
OFFICIAL MICROSOFT LEARNING PRODUCT

20410B

Installing and Configuring Windows Server® 2012

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

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

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

© 2012 Microsoft Corporation. All rights reserved.

Microsoft and the trademarks listed at <http://www.microsoft.com/about/legal/en/us/IntellectualProperty/Trademarks/EN-US.aspx> are trademarks of the Microsoft group of companies. All other trademarks are property of their respective owners

Product Number: 20410B

Released: 12/2012

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 silver or gold-level 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 Programs and Services.** The Licensed Content may contain third party programs or services. These license terms will apply to your use of those third party programs or services, unless other terms accompany those programs and services.

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 software, 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 software, 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 des consommateurs, que ce contrat ne peut modifier. La ou elles sont permises par le droit local, 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 September 2012

Module 1

Deploying and Managing Windows Server 2012

Contents:

Lesson 1: Windows Server 2012 Overview	2
Lesson 2: Overview of Windows Server 2012 Management	4
Lesson 3: Installing Windows Server 2012	7
Lesson 4: Post-Installation Configuration of Windows Server 2012	9
Lesson 5: Introduction to Windows PowerShell	11
Module Review and Takeaways	13
Lab Review Questions and Answers	14

Lesson 1

Windows Server 2012 Overview

Contents:

Question and Answers	3
Additional Reading	4

Question and Answers

On-Premises Servers

Question: What is the difference between a server and a client operating system?

Answer: The difference between a server and a client operating system is that a *server* provides resources to many users on a network, and a *client operating system* is used by only one user at a time.

Question: How has the role of the server evolved over time from the Microsoft Windows NT 4.0 Server operating system to Windows Server 2012?

Answer: Answers will vary. Solicit class discussion about their experience with different versions of Windows Server.

What Is Cloud Computing?

Question: Which type of cloud would you use to deploy a custom virtual machine running Windows Server 2012?

Answer: You would deploy a custom virtual machine to an IaaS cloud, which could be either a public cloud or a private cloud.

Windows Server 2012 Roles

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

Answer: Answers may 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.

Additional Reading

Windows Server 2012 Editions



Additional Reading: For more information about the differences between Windows Server 2012 editions, see the Windows Server Catalog at <http://go.microsoft.com/fwlink/?LinkID=266736>.

Lesson 2

Overview of Windows Server 2012 Management

Contents:

Question and Answers	6
Demonstration	6

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

Demonstration: Using Server Manager

Demonstration Steps

Sign in to Windows Server 2012 and view the Windows Server 2012 desktop

1. Sign in to server **LON-DC1** with the **Adatum\Administrator** account and the password **Pa\$\$w0rd**.
2. Click **Close** to close the Server Manager console.

Add a feature by Using the Add Roles and Features Wizard

1. On the Windows Server 2012 taskbar, click the **Server Manager** icon.
2. In the Server Manager console, click **Manage**, and then click **Add Roles and Features**.
3. In the Add Roles and Features Wizard, on the **Before you begin** page, click **Next**.
4. On the **Select Installation Type** page, select the **Role-based or featured-based installation** check box, and then click **Next**.
5. 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**.
6. On the **Select server roles** page, select **Fax Server**.
7. In the **Add Roles and Features Wizard** dialog box that opens, click **Add Features**. 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.



Note: 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. On the **DNS - Events Detail View**, 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. Hold down the **Alt** and **Home** keys to open the Start menu.

Sign out the currently signed-in user

1. In the Start menu, 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 15
```

Lesson 3

Installing Windows Server 2012

Contents:

Question and Answers	10
Additional Reading	10

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

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.

Additional Reading

Hardware Requirements for Windows Server 2012



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

Lesson 4

Post-Installation Configuration of Windows Server 2012

Contents:

Question and Answers

12

Question and Answers

Performing an Offline Domain Join

Question: In what situation would you perform an offline domain join rather than a traditional domain join?

Answer: You would you perform an offline domain join when deploying a server to a remote site with intermittent network connectivity.

Lesson 5

Introduction to Windows PowerShell

Contents:

Demonstration

12

Demonstration

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, execute the following command:

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

3. To view all the commands that are related to managing services, at the Windows PowerShell prompt, execute the following command:

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

4. To view a list of running processes on the server, at the Windows PowerShell prompt, execute the following command:

```
Get-Process
```

5. To view all the commands that are related to managing processes, at the Windows PowerShell prompt, execute the following command:

```
Get-Help Process
```

6. To view detailed information about the **Start-Process** cmdlet, at the Windows PowerShell prompt, execute the following command:

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

7. 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.

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 will demonstrate 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**.

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 allows you to spend more time planning and performing troubleshooting tasks.

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

Answer: The advantages 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: The Volume Activation Services role allows you to manage KMS.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
WinRM connections fail.	Verify firewall settings. Verify WinRM configuration.
Windows PowerShell cmdlets 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 files, and use the Install-WindowsFeature cmdlet -source option.
Unable to restart a computer 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: What IP address range is used by the computers in the lab?

Answer: The IP address range used by the computers in the lab 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 allows the computer to locate the Domain Controller when performing 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 %computename% /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:

Additional Reading

3

Additional Reading

Overview of AD DS



Additional Reading: For more information about domains and forests, see Domains and Forests Technical Reference at <http://go.microsoft.com/fwlink/?LinkId=104447>.

Lesson 2

Overview of Domain Controllers

Contents:

Question and Answers	5
Additional Reading	5
Demonstration	6

Question and Answers

Question: Why would you make a domain controller a global catalog server?

Answer: Queries that are directed at the forest (rather than the domain) need to be directed to a global catalog server. This is because a domain controller that is not a global catalog only holds information about the objects in its own domain. As a best practice, you should configure every domain controller to be a global catalog, even in a single domain forest.

What Is the Global Catalog?

Question: Should a domain controller be a global catalog?

Answer: Every domain controller should be a global catalog. (In some extreme situations, there might be a reason not to do so.) However, most large, distributed organizations are doing just that, so it also makes sense for less complex, smaller organizations.

Additional Reading

What Are Operations Masters?



Additional Reading: For more information about operations master roles, see Operations master roles at <http://go.microsoft.com/fwlink/?LinkID=266738>.

Demonstration

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 tree menu, expand **LON-DC1**, expand **Forward Lookup Zones**, expand **adatum.com**, and 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 the 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:

Question and Answers	9
Additional Reading	9

Question and Answers

Question: What is the reason to specify the Directory Services Restore Mode password?

Answer: If the AD DS database must be restored from backup, the domain controller must be restarted into Directory Services Restore Mode. You then must use the Directory Services Restore Mode password to log on to the domain controller when it starts in Directory Services Restore Mode.

Additional Reading

Installing a Domain Controller by Using Install from Media



Additional Reading: For more information about the steps necessary to install AD DS, see *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 deployment of GPOs.

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

Answer: You would want to 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 would allow you to install AD DS remotely
- Windows PowerShell 3.0
- Run the command **dcpromo /unattend** on the Server Core server

Lab Review Questions and Answers

Lab: Installing Domain Controllers

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

Answer: In Windows Server® 2012, dcpromo.exe is deprecated and its uses are limited. For example, it is only used at a command prompt, such as to perform an unattended installation of AD DS, or when it is necessary to do a complete domain controller promotion from a command-line interface. Server Manager is the preferred tool to use, or you can use Windows PowerShell® or some other scripted method.

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

Answer: The three operations masters are:

- Relative ID (RID) masters
- Infrastructure master
- Primary domain controller (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 Install From Media (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 Group Accounts	4
Lesson 4: Delegating Administration	6
Module Review and Takeaways	9
Lab Review Questions and Answers	12

Lesson 1

Managing User Accounts

Contents:

Additional Reading

3

Demonstration

4

Additional Reading

AD DS Administration Tools



Additional Reading: To download the RSAT installation files, see the Microsoft Download Center at <http://go.microsoft.com/fwlink/?LinkID=266735>.

Demonstration

Demonstration: Managing User Accounts

Demonstration Steps

Open the Active Directory Users Administrative Center

1. Sign in to LON-DC1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. On LON-DC1, in the **Server Manager**, click **Tools**.
3. Click **Active Directory Administrative Center**.
4. In the Active Directory Administrative Center, expand **Adatum (local)**, and then click **Managers**.

Delete a user account

1. In Managers, right-click **Ed Meadows**, and then click **Delete**.
2. 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 the **Full name** box, type **Ed Meadows**.
3. In the **User UPN logon** box, type **Ed**.
4. In the **Password** and **Confirm password** boxes, 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.

Lesson 2

Managing Group Accounts

Contents:

Demonstration

7

Demonstration

Demonstration: Managing Groups

Demonstration Steps

Create a new group

1. On LON-DC1, switch to **Active Directory Administrative Center**.
2. In the Tasks list, under IT, point to **New**, and then click **Group**.
3. In the **Create Group** dialog box, in the **Group name** box, 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 the **Enter the object names to select (examples):** box, type **April; Don;**, click **Check Names**, and then click **OK**.
3. 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 the **Enter the object names to select (examples):** box, type **IT Managers**, 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**. 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 Groups** dialog box, in the **Enter the object names to select (examples)** box, type **Ed Meadows**, click **Check Names**, and then click **OK**.
4. Select the **Manager can update membership list** check box, and then click **OK**.

Lesson 4

Delegating Administration

Contents:

Demonstration

12

Demonstration

Demonstration: Delegating Administrative Control

Demonstration Steps

Delegate a standard task

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

Delegate a custom task

1. In the navigation pane, right-click **IT**, 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 the **Enter the object names to select (examples):** box, 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 the **Computer objects** check box.
9. Select the **Create selected objects in this folder** and the **Delete selected objects in this folder** check boxes, and then click **Next**.
10. On the **Permissions** page, in the **Permissions** list, select the **Full Control** check box, 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 **IT**, and then click **Properties**.
3. In the **IT Properties** dialog box, click the **Security** tab.
4. In the **Security** tab, click **Advanced**.

5. In the **Advanced Security Settings for IT** dialog box, notice the Allow permissions that are assigned to IT (ADATUM\IT). These were created during the delegation process. 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 long.
- 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 managing access to resources, try to use both domain local group 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 computer 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: A company with branches in multiple cities has members of a sales team that travel frequently between domains. Each of these domains has their own printers that are managed by using domain local groups. How can you provide these members with access to the various domains printers?

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 having 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 somebody 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 OU. In addition, you cannot link a GPO to a container. Because of this, as a best practice you should move the newly created computer account 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 the computer's SID being lost, 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 to the OU such as shared files and printers. 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–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** 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	Use	Where to find it
Active Directory Users and Computers	Manage groups	Administrative Tools
Active Directory module for Windows PowerShell	Manage groups	Installed as Windows Feature
DS utilities	Manage groups	Command line
Active Directory module for Windows PowerShell	Computer account management	Administrative Tools
Djoin.exe	Offline domain join	Command line
Redircmp.exe	Change default computer	Command line

Tool	Use	Where to find it
	container	
DSACLS	View and modify AD DS permissions	Command line

Lab Review Questions and Answers

Lab: Managing Active Directory Domain Services Objects

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

Answer: To modify attributes of new and existing users, you can select multiple users and then open the **Properties** dialog box, you can use the **DSMod** command, or you can create a user account based on a user account template. Alternatively, you can use the **set-ADUser** Windows PowerShell command.

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: What are the two credentials that 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
Additional Reading	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.

Additional Reading

What Is Csvde?



Additional Reading: For more information about LDAP query syntax, see 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 would have occurred if the **ProtectedFromAccidentalDeletion** parameter was not used.

Lesson 3

Performing Bulk Operations with Windows PowerShell

Contents:

Question and Answers	7
Additional Reading	7
Demonstration	7

Question and Answers

Querying Objects with Windows PowerShell

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

Answer: The **-eq** operator is used to find an exact match, meaning that it is not case sensitive. The **-like** operator can be used 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 has been 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.

Additional Reading

Querying Objects with Windows PowerShell



Additional Reading: For more information about filtering with Get AD* cmdlets, see about_ActiveDirectory_Filter at <http://go.microsoft.com/fwlink/?LinkID=266740>.

Demonstration

Demonstration: Using Graphical Tools to Perform Bulk Operations

Demonstration Steps

Create a query for all users

1. Start **20410B-LON-DC1** and sign in as **Adatum\Administrator** by using the password **Pa\$\$w0rd**.
2. On LON-DC1, in Server Manager, click **Tools**, and then click **Active Directory Administrative Center**.
3. In 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 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 window, 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 Active Directory Administrative Center.

Demonstration: Performing Bulk Operations with Windows PowerShell

Demonstration Steps

Configure a department for users

1. Start 20410B-LON-DC1, and sign in as **Adatum\Administrator** by using the password of **Pa\$\$w0rd**.
2. On LON-DC1, on the task bar, click the Windows PowerShell icon.
3. At the Windows PowerShell prompt, type the following command, and then press Enter:

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

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

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

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

```
Get-ADUser -Filter 'department -eq "Research"' | Format-Table  
DistinguishedName,Department
```

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

```
Get-ADUser -Filter 'department -eq "Research"' -Properties Department | Format-Table  
DistinguishedName,Department
```

Create an 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 **Windows Explorer** icon.
2. In the Windows Explorer window, 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)** window, click **Notepad**.
5. In Notepad, review the contents of the .csv file, and read the header row.
6. Close Notepad.
7. In the Windows® Explorer window, right-click **DemoUsers.ps1**, and then click **Edit**.
8. In Windows PowerShell 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 the Windows PowerShell prompt.

Verify that new user accounts were created

1. In Server Manager, click **Tools**, and then click **Active Directory Administrative Center**.
2. In Active Directory Administrative Center, in the navigation pane, browse 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 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 can generate a list of the new students and then export it as a .csv file. After the data has been 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 with 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.

Lab Review Questions and Answers

Lab: Automating AD DS Administration by Using Windows PowerShell

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 4: Configuring and Troubleshooting IPv4	6
Module Review and Takeaways	9
Lab Review Questions and Answers	11

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 know 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 smaller organizations use simple networking to make configuration easier. Larger organizations with networking specialists are more likely to use complex networking.

Lesson 4

Configuring and Troubleshooting IPv4

Contents:

Question and Answers	9
Additional Reading	9
Demonstration	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: Are there any other steps that 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 application.

Additional Reading

Configuring IPv4 Manually



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

Demonstration

Demonstration: How to Capture and Analyze Network Traffic by Using Network Monitor

Demonstration Steps

Capture network traffic with Network Monitor

Prepare to perform a packet capture

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 **ipconfig /flushdns**, and then press Enter.
4. Hover your mouse in the lower-right corner, and when the Start button displays, click **Start**.
5. On the Start screen, click **Microsoft Network Monitor 3.4**.
6. In the Microsoft Update Op-In window, click **No**.
7. In Network Monitor, in the **Recent Captures** box, click the **New capture tab** link.

Capture packets from a ping request

1. In Network Monitor, on the toolbar, click **Start**.
2. At the Windows PowerShell prompt, type **ping LON-DC1.adatum.com**, and then press Enter.
3. In Network Monitor, on the toolbar, click **Stop**.

Analyze the captured network traffic

1. In Network Monitor, in the Frame Summary pane, scroll down to packets with the **Protocol Name** equal to **ICMP**.

2. Select the first **ICMP** packet.
3. In the Frame Details pane, expand the **Icmp** portion of the packet. Show that it is an **Echo Request**. This is a **ping** request.
4. Expand the **Ipv4** portion of the packet. Show the source and destination IP addresses.
5. Expand the **Ethernet** portion of the packet. Show the source and destination MAC addresses.
6. In the Frame Summary pane, click the second **ICMP** packet.
7. In the **Icmp** portion of the packet, verify that it is an **Echo Reply**. This is the response to the ping request.

Filter the network traffic

1. In the Display Filter pane, click **Load Filter**, point to **Standard Filters**, point to **DNS**, and then click **DNSQueryName**.
2. Scroll down in the Display Filter area, and replace the text **server** with **LON-DC1.adatum.com**.
3. Click **Apply**. Explain that the packets have now been filtered to show only packets that match the filter.

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 your IPv4 configuration scheme.
- Define purposes for specific address ranges and subnets. This allows you to easily identify hosts based on their IP address and 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 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 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 application that runs on a non-standard port number. A colleague is testing access to the new web-based application, and indicates that he cannot connect to it. What are the most likely causes of his problem?

Answer: When a server application runs on a non-standard port, you need to provide the client application 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
Network Monitor	Capture and analyze network traffic	Download from Microsoft website
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

Tool	Use for	Where to find it
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 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	<p>In most cases, computers that are running Windows operating systems display a pop-up 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.</p> <p>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.</p>
Multiple default gateways defined	<p>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.</p>
Incorrect IPv4 configuration	<p>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.</p>

Lab Review Questions and Answers

Lab: Implementing IPv4

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

Answer: The criteria in the scenario calls for one subnet with 100 IP addresses for clients. It is not possible to make all of the subnets this large. Variable length subnetting allows you to subdivide the single /24 network into variable sized subnets to allow for 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: Installing a DHCP Server Role	2
Lesson 2: Configuring DHCP Scopes	4
Module Review and Takeaways	6
Lab Review Questions and Answers	8

Lesson 1

Installing a DHCP Server Role

Contents:

Additional Reading	3
Demonstration	3

Additional Reading

How DHCP Lease Generation Works

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

Demonstration

Demonstration: Adding 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. On the Taskbar, click the Server Manager icon, then in **Server Manager**, 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 **Installation succeeded on LON-SVR1.Adatum.com** displays, and then click **Close**.

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 means that DHCP server has been authorized in AD DS.



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

Lesson 2

Configuring DHCP Scopes

Contents:

Demonstration

6

Demonstration

Demonstration: Creating and Configuring a DHCP Scope

Demonstration Steps

Configure scope and scope options in DHCP

1. 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**.

Module Review and Takeaways

Best Practices

- Spend time designing your IP addressing scheme so that it will accommodate both your current IT infrastructure and any potential future IT infrastructure needs.
- 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 redundant array of independent disks (RAID)-5 or RAID-1, to provide DHCP service availability in case of single disk failure.
- Back up the DHCP database regularly, and test the restore procedure in an isolated, non-production environment.
- Monitor the system utilization of DHCP servers, and upgrade the DHCP server hardware if needed to provide better service performance.

Review Question(s)

Question: You have two subnets in your organization and want to use DHCP to allocate addresses to client computers in both subnets. 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 if your single DHCP server should ever fail.

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, you can, 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
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 settings, including those for DHCP server role	Command-line

Tool	Use for	Where to find it
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: For what is the DHCP scope used?

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 Domain Name System

Contents:

Lesson 1: Name Resolution for Windows Clients and Servers	2
Lesson 2: Installing and Managing a DNS Server	4
Lesson 3: Managing DNS Zones	6
Module Review and Takeaways	9
Lab Review Questions and Answers	10

Lesson 1

Name Resolution for Windows Clients and Servers

Contents:

Additional Reading

3

Additional Reading

What Are Computer Names?



Additional Reading: For more information about NetBIOS name resolution, see NetBIOS Name Resolution at <http://go.microsoft.com/fwlink/?LinkId=269710>.

Lesson 2

Installing and Managing a DNS Server

Contents:

Demonstration

6

Demonstration

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 a password of **Pa\$\$w0rd**.
2. On LON-SVR1, in the Server Manager console, 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**.

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** two times.



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

Lesson 3

Managing DNS Zones

Contents:

Question and Answers	9
Demonstration	9

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, then you should not store it in AD DS.

Demonstration

Demonstration: Creating an Active Directory–Integrated Zone

Demonstration Steps

Promote LON-SVR1 as an additional domain controller

1. 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 **Add Roles and Features Wizard** window displays, 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. At the title bar where **Configuration required for Active Directory Domain Services at LON-SVR1** displays, 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. Type **Pa\$\$w0rd** in both text fields, and then click **Next**.
16. On the **DNS Options** page, click **Next**.
17. On the **Additional Options** page, click **Next**.
18. On the **Paths** page, click **Next**.
19. On the **Review Options** page, click **Next**.
20. On the **Prerequisites Check** page, click **Install**.



Note: The server will automatically restart as part of the procedure.

21. After LON-SVR1 restarts, sign in as **Adatum\Administrator**.

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: To the instructor: Point out that this option determines that that 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 **Allow only secure dynamic updates**, 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**, 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 may take a couple of minutes for the record to appear, and you may have to refresh the console display.

Module Review and Takeaways

Best Practices

When implementing 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 troubleshooting 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 is 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 can also 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.

Lab Review Questions and Answers

Lab: Implementing DNS

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

5

Demonstration

Demonstration: Configuring IPv6 Client Settings

Demonstration Steps

View IPv6 configuration by using IPconfig

1. Sign in to **LON-DC1** and **LON-SVR1** as **Adatum\Administrator** using the password of **Pa\$\$w0rd**.
2. On LON-DC1, click the Windows PowerShell® icon on the task bar.
3. At the Windows PowerShell prompt, type **ipconfig**, and then press Enter. Notice that this returns a link-local IPv6 address.
4. Type **Get-NetIPAddress**, and then press Enter.

Configure IPv6 on LON-DC1

1. On LON-DC1, in Server Manager, click **Local Server**.
2. In the **Local Server Properties** dialog box, next to **Local Area Connection**, click **172.16.0.10, IPv6 Enabled**.
3. In the **Network Connections** window, right-click **Local Area Connection**, 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 **Local Area Connection Properties** dialog box, click **Close**.
10. Close the Network Connections window.

Configure IPv6 on LON-SVR1

1. On LON-SVR1, in Server Manager, click **Local Server**.
2. In the **Local Server Properties** dialog box, next to **Local Area Connection**, click **172.16.0.21, IPv6 Enabled**.
3. In the Network Connections window, right-click **Local Area Connection**, and then click **Properties**.
4. In the **Local Area Connection 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, and then 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 **Local Area Connection Properties** dialog box, click **Close**.
10. Close the Network Connections window.

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 display.
3. At a command prompt, type **ping -6 lon-dc1**, and then press Enter.
4. Type **ping -4 lon-dc1**, and then press Enter.



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

Lesson 3

Coexistence with IPv4

Contents:

Additional Reading	8
Demonstration	8

Additional Reading

IPv4 and IPv6 Coexistence



Additional Reading: For more information about prefix policies, see Source and Destination Address Selection for IPv6 at <http://go.microsoft.com/fwlink/?LinkId=269711>.

Demonstration

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 dynamically registered their IPv6 addresses 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.

Lesson 4

IPv6 Transition Technologies

Contents:

Additional Reading

10

Additional Reading

What Is PortProxy?



Additional Reading: For more information about IPv6 Transition Technologies, see 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 randomly generated. This ensures the greatest likelihood that no two organizations are using 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 an IPv6 node be configured with?

Answer: There is not specific number of IPv6 addresses that an IPv6 node should have; it depends on the configuration of the organization. Each IPv6 node has a link-local IPv6 address. In addition, it may also 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: 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
Additional Reading	3

Question and Answers

RAID Levels

Question: Should all disks be configured 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 use RAID 5 for the data volumes.

Additional Reading

What Is Network Attached Storage?



Additional Reading: For more information about Windows Storage Server 2012, see <http://go.microsoft.com/fwlink/?LinkID=199647>.

Lesson 2

Managing Disks and Volumes

Contents:

Question and Answers	6
Additional Reading	6
Demonstration	8

Question and Answers

Selecting a File System

Question: What file system do you currently use on your file server? 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.

Additional Reading

Selecting a Partition Table Format

 **Additional Reading:** For frequently asked questions about the GUID partitioning table disk architecture, see <http://go.microsoft.com/fwlink/?LinkID=266748>.

Selecting a Disk Type

 **Additional Reading:**

- For more information about how basic disks and volumes work, see <http://go.microsoft.com/fwlink/?LinkID=199648>.
- For more information about dynamic disks and volumes, see <http://go.microsoft.com/fwlink/?LinkID=199649>.

Selecting a File System

 **Additional Reading:**

- For more information on how FAT works, see <http://go.microsoft.com/fwlink/?LinkID=199652>.
- For more information on how NTFS works, see <http://go.microsoft.com/fwlink/?LinkID=199654>.

Extending and Shrinking Volumes

Additional Reading:

- For more information about how to extend a basic volume, see <http://go.microsoft.com/fwlink/?LinkID=266749>.
- For more information about how to shrink a basic volume, see <http://go.microsoft.com/fwlink/?LinkID=266750>.

Demonstration

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, make sure all the other Disk check boxes are cleared, 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 Windows Explorer icon, and then click **Local Disk (C:)**. You should now 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. Point the mouse at the lower-right corner of the screen, and when the side bar appears, click the **Start** charm.
2. In the Start box, type **cmd**, and then press Enter.
3. In the Command Prompt window, at the command prompt, type **cd **, and then press Enter.

4. Type **md CustomApp** and then press Enter.
5. Type **copy C:\windows\system32\notepad.exe C:\CustomApp**, and then press Enter.
6. Type **mklink /j AppLink CustomApp**, and then press Enter.
7. In the Windows 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 Windows Explorer window and 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.

Lesson 3

Implementing Storage Spaces

Contents:

Question and Answers	11
Additional Reading	11
Demonstration	11

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.

Additional Reading

Advanced Management Options for Storage Spaces



Additional Reading: To learn more about storage cmdlets in Windows PowerShell, see <http://go.microsoft.com/fwlink/?LinkID=266751>.

Demonstration

Demonstration: Configuring Storage Spaces

Demonstration Steps

Create a storage pool

1. Sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. On LON-SVR1, on the taskbar, click the Server Manager icon.
3. In Server Manager, in the left pane, click **File and Storage Services**, and in the Servers pane, click **Storage Pools**.
4. In the STORAGE POOLS pane, click **TASKS** and then in the **TASKS** drop-down list, click **New Storage Pool**.
5. In the New Storage Pool Wizard, on the **Before you begin** page, click **Next**.
6. On the **Specify a storage pool name and subsystem** page, in the **Name** box, type **StoragePool1**, and then click **Next**.
7. On the **Select physical disks for the storage pool** page, click all available physical disks, and then click **Next**.
8. On the **Confirm selections** page, click **Create**.
9. 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 different types of disks in Disk Management?

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

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 manage them almost automatically, 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
Mklink.exe	Create a symbolic link	Command prompt

Tool	Use	Where to find it
	to a file or folder	
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: 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 only create a two-way mirrored virtual disk.

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	5
Lesson 3: Configuring Network Printing	8
Module Review and Takeaways	11
Lab Review Questions and Answers	12

Lesson 1

Securing Files and Folders

Contents:

Demonstration

4

Demonstration

Demonstration: Creating and Configuring a Shared Folder

Demonstration Steps

Create a shared folder

1. Sign in to LON-SVR1 as **Adatum\Administrator** with a password of **Pa\$\$w0rd**.
2. On the taskbar, click the **Windows Explorer** icon.
3. In Windows Explorer, in the navigation pane, 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 window, select the **Share this folder** check box, and then click **Permissions**.

Assign permissions for the shared folder

1. In the Permissions for Data window, click **Add**.
2. Type **Authenticated Users**, click **Check names**, and then click **OK**.
3. In the Permissions for Data window, click **Authenticated Users**, and then under **Allow**, select the **Change** permission check box.
4. Click **OK** to close the Permissions for Data window.
5. Click **OK** to close the Advanced Sharing window.
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**.
4. In the Shares pane, right-click **Data**, and then click **Properties**.
5. In the **Data Properties** dialog box, click **Settings**, and then select the **Enable access-based enumeration** check box.
6. Click **OK** to close the **Data Properties** dialog box.
7. Close Server Manager.

Configure Offline Files

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

6. Click **Close** to close the **Data Properties** dialog box.



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

Lesson 2

Protecting Shared Files and Folders by Using Shadow Copies

Contents:

Demonstration

7

Demonstration

Demonstration: Restoring Data from a Shadow Copy

Demonstration Steps

Configure shadow copies

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

Create a new file

1. In Windows Explorer, browse to drive C, and then click **New folder**.
2. In the **Name** field, type **Data**, and then press Enter.
3. Browse to the **Data** folder on drive C.
4. In the Data folder, right-click an open area, point to **New**, and then click **Text Document**.
5. In the **Name** field, type **TestFile**, and then press Enter.
6. Double-click **TestFile.txt** to open the document.
7. In Notepad, type **Version 1**.
8. Close Notepad, and click **Save** to save the changes.

Create a shadow copy

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

Modify the file

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

Restore the previous version

1. In Windows 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 warning window, 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 verify that the previous version is restored.
7. Close all open windows.



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

Lesson 3

Configuring Network Printing

Contents:

Demonstration

9

Demonstration

Demonstration: Creating Multiple Configurations for a Print Device

Demonstration Steps

Create a shared printer

1. On LON-SVR1, point to the bottom left of the screen, and click the **Start** charm.
2. In the Start box, type **Devices**, click **Settings**, and then click **Devices and Printers**.
3. In the Devices and Printers window, click **Add a printer**.
4. In the Add Printer window, click **The printer that I want isn't listed**.
If any printers have been discovered on the network, they will usually appear in the printer list.
5. Click **Add a local printer or network printer with manual settings**, and then click **Next**.
Other connections options are also available in this window.
6. Click **Use an existing port**, ensure that **LPT1: (Printer Port)** is selected, and then click **Next**.
Other ports can be created manually here, 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 using the same port

1. In the Devices and Printers window, click **Add a printer**.
2. In the Add Printer window, click **The printer that I want isn't listed**.
3. In the Add Printer window, 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 as was selected for the printer 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 as was used for the printer 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 the **Printer name** text box, 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 the **Priority** box, type **10**, and then click **OK**.

Now jobs that are submitted to the Executives printer have higher priority than 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 supersede 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 like accidental deletion, they are still 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: Branch Office Direct Printing is typically best used when the wide area network (WAN) connection between a printer and a print server is slow or unreliable. When clients are located in the same physical location as the printer, and they use Branch Office Direct Printing, time to print is decreased and network bandwidth use is reduced 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

Name of tool	Used for	Where to find it
Effective Permissions 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 use 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: 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, which creates a more streamlined navigation experience. It also makes for a more secure network browsing experience, as users are unaware of other folders and files that exist in the directory tree to which they have not been granted access.

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, if the Recycle Bin has been emptied, or if the file has been changed more than once, then the file cannot be recovered using this method.

In comparison, shadow copies maintain multiple, persistent copies of modified files that can be recovered by an administrator or by an end user.

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 connecting remotely using Windows PowerShell® 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

3

Demonstration

Demonstration: Creating and Managing GPOs

Demonstration Steps

Create a GPO by using the GPMC

1. Sign in to **LON-DC1** as **Administrator** with a password of **Pa\$\$w0rd**.
2. In Server Manager, click **Tools**, and then click **Group Policy Management**.
3. In the 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 with the Group Policy Management Editor

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, expand the **Prohibit Windows Messenger** GPO, expand **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.
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. To import the Group Policy cmdlets, at the Windows PowerShell command prompt, type the following and then press Enter:

```
import-module grouppolicy
```

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

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

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

Lesson 2

Group Policy Processing

Contents:

Question and Answers

6

Demonstration

7

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 to Control Panel, use security filtering to apply it to the correct group of users, and then assign it a preference order that ensures it is the last policy applied.

Question: Can GPO2 be applied to other department OUs?

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

Demonstration

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 command prompt, type **Gpupdate**, and then press Enter.

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

1. At the command prompt, type **Gpresult /H c:\Gpresult.html**, and then press Enter.
2. On the taskbar, click the Windows Explorer icon.
3. In the Windows 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, and note that the **Do not allow Windows Messenger to be run** setting is **Enabled**, and that **Winning GPO** is the **Prohibit Windows Messenger GPO**.
6. Close the report.
7. Close Windows Explorer.
8. 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 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 other uses. Instead, create new policies.
- Limit the use of security filtering and other mechanisms that make diagnostics more complex.
- Disable the User or Computer sections of policies if they have no settings configured.
- 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 they belong to. 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 a child domain.

One disadvantage of using a site-level GPO is that troubleshooting might be difficult because the GPO can potentially 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 without using scripts for selected users?

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 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 Object Editor	Configure settings in GPOs	Accessed by editing any GPO
Resulting Set of Policies (RSOP)	Determine what settings are applying to a user or computer	In the GPMC
Group Policy Modeling Wizard	Test what would occur if	In the GPMC

Tool	Use	Where to find it
	settings were applied to users or computers, prior to actually applying the settings	
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 Object 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 applying 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 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: What is the difference between ADMX and ADML files?

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

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 cmdlet can you use to force the immediate refresh of all GPOs on a client computer?

Answer: You would use the Windows PowerShell cmdlet **Gpupdate /force** to force the refresh.

Module 12

Securing Windows Servers Using Group Policy Objects

Contents:

Lesson 1: Windows Operating Systems Security Overview	2
Lesson 2: Configuring Security Settings	4
Lesson 3: Restricting Software	6
Module Review and Takeaways	9
Lab Review Questions and Answers	11

Lesson 1

Windows Operating Systems Security Overview

Contents:

Question and Answers	3
Additional Reading	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. The actual measures that you implement should be based on the needs and budget of your organization.

Additional Reading

Applying Defense-In-Depth to Increase Security



Additional Reading:

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

Best Practices for Increasing Security



Additional Reading: For more information about best practices for enterprise security, see <http://go.microsoft.com/fwlink/?LinkID=266743>.

Lesson 2

Configuring Security Settings

Contents:

Additional Reading

5

Additional Reading

 **Additional Reading:** For detailed information about Group Policy settings, see <http://go.microsoft.com/fwlink/?LinkID=266744>.

Configuring Security Auditing

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

Lesson 3

Restricting Software

Contents:

Additional Reading	7
Demonstration	7

Additional Reading

What Is AppLocker?



Additional Reading: For more information about AppLocker, see AppLocker overview at <http://go.microsoft.com/fwlink/?LinkID=266745>.

Demonstration

Demonstration: Creating AppLocker Rules

Demonstration Steps

Create a GPO to enforce the default AppLocker Executable rules

1. Sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. On LON-DC1, in Server Manager, click **Tools**, and then click **Group Policy Management**.
3. In GPMC, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, click **Group Policy Objects**, right-click **Group Policy Objects**, and then click **New**.
4. In New GPO window, in the **Name** field, 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, expand **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, expand **Application Control Policies**, expand **AppLocker**, click **Executable Rules**, and then right-click **Executable Rules** and select **Create New Rule**.
7. On the **Before You Begin** page, click **Next**.
8. On the **Permissions** page, select the **Deny** radio button, and then click **Next**.
9. On the **Conditions** page, select the **Publisher** radio button, and then click **Next**.
10. On the **Publisher** page, click **Browse**, and then click **Computer**.
11. On the **Open** page, double-click **Local Disk (C:)**.
12. On the **Open** page, double-click **Program Files**, double-click **Windows NT**, double-click **Accessories**, click **wordpad.exe**, and then click **Open**.
13. Move the slider up to the **File name:** position, and then click **Next**.
14. Click **Next** again, and then click **Create**.
15. If prompted to create default rules, click **Yes**.
16. In the Group Policy Management Editor, expand **Computer Configuration**, expand **Windows Settings**, and then expand **Security Settings**, expand **Application Control Policies**, and then right-click **AppLocker** and select **Properties**.
17. On the **Enforcement** tab, under **Executable rules**, select the **Configured** check box, click **Enforce rules**, and then click **OK**.
18. In the Group Policy Management Editor, expand **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, click **System Services**, and then double-click **Application Identity**.

19. In the **Application Identity Properties** dialog box, under **Select service startup mode**, click **Define this policy setting**, click **Automatic**, and then click **OK**.
20. Close the Group Policy Management Editor.

Apply the GPO to the domain

1. In the GPMC, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, and then expand **Group Policy Objects**.
2. In the GPMC, 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 GPMC.
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. Start and then sign in to **20410B-LON-CL1** as **Adatum\Alan** with the password **Pa\$\$w0rd**.
2. Point to the lower-right corner of the screen, click the **Search** charm, type **cmd**, and then press Enter.
3. In the Command Prompt window, type **gpupdate /force**, and then press Enter. Wait for the policy to update.
4. Click to the **Start** screen, type **WordPad**, and then press Enter.
5. Notice that WordPad does not start.

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 differing 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, non-production 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, the defense-in-depth model is used to organize your plans for defense, rather than prescribe specific technologies.

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

Answer: The **Account Lockout Threshold** setting ensures that users are allowed only three invalid logon attempts.

Question: You are creating a GPO with standardized firewall rules for the servers in your organization. You tested the rules on a standalone 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 would be required for member servers. To test rules on a standalone server, you would 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. In addition, 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	Use 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 are allowed to be run by users	GPO Editor in GPMC
Windows Firewall with Advanced Security	A host-based firewall that is included as a feature in Windows Server 2012 and Windows Server 2008	Server Manager/Tools if configured individually, or GPO Editor in GPMC 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 log on locally to a server.	First, verify that the user has the correct permissions to log on 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 log on 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: 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 the computers in a domain?

Answer: If the Domain Admins group is not included in the Local Administrators group, Domain Admins will not be a member of the Local Administrators group on all the computers in a domain.

Question: Why do you need to not allow local logon on some computers?

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

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

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 or not.

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

Answer: Events are generated in the Event Viewer security log, with information who has tried to log on to the domain and whether the attempt was successful or not.

Lab B: Configuring AppLocker and Windows Firewall

Question: You configured an AppLocker rule based on a software path. How can you prevent users from moving the folder containing the software so that they can still run the software?

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

Question: You would like to introduce a new application that requires the use of 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 are needed so 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 2: Implementing Hyper-V	2
Lesson 3: Managing Virtual Machine Storage	4
Lesson 4: Managing Virtual Networks	6
Module Review and Takeaways	8
Lab Review Questions and Answers	10

Lesson 2

Implementing Hyper-V

Contents:

Additional Reading

5

Additional Reading

Virtual Machine Hardware



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

Configuring Dynamic Memory



Additional Reading: For more information about Hyper-V Dynamic Memory, see 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, see Hyper-V Resource Metering Overview at <http://go.microsoft.com/fwlink/?LinkId=269714>.

Lesson 3

Managing Virtual Machine Storage

Contents:

Question and Answers	8
Additional Reading	8

Question and Answers

Creating Virtual Disk Types

Question: Why might you consider using fixed VHDs instead of dynamically expanding VHDs?

Answer: You may want to use fixed VHDs instead of dynamically expanding VHDs if:

- You want to maintain control over the growth of VHDs.
- You want to pre-allocate storage.

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

Answer: With dynamically expanding disks, it is easy to place multiple dynamically expanding disks on the same volume, and then have them grow to consume the volume.

Additional Reading

What Is a VHD?



Additional Reading: For more information about VHD formats, see Hyper-V Virtual Hard Disk Format Overview at <http://go.microsoft.com/fwlink/?LinkId=269715>.

Lesson 4

Managing Virtual Networks

Contents:

Additional Reading

11

Additional Reading

What Is a Virtual Switch?



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

Hyper-V Network Virtualization



Additional Reading: For more information about network virtualization, see Hyper-V Network Virtualization Overview at <http://go.microsoft.com/fwlink/?LinkId=269717>.

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 a virtualization server is provisioned 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 are hosted on the same virtualization server.

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 in the following situations:

- When the guest operating system does not support Dynamic Memory.
- When the management operating system has limited memory resources, and you need to ensure that operating systems are allocated memory fairly.

Question: In which situations must you use VHDs with the new .vhdx format instead of VHDs with the old .vhd format?

Answer: You should use VHDs with the new .vhdx format rather than VHDs with the old .vhd format in the following situations:

- You need to support VHDs larger than 2 TB. VHDs with the new .vhdx format can be a maximum of 64 TB, while VHDs with the old .vhd format are limited to 2 TB.
- You need to protect against data corruption caused by power failures. VHD with the new .vhdx format are less likely to become corrupted in the event of unexpected power failure because of how the file format processes updates.
- You need to deploy a VHD to a large sector disk.

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

Answer: You can only deploy VHDs 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 VHD 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: What type of virtual network switch would you create if you wanted 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 one single virtual machine uses all available bandwidth provided by the Hyper-V virtualization server?

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 on previous versions of Hyper-V.

Send Us Your Feedback

You can search the Microsoft Knowledge Base for known issues at Microsoft Help and Support before submitting feedback. Search using either the course number and revision, or the course title.

Note Not all training products will have a Knowledge Base article – if that is the case, please ask your instructor whether or not there are existing error log entries.

Courseware Feedback

Send all courseware feedback to support@microsoft.com. We truly appreciate your time and effort. We review every e-mail received and forward the information on to the appropriate team. Unfortunately, because of volume, we are unable to provide a response but we may use your feedback to improve your future experience with Microsoft Learning products.

Reporting Errors

When providing feedback, include the training product name and number in the subject line of your e-mail. When you provide comments or report bugs, please include the following:

1. Document or CD part number
2. Page number or location
3. Complete description of the error or suggested change

Please provide any details that are necessary to help us verify the issue.

Important All errors and suggestions are evaluated, but only those that are validated are added to the product Knowledge Base article.