Microsoft

OFFICIAL MICROSOFT LEARNING PRODUCT

10969B

Active Directory® Services with Windows Server®

Companion Content

Product Number: 10969B

Released: 01/2014

MICROSOFT LICENSE TERMS
MICROSOFT INSTRUCTOR-LED COURSEWARE

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to your use of the content accompanying this agreement which includes the media on which you received it, if any. These license terms also apply to Trainer Content and any updates and supplements for the Licensed Content unless other terms accompany those items. If so, those terms apply.

BY ACCESSING, DOWNLOADING OR USING THE LICENSED CONTENT, YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT THEM, DO NOT ACCESS, DOWNLOAD OR USE THE LICENSED CONTENT.

If you comply with these license terms, you have the rights below for each license you acquire.

1. DEFINITIONS.

a. "Authorized Learning Center" means a Microsoft IT Academy Program Member, Microsoft Learning Competency Member, or such other entity as Microsoft may designate from time to time.

b. "Authorized Training Session" means the instructor-led training class using Microsoft Instructor-Led Courseware conducted by a Trainer at or through an Authorized Learning Center.

c. "Classroom Device" means one (1) dedicated, secure computer that an Authorized Learning Center owns or controls that is located at an Authorized Learning Center's training facilities that meets or exceeds the hardware level specified for the particular Microsoft Instructor-Led Courseware.

d. "End User" means an individual who is (i) duly enrolled in and attending an Authorized Training Session or Private Training Session, (ii) an employee of a MPN Member, or (iii) a Microsoft full-time employee.

e. "Licensed Content" means the content accompanying this agreement which may include the Microsoft Instructor-Led Courseware or Trainer Content.

f. "Microsoft Certified Trainer" or "MCT" means an individual who is (i) engaged to teach a training session to End Users on behalf of an Authorized Learning Center or MPN Member, and (ii) currently certified as a Microsoft Certified Trainer under the Microsoft Certification Program.

g. "Microsoft Instructor-Led Courseware" means the Microsoft-branded instructor-led training course that educates IT professionals and developers on Microsoft technologies. A Microsoft Instructor-Led Courseware title may be branded as MOC, Microsoft Dynamics or Microsoft Business Group courseware.

h. "Microsoft IT Academy Program Member" means an active member of the Microsoft IT Academy Program.

i. "Microsoft Learning Competency Member" means an active member of the Microsoft Partner Network program in good standing that currently holds the Learning Competency status.

j. "MOC" means the "Official Microsoft Learning Product" instructor-led courseware known as Microsoft Official Course that educates IT professionals and developers on Microsoft technologies.

k. "MPN Member" means an active Microsoft Partner Network program member in good standing.

l. "Personal Device" means one (1) personal computer, device, workstation or other digital electronic device that you personally own or control that meets or exceeds the hardware level specified for the particular Microsoft Instructor-Led Courseware.

m. "Private Training Session" means the instructor-led training classes provided by MPN Members for corporate customers to teach a predefined learning objective using Microsoft Instructor-Led Courseware. These classes are not advertised or promoted to the general public and class attendance is restricted to individuals employed by or contracted by the corporate customer.

n. "Trainer" means (i) an academically accredited educator engaged by a Microsoft IT Academy Program Member to teach an Authorized Training Session, and/or (ii) a MCT.

o. "Trainer Content" means the trainer version of the Microsoft Instructor-Led Courseware and additional supplemental content designated solely for Trainers' use to teach a training session using the Microsoft Instructor-Led Courseware. Trainer Content may include Microsoft PowerPoint presentations, trainer preparation guide, train the trainer materials, Microsoft One Note packs, classroom setup guide and Pre-release course feedback form. To clarify, Trainer Content does not include any software, virtual hard disks or virtual machines.

2. USE RIGHTS. The Licensed Content is licensed not sold. The Licensed Content is licensed on a ***one copy per user basis***, such that you must acquire a license for each individual that accesses or uses the Licensed Content.

2.1 Below are five separate sets of use rights. Only one set of rights apply to you.

a. **If you are a Microsoft IT Academy Program Member:**
   i. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
   ii. For each license you acquire on behalf of an End User or Trainer, you may either:
      1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User who is enrolled in the Authorized Training Session, and only immediately prior to the commencement of the Authorized Training Session that is the subject matter of the Microsoft Instructor-Led Courseware being provided, **or**
      2. provide one (1) End User with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
      3. provide one (1) Trainer with the unique redemption code and instructions on how they can access one (1) Trainer Content,

   provided you comply with the following:
   iii. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
   iv. you will ensure each End User attending an Authorized Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Authorized Training Session,
   v. you will ensure that each End User provided with the hard-copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,
   vi. you will ensure that each Trainer teaching an Authorized Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Authorized Training Session,

vii. you will only use qualified Trainers who have in-depth knowledge of and experience with the Microsoft technology that is the subject of the Microsoft Instructor-Led Courseware being taught for all your Authorized Training Sessions,
viii. you will only deliver a maximum of 15 hours of training per week for each Authorized Training Session that uses a MOC title, and
ix. you acknowledge that Trainers that are not MCTs will not have access to all of the trainer resources for the Microsoft Instructor-Led Courseware.

b. **If you are a Microsoft Learning Competency Member**:
i. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
ii. For each license you acquire on behalf of an End User or Trainer, you may either:
    1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User attending the Authorized Training Session and only immediately prior to the commencement of the Authorized Training Session that is the subject matter of the Microsoft Instructor-Led Courseware provided, **or**
    2. provide one (1) End User attending the Authorized Training Session with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
    3. you will provide one (1) Trainer with the unique redemption code and instructions on how they can access one (1) Trainer Content,

    provided you comply with the following:
iii. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
iv. you will ensure that each End User attending an Authorized Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Authorized Training Session,
v. you will ensure that each End User provided with a hard-copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,
vi. you will ensure that each Trainer teaching an Authorized Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Authorized Training Session,
vii. you will only use qualified Trainers who hold the applicable Microsoft Certification credential that is the subject of the Microsoft Instructor-Led Courseware being taught for your Authorized Training Sessions,
viii. you will only use qualified MCTs who also hold the applicable Microsoft Certification credential that is the subject of the MOC title being taught for all your Authorized Training Sessions using MOC,
ix. you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and
x. you will only provide access to the Trainer Content to Trainers.

c. **If you are a MPN Member**:

i. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.

ii. For each license you acquire on behalf of an End User or Trainer, you may either:

1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User attending the Private Training Session, and only immediately prior to the commencement of the Private Training Session that is the subject matter of the Microsoft Instructor-Led Courseware being provided, **or**
2. provide one (1) End User who is attending the Private Training Session with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
3. you will provide one (1) Trainer who is teaching the Private Training Session with the unique redemption code and instructions on how they can access one (1) Trainer Content,

provided you comply with the following:

iii. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,

iv. you will ensure that each End User attending an Private Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Private Training Session,

v. you will ensure that each End User provided with a hard copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,

vi. you will ensure that each Trainer teaching an Private Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Private Training Session,

vii. you will only use qualified Trainers who hold the applicable Microsoft Certification credential that is the subject of the Microsoft Instructor-Led Courseware being taught for all your Private Training Sessions,

viii. you will only use qualified MCTs who hold the applicable Microsoft Certification credential that is the subject of the MOC title being taught for all your Private Training Sessions using MOC,

ix. you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and

x. you will only provide access to the Trainer Content to Trainers.

d. **If you are an End User:**

For each license you acquire, you may use the Microsoft Instructor-Led Courseware solely for your personal training use. If the Microsoft Instructor-Led Courseware is in digital format, you may access the Microsoft Instructor-Led Courseware online using the unique redemption code provided to you by the training provider and install and use one (1) copy of the Microsoft Instructor-Led Courseware on up to three (3) Personal Devices. You may also print one (1) copy of the Microsoft Instructor-Led Courseware. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.

e. **If you are a Trainer.**

i. For each license you acquire, you may install and use one (1) copy of the Trainer Content in the form provided to you on one (1) Personal Device solely to prepare and deliver an Authorized Training Session or Private Training Session, and install one (1) additional copy on another Personal Device as a backup copy, which may be used only to reinstall the Trainer Content. You may not install or use a copy of the Trainer Content on a device you do not own or control. You may also print one (1) copy of the Trainer Content solely to prepare for and deliver an Authorized Training Session or Private Training Session.

ii. You may customize the written portions of the Trainer Content that are logically associated with instruction of a training session in accordance with the most recent version of the MCT agreement. If you elect to exercise the foregoing rights, you agree to comply with the following: (i) customizations may only be used for teaching Authorized Training Sessions and Private Training Sessions, and (ii) all customizations will comply with this agreement. For clarity, any use of "*customize"* refers only to changing the order of slides and content, and/or not using all the slides or content, it does not mean changing or modifying any slide or content.

2.2 **Separation of Components.** The Licensed Content is licensed as a single unit and you may not separate their components and install them on different devices.

2.3 **Redistribution of Licensed Content**. Except as expressly provided in the use rights above, you may not distribute any Licensed Content or any portion thereof (including any permitted modifications) to any third parties without the express written permission of Microsoft.

2.4 **Third Party Notices**. The Licensed Content may include third party code tent that Microsoft, not the third party, licenses to you under this agreement. Notices, if any, for the third party code ntent are included for your information only.

2.5 **Additional Terms**. Some Licensed Content may contain components with additional terms, conditions, and licenses regarding its use. Any non-conflicting terms in those conditions and licenses also apply to your use of that respective component and supplements the terms described in this agreement.

3. LICENSED CONTENT BASED ON PRE-RELEASE TECHNOLOGY. If the Licensed Content's subject matter is based on a pre-release version of Microsoft technology ("**Pre-release**"), then in addition to the other provisions in this agreement, these terms also apply:

a. **Pre-Release Licensed Content.** This Licensed Content subject matter is on the Pre-release version of the Microsoft technology. The technology may not work the way a final version of the technology will and we may change the technology for the final version. We also may not release a final version. Licensed Content based on the final version of the technology may not contain the same information as the Licensed Content based on the Pre-release version. Microsoft is under no obligation to provide you with any further content, including any Licensed Content based on the final version of the technology.

b. **Feedback.** If you agree to give feedback about the Licensed Content to Microsoft, either directly or through its third party designee, you give to Microsoft without charge, the right to use, share and commercialize your feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft technology, Microsoft product, or service that includes the feedback. You will not give feedback that is subject to a license that requires Microsoft to license its technology, technologies, or products to third parties because we include your feedback in them. These rights survive this agreement.

c. **Pre-release Term**. If you are an Microsoft IT Academy Program Member, Microsoft Learning Competency Member, MPN Member or Trainer, you will cease using all copies of the Licensed Content on the Pre-release technology upon (i) the date which Microsoft informs you is the end date for using the Licensed Content on the Pre-release technology, or (ii) sixty (60) days after the commercial release of the technology that is the subject of the Licensed Content, whichever is earliest ("**Pre-release term**"). Upon expiration or termination of the Pre-release term, you will irretrievably delete and destroy all copies of the Licensed Content in your possession or under your control.

4. **SCOPE OF LICENSE**. The Licensed Content is licensed, not sold. This agreement only gives you some rights to use the Licensed Content. Microsoft reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the Licensed Content only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the Licensed Content that only allows you to use it in certain ways. Except as expressly permitted in this agreement, you may not:
   - access or allow any individual to access the Licensed Content if they have not acquired a valid license for the Licensed Content,
   - alter, remove or obscure any copyright or other protective notices (including watermarks), branding or identifications contained in the Licensed Content,
   - modify or create a derivative work of any Licensed Content,
   - publicly display, or make the Licensed Content available for others to access or use,
   - copy, print, install, sell, publish, transmit, lend, adapt, reuse, link to or post, make available or distribute the Licensed Content to any third party,
   - work around any technical limitations in the Licensed Content, or
   - reverse engineer, decompile, remove or otherwise thwart any protections or disassemble the Licensed Content except and only to the extent that applicable law expressly permits, despite this limitation.

5. **RESERVATION OF RIGHTS AND OWNERSHIP**. Microsoft reserves all rights not expressly granted to you in this agreement. The Licensed Content is protected by copyright and other intellectual property laws and treaties. Microsoft or its suppliers own the title, copyright, and other intellectual property rights in the Licensed Content.

6. **EXPORT RESTRICTIONS**. The Licensed Content is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the Licensed Content. These laws include restrictions on destinations, end users and end use. For additional information, see www.microsoft.com/exporting.

7. **SUPPORT SERVICES**. Because the Licensed Content is "as is", we may not provide support services for it.

8. **TERMINATION.** Without prejudice to any other rights, Microsoft may terminate this agreement if you fail to comply with the terms and conditions of this agreement. Upon termination of this agreement for any reason, you will immediately stop all use of and delete and destroy all copies of the Licensed Content in your possession or under your control.

9. **LINKS TO THIRD PARTY SITES**. You may link to third party sites through the use of the Licensed Content. The third party sites are not under the control of Microsoft, and Microsoft is not responsible for the contents of any third party sites, any links contained in third party sites, or any changes or updates to third party sites. Microsoft is not responsible for webcasting or any other form of transmission received from any third party sites. Microsoft is providing these links to third party sites to you only as a convenience, and the inclusion of any link does not imply an endorsement by Microsoft of the third party site.

10. **ENTIRE AGREEMENT.** This agreement, and any additional terms for the Trainer Content, updates and supplements are the entire agreement for the Licensed Content, updates and supplements.

11. **APPLICABLE LAW.**
    a. United States. If you acquired the Licensed Content in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.

b. Outside the United States. If you acquired the Licensed Content in any other country, the laws of that country apply.

12. LEGAL EFFECT. This agreement describes certain legal rights. You may have other rights under the laws of your country. You may also have rights with respect to the party from whom you acquired the Licensed Content. This agreement does not change your rights under the laws of your country if the laws of your country do not permit it to do so.

13. DISCLAIMER OF WARRANTY. THE LICENSED CONTENT IS LICENSED "AS-IS" AND "AS AVAILABLE." YOU BEAR THE RISK OF USING IT. MICROSOFT AND ITS RESPECTIVE AFFILIATES GIVES NO EXPRESS WARRANTIES, GUARANTEES, OR CONDITIONS. YOU MAY HAVE ADDITIONAL CONSUMER RIGHTS UNDER YOUR LOCAL LAWS WHICH THIS AGREEMENT CANNOT CHANGE. TO THE EXTENT PERMITTED UNDER YOUR LOCAL LAWS, MICROSOFT AND ITS RESPECTIVE AFFILIATES EXCLUDES ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

14. LIMITATION ON AND EXCLUSION OF REMEDIES AND DAMAGES. YOU CAN RECOVER FROM MICROSOFT, ITS RESPECTIVE AFFILIATES AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO US$5.00. YOU CANNOT RECOVER ANY OTHER DAMAGES, INCLUDING CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT OR INCIDENTAL DAMAGES.

This limitation applies to

- anything related to the Licensed Content, services, content (including code) on third party Internet sites or third-party programs; and
- claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

It also applies even if Microsoft knew or should have known about the possibility of the damages. The above limitation or exclusion may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential or other damages.

Please note: As this Licensed Content is distributed in Quebec, Canada, some of the clauses in this agreement are provided below in French.

Remarque : Ce le contenu sous licence étant distribué au Québec, Canada, certaines des clauses dans ce contrat sont fournies ci-dessous en français.

EXONÉRATION DE GARANTIE. Le contenu sous licence visé par une licence est offert « tel quel ». Toute utilisation de ce contenu sous licence est à votre seule risque et péril. Microsoft n'accorde aucune autre garantie expresse. Vous pouvez bénéficier de droits additionnels en vertu du droit local sur la protection dues consommateurs, que ce contrat ne peut modifier. La ou elles sont permises par le droit locale, les garanties implicites de qualité marchande, d'adéquation à un usage particulier et d'absence de contrefaçon sont exclues.

LIMITATION DES DOMMAGES-INTÉRÊTS ET EXCLUSION DE RESPONSABILITÉ POUR LES DOMMAGES. Vous pouvez obtenir de Microsoft et de ses fournisseurs une indemnisation en cas de dommages directs uniquement à hauteur de 5,00 $ US. Vous ne pouvez prétendre à aucune indemnisation pour les autres dommages, y compris les dommages spéciaux, indirects ou accessoires et pertes de bénéfices.
Cette limitation concerne:

- tout ce qui est relié au le contenu sous licence, aux services ou au contenu (y compris le code) figurant sur des sites Internet tiers ou dans des programmes tiers; et.
- les réclamations au titre de violation de contrat ou de garantie, ou au titre de responsabilité stricte, de négligence ou d'une autre faute dans la limite autorisée par la loi en vigueur.

Elle s'applique également, même si Microsoft connaissait ou devrait connaître l'éventualité d'un tel dommage. Si votre pays n'autorise pas l'exclusion ou la limitation de responsabilité pour les dommages indirects, accessoires ou de quelque nature que ce soit, il se peut que la limitation ou l'exclusion ci-dessus ne s'appliquera pas à votre égard.

EFFET JURIDIQUE. Le présent contrat décrit certains droits juridiques. Vous pourriez avoir d'autres droits prévus par les lois de votre pays. Le présent contrat ne modifie pas les droits que vous confèrent les lois de votre pays si celles-ci ne le permettent pas.

Revised July 2013

Module 1

Overview of Access and Information Protection

Contents:

Lesson 1

Introduction to Access and Information Protection Solutions in Business

Contents:

Question and Answers

Discussion: How Do You Manage Identities in Your Organization?

Question: What AIP technologies are you currently running in your organization?

Answer: It starts with the receptionist, who serves as an AIP component to identify visitors, determine access requirements, and grant access.

Question: What business enhancements do your AIP technologies provide?

Answer: Possible enhancements include tighter security, the ability to meet compliance requirements, and a reduction in operational overhead by simplifying the management of multiple authentication repositories.

Question: What risks does your business currently face that AIP could help to mitigate?

Answer: Possible risks include the inability to identify who has access to what, inefficient employee termination processes, and authentication repositories with mismatched information.

Question: How can AIP solutions simplify information technology (IT) operations?

Answer: AIP solutions simplify IT operations through centralizing access management and providing flexible technologies to manage various systems.

Question: How do AIP solutions change how people access enterprise resources?

Answer: AIP solutions can provide people with single sign-on (SSO) experiences, which allows them to access resources in the same way from multiple devices.

Lesson 3

Overview of FIM 2010 R2

Contents:

Question and Answers

Discussion: Business Scenarios for FIM Usage

Question: Do you use any identity management solution?

Answer: Answers might vary.

Question: Do you have the need for identity management?

Answer: Answers might vary.

Question: In which scenarios are common identities not appropriate?

Answer: If you have applications or systems where you specifically want to have separate identities from your main directory.

Question: What are some real-world examples of using identity management?

Answer: A real-world example would be if you have a heterogeneous system with Microsoft and non-Microsoft directory services that are implemented, and you want to centralize user provisioning and deprovisioning in a way that when user is created in AD DS, it is provisioned automatically in other systems.

Module Review and Takeaways

Best Practices

- Clearly define your business requirements.
- Identify which roles and solutions will best meet business needs.
- Thoroughly test the proposed solution before implementing any AIP solutions.

Review Question(s)

Question: What are the five server roles that support AIP solutions?

Answer: These roles include AD DS, AD CS, AD FS, AD RMS, and AD LDS.

Question: What technology can help you simplify and automate user provisioning?

Answer: FIM components.

Question: What server role and technology are required to implement and manage smart cards?

Answer: You need to have AD CS and FIM 2010 R2

Module 2

Advanced Deployment and Administration of AD DS

Contents:

Lesson 1

Deploying AD DS

Contents:

Demonstration: Remote Deployment of Domain Controllers

Demonstration Steps

Add LON-SVR1 to Server Manager on LON-DC1

1. On LON-DC1, in Server Manager, select the **All Servers** view.
2. On the top menu, click the **Manage** menu, and then select **Add Servers**.
3. In the **Add Servers** dialog box, maintain the default settings, and then click **Find Now**.
4. In the **Active Directory** list of servers, select **LON-SVR1**, click the arrow to add it to the **Selected** list, and then click **OK**.

Add the AD DS role on a remote server

1. On LON-DC1, in Server Manager, in the **All Servers** view, ensure that LON-SVR1 is added to the **Servers** list.
2. On the top menu, click the **Manage** menu, and then select **Add Roles and Features**.
3. In the Add Roles and Features Wizard, on the **Before You Begin** page, click **Next**.
4. On the **Select installation type** page, keep the default role-based or feature-based installation, and then click **Next**.
5. On the **Select destination server** page, in the **Server Pool** section, select **LON-SVR1.Adatum.com**, and then click **Next**.
6. On the **Select server roles** page, in the **Roles** section, select **Active Directory Domain Services**. The **Add features that are required for Active Directory Domain Services** dialog box opens.
7. In the **Add features that are required for Active Directory Domain Services** dialog box, accept the default, and then click **Add Features**. If required, click **Next**.
8. In the **Select features** page, click **Next**.
9. On the **Active Directory Domain Services** page, click **Next**.
10. On the **Confirm installation selections** page, click **Install**.
11. Wait until the Active Directory binaries are installed, and then click **Close**.

Configure AD DS remotely by using Server Manager

1. On LON-DC1, when the installation of the AD DS role on LON-SRV1 is finished, in Server Manager, on the top menu, click the **Notifications** flag symbol.
2. Note the Post-deployment Configuration of LON-SVR1, and then click the **Promote this server to a domain controller** link.
3. In the Active Directory Domain Services Configuration Wizard, on the **Deployment Configuration** page, **Select the deployment operation** to **Add a domain controller to an existing domain**. Ensure that the domain **Adatum.com** is specified. In the **Supply the credentials to perform this operation** section, click **Change**.
4. In the **Credentials for deployment operation** dialog box, enter the following, click **OK**, and then click **Next**:
   - User name: **Administrator**
   - Password: **Pa$$w0rd**
5. On the **Domain Controller Options** page, clear the selections for the **Domain Name System (DNS) server** and **Global Catalog (GC)**. **Read-only domain controller (RODC)** also should not be selected.

6. In the Type the Directory Services Restore Mode (DSRM) password section, enter and confirm the password **Pa$$w0rd**, and then click **Next**.
7. If present, on the **DNS Options** page, ignore the alert, and then click **Next**.
8. On the **Additional Options** page, click **Next**.
9. On the **Paths** page, keep the default path settings for the Database folder, Log files folder, and SYSVOL folder, and then click **Next**.
10. On the **Review Options** page, show the generated Windows PowerShell command-line interface script by clicking **View script**. When done, exit Notepad.exe, and then click **Next**.
11. When the Prerequisites Check is performed and finished, review the results, and then click **Install**.
12. After the installation completes, click **Close**.
13. Verify that the server is added to the AD DS view in Server Manager.

Lesson 2

Deploying and Cloning Virtual Domain Controllers

Contents:

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 Active Directory Administrative Center, double-click **Adatum (local)**, and then in the details pane, double-click the **Domain Controllers** organizational unit (OU).
3. In the details pane, select **LON-DC1**, and then in the Tasks panes, in the LON-DC1 section, click **Add to group**.
4. In the **Select Groups** dialog box, in the **Enter the object names to select text field**, 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 LON-DC1, in the taskbar, click the **Windows PowerShell** icon.
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, we need to verify each app or use a domain controller that has fewer apps installed by default. We accept taking the risk, type the following command, and then press Enter:

```
Get-ADDCCloningExcludedApplicationList –GenerateXML
```

9. Run the following command to create the DCCloneConfig.xml file:

```
New-ADDCCloneConfigFile
```

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

```
Stop-Computer
```

Export the source virtual machine

1. On the host computer, in Hyper-V Manager, in the details pane, select the **10969B-LON-DC1** virtual machine.
2. In the Actions pane, in the 10969B-LON-DC1 section, click **Export**.
3. In the **Export Virtual Machine** dialog box, select the location **D:\Program Files\Microsoft Learning\10969**, and then click **Export**.
4. Wait until the export finishes.
5. In the Actions pane, in the **10969-LON-DC1** section, click **Start**.

Create and start the cloned domain controller

1. In the Actions pane, in the upper 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**, select the folder **D:\Program Files\Microsoft Learning\10969\10969B-LON-DC1**, click **Select Folder**, and then click **Next**.

4. On the **Select Virtual Machine** page, select **10969B-LON-DC1**, and then click **Next**.
5. On the **Choose Import Type** page, select **Copy the virtual machine (create a new unique ID)**, 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\10969** as the path. Click **Next**.
7. On the **Choose Folders to Store Virtual Hard Disks** page, provide the path **D:\Program Files\Microsoft Learning\10969\,** and then click **Next**.
8. On the **Completing Import Wizard** page, click **Finish**.
9. In the details pane, identify and select the newly imported virtual machine named **10969B-LON-DC1**, which has the State shown as **Off**. In the lower section of the Actions pane, click **Rename**.
10. Type **10969B-LON-DC3** as the name, and then press Enter.
11. In the Actions pane, in the 10969B-LON-DC3 section, click **Start**, and then click **Connect** to see the virtual machine starting.

Lesson 4

Administering AD DS

Contents:

Demonstration: Using Active Directory Administrative Center to Administer and Manage AD DS

Demonstration Steps

Navigate within Active Directory Administrative Center

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

Perform an administrative task within Active Directory Administrative Center

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

Create objects

1. In Active Directory Administrative Center, in the details pane, double-click **Adatum (local)**, and then double-click the **Computers** container.
2. In the Tasks pane, in the Computers section, click **New**, 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**

View all object attributes

1. In Active Directory Administrative Center, double-click **Adatum (local)**, and then in the details pane, double-click **Computers**.
2. Select **LON-CL4**. 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 attributes of the computer object are available here.
4. Close LON-CL4 properties window by clicking **Cancel**.

Use the Windows PowerShell History viewer

1. In Active Directory Administrative Center, click the **Windows PowerShell History** toolbar at the bottom 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.

Demonstration: Administering AD DS with Windows PowerShell

Demonstration Steps

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

```
Get-ADUser –filter {Department –eq 'Marketing'} –properties department | ft
name,department
```

3. Verify in the output of the command that all users belong to the Marketing department.
4. At the Windows PowerShell command prompt, type the following, and then press Enter:

```
Get-ADUser –LDAPFilter "(&(objectClass=User)(department=Marketing))" –properties sn |
where {$_.sn –ge 'L'} | Set-ADUser –department 'Marketing2'
```

5. In Server Manager, click **Tools**, and then click **Active Directory Administrative Center**.
6. In Active Directory Administrative Center, double-click **Adatum (local)**, and then in the details pane, scroll down and double-click **Marketing**.
7. Confirm that user accounts with a last name beginning with L through Z have the department **Marketing2** in their properties.
8. At the Windows PowerShell command prompt, type the following, and then press Enter:

```
Get-ADOrganizationalUnit –filter * -Properties ProtectedFromAccidentalDeletion |
where {$_.ProtectedFromAccidentalDeletion –match $False}
```

9. Verify in the output of the command that the domain controller's default OU is not protected from accidental deletion.
10. At the Windows PowerShell command prompt, type the following, and then press Enter:

```
Get-ADOrganizationalUnit –filter * -Properties ProtectedFromAccidentalDeletion |
where {$_.ProtectedFromAccidentalDeletion –match $False} | Set-ADOrganizationalUnit –
ProtectedFromAccidentalDeletion $true
```

11. At the Windows PowerShell command prompt, type the following, and then press Enter:

```
Get-ADOrganizationalUnit –filter * -Properties ProtectedFromAccidentalDeletion |
where {$_.ProtectedFromAccidentalDeletion –match $False}
```

12. Verify that the domain controller's OU is no longer listed and that the results are empty because the Domain Controller OU is now protected from accidental deletion.

Module Review and Takeaways

Question: What is the benefit of deploying domain controllers remotely?

Answer: If you want to use the Server Core installation version of the operating system, which is streamlined to operate server loads, you can still use the tools that you are used to, without typing a lengthy command at the command prompt. Also, for RODCs, we do not recommend signing in locally or via remote desktop with elevated credentials. Promoting them remotely minimizes those risks. Lastly, you can automate the deployment of multiple servers remotely by using Windows PowerShell.

Question: Why have virtual domain controllers been a risk in previous version of the operating system, and how has this changed in Windows Server 2012?

Answer: It is important that virtual domain controllers have the correct time. You must not have a single point of failure across all your domain controllers, and you must not use checkpoints on the virtualization guests in previous versions of the operating system because this will cause your AD DS infrastructure to be in an inconsistent state. With Windows Server 2012 and a supported hypervisor, virtualization safeguards prevent this from happening.

Question: How can you find out which cmdlets are available for AD DS administration and deployment in the Active Directory module for Windows PowerShell?

Answer: You can use the following to get a list of AD DS cmdlets:

```
Get-Command –Module ActiveDirectory
```

```
Get-Command –Module ADDSDeployment
```

You then can use **Get-Help** for more information about a specific cmdlet.

Tools

Tool	Use for	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
Windows PowerShell cmdlets	Automating the management of the AD DS infrastructure and its objects.	Available for Active Directory, AD DS deployment, and Group Policy

Lab Review Questions and Answers

Lab: Deploying and Administering AD DS

Question and Answers

Question: In the lab, you used Active Directory Administrative Center and the Active Directory module for Windows PowerShell. Which tool would you prefer to use for each tasks?

Answer: Active Directory Administrative Center is better for individual tasks when you prefer to use the GUI. Windows PowerShell is better when performing the task multiple times, or if you prefer to do more complex operations. Also, automating tasks by using a script enables you to test it beforehand to avoid errors in production.

Question: In which scenarios can domain controller cloning be useful?

Answer: Cloning can be useful in any scenario where you want to deploy multiple domain controllers quickly, such as in private cloud scenarios where you need to scale out, in scenarios where you want to deploy multiple servers quickly in a remote location, or as part of a recovery plan.

Module 3

Securing AD DS

Contents:

Lesson 1

Securing Domain Controllers

Contents:

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 **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 **Thorsten**, and then click **Check Names**.
15. Verify that Thorsten Scholl 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 **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 **Anne**, and then click **Check Names**.
7. In the **Multiple Names Found** dialog box, select **Anne-Mette Stolze**, and then click **OK**.
8. Click **OK** in the **Select Users, Contacts, Computers, Service Accounts or Groups** dialog box, and then click **OK** in the **Munich Allowed RODC Password Replication Group Properties** dialog box.
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**.
3. In the **Advanced Password Replication Policy for MUC-RODC1** dialog box, note that you usually see the accounts whose passwords are stored on this RODC.
4. 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 note that this will only show accounts that have the permissions and have already been authenticated by this RODC.
5. 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 **Anne-Mette**, click **Check Names**, and then click **OK**.
6. Recognize that Anne-Mette has a Resultant Setting of Allow.
7. Close or Cancel all dialog boxes.

Lesson 2

Implementing Account Security

Contents:

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, type **20** in the **Keep password history for** field, click **OK**, and then double-click **Maximum password age**.
5. In the Maximum password age Properties dialog box, type **45** in the **Password will expire in** field, 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, type **10** in the **Password must be at least** field, 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**, type **30** in the **Minutes** field, 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, type **15** in the **Reset account lockout counter after** field, 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:
   - In the **Name** field, type **ManagersPSO**.
   - In the **Precedence** field, type **10**.
   - Select the **Enforce minimum password length** check box, and then in the **Minimum password length (characters)** field, type **15**.
   - Select the **Enforce password history** check box, and, then in the **Number of passwords remembered** field, type **20**.
   - Select the **Password must meet complexity requirements** check box.
   - Select the **Enforce minimum password age** check box, and then in the **User cannot change the password within (days)** field, type **1**.
   - Select the **Enforce maximum password age** check box, and then in the **User must change the password after (days)** field, type **30**.
   - Select the **Enforce account lockout policy** check box.
   - In the **Number of failed logon attempts allowed** field, type **3**.
   - 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 Active Directory Administrative Center.

Lesson 3

Implementing Audit Authentication

Contents:

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 show the configuration options:
   - If the **Define these policy settings** check box is selected, the policy is applied.
   - If **Success** is selected, only success audits will be logged.
   - If **Failure** is selected, only failure audits are logged.

   If multiple policies contain the setting and it is defined differently, the success and failure options are taken from 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. Show the 10 main categories in the **Audit Policies** policy, 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 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** and **Failure**, and then click **Apply**.
13. On the **Explain** tab, show and discuss the explanation, the default settings, and the predicted auditing volume.
14. Click **OK** to close the **Audit Kerberos Authentication Service Properties** dialog box.

Demonstration: Viewing Logon Events

Demonstration Steps

1. On LON-DC1, in 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 Start screen. In the upper-right corner, click **Administrator**, and then click **Sign Out**.
5. On LON-DC1, attempt to sign in as **Adatum\Benno** 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\Benno tried to log on 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 logged on successfully. Click **Close**.
13. Close Event Viewer.

Module Review and Takeaways

Review Question(s)

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

Answer: AD DS domain controllers store all information about any user, computer, group, and any other object in the domain. If someone is able to access the server physically, or the hard drive of the server, this person can circumvent security guards quite easily and get all information. This person then can use the information to attack the rest of the network or to modify the domain controller and put it back into the network.

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

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

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 can provide attackers an easily accessible denial of service (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 to lock out valid user accounts.

Tools

Tool	Use for	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 Settings\Security Settings\Local Policies\Security Options**.

Common Issue	Troubleshooting Tip
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 event 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, we configured the password settings for all users within the Default Domain Policy, and we configured the password settings for Administrators within a PSO. What other options were available to accomplish the solution?

Answer: We 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, we 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—for example, a subset of administrators to access HR data, or service accounts where 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 4

Implementing and Administering AD DS Sites and Replication

Contents:

Lesson 2

Configuring AD DS Sites

Contents:

Demonstration: Configuring AD DS Sites

Demonstration Steps

1. Switch to LON-DC1, and in Server Manager, click **Tools**, and then click **Active Directory Sites and Services**.
2. In Active Directory Sites and Services, expand **Sites**, and then click **Default-First-Site-Name**.
3. Right-click **Default-First-Site-Name**, and then click **Rename**.
4. 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:

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 Active Directory Sites and Services, expand **Sites**, and then expand **Inter-Site Transports**.
3. Click **IP**, right-click **DEFAULTIPSITELINK**, and then click **Rename**.
4. Type **LON-TOR**, and then press Enter.
5. Right-click **LON-TOR**, and then click **Properties**. Describe the **Cost**, **Replicate every**, and **Change Schedule** options.
6. In the **LON-TOR Properties** dialog box, next to Replicate every, configure the value to be **60** minutes.
7. Click **Change Schedule**.
8. Highlight the range from **Monday 12 PM** to **Friday 4PM**, click **Replication Not Available**, and then click **OK**.
9. Click **OK** to close the **LON-TOR Properties** dialog box.
10. 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 with them.
- Do not set up long intervals without replication when you configure replication schedules for intersite replication.
- Avoid using SMTP as a protocol for replication.

Review Question(s)

Question: Why is it important that all subnets are identified and associated with a site in a multisite enterprise?

Answer: The process of locating domain controllers and other services can be made 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 strange 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 three hours, it is really a matter of replication timing rather than replication quantity. However, in some extreme situations, it is possible that 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.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Client cannot locate the domain controller in its site.	Verify whether all SRV resource 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.
Replication between sites does not work.	Verify whether site links are configured correctly. Verify the replication schedule. Verify whether the firewall between the sites permits traffic for Active Directory replication.

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

Lab Review Questions and Answers

Lab: Implementing AD DS Sites and Replication

Question and Answers

Question: In the last exercise, there was a problem on TOR-DC1. What was the problem?

Answer: The subnet mask was incorrect for the current network configuration. This caused DNS problems that resulted in replication failures.

Question: You decide to add a new domain controller to the LondonHQ site named LON-DC2. How could you ensure that LON-DC2 is used to pass 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 that AD DS replication is configured correctly. If you are using AD DS–integrated DNS, then the domain controller records also will update in the DNS application partitions.

Module 5

Implementing Group Policy

Contents:

Lesson 1

Introducing Group Policy

Contents:

Demonstration: How to Create a GPO and Configure GPO Settings

Demonstration Steps

Use the Group Policy Management Console (GPMC) to create a new GPO

1. Sign in to LON-DC1 as **Adatum\Administrator** with password **Pa$$w0rd**.
2. In Server Manager, click **Tools**, and then click **Group Policy Management**.
3. If necessary, expand **Forest: Adatum.com**, expand **Domains**, and then expand **Adatum.com**.
4. Select and right-click the **Group Policy Objects** folder, and then click **New**.
5. In the **New GPO** dialog box, in the **Name** field, type **Desktop**, and then click **OK**.

Configure Group Policy settings

1. In Group Policy Management, expand the **Group Policy Objects** folder, right-click the **Desktop** policy, and then click **Edit**.
2. In Group Policy Management Editor window, under the Computer Configuration node, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, expand **Local Policies**, and then click **Security Options**.
3. In the details pane, double-click **Interactive logon: Do not display last user name**.
4. In the **Interactive logon: Do not display last user name Properties** dialog box, select the **Define this policy setting** check box, click **Enabled**, and then click **OK**.
5. Under the Security Settings node, click **System Services**.
6. In the details pane, double-click **Windows Installer**.
7. In the **Windows Installer Properties** dialog box, select the **Define this policy setting** check box, and then click **OK**.
8. Under the User Configuration node, expand **Policies**, expand **Administrative Templates**, and then click **Start Menu and Taskbar**.
9. In the details pane, double-click **Remove Search link from Start Menu**.
10. In the **Remove Search link from Start Menu** dialog box, click **Enabled**, and then click **OK**.
11. Under the **Administrative Templates** node, expand **Control Panel**, and then click **Display**.
12. In the details pane, double-click **Hide Settings tab**.
13. In the **Hide Settings tab** dialog box, click **Enabled**, and then click **OK**.

Lesson 3

Group Policy Scope and Group Policy Processing

Contents:

Demonstration: How to Link 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 window, type **Remove Run Command** in the **Name** field, 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 window, type **Do Not Remove Run Command** in the **Name** field, and then click **OK**.
7. Expand **Group Policy Objects**, right-click the **Remove Run Command** GPO, and then click **Edit**.
8. In 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. Right-click the **Do Not Remove Run Command** GPO, and then click **Edit**.
12. In 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**. The Remove Run Command GPO is now 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 no longer is 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 the 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 the Group Policy Management Console.

Demonstration: How to Filter Group Policies

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** field, 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, type **Ed Meadows**, 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** field, type **OS Version Filter**.
3. In the Queries pane, click **Add**.
4. In the **WMI Query** dialog box, in the **Query** field, type the following, and then click **OK**:

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

5. At the **Warning** 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** field, 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 the Group Policy Management Console.

Lesson 4

Troubleshooting the Application of GPOs

Contents:

Demonstration: Performing an Analysis with the Group Policy Modeling Wizard

Demonstration Steps

Use GPResult.exe to create a report

1. On LON-DC1, on the Start screen, under the Desktop tile, click the arrow.
2. In the **Apps** list, click **Command Prompt**.
3. In the Administrator: Command Prompt window, type **cd desktop**, and then press Enter.
4. In the Administrator: Command Prompt window, type the following, and then press Enter:

```
GPResult /r
```

5. Review the output in the Command Prompt window.
6. In the Administrator: Command Prompt window, type the following, and then press Enter:

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

7. Close the Command Prompt window, and then double-click the **results.html** file on the desktop.
8. In the Internet Explorer window, view the results of the report.
9. Close Internet Explorer.

Use the 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, right-click **Group Policy Results**, and then click **Group Policy Results Wizard**.
3. In the 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 the **Group Policy Results** folder, right-click the **Administrator on LON-DC1** report, and then click **Save Report**.
10. In the **Save GPO Report** dialog box, click **Desktop**, and then click **Save**.

Use the Group Policy Modeling Wizard to create a report

1. Right-click the **Group Policy Modeling** folder, and then click **Group Policy Modeling Wizard**.
2. In the 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, type **Ed Meadows**, and then click **OK**.
6. Under Computer information, 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

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 are applied across slow links by default?

Answer: Registry policy processing and Security policy are applied 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 global 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 Apply Group Policy permission to the Managers group.

Lab Review Questions and Answers

Lab: Implementing and Troubleshooting 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 Infrastructures, and in other standard environments.

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

Answer: The correct answer will be based on students' experiences and situations.

Question: In which situations have you used, or could you anticipate using Group Policy Modeling?

Answer: The correct answer will be based on students' experiences and situations.

Module 6

Managing User Settings with Group Policy

Contents:

Lesson 1

Implementing Administrative Templates

Contents:

Question and Answers

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.

Demonstration: Configuring Settings with Administrative Templates

Demonstration Steps

Filter Administrative Templates policy settings

1. Switch to LON-DC1.
2. If required, sign in as **Adatum\Administrator** with password **Pa$$w0rd**.
3. From Server Manager, click **Tools**, and then click **Group Policy Management**.
4. In the console tree, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, and then click the **Group Policy Objects** container.
5. Right-click the **Group Policy Objects** container, and then click **New**.
6. In the **New GPO** dialog box, in the **Name** field, type **GPO1**, and then click **OK**.
7. In the details pane, right-click **GPO1**, and then click **Edit**. The Group Policy Management Editor window appears.
8. In the console tree, expand **User Configuration**, expand **Policies**, and then click **Administrative Templates**.
9. Right-click **Administrative Templates**, and then click **Filter Options**.
10. Select the **Enable Keyword Filters** check box.
11. In the **Filter for word(s)** text box, type **screen saver**.
12. In the drop-down box next to the text box, select **All**, and then click **OK**. 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.
13. In the console tree, under User Configuration, right-click **Administrative Templates**, and then click **Filter Options**.
14. Clear the **Enable Keyword Filters** check box.
15. In the **Configured** drop-down list box, select **Yes**, and then click **OK**. Administrative Templates policy settings filter to show only those that have been configured as enabled or disabled. No settings have been enabled.
16. 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, click **Apply**, 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**, click **Apply**, and then click **OK**.

Add comments to a GPO

1. In the console tree of the Group Policy Management Editor window, 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***. This comment appears on the **Details** tab of the GPO in the Group Policy Management Console. Click **OK**.
4. Close the Group Policy Management Editor window.

Create a new GPO by copying an existing GPO

1. In the Group Policy Management Console tree, 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 Group Policy Management Console tree, 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 Group Policy Management Console tree, 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 Group Policy Management Console tree, 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 Group Policy Management Console.

Lesson 2

Configuring Folder Redirection and Scripts

Contents:

Question and Answers

Settings for Configuring Folder Redirection

Question: Users in the same department often log on 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 **File Explorer**.
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** box, type **Redirect**, and then press Enter.
5. Right-click the **Redirect** 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. Click **Start**.
2. Click **Administrative Tools**, and then double-click **Group Policy Management**.
3. Expand **Forest: Adatum.com**, and then expand **Domains**.
4. Right-click **Adatum.com**, and then click **Create a GPO in this domain and Link it here**.
5. In the **New GPO** dialog box, in the **Name** box, type **Folder Redirection**, and then click **OK**.
6. Expand **Adatum.com**, right-click **Folder Redirection**, and then click **Edit**.
7. In the Group Policy Management Editor window, under User Configuration, expand **Policies**, expand **Windows Settings**, and then expand **Folder Redirection**.
8. Right-click **Documents**, and then click **Properties**.
9. In the **Document Properties** dialog box, on the **Target** tab, next to Setting, click the drop-down arrow, and then select **Basic-Redirect everyone's folder to the same location**.
10. Ensure that the **Target folder location** box is set to **Create a folder for each user under the root path**.
11. In the **Root Path** box, type **\\LON-DC1\Redirect2**, and then click **OK**. Note: A shared folder called Redirect already existed on this server, so when you shared C:\Redirect, the share was created as Redirect2.
12. In the **Documents Properties** dialog box, click **Yes**.
13. Close all open windows.

Test Folder Redirection

1. Sign in to LON-CL1 as **Adatum\Administrator** with password **Pa$$w0rd**.
2. On Start screen, type **cmd.exe**, and then press Enter.
3. At the command prompt, type the following command, and then press Enter:

```
Gpupdate /force
```

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

```
Y
```

5. Sign in to LON-CL1 as **Adatum\Administrator** with password **Pa$$w0rd**.
6. From Start screen, click **Desktop**.
7. Right-click the desktop, and then click **Personalize**.
8. In the navigation pane, click **Change desktop icons**.
9. In **Desktop Icon Settings**, select the **User's Files** check box, and then click **OK**.
10. On the desktop, double-click **Administrator**.
11. Right-click **Documents**, and then click **Properties**.
12. In the **Document Properties** dialog box, note that the location of the folder is now the Redirect2 network share in a subfolder named for the user. If this is not successful, repeat steps 2 through 6 and then check the redirection once again.
13. Sign out of LON-CL1.

Demonstration: Configuring Scripts with GPOs

Demonstration Steps

Create a logon script to display a message

1. On LON-DC1, point to the lower-right corner, and then click **Start**.
2. On the Start screen, type **Notepad**, and then press Enter.
3. In Notepad, type the following command, and then press Enter:

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

4. Click the **File** menu, and then click **Save As**.
5. In the **Save As** dialog box, in the **File name** box, type **Logon.vbs**.
6. In the **Save as type** list, select **All Files (*.*)**.
7. In the navigation pane, click **Desktop**, and then click **Save**.
8. Close Notepad.
9. 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** box, type **ScriptTest**, and then click **OK**.
5. Expand **Adatum.com**, right-click the **ScriptTest** 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 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. On Start screen, type **cmd.exe**, and then press Enter.
3. At the command prompt, type the following command, and then press Enter:

```
Gpupdate /force
```

4. If prompted, at the command prompt, type the following, and then press Enter:

```
Y
```

5. Sign in to LON-CL1 as **Adatum\Adam** with password **Pa$$w0rd**.
6. Click **Desktop.**
7. Verify that the scripts runs, displaying the message. Note that this may take up to five to ten minutes to display. If the message does not appear, restart LON-CL1 and repeat step one through six.
8. Sign out of LON-CL1.

Lesson 3

Configuring Group Policy Preferences

Contents:

Demonstration: Configuring Group Policy Preferences

Demonstration Steps

Configure a desktop shortcut with Group Policy Preferences

1. On LON-DC1, from Server Manager, open the Group Policy Management Console.
2. In the console tree, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, and then click the **Group Policy Objects** container.
3. In the **Group Policy Objects** folder, in the details pane, right-click **Default Domain Policy**, and then click **Edit**.
4. Expand **User Configuration**, expand **Preferences**, expand **Windows Settings**, right-click **Shortcuts**, point to **New**, and then click **Shortcut**.
5. In the **New Shortcut Properties** dialog box, in the **Action** list, select **Create**.
6. In the **Name** box, type **Notepad**.
7. In the **Location** box, click the arrow, and then select **All Users Desktop**.
8. In the **Target path** box, type **C:\Windows\System32\Notepad.exe**.

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 **Computer Name**.
3. In the **Computer name** box, type **LON-CL1**, and then click **OK** twice.

Configure a new folder with Group Policy Preferences

1. Under Windows Settings, right-click **Folders**, point to **New**, and then click **Folder**.
2. In the **New Folder Properties** dialog box, in the **Action** list, select **Create**.
3. In the **Path** field, type **C:\Reports**.

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 8.1**, 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. Verify the presence of the Notepad shortcut on the desktop.
3. On the taskbar, click **File Explorer**.
4. Verify the presence of the C:\Reports folder.
5. If these do not appear, then click **Start** and type **cmd.exe**, and then press Enter.
6. At the command prompt, type the following command, and then press Enter:

```
gpupdate /force
```

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

```
Y
```

8. Sign in to LON-CL1 as **Adatum\Administrator** with password **Pa$$w0rd**.
9. From Start screen, click **Desktop**.
10. Verify the presence of the Notepad shortcut on the desktop.
11. On the taskbar, click **File Explorer**.
12. Verify the presence of the C:\Reports folder.

Module Review and Takeaways

Best Practices

Best Practices Related to Group Policy Management

- Include comments on GPO settings.
- Use a central store for Administrative templates when having clients with Windows Vista, Windows 7, and Windows 8.
- Use Group Policy Preferences to configure settings that are not available in the Group Policy settings.

Review Question(s)

Question: Why do some Group Policy settings take two logons before taking effect?

Answer: Users typically log on with cached credentials before Group Policy can apply to the current session. The settings will take effect at the next logon.

Question: How can you support Group Policy Preferences on Windows XP?

Answer: You must download and install the Group Policy client-side extensions for Group Policy Preferences.

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: GPO 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 XP and Windows 8 computers. After configuring several settings in the Administrative templates of a GPO, users with Windows XP operating systems report that some settings apply and others do not.	Not all new settings apply to older operating systems such as Windows XP. 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 Desktops with Group Policy

Question and Answers

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

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

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

Answer: You could use Windows Management Instrumentation 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: 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

Deploying and Managing AD CS

Contents:

Lesson 1

Deploying CAs

Contents:

Demonstration: Deploying an Enterprise Root CA

Demonstration Steps

Deploy an enterprise root CA

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

Lesson 2

Administering CAs

Contents:

Resources

Managing CA Hierarchy

Reference Links:

- AD CS Deployment Cmdlets in Windows PowerShell - http://go.microsoft.com/fwlink/?LinkId=331182
- AD CS Administration Cmdlets in Windows PowerShell - http://go.microsoft.com/fwlink/?LinkId=331183

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 locations.
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**.

Module Review and Takeaways

Best Practices

- When deploying a CA infrastructure, deploy a stand-alone (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 Question(s)

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

Answer: Some reasons are to improve security, to increase identity control, and to sign 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 FIM 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	Troubleshooting Tip
The location of the CA certificate that is specified in the AIA extension is not configured to include the certificate name suffix. Clients might not be able to locate the correct version of the issuing CA's certificate to build a certificate chain, and certificate validation might fail.	Use the Certification Authority snap-in to configure the AIA extension to include the certificate name suffix in each location.
The CA is not configured to include CDP locations in the extensions of issued certificates. Clients might not be able to locate a CRL to check the revocation status of a certificate, and certificate validation might fail.	Use the Certification Authority snap-in to configure the CDP extension and to specify the network location of the CRL.

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 8

Deploying and Managing Certificates

Contents:

Lesson 1

Using Certificates in a Business Environment

Contents:

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. 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 the 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 window without saving changes.
9. Open Word 2013.
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 2013, and 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 password **Pa$$w0rd**.
7. Open File Explorer, and then navigate 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 2

Deploying and Managing Certificate Templates

Contents:

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 note what you can modify on each. Note 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 **Read**, **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 3

Managing Certificates Deployment, Revocation, and Recovery

Contents:

Demonstration: Configuring a CA for Key Archival

Demonstration Steps

1. On LON-DC1, 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 Domain Admins and Enterprise Admins 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. On the taskbar, 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 the 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 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), and then click **OK** twice.

Module Review and Takeaways

Best Practices

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

Review Question(s)

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 certificates, 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 2012 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

Certification Authority console

Certificate Templates console

Certificates console

Certutil.exe

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
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

Common Issue	Troubleshooting Tip
	options in Group Policy, and that you assigned the Read, Enroll, and Autoenroll permissions to the appropriate group of users or computers.
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 9

Implementing and Administering AD RMS

Contents:

Lesson 2

Deploying and Managing an AD RMS Infrastructure

Contents:

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** field, 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, enter the following details, and then click **OK**:
   - First name: **ADRMSSVC**
   - User UPN logon: **ADRMSSVC**
   - Password: **Pa$$w0rd**
   - Confirm Password: **Pa$$w0rd**
   - Password never expires: **Enabled**
   - User cannot change password: **Enabled**

Prepare 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, enter 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 password **Pa$$w0rd**.
2. In Server Manager, click **Manage**, and then click **Add Roles and Features**.
3. In the Add Roles and Features Wizard, click **Next** three times.
4. On the **Server Roles** page, click **Active Directory Rights Management Services**.
5. In the **Add Roles and Features Wizard** dialog box, click **Add Features**, click **Next** four times, click **Install**, and then click **Close**.

Configure AD RMS

1. 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, enter the following details, click **OK**, and then click **Next (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)**:
   - User name: **ADRMSSVC**
   - Password: **Pa$$w0rd**
9. On the **Cryptographic Mode** page, click **Cryptographic Mode 2**, and then click **Next**.
10. On the **Cluster Key Storage** page, click **Use AD RMS centrally managed key storage**, and then click **Next**.
11. On the **Cluster Key Password** page, type password **Pa$$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 click **Close**.
17. On the Start screen, 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:

Demonstration: Creating a Rights Policy Template

Demonstration Steps

1. On LON-SVR1, in 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, enter 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 Application

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, enter 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 users to inform them of AD RMS functionality and to ask for feedback on the types of templates that they would like to have available.
- Strictly control membership of the Super Users group. Users in this group can access all protected content. Granting membership in this group gives users complete access to all AD RMS–protected content.

Review Question(s)

Question: What are the benefits of having a Secure Sockets Layer (SSL) certificate installed on the AD RMS server when you perform 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 are not members of your organization. Which method should you use to provide this access?

Answer: Use Windows Live ID 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 app exclusion for PowerPoint.

Lab Review Questions and Answers

Lab: Implementing an AD RMS Infrastructure

Question and Answers

Question: What steps can you take to ensure that you can use Information Rights Management (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 10

Implementing and Administering AD FS

Contents:

Lesson 2

Deploying AD FS

Contents:

Demonstration: Installing the AD FS Server Role

Demonstration Steps

Install AD FS

1. On LON-DC2, in 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-DC2.Adatum.com**, and then click **Next**.
5. On the **Select server roles** page, select the **Active Directory Federation Services** check box, and then click **Next**.
6. On the **Select features** page, click **Next**.
7. On the **Active Directory Federation Services (AD FS)** page, click **Next**.
8. On the **Confirm installation selections** page, click **Install**.
9. Wait until installation is complete, and then click **Close**.

Create a service account for AD FS

1. On LON-DC2, on the taskbar, click **Windows PowerShell**.
2. At the command prompt for the Windows PowerShell command-line interface, type **New-ADUser –Name adfsService**, and then press Enter.
3. Type **Set-ADAccountPassword adfsService**, and then press Enter.
4. At the **Password** prompt, press Enter.
5. At the second **Password** prompt, type **Pa$$w0rd**, and then press Enter.
6. At the **Repeat Password** prompt, type **Pa$$w0rd**, and then press Enter.
7. Type **Enable-ADAccount adfsService**, and then press Enter.
8. Close the Windows PowerShell Command Prompt window.

Add a DNS record for AD FS

1. In Server Manager, click **Tools**, and then click **DNS**.
2. In DNS Manager, expand **LON-DC2**, 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 **172.16.0.11**, and then click **Add Host**.
6. In the DNS window, click **OK**, and then click **Done**.
7. Close DNS Manager.

Configure AD FS

1. 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** 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 **Use an existing domain user account or group Managed Service Account**.
7. Click **Select**, in the **Enter the object name to select** box, type **adfsService**, and then click **OK**.
8. In the **Account Password** box, type **Pa$$w0rd** and then click **Next**.
9. On the **Specify Configuration Database** page, click **Create a database on this server using Windows Internal Database**, and then click **Next**.
10. On the **Review Options** page, click **Next**.
11. On the **Pre-requisite Checks** page, click **Configure**.
12. On the **Results** page, click **Close**.

Lesson 3

Implementing AD FS for a Single Organization

Contents:

Demonstration: Configuring Claims Provider and Relying Party Trusts

Demonstration Steps

Configure a Claims Provider Trust

1. On LON-DC2, in Server Manager, click **Tools**, and then click **AD FS Management**.
2. In the AD FS console, expand **Trust Relationships**, and then 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** box, select **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** drop-down list, select **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 WIF application for AD FS

1. On LON-SVR1, in 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** to continue.
4. On the **Security Token Service** page, click **Use an existing STS**, in the **STS WS-Federation metadata document location** box, type **https://adfs.adatum.com/federationmetadata/2007-06/federationmetadata.xml**, and then click **Next** to continue.
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 the federation server will offer, and then click **Next**.
8. On the **Summary** page, review the changes that the Federation Utility Wizard will make to the sample application, 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-DC2, in the AD FS console, click **Relying Party Trusts**.

2. In the Actions pane, click **Add Relying Party Trust**.
3. In the 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 that was configured in the previous section.
6. On the **Specify Display Name** page, in the **Display name** box, type **A. Datum Test App**, and then click **Next**.
7. On the **Configure Multi-factor Authentication Now** page, click **I do not want to configure multi-factor authentication settings for the relying party trust at this time**, and then click **Next**.
8. On the **Choose Issuance Authorization Rules** page, click **Permit all users to access this relying party**, and then click **Next**.
9. On the **Ready to Add Trust** page, review the relying party trust settings, and then click **Next**.
10. On the **Finish** page, click **Close**.
11. Leave the Edit Claim Rules for A. Datum Test App window open for the next demonstration.

Lesson 4

Deploying AD FS in a Business-to-Business Federation Scenario

Contents:

Demonstration: Configuring Claim Rules

Demonstration Steps

1. On LON-DC2, in AD FS Manager, in the Edit Claim Rules for A. Datum Test App window, on the **Issuance Transform Rules** tab, click **Add Rule**.
2. In the **Claim rule template** box, select **Pass Through or Filter an Incoming Claim**, and then click **Next**.
3. In the **Claim rule name** box, type **Send Group Name Rule**.
4. In the **Incoming claim type** drop-down list, click **Group**, and then click **Finish**.
5. In the Edit Claim Rules for A. Datum Test App window, on the **Issuance Authorization Rules** tab, click the rule named **Permit Access to All Users**, click **Remove Rule**, and then click **Yes** to confirm.

Note: With no rules, users are not permitted access.

6. On the **Issuance Authorization Rules** tab, click **Add Rule**.
7. On the **Select Rule Template** page, in the **Claim rule template** box, select **Permit or Deny Users Based on an Incoming Claim**, and then click **Next**.
8. On the **Configure Rule** page, in the **Claim rule name** box, type **Permit Production Group Rule**.
9. In the **Incoming claim type** drop-down list, select **Group**.
10. In the **Incoming claim value** box, type **Production**, click **Permit access to users with this incoming claim**, and then click **Finish**.
11. On the **Issuance Authorization Rules** tab, click **Add Rule**.
12. On the **Select Rule Template** page, in the **Claim rule template** box, select **Permit or Deny Users Based on an Incoming Claim**, and then click **Next**.
13. On the **Configure Rule** page, in the **Claim rule name** box, type **Allow A. Datum Users**.
14. In the **Incoming claim type** drop-down list, select **UPN**.
15. In the **Incoming claim value** box, type **@adatum.com**, click **Permit access to users with this incoming claim**, and then click **Finish**.
16. Click the **Allow A. Datum Users** rule, and then click **Edit Rule**.
17. In the **Edit Rule – Allow A. Datum Users** dialog box, click **View Rule Language**.

Note: Note that students will be editing the rule language in the lab.

18. Click **OK**, and then click **Cancel**.
19. In the Edit Claim Rules for A. Datum Test App window, click **OK**.

Lesson 5

Extending AD FS to External Clients

Contents:

Demonstration: Installing and Configuring Web Application Proxy

Demonstration Steps

Install Web Application Proxy

1. On LON-SVR2, in 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-DC2

1. On LON-DC2, on Start screen, type **mmc**, and then press Enter.
2. In the 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 the 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 the Microsoft Management Console, and then do not save the changes.

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

1. On LON-SVR2, on Start screen, type **mmc**, and then press Enter.
2. In the 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 the 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-DC2\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** 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 the Microsoft Management Console, and then do not save the changes.

Configure Web Application Proxy

1. In Server Manager, click the **Notifications** icon, and then click **Open the Web Application Proxy Wizard**.
2. In the Web Application Proxy Wizard, on the **Welcome** page, click **Next**.
3. On the **Federation Server** page, enter the following, 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** 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

Question: Your organization is planning to implement AD FS. In the short term, only internal clients will be using AD FS to access internal applications. However, in the long run, you will be providing access to web-based applications that are secured by AD FS to users at home. How many certificates should you obtain from a third-party CA?

Answer: The only AD FS certificate that needs to be trusted is the service communication certificate. The token signing and token decrypting certificates can remain self-signed. Therefore, only a single certificate from a third-party is required.

Question: Your organization has an application that allows customers to view their orders and invoices. Presently, all customers have a user name and password that is managed within the application. To simplify access to the application and reduce support calls, your organization has rewritten the application to support AD FS for authentication. What do you need to configure to support the application?

Question: Your organization has an application that allows customers to view their orders and invoices. Presently, all customers have a user name and password that is managed within the application. To simplify access to the application and reduce support calls, your organization has rewritten the application to support AD FS for authentication. A Web Application Proxy will support application access over the Internet. Internally, your AD FS server uses the host name adfs.contoso.com and resolves to 10.10.0.99. How will you allow external partners to resolve adfs.contso.com to the external IP address of Web Application Proxy?

Answer: Use split DNS to allow the proper resolution of adfs.contoso.com to the correct IP address internally and externally. The internal DNS server resolves adfs.contoso.com to the internal IP address of the AD FS server. The external DNS server resolves adfs.contoso.com to the external IP address of the Web Application Proxy.

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

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

Answer: Yes. The Windows Internal Database supports up to five AD FS servers. The first AD FS server is the primary server where all configuration changes take place. Changes in the primary server replicate to the other AD FS servers.

Lab Review Questions and Answers

Lab: Implementing AD FS

Question and Answers

Question: Why was 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 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: You can access https://*hostname*/federationmetadata/2007-06/federationmetadata.xml on the AD FS server.

Module 11

Implementing Secure Shared File Access

Contents:

Lesson 2

Implementing DAC Components

Contents:

Demonstration: Configuring Claims, Resource Properties, and Rules

Demonstration Steps

1. On LON-DC1, in Server Manager, click **Tools**, and then click **Active Directory Administrative Center**.
2. In the Active Directory Administrative Center, in the navigation pane, click **Dynamic Access Control**, and then double-click **Claim Types**.
3. In the Claim Types container, in the **Tasks** pane, click **New**, and then click **Claim Type**.
4. In the Create Claim Type window, in the Source Attribute section, select **department**.
5. In the **Display name** text box, type **Company Department**.
6. Select the **User** and **Computer** check boxes, and then click **OK**.
7. In the Active Directory Administrative Center, in the Tasks pane, click **New**, and then select **Claim Type**.
8. In the Create Claim Type window, in the Source Attribute section, click **description**.
9. Clear the **User** check box, select the **Computer** check box, and then click **OK**.
10. In the Active Directory Administrative Center, click **Dynamic Access Control**.
11. In the central pane, double-click **Resource Properties**.
12. In the **Resource Properties** list, right-click **Department**, and then click **Enable**.
13. In the **Resource Properties** list, right-click **Confidentiality**, and then click **Enable**.
14. Double-click **Department**, scroll down to the Suggested Values section, and then click **Add**.
15. In the Add a suggested value window, in both the **Value** and **Display name** text boxes, type **Research**, and then click **OK** twice.
16. Click **Dynamic Access Control**, and then double-click **Resource Property Lists**.
17. In the central pane, double-click **Global Resource Property List**, ensure that both Department and Confidentiality display, and then click **Cancel**. If they do not display, click **Add**, add these two properties, and then click **OK**.
18. In the Active Directory Administrative Center, in the navigation pane, click **Dynamic Access Control**, and then double-click **Central Access Rules**.
19. In the Tasks pane, click **New**, and then click **Central Access Rule**.
20. In the **Create Central Access Rule** dialog box, in the **Name** field, type **Department Match**.
21. In the Target Resources section, click **Edit**.
22. In the **Central Access Rule** dialog box, click **Add a condition**.
23. Set a condition as follows: **Resource-Department-Equals-Value-Research**, and then click **OK**.
24. In the **Permissions** section, click **Use following permissions as current permissions**.
25. In the **Permissions** section, click **Edit**.
26. Remove permission for **Administrators**.
27. In **Advanced Security Settings for Permissions**, click **Add**.
28. In **Permission Entry for Permissions**, click **Select a principal**.

29. In the Select User, Computer, Service Account, or Group window, type **Authenticated Users**, click **Check Names**, and then click **OK**.
30. In the **Basic permissions** section, select the **Modify**, **Read and Execute**, **Read** and **Write** check boxes, and then click **Add a condition**.
31. Click the **Group** drop-down list box, and then click **Company Department**.
32. Click the **Value** drop-down list box, and then click **Resource**.
33. In the last drop-down list box, click **Department**, and then click **OK** three times.

Note: You should have this expression as a result: **User-Company Department-Equals-Resource-Department**.

34. In the Tasks pane, click **New**, and then click **Central Access Rule**.
35. For the name of rule, type **Access Confidential Docs**.
36. In the Target Resources section, click **Edit**.
37. In the Central Access Rule window, click **Add a condition**.
38. In the last drop-down list box, click **High**, and then click **OK**.

Note: You should have this expression as a result: **Resource-Confidentiality-Equals-Value-High**.

39. In the **Permissions** section, click Use following permissions as current permissions.
40. In the Permissions section, click **Edit**.
41. Remove permission for **Administrators**.
42. In Advanced Security Settings for Permissions, click **Add**.
43. In the Permission Entry for Permissions, click **Select a principal**.
44. In the Select User, Computer, Service Account, or Group window, type **Authenticated Users**, click **Check Names**, and then click **OK**.
45. In the Basic permissions section, select the **Modify**, **Read and Execute**, **Read**, and **Write** check boxes, and then click **Add a condition**.
46. Set the first condition to: **User-Group-Member of each-Value-Managers**, and then click **Add a condition**.

Note: If you cannot find Managers in the last drop-down list box, click **Add items**. Then in the Select user, Computer, Service Account, or Group window, type **Managers**, click **Check Names**. In the Multiple Names Found window, click **Managers** and then click **OK** twice.

47. Set the second condition to: **Device-Group-Member of each-Value-ManagersWKS,** and then click **OK** three times.

Demonstration: Configuring Classification Rules

Demonstration Steps

1. On LON-SVR1, in Server Manager, click **Tools**, and then click **File Server Resource Manager**.
2. In File Server Resource Manager, expand **Classification Management**.

3. Select and then right-click **Classification Properties**, and then click **Refresh**.
4. Verify that the **Confidentiality** and **Department** properties are listed.
5. Click **Classification Rules**.
6. In the Actions pane, click **Create Classification Rule**.
7. In the Create Classification Rule window, for the **Rule name**, type **Set Confidentiality**.
8. Click the **Scope** tab, and then click **Add**.
9. In the **Browse For Folder** dialog box, expand **Local Disk (C:)**, click the **Docs** folder, and then click **OK**.
10. Click the **Classification** tab, make sure that following settings are set, and then click **Configure**:
    - Classification method: **Content Classifier**
    - Property: **Confidentiality**
    - Value: **High**
11. In the **Classification Parameters** dialog box, click the **Regular expression** drop-down list box, and then click **String**.
12. In the **Expression** field, which is next to the word String, type **secret**, and then click **OK**.
13. Click the **Evaluation Type** tab, select **Re-evaluate existing property values**, click **Overwrite the existing value**, and then click **OK**.
14. In File Server Resource Manager, in the Actions pane, click **Run Classification With All Rules Now**.
15. Click **Wait for classification to complete**, and then click **OK**.
16. After the classification is complete, you will be presented with a report. Verify that two files were classified. You can confirm this in Report Totals section.
17. Close the report.
18. On the taskbar, click the **File Explorer** icon.
19. In the File Explorer window, expand **Local Disk (C:)**, and then click the **Docs** folder.
20. In the Docs folder, right-click **Doc1.txt**, click **Properties**, and then click the **Classification** tab. Verify that **Confidentiality** is set to **High**.
21. Repeat step 20 on files **Doc2.txt** and **Doc3.txt**. Doc2.txt should have the same **Confidentiality** as Doc1.txt, while Doc3.txt should have no value. This is because only Doc1.txt and Doc2.txt have the word “secret” in their content.

Lesson 3

Implementing DAC for Access Control

Contents:

Demonstration: Creating and Deploying Central Access Policies

Demonstration Steps

1. On LON-DC1, in the Active Directory Administrative Center, click **Dynamic Access Control**, and then double-click **Central Access Policies**.
2. In the Tasks pane, click **New**, and then click **Central Access Policy**.
3. In the **Name** field, type **Protect confidential docs**, and then click **Add**.
4. Click the **Access Confidential Docs** rule, click **>>**, and then click **OK** twice.
5. In the Tasks pane, click **New**, and then click **Central Access Policy**.
6. In the **Name** field, type **Department Match**, and then click **Add**.
7. Click the **Department Match** rule, click **>>**, and then click **OK** twice.
8. Close the Active Directory Administrative Center.
9. On LON-DC1, in Server Manager, click **Tools**, and then click **Group Policy Management**.
10. In the Group Policy Management Console, under Domains, expand **Adatum.com**, right-click **DAC Protected**, and then click **Create a GPO in this domain, and Link it here**.
11. Type **DAC Policy**, and then click **OK**.
12. Right-click **DAC Policy**, and then click **Edit**.
13. Expand **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, expand **File System**, right-click **Central Access Policy**, and then click **Manage Central Access Policies**.
14. Press and hold the Ctrl key, click both **Department Match** and **Protect confidential docs**, click **Add**, and then click **OK**.
15. Close the Group Policy Management Editor window and the Group Policy Management Console.
16. On LON-SVR1, on the taskbar, click the **Windows PowerShell** icon.
17. At the command prompt in the Windows PowerShell command-line interface, type **gpupdate /force**, and then press Enter.
18. Close Windows PowerShell.
19. On the taskbar, click the **File Explorer** icon.
20. In File Explorer, browse to **Local Disk (C:)**, right-click the **Docs** folder, and then click **Properties**.
21. In the **Properties** dialog box, click the **Security** tab, and then click **Advanced**.
22. In the **Advanced Security Settings for Docs** window, click the **Central Policy** tab, and then click **Change**.
23. In the drop-down list box, select **Protect confidential docs**, and then click **OK** twice.
24. Right-click the **Research** folder, and then click **Properties**.
25. In the **Properties** dialog box, click the **Security** tab, and then click **Advanced**.
26. In the **Advanced Security Settings for Research** window, click the **Central Policy** tab, and then click **Change**.
27. In the drop-down list box, click **Department Match**, and then click **OK** twice.

Demonstration: Evaluating and Managing DAC

Demonstration Steps

1. On LON-DC1, open Server Manager, click **Tools**, and then click **Group Policy Management**.
2. In the Group Policy Management Console, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, and then click **Group Policy Objects**.
3. Right-click **DAC Policy**, and then click **Edit**.
4. In the Group Policy Management Editor, expand **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, expand **Advanced Audit Policy Configuration**, expand **Audit Policies**, and then click **Object Access**.
5. Double-click **Audit Central Access Policy Staging**, select all three check boxes, and then click **OK**.
6. Double-click **Audit File System**, select all three check boxes, and then click **OK**.
7. Close the Group Policy Management Editor window and the Group Policy Management Console.
8. On LON-DC1, open Server Manager, click **Tools**, and then click **Active Directory Administrative Center**.
9. In the navigation pane, click **Dynamic Access Control**.
10. Double-click **Central Access Rules**, right-click **Department Match**, and then click **Properties**.
11. Scroll down to the **Proposed Permissions** section, click **Enable permission staging configuration**, and then click **Edit**.
12. Click **Authenticated Users**, and then click **Edit**.
13. Change the condition to **User-Company Department-Equals-Value-Marketing**, and then click **OK**.
14. Click **OK** twice to close all windows.
15. Switch to LON-SVR1.
16. On the taskbar, click the **Windows PowerShell** icon.
17. At the Windows PowerShell command prompt, type **gpupdate /force**, and then press Enter.
18. Close Windows PowerShell.

Lesson 4

Implementing Access Denied Assistance

Contents:

Demonstration: Implementing Access Denied Assistance

Demonstration Steps

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**, expand **Domains**, expand **Adatum.com**, and then click **Group Policy Objects**.
3. Right-click **DAC Policy**, and then click **Edit**.
4. Under Computer Configuration, expand **Policies**, expand **Administrative Templates**, expand **System**, and then click **Access-Denied Assistance**.
5. In the details pane, double-click **Customize Message for Access Denied errors**.
6. In the Customize Message for Access Denied errors window, click **Enabled**.
7. In the **Display the following message to users who are denied access** text box, type **You are denied access because of permission policy**. **Please request access**.
8. Select the **Enable users to request assistance** check box. Review the other options, but do not make any changes, and then click **OK**.
9. In the details pane of the Group Policy Management Editor, double-click **Enable access-denied assistance on client for all file types**, click **Enabled**, and then click **OK**.
10. Close the Group Policy Management Editor and the Group Policy Management Console.
11. Switch to LON-SVR1, and on the taskbar, click the **Windows PowerShell** icon.
12. At the Windows PowerShell command prompt, type **gpupdate /force**, and then press Enter.

Lesson 5

Implementing and Managing Work Folders

Contents:

Demonstration: Implementing Work Folders

Demonstration Steps

1. On LON-SVR2, in **Server Manager**, click **File and Storage Services,** and then click **Work Folders**.
2. In the **WORK FOLDERS** tile, click **Tasks,** and then click **New Sync Share…**.
3. In the New Sync Share Wizard, on the **Before you begin** page, click **Next**.
4. On the **Select the server and path** page, click **Select by file share**, ensure that **WF-Share** is highlighted, and then click **Next**.
5. On the **Specify the structure for user folders**, accept the default selection (User alias), and then click **Next**.
6. On the **Enter the sync share name** page, accept the default, and then click **Next**.
7. On the **Grant sync access to groups** page, note the default selection to disable inherited permissions and grant users exclusive access, and then click **Add**.
8. In the **Select User or Group** dialog box, in the **Enter the object names to select**, type **WFsync**, click **Check Names**, and then click **OK**.
9. On the **Grant sync access to groups** page, click **Next**.
10. On the **Specify device policies page**, note the selections, accept the default selection, and then click **Next**.
11. On the **Confirm selections** page, click **Create**.
12. On the **View results** page, click **Close**.
13. Switch to LON-DC1, and then sign in as **Adatum\Administrator** with password **Pa$$w0rd**.
14. Open **Server Manager**, click **Tools,** and then click **Group Policy Management**.
15. Expand **Forest: Adatum.com, expand Domains, expand Adatum.com,** click **Group Policy Objects,** right-click the **Group Policy Objects** container, and then click **New**.
16. In the **New GPO** window, type **Work Folders GPO** in the **Name** field, and then click **OK**.
17. Right-click **Work Folders GPO**, and then click **Edit**.
18. In the **Group Policy Management Editor**, expand **User Configuration,** expand **Policies,** expand **Administrative Templates,** expand **Windows Components**, and then click **Work Folders**.
19. Double-click **Specify Work Folders settings** in the details pane.
20. In the **Specify Work Folders settings** dialog box, click **Enabled**.
21. In the **Work Folders URL** text box, type **https://lon-svr2.adatum.com**, and then select **Force automatic setup**.
22. Click **OK** to close the **Specify Work Folders** settings dialog box, and then close the **Group Policy Management Editor window**.
23. In the **Group Policy Management** Console, right-click the **Adatum.com** domain object, and then select **Link an Existing GPO…**.
24. In the **Select GPO** window, select **Work Folders GPO,** and then click **OK**.

Module Review and Takeaways

Best Practices

- Use central access policies instead of configuring conditional expressions on resources.
- Enable access-denied assistance settings.
- Always test changes that you have made to Central Access Rules and central access policies before implementing them.
- Use file classifications to assign properties to files.
- Use Work Folders to synchronize business data across devices.
- Use Workplace Join in Bring Your Own Device (BYOD) scenarios.

Review Question(s)

Question: What is a claim?

Answer: A claim is information that AD DS states about an object, which usually is a user or a computer.

Question: What is the purpose of Central Access Policy?

Answer: Central access policies enable administrators to create policies that apply to one or more file servers in an organization. Central access policies contain one or more Central Access Policy rules. Each rule contains settings that determine applicability and permissions.

Question: What is the BYOD concept?

Answer: BYOD is the policy of permitting employees to bring personal devices such as laptops, tablets, and smart phones to the workplace, and allowing employees to use those devices to access privileged company information and apps.

Tools

Tool	Use	Location
Active Directory Administrative Center	Administering and creating claims, Resource Properties, rules, and policies	Administrative tools
Group Policy Management Console (GPMC)	Managing Group Policy	Administrative tools
Group Policy Management Editor	Editing GPOs	GPMC

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Claims are not populated with the appropriate values. A conditional expression does not allow access.	Verify that the correct attribute is selected for the claim. In addition, check that the attribute value for a specific object is populated. Verify that the expression is well defined. In addition, try using the **Effective Access** tab to troubleshoot the problem.

Lab Review Questions and Answers

Lab: Implementing Secure File Access

Question and Answers

Question: How do file classifications enhance the use of DAC?

Answer: By using file classifications, you can set attributes on files automatically and then use these attributes in conditional expressions when implementing DAC.

Question: Can you implement DAC without Central Access Policy?

Answer: Yes. You can set conditional expressions directly on resources.

Module 12

Monitoring, Managing, and Recovering AD DS

Contents:

Lesson 1

Monitoring AD DS

Contents:

Demonstration: How to Monitor Performance

Demonstration Steps

Create a data collector set

1. Switch to the LON-SVR1 computer.
2. Sign in as **Adatum\Administrator** with password **Pa$$w0rd**.
3. Pause your mouse in the lower left of the taskbar, and then click **Start**.
4. In Start, type **Perf**, and then in the **Apps** list, click **Performance Monitor**.
5. In Performance Monitor, in the navigation pane, expand **Data Collector Sets**, and then click **User Defined**.
6. Right-click **User Defined**, point to **New**, and then click **Data Collector Set**.
7. In the Create New Data Collector Set Wizard, in the **Name** box, type **LON-SVR1 Performance**.
8. Click **Create manually (Advanced)**, and then click **Next**.
9. On the **What type of data do you want to include?** page, select the **Performance counter** check box, and then click **Next**.
10. On the **Which performance counters would you like to log?** page, click **Add**.
11. In the **Available counters** list, expand **Processor**, click **% Processor Time**, and then click **Add >>**.
12. In the **Available counters** list, expand **Memory**, click **Pages/sec**, and then click **Add >>**.
13. In the **Available counters** list, expand **PhysicalDisk**, click **% Disk Time**, and then click **Add >>**.
14. Click **Avg. Disk Queue Length**, and then click **Add >>**.
15. In the **Available counters** list, expand **System**, click **Processor Queue Length**, and then click **Add >>**.
16. In the **Available counters** list, expand **Network Interface**, click **Bytes Total/sec**, click **Add >>**, and then click **OK**.
17. On the **Which performance counters would you like to log?** page, in the **Sample interval** box, type **1**, and then click **Next**.
18. On the **Where would you like the data to be saved?** page, click **Next**.
19. On the **Create the data collector set?** page, click **Save and close**, and then click **Finish**.
20. In Performance Monitor, in the results pane, right-click **LON-SVR1 Performance**, and then click **Start**.

Create a disk load on the server

1. Click **Start**, type **Cmd**, and in the **Apps** list, click **Command Prompt**.
2. At the command prompt, type the following command, and then press Enter:

```
Fsutil file createnew bigfile 104857600
```

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

```
Copy bigfile \\LON-dc1\c$
```

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

```
Copy \\LON-dc1\c$\bigfile bigfile2
```

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

```
Del bigfile*.*
```

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

```
Del \\LON-dc1\c$\bigfile*.*
```

7. Close the Command Prompt window.

Analyze the resulting data in a report

1. Switch to Performance Monitor.
2. In the navigation pane, right-click **LON-SVR1 Performance**, and then click **Stop**.
3. In Performance Monitor, in the navigation pane, click **Performance Monitor**.
4. On the toolbar, click **View log data**.
5. In the **Performance Monitor Properties** dialog box, on the **Source** tab, click **Log files**, and then click **Add**.
6. In the **Select Log File** dialog box, double-click **Admin**.
7. Double-click **LON-SVR1 Performance**, double-click the **SVR1_date-000001** folder, and then double-click **DataCollector01.blg**.
8. Click the **Data** tab, and then click **Add**.
9. In the **Add Counters** dialog box, in the **Available counters** list, expand **Memory**, click **Pages/sec**, and then click **Add >>**.
10. Expand **Network Interface**, click **Bytes Total/sec**, and then click **Add >>**.
11. Expand **PhysicalDisk**, click **% Disk Time**, and then click **Add >>**.
12. Click **Avg. Disk Queue Length**, and then click **Add >>**.
13. Expand **Processor**, click **% Processor Time**, and then click **Add >>**.
14. Expand **System**, click **Processor Queue Length**, click **Add >>**, and then click **OK**.
15. In the **Performance Monitor Properties** dialog box, click **OK**.
16. On the toolbar, click the Down Arrow, and then click **Report**.

Lesson 2

Managing the AD DS Database

Contents:

Demonstration: Performing Database Management

Demonstration Steps

Stop AD DS

1. If necessary, on LON-DC1, on the taskbar, click the **Server Manager** shortcut.
2. In Server Manager, click **Tools**, and then click **Services**.
3. In the Services window, 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 AD DS database

1. On LON-DC1, on the taskbar, click the **Windows PowerShell** shortcut.
2. At the command prompt, type **NtdsUtil.exe**, and then press Enter.
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 maintenace:** prompt, type the following command, and then press Enter:

```
compact to C:\
```

Check the integrity of the offline AD DS database

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

```
Integrity
```

2. At the **file maintenace:** 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 command-line interface window.

Start AD DS

1. On the taskbar, click the **Server Manager** shortcut.
2. In Server Manager, click **Tools**, and then click **Services**.
3. In the Services window, 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

AD DS 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**, click **OK** in the warning message box, and then click **OK** to the refresh Active Directory Administrative Center message.
9. Press F5 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. Enter the following information under Account, 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. Select both **Test1** and **Test2**, right-click the selection, and then click **Delete**.
6. Click **Yes** at the confirmation prompt.

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

Review Question(s)

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 A: Monitoring AD DS

Question and Answers

Question: When analyzing the performance of a domain controller, aside from the AD DS–specific counters in Performance Monitor, what other factors can influence domain controller performance?

Answer: Many factors can influence the performance of a domain controller, but the server functioning as a domain controller must be specified correctly in terms of the four key server resources: processor, memory, disk, and network.

Lab B: 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. So 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.

Module 13

Implementing Windows Azure Active Directory

Contents:

Module Review and Takeaways

Review Question(s)

Question: Your organization has been doing some initial testing of Office 365 by using cloud-based users. Now that initial testing is complete, you need to ensure that accounts in Office 365 synchronize properly with the on premises instance of AD DS. How can you do this?

Answer: During initial synchronization, Directory Sync attempts a fuzzy match with existing accounts by using the primary Simple Mail Transfer Protocol (SMTP) address. To ensure that AD DS accounts correctly match with existing accounts in Windows Azure AD, you need to verify that the primary SMTP address is the same for both accounts.

Question: Your organization has created a new cloud-based application that uses Windows Azure AD as the identity store. All users are cloud-based and do not synchronize with any other source. Can you implement multifactor authentication for this application?

Answer: Yes. Windows Azure Active Authentication supports multifactor authentication that this application can use. This type of multifactor authentication is available only for cloud-based users. When implemented, users must enter a code that is provided by a smartphone application, text message, or phone call as the second factor.

Question: Your organization has implemented Exchange Server with an account forest and a resource forest. You want to implement hybrid mode with Office 365. Hybrid mode requires that user accounts from AD DS synchronize to Windows Azure AD. Do you need to use FIM, or can Directory Sync be used?

Answer: You can install Directory Sync in the resource forest when implementing Office 365 in hybrid mode. If SSO is required, the AD FS implementation is placed in the account forest.

Module 14

Implementing and Administering AD LDS

Contents:

Lesson 1

Overview of AD LDS

Contents:

Question and Answers

AD LDS or AD DS?

Question: A development team is creating a phone book app that will allow employees to find other employees by using a website. The site will include employee contact and group membership information. Should the development team use AD LDS or AD DS?

Answer: AD DS. It is likely that AD DS already exists and contains the contact and group membership information. The app will pull data from AD DS and will not need AD LDS in this situation.

Question: A development team is creating an ordering app for your company's partners. The partners will connect to the app, sign in, and then place orders. Should the development team use AD LDS or AD DS?

Answer: AD LDS would be a lighter, easier choice. AD DS could still work but would require additional overhead and management costs. Because the team only requires an authentication repository and not domain services or Group Policy, AD LDS is the best choice in this situation.

Question: The Information Technology (IT) team is deploying Microsoft Exchange Server 2013. Part of the deployment includes a server with the Edge Transport server role in the perimeter network. Should the IT team use AD LDS or AD DS?

Answer: AD LDS. Some apps require AD LDS or AD DS. In the case of Exchange Server 2013, the Edge Transport server role requires AD LDS. It is important to understand and be familiar with apps that require or bundle AD LDS as part of an installation.

Question: A company with AD DS is splitting into two separate companies. The first company will maintain AD DS. The second company is building a new IT infrastructure. It requires the ability to manage client computers by enforcing policies, and it plans to implement Active Directory Certificate Services (AD CS) for smart card logon. Should the company use AD LDS or AD DS?

Answer: AD DS. In this case, the company wants to use Group Policy and AD CS—two pieces that are available in AD DS only. When evaluating the business requirements of an organization, many times a requirement will indicate the use AD LDS or AD DS.

Lesson 2

Deploying AD LDS

Contents:

Demonstration: Installing the AD LDS Server Role

Demonstration Steps

1. Sign in to LON-DC1 as **Adatum\Administrator** with password **Pa$$w0rd**.
2. In Server Manager, click **Add roles and features**.
3. In the Add Roles and Features Wizard, on the **Before You Begin** page, click **Next**.
4. On the **Select installation type** page, click **Next**.
5. On the **Select destination server** page, click **Next**.
6. On the **Select server roles** page, in the **Roles** list, select the **Active Directory Lightweight Directory Services** check box.
7. In the **Add Roles and Features Wizard** dialog box, click **Add Features**, and then click **Next**.
8. On the **Select features** page, click **Next**.
9. On the **Active Directory Lightweight Directory Services (AD LDS)** page, click **Next**.
10. On the **Confirm installation selections** page, click **Install**.
11. On the **Installation progress** page, click **Close**.
12. Sign in to LON-SVR1 as **Adatum\Administrator** with password **Pa$$w0rd**.
13. In Server Manager, click **Add roles and features**.
14. In the Add Roles and Features Wizard, on the **Before You Begin** page, click **Next**.
15. On the **Select installation type** page, click **Next**.
16. On the **Select destination server** page, click **Next**.
17. On the **Select server roles** page, in the **Roles** list, select the **Active Directory Lightweight Directory Services** check box.
18. In the **Add Roles and Features Wizard** dialog box, click **Add Features**, and then click **Next**.
19. On the **Select features** page, click **Next**.
20. On the **Active Directory Lightweight Directory Services (AD LDS)** page, click **Next**.
21. On the **Confirm installation selections** page, click **Install**.
22. On the **Installation progress** page, click **Close**.

Lesson 3

Configuring AD LDS Instances and Partitions

Contents:

Demonstration: Creating AD LDS Instances

Demonstration Steps

1. On LON-DC1, in Server Manager, click **Tools**, and then click **Active Directory Lightweight Directory Services Setup Wizard**.
2. On the **Welcome to the Active Directory Lightweight Directory Services Setup Wizard** page, click **Next**.
3. On the **Setup Options** page, ensure that **A unique instance** is selected, and then click **Next**.
4. On the **Instance Name** page, click **Next**.
5. On the **Ports** page, click **Next**.
6. On the **Application Directory Partition** page, click **Yes, create an application directory partition**, and in the **Partition name** box, type **CN=Application1,DC=Adatum,DC=com**, and then click **Next**.
7. On the **File Locations** page, click **Next**.
8. On the **Service Account Selection** page, click **This account**, type **Administrator** in the **User name** box and **Pa$$w0rd** in the **Password** box, and then click **Next**.
9. In the **Active Directory Lightweight Directory Services Setup Wizard** message box, click **Yes**.
10. On the **AD LDS Administrators** page, ensure that **Currently logged on user: ADATUM\Administrator** is selected, and then click **Next**.
11. On the **Importing LDIF Files** page, in the **LDIF file name** list, select all check boxes, and then click **Next**.
12. On the **Ready to Install** page, click **Next**.
13. On the **Completing the Active Directory Lightweight Directory Services Setup Wizard** page, click **Finish**.

Demonstration: Creating a User in AD LDS

Demonstration Steps

1. On LON-DC1, in Server Manager, click **Tools**, and then click **ADSI Edit**.
2. In ADSI Edit, click **Action**, and then click **Connect to**.
3. In the **Connection Settings** dialog box, in the **Name** box, type **AD LDS Application1**.
4. In the **Connection Point** area, click **Select or type a Distinguished Name or Naming Context**, and then in the **Select or type a Distinguished Name or Naming Context** box, type **CN=Application1,DC=Adatum,DC=com**.
5. In the **Computer** area, click **Select or type a domain or server: (Server | Domain [:port])**, and in the **Select or type a domain or server: (Server | Domain [:port])** box, type **LON-DC1:50000**, and then click **OK**.
6. In the Active Directory Services Interfaces Editor (ADSI Edit), in the console tree, click and expand **AD LDS Application1 [LON-DC1:50000]**, and then click **CN=Application1,DC=Adatum,DC=com**.
7. In the **CN=Application1,DC=Adatum,DC=com** details pane, in the **Name** list, right-click **CN=Roles**, point to **New**, and then click **Object**.
8. In the **Create Object** dialog box, in the **Select a class** box, click **user**, and then click **Next**.
9. In the **Value** box, type **user1**, click **Next**, and then click **Finish**.

Lesson 4

Configuring AD LDS Replication

Contents:

Demonstration: Configuring AD LDS Replication

Demonstration Steps

Create an AD LDS replica

1. On LON-SVR1, in Server Manager, click **Tools**, and then click **Active Directory Lightweight Directory Services Setup Wizard**.
2. On the **Welcome to the Active Directory Lightweight Directory Services Setup Wizard** page, click **Next**.
3. On the **Setup Options** page, click **A replica of an existing instance**, and then click **Next**.
4. On the **Instance Name** page, click **Next**.
5. On the **Ports** page, in the **LDAP port number** box, type **50000**, and in the **SSL port number** box, type **50001**, and then click **Next**.
6. On the **Joining a Configuration Set** page, in the **Server** box, type **LON-DC1.Adatum.com**, and in the **LDAP port** field, type **50000**, and then click **Next**.
7. On the **Administrative Credentials for the Configuration Set** page, ensure that the **Currently logged on user: ADATUM\Administrator** option is selected, and then click **Next**.
8. On the **Copying Application Directory Partitions** page, in the **Partition DN** box, select the **CN=Application1,DC=Adatum,DC=com** check box, and then click **Next**.
9. On the **File Locations** page, click **Next**.
10. On the **Service Account Selection** page, ensure that **Network service account** is selected, and then click **Next**.
11. On the **AD LDS Administrators** page, ensure that **Currently logged on user: ADATUM\Administrator** is selected, and then click **Next**.
12. On the **Ready to Install** page, click **Next**.
13. On the **Completing the Active Directory Lightweight Directory Services Setup Wizard** page, click **Finish**.

Verify AD LDS replication

1. On LON-DC1, in Server Manager, click **Tools**, and then click **Active Directory Sites and Services**.
2. In the tree pane, right-click **Active Directory Sites and Services [LON-DC1.Adatum.com]**, and then click **Change Domain Controller**.
3. In the **Change Directory Server** dialog box, in the **Name** list, click **<Type a Directory Server name[:port]here>**, type **LON-DC1:50000**, press Enter, and then click **OK**.

Note: It can take a few moments for the next dialog box to appear.

4. In the **Active Directory Domain Services** message box, click **Yes**.
5. In the Active Directory Sites and Services console, in the tree pane, expand **Sites**, expand **Default-First-Site-Name**, and then expand **Servers**.
6. Under Servers, expand **LON-DC1$instance1**, right-click **NTDS Settings**, point to **All Tasks**, and then click **Check Replication Topology**.
7. In the **Check Replication Topology** message box, click **OK**.

8. Under Servers, expand **LON-SVR1$instance1**, right-click **NTDS Settings**, point to **All Tasks**, and then click **Check Replication Topology**.
9. In the **Check Replication Topology** message box, click **OK**.
10. Under **LON-DC1$instance1**, click **NTDS Settings**, right-click **NTDS Settings**, and then click **Refresh**.
11. In the tree pane, expand **LON-SVR1$instance1**, click **NTDS Settings**, right-click **NTDS Settings**, and then click **Refresh**.
12. On LON-SVR1, in Server Manager, click **Tools**, and then click **Active Directory Sites and Services**.
13. In the tree pane, right-click Active Directory Sites and Services [LON-DC1.Adatum.com], and then click Change Domain Controller.
14. In the Change Directory Server dialog box, click <Type a Directory Server name[:port]here>, type LON-SVR1:50000, press Enter, and then click OK.

Note: It can take a few moments for the next dialog box to appear.

15. In the Active Directory Domain Services message box, click Yes.
16. In the tree pane, expand **Sites**, expand **Default-First-Site-Name**, expand **Servers**, expand **LON-SVR1$instance1**, and then click **NTDS Settings**.
17. In the NTDS Settings details pane, in the **Name** list, right-click **<automatically generated>**, and then click **Replicate Now**.
18. In the **Replicate Now** message box, click **OK**.
19. In Server Manager, click **Tools**, and then click **ADSI Edit**.
20. In ADSI Edit, click **Action**, and then click **Connect to**.
21. In the Connection Settings dialog box, in the Name box, type AD LDS Application1.
22. In the Connection Point area, click Select or type a Distinguished Name or Naming Context, and then in the Select or type a Distinguished Name or Naming Context box, type CN=Application1,DC=Adatum,DC=com.
23. In the Computer area, click Select or type a domain or server: (Server | Domain[:port]), type LON-SVR1:50000, and then click OK.
24. In ADSI Edit, in the console tree, click and expand **AD LDS Application1 [LON-SVR1:50000]**, click and expand **CN=Application1,DC=Adatum,DC=com**, and then double-click **CN=Roles**.
25. Verify the presence of CN=user1 in the **Name** list.
26. On the **File** menu of ADSI Edit, click **Exit**.

Module Review and Takeaways

Question: Fabrikam, Inc. has development teams working at two locations, and the teams are working on the same directory-aware app. Currently, one location deploys AD LDS. Because of bandwidth constraints, the development team at the other location has reported poor performance when working with the app. What can you do to improve performance?

Answer: Create a replica in the other site.

Question: The IT team at Contoso, Ltd. deployed AD LDS for their development team. To keep things simple, at that time, the team deployed AD LDS on an existing domain controller. The development team has asked for administrative access to perform tasks such as installing Secure Sockets Layer certificates, stopping and starting services, and managing the AD LDS database. How should you proceed?

Answer: Move AD LDS to a member server, and then delegate management.

Lab Review Questions and Answers

Lab: Implementing and Administering AD LDS

Question and Answers

Question: In the lab, when you deployed AD LDS to LON-SVR1, what was the default port number? Why was this different from LON-DC1?

Answer: The port was 389. On LON-DC1 the default was 50000. This is because LON-DC1 is a domain controller and is running AD DS on port 389 already.

Question: What are the options for high availability for AD LDS?

Answer: Load balancing is one option, and adding additional replicas is another option.

Question: Do the instances that are part of the same configuration set run on the same computer or on separate computers?

Answer: Instances that are part of the same configuration set can run on the same computer or on separate computers.