click the report, then point to **View**, and then click **Folder**.
10. In the details pane, double-click **Performance Counter**.

The log is opened in a new instance of Reliability and Performance Monitor.

11. If the new instance of WRPM is minimized, open it by clicking its button on the taskbar.
12. Close the new instance of WRPM.
13. In the Server Manager console tree, expand **Monitoring Tools**, and then click **Performance Monitor**.
14. Click the **View Log Data** button in the toolbar, which is the second button from the leftmost edge of the toolbar.

The Performance Monitor Properties dialog box opens.
15. Click the **Log files** option.
16. Click the **Add** button.

The Select Log File dialog box opens, focused on C:\PerfLogs.
17. Double-click **ADDS**.
18. Double-click the folder with the same name as the report you generated.
19. Click **Performance Counter**, and then click **Open**.
20. Click **OK**.
21. Note that no counters are immediately visible.
22. Click the green plus sign—the **Add** button—on the toolbar.
23. In the **Available counters** list, expand the **DirectoryServices** object.
24. Select **DS Directory Reads/sec**, **DS Directory Searches/sec** and **DS DirectoryWrites/sec**, and then click **Add**.
25. Click **OK**.

► **Task 2: Create a Data Collector Set**

1. In the Server Manager console tree, expand **Diagnostics, Reliability and Performance**, and **Data Collector Sets**, and then click **User Defined**.
2. Right-click **User Defined**, point to **New**, and then click **Data Collector Set**.
3. On the **Create new Data Collector Set** page, in the **Name** box, type **Custom ADDS Diagnostics**.
4. Click the **Create from a template (Recommended)** option.
5. Click **Next**.

6. On the **Which template would you like to use?** page, select **Active Directory Diagnostics**, and then click **Next**.
7. On the **Where would you like the data to be saved?** page, in **Root directory**, create a folder **C:\ADDS Data Collector Sets**, and then click **Next**.
8. On the **Create the data collector set?** page, click the **Change** button.
A Reliability and Performance Monitor credentials dialog box appears.
9. In **User name**, type **CONTOSO\Pat.Coleman_Admin**.

10. In **Password**, type **Pa\$\$w0rd**, then click **OK**.

In a production environment, the account you use should be a unique domain account. It must be a member of the Performance Log Users group and must have the Log On As A Batch Job User logon right. By default, the Performance Log Users group has this right, so you can simply create a domain account and make it a member of the group.

11. Click **Finish**.

► **Task 3: Configure start conditions for a Data Collector Set**

1. In the console tree, right-click **Custom ADDS Diagnostics**, and then click **Properties**.

The Custom ADDS Diagnostics Properties dialog box appears.

2. Click the **Schedule** tab.
3. Click the **Add** button.

The Folder Action dialog box appears.

4. Confirm that **Beginning date** is today's date.
5. Select the **Expiration date** check box.
6. In the **Expiration date** drop-down list, select the date one week from today.
7. Configure the start time to the current time plus five minutes. Make a note of the start time you configure.

Note that the Expiration date property specifies when new instances of data collection will no longer be started. It does *not* stop existing sessions. You must configure the Stop Condition to specify when data collection is stopped.

8. Click **OK**.

9. In the **Custom ADDS Diagnostics Properties** dialog box, click **Apply**.
A Reliability and Performance Monitor credentials dialog box appears.
10. In **User name**, type **CONTOSO\Pat.Coleman_Admin**.
11. In **Password**, type **Pa\$\$w0rd**, then click **OK**.

► **Task 4: Configure stop conditions for a Data Collector Set**

1. Click the **Stop Condition** tab.
2. Select the **Overall Duration** check box.
3. Configure the duration to **2 Minutes**.
In a production environment, you would likely run a data collector for a longer period of time.
4. Select the check box, **Stop when all data collectors have finished**.
This option allows data collectors that are running when the Overall Duration is reached to finish recording the most recent values.
5. Click **OK**.

► **Task 5: Configure data management for a data collector**

1. Right-click **Custom ADDS Diagnostics**, and then click **Data Manager**.
2. On the **Data Manager** tab, click the **Resource policy** list, and then select **Delete oldest**.
3. Click the **Actions** tab.
4. Click **1 Day(s)**.
5. Click the **Edit** button.
The Folder Action dialog box appears.
6. In the **Action** section, select the check box **Copy cab file to this directory**.
7. In the **Copy cab file to this directory** box, type
\\hqdc01\ADDS_Diag_Reports.
8. Confirm that the **Create cab file** and **Delete data file** check boxes are selected.
9. Click **OK**.

10. Click **OK**.

A Reliability and Performance Monitor credentials dialog box appears.

11. In **User name**, type **Contoso\Pat.Coleman_Admin**.
12. In **Password**, type **Pa\$\$w0rd**, then click **OK**.

► **Task 6: View the results of data collection**

1. Wait until the time that you configured as the start time for the Data Collector Set passes.
2. Select the report under **Reports\User Defined\Custom ADDS Diagnostics**.

The Report Status indicates that data is being collected for 120 seconds (two minutes).

After data collection has completed, the Report Status indicates that the report is being generated.

3. Spend a few moments examining the report.
4. Right-click the report in the console tree, then point to **View**, and then click **Folder**.
5. Double-click **Performance Counter** in the details pane.

A new instance of Reliability and Performance Monitor opens, with Performance Monitor displaying the logged data in the Performance Counter log.

6. Spend a few moments examining the performance graph, and then close the window.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs in this module.

Lab Review Questions

Question: In what situations do you currently use, or can you envision using, event subscriptions as a monitoring tool?

Answer: Answers may vary depending on the situation.

Question: To what events or performance counters would you consider attaching e-mail notifications or actions? Do you use notifications or actions currently in your enterprise monitoring?

Answer: Answers may vary depending on the situation.

Lab B: Manage the Active Directory Database

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the user name.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the user name.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a user name and password:

1. In **User Name**, type the user name.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Perform Database Maintenance

► Task 1: Prepare for the lab

The virtual machines should already be started and available after completing Lab A. However, if they are not, you should complete the below steps.

1. Start 6425B-HQDC01-B.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Start 6425B-HQDC02-B, but do not log on.

► Task 2: Prepare to compact the Active Directory database

1. Run Command Prompt with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. Type **md D:\NTDSCompact**.
3. Type **md D:\NTDSOriginal**.

► Task 3: Stop the AD DS service

1. Click **Start**, then point to **Administrative Tools**, then right-click **Services**, and then click **Run as administrator**.
2. Click **Use another account**.
3. In **User name**, type **Pat.Coleman_Admin**.
4. In **Password**, type **Pa\$\$w0rd**, and then press ENTER.
The Services console opens.
5. Click **Active Directory Domain Services**.
6. Click the **Stop** button on the toolbar.
The Stop Other Services dialog box appears, informing you of dependent services that will also be stopped.
7. Click **Yes**.

► **Task 4: Compact the Active Directory database**

1. Switch to the command prompt.
2. Type **ntdsutil**, and then press ENTER.
3. Type **activate instance ntds**, and then press ENTER.
4. Type **files**, and then press ENTER.
5. Type **compact to D:\NTDSCompact**, and then press ENTER.
NTDSUtil compacts the database to a new copy of NTDS.dit in the D:\NTDSCompact folder.
6. Wait for the operation to complete.
You are reminded that you need to copy the compacted file over the current version of ntds.dit, and to delete the log files. In the next task, you will perform more effective procedures that also back up Active Directory.
7. Type **quit**, and then press ENTER.
8. Type **quit**, and then press ENTER.

► **Task 5: Replace the Active Directory database with the compacted copy**

1. Type **cd %systemroot%\ntds**, and then press ENTER.
2. Type **move ntds.dit D:\NTDSOriginal**, and then press ENTER.
3. Type **move *.log D:\NTDSOriginal**, and then press ENTER.
4. Type **copy D:\NTDSCompact\ntds.dit**, and then press ENTER.

► **Task 6: Verify the integrity of the compacted database**

1. Type **ntdsutil**, and then press ENTER.
2. Type **activate instance NTDS**, and then press ENTER.
3. Type **files**, and then press ENTER.
4. Type **integrity**, and then press ENTER.
5. Type **quit**, and then press ENTER.
6. Type **semantic database analysis**, and then press ENTER.

7. Type **go fixup**, and then press ENTER.
8. Type **quit**, and then press ENTER.
9. Type **quit**, and then press ENTER.

► **Task 7: Start the AD DS service**

1. Switch to the **Services** console.
2. Click **Active Directory Domain Services**.
3. Click the **Start** button on the toolbar.
4. Close the **Services** console.

Exercise 2: Work with Snapshots and Recover a Deleted User

► Task 1: Create a snapshot of Active Directory

1. Switch to the command prompt.
2. Type **ntdsutil**, and then press ENTER.
3. Type **snapshot**, and then press ENTER.
4. Type **activate instance ntds**, and then press ENTER.
5. Type **create**, and then press ENTER.

The command returns a message indicating that the snapshot set was generated successfully. The GUID that is displayed is important for commands in later tasks. Make a note of the GUID or, alternately, copy it to the Clipboard.

6. Type **quit**, and then press ENTER.
7. Type **quit**, and then press ENTER.

► Task 2: Make a change to Active Directory

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **contoso.com** domain, and the **User Accounts** OU, and then click the **Employees** OU.
3. Right-click the user account for **Adriana Giorgi**, and then click **Delete**.
A confirmation prompt appears.
4. Click **Yes**.

► Task 3: Mount an Active Directory snapshot and create a new instance

1. Switch to the command prompt.
2. Type **ntdsutil**, and then press ENTER.
3. Type **activate instance ntds**, and then press ENTER.
4. Type **snapshot**, and then press ENTER.

5. Type **list all**, and then press ENTER.

The command returns a list of all snapshots.

6. Type **mount guid**, where **guid** is the GUID returned by the create snapshot command, and then press ENTER.

i.e. `mount xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx`

You should receive a message saying the ".....xxxxxx was mounted"

7. Type **quit**, and then press ENTER.

8. Type **quit**, and then press ENTER.

9. Type **dsamain -dbpath**

c:\\$snap_datetime_volume\windows\ntds\ntds.dit -ldapport 50000, and then press ENTER.

Note that datetime will be a value that is unique for you. There should only be one folder on your drive C with a name that begins with *\$snap*.

A message indicates that Active Directory Domain Services startup is complete. Leave Dsamain.exe running. Do not close the command prompt.

► Task 4: Explore a snapshot with Active Directory Users and Computers

1. Switch to **Active Directory Users and Computers**.
2. Right-click the root node, and then click **Change Domain Controller**.
The Change Directory Server dialog box appears.
3. Click **<Type a Directory Server name[:port] here>**.
4. Type **HQDC01:50000**, and then press ENTER.
5. Click **OK**.
6. In the console tree, expand the **contoso.com** domain, and the **User Accounts** OU, and then click the **Employees** OU.
7. Note that Adriana Giorgi's object is displayed because the snapshot was taken prior to deleting it.
8. Close Active Directory Users and Computers.

► **Task 5 (Optional): Use LDP to restore a deleted object**

Restoring a deleted user account is a task that is not directly related to snapshots. You use the Ldp.exe command to reanimate objects from the Deleted Objects container of Active Directory. A deleted object is stripped of most of its attributes, so a snapshot can be helpful to examine attributes of the object prior to its deletion.

1. Click the **Start** button. In the **Start Search** box, type **LDP.exe** and press CTRL+SHIFT+ENTER, which executes the command as an administrator.
The User Account Control dialog box appears.
2. Click **Use another account**.
3. In **User name**, type **Pat.Coleman_Admin**.
4. In **Password**, type **Pa\$\$w0rd**, and then press ENTER.
LDP opens.
5. Click the **Connection** menu, then click **Connect**, and then click **OK**.
6. Click the **Connection** menu, then click **Bind**, and then click **OK**.
7. Click the **Options** menu, and then click **Controls**.
8. In the **Load Predefined** list, click **Return Deleted Objects**, and then click **OK**.
9. Click the **View** menu, then click **Tree**, and then click **OK**.
10. In the console tree, expand **DC=contoso,DC=com**, and then double-click **CN=Deleted Objects,DC=contoso,DC=com**.
11. Right-click **CN=Adriana Giorgi**, and then click **Modify**.
12. In the **Attribute** box, type **isDeleted**.
13. In the **Operation** section, click **Delete**.
14. Click the **Enter** button.
15. In the **Attribute** box, type **distinguishedName**.
16. In the **Values** box, type **CN=Adriana Giorgi,OU=Employees,OU=User Accounts,DC=contoso,DC=com**.
17. In the **Operation** section, click **Replace**.
18. Click the ENTER button.
19. Select the **Extended** check box.

20. Click the **Run** button.
21. Click the **Close** button.
22. Close LDP.
23. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
24. In the console tree, expand the **contoso.com** domain, and the **User Accounts** OU, and then click the **Employees** OU.
25. Note that Adriana Giorgi's account is restored; however, all attributes are missing, including the description and the password. Because the password is missing, the account has been disabled.
26. Switch to the instance of Active Directory Users and Computers that is displaying the snapshot data.
27. Note that you can use the attributes contained in the snapshot to manually repopulate attributes in Active Directory.
28. Close both instances of Active Directory Users and Computers.

► **Task 6: Unmount an Active Directory snapshot**

1. Switch to the command prompt.
2. Press CTRL+C to stop DSAMain.exe.
3. Type **ntdsutil**, and then press ENTER.
4. Type **activate instance ntds**, and then press ENTER.
5. Type **snapshot**, and then press ENTER.
6. Type **unmount guid**, where **guid** is the GUID of the snapshot, and then press ENTER.
7. Type **quit**, and then press ENTER.
8. Type **quit**, and then press ENTER.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs in this module.

Lab Review Questions

Question: In what other situations might it be useful to mount a snapshot of Active Directory?

Answer: If you discover a problem with Active Directory that will require restoring a backup, you might want to look at snapshots to determine just how far back you need to go to restore. Once you've found the snapshot in which the correct data resides, you can then restore the backup taken on the same date.

Question: What are the disadvantages of restoring a deleted object with a tool such as LDP?

Answer: You must repopulate all attributes.

Lab C: Backup and Restore Active Directory

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the user name.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the user name.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a user name and password:

1. In **User Name**, type the user name.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Back up Active Directory

► Task 1: Prepare for the lab

The virtual machines should already be started and available after completing Labs A and B. However, if they are not, you should complete the below steps.

1. Start 6425B-HQDC01-B.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Start 6425B-HQDC02-B.
4. Log on to HQDC02 as **Pat.Coleman** with the password **Pa\$\$w0rd**.

► Task 2: Install the Windows Server Backup feature

1. Switch to HQDC01.
2. Click the **Server Manager** icon next to the **Start** button.
The User Account Control dialog box appears.
3. In **User name**, type **Pat.Coleman_Admin**.
4. In **Password**, type **Pa\$\$w0rd**, and then press ENTER.
5. Server Manager opens.
6. In the console tree, click **Features**.
7. In the details pane, click the **Add Features** link.
8. On the **Select Features** page, expand **Windows Server Backup Features**, and then select the **Windows Server Backup** and **Command-line Tools** check boxes.

When you select Command-line Tools, the Add Features Wizard prompts you to install Windows PowerShell™, a required feature.

9. Click **Add Required Features**.
10. Click **Next**.
11. Click **Install**.
12. When the installation finishes, click **Close**.

► **Task 3: Create a scheduled backup**

1. Go to **Start>Administrative Tools>** and run **Windows Server Backup** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the Actions pane, click the **Backup Schedule** link.
The Backup Schedule Wizard appears.
3. On the **Getting Started** page, click **Next**.
4. On the **Select backup configuration** page, click **Custom**, and then click **Next**.
5. On the **Select backup items** page, clear the **6425B (D:) drive** check box, and then click **Next**.
6. On the **Specify backup time** page, click **Once a day**.
7. In the **Select time of day** list, select **12:00 am**.
8. Click **Next**.
9. On the **Select destination disk** page, click **Show All Available Disks**.
The Show All Available Disks dialog box appears.
10. Select the **Disk 1** check box, and then click **OK**.
11. On the **Select destination disk** page, select the **Disk 1** check box, and then click **Next**.
The Windows Server Backup dialog box appears, informing you that all data on the disk will be deleted.
12. Click **Yes** to continue.
13. On the **Label destination disk** page, click **Next**.
14. On the **Confirmation** page, click **Cancel** to avoid formatting D drive D.

► **Task 4: Perform an interactive backup**

1. In the Windows Server Backup console's **Actions** pane, click the **Backup Once** link.
The Backup Once Wizard appears.
2. On the **Backup options** page, ensure that **Different options** is selected, and then click **Next**.

3. On the **Select backup configuration** page, click **Custom**, and then click **Next**.
4. On the **Select backup items** page, ensure that the **Enable system recovery** check box is selected, and then click **Next**.
5. On the **Specify destination type** page, click **Next**.
6. On the **Select backup destination** page, click **Next**.
7. On the **Specify advanced option** page, click **VSS full backup**, and then click **Next**.
8. On the **Confirmation** page, click **Backup**.

The backup will take about 10-15 minutes to complete. When the backup is complete, close Windows Server Backup.

Exercise 2: Restore Active Directory and a Deleted OU

► Task 1: Delete the Employees OU

1. Still on HQDC01, run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand **contoso.com**, and then click the **User Accounts** OU.
3. In the details pane, right-click **Contractors**, and then click **Delete**.
A confirmation message appears.
4. Click **Yes**.
A warning message appears.
5. Click **Yes**.
6. Wait for the deletion to complete.
7. Switch to HQDC02.
8. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
9. In the console tree, expand **contoso.com**, and then click the **User Accounts** OU.
10. Verify that the **Contractors** OU is deleted.

► Task 2: Restart in Directory Services Restore Mode (DSRM)

1. Switch to HQDC01.
2. Run **Command Prompt** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
3. Type **bcdedit /set safeboot dsrepair**, and then press ENTER.
4. Type **shutdown -t 0 -r** and then press ENTER.

► **Task 3: Restore System State data**

1. Log on to HQDC01 as **Administrator** with the password **Pa\$\$w0rd**.
2. Click **Start**, then right-click **Command Prompt**, and then click **Run as administrator**.
The command prompt opens.
3. Type **wbadmin get versions -backuptarget:D: -machine:HQDC01**, and then press ENTER.
4. Note the version information that is returned.
5. Type **wbadmin start systemstaterecovery -version:version -backuptarget:D: -machine:HQDC01**, where version is the number that you recorded in the previous step, and then press ENTER.
i.e. **wbadmin start systemstaterecovery -version:10/14/2009-01:11 -backuptarget:D: -machine:HQDC01**
6. Type **Y**, and then press ENTER.
The restore will take about 30-35 minutes. Depending on the host machine it could take up to an hour.

► **Task 4: Mark the restored information as authoritative and restart the server**

1. At the command prompt, type **ntdsutil**, and then press ENTER.
2. Type **activate instance ntds**, and then press ENTER.
3. Type **authoritative restore**, and then press ENTER.
4. Type **restore subtree "ou=Contractors,ou=User Accounts,dc=contoso,dc=com"**, and then press ENTER.
5. Click **Yes** in the confirmation dialogue message box that appears.
6. Type **quit**, and then press ENTER.
7. Type **quit**, and then press ENTER.
8. Type **bcdedit /deletevalue safeboot**, and then press ENTER.
9. Type **shutdown -t 0 -r**, and then press ENTER.

► **Task 5: Verify that the deleted data has been restored**

1. Wait for HQDC01 to restart.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
4. In the console tree, expand **contoso.com**, and then click the **User Accounts** OU.
5. Verify that the **Contractors** OU is restored.
6. Switch to HQDC02.
7. In the **Active Directory Users and Computers** console tree, click the **User Accounts** OU.
8. Press F5 (Refresh).
9. Verify that the **Contractors** OU is restored.

Lab Review Questions

Question: What type of domain controller and directory service backup plan do you have in place? What do you expect to put in place after having completed this lesson and this Lab?

Answer: Answers will vary.

Question: When you restore a deleted user (or an OU with user objects) using authoritative restore, will the objects be exactly the same as before? What attributes might not be the same?

Answer: Answers may vary somewhat, but the question is designed to frame a discussion of group membership. A user's group membership is not an attribute of the user object but rather of the group object. When you authoritatively restore a user, you are not restoring users' membership in groups. The user was removed from the member attribute of groups when it was deleted. So the restored user will not be a member of any groups other than its primary group. In order to restore group memberships, you would have to consider authoritatively restoring groups as well. This may or may not always be desirable, because when you authoritatively restore the groups you return their membership to the day on which the backup was made.

Module 14

Lab Answer Key: Manage Multiple Domains and Forests

Contents:

Lab A: Raise Domain and Forest Functional Levels	
Exercise 1: Raise the Domain Functional Level to Windows Server 2003	4
Exercise 2: Raise the Forest Functional Level to Windows Server 2003	6
Exercise 3: Raise the Domain Functional Level to Windows Server 2008	9
Lab B: Administer a Trust Relationship	
Exercise 1: Configure DNS	13
Exercise 2: Create a Trust Relationship	15
Exercise 3: Validate a Trust Relationship	18
Exercise 4: Assign Permissions to Trusted Identities	19
Exercise 5: Implement Selective Authentication	22

Lab A: Raise Domain and Forest Functional Levels

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the user name.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the user name.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a user name and password:

1. In **User Name**, type the user name.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Raise the Domain Functional Level to Windows Server® 2003

► Task 1: Prepare for the lab

1. Start 6425B-TSTDC01-A.
2. Log on to TSTDC01 as **Sara.Davis** with the password **Pa\$\$w0rd**.

► Task 2: Confirm that the current domain functional level is Windows 2000 Native

1. Run **Active Directory Domains and Trusts** with administrative credentials. Use the account **Sara.Davis_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, right-click the **tailspintoys.com** domain, and then click **Raise Domain Functional Level**.
The Raise Domain Functional Level dialog box appears.
3. Confirm that the **Current domain functional level** is **Windows 2000 Native**.
4. Click **Cancel**. Do not make any change to the domain functional level.

► Task 3: Experience functionality not supported by the Windows 2000 Native domain functional level

1. Run the Command Prompt with administrative credentials. Use the account **Sara.Davis_Admin** with the password **Pa\$\$w0rd**.
2. Type **redircmp.exe "ou=Client Computers,dc=tailspintoys,dc=com"** and press ENTER.

A message appears indicating that redirection was not successful.

This is because the domain functional level is not at least Windows Server 2003.

3. Type **redirusr.exe "ou=User Accounts,dc=tailspintoys,dc=com"** and press ENTER.

A message appears indicating that redirection was not successful.

This is because the domain functional level is not at least Windows Server 2003.

► **Task 4: Raise the domain functional level to Windows Server 2003**

1. Switch to Active Directory Domains and Trusts.
2. In the console tree, right-click the **tailspintoys.com** domain, and then click **Raise Domain Functional Level**.
3. In the **Select an available domain functional level** list, select **Windows Server 2003**.
4. Click **Raise**.
A message appears to remind you that the action cannot be reversed.
5. Click **OK** to confirm your change.
A message appears informing you that the functional level was raised successfully.
6. Click **OK**.

► **Task 5: Verify functionality supported by the Windows Server 2003 domain functional level**

1. Switch to the Command Prompt.
2. Type **redircmp.exe "ou=Client Computers,dc=tailspintoys,dc=com"** and press ENTER.
A message appears indicating that redirection was successful.
3. Type **redirusr.exe "ou=User Accounts,dc=tailspintoys,dc=com"** and press ENTER.
A message appears indicating that redirection was successful.

Exercise 2: Raise the Forest Functional Level to Windows Server 2003

► Task 1: Confirm that the current forest functional level is Windows 2000 Native

1. Switch to Active Directory Domains and Trusts.
2. In the console tree, right-click the root node, **Active Directory Domains and Trusts**, and then click **Raise Forest Functional Level**.
The Raise Forest Functional Level dialog box appears.
3. Confirm that the **Current forest functional level** is **Windows 2000 Native**.
4. Click **Cancel**. Do not make any change to the forest functional level.

► Task 2: Experience functionality not supported by the Windows 2000 Native forest functional level

1. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Sara.Davis_Admin** with the password **Pa\$\$w0rd**.
2. In the console tree, expand the **Tailspintoys.com** domain, and then click the **Domain Controllers** OU.
3. Right-click the **Domain Controllers** OU, and then click **Pre-create Read-only Domain Controller account**.

The Active Directory Domain Services Installation Wizard appears.

4. Click **Next**.
5. On the **Operating System Compatibility** page, click **Next**.
6. On the **Network Credentials** page, click **Next**.

A message appears informing you that the forest functional level must be Windows Server 2003 or higher.

7. Click **OK**.
8. Click **Cancel** to close the Active Directory Domain Services Installation Wizard.

A confirmation message appears, asking you if you want to quit the wizard.

9. Click **Yes**.

► **Task 3: Raise the forest functional level to Windows Server 2003**

1. Switch to Active Directory Domains and Trusts.
2. In the console tree, right-click the root node, **Active Directory Domains and Trusts**, and then click **Raise Forest Functional Level**.
3. In the **Select an available forest functional level** list, select **Windows Server 2003**.
4. Click **Raise**.
A message appears to remind you that the action cannot be reversed.
5. Click **OK** to confirm your change.
A message appears informing you that the functional level was raised successfully.
6. Click **OK**.

► **Task 4: Verify functionality supported by the Windows Server 2003 forest functional level**

1. Switch to Active Directory Users and Computers.
2. Right-click the **Domain Controllers** OU, and then click **Pre-create Read-only Domain Controller account**.
The Active Directory Domain Services Installation Wizard appears.
3. Click **Next**.
4. On the **Operating System Compatibility** page, click **Next**.
5. On the **Network Credentials** page, click **Next**.
6. On the **Specify the Computer Name** page, type **TSTDC03**, and then click **Next**.
7. On the **Select a Site** page, click **Next**.
8. On the **Additional Domain Controller Options** page, click **Next**.

9. On the **Delegation of RODC Installation and Administration** page, click **Next**.
10. On the **Summary** page, click **Next**.
11. Click **Finish**.

A staged RODC object named **TSTDC03** is created in the **Domain Controllers** OU.

Exercise 3: Raise the Domain Functional Level to Windows Server 2008

► **Task 1: Confirm that the current domain functional level is lower than Windows Server 2008.**

1. Switch to Active Directory Domains and Trusts.
2. In the console tree, right-click the **tailspintoys.com** domain, and then click **Raise Domain Functional Level**.
The Raise Domain Functional Level dialog box appears.
3. Confirm that the **Current domain functional level** is **Windows Server 2003**.
4. Click **Cancel**. Do not make any change to the domain functional level.

► **Task 2: Confirm that DFS-R replication is not available at domain functional levels lower than Windows Server 2008**

1. Run the Command Prompt with administrative credentials. Use the account **Sara.Davis_Admin** with the password **Pa\$\$w0rd**.
2. Type **dfsrmig /getglobalstate** and then press ENTER.
A message appears informing you that dfsrmig is supported only on domains at the Windows Server 2008 functional level.

► **Task 3: Raise the domain functional level**

1. Switch to Active Directory Domains and Trusts.
2. In the console tree, right-click the **tailspintoys.com** domain, and then click **Raise Domain Functional Level**.
3. Confirm that the **Select an available domain functional level** list indicates **Windows Server 2008**.
4. Click **Raise**.

A message appears to remind you that the action cannot be reversed.

5. Click **OK** to confirm your change.

A message appears informing you that the functional level was raised successfully.

6. Click **OK**.
7. Close Active Directory Domains and Trusts.

► **Task 4: Confirm that DFS-R replication is available at the Windows Server 2008 domain functional level**

1. Switch to the command prompt.
2. Type **dfsrmig /getglobalstate** and then press ENTER.

A message appears informing you that DFS-R migration has not yet been initialized. This indicates that the feature is now available, but has not yet been initialized.



Note: Do not shut down the virtual machines once you are finished with this lab as the settings you have configured here will be used in subsequent labs.

Lab Review Questions

Question: Can you raise the domain functional level to Windows Server 2008 when your Microsoft Exchange server is still running Windows Server 2003?

Answer: Yes. As long as the Exchange server is not a domain controller. All that matters when determining the domain functional level is the operating system of the domain controller.

Question: Can you raise the domain functional level of a domain to Windows Server 2008 when other domains contain domain controllers running Windows Server 2003?

Answer: Yes. Domain functional levels within a forest can be different.

Lab B: Administer a Trust Relationship

► Log on to a virtual machine

Unless otherwise instructed, use the following steps to log on to a virtual machine.

1. Press ALT+DELETE.

This sends the secure key sequence (CTRL+ALT+DELETE) to the virtual machine. If you press CTRL+ALT+DELETE, you send the secure key sequence to the host operating system.

2. Click **Switch User**.
3. Click **Other User**.
4. In **User name**, type the user name.
5. In **Password**, type the password.
6. Press ENTER or click the log on arrow.

The Windows desktop appears.

► Run an application with administrative credentials

1. Right-click the application, and then click **Run as administrator**.

A User Account Control (UAC) dialog box appears.

2. The **UAC** dialog box will display one of three options. Do the steps based on the option you see:

If the UAC dialog box prompts you to continue or cancel:

- Click **Continue**.

If the UAC dialog box gives you the option to *Use another account*:

1. Click **Use Another Account**.
2. In **User Name**, type the user name.
3. In **Password**, type the password.
4. Press ENTER or click **OK**.

If the UAC dialog box does not give you the option to use another account, and prompts you for a user name and password:

1. In **User Name**, type the user name.
2. In **Password**, type the password.
3. Press ENTER or click **OK**.

Exercise 1: Configure DNS

► Task 1: Prepare for the lab

1. Start 6425B-HQDC01-A.
2. Log on to HQDC01 as **Pat.Coleman** with the password **Pa\$\$w0rd**.
3. Start 6425B-TSTDC01-A.
4. Log on to TSTDC01 as **Sara.Davis** with the password **Pa\$\$w0rd**.

► Task 2: Configure DNS in contoso.com

1. Switch to HQDC01.
2. Run DNS Management with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
3. In the console tree, expand **HQDC01**, and then click **Forward Lookup Zones**.
4. Right-click **Forward Lookup Zones**, and then click **New Zone**.
The Welcome to the New Zone Wizard page appears.
5. Click **Next**.
The Zone Type page appears.
6. Click **Stub Zone**, and then click **Next**.
The Active Directory Zone Replication Scope page appears.
7. Click **Next**.
The Zone Name page appears.
8. Type **tailspintoys.com**, and then click **Next**.
The Master DNS Servers page appears.
9. Type **10.0.0.31** and press **Tab**.
10. Select the **Use the above servers to create a local list of master servers** check box.
11. Click **Next**, and then click **Finish**.

► **Task 3: Configure DNS in tailspintoys.com**

1. Switch to TSTDC01.
2. Run **DNS Management** with administrative credentials. Use the account **Sara.Davis_Admin** with the password **Pa\$\$w0rd**.
3. In the console tree, expand **TSTDC01**, and then click **Conditional Forwarders**.
4. Right-click the **Conditional Forwarders** folder, and then click **New Conditional Forwarder**.
5. In the **DNS Domain** box, type **contoso.com**.
6. Click **Click here to add an IP** and type **10.0.0.11**.
7. Select the **Store this conditional forwarder in Active Directory, and replicate it as follows** check box.
8. Click **OK**.

Exercise 2: Create a Trust Relationship

► Task 1: Identify the trusted and trusting domains

Users in tailspintoys.com require access to a shared folder in contoso.com. Answer the following questions:

Questions:

- Which domain is the trusting domain, and which is the trusted domain?
- Which domain has an outgoing trust, and which has an incoming trust?

Answer:

- The contoso.com domain is the trusting domain with an outgoing trust to the tailspintoys.com domain, which is the trusted domain with an incoming trust.

► Task 2: Initiate the trust in the trusted domain

1. Switch to HQDC01.
2. Run **Active Directory Domains and Trusts** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.
3. In the console tree, right-click the **contoso.com** domain, and then click **Properties**.
4. Click the **Trusts** tab.
5. Click **New Trust**.

The Welcome to the New Trust Wizard page appears.

6. Click **Next**.

The Trust Name page appears.

7. In the **Name** box, type **tailspintoys.com**, and then click **Next**.

The Trust Type page appears.

8. Click **External Trust**. Click **Next**.

The Direction of Trust page appears.

9. Click **One-way: Outgoing**. Click **Next**.

The Sides of Trust page appears.

10. Click **This Domain Only**. Click **Next**.

The Outgoing Trust Authentication Level page appears.

11. Click **Domain-wide authentication**. Click **Next**.

The Trust Password page appears.

12. Type **Pa\$\$w0rd** in both the **Trust password** and **Confirm trust password** boxes.

In a production environment, you should use a complex password that is unique. It should not be the password of a user account.

13. Click **Next**.

The Trust Selections Complete page appears.

14. Review the settings. Click **Next**.

The Trust Creation Complete page appears.

15. Review the status of changes. Click **Next**.

The Confirm Outgoing Trust page appears. You should not confirm the trust until both sides of the trust have been created.

16. Click **Next**.

The Completing the New Trust Wizard page appears.

17. Click **Finish**.

A dialog box appears to remind you that SID filtering is enabled by default.

18. Click **OK**.

19. Click **OK** to close the **contoso.com Properties** dialog box.

► Task 3: Complete the trust in the trusting domain

1. Switch to TSTDC01.
2. Run **Active Directory Domains and Trusts** with administrative credentials. Use the account **Sara.Davis_Admin** with the password **Pa\$\$w0rd**.
3. In the console tree, right-click the **tailspintoys.com** domain, and then click **Properties**.
4. Click the **Trusts** tab.

5. Click **New Trusts**.
The Welcome to the New Trust Wizard page appears.
6. Click **Next**.
The Trust Name page appears.
7. In the **Name** box, type **contoso.com**. Click **Next**.
The Trust Type page appears.
8. Click **External Trust**. Click **Next**.
The Direction of Trust page appears.
9. Click **One-way: Incoming**. Click **Next**.
The Sides of Trust page appears.
10. Click **This Domain Only**. Click **Next**.
The Trust Password page appears.
11. Type **Pa\$\$w0rd** in the **Trust Password** and **Confirm Trust Password** boxes.
Click **Next**.
The Trust Selections Complete page appears.
12. Click **Next**.
The Trust Creation Complete page appears.
13. Review the status of changes. Click **Next**.
The Confirm Incoming Trust page appears.
You will validate the trust in the next exercise.
14. Click **Next**.
The Completing The New Trust Wizard page appears.
15. Click **Finish**.
16. Click **OK** to close the **tailspintoys.com Properties** dialog box.

Exercise 3: Validate a Trust Relationship

► Task 1: Validate a trust relationship

1. Switch to HQDC01.
2. In the console tree of **Active Directory Domains and Trusts**, right-click the **contoso.com** domain, and then click **Properties**.
3. Click the **Trusts** tab.
4. Click **tailspintoys.com**, and then click **Properties**.
5. Click **Validate**.
A message appears indicating that the trust has been validated and that it is in place and active.
6. Click **OK**.
7. Click **OK** twice to close the **Properties** dialog boxes.

Exercise 4: Assign Permissions to Trusted Identities

► Task 1: Assign permissions to trusted groups

1. Switch to TSTDC01.
2. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Sara.Davis_Admin** with the password **Pa\$\$w0rd**.
3. In the console tree, expand the **tailspintoys.com** domain, and then click the **User Accounts** OU.
4. Right-click **User Accounts**, then point to **New**, and then click **User**.
5. In **First Name**, type **Pat**.
6. In **Last Name**, type **Coleman**.
7. In **User logon name**, type **Pat.Coleman**.
8. Click **Next**.
9. In **Password** and **Confirm password**, type **Pa\$\$w0rd**.
10. Clear the **User must change password at next logon** check box.
11. Click **Next**.
12. Click **Finish**.
13. In the console tree, right-click the **tailspintoys.com** domain, then point to **New**, and then click **Organizational Unit**.
The New Object - Organizational Unit dialog box appears.
14. In the **Name** box, type **Groups**.
15. Click **OK**.
16. In the console tree, right-click the **Groups** OU, then point to **New**, and then click **Group**.
The New Object - Group dialog box appears.
17. In **Group name**, type **Product Team**.
18. Click **OK**.
19. Switch to HQDC01.
20. Run **Active Directory Users and Computers** with administrative credentials. Use the account **Pat.Coleman_Admin** with the password **Pa\$\$w0rd**.

21. In the console tree, expand the **contoso.com** domain, and the **Groups** OU, and then click the **Role** OU.
22. Right-click the **Role** OU, then point to **New**, and then click **Group**.
The New Object - Group dialog box appears.
23. In **Group name**, type **Product Developers**.
24. Click **OK**.
25. In the console tree, click the **Access** OU.
26. Right-click the **Access** OU, then point to **New**, and then click **Group**.
The New Object - Group dialog box appears.
27. In **Group name**, type **ACL_Product Information_Modify**.
28. In the **Group scope** section, click **Domain local**.
29. Click **OK**.
30. Open drive C.
31. Create a new folder named **Product Information** on drive C.
32. Right-click the **Product Information** folder, and then click **Properties**.
The Product Information Properties dialog box appears.
33. Click the **Security** tab.
34. Click **Edit**.
35. Click **Add**.
36. Type **ACL_Product Information_Modify**, and then press ENTER.
37. Select the check box below **Allow** and next to **Modify**.
38. Click **OK** twice to close the dialog boxes.
39. Switch to Active Directory Users and Computers.
40. In the details pane, double-click **ACL_Product Information_Modify**.
41. Click the **Members** tab.
42. Click **Add**.
43. Type **Product Developers**, and then press ENTER.
44. Click **Add**.

45. Type **TAILSPINTOYS\Product Team**, and then press ENTER.

A Windows Security dialog box appears.

Your account that is an administrator of contoso.com (Pat.Coleman_Admin) does not have permissions to read the directory of the tailspintoys.com domain.

You must have an account in tailspintoys.com to read its directory. If the trust were a two-way trust, this message would not have appeared.

Your standard user account in the tailspintoys.com domain will be used to provide you Read Access to the directory service.

46. In the **User Name** box, type **TAILSPINTOYS\Pat.Coleman**.

47. In the **Password** box, type **Pa\$\$w0rd**, and then click **OK**.

Note that the two global groups from the two domains are now members of the domain local group in the contoso.com domain that has access to the Product Information folder.

48. Click **OK** to close the group properties dialog box.

Exercise 5: Implement Selective Authentication

► Task 1: Implement selective authentication

1. On HQDC01, switch to **Active Directory Domains and Trusts**.
2. Right-click the **contoso.com** domain, and then click **Properties**.
3. Click the **Trusts** tab.
4. Click **tailspintoys.com**, and then click **Properties**.
5. Click the **Authentication** tab.
6. Click the **Selective Authentication** option, and then click **OK** twice.

With selective authentication enabled, users from a trusted domain cannot authenticate against computers in the trusting domain, even if they've been given permissions to a folder. Trusted users must also be given the Allowed To Authenticate permission on the computer itself.
7. Switch to **Active Directory Users and Computers**.
8. Click the **View** menu and ensure that **Advanced Features** is selected.
9. In the console tree, click the **Domain Controllers** OU.
10. In the details pane, right-click **HQDC01**, and then click **Properties**.
11. Click the **Security** tab.
12. Click **Add**.
13. Type **TAILSPINTOYS\Product Team** and click **OK**.

A Windows Security dialog box appears.

Your account that is an administrator of contoso.com (Pat.Coleman_Admin) does not have permissions to read the directory of the tailspintoys.com domain.

You must have an account in tailspintoys.com to read its directory. If the trust were a two-way trust, this message would not have appeared.

Your standard user account in the tailspintoys.com domain will be used to provide you Read Access to the directory service.
14. In the **User Name** box, type **TAILSPINTOYS\Pat.Coleman**.
15. In the **Password** box, type **Pa\$\$w0rd**, and then click **OK**.

16. Select the check box below **Allow** next to **Allowed to authenticate**.

Now, the Product Team from Tailspintoys.com can authenticate to HQDC01 and has been given permission to the Product Information folder through its membership in the ACL_Product Information_Modify group.

17. Click **OK**.



Note: After completing this exercise, turn off all virtual machines and discard undo disks.

Lab Review Questions

Question: You have given the Research and Development group from Tailspin Toys Modify permission to the Product Information folder on HQDC01. However, of the ten users in the group, only one user (who happens to also be a member of the Product Team group) has access. The others cannot access the folder. What must be done?

Answer: Because selective authentication is enabled, the users in the Research and Development group must be given Allowed to Authenticate permission to HQDC01. The Product Team group already had that permission, which is why one user was able to authenticate and then to access the folder.

Question: A user from Contoso attempts to access a shared folder in the Tailspin Toys domain, and receives an Access Denied error. What must be done to provide access to the user?

Answer: A trust relationship must be established in which Tailspin Toys trusts Contoso, then the user (or a group to which the user belongs) must be given permission to the shared folder in the Tailspin Toys domain.