20687B

Configuring Windows® 8

Product Number: 20687B

Released: 12/2012

MICROSOFT LICENSE TERMS
MICROSOFT INSTRUCTOR-LED COURSEWARE

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

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

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

1. **DEFINITIONS.**

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

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

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

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

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

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

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

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

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

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

   k. "MPN Member" means an active silver or gold-level Microsoft Partner Network program member in good standing.

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

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

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

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

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

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

   a. **If you are a Microsoft IT Academy Program Member:**
      i. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
      ii. For each license you acquire on behalf of an End User or Trainer, you may either:
         1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User who is enrolled in the Authorized Training Session, and only immediately prior to the commencement of the Authorized Training Session that is the subject matter of the Microsoft Instructor-Led Courseware being provided, **or**
         2. provide one (1) End User with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
         3. provide one (1) Trainer with the unique redemption code and instructions on how they can access one (1) Trainer Content,
      provided you comply with the following:
      iii. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
      iv. you will ensure each End User attending an Authorized Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Authorized Training Session,
      v. you will ensure that each End User provided with the hard-copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,
      vi. you will ensure that each Trainer teaching an Authorized Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Authorized Training Session,

vii. you will only use qualified Trainers who have in-depth knowledge of and experience with the Microsoft technology that is the subject of the Microsoft Instructor-Led Courseware being taught for all your Authorized Training Sessions,

viii. you will only deliver a maximum of 15 hours of training per week for each Authorized Training Session that uses a MOC title, and

ix. you acknowledge that Trainers that are not MCTs will not have access to all of the trainer resources for the Microsoft Instructor-Led Courseware.

b. **If you are a Microsoft Learning Competency Member**:

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

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

1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User attending the Authorized Training Session and only immediately prior to the commencement of the Authorized Training Session that is the subject matter of the Microsoft Instructor-Led Courseware provided, **or**

2. provide one (1) End User attending the Authorized Training Session with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**

3. you will provide one (1) Trainer with the unique redemption code and instructions on how they can access one (1) Trainer Content,

provided you comply with the following:

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

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

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

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

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

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

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

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

c. **If you are a MPN Member**:
   i. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
   ii. For each license you acquire on behalf of an End User or Trainer, you may either:
      1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User attending the Private Training Session, and only immediately prior to the commencement of the Private Training Session that is the subject matter of the Microsoft Instructor-Led Courseware being provided, **or**
      2. provide one (1) End User who is attending the Private Training Session with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
      3. you will provide one (1) Trainer who is teaching the Private Training Session with the unique redemption code and instructions on how they can access one (1) Trainer Content,
      provided you comply with the following:
   iii. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
   iv. you will ensure that each End User attending an Private Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Private Training Session,
   v. you will ensure that each End User provided with a hard copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,
   vi. you will ensure that each Trainer teaching an Private Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Private Training Session,
   vii. you will only use qualified Trainers who hold the applicable Microsoft Certification credential that is the subject of the Microsoft Instructor-Led Courseware being taught for all your Private Training Sessions,
   viii. you will only use qualified MCTs who hold the applicable Microsoft Certification credential that is the subject of the MOC title being taught for all your Private Training Sessions using MOC,
   ix. you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and
   x. you will only provide access to the Trainer Content to Trainers.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

LIMITATION DES DOMMAGES-INTÉRÊTS ET EXCLUSION DE RESPONSABILITÉ POUR LES DOMMAGES. Vous pouvez obtenir de Microsoft et de ses fournisseurs une indemnisation en cas de dommages directs uniquement à hauteur de 5,00 $ US. Vous ne pouvez prétendre à aucune indemnisation pour les autres dommages, y compris les dommages spéciaux, indirects ou accessoires et pertes de bénéfices.
Cette limitation concerne:
  •   tout ce qui est relié au le contenu sous licence, aux services ou au contenu (y compris le code) figurant sur des sites Internet tiers ou dans des programmes tiers; et.
  •   les réclamations au titre de violation de contrat ou de garantie, ou au titre de responsabilité stricte, de négligence ou d'une autre faute dans la limite autorisée par la loi en vigueur.

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

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

Revised September 2012

Module 1

Installing and Deploying Windows 8

Contents:

Lesson 2
Preparing to Install Windows 8

Contents:

Additional Reading

Determining Device Compatibility and Screen Resolution

Additional Reading: http://go.microsoft.com/fwlink/?LinkId=266551

Lesson 3
Installing Windows 8

Contents:

Question and Answers

Discussion: Deciding When to Perform a Clean Installation

Question: When do you typically perform a clean installation of Windows?

Answer: There are some cases when a clean installation is the only choice:

- No operating system is installed on the computer.

- The installed operating system does not support an upgrade to Windows 8.

You might prefer a clean installation over an upgrade if the previous version of Windows was experiencing file corruption or other performance-related issues. If there is no desire to retain applications or setting from the previous version of Windows, you typically will choose a clean installation over an upgrade or a migration.

Discussion: Common Installation Errors

Question: What potential issues might you encounter when installing Windows?

Answer: The answers may vary. The following table describes several installation problems and solutions that you can use to identify and solve specific problems.

Problem	Solution
Installation media is damaged.	Test the CD or DVD on another system.
BIOS upgrade is needed.	Check your computer supplier's Internet site to determine whether a BIOS upgrade is available for Windows 8.
Hardware is installed improperly.	Check any messages that appear during the boot phase. Install add-on hardware properly, such as video cards and memory modules.
Hardware fails to meet minimum requirements.	Use Windows Catalog to locate products designed for Microsoft Windows and ensure that your hardware meets the minimum requirements for the Windows 8 edition that you want to install.
Error messages appear during setup.	Carefully note any messages, and then search the Microsoft Knowledge Base for an explanation.

Lesson 4
Automating the Installation of Windows 8

Contents:

Question and Answers

What Is Windows PE?

Question: What are some of the tasks in which you can use Windows PE for troubleshooting?

Answer: You can use Windows PE to replace system files, recover data before installing Windows, and run diagnostic and configuration tools on a system where Windows is not installed, or the Windows installation is not functioning properly

Modifying Images by Using DISM

Question: How does DISM use ImageX technology?

Answer: ImageX is a command-line tool that you can use to mount an image or apply an image to a drive so that you can modify it with the DISM command-line utility. After you modify the image, you can use ImageX to capture the image, append the image to a WIM, or export the image as a separate file. If you do not need to capture, append, or export the image after you modify it, use DISM to mount the image instead of using ImageX.

Additional Reading

Modifying Images by Using DISM

Note: The full list of DISM command line options can found on the TechNet Library website at http://go.microsoft.com/fwlink/?LinkId=266552

Demonstration

Demonstration: Building an Answer File by Using Windows SIM

Demonstration Steps

1. Sign in to the **LON-CL1** virtual machine as **Adatum\Administrator** with the password **Pa$$w0rd.**

2. On the **Start** screen, type, **Image Manager** and then press Enter. The Windows System Image Manager starts.

3. In **Windows System Image Manager**, click **File**, and then click **Select Windows Image**.

4. In the Select a Windows Image window, browse to **E:\Labfiles\Mod01\Sources**, and double-click **install.wim**.

5. In Windows System Image Manager, click **File**, and then click **New Answer File**.

6. In the **Windows Image** section, expand **Components**, scroll down, right-click amd_64_**Microsoft-Windows-Setup_6.2.9200.16384_neutral**, and then click **Add Setting to Pass 1 windowsPE**.

7. In the **Answer File** section, expand **amd64_Microsoft-Windows-Setup_neutral**, and then click **UserData**.

8. In the **Properties** pane, under **Settings**, double-click the **Organization** setting, type **Adatum**, and then press Enter.

9. In the **Properties** pane, under **Settings**, double-click the **FullName** setting, type **Adatum**, and then press Enter.

10. In the **Properties** pane, under **Settings**, double-click the **AcceptEula** setting, and then from the drop-down menu, select **true**.

11. In **Windows System Image Manager**, click **File**, and then click **Save Answer File As**.

12. Navigate to the **Desktop**, type **autounattend.xml**, and then click **Save**.

13. Close the **Windows System Image Manager**.

14. Click back to return to the main Start screen.

Demonstration: Creating Bootable Windows PE Media

Demonstration Steps

1. On LON-CL1, on the **Start** screen, type the following, and then press Enter:

```
Deployment and Imaging Tools Environment
```

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

```
copype x86 C:\winpe_x86
```

This command copies the necessary files to the **C:\winpe_x86** folder. If the folder does not exist, Windows creates it.

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

```
Dism /mount-image /imagefile:c:\winpe_x86\media\sources\boot.wim /index:1
/mountdir:C:\winpe_x86\mount
```

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

```
Dism /Image:C:\winpe_x86\mount /Add-Package /PackagePath:"C:\Program Files
(x86)\Windows Kits\8.0\Assessment and Deployment Kit\Windows Preinstallation
Environment\x86\WinPE_OCs\WinPE-WinReCfg.cab"
```

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

```
Dism /unmount-image /mountdir:C:\winpe_x86\mount /commit
```

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

```
MakeWinPEMedia /ISO C:\winpe_x86 c:\winpe_x86\winpe.iso
```

Module Review and Takeaways

Review Question(s)

Question: Your organization is deploying Windows 8 AppLocker® to restrict certain applications. Which edition of Windows 8 do you need to install on the organization's computers?

Answer: AppLocker is available only in Windows 8 Enterprise.

Question: What are the methods available for using a .wim file to install Windows 8?

Answer: You can install from DVD, from a network share, from a USB key, by using WDS, by using the MDT integration with Microsoft System Center 2012, and from a PXE boot.

Tools

Tool	Use to	Where to find it
Application Compatibility Toolkit	Check application compatibility for Windows 8	http://go.microsoft.com/fwlink/?LinkId=266553
Windows ADK	Assess and deploy Windows	Wait for link***
Windows SIM	Create and edit answer files	Windows ADK
ImageX	Create, modify, and apply WIM-based image files	Windows ADK
USMT	Migrate user settings	Windows ADK
DISM	Service WIM-based image files	Windows ADK
Volume Activation Management Tool	Manage volume windows activation	Windows ADK

Lab Review Questions and Answers

Lab A: Installing Windows® 8

Question: After you test your operating systems on the virtual machines on the test computer, how can you migrate those virtual machines to the production environment?

Answer: You can export the virtual machines from Client Hyper-V, and then import them to Windows Server 2012 running the Hyper-V role in the production environment.

Question: Why would you not use Windows 8 Enterprise in the situation that the lab presents?

Answer: Windows 8 Enterprise would run on the hardware specified, and provide all of the functionality that you require. However, it typically is more expensive to license, and only is available to volume license subscribers.

Lab B: Performing an Unattended Installation of Windows 8

Question: Why would you use an answer file when you configure the installation of only one computer?

Answer: You would use an answer file for several reasons, including to ensure that user and organizational information is correct; because of an inability to interactively perform the installation process; to specify a detailed configuration; or when you are not requiring that a user enter the product key.

Question: If you need to deploy this answer file to numerous computers in your environment, what tools could you use?

Answer: MDT, System Center Configuration Manager, WDS, and Windows ADK

Module 2

Upgrading and Migrating to Windows 8

Contents:

Lesson 2
Migrating to Windows 8

Contents:

Question and Answers

What Is Migration?

Question: You have a user who wants to upgrade a Windows XP computer to Windows 8. The computer meets all of the hardware requirements for Windows 8, and the user wants to retain all of the existing user settings and use the same applications. The user has no time-related requirements, and can be without the computer while you install Windows 8. How should you perform the Windows 8 installation?

Answer: While most of the scenario would suggest an in-place upgrade, you cannot upgrade Windows XP directly to Windows 8. Therefore, you need to perform a migration in this scenario, retain the user's settings, and reinstall applications.

Question: One of your users has been promoted to a new position, and the user has been given a new computer. The user would like to have the new applications that the job requires installed, as well as the documents and settings from the old Windows 7 computer transferred to the new computer. How should you perform the Windows 8 installation?

Answer: You should perform an in-place migration in this scenario. A new computer and a new set of applications is being used. After installing Windows 8 on the new computer, and installing new applications, you need to copy the user's documents and settings, which are on the Windows 7 computer, to the new Windows 8 computer.

Module Review and Takeaways

Review Question(s)

Question: List the key steps in performing an in-place upgrade.

Answer: The key steps in performing an in-place upgrade are:

1. Assessing the current environment and determining the suitability of an in-place upgrade.

2. Backing up important files.

3. Running Windows Setup.

Question: Why would you not choose to perform an in-place upgrade?

Answer: Answers will vary, but may include that it would be:

*   Incompatible with a previous operating system.

*   Too extensive, since only a small subset of data needs to be kept.

*   Too extensive, since you do not want to retain old applications or user settings.

Question: What are the advantages of using the USMT versus WET?

Answer: In general, the USMT allows more customization of the migration process, and makes it easier to handle different variables in the migration process. Typically, you use WET for simple, one-time, one-user migrations, whereas you use USMT for larger and more-complex scenarios

Tools

Tool	Use to	Where to find it
Windows Easy Transfer	Perform user data migration	Start screen
User State Migration Tool	Perform user data migration	Windows ADK

Lab Review Questions and Answers

Lab: Migrating to Windows 8

Question: Why did you use WET rather than USMT in this lab?

Answer: WET provides a more simplified and easy-to-execute process for transferring user settings. USMT primarily is for scenarios that involve large-scale transfers or those involving complex user settings. The customizability of USMT migration makes it a better tool when you need to migrate specific user data.

Question: What location holds user settings information in Windows 8?

Answer: C:\Users\

Module 3

Managing Disks and Device Drivers

Contents:

Lesson 1
Managing Disks, Partitions, and Volumes

Contents:

Question and Answers

Converting an MBR Partition to a GPT Partition

Question: Which tool do you prefer to use to convert a new disk to GPT: the Disk Management snap-in, Windows PowerShell or the **diskpart.exe** command-line tool?

Answer: Each tool can achieve the same results. However, they have different uses. For example, if you are adding a single disk to a single computer, you may want to use Disk Management. If you are adding several disks, or are modifying several computers, you may want to use a Windows PowerShell script.

Creating a Simple Volume

Question: In what circumstances will you use less than all of the available space on a new volume's disk?

Answer: Answers vary, but one of the circumstances in which this is true is when you are partitioning a disk to support dual-boot scenarios.

Creating Spanned and Striped Volumes

Question: What is the advantage of using striped volumes, and conversely what is the major disadvantage?

Answer: Performance is the advantage, while the potential disadvantage is reduced fault tolerance.

Resizing a Volume

Question: When might you need to reduce the system partition's size?

Answer: Answers will vary, but to enable BitLocker® drive encryption, an unencrypted partition must be available. However, in some circumstances, an unencrypted partition might not be available on a computer, so reducing the system volume size might prove useful. It might be worth mentioning that fragmentation, and how the placement of certain types of files on the disks, such as the Master File Table (MFT), can prevent you from realizing all the available free space as a new volume.

Additional Reading

Additional Reading: For more information, see Storage in Windows PowerShell: http://go.microsoft.com/fwlink/?LinkId=266556.

Demonstration

Demonstration: Converting an MBR Partition to a GPT Partition

Demonstration Steps

Using diskpart

1. Sign in to the LON-CL2 virtual machine as **Adatum\Administrator** with the password **Pa$$w0rd**.

2. On the Start screen, type **c**, and then in the **Apps** search screen, click **Command Prompt**.

3. At the command prompt, type **diskpart**, and then press Enter.

4. At the **DISKPART>** prompt, type **list disk**, and then press Enter.

5. At the **DISKPART>** prompt, type **select disk 2**, and then press Enter.

6. At the **DISKPART>** prompt, type **convert gpt**, and then press Enter.

7.   Close the command prompt.

Using Windows PowerShell

1.   Open the Start screen, type **p**, and then in the **Apps** search screen, right-click **Windows PowerShell**.

2.   Click **Run as administrator**.

3.   In the Administrator: Windows PowerShell window, type **get-disk**, and then press Enter.

4.   Discuss the information in the Partition Style column.

5.   In the Administrator: Windows PowerShell window, type **Initialize-Disk -Number 3**, and then press Enter.

6.   Minimize the Administrator: Windows PowerShell window.

Using Disk Management

1.   Open the Start screen.

2.   Type **diskmgmt.msc**, and then press Enter.

3.   In the **Initialize Disk** dialog box, click **OK**.

4.   Right-click **Disk 4**, and then click **Convert to GPT Disk**.

5.   Close Disk Management.

Verifying the disk type

1.   Restore the Administrator: Windows PowerShell window.

2.   In the Administrator: Windows PowerShell window, type **get-disk**, and then press Enter.

3.   Discuss the information in the Partition Style column.

4.   Close the Administrator: Windows PowerShell window.

Demonstration: Creating a Simple Volume

Demonstration Steps

Using Disk Management

1.   If necessary, sign in to the LON-CL2 virtual machine as **Adatum\Administrator** with the password **Pa$$w0rd**.

2.   Open the Start screen.

3.   Type **diskmgmt.msc**, and then press **Enter**.

4.   Right-click the unallocated space on Disk 2, and then click **New Simple Volume**.

5.   In the New Simple Volume Wizard, on the **Welcome to the New Simple Volume Wizard** page, click **Next**.

6.   On the **Specify Volume Size** page, change the **Simple volume size in MB** value to **5103**, and then click **Next**.

7.   On the **Assign Drive Letter or Path** page, click **Next**.

8.   On the **Format Partition** page, in the **Volume label** text box, type **Simple1**, and then click **Next**.

9.   On the **Completing the New Simple Volume Wizard** page, click **Finish**.

10.   When the New Simple Volume Wizard is complete, close Disk Management.

Using Windows PowerShell

1. Open the Start screen, type **p**, and then in the **Apps** search screen, right-click **Windows PowerShell**.

2. Click **Run as administrator**.

3. In the **Administrator: Windows PowerShell** window, type **get-disk**, and then press Enter.

4. In the **Administrator: Windows PowerShell** window, type **get-disk -Number 3 | new-partition –size 5350879232 | Format-Volume -Confirm:$false –Filesystem NTFS –NewFileSystemLabel Simple2**, and then press Enter.

5. In the Administrator: Windows PowerShell window, type **Get-partition**, and then press Enter. Make note of the **PartitionNumber** of the volume you just created on **Disk Number 3**. You will use this information in the next step.

6. In the Administrator: Windows PowerShell window, type **Set-partition -DiskNumber 3 -PartitionNumber *x* -NewDriveLetter G**, (where *x* is the results of the previous step), and then press Enter.

7. Minimize the Administrator: Windows PowerShell window.

8. In Windows Explorer, verify the visibility of the volumes that you created.

9. Close Windows Explorer window.

Demonstration: Creating Spanned and Striped Volumes

Demonstration Steps

Creating a spanned volume

1. If necessary, sign in to the LON-CL2 virtual machine as **Adatum\Administrator** with the password **Pa$$w0rd**.

2. Open the Start screen.

3. Type **diskmgmt.msc**, and then press Enter.

4. Right-click the unallocated space on Disk 2, and then click **New Spanned Volume**.

5. In the New Spanned Volume Wizard, on the **Welcome to the New Spanned Volume Wizard** page, click **Next**.

6. On the **Select Disks** page, select **Disk 3**. Hold down the Shift key, select **Disk 4**, and then click **Add**.

7. On the **Select Disks** page, select **Disk 2**. In the **Select the amount of space in MB** text box, type **2000.**

8. On the **Select Disks** page, select **Disk 3**. In the **Select the amount of space in MB** text box, type **1500.**

9. On the **Select Disks** page, with **Disk 4** selected, in the **Select the amount of space in MB** text box type **4000**, and then click **Next.**

10. On the **Assign Drive Letter or Path** page, click **Next**.

11. On the **Format Volume** page, in the **Volume label** text box, type **SpanVol**.

12. Select the **Perform a quick format** check box, and then click **Next**.

13. On the **Completing the New Spanned Volume Wizard** page, click **Finish**.

14. Review the Disk Management warning, and then click **Yes**.

Creating a striped volume

1. Right-click the unallocated space on Disk 2, and then click **New Striped Volume**.

2. In the New Striped Volume Wizard, on the **Welcome to the New Striped Volume Wizard** page, click **Next**.

3. On the **Select Disks** page, select **Disk 3**. Hold down the Shift key, select **Disk 4**, and then click **Add**.

4. On the **Select Disks** page, in the **Select the amount of space in MB** text box, type **2000**, and then click **Next**.

5. On the **Assign Drive Letter or Path** page, click **Next**.

6. On the **Format Partition** page, in the **Volume label** text box, type **StripedVol**.

7. Select the **Perform a quick format** check box, and then click **Next**.

8. On the **Completing the New Striped Volume Wizard** page, click **Finish**.

9. Close Disk Management and any other open windows on LON-CL2.

Demonstration: Resizing a Volume

Demonstration Steps

Using diskpart

1. If necessary, sign in to the LON-CL2 virtual machine as **Adatum\Administrator** with the password **Pa$$w0rd**.

2. Open the Start screen, type **c**, and in the **Apps** search screen, click **Command Prompt**.

3. At the command prompt, type **Diskpart**, and then press Enter.

4. At the DISKPART> prompt, type **list volume**, and then press Enter.

5. Take note of the Volume number associated with Simple2.

6. At the DISKPART> prompt, type **select volume <n>**, and then press Enter. (Where <n> is the number noted in step 5)

7. At the DISKPART> prompt, type **shrink desired=50**, and then press Enter.

8. When the shrink command has completed, at the DISKPART> prompt, type **list volume**, and then press Enter.

9. Compare the reported size of the Simple2 volume as reported now with the value from the previous list volume command.

10. Close the command prompt.

Using Disk Management

1. Point to the lower-right corner of the screen, and then click the Start menu.

2. Type **diskmgmt.msc**, and then press Enter.

3. Right-click the Spanned Volume on Disk 3, and then click **Extend Volume**.

4. In the Extend Volume Wizard, on the **Welcome to the Extend Volume Wizard** page, click **Next**.

5. On the **Select Disks** page, select **Disk 3**. In the **Select the amount of space in MB** text box, type **50**, and then click **Next.**

6. On the **Completing the Extend Volume Wizard** page, click **Finish**.

7. When the Extend Volume Wizard is complete, close Disk Management.

Lesson 2
Maintaining Disks, Partitions, and Volumes

Contents:

Question and Answers

Configuring Disk Quotas

Question: Will Quota management be useful in your organizations?

Answer: Answers will vary. In most cases there is no need to limit disk usage on computers that are running Windows 8. However, it might be useful when multiple users share the same computer or when your users perform peer-to-peer networking in a workgroup. It is more common to implement quotas on servers.

Demonstration

Demonstration: Configuring Disk Quotas

Demonstration Steps

Create a disk quota

1. If necessary, sign in to the LON-CL2 virtual machine as **Adatum\Administrator** with the password **Pa$$w0rd**.

2. Click the Windows Explorer icon on the task bar.

3. In the Libraries window, click **Computer**.

4. Right-click **StripedVol (I:)**, and then click **Properties**.

5. In the **StripedVol (I:) Properties** dialog box, click the **Quota** tab.

6. On the **Quota** tab, select the **Enable quota management** check box.

7. Select the **Deny disk space to users exceeding quota limit** check box.

8. Click **Limit disk space to**, in the adjacent box type **6**, and then in the **KB** list, click **MB**.

9. In the **Set warning level to** box, type **4**, and then in the **KB** list, click **MB**.

10. Select the **Log event when a user exceeds their warning level** check box, and then click **OK**.

11. In the **Disk Quota** dialog box, review the message, and then click **OK**.

12. Close all open windows.

13. Open the Start screen, type **c**, and in the **Apps** search screen, click **Command Prompt**.

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

15. At the command prompt, type **fsutil file createnew 2mb-file 2097152**, and then press Ente**r**.

16. At the command prompt, type **fsutil file createnew 1kb-file 1024**, and then press Enter.

17. Close the Command Prompt window.

18. Open the Start screen, and then click **Administrator**.

19. Click **Sign out**.

Test a disk quota

1. Sign in to the LON-CL2 virtual machine as **Adatum\Alan** with the password **Pa$$w0rd**.

2. Click the Desktop tile.

3. Click the Windows Explorer icon on the task bar.

4. In the Libraries window, click **Computer**.

5.   Double-click **StripedVol (I:)**.

6.   On the toolbar, click **Home**, and then click **New Folder**.

7.   Type **Alan's files**, and then press Enter.

8.   In the file list, right-click **2mb-file**, drag it to **Alan's files**, and then click **Copy here**.

9.   In the file list, right-click **1kb-file**, drag it to **Alan's files**, and then click **Copy here**.

10.   Double-click **Alan's files**.

11.   Right-click **2mb-file**, and then click **Copy**.

12.   Press Ctrl+V.

13.   Right-click **2mb-file**, and then click **Copy**.

14.   Press Ctrl+V.

15.   In the **Copy Item** dialog box, review the message, and then click **Cancel**.

16.   Open the Start screen, and then click **Alan Steiner**.

17.   Click **Sign out**.

Review quota entries and events

1.   Sign in to the LON-CL2 virtual machine as **Adatum\Administrator** with the password **Pa$$w0rd**.

2.   Click the Desktop tile.

3.   Click the Windows Explorer icon on the task bar.

4.   In the Libraries window, click **Computer**.

5.   Right-click **StripedVol (I:)** and then click **Properties**.

6.   In the **StripedVol (I:) Properties** dialog box, click the **Quota** tab, and then click **Quota Entries**.

7.   In the **Quota Entries for Striped Volume (I:)**, in the **Name** column, double-click **Alan Steiner**.

8.   Review the entries in the **Quota Settings for Alan Steiner (Alan@Adatum.com)** dialog box.

9.   In the **Quota Settings for Alan Steiner (Alan@Adatum.com)** dialog box, click **OK**.

10.   Close **Quota Entries for StripedVol (I:)**.

11.   Close **StripedVol (I:) Properties**.

12.   Close Windows Explorer.

13.   Open the Start screen, type **eventvwr**, and then press Enter.

14.   Maximize the **Event Viewer** program.

15.   In the **Event Viewer (Local)** list, expand **Windows Logs**, and then click **System**.

16.   Right-click **System**, and then click **Filter Current Log**.

17.   In the **<All Events IDs>** box, type **36**, and then click **OK**.

18.   Examine the listed entry.

19.   Close all open windows.

Lesson 3
Working with Virtual Hard Disks

Contents:

Additional Reading

What Are Virtual Hard Disks?

Additional Reading: For more information on the VHDX format, go to
http://go.microsoft.com/fwlink/?LinkId=266557.

Lesson 4
Installing and Configuring Device Drivers

Contents:

Question and Answers

Managing Drivers

Question: If your computer does not startup normally due a device driver issue, what options are there for performing driver roll back?

Answer: Try starting in Safe mode and then rolling the driver back.

Additional Reading

Device Driver Management Tools

Additional Reading: For a list of device stage experiences, go to http://go.microsoft.com/fwlink/?LinkId=266558.

Demonstration

Demonstration: Managing Drivers

Demonstration Steps

Update a device driver

1. If necessary, sign in to the LON-CL2 virtual machine as **Adatum\Administrator** with the password **Pa$$w0rd**.

2. Open the Start screen.

3. Type **comp**, and then right-click **Computer** in the results section.

4. Click **Manage** from the context menu at the bottom of the screen.

5. In Computer Management, click **Device Manager**.

6. Expand **Keyboards**, right-click **Standard PS/2 Keyboard**, and then click **Update Driver Software**.

7. In the **Update Driver Software – Standard PS/2 Keyboard** dialog box, click **Browse my computer for driver software**.

8. On the **Browse for driver software on your compute**r page, click **Let me pick from a list of device drivers on my computer**.

9. In the **Show compatible hardware** list, click **PC/AT Enhanced PS/2 Keyboard (101/102 Key)**, and then click **Next**.

10. Click **Close**.

11. In the **System Settings Change** dialog box, click **Yes** to restart the computer.

Uninstall a device driver

1. Sign in to the LON-CL2 virtual machine as **Adatum\Administrator** with the password **Pa$$w0rd**.

2. Type **comp**, and then right-click **Computer** in the results section.

3. Click **Manage** from the context menu at the bottom of the screen.

4. In Computer Management, click **Device Manager**.

5. Expand **Keyboards**, right-click **PC/AT Enhanced PS/2 Keyboard (101/102 Key)**, and then click **Properties**.

6. In the **PC/AT Enhanced PS/2 Keyboard (101/102 Key) Properties** dialog box, click the **Driver** tab.

7. Click **Uninstall**.

8. In the **Confirm Device Uninstall** dialog box, click **OK**.

9. In the **System Settings Change** dialog box, click **Yes** to restart the computer.

10. Sign in to the LON-CL2 virtual machine as **Adatum\Administrator** with the password **Pa$$w0rd**.

11. Type **comp**, and then right-click **Computer** in the results section.

12. Click **Manage** from the context menu at the bottom of the screen.

13. In Computer Management, click **Device Manager**.

14. Expand **Keyboards**, click **Standard PS/2 Keyboard**, and then verify that you have successfully uninstalled the driver.

15. Close Computer Management.

Install a driver into the driver store

1. Open the Start screen, type **c**, and then in the **Apps** search screen, right-click **Command Prompt**.

2. Click **Run as administrator**.

3. At the Command Prompt, type **pnputil –a** "**E:\Labfiles\Mod03\Intellipoint\ipoint\setup64\files\driver\point64\point64.inf"**, and then press Enter.

4. In the Command Prompt, type **pnputil –e**, and then press Enter. Take note of the published name for the driver that you just installed into the store.

5. Close the command prompt.

Module Review and Takeaways

Review Question(s)

Question: You are implementing 64-bit Windows 8 and need to partition the disk to support 25 volumes, some of which will be larger than 2 terabytes. Can you implement this configuration by using a single hard disk?

Answer: Yes, you can format the disk for GPT rather than MBR. A GPT disk supports up to 128 volumes, each much larger than 2 terabytes. Additionally, you can boot 64-bit Windows 8 from a GPT disk.

Question: You have created a volume on a newly installed hard disk by using diskpart.exe. Now, you want to continue using diskpart.exe to perform the following tasks:

Format the volume for NTFS.

Assign the next available drive letter.

Assign a volume label of *sales-data*.

What two commands must you use for these tasks?

Answer: The two commands are as follows:

format fs=ntfs label=sales-data

assign

Question: You recently upgraded to Windows 8, and are experiencing occasional problems with the shortcut keys on your keyboard. Describe the first action you might take to the resolve the issue, and then list the steps to perform the action.

Answer: Update the device driver for the keyboard. To manually update the driver that the keyboard uses, follow these steps in Device Manager:

1.   Double-click the **Keyboard** category of devices.

2.   Right-click the device and then click **Update Driver Software**.

3.   Follow the instructions in the Update Driver Software Wizard.

Tools

The following table lists some of the tools available for managing hard disks and devices:

Tool	Used for	Where to find it
Defrag.exe	Performing disk defragmentation tasks from the command-line.	Command prompt
Device Manager	Viewing and updating hardware settings, and driver software for devices, such as internal hard drives, disc drives, sound cards, video or graphics cards, memory, processors, and other internal computer components.	Devmgmt.msc or Embedded in Computer Management
The Windows 8 device apps	Helps users interact with devices, and use the full functionality of the devices.	Start screen or Task bar
Devices and	Provides users a single location to	Control Panel

Tool	Used for	Where to find it
Printers	find and manage all the devices connected to their Windows 8-based computers. Also provides quick access to device status, product information, and key functions, such as faxing and scanning to enhance and simplify the customer experience with a Windows 8-connected device.	
The Optimize Drives tool	Rearranging fragmented data so that disks and drives can work more efficiently.	In Windows Explorer, right-click a volume, click **Properties**, click the **Tools** tab, and then click **Optimize**.
Disk Management	Managing disks and volumes, both basic and dynamic, locally or on remote computers.	diskmgmt.msc
Diskpart.exe	Managing disks, volumes, and partitions from the command-line or from Windows PE.	Open a command prompt and then type **diskpart**.
Fsutil.exe	Performing tasks that are related to FAT and NTFS file systems, such as managing reparse points, managing sparse files, or dismounting a volume.	Command prompt (elevated)
Pnputil.exe	Adding drivers to and managing drivers in the protected device store.	Command prompt (elevated)

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Configuring disk quotas on multiple volumes	Once you create a quota, you can export it, and then import it for a different volume. In addition to establishing quota settings on an individual computer by using this method, you can also use Group Policy settings to configure quotas. This lets administrators configure multiple computers with the same quota settings.
Exceeding the quota allowance	To increase free disk space after exceeding the quota allowance, the user can try the following: Delete unnecessary files Have another user claim ownership of nonuser-specific files Additionally an administrator could: Increase the quota allowance as volume size and policy permits
If you have a hardware problem, the hardware or a device driver may be causing it. Troubleshooting hardware problems often starts by troubleshooting device	To identify a device driver problem, answer the questions: Did you recently upgrade the device driver or other

Common Issue	Troubleshooting Tip
drivers.	software related to the hardware? If so, roll back the device driver to the previous version.
	Are you experiencing occasional problems, or is the device not compatible with the current version of Windows? If so, upgrade the device driver.
	Did the hardware suddenly stop working? If so, upgrade the device driver. If that does not solve the problem, reinstall the device driver. If the problem continues, try troubleshooting the hardware problem.

Lab Review Questions and Answers

Lab A: Managing Disks

Question: When would you use a spanned volume instead of a simple volume?

Answer: Spanned volumes allow you to combine space from multiple drives. You would use a spanned volume to present several drives as a single drive to the operating system.

Question: In your environment, where would you use disk quotas?

Answer: Answers will vary based on students' experience. One possible answer is that you would do this on a shared system to minimize the effect of users saving files on the shared system.

Question: When would you use a VHD on a workstation computer?

Answer: Answers will vary based on students' experience. One possible answer is that you can use VHDs to support multiple operating systems.

Lab B: Configuring Device Drivers

Question: When would you preinstall drivers on workstation computers?

Answer: Answers will vary based on students' experience. One possible answer is: You would preinstall a driver when you plan on using specific devices and are not planning on giving your users local administrative rights.

Question: When would you uninstall a device driver?

Answer: Answers will vary based on students' experience. One possible answer is: A recently installed driver is causing issues on the client system.

Module 4

Configuring and Troubleshooting Network Connections

Contents:

Lesson 1
Configuring IPv4 Network Connectivity

Contents:

Question and Answers

What Are Public and Private IPv4 Addresses?

Question: Which of the following is not a private IP address?

a. 171.16.16.254

b. 192.16.18.5

c. 192.168.1.1

d. 10.255.255.254

Answer: A and B. C and D are private IP addresses. C falls in the range of 192.168.0.1 to 192.168.255.254, and D falls in the range of 10.0.0.1 to 10.255.255.254.

Configuring an IPv4 Address

Question: When might you need to change a computer's IPv4 address?

Answer: You might need to change a computer's IPv4 address when two computers have the same IPv4 address. You must ensure that all computers on your network have a unique IPv4 address. If two computers have the same IPv4 address, then you must change the IPv4 address on one of the two computers.

Additional Reading

What Is a Subnet Mask?

Additional Reading: For additional information on CIDR, go to http://go.microsoft.com/fwlink/?LinkId=154437.

What Are Public and Private IPv4 Addresses?

Additional Reading: For additional information on CIDR, go to http://go.microsoft.com/fwlink/?LinkId=154437.

Demonstration

Demonstration: Configuring an IPv4 Address

Demonstration Steps

View the current network connection configuration

1. Sign in to the LON-CL1 virtual machine as **Adatum\Administrator** with the password **Pa$$w0rd**.

2. On the Start screen, right-click the display, click **All apps**, and then click **Command Prompt**.

3. At the command prompt, type **ipconfig /all**, and then press Enter. This displays the configuration for all network connections on the computer.

4. Close the command prompt.

View the IPv4 configuration

1. Point to the bottom-left corner of the taskbar, and then click **Start** to return to the Start screen.

2.   Point to the lower-right corner of the Start screen, and then click **Search**.

3.   In the Search box, type **Control**, and then click **Control Panel**.

4.   In Control Panel, click **Network and Internet**.

5.   In Network and Internet, click **View network status and tasks**.

6.   In Network and Sharing Center, to the right of the Adatum.com Domain network, click **Local Area Connection**.

7.   In the Local Area Connection Status window, click **Details**. This window shows the same configuration information for this adapter as the **ipconfig** command.

8.   In the **Network Connection Details** windows, click **Close**.

9.   In the **Local Area Connection Status** window, click **Properties**. You can configure protocols in this window.

10. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**. You can configure the IP address, subnet mask, default gateway, and Domain Name System (DNS) servers in this window.

11. Click **Advanced**. In the Advanced TCP/IP Settings window, you can configure additional settings, such as additional IP addresses, DNS settings, and Windows Internet Naming Service (WINS) servers for NetBIOS name resolution.

12. Close all open windows without modifying any settings.

Lesson 2
Configuring IPv6 Network Connectivity

Contents:

Additional Reading

Benefits of Implementing IPv6

📘   **Additional Reading:** For more information on IPv6, go to
http://go.microsoft.com/fwlink/?LinkId=154442.

📘   **Additional Reading:** For more information on IPv6, go to
http://go.microsoft.com/fwlink/?LinkId=154442.

IPv6 Addresses

📘   **Additional Reading:** For more information on IPv6 address types, go to
http://go.microsoft.com/fwlink/?LinkId=154445.

📘   **Additional Reading:** For 6 more information on IPv6 address types, go to
http://go.microsoft.com/fwlink/?LinkId=154445.

Lesson 3
Implementing Automatic IP Address Allocation

Contents:

Additional Reading

Troubleshooting Client-Side IPv4 Autoconfiguration Issues

Reference Links: See also:

- Test a TCP/IP configuration by using the ping command:
  http://go.microsoft.com/fwlink/?LinkId=154455

- Verify, release, or renew a client address lease:
  http://go.microsoft.com/fwlink/?LinkId=154456

- Configure TCP/IP for automatic addressing:
  http://go.microsoft.com/fwlink/?LinkId=154457

- Disable automatic address configuration:
  http://go.microsoft.com/fwlink/?LinkId=154458

- Manage Options and classes:
  http://go.microsoft.com/fwlink/?LinkId=154459

- Assigning options:
  http://go.microsoft.com/fwlink/?LinkId=154460

- DHCP Best Practices:
  http://go.microsoft.com/fwlink/?LinkId=154465

- Using superscopes:
  http://go.microsoft.com/fwlink/?LinkId=154466

- Configuring scopes:
  http://go.microsoft.com/fwlink/?LinkId=154467

Reference Links:

- Test a TCP/IP configuration by using the ping command:
  http://go.microsoft.com/fwlink/?LinkId=154455

- Verify, release, or renew a client address lease:
  http://go.microsoft.com/fwlink/?LinkId=154456

- Configure TCP/IP for automatic addressing:
  http://go.microsoft.com/fwlink/?LinkId=154457

- Disable automatic address configuration:
  http://go.microsoft.com/fwlink/?LinkId=154458

- Manage Options and classes:
  http://go.microsoft.com/fwlink/?LinkId=154459

- Assigning options:
  http://go.microsoft.com/fwlink/?LinkId=154460

- DHCP Best Practices:
  http://go.microsoft.com/fwlink/?LinkId=154465

- Using superscopes:
  http://go.microsoft.com/fwlink/?LinkId=154466

- Configuring scopes:
  http://go.microsoft.com/fwlink/?LinkId=154467

Demonstration

Demonstration: Configuring a Computer to Obtain an IPv4 Configuration Automatically

Demonstration Steps

View the current IPv4 configuration

1. If necessary, sign in to the LON-CL1 virtual machine as **Adatum\Administrator** with the password **Pa$$w0rd**.

2. If necessary, point to the bottom-left corner of the taskbar, and then click **Start** to return to the Start screen.

3. On the Start screen, right-click the display, click **All apps**, and then click **Command Prompt**.

4. At the command prompt, type **ipconfig /all**, and then press Enter. This displays the configuration for all network connections on the computer.

5. Close the command prompt.

Reconfigure the IPv4 configuration

1. Point to the bottom-left corner of the taskbar, and then click **Start** to return to the Start screen.

2. Point to the lower-right corner of the desktop, and then click **Search**.

3. In the Search box, type **Control**, and then click **Control Panel.**

4. In Control Panel, click **Network and Internet**.

5. In Network and Internet, click **View network status and tasks**.

6. In Network and Sharing Center, to the right of the Adatum.com Domain network, click **Local Area Connection**.

7. In the **Local Area Connection Status** window, click **Properties**. In this window, you can configure protocols.

8. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.

9. Click **Obtain an IP address automatically**. Notice that the **Alternate Configuration** tab becomes available when you do this.

10. Click **Obtain DNS server address automatically**.

11. Click the **Alternate Configuration** tab. Configuration information on this tab is used when no Dynamic Host Configuration Protocol (DHCP) server is available.

12. Click **OK** to save the changes.

13. In the **Local Area Connection Properties** window, click **Close**.

14. In the **Local Area Connection Status** window, click **Details**. Notice that DHCP is enabled and the IP address of the DHCP server is displayed.

15. Close all open windows.

Lesson 4
Implementing Name Resolution

Contents:

Additional Reading

Methods for Resolving Computer Names

Additional Reading: To read more about understanding DNS client settings on TechNet, go to http://go.microsoft.com/fwlink/?LinkId=154441.

Additional Reading: To read more about understanding DNS client settings on TechNet, go to http://go.microsoft.com/fwlink/?LinkId=154441.

Lesson 5
Troubleshooting Network Connectivity

Contents:

Question and Answers

Troubleshooting Common Network Issues

Question: How is the ping command useful for troubleshooting?

Answer: You can use the **ping** command to verify connectivity between hosts. Though the ping command can verify connectivity between hosts, be aware that firewalls can block ping packets but still allow the packets for other applications. If you obtain a response to a ping attempt, the host is definitely running. However, if you do not obtain a response to a ping attempt, the host may still be functional.

Additional Reading

Tools for Troubleshooting Network Issues

Additional Reading: To read more about network troubleshooting tools, go to http://go.microsoft.com/fwlink/?LinkId=154452.

Additional Reading: For more information, go to Microsoft Support at http://go.microsoft.com/fwlink/?LinkId=154452.

Demonstration

Demonstration: Troubleshooting Common Network Issues

Demonstration Steps

Verify the current network connection settings

- If necessary, sign in to the LON-CL1 virtual machine as **Adatum\Administrator** with the password **Pa$$w0rd**.

Use IPConfig to troubleshoot the network connections

1. If necessary, point to the lower-left corner of the taskbar, and then click **Start**.

2. On the Start screen, right-click the display, click **All apps**, and then click **Command Prompt**.

3. At the command prompt, type **ipconfig /all**, and then press Enter. This displays the configuration for all network connections on the computer.

4. At the command prompt, type **ipconfig /displaydns**, and then press Enter. This displays the contents of the DNS cache.

5. At the command prompt, type **ipconfig /flushdns**, and then press Enter. This clears the contents of the DNS cache.

Use Ping to troubleshoot the network connections

1. At the command prompt, type **ping 127.0.0.1**, and then press Enter. This pings the local host.

2. At the command prompt, type **ping 172.16.0.10**, and then press Enter. This verifies connectivity to LON-DC1 by using an IPv4 address.

3. At the command prompt, type **ping LON-DC1**, and then press Enter. This verifies connectivity to LON-DC1 by using a host name.

Use Nslookup to troubleshoot name resolution

1. At the command prompt, type **nslookup –d1 LON-DC1**, and then press Enter. This provides detailed information about the host name resolution. You can use the **–d2** option for even more detail.

2. Close the command prompt.

Module Review and Takeaways

Review Question(s)

Question: After starting her computer, Amy notices that she is unable to access her normal resources. What tool can she use to determine if she has a valid IP address?

Answer: Amy can run IPConfig /All or Ping her domain controller's IP Address.

Question: When transmitting Accounts Receivable updates to the billing partner in China, Amy notices that the files are being transmitted slowly. What tool can she use to determine the network path and latency of the network?

Answer: Amy can use Windows Diagnostics to identify the problem or use Pathping.exe to check for latency.

Question: Amy notices that she cannot access normal enterprise websites. She knows that she has a valid IP address but wants to troubleshoot the DNS access of her computer. What tool must she use?

Answer: Amy can use Nslookup.exe to troubleshoot DNS access issues.

Question: What is the IPv6 equivalent of an IPv4 APIPA address?

Answer: The IPv6 equivalent of IPv4 APIPA addresses are IPv6 link-local addresses.

Question: You are troubleshooting a network-related problem, and you suspect a name resolution issue. Before conducting tests, you want to purge the DNS resolver cache. How do you do that?

Answer: Use IPCongfig /flushdns to clear the DNS Resolver Cache.

Question: You are troubleshooting a network-related problem. The IP address of the host you are troubleshooting is 169.254.16.17. What is a possible cause of the problem?

Answer: The DHCP server is unavailable.

Tools

You can use the following tools to troubleshoot network connectivity issues.

Tool	Description
Network and Sharing Center	The Network and Sharing Center informs you about your network and verifies whether your PC can successfully access the Internet. Then, it summarizes this info in the form of a Network Map.
Netsh.exe	A command that you can use to configure network properties from the command-line.
Pathping.exe	A command-line tool that combines the functionality of Ping and Tracert, and that you can use to troubleshoot network latency and provide information about path data.
Nslookup.exe	A command-line tool that you can use to test and troubleshoot DNS and name resolution issues.
IPConfig.exe	A general IP configuration and troubleshooting tool.
Ping.exe	A basic command-line tool that you can use for verifying IP connectivity.
Tracert.exe	Similar to Pathping, which provides information about network routes.

Tool	Description
Windows PowerShell	Cmdlets available to view and configure network settings.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Windows 8 host cannot connect to a Microsoft SharePoint® 2010 site.	Use Windows Diagnostics to Identify the problem.
Windows 8 host cannot access the database server.	Use IPConfig tool to view, renew or release an IP Address.
Windows 8 Host cannot connect to the Internet.	Use **Ping** to test the connectivity to the DNS Server.
DNS server is not resolving FQDNS correctly.	Use the flushdns option with **IPConfig**.

Lab Review Questions and Answers

Lab A: Configuring a Network Connection

Question: How are APIPA addresses for IPv4 similar to link-local addresses in IPv6?

Answer: Both APIPA addresses are designed to allow computers to communicate on the local network automatically without the use of a DHCP server or any other IP address configuration. However, an APIPA address is only used when a DHCPv4 server is unavailable. An IPv6 link-local address is always generated for a host using IPv6. Additional IPv6 addresses can still be obtained for communication outside the local network.

Question: How can you update a Windows 8 computer to use the correct information after a host record is updated in DNS, but the Windows 8 computer is still resolving the name to the previous IP address?

Answer: When a computer resolves a name to an IP address by using DNS, the name and IP address are cached locally. You can clear this cache at a command prompt with the command ipconfig /flushdns.

Lab B: Troubleshooting Network Connectivity

Question: In the lab, what were the two problems that you encountered on the user's computer?

Answer: The first problem was the IPv4 configuration; specifically, the subnet mask was incorrect. The second problem was the DNS configuration on the client was referencing an incorrect DNS server address, preventing name resolution.

Question: How did you resolve these two problems?

Answer: Answers may vary, but students should have manually reconfigured the subnet mask and DNS server address.

Module 5

Implementing Wireless Network Connections

Contents:

Lesson 1
Overview of Wireless Networks

Contents:

Additional Reading

Security Protocols for a Wireless Network

Additional Reading: For more information on WEP and its disadvantages, refer to:
http://go.microsoft.com/fwlink/?LinkID=154212.

Lesson 2
Implementing a Wireless Network

Contents:

Question and Answers

Improving Wireless Signal Strength

Question: What devices can interfere with a wireless network signal?

Answer: The IEEE 802.11b and the IEEE 802.11g standard use the S-Band Industrial, Scientific, and Medical (ISM) frequency range, which ranges from 2.4 to 2.5 GHz. Many devices also use this frequency range, including microwave ovens, cordless phones, baby monitors, wireless video cameras, and Bluetooth adapters, and all of these devices can cause interference to the wireless network signal.

The IEEE 802.11a uses the C-Band ISM, which ranges from 5.725 to 5.875 GHz. Therefore, fewer devices will cause interference with a wireless network that is using this standard.

Additional Reading

Configuring Hardware for Connecting to a Wireless Network

Additional Reading: For more information on how to use netsh, refer to:
http://go.microsoft.com/fwlink/?LinkID=154213
For more information on how to use Group Policy to manage wireless network, refer to:
http://go.microsoft.com/fwlink/?LinkID=154214

Module Review and Takeaways

Real-world Issues and Scenarios

1. You are implementing wireless networking in your organization. Which wireless network technology standards and which type of security (authentication and encryption) will you choose?
    Answer: There are two main considerations that you need to take into account when choosing a wireless network technology standard: speed and cost. If possible, choose the latest standard, which is 802.11n, because it gives you the best signal strength and the highest maximum speed.
    However, devices that support this standard tend to be more expensive than the ones that support 802.11g.
    Answer: Always choose the highest level of security available. In this case, WPA2 enables secure authentication and encryption. Select the Enterprise mode for WPA2 because it offers centralized management of authentication with RADIUS servers.

2. Your organization already has a wireless network in place. Your users are complaining that the performance of the wireless network is not as good as the wired network. What can you do to increase the performance of the wireless network?
    Answer: There are three aspects that you should consider: proximity, obstruction, and interference. Based on these areas, you can implement one or more solutions, such as adding WAPs or removing obstruction and interference. Refer to the "Improving the Wireless Signal Strength" topic for more information.

Tools

Tool	Use to	Where to find it
Network and Sharing Center	Configure network settings	Control Panel System Tray
Connect to a Network	Configure Windows 8-based client to connect to a wireless network	Network and Sharing Center System Tray
Netsh	Configure local or remote network settings	Command Prompt
Windows Network Diagnostics	Troubleshoot access to wireless networks	Network and Sharing Center System Tray

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Proximity or physical obstruction	Ensure that your client computer is as close as possible to the WAP. If you are unable to get closer to the WAP, consider installing an external antenna to your wireless network adapter. Check for physical objects that may cause interference, such as a thick wall or metal cabinet, and consider removing the physical objects, or repositioning the WAP or the client. Add WAPs to the wireless network, whenever applicable.

Common Issue	Troubleshooting Tip
Interference from other signals	Check for devices that may cause interference, such as cordless phones, Bluetooth devices or any other wireless devices. Turn them off or move them farther away. Consider changing the WAP settings to use a different wireless channel, or set the channel to be selected automatically if it is set to a fixed channel number.
Cannot detect wireless network	Check that your wireless network adapter has the correct driver and its working properly. Check your computer for an external switch for the wireless network adapter. Check that the WAP is turned on and working properly. Check whether the WAP is configured to advertise its SSID.
Windows is not configured to connect to the right type of network	Check the information that came with the router or access point to determine to what connection mode the device is set. The mode must be either ad hoc (when devices communicate directly without going through a router or access point) or infrastructure (when devices communicate by going through a router or access point). Make sure the setting in Windows for this network matches the setting on the device.
The router or WAP is busy	If you have other computers that are connecting to the network, try disconnecting them temporarily.
The wireless network adapter is in monitor mode	If a network monitoring program is running on your computer, the wireless network adapter will be set to monitor mode, which prevents Windows from connecting to wireless networks. To connect to a wireless network, close the network monitoring program or follow the instructions in the program to exit monitor mode.

Lab Review Questions and Answers

Lab: Planning the Implementation of Wireless Network Connections

Question: In the lab, you were tasked with making the wireless network as secure as possible. Is this appropriate in situations where you want to make the wireless network accessible to anyone, for example, in a coffee shop? How will you go about configuring the wireless infrastructure to support access in this way?

Answer: No. If you use the settings from the lab results, that would make a network inaccessible to anyone other than users and computers that you specifically authorize. . To make the network accessible for anyone, enable broadcast of the SSID to make the network more visible. Additionally, configure the network for open security, which means that no certificate, shared key, or other authentication mechanism is required to connect.

Question: Is it advisable to connect this less-restricted wireless network to your corporate network?

Answer: No. We do not recommend this. You have little control over who connects to your network, or the status of these users' computers, so enabling unrestricted access to the corporate network can introduce significant security risks.

Question: Can you think of a way in which legitimate users from your organization can connect wirelessly to your infrastructure from the same coffee shop area, while not providing the same access to anonymous users?

Answer: Provide two wireless access points, and then configure your users' computers with a Group

Policy Object (GPO) that ensures that they can connect only to the defined wireless networks. These networks require the high-level authentication settings discussed in the lab. Conversely, anonymous users will see only the open network. However, you must be careful that you avoid interference between the two networks.

Module 6

Implementing Network Security

Contents:

Lesson 2
Configuring Windows Firewall

Contents:

Demonstration

Demonstration: Configuring Inbound and Outbound Rules

Demonstration Steps

Test remote desktop connectivity

1. Sign in to the LON-CL2 virtual machine as **Adatum\Administrator** with the password **Pa$$w0rd**.

2. On the Start screen, type **r**. In the Apps search screen, click **Remote Desktop Connection**.

3. In the computer field, type **LON-CL1**, and then press Enter.

4. Sign in to **LON-CL1** as **Adatum\Administrator** with the course password.

5. Open the Start screen on **LON-CL1**, click **Administrator**, and then click **Sign out**.

Configure an Inbound Rule

1. Sign in to the **LON-CL1** virtual machine as **Adatum\Administrator** with the password **Pa$$w0rd**.

2. On the Start screen click the **Desktop** tile.

3. Open the **Settings** charm, and then click **Control Panel**.

4. Click **System and Security**, and then click **Windows Firewall**.

5. In the left pane, click **Advanced settings**.

6. Click **Inbound Rules**.

7. Click **Remote Desktop – User Mode (TCP-In)** and then click **Disable Rule** in the Actions pane.

8. Click **Remote Desktop – User Mode (UDP-In)** and then click **Disable Rule** in the Actions pane.

9. Minimize the **Windows Firewall with Advanced Security** window.

Test the inbound rule

1. Switch to **LON-CL2**.

2. Open the Start screen, type **r**. In the Apps search screen, click **Remote Desktop Connection**.

3. In the computer field, type **LON-CL1**, and then press Enter.

4. Sign in to **LON-CL1** as **Adatum\Administrator** with the course password.

5. Verify that the connection attempt fails.

Test outbound remote desktop connectivity

1. Switch to LON-DC1.

2. On the Start screen, click **Control Panel**.

3. Click **System and Security**, and then click **Allow an app through Windows Firewall**.

4. Select the **Remote Desktop** check box, select the **Domain** check box, and click **OK**.

5. Close the open windows.

6. Switch to **LON-CL1**.

7. On the Start screen, type **r**. In the Apps search screen, click **Remote Desktop Connection**.

8. In the computer field, type **LON-DC1**, and then press Enter.

9. Sign in to **LON-DC1** as **Adatum\Administrator** with the password **Pa$$w0rd**.

10. Open the Start screen on **LON-DC1**, click **Administrator**, and then click **Sign out**.

Configure an outbound rule

1. On LON-CL1, on the taskbar, click the **Windows Firewall with Advanced Security** window.

2. Click **Outbound Rules**.

3. In the **Actions** pane, click **New Rule**.

4. On the **Rule Type** page, verify that you are creating a **Program** rule, and then click **Next**.

5. On the **Program** page, browse and select **C:\Windows\System32\mstsc.exe,** click **Open**, and then click **Next.**

6. On the **Action** page, verify the action is **Block the Connection**, and then click **Next**.

7. On the **Profile** page, verify that all profiles are selected, and then click **Next**.

8. On the **Name** page, type **Block Outbound RDP to LON-DC1** in the **Name** field, and then click **Finish.**

9. In the **Windows Advanced Firewall with Advanced Security** window, click the **Block Outbound RDP to LON-DC1** rule, and then in the Actions pane, click **Properties**.

10. Click the **Scope** tab, and then under the **Remote IP address** heading, select the **These IP addresses** option.

11. Under the **Remote IP address** heading, click the **Add** button, and then in the **This IP address or subnet** field, type **172.16.0.10**. Click **OK**.

12. On the **Block Outbound RDP to LON-DC1 Properties**, click **OK**.

Test outbound remote desktop connectivity

1. Open the Start screen, and then type **r**. In the Apps search screen, click **Remote Desktop Connection**.

2. In the computer field, type **LON-DC1**, and then press Enter.

3. In the Remote Desktop Connection dialog box, click **OK**.

4. In the computer field, type **LON-CL2**, and then press Enter.

5. Click **Cancel**, and then close all open windows.

Lesson 3
Securing Network Traffic

Contents:

Additional Reading

Tools for Configuring IPsec

🌐   **Additional Reading:** For a comparison of Netsh and Windows PowerShell®, refer the students to the following site: http://go.microsoft.com/fwlink/?LinkId=266559.

Demonstration

Demonstration: Configuring an IPsec Rule

Demonstration Steps

Create a connection rule

1. In the Host system, click the **20687B-LON-CL1** window.

2. Open the **Settings** charm, and then click **Control Panel**.

3. Click **System and Security**, and then click **Windows Firewall**.

4. In the left pane, click **Advanced settings**.

5. Click **Connection Security Rules**.

6. In the **Actions** pane, click **New Rule**.

7. On the **Rule Type** page, verify **Isolation** is selected, and then click **Next**.

8. On the **Requirements** page, select **Require authentication for inbound and request authentication for outbound connections**, and then click **Next**.

9. On the **Authentication Method** page, select **Computer and user (Kerberos V5)**, and then click **Next**.

10. On the **Profile** page, click **Next**.

11. On the **Name** page, in the **Name** text box, type **Authenticate all inbound connections**, and then click **Finish**.

12. Close the **Windows Firewall with Advanced Security** window.

Test connectivity between LON-CL2 and LON-CL1

1. In the host system, click the **20687B-LON-CL2** window.

2. At the command prompt, type **ping LON-CL1**, and then press Enter.

3. Verify that the ping generated four **Request timed out** messages.

4. Close the Command Prompt.

Create a connection rule by using Windows PowerShell

1. Open the Start screen, and then type **p**.

2. Right-click **Windows PowerShell**, and then click **Run as Administrator**.

3. In the **Administrator: Windows PowerShell** window type:

```
New-NetIPsecRule –DisplayName "Authenticate all inbound connections" –InboundSecurity Require –
OutboundSecurity Request -Phase1AuthSet ComputerKerberos -Phase2AuthSet UserKerberos
```

4. Press Enter.

Test connectivity between LON-CL2 and LON-CL1

1. In the **Administrator: Windows PowerShell** window, type **ping LON-CL1**, and then press Enter.

2. Verify that the ping generated four **Reply from 172.16.0.50: bytes=32 time=*x*ms TTL=128** messages (your times may vary).

3. Open the **Settings** charm, and then click **Control Panel**.

4. Click **System and Security** and then click **Windows Firewall**.

5. In the left pane, click **Advanced settings**.

6. In the left pane, expand **Monitoring**, and then expand **Security Associations**.

7. Click **Main Mode**, and examine the information in the center pane.

8. Click **Quick Mode**, and examine the information in the center pane.

9. Close all open windows.

Examine the security associations on LON-CL1 by using Windows PowerShell

1. In the Host system, click the **20687B-LON-CL1** window.

2. Open the Start screen, and then type **p**.

3. Right click **Windows PowerShell**, and then click **Run as Administrator**.

4. To examine the Main Mode Security Associations, run the following cmdlet:

```
Get-NetIPsecMainModeSA
```

5. To examine the Quick Mode Security Associations, run the following cmdlet:

```
Get-NetIPsecQuickModeSA
```

Lesson 4
Configuring Windows Defender

Contents:

Demonstration

Demonstration: Configuring Windows Defender Settings

Demonstration Steps

Perform a quick scan

1. In the Host system, click the **20687B-LON-CL1** window.

2. Open the **Settings** charm, and then on the Desktop menu, click **Control Panel**.

3. Click **View by:** select **Large Icons**, and then click **Windows Defender**.

4. On the Windows Defender **Home** tab, ensure the **Quick** scan option is selected.

5. Click **Scan now**.

6. Review the results.

Test malware detection

1. Open Windows Explorer, and then browse to E:\Labfiles\Mod06\Malware

2. In the **Malware** folder, open sample.txt in Notepad. The sample.txt file contains a text string used to test malware detection.

3. In the sample.txt file, delete both instances of <remove> (including the brackets).

4. Save and close the file. Immediately, Windows Defender detects a potential threat.

5. Shortly thereafter, the sample.txt will be removed from the Malware folder (quarantined).

Examine the Windows Defender history

1. Open the **Settings** charm, and then on the **Desktop** menu, click **Control Panel**.

2. Click **Windows Defender**.

3. In Windows Defender click the **History** tab.

4. Click the **View details** button.

5. Review the results.

6. Select the check box for the **Virus:DOS/EICAR_Test_File**, and then click **Remove**.

7. Close all open windows.

Module Review and Takeaways

Best Practices

Configuration Guidelines for Windows Firewall with Advanced Security

You can configure Windows Firewall with Advanced Security in the following ways:

- Configure a local or remote computer by using either the Windows Firewall with Advanced Security snap-in or the cmdlets in the **PowerShell NetSecurity** module.
- Configure Windows Firewall with Advanced Security settings by using the Group Policy Management Console (GPMC) or the cmdlets in the **PowerShell NetSecurity** module.
- If you are configuring the firewall by using Group Policy, you need to ensure that the Windows Firewall service has explicit write access by its service security identifier (SID) to the location that you specify.
- If you deploy Windows Firewall with Advanced Security by using Group Policy and then block outbound connections, ensure that you enable the Group Policy outbound rules, and do full testing in a test environment before deploying. Otherwise, you might prevent all of the computers that receive the policy from updating the policy in the future, unless you intervene manually.

Implementing Defense-in-Depth

Supplement or modify 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 antivirus and antispyware software.
- Implement host-based firewalls.

Windows Defender

Supplement or modify the following best practices for your own work situations:

- When you use Windows Defender, you must have current definitions.
- To help keep your definitions current, Windows Defender automatically installs new definitions as they are released. You also can set Windows Defender to check online for updated definitions before scanning.
- When you scan your computer, we recommend that you select the advanced option to Create a restore point before applying actions to detected items. Because you can set Windows Defender to remove detected items automatically, selecting this option allows you to restore system settings in case you want to use software that you did not intend to remove.

Review Question(s)

Question: You need to ensure that traffic passing between a computer in the perimeter network and one deployed in the internal network is encrypted and authenticated. The computer in the perimeter is not a member of your AD DS forest. What authentication methods could you use if you attempted to establish an IPsec rule between these two computers?

Answer: You could not use Kerberos because the perimeter computer is not in the forest. Therefore, you could use certificates or a preshared key.

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

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

Question: You decide to deploy a third-party messaging application on your company's laptop computers. This application uses POP3 to retrieve email from the corporate mail server, and Simple Mail Transfer Protocol (SMTP) to send mail to the corporate email relay. Which ports must you open in Windows Firewall?

Answer: POP3 uses TCP port 110, and SMTP uses TCP Port 25.

Question: What does Windows Defender do to software that it quarantines?

Answer: It immediately moves the file to a quarantine area. After the scan is complete, you can choose to restore or delete quarantined files. You also can view and manage the quarantined files at any time. Finally, you can configure an option to remove quarantined items automatically after a set period of time.

Tools

Tool	Use for	Where to find it
Ping	Testing network connectivity	Command-line
Windows Firewall with Advanced Security	Managing inbound, outbound, and IPsec rules	Control Panel
Windows Defender	Anti-malware detection and removal	Control Panel

Lab Review Questions and Answers

Lab A: Configuring Inbound and Outbound Firewall Rules

Question: In your environment, where do you use workstation-based firewalls?

Answer: Answers will vary based on students' experience, but one possible answer is on workstations with sensitive financial data.

Lab B: Configuring IPsec Rules

Question: In your environment, where do you use authenticated connections between workstation computers?

Answer: Answers will vary based on students' experience, although one possible answer is when computers are on a segment that nonemployees can access.

Lab C: Configuring Host-Based Virus and Malware Protection

Question: In your environment, how often are your client computers infected with malware?

Answer: Answers will vary based on students' experience, so use this question as a discussion starter on the importance of using malware protection.

Module 7

Configuring File Access and Printers on Windows® 8 Clients

Contents:

Lesson 1
Managing File Access

Contents:

Question and Answers

Discussion: Determining Effective Permissions

Question: The Users group has Write permission, and the Sales group has Read permission for Folder1. What permissions does User1 have for Folder1?

Answer: User1 has Write and Read permissions for Folder1, because User1 is a member of the Users group, which has Write permission, and the Sales group, which has Read permission.

Question: The Users group has Read permission for Folder1. The Sales group has Write permission for Folder2. What permissions does User1 have for File2?

Answer: User1 has Read and Write permissions for File2, because User1 is a member of the Users group, which has Read permission for Folder1, and the Sales group, which has Write permission for Folder2. File2 inherits permissions from both Folder2 and Folder1.

Question: The Users group has Modify permission for Folder1. The files in Folder 2 should only be accessible to the Sales group, and they should only have read permissions to the files. What do you need to do to ensure that the members of the Sales group only have Read permission to the files in Folder 2?

Answer: Prevent permissions inheritance for Folder2. Remove the permissions for Folder2 that were inherited from Folder1. Grant only Read permission for Folder2 to the Sales group.

Demonstration

Demonstration: Configuring NTFS Permissions for Files and Folders

Demonstration Steps

Create a new folder

1. Sign in to the LON-CL1 virtual machine as **Adatum\Administrator** with the password **Pa$$w0rd**.

2. On the Start screen, click the **Desktop** tile.

3. On the taskbar, click **Windows Explorer**

4. In the Windows Explorer navigation pane, click the **Allfiles (E:)** drive.

5. Double-click the **Labfiles** folder, and then double-click the **Mod07** folder.

6. In the Mod07 window, right-click, point to **New**, and then click **Folder**.

7. Name the folder **Adatum**.

Disable inherited permissions on the Adatum folder

1. With the **Adatum** folder selected, click the **Share** menu, and then in the ribbon, click **Advanced security**.

2. Click the **Disable inheritance** button.

3. In the Block Inheritance dialog box, select **Convert inherited permissions into explicit permissions on this object**.

4. Click the **Apply** button.

5. Point out the change in the **Inherited from** column. Point out the contents of the **Applies to** column.

6. Click **OK** to close the **Advanced Security Settings for Adatum** dialog box.

Create a file in the Adatum folder

1. Double-click the **Adatum** folder.

2. Click the **Home** menu, and in the ribbon, click **New item**, select **Text Document**, and then name the file **PermissionsTest.txt**.

Examine the permissions on the PermissionsTest file

1. Ensure that the PermissionsTest file selected, click the **Share** menu, and then in the ribbon, click **Advanced security**.

2. Review the permissions on the Permissions test file. Point out that there is not an Applies to column.

Grant managers modify permissions to the PermissionsTest file

1. Click the **Add** button.

2. In the **Permission Entry for PermissionsTest.txt** dialog box, click the **Select a principal** link.

3. In the **Enter the object name to select** field, type **Managers**, click **Check Names**, and then click **OK**.

4. Leave the **Type** set to **Allow**, in the **Permissions** list, select the **Modify** check box.

5. In the **Permission Entry for PermissionsTest.txt** dialog box, click **OK**.

6. Point out the Managers permission and from where it is inherited.

7. Click **OK**, and then close all open windows.

Lesson 2
Managing Shared Folders

Contents:

Question and Answers

Discussion: Combining NTFS and Share Permissions

Question: If a user is assigned Full Control NTFS permission to a file, but is accessing the file through a share with Read permission, what will be the effective permission the user will have on the file?

Answer: The user will have only Read access to the file when accessing it over the network through the share (because Read access is more restrictive than Full Control). If the user is logged on to the console of the computer that is storing the file, and accessing it locally, then the user has Full Control.

Question: If you want a user to view all files in a shared folder, but can modify only certain files in the folder, what permissions do you give the user?

Answer: The share permissions will have to allow the user to modify all files (this opens the folder window wide, but it will get locked down with NTFS permissions). You must set the NTFS permissions for the folder to allow the user Read access only (which flows to all the files). Then on the individual files in the folder that you want the user to modify, assign the Modify NTFS permission.

Question: Identify a scenario at your organization where it might be necessary to combine NTFS and Share permissions. What is the reason for combining permissions?

Answer: Answers will vary, based on the experiences of each student.

Lesson 3
Configuring File Compression

Contents:

Question and Answers

Discussion: What Is the Impact of Moving and Copying Compressed Files and Folders?

Question: What happens to the compression state of a file or folder when you copy it within an NTFS partition?

Answer: When you copy a file or folder within an NTFS partition, the file or folder inherits the compression state of the target folder. For example, if you copy a compressed file or folder to an uncompressed folder, the file or folder is uncompressed automatically.

Question: What happens to the compression state of a file or folder when you move it within an NTFS partition?

Answer: When you move a file or folder within an NTFS partition, the file or folder retains its original compression state. For example, if you move a compressed file or folder to an uncompressed folder, the file remains compressed.

Question: What happens to the compression state of a file or folder when you copy or move it between NTFS partitions?

Answer: When you move a file or folder between NTFS partitions, the file or folder inherits the target folder's compression state. Because Windows 8 treats a move between partitions as a copy followed by a delete operation, the files inherit the target folder's compression state.

When you copy a file to a folder that already contains a file of the same name, the copied file takes on the compression attribute of the target file, regardless of the compression state of the folder.

Question: What happens to the compression state of a file that you copy or move between FAT and NTFS volumes?

Answer: Compressed files that you copy to a FAT partition are uncompressed, because FAT volumes do not support compression. However, when you copy or move files from a FAT partition to an NTFS partition, they inherit the compression attribute of the folder into which you copy them. Because Windows 8 treats a move between partitions as a copy followed by a delete operation, the files inherit the compression state of the target folder. When you copy files, the NTFS file system calculates disk space based on the uncompressed file's size. This is important, because files are uncompressed during the copy process, and the system must ensure there is enough space. If you copy a compressed file to an NTFS partition that does not have enough space for the uncompressed file, an error message notifies you that there is not enough disk space.

Demonstration

Demonstration: Compressing Files and Folders

Demonstration Steps

Compress a file

1. Sign in to the LON-CL1 virtual machine as **Adatum\Administrator** with the password **Pa$$w0rd**.

2. On the Start screen, click the **Desktop** tile.

3. On the taskbar, click **Windows Explorer**.

4. In the Windows Explorer navigation pane, click the **Allfiles (E:)** drive.

5. Double-click the **Labfiles** folder, double-click the **Mod07** folder, and then double-click the **Windows8Docs** folder.

6. In Windows Explorer, click the **Size** column header until the largest file is at the top.

7. Point out the size of the largest file in the folder.

8. Right-click the file, and then select **Properties**.

9. On the **General** tab, click the **Advanced** button.

10. Select the **Compress contents to save disk space** check box.

11. In the **Advanced Attributes** dialog box, click **OK**.

12. In the file **Properties** dialog box, click **OK**.

13. Point out the color of the file.

14. Point out that the other files are not changed.

15. Point out the displayed file size.

16. Right-click the file, and then select **Properties**.

17. Point out the **Size on disk** attribute.

18. In the file **Properties** dialog box, click **OK**.

Compress a folder

1. In the Address bar, click **Mod07**.

2. Right-click the **Windows8Docs** folder, and then select **Properties**.

3. Point out the **Size** and **Size on disk** attributes.

4. On the **General** tab, click the **Advanced** button.

5. Select the **Compress contents to save disk space** check box.

6. In the **Advanced Attributes** dialog box, click **OK**.

7. In the **Windows8Docs Properties** dialog box, click **Apply**.

8. In the **Confirm Attribute Changes** dialog box, ensure that the **Apply changes to this folder, subfolders and files** option button is selected, and then click **OK**.

9. Point out the change in the **Size on disk** attribute.

10. Click **OK** to close the **Windows8Docs Properties** dialog box.

11. Point out that the Windows8Docs folder has changed colors.

12. Double-click **Windows8Docs** folder.

13. Point out that all the files are now blue.

14. Close all open windows.

Lesson 4
Managing Printers

Contents:

Demonstration

Demonstration: Installing and Sharing a Printer

Demonstration Steps

Create and share a printer

1. Sign in to the LON-CL1 virtual machine as **Adatum\Administrator** with the password **Pa$$w0rd**.

2. While on the Start screen, type the letter **c**, and then click **Control Panel** in the Apps search results.

3. In Control Panel, click the **View devices and printers** link.

4. In **Devices and Printers**, click the **Add a printer** link.

5. In the Add Printer Wizard, click **The printer that I want isn't listed**.

6. On the **Find a printer by other options** page, select the **Add a local printer or network printer with manual settings** option, and then click **Next**.

7. On the **Choose a printer port** page, select the dropdown for **Use an existing port**, select **nul: (Local Port)**, and then click **Next**.

8. On the **Install the printer driver** page, in the **Manufacturer** list, select **Microsoft**.

9. In the **Printers** list, select **Microsoft OpenXPS Class Driver**, and then click **Next**.

10. On the **Type a printer name** page, in the **Printer name** field, type **AdatumPrinter**, and then click **Next**.

11. Review the **Printer Sharing** page, and then click **Next**.

12. Review the **You've successfully added AdatumPrinter** page, and then click **Finish**.

Lesson 5
Overview of SkyDrive

Contents:

Additional Reading

What Is SkyDrive?

Additional Reading: For more information on SkyDrive features, see:
http://go.microsoft.com/fwlink/?LinkId=266561.

Module Review and Takeaways

Best Practices

NTFS Permissions

Supplement or modify the following best practices for your own work situations:

- To simplify the assignment of permissions, you can grant the Everyone group Full Control share permission to all shares and use only NTFS permissions to control access. Restrict share permissions to the minimum required, to provide an extra layer of security in case NTFS permissions are configured incorrectly.
- When permissions inheritance is blocked, you have the option to copy existing permissions, or begin with blank permissions. If you only want to restrict a particular group or user, then copy existing permissions to simplify the configuration process.

Managing Shared Folders

Supplement or modify the following best practices for your own work situations:

- If the guest user account is enabled on your computer, the Everyone group includes anyone. In practice, remove the Everyone group from any permission lists and replace it with the Authenticated Users group.
- Using a firewall other than that supplied with Windows 8 can interfere with the Network Discovery and file-sharing features.

Review Question(s)

Question: A. Datum is installing Microsoft Dynamics GP, and they have contracted with a vendor to provide some custom programming work. A. Datum asked Joseph, their senior IT desktop specialist, to configure the NTFS permissions for the GP planning files it will be accumulating. A. Datum has asked that all IT users be assigned Modify permissions to the GP Implementation Planning folder. However, A. Datum only wants the subfolder titled Vendor Contracts to be available for viewing by a select group of managers. How can Joseph accomplish this by taking into account permission inheritance?

Answer: Joseph could take a three-step approach. First, he can assign the IT user group the Modify permission for the GP Implementation Planning folder. Next, he can block inherited permissions on the Vendor Contract subfolder. Third, he can restrict access to the subfolder by providing Read access to the selected list of managers identified by A. Datum.

Question: Robin recently created a spreadsheet in which she explicitly assigned it NTFS file permissions that restricted file access to just herself. Following the system reorganization, the file moved to a folder on another NTFS partition and Robin discovered that other users were able to access the spreadsheet. What is the probable cause of this situation?

Answer: Since this was a move across partitions, NTFS permissions are inherited from the new parent, which would not have included any special permissions that Robin had configured.

Tools

Use the following command prompt tools to manage file and printer sharing.

Tool	Description
Net share	Share folders from the command prompt.
Net use	Connect to shared resources from the command prompt.

Tool	Description
Cacls.exe	Configure NTFS file and folder permissions from the command prompt.
Compact.exe	Compress NTFS files and folders from the command prompt.
Pnputil.exe	Preinstall printer drivers into the driver store.

Lab Review Questions and Answers

Lab A: Configuring File Access

Question: Why were you unable to create a file in the Adatum shared folder?

Answer: The folder was shared with the permission level of **Read** for everyone.

Question: Why was Adam able to create a file, whereas Ed was not?

Answer: Adam is in the Marketing group, and Ed is not.

Question: What other ways could you share a folder?

Answer: You could use the Folder Properties or the Advanced Security Settings dialog box.

Lab B: Configuring Printers

Question: When creating a printer, what must you specify?

Answer: You must specify the driver that it is using and the port on which it is communicating.

Module 8

Securing Windows 8 Desktops

Contents:

Lesson 1
Authentication and Authorization in Windows 8

Contents:

Question and Answers

The Process of Authentication and Authorization

Question: Which authentication method is used when a client computer that is running the Windows 8 operating system logs on to AD DS?

Answer: Windows uses the Kerberos version 5 protocol unless your enterprise is using smart cards. If your enterprise uses smart cards, Windows uses the certificate mapping method for authentication.

Lesson 2
Implementing GPOs

Contents:

Question and Answers

How Multiple Local GPOs Work

Question: An administrator selects the **Disable the Security page** setting in the Local GPO. The administrator then enables the same setting in a user-specific Local GPO. The user logging on to the computer is not an administrator. Which policy setting will be applied to this Local GPO?

Answer: Windows reads the Local GPO first, followed by the Non-Administrators Local GPO, and then the user-specific Local GPO. Windows disables the state of the policy setting when it reads the Local GPO. The policy setting is not configured in the Non-Administrators Local GPO. This has no effect on the state of the setting, so it remains enabled. The policy setting is enabled in the user-specific Local GPO. This changes the state of the setting to Enabled. Windows reads the user-specific Local GPO last. Therefore, it has the highest precedence. The Local Computer Policy has a lower precedence.

Additional Reading

🗒️ **Note:** You must download the RSAT for Windows 8 client from the Microsoft download website at http://www.microsoft.com/en-us/download/details.aspx?id=28972

Demonstration

Demonstration: How to Create Multiple Local GPOs

Demonstration Steps

Create a custom management console

1. Sign in to LON-CL1 as **Adatum\Administrator** with the password **Pa$$w0rd**.

2. At the Start screen, type **run**. In the returned **Apps** list, click **Run**.

3. In the **Open** box, type **mmc**, and then press Enter.

4. In **Console1 – [Console Root]**, click **File**, and then click **Add/Remove Snap-in**.

5. In the **Add or Remove Snap-ins** dialog box, in the **Available snap-ins** list, click **Group Policy Object Editor**, and then click **Add**.

6. In the **Select Group Policy Object** dialog box, click **Finish**.

7. In the **Add or Remove Snap-ins** dialog box, in the **Available snap-ins** list, click **Group Policy Object Editor** and then click **Add**.

8. In the **Select Group Policy Object** dialog box, click **Browse**.

9. In the **Browse for a Group Policy Object** dialog box, click the **Users** tab.

10. In the **Local Users and Groups compatible with Local Group Policy** list, click **Administrators**, and then click **OK**.

11. In the **Select Group Policy Object** dialog box, click **Finish**.

12. In the **Add or Remove Snap-ins** dialog box, in the **Available snap-ins** list, click **Group Policy Object Editor**, and then click **Add**.

13. In the **Select Group Policy Object** dialog box, click **Browse**.

14. In the **Browse for a Group Policy Object** dialog box, click the **Users** tab.

15. In the **Local Users and Groups compatible with Local Group Policy** list, click **Non-Administrators**, and then click **OK**.

16. In the **Select Group Policy Object** dialog box, click **Finish**.

17. In the **Add or Remove Snap-ins** dialog box, click **OK**.

18. In **Console1 – [Console Root]**, on the menu, click **File** and then click **Save**.

19. In the **Save As** dialog box, click **Desktop**.

20. In the **File name** box, type **Multiple Local Group Policy Editor**, and then click **Save**.

Modify the local policy settings

1. In **Multiple Local Group Policy Editor – [Console Root]**, in the tree, expand **Local Computer Policy**.

2. Expand **User Configuration**, expand **Windows Settings**, and then click **Scripts (Logon/Logoff)**.

3. In the results pane, double-click **Logon**.

4. In the **Logon Properties** dialog box, click **Add**.

5. In the **Add a Script** dialog box, click **Browse**.

6. In the **Browse** dialog box, right-click in the empty folder, point to **New**, click **Text Document**, and then press Enter.

7. Right-click **New Text Document**, and then click **Edit**.

8. Type **msgbox "Default Computer Policy"**, click **File**, and then click **Save As**.

9. Type **ComputerScript.vbs**, change Save as type: to **All Files**, and then click **Save**.

10. Close ComputerScript.vbs.

11. In the **Browse** dialog box, click the **ComputerScript.vbs** file, and then click **Open**.

12. In the **Add a Script** dialog box, click **OK**.

13. In the **Logon Properties** dialog box, click **OK**.

14. In **Multiple Local Group Policy Editor – [Console Root]**, in the tree, expand **Local Computer\Administrators Policy**.

15. Expand **User Configuration**, expand **Windows Settings**, and then click **Scripts (Logon/Logoff)**.

16. In the results pane, double-click **Logon**.

17. In the **Logon Properties** dialog box, click **Add**.

18. In the **Add a Script** dialog box, click **Browse**.

19. In the **Browse** dialog box, right-click in the empty folder, click **New**, click **Text Document**, and then press Enter.

20. Right-click **New Text Document**, and then click **Edit**.

21. Type **msgbox "Default Administrator's Policy"**, click **File**, and then click **Save As**.

22. Type **AdminScript.vbs**, change **Save as type:** to **All Files**, and then click **Save**.

23. Close AdminScript.vbs.

24. In the **Browse** dialog box, click the **AdminScript** file, and then click **Open**.

25. In the **Add a Script** dialog box, click **OK**.

26. In the **Logon Properties** dialog box, click **OK**.

27. In **Multiple Local Group Policy Editor – [Console Root]**, in the tree, expand **Local Computer\Non-Administrators Policy**.

28. Expand **User Configuration**, expand **Windows Settings**, and then click **Scripts (Logon/Logoff)**.

29. In the results pane, double-click **Logon**.

30. In the **Logon Properties** dialog box, click **Add**.

31. In the **Add a Script** dialog box, click **Browse**.

32. In the **Browse** dialog box, right-click in the empty folder, click **New**, click **Text Document**, and then press Enter.

33. Right-click **New Text Document** and then click **Edit**.

34. Type **msgbox "Default User's Policy"**, click **File**, and then click **Save As**.

35. Type **UserScript.vbs**, change **Save as type:** to **All Files**, and then click **Save**.

36. Close UserScript.vbs.

37. In the **Browse** dialog box, click the **UserScript** file, and then click **Open**.

38. In the **Add a Script** dialog box, click **OK**.

39. In the **Logon Properties** dialog box, click **OK**.

Test multiple local Group Policies

1. Sign out LON-CL1. To sign out, on your host computer, in the **20687B-LON-CL1 on localhost – Virtual Machine Connection** window, click the **Action** menu, click **Ctrl+Alt+Delete**, and then click **Sign out**.

2. Sign in to LON-CL1 as **Adatum\Holly** with the password **Pa$$w0rd**. To sign in as a different user, on the logon screen, click **Other user**, enter the required credentials, and then press Enter.

3. In the Start screen, click the **Desktop** tile.

4. Click **OK** when prompted by the message box, and then click **OK** again.

5. Sign out.

6. Sign in to LON-CL1 as **Adatum\Administrator** with the password **Pa$$w0rd**.

7. In the Start screen, click **Desktop**.

8. Click **OK** when prompted by the message box, and then click **OK** again.

9. On the desktop, right-click **Multiple Local Group Policy Editor**, and then click **Open**.

10. In **Multiple Local Group Policy Editor – [Console Root]**, in the tree, expand **Local Computer\Non-Administrators Policy**.

11. Expand **User Configuration**, expand **Windows Settings**, and then click **Scripts (Logon/Logoff)**.

12. In the results pane, double-click **Logon**.

13. In the **Logon Properties** dialog box, click **Remove**, and then click **OK**.

14. In **Multiple Local Group Policy Editor – [Console Root]**, in the tree, expand **Local Computer\Administrators Policy**.

15. Expand **User Configuration**, expand **Windows Settings**, and then click **Scripts (Logon/Logoff)**.

16. In the results pane, double-click **Logon**.

17. In the **Logon Properties** dialog box, click **Remove**, and then click **OK**.

18. In **Multiple Local Group Policy Editor – [Console Root]**, in the tree, expand **Local Computer Policy**.

19. Expand **User Configuration**, expand **Windows Settings**, and then click **Scripts (Logon/Logoff)**.

20. In the results pane, double-click **Logon**.

21. In the **Logon Properties** dialog box, click **Remove**, and then click **OK**.

22. Close the Multiple Local Group Policy Editor – [Console Root] snap-in.

23. Click **Yes** if prompted to save.

24. Sign out.

Demonstration: How to Configure Local Security Policy Settings

Demonstration Steps

1. Sign in to LON-CL1 as **Adatum\Administrator** with the password **Pa$$w0rd**.

2. On the Start screen, right-click the display, and then click **All apps**.

3. In the **Apps** list, click **Run**.

4. In the **Open** box, type **gpedit.msc**, and press Enter.

5. In the Local Group Policy Editor, expand **Computer Configuration**, expand **Windows Settings**, and then expand **Security Settings**.

6. Expand **Account Policies**, and then click **Password Policy**.

7. Click **Account Lockout Policy**.

8. In the left pane, click and expand **Local Policies**, and then click **Audit Policy**.

9. In the main window, right-click **Audit account management**, and then select **Properties**.

10. In the **Audit account management Properties** dialog box, select **Success** and **Failure**, and then click **OK**.

11. Click **User Rights Assignments**.

12. Click **Security Options**.

13. In the left pane, click and expand **Windows Firewall with Advanced Security**, and then click **Windows Firewall with Advanced Security – Local Group Policy Object**.

14. In the left pane, click **Network List Manager Policies**.

15. In the left pane, click and expand **Public Key Policies**, and then click **Encrypting File System**.

16. Click **BitLocker Drive Encryption**.

17. In the left pane, click **Software Restriction Policies.**

18. In the left pane, click and expand **Application Control Policies**.

19. Click and expand **AppLocker**.

20. In the left pane, click **IP Security Policies on Local Computer**.

21. In the left pane, click and expand **Advanced Audit Policy Configuration**.

22. Click and expand **System Audit Policies – Local Group Policy Object**.

23. Close the Local Group Policy Editor.

24. Sign out LON-CL1.

Lesson 3
Securing Data with EFS and BitLocker

Contents:

Question and Answers

What Is EFS?

Question: Why is it not possible to encrypt system files with EFS?

Answer: EFS keys are not available during the startup process. Therefore, if system files are encrypted, the system file cannot start.

What Is BitLocker?

Question: BitLocker provides full volume encryption. What does this mean?

Answer: Full volume encryption means:

1. You can encrypt the entire Windows operating system volume can be encrypted.

2. You can encrypt fixed -data volumes, with the requirement that the operating system volume also is encrypted.

BitLocker Modes

Question: What is a disadvantage of running BitLocker on a computer that does not contain TPM 1.2?

Answer: Computers without TPMs will not be able to use the system integrity verification during boot-up that BitLocker can also provide.

Configuring BitLocker

Question: When turning on BitLocker on a computer with TPM 1.2, what is the purpose of saving the recovery password?

Answer: If the TPM ever changes or cannot be accessed, if there are changes to key system files, or if someone tries to start the computer from a product CD or DVD to circumvent the operating system, the computer will switch to recovery mode and will remain there until the user provides the recovery password. Storing the recovery password so that it is accessible to the user allows him or her to complete the startup process.

Configuring BitLocker To Go

Question: How do you enable BitLocker To Go for a USB flash drive?

Answer: Insert the drive, and in **Windows Explorer**, right-click the drive, and then click **Turn On BitLocker**.

Recovering BitLocker-Encrypted Drives

Question: What is the difference between the recovery password and the password ID?

Answer: The recovery password is a 48-digit password that unlocks a system in recovery mode. The recovery password is unique to a particular BitLocker encryption, and you can store it in AD DS. A computer's password ID is a 32-character password unique to a Computer Name. Find the password ID under a Computer's properties, which you can use to locate recovery passwords stored in AD DS.

Demonstration

Demonstration: How to Encrypt Files and Folders with EFS

Demonstration Steps

Create a new Microsoft Office Word document

1. Sign in to LON-CL1 as **Adatum\Administrator** with the password **Pa$$w0rd**.

2. On the Start screen, click **Desktop**, and on the Taskbar, click **Windows Explorer**.

3. In the navigation pane, click **Computer**, and then in the results pane, double-click **Local Disk (C:)**.

4. Right-click an empty space in the Name column, point to **New**, and then click **Folder**.

5. Type **Encrypted** in the folder name, and then press Enter.

6. Double-click **Encrypted**, and then right-click an empty space in the Name column, point to **New**, and then click **Microsoft Word Document**.

7. Type **Private**, and then press Enter.

8. Click the left arrow in the menu bar to return to Local Disk (C:).

Encrypt the folder

1. Right-click the **Encrypted** folder, and then click **Properties**.

2. On the **General** tab, click **Advanced**.

3. Select the **Encrypt contents to secure data** check box, and then click **OK**.

4. In the **Encrypted Properties** dialog box, click **OK**, and then in the **Confirm Attribute Changes** dialog box, click **Apply changes to this folder, subfolders and files**.

5. Click **OK**.

6. Sign out.

Sign in as Holly, and attempt to access the file

1. Sign in to LON-CL1 as **Adatum\Holly** with the password **Pa$$w0rd**.

2. On the Start screen, click **Desktop**, and on the Taskbar, click **Windows Explorer**.

3. In the navigation pane, click **Computer**, and then in the results pane, double-click **Local Disk (C:)**.

4. Double-click the **Encrypted** folder.

5. Double-click **Private**.

6. Click **OK** to close the **User Name** box.

7. Click **OK** at the Help Protect and Improve Microsoft Office dialog box.

8. Close Microsoft Word.

9. Sign out.

Sign in again as administrator, and decrypt the folder

1. Sign in to LON-CL1 as **Adatum\Administrator** with the password **Pa$$w0rd**.

2. On the Start screen, click **Desktop**, and on the Taskbar, click **Windows Explorer**.

3. In the navigation pane, click **Computer**, and then in the results pane, double-click **Local Disk (C:)**.

4. Right-click the **Encrypted** folder, and then click **Properties**.

5. On the **General** tab, click **Advanced**.

6. Clear the **Encrypt contents to secure data** check box, and then click **OK**.

7. Click **OK** to close the **Encrypted Properties** dialog box.

8. In the **Confirm Attribute Changes** dialog box, click **OK**.

9. Sign out.

Sign in as Holly, and attempt to access the file again

1. Sign in to LON-CL1 as **Adatum\Holly** with the password **Pa$$w0rd**.

2. On the Start screen, click **Desktop**, and on the Taskbar, click **Windows Explorer**.

3. In the navigation pane, click **Computer**, and then in the results pane, double-click **Local Disk (C:)**.

4. Double-click the **Encrypted** folder.

5. Double-click **Private**.

6. Type **Decrypted** in the file.

7. Press Ctrl+S, and then close Word.

8. Sign out.

Lesson 4
Configuring User Account Control

Contents:

Question and Answers

How UAC Works

Question: What are the differences between a consent prompt and a credential prompt?

Answer: A consent prompt displays to administrators in Admin Approval Mode when a user attempts to perform an administrative task. It requests approval from the user to continue with the task being performed. A credential prompt is displayed to standard users when they attempt to perform an administrative task.

Configuring UAC Notification Settings

Question: Which two configuration options are combined to produce the end-user elevation experience?

Answer: UAC security settings configured in Local Security Policy and User Account Control settings configured in the Action Center in Control Panel.

How to Configure UAC with GPOs

Question: Which UAC feature detects when an application is being installed in Windows 8?

Answer: User Account Control: Detect application installations and prompt for elevation.

Demonstration

Demonstration: How to Configure UAC with GPOs

Demonstration Steps

View the current UAC settings

1. Sign in to LON-CL1 as **Adatum\Administrator** with a password of **Pa$$w0rd**.

2. Right-click the display, and then click **All apps**.

3. In the **Apps** list, click **Run**.

4. In the **Open** box, type **gpedit.msc**, and press Enter.

5. In the Local Group Policy Editor, expand **Computer Configuration**, expand **Windows Settings**, and then expand **Security Settings**, expand **Local Policies**, and then click **Security Options**.

Configure UAC settings

1. In the results pane, double-click **User Account Control: Behavior of the elevation prompt for standard users**.

2. In the **User Account Control: Behavior of the elevation prompt for standard users** dialog box, click **Automatically deny elevation requests**, and then click **OK**.

3. Close Local Group Policy Editor console.

4. Sign out.

Test the UAC settings

1. Sign in to LON-CL1 as **Adatum\Holly** with the password **Pa$$w0rd**.

2. Right-click the display, and then click **All apps**.

3. In the **Apps** list, right-click **Computer**, and then click **Manage**. Windows does not display the Computer Management snap-in.

4. Sign out.

Reconfigure UAC settings

1. Sign in to LON-CL1 as **Adatum\Administrator** with the password **Pa$$w0rd**.

2. Right-click the desktop, and then click **All apps**.

3. In the **Apps** list, click **Run**.

4. In the **Open** box, type **gpedit.msc**, and then press Enter.

5. In the Local Group Policy Editor, expand **Computer Configuration**, expand **Windows Settings**, expand **Security Settings**, expand **Local Policies**, and then click **Security Options**.

6. In the results pane, double-click **User Account Control: Behavior of the elevation prompt for standard users**.

7. In the **User Account Control: Behavior of the elevation prompt for standard users** dialog box, click **Prompt for credentials**, and then click **OK**.

8. Close Local Group Policy Editor console.

9. Sign out.

Test these settings

1. Sign in to LON-CL1 as **Adatum\Holly** with the password **Pa$$w0rd**.

2. Right-click the Start screen, and then click **All apps**.

3. In the **Apps** list, right-click **Computer**, and then select **Manage**. Windows displays the User Account Control prompt.

4. Type **Administrator** in the **User name** field.

5. Type **Pa$$w0rd** in the **Password** field, and then click **Yes**.

6. Close the Computer Management console.

7. Sign out.

Module Review and Takeaways

Best Practices

Best Practices for EFS Users

- Users should export their certificates and private keys to removable media, and then 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 you must access the encrypted files, you can import the private key easily 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 by default.
- Users should encrypt folders rather than individual files. Programs work on files in various ways. Encrypting files consistently at the folder level ensures that files are not decrypted unexpectedly.
- The private keys that are associated with recovery certificates are extremely sensitive. You must generate these keys either on a computer that you secure is physically secured, or you must export their certificates to a .pfx file, protect them with a strong password, and save them on a disk that is stored in a physically secure location.
- You must assign recovery agent certificates to user accounts that you do not use for any other purpose.
- Do not destroy recovery certificates or private keys when recovery agents are changed. (Agents are changed periodically). Keep them all, until all files that may have been encrypted with them are updated.
- Designate two or more recovery agent accounts per OU, depending on the size of the OU. Designate two or more computers for recovery, one for each designated recovery agent account. Grant permissions to appropriate administrators to use the recovery agent accounts. It is a good idea to have two recovery agent accounts to provide redundancy for file recovery. Having two computers that hold these keys provides more redundancy to allow recovery of lost data.
- Implement a recovery agent archive program to ensure that you can recover encrypted files by using obsolete recovery keys. Recovery certificates and private keys must be exported and stored in a controlled and secure manner. Ideally, as with all secure data, archives must be stored in a controlled access vault, and you must have two archives: a master and a backup. The master is kept on site, while the backup is located in a secure, off-site location.
- Avoid using print spool files in your print server architecture, or make sure that print spool files are generated in an encrypted folder.
- The Encrypting File System does take some CPU overhead every time a user encrypts and decrypts a file. Plan your server usage wisely. Load balance your servers when there are many clients that are using EFS.

Best Practices for User Account Control

- 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. There are nine GPO settings that you can configure for UAC.
- 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 may 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.

- Although UAC enables you to be signed in using an administrative user account to perform everyday user tasks, it is still good practice to sign in using a standard user account for these everyday tasks, signing in as an administrator only when necessary.

Best Practices for Windows BitLocker

- BitLocker stores its own encryption and decryption key in a hardware device that is separate from the hard disk, so you must have one of the following:
- A computer with TPM.
- A removable USB storage device, such as a USB flash drive. If your computer does not have TPM 1.2 or newer, BitLocker stores its key on the memory device.
- The most secure implementation of BitLocker leverages the enhanced security capabilities of TPM 1.2.
- On computers that do not have a TPM 1.2, 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 prestartup-system integrity verification that BitLocker offers when it works with a TPM.

Review Question(s)

Question: When you implement UAC, what happens to standard users and administrative users when they perform a task requiring administrative privileges?

Answer: For standard users, UAC prompts the user for the credentials of a user with administrative privileges. For administrative users, UAC prompts the user for permission to complete the task.

Question: What are the requirements for BitLocker to store its own encryption and decryption key in a hardware device that is separate from the hard disk?

Answer: A computer with TPM or a removable USB memory device, such as a USB flash drive. If your computer does not have TPM 1.2 or newer, BitLocker stores its key on the memory device.

Question: An administrator configures Group Policy to require that data can be saved only on data volumes that are protected by BitLocker. Specifically, the administrator enables the Deny write access to removable drives not protected by BitLocker policy and deploys it to the domain. Meanwhile, an end user inserts a USB flash drive that is not protected with BitLocker. What happens, and how can the user resolve the situation.

Answer: Since the USB flash drive is not protected with BitLocker, Windows 8 displays an informational dialog indicating that the device must be encrypted with BitLocker. From this dialog, the user chooses to launch the BitLocker wizard to encrypt the volume or continues working with the device as read-only.

Lab Review Questions and Answers

Lab A: Implementing Local Group Policy Objects (GPOs)

Question: Can you create multiple local Group Policies and apply them to different users?

Answer: Yes, in addition to the computer policy, you can create and configure multiple local Group Policies for different types of users, such as administrative and non-administrative users. You also can do this for individual local user accounts.

Lab B: Securing Data

Question: What are some ways of protecting sensitive data in Windows 8?

Answer: Windows 8 supports data encryption by using BitLocker, BitLocker To Go, and EFS.

Lab C: Configuring and Testing User Account Control (UAC)

Question: How can you suppress the notifications about changes to the computer?

Answer: You can use UAC settings in the Action Center to turn off UAC, so that you never are notified about changes to your computer.

Module 9

Configuring Applications

Contents:

Lesson 3
Configuring Internet Explorer Settings

Contents:

Question and Answers

Other Security Features

Question: What is the XSS filter?

Answer: The XSS Filter has visibility into all requests and responses flowing through the browser. When the filter discovers likely XSS in a request, it identifies and neutralizes the attack if it is replayed in the server's response. The XSS filter helps protect users from website vulnerabilities. It does not ask difficult questions that users are unable to answer, nor does it harm functionality on the website.

Demonstration

Demonstration: How to Configure Internet Explorer

Demonstration Steps

Enable Compatibility View for All Websites

1. Sign in to the LON-CL1 as **Adatum\Administrator** with the password **Pa$$w0rd**.

2. On the Start screen, click **Desktop**.

3. On the Taskbar, click **Internet Explorer**.

4. Right-click the bar to the left of the home symbol, and then click **Menu bar**.

5. On the menu bar, click **Tools**, and then click **Compatibility View settings**.

6. Select the **Display all websites in Compatibility View** check box, and then click **Close**.

Delete browsing history

1. On LON-CL1, click the Internet Explorer icon on the taskbar.

2. Type **http://LON-DC1** into the **Address** bar, and then press Enter.

3. Click on the down arrow next to the Address bar, to confirm that the address you typed into it is stored.

4. In Windows® Internet Explorer®, click the **Tools**, and then click **Internet Options**.

5. Click the **General** tab. Under **Browsing History**, click **Delete**.

6. In the Delete Browsing History dialog box, clear **Preserve Favorites website data**, select **Temporary Internet files and website files**, **Cookies and website data**, **History**, and then click **Delete**.

7. Click **OK** to close Internet Options.

8. Confirm that there are no addresses stored in the Address bar, by clicking on the down arrow next to the Address bar.

Configure InPrivate® browsing

1. On the **Tools** menu, click **InPrivate Browsing**.

2. Type **http://LON-DC1** into the Address bar, and then press Enter.

3. Confirm the address you entered is not stored, by clicking on the down arrow next to the Address bar.

4. Close the InPrivate Browsing window.

View the Add-on management interface

1. On the **Tools** menu, click **Manage Add-ons**.

2.   Click **Search Providers**.

3.   Click **Bing**.

4.   Click **Accelerators**.

5.   Click **Tracking Protection**.

6.   Click Close.

Download a file

1.   In the address bar, type **http://lon-dc1**, and then press Enter.

2.   Click **Download current projects**.

3.   In the Windows Internet Explorer dialog box, click **Save**.

4.   In the banner, click **View downloads**.

5.   In **View Downloads – Windows Internet Explorer**, click **Open**.

6.   The file opens in Excel.

7.   Close Excel.

8.   Close Internet Explorer, and then sign out.

Lesson 4
Configuring Application Restrictions in the Enterprise

Contents:

Question and Answers

What Is AppLocker?

Question: What are some of the applications that are good candidates for you to apply an AppLocker rule?

Answer: Answers will vary based upon student experience.

AppLocker Rules

Question: When testing AppLocker, you must consider carefully how you will organize rules between linked GPOs. What do you do if a GPO does not contain the default AppLocker rules?

Answer: If a GPO does not contain the default rules, either add the rules directly to the GPO or add them to a GPO that links to it.

How to Enforce AppLocker Rules

Question: What is the command that updates a computer's policy, and where is it run?

Answer: The command to update a computer's policy automatically is **gpupdate /force**, and you run it as an administrator in the command prompt.

Demonstration

Demonstration: How to Configure AppLocker Rules

Demonstration Steps

Create a new executable rule

1. Sign in to LON-CL1 as **Adatum\Administrator** with the password **Pa$$w0rd**.

2. On the Start screen, type **gpedit.msc**, and then press Enter.

3. In the Local Group Policy Editor, expand **Computer Configuration**, expand **Windows Settings**, and then expand **Security Settings**.

4. Expand **Application Control Policies**, and then double-click **AppLocker**.

5. Click **Executable Rules**, and then right-click and select **Create New Rule**.

6. Click **Next**.

7. On the **Permissions** screen, select **Deny**, and then click the **Select** button.

8. In the **Select User or Group** dialog box, in the **Enter the object names to select (examples)** box, type **Marketing**, click **Check Names**, and then click **OK**.

9. Click **Next**.

10. On the **Conditions** screen, select **Path**, and then click **Next**.

11. Click the **Browse Files** button, and in the **File name** box, type **C:\Windows\Regedit.exe**, and then click **Open**.

12. Click **Next**.

13. Click **Next** again, and then click **Create**.

14. Click **Yes** when prompted to create default rules.

Automatically generate the script rules

1. Select **Script Rules**, and then right-click and select the **Automatically Generate Rules** option.

2. In **Automatically Generate Script Rules**, on the **Folder and Permissions** screen, click **Next**.

3. Click **Next** again.

4. Click **Create**.

5. Click **Yes** when prompted to create default rules.

Demonstration: How to Enforce AppLocker Rules

Demonstration Steps

Enforce Windows 8 AppLocker® rules

1. In the Local Group Policy Editor, click **AppLocker**, and then right-click and select **Properties**.

2. On the **Enforcement** tab, under **Executable rules**, click the **Configured** check box, and then select **Enforce rules**.

3. On the **Enforcement** tab, under **Script rules**, click the **Configured** check box, and then select **Audit only**.

4. Click **OK**.

5. Close the Local Group Policy Editor.

Confirm the executable rule enforcement

1. Point to the bottom-left corner of the taskbar, and then click **Start** to return to the Start screen.

2. On the Start screen, type **cmd.exe**, and then press Enter.

3. In the Command Prompt window, type **gpupdate /force**, and then press Enter. Wait for the policy to update.

4. Point to the bottom-left corner of the taskbar, and then click **Start** to return to the Start screen.

5. Right-click the Start screen, and then click **All apps**.

6. In the **Apps** list, right-click **Computer**, and then click **Manage**.

7. Expand **Event Viewer**, and then expand **Windows Logs**.

8. Click **System**.

9. In the result pane, locate and then click the latest event with Event ID 1502.

10. Review the event message details under the **General** tab.

11. Expand **Services and Applications**, and then click **Services**.

12. Right-click **Application Identity** service in the main window pane, and then click **Start**.

Test the executable rule enforcement

1. Sign in as **Adatum\Adam** with the password **Pa$$w0rd**.

2. On the Start screen, type **cmd.exe**, and then press Enter.

3. At the command prompt, type **Regedit.exe**, and then press Enter.

4. Close the Command Prompt.

5. Sign in as **Adatum\Administrator** with the password **Pa$$w0rd**.

6. Right-click the Start screen, and then click **All apps**.

7. In the **Apps** list, right-click **Computer**, and then click **Manage**.

8. Expand **Event Viewer**, and then expand **Application and Services Logs**, and then expand **Microsoft**.

9. Expand **Windows**, expand **AppLocker**, and then click **EXE and DLL**.

10. Review the entries in the results pane. Locate event ID 8004. This shows Adam's attempt to run Regedit.exe.

11. Close Computer Management.

12. Close **Regedit.exe**.

13. Sign out.

Module Review and Takeaways

Best Practices

Best Practices for AppLocker

- Before creating new rules manually, or automatically generating rules for a specific folder, create the default rules. The default rules ensure that the key operating system files can run for all users.
- When testing AppLocker, carefully consider how you will organize rules between linked GPOs. If a GPO does not contain the default rules, then either add the rules directly to the GPO or add them to a GPO that links to it.
- After creating new rules, you must configure enforcement for the rule collections, and then refresh the computer's policy.
- By default, AppLocker rules do not allow users to open or run any files that are not specifically allowed. Administrators must maintain a current list of allowed applications.
- If AppLocker rules are defined in a GPO, only those rules are applied. To ensure interoperability between Software Restriction Policies rules and AppLocker rules, define Software Restriction Policies rules and AppLocker rules in different GPOs.
- When you set an AppLocker rule to Audit only, the rule is not enforced. When a user runs an application that the rule includes, the application opens, runs normally, and then Windows adds information about that application to the AppLocker event log.

Review Question(s)

Question: What are some of the privacy features in Internet Explorer?

Answer: InPrivate browsing and Tracking Protection

Question: Trevor has implemented Windows AppLocker. Before he created the default rules, he created a custom rule that allowed all Windows processes to run except for Regedit.exe. Because he did not create the default rules first, he is blocked from performing administrative tasks. What does he need to do to resolve the issue?

Answer: Trevor must restart the computer in safe mode, add the default rules, delete any deny rules that are preventing access, and then refresh the computer policy.

Tools

Tool	Use for	Where to find it
Windows PowerShell	Command –line management tool	Windows 8
DISM	Servicing and managing Windows images	Windows 8
Msiexec.exe	Managing installations	Command line
Application Compatibility Toolkit	Inventorying and analyzing organization application compatibility	Microsoft Download Center
Compatibility Administrator Tool	Creating application fixes	ACT
GPupdate	Managing policy application	Command line

Lab Review Questions and Answers

Lab A: Configuring Internet Explorer Security

Question: In the lab, you added the local intranet home page to the Trusted sites. How else could you have ensured that the required ActiveX controls did run?

Answer: You could ensure that the required ActiveX controls run by adjusting the security level for the appropriate security zone, rather than adding the site to a new zone.

Lab B: Configuring AppLocker

Question: In the lab, you configured an executable path for the executable rule. What could you do if you wanted to allow users to run an earlier version of Windows Media Player?

Answer: You could create a publisher executable rule, and specify the version to be restricted as version 12.0.0.0, citing wmplayer.exe as the reference file. Different versions now could run.

Module 10

Optimizing and Maintaining Windows® 8 Client Computers

Contents:

Lesson 1
Optimizing the Performance of Windows 8

Contents:

Question and Answers

Discussion: Common Issues with Performance and Reliability

Question: What factors can influence computer-system performance?

Answer: Answer will vary, but may include the:

- Access speed of the physical hard disks.

- Memory available for all running processes.

- Fastest speed of the processor.

- Maximum throughput of the network interfaces.

- Resources that the individual applications consume.

- Faulty or poor configuration of components, which leads to the unnecessary consumption of resources.

Question: What factors may contribute to reliability issues in a computer system?

Answer: Answers will vary, but may include:

- Application failures.

- Service becomes unresponsive and restarts.

- Driver-initialization failures.

- Operating system failures.

- Hardware failures.

What Are Performance Monitor and Data Collector Sets?

Question: A shortage of which resources can cause performance problems for your computer?

Answer: A shortage of CPU, RAM, disk space, or network connectivity can cause performance problems for your computer.

Using the Resource Monitor

Question: How can you simplify monitoring the activity of a single process when it spans different tabs?

Answer: If you select the check box for a process, then that process will be at the top of the list when you move between tabs. This simplifies your ability to view different characteristics of a single process, and can be useful when you are trying to find the resource that is a performance bottleneck for a process.

Analyzing System Performance by Using Data Collector Sets and Performance Monitor

Question: How can you use Performance Monitor for troubleshooting?

Answer: You can use Performance Monitor to monitor resources when you are running an application that is having problems. If a problem is occurring at a specific time, you can schedule a data collector set to run at that time, and then collect additional information about resource usage when this problem occurs.

Demonstration

Demonstration: Using the Resource Monitor

Demonstration Steps

1. Sign in to LON-CL1 as **Adatum\administrator** with the password **Pa$$w0rd**.

2. Right-click the Start screen, and then click **All Apps**.

3. In the **Apps** list, right-click **Computer**, and then click **Properties**.

4. In System, click **Performance Information and Tools**.

5. In the **Performance Information and Tools** page, click **Advanced tools**.

6. In the **Advanced Tools** page, click **Open Resource Monitor**. The **Overview** tab shows CPU usage, disk I/O, network usage, and memory usage information for each process. A bar above each section provides summary information.

7. Click the down arrow button in the Disk section to expand it.

8. Click the drop-down arrow next to the **Views** button, and then click **Medium**. This controls the size of the graphs that display CPU usage, disk I/O, network usage, and memory activity.

9. Click the **CPU** tab. This tab has more detailed CPU information that you can filter, and is based on the process.

10. In the Processes area, select the check box for a process, and then expand the **Associated Handles** area. This shows the files that the specific process is using, and also keeps the selected process at the top of the list to provide you with easy monitoring.

11. Click the **Memory** tab. This tab provides detailed information about memory usage for each process. Notice that the process that you selected previously remains selected, so that you can review multiple kinds of information about a process as you switch between tabs.

12. Click the **Disk** tab. This tab shows processes with recent disk activity.

13. Expand the **Disk Activity** area. The Disk Activity area provides detailed information about the files in use. The Storage area provides general information about each logical disk.

14. Click the **Network** tab. This tab provides information about all processes with current network activity.

15. Expand the **TCP Connections** area. This shows current TCP connections and information about those connections.

16. Expand the **Listening Ports** area. This shows the processes that are listening for network connections and the ports on which they are listening. The firewall status for those ports also is shown.

17. Close the Resource Monitor.

Demonstration: Analyzing System Performance by Using Data Collector Sets and Performance Monitor

Demonstration Steps

Open Performance Monitor

1. On LON-CL1, in **Advanced tools**, click **Open Performance Monitor**.

2. In the Performance Monitor window, click the **Performance Monitor** node. Notice that only **% Processor Time** is displayed by default.

Add new values to the chart

1. Click the **+** symbol in the toolbar to add an additional counter.

2. In the Available counters area, expand **PhysicalDisk**, and then click **% Idle Time**.

3. In the **Instances of selected object** box, click **0 C:**, click **Add**, and then click **OK**.

4. Right-click **% Idle Time**, and then click **Properties**.

5. In the **Color** box, click **green**, and then click **OK**.

Create a data collector set

1. In the left pane, expand **Data Collector Sets**, and then click **User Defined**.

2. Right-click **User Defined**, point to **New**, and then click **Data Collector Set**.

3. In the **Name** box, type **CPU and Disk Activity**, and then click **Next**.

4. In the **Template Data Collector Set** box, click **Basic**, and then click **Next**. We recommend that you use a template.

5. Click **Next** to accept the default storage location for the data.

6. Click **Open properties for this data collector set**, and then click **Finish**. On the **General** tab, you can configure general information about the data collector set and the credentials that the data collector set uses when it is running.

7. Click the **Directory** tab. This tab lets you define information on how the collected data is stored.

8. Click the **Security** tab. This tab lets you configure which users can change this data collector set.

9. Click the **Schedule** tab. This tab lets you define when the data collector set is active and collecting data.

10. Click the **Stop Condition** tab. This tab lets you define when data collection is stopped, based on time or data that is collected.

11. Click the **Task** tab. This tab lets you run a scheduled task when the data collector set stops. You can use this to process the collected data.

12. Click **Cancel**. Notice that there are three kinds of logs in the right pane:

    o   **Performance Counter** collects data that you can view in the Performance Monitor.

    o   **Kernel Trace** collects detailed information about system events and activities.

    o   **Configuration** records changes to registry keys.

13. In the right pane, double-click **Performance Counter**. Notice that all Processor counters are collected, by default.

14. Click **Add**.

15. In the Available counters area, click **PhysicalDisk**, click **Add**, and then click **OK**. All the counters for the PhysicalDisk object are now added.

16. Click **OK**.

17. In the left pane, right-click **CPU and Disk Activity**, and then click **Start**.

Examine a report

1. Wait a few moments, and the data collector set will stop automatically.

2. Right-click **CPU and Disk Activity**, and then click **Latest Report**. This report shows the data that is collected by the data collector set.

3.   Close the Performance Monitor.

Lesson 3
Managing Windows 8 Updates

Contents:

Question and Answers

Windows Update Group Policy Settings

Question: What is the benefit of configuring Windows Update by using Group Policy rather than by using Control Panel?

Answer: Using Group Policy enables you to apply configuration settings to multiple computers by performing a single action. It also prevents users from overriding the settings.

Module Review and Takeaways

Review Question(s)

Question: You have problems with your computer's performance, how can you create a data collector set to analyze a performance problem?

Answer: You can create a data collector set from counters in the Performance Monitor display, use a template, or do it manually.

Question: What are the benefits of creating a data collector set?

Answer: When you configure a data collector set, you can customize the information that will be included in the data collector set, and you can customize when the data will be collected. This is useful if you need to analyze a specific computer performance issue at a specific time.

Tools

Tool	Use for	Where to find it
Performance Information and Tools	List information for speed and performance	Control Panel
Performance Monitor	Multiple graph views of performance	Administrative Tools
Resource Monitor	Monitor use and performance for CPU, disk, network, and memory	Advanced tools in Performance Information and tools
Windows Experience Index	Measure the computer's key components	Performance Information and Tools
Monitoring Tools	Performance monitoring	Performance monitor
Data Collector Set	Performance counters, event traces, and system configuration data	Performance monitor
Windows Memory Diagnostic	Check your computer for memory problems	Administrative Tools
Fix a Network Problem	Troubleshoot network problems	Network and Sharing

Lab Review Questions and Answers

Lab A: Optimizing Windows 8 Performance

Question: What are the benefits of creating a data collector set?

Answer: When you configure a data collector set, you can customize the information that it will include, and you can customize when data collection occurs. This is useful if you need to analyze a specific computer's performance issues at a given time

Lab B: Maintaining Windows Updates

Question: How is the Automatic Updates feature useful?

Answer: It is an online catalog that ensures that your computer is always up to date.

Module 11

Configuring Mobile Computing and Remote Access

Contents:

Lesson 1
Configuring Mobile Computers and Device Settings

Contents:

Question and Answers

Tools for Configuring Mobile Computers and Device Settings

Question: Aside from USB, how can you establish a connection for synchronizing a Windows Phone device?

Answer: Depending upon the specific device, you can establish a connection for synchronizing a Windows Phone device with Bluetooth, wireless, and Infrared connections.

Configuring Power Plans

Question: Why is it not possible to configure options such as what occurs when the user shuts the computer's lid in the Wireless Adapter Settings, Power Saving Mode?

Answer: This virtual machine emulates a desktop computer, and those options are unavailable on desktop computers.

Demonstration

Demonstration: Configuring Power Plans

Demonstration Steps

Create a power plan for Adam's laptop

1. Sign in to LON-CL1 as **Adatum\Adam** using the password **Pa$$w0rd**.

2. On the Start screen, click **Desktop**.

3. Pause the pointer in the lower-right corner of the display, and then click **Settings**.

4. Click **Control Panel.**

5. Click **System and Security**, click **Power Options**, and then on the left, click **Create a power plan**.

6. On the **Create a power plan** page, click **Power saver**.

7. In the **Plan name** box, type **Adam's plan**, and then click **Next**.

Configure the power plan

1. On the **Change settings for the plan: Adam's plan** page, in the **Turn off the display** box, click **3 minutes**, and then click **Create**.

2. In **Power Options**, next to **Adam's plan**, click **Change plan settings**.

3. On the **Change settings for the plan: Adam's plan** page, click **Change advanced power settings**.

4. Configure the following properties for the plan, and then click **OK**.

   o Turn off hard disk after: **10 minutes**

   o Wireless Adapter Settings, Power Saving Mode: **Maximum Power Saving**

   o Power buttons and lid, Power button action: **Shut down**

5. On the **Change settings for the plan: Adam's plan** page, click **Cancel**.

6. Close the **Power Options** window.

7. Sign out from LON-CL1.

Lesson 2
Configuring VPN Access

Contents:

Demonstration

Demonstration: Configuring a VPN

Demonstration Steps

Create a new VPN connection

1. Switch to the NYC-CL1 computer and sign in as **Adatum\Administrator** with the password **Pa$$w0rd**.

2. Open **Control Panel**.

3. In the Control Panel window, under **Network and Internet**, click **View network status and tasks**.

4. In the **Network and Sharing Center** window, under Change your networking settings, click **Set up a new connection or network**.

5. In the **Choose a connection option** dialog box, click **Connect to a workplace**, and then click **Next**.

6. In the **Connect to a workplace** dialog box, select the **Use my Internet connection (VPN)** option. When prompted, select **I'll set up an Internet connection later**.

7. In the **Type the Internet address to connect to** dialog box, specify an Internet address of **172.16.0.10** and a Destination name of **HQ**, and then click **Create**.

Configure the VPN connection

1. In the Network and Sharing Center window, click **Change adapter settings**.

2. On the **Network Connections** page, right-click **HQ**, and then click **Properties**.

3. In **HQ Properties**, click the **Security** tab.

4. Click **Allow these protocols**.

5. In the Type of VPN list, click **Point to Point Tunneling Protocol (PPTP)**, and then click **OK**.

6. On the **Network Connections** page, right-click **HQ**, and then click **Connect/Disconnect**.

Test the connection

1. In the Networks list on the right, click **HQ**, and then click **Connect**.

2. Use the following information in the **Network Authentication** text boxes, and then click **OK**:

1. User name: **Adatum\Administrator**

2. Password: **Pa$$w0rd**

3. The VPN connects.

4. Right-click **HQ**, and then click **Connect/Disconnect**.

5. Click **HQ**, and then click **Disconnect**.

Demonstration: Creating a Connection Profile

Demonstration Steps

Install the CMAK feature

1. If necessary, on LON-CL1, sign in as **Adatum\administrator** with the password **Pa$$w0rd**.

2. Open **Control Panel**.

3. Click **Programs**, and in Programs, click **Turn Windows features on or off**.

4. In Windows Features, select the **RAS Connection Manager Administration Kit (CMAK)** check box, and then click **OK**.

5. Click **Close**.

Create a connection profile

1. In Control Panel, click **Control Panel Home**.

2. In the **View by** list, click **Large icons**.

3. Click **Administrative Tools**, and then double-click **Connection Manager Administration Kit**.

4. In the Connection Manager Administration Kit Wizard, click **Next**.

5. On the **Select the Target Operating System** page, click **Windows Vista or above**, and then click **Next**.

6. On the **Create or Modify a Connection Manager profile** page, click **New profile**, and then click **Next**.

7. On the **Specify the Service Name and the File Name** page, in the **Service name** box, type **Adatum HQ**, in the **File name** box, type **Adatum**, and then click **Next**.

8. On the **Specify a Realm Name** page, click **Do not add a realm name to the user name**, and then click **Next**.

9. On the **Merge Information from Other Profiles** page, click **Next**.

10. On the **Add Support for VPN Connections** page, select the **Phone book from this profile** check box.

11. In the **VPN server name or IP address** box, type **172.16.0.10**, and then click **Next**.

12. On the **Create or Modify a VPN Entry** page, click **Next**.

13. On the **Add a Custom Phone Book** page, clear the **Automatically download phone book updates** check box, and then click **Next**.

14. On the **Configure Dial-up Networking Entries** page, click **Next**.

15. On the **Specify Routing Table Updates** page, click **Next**.

16. On the **Configure Proxy Settings for Internet Explorer** page, click **Next**.

17. On the **Add Custom Actions** page, click **Next**.

18. On the **Display a Custom Logon Bitmap** page, click **Next**.

19. On the **Display a Custom Phone Book Bitmap** page, click **Next**.

20. On the **Display Custom Icons** page, click **Next**.

21. On the **Include a Custom Help File** page, click **Next**.

22. On the **Display Custom Support Information** page, click **Next**.

23. On the **Display a Custom License Agreement** page, click **Next**.

24. On the **Install Additional Files with the Connection Manager profile** page, click **Next**.

25. On the **Build the Connection Manager Profile and Its Installation Program** page, click **Next**.

26. On the **Your Connection Manager Profile is Complete and Ready to Distribute** page, click **Finish**.

Examine the created profile

1. Open Windows Explorer.

2. Navigate to **C:\Program Files\CMAK\Profiles\Windows Vista and above\Adatum**. You must distribute these files.

3. Close all open windows, and sign out from LON-CL1.

Lesson 3
Configuring Remote Desktop and Remote Assistance

Contents:

Question and Answers

Configuring Remote Assistance

Question: Under what circumstances would you use Remote Desktop Connection or Remote Assistance?

Answer: Use Remote Desktop to access one computer from another computer remotely. For example, you can use Remote Desktop to connect to your work computer from home. You potentially will have access to all of your programs, files, and network resources, as if you were sitting at your work computer.

Use Remote Assistance to give or receive assistance remotely. For example, a friend or a technical-support person can remotely access your computer to help you with a computer problem, or show you how to do something. You can help someone else the same way. In either case, both you and the other person see the same computer screen, and you both can control the mouse pointer.

Demonstration

Demonstration: Configuring Remote Assistance

Demonstration Steps

Create a Microsoft Word 2010 Document

1. Sign in to LON-CL1 as **Adatum\Adam** using the password **Pa$$w0rd**.

2. On the Start screen, right-click and then click **All apps**.

3. Click **Microsoft Word 2010**.

4. In the **User Name** dialog box, click **OK.**

5. In Word, if prompted to Help Protect and Improve Microsoft Office, click **Don't make changes**, and then click **OK**.

6. In the Document window, type **This is my document**,

7. On the ribbon, click the **File** tab, and then click **Save**.

8. Click **Save**.

Enable and then request Remote Assistance

1. Pause the pointer in the lower right of the display, and then click **Start**.

2. On the Start screen, right-click and then click **All apps**.

3. In the **Apps** list, right-click **Computer**, and then click **Properties**.

4. In **System**, click **Remote Settings**.

5. In the **User Account Control** dialog box, in the **User name** box, type **administrator**.

6. In the **Password** box, type **Pa$$w0rd**, and then click **Yes**.

7. Verify that the **Allow Remote Assistance connections to this computer** check box is selected, and then click **OK**.

8. Close System.

9. Pause the pointer in the lower right of the display, and then click **Start**.

10. Type **msra**, and then in the **Apps** list, click **msra**.

11. In the Windows Remote Assistance wizard, click **Invite someone you trust to help you**.

12. On the **How do you want to invite someone to help you** page, click **Save this invitation as a file**.

13. On the **Save as** page, in the **File name** box, type **\\LON-dc1\data\Adam's-Invite**, and then click **Save**.

14. Note the password.

Provide Remote Assistance

1. Switch to the LON-CL2 virtual machine, and then sign in as **Adatum\Holly** with the password **Pa$$w0rd**.

2. On the Start screen, click Desktop, click **Windows Explorer**, navigate to **\\LON-DC1\data**, and then double-click **Adam's-Invite.msrcincident**.

3. In the **Remote Assistance** dialog box, in the **Enter password** box, type the password that you noted in the previous task, and then click **OK**.

4. Switch to the LON-CL1 virtual machine.

5. In the **Windows Remote Assistance** dialog box, click **Yes**.

6. Switch to the LON-CL2 virtual machine.

7. On the menu, click **Request control**.

8. Switch to the LON-CL1 virtual machine.

9. In the **Windows Remote Assistance** dialog box, click **Yes**.

10. Switch to the LON-CL2 virtual machine.

11. In Word, click the **Review menu**, and then select the text in the document window.

12. In the menu, click **New Comment**, and then type **This is how you place a comment in a document**.

13. Click the cursor elsewhere in the document window.

14. In the **Windows Remote Assistance – Helping Adam** menu, click **Chat**.

15. In the **Chat** window, type **Does that help?** and then press Enter.

16. Switch to the LON-CL1 virtual machine.

17. Observe the message.

18. Type **Yes, thanks**, press Enter, and then in the **Menu**, click **Stop sharing**.

19. Close all open windows.

20. Discard the file changes, and then sign out from LON-CL1.

21. Switch to the LON-CL2 virtual machine.

22. Close all open windows, and then sign out from LON-CL2.

Lesson 4
Overview of DirectAccess

Contents:

Question and Answers

Configuring DirectAccess

Question: Why is it important that the DirectAccess client should have access to a CRL distribution point?

Answer: The Certificate Authority server publishes data about revoked certificates at the CRL distribution point. Each certificate has a validity period, but if it is not yet expired, the client must check the CRL to confirm that the certificate is not revoked.

Module Review and Takeaways

Review Question(s)

Question: Amy wants to connect to the network wirelessly but is unable to, so she checks the Windows Mobility Center to turn on her wireless network adapter. She does not see it in the Windows Mobility Center. Why is that?

Answer: If a setting does not appear in the Windows Mobility Center, it might be because the requested hardware, such as a wireless network adapter, is missing, or that drivers are missing.

Question: You have some important files on your desktop work computer that you need to retrieve when you are at a client's location with your laptop computer. What do you need to do on your desktop computer to ensure that you can download your files when at a customer site?

Answer: You need to configure remote access on your desktop computer. Select one of the access options in the **Remote Settings** tab of System from System and Security in Control Panel.

Question: Your company recently purchased a Windows Server 2008 server computer. What do you need to do before you can configure this computer with DirectAccess?

Answer: You will need to upgrade to Windows Server 2008 R2 or Windows Server 2012, and potentially upgrade to an IPv6 infrastructure, in addition to possibly installing a second network adapter in the server.

Lab Review Questions and Answers

Lab A: Configuring a Power Plan

Question: In the lab, you configured a power plan to optimize the battery life of Adam's laptop computer. What are the compromises that arise from this?

Answer: Enabling some power-saving features can affect performance so that programs may take longer to perform typical workloads. Often, you must strike a balance between battery life and performance.

Lab B: Implementing a Virtual Private Network Connection

Question: You created and test a VPN connection in the lab. When you are configuring the client-side of a VPN connection, what should factors do you need to consider?

Answer: You must consider the server-side settings. The client-side settings, in terms of authentication, encryption, tunneling type and so on, must match those of the server accepting inbound connections. Otherwise, the connection attempt will fail.

Lab C: Implementing Remote Desktop

Question: In the lab, you enabled the Remote Desktop feature through the firewall by editing the local firewall settings. Is there an alternative way in which you can make this change?

Answer: Yes, you can configure the settings through Group Policy on a domain controller. This enables you to apply the settings to a larger group of computers in a single administrative step.

Question: In the lab, you configured Remote Desktop. In what circumstances can you envision using Remote Desktop to troubleshoot a user's computer?

Answer: Answers will vary, but will include any situation in which access is required to a user's computer to perform configuration changes, but physical access is not possible.

Question: If attempting to connect to a remote computer with Remote Desktop from an Internet-connected computer, what other possible configuration changes might you need to make?

Answer: It is likely that in addition to a user's computer firewall settings, you will need to configure–or request configuration of–the corporate firewall. You will need to enable TCP port 3389 to support remote desktop. It is possible to use different ports over which to connect using Remote Desktop, but this must be configured at the computer to which you want to connect.

Module 12

Implementing Hyper-V

Contents:

Module Review and Takeaways

Question: Why would you deploy Client Hyper-V to a Windows client computer in a corporate environment?

Answer: Users can use Client Hyper-V to work with Hyper-V-based virtual machines for troubleshooting and testing purposes. You also can use it as an isolated test environment, or for running multiple operating systems on the same computer.

Question: When using the Hyper-V Virtual Machine Connection tool to connect to virtual machines hosted on a Windows 8 computer in your environment, often the tool cannot connect to the virtual machines. When you check the host computer, you notice in Event Viewer that the virtual machines are going in and out of the Saved state. What might be the problem, and how could you solve it?

Answer: The power-management features likely are turned on for the host machine, and it is going into sleep mode. To solve the problem, you could configure the host computer so that it does not go into sleep mode.

Question: Why should you not use virtual machine snapshots for backup and disaster recovery?

Answer: Snapshots are still dependent on the virtual machine's availability in order to take and apply the snapshots. Typically, snapshots also reside in the same directory as the rest of the virtual machine. Therefore, if the virtual machine fails in some way, or if the disk that houses the virtual machine and snapshot files fails, the snapshots will not be able to aid you in recovering the virtual machine.

Tools

Tool	Description	Where to Find It
Hyper-V Manager	Management console for Client Hyper-V	Start screen
Hyper-V Virtual Machine Connection Tool	Connect directly to local or remote virtual machines without opening Hyper-V Manager	Start screen

Lab Review Questions and Answers

Lab A: Implementing Hyper-V®

Question: Why did you have to boot from a Windows 8 VHD file in order to complete this lab?

Answer: An operating system that performs virtualization needs to run directly on the computer's hardware. The Windows Server 2008 R2 virtual environment that hosts the A. Datum virtual machines will not support one of those virtual machines to host virtualization itself.

Question: In the lab, you configured created a private virtual network to connect the virtual machine to. Would a private network type be the logical choice if you were using the virtual machine for testing Windows Updates? Why or why not?

Answer: A private network type would limit the virtual machine to connectivity with other virtual machines only. This would not be a good choice for Windows Updates, because the computer will need Internet connectivity to download the updates. The external network type would be best suited for a virtual machine that you are using to test Windows Updates.

Module 13

Troubleshooting and Recovering Windows 8

Contents:

Lesson 1
Backing Up and Restoring Files in Windows 8

Contents:

Demonstration

Demonstration: How to Prepare for File Recovery

Demonstration Steps

Create and edit a Word document

1. Switch to the LON-CL1 computer and sign in as **Adatum\Administrator** with the password **Pa$$w0rd**.

2. On the **Start** screen, click **Desktop**, and on the Taskbar, click **Windows Explorer**.

3. In Windows Explorer, double-click **Documents**.

4. Right-click an area of free space in Documents, point to **New**, and then click **Microsoft Word Document**.

5. Type **Recovery file**, and then press Enter.

6. Double-click **Recovery file.docx**.

7. In the **User Name** dialog box, click **OK**.

8. In Word, if prompted to Help Protect and Improve Microsoft Office, click **Don't make changes**, and then click **OK**.

9. In Word, type **This is my file**, and then press Ctrl+S.

10. Close Microsoft Word.

Enable and configure file history

1. Pause your mouse pointer in the lower right of the display, and then click **Settings**.

2. Click **Control Panel**.

3. Click **System and Security**, and then click **File History**.

4. In File History, click **Turn on**.

5. In the **File History** window, click **Advanced settings**. Review the options, and then click **Cancel**.

Enable and configure a Windows 7 File Recovery

1. In File History, click **Windows 7 File Recovery**.

2. Click **Set up backup**.

3. In the **Set up backup** dialog box, click **Save on a network**.

4. On the **Select a network location** page, in the **Network Location** box, type **\\lon-dc1\data**.

5. In the **Username** box, type **administrator**.

6. In the **Password** box, type **Pa$$w0rd**, and then click **OK**.

7. On the **Select where you want to save your backup?** page, click **Next**.

8. On the **What do you want to back up?** page, click **Next**.

9. On the **Review your backup settings** page, click **Save settings and run backup**.

Note: It is not necessary to complete the backup process.

10. Switch to the LON-DC1 computer, and then open Windows Explorer.

11. Navigate to **E:\Labfiles\Mod04\Data**.

12. Double-click the **LON-CL1** folder. This is the Windows Backup folder. Go back to the Data folder. Note that this folder may take a while to appear.

13. Switch to LON-CL1.

14. Switch to **Windows Explorer**.

15. In the navigation pane, click **Allfiles (E:)**.

16. In the details pane, double-click FileHistory.

17. Double-click the **Administrator@Adatum.com** folder. This is the File History backup folder.

18. Double-click the LON-CL1 folder.

Test the file history

1. In the navigation pane, click **Documents**.

2. In Windows Explorer, right-click **Recovery file.docx**, and then click **Delete**.

3. In Windows Explorer, click the **Home** tab on the ribbon.

4. Click **History**.

5. In **Documents – File History**, right-click **Recovery file.docx**, and then click **Restore**.

6. In Windows Explorer, notice that the Word document has been recovered.

7. Shut down LON-CL1.

Lesson 2
Recovery Options in Windows 8

Contents:

Demonstration

Demonstration: How to Resolve Startup-Related Problems

Demonstration Steps

Access Windows RE to perform startup repair options

1. On your host computer, in the **20687B-LON-CL1 on localhost – Virtual Machine Connection** dialog box, on the **Media** menu, point to **DVD Drive**, and then click **Insert Disk**.

2. In the **Open** dialog box, in the **File name** box, type C**:\Program Files\Microsoft Learning\20687\Drives\Windows8.iso**, and then click **Open**.

3. On the **Action** menu, click **Start**.

4. When you see the **Press any key to boot from CD or DVD** message, press **Spacebar**. Setup loads.

5. When prompted, in the **Windows Setup** dialog box, click **Next**.

6. On the **Windows Setup** page, click **Repair your computer**.

7. On the **Choose an option** page, click **Troubleshoot**.

8. On the **Troubleshoot** page, click **Advanced options**.

9. On the **Advanced Options** page, click **Command Prompt**.

10. At the Command Prompt, type **bcdedit /enum**, and then press Enter.

11. At the Command Prompt, type **Bootrec /scanos**, and then press Enter. This command scans disks for installations compatible with Windows 8. This option displays installations that bcdedit /enum does not list. You can use the /RebuildBcd to add the missing installations to the boot store.

12. At the Command Prompt, type **diskpart**, and then press Enter.

13. At the Command Prompt, type **list disk**, and then press Enter.

14. At the Command Prompt, type **list volume**, and then press Enter.

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

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

17. On the **Choose an option** page, click **Troubleshoot**.

18. On the **Troubleshoot** page, click **Advanced options**.

19. On the **Advanced Options** page, click **Automatic Repair**.

20. On the **Automatic Repair** page, click **Windows 8**. Automatic repair starts.

21. On the **Automatic Repair** page, click **Advanced options**.

22. On the **Choose an option** page, click **Continue**. Windows starts normally.

Enable access to the Advanced Boot Options menu

1. On LON-CL1, sign in as **Adatum\administrator** with the password **Pa$$w0rd**.

2. On the Start screen, type **cmd**.

3. In the **Apps** list, right-click **Command Prompt**, and then click **Run as administrator**.

4. At the command prompt, type **bcdedit /copy {current} /d "Duplicate boot entry"**, and then press Enter.

5. At the command prompt, type **bcdedit /enum**, and then press Enter.

6. At the command prompt, type **shutdown /r**, and then press Enter.

7. When Windows restarts, wait until the **Choose an operating system** menu appears.

8. Click **Change defaults or choose other options**.

9. On the **Options** page, click **Choose other options**.

10. On the **Choose an option** page, click **Troubleshoot**.

11. On the **Troubleshoot** page, click **Advanced options**.

12. On the **Advanced options** page, click **Startup Settings**.

13. On the **Startup Settings** page, click **Restart**.

14. In the **Startup Settings** menu, type **4** to enable **Safe Mode**.

15. On LON-CL1, sign in as **Adatum\administrator** with the password **Pa$$w0rd**.

Module Review and Takeaways

Review Question(s)

Question: After installing a new video driver, your user's computer becomes unstable and will not start correctly. What would you try first to resolve this problem?

Answer: Use Safe Mode to access System Restore, and then roll back the configuration to a previous point. If System Restore is unavailable, attempt a driver rollback.

Question: The boot environment of a user's computer is corrupt, and you suspect a virus. Before you can run virus removal tools, you must recover the boot environment. What command-line tool(s) could you use?

Answer: You can use **Bootrec.exe** with the **fixmbr** and **fixboot** switches.

Question: Your user adds a new hard disk to the computer, which changes the computer's partition numbering. To enable the computer to start, the user needs you to change the BCD. What tool would you use?

Answer: You can use **BCDEdit /enum** to view the entries in the store. Then use **BCDEdit** to edit the store to reflect the changes in the computer.

Question: A user has reported a problem to the help desk. The user is experiencing problems with starting a computer after a new device driver was added. You decide to start the computer by using a minimal boot, but want to configure that from Windows before restarting. What tool could you use?

Answer: System Configuration (MSConfig.exe) enables you to configure advanced startup options including various minimal startup environments.

Question: A system service is causing startup problems, and your help-desk user has started the problematic computer into Windows RE. What command-line tools, accessible from Windows RE, enable you to control the startup of services?

Answer: Sc.exe enables you to view and configure system services within Windows RE and the running Windows operating system.

Question: The help desk recently installed a new device driver on a computer. A stop code is generated, as is a blue screen during startup. What recovery mechanism would you try first?

Answer: Safe mode and driver rollback might be worth trying, although the computer may not be able to boot from safe mode. If it cannot, try using Windows RE and a system restore point.

Tools

Tool	Use for	Where to find it
BCDEdit.exe	Viewing and configuring the BCD store	Command-line
sc.exe	Managing services	Command-line
MSConfig.exe	Managing services and the startup environment	Windows
Windows RE	Troubleshooting Windows 8 computers	Elements available on hard disk (automatic failover) and the product DVD
Safe Mode	Troubleshooting startup	Accessible from the Advanced Boot Options menu

Tool	Use for	Where to find it
Bootrec.exe	Managing the boot environment	Command-line

Lab Review Questions and Answers

Lab: Recovering Windows 8

Question: In the lab, what was the problem?

Answer: Corrupted BCD resulted in failure to start correctly.

Question: How did you resolve the problem?

Answer: Use the product DVD to access Setup and then repair the BCD manually.

Question: What other approach could you have taken?

Answer: Automatic repair may have been successful.

Module XA

Using Windows PowerShell®

Contents:

Lesson 1
Introduction to Windows PowerShell 3.0

Contents:

Additional Reading

Cmdlets in Windows PowerShell

Additional Reading: To read about Cmdlet Verbs, go to
http://go.microsoft.com/fwlink/?LinkId=266562.

Demonstration

Demonstration: Using the Windows PowerShell ISE Editor

Demonstration Steps

1. Sign in to the **LON-DC1** virtual machine with username of **Adatum\Administrator** and password **Pa$$w0rd**.

2. Click to the Start screen, and then on the Start screen, type **Windows PowerShell ISE**, and right-click **Windows PowerShell ISE**. In the pop-up, click **Run as administrator**.

3. Click **View**, and then click **Show Script Pane**.

4. Click **File**, and then click **Open**. Navigate to the demonstration script at **E:\ModXA\Democode\Using Windows PowerShell ISE.ps1**, and then click **Open**.

5. Follow the instructions within the script to complete the demonstration.

Module Review and Takeaways

Best Practices

- Make a goal to spend time learning how to use Windows PowerShell for your common tasks. This makes you more comfortable while working with Windows PowerShell, and will equip you for using it to solve more complicated problems.
- Save the commands that you have used to solve problems in a script file for later reference.
- Use Windows PowerShell ISE for help with writing scripts, and also to ensure that you are using the proper syntax.

Review Question(s)

Question: Which cmdlet will display the content of a text file?

Answer: Get-Content displays the content of a text file. It also is acceptable to use **type,** because it is an alias for **Get-Content**.

Question: Which cmdlet will move a file to another directory?

Answer: Move-Item moves a file to another directory. It also is acceptable to use **move** and **mi** as aliases for **Move-Item**.

Question: Which cmdlet will rename a file?

Answer: New-Item creates a new directory. It also is acceptable to use **ni**, because this is an alias for **New-Item**.

Question: Which cmdlet will create a new directory?

Answer: New-Item creates a new directory. It also is acceptable to use **ni**, because this is an alias for **New-Item**.

Question: Which cmdlet do you think would retrieve information from the Event Log?

Answer: Get-EventLog retrieves information from the event log.

Question: Which cmdlet do you think would start a stopped virtual machine?

Answer: Start-VM would start a stopped virtual machine.

Tools

You can use the following tools to work with Windows PowerShell:

Tool	Description
Windows PowerShell Integrated Script Editor (ISE)	Windows PowerShell ISE provides a simple, yet powerful interface to create and test scripts, and discover new cmdlets.
Microsoft Visual Studio Workflow Designer	This is a development tool used to create Windows PowerShell workflows.
Windows PowerShell.exe	This is the Windows PowerShell executable.
Active Directory® Administrative Center	This tool enables you to perform common Active Directory management tasks, such as creating and modifying user and computer accounts. All of the changes

Tool	Description
	made by using this management tool are logged in the Windows PowerShell History pane.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Administrators are unable to find the correct Windows PowerShell cmdlet for a task.	Use the **Get-Command** cmdlets and Help in Windows PowerShell ISE to search for cmdlets.
Administrator is not able to connect to a server with remote Windows PowerShell.	There are a few possible reasons this could happen, such as Remote Windows PowerShell connections may be blocked using Windows Advanced Firewall, or the WinRM service may be misconfigured or disabled. For more information, see about_remote_troubleshooting.
Get-Help does not provide any help for cmdlets.	You may need to download the latest help files. You can download the latest files by using the **Update-Help** cmdlet.
An administrator is new to Windows PowerShell and is uncomfortable with the command-line.	Use Windows PowerShell ISE to become more familiar with the command-line. Also, use the **Get-Command** and **Show-Command** cmdlets to provide additional help.

Send Us Your Feedback

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

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

Courseware Feedback

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

Reporting Errors

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

1. Document or CD part number

2. Page number or location

3. Complete description of the error or suggested change

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

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