Microsoft

OFFICIAL MICROSOFT LEARNING PRODUCT

28742A

Windows Server 2016 的身份管理

Companion Content

Product Number: 28742A

Released: 09/2016

Insert EULA pdf in final pdf here

Module 1

Installing and configuring domain controllers

Contents:

Lesson 1

Overview of AD DS

Contents:

Question and Answers

Question: What are the two main purposes of OUs?

> **Answer:** The two main purposes of OUs are to provide a framework for the delegation of administration and to provide a structure that enables targeted GPO deployment.

Question: Why would you need to deploy an additional tree in the AD DS forest?

> **Answer:** You would deploy an additional tree in the AD DS forest if you needed more than one Domain Name System (DNS) namespace.

Resources

Additional Reading: For more information on domains and forests, refer to: "Active Directory Domain Services Overview" at: http://aka.ms/M2lr5a

What is new in AD DS in Windows Server 2016?

Additional Reading: For more information on PAM, refer to: "Privileged Access Management for Active Directory Domain Services (AD DS)" at: http://aka.ms/Ibsyai

Additional Reading: For more information on Azure AD Join, refer to: "Windows 10 for enterprise: Ways to use devices for work" at: http://aka.ms/F7dfxe

Additional Reading: For more information on using Microsoft Passport with AD DS in Windows Server 2016, refer to: "Authenticating identities without passwords through Microsoft Passport" at: http://aka.ms/Nyrund

Additional Reading: For more information on the new AD DS features in Windows Server 2016, refer to: "What's new in Active Directory Domain Services Technical Preview" at: http://aka.ms/Nzrl6u

Demonstration: Using the Active Directory Administrative Center to administer and manage AD DS

Demonstration Steps

Navigate within the Active Directory Administrative Center

1. On **LON-DC1**, in Server Manager, click **Tools**, and then click **Active Directory Administrative Center**.
2. Click **Adatum (local)**
3. Click **Dynamic Access Control**
4. Click **Global Search**.
5. In the navigation pane, click the **Tree View** tab, and then expand the **Adatum (local)** node to view the details of the Adatum.com domain.

Perform an administrative task within the Active Directory Administrative Center

1. In the Active Directory Administrative Center, click **Overview**.
2. In the **Reset Password** box, in the **User name** box, type **Adatum\Adam**.
3. In the **Password** and **Confirm password** boxes, type **Pa$$w0rd**.
4. Clear the **User must change password at next log on** check box, and then click **Apply**.

5. In the **Global Search** box, in the **Search** box, type **lon**, and then press Enter.

Create an object

1. In the Active Directory Administrative Center, in the navigation pane tree view, expand **Adatum (local)**, and then click the **Computers** container.
2. In the **Tasks** pane, in the **Computers** section, click **New**, and then select **Computer**.
3. In the **Create Computer** dialog box, enter the following information, and then click **OK**:
   - Computer name: **LON-CL4**
   - Computer (NetBIOS) name: **LON-CL4**
4. Click **OK**.

View all object attributes

1. In the Active Directory Administrative Center, double-click **Adatum (local)**, and then in the management list, double-click **Computers**.
2. Select **LON-CL4**, and then in the **Tasks** pane, in the **LON-CL4** section, click **Properties**.
3. In the **LON-CL4 properties** window, scroll down to the **Extensions** section, click the **Attribute Editor** tab, and then note that all the attributes of the computer object are available here.
4. Click **Cancel** to close the **LON-CL4 properties** window.

Use the Windows PowerShell History viewer

1. In the Active Directory Administrative Center, click the **Windows PowerShell History** toolbar in the lower part of the screen.
2. View the details for the **New-ADComputer** cmdlet that was used to perform the most recent task.
3. On **LON-DC1**, close all open windows.

Lesson 2

Overview of AD DS domain controllers

Contents:

Question and Answers

Question: Should a domain controller be a global catalog?

Answer: Global catalog placement affects how long a user takes to sign in. Therefore, you must carefully plan global catalog placement. In a single-domain environment, every domain controller should host the global catalog, because every domain controller already holds a complete copy of the domain. In a multiple-domain scenario, you need to consider user sign-in times, program dependencies, the need for high availability of the global catalog, and replication traffic when planning global catalog placement.

Question: In a multiple-domain forest, a copy of the global catalog should be stored on every domain controller.

( ) True

( ) False

Answer:

( ) True

(√) False

Feedback:

In a single domain, all domain controllers should be configured to hold a copy of the global catalog. However, in a multiple-domain environment, the infrastructure master should not be a global catalog server unless all the domain controllers in the domain are also global catalog servers.

Resources

Transferring and seizing roles

Additional Reading:

- For more information on using Windows PowerShell to transfer or seize FSMO roles, refer to: "Move (Transferring or Seizing) FSMO Roles with AD-Powershell Command to Another Domain Controller" at: http://aka.ms/Rn7kfi
- For information on using ntdsutil.exe to transfer or seize FSMO roles, refer to: "Using Ntdsutil.exe to transfer or seize FSMO roles to a domain controller" at: http://aka.ms/Npye86

Demonstration: Viewing the SRV records in DNS

Demonstration Steps

View the SRV records by using DNS Manager

1. On **LON-DC1**, sign in with the user name **Adatum\Administrator** and the password **Pa$$w0rd**.
2. In **Server Manager**, click the **Tools** menu.
3. In the **Tools** list, click **DNS**.
4. In the **DNS Manager** window, on the tree menu, expand **LON-DC1,** expand **Forward Lookup Zones,** and then click **Adatum.com**. Show the following four DNS subzones:
   - **_msdcs**
   - **_sites**

- **_tcp**
- **_udp**

5. Expand **Adatum.com**, expand **_sites**, expand **Default-First-Site-Name**, expand **_tcp**, and then select the following record:
   - **_ldap Service Location (SRV) [0][100][389] lon-dc1.adatum.com**
6. If the students have sufficient expertise and interest, open **c:\windows\system32\config**, and then open the **netlogon.dns** file in Microsoft Notepad. Show all the service records (SRV records) that this domain controller will register in DNS.

Lesson 3

Deploying a domain controller

Contents:

Question and Answers

Question: What is the fastest way to replicate domain controllers in a virtualized environment?

Answer: Cloning

Feedback: The fastest way to deploy multiple computers that are identically configured, especially when those computers run in a virtualized environment such as Hyper-V, is to clone those computers. Cloning means that the virtual hard disks of the computers are copied, and minor configurations such as computer names and IP addresses are changed to be unique. Then the computers are instantly operational.

Question: What are the two major considerations for deploying domain controllers to Azure?

Answer: The two major considerations are rollback and virtual machine limitations.

Feedback:

- Rollback. When an AD DS system is rolled back, duplicate update sequence numbers (USNs) can be created, and because domain controller replication depends on USNs, duplicate numbers can cause problems. To prevent this, Windows Server 2016 Active Directory has an identifier named VM-Generation ID. VM-Generation ID can detect a rollback, and it prevents the virtualized domain controller from replicating changes outbound until the virtualized AD DS has converged with the other domain controllers in the domain.
- Virtual machine limitations. Azure virtual machines are limited to 14 gigabytes (GB) of random access memory (RAM) and one network adapter. Also, the checkpoint feature is not supported.

Resources

Installing a domain controller on a Server Core installation of Windows Server 2016

Additional Reading:

- For more information on using the Windows PowerShell cmdlet **Install-ADDSDomainController**, refer to: "Install Active Directory Domain Services (Level 100)" at: http://aka.ms/A9jlvk
- For more information, refer to: "AD DS Deployment Cmdlets in Windows PowerShell" at: http://aka.ms/Lnxifx

Installing a domain controller by installing from media

Additional Reading: For more information on the steps required to install AD DS, refer to: "Install Active Directory Domain Services (Level 100)" at: http://aka.ms/Rvcwlz

Best practices for domain controller virtualization

Additional Reading: For more information on virtualizing domain controllers, refer to: "Running Domain Controllers in Hyper-V" at: http://aka.ms/Tjjl9g

Demonstration: Cloning a domain controller

Demonstration Steps

Prepare a source domain controller to be cloned

1. On **LON-DC1**, In **Server Manager**, click **Tools**, and then click **Active Directory Administrative Center**.
2. In the **Active Directory Administrative Center**, double-click **Adatum (local)**, and then in the management list, double-click the **Domain Controllers** OU.
3. In the management list, select **LON-DC1**, if it is not already selected, and then in the **Tasks** pane, in the **LON-DC1** section, click **Add to group**.
4. In the **Select Groups** dialog box, in the **Enter the object names to select** box, type **Cloneable**, and then click **Check Names**.
5. Ensure that the group name is expanded to **Cloneable Domain Controllers**, and then click **OK**.
6. On Start menu, click **Windows PowerShell**.
7. At the Windows PowerShell command prompt, type the following command, and then press Enter.

```
Get-ADDCCloningExcludedApplicationList
```

8. Verify the list of critical apps. In production, you need to verify each app or use a domain controller that has fewer apps installed by default. Type the following command, and then press Enter.

```
Get-ADDCCloningExcludedApplicationList –GenerateXML
```

9. Type the following command to create the DCCloneConfig.xml file, and then press Enter.

```
New-ADDCCloneConfigFile
```

10. Type the following command to shut down LON-DC1, and then press Enter.

```
Stop-Computer
```

11. Wait for the virtual machine to shut down. You might be asked to confirm the shutdown.

Export the source virtual machine

1. On the host computer, in Microsoft Hyper-V Manager, in the details pane, select the **28742A-LON-DC1** virtual machine.
2. In the **Actions** pane, in the **28742A-LON-DC1** section, click **Export**.
3. In the **Export Virtual Machine** dialog box, go to the location **D:\Program Files\Microsoft Learning\28742**, and then click **Export**. Wait until the export finishes.
4. In the **Actions** pane, in the **28742-LON-DC1** section, click **Start**.

Create and start the cloned domain controller

1. On the host computer, in Hyper-V Manager, in the **Actions** pane, in the section that is named for the host computer, click **Import Virtual Machine**.
2. In the Import Virtual Machine Wizard, on the **Before You Begin** page, click **Next**.
3. On the **Locate Folder** page, click **Browse**, go to the folder **D:\Program Files\Microsoft Learning\28742\28742A-LON-DC1**, click **Select Folder**, and then click **Next**.

4. On the **Select Virtual Machine** page, select **28742A-LON-DC1** (if it is not already selected), and then click **Next**.
5. On the **Choose Import Type** page, select **Copy the virtual machine (create a new unique ID)**, and then click **Next**.
6. On the **Choose Folders for Virtual Machine Files** page, select the **Store the virtual machine in a different location** check box. For each folder location, specify **D:\Program Files\Microsoft Learning\28742** as the path. Click **Next**.
7. On the **Choose Folders to Store Virtual Hard Disks** page, provide the path **D:\Program Files\Microsoft Learning\28742**, and then click **Next**.
8. On the **Completing Import Wizard** page, click **Finish**.
9. In the management list, identify and select the newly imported virtual machine named **28742A-LON-DC1**, which has the **State** shown as **Off**. In the lower section of the **Actions** pane, click **Rename**.
10. Type **28742A-LON-DC3** as the name, and then press Enter.
11. In the **Actions** pane, in the **28742A-LON-DC3** section, click **Start**, and then click **Connect** to see the virtual machine starting.
12. While the server is starting, you may see the message **Domain Controller cloning is at** x**% completion**.

Module Review and Takeaways

Review Questions

Question: Which deployment method would you use if you had to install an additional domain controller in a remote location that had a limited WAN connection?

> **Answer:** You would use the **Install from media** option, because it eliminates the need to copy the entire AD DS database over the WAN link.

Question: If you need to promote a Server Core installation of Windows Server 2016 to be a domain controller, which tool or tools can you use?

> **Answer:** To promote a Server Core installation of Windows Server 2016 to a domain controller, you can use the following tools:
>
> - Server Manager, which allows you to remotely install AD DS
> - Windows PowerShell
> - The command **dcpromo /unattend**, which you run on the server running the Server Core installation

Question: If you want to run a domain controller in the cloud, which service should you consider using: Azure AD or Infrastructure as a Service (IaaS) Azure virtual machines?

> **Answer:** Answers will vary depending on the students' needs. Azure AD is designed to provide identity and access management for web-based applications. Using IaaS Azure virtual machines allows you to deploy a full-featured AD DS domain controller.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Syntax errors	Syntax errors often result from mistyping or forgetting a parameter when typing Windows PowerShell cmdlets. Examine the console output for specifics about why a particular command failed.
Prerequisite problems	Many fatal errors are directly related to errors that the prerequisite checker finds. Be sure to carefully examine the results and follow any guidance provided.
Network and forest configuration problems	Network configuration problems or other AD DS forest configuration issues might prevent the promotion of new domain controllers. Use the dcpromoui.log and dcpromo.log files to view specific promotion errors or the event log for errors that indicate configuration issues. You can also use dcdiag.exe and repadmin.exe to check overall forest health.

Module 2

Managing objects in AD DS

Contents:

Lesson 1

Managing user accounts

Contents:

Question and Answers

Question: What is the purpose of a roaming profile?

> **Answer:** It stores and synchronizes the user profile to a network share. This allows the user to roam between computers and still receive the same profile when they sign on to a new computer.

Question: What is the difference between disabling an account and an account being locked out?

> **Answer:** Disabling an account is an intentional act by an administrator to prevent the use of an account. An account lockout can only be the result of too many bad logon attempts (assuming that the password policy is configured enforce that).

Demonstration: Managing user accounts

Demonstration Steps

Create a new user account

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **Active Directory Administrative Center**.
2. In Active Directory Administrative Center, click **Adatum (local)**, and then double-click **Managers**.
3. In the **Action** pane, click **New**, and then click **User**.
4. In the **Create User** dialog box, in the **First name** field, type **Sales**.
5. In the **Last name** field, type **Manager**.
6. In the **User UPN logon** text box, type **SalesManager**.
7. In the **Password** and **Confirm password** fields, type **Pa$$w0rd**, and then click **OK**.

Delete a user account

1. Click the **Art Odum** account.
2. In the **Action** pane, click **Delete**.
3. In the **Delete Confirmation** box, click **Yes**.

Move a user account

1. Click the Burton Bartels account.
2. In the Action pane, click Move…
3. Click the Development OU, and then click OK.
4. In the left pane, click **Adatum (local)**.
5. In the right pane, double-click the **Development** OU and ensure that the Burton Bartels account is present.

Configure user attributes

1. Double-click the Burton Bartels account.
2. In the left pane, click Organization, and then change the Department field from Managers to Development.
3. Click Member Of in the left pane.
4. In the Member Of section, click Managers, and then click Remove.
5. Click Add. In the Select Groups dialog box in the Enter the object names to select (example): window, type Development, and then click OK.

6. Click OK to close the Burton Bartels properties.
7. Close **Active Directory Administrative Center**. Leave Server Manager open for the next demonstration.

Demonstration: Using templates to manage accounts

Demonstration Steps

Create a user template

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **Active Directory Users and Computers**.
2. Expand **Adatum.com**, and then click the **Sales** OU.
3. Click the new user icon on the toolbar.
4. In the **New Object – User** dialog box, enter the following information, and then click **Next**:
   - First name: **_sales**
   - Last name: **template**
   - User logon name: **salestemplate**
5. In the **Password** and **Confirm password** fields, type **Pa$$w0rd**.
6. Clear the **User must change password at next logon** check box, select the **Password never expires** check box, select the **Account is disabled** check box, and then click **Next**.
7. Click **Finish**.

Configure template properties

1. Double-click the **_sales template** account.
2. In the **_sales template properties** dialog box, click the **Member Of** tab, and then click **Add**.
3. In the **Select Groups** dialog box, type **Sales**, and then click **OK.**
4. Click the **Organization** tab. In the **Department** field, type **Sales**.
5. In the **Manager** section, click **Change**. In the **Select User or Contact** dialog box, type **Erin**, and then click **Check Names**. Click **OK**.
6. Click the **Profile** tab. In the **User profile** section, in the **Logon script** field, type **\\lon-dc1\netlogon\logon.bat**, and then click **OK**.

Create a new user by copying the template

1. Right-click the **_sales template** account, and then click **Copy**.
2. In the **Copy Object – User** dialog box, type **Sales** in the **First name** field. Type **User** in the **Last name** field.
3. Type **salesuser** in the **User logon name** field, and then click **Next**.
4. In the **Password** and **Confirm password** fields, type **Pa$$w0rd**.
5. Clear the **Password never expires** check box, clear the **Account is disabled** check box, select the **User must change password at next logon** check box, and then click **Next**.
6. Click **Finish**.
7. Double-click the **Sales User** account, and then click the **Member Of** tab. Ensure that the user is a member of the Sales group.

8. Click the **Organization** tab. Ensure that the Department is Sales and the Manager is Erin Bull.
9. Click the **Profile** tab. Ensure that the Logon script path is \\lon-dc1\netlogon\logon.bat. Click **OK** to close the dialog box**.**
10. Close **Active Directory Users and Computers**.

Lesson 2

Managing groups in AD DS

Contents:

Demonstration: Managing groups in Windows Server

Demonstration Steps

Create a new group and add members

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **Active Directory Administrative Center**.
2. Expand **Adatum (Local)**, and then double-click **IT**.
3. In the **Tasks** list, under **IT**, point to **New**, and then click **Group**.
4. In the **Create Group** dialog box, in the **Group name** field, type **IT Managers**. Notice that the default is a global security group.
5. In the left pane, click **Members**, and then click **Add**.
6. In the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, in **Enter the object names to select (examples)**, type **Beth; Logan**, click **Check Names**, and then click **OK**.
7. Click **OK** to close the **Create Group: IT Managers** dialog box.

Add a user to the group

1. Right-click the user named **Maj Hojski**, and then click **Add to group**.
2. In the **Select Groups** dialog box, in **Enter the object names to select (examples)**, type **IT Managers**.
3. Click **Check Names**, and then click **OK**.

Change the group type and scope

1. Double-click the **IT Managers** group.
2. In the **IT Managers** window, under **Group type**, click **Distribution**. Read the highlighted message. Under **Group scope**, click **Universal**, and then click **OK**.

Configure a manager for the group

1. Double-click the **IT Managers** group.
2. In the **Managed By** section, click **Edit**.
3. In the **Select User, Contact or Groups** dialog box, in **Enter the object names to select (examples)**, type **Parsa**, click **Check Names**, and then click **OK**.
4. Select the check box beside the **Manager can update membership** list.
5. Click **OK** to close the IT Managers properties.
6. Close **Active Directory Administrative Center**.

Lesson 3

Managing computer objects in AD DS

Contents:

Question and Answers

Question: What causes a computer to lose its trust relationship with the domain?

Answer: Typically, it is the result of a password mismatch between the local computer and what is stored in Active Directory.

Lesson 4

Using Windows PowerShell for AD DS administration

Contents:

Question and Answers

Question: What is Windows PowerShell Integrated Scripting Environment?

> **Answer:** Windows PowerShell Integrated Scripting Environment provides an environment to write, run, and test Windows PowerShell scripts. It provides syntax-coloring, tab completion, visual debugging, and context-sensitive Help that is not available in the standard Windows PowerShell window.

Resources

Querying objects with Windows PowerShell

 **Additional Reading:** For more information, refer to about_ActiveDirectory_Filter: http://aka.ms/Kv5dy3

 **Additional Reading:** For more information, refer to How to use the UserAccountControl flags to manipulate user account properties: http://aka.ms/Mxt8a1

Modifying objects with Windows PowerShell

 **Additional Reading:** For more information, refer to Set-ADUser: http://aka.ms/K34c8d

Demonstration: Using graphical tools to perform bulk operations

Demonstration Steps

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **Active Directory Users and Computers**.
2. Expand **Adatum.com**, and then click the **Research** OU.
3. In the details pane, click the top of the **Type** column to sort the object by type.
4. Click the **first User object** in the list (this should be **Arturs Prede**).
5. Scroll to the bottom of the list, hold the **Shift** key, and click the last User object in the list (this should be Vera Pace).
6. Right-click the block of selected objects, and then click **Properties**.
7. In the **Properties for Multiple Items** dialog box, select the check box beside **Office**, type **Winnipeg** in the field, and then click **OK**.
8. Double-click any of the user objects and note that the **Office** field is now set to be **Winnipeg**.
9. Click **Cancel**, and then close **Active Directory Users and Computers**.

Demonstration: Performing bulk operations with Windows PowerShell

Demonstration Steps

Create a new global group in the IT department

1. On **LON-DC1**, right-click the **Start** button, click **Run**, type **PowerShell**, and then press Enter.
2. In the **Administrator: Windows PowerShell** window, type the following command, and then press Enter:

```
New-ADGroup -Name Helpdesk -Path "ou=IT,dc=Adatum,dc=com" –GroupScope Global
```

Add all users in the IT department to the Helpdesk group

- In the **Administrator: Windows PowerShell** window, type the following command, and then press Enter:

```
Get-ADUser -Filter "Department -eq 'IT'" | Foreach {Add-ADGroupMember "Helpdesk" -
members $_}
```

Set the address for all users in the Research department

- In the **Administrator: Windows PowerShell** window, type the following command, and then press Enter:

```
Get-ADuser -Filter {Department -eq "Research"} | Set-ADuser -StreetAddress "1530
Taylor Ave." -City "Winnipeg" -State "Manitoba" -Country "CA"
```

 **Note:** Notice that this command filters using brackets rather than quotes and uses the **Set-ADUser** cmdlet rather than a **foreach** loop.

Create a new OU

- In the **Administrator: Windows PowerShell** window, type the following command, and then press Enter:

```
New-ADOrganizationalUnit London -Path "dc=Adatum,dc=com”
```

Run a script to create new users from a .csv file

1. Open File Explorer, type **E:\Labfiles\Mod02** in the address bar, and then press Enter.
2. Right-click **DemoUsers.csv**, click **Open with**, and then click **Notepad**. Explain the structure of the file to students.
3. Close Notepad.
4. Switch back to the **Windows PowerShell** window, and then type **cd E:\Labfiles\Mod02**.
5. To run the script, type **.\DemoUsers.ps1**, and then press Enter.

Verify that the user accounts were created and that the accounts were modified

1. In Server Manager, click **Tools**, and then click **Active Directory Users and Computers**.
2. Ensure that the London OU exists.
3. Click the **London** OU. See that there are three users as defined in the .csv file. Notice that the users' accounts are disabled. This is because there were no passwords provided.
4. Click the **IT** OU. Ensure that the **Helpdesk** group exists.
5. Double-click the **Helpdesk** group, and then in **Helpdesk Properties**, click the **Members** tab. Ensure that the members are populated with the IT department users, and then click **Cancel**.
6. Click the **Research** OU, and then double-click one of the user accounts.
7. In the user's properties page, click the **Address** tab. Ensure that the address fields are filled out as expected, and then click **Cancel**.

Lesson 5

Implementing and managing OUs

Contents:

Question and Answers

Question: What is the advantage of using the **Delegation of Control Wizard**?

> **Answer:** The **Delegation of Control Wizard** can simplify the delegation of administration by assigning permissions based on the selected task.

Demonstration: Delegating administrative permissions on an OU

Demonstration Steps

Create a new OU

1. On LON-DC1, in Active Directory Users and Computers, click **Adatum.com**.
2. Click the New OU icon on the toolbar.
3. In the **New Object – Organizational Unit** dialog box, type **Human Resources** in the **Name** field, and then click **OK**.

Use the Delegation of Control Wizard to assign a task

1. Right-click the **Adatum.com** domain object, and then click **Delegate Control**.
2. In the **Delegation of Control Wizard**, click **Next**.
3. On the **Users or Groups** page, click **Add**.
4. In the **Select Users, Computers, or Groups** dialog box, in **Enter the object names to select (examples)**, type **Helpdesk**, click **Check Names**, click **OK**, and then click **Next**.
5. On the **Tasks to Delegate** page, select the check boxes beside **Reset user passwords and force password change at next logon** and **Join a computer to the domain**, and then click **Next**.
6. Click **Finish**.

Assign the Research group the right to modify user addresses and job titles in the Research OU

1. In Active Directory Users and Computers, click **View**, and then click **Advanced Features**.
2. Right-click the **Research** OU, and then click **Properties**.
3. Click the **Security** tab, click **Advanced**, and then click **Add**.
4. In the **Permission Entry for Research** window, click **Select a principal**.
5. In the **Select Users, Computers, or Groups** dialog box, in **Enter the object names to select (examples)**, type **Research.** Click **Check Names**, and then click **OK**.
6. In the **Applies to** drop-down list box, select **Descendant User objects**. (Hint: it is at the bottom of the list.)
7. In the **Properties** section, scroll down, locate, and select the check box beside **Write Home Address**.
8. Scroll down further, select the check box beside **Write Job Title**, and then click **OK**.
9. Click **OK** to close the **Research Properties** dialog box.

Module Review and Takeaways

Best Practices

Take away the following best practices for AD DS administration:

- Avoid using the built-in groups to delegate administrative access unless you understand all the permissions that the group membership grants.
- Create specialized administrative groups and assign them only the rights and permissions required to complete the tasks assigned.
- Develop Windows PowerShell scripts to perform repetitive tasks.
- Do not sign in with your administrative account for day-to-day activities. Only use it when you need to perform an administrative task.

Real-world Issues and Scenarios

Many organizations will create some user accounts based on job role rather than the user filling the role. For example, the organization will always have a receptionist. To provide continuity, the person filling that role uses a generic account named reception. That way, when a new person fills the position all that is required is to change the password of the reception user. Applications, settings, documents, emails, and so on will stay consistent.

Tools

The following table lists the tools that this module references:

1. Tool	2. Used for	3. Where to find it
Windows PowerShell	Command-line and scripting of all administrative tasks.	Native to the operating system.
Active Directory Administrative Center	Performing day-to-day administrative tasks in AD DS.	In Server Manager, under the **Tools** menu or in **Control Panel** in **Administrative Tools**.
Active Directory Users and Computers	Performing day to day administrative tasks in AD DS.	In Server Manager, under the **Tools** menu or in **Control Panel** in **Administrative Tools**.
Delegation of Control Wizard	Assigning permissions to perform administrative tasks.	Right-click on an OU in Active Directory Users and Computers.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Users are unable to access network resources.	Check group memberships. Look for nested groups that are causing conflicts.
You have assigned a user some administrative rights in AD DS, but he says that he has no tool to perform the task.	You must download and install Remote Server Administration Tools for Windows 10 and then install it on the user's workstation to provide him with the administrative tools that he requires.

Lab Review Questions and Answers

Lab A: Managing AD DS objects

Question and Answers

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

Answer: Users and other roles (global groups) from the same domain are objects that can be members of global groups.

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

Answer: You must provide the credentials of a user who has permission to join computers to the domain. Typically, the credentials of a domain administrator.

Lab B: Administering AD DS

Question and Answers

Question: Why are the users created by this script enabled?

Answer: The script assigns a password to the users when creating them.

Question: What is the status of accounts created by the **New-ADUser** cmdlet?

Answer: By default, those accounts will be disabled if they are not assigned passwords at the time of creation.

Module 3

Advanced AD DS infrastructure management

Contents:

Lesson 1

Overview of advanced AD DS deployments

Contents:

Question and Answers

Question: Which of the following requirements necessitates the implementation of a multiple forest AD DS deployment?

( ) Security isolation requirements

( ) Schema requirements

( ) DNS namespace requirements

( ) Business mergers

( ) Distributed administration requirements

Answer:

(√) Security isolation requirements

(√) Schema requirements

( ) DNS namespace requirements

( ) Business mergers

( ) Distributed administration requirements

Feedback:

Security isolation and schema requirements are the only requirements presented in the above options that require implementation of multiple forests. DNS namespace and distribution administration requirements require multiple domains, but separate forests are not necessary because a single forest can have multiple namespaces and is not necessary for administrative autonomy. In a business merger scenario, you might decide to maintain separate forests if there is little need for collaboration between organizations, but doing so would not be required.

Question: Before you deploy a replica AD DS domain controller on an Azure virtual machine, which of the following requirements must be met?

( ) Create an AD DS site to control replication from your on-premises networks to the Azure Virtual Network.

( ) Add an additional hard disk to the virtual machine that has read and write caching disabled.

( ) Create and configure an Azure Virtual Network.

( ) Manually create required SRV records in an Azure DNS zone for your domain.

( ) Configure the initial dynamic IP address of the virtual machine as static by using the Set-AzureStaticVNetIP cmdlet.

Answer:

( ) Create an AD DS site to control replication from your on-premises networks to the Azure Virtual Network.

(√) Add an additional hard disk to the virtual machine that has read and write caching disabled.

(√) Create and configure an Azure Virtual Network.

( ) Manually create required SRV records in an Azure DNS zone for your domain.

(√) Configure the initial dynamic IP address of the virtual machine as static by using the Set-AzureStaticVNetIP cmdlet.

Feedback:

Although we recommend that you create an AD DS site for tighter control of replication, doing so is not necessary. You should, however, create an additional hard disk on the Azure virtual machine in which caching is disabled. This hard disk should contain the NTDS.DIT file and SYSVOL folder. You must also have already provisioned and correctly configured an Azure Virtual Network and attached the virtual machine to it. Manually creating SRV records in Azure DNS is an incorrect answer, because doing so is not possible. The virtual machine must also have a static IP configured before deploying AD DS to ensure the IP is never changed if the virtual machine is deallocated due to shutdown or service healing actions.

Lesson 2

Deploying a distributed AD DS environment

Contents:

Question and Answers

Question: What is the minimum domain functional level in which you should deploy a Windows Server 2016 AD DS domain controller?

( ) Windows Server 2003

( ) Windows Server 2008

( ) Windows Server 2008 R2

( ) Windows Server 2012 R2

( ) Windows Server 2016

Answer:

( ) Windows Server 2003

(√) Windows Server 2008

( ) Windows Server 2008 R2

( ) Windows Server 2012 R2

( ) Windows Server 2016

Feedback:

Windows Server 2008 is the minimum recommended domain functional level in which you should deploy a Windows Server 2016 AD DS domain controller. Windows Server 2003 is no longer supported. Although the Windows Server 2003 domain/forest functional levels are still supported, you should be at the Windows Server 2008 functional levels in order to ensure SYSVOL folder replication occurs using DFS replication and not the deprecated FRS method used by Windows Server 2003 and earlier. You should remove from the domain any domain controllers still operating on Windows Server 2003 prior to introducing a Windows Server 2016 domain controller.

Question: Which of the following can you use to optimize name resolution across DNS namespaces?

( ) Conditional forwarders

( ) AD DS sites

( ) DNS suffix search order

( ) DNS stub zones

( ) Global catalog servers

Answer:

(√) Conditional forwarders

( ) AD DS sites

(√) DNS suffix search order

(√) DNS stub zones

( ) Global catalog servers

Feedback:

The correct answers are conditional forwarders, DNS stub zones, and DNS suffix search order. Conditional forwarders and DNS stub zones allow you to create shortcuts so that name resolution does not have to traverse up and down a domain tree or across forests. By configuring a DNS suffix search order, clients do not have to rely on DNS devolution to resolve single-label names.

The incorrect answers are AD DS sites and global catalog servers. Although AD DS sites can help you optimize the replication of AD DS-integrated DNS zones, they do not inherently make name resolution more efficient. Global catalog servers are not involved in DNS name resolution.

Resources

AD DS domain functional levels

 **Additional Reading:** For more information on AD DS features in the Windows Server 2016 Technical Preview release, refer to: http://aka.ms/Bxg2z0

 **Additional Reading:** For more information on the AD DS domain functional levels, refer to: http://aka.ms/Ynmvma

Migrating to Windows Server 2016 AD DS from a previous version

 **Additional Reading:** For more information on using ADMT, refer to: http://aka.ms/Jiauyg

Demonstration: Installing a domain controller in a new domain in an existing forest

Demonstration Steps

Install the AD DS binaries on TOR-DC1

1. On TOR-DC1, click **Start**, and then click **Server Manager**. In **Server Manager**, click **Add roles and features**.
2. In the **Add Roles and Features Wizard**, click **Next**.
3. On the **Select installation type** page, ensure that **Role-based or feature-based installation** is selected, and then click **Next**.
4. On the **Select destination server** page, ensure that **Select a server from the server pool** is selected. In the **Server Pool** page, verify that **TOR-DC1.Adatum.com** is highlighted, and then click **Next**.
5. On the **Select server roles** page, select the **Active Directory Domain Services** check box, click **Add Features**, and then click **Next**.
6. On the **Select features** page, click **Next**.
7. On the **Active Directory Domain Services** page, review the message, and then click **Next**.
8. On the **Confirm installation selections** page, review the message, and then click **Install**. Installation will take several minutes.
9. On the **Results** page, click **Promote this server to a domain controller**. The wizard continues.

Configure TOR-DC1 as an AD DS domain controller using the Active Directory Domain Services Configuration Wizard

1. On the **Deployment Configuration** page, select the **Add a new domain to an existing forest** option, and then next to **Select domain type**, confirm that **Child Domain** is selected.
2. In the **Parent domain name** field, verify that **Adatum.com** is listed.
3. In the **New domain name** box, type **NA**, and then click **Next**.

4. On the **Domain Controller Options** page, ensure that **Windows Server Technical Preview** is selected as the **Domain functional level**, that **Domain Name System (DNS) server** is selected, and that **Global Catalog (GC)** is selected.
5. In the **Type the Directory Services Restore Mode (DSRM) password** text boxes, type **Pa$$w0rd** in both boxes, and then click **Next**.
6. On the **DNS Options** page, click **Next**.
7. On the **Additional Options** page, click **Next**. On the **Paths** page, click **Next**. On the **Review Options** page, click **Next**. In the **Prerequisites Check** window, click **Install**.
8. Review the information, and allow TOR-DC1 to restart as an AD DS domain controller in the new AD DS domain that you created in the AD DS forest.
9. Sign in to TOR-DC1 as **NA\Administrator** with the password as **Pa$$w0rd**, and review some of the AD DS tools to confirm the installation of the new domain.

Lesson 3

Configuring AD DS trusts

Contents:

Question and Answers

Question: Which of the following must be in place before you can create a forest trust?

( ) Name resolution between the root domains in each forest

( ) Forest functional level of Windows Server 2003 or higher

( ) Forest functional level of Windows Server 2008 or higher

( ) Forest functional level of Windows Server 2012 or higher

( ) Domain controllers must be enabled for selective authentication.

Answer:

(√) Name resolution between the root domains in each forest

(√) Forest functional level of Windows Server 2003 or higher

( ) Forest functional level of Windows Server 2008 or higher

( ) Forest functional level of Windows Server 2012 or higher

( ) Domain controllers must be enabled for selective authentication.

Feedback:

In order to create a forest trust, you must have configured name resolution between the root domains in each forest. In addition, the forest functional level of each forest must be Windows Server 2003 or higher.

Question: Which AD DS trust setting allows you to control the scope of authentication of trusted security principals?

( ) Name suffix routing

( ) Kerberos constrained delegation (KCD)

( ) Selective authentication

( ) SID filtering

( ) SID-History

Answer:

( ) Name suffix routing

( ) Kerberos constrained delegation (KCD)

(√) Selective authentication

( ) SID filtering

( ) SID-History

Feedback:

Selective authentication allows you to manage the scope of authentication of trusted security principals by allowing authentication for services only on computers that you specify.

Resources

Configuring advanced AD DS trust settings

Additional Reading:

- For more information on configuring SID filter quarantining on external trusts, refer to: http://aka.ms/Sveqfn
- For more information on enabling selective authentication over a forest trust, refer to: http://aka.ms/Blp826
- For more information on name-suffix routing, refer to: http://aka.ms/Egc6g7

Demonstration: Configuring a forest trust

Demonstration Steps

Configure DNS name resolution by using a conditional forwarder

1. On LON-DC1, in **Server Manager**, click the **Tools** menu, and in the drop-down list, click **DNS**. The **DNS Manager** opens.
2. In **DNS Manager**, expand **LON-DC1**, click and then right-click **Conditional Forwarders**, and then click **New Conditional Forwarder**.
3. In the **New Conditional Forwarder** window, in the **DNS Domain** box, type **treyresearch.net**.
4. In the **IP addresses of the master servers:** text box, type **172.16.10.10**. Click in the open space, and then click **OK**. (If an error displays, ignore it.)
5. Close **DNS Manager**.
6. Switch to **TREY-DC1** and repeat steps 1 through 5. Use the domain name **adatum.com** with the IP address **172.16.0.10**.

Configure a two-way selective forest trust

1. In **LON-DC1**, on the **Tools** menu, click **Active Directory Domains and Trusts**.
2. When the **Active Directory Domains and Trusts** window opens, right-click **Adatum.com**, and then click **Properties**.
3. In the **Adatum.com Properties** dialog box, on the **Trusts** tab, click **New Trust**.
4. In the **New Trust Wizard**, click **Next**.
5. On the **Trust Name** page, in the **Name** text box, type **treyresearch.net**, and then click **Next**.
6. In the **New Trust Wizard**, click **Forest trust**, and then click **Next**.
7. In the **Direction of Trust** page, click **Two-way**, and then click **Next**.
8. In the **Sides of Trust** page, click **Both this domain and the specified domain**, and then click **Next**.
9. In the **User name** text box, type **Administrator**. In the **Password** text box, type **Pa$$w0rd**, and then click **Next**.
10. In the **Outgoing Trust Authentication Level-Local Forest** page, click **Selective authentication**, and then click **Next**,
11. In the **Outgoing Trust Authentication Level-Specified Forest** page, click **Selective authentication**, and then click **Next**.
12. In the **Trust Selections Complete** page, click **Next**.
13. In the **Trust Creation Complete** page, click **Next**.
14. In the **Confirm Outgoing Trust** page, click **Yes, confirm the outgoing trust**, and then click **Next**.

15. In the **Confirm Incoming Trust** page, click **Yes, confirm the incoming trust**, and then click **Next**.
16. On the **Completing the New Trust Wizard** page, click **Finish**.
17. In the **Adatum.com Properties** dialog box, click **OK**.

Module Review and Takeaways

Review Questions

Question: You are the AD DS administrator for A. Datum Corporation. Currently, your AD DS environment is configured in a single-domain, single-forest model using the adatum.com namespace. A. Datum has recently announced that they are expanding from Europe into new continents through the acquisition of a company named Trey Research. Trey Research currently operates in North America and Asia. The AD DS environment of Trey Research consists of a single forest named treyresearch.net with an empty forest root domain, and child domains which align to each continent they operate in (na.treyresearch.net and asia.treyresearch.net). The long-term objectives for A. Datum are to fully integrate Trey Research into the daily operations of A. Datum. A. Datum leadership also wishes to adopt the regional operations model used by Trey Research. As the AD DS administrator for A. Datum, how would you combine the adatum.com forest with the treyresearch.net forest? Discuss both short-term and long-term objectives for AD DS integration and how different requirements might change your approach.

Answer: Short-term objectives

- Create a forest trust between the adatum.com and treyresearch.net AD DS forests. Doing so will allow cross-forest authentication and authorization so that employees of both A. Datum and Trey Research can access resources in either forest.

Long-term objectives

- Create the following new child domains in adatum.com:
  - europe.adatum.com
  - na.adatum.com
  - asia.adatum.com
- You should plan a forest restructuring effort for the adatum.com forest:
  - Migrate existing adatum.com domain objects into europe.adatum.com. Leave the necessary forest-level objects in the adatum.com forest root domain.
  - Move na.treyresearch.net domain objects into na.adatum.com.
  - Move asia.treyresearch.net domain objects into asia.adatum.com

Feedback:

In this scenario, your short-term objective is to integrate the AD DS environments as quickly as possible so that employees from both companies can start collaborating immediately. The quickest and easiest way for you to accomplish this would be to create a forest trust between the two forests. While this approach could work for both the short-term and long-term needs of A. Datum, leadership has expressed that Trey Research is part of their long-term strategy. Additionally, they have indicated a desire to adopt a regional operations model similar to what Trey Research is already using. Given these two key pieces of information, your long-term plan for AD DS should be to restructure the adatum.com forest and create child domains for each region in which A. Datum will operate.

If acquisition of Trey Research was merely a short-term objective and future divestiture of Trey Research is a likely possibility, you may decide to implement only a forest trust so that you could easily separate from Trey Research in the future.

If a regional operations model is not a requirement, you may decide to maintain a single-forest, single-domain model and migrate all treyresearch.net objects into the adatum.com forest root domain.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
You receive error messages such as: • DNS lookup failure • RPC server unavailable • Domain does not exist • Domain controller could not be found	Usually, these errors are caused by a DNS record lookup failure or incorrectly configured firewall. Ensure that there are at least two working DNS servers available on the network. Ensure that every computer has at least two DNS servers configured in the network configuration. Verify that DNS servers are able to successfully resolve queries for DNS records outside of their DNS domain (for instance, Internet addresses). Use various troubleshooting tools such as nslookup, dnslint, DCdiag, netdiag, repadmin, replmon, and Event Viewer.
User cannot be authenticated to access resources on another AD DS domain or Kerberos realm.	Use the Active Directory Domains and Trusts console, (Domain.msc), or the Netdom command-line tool to validate trust relationships. If necessary, reset the trust password. Check to ensure that trust relationships are configured for the right direction. Verify that all AD DS domain controllers have registered all of the correct SRV records in the DNS database. (You can restart the netlogon service on an AD DS domain controller to force it to reregister the SRV records in the DNS database.)

Lab Review Questions and Answers

Lab: Domain and trust management in AD DS

Question and Answers

Question: When creating the forest trust between Adatum.com and TreyResearch.net, DNS stub zones were created to enable name resolution between the two forests. What alternative could you have used in place of a DNS stub zone?

Answer: Instead of creating DNS stub zones in each forest, you also could have used a conditional forwarder. A secondary DNS would also accomplish the required name resolution, but would cause unnecessary replication.

Question: When you are creating a forest trust, why would you create a selective trust instead of a complete trust?

Answer: By using selective authentication when configuring a trust, you have more control over the resources that users from the trusted domain/forest are allowed to authenticate to. If you do not use selective authentication, users in the trusted domain forest are allowed to authenticate to any resource.

Module 4

Implementing and administering AD DS sites and replication

Contents:

Lesson 1

Overview of AD DS replication

Contents:

Question and Answers

Question: Why is replication important to the global catalog?

> Answer: The configuration partition contains global catalog information that is replicated to all domain controllers that are designated as global catalog servers.

How AD DS replication works within a site

Question: Describe the circumstances that result when you manually create a connection object between domain controllers within a site.

> Answer: Creating a connection object manually is not typically required or recommended, because the Knowledge Consistency Checker does not verify or use the manual connection object for failover. The Knowledge Consistency Checker will also not remove manual connection objects, which means that you must remember to delete connection objects that you create manually.

Lesson 2

Configuring AD DS sites

Contents:

Question and Answers

Question: Which of the following is not a consideration for implementing AD DS sites?

( ) Reducing bandwidth usage between network locations

( ) Applying Group Policy settings to a single location in your organization

( ) Controlling which domain controller client computers use for authentication

( ) Creating a backup site for disaster recovery

( ) Controlling access to apps and services for a certain segment of your network

Answer:

( ) Reducing bandwidth usage between network locations

( ) Applying Group Policy settings to a single location in your organization

( ) Controlling which domain controller client computers use for authentication

(√) Creating a backup site for disaster recovery

( ) Controlling access to apps and services for a certain segment of your network

Resources

How client computers locate domain controllers within sites

 **Additional Reading:** For more information, refer to Finding a Domain Controller in the Closest Site: http://aka.ms/Cjpzdd

Demonstration: Configuring AD DS sites

Demonstration Steps

1. On **LON-DC1**, click **Start**, and then click **Server Manager**.
2. In **Server Manager**, click **Tools**, and then click **Active Directory Sites and Services**.
3. In the **Active Directory Sites and Services** console, expand **Sites**, and then click **Default-First-Site-Name**.
4. Right-click **Default-First-Site-Name**, click **Rename**, type **LondonHQ**, and then press Enter.
5. In the navigation pane, right-click **Sites**, and then click **New Site**.
6. In the **New Object – Site** dialog box, in the **Name** text box, type **Toronto**.
7. Select **DEFAULTIPSITELINK**, and then click **OK**.
8. In the **Active Directory Domain Services** dialog box, click **OK**.
9. In the navigation pane, right-click **Subnets**, and then click **New Subnet**.
10. In the **New Object – Subnet** dialog box, in the **Prefix** text box, type **172.16.0.0/24**.
11. Under **Select a site object for this prefix**, click **LondonHQ**, and then click **OK**.
12. In the navigation pane, right-click **Subnets**, and then click **New Subnet**.
13. In the **New Object – Subnet** dialog box, in the **Prefix** text box, type **172.16.1.0/24**.
14. Under **Select a site object for this prefix**, click **Toronto**, and then click **OK**.
15. In the navigation pane, expand **LondonHQ**, and then expand **Servers**.
16. Right-click **TOR-DC1**, and then click **Move**.

17. In the **Move Server** dialog box, select **Toronto**, and then click **OK**.
18. In the navigation pane, expand **Toronto**, and then expand **Servers**.
19. Verify that **TOR-DC1** is now located in the **Toronto** site.

Lesson 3

Configuring and monitoring AD DS replication

Contents:

Question and Answers

Question: The shortest replication duration that you can configure with site replication scheduling is 15 minutes.

( ) True

( ) False

Answer:

(√) True

( ) False

Resources

Tools for monitoring and managing replication

 **Additional Reading:** For more information, refer to AD DS Administration Cmdlets in Windows PowerShell: http://aka.ms/Itjgof

Demonstration: Configuring AD DS intersite replication

Demonstration Steps

1. On **TOR-DC1**, in **Server Manager**, click **Tools**, and then click **Active Directory Sites and Services**.
2. In the **Active Directory Sites and Services** console, expand **Sites**, and then expand **Inter-Site Transports**.
3. Click **IP**, right-click **DEFAULTIPSITELINK**, click **Rename**, type **LON-TOR**, and then press Enter.
4. Right-click **LON-TOR**, and then click **Properties**. Explain the **Cost**, **Replicate every**, and **Change Schedule** options.
5. In the **LON-TOR Properties** dialog box, in the **Replicate every** spin box, configure the value to be **60** minutes.
6. Click **Change Schedule**.
7. Highlight the range from **Monday 12 PM** to **Friday 4 PM**, as follows:
8. Click the **Monday at 12:00 PM** tile, press and hold the mouse button, and then drag the cursor to the **Friday at 4:00 PM** tile.
9. Click **Replication Not Available**, and then click **OK**.
10. Click **OK** to close the **LON-TOR Properties** dialog box.
    - In the **navigation** pane, right-click **IP**, and then click **Properties**.
11. In the **IP Properties** dialog box, point out and explain the **Bridge all site links** option.
12. Click **OK** to close the **IP Properties** dialog box.

Module Review and Takeaways

Best Practices

Implement the following best practices when you manage Active Directory sites and replication in your environment:

- Always provide at least one or more global catalog servers per site.
- Ensure that all sites have appropriate subnets associated.
- When you configure replication schedules for intersite replication, do not set up long intervals without replication.
- Avoid using Simple Mail Transfer Protocol (SMTP) as a protocol for replication.

Review Questions

Question: In a multisite enterprise, why is it important that all subnets are identified and associated with a site?

Answer: You can make the process of locating domain controllers and other services more 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 domain controllers in the domain. This is not an efficient strategy. In fact, a single client can perform actions against domain controllers in different sites, which can lead to unexpected results if those changes have not yet replicated. Therefore, it is crucial that each client knows what site it is in, which you can achieve by ensuring that domain controllers can identify a client's site location.

Question: What are the advantages and disadvantages of reducing the intersite replication interval?

Answer: Reducing the intersite replication interval improves convergence. Changes made in one site replicate 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 is primarily a matter of replication timing rather than replication quantity. However, in some extreme situations, allowing a smaller number of changes to occur more frequently might be less preferable than allowing a large number of changes to replicate less frequently.

Question: What is the purpose of a bridgehead server?

Answer: A bridgehead server is responsible for all replication into and out of a site. Instead of replicating all domain controllers from one site with all domain controllers in another site, you can use bridgehead servers to manage intersite replication. However, if a particular bridgehead server is not specifically necessary for performance reasons or other factors, a best practice is to let the ISTG choose the bridgehead servers from among the available pool of site domain controllers.

Tools

The following table lists the tools that this module references.

1. Tool	2. Use	3. Location
Active Directory Sites and Services console	Create sites, subnets, site links, site link bridging, force replication, and restart the Knowledge Consistency Checker.	**Server Manager** tools
Repadmin.exe	Reports the status of replication on each domain controller, create replication topology and force replication, and view levels of detail down to the replication metadata.	Command line

1. Tool	2. Use	3. Location
Dcdiag.exe	Performs a number of tests and reports on the overall health of replication and security for AD DS.	Command line
Get-ADReplicationConnection	A specific AD DS replication connection or set of AD DS replication connection objects based on a specified filter.	Windows PowerShell
Get-ADReplicationFailure	A description of an AD DS replication failure.	Windows PowerShell
Get-ADReplicationPartnerMetadata	Replication metadata for a set of one or more replication partners.	Windows PowerShell
Get-ADReplicationSite	A specific AD DS replication site or a set of replication site objects based on a specified filter.	Windows PowerShell
Get-ADReplicationSiteLink	A specific Active Directory site link or a set of site links based on a specified filter.	Windows PowerShell
Get-ADReplicationSiteLinkBridge	A specific Active Directory site link bridge or a set of site link bridge objects based on a specified filter.	Windows PowerShell
Get-ADReplicationSubnet	A specific Active Directory subnet or a set of Active Directory subnets based on a specified filter.	Windows PowerShell

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
A client cannot locate a domain controller in its site.	• Verify whether all SRV records for the domain controller are present in DNS. • Verify whether the domain controller has an IP address from the subnet that is associated with that site. • Verify that the client is a domain member and has the correct time setting.
Replication between sites does not work.	• Verify correct configuration of site links. • Verify the replication schedule. • Verify whether the firewall between the sites permits traffic for AD DS replication. Use repadmin /bind.
Replication between two domain controllers in the same site does not work.	• Verify whether both domain controllers appear in same site. • Verify whether AD DS is operating correctly on the domain controllers.

Common Issue	Troubleshooting Tip
	• Verify network communication and that the time setting on each server is valid.

Lab Review Questions and Answers

Lab: Implementing AD DS sites and replication

Question and Answers

Question: You decide to add a new domain controller named LON-DC2 to the LondonHQ site. How can you ensure that LON-DC2 passes all replication traffic to the Toronto site?

> Answer: You would have to configure this new domain controller as the preferred bridgehead server for the LondonHQ site.

Question: You have added a new domain controller named LON-DC2 to the LondonHQ site. Which AD DS partitions will be modified as a result?

> Answer: It is likely that all of the partitions except the schema partition will be modified. You add the new domain controller to both the domain partition and the configuration partition to ensure correct configuration of AD DS replication. If you are using Active Directory–integrated DNS, then the domain controller records also will update in the DNS application partitions.

Question: In the lab, you created a separate site link for the Toronto and TestSite sites. What might you also have to do to ensure that LondonHQ does not automatically create a connection object directly with the TestSite site?

> Answer: You might also have to turn off automatic site link bridging so that you disable site transitivity among LondonHQ, Toronto, and the TestSite.

Module 5

Implementing Group Policy

Contents:

Lesson 1

Introducing Group Policy

Contents:

Question and Answers

Categorize Activity

Question: Categorize each item into the appropriate category. Indicate your answer by writing the category number to the right of each item.

Items	
1	Domain
2	User
3	Organizational unit
4	Computer
5	Site
6	Group
7	Users container
8	Computers container

Category 1		Category 2
Can link GPOs to		Cannot link GPOs to

Answer:

Category 1		Category 2
Can link GPOs to		Cannot link GPOs to
Domain Organizational unit Site		User Computer Group Users container Computers container

Demonstration: Exploring Group Policy tools and consoles

Demonstration Steps

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **Group Policy Management**.
2. If necessary, switch to the **Group Policy Management** window.
3. In Group Policy Management Editor, in the navigation pane, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, and then click **Group Policy Objects**.
4. Right-click **Group Policy Objects**, and then click **New**.
5. In the **New GPO** dialog box, type **Disable Control Panel**, and then click **OK**.
6. In the details pane, right-click **Disable Control Panel**, and then click **Edit**.
7. In Group Policy Management Editor, in the navigation pane, under **User Configuration**, expand **Policies**, expand **Administrative Templates**, and then click **Control Panel**.
8. In the details pane, double-click **Prohibit access to Control Panel and PC Settings**.
9. In the **Prohibit access to Control Panel and PC Settings** dialog box, show the three possible values for a setting in **Administrative Templates**, show the **Supported on** text, and then show the **Help** text.
10. Click **Enabled**. In the **Comment** text box, type **Enabled** <*date*> **by** <*your name*>, where you replace <*date*> with today's date and <*your name*> with your name, and then click **OK**.
11. In the navigation pane, under **User Configuration**, expand **Preferences**, and show the different categories under both **Policies** and **Preferences**.
12. Close the **Group Policy Management Editor** window.
13. In the **Group Policy Management** window, in the navigation pane, expand **Group Policy Objects**, and then click **Disable Control Panel**.
14. In the details pane, show the **Scope**, **Details**, and **Settings** tabs.
15. In the navigation pane, click and then right-click **Adatum.com**, and then click **Link an Existing GPO**.
16. In the **Select GPO** dialog box, click **Disable Control Panel**, and then click **OK**.
17. In the navigation pane, click **Adatum.com**.
18. In the details pane, show the **Linked Group Policy Objects** and **Group Policy Inheritance** tabs.
19. Click **Start**, and then click **Windows PowerShell**.
20. In the **Administrator: Windows PowerShell** window, type the following command, and then press Enter:

```
gpupdate
```

21. Verify that both the computer and user settings updated successfully.
22. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
gpresult /r
```

23. In the output from the command, in the **User Settings** section, in the **Applied GPOs** list, verify that the **Disable Control Panel** GPO is listed.
24. Close the **Windows PowerShell** window.

Lesson 2

Implementing and administering GPOs

Contents:

Question and Answers

Question: Members of which built-in AD DS groups can create GPOs by default? (Select three.)

( ) Domain Admins

( ) Account Operators

( ) Enterprise Admins

( ) GPO Admins

( ) Group Policy Creator Owners

Answer:

(√) Domain Admins

( ) Account Operators

(√) Enterprise Admins

( ) GPO Admins

(√) Group Policy Creator Owners

Feedback:

The GPO Admins group does not exist. The Domain Admins and Enterprise Admins groups can perform all administrative tasks in the domain including create GPOs. Group Policy Creator Owners is the only group that you can add users to, if you want them to be able to create GPOs without getting administrative rights on the domain or forest. Account Operators do not have any permissions regarding Group Policy. Only administering users, computers and groups in AD DS.

Demonstration: Delegating administration of Group Policy

Demonstration Steps

Make Beth a local administrator on LON-SVR1

1. Switch to **LON-DC1**.
2. On the taskbar, click the **File Explorer** icon.
3. In the **File Explorer** window, in the navigation pane, expand **Allfiles (E:)**, expand **Labfiles**, and then click **Mod05**.
4. In the details pane, right-click the **Set-LocalAdmin.ps1** file, and then click **Run with Powershell**. Type **Y**, if prompted, and then press Enter.

Check user permissions before delegation

1. Switch to **LON-SVR1**.
2. Sign in as **Adatum\Beth** with the password **Pa$$w0rd**.
3. In **Server Manager**, click **Add roles and features**.
4. In **Add Roles and Features Wizard**, on the **Before you begin** page, click **Next**.
5. On the **Select installation type** page, click **Next**.
6. On the **Select destination server** page, click **Next**.
7. On the **Select server roles** page, click **Next**.
8. On the **Select features** page, select the **Group Policy Management** check box, and then click **Next**.

9. On the **Confirm installation selections** page, click **Install**.
10. When the installation completes, click **Close**.
11. In **Server Manager**, click **Tools**, and then click **Group Policy Management**.
12. If necessary, switch to the **Group Policy Management** window.
13. In **Group Policy Management**, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum,com**, and then click **Group Policy Objects**.
14. Right-click **Group Policy Objects**, and then notice that the **New** item is dimmed because Beth does not have permissions to create GPOs.
15. In the navigation pane, right-click the **Adatum.com** domain, and then notice that menu item **Link an Existing GPO** is dimmed because Beth does not have permissions to link GPOs to the domain.
16. In the navigation pane, right-click the **IT** OU, and then notice that menu item **Link an Existing GPO** is dimmed because Beth also does not have permissions to link GPOs to the **IT** OU.
17. Click **Start**, and then click **Windows PowerShell**.
18. In the **Windows PowerShell** window, type the following command, and then press Enter:

```
GPResult /r
```

19. In the output from the command, notice that only the **User** settings is displayed because Beth is not assigned the permissions view Group Policy results for computer settings.

Delegate permissions

1. On **LON-DC1**, switch to the **Group Policy Management** window.
2. In **Group Policy Management**, in the navigation pane, click the **Group Policy Objects** container, and then in the details pane, click the **Delegation** tab.
3. Click **Add**. In the **Select User, Computer, or Group** dialog box, type **Beth**, click **Check Names**, and then click **OK**.
4. In the navigation pane, click the **IT** OU, and then in the details pane, click the **Delegation** tab.
5. In the **Permission** dropdown list, **Link GPOs** is selected, and then click **Add**.
6. In the **Select User, Computer, or Group** dialog box, type **Beth**, click **Check Names**, and then click **OK**.
7. In the **Add Group or User** dialog box, click **OK**.
8. In the navigation pane, click the **Adatum.com** domain, and then in the details pane, click the **Delegation** tab.
9. In the **Permission** drop-down list, select **Read Group Policy Results data**, and then click **Add**.
10. In the **Select User, Computer, or Group** dialog box, type **Authenticated Users**, click **Check Names**, and then click **OK**.
11. In the **Add Group or User** dialog box, click **OK**.

Check permissions after delegation

1. Switch to **LON-SVR1**.
2. Switch to **Group Policy Management**.
3. In the **Group Policy Management** window, click and then right-click the **Adatum.com** domain, and then click **Refresh**.
4. In the navigation pane, right-click **Group Policy Objects**, and then click **New**.

5. In the **New GPO** dialog box, in the **Name** text box, type **Beth's GPO**, and then click **OK**.
6. In the navigation pane, right-click **Adatum.com**, and then notice that **Link an Existing GPO** is still dimmed.
7. In the navigation pane, right-click **IT**, and then click **Link an Existing GPO**.
8. In the **Select GPO** dialog box, click **Beth's GPO**, and then click **OK**.
9. Switch to the **Windows PowerShell** window.
10. In the **Windows PowerShell** window, type the following command and then press Enter:

```
GPResult /r
```

11. In the output from the command, notice that both the **Computer** and the **User** settings are displayed.

Lesson 3

Group Policy scope and Group Policy processing

Contents:

Question and Answers

Question: It is possible to link more than one WMI filter to a GPO.

( ) True

( ) False

Answer:

( ) True

(√) False

Feedback:

Although you cannot link more than one WMI filter to a GPO, you can create advanced WMI filters that include more than one WMI query.

Question: Which of the following options can you configure in the GPMC to change the default Group Policy processing order? (Select all that apply.)

( ) WMI filters

( ) Security filtering

( ) Block inheritance

( ) Enforce

( ) Loopback processing

Answer:

(√) WMI filters

(√) Security filtering

(√) Block inheritance

(√) Enforce

(√) Loopback processing

Feedback:

All the options are viable options to change the way Group Policy normally applies. You should use the different options sparingly because troubleshooting becomes increasingly difficult when you use these options.

Demonstration: Linking GPOs

Demonstration Steps

Create and edit two GPOs

1. On **LON-DC1**, if necessary, open **Server Manager**.
2. In **Server Manager**, click **Tools**, and then click **Group Policy Management**.
3. In the **Group Policy Management** window, expand **Forest: Adatum.com**, **Domains**, and **Adatum.com**, right-click the **Group Policy Objects** container, and then click **New**.
4. In the **New GPO** dialog box, type **Remove Run Command** in the **Name** text box, and then click **OK**.
5. In the **Group Policy Management** window, right-click the **Group Policy Objects** container, and then click **New**.

6. In the **New GPO** dialog box, type **Do Not Remove Run Command** in the **Name** text box, and then click **OK**.
7. Expand **Group Policy Objects**, right-click the **Remove Run Command** GPO, and then click **Edit**.
8. In the **Group Policy Management Editor** window, under **User Configuration**, expand **Policies**, expand **Administrative Templates**, click **Start Menu and Taskbar**, and then double-click **Remove Run menu from Start Menu**.
9. In the **Remove Run menu from Start Menu** window, click **Enabled**, and then click **OK**.
10. Close the **Group Policy Management Editor** window.
11. In **Group Policy Management**, right-click the **Do Not Remove Run Command** GPO, and then click **Edit**.
12. In the **Group Policy Management Editor** window, under **User Configuration**, expand **Policies**, expand **Administrative Templates**, click **Start Menu and Taskbar**, and then double-click **Remove Run menu from Start Menu**.
13. In the **Remove Run menu from Start Menu** window, click **Disabled**, and then click **OK**. Close the **Group Policy Management Editor** window.

Link the GPOs to different locations

1. In the **Group Policy Management** window, right-click the **Adatum.com** domain node in the navigation pane, and then click **Link an Existing GPO**.
2. In the **Select GPO** window, click **Remove Run Command**, and then click **OK**. Now the **Remove Run Command** GPO is attached to the Adatum.com domain.
3. Click and drag the **Do Not Remove Run Command** GPO on top of the **IT** OU.
4. In the **Group Policy Management** window, click **OK** to link the GPO.
5. Click the **IT** OU in the navigation pane, and then click the **Group Policy Inheritance** tab in the details pane. The **Group Policy Inheritance** tab shows the order of precedence for the GPOs.

Disable a GPO link

- In the left pane, right-click the **Remove Run Command** link that is listed under **Adatum.com**, and then click **Link Enabled** to clear the check mark. Refresh the **Group Policy Inheritance** pane for the information technology (**IT**) OU, and then notice the results in the details pane. The **Remove Run Command** GPO is no longer listed.

Delete a GPO link

1. In the left pane, expand the **IT** OU, right-click the **Do Not Remove Run Command** link, and then click **Delete**. Click **OK** in the pop-up window.
2. Click the **IT** OU in the left pane, and then click the **Group Policy Inheritance** tab in the details pane. Verify the removal of **Do Not Remove Run Command** and the absence of the **Remove Run Command** GPOs.
3. In the left pane, right-click the **Remove Run Command** GPO that is listed under **Adatum.com**, and then click **Link Enabled** to re-enable the link. Refresh the **Group Policy Inheritance** window for the **IT** OU, and then notice the results in the right pane.
4. Close **Group Policy Management.**

Demonstration: Filtering Group Policy application

Demonstration Steps

Create a new GPO and link it to the IT OU

1. On **LON-DC1**, from **Server Manager**, click **Tools**, and then click **Group Policy Management**.

2. In the **Group Policy Management** window, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, and then click the **IT** OU.
3. Right-click **IT**, and then click **Create a GPO in this domain, and Link it here**.
4. In the **New GPO** window, type **Remove Help menu** in the **Name** text box, and then click **OK**.
5. In the **Group Policy Management** window, expand **Group Policy Objects**, right-click the **Remove Help menu** GPO, and then click **Edit**.
6. In the **Group Policy Management Editor** window, under **User Configuration**, expand **Policies**, expand **Administrative Templates**, click **Start Menu and Taskbar**, and then double-click **Remove Help menu from Start Menu**.
7. In the **Remove Help menu from Start menu** window, click **Enabled**, and then click **OK**.
8. Close the **Group Policy Management Editor** window.

Filter Group Policy application by using security group filtering

1. Expand **IT**, and then click the **Remove Help menu** GPO link.
2. In the **GPMC** message box, click **OK**.
3. In the details pane, under **Security Filtering**, click **Authenticated Users**, and then click **Remove**.
4. In the confirmation dialog box, click **OK**.
5. In the details pane, under **Security Filtering**, click **Add**.
6. In the **Select User, Computer, or Group** dialog box, in the **Enter Object Names to select (Examples):** text box, type **Beth Burke**, and then click **OK**.

Filter the Group Policy application by using WMI filtering

1. In the **Group Policy Management** window, right-click **WMI Filters**, and then click **New**.
2. In the **New WMI Filter** dialog box, in the **Name** text box, type **OS Version Filter**.
3. In the **Queries** pane, click **Add**.
4. In the **WMI Query** dialog box, in the **Query** text box, type the following query, and then click **OK**:

```
select * from Win32_OperatingSystem where Version like "6.%"
```

5. If a **Warning** dialog box appears, click **OK**.
6. In the **New WMI Filter** dialog box, click **Save**.
7. Right-click the **Group Policy Objects** folder, and then click **New**.
8. In the **New GPO** window, type **Software Updates** in the **Name** text box, and then click **OK**.
9. Expand **Group Policy Objects**, and then click the **Software Updates** GPO.
10. In the details pane, under **WMI Filtering**, in the **This GPO is linked to the following WMI filter** list, select **OS Version Filter**.
11. In the confirmation dialog box, click **Yes**.
12. Close **Group Policy Management**.

Lesson 4

Troubleshooting the application of GPOs

Contents:

Resources

Examining Group Policy event logs

Additional Reading: To download Group Policy Log View, go to: http://aka.ms/E8oi7g

Demonstration: Performing a what-if analysis with Group Policy Modeling Wizard

Demonstration Steps

Use GPResult.exe to create a report

1. On **LON-DC1**, click **Start**, type **cmd**, and then press Enter.
2. In the **Administrator: C:\Windows\System32\cmd.exe** window, type **cd **, and then press Enter.
3. Type the following command, and then press Enter:

```
GPResult /r
```

4. Review the output in the **Command Prompt** window.
5. Type the following command, and then press Enter:

```
GPResult /h results.html
```

6. Close the **Command Prompt** window.
7. Click **Start**, click **All apps**, click **Windows Accessories**, and then click **Internet Explorer**.
8. In the **Internet Explorer** window, press the Alt key, click **File**, and then click **Open**.
9. In the **Open** dialog box, in the **Open** text box, type **C:\results.html**, and then click **OK**.
10. In the warning message, click **Allow blocked content**.
11. View the results of the report.
12. Close Microsoft Internet Explorer.

Use Group Policy Reporting Wizard to create a report

1. Open **Server Manager**, click **Tools**, and then click **Group Policy Management**.
2. In the **Group Policy Management** window, in the navigation pane, right-click **Group Policy Results**, and then click **Group Policy Results Wizard**.
3. In **Group Policy Results Wizard**, click **Next**.
4. On the **Computer Selection** page, click **Next**.
5. On the **User Selection** page, click **Next**.
6. On the **Summary of Selections** page, click **Next**.
7. On the **Completing the Group Policy Results Wizard** page, click **Finish**.
8. Review the Group Policy results.
9. Expand **Group Policy Results**, right-click **Administrator on LON-DC1**, and then click **Save Report**.
10. In the **Save GPO Report** dialog box, click **Desktop**, and then click **Save**.

Use Group Policy Modeling Wizard to create a report

1. Right-click **Group Policy Modeling**, and then click **Group Policy Modeling Wizard**.
2. In **Group Policy Modeling Wizard**, click **Next**.
3. On the **Domain Controller Selection** page, click **Next**.
4. On the **User and Computer Selection** page, under **User information**, click **User**, and then click **Browse**.
5. In the **Select User** dialog box, in the **Enter object names to select (Examples)** text box, type **Beth**, and then click **OK**.
6. Under **Computer information**, verify that the **Container** option is selected, and then click **Browse**.
7. In the **Choose Computer Container** dialog box, expand **Adatum**, click **IT**, and then click **OK**.
8. On the **User and Computer Selection** page, click **Next**.
9. On the **Advanced Simulation Options** page, click **Next**.
10. On the **Alternate Active Directory Paths** page, click **Next**.
11. On the **User Security Groups** page, click **Next**.
12. On the **Computer Security Groups** page, click **Next**.
13. On the **WMI Filters for Users** page, click **Next**.
14. On the **WMI Filters for Computers** page, click **Next**.
15. On the **Summary of Selections** page, click **Next**.
16. On the **Completing Group Policy Modeling Wizard** page, click **Finish**.
17. Review the report.
18. Close all open windows.

Module Review and Takeaways

Review Questions

Question: You have assigned a logon script to an OU via Group Policy. The script is located in a shared network folder named **Scripts**. Some users in the OU receive the script and others do not. What might be the possible causes?

> **Answer:** Security permissions might be a problem. If some users do not have Read access to the **Scripts** folder, they will not be able to apply policy. Also, security filtering on a GPO might be the cause of this problem.

Question: What GPO settings apply across slow links by default?

> **Answer:** Registry policy processing and security policy apply even when a slow link is detected. You cannot change this setting.

Question: You must ensure that a domain-level policy is enforced, but the Managers group must be exempt from the policy. How would you accomplish this?

> **Answer:** Set the link to be enforced at the domain level and use security group filtering to deny the Apply Group Policy permission to the Managers group.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Group Policy settings are not applied to all users or computers in an OU where a GPO is applied.	• Check security filtering on the GPO. • Check WMI filters on the GPO.
Group Policy settings sometimes require two restarts to apply.	Enable the **Always Wait For Network At Startup and Logon policy** setting.

Lab Review Questions and Answers

Lab A: Implementing a Group Policy infrastructure

Question and Answers

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

Answer: The fundamental problem of relying on OUs to scope the application of GPOs is that an OU is a fixed, inflexible structure within AD DS; a single user or computer can exist within only one OU. As organizations get larger and more complex, configuration requirements become 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 you can add or remove them 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 guarantee 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 also can help in troubleshooting compatibility and functionality problems. Sometimes, specific GPO settings can interfere with the functionality of an application. To test whether the application works on a clean installation of the Windows operating system, you might need to exclude the user or computer temporarily from the scope of GPOs.

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

Answer: Answers will vary. Scenarios could include: in conference rooms and kiosks, on Virtual Desktop Infrastructure computers, and in other standard environments.

Lab B: Troubleshooting Group Policy infrastructure

Question and Answers

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

Answer: Answers will vary based on students' experiences and situations. Possible answers might include:

- Solved a Group Policy issue where one GPO did not apply because of security filtering.
- Solved a Group Policy issue where one client-side extension took 20 seconds to apply because of a Domain Name System (DNS) issue.
- Located a GPO setting that was configured in the wrong GPO.
- Located a Group Policy issue where the incorrect user settings were applied because of loopback processing.

Question: In what situations have you used Group Policy modeling? If you have not done this yet, in what situations can you anticipate using Group Policy modeling?

Answer: Answers will vary based on students' experiences and situations. Possible answers might include:

- Managed to configure Group Policy correctly based on Group Policy modeling simulations.
- Tested the result of adding a user to a security group.
- Tested the result of moving a user to another OU.
- Tested the result of configuring loopback processing for a computer.

Module 6

Managing user settings with Group Policy

Contents:

Lesson 1

Implementing administrative templates

Contents:

Question and Answers

Question: Which sections are available in the **Administrative Templates** node under the **User Configuration** node? (Select all that apply.)

( ) Desktop

( ) Windows Components

( ) Server

( ) System

( ) Control Panel

Answer:

(√) Desktop

(√) Windows Components

( ) Server

(√) System

(√) Control Panel

Feedback:

Some of the sections display in **Administrative Templates** in both the computer and user sections of a GPO. The Desktop section is only in the user section, and the Server section is only in the computer section. Windows Components, System, and Control panel are in both the computer and user sections of a GPO, although the settings that you can configure in these sections are not the same.

Question: You can create the central store through the GPMC.

( ) True

( ) False

Answer:

( ) True

(√) False

Feedback:

To create the central store, you have to manually create the **PolicyDefinitions** folder in SYSVOL, and then copy both the .admx and .adml files to the **PolicyDefinitions** folder.

Discussion: Practical uses of administrative templates

Question: How do you provide desktop security currently?

Answer: Answers will vary.

Question: How much administrative access do users have to their systems?

Answer: Answers will vary.

Question: Which Group Policy settings will you find useful in your organization?

Answer: Answers will vary.

Resources

Importing security templates

 **Additional Reading:** For more information, refer to Security Compliance Manager (SCM): http://aka.ms/Ypdcmd

Managing administrative templates

 **Additional Reading:** For more information, refer to ADMX Migrator: http://aka.ms/Ny5p5c

 **Additional Reading:** For more information, refer to Office 2016 Administrative Template files (ADMX/ADML) and Office Customization Tool: http://aka.ms/Nknzlx

Demonstration: Configuring settings with administrative templates

Demonstration Steps

Configure an administrative templates policy setting

1. Switch to **LON-DC1**.
2. From **Server Manager**, click **Tools**, and then click **Group Policy Management**.
3. In the navigation pane, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, and then click the **Group Policy Objects** container.
4. Right-click the **Group Policy Objects** container, and then click **New**.
5. In the **New GPO** dialog box, in the **Name** field, type **GPO1**, and then click **OK**.
6. In the details pane, right-click **GPO1**, and then click **Edit**.
7. In the **Group Policy Management Editor** window, in the navigation pane, expand **User Configuration**, expand **Policies**, expand **Administrative Templates**, and then click **System**.
8. In the details pane, double-click **Prevent Access to the command prompt**.
9. In the **Prevent Access to the command prompt** dialog box, show the three possible values, and then click **Cancel**.

Filter administrative templates policy settings

1. Right-click **Administrative Templates**, and then click **Filter Options**.
2. Select the **Enable Keyword Filters** check box.
3. In the **Filter for word(s)** text box, type **screen saver**.
4. In the drop-down box next to the text box, select **All**, and then click **OK**.
5. Point out that administrative templates policy settings filter to show only those that contain the words **screen saver**. Spend a few moments examining the settings that you have found. Explain that settings may appear without screen saver in the title, because screen saver can also appear in the help text.
6. In the console tree, under **User Configuration**, right-click **Administrative Templates**, and then click **Filter Options**.
7. Clear the **Enable Keyword Filters** check box.

8. In the **Configured** drop-down list box, select **Yes**, and then click **OK**. Point out that now the administrative templates policy settings filter to show only those that have been configured as enabled or disabled. No settings have been configured.
9. In the console tree, under **User Configuration**, right-click **Administrative Templates**, and then clear the **Filter On** option.

Add comments to a policy setting

1. In the console tree, under **User Configuration**, expand **Policies**, expand **Administrative Templates**, expand **Control Panel**, and then click **Personalization**.
2. In the details pane, double-click the **Enable screen saver** policy setting.
3. In the **Comment** section, type **Corporate IT Security Policy implemented with this policy in combination with Password Protect the Screen Saver**. Click **Enabled** to enable the policy, and then click **OK**.
4. Double-click the **Password protect the screen saver** policy setting, and then click **Enabled**.
5. In the **Comment** section, type **Corporate IT Security Policy implemented with this policy in combination with Enable screen saver**, and then click **OK**.

Add comments to a GPO

1. In the **Group Policy Management Editor**, in the console tree, right-click the root node **GPO1 [LON-DC1.ADATUM.COM]**, and then click **Properties**.
2. Click the **Comment** tab.
3. Type **Adatum corporate standard policies. Settings are scoped to all users and computers in the domain. Person responsible for this GPO:** ***your name***.
4. Point out that this comment displays on the **Details** tab of the GPO in the **Group Policy Management Console**, and then click **OK**.
5. Close the **Group Policy Management Editor** window.

Create a new GPO by copying an existing GPO

1. In the GPMC, in the navigation pane, click the **Group Policy Objects** container, right-click **GPO1**, and then click **Copy**.
2. Right-click the **Group Policy Objects** container, click **Paste**, and then click **OK** twice.

Create a new GPO by importing settings that were exported from another GPO

1. In the GPMC, in the navigation pane, click the **Group Policy Objects** container, right-click **GPO1**, and then click **Back Up**.
2. In the **Location** box, type **c:**, and then click **Back Up**.
3. When the backup finishes, click **OK**.
4. In the GPMC, in the navigation pane, right-click the **Group Policy Objects** container, and then click **New**.
5. In the **Name** box, type **ADATUM Import**, and then click **OK**.
6. In the GPMC, in the navigation pane, right-click the **ADATUM Import** GPO, and then click **Import Settings**.
7. In the **Import Settings Wizard**, click **Next** three times.
8. Select **GPO1**, and then click **Next** two times.
9. Click **Finish**, and then click **OK**.
10. Close the GPMC.

Lesson 2

Configuring Folder Redirection, Software Installation, and Scripts

Contents:

Question and Answers

Question: Which of the following folders can you redirect by using Folder Redirection? (Select all that apply.)

( ) Documents

( ) Favorites

( ) AppData (Roaming)

( ) AppData (Local)

( ) Program Files

Answer:

(√) Documents

(√) Favorites

(√) AppData (Roaming)

( ) AppData (Local)

( ) Program Files

Feedback:

You can redirect **Documents**, **Favorites**, and **AppData (Roaming)**. Three directories exist in a user's AppData directory: **Local**, **LocalLow**, and **Roaming**. You can only redirect **Roaming** by using Folder Redirection. You cannot redirect **Program Files**. This folder has to be located on the local hard drive.

Categorize Activity

Question: Categorize each item into the appropriate category. Indicate your answer by writing the category number to the right of each item.

Items	
1	Logon Scripts
2	Startup Scripts
3	Assign Software
4	Logoff Scripts
5	Shutdown Scripts
6	Folder Redirection
7	Publish Software

Category 1		**Category 2**		**Category 3**
User Configuration		Computer Configuration		User Configuration and Computer Configuration

Category 1		Category 2		Category 3

Answer:

Category 1		Category 2		Category 3
User Configuration		Computer Configuration		User Configuration and Computer Configuration
Logon Scripts Logoff Scripts Folder Redirection Publish Software		Startup Scripts Shutdown Scripts		Assign Software

Settings for configuring Folder Redirection

Question: Users in the same department often sign in to different computers. They need access to their Documents folders. They also need data to be private. What Folder Redirection setting would you choose?

> Answer: Create a folder for each user under the root path. This creates a Documents folder to which only the user has access.

Demonstration: Configuring Folder Redirection

Demonstration Steps

Create a shared folder

1. On LON-DC1, on the taskbar, click the File Explorer icon.
2. In the navigation pane, click This PC.
3. In the details pane, double-click Local Disk (C:), and then on the Home tab, click New folder.
4. In the Name text box, type Redir, and then press Enter.
5. Right-click the Redir folder, click Share with, and then click Specific people.
6. In the File Sharing dialog box, click the drop-down arrow, select Everyone, and then click Add.
7. For the Everyone group, click the Permission Level drop-down arrow, and then click Read/Write.

8. Click **Share**, and then click **Done**.
9. Close the **Local Disk (C:)** window.

Create a GPO to redirect the Documents folder

1. In Server Manager, click **Tools** and then click **Group Policy Management**.
2. In the navigation pane, right-click the **Adatum.com** domain, and then click **Create a GPO in this domain and Link it here**.
3. In the **New GPO** dialog box, in the **Name** text box, type **Folder Redirection**, and then click **OK**.
4. In the navigation pane, right-click **Folder Redirection**, and then click **Edit**.
5. In the **Group Policy Management Editor** window, under **User Configuration**, expand **Policies**, expand **Windows Settings**, and then expand **Folder Redirection**.
6. Right-click **Documents**, and then click **Properties**.
7. In the **Document Properties** dialog box, on the **Target** tab, click the **Setting** drop-down arrow, and then select **Basic-Redirect everyone's folder to the same location**.
8. Ensure that the **Target folder location** box is set to **Create a folder for each user under the root path**.
9. In the **Root Path** text box, type **\\LON-DC1\Redir**, and then click **OK**.
10. In the **Warning** dialog box, click **Yes**.
11. Close the Group Policy Management Editor.

Test Folder Redirection

1. Sign in to **LON-CL1** as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. Right-click **Start**, and then click **Command Prompt**.
3. In the Command Prompt window, type the following command, and then press Enter:

```
Gpupdate /force
```

4. In the command prompt window, when prompted, type the following, and then press Enter:

```
Y
```

5. Sign in to **LON-CL1** as **Adatum\Administrator** with the password **Pa$$w0rd**.
6. On the taskbar, click the **File Explorer** icon.
7. In the navigation pane, in the **Quick Access** section, right-click **Documents**, and then click **Properties**.
8. Verify that on the **General** tab, the Location field has a value of **\\lon-dc1\redir\Administrator**.
9. If this is not successful, repeat steps 2 through 7, and then check the redirection once again.
10. Sign out of **LON-CL1**.

Demonstration: Configuring scripts with GPOs

Demonstration Steps

Create a logon script to display a message

1. On **LON-DC1**, click **Start**, type **Notepad**, and then click **Notepad**.
2. In Notepad, type the following command, and then press Enter:

```
Msgbox "This is the script"
```

3. Click the **File** menu, and then click **Save As**.
4. In the **Save As** dialog box, in the **File name** text box, type **Logon.vbs**.
5. In the **Save as type** list, select **All Files (*.*)**.
6. In the navigation pane, click **Desktop**, and then click **Save**.
7. Close **Notepad**.
8. On the desktop, right-click the **Logon.vbs** file, and then click **Copy**.

Create and link a GPO to use the script

1. Open **Server Manager**, click **Tools**, and then click **Group Policy Management**.
2. Expand **Forest: Adatum.com**, and then expand **Domains**.
3. Right-click **Adatum.com**, and then click **Create a GPO in this domain and Link it here**.
4. In the **New GPO** dialog box, in the **Name** text box, type **User Logon Script**, and then click **OK**.
5. Expand **Adatum.com**, right-click the **User Logon Script** GPO, and then click **Edit**.
6. In the **Group Policy Management Editor** window, under **User Configuration**, expand **Policies**, expand **Windows Settings**, and then click **Scripts (Logon/Logoff)**.
7. In the details pane, double-click **Logon**.
8. In the **Logon Properties** dialog box, click **Show Files**.
9. In the details pane, right-click a blank area, and then click **Paste**.
10. Close the **Logon** window.
11. In the **Logon Properties** dialog box, click **Add**.
12. In the **Add a Script** dialog box, click **Browse**.
13. Click the **Logon.vbs** script, and then click **Open**.
14. Click **OK** twice to close all dialog boxes.
15. Close both the **Group Policy Management Editor** window and the **Group Policy Management Console**.

Sign in to a client computer and test the results

1. On **LON-CL1**, sign out and then sign in as **Adatum\Administrator** with password **Pa$$word**.
2. Right-click **Start**, and then click **Command Prompt**.
3. In the Command Prompt window, type the following command, and then press **Enter**:

```
Gpupdate /force
```

4. If prompted, in the command prompt window, type the following, and then press **Enter**:

```
Y
```

5. Sign in to **LON-CL1** as **Adatum\Connie** with the password **Pa$$w0rd**.
6. Verify that the script runs, displaying the message you configured in the GPO earlier.

Note: This could take up to ten minutes to display. If the message does not display, restart LON-CL1 and repeat step one through five.

7. Sign out of LON-CL1.

Lesson 3

Configuring Group Policy preferences

Contents:

Question and Answers

Question: Which Group Policy preferences settings can you use to configure a user's Internet Explorer experience? (Select all that apply)

( ) Internet Explorer

( ) Shortcuts

( ) Registry

( ) Power Options

( ) Folder Options

Answer:

(√) Internet Explorer

(√) Shortcuts

(√) Registry

( ) Power Options

( ) Folder Options

Feedback:

You can use the Internet Explorer settings in Group Policy preferences to configure Microsoft Internet Explorer. Shortcuts can create favorites that users can open in Internet Explorer. You can use the registry to configure the registry-based settings of Internet Explorer. You cannot use Power Options or Folder Options to configure Internet Explorer.

Question: You can use item-level targeting to limit Group Policy preferences depending on which AD DS forest the user belongs to.

( ) True

( ) False

Answer:

( ) True

(√) False

Feedback:

Group Policy cannot traverse forests. You can use domains, sites, security groups, and organizational units in item-level targeting.

Question: In what scenarios have you used Group Policy preferences and item-level targeting?

Answer: The answers will vary. In addition to the students' answers, share your own experiences with the rest of the class.

Demonstration: Configuring Group Policy preferences

Demonstration Steps

Create a printer with Group Policy preferences

1. On **LON-DC1**, right-click **Start**, and then click **Control Panel**.
2. In Control Panel, click **View devices and printers**.
3. Click **Add a printer**.

4. In the **Add a device** dialog box, click **The printer that I want isn't listed**.
5. In the **Add Printer** dialog box, select **Add a local printer or network printer with manual settings**, and then click **Next**.
6. On the **Choose a printer port** page, click **Next**.
7. On the **Install the printer driver** page, click **Next**.
8. On the **Type a printer name** page, in the **Printer name** text box, type **Brother**, and then click **Next**.
9. On the **Printer Sharing** page, click **Next**.
10. On the **You've successfully added Brother** page, click **Finish**.
11. Close Control Panel.
12. If necessary, switch to **Server Manager**.
13. In **Server Manager**, click **Tools**, and then click **Group Policy Management**.
14. In the navigation pane, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, and then click the **Adatum.com** domain.
15. Right-click the **Adatum.com** domain, and click **Create a GPO in this domain, and Link it here**.
16. In the **New GPO** dialog box, type **GP Prefs**, and then click **OK**.
17. In the navigation pane, right-click **GP Prefs**, and then click **Edit**.
18. In the **Group Policy Management Editor**, expand **User Configuration**, expand **Preferences**, expand **Control Panel Settings**, right-click **Printers**, hover over **New**, and then click **Shared Printer**.
19. In the **New Shared Printer Properties** dialog box, in the **Share Path** text box, type **\\LON-DC1\Brother**.
20. Select the **Set this printer as the default printer** check box.

Target the preference

1. On the **Common** tab, select the **Item-level targeting** check box, and then click **Targeting**.
2. In the **Targeting Editor** dialog box, click **New Item**, and then click **IP Address Range**.
3. In the **between** text box, type **172.16.0.50**, in the **and** text box, type **172.16.0.99**, and then click **OK** twice.

Configure a power plan with Group Policy preferences

1. In Group Policy Management Editor, expand **Computer Configuration**, expand **Preferences**, expand **Control Panel Settings**, and then click **Power Options**.
2. Right-click **Power Options**, hover over **New**, and then click **Power Plan (At least Windows 7)**.
3. In the **New Power Plan (At least Windows 7) Properties** dialog box, click in the **Balanced** drop-down list and then type **Adatum Power Plan**.
4. Select the **Set as the active power plan** check box.

Target the preference

1. On the **Common** tab, select the **Item-level targeting** check box, and then click **Targeting**.
2. In the **Targeting Editor** dialog box, click **New Item**, and then click **Operating System**.
3. In the **Product** list, select **Windows 10**, and then click **OK** twice.
4. Close the **Group Policy Management Editor** window.

Test the preferences

1. Sign in to **LON-CL1** as **Adatum\Administrator** with password **Pa$$w0rd**.
2. Right-click **Start**, and then click **Command Prompt**.
3. In the **Command Prompt** window, type the following command, and then press Enter:

```
gpupdate /force
```

4. In the command prompt window, when prompted, type the following, and then press Enter:

```
Y
```

5. Sign in to **LON-CL1** as **Adatum\Administrator** with password **Pa$$w0rd**.
6. Right-click **Start**, and then click **Control Panel**.
7. Click **Hardware and Sound** and then click **Devices and Printers**.
8. Verify the presence of the **Brother on LON-DC1** printer.
9. Click the back arrow, and then click **Power Options**.
10. Verify that the **Adatum Power Plan** is present and is the active power plan.

Module Review and Takeaways

Best Practices

Best Practices Related to Group Policy Management

- When configuring settings in GPOs, include comments on GPO settings.
- Use a central store for Administrative templates.
- Use Group Policy preferences to configure settings that are not available in Group Policy settings.

Review Questions

Question: Why do some Group Policy settings take two sign-ins before taking effect?

Answer: Users typically sign in with cached credentials, which can prevent Group Policy from applying to the current session. The settings will take effect at the next sign-in.

Question: What is the benefit of having a central store?

Answer: A central store is a single folder in SYSVOL that holds all the .admx and .adml files that are required. After you have set up the central store, the Group Policy Management Editor recognizes it and then loads all Administrative templates from the central store, instead of from the local machine.

Question: What is the main difference between Group Policy settings and Group Policy preferences?

Answer: Group Policy settings enforce some settings on the client side, and they disable client interfaces for modification. However, Group Policy preferences provide settings, and they allow clients to modify them.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
You have configured Folder Redirection for an OU, but none of the users' folders are redirecting to the network location. When you look in the root folder, you observe that a subdirectory named for each user has been created, but they are empty.	The problem is most likely permissions-related. Group Policy creates users' named subdirectories, but users do not have enough permissions to create the redirected folders inside them.
You have a mixture of Windows 7 and Windows 10 computers. After configuring several settings in the Administrative templates of a GPO, users with Windows 7 operating systems report that some settings apply and others do not.	Not all new settings apply to older operating systems such as Windows 7. Check the setting itself to see to which operating systems the setting applies.
Group Policy preferences do not apply.	Check the preference settings for item-level targeting or incorrect configuration.

Lab Review Questions and Answers

Lab: Managing user settings with Group Policy

Question and Answers

Question: Which options can you use to separate users' redirected folders to different servers?

Answer: You can use the **Advanced** setting in Folder Redirection to choose different shared folders on different servers for different security groups.

Question: Can you name two methods that you could use to assign a GPO to selected objects within an OU?

Answer: You could use Windows Management Instrumentation (WMI) filters to define a criterion for applying Group Policy, such as whether or not the machine is a laptop or what version of the operating system is installed. You also could use permissions on the GPO itself to allow or deny GPO settings to users or computers.

Question: You have created Group Policy preferences to configure new power options. How can you make sure that they apply only to laptop computers?

Answer: You could use item-level targeting to apply the preference to portable computers. Then, the preference will apply if the hardware profile of the computer identifies it as a portable computer.

Module 7

Securing Active Directory Domain Services

Contents:

Lesson 1

Securing domain controllers

Contents:

Question and Answers

Question: How can you provide extra security for hard drives in domain controllers?

> Answer: To provide an extra level of security, consider using BitLocker drive encryption to encrypt domain-controller hard drives.

Demonstration: Configuring a password replication policy

Demonstration Steps

Stage a delegated installation of an RODC

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **Active Directory Sites and Services**.
2. In **Active Directory Sites and Services**, in the navigation pane, click **Sites**. From the **Action** menu, click **New Site**.
3. In the **New Object – Site** dialog box, in the **Name** field, type **Munich**, select the **DEFAULTIPSITELINK** site link object, and then click **OK**.
4. In the **Active Directory Domain Services** message box, click **OK**.
5. Switch to **Server Manager**, click **Tools**, and then click **Active Directory Administrative Center**.
6. In **Active Directory Administrative Center**, in the navigation pane, click **Adatum (local)**, and then in the details pane, double-click the **Domain Controllers** organizational unit (OU).
7. In the **Tasks** pane, in the **Domain Controllers** section, click **Pre-create a Read-only domain controller account**.
8. In the **Active Directory Domain Services Installation Wizard**, on the **Welcome to the Active Directory Domain Services Installation Wizard** page, click **Next**.
9. On the **Network Credentials** page, click **Next**.
10. On the **Specify the Computer Name** page, type the computer name as **MUC-RODC1**, and then click **Next**.
11. On the **Select a Site** page, click **Munich**, and then click **Next**.
12. On the **Additional Domain Controller Options** page, accept the default settings, select the **DNS server** and **Global catalog** check boxes, and then click **Next**.
13. On the **Delegation of RODC Installation and Administration** page, click **Set**.
14. In the **Select User or Group** dialog box, in the **Enter the object name to select** field, type **Bill**, and then click **Check Names**.
15. Verify that Bill Norman is resolved, and then click **OK**.
16. On the **Delegation of RODC Installation and Administration** page, click **Next**.
17. On the **Summary** page, review your selection, and then click **Next**.
18. On the **Completing the Active Directory Domain Services Installation Wizard** page, click **Finish**.

View an RODC's password replication policy

1. In **Active Directory Administrative Center**, in the **Domain Controllers** OU, select **MUC-RODC1**.
2. In the **Tasks** pane, in the **MUC-RODC1** section, click **Properties**.
3. In the **MUC-DC1 (Disabled) Properties** dialog box, scroll down to **Extensions**, and then click the **Password Replication Policy** tab.
4. Review the default groups, users, and computers in the Password Replication Policy.
5. Leave the dialog box open.

Configure an RODC-specific password replication policy

1. Switch to **Server Manager**, click **Tools**, and then click **Active Directory Users and Computers**.
2. In the navigation pane, expand **Adatum.com**, and then click **Users**.
3. On the **Action** menu, click **New**, and then click **Group**.
4. In the **New Object – Group** dialog box, type the group name as **Munich Allowed RODC Password Replication Group**, and then click **OK**.
5. Double-click **Munich Allowed RODC Password Replication Group**, click the **Members** tab, and then click **Add**.
6. In the **Select Users, Contacts, Computers, Services Accounts, or Groups** dialog box, in the **Enter the object names to select** text box, type **Ana**, and then click **Check Names**.
7. In the **Multiple Names Found** dialog box, select **Ana Cantrell**, and then click **OK**.
8. In the **Select Users, Contacts, Computers, Service Accounts or Groups** dialog box, click **OK**, and then in the **Munich Allowed RODC Password Replication Group Properties** dialog box, click **OK**.
9. Close **Active Directory Users and Computers**.
10. Switch to **Active Directory Administrative Center**, and then open the **MUC-RODC1 Properties**. In the **Extensions** section, on the **Password Replication Policy** tab, click **Add**.
11. In the **Add Groups, Users and Computers** dialog box, select the **Allow passwords for the account to replicate to this RODC** option, and then click **OK**.
12. In the **Select Users, Computers, Service Accounts, or Groups** dialog box, in the **Enter the object names to select** text box, type **Munich**, click **Check Names**, and then click **OK**.
13. In the **MUC-RODC1 (Disabled)** dialog box, click **OK**.

Verify the resultant password policy

1. In **Active Directory Administrative Center**, in the **Tasks** pane, in the **MUC-RODC1** section, click **Properties**.
2. In the **MUC-RODC1 (Disabled) Properties** dialog box, in the **Extensions** section, on the **Password Replication Policy** tab, click **Advanced**.

   Note: The **Advanced Password Replication Policy for MUC-RODC1** dialog box displays all of the accounts with passwords that are stored in this RODC.

3. In the **Display users and computers that meet the following criteria** drop-down list, click **Accounts that have been authenticated to this Read-only Domain Controller**, and then tell students that this page will only show accounts that have the requisite permissions and that the RODC has authenticated.
4. On the **Resultant Policy** tab, click **Add**, and in the **Select Users or Computers** dialog box, in the **Enter the object name to select** field, type **Ana**, click **Check Names**, and then click **OK**.
5. Note that Ana has a **Resultant Setting** of **Allow**.
6. Close or cancel all dialog boxes.

Lesson 2

Implementing account security

Contents:

Question and Answers

Question: Which technology allows you to use biometric functionality to sign in to Windows devices?

> Answer: Windows Hello is a new technology in Windows 10 and Windows 10 Mobile that allows you to authenticate by using your fingerprint, an iris scan, or other biometric data.

Resources

Account-security options in Windows Server 2016

 Additional Reading: For more information on credentials protection and management, refer to: http://aka.ms/R5bfid

Demonstration: Configuring domain account policies

Demonstration Steps

Configure a domain-based password policy

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **Group Policy Management**.
2. In the **Group Policy Management Console**, expand **Forest: Adatum.com\Domains\Adatum.com\Group Policy Objects**, right-click **Default Domain Policy**, and then click **Edit**.
3. In the **Group Policy Management Editor** window, in the navigation pane, under **Computer Configuration**, expand **Policies\Windows Settings\Security Settings\Account Policies**, double-click **Password Policy**, and then double-click **Enforce password history**.
4. In the **Enforce password history Properties** dialog box, in the **Keep password history for** field, type **20**, click **OK**, and then double-click **Maximum password age**.
5. In the **Maximum password age Properties** dialog box, in the **Password will expire in** field, type **45**, click **OK**, and then double-click **Minimum password age**.
6. In the **Minimum password age Properties** dialog box, ensure that the **Password can be changed after** field is **1**, click **OK**, and then double-click **Minimum password length**.
7. In the **Minimum password length Properties** dialog box, in the **Password must be at least** field, type **10**, click **OK**, and then double-click **Password must meet complexity requirements**.
8. In the **Password must meet complexity requirements Properties** dialog box, click **Enabled**, and then click **OK**.
9. Do not close the **Group Policy Management Editor** window.

Configure an account lockout policy

1. In the **Group Policy Management Editor** window, in the navigation pane, click **Account Lockout Policy**, and then double-click **Account lockout duration**.
2. In the **Account lockout duration Properties** dialog box, click **Define this policy setting**, in the **Minutes** field, type **30**, and then click **OK**.
3. In the **Suggested Value Changes** dialog box, note the suggested values including the automatic configuration of **Account lockout threshold**, click **OK**, and then double-click **Reset account lockout counter after**.
4. In the **Reset account lockout counter after Properties** dialog box, in the **Reset account lockout counter after** field, type **15**, and then click **OK**.

5. Close the **Group Policy Management Editor** window and the **Group Policy Management Console**.

Demonstration: Configuring a fine-grained password policy

Demonstration Steps

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **Active Directory Administrative Center**.
2. In **Active Directory Administrative Center**, in the navigation pane, click **Adatum (local)**.
3. In the details pane, double-click the **Managers** OU.
4. In the details pane, locate and right-click the **Managers** group, and then click **Properties**.

   Note: Ensure that you open the **Properties** dialog box for the Managers group, and not the Managers OU.

5. In the **Managers** dialog box, under **Group scope**, click **Global**, and then click **OK**.
6. In **Active Directory Administrative Center**, in the navigation pane, click **Adatum (local)**.
7. In the details pane, double-click the **System Container**.
8. In the details pane, right-click the **Password Settings Container**, click **New**, and then click **Password Settings**.
9. In the **Create Password Settings** window, complete the following steps:
   a. In the **Name** field, type **ManagersPSO**.
   b. In the **Precedence** field, type **10**.
   c. Select the **Enforce minimum password length** check box, and then in the **Minimum password length (characters)** field, type **15**.
   d. Select the **Enforce password history** check box, and, then in the **Number of passwords remembered** field, type **20**.
   e. Select the **Password must meet complexity requirements** check box.
   f. Select the **Enforce minimum password age** check box, and then in the **User cannot change the password within (days)** field, type **1**.
   g. Select the **Enforce maximum password age** check box, and then in the **User must change the password after (days)** field, type **30**.
   h. Select the **Enforce account lockout policy** check box.
   i. In the **Number of failed logon attempts allowed** field, type **3**.
   j. In the **Reset failed logon attempts count** field, type **30**, and then click **Until an administrator manually unlocks the account**.
10. In the **Directly Applies To** section, click **Add**.

11. In the **Enter the object names to select** text box, type **Adatum\Managers**, click **Check Names**, and then click **OK**.
12. In the **Create Password Settings: ManagersPSO** window, click **OK**.
13. Close the **Active Directory Administrative Center**.

Lesson 3

Implementing audit authentication

Contents:

Question and Answers

Question: When a user signs in to a domain controller, a logon event is generated.

( ) True

( ) False

Answer:

( ) True

(√) False

Feedback:

When a user signs in to a domain controller, an account-logon event, and not a logon event, is generated.

Demonstration: Configuring authentication-related audit policies

Demonstration Steps

1. On **LON-DC1**, in **Server Manager**, click the **Tools** menu, and then click **Group Policy Management**.
2. In the **Group Policy Management Console**, in the navigation pane, expand **Forest: Adatum.com\Domains\Adatum.com\Group Policy Objects**, and then select the **Default Domain Controllers Policy**.
3. Right-click the **Default Domain Controllers Policy**, and then click **Edit**.
4. In the **Group Policy Management Editor** window, in the navigation pane, expand **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies**, and then click **Audit Policy**.
5. In the details pane, double-click **Audit account logon events**, and then explain the following configuration options:
   - If you select the **Define these policy settings** check box, the policy is applied.
   - If you select **Success**, only success audits are logged.
   - If you select **Failure**, only failure audits are logged.

   If multiple policies contain the setting, and it is defined differently, the success and failure options apply based on the last applied policy that defined those settings. If one policy defines success audits and another defines failure audits, they do not merge.
6. On the **Explain** tab, show and discuss the explanation. Click **Cancel** to close the **Audit account logon events Properties** dialog box.
7. Repeat steps five and six with the **Audit logon events** policy.
8. In the **Group Policy Management Editor** window, in the navigation pane, navigate to **Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy configuration\Audit Policies**, and then click **Audit Policies**.
9. In the **Audit Policies** policy, show the ten main categories, and then click **Account Logon**.
10. Show the four subcategories, and then double-click **Audit Kerberos Authentication Service**.
11. Show that the subcategory has the same settings as in the **Audit Policy Audit Account Logon** setting, and then explain that they are now on a more detailed level and allow a more selective auditing.
12. Select **Configure the following audit events**, select **Success**, select **Failure**, and then click **Apply**.

13. On the **Explain** tab, show and discuss the explanation, the default settings, and the predicted auditing volume.
14. To close the **Audit Kerberos Authentication Service Properties** dialog box, click **OK**.

Demonstration: Viewing logon events

Demonstration Steps

1. On **LON-DC1**, in the Start screen, type **cmd**, and then click **Command Prompt**.
2. Type **gpupdate /force**, and then press Enter.
3. Wait until the policy has been updated.
4. Switch to the Start screen. In the upper-right corner, click **Administrator**, and then click **Sign Out**.
5. On **LON-DC1**, attempt to sign in as **Adatum\Aidan** with password **123456**.
6. You will get a message that the user name or password is incorrect. Click **OK**.
7. Sign in as **Adatum\Administrator** with password **Pa$$w0rd**.
8. Wait until the logon is finished and **Server Manager** has started.
9. In **Server Manager**, click **Tools**, and then click **Event Viewer**.
10. In Event Viewer, in the navigation pane, expand **Windows Logs**, and then click **Security**.
11. In the details pane, locate the **Event ID 4771**, and then show that this event is an Audit Failure event. Double-click the **Audit Failure** event. Show that this event was logged when Adatum\Aidan tried to sign in with the wrong password. Click **Close**.
12. Locate the event with the **Event ID 4768**. Show that this is an Audit Success event. Double-click the **Audit Success** event. Show that this event was logged when Adatum\Administrator signed in successfully. Click **Close**.
13. Close Event Viewer.

Lesson 4

Configuring managed service accounts

Contents:

Question and Answers

Question: How are group MSAs different from standard MSAs?

> Answer: Group MSAs enable you to extend the capabilities of standard MSAs to more than one server in your domain.

Demonstration: Configuring group MSAs

Demonstration Steps

Create the KDS root key for the domain

1. On LON-DC1, from Server Manager, click Tools and open the Active Directory Module for Windows PowerShell console.
2. At the command prompt, type the following command, and then press Enter:

```
Add-KdsRootKey –EffectiveTime ((get-date).addhours(-10))
```

Create and associate an MSA

1. At the command prompt, type the following command, and then press Enter:

```
New-ADServiceAccount –Name SampleApp_SVR1 –DNSHostname LON-DC1.Adatum.com -
PrincipalsAllowedToRetrieveManagedPassword LON-SVR1$
```

2. At the command prompt, type the following command, and then press Enter:

```
Add-ADComputerServiceAccount –identity LON-SVR1 –ServiceAccount SampleApp_SVR1
```

3. At the command prompt, type the following command, and then press Enter:

```
Get-ADServiceAccount -Filter *
```

4. Verify that the SampleApp_SVR1 service account is listed.

Install an MSA

1. On LON-SVR1, click Start, click Server Manager, and then from the Tools menu, open the Active Directory Module for Windows PowerShell console.
2. At the command prompt, type the following command, and then press Enter:

```
Install-ADServiceAccount -Identity SampleApp_SVR1
```

3. In Server Manager, on the Menu toolbar, click Tools, and then click Services.
4. In the Services console, right-click Data Sharing Service, and then click Properties.

> Note: This demonstration uses the Data Sharing Service as an example. In a production environment, you would use the actual service that should be assigned the MSA.

5. In the Data Sharing Service Properties (Local Computer) dialog box, click the Log On tab.
6. On the Log On tab, click This account, and then type Adatum\SampleApp_SVR1$.
7. Clear the password for both the Password and Confirm password boxes, and then click OK.
8. Click OK at all prompts.

Module Review and Takeaways

Review Questions

Question: Why is physical security so important, especially for AD DS domain controllers?

> Answer: AD DS domain controllers store all information about all users, computers, groups, and any other objects in the domain. If someone gains physical access to the server or its hard drive, this person can circumvent security guards easily and retrieve all of this information. This person then can use the information to attack your network, or could modify your domain controller and put it back into the network with malicious intent.

Question: You need to implement auditing policies for domain authentication and changes to directory services. What is the best way to implement these auditing settings?

> Answer: If you want to enable auditing, it is very important that you configure the same auditing settings for all relevant servers on which the event might occur. If you want to configure auditing for domain authentication or changes in AD DS, configure these settings in the Default Domain Controllers Policy or a GPO that is linked to the Domain Controllers OU.

Question: Your organization requires you to maintain a highly reliable and secure AD DS infrastructure. It also requires that users can access corporate email from the Internet by using Outlook Web Access. You are considering implementing account-lockout settings. What must you consider?

> Answer: Account-lockout settings are not just a security feature. They also provide attackers an easily accessible DoS interface. If Outlook Web Access is accessible from the Internet, you must configure additional protocols or services to ensure that only your domain users are able to enter their logon credentials. Other users must not be allowed to use the website to enter false passwords and lock out valid user accounts.

Tools

The following table lists the tools that this module references.

1. Tool	2. Use for	3. Where to find it
Active Directory Users and Computers	Managing objects within AD DS, such as users, groups, and computers.	Server Manager
Active Directory Administrative Center	Managing objects within AD DS, such as users, groups, and computers.	Server Manager
Group Policy Management	Managing, reporting, backup, and restoration of GPOs.	Server Manager
Gpupdate.exe	Manually updating the GPOs of local machines.	Command-line

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
You have configured advanced auditing policy settings, but they do not apply.	Verify that you have set the Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings policy setting under Computer Configuration\Policies\Windows

Common Issue	Troubleshooting Tip
	Settings\Security Settings\Local Policies\Security Options.
You have configured auditing of account logon or directory services changes. Now you are testing them, but you cannot find the events in your server's event log.	If you have multiple domain controllers, you need to look at the Security log of every domain controller. Also, ensure that you have the auditing policy configured for every domain controller.

Lab Review Questions and Answers

Lab: Securing AD DS

Question and Answers

Question: In the lab, you configured the password settings for all users within the Default Domain Policy, and you configured the password settings for Administrators within a PSO. What other options were available to help you accomplish the solution?

> **Answer:** You could have created a PSO with specific settings for all users, configured it with a very high precedence, and linked it to the Domain Users security group. The benefit would be that there is only one interface for managing domain password policies, and the default settings for local accounts on domain members can be set differently across the whole domain.

Question: In the lab, you were using precedence for the administrative PSO with a value of 10. What is the reason for this?

> **Answer:** The administrative PSO is very restrictive, so the precedence should be low. However, there might be groups of administrators in the future with more restrictive settings, such as a subset of administrators to access human-resources data, or service accounts for which you might want to enforce longer passwords with administrative rights that change less frequently. For these reasons, using a value of 10 allows some space for implementing PSOs that are more precise.

Module 8

Deploying and managing AD CS

Contents:

Lesson 1

Deploying CAs

Contents:

Question and Answers

Question: Which of the following options describe the advantages of deploying an enterprise CA instead of a standalone CA?

( ) Provides multiple ways in which users and devices can receive certificates.

( ) Does not require AD DS.

( ) Certificate requests can be issued or denied automatically based on policy.

( ) Can be taken offline to prevent compromise.

( ) Can use templates to issue certificates based on data in AD DS.

Answer:

(√) Provides multiple ways in which users and devices can receive certificates.

( ) Does not require AD DS.

(√) Certificate requests can be issued or denied automatically based on policy.

( ) Can be taken offline to prevent compromise.

(√) Can use templates to issue certificates based on data in AD DS.

Feedback:

The advantages of an enterprise CA are that you can take advantage of multiple ways to enroll for certificates, including autoenrollment by using certificate templates. Enterprise CAs also allow for automatic approval or denial of requests based on issuance policies. Enterprise CAs, however, require AD DS and must be left online to facilitate certificate enrollment.

Question: Which of the following options are reasons for which you might deploy multiple subordinate CAs?

( ) You want to segment certificate issuance based on unique usage policies.

( ) You have multiple domains in your AD DS environment and each domain requires its own subordinate CA.

( ) You want to segment certificate issuance based on organizational division or geographic region.

( ) You want multiple subordinate CAs for high availability and load balancing of requests.

( ) You need to publish multiple certificate templates and each template requires its own subordinate CA.

Answer:

(√) You want to segment certificate issuance based on unique usage policies.

( ) You have multiple domains in your AD DS environment and each domain requires its own subordinate CA.

(√) You want to segment certificate issuance based on organizational division or geographic region.

(√) You want multiple subordinate CAs for high availability and load balancing of requests.

( ) You need to publish multiple certificate templates and each template requires its own subordinate CA.

Feedback:

You might deploy multiple CAs for unique usage policies, organizational divisions, or geographic regions. In addition, you might deploy multiple CAs to ensure high availability for load balancing of requests.

Multiple subordinate CAs are not required in a multi-domain AD DS environment, although you might use this approach if your AD DS domains already align to organizational divisions or geographic regions. Multiple subordinate CAs are not required if you need to publish different certificate templates because a CA can be configured to issue certificates from more than one template.

Demonstration: Deploying an enterprise root CA

Demonstration Steps

Deploy an enterprise root CA

1. On **LON-SVR1**, click **Start**, and then click **Server Manger**.
2. In **Server Manager**, click **Add roles and features**.
3. On the **Before you begin** page, click **Next**.
4. On the **Select installation type** page, click **Next**.
5. On the **Select destination server** page, click **Next**.
6. On the **Select server roles** page, select **Active Directory Certificate Services**.
7. In the **Add Roles and Features Wizard**, click **Add Features**, and then click **Next**.
8. On the **Select features** page, click **Next**.
9. On the **Active Directory Certificate Services** page, click **Next**.
10. On the **Select role services** page, ensure that **Certification Authority** is selected, and then click **Next**.
11. On the **Confirm installation selections** page, click **Install**.
12. On the **Installation progress** page, after the installation completes successfully, click the **Configure Active Directory Certificate Services on the destination server** text.
13. In the **AD CS Configuration** wizard, on the **Credentials** page, click **Next**.
14. On the **Role Services** page, select **Certification Authority**, and then click **Next**.
15. On the **Setup Type** page, select **Enterprise CA**, and then click **Next**.
16. On the **CA Type** page, click the **Root CA** option, and then click **Next**.
17. On the **Private Key** page, ensure that **Create a new private key** is selected, and then click **Next**.
18. On the **Cryptography for CA** page, keep the default selections for Cryptographic Service Provider (CSP) and Hash Algorithm, but set the Key length to **4096**, and then click **Next**.
19. On the **CA Name** page, in the **Common name for this CA** box, type **AdatumRootCA**, and then click **Next**.
20. On the **Validity Period** page, click **Next**.
21. On the **CA Database** page, click **Next**.
22. On the **Confirmation** page, click **Configure**.
23. On the **Results** page, click **Close**.
24. On the **Installation progress** page, click **Close**.

Lesson 2

Administering CAs

Contents:

Question and Answers

Question: Which of the following options are true statements regarding role-based administration of your AD CS deployment?

( ) AD CS automatically creates three built-in roles and groups for CA Administrator, Certificate Manager, and Enrollee.

( ) You can grant AD CS role groups one or more of the following CA permissions: Manage CA, Issue and Manage Certificates, Read, Request Certificates.

( ) You can limit the Issue and Manage Certificates CA permission to a specific template or set of templates.

( ) You can create custom AD CS role groups based upon the specific needs of your organization.

( ) The Authenticated Users security principal can enroll for any certificate published on a CA.

Answer:

( ) AD CS automatically creates three built-in roles and groups for CA Administrator, Certificate Manager, and Enrollee.

(√) You can grant AD CS role groups one or more of the following CA permissions: Manage CA, Issue and Manage Certificates, Read, Request Certificates.

(√) You can limit the Issue and Manage Certificates CA permission to a specific template or set of templates.

(√) You can create custom AD CS role groups based upon the specific needs of your organization.

( ) The Authenticated Users security principal can enroll for any certificate published on a CA.

Feedback:

Role-based administration in AD CS is a concept, not a feature that is installed automatically; therefore, you must manually create any role groups. After you have created a role group, you can assign it one or more of the following CA permissions: Manage CA, Issue and Manage Certificates, Read, Request Certificates. You can customize the roles according to the needs of your organization, including restriction of the Issue and Manage Certificates permission to a specific template or set of templates. The Authenticated Users security principal can request any certificate, but the certificate template controls the ability to enroll, not the CA itself.

Question: Which of the following are true statements regarding the AIA and CDP extensions of a CA?

( ) Each extension requires a minimum of two valid and accessible URLs for certificate validation to function properly.

( ) You can manually publish offline and standalone CA certificates and CRLs into an AD DS environment.

( ) The order in which you specify AIA and CDP URLs is not important as the certificate-chaining engine automatically orders locations based on the fastest connection.

( ) To facilitate certificate validation for external clients, you should publish external AIA and CDP URLs using HTTP through a Windows Server 2016 Web Application Proxy.

( ) If you are using an enterprise CA, internal certificate validation will work without any additional configuration.

Answer:

( ) Each extension requires a minimum of two valid and accessible URLs for certificate validation to function properly.

(√) You can manually publish offline and standalone CA certificates and CRLs into an AD DS environment.

( ) The order in which you specify AIA and CDP URLs is not important as the certificate-chaining engine automatically orders locations based on the fastest connection.

(√) To facilitate certificate validation for external clients, you should publish external AIA and CDP URLs using HTTP through a Windows Server 2016 Web Application Proxy.

(√) If you are using an enterprise CA, internal certificate validation will work without any additional configuration.

Feedback:

For certificate validation to function, the AIA and CDP extensions must contain a minimum of one valid and accessible URL. For offline and standalone CAs, you can manually publish the CA certificate and CRL into AD DS. The order of AIA and CDP URLs is important, as the certificate-chaining engine will search them sequentially. You should place the URLs most likely to be available at the top of the URL order. To facilitate certificate validation for external clients, you can publish AIA and CDP URLs by using HTTP through a Windows Server 2016 Web Application Proxy or other third-party reverse proxy solution. If you are using an enterprise CA, certificate validation will work automatically for internal clients, but might require further configuration in other scenarios.

Resources

Managing CAs

Additional Reading: For more information, refer to:

- AD CS Deployment Cmdlets in Windows PowerShell http://aka.ms/Giih2g
- AD CS Administration Cmdlets in Windows PowerShell http://aka.ms/Dekm5i

Demonstration: Configuring CA properties

Demonstration Steps

1. On **LON-SVR1**, open **Server Manager**, click **Tools**, and then click **Certification Authority**.
2. In the Certsrv console, right-click **AdatumRootCA**, and then select **Properties**.
3. On the **General** tab, click **View Certificate**. When the Certificate window opens, review the data on the **General**, **Details**, and **Certification Path** tabs, and then click **OK**.
4. On the **Policy Module** tab, click **Properties**. Review the settings available for the Default policy module, and then click **OK**.
5. On the **Exit Module** tab, click **Properties**. Show the Publication Settings available in the default Exit module, and then click **OK**.
6. On the **Extensions** tab, review the options available for the CDP and AIA extension under the **Select extension** drop down list.
7. On the **Security** tab, review the available options on the access control list (ACL), and review the default permissions.
8. On the **Certificate Managers** tab, review the options and explain how to restrict security principals to specific certificate templates, and then click **Cancel**.
9. Close the Certsrv console.

Lesson 3

Troubleshooting and maintaining CAs

Contents:

Question and Answers

Question: Which of the following issues could prevent autoenrollment from correctly working in AD CS?

( ) The computer that you expect to autoenroll for a certificate is in an AD DS OU where policy inheritance is blocked.

( ) The user that you expect to autoenroll for a certificate is in an AD DS OU where the necessary Group Policy setting is not linked or inherited.

( ) The CA is a standalone CA.

( ) The certificate template is not published on a CA.

( ) The AIA URL is configured incorrectly on the extensions tab of the CA.

Answer:

(√) The computer that you expect to autoenroll for a certificate is in an AD DS OU where policy inheritance is blocked.

(√) The user that you expect to autoenroll for a certificate is in an AD DS OU where the necessary Group Policy setting is not linked or inherited.

(√) The CA is a standalone CA.

(√) The certificate template is not published on a CA.

( ) The AIA URL is configured incorrectly on the extensions tab of the CA.

Feedback:

Group Policy object inheritance is a common issue that can prevent autoenrollment. Users and computers must be in an AD DS organization where you have linked the required GPO settings and not blocked policy inheritance. Additionally, CAs must be enterprise CAs for autoenrollment to work correctly, because clients use AD DS to determine the available CAs and templates. You must publish templates on an enterprise CA, and the user or computer must have the autoenroll permissions configured on the template. An invalid AIA or CDP URL configured on the CA will not prevent autoenrollment, but it may prevent the certificate from validating correctly when used by a client application or service.

Question: Which of the following are true statements regarding the PKIVIew tool?

( ) PKIView shows all of your enterprise CAs and their current health state.

( ) You can use PKIView to manually add standalone CAs.

( ) You can use PKIView to configure autoenrollment for users and computers.

( ) PKIView evaluates the CDP or AIA state for each location defined on each CA.

( ) PKIView can evaluate the status of the AD CS Online Responder role service.

Answer:

(√) PKIView shows all of your enterprise CAs and their current health state.

( ) You can use PKIView to manually add standalone CAs.

( ) You can use PKIView to configure autoenrollment for users and computers.

(√) PKIView evaluates the CDP or AIA state for each location defined on each CA.

(√) PKIView can evaluate the status of the AD CS Online Responder role service.

Feedback:

You can use PKIView to see all of your enterprise CAs and their current health state, but it cannot show the status of a standalone CA. You configured autoenrollment for users and computers through Group Policy, not through the PKIView tool. PKIVIew allows you to evaluate the CDP and AIA state for each location defined on each CA as well as the status of the AD CS Online Responder role service, if you have deployed it.

Module Review and Takeaways

Best Practices

- When deploying a CA infrastructure, deploy a standalone (not domain-joined) root CA and an enterprise subordinate CA (issuing CA). After the enterprise subordinate CA receives a certificate from the root CA, take the root CA offline.
- Review the validation time of root CA certificate revocation lists (CRLs).
- Provide more than one location for AIA and CRL.

Review Questions

Question: What are some reasons that an organization would use a PKI?

> Answer: Some of the reasons to use a PKI include improving security, increasing identity control, and signing code digitally.

Question: Why would you deploy a custom policy and exit modules?

> Answer: If you have an additional application for certificate management, such as MIM Certificate Management, you will have to install a custom policy and exit modules so that you can integrate your application with CA.

Tools

- CA admin console
- Certutil command-line utility
- Windows PowerShell command-line interface
- PKIView.msc
- Server Manager

Common Issues and Troubleshooting Tips

Common Issue
The location of the CA certificate that is specified in the AIA extension is not configured to include the certificate name suffix issuing CA's certificate to build a certificate chain, and certificate validation might fail.
The CA is not configured to include CDP locations in the extensions of issued certificates. Clients might not be able to locate validation might fail.

Lab Review Questions and Answers

Lab: Deploying and configuring a two-tier CA hierarchy

Question and Answers

Question: Why is it not recommended to install only an enterprise root CA?

Answer: For security reasons, a root CA should be taken offline and should not have any network access. Because the enterprise root CA cannot be offline, you cannot provide maximum protection for its key and identity.

Question: What are some reasons that an organization would use an enterprise root CA?

Answer: If an organization wants to use only one CA, and it wants to use certificate templates and autoenrollment, an enterprise root CA is the only choice.

Module 9

Deploying and managing certificates

Contents:

Lesson 1

Deploying and managing certificate templates

Contents:

Question and Answers

Question: Which of the following statements are true regarding version 2 certificate templates in AD CS? (Choose all that apply.)

( ) Version 2 templates support autoenrollment.

( ) You can only modify the Security tab on a version 2 template.

( ) You can upgrade to a version 2 template by duplicating a version 1 template.

( ) Version 2 templates are only supported on Windows Server 2008 and Windows Vista or later operating systems.

( ) Version 2 templates are only supported on Windows Server 2012 and Windows 8 or later operating systems.

Answer:

(√) Version 2 templates support autoenrollment.

( ) You can only modify the Security tab on a version 2 template.

(√) You can upgrade to a version 2 template by duplicating a version 1 template.

( ) Version 2 templates are only supported on Windows Server 2008 and Windows Vista or later operating systems.

( ) Version 2 templates are only supported on Windows Server 2012 and Windows 8 or later operating systems.

Feedback:

One important aspect of version 2 templates is that they support autoenrollment by AD DS users and computers. Unlike version 1 templates, you can modify all aspects of a version 2 template. To upgrade to a version 2 template, you can duplicate a version 1 template. Version 2 templates are supported on Windows Server 2003 Enterprise Edition, Windows Server 2008 Enterprise, and Windows Server 2008 R2 and later. Version 2 templates are fully supported as long as the CA is running Windows Server 2008 or later.

Question: You are the AD CS administrator for A. Datum Corporation. Several users in your AD DS environment have autoenrolled for a user certificate. You want to shorten the validity period of the user certificate and need to ensure that users get a new certificate immediately without experiencing any break in validity of the existing certificate. Which of the following actions should you take? (Choose all that apply.)

( ) Duplicate the existing template and provide a new template name. Modify the validity period of the new template.

( ) Modify the validity period of the existing template.

( ) Modify the autoenrollment settings of the existing template.

( ) Revoke all user certificates issued from the existing template.

( ) Modify the new template so that it supersedes the existing template. Publish the new template.

Answer:

(√) Duplicate the existing template and provide a new template name. Modify the validity period of the new template.

( ) Modify the validity period of the existing template.

( ) Modify the autoenrollment settings of the existing template.

(√) Revoke all user certificates issued from the existing template.

(√) Modify the new template so that it supersedes the existing template. Publish the new template.

Feedback:

In this situation, you should duplicate the existing template, providing a new template name and validity period. In addition, you should update the new template so that it supersedes the previous template. After you publish the new template to an enterprise CA, users who had autoenrolled against the previous template will autoenroll again for the new template. Once new certificates with the correct validity period have replaced the previously issued certificates, you should revoke all user certificates from the existing template so they can no longer be used.

If you modify the validity period of the existing template, new enrollments against the template will have the correct settings, but previously issued certificates will still contain the undesired validity period. Modifying the autoenrollment settings on the existing template is not necessary and would not achieve the desired effect.

Demonstration: Modifying and enabling a certificate template

Demonstration Steps

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **Certification Authority**.
2. In the **Certification Authority** console, expand **AdatumCA**, right-click **Certificate Templates**, and then click **Manage**.
3. Review the list of default templates. Examine the templates and their properties.
4. In the **Details** pane, double-click **IPSec**.
5. In the **IPsec Properties** dialog box, click through the tabs, and then notice what you can modify on each. Notice that on the **Security** tab, you can define permissions for enrollment. Click **Cancel** to close the template.
6. In the **Certificate Templates Console**, in the **Details** pane, right-click the **Exchange User** certificate template, and then click **Duplicate Template**.
7. In the **Properties of New Template** dialog box, review options on the **Compatibility** tab.
8. Click the **General** tab, and then in the **Template display name** text box, type **Exchange User Test1**.
9. Click the **Superseded Templates** tab, and then click **Add**.
10. Click the **Exchange User** template, and then click **OK**.
11. Click the **Security** tab, and then click **Authenticated Users**.
12. Under the **Permissions for Authenticated Users** node, select the **Allow** check boxes for both **Enroll** and **Autoenroll**, and then click **OK**.
13. Close the **Certificate Templates** console.
14. In the **Certification Authority** console, right-click **Certificate Templates**, point to **New**, and then click **Certificate Template to Issue**.
15. In the **Enable Certificate Templates** dialog box, select the **Exchange User Test1** certificate, and then click **OK**.

Lesson 2

Managing certificate deployment, revocation, and recovery

Contents:

Question and Answers

Question: When you revoke a certificate, where is the thumbprint of the certificate published?

( ) CRL distribution point (CDP)

( ) Authority information access (AIA)

( ) Certificate revocation list (CRL)

( ) AD DS

( ) The Online Responder service

Answer:

( ) CRL distribution point (CDP)

( ) Authority information access (AIA)

(√) Certificate revocation list (CRL)

( ) AD DS

( ) The Online Responder service

Feedback:

When you revoke a certificate, the thumbprint of the certificate is published to the certificate revocation list (CRL). A CRL distribution point (CDP) is the URL location where the CRL is stored. The authority information access (AIA) is the URL where the CA certificate is located. AD DS is a valid location for a CDP, but revoked certificates are not directly published to AD DS. An Online Responder service validates the status of a specific certificate using a local copy of the CRL, but revoked certificates are not published directly to an Online Responder service.

Question: Which of the following actions must you take to configure key archival on an AD CS CA? (Choose all that apply.)

( ) Configure the KRA certificate template.

( ) Enroll a designated user for a KRA certificate.

( ) Publish the KRA public key by using Group Policy.

( ) Configure a recovery agent on the CA.

( ) Configure desired certificate templates for key archival.

Answer:

(√) Configure the KRA certificate template.

(√) Enroll a designated user for a KRA certificate.

( ) Publish the KRA public key by using Group Policy.

(√) Configure a recovery agent on the CA.

(√) Configure desired certificate templates for key archival.

Feedback:

To configure key archival, you should:

1. Configure the KRA certificate so that only trusted users can enroll for a certificate.
2. Enroll a trusted user for the KRA certificate.
3. Configure a recovery agent on the CA by using the KRA certificate.
4. Configure the desired certificate templates for key archival.

You do not need to publish the KRA public key by using Group Policy.

Demonstration: Configuring a CA for key archival

Demonstration Steps

1. On **LON-DC1**, in **Server Manager**, click **Tools**, then click **Certification Authority**. In the **Certification Authority** console, expand the **AdatumCA** node, right-click the **Certificates Templates** folder, and then click **Manage**.
2. In the **Details** pane, right-click the **Key Recovery Agent** certificate, and then click **Properties**.
3. In the **Key Recovery Agent Properties** dialog box, click the **Issuance Requirements** tab, clear the **CA certificate manager approval** check box, and then click the **Security** tab. Notice that the Domain Admins and Enterprise Admins groups are the only groups that have the **Enroll** permission, and then click **OK**.
4. Close the **Certificate Templates** console.
5. In the **Certification Authority Console**, right-click **Certificate Templates**, point to **New**, and then click **Certificate Template to Issue**.
6. In the **Enable Certificate Templates** dialog box, click the **Key Recovery Agent** template, and then click **OK**.
7. Click **Start**, and then click the **Windows PowerShell** icon.
8. At the Windows PowerShell command prompt, type **mmc.exe**, and then press Enter.
9. In the **Console1-[Console Root]** console, click **File**, and then click **Add/Remove Snap-in**.
10. In the **Add or Remove Snap-ins** dialog box, click **Certificates**, and then click **Add**.
11. In the **Certificates snap-in** dialog box, select **My user account**, click **Finish**, and then click **OK**.
12. Expand the **Certificates - Current User** node, right-click **Personal**, point to **All Tasks**, and then click **Request New Certificate**.
13. In **Certificate Enrollment Wizard**, on the **Before You Begin** page, click **Next**.
14. On the **Select Certificate Enrollment Policy** page, click **Next**.
15. On the **Request Certificates** page, select the **Key Recovery Agent** check box, click **Enroll**, and then click **Finish**.
16. Refresh the console, and then view the KRA in the personal store; that is, scroll across the certificate properties and verify that the certificate template with intended purpose **Key Recovery Agent** is present.
17. Close **Console1** without saving changes.
18. Return to the **Certification Authority** console, right-click **AdatumCA**, and then click **Properties**.
19. In the **AdatumCA Properties** dialog box, click the **Recovery Agents** tab, and then select **Archive the key**.
20. Under Key recovery agent certificates, click **Add**.
21. In the **Key Recovery Agent Selection** dialog box, click the certificate that is for the KRA purpose (it most likely will be last on the list issued to **Administrator**), and then click **OK** twice.
22. When prompted to restart the CA, click **Yes**.

Lesson 3

Using certificates in a business environment

Contents:

Question and Answers

Question: Which of the following are true statements regarding the use of certificates in a business environment? (Choose all that apply.)

( ) Certificates can be used to encrypt HTTP traffic between a web server and browser.

( ) Certificates can be used to digitally sign documents.

( ) Digitally signed documents are invalidated if the contents are modified.

( ) To send encrypted e-mail to an external recipient who is not part of your internal PKI, you must use an encryption certificate issued by a public CA.

( ) Files encrypted using Encrypting File System (EFS) can only be read by the individual who first encrypted the file.

Answer:

(√) Certificates can be used to encrypt HTTP traffic between a web server and browser.

(√) Certificates can be used to digitally sign documents.

(√) Digitally signed documents are invalidated if the contents are modified.

( ) To send encrypted e-mail to an external recipient who is not part of your internal PKI, you must use an encryption certificate issued by a public CA.

( ) Files encrypted using Encrypting File System (EFS) can only be read by the individual who first encrypted the file.

Feedback:

Certificates can be used for encrypting HTTP traffic, to digitally sign and/or encrypt documents and e-mails, and for client/server authentication. Digitally signed documents are invalidated if the contents are modified. To send encrypted e-mail to an external recipient, you can use either an internal or publically issued certificate as long as you have access to the public key of the recipient. Files encrypted using EFS can be read by the individual who encrypted the file and by any users explicitly designated for EFS sharing. If the private key of the encrypting individual is lost or deleted, a Data Recovery Agent can access the file or a Key Recovery Agent can be used to retrieve the private key if key archival was previously configured on the EFS certificate template and issuing CA.

Question: You are the AD CS administrator for A. Datum. You want to enable your AD DS users to perform digital signature and encryption using certificates from your internal PKI. Which of the following steps are required?

( ) Enable a key recovery agent.

( ) Enable a data recovery agent.

( ) Publish the User certificate template and configure the desired groups of users for autoenrollment.

( ) Enable EFS on AD DS domain computers by using Group Policy.

( ) Upgrade all AD DS domain computers to Windows Server 2016 or Windows 10.

Answer:

( ) Enable a key recovery agent.

( ) Enable a data recovery agent.

(√) Publish the User certificate template and configure the desired groups of users for autoenrollment.

( ) Enable EFS on AD DS domain computers by using Group Policy.

( ) Upgrade all AD DS domain computers to Windows Server 2016 or Windows 10.

Feedback:

To enable digital signature and encryption, you should only need to publish the User certificate template and configure it for autoenrollment. Although using a key recovery agent and data recovery agent are best practices, they are not required to enable digital signatures and encryption. You do not need to enable EFS on AD DS domain computers, nor do you need to upgrade all AD DS domain computers to Windows Server 2016 or Windows 10.

Demonstration: Signing a document digitally

Demonstration Steps

1. On **LON-CL1**, open the **Windows PowerShell** command-line interface.
2. At the **Windows PowerShell** command prompt, type **mmc.exe**, and then press Enter.
3. In the **Console1 – [Console Root]** window, click the **File** menu, and then select **Add/Remove Snap-in**.
4. Select **Certificates**, click **Add**, select **My user account**, click **Finish**, and then click **OK**.
5. Expand **Certificates - Current User**, right-click **Personal**, select **All Tasks**, and then click **Request New Certificate**.
6. In **Certificate Enrollment Wizard**, click **Next** twice.
7. On the **Certificate Enrollment** page, in the list of available templates, select **User**, click **Enroll**, and then click **Finish**.
8. Close the **Console1 – [Console Root]** window without saving changes.
9. Open Word 2016.

 **Note:** If the **Microsoft Office Activation Wizard** appears, click **Close**. Click **Ask me later**, then click **Accept**.

10. In a blank document, type some text, and then save the file to the desktop.
11. On the toolbar, click **INSERT**, and then in the **Text** pane, in the **Signature Line** drop-down list, click **Microsoft Office Signature Line**.
12. In the **Signature Setup** window, type your name in the **Suggested signer** text box, type **Administrator** in the **Suggested signer's title** text box, type **Administrator@adatum.com** in the **Suggested signer's email address** text box, and then click **OK**.
13. Right-click the signature line in the document, and then click **Sign.**
14. In the **Sign** window, click **Change**.
15. In the **Certificate** list, select the certificate with today's date, and then click **OK**.
16. In the text box to the right of the X, type your name, click **Sign**, and then click **OK**.

 **Note:** Ensure that you explain to students that besides typing your name, you can select an image instead. This image can be your scanned, handwritten signature.

17. Ensure that the document cannot be edited anymore.
18. Close Word 2016, and then save the changes when prompted.
19. Stay signed in for the next demonstration.

Demonstration: Encrypting a file with EFS

Demonstration Steps

1. On **LON-CL1**, right-click the Word document that you saved to the desktop in the previous demonstration, and then click **Properties**.
2. On the **General** tab of the **Properties** dialog box, click **Advanced**, click **Encrypt contents to secure data**, and then click **OK** twice.
3. In the prompt window, select **Encrypt the file only**, and then click **OK**.
4. Move the document that you encrypted to the **C:\Users\Public\Public Documents** folder.
5. Sign out of **LON-CL1**.
6. Sign in as **Adatum\Aidan** with the password **Pa$$w0rd**.
7. Open File Explorer, and then go to **C:\Users\Public\Public Documents**.
8. Try to open the encrypted document.
9. Verify that you cannot open the document.
10. Sign out of **LON-CL1**.

Lesson 4

Implementing and managing smart cards

Contents:

Question and Answers

Question: Which of the following statements are true regarding smart cards?

( ) Smart cards provide an option for multifactor authentication.

( ) Smart cards cannot be used for interactive sign in.

( ) Smart cards contain a certificate and private key that can only be accessed by using a PIN.

( ) Smart cards provide enhanced security beyond a password.

( ) Smart cards can only be used for digital signature and encryption.

Answer:

(√) Smart cards provide an option for multifactor authentication.

( ) Smart cards cannot be used for interactive sign in.

(√) Smart cards contain a certificate and private key that can only be accessed by using a PIN.

(√) Smart cards provide enhanced security beyond a password.

( ) Smart cards can only be used for digital signature and encryption.

Feedback:

Smart cards provide an option for multifactor authentication: users must have the smart card in their physical possession and must additionally know their PIN. By entering the PIN, certificates and private keys stored on the smart card become available for authentication, digital signature, and encryption. Using smart cards for interactive sign in provides enhanced security beyond a password.

Question: When implementing a smart card infrastructure, which of the following processes should be part of your certificate management framework?

( ) Issuance

( ) Revocation

( ) Renewal

( ) Blocking and unblocking

( ) Suspension

Answer:

(√) Issuance

(√) Revocation

(√) Renewal

(√) Blocking and unblocking

(√) Suspension

Feedback:

All of the above are correct processes that you should include in your certificate management plan. Some of the processes can be performed with built-in utilities; however, because of the complexity involved, we recommend that you implement a dedicated solution for smart card and certificate management, such as MIM.

Module Review and Takeaways

Best Practices

- When replacing old certificate templates, use superseding templates.
- Always archive certificates that are used for encryption purposes.
- Use autoenrollment for mass deployment of certificates.
- If you are using smart cards, make sure that users change their PINs regularly.
- If you are using smart cards, implement a smart card management solution.

Review Questions

Question: List the requirements to use autoenrollment for certificates.

> **Answer:** To use autoenrollment for certificates, you must have an enterprise CA, and you must configure Group Policy options. In addition, you must enable autoenrollment for the desired certificate templates, and you must configure Group Policy Objects.

Question: How do virtual smart cards work?

> **Answer:** Virtual smart cards emulate the functionality of traditional smart cards, but instead of requiring the purchase of additional hardware, they utilize technology that users already own and likely have with them at all times.

Real-world Issues and Scenarios

Contoso, Ltd. wants to deploy a PKI to support and secure several services. It has decided to use Windows Server 2016 AD CS as a platform for PKI. Certificates will be used primarily for EFS, digital signing, and for web servers. Because documents that will be encrypted are important, it is crucial to have a disaster recovery strategy in case of key loss. In addition, clients that will access secure parts of the company website must not receive any warning in their browsers.

- What kind of deployment should Contoso choose?
- What kind of certificates should Contoso use for EFS and digital signing?
- What kind of certificates should Contoso use for a website?
- How will Contoso ensure that EFS-encrypted data is not lost if a user loses a certificate?

Tools

- The **Certification Authority** console
- The **Certificate Templates** console
- The **Certificates** console
- **Certutil.exe**

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
The certificate template is not visible during enrollment.	Make sure that you configured the Read and Enroll permissions on the template correctly.
Autoenrollment does not work.	Ensure that you configured the autoenrollment options in Group Policy and that you assigned the Read, Enroll, and Autoenroll permissions to the appropriate group of users or computers.

Common Issue	Troubleshooting Tip
The user who encrypted a file cannot decrypt it.	Ensure that the user possesses the private key from the key pair. Also, ensure that the certificate has not expired. If a private key is lost or a certificate has expired, use KRA or DRA.

Lab Review Questions and Answers

Lab: Deploying and using certificates

Question and Answers

Question: What must you do to recover private keys?

Answer: To recover private keys, you must configure a CA to archive private keys for specific templates, and you must issue a KRA certificate.

Question: What is the benefit of using a restricted Enrollment Agent?

Answer: Enrollment Agent allows you to limit the permissions for users who are designated as Enrollment Agents to enroll for smart card certificates on behalf of other users.

Module 10

Implementing and administering AD FS

Contents:

Lesson 1

Overview of AD FS

Contents:

Question and Answers

Question: A federated trust is the same as a forest trust that organizations can configure between AD DS forests.

( ) True

( ) False

Answer:

( ) True

(√) False

Feedback:

A federated trust is not the same as a forest trust that organizations can configure between AD DS forests. In a federated trust, the AD FS servers in two organizations never have to communicate directly with each other. In addition, all communication in a federation deployment occurs over HTTPS, so you do not need to open multiple ports on any firewalls to allow federation.

Lesson 2

AD FS requirements and planning

Contents:

Question and Answers

Question: In Windows Server 2016, the federation server proxy functionality is part of the Web Application Proxy role.

( ) True

( ) False

Answer:

(√) True

( ) False

Feedback:

The federation server proxy is an optional component that you usually deploy in a perimeter network. It does not add any functionality to the AD FS deployment, but it provides a layer of security enhancement for connections from the Internet to the federation server. In Windows Server 2016, the federation server proxy functionality is part of Web Application Proxy.

Demonstration: Installing the AD FS server role

Demonstration Steps

Install AD FS

1. On **LON-DC1**, click Start, right-click **Windows PowerShell**, and then click **Run as Administrator**.
2. At the command prompt, type the following command, and then press Enter.

```
Add-KdsRootKey –EffectiveTime ((get-date).addhours(-10))
```

   This command creates the Microsoft Group Key Distribution Service root key to generate group Managed Service Account (gMSA) passwords for the account that will be used later in this lab. You should receive a globally unique identifier (GUID) as a response to this command.

3. On **LON-DC1**, in Server Manager, click **Manage**, and then click **Add Roles and Features**.
4. In the **Add Roles and Features Wizard**, on the **Before you begin** page, click **Next**.
5. On the **Select installation type** page, click **Role-based or feature-based installation**, and then click **Next**.
6. On the **Select destination server** page, click **LON-DC1.Adatum.com**, and then click **Next**.
7. On the **Select server roles** page, select the **Active Directory Federation Services** check box, and then click **Next**.
8. On the **Select features** page, click **Next**.
9. On the **Active Directory Federation Services (AD FS)** page, click **Next**.
10. On the **Confirm installation selections** page, click **Install**.
11. Wait until installation is complete, and then click **Close**.

Add a DNS record for AD FS

1. On **LON-DC1**, in Server Manager, click **Tools**, and then click **DNS**.
2. In DNS Manager, expand **LON-DC1**, expand **Forward Lookup Zones**, and then click **Adatum.com**.
3. Right-click **Adatum.com**, and then click **New Host (A or AAAA)**.
4. In the **New Host** window, in the **Name** box, type **adfs**.

5. In the **IP address** box, type **172.16.0.10**, and then click **Add Host**.
6. In the **DNS** window, click **OK**, and then click **Done**.
7. Close DNS Manager.

Configure AD FS

1. On **LON-DC1**, in Server Manager, click the **Notifications** icon, and then click **Configure the federation service on this server**.
2. In the **Active Directory Federation Services Configuration Wizard**, on the **Welcome** page, click **Create the first federation server in a federation server farm**, and then click **Next**.
3. On the **Connect to Active Directory Domain Services** page, click **Next** to use **Adatum\Administrator** to perform the configuration.
4. On the **Specify Service Properties** page, in the **SSL Certificate** dialog box, select **adfs.adatum.com**.
5. In the **Federation Service Display Name** box, type **A. Datum Corporation**, and then click **Next**.
6. On the **Specify Service Account** page, click **Create a Group Managed Service Account**.
7. In the **Account Name** box, type **ADFSService**, and then click **Next**.
8. On the **Specify Configuration Database** page, click **Create a database on this server using Windows Internal Database**, and then click **Next**.
9. On the **Review Options** page, click **Next**.
10. On the **Pre-requisite Checks** page, click **Configure**.
11. On the **Results** page, click **Close**.

Lesson 3

Deploying and configuring AD FS

Contents:

Question and Answers

Question: What are claim rules? What can you use claim rules for?

Answer: Claim rules define how AD FS servers send and consume claims. Claim rules define the business logic that is applied to claims that the claims providers provide and that the relying parties accept. You can use claim rules to:

- Define which incoming claims are accepted from one or more claims providers.
- Define which outbound claims are provided to one or more relying parties.
- Apply authorization rules to enable access to a specific relying party for one or more users or groups of users.

Resources

How home realm discovery works

 Additional Reading: For more on *RelayState*, refer to "Supporting Identity Provider Initiated RelayState" at: http://aka.ms/Df8hqs

Demonstration: Configuring claims provider and relying party trusts

Demonstration Steps

Configure a claims provider trust

1. On LON-DC1, in Server Manager, click Tools, and then click AD FS Management.
2. In the AD FS Management console, click Claims Provider Trusts.
3. Right-click Active Directory, and then click Edit Claim Rules.
4. In the Edit Claim Rules for Active Directory window, on the Acceptance Transform Rules tab, click Add Rule.
5. In the Add Transform Claim Rule Wizard, on the Select Rule Template page, in the Claim rule template list, click Send LDAP Attributes as Claims, and then click Next.
6. On the Configure Rule page, in the Claim rule name box, type Outbound LDAP Attributes Rule.
7. In the Attribute store list, click Active Directory.
8. In the Mapping of LDAP attributes to outgoing claim types section, select the following values for the LDAP Attribute and the Outgoing Claim Type:
   - E-Mail-Addresses: E-Mail Address
   - User-Principal-Name: UPN
9. Click Finish, and then click OK.

Configure a Windows Identity Foundation (WIF) application for AD FS

1. On LON-SVR1, open Server Manager, click Tools, and then click Windows Identity Foundation Federation Utility.
2. On the Welcome to the Federation Utility Wizard page, in the Application configuration location box, type C:\inetpub\wwwroot\AdatumTestApp\web.config for the location of the sample Web.config file.
3. In the Application URI box, type https://lon-svr1.adatum.com/AdatumTestApp/ to indicate the path to the sample application that will trust the incoming claims from the federation server, and then click Next.

4. On the **Security Token Service** page, click **Use an existing STS**, and then in the **STS WS-Federation metadata document location** box, type **https://adfs.adatum.com/federationmetadata/2007-06/federationmetadata.xml**. Click **Next**.
5. On the **STS signing certificate chain validation error** page, click **Disable certificate chain validation**, and then click **Next**.
6. On the **Security token encryption** page, click **No encryption**, and then click **Next**.
7. On the **Offered claims** page, review the claims that will be offered by the federation server, and then click **Next**.
8. On the **Summary** page, review the changes that will be made to the sample application by the **Federation Utility Wizard**, scroll through the items to understand what each item is doing, and then click **Finish**.
9. In the **Success** window, click **OK**.

Configure a relying party trust

1. On **LON-DC1**, in the **AD FS** console, click **Relying Party Trusts**.
2. In the **Actions** pane, click **Add Relying Party Trust**.
3. In the **Add Relying Party Trust Wizard**, on the **Welcome** page, click **Start**.
4. On the **Select Data Source** page, click **Import data about the relying party published online or on a local network**.
5. In the **Federation Metadata address (host name or URL)** box, type **https://lon-svr1.adatum.com/adatumtestapp/**, and then click **Next**. This downloads the metadata configured in the previous task.
6. On the **Specify Display Name** page, in the **Display name** box, type **A. Datum Corporation Test App**, and then click **Next**.
7. On the **Choose Access Control Policy** page, click **Permit everyone**, and then click **Next**.
8. On the **Ready to Add Trust** page, review the relying party trust settings, and then click **Next**.
9. On the **Finish** page, click **Close**.
10. In the list of Relying Party Trusts, click **A. Datum Corporation Test App**, and then select **Edit Claim Issuance policy**.
11. In the **Edit Claim Issuance Policy for A. Datum Corporation Test App** window, on the **Issuance Transform Rules** tab, click **Add Rule**.
12. In the **Claim rule template** dialog box, select **Pass Through or Filter an Incoming Claim**, and then click **Next**.
13. In the **Claim rule name** box, type **Pass through Windows account name**.
14. In the **Incoming claim type** list, click **Windows account name**, and then click **Finish**.
15. On the **Issuance Transform Rules** tab, click **Add Rule**.
16. In the **Claim rule template** dialog box, select **Pass Through or Filter an Incoming Claim**, and then click **Next**.
17. In the **Claim rule name** box, type **Pass through E-Mail Address**.
18. In the **Incoming claim type** list, click **E-Mail Address**, and then click **Finish**.
19. On the **Issuance Transform Rules** tab, click **Add Rule**.
20. In the **Claim rule template** dialog box, select **Pass Through or Filter an Incoming Claim**, and then click **Next**.
21. In the **Claim rule name** box, type **Pass through UPN**.

22. In the **Incoming claim type** list, click **UPN**, and then click **Finish**.
23. On the **Issuance Transform Rules** tab, click **Add Rule**.
24. In the **Claim rule template** dialog box, select **Pass Through or Filter an Incoming Claim**, and then click **Next**.
25. In the **Claim rule name** box, type **Pass through Name**.
26. In the **Incoming claim type** list, click **Name**, and then click **Finish**.
27. On the **Issuance Transform Rules** tab, click **OK**.

Demonstration: Configuring claims rules

Demonstration Steps

1. On **LON-DC1**, in the AD FS Manager, select **Relying Party Trusts**, right-click **A. Datum Corporation Test App**, and then click **Edit Claim Issuance Policy**.
2. In the **Edit Claim Issuance Policy for A. Datum Corporation Test App** window, on the **Issuance Transform Rules** tab, click **Add Rule**.
3. In the **Claim Rule Template** dialog box, select **Pass Through or Filter an Incoming Claim**, and then click **Next**.
4. In the **Claim rule name** box, type **Send Group Name Rule**.
5. In the **Incoming claim type** list, click **Group**, and then click **Finish**.
6. Click **OK**.
7. Right-click **A. Datum Corporation Test App**, and then click **Edit Access Control Policy**
8. In the **Edit Access Control Policy for A. Datum Corporation Test App** window, on the **Access control policy** tab, click the **Permit specific group** rule.
9. Under **Policy** click the **<parameter>** link.
10. Click **Add** and then in the **Select Groups** box, type **Research** and then click **OK**. Click **OK** again to close the **Select Groups** box.
11. Click **OK** to close the Access Control Policy dialog box.
12. Right-click **A. Datum Corporation Test App**, and then click **Edit Claim Issuance Policy**
13. On the **Issuance Transform Rules** tab, click **Pass through UPN** and then click **Edit Rule**.
14. In the **Incoming claim type** list, verify that **UPN** is selected.
15. Select **Pass through only a specific claim value**.
16. In the **Incoming claim value** box, type **@adatum.com**.
17. Click **View Rule Language**.
18. Click **OK**, and then click **OK** again.
19. In the **Edit Claim Issuance Policy for A. Datum Corporation Test App** window, click **OK**.

Lesson 4
Web Application Proxy overview

Contents:

Question and Answers

Question: Which of the following statements about configuring the Web Application Proxy is true? (Choose all that apply.)

( ) To install the Web Application Proxy, you must have implemented AD FS in your organization.

( ) To install the Web Application Proxy, you need not have implemented AD FS in your organization.

( ) For each application that you publish, you must configure an external URL and an internal server URL.

( ) When you define the external URL, you must also select a certificate that contains the host name in the internal URL.

( ) When you define the external URL, you must also select a certificate that contains the host name in the external URL.

Answer:

(√) To install the Web Application Proxy, you must have implemented AD FS in your organization.

( ) To install the Web Application Proxy, you need not have implemented AD FS in your organization.

(√) For each application that you publish, you must configure an external URL and an internal server URL.

( ) When you define the external URL, you must also select a certificate that contains the host name in the internal URL.

(√) When you define the external URL, you must also select a certificate that contains the host name in the external URL.

Feedback:

Option 4 is incorrect. The certificate must contain the host name of the external URL.

Option 2 is incorrect. To install the Web Application Proxy, AD FS must already be implemented in your organization.

Resources

Scenarios for using the Web Application Proxy

 Additional Reading: For more information on configuring a website to use IWA and Kerberos constrained delegation, refer to "Configure a site to use Integrated Windows authentication" at: http://aka.ms/Nbsbll

 Additional Reading: For more information on configuring Kerberos authentication for load-balanced Exchange servers, refer to "Configuring Kerberos authentication for load-balanced Client Access servers" at: http://aka.ms/Nd2avi

 Additional Reading: For more information on publishing RD Gateway through the Web Application Proxy, refer to Publishing Applications with SharePoint, Exchange and RDG: http://aka.ms/C7f0wn

Demonstration: Installing and configuring the Web Application Proxy

Demonstration Steps

Install the Web Application Proxy

1. On **LON-SVR2**, open Server Manager, click **Manage**, and then click **Add Roles and Features**.
2. In the **Add Roles and Features Wizard**, on the **Before you begin** page, click **Next**.
3. On the **Select installation type** page, click **Role-based or feature-based installation**, and then click **Next**.
4. On the **Select destination server** page, click **LON-SVR2.Adatum.com**, and then click **Next**.
5. On the **Select server roles** page, select the **Remote Access** check box, and then click **Next**.
6. On the **Select features** page, click **Next**.
7. On the **Remote Access** page, click **Next**.
8. On the **Select role services** page, select **Web Application Proxy**.
9. In the **Add Roles and Features Wizard**, click **Add Features**.
10. On the **Select role services** page, click **Next**.
11. On the **Confirm installation selections** page, click **Install**.
12. On the **Installation progress** page, click **Close**.

Export the adfs.adatum.com certificate from LON-DC1

1. On **LON-DC1**, on the Start screen, type **mmc**, and then press Enter.
2. In Microsoft Management Console, click **File**, and then click **Add/Remove Snap-in**.
3. In the **Add or Remove Snap-ins** window, in the **Available snap-ins** column, double-click **Certificates**.
4. In the **Certificates snap-in** window, click **Computer account**, and then click **Next**.
5. In the **Select Computer** window, click **Local Computer (the computer this console is running on)**, and then click **Finish**.
6. In the **Add or Remove Snap-ins** window, click **OK**.
7. In Microsoft Management Console, expand **Certificates (Local Computer)**, expand **Personal**, and then click **Certificates**.
8. Right-click **adfs.adatum.com**, point to **All Tasks**, and then click **Export**.
9. In the **Certificate Export Wizard**, click **Next**.
10. On the **Export Private Key** page, click **Yes, export the private key**, and then click **Next**.
11. On the **Export File Format** page, click **Next**.
12. On the **Security** page, select the **Password** check box.
13. In the **Password** and **Confirm password** boxes, type **Pa$$w0rd**, and then click **Next**.
14. On the **File to Export** page, in the **File name** box, type **C:\adfs.pfx**, and then click **Next**.
15. On the **Completing the Certificate Export Wizard** page, click **Finish**, and then click **OK** to close the success message.
16. Close Microsoft Management Console, and do not save the changes.

Import the adfs.adatum.com certificate onto LON-SVR2

1. On **LON-SVR2**, on the Start screen, type **mmc**, and then press Enter.

2. In Microsoft Management Console, click **File**, and then click **Add/Remove Snap-in**.
3. In the **Add or Remove Snap-ins** window, in the **Available snap-ins** column, double-click **Certificates**.
4. In the **Certificates snap-in** window, click **Computer account**, and then click **Next**.
5. In the **Select Computer** window, click **Local Computer (the computer this console is running on)**, and then click **Finish**.
6. In the **Add or remove Snap-ins** window, click **OK**.
7. In Microsoft Management Console, expand **Certificates (Local Computer)**, and then click **Personal**.
8. Right-click **Personal**, point to **All Tasks**, and then click **Import**.
9. In the **Certificate Import Wizard**, click **Next**.
10. On the **File to Import** page, in the **File name** box, type **\\LON-DC1\c$\adfs.pfx**, and then click **Next**.
11. On the **Private key protection** page, in the **Password** box, type **Pa$$w0rd**.
12. Select the **Mark this key as exportable. This will allow you to back up or transport your keys at a later time** check box, and then click **Next**.
13. On the **Certificate Store** page, click **Place all certificates in the following store**.
14. In the **Certificate store** box, select **Personal**, and then click **Next**.
15. On the **Completing the Certificate Import Wizard** page, click **Finish**.
16. Click **OK** to clear the success message.
17. Close Microsoft Management Console, and do not save the changes.

Configure the Web Application Proxy

1. On **LON-SVR2**, in Server Manager, click the **Notifications** icon, and then click **Open the Web Application Proxy Wizard**.
2. In the **Web Application Proxy Configuration Wizard**, on the **Welcome** page, click **Next**.
3. On the **Federation Server** page, type the following information, and then click **Next**:
   - Federation service name: **adfs.adatum.com**
   - User name: **Adatum\Administrator**
   - Password: **Pa$$w0rd**
4. On the **AD FS Proxy Certificate** page, in the **Select a certificate to be used by the AD FS proxy** dialog box, select **adfs.adatum.com**, and then click **Next**.
5. On the **Confirmation** page, click **Configure**.
6. On the **Results** page, click **Close**.

Module Review and Takeaways

Best Practice

In earlier versions of AD FS, it was common to use the Security Configuration Wizard (SCW) to apply AD FS–specific security best practices to federation servers and federation server proxy computers. In Windows Server 2016, SCW was removed because features are security enhanced by default. Consequently, if you need to control specific security settings, you can use either Group Policy or Microsoft Security Compliance Manager (see http://aka.ms/Ncq8jm).

Review Questions

Question: Your organization is planning to implement AD FS. In the short term, only internal clients will use AD FS to access internal applications. However, you must later provide access to web-based applications that are security enhanced by AD FS to users at home. How many certificates should you obtain from a third-party CA?

> Answer: You require only one certificate from a third-party CA, because the only AD FS certificate that needs to be trusted is the service communication certificate. You can leave the token signing and token decrypting certificates as self-signed.

Question: Your organization has successfully implemented a single AD FS server and a single Web Application Proxy. Initially, AD FS was used for only a single application, but now it is used for several business-critical applications. AD FS must be configured to be highly available.

During the installation of AD FS, you chose to use WID. Can you use this database in a highly available configuration?

> Answer: Yes, you can use Windows Internal Database (WID) to support up to five AD FS servers. The first AD FS server is the primary server, where all the configuration changes take place. Changes in the primary server are replicated to the other AD FS servers.

Lab Review Questions and Answers

Lab: Implementing AD FS

Question and Answers

Question: Why is it important to configure adfs.adatum.com to use as a host name for the AD FS service?

Answer: If you use the host name of an existing server for the AD FS server, you will not be able to add additional servers to your server farm. All the servers in the server farm must share the same host name when providing AD FS services. AD FS proxy servers also use the host name for AD FS.

Question: How can you test whether AD FS is functioning properly?

Answer: If you can successfully access **https://hostname/federationmetadata/2007-06/federationmetadata.xml** on the AD FS server, it means that AD FS is functioning properly.

Module 11

Implementing and administering AD RMS

Contents:

Lesson 1

Overview of AD RMS

Contents:

Question and Answers

Question: When does a user receives a RAC?

Answer: A RAC is issued the first time a user attempts to access AD RMS–protected content or to perform an AD RMS task, such as creating a protected document.

Question: Azure RMS is deployed locally on a server.

( ) True

( ) False

Answer:

( ) True

(√) False

Feedback:

Azure RMS is a cloud-based service, and you do not have to deploy it locally.

Resources

What is Azure RMS?

 Reference Links: To download the free RMS sharing application from Microsoft go to: http://aka.ms/v1s1xd

Comparing AD RMS, Azure RMS, and Azure RMS for Office 365

 Additional Reading: For more information, refer to Comparing Azure Rights Management and AD RMS: http://aka.ms/sndlw0

Lesson 2

Deploying and managing an AD RMS infrastructure

Contents:

Question and Answers

Question: To implement an AD RMS cluster, which components are necessary?

( ) Office

( ) A service account

( ) A database

( ) AD FS

( ) A Secure Sockets Layer (SSL) certificate

Answer:

( ) Office

(√) A service account

(√) A database

( ) AD FS

( ) A Secure Sockets Layer (SSL) certificate

Feedback:

You need to have service account created to implement AD RMS, and you need to have a database available, as either a WID or a SQL Server database.

Question: When you decide to remove your AD RMS cluster from AD DS, what should you do first?

Answer: Prior to removing an AD RMS server, you should decommission that server.

Resources

Monitoring AD RMS

Additional Reading: For more information, refer to Monitoring Scenarios: http://aka.ms/Pyumg7

Demonstration: Installing the first server of an AD RMS cluster

Demonstration Steps

Configure a service account

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **Active Directory Administrative Center**.
2. Select and then right-click **Adatum (local)**, click **New**, and then click **Organizational Unit**.
3. In the **Create Organizational Unit** dialog box, in the **Name** box, type **Service Accounts**, click **OK**, right-click the **Service Accounts** organizational unit (OU), point to **New**, and then click **User**.
4. In the **Create User** dialog box, provide the following details, and then click **OK**:
   - First name: **ADRMSSVC**
   - User UPN logon: **ADRMSSVC**
   - **User SamAccountName Logon**: **Adatum\ADRMSSVC**
   - Password: **Pa$$w0rd**
   - Confirm Password: **Pa$$w0rd**

- Password never expires: **Enabled** (you should click on **Other password options** to be able to select this)
- User cannot change password: **Enabled**

Prepare the Domain Name System (DNS)

1. In **Server Manager**, click **Tools**, and then click **DNS**.
2. In the **DNS Manager** console, expand **LON-DC1**, and then expand **Forward Lookup Zones**.
3. Select and then right-click **Adatum.com**, and then click **New Host (A or AAAA)**.
4. In the **New Host** dialog box, type the following information, and then click **Add Host**:
   - Name: **adrms**
   - IP address: **172.16.0.21**

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

5. Close the **DNS Manager** console.

Install the AD RMS role

1. Sign in to **LON-SVR1** as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. Click Start and then click **Server Manager**.
3. In **Server Manager**, click **Manage**, and then click **Add Roles and Features**.
4. In the **Add Roles and Features Wizard**, click **Next** three times.
5. On the **Server Roles** page, click **Active Directory Rights Management Services**.
6. In the **Add Roles and Features Wizard** dialog box, click **Add Features**, click **Next** six times, click **Install**, and then click **Close**.

Configure AD RMS

1. On **LON-SVR1**, in **Server Manager**, click the **AD RMS** node.
2. Next to **Configuration required for Active Directory Rights Management Services at LON-SVR1**, click **More**.
3. On the **All Servers Task Details and Notifications** page, click **Perform additional configuration**.
4. On the **AD RMS** page, in the **AD RMS Configuration: LON-SVR1.adatum.com** dialog box, click **Next**.
5. On the **AD RMS Cluster** page, click **Create a new AD RMS root cluster**, and then click **Next**.
6. On the **Configuration Database** page, click **Use Windows Internal Database on this server**, and then click **Next**.
7. On the **Service Account** page, click **Specify**.
8. In the **Windows Security** dialog box, type the following details, click **OK**, and then click **Next**:
   - User name: **ADRMSSVC**
   - Password: **Pa$$w0rd**

   Note: If you get an error when you try to use the ADRMSSVC service account, force replication between **LON-DC1** and **LON-DC2**, and then try the step again.

9. On the **Cryptographic Mode** page, click **Cryptographic Mode 2**, and then click **Next**.
10. On the **Cluster Key Storage** page, click **Use AD RMS centrally managed key storage**, and then click **Next**.

11. On the **Cluster Key Password** page, type **Pa$$w0rd** twice, and then click **Next**.
12. On the **Cluster Web Site** page, verify that **Default Web Site** is selected, and then click **Next**.
13. On the **Cluster Address** page, provide the following information, and then click **Next**:
    - Connection Type: **Use an unencrypted connection (http://)**
    - Fully-Qualified Domain Name: **adrms.adatum.com**
    - Port: **80**
14. On the **Licensor Certificate** page, type **AdatumADRMS**, and then click **Next**.
15. On the **SCP Registration** page, click **Register the SCP now**, and then click **Next**.
16. On the **Confirmation** page, click **Install**, and then after the installation is complete, click **Close**.
17. On the Start menu, click **Administrator**, and then click **Sign Out**.

Note: You must sign out before you can manage AD RMS.

Lesson 3

Configuring AD RMS content protection

Contents:

Question and Answers

Question: What kinds of permissions does a Super Users group have?

> Answer: Super Users group members are granted full owner rights in all use licenses that are issued by the AD RMS cluster on which the Super Users group is configured.

Resources

What are exclusion policies?

 Additional Reading: For more information, refer to Enabling Exclusion Policies: http://aka.ms/Lnwbcr

Demonstration: Creating a rights policy template

Demonstration Steps

1. On LON-SVR1, open Server Manager, click Tools, and then click Active Directory Rights Management Services.
2. In the AD RMS console, click the LON-SVR1\Rights Policy Templates node.
3. In the Actions pane, click Create Distributed Rights Policy Template.
4. In the Create Distributed Rights Policy Template wizard, on the Add Template Identification Information page, click Add.
5. On the Add New Template Identification Information page, provide the following information, click Add, and then click Next:
   - Language: English (United States)
   - Name: ReadOnly
   - Description: Read-only access. No copy or print.
6. On the Add User Rights page, click Add.
7. On the Add User or Group page, type executives@adatum.com, and then click OK.
8. When executives@adatum.com is selected, under Rights, click View. Verify that Grant owner (author) full control right with no expiration is selected, and then click Next.
9. On the Specify Expiration Policy page, choose the following settings, and then click Next:
   - Content Expiration: Expires after the following duration (days): 7
   - Use license expiration: Expires after the following duration (days): 7
10. On the Specify Extended Policy page, click Require a new use license every time content is consumed (disable client-side caching), click Next, and then click Finish.

Demonstration: Creating an exclusion policy for an app

Demonstration Steps

1. On LON-SVR1, in the AD RMS console, click the Exclusion Policies node, and then click Manage application exclusion list.
2. In the Actions pane, click Enable Application Exclusion.
3. In the Actions pane, click Exclude Application.

4. In the **Exclude Application** dialog box, type the following information, and then click **Finish**:
   - Application File name: **Powerpnt.exe**
   - Minimum version: **14.0.0.0**
   - Maximum version: **16.0.0.0**

Module Review and Takeaways

Best Practices

- Prior to deploying AD RMS, you must analyze your organization's business requirements and create the necessary templates. You should meet with the users to inform them of AD RMS functionality and to ask for feedback on the types of templates that they want to have available.
- Strictly control the membership of the Super Users group. Users in this group have complete access to all AD RMS–protected content.

Review Questions

Question: What are the benefits of having an SSL certificate installed on the AD RMS server when you perform an AD RMS configuration?

Answer: You can protect the connection between clients and the AD RMS server with SSL.

Question: You need to provide access to AD RMS–protected content for five users who are unaffiliated contractors and who are not members of your organization. Which method should you use to provide this access?

Answer: Use a Microsoft account to provide RACs to the unaffiliated contractors.

Question: You want to block users from protecting PowerPoint content by using AD RMS templates. What steps should you take to accomplish this goal?

Answer: You should configure Application Exclusion for PowerPoint.

Lab Review Questions and Answers

Lab: Implementing an AD RMS infrastructure

Question and Answers

Question: What steps can you take to help ensure that you can use IRM services with the AD RMS role?

Answer: You need to configure a server certificate for the AD RMS server prior to deploying AD RMS.

Module 12

Implementing AD DS synchronization with Microsoft Azure AD

Contents:

Lesson 1

Planning and preparing for directory synchronization

Contents:

Question and Answers

Question: When you implement directory synchronization, user accounts and groups move from your local AD DS to Azure AD.

( ) True

( ) False

Answer:

( ) True

(√) False

Feedback:

Directory synchronization does not move objects. It copies objects from the local AD DS with a subset of their attributes, and it creates new objects in Azure AD.

Resources

Planning directory synchronization

 **Additional Reading:** For more information, refer to the Azure Hybrid Identity Design Considerations Guide: http://aka.ms/ibuqek

Prerequisites and preparation for directory synchronization

 **Additional Reading:** For more information, refer to You receive a "This company has exceeded the number of objects that can be synchronized" error in a directory synchronization report: http://aka.ms/r4x1q4

Lesson 2

Implementing directory synchronization by using Azure AD Connect

Contents:

Question and Answers

Question: When you implement synchronization between AD DS and Azure AD, where do you master AD DS objects?

> **Answer:** If you have deployed Azure AD Connect for Active Directory synchronization, you are mastering objects from within your on-premises AD DS by using tools such as Active Directory Users and Computers or Windows PowerShell—the source of authority is the on-premises AD DS.

Resources

Azure AD Connect customized synchronization

Additional Reading: For more information, refer to "Configuring Alternate Login ID" at: http://aka.ms/nqh5gc

Azure AD Connect monitoring features

Additional Reading: For more information, refer to Monitor your on-premises identity infrastructure and synchronization services in the cloud: http://aka.ms/dqaaps

Demonstration: Installing and configuring Azure AD Connect

Demonstration Steps

1. On LON-SVR1, sign in as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. Open Internet Explorer, and then browse to **http://www.microsoft.com/en-us/download/details.aspx?id=47594**.
3. On the **Microsoft Azure Active Directory Connect** page, click **Download**.
4. Click **Run**. Wait for a few minutes, so that the download can finish.

   Note: If you experience any problems with starting the download, add the https://download.microsoft.com website to your trusted sites.

5. In Microsoft Azure Active Directory Connect Wizard, on the **Welcome to Azure AD Connect** page, select the **I agree to the license terms and privacy notice** check box, and then click **Continue**.
6. On the **Express Settings** page, click **Customize**.
7. On the **Install required components** page, review the available options, but do not make any changes, and then click **Install**.
8. On the **User sign-in** page, select **Password Synchronization**, and then click **Next**.
9. On the **Connect to Azure AD** page, in the **USERNAME** and **PASSWORD** text boxes, type **SYNC@yourdomain.onmicrosoft.com** for the account user name, type the password **Pa$$w0rd**, and then click **Next**. It might take a couple of minutes for the connection to establish.
10. On the **Connect your directories** page, in the **USERNAME** text box, type ***Adatum*\administrator**, and then in the **PASSWORD** text box, type **Pa$$w0rd**. Click **Add Directory**, and then click **Next**.

11. On the **Azure AD sign-in configuration** page, select the check box next to **Continue without any verified domains** and then click **Next**.
12. On the **Domain and OU filtering** page, click **Next**.
13. On the **Uniquely identifying your users** page, review and explain the available options, but do not make any changes.
14. Click **Next**.
15. On the **Filter users and devices** page, click **Synchronize selected**. In the **GROUP** text box, type **Research**, and then click **Resolve**. Ensure that a green check mark appears after you click **Resolve**.
16. Click **Next**.
17. On the **Optional features** page, select **Password writeback**, explain the other options to students, and then click **Next**.
18. On the **Ready to Configure** page, click **Install**, and then when the installation completes, click **Exit**.
19. The synchronization of objects from your local AD DS and Azure AD should begin. Wait for approximately 5 minutes for this process to complete.
20. Open Internet Explorer on your host computer, and then open the Azure classic portal by browsing to **https://manage.windowsazure.com**.
21. Sign in to Azure by using the Microsoft account associated with your trial subscription. When the Azure classic portal opens, click the **Adatum** directory.
22. On the **adatum** page, click the **USERS** tab.

 **Note:** Do you see the user accounts from your local AD DS? You should be able to see Research users from your local adatum.com domain.

23. Minimize Internet Explorer on your host machine.
24. On the **LON-SVR1** computer, click the **Start** button, and then type **Synchronization**.
25. In the search pane, click **Synchronization Service**.
26. In the **Synchronization Service Manager on LON-SVR1** window, click the **Operations** tab.
27. Ensure that you see the **Export**, **Delta Synchronization**, and **Delta Import** tasks. Ensure that all tasks have the current time and date in the **Start Time** and **End Time** columns. Also, ensure that latest tasks have **success** listed in the **Status** column.
28. Close Synchronization Service Manager.

Lesson 3

Managing identities with directory synchronization

Contents:

Question and Answers

Question: If you want to have SSO for both cloud-based and on-premises services, what do you need to deploy? Choose all that apply.

( ) Azure AD Connect Health

( ) AD FS

( ) Azure AD Connect

( ) Office 365

( ) Azure AD

Answer:

( ) Azure AD Connect Health

(√) AD FS

(√) Azure AD Connect

( ) Office 365

( ) Azure AD

Question: If you implement AD FS and federation between locally deployed AD DS and Azure AD, then you do not need to use Azure AD Connect.

( ) True

( ) False

Answer:

( ) True

(√) False

Feedback:

The on-premises AD DS performs authentication and then passes that information to Azure AD. The password for Azure AD is not used. However, the accounts in both directory services must match. Therefore, it is required that you use both Azure AD Connect and AD FS.

Resources

Modifying directory synchronization

Additional Reading: For more information, refer to "Azure AD Connect sync: Configure Filtering" at: http://aka.ms/au8smo

Monitoring directory synchronization

Additional Reading: For more information, refer to "Azure Active Directory cmdlets" at: http://aka.ms/pfsm1x

Troubleshooting directory synchronization

Additional Reading: For more information, refer to “Integrating your on-premises identities with Azure Active Directory” at: http://aka.ms/cdm2kk

Additional Reading: For more ore information, refer to “How to troubleshoot Azure Active Directory Sync tool installation and Configuration Wizard errors” at: http://aka.ms/bz5cjw

Module Review and Takeaways

Best Practices

- For simple environments, use the Azure AD Connect express settings.
- Enable users to use the self-service password reset functionality with at least two authentication methods.
- Consider using writeback functionalities.
- Implement Azure AD Connect Health if you have an Azure AD Premium subscription.

Real-world Issues and Scenarios

Because directory synchronization is the link between your on-premises AD DS objects and the services in Azure AD, be careful when making changes to Azure AD Connect or Synchronization Service Manager after production deployment. For example, a minor mistake in filtering could accidentally delete all user mailboxes in Office 365.

In some environments, for example, in a test environment, you might test all changes on a separate directory synchronization server that is connected to a separate Azure AD tenant (trial). In addition, you should manually initiate run profiles for each management agent in Synchronization Service Manager and observe the pending actions before exporting to Azure AD. In some cases, it might be a good idea to create a new run profile for exporting to Azure AD that includes a maximum limit on the number of allowed deletions.

Review Question(s)

Question: What feature do you need to configure so that objects synchronize from Azure AD to your on-premises AD DS?

> **Answer:** You need to deploy writeback functionalities. Currently, you can use password writeback, groups writeback, and devices writeback.

Tools

The following table lists the tools that this module references:

Tool	Use for	Where to find it
Azure AD Connect	Establishing synchronization between AD DS and Azure AD	Microsoft Download Center
Azure AD Connect Health	Monitoring AD DS to Azure AD synchronization health	The Azure classic portal
The Azure classic portal	Azure AD management	http://aka.ms/n2l3cb

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Directory synchronization filtering is no longer working.	It is important to be on the latest version of the directory synchronization tool. However, when upgrading to a new version of the tool, all existing filters and other management agent customizations will not automatically import into the new installation. If you are upgrading to a newer version of directory synchronization, you

Common Issue	Troubleshooting Tip
	must always manually reapply filtering configurations after you upgrade but before you run the first synchronization cycle.
After installing Azure AD Connect, you might receive a prompt with the following error message when you open Synchronization Service Manager: **Unable to connect to the Synchronization Service**.	Add the appropriate Azure AD Connect domain user account to the ADSyncAdmins group, sign out, and then sign in again. The domain user account that you use to sign in during installation of Azure AD Connect is automatically added to the group, but you will still need to sign out and then sign in again before you can successfully open Synchronization Service Manager.

Lab Review Questions and Answers

Lab: Configuring directory synchronization

Question and Answers

Question: What do you need to do before you begin configuring Azure AD Connect?

Answer: You must create a synchronization account in Azure AD, and then add your domain to the Azure AD tenant.

Question: Which cmdlet should you use to change the synchronization schedule for Azure AD Connect?

Answer: You should use the **Set-ADSyncScheduler** cmdlet on the computer on which you install Azure AD Connect.

Module 13

Monitoring, managing, and recovering AD DS

Contents:

Lesson 1

Monitoring AD DS

Contents:

Resources

Overview of monitoring tools

Additional Reading: For more information, refer to "Using PowerShell To Gather Performance Data," at: http://aka.ms/F8mxnr

Demonstration: Monitoring AD DS

Demonstration Steps

Configure Performance Monitor to monitor AD DS

1. Switch to **LON-DC1**.
2. In Server Manager, click **Tools**, and then click **Performance Monitor**.
3. Under the Monitoring Tools node, click Performance Monitor.
4. Click the **Add** button—the green **Plus Sign** (**+**) on the toolbar—to add objects and counters.
5. In the **Add Counters** dialog box, in the **Available Counters** list, expand the **Directory Services** object.
6. Click the **DRA Inbound Bytes Total/sec** counter, and then click **Add**.
7. Repeat the previous step (step 6) to add the following counters:
   - **DirectoryServices\DRA Outbound Bytes Total/sec**
   - **DirectoryServices\DS Threads In Use**
   - **DirectoryServices\DS Directory Reads/sec**
   - **DirectoryServices\DS Directory Writes/sec**
   - **DirectoryServices\DS Directory Searches/sec**
   - **NTDS\DRA Inbound Objects/sec**
   - **NTDS\DRA Pending Replication Synchronizations**
   - **Security System-Wide Statistics\NTLM Authentications**
   - **Security System-Wide Statistics\Kerberos Authentications**
8. Click **OK**, and then wait for a few moments.
9. In the counter list below the graph, select **DS Directory Searches/sec**.
10. On the toolbar, click **Highlight**. The selected counter is highlighted, making it easier to see that counter's performance.
11. On the toolbar, click **Highlight** to turn off the highlight.

Create a data collector set

1. In the console tree, expand **Performance**, expand **Monitoring Tools**, and then click **Performance Monitor**. Right-click **Performance Monitor**, point to **New**, and then click **Data Collector Set**.
2. In the **Create new Data Collector Set** dialog box, in the **Name** text box, 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, click **Next**, and then click **Finish.**

Start the data collector set

1. In the console tree, expand **Data Collector Sets**, expand **User Defined**, and then click **User Defined**.
2. Right-click **Custom ADDS Performance Counters**, and then click **Start**. Point out that the **Custom ADDS Performance Counters** node is selected automatically.

Note: You can identify the individual data collectors in the data collector set. In this case, only one data collector—the System Monitor Log performance counter—is contained in the data collector set. You also can 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**.

Analyze the resulting data in a report

1. In the console tree, expand **Reports**, expand **User Defined**, expand **Custom ADDS Performance Counters**, and then click **System Monitor Log.blg**.
2. Verify that the graph of the log's performance counters displays.

Lesson 2

Managing the Active Directory database

Contents:

Demonstration: Performing database management

Demonstration Steps

Stop AD DS

1. If necessary, on **LON-DC1**, on the taskbar, click the **Server Manager** icon.
2. In Server Manager, click **Tools**, and then click **Services**.
3. In the **Services** console, right-click **Active Directory Domain Services**, and then click **Stop**.
4. In the **Stop Other Services** dialog box, click **Yes**.

Perform an offline defragmentation of the Active Directory database

1. On **LON-DC1**, click Start and then click **Windows PowerShell**.
2. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
NtdsUtil.exe
```

3. At the **NtdsUtil.exe:** prompt, type the following command, and then press Enter:

```
activate instance NTDS
```

4. At the **NtdsUtil.exe:** prompt, type the following command, and then press Enter:

```
files
```

5. At the **file maintenance:** prompt, type the following command, and then press Enter:

```
compact to C:\
```

Check the integrity of the offline Active Directory database

1. At the **file maintenance:** prompt, type the following command, and then press Enter:

```
Integrity
```

2. At the **file maintenance:** prompt, type the following command, and then press Enter:

```
quit
```

3. At the **NtdsUtil.exe:** prompt, type the following command, and then press Enter:

```
Quit
```

4. Close the **Windows PowerShell** window.

Start AD DS

1. On the taskbar, click the **Server Manager** icon.
2. In Server Manager, click **Tools**, and then click **Services**.
3. In the **Services** console, right-click **Active Directory Domain Services**, and then click **Start**.
4. Confirm that the Status column for Active Directory Domain Services is listed as Running.

Lesson 3

Active Directory backup and recovery options for AD DS and other identity and access solutions

Contents:

Demonstration: Implementing the Active Directory Recycle Bin

Demonstration Steps

Enable the Active Directory Recycle Bin

1. On **LON-DC1**, in Server Manager, click **Tools**, and then click **Active Directory Sites and Services**.
2. Expand **Sites**, expand **Default-First-Site-Name**, expand **Servers**, expand **LON-DC1**, and then click **NTDS Settings**.
3. Right-click **<automatically generated>**, click **Replicate Now**, and then click **OK**.
4. Expand **LON-DC2**, and then click **NTDS Settings**.
5. Right-click **<automatically generated>**, click **Replicate Now**, and then click **OK**.
6. In Server Manager, click **Tools**, and then click **Active Directory Administrative Center**.
7. Click **Adatum (local)**.
8. In the tasks pane, click **Enable Recycle Bin**. In the warning message box, click **OK**, and then click **OK** again to the refresh Active Directory Administrative Center message.
9. Press the **F5** key to refresh Active Directory Administrative Center.

Create and then delete test accounts

1. In Active Directory Administrative Center, double-click the **Research** organizational unit (OU).
2. In the **Task** pane, click **New**, and then click **User**.
3. Under Account, type the following information, and then click **OK**:
   - Full name: **Test1**
   - User UPN logon: **Test1**
   - Password: **Pa$$w0rd**
   - Confirm password: **Pa$$w0rd**
4. Repeat the previous steps to create a second user, **Test2**.
5. In the **Accounts** box, select both **Test1** and **Test2**, right-click the selection, and then click **Delete**.
6. At the confirmation prompt, click **Yes**.

Restore deleted accounts

1. In Active Directory Administrative Center, click **Adatum (Local)**, and then double-click **Deleted Objects**.
2. Right-click **Test1**, and then click **Restore**.
3. Right-click **Test2**, and then click **Restore To**.
4. In the **Restore To** window, click the **IT** OU, and then click **OK**.
5. Confirm that Test1 is now located in the Research OU, and that Test2 is in the information technology (IT) OU.

Module Review and Takeaways

Best Practice

- Back up your domain controllers regularly.
- Consider AD DS database recovery as one of your restore scenarios for domain controllers.
- Enable Active Directory Recycle Bin to allow for simplified recovery of deleted objects.
- Use restartable AD DS when performing database maintenance tasks.

Review Question

Question: What kind of restoration can you perform with AD DS?

Answer: You can perform authoritative restore, nonauthoritative restore, and restoration of single objects with Active Directory Recycle Bin.

Lab Review Questions and Answers

Lab: Recovering Objects in AD DS

Question and Answers

Question: When you restore a deleted user or an OU with user objects by using authoritative restore, will the objects be exactly the same as before? Which attributes might not be the same?

Answer: Answers might vary, but the question is designed to frame a discussion about 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 the user's membership in groups. The user was removed from the member attribute of groups when it was deleted. Therefore, the restored user will not be a member of any groups other than the user's primary group. To restore group memberships, you also would have to consider authoritatively restoring groups. This might not always be desirable—when you authoritatively restore groups, you return their membership to the day on which the backup was made.

Question: In the lab, would it be possible to restore these deleted objects if they were deleted before Active Directory Recycle Bin has been enabled?

Answer: Yes, but only as tombstone objects without most attributes, or by using authoritative restore of AD DS.