OFFICIAL MICROSOFT LEARNING PRODUCT

20410D

Installing and Configuring Windows Server® 2012

Companion Content

Product Number: 20410D

Released: 04/2014

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

Deploying and Managing Windows Server 2012

Contents:

Lesson 1: Windows Server 2012 Overview 2

Lesson 2: Installing Windows Server 2012 4

Lesson 3: Post-Installation Configuration of Windows Server 2012 6

Lesson 4: Overview of Windows Server 2012 Management 8

Lesson 5: Introduction to Windows PowerShell 12

Module Review and Takeaways 15

Lab Review Questions and Answers 17

Lesson 1
Windows Server 2012 Overview

Contents:

Question and Answers 3
Resources 3

Question and Answers

Windows Server 2012 R2 Roles

Question: Which roles are often co-located on the same server?

> **Answer:** Answers might vary. Domain Name System (DNS) and Active Directory® Domain Services (AD DS) are often co-located.

What Are the Windows Server 2012 Features?

Question: Which feature do you need to install to support NetBIOS name resolution for client computers running a Microsoft Windows NT® 4.0 operating system workstation?

> **Answer:** You need to install the Windows Internet Name Service (WINS) server role to support NetBIOS name resolution.

Resources

Windows Server 2012 R2 Editions

Additional Reading:

- For detailed information on the new features in Windows Server 2012 R2 Essentials, refer to "What's New in Windows Server 2012 R2 Essentials" at http://go.microsoft.com/fwlink/?LinkID=331071.
- For more information about the differences between Windows Server 2012 R2 editions, download the Windows Server 2012 R2 Products and Editions Comparison chart at http://go.microsoft.com/fwlink/?LinkID=331070.
- Many features have been removed or deprecated in Windows Server 2012 R2. For more information, go to: Features Removed or Deprecated in Windows Server 2012 R2 Preview at http://go.microsoft.com/fwlink/?LinkID=331069.

Lesson 2

Installing Windows Server 2012

Contents:

Question and Answers 5
Resources 5

Question and Answers

Installation Methods

Question: What is another method that you can use to deploy Windows Server 2012 ?

> **Answer:** You can also configure Windows Server 2012 to boot to either a .vhd or a .vhdx file. Deployment involves copying the .vhd file to a computer, either from a network share or from local media.

Hardware Requirements for Windows Server 2012 R2

Question: Why does a server need more hard disk drive space if it has more than 16 GB of RAM?

> **Answer:** A server needs more hard disk drive space because it requires additional hard disk space for virtual memory.

Resources

Additional Reading: For more information about the Windows Server Virtualization Validation Program, refer to http://go.microsoft.com/fwlink/?LinkID=266736.

Migrating Server Roles

Reference Links: To view the Windows Server 2012 migration guides, refer to http://go.microsoft.com/fwlink/?LinkID=331068.

Lesson 3
Post-Installation Configuration of Windows Server 2012

Contents:

Demonstration: Using DISM to Add Windows Features 7

Demonstration: Using DISM to Add Windows Features

Demonstration Steps

View a list of all Windows features and their current state

1. In Server Manager click the **Tools** menu, and then click **Windows Server Backup**.

   In the details pane, notice that Windows Server Backup is not installed on the computer.

2. Close the wbadmin-[Windows Server Backup(Local)] window.

Gather information about the Windows Server Backup feature

1. Right-click the **Windows PowerShell** icon on the taskbar, and then click **Run as Administrator**.
2. Type the following command, and then press Enter:

   ```
   DISM /online /get-features
   ```

3. Type the following command, and then press Enter:

   ```
   DISM /online /get-featureinfo /featurename:WindowsServerBackup
   ```

Enable the Windows Server Backup feature

1. Type the following command, and then press Enter:

   ```
   DISM /online /enable-feature /featurename:WindowsServerBackup
   ```

Note: The feature name is case-sensitive.

2. In Server Manager, click the **Tools** menu, and then click **Windows Server Backup**.

   In the details pane, notice that Windows Server Backup is now available.

3. Close all open windows.

Lesson 4
Overview of Windows Server 2012 Management

Contents:

Question and Answers 9
Demonstration: Using Server Manager 9
Demonstration: Performing Remote Management 10

Question and Answers

Configuring Services

Question: What is the advantage of a managed service account compared to a traditional domain-based service account?

> **Answer:** The advantage of a managed service account is that you do not have to manage passwords for it.

Demonstration: Using Server Manager

Demonstration Steps

Add a feature by using the Add Roles and Features Wizard

1. In the Server Manager console, 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, select **Role-based or featured-based installation**, and then click **Next**.
4. On the Select destination server page, click **Select a server from the server pool**, verify that **LON-DC1.Adatum.com** is selected, and then click **Next**.
5. On the **Select server roles** page, select **Fax Server**.
6. In the **Add Roles and Features Wizard** dialog box that opens, click **Add Features**.
7. On the **Select server roles** page, click **Next**.
8. On the **Select features** page, select **BranchCache**, and then click **Next**.
9. On the **Fax Server** page, click **Next**.
10. On the **Print and Document Services** page, click **Next**.
11. On the **Select role services** page, click **Next**.
12. On the **Confirmation** page, select the **Restart the destination server automatically if required** check box, click **Yes**, and then click **Install**.
13. On the **Installation progress** page, click **Close**.
14. Click the flag icon next to **Server Manager Dashboard**, and review the messages.

    You can close this console without terminating the task.

View role-related events

1. In the **Server Manager** console, click the **Dashboard** node.
2. In the Roles and Server Groups area, under **DNS**, click **Events**.
3. In the **DNS - Events Detail View** dialog box, change the time period to **12 hours** and the **Event Sources** to **All**, and then click **OK**.

Run the Best Practice Analyzer for a role

1. In the Roles and Server Groups area, under DNS, click **BPA results**.
2. In the **DNS - BPA Results Detail View** dialog box, click the **Severity Levels** drop-down menu, click **All**, and then click **OK**.

List the tools available in Server Manager

1. In the Server Manager console, click the **Tools** menu, and review the tools that are installed on **LON-DC1**.
2. Press the **Windows logo key** to open the Start menu.

Sign out the currently signed-in user

1. In the Start screen, click **Administrator**, and then click **Sign Out**.
2. Sign back in to **LON-DC1** using the **Adatum\Administrator** account and the password **Pa$$w0rd**.

Restart Windows Server 2012

1. On the taskbar, click the **Windows PowerShell** icon.
2. In the Windows PowerShell window, type the following command, and then press Enter:

```
Shutdown /r /t 5
```

Demonstration: Performing Remote Management

Demonstration Steps

Use Server Manager to manage a remote server

1. Sign in to LON-DC1 as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. In the Server Manager Dashboard detail pane, click **Add other servers to manage**.
3. In the Add Servers dialog box, in the Name box, type **LON-SVR1**, and then click **Find Now**.
4. Select **LON-SVR1**, click the arrow to move it into the **Selected** pane, and then click **OK**.

Add the DNS Server role on a remote server

1. In the Server Manager Dashboard detail pane, 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 **LON-SVR1.Adatum.com** and click **Next**.
5. On the **Select server roles** page, select the **DNS Server** check box.
6. In the **Add Roles and Features Wizard** dialog box, click **Add Features**, and then click **Next**.
7. On the **Select features** page, click **Next**.
8. On the **DNS Server** page, click **Next**.
9. On the **Confirm installation selections** page, click **Install**, and then click **Close**.

Connect to and configure a remote server by using RDP

1. Sign in to LON-SVR1 as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. In Server Manager, click **Local Server**.
3. In the details pane, next to **Remote Desktop**, click **Disabled**.
4. In the **System Properties** dialog box, click **Allow remote connections to this computer**.
5. In the **Remote Desktop Connection** dialog box, click **OK**, and then click **OK**.
6. On LON-DC1, click the **Start** screen button in the lower-left corner.

7. Type **Remote**, and then click the **Remote Desktop Connection** icon.
8. In the **Remote Desktop Connection** dialog box, type **LON-SVR1**, and then click **Connect**.
9. Connect as **Adatum\Administrator** with the password **Pa$$w0rd**.
10. Sign out from LON-SVR1.

Lesson 5

Introduction to Windows PowerShell

Contents:

Demonstration: Using Windows PowerShell 13
Demonstration: Using Windows PowerShell ISE 14

Demonstration: Using Windows PowerShell

Demonstration Steps

Use Windows PowerShell to display the running services and processes on a server

1. On LON-DC1, on the taskbar, click the **Windows PowerShell** icon.

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

```
Get-Service | where-object {$_.status -eq "Running"}
```

3. To view all the commands that are related to managing services, at the Windows PowerShell prompt, type the following command, and then press Enter:

```
Get-Command -Noun Service
```

4. To view a list of running possesses on the server, at the Windows PowerShell prompt, type the following command, and then press Enter:

```
Get-Process
```

5. To view all the commands that are related to managing processes, at the Windows PowerShell prompt, type the following command, and then press Enter:

```
Get-Help Process
```

6. To view detailed information about the **Start-Process** cmdlet, at the Windows PowerShell prompt, type the following command, and then press Enter:

```
Get-Help -Full Start-Process
```

7. Close the Windows PowerShell window.

8. On the taskbar, right-click the **Windows PowerShell** icon, and then click **Run as Administrator**. Discuss with students why you might need to run a Windows PowerShell session using this option.

Use Windows PowerShell to connect to a remote computer and display all services and their current status

1. On LON-SVR1, click the **Windows PowerShell** icon on the taskbar to start Windows PowerShell.

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

```
Enable-PSRemoting
```

3. Read the output, and respond to each of the ensuing prompts by pressing Enter (five times) to accept the default response of **Yes**.

4. Switch to **LON-DC1**, and then click the **Windows PowerShell** icon on the taskbar to start Windows PowerShell.

5. At a Windows PowerShell prompt, type the following commands, and press Enter after each one:

```
Enter-PSSession –Computername LON-SVR1
Get-Service
Exit-PSSession
```

6. View the resulting output.

Use Windows PowerShell to invoke commands to multiple computers and display running services

1. On LON-DC1, type the following command, and then press Enter:

```
Invoke-Command –computername LON-DC1, LON-SVR1 –Scriptblock {Get-Process}
```

2. Examine the output, and then close the Windows PowerShell window.

Demonstration: Using Windows PowerShell ISE

Demonstration Steps

Use Windows PowerShell ISE to import the ServerManager module

1. Ensure that you are signed in to LON-DC1 as Administrator.
2. In Server Manager, click **Tools**, and then click **Windows PowerShell ISE**.
3. At the prompt, type **Import-Module ServerManager**, and then press Enter.

   This demonstrates the command-completion feature of the Windows PowerShell ISE.

View the cmdlets made available in the ServerManager module

- In the Commands pane, use the **Modules** drop-down menu to select the **ServerManager** module. Describe the function of the listed Windows PowerShell cmdlets.

Use the Get-WindowsFeature cmdlet from Windows PowerShell ISE

1. Click **Get-WindowsFeature**, and then click **Show Details**.
2. In the **ComputerName** field, type **LON-DC1**, and then click **Run**.

Run a Windows PowerShell script from the scripting pane to create a universal group named Helpdesk and add members

1. In Server Manager, click **Tools**, and then click **Active Directory Users and Computers.**
2. Expand **Adatum.com**, and then click the **IT** organizational unit (OU). Note that there is no group named Helpdesk.
3. Use File Explorer to go to **E:\Labfiles\Mod01**, right-click **CreateAndPopulateHelpdesk.ps1**, and then click **Edit.**

   This opens a new instance of Windows PowerShell ISE and exposes the scripting pane.

4. View the script, and then click the green arrow on the toolbar to run the script.
5. Switch back to **Active Directory Users and Computers** and refresh the view of the IT OU.

   You should now see a group named Helpdesk.

6. Right-click the **Helpdesk** group and click **Properties**.
7. Click the **Members** tab.

   You will see that the group is populated by the members of the IT department

8. Close all open windows.

Module Review and Takeaways

Review Question(s)

Question: What is the benefit of using Windows PowerShell to automate common tasks?

> **Answer:** Automating common tasks by using Windows PowerShell enables you to spend more time planning and performing troubleshooting tasks.

Question: What are the advantages of performing a Server Core deployment compared to the full GUI deployment?

> **Answer:** The advantages of a Server Core deployment are that the operating system will require fewer updates and fewer hardware resources.

Question: What tool can you use to determine which cmdlets are contained in a Windows PowerShell module?

> **Answer:** You can use Windows PowerShell or the Windows PowerShell ISE to determine which cmdlets are contained in a Windows PowerShell module.

Question: Which role can you use to manage KMS?

> **Answer:** You can use the Volume Activation Services role to manage KMS.

Tools

Tool	Use	Where to find it
Windows PowerShell	Performing multiple administrative and configuration tasks	Taskbar
DISM.exe	Image servicing and management	Start from a command prompt or from a Windows PowerShell prompt
RSAT	Managing servers remotely from a Windows 8.1 system	Download from the Microsoft download center and install
Windows Server Migration Tools	Assisting with migrating to different versions of Windows Server	Download from the Microsoft download center and install

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
WinRM connections fail.	Verify firewall settings. Verify WinRM configuration.
Windows PowerShell cmdlets are not available.	Ensure that appropriate Windows PowerShell modules (such as Server Manager) are loaded.
Cannot install the GUI features on Server Core deployments.	Mount a .wim image containing all of the Windows Server 2012 R2 files, and use the Install-WindowsFeature cmdlet **-source** option.

Common Issue	Troubleshooting Tip
You need a non-GUI interface method to shut down or restart a computer that is running Server Core.	Use **sconfig.cmd** or the **shutdown /r** command.
Unable to join the domain.	Verify DNS resolution and network connectivity between the host and the domain controller. Verify that user account has necessary domain-join permissions.

Lab Review Questions and Answers

Lab: Deploying and Managing Windows Server 2012

Question and Answers

Question: What IP address range do the computers in the lab use?

Answer: The IP address range the computers in the lab use is 172.16.0.0 to 172.16.255.255.

Question: Why must you set the DNS server address prior to joining the domain?

Answer: The DNS server enables the computer to locate the Domain Controller when it performs the domain join operation.

Question: Besides **sconfig.cmd**, what other tool can you use to rename a computer running the Server Core operating system?

Answer: You can use the command **netdom renamecomputer %computername% /newname:** to rename a computer running the Server Core operating system.

Module 2

Introduction to Active Directory Domain Services

Contents:

Lesson 1: Overview of AD DS 2

Lesson 2: Overview of Domain Controllers 4

Lesson 3: Installing a Domain Controller 6

Module Review and Takeaways 8

Lab Review Questions and Answers 9

Lesson 1
Overview of AD DS

Contents:

Resources 3

Resources

Overview of AD DS

Additional Reading: For more information about domains and forests, refer to "Active Directory Domain Services Overview" at http://go.microsoft.com/fwlink/?LinkID=331086.

What Is New for Windows Server 2012 Active Directory?

Additional Reading: For more information about new features in AD DS, refer to "What's New in Active Directory Domain Services (AD DS)" at http://go.microsoft.com/fwlink/?LinkID=392102.

What Is New for Windows Server 2012 R2 Active Directory?

Additional Reading: For more information about how to manage risk with multi-factor access control, refer to "Overview: Manage Risk with Multi-Factor Access Control" at http://go.microsoft.com/fwlink/?LinkID=331088.

Lesson 2
Overview of Domain Controllers

Contents:

Question and Answers 5
Demonstration: Viewing the SRV Records in DNS 5

Question and Answers

What Is the Global Catalog?

Question: Should a domain controller be a global catalog?

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

Demonstration: Viewing the SRV Records in DNS

Demonstration Steps

View the SRV records by using DNS Manager

1. On LON-DC1, sign in with the user account **Adatum\Administrator** and the password **Pa$$w0rd**.
2. In Server Manager, click the **Tools** menu.
3. In the Tools list, click **DNS**.
4. In the DNS Manager window, in the tree menu, go to **LON-DC1\Forward Lookup Zones\adatum.com**. Show the following four DNS subzones:
   - _msdcs
   - _sites
   - _tcp
   - _udp
5. Expand **Forward Lookup Zones**, expand **adatum.com**, expand **_sites**, expand **Default-First-Site-Name**, expand **_tcp**, and then, in the right pane, show the following record: **_ldap Service Location (SRV) [0][100][389] lon-dc1.adatum.com**.
6. If students have sufficient expertise and interest, open **c:\windows\system32\config**, and then open the **netlogon.dns** file in Notepad.

   Show all the SRV records that this domain controller will register in DNS.

Lesson 3
Installing a Domain Controller

Contents:

Resources 7

Resources

Installing a Domain Controller on a Server Core Installation of Windows Server 2012

Additional Reading: For complete details about using the Windows PowerShell cmdlet **Install-ADDSDomainController** refer to "Install Active Directory Domain Services (Level 100)" at http://go.microsoft.com/fwlink/?LinkID=331087.

Refer to the links on the following webpage for more information:
AD DS Deployment Cmdlets in Windows PowerShell, at
http://go.microsoft.com/fwlink/?LinkID=331089

Installing a Domain Controller by Using Install from Media

Additional Reading: For more information about the steps required to install AD DS, refer to "Install Active Directory Domain Services (Level 100)" at http://go.microsoft.com/fwlink/?LinkID=266739.

Module Review and Takeaways

Review Question(s)

Question: What are the two main purposes of OUs?

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

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

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

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

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

Question: If you needed to promote a Server Core installation of Windows Server 2012 to be a domain controller, which tool or tools could you use?

> **Answer:** To promote a Server Core installation of Windows Server 2012 to a domain controller, you could use the following tools:
>
> - Server Manager, which allows you to install AD DS remotely
> - Windows PowerShell 4.0
> - The command **dcpromo /unattend**, run on the Server Core server

Question: If you wish to run a Domain Controller in the cloud, which service should you consider using, Windows Azure AD or Windows Azure IaaS virtual machines?

> **Answer:** Answers will vary depending on student’s needs. Windows Azure AD is designed to provide identity and access management for web-based applications. Using Windows Azure IaaS allows you to deploy a full-featured Active Directory domain controller.

Lab Review Questions and Answers

Lab: Installing Domain Controllers

Question and Answers

Question: Why did you use Server Manager and not **dcpromo** when you promoted a server to be a domain controller?

> **Answer:** In Windows Server 2012, the **dcpromo** tool is deprecated and its uses are limited. It is used only at a command prompt, for example, to perform an unattended installation of AD DS, or to do a complete domain controller promotion from a command-line interface. Although Server Manager is the preferred tool to use to promote a server, you also can use Windows PowerShell or another type of scripted procedure.

Question: What are the three operations masters found in each domain?

> **Answer:** The three operations masters are:
>
> - RID master
> - Infrastructure master
> - PDC emulator masters

Question: What are the two operations masters that are present in a forest?

> **Answer:** The two operations masters that are present in a forest are the schema master and the domain naming master.

Question: What is the benefit of performing an IFM install of a domain controller?

> **Answer:** When you have an unreliable wide area network (WAN) link, performing an IFM install reduces the use of the WAN link and provides for a more reliable installation process.

Module 3

Managing Active Directory Domain Services Objects

Contents:

Lesson 1: Managing User Accounts 2

Lesson 2: Managing Groups 6

Lesson 4: Delegating Administration 8

Module Review and Takeaways 11

Lab Review Questions and Answers 14

Lesson 1
Managing User Accounts

Contents:

Resources 3
Demonstration: Managing User Accounts 3
Demonstration: Using Templates to Manage User Accounts 4

Resources

AD DS Administration Tools

Reference Links: To download the RSAT installation files, go to the Microsoft Download Center at http://go.microsoft.com/fwlink/?LinkID=266735.

Demonstration: Managing User Accounts

Demonstration Steps

Delete a user account

1. Sign in to LON-DC1 as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. On LON-DC1, in Server Manager, click **Tools**.
3. Click **Active Directory Administrative Center**.
4. In the Active Directory Administrative Center, click **Adatum (local)**, and then double-click **Managers**.
5. In Managers, right-click **Ed Meadows**, and then click **Delete**.
6. In the **Delete Confirmation** dialog box, click **Yes**.

Create a new user account

1. In the Action pane, click **New**, and then click **User**.
2. In the **Create User** dialog box, in **Full name**, type **Ed Meadows**.
3. In **User UPN logon**, type **Ed**.
4. In **Password** and **Confirm password**, type **Pa$$w0rd**, and then click **OK**.

Move the user account

1. Right-click **Ed Meadows**, and then click **Move**.
2. Click the **IT** organizational unit (OU), and then click **OK**.
3. In the navigation pane, click **Adatum (local)**.
4. In the results pane, double-click **IT**.
5. Verify that Ed Meadow's account is listed.

View the WINDOWS POWERSHELL HISTORY

1. If you have not already done so, maximize Active Directory Administrative Center.
2. At the bottom of the Active Directory Administrative Center window, click **WINDOWS POWERSHELL HISTORY** to expand the history section.
3. Discuss the following commands and switches:
   - The **Remove-ADObject** command and the switches used with it to delete Ed Meadows.
   - The **New-ADUser** command and the switches used with it to recreate Ed Meadows.
   - The additional commands used to configure the Ed Meadows account.
   - The **Move-ADObject** command and the switches used with it to move Ed Meadows.
4. Close the Active Directory Administrative Center.

Find users who have not signed in during the last 30 days

1. On the taskbar, click the **Windows PowerShell** icon.

2. To create a variable to specify the past 30 days, type the following command, and then press Enter:

   ```
   $logonDate = (get-date).AddDays(-30)
   ```

3. To find all the user accounts that have not signed in during the past 30 days, type the following command, and then press Enter:

   ```
   Get-ADUser -Filter{lastLogon -le $logonDate}
   ```

   The results include nearly every account in the domain because most of the accounts have never signed in.

Find and delete all disabled user accounts

1. To find all the disabled user accounts, type the following command, and then press Enter:

   ```
   Get-ADUser -Filter{enabled -ne $True}
   ```

   The results should list four accounts in the Sales OU and two system accounts in the Users container, Guest and krbtgt.

2. To delete the disabled user accounts in the Sales OU without being prompted for confirmation, type the following command, and then press Enter:

   ```
   Get-ADUser -SearchBase "OU=Sales,DC=Adatum,DC=com" -Filter{enabled -ne $true} |
   Remove-adobject -Confirm:$False
   ```

   If this command runs successfully, there is no output.

3. To verify that the disabled accounts have been deleted, type the following command, and then press Enter:

   ```
   Get-ADUser -Filter{enabled -ne $True}
   ```

   The results should list the two system accounts in the Users container, Guest and krbtgt.

Demonstration: Using Templates to Manage User Accounts

Demonstration Steps

Create a template account

1. On LON-DC1, in Server Manager, click **Tools**, and then click **Active Directory Administrative Center**.

2. In the Active Directory Administrative Center, click **Adatum (local)**, and then double-click **Sales.**

3. In the Action pane, click **New**, and then click **User**.

4. In the **Create User** dialog box, in **First name**, type **_LondonSales**, in **Last name**, type **Template**.

5. In **User UPN logon**, type **_LondonSales**.

6. Select **Protect from accidental deletion**.

7. Under Organization, in **Department**, type **Sales**.

8. In **Company,** type **A. Datum**.

9. In **City**, type **London**.

10. In **Description**, type **London Sales users**.
11. In the **Member of** section, click **Add**.
12. In **Enter the object names to select**, type **Sales**, and then click **OK**.
13. In the **Create User _LondonSales Template** dialog box, click **OK**.

Create a user from the _LondonSales template

1. In the Windows PowerShell window, create a variable ($LondonSales) to hold the _LondonSales properties by using the following command, and then press Enter:

```
$LondonSales = Get-ADUser -Identity "_LondonSales" -Properties
Department,Company,City
```

2. To create a new Sales user in the Sales OU, type the following command, and then press Enter:

```
New-ADUser -Name "Dan Park" -SamAccountName "Dan" -Path "OU=Sales,DC=Adatum,DC=com"
-AccountPassword (ConvertTo-SecureString -AsPlaintext "Pa$$w0rd" -Force) -GivenName
"Dan" -Surname "Park" -DisplayName "Dan Park" -Enabled $True -UserPrincipalName
"Dan@Adatum.com" -ChangePasswordAtLogon $true -Instance $LondonSales
```

Verify the User Properties

1. In the Windows PowerShell window, type the following command, and then press Enter:

```
Get-ADUser –Identity “Dan” –Properties *
```

2. Verify that the properties that you defined in the template were copied to the new user.

Lesson 2
Managing Groups

Contents:

Demonstration: Managing Groups 7

Demonstration: Managing Groups

Demonstration Steps

Create a new group

1. On LON-DC1, switch to **Active Directory Administrative Center**.
2. Expand Adatum (Local), and then click **IT**.
3. In the Tasks list, under IT, point to **New**, and then click **Group**.
4. In the **Create Group** dialog box, in **Group name**, type **IT Managers**.

Add members to the group

1. Scroll down, and under Members, click **Add**.
2. In the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, in **Enter the object names to select (examples)**, type **April; Don**.
3. Click **Check Names**, and then click **OK**.
4. In the **Create Group IT Managers** dialog box, click **OK**.

Add a user to the group

1. In the details pane, right-click **Ed Meadows**.
2. Click **Add to group**.
3. In the **Select Groups** dialog box, in **Enter the object names to select (examples)**, type **IT Managers.**
4. Click **Check Names**, and then click **OK**.

Change the group type and scope

1. In the details pane, double-click **IT Managers**.
2. In the **IT Managers** dialog box, under **Group scope**, click **Universal**.
3. Under **Group type**, click **Distribution**, and then click **OK**.

Modify the group's Managed By property

1. In the details pane, double-click **IT Managers**.
2. In the details pane, under Managed By, click **Edit**.
3. In the **Select User, Contact or Groups** dialog box, in **Enter the object names to select (examples)**, type **Ed Meadows**, click **Check Names**, and then click **OK**.
4. Select **Manager can update membership list**, and then click **OK**.

Lesson 4
Delegating Administration

Contents:

Demonstration: Delegating Administrative Permissions 9

Demonstration: Delegating Administrative Permissions

Demonstration Steps

Create an OU

1. On LON-DC1, in Server Manager, click **Tools**, and then click **Active Directory Users and Computers**.
2. Expand the **Adatum.com** domain.
3. Right click **Adatum.com,** point to **New**, and then click **Organizational Unit**.
4. In the **New Object – Organizational Unit** dialog box, in **Name**, type **Executives**.

Note: Discuss the purpose of the **Protect Container From Accidental Deletion** setting.

5. In the **New Object – Organizational Unit** dialog box, click **OK**.

Move users into the Executives OU

1. Click the **Managers** OU.
2. Click **Carol Troup**, and then hold down Shift while clicking **Euan Garden**.
3. Right click **Euan Garden**, and then click **Move**.
4. In the **Move** dialog box, click **Executives**, and then click **OK**.

Delegate a standard task

1. In the navigation pane, right-click **Executives**, and then click **Delegate Control**.
2. In the Delegation of Control Wizard, click **Next**.
3. On the **Users or Groups** page, click **Add**.
4. In the **Select Users, Computers, or Groups** dialog box, in **Enter the object names to select (examples)**, type **IT**, and then click **OK**.
5. On the **Users or Groups** page, click **Next**.
6. On the **Tasks to Delegate** page, in the **Delegate the following common tasks** list, select the following options, and then click **Next**
   - **Create, delete, and manage user accounts**,
   - **Reset user passwords and force password change at next logon**,
   - **Read all user information**
7. On the **Completing the Delegation of Control Wizard** page, click **Finish**.

Delegate a custom task

1. In the navigation pane, right-click **Executives**, and then click **Delegate Control**.
2. In the Delegation of Control Wizard, click **Next**.
3. On the **Users or Groups** page, click **Add**.
4. In the **Select Users, Computers, or Groups** dialog box, in **Enter the object names to select (examples)**, type **IT**, and then click **OK**.
5. On the **Users or Groups** page, click **Next**.
6. On the **Tasks to Delegate** page, click **Create a custom task to delegate**, and then click **Next**.

7. On the **Active Directory Object Type** page, click **Only the following objects in the folder**.
8. In the list, select **Computer objects**.
9. Select **Create selected objects in this folder** and **Delete selected objects in this folder**, and then click **Next**.
10. On the **Permissions** page, in the **Permissions** list, select **Full Control**, and then click **Next**.
11. On the **Completing the Delegation of Control Wizard** page, click **Finish**.

View AD DS permissions resulting from these delegations

1. On the **View** menu, click **Advanced Features**.
2. In the navigation pane, right-click **Executives**, and then click **Properties**.
3. In the **Executives Properties** dialog box, on the **Security** tab, click **Advanced**.

   In the **Advanced Security Settings for Executives** dialog box, notice the Allow permissions that are assigned to IT (ADATUM\IT). These were created during the delegation process.
4. Click **Cancel** twice, and then close all open windows except Server Manager.

Module Review and Takeaways

Best Practices

Best Practices for User Account Management

- Do not let users share user accounts. Always create a user account for each individual, even if that person will not be with your organization for a long time.
- Educate users about the importance of password security.
- Ensure that you choose a naming strategy for user accounts that enables you to identify the user to whom the account relates. Also ensure that your naming strategy uses unique names within your domain.

Best Practices for Group Management

- When you manage access to resources, try to use both domain-local groups and role groups.
- Use universal groups only when necessary because they add weight to replication traffic.
- Use Windows PowerShell with Active Directory Module for batch jobs on groups.
- Avoid adding users to built-in and default groups.

Best Practices Related to Computer Account Management

- Always provision a computer account before joining computers to a domain, and then place them in appropriate OU.
- Redirect the default Computers container to another location.
- Reset the computer account, instead of disjoining and rejoining.
- Integrate the offline domain join functionality with unattended installations.

Review Question(s)

Question: Your company has branches in multiple cities, and each branch has a local domain that is part of the company forest. Each branch also has their own printers that are managed by using domain-local groups from their local domain. The company's sales people frequently travel between locations.

How can you provide the sales people with access to the various printers as they travel between locations?

> **Answer:** You can create a group with domain local scope, and assign it permission to access the printer. Put the Sales user accounts in a group with global scope, and then add this group to the group that has domain-local scope. When you want to give the Sales users access to a new printer, assign the group with domain-local scope permission to access the new printer. All members of the group with global scope receive access to the new printer automatically.

Question: You are responsible for managing accounts and access to resources for your group members. A user in your group transfers to another department within the company. What should you do with the user’s account?

> **Answer:** Although your company might have a Human Resources representative with AD DS permissions to move user accounts, the best solution is to move the user account into the appropriate OU of the new department. In this manner, the Group Policies associated with the new department are enforced. If applying the correct Group Policies is important, the user’s account should be disabled until someone with appropriate security permissions can move it into the new OU.

Question: What is the main difference between the Computers container and an OU?

Answer: You cannot create an OU within a Computers container, so you cannot subdivide the Computers container. In addition, you cannot link a GPO to a container. Because of this, as a best practice you should move newly created computer accounts from the Computers container to an OU.

Question: When should you reset a computer account? Why is it better to reset the computer account rather than to disjoin and then rejoin it to the domain?

Answer: You should reset a computer account when the computer is no longer able to authenticate to the domain. That can happen if the operating system is reinstalled, if the computer is restored from backup, or if the password is out of the synchronization interval.

It is better to reset the computer account because if you disjoin the computer from a domain and then rejoin it, you risk losing the computer account completely, which results in loss of the computer's SID and, more importantly, its group memberships. When you rejoin the domain, even though the computer has the same name, the account has a new SID, and all the group memberships of the previous computer object must be recreated.

Question: A project manager in your department is starting a group project that will continue for the next year. Several users from your department and other departments will be dedicated to the project during this time. The project team must have access to the same shared resources. The project manager must be able to manage the user accounts and group accounts in AD DS; however, you do not want to give the project manager permission to manage anything else in AD DS. What is the best way to do this?

Answer: The best way to do this is to create a new global security group and then add the project members to the group. Create a new OU outside your department's OU, and then assign full control of the OU to the project manager. Add the global group to the new OU, and then add resources, such as shared files and printers, to the OU. Keep track of the project, and delete the global group when the work finishes. You can keep the OU if another project requires it; however, you should delete it if there is no immediate need for it.

Question: You are working as an IT technician in Contoso, Ltd. You are managing the Windows Server–based infrastructure. You have to find a method for joining new Windows 8.1-based computers to a domain during the installation process, without intervention of a user or an administrator. What is the best way to do this?

Answer: The best way to do this is to provision the computer accounts to AD DS by using the **djoin** command-line tool with the **/provision** switch, and then use an unattended setup to perform the installation. By using a tool such as Windows System Image Manager, you can perform an unattended domain join during an operating system installation by providing information in an Unattend.xml file that is relevant to the domain join.

Tools

Tool	Used for	Where to find it
Active Directory Administrative Center	Manage users and groups	Administrative Tools
Active Directory Users and Computers	Manage users and groups	Administrative Tools
Active Directory module for Windows PowerShell	Manage users and groups	Installed as Windows Feature
Active Directory module for Windows PowerShell	Computer account management	Administrative Tools

Tool	Used for	Where to find it
djoin	Offline domain join	Must be launched from a Command Prompt or a Windows PowerShell prompt
redircmp	Change default computer container	Command line
dsacls	View and modify AD DS permissions	Command line

Lab Review Questions and Answers

Lab: Managing Active Directory Domain Services Objects

Question and Answers

Question: What are the options for modifying the attributes of new and existing users?

Answer: You can modify attributes of new and existing users in the following ways:

- Select multiple users and then open the Properties dialog box
- Use the **dsmod** command
- Create a user account based on a user account template
- Use the **Set-ADUser** Windows PowerShell cmdlet

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

Answer: Global groups can include as members users and other roles (global groups) from the same domain.

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

Answer: Domain-local groups can contain roles (global groups) and individual users from any trusted domain in the same forest or an external forest, and other domain-local groups in the same domain. Finally, domain-local groups can contain universal groups from anywhere in the forest.

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

Answer: The necessary credentials are the local credentials that are in the local Administrators group of the computer, and domain credentials that have permissions to join a computer to the computer account.

Module 4

Automating Active Directory Domain Services Administration

Contents:

Lesson 1: Using Command-line Tools for AD DS Administration 2

Lesson 2: Using Windows PowerShell for AD DS Administration 4

Lesson 3: Performing Bulk Operations with Windows PowerShell 6

Module Review and Takeaways 10

Lab Review Questions and Answers 11

Lesson 1
Using Command-line Tools for AD DS Administration

Contents:

Question and Answers 3
Resources 3

Question and Answers

What Are DS Commands?

Question: What criteria would you use to select between using **csvde**, **ldifde**, and the **ds*** commands?

Answer: If you are using a data source that can export as a .csv file, you most likely will use **csvde**. However, **csvde** cannot modify existing objects. You are also likely to use **csvde** when exporting data from AD DS.

If you are using a data source that can export as an LDIF file, then you would most likely use **ldifde**. You would also use **ldifde** if you need to remove or modify existing objects.

If you are modifying individual objects, then you will most likely use the **ds*** commands if you have chosen not to use graphical tools.

Resources

What Is Csvde?

Additional Reading: For more information about LDAP query syntax, refer to LDAP Query Basics at http://go.microsoft.com/fwlink/?LinkId=168752.

Lesson 2
Using Windows PowerShell for AD DS Administration

Contents:

Question and Answers 5

Question and Answers

Using Windows PowerShell Cmdlets to Manage User Accounts

Question: Are all cmdlet parameters that you use to manage user accounts the same?

> **Answer:** No. Many of the parameters are the same or similar, but each cmdlet has its own list of parameters.

Using Windows PowerShell Cmdlets to Manage OUs

Question: In the slide example, is the **ProtectedFromAccidentalDeletion** parameter required?

> **Answer:** No. The default value is set to **$true**. The same result occurs if the **ProtectedFromAccidentalDeletion** parameter is not used.

Lesson 3
Performing Bulk Operations with Windows PowerShell

Contents:

Question and Answers 7
Resources 7
Demonstration: Using Graphical Tools to Perform Bulk Operations 7
Demonstration: Performing Bulk Operations with Windows PowerShell 8

Question and Answers

Querying Objects with Windows PowerShell

Question: What is the difference between using **-eq** and **-like** when you are comparing strings?

> **Answer:** The **-eq** operator finds an exact match, meaning that it is not case sensitive. However, you can use the **-like** operator with the asterisk (*) wildcard to find partial matches.

Modifying Objects with Windows PowerShell

Question: Which attributes of a user account can you use when creating a query by using the **Filter** parameter?

> **Answer:** You can use any user account parameter that you can query. Use the **Properties** parameter with a value of * (**-Properties ***) to identify all properties that can be retrieved.

Working with CSV Files

Question: In the **foreach** loop, how does **$i** change?

> **Answer:** The **foreach** loop processes each row from the .csv file that is loaded into the **$users** variable. The loop is performed once for each row from the .csv file. The variable **$i** represents each row as it is processed.

Resources

Querying Objects with Windows PowerShell

Additional Reading: For more information about filtering with **Get-AD*** cmdlets, refer to "about_ActiveDirectory_Filter" at http://go.microsoft.com/fwlink/?LinkID=266740.

Additional Reading: For the full list of flags in the **UserAccountControl** property, refer to "How to use the UserAccountControl flags to manipulate user account properties" at http://go.microsoft.com/fwlink/?LinkID=331075.

Modifying Objects with Windows PowerShell

Additional Reading: For more information on the **Set-ADUser** cmdlet, refer to "Set-ADUser" at http://go.microsoft.com/fwlink/?LinkID=331074.

Demonstration: Using Graphical Tools to Perform Bulk Operations

Demonstration Steps

Create a query for all users

1. Sign in to LON-DC1 as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. On LON-DC1, in Server Manager, click **Tools**, and then click **Active Directory Administrative Center**.
3. In the Active Directory Administrative Center, in the navigation pane, click **Global Search**.
4. At the far right of the Global Search pane, click the down arrow that is displayed inside a circle to display **Add criteria**.

5. Click **Add criteria**, select the **Object type is user/inetOrgPerson/computer/group/organization unit** check box, and then click **Add**.
6. Verify that the criteria that you added is **and The object type is: User**.
7. Click the **Search** button.

Configure the Company attribute for all users

1. Press **Ctrl+A** to select all of the user accounts, and then click **Properties**.
2. In the Multiple Users pane, in the Organization section, select the **Company** check box.
3. In the **Company** text box, type **A. Datum**, and then click **OK**.

Verify that the Company attribute has been modified

1. In the Global Search pane, click **Adam Barr**, and then click **Properties**.
2. In the Adam Barr window, verify that the Company is **A. Datum**.
3. Click **Cancel**.
4. Close the Active Directory Administrative Center.

Demonstration: Performing Bulk Operations with Windows PowerShell

Demonstration Steps

Configure a department for users

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

```
Get-ADUser -Filter * -SearchBase “ou=Research,dc=adatum,dc=com”
```

3. Type the following command, and then press Enter:

```
Get-ADUser -Filter * -SearchBase “ou=Research,dc=adatum,dc=com” | Set-ADUser
-Department Research
```

4. Type the following command, and then press Enter:

```
Get-ADUser -Filter ‘department -eq “Research”’ | Format-Table
DistinguishedName,Department
```

5. Type the following command, and then press Enter:

```
Get-ADUser -Filter ‘department -eq “Research”’ -Properties Department | Format-Table
DistinguishedName,Department
```

Create an organizational unit (OU)

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

```
New-ADOrganizationalUnit LondonBranch -Path “dc=adatum,dc=com”
```

Run a script to create new user accounts

1. On the taskbar, click the **File Explorer** icon.
2. In File Explorer, expand drive **E**, expand **Labfiles**, and then click **Mod04**.
3. Double-click **DemoUsers.csv**.

4. In the **How do you want to open this type of file (.csv)?** message, click **Notepad**.
5. In Notepad, review the contents of the .csv file, and then read the header row.
6. Close **Notepad**.
7. In File Explorer, right-click **DemoUsers.ps1**, and then click **Edit**.
8. In Windows PowerShell Integrated Scripting Environment (ISE), review the contents of the script.

   Note that the script:

   - Refers to the location of the .csv file.
   - Uses a **foreach** loop to process the .csv file contents.
   - Refers to the columns defined by the header in the .csv file.
9. Close Windows PowerShell ISE.
10. At the Windows PowerShell prompt, type **cd E:\Labfiles\Mod04**, and then press Enter.
11. Type **.\DemoUsers.ps1**, and then press Enter.
12. Close Windows PowerShell.

Verify that new user accounts were created

1. In Server Manager, click **Tools**, and then click **Active Directory Administrative Center**.
2. In the Active Directory Administrative Center, in the navigation pane, go to **Adatum (local)>LondonBranch**.
3. Verify that the user accounts were created.

   Note that the accounts are disabled, because no password was set during creation.
4. Close the Active Directory Administrative Center.

Module Review and Takeaways

Review Question(s)

Question: A colleague is creating a Windows PowerShell script that creates user accounts from data in a .csv file. However, his script is experiencing errors when attempting to set a default password. Why might this be happening?

> **Answer:** The most common source of errors received when setting passwords during user account creation is the format of the variable containing the password. The variable containing a user password must be a secure string. After importing default passwords from the .csv file, your colleague must convert the value to a secure string so that it is encrypted in memory.
>
> Another common problem is trying to use passwords that do not meet complexity requirements. If you try to create a user account with the **New-ADUser** cmdlets and use a password that does not meet complexity requirements, the user account is created but the password is not set, causing the user account to be disabled.

Question: You are an administrator for a school district that creates 20,000 new user accounts for students each year. The administration system for students generates a list of the new students and then exports it as a .csv file. After the data is exported to a .csv file, what information do you need to work with the data in a script?

> **Answer:** To work with a .csv file, you need to know the name and location of the .csv file. This information allows you to import the .csv file into a variable. You also need to know the name of each column in the .csv file. If there is no header row with column names, then you need to create one.

Question: The Research department in your organization has been renamed "Research and Development." You need to update the **department** property of users in the Research department to reflect this change.

You have created a query for user accounts that have the **department** property set to **Research**, by using the **Get-ADUser** cmdlet and the **-filter** parameter. What is the next step to update the **department** property to Research and Development?

> **Answer:** You need to pipe the output from the query to the **Set-ADUser** cmdlet. The **Set-ADUser** cmdlet modified the **department** property of the user accounts.

Tools

Tool	Used for	Where to find it
csvde	**Csvde** is a command-line tool that exports or imports AD DS objects to or from a comma-separated values (.csv) file.	In Windows Server 2012.
ldifde	**Ldifde** is a command-line tool that you can use to export, create, modify, or delete AD DS objects. Like **csvde**, **ldifde** uses data that is stored in a file.	In Windows Server 2012.
ds* commands	You can use **ds*** commands to create, view, modify, and remove AD DS objects. These tools are suitable for scripts and include: **dsadd**, **dsget**, **dsquery**, **dsmod**, **dsrm** and **dsmove**.	In Windows Server 2012

Lab Review Questions and Answers

Lab: Automating AD DS Administration by Using Windows PowerShell

Question and Answers

Question: By default, are new user accounts enabled or disabled when you create them by using the **New-ADUser** cmdlet?

> **Answer:** By default, new user accounts are disabled when you create them by using the **New-ADUser** cmdlet.

Question: What file extension do Windows PowerShell scripts use?

> **Answer:** Windows PowerShell scripts use the .ps1 file extension.

Module 5

Implementing IPv4

Contents:

Lesson 1: Overview of TCP/IP 2

Lesson 2: Understanding IPv4 Addressing 4

Lesson 3: Subnetting and Supernetting 6

Lesson 4: Configuring and Troubleshooting IPv4 8

Module Review and Takeaways 11

Lab Review Questions and Answers 14

Lesson 1
Overview of TCP/IP

Contents:

Question and Answers 3

Question and Answers

What Is a Socket?

Question: Are there other well-known ports that you can think of?

Answer: Other well-known ports include:

- RDP. TCP 3389
- Kerberos protocol. TCP/UDP 88
- Remote procedure call (RPC). TCP/UDP 135
- Internet Message Application Protocol (IMAP). TCP 143
- Microsoft SQL Server® TCP 1433

Lesson 2
Understanding IPv4 Addressing

Contents:

Question and Answers 5

Question and Answers

IPv4 Addressing

Question: How is network communication affected if a default gateway is configured incorrectly?

> **Answer:** A host with an incorrect default gateway is unable to communicate with hosts on a remote network. Communication on the local network is unaffected.

More Complex IPv4 Implementations

Question: Does your organization use simple or complex networking?

> **Answer:** Answers will vary. Most small organizations use simple networking to make configuration easier. Larger organizations with networking specialists are more likely to use complex networking.

Lesson 3
Subnetting and Supernetting

Contents:

Question and Answers 7

Question and Answers

Discussion: Creating a Subnetting Scheme for a New Office

Question: How many subnets are required?

> **Answer:** Five subnets are required in this scenario. Of these, four subnets are required for buildings, and one is required for the data center.

Question: How many bits are required to create that number of subnets?

> **Answer:** Three bits are required to create five subnets, because three bits allow for eight subnets. Because printers in this scenario have networking capability, you assign IP addresses to them.

Question: How many hosts are required on each subnet?

> **Answer:** Because each subnet must support 700 users and 14 printers, 714 hosts are required on each subnet.

Question: How many bits are required to support that number of hosts?

> **Answer:** Ten bits are required to support up to 1,022 hosts.

Question: What is an appropriate subnet mask that would satisfy these requirements?

> **Answer:** Several subnet masks can allow for the minimum number of networks and the minimum number of hosts:

- 255.255.224.0 (3 subnet bits, 13 host bits)
- 255.255.240.0 (4 subnet bits, 12 host bits)
- 255.255.248.0 (5 subnet bits, 11 host bits)
- 255.255.252.0 (6 subnet bits, 10 host bits)

Lesson 4
Configuring and Troubleshooting IPv4

Contents:

Question and Answers 9

Resources 9

Demonstration: How to Capture and Analyze Network Traffic by Using Microsoft Message Analyzer 9

Question and Answers

Configuring IPv4 Manually

Question: Do any computers or devices in your organization have static IP addresses?

> **Answer:** In most cases, servers have static IP addresses. Other network devices such as printers also typically have static IP addresses.

The IPv4 Troubleshooting Process

Question: What additional steps might you use to troubleshoot network connectivity problems?

> **Answer:** Answers will vary. Some students may monitor firewalls if the problem is related to Internet connectivity. Students may also use application logs when troubleshooting connectivity to a specific program.

Resources

Configuring IPv4 Manually

Additional Reading: For more information about net TCP/IP cmdlets in Windows PowerShell, go to http://go.microsoft.com/fwlink/?LinkId=269708.

What Is Microsoft Message Analyzer?

Reference Links: For more information about Microsoft Message Analyzer, see the Microsoft Message Analyzer Operating Guide at http://go.microsoft.com/fwlink/?LinkID=331073.
To download Microsoft Message Analyzer, go to http://go.microsoft.com/fwlink/?LinkID=331072.

Demonstration: How to Capture and Analyze Network Traffic by Using Microsoft Message Analyzer

Demonstration Steps

Start a new Capture/Trace in Microsoft Message Analyzer

1. Sign in to **LON-SVR2** as **Adatum\Administrator** with a password of **Pa$$w0rd**.
2. On the taskbar, click the **Windows PowerShell** icon.
3. At the Windows PowerShell prompt, type the following, and then press Enter:

```
ipconfig /flushdns
```

4. On the Start screen, click **Microsoft Message Analyzer**.
5. In the Microsoft Message Analyzer dialog box, click **Do not update items**, and then click **OK**.
6. In the navigation pane, click **Capture/Trace**, and then, in the **Trace Scenarios** section, click **Firewall**.

Capture packets from a ping request

1. In Microsoft Message Analyzer, on the toolbar, click **Start With**.
2. At the Windows PowerShell prompt, type the following, and then press Enter:

```
Test-NetConnection LON-DC1.adatum.com
```

3. In Microsoft Message Analyzer, on the toolbar, click **Stop**.

Analyze the captured network traffic

1. In Microsoft Message Analyzer, in the results pane, under the Module column, select the first **ICMP** packet group.
2. In the results pane, click the plus sign '**+**' beside the selected packet group.
3. Show that the packet group includes both the **Echo Request** and the **Echo Reply** packets, due to the ping request that was executed when running the **Test-NetConnection** cmdlet.
4. View the source and destination IP addresses for each packet.

Filter the network traffic

1. On the Microsoft Message Analyzer toolbar, in the View Filter section, in the Filter box, type the following, and then click **Apply Filter**:

   *DestinationAddress == 172.16.0.10

2. Verify that only packets that match the filter are displayed.
3. Close **Microsoft Message Analyzer**.

Module Review and Takeaways

Best Practices

When implementing IPv4, use the following best practices:

- Allow for growth when planning IPv4 subnets. This ensures that you do not need to change you IPv4 configuration scheme.
- Define purposes for specific address ranges and subnets. This enables you to both identify hosts based on their IP address easily and to use firewalls to increase security.
- Use dynamic IPv4 addresses for clients. It is much easier to manage the IPv4 configuration for client computers by using DHCP than with manual configuration.
- Use static IPv4 addresses for servers. When servers have a static IPv4 address, it is easier to identify where services are located on the network.

Review Question(s)

Question: You have just started as a server administrator for a small organization with a single location. The organization is using the 131.107.88.0/24 address range for the internal network. Is this a concern?

> **Answer:** Yes, that is a concern because those are Internet-routable addresses. Most IPv4 networks use private addresses with network address translation (NAT) to allow access to the Internet. This organization will not be able to access the 131.107.88.0/24 network on the Internet.

Question: You are working for an organization that provides web hosting services to other organizations. You have a single /24 network from your ISP for the web hosts. You are almost out of IPv4 addresses and have asked your ISP for an additional range of addresses. Ideally, you would like to supernet the existing network with the new network. Are there any specific requirements for supernetting?

> **Answer:** Yes. To perform supernetting, the two networks must be consecutive. The networks must allow you to remove a single bit from the subnet mask and identify both as the same network.

Question: You have installed a new web-based program that runs on a non-standard port number. A colleague is testing access to the new web-based program, and indicates that he cannot connect to it. What are the most likely causes of his problem?

> **Answer:** When a server program runs on a non-standard port, you need to provide the client program with the port number to which it should be connecting. For example, http://*servername*:*port*. It is also possible that your colleague is attempting to connect using http, when he should be using https.

Tools

Tool	Use for	Where to find it
Microsoft Message Analyzer	Capture and analyze network traffic.	Download from the Microsoft website
Get-NetIPAddress	Obtains a list of IP addresses that are configured for interfaces.	Windows PowerShell
Test-NetConnection	Displays the following: Results of a DNS lookup Listing of IP interfaces Option to test a TCP connection	Windows PowerShell

Tool	Use for	Where to find it
	Internet Protocol security (IPsec) rules Confirmation of connection establishment	
Ipconfig	View network configuration.	Command prompt
Ping	Verify network connectivity.	Command prompt
Tracert	Verify network path between hosts.	Command prompt
Pathping	Verify network path and reliability between hosts.	Command prompt
Route	View and configure the local routing table.	Command prompt
Telnet	Test connectivity to a specific port.	Command prompt
Netstat	View network connectivity information.	Command prompt
Resource monitor	View network connectivity information.	Tools in Server Manager
Windows Network Diagnostics	Diagnose a problem with a network connection.	Properties of the network connection
Event Viewer	View network-related system events.	Tools in Server Manager

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
IP conflicts	In most cases, computers that are running Windows operating systems display a message when they have an IP conflict with another network device. However, some network devices do not. When performing a packet capture, duplicate TCP acknowledgements can be an indication that two devices have the same IP address, and that both are responding to connection attempts. To prevent IP conflicts, clearly document which IPv4 addresses are in use on your network, and do not assign new IPv4 addresses without checking the documentation.
Multiple default gateways defined	On hosts with multiple network cards, only one should have a default gateway defined. Windows Server 2012 is designed to function with only a single default gateway. When multiple default gateways are defined, network communication may be unpredictable. You can verify that only a single default gateway is configured by using the **Get-NetRoute** cmdlet.

Common Issue	Troubleshooting Tip
Incorrect IPv4 configuration	Incorrect IPv4 configuration information is most commonly a result of a manual configuration error. To ensure that this does not affect a production environment, you should test network connectivity thoroughly for any new servers that you place into production. You should also perform testing after making any network configuration changes.

Lab Review Questions and Answers

Lab: Implementing IPv4

Question and Answers

Question: Why is variable-length subnetting required in this lab?

> **Answer:** The criteria in the scenario call for one subnet with 100 IP addresses for clients. It is not possible to make all of the subnets this large. Variable-length subnetting enables you to subdivide the single /24 network into variable-sized subnets to accommodate one large subnet and two smaller subnets.

Question: Which Windows PowerShell cmdlet can you use to view the local routing table of a computer instead of using **route print**?

> **Answer:** You can use the **Get-NetRoute** cmdlet to view the local routing table of a computer.

Module 6

Implementing Dynamic Host Configuration Protocol

Contents:

Lesson 1: Overview of the DHCP Server Role 2

Lesson 2: Configuring DHCP Scopes 4

Module Review and Takeaways 7

Lab Review Questions and Answers 9

Lesson 1
Overview of the DHCP Server Role

Contents:

Resources 3

Demonstration: Installing the DHCP Server Role 3

Resources

How DHCP Lease Generation Works

Additional Reading: For more information about DHCP technology in Windows Server 2012, refer to "Dynamic Host Configuration Protocol (DHCP) Overview" at http://go.microsoft.com/fwlink/?LinkId=269709.

Demonstration: Installing the DHCP Server Role

Demonstration Steps

Install the DHCP server role

1. Sign in to **LON-SVR1** as **Adatum\Administrator** with the password **Pa$$w0rd.**
2. In Server Manager, in the Manage drop-down menu, click **Add Roles and Features**.
3. In the Add Roles and Features Wizard, click **Next**.
4. On the **Select installation type** page, click **Next**.
5. On **Select destination server** page, click **Next**.
6. On **Select server roles** page, select the **DHCP Server** check box.
7. In Add Roles and Features Wizard, click **Add Features**, and then click **Next**.
8. On the **Select features** page, click **Next**.
9. On the **DHCP Server** page, click **Next**.
10. On the Confirm installation selections page, click **Install**.
11. On the **Installation progress** page, wait until the "Installation succeeded on lon-svr1.adatum.com" message appears, and then click **Close**.
12. Repeat steps 1 through 11 on LON-SVR2.

Authorize the DHCP Server

1. On LON-SVR1, on the Server Manager dashboard, click **Tools**, and then click **DHCP**.
2. In the DHCP console, expand **lon-svr1.adatum.com**.
3. Right-click **lon-svr1.adatum.com**, and then click **Authorize**.
4. In the DHCP console, right-click **lon-svr1.adatum.com**, and then click **Refresh**.

   Notice that the icons next to IPv4 and IPv6 change color from red to green, which indicates that the DHCP server has been authorized in Active Directory® Domain Services (AD DS).
5. Repeat steps 1 through 3 on LON-SVR2, replacing the FQDN in step 4 with **lon-svr2.adatum.com**.

Note: Leave all virtual machines in their current state for the next demonstration.

Lesson 2
Configuring DHCP Scopes

Contents:

Resources 5
Demonstration: Creating and Configuring a DHCP Scope 5

Resources

What Are DHCP Scopes?

Additional Reading: For more information about DHCP server cmdlets in Windows PowerShell, go to http://go.microsoft.com/fwlink/?LinkID=331064.

Additional Reading: For additional Windows PowerShell cmdlets for DHCP that have been added in Windows Server 2012 R2, go to http://go.microsoft.com/fwlink/?LinkID=331065.

Demonstration: Creating and Configuring a DHCP Scope

Demonstration Steps

Configure scope and scope options in DHCP

1. On LON-SVR1, in DHCP, in the navigation pane, click **lon-svr1.adatum.com**, expand **IPv4**, right-click **IPv4**, and then click **New Scope**.
2. In the New Scope Wizard, click **Next**
3. On the **Scope Name** page, in the **Name** box, type **Branch Office**, and then click **Next**.
4. On the **IP Address Range** page, complete the page using the following information, and then click **Next**:
   - Start IP address: **172.16.0.100**
   - End IP address: **172.16.0.200**
   - Length: **16**
   - Subnet mask: **255.255.0.0**
5. On the **Add Exclusions and Delay** page, complete the page using the following information:
   - Start IP address: **172.16.0.190**
   - End IP address**: 172.16.0.200**
6. Click **Add**, and then click **Next**.
7. On the **Lease Duration** page, click **Next**.
8. On the **Configure DHCP Options** page, click **Next**.
9. On the **Router (Default Gateway)** page, in the IP address box, type **172.16.0.1**, click **Add**, and then click **Next**.
10. On the **Domain Name and DNS Servers** page, click **Next**.
11. On the **WINS Servers** page, click **Next**.
12. On the **Activate Scope** page, click **Next**.
13. On the **Completing the New Scope Wizard** page, click **Finish**.

Configure scope and scope options in DHCP with Windows PowerShell

1. Explain that you will use similar settings to those that you just applied to LON-SVR1, but you will alter the address range and default gateway for the 10.10.0.0 network, as appropriate.
2. On LON-SVR2, from the desktop, click the **PowerShell** icon on the taskbar.
3. In Windows PowerShell®, type the following cmdlets, and then press Enter after each one:

```
Add-DhcpServerv4Scope –Name "Branch Office 2" –StartRange 10.10.0.100 –EndRange
10.10.0.200 –SubnetMask 255.255.0.0
Add-Dhcpserverv4ExclusionRange –ScopeID 10.10.0.0 –StartRange 10.10.0.190 –EndRange
10.10.0.200
Set-DhcpServerv4OptionValue –Router 10.10.0.1
Set-DhcpServerv4Scope –ScopeID 10.10.0.0 –State Active
```

4. In LON-SVR2 Server Manager, click the **Tools** drop-down menu, and then select **DHCP**.

5. In the DHCP Manager, expand **lon-svr2.adatum.com**, and then expand **IPv4**.

Module Review and Takeaways

Best Practices

The following are some best practices that you can follow:

- Design your IP addressing scheme carefully so that it accommodates the requirements of both your current and future IT infrastructure.
- Determine which devices need DHCP reservations, such as network printers, network scanners, or IP-based cameras.
- Secure your network from unauthorized DHCP servers.
- Configure the DHCP database on highly available disk drive configurations, such as a redundant array of independent disks (RAID)-5 or RAID-1, to provide DHCP service availability in case of a disk failure.
- Back up the DHCP database regularly. Test the restore procedure in an isolated, non-production environment.
- Monitor the system utilization of DHCP servers. Upgrade the DHCP server hardware if necessary to provide better service performance.

Review Question(s)

Question: You have two subnets in your organization. You want to use DHCP to allocate addresses to client computers in both subnets, but you do not want to deploy two DHCP servers. What factors must you consider?

> **Answer:** Either the router that interconnects the two subnets must support DHCP relaying, or you must place a DHCP relay agent on the subnet that does not host the DHCP server. Additionally, you should consider the impact on service availability in case the single DHCP server fails.

Question: Your organization has grown, and your IPv4 scope is almost out of addresses. What should you do?

> **Answer:** Consider redesigning your IPv4 scope.

Question: What information do you require to configure a DHCP reservation?

> **Answer:** You require the MAC address of the client that will lease the reservation.

Question: Can you configure option 003 – Router as a Server-level DHCP scope option?

> **Answer:** Yes, but you should configure the option in each subnet. In a multi-subnet environment, all clients from the same subnet should obtain the same gateway setting.

Tools

Tool	Use for	Where to find it
DHCP	Graphical User Interface for managing DHCP Server	Server Manager
Windows PowerShell	Command-line interface for managing DHCP Server	Windows taskbar on the desktop
Ipconfig.exe	Managing and troubleshooting client IP settings	Command line
Netsh.exe	Configuring both client and server-side IP	Command line

Tool	Use for	Where to find it
	settings, including those for DHCP server role	
Regedit.exe	Editing and fine-tuning settings, including those for the DHCP server role	Windows interface or Command line

Lab Review Questions and Answers

Lab: Implementing DHCP

Question and Answers

Question: What purpose does the DHCP scope have?

> **Answer:** The DHCP scope defines what information is leased to DHCP clients through the DHCP process, such as the IP address, the subnet mask, the DNS server IP address, and the Default Gateway IP address.

Question: How should you configure a computer to receive an IP address from the DHCP server?

> **Answer:** You should not have to do anything. The computer should be configured to obtain its IP address automatically.

Question: Why do you need MAC address for a DHCP server reservation?

> **Answer:** The MAC address uniquely identifies a computer or any other network device, such as network printer. The DHCP reservation process needs to identify the computer or the network device through the MAC address, so it can lease an IP address to the computer or network device.

Question: What information do you need to configure on a DHCP relay agent?

> **Answer:** For a DHCP relay agent to provide IP addresses for subnets that have no DHCP server installed, you need to install DHCP relay agent protocol on a server that will act as a DHCP relay agent. In addition, you must configure the DHCP relay agent to contact the IP address of the DHCP server in another subnet, for purposes of leasing IP addresses to DHCP clients.

Module 7

Implementing DNS

Contents:

Lesson 1: Name Resolution for Windows Clients and Servers 2

Lesson 2: Installing a DNS Server 7

Lesson 3: Managing DNS Zones 10

Module Review and Takeaways 13

Lab Review Questions and Answers 14

Lesson 1
Name Resolution for Windows Clients and Servers

Contents:

Resources 3
Demonstration: Troubleshooting Name Resolution 3

Resources

How a Client Resolves a Name

Additional Reading: To learn more about LLMNR, refer to http://go.microsoft.com/fwlink/?LinkID=331077.

Troubleshooting Name Resolution

Additional Reading: For more information on the parameters for the **Get-DnsServerStatistics** cmdlet, refer to http://go.microsoft.com/fwlink/?LinkID=331076.

Reference Links: You can download the **Dnslint** command at http://go.microsoft.com/fwlink/?LinkId=286763.

Demonstration: Troubleshooting Name Resolution

Demonstration Steps

Use Windows PowerShell cmdlets to troubleshoot DNS

1. Sign in to LON-DC1 and LON-CL1 as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. On LON-CL1, at the lower-left of the **Start screen**, click the white **Down Arrow** icon.
3. In the **Apps** screen, scroll to the right, and in the **Windows System** category, click **Windows PowerShell**.
4. In **Windows PowerShell**, type the following cmdlets, and press Enter after each one:

   ```
   Get-DnsClientServerAddress
   Clear-DnsClientCache
   ```

   Note that the DNS Server address assigned to Ethernet IPv4 is **172.16.0.10**. This is LON-DC1.
5. Explain the Interface Index number and how it is used to modify certain settings.
6. Note the entries labeled **Ethernet** in the InterfaceAlias column, and the entry labeled **IPv4** in the Address Family column. In the Interface Index column, note the Interface Index number that is in the same row as Ethernet and IPv4. Write this number here:

   You will use this specific Interface Index number in a later step.
7. In Windows PowerShell, type the following cmdlet, and then press Enter:

   ```
   Resolve-DnsName lon-dc1
   ```

   Note the address returned. Do not close Windows PowerShell.
8. Press **Windows key**+**X**, and then click **Control Panel**.
9. In **Control Panel**, click the **Network and Internet** hyperlink.
10. On the **Network and Internet** page, select and then click the **Network and Sharing Center** hyperlink.
11. On the **Network and Sharing Center** page, click the **Ethernet** hyperlink.
12. In the **Ethernet Status** window, click the **Details** button.

13. In the **Network Connections Details** pop-up window, write down the information shown in the following table.

IPv4 Address	
IPv4 Subnet Mask	
IPV4 Default Gateway	
IPv4 DNS Server	

    You need to write down this information before you proceed to the next step, because you need to enter this information in a later step.

14. Click the **Close** button.

15. On the **Ethernet Status** page, click the **Properties** button.

16. In the **This connection uses the following items** section, scroll down, select **Internet Protocol Version 4 (TCP/IPv4)**, and then click the **Properties** button.

17. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, select the **Obtain an IP address automatically** and **Obtain DNS server address automatically** option buttons, click **OK**, and then click **Close** twice.

18. Return to **Windows PowerShell**, type the following cmdlets, pressing Enter after each cmdlet, where *X* is the Interface Index number you wrote down in step 6:

    ```
    Set-DnsClientServerAddress –InterfaceIndex X -ResetServerAddresses
    Clear-DnsClientCache
    ```

    Note that there is no IP address for IPv4.

19. In **Windows PowerShell**, type the following cmdlet, press Enter, and then note the message that is returned:

    ```
    Resolve-DnsName lon-dc1
    ```

20. In **Windows PowerShell**, type the following cmdlet, where *X* is the Interface Index number you wrote down in step 6, and then press Enter:

    ```
    Set-DnsClientServerAddress –InterfaceIndex X –ServerAddress 172.16.0.10
    ```

21. In **Windows PowerShell**, type the following cmdlet, and then press Enter:

    ```
    Get-DnsClientServerAddress
    ```

    Note that there is now an address for IPv4.

22. In Windows PowerShell, type the following cmdlet, press Enter, and then note the address returned:

    ```
    Resolve-DnsName lon-dc1
    ```

23. Return to the **Network and Sharing Center**, and then click the **Ethernet** hyperlink.

24. On the **Ethernet Status** page, click the **Properties** button.

25. On the **Ethernet Properties** page, in the **This connection uses the following items** section, scroll down and select **Internet Protocol Version 4 (TCP/IPv4)**, and then click the **Properties** button.

26. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, select the **Use the following IP address** option button, enter the information that you wrote down in Step 13 into the same IP blocks you copied them from, click **OK**, and then click **Close** twice.

27. To demonstrate the output of the following cmdlets, in the Windows PowerShell window, type each of the following cmdlets, and press Enter after each one:

    ```
    Get-DnsClientCache
    Clear-DnsClientCache
    Get-DnsClientCache
    Get-DnsClientGlobalSetting
    Register-DnsClient
    ```

28. Close **Windows PowerShell** and **Network and Sharing Center**.

Using Command Line tools to troubleshoot DNS

1. Go to the **Start screen** and, at the lower-left of the Start screen, click the white **Down Arrow** button.

2. In the **Apps screen**, scroll to the right, in the **Windows System** category, right-click **Command Prompt**, and then in the app bar, click **Run as Administrator**.

3. In the Command Prompt window, type the following, and then press Enter:

    ```
    ipconfig /all
    ```

4. Review the output returned, and note the DNS server section.

5. Type **nslookup**, and then press Enter.

    You should see the address of the DNS server from step 3 above returned.
    Note the > prompt, which means that you are in the nslookup prompt.

6. Type **lon-cl1**, and then press Enter.

7. Type **exit**, and do not close any open Windows.

8. Switch to **LON-DC1**.

9. Go to the Start screen and then, at the lower-left of the **Start screen**, click the white **Down Arrow** icon.

10. On the Apps screen, scroll to the right, in the **Windows System** category, right-click **Command Prompt**, and then in the app bar, click **Run as Administrator**.

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

    ```
    dnscmd /?
    ```

    Use the output to review some of the dsncmd options available. Do not spend much time here because the second DNS server has not been set up.

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

    ```
    ipconfig /displaydns
    ```

    Note the output values displayed.

13. At the command prompt, type the following, and press Enter after each line:

    ```
    ipconfig /flushdns
    ipconfig /displaydns
    ```

    Note that the output values are gone.

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

    ```
    ping LON-CL1
    ```

    Note that while the ping replies are not successful (the client firewall is blocking ICMP packets), the ping command returned the fully qualified domain name (FQDN) of **LON-CL1**. Point out to the students that this is an indicator that DNS name resolution occurred even before the ping packet was generated.

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

    ```
    ipconfig /displaydns
    ```

    Note that information on the LON-CL1 DNS resource record is displayed.

16. Close all open windows, and sign out from **20410D-LON-DC1** and **20410D-LON-CL1.**

Lesson 2
Installing a DNS Server

Contents:

Resources 8
Demonstration: Installing the DNS Server Role 8

Resources

What Is Forwarding?

Best Practice: Use a central forwarding DNS server for Internet name resolution. This can improve security because you can isolate the forwarding DNS server in a perimeter network, which ensures that no server within the network is communicating directly to the Internet.

Best Practice: Use conditional forwarders if you have multiple internal namespaces. This results in faster name resolution.

Demonstration: Installing the DNS Server Role

Demonstration Steps

Install a second DNS server

1. Sign in to LON-DC1 and LON-SVR1 as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. On LON-SVR1, in the Server Manager console, in the Manage tab, click **Add roles and features**.
3. On the **Before you begin** page, click **Next**.
4. On the **Select installation type** page, click **Next**.
5. On the **Select destination server** page, ensure that **LON-SVR1.Adatum.com** is selected, and then click **Next**.
6. On the **Select server roles** page, click **DNS Server**.
7. In the Add Roles and Features Wizard window, click **Add Features**, and then click **Next**.
8. On the **Select Features** page, click **Next**.
9. On the **DNS Server** page, click **Next**.
10. On the **Confirm installation selections** page, click **Install**.
11. On the **Installation progress** page, when a message displays that installation succeeded, click **Close**.

Create a forward lookup zone by using Windows PowerShell

1. Switch to LON-DC1.
2. On the taskbar, select the **Windows PowerShell** icon.
3. In the Windows PowerShell window, type the following cmdlet, and then press Enter:

   ```
   Add-DnsServerPrimaryZone –Name fabrikam.com –DynamicUpdate Secure –ReplicationScope
   Domain
   ```

4. Switch to the DNS Console.

   If the DNS console is not open, in Server Manager, click the **Tools** menu, and then click **DNS**.

5. In the console tree, expand **LON-DC1**, and then expand **Forward Lookup Zones**.

   You should see the **fabrikam.com** zone.

6. Select and then right-click the **fabrikam.com** zone, and then click **Properties**.
7. On the General tab, confirm that **Replication** is set to **All DNS Servers in the Domain**, and that **Dynamic Updates** are set to **Secure only**.
8. On the **fabrikam.com Properties** page, click **Cancel**.

Configure forwarding

1. On LON-SVR1, open the **DNS Manager** console.
2. In the DNS Manager console, right-click **LON-SVR1**, click **Properties**, and then click the **Forwarders** tab.
3. In the **Forwarders** dialog box, click **Edit**.
4. In the **Edit Forwarders** page, type **172.16.0.10**, and then click **OK** twice.

   Leave all virtual machines in their current state for the next demonstration.

Lesson 3
Managing DNS Zones

Contents:

Question and Answers 11

Demonstration: Creating an Active Directory–Integrated Zone 11

Question and Answers

What Are Active Directory–Integrated Zones?

Question: Can you think of any disadvantages to storing DNS information in AD DS?

> **Answer:** If you want to replicate DNS data to other non-Microsoft DNS servers, you should not store it in AD DS.

Demonstration: Creating an Active Directory–Integrated Zone

Demonstration Steps

Promote a server as a domain controller

1. On LON-SVR1, in the Server Manager console, 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, ensure that **LON-SVR1.Adatum.com** is selected, and then click **Next**.
5. On the **Select server roles** page, click **Active Directory Domain Services**.
6. When the **Add Roles and Features Wizard** window appears, click **Add Features**, and then click **Next**.
7. On the **Select features** page, click **Next**.
8. On the **Active Directory Domain Services** page, click **Next**.
9. On the **Confirm installation selections** page, click **Install**.
10. On the **Installation progress** page, when the **Installation succeeded** message displays, click **Close**.
11. In the **Server Manager** console, on the Navigation page, click **AD DS**.
12. On the title bar where **Configuration required for Active Directory Domain Services at LON-SVR1** is visible, click **More**.
13. On the **All Server Task Details and Notifications** page, click **Promote this server to a domain controller**.
14. In the Active Directory Domain Services Configuration Wizard, on the **Deployment Configuration** page, ensure that **Add a domain controller to an existing domain** is selected, and then click **Next**.
15. On the **Domain Controller Options** page, select the **Domain Name System (DNS) server** check box, and leave the **Global Catalog (GC)** check box selected.
16. Type **Pa$$w0rd** in both text fields, and then click **Next**.
17. On the **DNS Options** page, click **Next**.
18. On the **Additional Options** page, click **Next**.
19. On the **Paths** page, click **Next**.
20. On the **Review Options** page, click **Next**.
21. On the **Prerequisites Check** page, click **Install**.
22. On the **You're about to be signed out** app bar, click **Close**.

Note: The server automatically restarts as part of the procedure.

23. After-LON-SVR1 restarts, sign in as **Adatum\Administrator** with the password **Pa$$w0rd**.

Create an Active Directory–integrated zone

1. On LON-DC1, open **Server Manager**.
2. Click **Tools**, and then click **DNS**.
3. In the DNS Manager console, click and then right-click **LON-DC1**, and then select **New Zone**.
4. In the New Zone Wizard, click **Next**.
5. On the **Zone Type** page, click **Primary zone**, ensure that the **Store the zone in Active Directory** option is selected, and then click **Next**.

Note: Point out that this option determines that the zone is in AD DS.

6. On the **Active Directory Zone Replication Scope** page, review the available options, and then, without making any changes, click **Next**.
7. On the **Forward or Reverse Lookup Zone** page, select **Forward lookup zone**, and then click **Next**.
8. On the **Zone Name** page, in the **Zone name** field, type **Contoso.com**, and then click **Next**.
9. On the **Dynamic Update** page, review the available options, select the **Allow only secure dynamic updates** option, and then click **Next**.
10. On the **Completing the New Zone Wizard** page, click **Finish**.
11. In DNS Manager console, expand **Forward Lookup Zones**, click **Contoso.com**, and then review the records that are created automatically.

Create a record

1. In the DNS Manager console, expand **LON-DC1**, expand **Forward Lookup Zones**, and then click **Contoso.com**.
2. Right-click **Contoso.com**, and then select **New Host (A or AAAA)**.
3. In the **New Host** window, in the **Name** field, type **www**, and in the IP address field, type **172.16.0.100**, click **Add Host**, and then click **OK**.
4. Click **Done**.

Verify replication to a second DNS server

1. On LON-SVR1, in the **Server Manager** console, click **Tools**, and then click **DNS**.
2. In the **DNS Manager** console, expand **LON-SVR1**, expand **Forward Lookup Zones**, and then click **Contoso.com**.
3. Verify that **www** resource record exists. It might take a couple of minutes for the record to appear, and you might have to refresh the console display.

Module Review and Takeaways

Best Practices

When you implement DNS, use the following best practices:

- Always use host names instead of NetBIOS names.
- Use forwarders rather than root hints.
- Be aware of potential caching issues when you troubleshoot name resolution.
- Use Active Directory–integrated zones instead of primary and secondary zones.

Review Question(s)

Question: You are troubleshooting DNS name resolution from a client computer. What must you remember to do before each test?

> **Answer:** You should clear the resolver cache before starting to troubleshoot.

Question: You are deploying DNS servers into an Active Directory domain, and your customer requires that the infrastructure be resistant to single points of failure. What must you consider when planning the DNS configuration?

> **Answer:** You should deploy more than one AD DS domain controller with the DNS server role installed.

Question: What benefits do you realize by using forwarders?

> **Answer:** Forwarders are used when your local DNS server cannot resolve a query from the client using its own local zones. You usually configure forwarders to resolve Internet names. However, you also can use forwarders to optimize performance, to optimize Internet link usage on your local DNS server, and to enhance security.

Tools

Name of tool	Used for	Where to find it
DNS Manager console	Manage DNS server role	Administrative Tools
Nslookup	Troubleshoot DNS	Command-line tool
Ipconfig	Troubleshoot DNS	Command-line tool
Windows PowerShell cmdlets	Manage and troubleshoot DNS	Windows PowerShell

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Clients sometimes cache invalid DNS records.	Clear the cache.
DNS Server performs slowly.	Use the Performance Monitor to measure the load on DNS.

Common Issue	Troubleshooting Tip

Lab Review Questions and Answers

Lab: Implementing DNS

Question and Answers

Question: Can you install the DNS server role on a server that is not a domain controller? If yes, are there any limitations?

> **Answer:** Yes, you can. However, you cannot create Active Directory–integrated zones on a DNS server that is not a domain controller.

Question: What is the most common way to carry out Internet name resolution on a local DNS?

> **Answer:** Companies typically configure their local DNS with a forwarder. That forwarder is most often a DNS server of their ISP.

Question: How can you browse the content of the DNS resolver cache on a DNS server?

> **Answer:** You can browse the content of the DNS resolver cache on a DNS server by enabling the Advanced view in the DNS Manager console or by using Windows PowerShell cmdlets.

Module 8

Implementing IPv6

Contents:

Lesson 2: IPv6 Addressing 2

Lesson 3: Coexistence with IPv4 5

Lesson 4: IPv6 Transition Technologies 7

Module Review and Takeaways 9

Lab Review Questions and Answers 10

Lesson 2
IPv6 Addressing

Contents:

Demonstration: Configuring IPv6 Client Settings 3

Demonstration: Configuring IPv6 Client Settings

Demonstration Steps

View IPv6 configuration by using ipconfig and Get-NetIPAddress

1. Sign in to LON-DC1 and LON-SVR1 as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. On LON-DC1, on the taskbar, click the **Windows PowerShell®** icon.
3. At the Windows PowerShell prompt, type **ipconfig**, and then press Enter.

   Notice that this returns a link-local IPv6 address.

4. At the Windows PowerShell prompt, type **Get-NetIPAddress**, and then press Enter.

   Notice that the **Get-NetIPAddress** command returns a link-local IPv6 address.

Configure IPv6 on LON-DC1

1. On LON-DC1, in Server Manager, click **Local Server**.
2. In the **local server's Properties pane**, next to **Ethernet**, click **172.16.0.10, IPv6 enabled**.
3. In the **Network Connections** dialog box, right-click **Ethernet**, and then click **Properties**.
4. Click **Internet Protocol Version 6 (TCP/IPv6)**, and then click **Properties**.
5. In the **Internet Protocol Version 6 (TCP/IPv6) Properties** dialog box, click **Use the following IPv6 address**.
6. In the **IPv6 address** box, type **FD00:AAAA:BBBB:CCCC::A**.
7. In the **Subnet prefix length** box, type **64**.
8. In the **Preferred DNS server** box, type **::1**, and then click **OK**.
9. In the **Ethernet Properties** dialog box, click **Close**.
10. Close the **Network Connections** dialog box.

Configure IPv6 on LON-SVR1

1. On LON-SVR1, in Server Manager, click **Local Server**.
2. In the local server's **Properties pane**, next to **Ethernet**, click **172.16.0.11, IPv6 enabled**.
3. In the **Network Connections** dialog box, right-click **Ethernet**, and then click **Properties**.
4. In the **Ethernet Properties** dialog box, click **Internet Protocol Version 6 (TCP/IPv6)**, and then click **Properties**.
5. In the **Internet Protocol Version 6 (TCP/IPv6) Properties** dialog box, click **Use the following IPv6 address**.
6. In the **IPv6 address** box, type **FD00:AAAA:BBBB:CCCC::15**.
7. In the **Subnet prefix length** box, type **64**.
8. In the **Preferred DNS server** box, type **FD00:AAAA:BBBB:CCCC::A**, and then click **OK**.
9. In the **Ethernet Properties** dialog box, click **Close**.
10. Close the **Network Connections** dialog box.

Verify that IPv6 communication is functional

1. On LON-SVR1, on the taskbar, click the **Windows PowerShell** icon.
2. At the Windows PowerShell prompt, type **ipconfig**, and then press Enter.

Notice that both the link-local IPv6 address and the IPv6 address that you have configured are displayed.

3. At a command prompt, type **ping -6 lon-dc1**, and then press Enter.

   Verify that you receive four replies from **LON**-**DC1** IPv6 address.

4. Type **ping -4 lon-dc1**, and then press Enter.

   Verify that you receive four replies from **LON**-**DC1** IPv4 address.

5. Type **Test-NetConnection FD00:AAAA:BBBB:CCCC::A**, and then press Enter.

   Verify that you receive **Ping Succeeded: True** from **LON**-**DC1** IPv6 address.

Lesson 3
Coexistence with IPv4

Contents:

Demonstration: Configuring DNS to Support IPv6 6

Demonstration: Configuring DNS to Support IPv6

Demonstration Steps

Configure an IPv6 host (AAAA) resource record

1. On LON-DC1, in Server Manager, click **Tools**, and then click **DNS**.
2. In DNS Manager, expand **LON-DC1**, expand **Forward Lookup Zones**, and then click **Adatum.com**.
3. Read the records listed for the zone, and notice that LON-DC1 and LON-SVR1 have registered their IPv6 addresses dynamically with the DNS server.
4. Right-click **Adatum.com**, and then click **New Host (A or AAAA)**.
5. In the New Host window, in the **Name** box, type **WebApp**.
6. In the **IP address** box, type **FD00:AAAA:BBBB:CCCC::A**, and then click **Add Host**.
7. Click **OK** to clear the success message.
8. Click **Done** to close the New Host window.

Verify name resolution for an IPv6 host (AAAA) resource record

1. On LON-SVR1, if necessary, open a Windows PowerShell prompt.
2. At the Windows PowerShell prompt, type **ping WebApp.adatum.com**, and then press Enter.

   Verify that you receive four replies from **WebApp.adatum.com** IPv6 address.

3. Type **Test-NetConnection WebApp.Adatum.com**, and then press Enter.

   Verify that you receive **Ping Succeeded: True** from **WebApp.Adatum.com** IPv6 address.

Lesson 4
IPv6 Transition Technologies

Contents:

Resources 8

Resources

What Is PortProxy?

Additional Reading: For more information about IPv6 Transition Technologies, refer to "IPv6 Transition Technologies" at http://go.Microsoft.com/fwlink/?LinkID=112079&clcid=0x409.

Module Review and Takeaways

Best Practices

Use the following best practices when implementing IPv6:

- Do not disable IPv6 on Windows 8 or Windows Server 2012.
- Enable coexistence of IPv4 and IPv6 in your organization rather than using transition technologies.
- Use unique local IPv6 addresses on your internal network.
- Use Teredo to implement IPv6 connectivity over the IPv4 Internet.

Review Question(s)

Question: What is the main difference between 6to4 and Teredo?

> **Answer:** Both protocols allow IPv6 connectivity over the IPv4 Internet. However, only Teredo is able to provide connectivity through NAT.

Question: How can you provide a DNS server to an IPv6 host dynamically?

> **Answer:** To provide a DNS server to an IPv6 host dynamically, you must use DHCPv6. You can use router advertisements to provide the network portion of an IPv6 address, but router advertisements cannot distribute DNS server IP addresses.

Question: Your organization is planning to implement IPv6 internally. After some research, you have identified unique local IPv6 addresses as the correct type of IPv6 addresses to use for private networking. To use unique local IPv6 addresses, you must select a 40-bit identifier that is part of the network. A colleague suggests using all zeros for the 40 bits. Why is this not a good idea?

> **Answer:** The 40-bit organization identifier in a unique local IPv6 address should be generated randomly. This makes it as likely as possible that no two organizations will use the same organization identifier. If two organizations use the same organization identifier, then the networks cannot be joined together after a merger.

Question: How many IPv6 addresses should be configured on an IPv6 node?

> **Answer:** There is no specific number of IPv6 addresses that an IPv6 node should have. It depends on the organization's configuration. Each IPv6 node has a link-local IPv6 address. Additionally, it also may have a unique local IPv6 address for internal connectivity and a global unicast IPv6 address for IPv6 Internet connectivity.

Lab Review Questions and Answers

Lab: Implementing IPv6

Question and Answers

Question: Did you configure IPv6 statically or dynamically in this lab?

> **Answer:** You configured IPv6 dynamically in this lab. You added both IPv6 networks to the router, and router advertisements configured LON-DC1 and LON-SVR2 with the correct network address.

Question: Why did you not need to configure LON-DC1 with the IPv4 address of the ISATAP router?

> **Answer:** The default configuration for Windows client operating systems is set to resolve ISATAP by using DNS to locate the IPv4 address of the ISATAP router. LON-DC1 used the default configuration.

Module 9

Implementing Local Storage

Contents:

Lesson 1: Overview of Storage 2

Lesson 2: Managing Disks and Volumes 4

Lesson 3: Implementing Storage Spaces 8

Module Review and Takeaways 11

Lab Review Questions and Answers 13

Lesson 1
Overview of Storage

Contents:

Question and Answers 3
Resources 3

Question and Answers

RAID Levels

Question: Should you configure all disks with the same amount of fault tolerance?

> **Answer:** No, not all disks need the same tolerance. A common practice is to use RAID 1 for the operating-system volume and RAID 5 for the data volumes.

Resources

What Is Network Attached Storage?

Additional Reading: For more information about Windows Storage Server 2012 R2, refer to "Windows Server 2012 R2" at http://go.microsoft.com/fwlink/?LinkID=199647.

Lesson 2
Managing Disks and Volumes

Contents:

Question and Answers 5

Resources 5

Demonstration: Creating Mount Points and Links 6

Demonstration: Managing Virtual Hard Disks 7

Question and Answers

Selecting a File System

Question: What file system do you use on your file server currently? Will you continue to use it?

Answer: Answers may vary. A common answer is NTFS, because NTFS should be the basis for any file system used on a Windows Server operating system. If you use FAT32 or Extended FAT (exFAT), you should be able to support your decision, because these file systems do not support security access control lists (ACLs) on files and folders.

The second part of the question focuses on switching to ReFS when upgrading to Windows Server 2012. You might answer yes because it is more reliable, or you might answer no, because you want to wait until it is used more widely in the market.

Resources

Selecting a Partition Table Format

Additional Reading: For more information, refer to "Frequently asked questions about the GUID Partitioning Table disk architecture" at http://go.microsoft.com/fwlink/?LinkID=266748.

Selecting a Disk Type

Additional Reading:

- For more information, refer to "How Basic Disks and Volumes Work" at http://go.microsoft.com/fwlink/?LinkID=199648.
- For more information, refer to "Dynamic disks and volumes" at http://go.microsoft.com/fwlink/?LinkID=199649.

Selecting a File System

Additional Reading:

- For more information, refer to "How FAT Works" at http://go.microsoft.com/fwlink/?LinkID=199652.
- For more information, refer to "How NTFS Works" at http://go.microsoft.com/fwlink/?LinkID=199654.

What Is ReFS?

Additional Reading: For more information about ReFS, refer to "Building the next generation file system for Windows: ReFS" at http://go.microsoft.com/fwlink/?linkID=270872.

Extending and Shrinking Volumes

Additional Reading:

- For more information, refer to "Extend a Basic Volume" at http://go.microsoft.com/fwlink/?LinkID=266749.
- For more information, refer to "Shrink a Basic Volume" at http://go.microsoft.com/fwlink/?LinkID=266750.

Demonstration: Creating Mount Points and Links

Demonstration Steps

Create a mount point

1. Sign in to **LON-SVR1** with the username **Adatum\Administrator** and the password **Pa$$w0rd**.
2. In Server Manager, click the **Tools** menu, and then click **Computer Management**.
3. In the Computer Management console, under the Storage node, click **Disk Management**.
4. In the Disks pane, right-click **Disk2**, and then click **Online**.
5. Right-click **Disk2**, and then click **Initialize Disk**.
6. In the **Initialize Disk** dialog box, select the **Disk2** check box, click **GPT (GUID Partition Table)**, and then click **OK**.
7. In the Computer Management console, in Disk Management, right-click the black box to the right of Disk2, and then click **New Simple Volume**.
8. In the New Simple Volume Wizard, on the **Welcome to the New Simple Volume Wizard** page, click **Next**.
9. On the **Specify Volume Size** page, in the **Simple volume size in MB** field, type **4000**, and then click **Next**.
10. On **Assign Drive Letter or Path** page, click **Do not assign a drive letter or drive path**, and then click **Next**.
11. On the **Format Partition** page, from the **File system** drop-down list, click **NTFS**, in the **Volume label** text box, type **MountPoint**, and then click **Next**.
12. On the **Completing the New Simple Volume Wizard** page, click **Finish**.
13. Wait until the volume is created, right-click **MountPoint**, and then click **Change Drive Letter and Paths**.
14. In the **Change Drive Letter and Paths for MountPoint** dialog box, click **Add**.
15. On the **Assign Drive Letter or Path** page, click **Mount in the following empty NTFS folder**, and then click **Browse**.
16. In the Browse for Drive Path window, make sure that **C:\** is selected, and then click **New Folder**.
17. In the Browse for Drive Path box, type **MountPointFolder**, and then click **OK**.
18. In the Add drive Letter or Path window, click **OK**.
19. On the taskbar, click the File Explorer icon, and then double-click **Local Disk (C:)**. You should see the **MountPoint** folder with a size of **4,095,996 KB** assigned to it. Point out the icon assigned to the mount point.

Create a directory junction for a folder

1. Right-click the **Start** button, and then click **Command Prompt**.
2. In the Command Prompt window, at the command prompt, type **cd **, and then press Enter.

3. Type **md CustomApp**, and then press Enter.
4. Type **copy C:\windows\system32\notepad.exe C:\CustomApp**, and then press Enter.
5. Type **mklink /j AppLink CustomApp**, and then press Enter.
6. In the File Explorer window, double-click the **AppLink** folder. Notice that because it is a link, the directory path in the address bar is not updated to C:\CustomApp.

Create a hard link for a file

1. At the command prompt, type **mklink /h C:\AppLink\Notepad2.exe C:\AppLink\Notepad.exe**, and then press Enter.
2. Switch to the File Explorer window, and then read the list of files. Notice that Notepad2.exe appears exactly the same as Notepad.exe. Both file names point to the same file.
3. Close all open Windows.

Demonstration: Managing Virtual Hard Disks

Demonstration Steps

Create a virtual hard disk

1. On LON-SVR1, if required, start **Server Manager**.
2. Click **Tools**, and then click **Computer Management**.
3. In Computer Management, click **Disk Management**.
4. Wait for the disks to display, right-click **Disk Management**, and then click **Create VHD**.
5. In the **Create and Attach Virtual Hard Disk** dialog box, click **Browse**.
6. Type **DiskF** as the **File name**, and then click **Save**.
7. In the **Create and Attach Virtual Hard Disk** dialog box, type **10** as the **Virtual hard disk** size.
8. Click **VHDX**, click **Dynamically expanding** and then click **OK**.
9. On the taskbar, click **File Explorer**.
10. Browse to **Documents**, and then verify that a .vhdx file named DiskF.vhdx was created.

Manage a virtual hard disk

1. In Disk Management, right-click **Disk 9**, click **Initialize disk**, and then click **OK**.
2. Right-click the unallocated space on Disk 9, and then click **New Simple Volume**.
3. On the **Welcome to the New Simple Volume Wizard** page, click **Next**.
4. On the **Specify Volume Size** page, click **Next**.
5. On the **Assign Drive Letter or Path** page, click **Next**.
6. On the **Format Partition** page, type **Data** as the **Volume label**, click **Next**, and then click **Finish**.

   If the **Microsoft Windows** dialog box appears, click **Cancel**.
7. In File Manager, verify that the **Data (F:)** drive is listed.
8. Close all open windows.

Lesson 3
Implementing Storage Spaces

Contents:

Question and Answers 9

Resources 9

Demonstration: Configuring Storage Spaces 9

Question and Answers

Virtual Disk Configuration Options

Question: What is the name for a virtual disk that is larger than the amount of disk space available on the physical disks portion of the storage pool?

> **Answer:** This kind of virtual disk is a thin provisioned virtual disk. With a thin provisioned virtual disk, you can use the available space immediately, but you need to add more physical disks to the storage pool to provide the disk space required.

Discussion: Comparing Storage Spaces with Other Storage Solutions

Question: Does your organization currently use SANs or NAS?

> **Answer:** Answers will vary.

Question: What are the advantages of using Storage Spaces compared to using SANs or NAS?

> **Answer:** Storage Spaces provides an inexpensive way to manage storage on servers. With Storage Spaces, you do not need to buy specialized storage or network devices. You can attach almost any kind of disk to a server, and manage all the disks on your server as a block. You can provide redundancy by configuring mirroring or parity on the disks. Storage Spaces are also easy to expand by adding more disks. By using Storage Space tiering, you also can optimize the use of fast and slow disks in your Storage Space.

Question: What are the disadvantages of using Storage Spaces compared to using SANs or NAS?

> **Answer:** Most SAN and NAS devices provide many of the same features as Storage Spaces. These storage devices also provide redundancy, data tiering, and easy-capacity expansion. These devices also improve performance by removing all of the storage-related calculations from the server and performing these tasks on dedicated hardware devices. This means that SAN devices, in particular, are likely to provide better performance than Storage Spaces.

Question: In what scenarios would you recommend each option?

> **Answer:** Answers will vary. Storage Spaces provide a potentially inexpensive way to provide full-featured storage solution that traditionally has only been available with more expensive NAS or SAN solutions. Additionally, Storage Spaces are easy to manage, and do not require any specialized equipment or expertise. However, in larger enterprises that currently are using SANs or NAS, the enhanced performance of using the specialized hardware is likely to be a more important factor than the ease of use and low cost that Storage Spaces provide.

Resources

Advanced Management Options for Storage Spaces

Additional Reading: For more information, refer to “Storage Cmdlets in Windows PowerShell” at http://go.microsoft.com/fwlink/?LinkID=266751.

Demonstration: Configuring Storage Spaces

Demonstration Steps

Create a storage pool

1. On LON-SVR1, sign in as **Adatum\Administrator** with the password **Pa$$w0rd**.

2. In Server Manager, in the left pane, click **File and Storage Services**, and in the Servers pane, click **Storage Pools**.
3. In the STORAGE POOLS pane, click **TASKS** and then in the **TASKS** drop-down list, click **New Storage Pool**.
4. In the New Storage Pool Wizard, on the **Before you begin** page, click **Next**.
5. On the **Specify a storage pool name and subsystem** page, in the **Name** box, type **StoragePool1**, and then click **Next**.
6. On the **Select physical disks for the storage pool** page, click all available physical disks, and then click **Next**.
7. On the **Confirm selections** page, click **Create**.
8. On the **View results** page, wait until task completes, and then click **Close**.

Create a virtual disk and a volume

1. Under Storage Pools, click **StoragePool1**.
2. In the VIRTUAL DISKS pane, click **TASKS**, and then in the **TASKS** drop-down list, click **New Virtual Disk**.
3. In the New Virtual Disk Wizard, on the **Before you begin** page, click **Next**.
4. On the **Select the storage pool** page, click **StoragePool1**, and then click **Next**.
5. On the **Specify the virtual disk name** page, in the **Name** box, type **Simple vDisk**, and then click **Next**.
6. On the **Select the storage layout** page, in the **Layout** list, select **Simple**, and then click **Next**.
7. On the **Specify the provisioning type** page, click **Thin**, and then click **Next**. You should mention that this configures thin provisioning for that volume.
8. On the **Specify the size of the virtual disk** page in the **Virtual disk size** box, type **2**, and then click **Next**.
9. On the **Confirm selections** page, click **Create**.
10. On the **View results** page, wait until the task completes. Make sure that the **Create a volume when this wizard closes** check box is selected, and then click **Close**.
11. In the New Volume Wizard, on the **Before you begin** page, click **Next**.
12. On the **Select the server and disk** page, under **Disk**, click **Simple vDisk** virtual disk, and then click **Next**.
13. On the **Specify the size of the volume** page, click **Next** to confirm the default selection.
14. On the **Assign to a drive letter or folder** page, click **Next** to confirm the default selection.
15. On the **Select file system settings** page, in the **File system** drop-down list, select **ReFS**, in the **Volume label** box, type **Simple Volume**, and then click **Next**.
16. On the **Confirm selections** page, click **Create**.
17. On the **Completion** page, wait until the task completes, and then click **Close**.

Module Review and Takeaways

Best Practices

The following are recommended best practices:

- If you want to shrink a volume, defragment the volume first so you can reclaim more space from the volume.
- Use the GPT partition table format for disks larger than 2 TB.
- For very large volumes, use ReFS.
- Do not use FAT or FAT32 on Windows Server operating system disks.
- Use the Storage Spaces feature to have the Windows operating system manage your disks.

Review Question(s)

Question: Your current volume runs out of disk space. You have another disk available in the same server. What actions in the Windows operating system can you perform to help you add disk space?

Answer: Your answers can include converting the disk to a dynamic disk and extending the volume with the second disk. You can also use the second disk as a mount point to move some large files and re-assign their path. You could also use links to move large files to the new volume, and then create a link from their original location.

Question: What are the two disk types in Disk Management?

Answer: The two types of disks are basic and dynamic.

Question: What are the most important implementations of RAID?

Answer: The most important implementations of RAID are:

- RAID 1: Mirrored set without parity or striping.
- RAID 5: Striped set with parity.
- RAID 6: Striped set with dual distributed parity.
- RAID 1+0: Mirrored drives configured as a strip set.

Question: You attach five 2 TB disks to your Windows Server 2012 computer. You want to simplify the process of managing the disks, and if one disk fails, you want to make sure the data is not lost. What feature can you implement to accomplish this?

Answer: You can implement the Storage Spaces feature, create a storage pool with all five disks, and then create a virtual disk with parity or mirroring to make it highly available. Alternatively, you could create a RAID-5 volume in Disk Management, but this would not manage the disks automatically.

Tools

Tool	Use	Where to find it
Disk Management	Initialize disks Create and modify volumes	In Server Manager on the Tools menu (part of Computer Management)
Diskpart.exe	Initialize disks Create and modify volumes from a command prompt	Command prompt

Tool	Use	Where to find it
Mklink.exe	Create a symbolic link to a file or folder	Command prompt
Chkdsk.exe	Check a disk for a NTFS-formatted volume Cannot be used for ReFS or virtual disks	Command prompt
Defrag.exe	Disk defragmentation tool for NTFS-formatted volumes. Cannot be used for ReFS or virtual disks	Command prompt

Lab Review Questions and Answers

Lab: Implementing Local Storage

Question and Answers

Question: At a minimum, how many disks must you add to a storage pool to create a three-way mirrored virtual disk?

> **Answer:** You require at least five disks. If you do not have five disks available in disk pool, you can create a two-way mirrored virtual disk only.

Question: You have a USB-attached disk, four SAS disks, and one SATA disk that are attached to a Windows Server 2012 server. You want to provide a single volume to your users that they can use for file storage. What would you use?

> **Answer:** Answers may vary.
>
> The most common answer might be to create a storage pool out of the existing disks, and then create a virtual disk that spans all of the disks and has the largest capacity possible.
>
> For reliability reasons, USB disks should not be part of a storage pool. However, you can mix the disk types in a storage pool and create highly available disks using two-way or three-way mirroring or parity for virtual disks.

Module 10

Implementing File and Print Services

Contents:

Lesson 1: Securing Files and Folders 2

Lesson 2: Protecting Shared Files and Folders by Using Shadow Copies 4

Lesson 3: Configuring Work Folders 6

Lesson 4: Configuring Network Printing 9

Module Review and Takeaways 12

Lab Review Questions and Answers 13

Lesson 1
Securing Files and Folders

Contents:

Demonstration: Creating and Configuring a Shared Folder 3

Demonstration: Creating and Configuring a Shared Folder

Demonstration Steps

Create a shared folder

1. Sign in to LON-SVR1 as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. On the taskbar, click the **File Explorer** icon.
3. In File Explorer, in the navigation pane, expand **This PC**, and then click **Allfiles (E:)**.
4. On the menu toolbar, click **Home**, click **New folder**, type **Data**, and then press Enter.
5. Right-click the **Data** folder, and then click **Properties**.
6. In the **Data Properties** dialog box, click the **Sharing** tab, and then click **Advanced Sharing**.
7. In the **Advanced Sharing** dialog box, select **Share this folder**, and then click **Permissions**.

Assign permissions for the shared folder

1. In the **Permissions for Data** dialog box, click **Add**.
2. Type **Authenticated Users**, click **Check names**, and then click **OK**.
3. In the **Permissions for Data** dialog box, click **Authenticated Users**, and then under **Allow**, select **Change** permission.
4. Click **OK** to close the **Permissions for Data** dialog box.
5. Click **OK** to close the **Advanced Sharing** dialog box.
6. Click **Close** to close the **Data Properties** dialog box.

Configure access-based enumeration

1. On the taskbar, click the **Server Manager** icon.
2. In Server Manager, in the navigation pane, click **File and Storage Services**.
3. On the **File and Storage Services** page, in the navigation pane, click **Shares**. You may need to refresh the view to see the Shares.
4. In the Shares pane, right-click **Data**, and then click **Properties**.
5. In the **Data Properties** dialog box, click **Settings**, and then select **Enable access-based enumeration**.
6. Click **OK** to close the **Data Properties** dialog box.
7. Close Server Manager.

Configure Offline Files

1. In File Explorer, navigate to drive **E**, right-click the **Data** folder, and then click **Properties**.
2. In the **Data Properties** dialog box, click the **Sharing** tab, click **Advanced Sharing**, and then click **Caching**.
3. In the **Offline Settings** dialog box, select **No files or programs from the shared folder are available offline**, and then click **OK**.
4. Click **OK** to close the **Advanced Sharing** dialog box.
5. Click **Close** to close the **Data Properties** dialog box.

Lesson 2
Protecting Shared Files and Folders by Using Shadow Copies

Contents:

Demonstration: Restoring Data from a Shadow Copy 5

Demonstration: Restoring Data from a Shadow Copy

Demonstration Steps

Configure shadow copies

1. On LON-SVR1, on the taskbar, click the **File Explorer** icon.
2. In File Explorer, right-click **Local Disk (C:)**, and then click **Configure Shadow Copies**.
3. In the **Shadow Copies** dialog box, click **C:\**, and then click **Enable**.
4. In the **Enable Shadow Copies** dialog box, click **Yes**.
5. Click **OK**.

Create a new file

1. In File Explorer, browse to drive C, and then click the **New folder** icon on the Quick Launch toolbar.
2. Name the new folder **Data**, and then press Enter.
3. Browse to the **Data** folder on drive C.
4. In the Data folder, right-click an empty space, point to **New**, and then click **Text Document**.
5. Name the new text document **TestFile**, and then press Enter.
6. Double-click **TestFile.txt** to open the document.
7. In Notepad, type **Version 1**.
8. Close Notepad, and then click **Save** to save the changes.

Create a shadow copy

1. In File Explorer, right-click **Local Disk (C:)**, and then click **Configure Shadow Copies**.
2. In the **Shadow Copies** dialog box, click **Create Now**.
3. When the shadow copy is complete, click **OK**.

Modify the file

1. In File Explorer, double-click **TestFile.txt**.
2. In Notepad, type **Version 2**.
3. Close Notepad, and then click **Save** to save the changes.

Restore the previous version

1. In File Explorer, in the Data folder, right-click **TestFile.txt**, and then click **Restore previous versions**.
2. In the **TestFile.txt Properties** dialog box, on the **Previous Versions** tab, click the most recent file version, and then click **Restore**.
3. In the **Are you sure you want to restore** message, click **Restore**.
4. Click **OK** to close the success message.
5. Click **OK** to close the **TestFile.txt Properties** dialog box.
6. Double-click **TestFile.txt** to open the document, and then verify that the previous version is restored.
7. Close all open windows.

Lesson 3
Configuring Work Folders

Contents:

Resources 7
Demonstration: How to Configure Work Folders 7

Resources

Configuring Work Folders

Additional Reading: For more information about certificates for Work Folders, refer to "Work Folders Certificate Management" at http://go.microsoft.com/fwlink/?LinkID=331094.

Demonstration: How to Configure Work Folders

Demonstration Steps

Install the Work Folders role service

1. On LON-SVR1, in Server Manager click **Add roles and features**.
2. In the Add Roles and Features Wizard, click **Next**.
3. On the **Select installation type** page, click **Next**.
4. On the **Select destination server** page, click **Next**.
5. On the **Select server roles** page, expand **File and Storage Services (2 of 12 installed)**, and then expand **File and iSCSI Services (1 of 11 installed)**.
6. Select **Work Folders**, click **Add Features**, and then click **Next**.
7. On the **Select features** page, click **Next**.
8. On the **Confirm installation selections** page, click **Install**.
9. When the installation completes, click **Close**.

Create a sync share on a file server

1. In Server Manager, click **File and Storage Services**, and then click **Work Folders**.
2. In the details pane, click the **Tasks** drop-down arrow, and then click **New Sync Share**.
3. In the New Sync Share Wizard, click **Next**.
4. On the **Select the server and path** page, ensure that **LON-SVR1** is selected, click **Select by file share**, and then click **Next**.

   This procedure uses the shared folder Data which was created in the demonstration "Creating and Configuring a Shared Folder".
5. On the **Specify the structure for user folders** page, click **Next**.
6. On the **Enter the sync share name** page, type **WorkFolders**, and then click **Next**.
7. On the **Grant sync access to groups** page click **Add**.
8. In the **Select User or Group** dialog box, type **Domain Users**, click **OK**, and then click **Next**.
9. On the **Specify device policies** page click **Next**.
10. On the **Confirm selections** page, click **Create**, and then click **Close** when complete.

Configure Work Folder access on a Windows 8.1 client

1. Sign in to **LON-CL1** as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. On the **Start** screen, click **Desktop**.
3. On the taskbar, click the **File Explorer** icon.

4. Navigate to **C:\Labfiles\Mod10**, and then double-click **WorkFolders.bat**.

   This batch file adds a registry entry that allows unsecured connections to work folders.

5. Close File Explorer.
6. In the lower-left corner of the screen, right-click **Start**, and then click **Control Panel**.
7. Click **System and Security**, and then click **Work Folders**.
8. In the **Work Folders** dialog box, click **Set up Work Folders**, and then click **Enter a Work Folders URL instead**.
9. On the **Enter a Work Folders URL** page, type **http://lon-svr1.adatum.com**, and then click **Next**.

   Normally this requires a secure connection.

10. On the **Introducing Work Folders** page, click **Next**.
11. On the **Security policies** page, select the check box to accept the policies, and then click **Set up Work Folders**.
12. Close the **Work Folders** dialog box, and then on the taskbar, click the **File Explorer** icon.

    Notice there is now a **Work Folders** folder under the **This PC** folder.

Create a file in the work folder

1. Double-click the **Work Folders** icon to open the folder.
2. Right-click a blank space in the details, click **New>Text Document**, and then press Enter.

Synchronize data on a second client computer

1. Sign in to **LON-CL2** as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. On the Start screen, click **Desktop**.
3. Right-click the **Start** charm, and then click **Network Connections**.
4. Right-click the **Ethernet 2** adapter, and then click **Enable**.
5. Close Network Connections.
6. Repeat steps 4 through 12 from the **Configure Work Folder access on a Windows 8.1 client** task.
7. Open the **Work Folders** folder, and then notice the file that you created is available from this computer**.**
8. Close all open windows.
9. On the host computer, open **Hyper-V manager**, and then locate 20410D-LON-CL2. Right-click the virtual machine, and then click **Revert**.

Lesson 4
Configuring Network Printing

Contents:

Resources 10
Demonstration: Creating Multiple Configurations for a Print Device 10

Resources

Benefits of Network Printing

Additional Reading: For more information about managing printers, refer to "Print Management Step-by-Step Guide" at http://go.microsoft.com/fwlink/?LinkID=331093.

Demonstration: Creating Multiple Configurations for a Print Device

Demonstration Steps

Create a shared printer

1. On LON-SVR1, in the lower-left corner of the screen, click the **Start** button
2. In the **Start** box, type **Devices**, and then click **Devices and Printers**.
3. In the Devices and Printers window, click **Add a printer**.
4. In the Add Printer Wizard, on the **Select a Printer** page, click **The printer that I want isn't listed**.
5. Click **Add a local printer or network printer with manual settings**, and then click **Next**.

   Other connections options are also available in this dialog box.
6. Click **Use an existing port**, ensure that **LPT1: (Printer Port)** is selected, and then click **Next**.

   You can create other ports here manually, including TCP/IP, for network-connected printers.
7. Leave the driver choice as the default, and then click **Next**.
8. Change the printer name to **AllUsers**, and then click **Next** to finish the printer installation.
9. On the **Printer Sharing** page, ensure that the printer is shared, and then click **Next**.
10. Click **Finish** to close the Add Printer Wizard.

Create a second shared printer on the same port

1. In the Devices and Printers window, click **Add a printer**.
2. In the Add Printer Wizard, on the **Select a Printer** page, click **The printer that I want isn't listed**.
3. Click **Add a local printer or network printer with manual settings**, and then click **Next**.
4. On the **Choose a printer port** page, click **Next**.

   This is the same port that you selected for the printer you created in the previous task.
5. On the **Install the printer driver** page, click **Next** to accept the default selection.

   This is the same printer driver that you used for the printer you created in the previous task.
6. On the **Which version of the driver do you want to use** page, click **Next** to reuse the same printer driver.
7. On the **Type a printer name** page, in **Printer name**, type **Executives**, and then click **Next**.
8. On the **Printer Sharing** page, click **Next** to share the printer with the default settings.
9. On the **You've successfully added Executives** page, click **Finish**.
10. In the Devices and Printers window, review the list of devices.

    Notice that only the Executives printer displays.

Increase printing priority for a high priority print queue

1. In the Devices and Printers window, right-click **Executives**, point to **Printer properties**, and then click **Executives**.

2. On the **Advanced** tab, in **Priority**, type **10**, and then click **OK**.

   Now jobs that are submitted to the Executives printer have higher priority that those submitted to the AllUsers printer, and will be printed first.

Module Review and Takeaways

Review Question(s)

Question: How does inheritance affect explicitly assigned permissions on a file?

> **Answer:** While inherited permissions accumulate with explicit permissions, explicitly assigned permissions always take precedence over inherited permissions.

Question: Why should you not use shadow copies as a means for data backup?

> **Answer:** While shadow copies can store copies of files and protect against issues such as accidental deletion, they are reliant on the local files system and Windows Server 2012 for their functionality. Hard drive corruption, or destruction of the local machine, renders shadow copies useless in a disaster-recovery situation.

Question: In which scenarios could Branch Office Direct Printing be beneficial?

> **Answer:** You should use Branch Office Direct Printing if the WAN connection between a printer and a print server is slow or unreliable. When clients are in the same physical location as the printer, and they use Branch Office Direct Printing, documents are printed quicker and network bandwidth is freed up because print jobs are sent from the client computer directly to the printer and not to the central server and then back to the branch office printer.

Tools

Tool	Used for	Where to find it
Effective Access Tool	Assessing combined permissions for a file, folder, or shared folder.	Under Advanced, on the Security tab of the Properties dialog box of a file, folder or shared folder.
net share command-line tool	Configuring Windows Server 2012 networking components.	Command Prompt window.
Print Management console	Managing the print environment in Windows Server 2012.	The Tools menu in Server Manager.

Lab Review Questions and Answers

Lab: Implementing File and Print Services

Question and Answers

Question: How does implementing access-based enumeration benefit the users of the Data shared folder in this lab?

> **Answer:** With access-based enumeration, users see only the folders for their department, so it is easier to navigate within the folder structure. Access-based enumeration also increases the network's security because users cannot see any folders and files for which they do not have permissions.

Question: Is there another way you could recover the file in the shadow copy exercise? What benefit do shadow copies provide in comparison?

> **Answer:** Within the lab itself, the user could recover the file from the Recycle Bin. However, in a real-world scenario, the Recycle Bin is not available for network shared folders. The file would have to be recovered from a backup if shadow copies were not available.
>
> In comparison, shadow copies maintain multiple, persistent copies of modified files that an administrator or end user can recover.

Question: In Exercise 3, how could you configure Branch Office Direct Printing if you were in a remote location and did not have access to the Windows Server 2012 GUI for the print server?

> **Answer:** You could configure Branch Office Direct Printing by using Windows PowerShell to connect remotely from a Windows 8 or Windows Server 2012 computer. Then, you could use the **Set-Printer** cmdlet to change the configuration.

Module 11

Implementing Group Policy

Contents:

Lesson 1: Overview of Group Policy 2

Lesson 2: Group Policy Processing 4

Module Review and Takeaways 7

Lab Review Questions and Answers 9

Lesson 1
Overview of Group Policy

Contents:

Demonstration: Creating and Managing GPOs 3

Demonstration: Creating and Managing GPOs

Demonstration Steps

Create a GPO by using the GPMC

1. Sign in to **LON-DC1** as **Administrator** with the password **Pa$$w0rd**.
2. In Server Manager, click **Tools**, and then click **Group Policy Management**.
3. In the Group Policy Management Console (GPMC), expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, right-click the **Group Policy Objects** folder, and then click **New**.
4. In the **New GPO** dialog box, in the **Name** field, type **Prohibit Windows Messenger**, and then click **OK**.

Edit a GPO in the Group Policy Management Editor window

1. Click the **Group Policy Objects** node, right-click the **Prohibit Windows Messenger** GPO, and then click **Edit**.
2. In the Group Policy Management Editor window, under **User Configuration**, expand **Policies**, expand **Administrative Templates**, expand **Windows Components**, and then click **Windows Messenger**.
3. In the details pane, double-click the **Do not allow Windows Messenger to be run** setting.
4. Click **Enabled**, and then click **OK**.
5. Close the **Group Policy Management Editor** window.
6. Right-click the **Adatum.com** domain, and then click **Link an Existing GPO**.
7. In the **Select GPO** dialog box, click **Prohibit Windows Messenger**, and then click **OK**.
8. Minimize the GPMC.

Use Windows PowerShell® to create a GPO named Desktop Lockdown

1. On the taskbar, click the **Windows PowerShell** icon.
2. At the Windows PowerShell prompt, type the following, and then press Enter:

   ```
   New-GPO -Name "Desktop Lockdown"
   ```

3. Close Windows PowerShell.
4. Restore the GPMC from the taskbar.
5. Right-click the **Group Policy Objects** folder, and then click **Refresh** to refresh the view. You should see the new Desktop Lockdown GPO.
6. Minimize the GPMC.

Lesson 2
Group Policy Processing

Contents:

Question and Answers 5
Demonstration: Using Group Policy Diagnostic Tools 6

Question and Answers

Discussion: Identifying Group Policy Application

Question: What power options will the servers in the Servers OU receive?

> **Answer:** They will receive the power options from GPO4, because it is applied after the domain-level GPOs.

Question: What power options will the laptops in the Sales Laptops OU receive?

> **Answer:** They will receive the power options from GPO3, because it is applied after the domain-level GPOs.

Question: What power options will all other computers in the domain receive?

> **Answer:** They will receive the domain-level policy.

Question: Will users in the Sales Users OU who have created local policies to grant access to Control Panel be able to access Control Panel?

> **Answer:** No. Local settings are applied first, and are overwritten by domain and OU policies. Therefore, a local policy will not reverse a domain setting.

Question: If you needed to grant access to Control Panel to some users, how would you do it?

> **Answer:** You would create a Group Policy that specifically grants access specifically to Control Panel. You then would use security filtering to apply it to the correct group of users, and assign it a preference order that ensures that it is the last policy applied.

Question: Can you apply GPO2 to other department OUs?

> **Answer:** Yes. By linking GPO2 to other containers, those users will receive the GPO2 settings.

Demonstration: Using Group Policy Diagnostic Tools

Demonstration Steps

Use Gpupdate to refresh Group Policy

1. On LON-DC1, on the taskbar, click the **Windows PowerShell** icon.
2. In Windows PowerShell, at the command prompt, type the following, and then press Enter:

```
Gpupdate
```

Use the Gpresult cmdlet to output the results to an HTML file

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

```
Gpresult /H c:\Gpresult.html
```

2. On the taskbar, click the **File Explorer** icon.
3. In the File Explorer window, expand **Computer**, and then click **Local Disk (C:)**.
4. Double-click the **Gpresult.html** file and review the results.
5. In the Gpresult.html file, scroll down to the User Details section, note that the “Do not allow Windows Messenger to be run” setting is Enabled, and then note that Winning GPO is the Prohibit Windows Messenger GPO.
6. Close the report.
7. Close File Explorer, and then close Windows PowerShell.

Use the Group Policy Modeling Wizard to test the policy

1. From the taskbar, restore the GPMC.
2. Right-click **Group Policy Modeling**, and then click **Group Policy Modeling Wizard**.
3. In the Group Policy Modeling Wizard, on the **Welcome** page, click **Next**.
4. On the **Domain Controller Selection** page, click **Next**.
5. On the **User and Computer Selection** page, in the User information section, click **Browse**.
6. Expand **Adatum**, click the **Managers** OU, click **OK**, and then click **Next**.
7. On the **Advanced Simulation Options** page, click **Next**.
8. On the **User Security Groups** page, click **Next**.
9. On the **WMI Filters for Users** page, click **Next**.
10. On the **Summary of Selections** page, click **Next**, and then click **Finish**.
11. Click the **Details** tab of the report, and then point out some of the results.

Module Review and Takeaways

Best Practices

The following are recommended best practices:

- Do not use the Default Domain and Default Domain Controllers policies for uses other than their default uses. Instead, create new policies.
- Limit the use of security filtering and other mechanisms that make diagnostics more complex.
- If they have no settings configured, disable the User or Computer sections of policies.
- If you have multiple administration workstations, create a central store.
- Add comments to your GPOs to explain what the policies are doing.
- Design your OU structure to support Group Policy application.

Review Question(s)

Question: What are some of the advantages and disadvantages of using site-level GPOs?

> **Answer:** One advantage of using a site-level GPO is that all the users or computers in a site can have GPO settings applied regardless of the domain to which they belong. For example, you might want to configure the Internet Explorer proxy settings for all computers in a given site, whether they belong to your root domain or to a child domain.
>
> One disadvantage of using a site-level GPO is that troubleshooting might be difficult because the GPO can be applied to systems from multiple domains.
>
> Another disadvantage of using a site-level GPO is that the GPO must be created in a domain, and then linked to the site. Site-based computers must then pull that GPO from a domain controller in the domain in which the GPO was created, which could lead to excessive wide area network (WAN) traffic.

Question: You have a number of logon scripts that map network drives for users. Not all users need these drive mappings, so you must ensure that only the desired users receive the mappings. You want to move away from using scripts. What is the best way to map network drives for selected users without using scripts?

> **Answer:** You can use Group Policy preferences to map network drives without using scripts for selected users. In Group Policy preferences, select the option to configure drive mapping, and then use Preferences Targeting to distribute the mappings to the appropriate users.

Tools

Tool	Use	Where to find it
Group Policy Management Console (GPMC)	Controls all aspects of Group Policy	In Server Manager, on the Tools menu
Group Policy Management Editor snap-in	Configure settings in GPOs	Accessed by editing any GPO
Resultant Set of Policy (RSoP)	Determine what settings are applying to a user or computer	In the GPMC

Tool	Use	Where to find it
Group Policy Modeling Wizard	Test what would occur if settings were applied to users or computers, prior to actually applying the settings	In the GPMC
Local Group Policy Editor	Configure Group Policy settings that apply only to the local computer	Accessed by creating a new Microsoft Management Console (MMC) on the local computer, and adding the Group Policy Management Editor snap-in

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
A user is experiencing abnormal behavior on their workstation.	Use the RSoP tools to determine what settings are applied to the client workstation.
All users in a particular OU are having issues, and the OU has multiple GPOs applied.	Disable the GPO links one by one, and then test the workstations to see if one of the GPOs is responsible for the issue.

Lab Review Questions and Answers

Lab: Implementing Group Policy

Question and Answers

Question: What is the difference between ADMX and ADML files?

> **Answer:** ADMX files contain the registry location that will be modified by a setting, and ADML files provide the language-specific UI for the setting that is viewed in the Group Policy Management Editor window.

Question: The Sales Managers group should be exempted from the desktop lockdown policy that is being applied to the entire Sales OU. All sales user accounts and sales groups reside in the Sales OU. How would you exempt the Sales Managers group?

> **Answer:** You would use security filtering to deny access to the policy for the Sales Managers group.

Question: What Windows command can you use to force the immediate refresh of all GPOs on a client computer?

> **Answer:** You would use the Windows command, **Gpupdate /force**, to force the refresh.

Module 12

Securing Windows Servers Using Group Policy Objects

Contents:

Lesson 1: Security Overview for Windows Operating Systems 2

Lesson 2: Configuring Security Settings 4

Lesson 3: Restricting Software 6

Lesson 4: Configuring Windows Firewall with Advanced Security 9

Module Review and Takeaways 12

Lab Review Questions and Answers 14

Lesson 1
Security Overview for Windows Operating Systems

Contents:

Question and Answers 3
Resources 3

Question and Answers

Applying Defense-In-Depth to Increase Security

Question: How many layers of the defense-in-depth model should you implement in your organization?

Answer: You should implement all layers of the defense-in-depth model, to some extent. You should base the actual measures that you implement on your organization's needs and budget.

Resources

Additional Reading:

- For the latest Microsoft security bulletin and advisory information, refer to "Security for IT Pros" at http://go.microsoft.com/fwlink/?LinkID=266741.
- For more information about common types of network attacks, refer to http://go.microsoft.com/fwlink/?LinkID=266742.

Best Practices for Increasing Security

Additional Reading: For more information about best practices for enterprise security, refer to the articles about Windows Server Security at http://go.microsoft.com/fwlink/?LinkID=392100.

Lesson 2
Configuring Security Settings

Contents:

Resources 5

Resources

Additional Reading: For a detailed list of Group Policy settings, refer to "Group Policy Settings Reference for Windows and Windows Server" at http://go.microsoft.com/fwlink/?LinkID=266744.

Configuring Security Auditing

Additional Reading: For more information about security auditing, refer to "What's New in Security Auditing" at http://go.microsoft.com/fwlink/?LinkID=266747.

Configuring Restricted Groups

Additional Reading: For more information about Restricted Groups policies, refer to "Description of Group Policy Restricted Groups" at http://go.microsoft.com/fwlink/?LinkID=392101.

Lesson 3
Restricting Software

Contents:

Resources	7
Demonstration: Creating AppLocker Rules	7

Resources

What Is AppLocker?

Additional Reading: For more information about AppLocker, refer to "AppLocker overview" at http://go.microsoft.com/fwlink/?LinkID=266745.

Demonstration: Creating AppLocker Rules

Demonstration Steps

Create a GPO to enforce the default AppLocker Executable rules

1. On LON-DC1, in Server Manager, click **Tools**, and then click **Group Policy Management**.
2. In GPMC, go to **Forest: Adatum.com\Domains\Adatum.com**.
3. Click **Group Policy Objects**, right-click **Group Policy Objects**, and then click **New**.
4. In the New GPO window, in **Name**, type **WordPad Restriction Policy**, and then click **OK**.
5. Right-click **WordPad Restriction Policy**, and then click **Edit**.
6. In the Group Policy Management Editor window, go to **Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies\AppLocker**.
7. Click **Executable Rules**, right-click **Executable Rules**, and then select **Create New Rule**.
8. On the **Before You Begin** page, click **Next**.
9. On the **Permissions** page, click **Deny**, and then click **Next**.
10. On the **Conditions** page, click **Publisher**, and then click **Next**.
11. On the **Publisher** page, click **Browse**, and then click **Computer**.
12. On the **Open** page, double-click **Local Disk (C:)**.
13. On the **Open** page, double-click **Program Files**, double-click **Windows NT**, double-click **Accessories**, click **wordpad.exe**, and then click **Open**.
14. Move the slider up to the **File name** position, and then click **Next**.
15. Click **Next** again, and then click **Create**.
16. If prompted to create default rules, click **Yes**.
17. In the Group Policy Management Editor window, go to **Computer Configuration\Policies\Windows Settings\Security Settings**.
18. Expand **Application Control Policies**, right-click **AppLocker**, and then select **Properties**.
19. On the **Enforcement** tab, under Executable rules, select the **Configured** check box, click **Enforce rules**, and then click **OK**.
20. In the Group Policy Management Editor window, go to **Computer Configuration\Policies\Windows Settings\Security Settings**.
21. Click **System Services**, and then double-click **Application Identity**.
22. In the **Application Identity Properties** dialog box, above **Select service startup mode**, click **Define this policy setting**, then click **Automatic**, and then click **OK**.

23. Close the Group Policy Management Editor window.

Apply the GPO to the domain

1. In the Group Policy Management Console, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, and then expand **Group Policy Objects**.
2. In the Group Policy Management Console, right-click **Adatum.com**, and then click **Link an Existing GPO**.
3. In the Select GPO window, in the Group Policy Objects window, click **WordPad Restriction Policy**, and then click **OK**.
4. Close the Group Policy Management Console.
5. Switch to the **Start** screen, type **cmd**, and then press Enter.
6. In the Command Prompt window, type **gpupdate /force**, and then press Enter.

   Wait for the policy to update.

Test the AppLocker rule

1. Sign in to LON-CL1 as **Adatum\Alan** with the password **Pa$$w0rd**.
2. Point to the lower-right corner of the screen, and then click the **Search** charm when it appears.
3. In the **Search** box type **cmd**, and then press Enter.
4. In the Command Prompt window, type **gpupdate /force**, and then press Enter.

   Wait for the policy to update.

5. In the lower-left corner of the screen, click the **Start** button.
6. In the **Search** box type **WordPad**, and then press Enter.

   Notice that WordPad does not start.

Lesson 4
Configuring Windows Firewall with Advanced Security

Contents:

Demonstration: Implementing secured network traffic with Windows Firewall 10

Demonstration: Implementing secured network traffic with Windows Firewall

Demonstration Steps

Check to see if ICMP v4 is blocked

1. Sign in to LON-CL2 as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. On LON-CL2, click the **Desktop** tile, right-click the **Windows Start** menu, and then click **Command Prompt**.
3. At the command prompt, type **ping 10.10.0.11**, and then press Enter.

   Notice that the ping times out.

Enable ICMP v4 from LON-CL2 to LON-SVR2

1. Sign in to LON-SVR2 as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. On LON-SVR2, right-click the **Windows Start** menu, and then click **Control Panel**.
3. In Control Panel, click the **View by** drop-down menu, and then click **Small icons**.
4. Click **Windows Firewall**.
5. Click **Advanced settings**.
6. In the left-hand pane, click **Inbound Rules**.
7. In the right-hand pane, click **New Rule**.
8. On the New Inbound Rule Wizard, on the **Rule Type** page, click **Custom**, and then click **Next**.
9. On the **Program** page, click **Next**.
10. On the **Protocol and Ports** page, click the **Protocol type** drop-down menu, click **ICMPv4**, and then click **Next**.
11. In the **Which remote IP addresses does this rule apply to** section, click **These IP addresses**, and then click **Add**.
12. In the IP Address window, type **10.10.0.50** in the **This IP address or subnet** box, click **OK**, and then click **Next**.
13. On the **Action** page, click **Next** to accept the Allow the connection default action.
14. On the **Profile** page, click **Next** to accept the application of the rule for all profiles.
15. On the **Name** page, type **ICMPv4-Allow-From-10.10.0.50**, and then click **Finish**.
16. Switch to LON-CL2.
17. At the command prompt, type **ping 10.10.0.11**, and then press Enter.

    Notice that the ping goes through successfully.

Create a connection security rule

1. Switch to LON-SVR2.
2. In the Windows Firewall with Advanced Security window, in the left-hand pane, right-click **Connection Security Rules**, and then click **New Rule**.
3. On the **Rule Type** page, click **Next** to accept the default of **Isolation**.
4. On the **Requirements** page, click **Require authentication for inbound connections and request authentication for outbound connections**, and then click **Next**.

5. On the **Authentication Method** page, click **Advanced**, and then click **Customize**.
6. In the **Customize Advanced Authentication Method** dialog box, in the **First authentication** section, click **Add**.
7. In the **Add First Authentication Method** dialog box, click **Preshared key (not recommended)**, type **Pa$$w0rd** for the preshared key, and then click **OK**. Click **OK** again to close the dialog box.
8. On the **Authentication Method** page, click **Next**.
9. On the **Profile** page, click **Next**.
10. On the **Name** page, in **Name**, type **Require Inbound Authentication**, and then click **Finish**.
11. Repeat steps 2 through 10 on LON-CL2 before moving to the next demonstration section.

Validate ICMP v4

1. Switch to LON-CL2.
2. At the command prompt, type **ping 10.10.0.11**, and then press Enter.

   Notice that the ping goes through successfully.

Module Review and Takeaways

Best Practices

The following are best practices:

- Always make a detailed security risk assessment before planning which security features your organization should deploy.
- Create a separate GPO for security settings that apply to different type of users in your organization, because each department might have different security needs.
- Ensure that the security settings that you configure are reasonably easy to use so that employees accept them. Frequently, very strong security policies are too complex or difficult for employees to adopt.
- Always test security configurations that you plan to implement with a GPO in an isolated, nonproduction environment. Only deploy policies in your production environment after you complete this testing successfully.

Review Question(s)

Question: Does the defense-in-depth model prescribe specific technologies that you should use to protect Windows Server operating system servers?

Answer: No, you use the defense-in-depth model to organize your plans for defense. It does not prescribe specific technologies.

Question: What setting must you configure to ensure that users are allowed only three invalid sign-in attempts?

Answer: The account lockout threshold setting ensures that users are allowed only three invalid sign-in attempts.

Question: You are creating a GPO with standardized firewall rules for the servers in your organization. You tested the rules on a stand-alone server in your test lab. The rules appear on the servers after the GPO is applied, but they are not taking effect. What is the most likely cause of this problem?

Answer: The firewall rules are most likely not being applied to the correct firewall profile. It is possible that you did not apply them to the domain profile as is required for member servers. To test rules on a stand-alone server, you have to apply the rules to either the public or private firewall profiles.

Question: Last year, your organization developed a security strategy that included all aspects of a defense-in-depth model. Based on that strategy, your organization implemented security settings and policies on the entire IT infrastructure environment. Yesterday, you read in an article that new security threats were detected on the Internet, but now you realize that your company strategy does not include a risk analysis and mitigation plan for those new threats. What should you do?

Answer: You should immediately initiate a new risk assessment in your organization to help you develop a plan outlining how to address the new threats.

Additionally, ensure that your organization's security risk assessments and strategies are being evaluated and updated regularly. As technology evolves, security strategies change, so security best practices must also evolve. Organizations must be ready to protect their IT infrastructure from any new potential security threats.

Tools

Tool	Used for	Where to find it

Group Policy Management Console	A graphical tool that you use to create, edit, and apply GPOs	Server Manager\Tools
AppLocker	Applies security settings that control which applications users are allowed to run	Group Policy Management Editor snap-in
Windows Firewall with Advanced Security	A host-based firewall that is included as a feature in Windows Server 2008 and newer versions	Server Manager\Tools if configured individually, or Group Policy Management Editor snap-in for deploying with Group Policy
Security Compliance Manager	Deploying security policies based on Microsoft Security Guide recommendations and industry best practices	Download from the Microsoft website at http://go.microsoft.com/fwlink/?LinkID=266746.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
The user cannot sign in locally to a server.	First, verify that the user has the correct permissions to sign in locally, because company security regulations might be preventing it. If the user has the correct permissions, then change the appropriate GPO to allow the user to sign in locally on to that server.
After configuring auditing, there are too many events logged in the Security Event Log in Event Viewer.	Consider the following possible solutions: Increase the size of security event log. Evaluate the configuration of the audit settings. It may be that not all of the audit data is necessary. Use System Center Operations Manager 2012 to implement a solution for centralized management and monitoring of security events.
Some users complain that their business applications can no longer access resources on the server.	Check the rules that are configured in the Windows Firewall GPO for any misconfigurations. Ensure that all ports that are necessary for user business applications are open.

Lab Review Questions and Answers

Lab A: Increasing Security for Server Resources

Question and Answers

Question: What happens if you configure the Computer Administrators group, but not the Domain Admins group, to be a member of the Local Administrators group on all of a domain's computers?

> **Answer:** If you do not include the Domain Admins group in the Local Administrators group, Domain Admins will not be a member of the Local Administrators group on all of a domain's computers.

Question: Why do you need to restrict local logon to some computers?

> **Answer:** It is not a good security practice for every domain user to be able to log on to every domain computer. Typically, all servers, and some clients with sensitive local information or applications, should not allow all users to log on locally..

Question: What happens when an unauthorized user tries to access a folder that has auditing enabled for both successful and unsuccessful access attempts?

> **Answer:** An event is generated in the Event Viewer security log, with information about who has tried to access the folder and whether the attempt was successful.

Question: What happens when you configure auditing for domain logons for both successful and unsuccessful logon attempts?

> **Answer:** Events are generated in the Event Viewer security log, with information about who has tried to log on to the domain and whether the attempt was successful.

Lab B: Configuring AppLocker and Windows Firewall

Question and Answers

Question: You configured an AppLocker rule that prevents users from running software in a specified file path. How can you prevent users from moving the folder containing the software so that they can circumvent the rule and still run it?

> **Answer:** You can configure an AppLocker rule that is based on a file hash rather than a rule based on a file path.

Question: You want to introduce a new application that needs to use specific ports. What information do you need to configure Windows Firewall with Advanced Security, and from what source can you get it?

> **Answer:** You need to know which ports and IP addresses you need so that the application can run while still being protected from security threats. You can get this information from the application vendor.

Module 13

Implementing Server Virtualization with Hyper-V

Contents:

Lesson 1: Overview of Virtualization Technologies 2

Lesson 2: Implementing Hyper-V 4

Lesson 3: Managing Virtual Machine Storage 6

Lesson 4: Managing Virtual Networks 8

Module Review and Takeaways 10

Lab Review Questions and Answers 12

Lesson 1
Overview of Virtualization Technologies

Contents:

Resources 3

Resources

Server Virtualization

Best Practice: We recommend that you do not deploy a Microsoft Exchange mailbox server or a SQL Server 2012 database engine instance on a computer that hosts the domain controller role. Microsoft does support deploying each of these workloads on separate virtual machines that are running on the same virtual machine host.

Lesson 2
Implementing Hyper-V

Contents:

Resources 5

Resources

Virtual Machine Hardware

Additional Reading: For more information about virtual Fibre channel adapters, refer to “Hyper-V Virtual Fibre Channel Overview” at http://go.microsoft.com/fwlink/?LinkId=269712.

Generation 2 Virtual Machines

Additional Reading: For more information about generation 2 virtual machines, refer to “Generation 2 Virtual Machine Overview” at http://go.microsoft.com/fwlink/?LinkID=392187.

What Is Dynamic Memory?

Additional Reading: For more information about Hyper-V Dynamic Memory, refer to “Hyper-V Dynamic Memory Overview” at http://go.microsoft.com/fwlink/?LinkId=269713.

Hyper-V Resource Metering

Additional Reading: For more information about resource metering for Hyper-V, refer to “Hyper-V Resource Metering Overview” at http://go.microsoft.com/fwlink/?LinkId=269714.

What’s New with Hyper-V in Windows Server 2012 R2

Additional Reading: For more information, refer to “What’s New in Hyper-V in Windows Server 2012 R2” at http://go.microsoft.com/fwlink/?LinkID=331078.

Lesson 3
Managing Virtual Machine Storage

Contents:

Question and Answers 7

Resources 7

Question and Answers

Creating Virtual Disk Types

Question: Why might you consider using fixed virtual hard disks instead of dynamically expanding virtual hard disks?

> **Answer:** You might want to use fixed virtual hard disks instead of dynamically expanding virtual hard disks when:
>
> o You want to maintain control over the growth of virtual hard disks.
>
> o You want to pre-allocate storage.

Question: In what situations might you encounter difficulties if you use dynamically expanding disks?

> **Answer:** It is easy to place multiple dynamically expanding disks on the same volume. They can then grow and consume the volume.

Resources

What Is a Virtual Hard Disk?

Additional Reading: For more information about virtual hard disk formats, refer to "Hyper-V Virtual Hard Disk Format Overview" at http://go.microsoft.com/fwlink/?LinkId=269715.

Additional Reading: For more information about virtual hard disk sharing, refer to http://go.microsoft.com/fwlink/?LinkID=331079.

Additional Reading: For more information about the storage quality of service for Hyper-V, see refer to http://go.microsoft.com/fwlink/?LinkID=331080.

Lesson 4
Managing Virtual Networks

Contents:

Resources 9

Resources

What Is a Virtual Switch?

Additional Reading: For more information about virtual switches, refer to “Hyper-V Virtual Switch Overview” at http://go.microsoft.com/fwlink/?LinkId=269716.

Virtual Switch Extensions

Additional Reading: For more information about virtual switch extensions, refer to “Hyper-V Virtual Switch Overview” at http://go.microsoft.com/fwlink/?LinkID=331084.

Module Review and Takeaways

Best Practices

When implementing server virtualization with Hyper-V, use the following best practices:

- Ensure that the processor on the computer that will run Hyper-V supports hardware assisted virtualization.
- Ensure that you provision a virtualization server with adequate RAM. Having multiple virtual machines paging the hard disk drive because they have inadequate memory decreases performance for all virtual machines on the server.
- Monitor virtual machine performance carefully. A virtual machine that uses a disproportionate amount of server resources can reduce the performance of all other virtual machines that the same virtualization server is hosting.

Review Question(s)

Question: In which situations should you use a fixed memory allocation instead of Dynamic Memory?

Answer: You should use fixed memory allocation when the:

- Guest operating system does not support Dynamic Memory.
- Management operating system has limited memory resources, and you need to ensure balanced allocation of memory to the operating systems.

Question: In which situations must you use virtual hard disks with the new .vhdx format, instead of virtual hard disks with the old .vhd format?

Answer: You should use virtual hard disks with the new .vhdx format rather than virtual hard disks with the old .vhd format when you need to:

- Support virtual hard disks larger than 2 TB. Virtual hard disks with the new .vhdx format can be a maximum of 64 TB, while virtual hard disks with the old .vhd format are limited to 2 TB.
- Protect against data corruption that power failures cause. Virtual hard disks with the new .vhdx format are less likely to become corrupt if an unexpected power failure occurs, because of how the file format processes updates.
- Deploy a virtual hard disk to a large sector disk.

Question: You want to deploy a Windows Server 2012 Hyper-V virtual machine's virtual hard disk on a file share. What operating system must the file server be running to support this configuration?

Answer: You can only deploy virtual hard disks to file shares that support SMB 3.0, and only the Windows Server 2012 operating system supports hosting of SMB 3.0 file shares.

Tools

You can use the following tools with Hyper-V to deploy and manage virtual machines.

Name of tool	Used for	Where to find it
Sysinternals disk2vhd tool	Use to convert physical hard disks to virtual hard disk format.	Microsoft TechNet website.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Cannot deploy Hyper-V on an x64 platform.	Check if the processor supports hardware-assisted virtualization.
Virtual machine does not use Dynamic Memory.	The operating system may not support Dynamic Memory. In some non-Microsoft operating systems, applying a service pack or installing virtual machine integration services resolves this issue.

Lab Review Questions and Answers

Lab: Implementing Server Virtualization with Hyper-V

Question and Answers

Question: What type of virtual network switch would you create if you want to allow the virtual machine to communicate with the LAN that is connected to the Hyper-V virtualization server?

> **Answer:** You would create an external virtual network switch.

Question: How can you ensure that no single virtual machine uses all of the available bandwidth that the Hyper-V virtualization server provides?

> **Answer:** You would configure maximum and minimum bandwidth settings on virtual network adapters.

Question: What Dynamic Memory configuration task was not possible on previous versions of Hyper-V, but which you can now perform on a virtual machine that is hosted on the Hyper-V role on a Windows Server 2012 server?

> **Answer:** You can modify some Dynamic Memory settings while the virtual machine is running on Hyper-V. You could not do this in previous Hyper-V versions.