

OFFICIAL MICROSOFT LEARNING PRODUCT

10967A

Fundamentals of a
Windows Server®
Infrastructure

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.

© 2013 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: 10967A

Released: July 2013

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 locale, les garanties implicites de qualité marchande, d'adéquation à un usage particulier et d'absence de contrefaçon sont exclues.

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

Cette limitation concerne:

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

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

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

Revised September 2012

Module1

Installing and Configuring Windows Server

Contents:

Lesson 1: Windows Server Architecture	2
Lesson 2: Installing Windows Server	4
Lesson 3: Configuring Services	8
Lesson 4: Configuring Devices and Device Drivers	10
Module Review and Takeaways	12
Lab Review Questions and Answers	12

Lesson 1

Windows Server Architecture

Contents:

Question and Answers

3

Question and Answers

What Is a Server?

Question: What different functions might a server perform in a network environment?

Answer: A server might perform some defined Windows Server 2012 roles, such as application server, file server, or web server. A server can also perform more general functions like branch server, or functions based on Microsoft® server-based applications such as SQL Server® or Exchange Server.

Windows Server Components

Question: In what ways can 64-bit computing improve performance?

Answer: 64-bit operating systems can take advantage of 64-bit processors' ability to access more memory. i.e. 32 GB processors can address up to 4 GB of memory whereas 64 bit processors can address up to 1024 GB of memory. This enables applications to access more physical memory.

Limits in 32-bit addressing imply smaller default values being assigned to applications, such as the combined size of all event logs, the system cache and so forth, which would be small for today's requirements.

Lesson 2

Installing Windows Server

Contents:

Question and Answers	5
Demonstration	5

Question and Answers

Installation Methods

Question: Why is it important to be able to change the installation files on a writable media type?

Answer: You may have to provide hardware drivers, install software upgrades, or meet specific organizational requirements. Doing these things during installation will save time and make sure consistency across multiple servers.

What Is Server Core

Question: In what situations might a Server Core installation be used instead of a full installation of Windows Server 2012?

Answer: The general recommended approach is that, where you can, all Windows Server 2012 servers should be run in a non-GUI or reduced GUI environment and managed remotely, reducing the administration, update, and resource overhead in addition to reducing the attack surface. Some scenarios would also add weight to the recommendation to run in Server Core, such as remote branches, single-role servers, or locations where the physical security of the server might be compromised.

Automating Deployment with Windows Deployment Services

Question: In what situations would a Windows Deployment Services server be used by an organization? In what situations would a Windows Deployment Services Server not be efficient to implement?

Answer: If an organization frequently has lots of computers that require deployment (clients or servers), Windows Deployment Services would be an effective solution. Also, if most computers are configured similarly or if manual, onsite installation is not possible, Windows Deployment Services can provide an effective solution. Some situations where Windows Deployment Services might not be effective are heavily congested networks, environments where few new installations are performed, or organizations that cannot afford the hardware or administration overhead to implement a Windows Deployment Services solution.

Demonstration

Demonstration: What Is Server Core

Demonstration Steps

1. On **10967A-LON-DC1**, if you have not already done so, log in as **ADATUM\Administrator** with password **pa\$\$w0rd**.
2. Open Server Manager.
3. Generally discuss Server Manager and call out that the presence of the GUI means that you are not in Server Core mode.
4. Click the **Manage** menu, and then select **Remove Roles and Features**.
5. On the **Before you Begin** page click **Next**.
6. On the **Select Destination Server** page ensure **LON-DC1** is highlighted and click **Next**.
7. On the Remove Server Roles page click Next.
8. On the **Remove Features** page scroll down to **User Interfaces and Infrastructure** page and expand the node, and discuss how you could remove or add these graphical components.
9. Close the Remove Roles and Feature Wizard window.
10. In Server Manager, click the **Tools** menu, then select **Windows PowerShell®**.

11. Generally discuss Windows PowerShell.
12. At the command prompt, type the following command, and then press **Enter**.

```
Get-WindowsFeature
```

13. In the resultant output scroll to the **User Interfaces and Infrastructure** feature and highlight it as the same as what was listed in the **Remove Features Wizard** earlier
14. At the command prompt, type the following command, and do not press **Enter**.

```
Uninstall-WindowsFeature Server-GUI-Mgmt-Infra,Server-GUI-Shell
```

15. Discuss how this command could be used to remove the graphical components of the server.
16. Explain that to save time you will switch to an already configured Server Core installation.
17. Switch to **10967A-LON-SVR3**, if you have not already done so, log in as **ADATUM\Administrator** with password **Pa\$\$w0rd**
18. At the command prompt type the following command, and press **Enter**

```
Powershell
```

19. At the Windows PowerShell prompt type the following command, and press **Enter**.

```
Get-windowsfeature
```

20. In the resultant output scroll to the **User Interfaces and Infrastructure** feature and highlight the graphical components as now having no **X** beside them indicating they are not installed.
21. At the command prompt, type the following command, and then press **Enter**.

```
sconfig
```

22. Generally discuss Sconfig management options.
23. As you have time, show any other administration tools the students might be interested in such as Task Manager.
24. Revert the 10967A-LON-DC1 and the 10967A-LON-SVR3 virtual machines for the next demo steps.

Demonstration: How to Configure a Server after Installation

Demonstration Steps

1. Log on to the 10967A-LON-SVR2 virtual machine as **Administrator** with a password of **Pa\$\$w0rd**.
2. Click the Server Manager icon on the bottom tool bar if Server Manager is not already available.
3. In the navigation pane, click **Local Server**, and quickly review the main information areas such as **Properties** and **Roles and Features**.
4. In the **Properties** area, scroll to the right side, and then click the **Time zone** entry.
5. In the **Date and Time** dialog box, click the **Change time zone** button.
6. Select (UTC) Dublin, Edinburgh, Lisbon, London, make sure that Automatically adjust clock for Daylight Saving Time is selected, and then click OK.
7. In the **Date and Time** dialog box, click **OK**.
8. In the **Properties** area, click the **Local Area Connection** entry.

9. In the **Local Area Connection Properties** page, right-click **Local Area Connection**, and then select **Properties**.
10. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click the **Properties** button.
11. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** page, select Use the following IP address.
 - IP address: **172.16.0.25**
 - Subnet mask: **255.255.0.0**
 - Default gateway: **172.16.0.1**
12. Select Use the following DNS server addresses.
 - Preferred DNS server: **172.16.0.10**
13. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** page, click **OK**.
14. In the **Local Area Connections Properties** page, click **Close**.
15. Close the Network Connections window.
16. In the **Properties** area, click the **Windows Update** entry.
17. In the **Windows Update** window, click Change settings
18. In the important updates section select **Check for updates but let me to choose whether to download and install them** in the drop down list, and then click **OK**.
19. Close the **Windows Update** window console.
20. Return to **Server Manager** in the **Properties** area, click the **Computer name** entry.
21. In the **System Properties** window, click the **Change** button.
22. In the **Computer Name/Domain Changes** dialog box, make sure that **LON-SVR2** is in the **Computer name** field.
23. Select **Domain** in the **Member of** section, and then type **Adatum.com** in the **Domain** field.
24. Click **OK**.
25. When you are prompted to provide administrative account details, use **ADATUM\Administrator** and a password of **Pa\$\$w0rd**.
26. When the **Welcome to the ADATUM domain** dialog box appears, click **OK**.
27. When you are prompted that you must restart your computer to apply these changes, click **OK**.
28. In the **System Properties** window, click **Close**.
29. When you are prompted to restart, click **Restart Now**.
30. Do not revert the virtual machines. You will continue configuration in the next demonstration.

Lesson 3

Configuring Services

Contents:

Demonstration

9

Demonstration

Demonstration: How to Configure Service Startup

Demonstration Steps

1. Log on to the 10967A-LON-SVR2 virtual machine as **ADATUM\Administrator** with a password of **Pa\$\$w0rd**.
2. In Server Manager, click the **Tools** menu, and then select **Services**.
3. Scroll down to **Print Spooler**. Notice that the Print Spooler status is **Running** and startup is set to **Automatic**.
4. Right-click **Print Spooler**, and then click **Properties**.
5. Click the drop-down box for **Startup type**, and then select **Disabled**.
6. Click the **Log On** tab, and then show the settings available from this tab.
7. Click the **Recovery** tab, and then show the settings available from this tab.
8. Click the **Dependencies** tab, and then show the settings available from this tab.
9. Click **OK** to close the **Print Spooler Properties** dialog box.
10. If you have time, restart the server to show that the Print Spooler service is disabled and not automatically started.
11. Close Server Manager.
12. Do not revert the virtual machines. You will continue configuration in the next demonstration.

Lesson 4

Configuring Devices and Device Drivers

Contents:

Demonstration	11
---------------	----

Demonstration

Demonstration: How to Update a Device Driver

Demonstration Steps

1. Switch to the 10967A-LON-SVR2
2. Open Server Manager, click the **Tools** menu, and then click **Computer Management**.
3. In the navigation frame, expand **System Tools**, and then click **Device Manager**.
4. Expand **Display Adapters**, right-click **Microsoft Hyper-V Video**, and then select **Properties**.
5. Click the **Resources** tab, and then show the **Memory Range**.
6. Click OK to close the **Properties** dialog
7. Expand **Keyboards**, right-click **Standard PS/2 Keyboard**, and then click **Update Driver Software**.
8. In the **Update Driver Software – Standard PS/2 Keyboard** dialog box, click **Browse my computer for driver software**.
9. On the **Browse for driver software on your computer** page, click **Let me pick from a list of device drivers on my computer**.
10. In the **Show compatible hardware** list, click **PC/AT Enhanced PS/2 Keyboard (101/102 Key)**, and then click **Next**.
11. Notice that Windows has successfully updated your driver software.
12. Click **Close**.
13. In the **System Settings Change** dialog box, click **Yes** to restart the computer.
14. Do not revert the virtual machines. You will continue configuration in the next demonstration.

Demonstration: How to Roll Back a Driver

Demonstration Steps

1. Switch to LON-SVR2
2. Open Server Manager, click the **Tools** menu, and then click **Computer Management**.
3. In the navigation frame, expand **System Tools**, and then click **Device Manager**.
4. In the center pane, expand **Keyboards**, right-click **PC/AT Enhanced PS/2 Keyboard (101/102 Key)**, and then click **Properties**.
5. In the **PC/AT Enhanced PS/2 Keyboard (101/102 Key) Properties** dialog box, click the **Driver** tab.
6. Click **Roll Back Driver**.
7. In the **Driver Package rollback** dialog box, click **Yes**.
8. Click **Close**, and then in the **System Settings Change** dialog box, click **Yes** to restart the computer.
9. As you have time, wait for the computer to restart. Then log on and verify that you have successfully rolled back the driver.
10. Close Server Manager.
11. Revert the 10967A-LON-DC1 and the 10967A-LON-SVR2 virtual machines.

Module Review and Takeaways

Question: Why is it potentially more difficult to perform post-installation tasks on a Server Core installation of Windows Server instead of a Server with a GUI?

Answer: A Server Core installation contains limited or no GUI elements used for common post configuration tasks.

Question: If you have to troubleshoot system instability, what tool should you use to disable a specific set of services from running at startup?

Answer: **MSConfig** would be the best choice, because it enables you to enable or disable individual services at startup. You could use **MSConfig** to disable the specific set of services, troubleshoot the instability, and enable the services again using **MSConfig** when the troubleshooting is finished.

Question: If a newly installed video adapter device driver is preventing Windows from starting correctly, what tools would you use first to return the system to an operable state?

Answer: Typically, starting in safe mode or using the Last Known Good Configuration should enable the system to start and then the video adapter driver could be rolled back and possibly further diagnosed.

Question: What factors should be considered when staging drivers in the Windows driver store?

Answer: Staged drivers must be digitally signed. Drivers are typically staged for devices that are frequently used or that have hard-to-locate drivers.

Tools

Tool	Use for	Where to find it
Sconfig	Menu-based administration of Server Core installations.	
Windows Deployment Services	Windows Deployment Services for automated deployment of Windows operating systems.	Server role
Registry editor	Editing settings in the Windows registry.	From the Run prompt: regedit.exe
MSConfig	Editing Windows Server settings and troubleshooting startup issues.	Server Manager, System Configuration
Device Manager	Managing server devices and settings.	Server Manager, Computer Management, Device Manager

Lab Review Questions and Answers

Question and Answers

Question: How could the steps in this lab be performed remotely without the need for user intervention?

Answer: A Windows Deployment Services deployment by using a preconfigured image and network (PXE) startup on the computer being installed would allow for automated, unattended execution of the steps in this lab.

Question: When would rolling back a driver not be an effective solution to driver-related problems?

Answer: When there is only one version of the driver installed, or when the system will not start correctly because of driver-related issues.

Module2

Implementing Storage in Windows Server

Contents:

Lesson 1: Identifying Storage Technologies	2
Lesson 2: Managing Disks and Volumes	3
Lesson 3: Fault Tolerance	8
Module Review and Takeaways	13
Lab Review Questions and Answers	13

Lesson 1

Identifying Storage Technologies

Contents:

This lesson does not have any supplemental content

Lesson 2

Managing Disks and Volumes

Contents:

Question and Answers	4
Demonstration	4

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 will vary. A common answer is NTFS, because NTFS should be the basis for any file system that is used on a Windows Server operating system. If you use File Allocation Table 32 (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 about how to change to ReFS when you upgrade 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.

Demonstration

Demonstration: How to Create and Manage Volumes

Demonstration Steps

Bring a Disk Online

1. On 10967A-LON-SVR1, open **Server Manager** then click **Tools** and select **Computer Management**
2. In the Computer Management console expand **Storage**, and then click **Disk Management**.

Note: Alternatively, you can hover the mouse over the bottom left side corner, then right-click the mouse and select **Disk Management**

3. Call out the state the Disk zero being listed as **Basic** and **Online**
4. Right-click **Disk 1** and select **Online**
5. Call out that the state of the Disk now says it is **Not Initialized**

Initialize a Disk

1. Right-click **Disk 1** and choose **Initialize Disk**
2. In the **Initialize Disk** dialog ensure **Disk 1** is selected and **MBR** is select as the partition style and click **OK**
3. Call out the state change of the disk as displayed

Create a Simple Volume

1. Right-click the unallocated space in **Disk 1** and choose **New Simple Volume...**
2. In the opening page of the **New Simple Volume Wizard** click **Next**
3. On the Specify Volume Size screen in the **Simple volume size in MB:** text box enter **8000**, and then click **Next**
4. In the **Assign Driver Letter or Path** accept the defaults and click **Next**
5. In the **Format Partition** page use the following values and ensure that **Perform a quick format** is selected then click **Next**
 - o File system: **NTFS**
 - o Allocation unit size: **Default**
 - o Volume Label: **SimpleVol1**
6. On the **Completing the New Simple Volume Wizard** page click **Finish**

7. Open File Explorer from the task bar. A dialog should appear prompting that the newly attached disk needs to be formatted, In this dialog click **Format Disk**
8. In the resultant **Format SimpleVol1** dialog accept the defaults and ensure Perform a quick format is selected then click **Start**
9. Click **OK** in the resultant warning dialog, and then click **Yes** in the **Formatting SimpleVol1** dialog.
10. When the format is complete click **OK** in the format complete dialog.
11. On the **Format SimpleVol1** dialog click **Close**
12. Open File Explorer and ensure the new volume is displayed as a drive

Create a volume by using File and Storage Services

1. Open **Server Manager**
 2. Click **File and Storage Services** on the left side
 3. Click **Volumes** and then **Disks**
 4. In the **Disks** section right-click **Disk 2** and select **Bring Online**
- Note:** Ensure you sort by Number first to make sure the correct Disk, i.e. Disk 2, is chosen
5. In the **Bring Disk Online** dialog click **Yes**. Notice the status change for the disk
 6. Right-click **Disk 2** again and select **Initialize**
 7. In the **Initialize disk** dialog click **Yes**. Callout that the default here is GPT whereas in the Disk Management console it was MBR partition style
 8. Right-click **Disk 2** again and select **New Volume...**
 9. In the **New Volume Wizard** on the before you begin page click **Next**
 10. On the **Select the server and disk** page click **Next**
 11. On the **Specify the size of the volume** page in the **Volume size:** text box enter **8 GB** and click **Next**
 12. On the **Assign to a drive letter or folder** page accept the defaults and click **Next**
 13. On the **Select file system settings** page enter **SimpleVol2** for **Volume Label:** and click **Next**
 14. On the **Confirm selections** page click **Create**
 15. On the **Completion** page click **Close**
 16. Open File Explorer and view the newly created volumes

Convert a Basic disk to a Dynamic disk using Disk Management

1. Switch to Computer Management console, expand Storage, click Disk Management, right-click **Disk 1**, and then click **Convert to Dynamic Disk**.
2. In the Convert to Dynamic Disk dialog select **Disk 1** and **Disk 2** and Click **OK**.
3. In the Disks to convert dialog Click **Convert**, and then click **Yes**.
4. Notice the change in state and color indicator of the disks

Create a striped volume using Disk Management

1. Right-click the unallocated space on **Disk 1**, and then select **New Striped Volume**.
2. Click **Next**.
3. Make sure that Disk 1 is selected. Click **Disk 2**, and then click **Add**.

4. Change **Select the amount of space in MB** to **4000 MB**.
5. Click **Next**.
6. Accept the default drive letter assignment, and then click **Next**.
7. Type **StripedVol1** as the **Volume label**, and then click **Next**.
8. Click **Finish**.
9. View the results in Disk Management and the change in color indication.
10. Open File Explorer and Show the striped volume present as a single drive.

Configure a volume mount point

1. In Disk Management, right-click **StripedVol1**, and then select **Change Drive Letter and Paths**.
2. Click **Add**.
3. Select **Mount in the following empty NTFS folder**, and then click **Browse**.
4. With **C:** selected, click **New Folder** and call the folder **MountPoint**.
5. Click **OK**.
6. Click **OK**.
7. In File Explorer, show that **C:\MountPoint** exists and point out the icon assigned to the mount point.

Resize volumes using Disk Management

1. In Disk Management, right-click the Volume you created earlier called **SimpleVol2**, and then select **Extend Volume**. Click **Next**.
2. Change **Select the amount of space in MB** to **2000**.
3. Click **Next**.
4. Click **Finish**.
5. Notice the increase in volume size in the Disk Management console and if you have time also in the properties in File Explorer

Create a volume by using Windows PowerShell

1. Open the Windows PowerShell console by right-clicking the Windows PowerShell icon in the task bar and selecting **Run as Administrator**
2. Type the following to view the available disks and press **Enter**.

```
Get-Disk
```

3. Now Type the following and press **Enter**.

```
Get-Volume
```

4. To bring the disk online, type the following:

```
Set-Disk –number 3 -IsOffline $False
```

5. Type the Get-Disk command as outlined in Step 2 to validate the change in Disk status
6. Now type the following to initialize and disk with an MBR partition style

```
Initialize-Disk –Number 3 –PartitionStyle MBR
```

7. Now type the followed to create a partition

```
New-Partition -Disknumber 3 -size 4GB -DriveLetter W | Format-Volume -NewFileSystemLabel  
PoshVol
```

8. And type **A** at the prompt to accept the command
9. Open Disk Management, and view the disk.
10. Click **Cancel** in the **You need to format the disk in drive H: before you can use it** dialog.
11. Open File Explorer and view the Volume.
12. Revert the virtual machines before the next demonstration.

Demonstration: How to Create a Quota by Using FSRM

Demonstration Steps

1. On **10967A-LON-SVR1** on the taskbar, right-click the **Windows PowerShell®** icon and choose Run as Administrator
2. In the **Windows PowerShell** window, type the following commands, and press **Enter** after each line.

```
cd C:\Temp
```

3. Then type the following all on a single line and press **Enter**

```
Fsutil file createnew largefile_1.txt 130000000
```

4. Open File Explorer and verify the file was created successfully and is approximately 130 MB in size.
5. On the taskbar, click the **Server Manager** shortcut.
6. In Server Manager, click **Tools**, and then click **File Server Resource Manager**.
7. In File Server Resource Manager, expand the **Quota Management** node, and then click **Quota Templates**.
8. Right-click the **100 MB Limit** template, and then click **Create quota from template**.
9. In the **Create Quota** window, click **Browse**.
10. In the **Browse for Folder** window, expand **C:\Temp** and then click **OK**.
11. In the **Create Quota** window, click **Create**.
12. In the **File Server Resource Manager** window, click **Quotas** to view the newly created quota t
13. Return to the Windows PowerShell console
14. In the **Windows PowerShell** window, ensure the command line focus is on C:\temp, then type the following commands, and press **Enter** after each line.

```
Fsutil file createnew largefile_2.txt 100000000
```

15. Notice the message returned: **Error: There is not enough space on the disk.**
16. Close the **Windows PowerShell** window.
17. Revert the virtual machines before the next demonstration.

Lesson 3

Fault Tolerance

Contents:

Demonstration

9

Demonstration

Demonstration: How to Implement and Manage Storage Spaces

Demonstration Steps

Create a Storage Pool

1. Ensure you are signed in to 10967A-LON-SVR1 and open Server Manager
2. In Server Manager click on **File and Storage Services** followed by **Volumes** then **Storage Pools**
3. In the Storage Pool section click on **Tasks** and choose **New Storage Pool...**
4. On the opening page of the **New Storage Pool Wizard** click **Next**
5. On the **Specify a storage pool name and subsystem** page enter **StoragePoolTest1** into the **Name** textbox, and then click **Next**.
6. On the **Select physical disks for the storage pool** page select PhysicalDisks **4** and **5** and then click **Next**.
7. On the Confirm selections page click **Create**
8. On the **View results** page click **Close**

Create Storage Space Virtual Disk

1. In Server Manager in the File and Storage Services section click **Volumes** and then **Storage Pools**
2. Click **StoragePoolTest1** under Storage Pools, and then in the **Virtual Disks** section click **Tasks** and choose **New Virtual Disk...**
3. In the **New Virtual Disk Wizard** on the **Before You Begin** page click **Next**
4. On the **Select Storage Pool** page ensure **StoragePoolTest1** is selected and click **Next**
5. On the **Specify the virtual disk name** page enter **VirtualDiskTest1** into the **Name** field and click **Next**
6. On the **Storage Layout** page select **Mirror** and click **Next**
7. On the **Specify provisioning type** page select **Thin** and click **Next**
8. On the **Specify the size of the virtual disk** page enter **4 GB** into the virtual disk size textbox click **Next**
9. On the **Confirm selections** page click **Create** and then click **Close**
10. The **New Volume Wizard** appears and on the **Before you Begin** page click **Next**
11. On the **Select the server and disk** page click **Next**
12. On the **Specify the size of the volume** page accept the defaults and click **Next**
13. On the **Assign to a drive letter or folder** select the **Drive Letter: X** from the drop down box and click **Next**
14. On the **Select file system settings** page select **NTFS** as the file system, Enter **VirtualDiskMirVol** as the Volume Label and click **Next**
15. On the **Confirm selections** page click **Create**
16. On the **Completion** page click **Close**

Verify Virtual Disk is accessible

1. Open File Explorer and locate the drive with the volume label **VirtualDiskMirVol**

2. Create a .txt files in this driver called **Test File.txt**

Add an additional Physical Disk to the Storage Pool

1. In Server Manager in the File and Storage Services section click Volumes and then Storage Pools
2. Right-click **StoragePoolTest1** under Storage Pools, and select **Add Physical Disk...**
3. In the Add Physical Disk dialog select PhysicalDisk 6 and click OK
4. Verify three disks are now listed in the **Physical Disks** section in **Storage Pools**

Remove Physical Disk to simulate Disk Failure

1. In Server Manager in the File and Storage Services section click Volumes and then Storage Pools
2. In the Physical Disks section right-click PhysicalDisk 4 and select Remove Disk
3. In the resultant **Remove Physical Disk** prompt click **Yes**
4. Click **OK** again in the Remove Physical Disk dialog

Verify Virtual Disk is still Available

1. Open File Explorer by clicking on the File Explorer icon in the **Task bar**
2. Verify the **Test File.txt** is still present and accessible on the **VirtualDiskMirVol**

Verify Virtual Disk Status in Server Manager

1. Return to Server Manager, click on **File and Storage Services** followed by **Volumes** then **Storage Pools** then go to the **Physical Disks** section
2. Notice that there are only two disks now as part of the Virtual Disk listed in the Physical Disks section
3. In the **Virtual Disk** section verify a warning exists alongside the **VirtualDiskTest1**
4. Right-click the Virtual Disk **VirtualDiskTest1**, select **Properties** and in the Virtual Disk Properties dialog click on **Health**.
5. Note the status is listed as **Warning**
6. Click **OK** to close the **VirtualDiskTest1 Properties** window

Repair Virtual Hard Disk

1. In Server Manager in the Storage Pools pane in the Virtual Disk section right-click **VirtualDiskTest1** and select **Repair Virtual Disk**

Verify Virtual Disk Status Returns to healthy

1. Refresh the settings and verify the Virtual Disk warning message is no longer present
2. Right-click the Virtual disk **VirtualDiskTest1** and select properties and click **Health**
3. Verify the health status now reads healthy, and then **close** the **VirtualDiskTest1 Properties** window
4. Open File Explorer and verify the file you created earlier is still accessible and available

Delete Virtual Disk

1. In Server Manager in the Storage Pools pane in the Virtual Disk section right-click **VirtualDiskTest1** and select **Detach Virtual Disk...**
2. Click **Yes** in the **Detach Virtual Disk** dialog
3. Right-click **VirtualDiskTest1** and select **Delete Virtual Disk**
4. Click **Yes** in the **Delete Virtual Disk** dialog

5. Verify the Virtual Disk is deleted

Delete Storage Pool

1. In Server Manager in the Storage Pools pane in the Storage Pools section right-click **StoragePoolTest1** and select **Delete Storage Pool**
2. Click **OK** in the **Delete Storage Pool** dialog
3. Verify the Storage Pool is deleted
4. Revert the virtual machines before the next demonstration.

Demonstration: How to Implement RAID by Using the Disk Management console

Demonstration Steps

1. Ensure you are signed in to **10967A-LON-SVR1** and then open Server Manager, click **Tools** and select **Computer Management**.
2. In the **Computer Management** console expand **Storage**, and then click **Disk Management**.
3. **Note:** All disks must be online and initialized before the RAID can be created.
4. Right-click **Disk 4**, and then select **Online**
5. Right click **Disk 4** again and select **Initialize Disk**
6. Accept the defaults in **the Initialize Disk** dialog and click **OK**
7. Repeat steps 4 to 6 for Disk 1, Disk2, Disk3 , Disk 5 and Disk 6
8. Right the unallocated space on **Disk 4** and choose **New Mirrored Volume**.
9. On the Welcome to the New Mirrored Volume Wizard click **Next**.
10. Add **Disk 5** to the mirrored volume so two disks are listed.
11. Change **Select the amount of space in MB** to be **1000**.
12. Click **Next**.
13. On the **Assign driver letter or path** screen choose **Y** from the drop down box and click **Next**
14. On the **Format Volume** page enter a **Volume** label of **MirroredVol**, and then click **Next**.
15. Click **Finish**.
16. Accept the prompt by clicking **Yes**.
17. Notice the change in Disk type and color indicator.
18. Open File Explorer and view the **Y** volume ensuring you can access it
19. Right-click the unallocated space on **Disk 4**, and then select **New RAID-5 Volume**.
20. Click **Next**.
21. Add **Disk 5** and **Disk 6** to the volume so three disks are listed
22. Change **Select the amount of space in MB** to **1000**.
23. Click **Next**.
24. On the Assign driver letter or path screen choose **X** from the drop down box and click **Next**
25. On the Format Volume page enter a Volume label of **RAID-5Vol** and Click **Next**.
26. Click **Finish**.

27. Accept the prompt by clicking **Yes**.
28. Notice the color and describe the RAID-5 Volume. Open File Explorer and view the volume verifying it is available.
29. Revert the virtual machines.

Module Review and Takeaways

Question: What are the different kinds of disks?

Answer: Basic and dynamic disks

Question: What are some different storage technologies?

Answer: DAS, SAN, and NAS

Question: What are the most important implementations of RAID?

Answer: RAID 1 mirrored set without parity or striping

RAID 5 striped set with distributed parity or interleave parity

RAID 6 striped set with dual distributed parity

RAID 1+0 mirrored drives configured as a striped set

Question: What options are available for fault tolerance in Storage Spaces?

Answer: Three options are available for disk configuration in Storage Spaces. These are simple, mirrored, and parity. Both mirrored and parity options would provide some fault tolerance. Simple provides for increased capacity but not for fault tolerance.

Tools

Tool	Use for	Where to find it
Diskpart	Manipulating disks and volumes.	Command Prompt
FSUtil	Manipulating files and storage services.	Run fsutil.exe from the command line.
Windows PowerShell	Managing and configuring storage and Storage Spaces.	The Storage module is part of the operating system. The Storage Spaces module has to be downloaded.
Disk Manager	Manages disks and volumes	Server Manager

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Determining the allocation unit when formatting a drive with a file system	Let Windows Server 2012 to automatically select the allocation unit.
General storage configuration issues	Use Windows PowerShell if you can and try to find the cmdlet that provides for more functionality than any of the other command-line tools and more fine-grained control than the GUI.

Lab Review Questions and Answers

Question and Answers

Question: What kind of storage is easiest to configure and why?

Answer: DAS is usually the easiest storage to configure. DAS is attached to the server and the operating system will automatically detect it.

Question: How would you determine the kind of storage to implement?

Answer: Storage requirements for specific environments vary. When you evaluate what kind of storage to implement, you have to consider organizational requirements, amount of storage required, and performance requirements. You will also have to consider the cost of implementing the storage options and the expertise available to configure and manage the storage.

Module3

Understanding Network Infrastructure

Contents:

Lesson 1: Network Architecture Standard	2
Lesson 2: Local Area Networking	3
Lesson 3: Wide Area Networking	5
Lesson 4: Wireless Networking	6
Lesson 5: Connecting to the Internet	7
Lesson 6: Remote Access	8
Module Review and Takeaways	10
Lab Review Questions and Answers	10

Lesson 1

Network Architecture Standard

Contents:

This lesson does not have any supplemental content.

Lesson 2

Local Area Networking

Contents:

Question and Answers

4

Question and Answers

Question: What topology configuration might you recommend for a new Ethernet LAN being built to connect computers located in several buildings together on a school campus?

Answer: The most common configuration would be a hybrid topology using star topology to connect computers together in each building and bus topology to connect the individual buildings to each other. Students might also mention the use of a mesh topology to provide a fault tolerant configuration between buildings.

Lesson 3

Wide Area Networking

Contents:

This lesson does not have any supplemental content.

Lesson 4

Wireless Networking

Contents:

This lesson does not have any supplemental content.

Lesson 5

Connecting to the Internet

Contents:

This lesson does not have any supplemental content.

Lesson 6

Remote Access

Contents:

Question and Answers

9

Question and Answers

What Is Remote Access?

Question: What other scenarios can you think of that would require remote access?

Answer: Answers will vary depending on student experience. If no plausible examples are offered, share one or two of your own experiences with remote access (traveling employee connecting from a hotel, mobile devices, or vehicle-based branch offices).

Module Review and Takeaways

Question: Why are firewalls so critical when designing and deploying networks?

Answer: Firewalls provide selective separation between networks. They allow potentially untrusted networks to be connected to each other without posing a significant security risk. The traffic and data that needs to travel between networks can be filtered and monitored by the firewall to ensure the integrity of the relationship between networks.

Question: What makes a wireless network more vulnerable to unauthorized access than a wired network?

Answer: A wired network requires a node to have immediate physical access to network hardware (an Ethernet jack for instance) to try to gain access to the network. On a wireless network, however, successfully receiving the wireless signal is the only requirement for physical access. Methods that govern access to a wired network such as locked doors, specific office hours, and security cameras do not necessarily govern physical access to a wireless network.

Lab Review Questions and Answers

Question and Answers

Question: What other options exist to connect the home office employees if their role changes and requires consistent access to information on the Seattle LAN?

Answer: More bandwidth would be required, so an OC-X connection might be necessary, perhaps OC-24 or OC-48 to get close to the same bandwidth as 1000BASET Ethernet, depending on cost and availability.

Question: What infrastructure should be used to connect the conference room portion of the Seattle location?

Answer: With the conference room's size and the variance in location and mobility of users and their laptops, a wireless infrastructure should be used for the conference room, preferably the fastest available, 802.11n. Encryption should also be added to the wireless network, preferably using WPAv2 and RADIUS, the most secure and current wireless encryption protocol and also the ability to control access with the use of certificates.

Module4

Connecting Network Components

Contents:

Lesson 1: Understanding the Open Systems Interconnection Reference Model	2
Lesson 2: Understanding Media Types	3
Lesson 3: Understanding Adapters, Hubs, and Switches	5
Lesson 4: Understanding Routing	6
Module Review and Takeaways	8
Lab Review Questions and Answers	8

Lesson 1

Understanding the Open Systems Interconnection Reference Model

Contents:

This lesson does not have supplemental content.

Lesson 2

Understanding Media Types

Contents:

Question and Answers

4

Question and Answers

Discussion: What Cabling Strategy Would You Use?

Question: For Fabrikam, Inc., what cabling system would you recommend within the new building?

Answer: The reference to each workstation requiring a telephone implies that twisted-pair cabling within the building will meet the requirements and Cat 5e or 6 would deliver Gigabit Ethernet.

Question: Fabrikam's R & D center is across the private parking lot from the head offices. You will have to connect the R & D office back to the head office so that research staff has access to corporate services. What cable would you recommend for this application to link the two buildings?

Answer: Fiber-optic cabling. Currently, multimode fiber would probably do, because it is less expensive. However, 10 Gbps might not be sufficient for future applications, and it is expensive to dig up the parking lot. Single-mode fiber might be more sensible to future-proof the installation.

Lesson 3

Understanding Adapters, Hubs, and Switches

Contents:

This lesson does not have supplemental content.

Lesson 4

Understanding Routing

Contents:

Question and Answers

7

Question and Answers

Discussion: Which Routing Protocol Would You Use?

Question: For the Fabrikam scenario, would you recommend static or dynamic routing?

Answer: It depends on the number of routers involved. Static routing has the advantage of being completely predictable; it does not change unless you change it. However, there might be 20 or more networks in this organization. Because some are remotely connected, there is the possibility of link-failure. A routing protocol to provide dynamic routing would be useful in this respect.

Question: For the Fabrikam medium-sized network, is the use of a routing protocol indicated? If so, which one would you recommend?

Answer: The use of Open Shortest Path First (OSPF) would be sensible. The network is not too large to implement Routing Information Protocol (RIP). However, the presence of remote links with their potential for failure would better suit a link-state instead of a distance-vector protocol. Therefore, use OSPF instead of RIP.

Question: For the Tailspin Toys scenario, would you recommend static or dynamic routing?

Answer: With only a few routers, there is no need for dynamic routing. Static routing tables would be quick and easy to configure.

Question: For the Tailspin Toys small network, are routing tables required?

Answer: If one of the routers is also connected to the Internet, this router must be configured to choose whether to forward a packet internally to the other router or externally to the Internet. The other router can forward all none-LAN traffic to this first router and therefore only has to be configured with its LAN information.

Question: If Tailspin Toys implements an Internet connection by using a router, how would this change the configuration that you have selected?

Answer: The default gateway method would no longer work; two routers in sequence is the maximum possible.

If one of the routers is also connected to the Internet, this router must be configured to choose whether to forward a packet internally to the other router or externally to the Internet. The other router can forward all none-LAN traffic to this first router and therefore only has to be configured with its LAN information. Implementing a routing protocol would also be appropriate, but in a small scenario such as this, RIP is sufficient.

Module Review and Takeaways

Question: How does a switch differ from a hub?

Answer: Switches enable you to manage traffic in several ways: first, by segmenting the network and, second, by supporting VLANs. In addition, switches can support more advanced features, such as routing, firewalls, and QoS prioritization.

Question: You plan to implement a large, routed internetwork. What routing protocol would you consider for this completely autonomous network?

Answer: OSPF supports larger, autonomous networks.

Question: Why is coaxial cable generally not a good choice for data networks?

Answer: There are several reasons. This includes the following:

- Relatively expensive to lay
- Difficult to troubleshoot
- Does not support higher speeds of today's structured copper or fiber wiring systems.
- Coaxial cable is outdated. Most of today's devices do not include Ethernet NICs.

Lab Review Questions and Answers

Question and Answers

Question: In the lab, you were asked to consider a wiring scheme for branch offices. You were constrained by budget. Had you not been, how would that have changed your plans, if at all?

Answer: Answers will vary, but students might decide to use more fiber and opt for single-mode fiber instead of multimode fiber.

Module5

Implementing TCP/IP

Contents:

Lesson 1: Overview of TCP/IP	2
Lesson 2: IPv4 Addressing	3
Lesson 3: IPv6 Addressing	8
Lesson 4: Name Resolution	9
Module Review and Takeaways	14
Lab Review Questions and Answers	15

Lesson 1

Overview of TCP/IP

Contents:

This lesson does not have any supplemental content.

Lesson 2

IPv4 Addressing

Contents:

Demonstration

4

Demonstration

Demonstration: How to Configure IPv4

Demonstration Steps

1. On the 10967A-LON-SVR1 virtual machine, if not already done so log in as **ADATUM\Administrator** with password **pa\$\$w0rd**
 2. Open **Server Manager**, on the **Tools** menu select **DHCP**.
 3. In DHCP, expand **lon-svr1.adatum.com**, click **IPv4**, right-click on IPv4, and then select **New Scope...**
 4. In the **New Scope Wizard** click **Next**
 5. On the **Scope Name** page, in the **Name** textbox enter **Adatum**, and click **Next**
 6. On the **IP Address Range** page enter the following information then click **Next**
 - Start IP Address: **172.16.0.5**
 - End IP Address: **172.16.0.50**
 - Length: **16**
 - Subnet Mask: **255.255.0.0**
 7. On the **Add Exclusions and Delay** page click **Next**
 8. On the **Lease Duration** page click **Next**
 9. On the **Configure DHCP Options** page accept the default and click **Next**
 10. On the **Router(Default Gateway)** page enter **172.16.0.1** in the IP Address box and click **Add**, then click **Next**
 11. On the **Domain Name** and **DNS Servers** page enter the following data
 - Parent Domain box : **Adatum.com**
 - Server Name: **LON-DC1**
- And click **Resolve** and ensure the Server name resolves to **172.16.0.10** IP Address
12. Click **Add** to add the address then click **Next**
 13. On the **WINS Server** page click **Next**
 14. On the **Activate Scope** page, ensure **Yes, I want to activate this scope now** is selected, click **Next**, and then click **Finish**
 15. Expand IPv4, expand **Scope [172.16.0.0] Adatum**, and then click **Address Leases**.
 16. Verify there are no Address Leases listed.
 17. Switch to the **10967A-LON-CL1** virtual machine and if not already done so log in as **ADATUM\Administrator** with password **pa\$\$w0rd**
 18. Press the Windows logo key to display the **Start** home page and start typing **cont** until **control panel** appears. Click it when it appears.
 19. Click **Network and Internet**, click **Network and Sharing Center**, and then click **Change adapter settings**.
 20. In the **Network Connections** window, double-click **Ethernet**, and then click the **Properties** button.
 21. In the **Ethernet Properties** dialog box, locate and double-click **Internet Protocol Version 4 (TCP/IPv4)**.

22. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**, and then click **OK**.
23. In the **Ethernet Properties** dialog box, click **OK**.
24. In the **Ethernet Status** dialog box, click **Close**.
25. Return to the **10967A-LON-SVR1** virtual machine.
26. In the **DHCP** window, press **F5** to refresh the Address Leases.
27. Verify that you have a new lease for **10967A-LON-CL1**. The client was assigned the first available IP address.
28. Return to 10967A-LON-CL1.
29. Press the Windows logo key, type **cmd**, and then press **Enter**.
30. At the Command Prompt, type the following command, and then press **Enter**. Verify the IP address information.

```
ipconfig
```

31. Alternatively, in a Windows PowerShell console window you can type.

```
Get-NetIPConfiguration
```

or

```
Get-NetIPAddress
```

32. Type the following command to release the IP address, and then press **Enter**. Verify that the IP address was released.

```
ipconfig /release
```

33. Return to the **10967A-LON-SVR1** computer.
34. In the **DHCP** windows, press **F5**, and verify that the Address Lease was released.
35. Return to the **10967A-LON-CL1** computer.
36. In the **Network Connections** windows, double-click **Ethernet**. In the **Ethernet Status** dialog box, click **Properties**. In the **Ethernet Properties** dialog box, double-click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Use the following IP address**.
37. Use the following information to complete the configuration, and then click **OK**.
 - IP address: **172.16.0.20**
 - Subnet mask: **255.255.0.0**
 - Default gateway: **172.16.0.1**
 - Preferred DNS server: **172.16.0.10**
38. In the **Ethernet Properties** dialog box, click **OK**.
39. Alternatively, you can use Windows PowerShell to disable DHCP and then assign new IP address information. You can do this by typing the following in a Windows PowerShell console.

```
Get-NetIPInterface
```

In the output, identify the Index number on the left side associated with the IPv4 addresses that have DHCP enabled and write the number down [x]. Then type the following.

```
Set-NetIPInterface -InterfaceIndex [x] -dhcp disabled
New-NetIPAddress -InterfaceIndex [X] -IPAddress 172.16.0.20 -PrefixLength 16 -
DefaultGateway 172.16.0.1
```

Followed by

```
Set-DNSClientServerAddress -InterfaceIndex [X] -ServerAddresses 172.16.0.10
```



Note: Leave the virtual machines running for the next demonstration.

Demonstration: How to Verify IPv4 Configuration

Demonstration Steps

1. On the 10967A-LON-CL1, sign in as **ADATUM\Administrator** with password **Pa\$\$w0rd**
2. Hover the mouse over the bottom left corner and right-click and from the resultant menu select **Command Prompt (Admin)**
3. At the Command Prompt, type the following command, and then press **Enter**.

```
ipconfig /all
```

4. Discuss the information returned by the command, including Host Name and DHCP Enabled.
5. Use the student notes to discuss the **release** and **renew** switches.
6. Switch to the **10967A-LON-SVR1** virtual machine.
7. In the **DHCP** window, right-click **lon-svr1.adatum.com**, select **All Tasks**, and then click **Stop**. Notice the warning that the DHCP server cannot be found.
8. Switch to the **10967A-LON-CL1** virtual machine.
9. In **Ethernet** status dialog box, click the **Properties** button, and in the **Ethernet** dialog box, double-click **Internet Protocol Version 4 (TCP/IPv4)**.
10. Click **Obtain an IP address automatically**, click **Obtain DNS server address automatically**, click **OK**, and then click **OK** again to apply the changes.
11. Switch to the **Command Prompt**.
12. At the Command Prompt, type the following command, and then press **Enter**.

```
ipconfig
```

13. What IPv4 address is listed?

Answer: The address begins with 169.254.

14. What does the IP address mean?

Answer: The computer is using an APIPA address because it has failed to obtain an address from a DHCP server.

15. At the Command Prompt, type the following command, and then press **Enter**.

```
ping lon-dc1.adatum.com
```

Alternatively, you can type the following in a Windows PowerShell console.

```
Test-Connection LON-DC1.Adatum.com
```

16. You are not successful.

17. Switch to 10967A-**LON-SVR1**.

18. In DHCP, right-click **lon-svr1.adatum.com**, point to **All Tasks**, and then click **Start**.

19. Switch to **10967A-LON-CL1**. At the Command Prompt, type the following command, and then press **Enter**.

```
ipconfig /renew
```

20. What IPv4 address is listed?

Answer: The address begins 172.16.0.

21. What does this IP address mean?

Answer: The computer has successfully obtained an IPv4 address.

22. At the Command Prompt, type the following command, and then press **Enter**.

```
ping 1on-dc1.adatum.com
```

23. You are successful.

24. As you have time, discuss **tracert** and **pathping** or compare these with the Windows PowerShell equivalent, **Get-NetRoute**.



Note: Leave the virtual machines running for the next demonstration.

Lesson 3

IPv6 Addressing

Contents:

This lesson does not have any supplemental content.

Lesson 4

Name Resolution

Contents:

Question and Answers	10
Demonstration	10

Question and Answers

How Internet DNS Names Are Resolved

Question: Which computers in your organization should have an A record configured?

Answer: Most likely all of the organizations computers are A records. "A" records are required to map host names to IPv4 addresses, which most of the computers and nodes on the network will have.

Demonstration

Demonstration: How to Troubleshoot Name Resolution

Demonstration Steps

This demonstration provides steps for just the command-line tools and not for the Windows PowerShell commands, to avoid any confusion and in an attempt to save time. Some details are present in the student handbook if you want to use the Windows PowerShell commands and time allows.

1. Switch to the LON-DC1 computer.
2. Log on by using the following information:
 - o Username: **Administrator**
 - o Password: **Pa\$\$w0rd**
 - o Domain: **Adatum**
3. In the **Server Manager**, on the **Tools** menu, select **DNS**.
4. In **DNS Manager**, right-click **LON-DC1**, point to **All Tasks**, and then click **Stop**.
5. As you have time, discuss the forward and reverse lookup zones.
6. Switch to LON-CL1.
7. At a Command Prompt, type the following command, and then press **Enter**.

```
ping lon-dc1.adatum.com
```

8. The ping may be successful if the details are stored in the local cache.
9. At the Command Prompt, type the following command, and then press **Enter**.

```
ipconfig /flushdns
```

10. At the Command Prompt, type the following command, and then press **Enter**.

```
ping lon-dc1.adatum.com
```



Note: You are not successful.


11. Switch to the LON-DC1 computer.
12. In **DNS Manager**, right-click **LON-DC1**, point to **All Tasks**, and then click **Start**.
13. Switch to the **LON-CL1** computer.
14. At the Command Prompt, type the following command, and then press **Enter**.

```
ping lon-dc1.adatum.com
```


 **Note:** The only record listed is that of the LON-DC1.adatum.com server.

15. At the Command Prompt, type the following command, and then press **Enter**.

```
ipconfig /displaydns
```

 **Note:** The only record listed is that of the LON-DC1.adatum.com server.

16. At the Command Prompt, type the following command, and then press **Enter**.

```
nslookup -d2 lon-dc1.adatum.com. > C:\file.txt
```

17. At the Command Prompt, type the following command, and then press **Enter**.

```
notepad C:\file.txt
```

18. Review the file and discuss the name resolution process.
19. In the first section of the following output sample, the client resolver performs a reverse lookup to determine the DNS server host name. You can view the query 172.16.0.10.in-addr.arpa, type = PTR, class = IN in the QUESTIONS section. The returned result is a time out as per the below as no reverse lookup zone exists

```
-----
SendRequest(), len 42
HEADER:
opcode = QUERY, id = 1, rcode = NOERROR
header flags: query, want recursion
questions = 1, answers = 0, authority records = 0, additional = 0
QUESTIONS:
10.0.16.172.in-addr.arpa, type = PTR, class = IN
-----
DNS request timed out
    Timeout was 2 seconds.
Timeout (2secs)
Server: Unknown
Address: 172.16.0.10
-----
```

20. Switch to the **LON-DC1** computer.
21. In **DNS Manager**, expand **LON-DC1**, right-click **Reverse Lookup Zones** and select **New Zone...**
22. On the **Welcome to the New Zone Wizard** click **Next**
23. On the **Zone Type** page select **Primary zone**, ensure the **Store the zone in Active directory** checkbox is selected and click **Next**
24. On the **Active Directory Zone Replication Scope** page click **Next**
25. On the **Reverse Lookup Zone Name** page, ensure **IPv4** is selected and click **Next**
26. On the **Reverse Lookup Zone Name** page, enter **172.16.0** and click **Next**
27. On the **Dynamic Update** page click **Next**
28. On the **Completing the New Zone Wizard** page click **Finish**
29. Right-click the **0.16.172.in-addr.arpa** zone underneath **Reverse Lookup Zones** and select **New Pointer (PTR)...**

30. In the **New Resource Record** dialog select **Browse...** click on **LON-DC1**, double-click **Forward Lookup Zones**, double-click **Adatum.com**, click **lon-dc1**, click **OK**, and then click **OK** again.
31. Notice the new PTR record that's been created.
32. Switch to the **LON-CL1** computer
33. At the Command Prompt, type the following command, and then press **Enter**.

```
nslookup -d2 lon-dc1.adatum.com. > C:\file1.txt
```

34. At the Command Prompt, type the following command, and then press **Enter**.

```
notepad C:\file1.txt
```

35. Review the file and discuss the name resolution process.
36. Again In the first section of the following output sample, the client resolver performs a reverse lookup to determine the DNS server host name. You can view the query 172.16.0.10.in-addr.arpa, type = PTR, class = IN in the QUESTIONS section. Except this time it is resolved successfully indicated by the value, name = lon-dc1.adatum.com, which identifies the host name of the petitioned DNS server.

```
-----
SendRequest(), len 42
HEADER:
opcode = QUERY, id = 1, rcode = NOERROR
header flags: query, want recursion
questions = 1, answers = 0, authority records = 0, additional = 0
QUESTIONS:
10.0.16.172.in-addr.arpa, type = PTR, class = IN
-----
-----
Got answer (74 bytes):
HEADER:
opcode = QUERY, id = 1, rcode = NOERROR
header flags: response, auth. answer, want recursion, recursion avail.
questions = 1, answers = 0, authority records = 1, additional = 0
QUESTIONS:
10.0.16.172.in-addr.arpa, type = PTR, class = IN
ANSWERS:
-> 10.0.16.172.in-addr.arpa
type = PTR, class = IN, dlen = 20 name = lon-dc1.adatum.com
ttl = 3600 (1 hour)
-----
Server: lon-dc1.adatum.com
Address: 172.16.0.10
```

37. Scroll down in the File1.txt file to the section starting with **SendRequest (), len 36**. In the following section, the client resolver performs a recursive query of the DNS server for the host lon-dc1.adatum.com, type = A, class = IN. The returned result is shown in the ANSWERS section within the Got Answer section, as shown in the following code in bold. Notice that the answer also includes a time-to-live (TTL) value, which determines how long the record is valid.

```
-----
SendRequest(), len 36
HEADER:
opcode = QUERY, id = 4, rcode = NOERROR
header flags: query, want recursion
questions = 1, answers = 0, authority records = 0, additional = 0
QUESTIONS:
lon-dc1.adatum.com, type = A, class = IN
-----
-----
```

```

Got answer (52 bytes):
HEADER:
opcode = QUERY, id = 4, rcode = NOERROR
header flags: response, auth. answer, want recursion, recursion avail.
questions = 1, answers = 1, authority records = 0, additional = 0
QUESTIONS:
lon-dc1.adatum.com, type = A, class = IN
ANSWERS:
-> lon-dc1.adatum.com
type = A, class = IN, dlen = 4
internet address = 172.16.0.10
ttl = 3600 (1 hour)

```

38. In the remaining section, the client resolver performs a query for the IPv6 address of the lon-dc1 host, as indicated in the QUESTIONS section by the quad A record indicator 'AAAA'. There is no Answer returned for this query, as indicated by the lack of an ANSWERS section at the bottom as shown in previous examples.

```

-----
SendRequest(), len 36
HEADER:
opcode = QUERY, id = 5, rcode = NOERROR
header flags: query, want recursion
questions = 1, answers = 0, authority records = 0, additional = 0
QUESTIONS:
lon-dc1.adatum.com, type = AAAA, class = IN
-----
Got answer (83 bytes):
HEADER:
opcode = QUERY, id = 5, rcode = NOERROR
header flags: response, auth. answer, want recursion, recursion avail.
questions = 1, answers = 0, authority records = 1, additional = 0
QUESTIONS:
lon-dc1.adatum.com, type = AAAA, class = IN
AUTHORITY RECORDS:
-> adatum.com
type = SOA, class = IN, dlen = 35
ttl = 3600 (1 hour)
primary name server = lon-dc1.adatum.com
responsible mail addr = hostmaster.adatum.com
serial = 34
refresh = 900 (15 mins)
retry = 600 (10 mins)
expire = 86400 (1 day)
default TTL = 3600 (1 hour)
-----
Name: lon-dc1.adatum.com
Address: 172.16.0.10

```

39. Revert the virtual machines.

Module Review and Takeaways

Question: NetBIOS operates at which layer of the OSI reference model?

Answer: NetBIOS is a session management protocol and operates at layer 5 of the OSI reference model.

Question: Which transport layer protocol provides for connectionless oriented delivery in IP-based networks?

Answer: UDP.

Question: Your host computer was assigned the following IPv4 configuration: 10.10.16.1/20. The default gateway is 10.10.8.1. You are experiencing communications problems. Why?

Answer: Either the default gateway is wrong (it should be in the same subnet: 10.10.16.0/20) or else the host has the wrong IP address and should have an address in the range 10.10.8.2>10.10.15.254.

Question: You do not want to implement WINS in the network. However, you do have some legacy applications that require Short name resolution. How could you manage short names within your existing DNS infrastructure?

Answer: Implement the GlobalNames Zone within DNS and manually add alias records into the zone for the legacy names.

Do not mix up the fact that we say short names to mean NetBIOS. Applications usually don't care about the protocol, but they either want to resolve short names or Fully Qualified Domain Names (FQDNs). If they need short names and are in different DNS domains (and the name that should be resolved is not in a hierarchically parent DNS zone), measures must be taken to enable the short names to be resolved, by either implementing a CNAME in the same domain where the client resides or by using the Globalnames zone.

You should be clear that **shortnames do not equal NetBios**. This is be a common misconception and can result in some companies struggling to migrate from WINS.

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

Answer: Clear the resolver cache. You can do this at the Command Prompt by using **Ipconfig.exe /flushdns**. Or, in Windows PowerShell using the **Clear-DNSClientcache** cmdlet. Also, you can use **NSLookup** to determine whether the cache is being used.

Tools

Tool	Use	Where to find it
Ipconfig.exe	Verifying and testing IP configuration.	Command Prompt
Nslookup.exe	Troubleshooting DNS.	Command Prompt
Ping.exe	Verifying basic IP functionality and that another computer is contactable.	Command Prompt
Netsh.exe	Configuring network settings, including IP settings, from the command line.	Command Prompt
Test-Connection	Functionality similar to ping . You can ping multiple computers concurrently by using Test-Connection.	Windows PowerShell

Tool	Use	Where to find it
Resolve DNS-Cache	Type help *DNS* in the Windows PowerShell console to see a list of Windows PowerShell commands that might help when troubleshooting or configuring DNS.	Windows PowerShell
Get-NetIPAddress	Similar to subset of functionality in the older IPConfig command.	Windows PowerShell
Get-NetIPConfiguration	Similar to subset of functionality in older IPConfig command. As described earlier, type help *NET* in the Windows PowerShell console to see a list of Windows PowerShell commands that might help when troubleshooting or configuring DNS.	Windows PowerShell

Lab Review Questions and Answers

Question and Answers

Question: In the lab, you were tasked with providing an addressing scheme that would accommodate 100 hosts per subnet. Ed provided the first subnet ID of 172.16.16.0/20. How many hosts could be accommodated within this subnet?

Answer: A 20 bit subnet mask leaves 12 bits for host addresses. $2^{12} - 2 = 4,094$ hosts. 172.16.16.0 can accommodate no more than 4,094 hosts.

Question: The subnet might grow. If you had to accommodate 100 addresses, what would you recommend as the subnet mask?

Answer: 100 hosts could be expressed in 7 binary bits. $2^7 - 2 = 126$. Therefore, a subnet mask of 25 would be appropriate. However, 24 would be more sensible as it allows for growth of the number of hosts.

Question: What would the first subnet address be?

Answer: Assuming 24 bits, the first subnet would be 172.16.1.0/24, the next would be 172.16.2.0 and so on.

Module6

Windows Server Roles

Contents:

Lesson 1: Role-Based Deployment	2
Lesson 2: Deploying Role-Specific Servers	4
Lesson 3: Considerations for Provisioning Roles	7
Module Review and Takeaways	8
Lab Review Questions and Answers	8

Lesson 1

Role-Based Deployment

Contents:

Demonstration

3

Demonstration

Demonstration: How to Deploy Server Roles and Features

Demonstration Steps

1. Ensure you are signed in to the **10967A-LON-DC1** virtual machine.
2. In Server Manager, click the **Manage** menu, and show the **Add Roles and Features** and the **Remove Roles and Features** selections.
3. Select **Add Roles and Features**.
4. Click **Installation Type** and discuss how the wizard can be used on a physical computer, virtual machine, or offline virtual hard disk (VHD).
5. Click **Server Selection** and discuss how the wizard can be used on any server in the server pool.
6. Click **Server Roles**, and scroll through the **Roles** pane, pointing out the server roles that were discussed in this lesson.
7. Click the **DHCP Server** label (not the check box) and discuss the description on the right side.
8. Select the **DHCP Server** check box and discuss how different server roles require different features.
9. Click the **Add Features** button.
10. Show how the **DHCP Server** check box is now selected and click **Next**.
11. On the **Features page**, scroll through the additional features that could be selected.
12. As you have time, discuss several of the features.
13. In the navigation pane, click **DHCP Server**, and discuss how certain roles might have helpful hints.
14. Discuss how the Add Roles and Features Wizard only provides installation and that additional configuration of the server role might be required. Give an example of authorizing the DHCP server or assigning IP addresses to the Dynamic Host Configuration Protocol (DHCP) server.
15. Click **Confirmation**, and discuss and then check the **Restart the destination server automatically if required** check box and then click **Yes** in the resultant dialog.
16. On the **Confirm installation selections** page, click the **Export Configuration Settings** link.
17. In the **Save As** dialog box, in the navigation pane under **Libraries**, click **Documents**, in the **File name:** box type **LON-DC1 DHCP Server Role Install**, and then click **Save**.
18. On the Confirm installation selections page, click **Install**.
19. On the **Installation progress** page, click **Close**. Point out to students that the install will run in the background with the wizard closed.
20. In Server Manager click the **Notification Flag** icon at the top of the console. Point out to students that you can view the progress of the installation here and it will also tell you when it is complete.
21. On the taskbar, click **File Explorer**, double-click **Documents**, right-click **LON-DC1 DHCP Server Role Install**, click **Open with**, and then click **Notepad**.
22. Review the XML code in the configuration file. This file contains the configuration settings that were generated automatically as you ran through the Add Roles and features Wizard. You can now use or customize this file for automation purposes to install the role on this or multiple servers.
23. Close Notepad, and then close **File Explorer**.
24. Revert the virtual machines before the next demonstration.

Lesson 2

Deploying Role-Specific Servers

Contents:

Question and Answers	5
Demonstration	5

Question and Answers

What Is a Remote Access Server?

Question: What are some examples of security concerns for data that is accessed remotely?

Answer: Concerns for data that is accessed remotely include the following:

- Use of packet sniffers to capture data in transit.
- Storage of files on remote systems that are not secure.
- Transmission of user names and passwords over the Internet.
- Data that is stored on mobile devices and laptops that are lost or stolen.
- Computers or devices accessing the network and carrying viruses that could potentially spread that virus throughout the network.

Demonstration

Demonstration: Remotely Manage Windows Server 2012 Servers

Demonstration Steps

1. Ensure you are signed on to 10967A-LON-CL1.
2. Click the Windows logo key, type **run**, and then press **Enter**
3. In the **Run** textbox type the following and press **Enter**.

```
\\LON-DC1\E$
```

4. If prompted, provide the credentials **ADATUM\Administrator** and password **Pa\$\$word**
5. Go to the folder ...**mod06\Labfiles** and copy the file **Windows6.2-KB2693643-x64.msu** to the **Desktop** and then double-click it
6. In the **Windows Update Standalone** installer dialog click **Yes**
7. In the **Download and Install Updates license terms** window click **I Accept**
8. In the installation complete dialog click **Restart Now**

Or if you are not given a restart option, only a Close option, click **Close**, then hover the mouse in the bottom right hand corner of the task bar, select **Settings**, then **Power**, then **Restart**

9. The **10967A-LON-CL1** virtual machine will update and restart. This will take approx. 5 minutes
10. After 10967A-LON-CL1 restarts log on with the credentials **ADATUM\Administrator** and password **Pa\$\$w0rd**
11. Scroll across to the right side of the Start Menu and notice the presence of **Administrative Tools** and **Server Manager** icons. Click on **Server Manager**
12. In Server Manager within the Dashboard section click on the **Create a server group** link.
13. In the **Server group name** box type **LON Servers**
14. Click the **DNS** tab.
15. In the **Search:** box type **LON-DC1** and press search icon. LON-DC1.adatum.com should be returned and click the arrow to add the server to the selected box on the right side.
16. In the **Search:** box type **LON-SVR3** and press search icon. LON-SVR3.adatum.com should be returned and click the arrow to add the server to the selected box on the right side

17. Click **OK**
18. Click the **LON Servers** group on the left side
19. Right click on LON-SVR3 and select **Add Roles and Features**
20. In the **Add Roles and Features Wizard** click **Next**.
21. On the **Installation Type** page click **Next**
22. On the **Server selection** page click lon-svr3.Adatum.com and click **Next**
23. On the **Server Roles** page select **Web Server (IIS)** and click **Next**
24. Click **Next** through the remaining pages, click **Install**, and then close the wizard when installation begins
25. Click the **LON Servers** group on the left side
26. Right click on **LON-DC1** and select **Add Roles and Features**
27. In the **Add Roles and Features Wizard** click **Next**.
28. On the **Installation Type** page click **Next**
29. On the **Server selection** page click lon-dc1.Adatum.com and click **Next**
30. On the **Server Roles** page select **Print and Document Services** and click **Next**
31. Click **Add Features** button when prompted
32. Click **Next** through the remaining pages, click **Install**, and close the wizard when as soon as the installation begins.
33. Click the **Notification Flag** icon in Server Manager and view the status of the Role installations
34. Click the **LON Servers** group on the left side again.
35. Click on **LON-DC1** press **CTRL** and click **LON-SVR3** then right-click on the highlighted servers.
36. In the resultant menu select **Restart Server**.
37. In the resultant prompt ensure **LON-DC1** and **LON-SVR3** are listed and click **OK**
38. Switch to the LON-DC1 and LON-SVR3 servers and show students that they are restarting as specified.

Call out to students that you can have many more servers as member of a Server Group and managing in bulk can reduce Administrative overhead. If you have time you can also step through some other management items in the server group management list when you click on the two servers

39. Revert the virtual machines.

Lesson 3

Considerations for Provisioning Roles

Contents:

This lesson does not have any supplemental content.

Module Review and Takeaways

Best Practice

- Supplement or modify the following best practices for your own work situations:
- Combine multiple roles on a single server when you deploy servers in smaller organizations; scale out these roles in larger organizations so that you can optimize performance.

Question: How is a server role different from a server feature?

Answer: A server role defines primary functionality, whereas a server feature adds supplementary or supporting functions to server roles.

Tools

Tool	Use for	Where to find it
Server Manager	Managing server configuration, including adding roles and features.	Start Menu
Windows PowerShell	Managing both Server Manager; most server roles have cmdlets available to support them.	Windows PowerShell console

Lab Review Questions and Answers

Question and Answers

Question: When installing the File Services role during the lab, which role services might prove especially useful for a branch office?

Answer: BranchCache® would be useful for certain situations.

Module7

Implementing Active Directory

Contents:

Lesson 1: Introducing Active Directory Domain Services	2
Lesson 2: Implementing AD DS	4
Lesson 3: Managing Users, Groups, and Computers	6
Lesson 4: Implementing Group Policy	8
Module Review and Takeaways	11
Lab Review Questions and Answers	12

Lesson 1

Introducing Active Directory Domain Services

Contents:

Question and Answers	3
Demonstration	3

Question and Answers

Implementing Organizational Units

Question: Describe a scenario in which you would use a domain to organize a network. Describe a scenario in which you would use an OU to organize a network.

Answer: Answers may vary. Students should understand that a domain represents an administrative boundary and requires at least one domain controller. You would use domains to cluster the management and administrative tasks of an organization. The level to which the domain is broken down depends on the organizational structure. Typically, it makes sense to keep the number of domains to a minimum. Organize the domains at a high level based geographical location. Because multiple OUs can exist in a single domain, OUs are useful for mapping the logical structure of Active Directory to the actual structure of the organization. This is a more fine-grained structure. OUs can be used instead of domains to define different administrative organizations. The administrative structure is the main reason for the OU model.

Demonstration

Demonstration: How to Manage Organizational Units

Demonstration Steps

1. Make sure that you are logged on to the 10967A-LON-DC1 virtual machine.
2. In Server Manager, point to **Tools**, and then click **Active Directory Administrative Center**.
3. Double-click **Adatum (local)**, and point to the **Sales** OU. Double-click the **Sales** OU, and notice **Claus Hansen** is not a member of the group.
4. Double-click **Adatum (local)**, and then double-click the **Users** container, double-click the **Domain Users** group, click **Members**, and locate **Claus Hansen**.
5. Double-click **Claus Hansen**, and then in the **Tasks** drop-down list, select **Move**.
6. In the **Move** dialog box, click **Sales** in the middle column, and then click **OK**.
7. Close the **Domain Users** windows by clicking the **X** icon.
8. Return to the **Sales** OU, press **F5** to refresh the information, and verify that **Claus Hansen** is in the group.
9. As you have time, show other objects in the Adatum domain.
10. Leave the virtual machines running for the next demonstration.

Lesson 2

Implementing AD DS

Contents:

Question and Answers

5

Question and Answers

What Is a Read-Only Domain Controller?

Question: In your work environment, do you have scenarios where an RODC could be used?

Answer: Answers may vary. RODCs are useful in remote sites with limited WAN bandwidth, locations with less physical security, or perimeter network or edge placements.

Lesson 3

Managing Users, Groups, and Computers

Contents:

Question and Answers	7
Demonstration	7

Question and Answers

What Are Groups?

Question: Describe a situation where you would use a distribution group instead of a security group.

Answer: Answers will vary. You would use a distribution group when security is not required, such as an email distribution lists. The main benefit of using distribution groups becomes more evident in large scale Exchange deployments, especially where there may be a need to nest these distribution groups

Demonstration

Demonstration: How to Manage Accounts

Demonstration Steps

1. Make sure that you are logged on to the 10967A-LON-DC1 virtual machine.
2. Open Server Manager, click **Tools**, and then click **Active Directory Users and Computers**.
3. Click **Adatum.com**.
4. In the Results pane, right-click **Users**, click **New**, and then click **User**.
5. In the **New Object - User** dialog box, in the **First name** text box, type **Jeff**.
6. In the **Last name** text box, type **Hay**.
7. In the **User logon name** text box, type **Jeffh**, and then click **Next**.
8. In the **Password** text box, type **Pa\$\$w0rd**.
9. In the **Confirm password** text box type **Pa\$\$w0rd**, click **Next**, and then click **Finish**.
10. Verify **Jeff Hay** was created in the **Users** container.
11. Double-click **Jeff Hay**, and then select the **Member Of** tab.
12. Notice that **Jeff Hay** is a member of the **Domain Users** group.
13. Click **Add**. Then in the **Enter the object names to select (examples):** text box, type **Domain Admins**, click **Check Names**, and then click **OK**.
14. Verify that **Jeff Hay** is now a member of the **Domain Admins** group, and then click **OK** to close Jeff Hay Properties window.
15. Right-click **Sales**, and then click **Delegate Control**.
16. In the **Delegation of Control Wizard**, on the **Welcome to the Delegation of Control Wizard** page, click **Next**.
17. On the **Users** or **Groups** page, click **Add**.
18. In the **Select Users, Computers, or Groups** dialog box, in the **Enter the object names to select (examples)** text box, type **Jeff Hay**, click **Check Names**, and then click **OK**.
19. On the **Users** or **Groups** page, click **Next**.
20. On the **Tasks to Delegate** page, select the **Create, delete and manage user accounts** checkbox.
21. As you have time, discuss the common tasks that might be delegated, click **Next**, and then click **Finish**.
22. Leave the virtual machines running for the next demonstration.

Lesson 4

Implementing Group Policy

Contents:

Question and Answers	9
Demonstration	9

Question and Answers

Applying GPOs

Question: What would be some advantages and disadvantages to lowering the refresh interval?

Answer: Advantages

- Provides faster updates for new settings
- Makes sure that mobile users receive the latest updates

Disadvantages

- Increases network traffic
- Consumes more local computer resources to check for updates

Demonstration

Demonstration: How to Create a GPO and Link It to an Organizational Unit

Demonstration Steps

1. Make sure that you are logged on to the LON-DC1 virtual machine.
2. In Server Manager, click **Tools**, and then click **Group Policy Management**.
3. Expand **Forest: Adatum.com**, expand **Domains**, and then expand **Adatum.com**.
4. Right-click **Group Policy Objects**, and then click **New**.
5. In the **New GPO** dialog box, in the **Name** text box, type **Disable CAD Task Manager**, and then click **OK**.
6. Expand Group Policy Objects, right-click **Disable CAD Task Manager**, and then click **Edit**.
7. In the Group Policy Management Editor, expand **User Configuration**, expand **Policies**, expand **Administrative Templates**, expand **System**, and then click **Ctrl+Alt+Del Options**.
8. In the Results pane, double-click **Remove Task Manager**.
9. In the **Remove Task Manager** dialog box, click **Enabled**, and then click **OK**.
10. Close the Group Policy Management Editor.
11. In the Navigation pane, right-click **Sales**, and then click **Link an Existing GPO**.
12. In the **Select GPO** dialog box, in the **Group Policy objects** list, click **Disable CAD Task Manager**, and then click **OK**.
13. Close Group Policy Management.
14. Switch to the LON-CL1 computer.
15. Sign in to the 10967A-LON-CL1 as **Adatum\Joanna** with the password of **Pa\$\$w0rd**.
(Joanna Yuan is a member of the Sales group)
16. If you are prompted, change the password to **Pa\$\$w0rd1**, and then click **OK**.
17. In the window which contains the **10967A-LON-CL1** virtual machine click the **Ctrl+Alt+Delete** button in the top left corner to get to the virtual machine sign in options.
18. Does Start Task Manager display as an option in the list of items?

Answer: No

19. Sign out of 10967A-LON-CL1

20. Sign into 10967A-LON-CL1 as **ADATUM\Administrator** with the password of **Pa\$\$w0rd**.
21. Again, in the window which contains the **10967A-LON-CL1** virtual machine click the **Ctrl+Alt+Delete** button in the top left corner to get to the virtual machine sign in options.
22. Does Start Task Manager display as an option?

Answer: Yes.

23. Revert the virtual machines.

Module Review and Takeaways

Question: For most organizations, how many AD DS forests are required?

Answer: One. Multiple forests enable organizations to create separate administrative security boundaries. This is not a requirement for most organizations. Separate administration is also done with delegation.

Question: If you are installing an AD DS-compatible email application, what implications does this have for your AD DS schema?

Answer: If adding Microsoft Exchange Server, it will change the schema. However, just because the email application is compatible with Active Directory does not necessarily mean that the schema will change.

Lotus Notes works with Active Directory. Active Directory accounts can be used for logging on to Lotus Notes, and you can extend Lotus Notes to use Active Directory as an LDAP-based Phonebook. However, it does not extend the schema.

Also, other applications can be compatible without extending the schema. Therefore, you have to assess and understand what the implications are before integrating your email application.

Question: What trusts are implemented between domains in a single forest?

Answer: Automatically created two-way, transitive trusts

Question: Why create organizational units?

Answer: OUs are useful in grouping and organizing objects for administrative purposes, such as delegating administrative rights and assigning policies to a collection of objects as a single unit.

Tools

Tool	Use for	Where to find it
Active Directory Users and Computers	Managing objects within AD DS such as users, groups, and computers	Server Manager
Active Directory Administrative Center	Managing objects within AD DS such as users, groups, and computers	Server Manager
Group Policy Management Console (GPMC)	Creating, managing, and editing Group Policy objects (GPOs)	Server Manager
Group Policy Management Editor	To edit Group Policy settings and preferences	By editing a GPO in GPMC, you can access the Group Policy Management Editor
Windows PowerShell cmdlets	Available in the Windows PowerShell console	Available for Active Directory and Group Policy
Command-line tools such as dsget , dsquery , dsmod , ntdsutil , and more	Allow for configuration and management of objects	Command Prompt

Lab Review Questions and Answers

Question and Answers

Question: In the lab, you used Active Directory Administrative Center to manage accounts. What other tool could you use?

Answer: Active Directory Users and Computers, Windows PowerShell, or command line tools.

Question: In the lab, you added Tony Allen, a single user, to a management group. Why not grant Tony the required permissions directly?

Answer: If Tony changes job roles, you will have to revoke his management permissions and grant the new user permissions. It is easier to grant the permissions to a group and add or remove users from the group—thereby granting or revoking their management permissions.

Module8

Implementing IT Security Layers

Contents:

Lesson 1: Overview of Defense-in-Depth	2
Lesson 2: Physical Security	4
Lesson 3: Internet Security	5
Module Review and Takeaways	9
Lab Review Questions and Answers	10

Lesson 1

Overview of Defense-in-Depth

Contents:

Question and Answers

3

Question and Answers

What Is Defense-In-Depth?

Question: How many layers of the defense-in-depth model should be secured?

Answer: All of them should be secured to some extent. The actual measures that are implemented should be based on the needs and budget of the organization.

Lesson 2

Physical Security

Contents:

This lesson does not have supplemental content.

Lesson 3

Internet Security

Contents:

Demonstration

6

Demonstration

Demonstration: How to Secure Internet Explorer

Demonstration Steps

Enable the Menu Bar

1. Ensure you are logged on to the **10967A-LON-CL1** virtual machine using credentials **ADATUM\Administrator** and password **Pa\$\$w0rd**.
2. Go to the **Desktop**, and then click the **Internet Explorer** icon in the taskbar
3. Right-click beside the tabs at the top of the Internet Explorer window and then select **Status bar**
4. Repeat Step 3 for the **Menu bar** and **Command bar**



Note: The content on the websites called out in these demo steps is constantly changing, as such the behavior called out on specific websites may alter over time. You should step through the demo prior to carrying it out to ensure the functionality you expect is still present and the website hasn't changed, thus altering the functionality.

Filter ActiveX controls

1. On 10967A-LON-CL1 Click **Tools and select** ActiveX Filtering
2. Go to www.microsoft.com
3. Notice a blue circle with a line through the middle now present in the address bar. **Click on this blue circle in the address bar.**

(If this icon does not appear go to an alternative media rich website)

4. A message may appear stating that some content is filtered on this site and you have the option to **Turn off ActiveX Filtering**.
5. Click the **Turn off ActiveX Filtering** button.
6. Now click again on the blue circular icon in the address bar again and notice the message now states that no content is filtered on this site.
7. Click **X** to close the message box.
8. Click **Tools**, then click **Manage Add-ons**, examine the various **Add-on Types**, and then click **Close**.

View Security Reports

1. Go to the website **<https://www.microsoft.com>**. Notice the secure https connection.
2. Notice the presence of a **lock icon** now appearing in the address bar
3. Click the **lock icon**
4. A website identification dialog appears which contains information about the identity of the website and who if anyone has identified the site, if the site has a certificate. You can also view the certificate. You should discuss this with students.
5. Click the **X** icon to close the message box.

Certificate Errors

1. Go to the website **<https://www.msn.com>**
2. The page does not display correctly and you receive a message stating **There is a problem with this website's security certificate.**

3. Notice several options are listed: Click here to close this webpage, Continue to this website (not recommended), and More Information.

Manage Add-ons

1. In Internet Explorer go to Tools then select **Manage add-ons**
2. **There may not be a lot of add-ons** installed on the browser as not many sites have been accessed
3. However talk through the settings that are there, stating that add-ons can significantly affect browser performance as they accumulate over time. Explain that you can pro-actively enable, disable or uninstall add-ons using the **Manage Add-ons** console
4. Click **Close** to close the Manage Add-ons window

IE Enhanced Security Configuration

1. Switch to **10967A-LON-DC1**
2. In **Server Manager** click on **Local Server**
3. In the **Properties** pane click on the **IE Enhanced security Configuration (IE ESC) On** setting link
4. In the **IE ESC dialog** notice the settings that are available and discuss them, saying this is present only on server.
5. You should also call out that you would not typically use web browsing on production servers, and most organizations would disable it and in some cases block the port as well.
6. You may also want to show and talk about Protected mode in Internet Options in Internet Explorer, which is present on server and client.

If no Internet Access is available you can do some limited demonstrations with the following steps. If you have Internet Access you can still carry out these steps

We will carry out these steps on **10967A-LON-DC1**, as there are more restrictive security settings and as such provides us with more options to easily access security and configuration settings for IE.

1. On 10967A-LON-DC1, In Internet Explorer if not already done so, right-click beside the tabs at the top of the Internet Explorer windows and select **Status bar**
2. Repeat Step 1 for the **Menu bar** and **Command bar**
3. In Internet Explorer, in the Address bar, type **http://lon-dc1/intranet**, and then press **Enter**.
4. On the **A. Datum Intranet Home Page** website, click **Current Projects**.
5. Verify the **Current A. Datum Projects** page displays correctly in a new browser page window, but there are no names listed under **Project** and **Project Lead**. Also, verify a message appears stating an add-on was blocked.
6. Click on **Tools** then **Internet Options**, then go to the **Security** tab
7. Click **Trusted Sites** then click **Sites**
8. Uncheck the Require server verification (https:) for all sites in this zone checkbox
9. Ensure http://lon-dc1/Intranet is listed in the **Add this website to the zone:** box and click **Add**
10. Click **Close** then click **OK**
11. Click **Tools** and ensure **Active Filtering** is turned off
12. Close **Internet Explorer** then open it again and go to the website http://lon-dc1/intranet
13. Click **Current Projects** and verify the projects page opens successfully and all names are listed under the **Project** and **Project Lead** columns

14. In Internet Explorer click **Tools** and then click **Manage Add-ons**.
15. Click Toolbars and Extensions then click on **Tabular Data Control**
16. Notice the data associated with the add-on then click **Disable**
17. Click **Close**.

IE Enhanced Security Configuration

You can repeat the steps under the IE Enhanced Security Configuration section called out earlier.

Module Review and Takeaways

Best Practice

Best practices for implementing defense-in-depth.

- Supplement or change the following best practices for your own work situations:
- Create specific rules that help prevent social engineering and educate users on these rules and their relevance.
- Restrict physical access to servers by locking doors and then monitor server room access.
- Implement firewalls at network boundaries.
- Implement NAT.
- Use virtual private networks (VPNs) and implement network encryption.
- Segment the network.
- Require mutual authentication.
- Restrict switch ports and wireless access points based on media access control (MAC) address or client certificates.
- Harden operating systems.
- Monitor access attempts.
- Implement antivirus and antispymware software.
- Implement host-based firewalls.
- Run applications that have the least user rights possible.
- Install security updates.
- Enable only required features and functionality.
- Implement and configure suitable NTFS or ReFS file system permissions.
- Implement file and volume encryption.
- Implement rights management.

Question: Why is it important to educate users about your organization's acceptable use policy?

Answer: Security starts at the human layer. If users are unaware of rules, they cannot be expected to follow them. Therefore, they will not be followed.

Question: How could you help reduce the risk that your wireless network is the target of unauthorized packet sniffing?

Answer: Implement suitable security settings on your wireless network, possibly including encryption or provide a public wireless local area network (WLAN) only and instruct users using VPN technologies accessing internal resources.

Question: What are the risks associated with allowing your users to connect their laptops to Wi-Fi hotspots?

Answer: Users' computers are susceptible to malicious code being installed on their computers when they connect to unmanaged networks. Additionally, the network is at greater risk when these roaming computers connect once more to the corporate network. When users connect to third-party unmanaged networks, it is possible that the data they send and receive can be viewed by third parties.

Lab Review Questions and Answers

Question and Answers

Question: In the lab, you were concerned primarily with physical security concerns. What potential support issues might arise following implementation of your proposed changes? Specifically, what issues might arise surrounding the encryption of files and volumes and the prohibition of USB storage devices?

Answer: The important thing with encryption is managing keys; if keys are inaccessible, data is also inaccessible. In terms of support issues arising from USB memory stick prohibition, users are not going to be pleased that this easy way for them to manage their files is no longer available. Education as to why this change has been made would be helpful, but also a way in which, where needed, users could get files placed onto an encrypted drive (BitLocker).

Module9

Implementing Security in Windows Server

Contents:

Lesson 1: Overview of Windows Security	2
Lesson 2: Securing Files and Folders	4
Lesson 3: Implementing Encryption	7
Module Review and Takeaways	9
Lab Review Questions and Answers	10

Lesson 1

Overview of Windows Security

Contents:

Question and Answers

3

Question and Answers

What Is User Access Control?

Question: From a system administrator viewpoint, what are some of the advantages and benefits of UAC?

Answer: Answers will vary but include:

- UAC allows admins to work securely, but enables them to use the administrative part of their credentials when required.
- UAC notifies both standard and administrative users when potentially harmful system changes are made.
- By reducing the number of operating system applications and tasks that require elevation and user prompts, UAC enables standard users to do more and with fewer prompts.

Account Policies

Question: What would be the effect on a user's account if the user entered his or her password incorrectly five times between 10:00 A.M. and 10:25 A.M. with the following settings applied to the account:

Account lockout threshold: 4

Account lockout duration: 60 minutes

Reset account lockout after: 30 minutes.

Answer: The user would be locked out of his or her account for 60 minutes because the maximum number of failed logon attempts (four) was exceeded within the time specified (30 minutes) by the Reset Account Lockout After setting.

Lesson 2

Securing Files and Folders

Contents:

Demonstration

5

Demonstration

Demonstration: How to Secure a Shared Folder

Demonstration Steps

1. Ensure you are signed on to 10967A-LON-SVR1 as **ADATUM\Administrator** and password **Pa\$\$w0rd**
2. Right-click the desktop, click **New**, and then click **Folder**.
3. Type **Deliverables** for the folder name.
4. Right-click the **Deliverables** folder, and then click **Properties**.
5. In the **Deliverables Properties** dialog box, on the **Security** tab, click **Edit**.
6. In the **Permissions for Deliverables** dialog box, click **Add**.
7. In the **Select Users, Computers, Service Accounts, or Groups** dialog box, in the **Enter the object names to select (examples)** box, type **ADATUM\Maxim**, click **Check Names**, and then click **OK**.
8. In the **Group or user names** box, click **Maxim Goldin (ADATUM\Maxim)**.
9. In the **Permissions for Deliverables** dialog box, next to **Write**, select the **Allow** check box, and then click **OK**.
10. In the **Deliverables Properties** dialog box, click the **Sharing** tab, and then click **Advanced Sharing**.
11. Select the **Share this folder** check box, leave the **Share name:** as **Deliverables**, and then click the **Permissions** button.
12. In the **Permissions for Deliverables** dialog box, click **Add**.
13. In the **Select Users, Computers, Service Accounts, or Groups** dialog box, in the **Enter the object names to select (examples)** box, type **ADATUM\Maxim**, click **Check Names**, and then click **OK**.
14. In the **Group or user names:** section click **Maxim Goldin (ADATUM\Maxim)**.
15. In the **Permissions for Deliverables** dialog box, next to **Read** and **Change**, ensure that the **Allow** check box is selected and then click **OK**.
16. In the **Advanced Sharing** dialog box, click **OK**.
17. In the **Deliverables Properties** dialog box, click **Close**.
18. Right-click the **Deliverables** folder, click **Properties**, click the **Security** tab, and then click the **Advanced** button.
19. Review Maxim Goldin's permissions on the **Permissions** and **Share** tabs.
20. As you have time, click on the **Effective Access** tab.
21. Click the **Select a user** link
22. In the **Select Users, Computers, Service Accounts, or Groups** dialog box, in the **Enter the object names to select (examples)** box, type **ADATUM\Maxim**, click **Check Names**, and then click **OK**
23. Click the **View Effective Access** button and verify the permissions are as you have just assigned discussing each column.
24. Close all dialog boxes.
25. Leave the virtual machines running for the next demonstration.

Demonstration: How to Configure File Auditing

Demonstration Steps

1. Ensure you are signed on to 10967A-LON-SVR1 as **ADATUM\Administrator** and password **Pa\$\$w0rd**
 2. In Server Manager, click **Tools**, and then select **Local Security Policy**.
 3. In the **Local Security Policy** window, expand Security Settings then Advanced Audit Policy Configuration
 4. Expand System Audit Policies - Local Group Policy Object and select Object Access
 5. In **Object Access** double-click on **Audit File System**
 6. Read the explanatory text on the **Explain** tab, click the **Policy** tab, click the check box next to **Configure the following audit events**, select the **Success** and **Failure** checkboxes, and then click **OK**
 7. On the desktop, right-click the **Deliverables** folder, and then click **Properties**.
 8. Click the **Security** tab, and then click the **Advanced** button.
 9. Click the **Auditing** tab, and then click the **Add** button.
 10. In the Auditing Entry for Deliverables dialog box, click Select a principal.
 11. In the Select User, Computer, Service Account, or Group dialog box, type **Everyone** into the **Enter the object name to select** box, and then click **OK**.
 12. Select the **Full Control** check box, and then click **OK**.
 13. In the **Advance Security Settings for Deliverables Folder** dialog box, click **OK**.
 14. In the **Deliverables Folder Properties** dialog box, click **OK**.
 15. Switch to **10967A-LON-CL1** and sign in as ADATUM\Maxim with password **Pa\$\$w0rd**
 16. Hover the mouse over the lower left corner and when the start menu appears right-click then go to the **Run** command
 17. Type **\\lon-svr1**, and then press **Enter**
 18. Once connected, double-click on the folder share **Deliverables**
 19. In the empty space in the right pane, right-click and point to **New**, and then click **Text Document**. Press **Enter**.
 20. Double-click New Text Document.
 21. In Notepad, type **Hello World**.
 22. Close Notepad. Click **Save** when prompted to save changes.
 23. Switch back to the **10967A-LON-SVR1** virtual machine
 24. In Server Manager, click **Tools**, and then click **Event Viewer**.
 25. Expand **Windows Logs**, and then click **Security**.
 26. Review the log for events with ID **4663** that reference the changes made to the New Text Document
- If you have time you could modify the permissions on the Deliverables folder, then return to the Security log in Event Viewer and view the events generated by that permission change you just made on folder, this will generate event ID, **4670**.

Lesson 3

Implementing Encryption

Contents:

Question and Answers

8

Question and Answers

How Are Digital Certificates Used?

Question: In what situations would a public certificate signed by a trusted CA be requested or required?

Answer: When the party who is signing the certificate with a digital signature key is not explicitly trusted (in a non-technical sense), a trusted CA might be requested to sign the certificate as an intermediary party. Specific examples can be brought up and discussed.

Question: Why would a private certificate created by its owner be used instead of a public certificate provided by a third party?

Answer: If an organization requires a large number of certificates to be issued for internal use. This way, the organization avoids the cost associated with public certificates. It does however limit the use of the certificates for internal use because no other parties will trust certificates.

Question: Why would an organization choose to use self-signed certificates over private certificates?

Answer: If the requirement of an application is simple regarding certificate use, self-signed certificates allow an organization to avoid the overhead of maintaining a private CA. Self-signed certificates have a use typically limited to the application or service in question, but they can be useful also in test or development environments.

Module Review and Takeaways

Best Practice

Best practices for UAC

The following are best practices for UAC users:

- UAC Security Settings are configurable in the local Security Policy Manager (**secpol.msc**) or the Local Group Policy Editor (**gpedit.msc**). However, in most corporate environments, Group Policy is preferred because it can be centrally managed and controlled.
- Because the user experience can be configured with Group Policy, there can be different user experiences, depending on policy settings. The configuration choices made in your environment affect the prompts and dialog boxes that standard users, administrators, or both, can view.
- For example, you might require administrative permissions to change the UAC setting to Always Notify Me or Always Notify Me And Wait For My Response. With this type of configuration, a yellow notification appears at the bottom of the User Account Control Settings page indicating the requirement.

Best Practice

Best practices for EFS

The following are best practices for EFS users:

- Users should export their certificates and private keys to removable media and store the media securely when it is not in use. For the greatest possible security, the private key must be removed from the computer whenever the computer is not in use. This protects against attackers who physically obtain the computer and try to access the private key. When the encrypted files must be accessed, the private key can easily be imported from the removable media.
- Encrypt the My Documents folder for all users (User_profile\My Documents). This makes sure that the personal folder, where most documents are stored, is encrypted.
- Users should encrypt folders rather than individual files. Programs work on files in various ways. Encrypting files consistently at the folder level makes sure that files are not unexpectedly decrypted. Also, when files are encrypted, the temp folder is used, where you would be able to access the unencrypted file when you have a tool to recover deleted files.
- The private keys that are associated with recovery certificates are extremely sensitive. These keys must be generated either on a computer that is physically secured, or their certificates must be exported to a .pfx file, or protected with a strong password, and saved on a disk that is stored in a physically secure location.
- You should plan and roll out EFS with some thought, including the proper use of a recovery agent. It is possible to lose access to all EFS-encrypted files, and have no way of recovering them as such proper planning including the use of Recovery Agents is essential.

Best Practice

Best practices for BitLocker

- Because BitLocker stores its own encryption and decryption key in a hardware device that is separate from the hard disk, consider the following:
- The most secure implementation of BitLocker takes advantage of the enhanced security capabilities of TPM version 1.2 or higher
- On computers that do not have a TPM version 1.2 or higher, you can still use BitLocker to encrypt the Windows operating system volume. However, this implementation will require the user to insert a USB startup key to start the computer or resume from hibernation and does not provide the pre-startup system integrity verification offered by BitLocker that is working with a TPM.

- If you are making any significant hardware changes, such as adding Hard Drives or optical drives, suspend BitLocker before doing so; otherwise, the changes might cause BitLocker to start in recovery mode when it restarts.

Best Practice

Best practices for securing files and folders

- Use the most restrictive permissions possible. Do not grant more permissions for a file or folder than the users legitimately require. For example, if a user only has to read the files in a folder, grant Read permission for the folder to the user or group to which the user belongs.
- Avoid assigning permissions to individual users. Use groups whenever possible. It is very inefficient to maintain user accounts directly.
- Use restrictive shared folder permissions only when necessary. To avoid complicated combined permissions scenarios, use NTFS file and folder permissions to restrict or grant access as much as possible. NTFS file and folder permissions offer much more precise control over user access and always apply to file and folder security, whether being accessed locally or over the network.
- Use Deny permissions with caution. Deny permissions always override Allow permissions and can result in users being mistakenly restricted from access to files or folders.
- Remember that Full Control lets users modify permissions. Assign Full Control permissions with caution, as any change in existing permissions could potentially affect security.
- Use the Authenticated Users or the Domain Users group instead of the Everyone group (if present) from the shared folder's permissions list. The Everyone group includes guest users. Using the Authenticated or Domain Users group limits file or folder access to only authenticated users, and prevents users or viruses from accidentally deleting or damaging files.
- Be conscious of explicitly set permissions and the effects of blocked inheritance. When assigning permissions to a parent folder, be aware that some subfolders and files might have inheritance blocked and explicit permissions specified. In this case, such subfolders and files will not inherit the parent folder's permissions when changes are made.
- You can use the Effective Permissions tool to evaluate the permissions assigned to a user or group for a specific file or folder. Effective Permissions allows you to select users or groups and then shows you the effective permissions for those users or groups according to all the permissions set on the specific file or folder.

Tools

Tool	Use for	Where to find it
Server Manager	Managing server configuration, including adding roles and features.	Start menu
Windows PowerShell	Managing both Server Manager. Also, almost all server roles have cmdlets available to support them.	Windows PowerShell console and Windows PowerShell ISE
Auditpol.exe	Viewing and managing audit policy.	Command Prompt
Icacls.exe	Viewing and managing access control list details.	Command Prompt

Lab Review Questions and Answers

Question and Answers

Question: What is the most efficient way to give several users who all require the same permissions access to a shared folder?

Answer: Create a group, add the users to the group, and then add the group to the folder's shared permissions list.

Question: What are some of the ways of protecting sensitive data in Windows Server?

Answer: Windows Server supports data encryption by using BitLocker, BitLocker To Go, and EFS. Additionally, NTFS and Share permissions can be configured to protect data.

Module10

Implementing Network Security

Contents:

Lesson 1: Overview of Network Security	2
Lesson 2: Implementing Firewalls	3
Lesson 3: Internet Protocol Security	6
Module Review and Takeaways	9
Lab Review Questions and Answers	9

Lesson 1

Overview of Network Security

This lesson does not have any supplemental content.

Lesson 2

Implementing Firewalls

Contents:

Demonstration

4

Demonstration

Demonstration: How to Use Windows Firewall to Manage Inbound Network Traffic

Demonstration Steps

1. Ensure you are logged on to the **10967A-LON-DC1** virtual machine with username **ADATUM\Administrator** and password **Pa\$\$w0rd**
2. Press the **Windows** logo key, type **cmd.exe**, and then press **Enter**.
3. At the Command Prompt, type the following command, and then press **Enter**.

```
ping lon-cl1
```



Note: You are successfully able to ping 10967A-LON-CL1

4. To use Windows PowerShell open the console and type:

```
Test-Connection LON-CL1
```



Note: If you receive an error and you are not able to successfully ping or test the connection to **10967A-LON-CL1**, do the following.

5. On **10967A-LON-CL1**, navigate to the **Control Panel**, click **Network and Internet**, and then click **Network and Sharing Center**
6. Click on **Change advanced sharing settings** and in the **domain (current profile)** section click the following radio buttons
 - Turn on network discovery
 - Turn on file and printer sharing
7. Click **Save Changes** and retry steps **3** and **4**. You should now be able to successfully ping **10967A-LON-CL1** from **10967A-LON-DC1**
8. Switch to the **10967A-LON-CL1** virtual machine.
9. Hover the mouse over the lower left of the Desktop until the **Start** menu appears.
10. Right-click and choose **Control Panel**
11. Click **System and Security** and then click on **Windows Firewall**
12. In the Windows Firewall pane, click the **Advanced settings** link on the left side to open the Windows Firewall with Advanced Security management console.
13. Under **Windows Firewall with Advanced Security on Local Computer**, in the navigation pane, click **Inbound Rules**.
14. Right-click **Inbound Rules**, and then click **New Rule**.
15. In the **New Inbound Rule Wizard**, on the **Rule Type** page, click **Custom**, and then click **Next**.
16. On the **Program** page, click **All programs**, and then click **Next**.
17. On the **Protocol and Ports** page, in the **Protocol** type list, click **ICMPv4**, and then click **Next**.
18. On the **Scope** page, click **Next**.
19. On the **Action** page, click **Block the connection**, and then click **Next**.

20. On the **Profile** page, click **Next**.
21. On the **Name** page, in the **Name** box, type **Ping Rule**, and then click **Finish**.
22. In the navigation pane, expand **Monitoring**, and then click **Firewall**.
23. Scroll down.
24. Can you see the new Ping Rule?

Answer: Yes.

25. Switch to the **10967A-LON-DC1** virtual machine.
26. At the Command Prompt, type the following command, and then press **Enter**.

```
ping LON-CL1
```



Note: You are unable to successfully ping LON-CL1

27. Switch to the **10967A-LON-CL1** virtual machine.
28. In **Windows Firewall with Advanced Security**, in the navigation pane, click **Inbound Rules**.
29. In the Results pane, right-click **Ping Rule**, and then click **Disable Rule**.
30. Close **Windows Firewall with Advanced Security**.
31. Switch to **10967A-LON-DC1**, and then ping **10967A-LON-CL1**. Verify that the **ping** command is successful now.
32. Revert the virtual machines.

Lesson 3

Internet Protocol Security

Contents:

Demonstration

7

Demonstration

Demonstration: Create Server to Server Connection Security Rule

Demonstration Steps

1. Ensure you are logged on to the **10967A-LON-DC1** virtual machine with username **ADATUM\Administrator** and password **Pa\$\$w0rd**
2. In Server Manager navigate to Tools then select Windows Firewall with Advanced Security

Enable ICMPv4 Traffic on 10967A-LON-DC1

1. Right-click **Inbound Rules** and then click **New Rule**.
2. In the **New Inbound Rule Wizard** dialog box, click **Custom**, and then click **Next**.
3. On the **Programs** page, click **Next**.
4. On the **Protocols and Ports** page, in the **Protocol type** list, click **ICMPv4** and then click **Next**.
5. On the **Scope** page, click **Next**.
6. On the **Action** page, click **Allow the connection if it is secure**, and then click **Next**.
7. On the **Users** page, click **Next**.
8. On the **Computers** page, click **Next**.
9. On the **Profile** page, click **Next**
10. On the **Name** page, in the **Name** box, type **ICMPv4 allowed** and then click **Finish**

Create Server to Server Connection Security Rule on 10967-LON-DC1

1. Right-click **Connection Security Rules** and then click **New Rule**.
2. In the **New Connection Security Rule Wizard**, click **Server-to-Server** and then click **Next**.
3. On the **Endpoints** page, click **Next**.
4. On the **Requirements** page, click **Require authentication for inbound and outbound connections** and then click **Next**.
5. On the **Authentication Method** page, click **Advanced**, and then click **Customize**.
6. In the **Customize Advanced Authentication Methods** dialog box, under **First authentication**, click **Add**.
7. In the **Add First Authentication Method** dialog box, click **Preshared Key**, type **secret** and then click **OK**.
8. In the **Customize Advanced Authentication Methods** dialog box, click **OK**.
9. On the **Authentication Method** page, click **Next**.
10. On the **Profile** page, click **Next**.
11. On the **Name** page, in the **Name** box, type **A Datum-Server-to-Server** and click **Finish**.

Create Server to Server Connection Security Rule on 10967-LON-SVR1

1. Switch to **10967A-LON-SVR1** and ensure you are logged on as **ADATUM\Administrator** with password **Pa\$\$w0rd**
2. In **Server Manager** navigate to **Tools** then select **Windows Firewall with Advanced Security**
3. Right-click **Connection Security Rules** and then click **New Rule**.
4. In the **New Connection Security Rule Wizard**, click **Server-to-Server** and then click **Next**.

5. On the **Endpoints** page, click **Next**.
6. On the **Requirements** page, click **Require authentication for inbound and outbound connections** and then click **Next**.
7. On the **Authentication Method** page, click **Advanced**, and then click **Customize**.
8. In the **Customize Advanced Authentication Methods** dialog box, under **First authentication**, click **Add**.
9. In the **Add First Authentication Method** dialog box, click **Preshared Key**, type **secret** and then click **OK**.
10. In the **Customize Advanced Authentication Methods** dialog box, click **OK**.
11. On the **Authentication Method** page, click **Next**.
12. On the **Profile** page, click **Next**.
13. On the **Name** page, in the **Name** box, type **A Datum-Server-to-Server** and click **Finish**.

Verify The Server to Server Connection security rule

1. Open an administrator **Command Prompt**.
2. At the Command Prompt, type **ping LON-DC1** and press **Enter**.
3. Switch to **Windows Firewall with Advanced Security**.
4. Expand **Monitoring**, expand **Security Associations**, and then click **Main Mode**.
5. In the right-pane, double-click the listed item.
6. View the information in **Main Mode**, and then click **OK**.
7. Click **Quick Mode**.
8. In the right-pane, double-click the listed item.
9. View the information in **Quick Mode**, and then click **OK**.
10. Revert the virtual machines.

Module Review and Takeaways

Best Practice

- Implement firewalls.
- Publish services to your perimeter network.
- Secure some network traffic and communication if it is highly sensitive
- Encrypt network communication.
- Segment the network.
- Require mutual authentication.

Question: Why is it important to publish services to the perimeter instead of connecting servers directly to the Internet?

Answer: Services which are routed through the perimeter network can be additionally secured. For example, mail services can be sender verified; antivirus spammed and can be a SMTP filtering and forwarding application instead of a full Exchange Server. Publishing to the perimeter network provides an additional layer of protection from external attack.

Tools

Tool	Use for	Where to find it
Ping.exe	Testing network connectivity	Command Prompt
Windows Firewall with Advanced Security	Managing inbound, outbound, and IPsec rules	Server Manager
Group Policy Management Console	Can configure Advanced Firewall settings and apply them across the domain when used with Active Directory	Server Manager
Windows PowerShell	Configuring Advanced Firewall settings, only present in Windows Server 2012	NetSecurity Module
Netsh	Configuring Advanced firewall settings, present in Windows Server 2012 and pre Windows Server 2012 versions	Command Prompt

Lab Review Questions and Answers

Question and Answers

Question: If you wanted to make sure that only domain computers could communicate with other domain computers, how could you easily achieve this with Windows Firewall?

Answer: Windows Firewall with Advanced Security supports the use of Connection Security rules, based on IPsec; one of these rule types is a domain isolation rule. Only computers that have a configured domain membership can communicate.

Module11

Implementing Security Software

Contents:

Lesson 1: Client Software Protection Features	2
Lesson 2: Email Protection	5
Lesson 3: Server Protection	6
Module Review and Takeaways	8
Lab Review Questions and Answers	8

Lesson 1

Client Software Protection Features

Contents:

Question and Answers	3
Demonstration	3

Question and Answers

Create and Enforce a AppLocker Rule

Question: How could the AppLocker rule that you created be changed to make sure that WordPad could not be run from any location on the client computers?

Answer: You could re-create the rule as a hash rule.

Demonstration

Demonstration: Create and Enforce a AppLocker Rule

Demonstration Steps

1. Ensure you are logged on to **10967A-LON-DC1** with user name **ADATUM\Administrator** and password **Pa\$\$w0rd**
2. On LON-DC1, in Server Manager, click **Tools**, and then select **Group Policy Management**.
3. Expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, right-click **Group Policy Objects**, and then click **New**.
4. Name the new GPO **WordPad Restriction Policy**, and then click **OK**.
5. Expand **Group Policy Objects**, 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**, and then double-click **AppLocker**.
7. Click **Executable Rules**, right-click **Executable Rules**, select **Create New Rule**, and then click **Next**.
8. On the Before you Begin page click **Next**
9. **Permissions** page, select **Deny**, Notice that the rule could be restricted to a specific user or group, and then click **Next**.
10. On the **Conditions** page, select **Publisher**, and then click **Next**.
11. Click **Browse**, double-click **Windows NT**, double-click **Accessories**, select **wordpad.exe**, and then click **Open**.
12. Move the slider up to the **File name** position. Notice the text explaining the slider usage at the top of the page, and then click **Next**.
13. On the **Exceptions** page, click **Next**.
14. On the **Name and Description** page, click **Create**.
15. Click **Yes** if you are prompted to create default rules.
16. Click **AppLocker**, and then click **Configure Rule Enforcement**.
17. Under **Executable rules**, select the **Configured** check box, click **Enforce rules**, and then click **OK**.



Note: Before you can enforce AppLocker policies, you must start the Application Identity service.

18. In the Group Policy Management Editor, expand **Computer Configuration**, expand **Windows Settings**, expand **Security Settings**, click **System Services**, and then double-click **Application Identity**.

19. In the **Application Identity Properties** dialog box, select the **Define this policy setting** check box.
20. Select **Automatic** under **Select service startup mode**, and then click **OK**.
21. Close the **Group Policy Management Editor**.
22. In the **Group Policy Management** window, drag the **WordPad Restriction Policy** GPO over the Adatum.com domain container.
23. Click **OK** to link the GPO to the domain.
24. Close the Group Policy Management console.
25. Open a Command Prompt window, type **gpupdate /force**, and then press **Enter**. Wait for the policy to be updated.



Note: Alternatively you can open a Windows PowerShell console and run the **Invoke-GPUdate** cmdlet. You should demonstrate both options to students

26. Switch to **10967A-LON-CL1** sign out as **ADATUM\Administrator** if need be and sign in as **ADATUM\Allie** with a password of **Pa\$\$w0rd**.
27. While on the **Start** page, open a Command Prompt window by typing **cmd** then double clicking the **Command Prompt** icon
28. In the **Command Prompt** window, type **gpupdate /force**, and then press **Enter**. Wait for the policy to be updated.
29. You could attempt to run the **Invoke-Gpupdate** cmdlet in a Windows PowerShell console as you did on **10967A-LON-DC1**. If you do you will receive an error. You could ask students why do you receive an error?

Answer: Because the module that contains this cmdlet, i.e. **GroupPolicy**, is not installed. The Group Policy Windows PowerShell cmdlets are only available where the Group Policy Management Console (GPMC) is installed. The GPMC is not available by default in Windows 8.

30. You could ask students how could they install the GPMC in Windows 8?

Answer: by installing the Remote Server administration Tools for Windows 8 (RSAT for Win 8). If you have time you can install the RSAT for Win 8 from \\LON-DC1\E\$\Mod06\Labfiles. It will take approximately two to three minutes and will require a restart.

31. Open the Start page by pointing to the lower-left corner of the page and clicking the Start page.
32. Type **WordPad**, and then click the WordPad.
33. Notice that no message displays however WordPad does not open.
34. Revert the virtual machines.

Lesson 2

Email Protection

Contents:

This lesson does not include supplemental content.

Lesson 3

Server Protection

Contents:

Demonstration

7

Demonstration

Demonstration: How to Use the Best Practices Analyzer

Demonstration Steps

1. Ensure you are logged on to **10967A-LON-DC1** with user name **ADATUM\Administrator** and password **Pa\$\$w0rd**
2. In Server Manager, click **IIS** in the left navigation pane.
3. In the center details pane, locate the **Best Practices Analyzer**.
4. In the **TASKS** drop-down list, select **Start BPA Scan**.
5. In the **Select Servers** dialog box, make sure that **LON-DC1.Adatum.com** is selected, and then click **Start Scan**.



Note: It can take a minute for results to appear. Refresh the results by using the TASKS menu.

6. Review the results, noting the severity and category. You may need to click the **X Clear All** button to remove all filters and view the results.
7. Select an item to view more detailed information.
8. Notice that there are no warnings or errors on the Internet Information Services (IIS) server role.



Note: If you have time and you wish to show more scan results containing Information, Warnings and Error data you can perform a BPA scan on the AD DS role, the AD DS role will be scanned as part of the lab.

9. Revert the virtual machines.

Module Review and Takeaways

Question: What are the key differences between AppLocker and legacy Software Restriction Policies?

Answer: AppLocker is much more customizable and allows for more flexibility in identifying applications in rules. AppLocker works with only Windows Server 2012, Windows 8, Windows Server 2008 R2, and Windows 7 operating systems.

Question: Why are server-side email security solutions typically more effective and easy to implement than client-side solutions?

Answer: Server-side solutions address the threat prior to the threat reaching client machines. If the server-side solution is hosted in the perimeter network, it protects the rest of the network also. Additionally, server-side solutions require less overall maintenance updating because they are hosted on only a few servers instead of on every client in an organization.

Tools

Tool	Use for	Where to find it
Software Restriction Policies	Managing software execution in legacy environments or in environments where Windows Server 2008 R2 or Windows 7 coexist with legacy Windows operating systems	Group Policy Management
AppLocker	Managing software execution in Windows Server 2012, Windows 8, Windows Server 2008 R2, and Windows 7 environments	Group Policy Management
Microsoft Forefront Protection for Exchange Server	Providing anti-malware protection for an Exchange Server environment	Separate Downloadable Product
Security Configuration Wizard	Generating and applying security policy templates to decrease the vulnerability of Windows Server.	Server Manager
Microsoft Baseline Security Analyzer	Analyzing the security state of an environment according to Microsoft security recommendations.	Server Manager
Best Practices Analyzer	Reviewing server roles for compliance with best practices	Server Roles Summary Details
Security Compliance Manager	Viewing, updating, customizing, and exporting security baselines	Solution Accelerator
Windows PowerShell	Configuring AppLocker and Best Practice Analyzer	Windows PowerShell console
Scwcmd.exe	Transforms BPA results xml file into Group Policy Object that can be deployed with Group Policy	Command Prompt

Lab Review Questions and Answers

Question and Answers

Question: What is the benefit of exporting a SCW security policy to a GPO?

Answer: A GPO can be assigned to organizational units (OUs) in Group Policy, allowing the security policy to be applied to multiple servers.

Question: When would you use the Security Policy XML format?

Answer: The XML file could be stored on a removable drive or sent by email message for use in another domain.

Module12

Monitoring Server Performance

Contents:

Lesson 1: Event Logging	2
Lesson 2: Performance Monitoring	4
Module Review and Takeaways	9
Lab Review Questions and Answers	9

Lesson 1

Event Logging

Contents:

Demonstration

3

Demonstration

Demonstration: How to Use the Event Viewer

Demonstration Steps

1. Ensure you are signed in to **10967A-LON-SVR1** as **ADATUM\Administrator** with password **Pa\$\$w0rd**
2. In Server Manager, click the **Tools** menu, and then click the **Event Viewer**.
3. In the navigation pane, expand **Windows Logs**.
4. Review the different kinds of logs that are available.
5. Click the **Application** node.
6. Select an event and review the information that is provided.
7. In the navigation pane, expand the **Application and Services Logs** node.
8. Review the different kinds of logs.



Note: Students accessed the Microsoft\Windows\AppLocker log as part of the lab in Module 11, so you may want to mention this to students.

9. Review the items in the Action pane, specifically **Filter Current Log**.
10. In the Action pane, click **Create Custom View**.
11. For the **Event Level**, select the **Warning** and **Error** check boxes.
12. In the **Event Logs** drop-down list, select the **Windows Log** check box.
13. As you have time, review other parameters.
14. Click **OK**.
15. In the **Name** text box, type **Windows Logs Warnings and Errors**, and then click **OK**.
16. Verify that your custom view was saved in the navigation pane under **Event Viewer\Custom Views**
17. Open the Windows PowerShell® console.
18. Type **Get-WinEvent -listlog ***, and then press **Enter**.
19. The output is a list of all the logs. Scroll through the list of returned logs.
20. Type **Get-WinEvent | Get-member**
21. The output is a list of the properties that are available for the **Get-WinEvent** cmdlet and can be manipulated and automated by administrators. Call out some items that may be useful such as **MachineName**, **Id**, and **LevelDisplayName**. We will not go into detail on these in this course so we are just calling them out here so students are aware of the greater possibilities for managing logs with **Windows PowerShell**.
22. Revert the virtual machines.

Lesson 2

Performance Monitoring

Contents:

Demonstration

5

Demonstration

Demonstration: How to Capture Current Performance Activity

Demonstration Steps

1. Ensure you are signed in to **10967A-LON-SVR1** as **ADATUM\Administrator** with password **Pa\$\$w0rd**
2. In Server Manager, point to **Tools**, and then click **Performance Monitor**.
3. In **Performance Monitor**, in the **Results** pane in the middle of the console, scroll down and review the **System Summary** information.

Notice the four areas: Memory, Network Interface, Physical Disk, and Processor.

4. In **Performance Monitor**, in the navigation pane, under the **Monitoring Tools** node, click **Performance Monitor**.
5. On the toolbar, click the **Add button** (green cross).
6. In the **Available counters** list, expand **Memory**, click **Pages/sec**, and then click **Add >>**.
7. In the **Available counters** list, expand **Network Interface**, click **Bytes Total/sec**, and then click **Add >>**.
8. In the **Available counters** list, expand **PhysicalDisk**, click **% Disk Time**, and then click **Add >>**.
9. Still under **PhysicalDisk**, click **Avg. Disk Queue Length**, and then click **Add >>**.
10. In the **Available counters** list, expand **System**, click **Processor Queue Length**, and then click **Add >>**.
11. Make sure that there are five counters in the Added Counters pane, and then click **OK**.
12. Discuss the graph, you may want to connect to \\LON-DC1 or open a Command Prompt and type `dir *.* /s` to generate some activity if you need. You should hover the mouse over the graphed items and show the different counters
13. On the toolbar, click the **Change graph type** drop-down arrow, and then click **Histogram bar**.
14. Discuss the report. Again you may need to generate some activity as outlined earlier.
15. On the toolbar, click the **Change graph type** drop-down arrow, and then click **Report**.
16. Discuss the report.
17. Do **not** close the Performance Monitor. You will be using this data in the next demonstration.

Demonstration: How to Use Data Collector Sets to Capture Performance Data

Demonstration Steps

1. Ensure you are signed in to **10967A-LON-SVR1** as **ADATUM\Administrator** with password **Pa\$\$w0rd**
2. In Performance Monitor, in the navigation pane, expand **Monitoring Tools**, right-click the **Performance Monitor**, click **New**, and then click **Data Collector Set**.
3. In the **Create New Data Collector Set** wizard, in the **Name** box, type **LON-SVR1 Performance**.
4. On the **Where would you like the data to be saved?** page, click **Next**.
5. On the **Create the data collector set?** page, click **Start this data collector set now**, and then click **Finish**.
6. Open the Start Screen and, type **cmd.exe**, and then press **Enter**.



Note: Create a workload on the server and the network by creating, copying, and deleting a large file.

- At the Command Prompt, type the following command, and then press **Enter**. (this creates approx. 100 MB file)

```
fsutil file createnew bigfile 104857600
```

- At the Command Prompt, type the following command, and then press **Enter**.

```
copy bigfile \\lon-dc1\c$
```

- At the Command Prompt, type the following command, and then press **Enter**. (This copies the file back to LON-SVR1 and renames it)

```
copy \\lon-dc1\c$\bigfile bigfile2
```

- At the Command Prompt, type the following command, and then press **Enter**.

```
del bigfile*.*
```

- At the Command Prompt, type the following command, and then press **Enter**.

```
del \\lon-dc1\c$\bigfile*.*
```

- Close the Command Prompt.
- Switch to Performance Monitor.
- In the navigation pane, expand **Data Collector Sets**, expand **User Defined**, right-click **LON-SVR1 Performance**, and then click **Stop**.
- In Performance Monitor, in the navigation pane, click **Performance Monitor**.
- On the toolbar, click **View log data** (second icon from the left).
- In the **Performance Monitor Properties** dialog box, on the **Source** tab, click **Log files**, and then click **Add**.
- In the **Select Log File** dialog box, double-click **Admin**.
- Double-click LON-SVR1 Performance, double-click the **System Monitor Log.blg**.
- In the Performance **Monitor Properties** dialog box, click **OK**.
- Click the **Change graph type** dropdown list, and then select **Line**.
- Notice the graph is static and just covers the logging period.
- On the toolbar, click the **Change graph type** drop-down arrow, and then click **Report**.
- You could also view other report types such as **Line**, **Area** and **Stacked Area**
- Do not close Performance Monitor. You will use it in the next demonstration.

Demonstration: How to Use Alerts to Identify Performance Bottlenecks

Demonstration Steps

- Ensure you are still signed in to **10967A-LON-SVR1** as **ADATUM\Administrator** with password **Pa\$\$w0rd**

2. In Performance Monitor, in the navigation pane, expand **Data Collector Sets**, and then click **User Defined**.
3. Right-click **User Defined**, point to **New**, and then click **Data Collector Set**.
4. In the **Create new Data Collector Set** wizard, in the **Name** textbox, type **LON-SVR1 Alert**.
5. Click **Create manually (Advanced)**, and then click **Next**.
6. On the **What type of data do you want to include?** page, click the **Performance Counter Alert** radio button, and then click **Next**.
7. On the **Which performance counters would you like to monitor?** page, click **Add**.
8. In the **Available counters** list, expand **Processor**, click **%Processor Time**, click **Add >>**, and then click **OK**.
9. On the **Which performance counters would you like to monitor?** page, in the **Alert when** list, select **Above**.
10. In the **Limit** box, type **10**, and then click **Next**.
11. On the **Create the data collector set?** page, click **Finish**.
12. In the navigation pane, expand the **User Defined** node, and then click **LON-SVR1 Alert**.
13. In the Results pane, right-click **DataCollector01**, and then click **Properties**.
14. In the **DataCollector01 Properties** dialog box, in the **Sample interval** box, type **1**, and then click the **Alert Action** tab.
15. Select the **Log an entry in the application event log** check box, and then click **OK**.
16. In the navigation pane, right-click **LON-SVR1 Alert**, and then click **Start**.
17. Open the Start screen and type **cmd.exe**, and then press **Enter**.
18. At the Command Prompt, type the following command, and then press **Enter**.

```
cd C:\Labfiles\StressTool\amd64
```

19. At the Command Prompt, type the following command, and then press **Enter**.

```
StressTool 95
```

20. Wait for one minute to allow for alerts to be generated. Press **Ctrl+C** to stop the StressTool. Close the Command Prompt.
21. In Server Manager, click **Tools**, and then click **Event Viewer**.
22. Expand **Application and Services Logs**, and then select **the Microsoft-Windows-Diagnosis-PLA/Operational** log
23. Scroll through the list of events. Look for Event ID 2031 and read the details in the General tab, which should say something like **"....Performance counter \Processor (_Total)\%Processor Time has tripped its alert threshold. The counter value of < X > is over the limit value of 10.000. 10.000 is the alert threshold value."**



Note: If you have time you could discuss what would be the next steps if you identified that the CPU is regularly exceeding its alert threshold value. Also to relate it back to earlier conversations, you could also discuss what an appropriate threshold value is for a CPU.

24. Revert the virtual machines.

Module Review and Takeaways

Tools

Tool	Use for	Where to find it
Performance Monitor	Monitoring and analyzing real-time and logged performance data.	Server Manager
Resource Monitor	Monitoring resources in real time.	Server Manager
Windows PowerShell	Cmdlets available for event logging, performance counters, and data collectors.	Built in to Windows Server 2012
Event Viewer	Viewing Logs and determining what happened	Server Manager

Lab Review Questions and Answers

Question and Answers

Question: During the lab, you collected data in a Data Collector Set. What is the advantage of collecting data in this manner?

Answer: By collecting data in Data Collector Sets, you can analyze and compare the data against historical data and draw conclusions over server capacity.

Question: What significant counters should you monitor in Windows Server Performance Monitor?

Answer: It depends on the server functionality, for example, Web Server, Exchange Mail server, or Domain Controller. However, the counters mentioned here would provide for a baseline recommendation.

- Memory\Pages/sec
- Network Interface\Bytes Total/sec
- PhysicalDisk\% Disk Time
- PhysicalDisk\Avg. Disk Queue Length
- Processor\% Processor Time
- System\Processor Queue Length

Module13

Maintaining Windows Server

Contents:

Lesson 1: Troubleshooting Windows Server Startup	2
Lesson 2: Business Continuity and Disaster Recovery	5
Lesson 3: Applying Updates to Windows Server	7
Lesson 4: Troubleshooting Windows Server	9
Module Review and Takeaways	11
Lab Review Questions and Answers	12

Lesson 1

Troubleshooting Windows Server Startup

Contents:

Question and Answers	3
Demonstration	3

Question and Answers

Considerations for Troubleshooting Startup

Question: Which tool would you use to recover a system that does not start correctly immediately following the installation of a new network adapter?

Answer: The most likely cause of the issue would be problems with the network adapter's drivers. In this case, safe mode would enable Windows to start without loading the network adapter drivers. Then, the card could be removed to enable the system to start, or updated drivers could be obtained that would enable the network adapter to function correctly.

Demonstration

Demonstration: How to Recover the Startup Environment

Demonstration Steps

1. Start the **10967A-LON-DC1** virtual machine
2. Press and hold the **F8** key



Note: The startup of the virtual machines is very fast and it is easy to miss the opportunity to access the Recovery Environment by pressing F8. It is recommended to do this prior to the start of the module in case several attempts are needed, saving the state with a snapshot so you can return to it if need be. It is also recommended to press and continue to hold the **F8** key when the virtual machine is restarting to help ensure you do not miss the opportunity to enter into the Windows Recovery Environment.

3. In the **System Recovery Options** menu use the arrow keys to move through the options, viewing the description of each at the bottom of the screen.



Note: The Directory Services Restore Mode option is present here as this is a domain controller

4. Use the arrows to select **Repair Your Computer**, and then press **Enter**.
5. On the **Choose an option** menu, select **Troubleshoot**.
6. On the **Advanced options** menu, select **Command Prompt**.
7. On the **Command Prompt** menu, select **Administrator**.
8. Type the password of **Pa\$\$w0rd**, and then click **Continue**.
9. At the Command Prompt, type the following, and then press Enter.

```
BCDEdit /enum osloader
```

10. Generally discuss what BCDEdit is used for and compare some of the values returned for the Operating system and those for the Recovery Environment.
11. At the Command Prompt, type the following, and then press **Enter**.

```
BCDEdit /enum bootmgr
```

12. Discuss the setting returned by BCDEdit and that there is only one entry compared to the OS Loader data
13. At the Command Prompt, type the following, and then press **Enter**.

```
bootrec /?
```

14. Generally discuss the switches and what bootrec is used for.
15. Close the Command Prompt window by typing **exit** and pressing **Enter**.
16. On the Choose an option screen select **Turn off your PC**.
17. The **10967A-LON-DC1** virtual machine will turn off.
18. Start the **10967A-LON-DC1** virtual machine normally and sign in with user name **ADATUM\Administrator** and password **Pa\$\$w0rd** to prepare for the next demonstration.

Alternative Demonstration to Access to Windows Recovery Environment Advanced Options



Note: The **10967A-LON-SVR5** virtual machine has been configured with the Windows Server 2012 Eval iso installation files already attached to the virtual machine to assist with steps required in the lab. As such the **10967A-LON-SVR5** virtual machine will give the prompt "**Press any key to boot from CD or DVD...**" each time when starting up. This has been done as it is possible to miss time pressing F8 to gain access to the recovery Environment. As an alternative for this demonstration you can select to startup from CD/DVD and enter the Windows Recovery Environment, Advanced Options that way. While you will not be able to access the System recovery options menu, you will be able to access the advanced options and Command Prompt tools

1. Start the **10967A-LON-SVR5** virtual machine
2. You receive the prompt "**Press any key to boot from CD or DVD...**"
3. Press **Enter** and allow the virtual machine to boot into the installation files
4. In the **Install Windows** dialog box, click **Next**.
5. In the **Install Windows** dialog box, click the **Repair your computer** link.
6. In the **System Recovery Options** dialog use the arrow keys to move through the options, viewing the description of each at
7. In the **Choose an option** dialog box, click **Troubleshoot**
8. On the **Advanced Options** page click **Command Prompt**.
9. Continue from step 9 to step 17 listed above previous task

Lesson 2

Business Continuity and Disaster Recovery

Contents:

Question and Answers

6

Question and Answers

Discussion: The Importance of Business Continuity

Question: What kinds of events could interfere with business continuity?

Answer: As previously mentioned, hardware or software failures which may cause data corruption or corruption of whole volumes or disks, natural disasters like a flood, an earthquake, or a lightning strike can interfere with business continuity. Environmental issues such as fire, plumbing malfunctions, or power surges can also contribute to the loss of data. Finally, malicious or accidental activity like hacking, file deletion, equipment theft, or intentional damage frequently lead to data being lost.

Question: What would the cost be to your organization if your server infrastructure was unavailable for an hour, a day, or a week?

Answer: Answers will vary, but depending on the business type, even a small amount of downtime for a server can have a serious effect on a company's bottom line. An example to use would be an application server that ran a grocery store's purchase and inventory system.

Increased Availability and Data Recovery

Question: Why would an organization have to implement both high availability and data recovery processes to make sure of business continuity?

Answer: High availability provides uninterrupted service to clients for a given group of services. However, it does not protect against a disaster like an earthquake or a fire where all of the servers in the group are destroyed or made unavailable at the same time. If this occurs, the services and the data could be permanently lost. Data recovery, on the other hand, will make sure data is retained if there is a disaster. However, it does not provide for continually available servers and services, because restoring lost or destroyed data typically involves the server being unavailable. For these reasons, high availability and disaster recovery should be used together to ensure the highest level of business continuity possible.

Providing for Data Recovery

Question: What would an appropriate backup plan be for your organization or department?

Answer: Answers will vary. Specific requirements might include critical business data having to be backed up more frequently than the rest of the data, possible media choices, depending on size and speed, or offsite location availability.

Lesson 3

Applying Updates to Windows Server

Contents:

Demonstration

8

Demonstration

Demonstration: Review WSUS Group Policy Settings

Demonstration Steps

1. Ensure you are signed in to the **10967A-LON-DC1** virtual machine with user name **ADATUM\Administrator** and password **Pa\$\$w0rd**
2. In Server Manager, point to **Tools**, and then click **Group Policy Management**.
3. In the Group Policy Management Console (GPMC), expand **Forest: Adatum.com**, expand **Domains**, and then expand **Adatum.com**.
4. Expand **Group Policy Objects** to view current GPOs.
5. Right-click **Default Domain Policy**, and then click **Edit**.
6. In the Group Policy Management Editor, expand **Computer Configuration**, expand **Policies**, expand **Administrative Templates**, expand **Windows Components**, and then click **Windows Update**.
7. Double-click each setting in the right side column to view details about that setting.
8. Revert the virtual machines

Lesson 4

Troubleshooting Windows Server

Contents:

Demonstration

10

Demonstration

Demonstration: How to Use Windows Tools to Help Troubleshoot Windows Server Problems

Demonstration Steps

Demonstrate Event Viewer

1. Ensure you are signed in to the **10967A-LON-DC1** virtual machine with user name **ADATUM\Administrator** and password **Pa\$\$w0rd**
2. In Server Manager, point to **Tools**, and then click **Event Viewer**.
3. Expand the **Windows Logs** folder in the navigation pane.
4. Click the **Application Log**.
5. Click an event in the middle pane to show event details.
6. Expand **Application and Services Logs**, expand **Microsoft**, and then expand **Windows** in the navigation pane.
7. Scroll down to view the list of Windows® log groupings.
8. Expand any of the folders to show the events within.
9. In the navigation pane on the left side of the Event Viewer console scroll to the end and right-click **Subscriptions** in the left column,
10. Click **Yes** if prompted and then click **Create Subscription**.
11. View the various options within the **Subscription Properties** window.
12. Close the **Subscription Properties** window.
13. Close the **Event Viewer** window.

Demonstrate Task Manager

1. Right-click the taskbar, click **Task Manager**, and then click **More details**
2. View the details on each tab.
3. Do *not* close Task Manager.

Demonstrate Resource Monitor

1. In Task Manager, click the **Performance** tab, and then click the **Open Resource Monitor** link.
2. Click the **Overview** tab.
3. Click the **CPU**, **Disk**, **Network** and **Memory** header bars, discussing the contents of each.
4. Click the **CPU** tab, clicking the header bars to show the contents.
5. Click the **Memory** tab, clicking the header bars to show the contents.
6. Click the **Disk** tab, clicking the header bars to show the contents.
7. Click the **Network** tab, clicking the header bars to show the contents.
8. View the details on each tab.
9. Close **Resource Monitor**.
10. As you have time, show the **Reliability Monitor**.
11. Revert the virtual machines.

Module Review and Takeaways

Question: What is the key functionality of a boot loader?

Answer: A boot loader loads the kernel or most basic part of an operating system.

Question: How does fault-tolerant hardware provide for high availability, provided the hardware is supported by Windows Server 2012

Answer: Fault-tolerant hardware allows for the removal and replacement of redundant hardware items in a server while the server is still running. Some examples include power supplies, memory, and hard disks.

Question: What benefits does Performance Monitor offer over Resource Monitor?

Answer: Performance Monitor allows for the historical tracking of system performance data and configuration information in log form for later review and analysis. Resource Monitor captures system performance data in real time only.

Tools

Tool	Use for	Where to find it
BCDEdit	Editing Windows Boot Configuration Data Store.	From the command line, type bcdedit .
Chkdsk	Checking the file for unreadable or corrupted sectors.	From the command line, type chkdsk .
WSUS	Managing Windows Updates in the enterprise.	Available from the Microsoft Download Center.
Windows Recovery Environment	Repairing various aspects of a Windows Server.	Select Repair Computer from the F8 Windows Advance Options boot menu, or select Repair Computer when booting from Windows installation media.
Last Known Good Configuration	Loading system registry settings saved from the last successful system startup.	Select Last Known Good Configuration from the F8 Windows Advance Options boot menu.
Safe mode	Loading Windows Server that has a minimal set of drivers and services for troubleshooting.	Select one of the Safe Mode options from the F8 Windows Advanced Options boot menu.
Windows Server Backup (wbadmin.exe)	Backing up Windows Server computers.	Click Start, type Windows Server Backup in the Start Search field, and then press Enter. Can also run wbadmin.exe from the command line.
Windows Update	Updating operating system, device driver, and Microsoft application components.	Click Start, type Windows Update in the Start Search field, and then press Enter.
WSUS	Allowing centralized management of the Windows Update process.	Visit the Windows Server Update Services home page.
Event Viewer	Viewing Windows logs.	Click Start, click Administrative Tools, and then click Event Viewer.

Tool	Use for	Where to find it
Task Manager	Viewing basic real-time information about the Windows environment.	Press Ctrl+Shift+Esc.
Resource Monitor	Viewing detailed real-time information about the Windows environment.	From Task Manager, click the Performance tab, and then click the Resource Monitor button.
Performance Monitor	Viewing and collecting real-time and historical performance and configuration information about the Windows environment.	Click Start, click Administrative Tools, and then click Performance Monitor.
Reliability Monitor	Viewing an overview of system events and relative system stability.	Click Start , and then in the Start Search box, type perfmon /rel , and then press Enter.
System File Checker (sfc.exe)	Scans integrity of all protected files and replaces incorrect versions if need be	From the command line tool, type sfc
Wuauclt.exe	Windows Update Automatic update client command line tool	From the command line, type wuauclt

Lab Review Questions and Answers

Question and Answers

Question: If, after a network adapter installation on a server, Windows startup failed while the splash screen was displayed, which startup based tool would you use to troubleshoot the issue?

Answer: Starting Windows in safe mode would start the computer using only the essential drivers and services, which would not include the drivers for the newly installed network adapter. The problem with the driver or the adapter itself could then be investigated within Windows.

Question: What would be the most efficient way to configure hundreds of clients in a Windows domain to receive updates from a newly installed WSUS server?

Answer: Group Policy, and more specifically, the domain-based Group Policy Management Console, could be used to assign a Group Policy Object (GPO) to the domain or organizational unit(s) that the computers belong to. This GPO could contain all of the settings required to enable automatic updates by using the new WSUS server as the source for obtaining updates.