Microsoft

20698B

Installing and Configuring Windows 10

Companion Content

MICROSOFT LICENSE TERMS
MICROSOFT INSTRUCTOR-LED COURSEWARE

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

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

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

1. **DEFINITIONS.**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

provided you comply with the following:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   This limitation applies to
   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 July 2013

Module 1

Installing Windows 10

Contents:

Lesson 1
Overview of Windows 10

Contents:

Question and Answers

Question: Contoso Pharmaceuticals considers purchasing new computers to better control its production lines. The production lines require special hardware with sensors in the computers that employees will use to supervise the lines. The production line software is sensitive to major changes in the operating system.

Which edition of Windows 10 would you recommend for purchase by Contoso Pharmaceuticals for supervision of its production lines?

> **Answer:** Windows 10 Enterprise Long-Term Servicing Channel because the production line software requires a stable operating system that does not receive new features.

Lesson 2
Planning your Windows 10 deployment

Contents:

Question and Answers

Question: Is your organization ready for Windows 10?

Answer: Answers will vary based on students' organizational IT infrastructure.

Question: Which Windows ADK tool do you use to create provisioning packages?

( ) Application Compatibility Toolkit

( ) Windows PE

( ) Deployment Image Servicing and Management

( ) Windows Configuration Designer

( ) Windows System Image Manager

Answer:

( ) Application Compatibility Toolkit

( ) Windows PE

( ) Deployment Image Servicing and Management

(√) Windows Configuration Designer

( ) Windows System Image Manager

Resources

Determine hardware readiness

Reference Links: For more information, refer to Microsoft Assessment and Planning (MAP) Toolkit: https://aka.ms/anwv94

Demonstration: Using MAP to determine readiness for Windows 10

Demonstration Steps

Create an inventory database

1. On **LON-CL1**, click **Start**, scroll down, click the **Microsoft Assessment and Planning Toolkit** folder, and then click **Microsoft Assessment and Planning Toolkit**. You might want to resize the application to full screen.

2. In the **Microsoft Assessment and Planning Toolkit** dialog box, click **Create an inventory database**. In the **Name** box, type **Demo**, and then click **OK**.

3. Click **File**, and then click **Manage Databases** to open the **Microsoft Assessment and Planning Toolkit** dialog box.

4. Select the **Demo** database, and then click **Export**.

5. Type **Demo** as the file name, and then click **Save**.

6. After successfully exporting the database, click **OK**.

7. In the **Microsoft Assessment and Planning Toolkit** dialog box, click **Import**.

8. In the **Microsoft Assessment and Planning Toolkit** dialog box, click **Browse**, select the **MAP_SampleDB.bak** demonstration database from the **DatabaseBackups** folder (**C:\Program Files\Microsoft Assessment and Planning Toolkit**), and then click **Open**.

9. In the **Microsoft Assessment and Planning Toolkit** dialog box, in the **Database Name** box, type **MAP_SampleDB**, and then click **OK**.

10. In the **Microsoft Assessment and Planning Toolkit** dialog box, click **OK**.

11. Click **Close** in the **Microsoft Assessment and Planning Toolkit** dialog box.

View inventory data

1. Click **File**, and then click **Create/Select Database**.

2. Click **Use an existing database**, select the **MAP_SampleDB** database, and then click **OK**.

3. Click the **Desktop** node, and then select the **Windows 10 Readiness** scenario after the database is ready.

4. Under **Options**, click **Generate Windows 10 Readiness Report**.

5. When the **Report Generation Status** dialog box displays **Reports Generated 1 of 1**, click **Close**.

6. Open the **Windows10Assessment-xxxx.xlsx** report.

7. In Excel, if prompted, in the **Microsoft Office Activation Wizard**, click **Close**.

8. Review the **Windows10Assessment-xxxx.xlsx** report. Close the report when your review is complete.

9. Perform a similar report generation on the **Environment** node for the **Inventory Results** scenario. Review the generated Microsoft Excel report.

10. Close the report when your review is complete.

11. Close the console.

Lesson 3
Installing and deploying Windows 10

Contents:

Question and Answers

Question: Which deployment option is typically used by small organizations?

> **Answer:** The high touch with retail media deployment strategy is suitable for small organizations that do not have IT staff or that have IT staff members without deployment experience.

Demonstration: Installing Windows 10 (optional)

Demonstration Steps

Mount the Windows 10 DVD

1. Start Hyper-V Manager, if it is not already running.

2. In the **Virtual Machines** pane, right-click **20698B-LON-CL5**, and then click **Settings**.

3. In the hardware pane, click **DVD Drive**.

4. In the DVD drive pane, click **Image file**, and then click **Browse**.

5. In the **Open** window, locate the .iso file. It should be located at **C:\Program Files\Microsoft Learning\20698\Drives\ Win10_1709_Eval.iso**, but the location might vary depending upon where the virtual machines were extracted.

6. Click **Open**.

7. In the **Settings** window, click **OK**.

Start the 20698B-LON-CL5 VM

1. Double-click the **20698B-LON-CL5** virtual machine (VM).

2. Click the **Start** icon to start the **20698B-LON-CL5** VM.

Install Windows 10

1. On the first page of the Windows setup program, make sure that the settings are:

   o Language to install: **English (United States)**

   o Time and currency format: **English (United States)**

   o Keyboard or input method: **US**

2. Click **Next**.

3. On the second page of the **Windows Setup** wizard, click **Install now**.

4. On the **Applicable notices and license terms** page, select the **I accept the license terms** check box, and then click **Next**.

5. On the **Which type of installation do you want?** page, click **Custom: Install Windows only (advanced)**.

6. On the **Where do you want to install Windows?** page, ensure that **Drive 0 Unallocated Space** is selected, and then click **Next**. The installation begins. It will take a few minutes to complete.

7. On the **Let's start with region. Is this right?** page, click **Yes**.

8. On the **Is this the right keyboard layout?** page, click **Yes**, and then click **Skip**.

9. On the **Let's connect you to a network** page, click Skip for now.

10. On the **Who's going to use this PC?** page, in the **Name** box, type **LocalAdmin**, and then click **Next**.

11. On the two subsequent pages, type the password **Pa55w.rd**, and then click **Next**.

12. On the **Add a hint for your password** page, in the **Password hint** box, type **Standard**, and then click **Next**.

13. On the **Make Cortana your personal assistant?** page, click **No**.

14. On the **Choose privacy settings for your device** page, click **Accept**.

15. **LocalAdmin** is signed in.

Lesson 4
Upgrading to Windows 10

Contents:

Question and Answers

Question: Migration is the preferred method of upgrading to Windows 10.

( ) True

( ) False

> **Answer:**
>
> ( ) True
>
> (√) False
>
> **Feedback:** Performing an in-place upgrade is the preferred method of upgrading to Windows 10.

Question: You must migrate the user state after an in-place upgrade.

( ) True

( ) False

> **Answer:**
>
> ( ) True
>
> (√) False
>
> **Feedback:** All applications, user settings, and files are available after an in-place upgrade.

Discussion: Common upgrade and migration scenarios

Question: What is the best upgrade method for the 100 workstations running Windows 7 at Contoso Pharmaceuticals?

> **Answer:** Side-by-side migration
>
> **Feedback:** Side-by-side migration is the most suitable method because Contoso Pharmaceuticals wants a more standardized environment. Therefore, it is better to start with the same baseline on all computers.

Question: What is the best upgrade method for the 25 computers at Litware, Inc.?

> **Answer:** In-place upgrade
>
> **Feedback:** In-place upgrade is the preferred upgrade method in Windows 10, and this scenario does not require a different method. This is a straightforward upgrade from supported operating systems.

Question: What is the best upgrade method for the 5,000 client computers at A. Datum?

> **Answer:** In-place upgrade
>
> **Feedback:** In-place upgrade is the preferred upgrade method in Windows 10, and this scenario does not require a different method.

Question: What is the best upgrade method for the 50 users who are getting new computers at Contoso Pharmaceuticals?

> **Answer:** Wipe-and-load migration
>
> **Feedback:** Wipe-and-load migration is the best method for the users receiving new computers with Windows 10. This method will take all the settings and files from the old computers and migrate them to the new computers. The only issue is that the new computers will require installation of all applications.

Demonstration: Migrating user state with USMT

Demonstration Steps

Prepare the source computer

1. On **LON-CL3**, right-click the desktop, point to **New**, and then click **Text Document**. Type **Demofile**, and then press Enter.

2. Double-click **Demofile.txt**, and then type some text. Press Alt+F4, and then click the **Save** button.

3. Click **Start**, type **cmd**, and then press Enter.

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

   ```
   Net Use F: \\LON-DC1\USMT
   ```

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

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

   ```
   Scanstate \\LON-DC1\MigStore\LON-CL3\ /i:migapp.xml /i:miguser.xml /o
   ```

Complete the migration

1. Switch to **LON-CL1**.

2. Notice that there is no **Demofile.txt** on the desktop and no Internet Explorer or Windows Media Player icon in the taskbar.

3. Click **Start**, type **cmd**, and then press Enter.

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

   ```
   Net Use F: \\LON-DC1\USMT
   ```

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

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

   ```
   Loadstate \\LON-DC1\MigStore\Lon-CL3\ /i:migapp.xml /i:miguser.xml /lac:Pa55w.rd /lae
   /c
   ```

   This will take several minutes to complete. If you receive a 'Write error 5' message, you can ignore it.

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

   ```
   Exit
   ```

8. Notice that **Demofile.txt** is now on the desktop.

Lesson 5

Windows 10 installation maintenance

Contents:

Question and Answers

Sequencing Activity

Question:

Put the following steps in order by numbering each to indicate the correct order.

	Steps
	Open Windows Imaging and Configuration Designer.
	Click the appropriate package tile.
	Enter the project details information.
	Choose which settings to view and configure.
	Import a provisioning package (optional).
	Click **Finish**.
	Add available customizations.
	Save the project.
	Deploy or execute the provisioning package.

Answer:

	Steps
1	Open Windows Imaging and Configuration Designer.
2	Click the appropriate package tile.
3	Enter the project details information.
4	Choose which settings to view and configure.
5	Import a provisioning package (optional).
6	Click **Finish**.
7	Add available customizations.
8	Save the project.
9	Deploy or execute the provisioning package.

Resources

Using DISM for installation and image maintenance

Additional Reading: For a complete reference for the various DISM command-line options, refer to Deployment Image Servicing and Management (DISM) Command-Line Options: https://aka.ms/mb2m71

Demonstration: Using Windows Configuration Designer to create provisioning packages

Demonstration Steps

Create a provisioning package

1. On **LON-CL1**, click **Start**, and then scroll down the list. Select and expand **Windows Kits**, scroll down within **Windows Kits**, and then click **Windows Imaging and Configuration Designer**.

2. After the Windows Configuration Designer console loads, click the **Advanced provisioning** tile. The **New Project** wizard will start.

3. On the **Enter project details** page, in the **Name** text box, type **DemoProvPackage**. In the **Description** text box, type **Demonstration of a Provisioning Package**, and then click **Next**.

4. On the **Choose which settings to view and configure** page, select **All Windows editions**. Take a moment to discuss the other choices on this page with the class, and then click **Next**.

5. On the **Import a provisioning package (optional)** page, notice that you can perform this action by typing the name of a package in the text box and then clicking **Browse**. However, explain that because this the first time that you are running the **New Project** wizard, there are no previous packages to import. Click **Finish**.

6. The **DemoProvPackage** window appears. In the **Available customizations** list, examine the **View** drop-down list. There are five items within it: **All settings**, **Common IT Pro settings**, **Common IoT settings**, **Common Team Edition settings**, and **Common Imaging settings**. The default is **All settings**. Ensure that **All settings** is selected.

7. One node will be available below **View**: Runtime settings. Refer to the table in the previous topic for details about the items found in this node. Expand **Runtime settings**.

8. Scroll down, expand **ConnectivityProfiles**, and then click **WiFiSense**.

9. In the details pane, under the **ConnectivityProfiles/WifiSense/FirstBoot** section, in the **WiFiSenseAllowed** item, click the drop-down list. It has three settings: **NOT CONFIGURED**, **Enabled**, and **Disabled**. Click **Disabled**.

10. In the **Runtime settings** console tree, select and expand **Policies**, and then click **Connectivity**.

11. In the sub-items under the **Connectivity** node, click **AllowVPNOverCellular**.

12. In the details pane, click the **NOT CONFIGURED** drop-down list item, and then click **No**.

13. Collapse the **Connectivity** node. Below it, expand the **Update** node.

14. Select the first sub-item, **ActiveHoursEnd**, and then, in the **Numeric only, Default = 17** field, type **18**.

15. On the menu bar, in the **Export** drop-down list, click **Provisioning package**.

16. In the **Build** window, under **Owner**, in the **OEM** drop-down list, click **IT Admin**, and then click **Next**.

17. On the **Select security details for the provisioning package** page, click **Next**.

18. On the **Select where to save the provisioning package** page, click **Next**.

19. On the **Build the provisioning package** page, click **Build**, and then click **Finish**.

Lesson 6
Managing volume activation

Contents:

Resources

Subscription models

Additional Reading: For more information, refer to Windows 10 Enterprise E3 in CSP Overview: https://aka.ms/ke729y

Module Review and Takeaways

Review Questions

Question: Your organization wants to deploy Windows 10 and wants to be able to join the computers to Microsoft Azure Active Directory. Which editions of Windows 10 will you be able to use?

> **Answer:** Windows 10 Pro, Windows 10 Enterprise, and Windows 10 Education.

Question: The IT staff at A Datum want to enable device health attestation within the organization. What hardware feature is required to enable this Windows 10 feature?

> **Answer:** Device health attestation requires a Trusted Platform Module (TPM) version 2.0 or later.

Question: Contoso Pharmaceuticals is trying to secure their IT infrastructure by limiting the apps that users can run. Some employees install unauthorized apps on their devices. Contoso wants to limit users to apps that are on the company's list of approved apps.

Which edition of Windows 10 would you recommend that Contoso Pharmaceuticals use on its devices?

> **Answer:** Windows 10 Enterprise, because you can use AppLocker to limit users to running only authorized apps.

Question: One of your users has been promoted to a new position and has been given a new computer. The user needs the new apps that the job requires. The user also needs to have the documents and settings from their old Windows 7 computer transferred to their new computer. How should you perform the Windows 10 installation?

> **Answer:** In this scenario, you should perform a side-by-side migration because a new computer and a new set of apps are being used. After installing Windows 10 on the new computer and installing the new apps, you need to migrate the user's documents and settings that are on the Windows 7 computer to the new computer.

Lab Review Questions and Answers

Lab A: Upgrading to Windows 10

Question and Answers

Question: Which tools from Microsoft can help you automate the deployment of Windows 10?

> **Answer:** You can use the Windows Assessment and Deployment Kit (Windows ADK), which contains the Windows System Image Manager (Windows SIM), Deployment Image Servicing and Management (DISM), and Windows Configuration Designer to build answer files and images. You can use the Microsoft Deployment Toolkit (MDT) to automate the deployment itself. Use the User State Migration Tool (USMT) to migrate user settings if you do a migration instead of an in-place upgrade.

Question: You have a few computers running Windows Vista. What is a supported method of upgrading the computers to Windows 10?

> **Answer:** First, upgrade to Windows 7 Service Pack 1 (SP1), and then upgrade to Windows 10. Alternatively, capture user settings, perform a clean installation of Windows 10, install applications, and then restore user settings.

Lab B: Maintaining a Windows 10 installation with Windows Configuration Designer

Question and Answers

Question: What type of project can you create in Windows Configuration Designer?

> **Answer:** You can create a provisioning package.

Module 2
Performing post-installation configuration

Contents:

Lesson 1
Overview of management tools

Contents:

Question and Answers

Question: You cannot execute standard command prompt commands at the Windows PowerShell command prompt.

(   ) True

(   ) False

> **Answer:**
>
> (   ) True
>
> (√) False

Resources

Using Windows PowerShell

> 🌐   **Additional Reading:** For more information, refer to Microsoft Script Center:
> http://aka.ms/ipge1q
>
> 🌐   **Additional Reading:** For more information, refer to Microsoft Script Center:
> http://aka.ms/ipge1q

Demonstration: Configuring a device

Demonstration Steps

Explore and use the Settings app

1. On **LON-CL1**, click **Start**, and then click **Settings**.

2. Maximize the **Settings** page.

3. On the **Settings** page, click the **System** item.

4. Ensure that the **Display** item is selected in the console tree.

5. Under **Scale and layout**, click the down arrow in the **Resolution** box, select **1280 x 800**, and then click **Apply**.

6. In the **Keep these display settings** window, click **Keep changes**.

7. At the upper left side of the screen, notice the back arrow by Settings. Click the back arrow. This will take you to the main **Settings** page.

8. On the **Settings** page, click the **Devices** item.

9. In the navigation pane, click **Printers & scanners**.

10. In the details pane, click the **Add a printer or scanner** plus sign.

11. Note how the Settings app scans for printers or scanners, but finds none.

12. Click **Start**, type **Control Panel**, and then press Enter.

13. Under **Hardware and Sound**, click **View devices and printers**.

14. Click **Add a printer**. Explain that to make some configurations at the Settings level, you will need to use the Control Panel.

15. In the **Choose a device or printer to add to this PC** window, click **The printer that I want isn't listed**.

16. In the **Add Printer** window, click **Add a local printer or network printer with manual settings**, and then click **Next**.

17. On the **Choose a printer port** page, click **Next**.

18. On the **Install the printer driver** page, under the **Manufacturer** column, select **HP**, under the **Printers** column, scroll down, click **HP Photosmart 7520 series Class Driver**, and then click **Next**.

19. On the **Type a printer name** page, delete the text that says **series Class Driver**, leaving only the **HP Photosmart 7520** text, and then click **Next**.

20. On the **Printer Sharing** page, click **Next**.

21. On the **You've successfully added HP Photosmart 7520** page, click **Finish**.

22. Switch to the **Printers & scanners** page of **Settings**.

23. Click the **HP Photosmart 7520** icon. Note the options that appear: **Open queue**, **Manage**, and **Remove device**.

24. Review other Settings items, explaining what they do.

Explore and use the Control Panel

1. Switch to **Control Panel**.

2. Spend just a few moments going over some of the items in Control Panel, as most of the functionality in the Control Panel has not changed. If you have time, you can try to find the equivalent item in the Settings app, or ask the students if they can find it.

Open and use Windows PowerShell

1. In the **Ask me anything** text box on the taskbar, type **PowerShell**, and then press Enter.

2. At the Windows PowerShell command prompt, type **Get-Command**, and then press Enter.

3. Tell the class about cmdlet **History**, explain how to access it by pressing the Up Arrow key, and explain how the Tab key can help finish long cmdlets.

4. Press the Up Arrow key, and after **Get-Command**, press the space bar once, type **–Listi**, and then press the Tab key. The parameter should change to **–ListImported**. Press Enter. Review the reduced return set with the class.

5. At the Windows PowerShell command prompt, type **Get-Help New-Item**, and then press Enter. If a message is returned that says **Do you want to run Update-Help?**, type **N**, and then press **Enter**.

📋   **Note:** Note the **Remarks** section of the reply, and explain how you would want to use the **–Online** parameter to get the additional content.

6. At the Windows PowerShell command prompt, type **ipconfig.exe /all**, and then press Enter.

7. At the Windows PowerShell command prompt, type **Get-NetIPAddress**, and then press Enter. Note the similarities and differences between the two output returns. Close Windows PowerShell.

8. Sign out.

Lesson 2
Customizing the user interface

Contents:

Question and Answers

Question: When you sign in to on a Windows 10 touch device, it runs only in Tablet mode.

( ) True

( ) False

Answer:

( ) True

(√) False

Feedback: Windows 10 runs in Tablet mode by default, but you can switch it manually to Desktop mode.

Question: What happens to a Windows 10 tablet device when you remove the magnetically attached keyboard?

Answer: Windows 10 has a feature called Continuum that senses when you remove a tablet's keyboard or remove the tablet from a docking station. When this happens, Continuum puts the device into tablet mode, which changes the Start menu back to a Start screen. The Continuum feature maintains the desktop and ensures that the taskbar is accessible in Tablet mode, and you can scroll the Start screen tiles across the desktop, just as you did with the Start screen tiles in Windows 8.

Demonstration: Navigating the user interface

Demonstration Steps

Sign in

1.   Switch to LON-CL1, and then click the Lock screen.

2.   Click **Other user**.

3.   In the **User name** text box, type **Beth**.

4.   In the **Password** text box, type **Pa55w.rd**, and then press Enter.

Open Action Center

1.   On the taskbar, click **Action Center**.

📝   **Note:** If the tiles at the bottom of Action Center do not display, close and open **Action Center** again.

2.   Click **Tablet mode**.

3.   Click **Start** to close Action Center.

View installed apps

1.   In Start, click **All apps**. (The **All apps** icon is the third from the top on the left side of the screen).

2.   In the **All apps** list, click **Calculator**.

3.   Click **Start**.

4.   Click **All apps**, and then click **Alarms & Clock**.

Switch between running apps

1. On the taskbar, click **Task View**. Both running apps should display.

2. Click **Action Center**.

3. Click **Tablet mode**.

4. In **Alarms & Clock**, click **Restore Down**.

5. Drag **Alarms & Clock** to the right side of the display, and then release it.

6. Click **Calculator**. Both apps should display, side by side.

Add a new desktop

1. On the taskbar, click **Task View**.

2. On the right side of the display, click **New desktop**.

3. Click **Desktop 2**.

4. Click **Start**, scroll down, and then click **Word 2016**.

5. On the taskbar, click **Task View**. Both desktops should display, side by side.

Sign out

- Close all apps, right-click **Start**, point to **Shut down or sign out**, and then click **Sign out**.

Demonstration: Customizing the Windows 10 Start menu

Demonstration Steps

Sign in

1. Switch to LON-CL1, and then click the Lock screen.

2. Sign in as **ADATUM\Beth** with the password as **Pa55w.rd**.

3. On the taskbar, click **Action Center**.

📋   **Note:** If the tiles at the bottom of Action Center do not display, close and then open **Action Center** again.

4. Click **Tablet mode**.

5. Click **Start** to close Action Center.

Configure Start

1. In Start, click **All apps**.

2. Right-click **Word 2016**, and then click **Pin to Start**.

3. Right-click **PowerPoint 2016**, and then click **Pin to Start**.

4. Right-click **Excel 2016**, and then click **Pin to Start**.

5. Right-click **Alarms & Clock**, and then click **Pin to Start**.

6. Click the **Pinned tiles** icon to close **All apps**.

7. Click the space immediately above the four tiles.

8. A text box appears. Type **Microsoft Office**, and then press Enter.

9. Right-click **Alarms & Clock**, and then click **Unpin from Start**.

10. Click and hold the **Microsoft Office** group, and then drag it to the top of the display above the default groups. Release it.

Configure the taskbar

1. On the taskbar, click **Action Center**.

2. Click **Tablet mode**.

3. Click the desktop to close Action Center.

4. Click **Start**, right-click **Calculator**, point to **More**, and then click **Pin to taskbar**.

5. Sign out.

Lesson 3
Managing devices, device drivers, and services

Contents:

Question and Answers

Question: You can use a device driver that is not signed digitally with 64-bit editions of Windows 10.

( ) True

( ) False

> **Answer:**
>
> ( ) True
>
> (√) False
>
> **Feedback:** 64-bit editions of Windows 10 require that device drivers are signed digitally, and you cannot use device drivers if they are unsigned. The only exception is if you restart the computer and select the Disable driver signature enforcement advanced startup option that does not enforce this limitation. All 32-bit editions of Windows 10 will warn you if you try to add drivers that are not signed digitally, but they will use the drivers if you select them.

Demonstration: Managing device drivers

Demonstration Steps

1.   On LON-CL1, sign in as **Adatum\Administrator** with the password as **Pa55w.rd**.

2.   On the taskbar, right-click **Start**, and then click **Device Manager**.

3.   In Device Manager, expand **Keyboards**, right-click **Standard PS/2 Keyboard**, and then click **Properties**.

4.   In the **Standard PS/2 Keyboard Properties** dialog box, click the **Driver** tab.

> 📝   **Note:** The **Roll Back Driver** button is not available.

5.   Click **Update Driver**.

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

7.   On the **Browse for drivers on your computer** page, click **Let me pick from a list of available drivers on my computer**.

8.   On the **Select the device driver you want to install for this hardware** page, in the **Show compatible hardware** list, click **PC/AT Enhanced PS/2 Keyboard (101/102-Key)**, click **Next**, and then click **Close**.

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

10. In the **Driver Package rollback** dialog box, click **Previous version of the driver had more features**, and then click **Yes**.

> 📝   **Note:** Explain that after the rollback operation, the name of the dialog box changes to **Standard PS/2 Keyboard Properties**, and the Roll Back Driver is not available. This is because driver rollback can go back by one version only.

11. Click **Close**, click **No**, and then close **Device Manager**.

12. On the taskbar, click **File Explorer**.

13. In File Explorer, in the navigation pane, expand **This PC**, expand **Local Disk (C:)**, expand **Windows**, expand **System32**, expand **DriverStore**, and then click **FileRepository**.

14. In the details pane, click the **Date modified** column, and note that the top folder was created most recently.

15. Click **Start**, type **cmd.exe**, right-click **Command Prompt**, and then click **Run as administrator**.

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

```
PnPutil.exe /add-driver E:\Labfiles\Mod02\dc3dh\*.inf
```

17. In File Explorer, in the details pane, point out that the top folder was created when you installed the driver package, and that its name starts with **dc3dh**, as was the name of the .inf file. Double-click the folder, and then point out that it contains driver package files.

18. Close File Explorer and the command prompt.

Lesson 5
Overview of Client Hyper-V

Contents:

Question and Answers

Question: What is the purpose of Client Hyper-V in Windows 10?

> **Answer:** Client Hyper-V enables you to create discrete operating-system environments within Windows 10 that can support legacy or specialized apps that might not work correctly in Windows 10 natively. For example, these apps might require earlier Windows versions.

Resources

What is Client Hyper-V?

Additional Reading: For more information, refer to Hyper-V: List of SLAT-Capable CPUs for Hosts: http://aka.ms/aqufzi

Module Review and Takeaways

Question: Do you need to add a device driver for each device that you want to use with Windows 10?

> **Answer:** No. Windows 10 includes device drivers for tens of thousands of devices. It is very likely that Windows 10 will include the device driver for any device that you want to use. Of course, you can add additional device drivers and update existing device drivers with newer versions.

Question: Which tool can you use to verify, in one view, that on a Windows 10 computer, all of the device drivers are signed?

> **Answer:** You can use the SigVerif.exe tool or driverquery.exe with **/si** switch to verify in one location that all of the device drivers are signed digitally.

Question: How can you use multiple operating systems on a Windows 10 computer simultaneously?

> **Answer:** You can use multiple operating systems on a Windows 10 computer simultaneously by installing the Client Hyper-V feature. With this feature, you can create multiple VMs, install a different operating system in each VM, and then use them all at the same time.

Lab Review Questions and Answers

Lab A: Managing devices

Question and Answers

Question: Why did you have to configure picture password as a sign-in option?

> **Answer:** In the exercise, you simulated a keyboard problem. The keyboard was not working, so you could not sign in by typing user credentials. You could sign in only by using the mouse with a picture password.

Question: You want to install a driver into the driver store. How would you go about doing that?

> **Answer:** You could use the pnputil.exe command with the **/Add-driver** parameter.

Lab B: Configuring features and power options

Question and Answers

Question: In the lab, you used both Windows PowerShell and Control Panel to manage Windows features. What is the other tool that can you use?

> **Answer:** You can also use the Dism.exe command-line tool to add or remove Windows features.

Module 3

Implementing networking

Contents:

Lesson 1
Homegroups, workgroups, and domains

Contents:

Demonstration: Adding a computer to a domain

Demonstration Steps

1. Switch to **LON-CL4** and sign in as **Admin** with the password **Pa55w.rd**.

2. On the taskbar, click **File Explorer**, and then click **This PC**.

3. Right-click **This PC**, and then click **Properties**.

4. In the **System** window, click the **Change settings** link.

5. In the **System Properties** dialog box, on the **Computer Name** tab, click **Change**.

6. In the **Computer Name/Domain Changes** dialog box, click **Domain**.

7. In the **Domain** text box, type **Adatum.com**, and then click **OK**.

8. In the **Windows Security** dialog box, in the **User name** text box, type **Administrator**.

9. In the **Password** text box, type **Pa55w.rd**, and then click **OK**.

10. At the "Welcome to the Adatum.com domain" message, click **OK**.

11. At the "You must restart your computer to apply these changes" message, click **OK**.

12. In the **System Properties** dialog box, click **Close**, and then click **Restart Now**.

13. Sign in as **Adatum\Administrator** with the password **Pa55w.rd**.

14. On the taskbar, click **File Explorer**, and then click **This PC**.

15. Right-click **This PC**, and then click **Properties**.

16. In the **System** window, click the **Change settings** link.

17. In the **System Properties** dialog box, on the **Computer Name** tab, click **Change**.

18. Verify that the computer is now a part of the Adatum.com domain. Close all open windows without making any further changes.

Lesson 2
Configuring IPv4 network connectivity

Contents:

Question and Answers

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

> **Answer:** Yes, that is a concern, because those are Internet-routable addresses. Most IPv4 networks use private addresses with NAT to allow access to the Internet. If this organization does not own the 131.107.88.0/24 network, they will not be able to access resources on the 131.107.88.0/24 network on the Internet, because all clients will consider them as local addresses.

Question: What would be the best way to configure IP addresses for a branch office with only 50 desktop computers?

> **Answer:** Answers could vary. Although you could assign IPv4 configurations manually for such a small group of computers, this process is still prone to human error. It would be advisable to implement the automatic IPv4 configuration by using a DHCP server or the DHCP function in a device, such as a router.

Demonstration: Configuring IPv4

Demonstration Steps

View IPv4 configuration from a GUI

1. Switch to **LON-CL1**.

2. Click the **Network** icon in the notification area, and then click **Network & Internet settings**.

3. Click **Network and Sharing Center**.

4. In **Network and Sharing Center**, to the right of the **Adatum.com** Domain network, click **Ethernet**.

5. In the **Ethernet Status** dialog box, click **Details**. This window displays the same configuration information for this adapter as would the **Ipconfig** command.

6. In the **Network Connection Details** window, click **Close**.

7. In the **Ethernet Status** dialog box, click **Properties**. You can configure protocols in this window.

8. 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.

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

10. Click **Cancel** three times and then close all open windows without modifying any settings.

View IPv4 configuration from a command line

1. Right-click **Start**, and then click **Windows PowerShell (Admin)**.

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

3. At the Windows PowerShell command prompt, type **Get-NetIPv4Protocol**, and then press Enter.

4. At the Windows PowerShell command prompt, type **netsh interface ipv4 show config**, and then press Enter. The current IPv4 configuration displays.

5. At the Windows PowerShell command prompt, type **ipconfig /all**, and then press Enter.

Test connectivity

1. At the Windows PowerShell command prompt, type **test-connection LON-DC1**, and then press Enter.

2. At the Windows PowerShell command prompt, type **netstat -n**, and then press Enter. Observe and describe the active connections to 172.16.0.10. Most connections to services are transient.

3. If no connections appear, create a connection. To create a connection, in the **Ask me anything** text box, type **\\LON-DC1**, and then press Enter.

4. In **File Explorer**, double-click **NETLOGON**.

5. At the Windows PowerShell command prompt, type **netstat -n**, and then press Enter. Identify the services that **LON-CL1** has connections to on **LON-DC1**.

Reconfigure the IPv4 configuration

1. Click the **Network** icon in the notification area, and then click **Network & Internet settings**.

2. Click **Network and Sharing Center**.

3. In **Network and Sharing Center**, to the right of the **Adatum.com** Domain network, click **Ethernet**.

4. In the **Ethernet Status** dialog box, click **Properties**. In this window, you can configure protocols.

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

6. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, click **Obtain an IP address automatically**. Notice that when you click this, the **Alternate Configuration** tab is enabled.

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

8. Click the **Alternate Configuration** tab. Configuration information on this tab is used when no DHCP server is available.

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

10. In the **Ethernet Properties** dialog box, click **OK** or **Close** as appropriate.

11. In the **Ethernet Status** dialog box, click **Details**. Notice that DHCP is enabled, and that the IP address of the DHCP server displays.

12. Switch to the Windows PowerShell command prompt.

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

14. Close all open windows.

Lesson 3
Configuring IPv6 network connectivity

Contents:

Question and Answers

Question: How many IPv6 addresses does a Windows 10 host typically have?

> **Answer:** An IPv6 network interface typically has two or more addresses:
>
> - A link-local address, which is automatically generated and is used for local link traffic.
>
> - An additional unicast address (which might be a global address or a unique local address), which is used for traffic routed beyond the local link.

Demonstration: Configuring IPv6

Demonstration Steps

View IPv6 configuration by using IPConfig

1. On **LON-CL1**, if necessary, open a Windows PowerShell command prompt.

2. At the Windows PowerShell command prompt, type **ipconfig**, and then press Enter.

    Notice that this returns a link-local IPv6 address.

3. Type **Get-NetIPAddress**, and then press Enter.

Configure IPv6 on LON-CL1

1. On **LON-CL1**, click the **Network** icon in the notification area, and then click **Network & Internet settings**.

2. Click **Network and Sharing Center**.

3. In **Network and Sharing Center**, to the right of the **Adatum.com** Domain network, click **Ethernet**.

4. In the **Ethernet Status** dialog box, click **Properties**.

5. Click **Internet Protocol Version 6 (TCP/IPv6)**, and then click **Properties**.

6. In the **Internet Protocol Version 6 (TCP/IPv6) Properties** dialog box, click **Use the following IPv6 address**.

7. In the **IPv6 address** text box, type **FD00:AAAA:BBBB:CCCC::A**.

8. In the **Subnet prefix length** text box, type **64**.

9. In the **Preferred DNS server** text box, type **::1**, and then click **OK**.

10. In the **Ethernet Properties** dialog box, click **OK** or **Close** as appropriate.

11. In the **Ethernet Status** dialog box, click **Close**.

12. In Windows PowerShell, type **ipconfig /all**, and then press Enter. Verify the new IPv6 configuration.

13. In **Network and Sharing Center**, to the right of the **Adatum.com** Domain network, click **Ethernet**.

14. In the **Ethernet Status** dialog box, click **Properties**.

15. Click **Internet Protocol Version 6 (TCP/IPv6)**, and then click **Properties**.

16. In the **Internet Protocol Version 6 (TCP/IPv6) Properties** dialog box, click **Obtain an IPv6 address automatically**.

17. Click **Obtain DNS server address automatically**, and then click **OK**.

18. In the **Ethernet Properties** dialog box, click **OK** or **Close** as appropriate.

19. In the **Ethernet Status** dialog box, click **Close**.

20. Close all open windows.

Lesson 4
Implementing name resolution

Contents:

Question and Answers

Question: What is a reverse lookup zone?

> **Answer:** Reverse lookup zones contain PTR records. The PTR records are used to resolve IP addresses to host names.

Demonstration: Configuring and verifying name resolution

Demonstration Steps

Verify the IPv4 configuration

1. Switch to **LON-CL1**.

2. In the notification area, click the **Network** icon, and then click **Network & Internet settings**.

3. Click **Network and Sharing Center**.

4. In **Network and Sharing Center**, to the right of the **Adatum.com** Domain network, click **Ethernet**.

5. In the **Ethernet Status** dialog box, click **Details**.

6. Notice that DHCP is enabled, and that the IP address of the DHCP server displays. Note the DNS server address.

7. In the **Network Connection Details** dialog box, click **Close**.

8. In the **Ethernet Status** dialog box, click **Close**.

View and clear the name cache

1. If necessary, right-click **Start**, and then click **Windows PowerShell (Admin)**.

2. At the Windows PowerShell command prompt, type **ipconfig /displaydns**, and then press Enter.

3. At the Windows PowerShell command prompt, type **Get-DnsClientCache**, and then press Enter.

4. At the Windows PowerShell command prompt, type **ipconfig /flushdns**, and then press Enter.

5. At the Windows PowerShell command prompt, type **Clear-DnsClientCache**, and then press Enter.

6. At the Windows PowerShell command prompt, type **ipconfig /displaydns**, and then press Enter.

Test name resolution to LON-DC1

1. At the Windows PowerShell command prompt, type **test-connection lon-dc1**, and then press Enter.

2. At the Windows PowerShell command prompt, type **Get-DnsClientCache | fl**, and then press Enter.

3. At the Windows PowerShell command prompt, type **ipconfig /displaydns**, and then press Enter.

Create an entry in the Hosts file

1. At the Windows PowerShell command prompt, type **notepad C:\Windows\System32\drivers\etc\hosts**, and then press Enter.

2. Scroll to the end of the file, type **172.16.0.10 intranet**, and then press Enter.

3. Click **File**, and then click **Save**.

4. Close Notepad.

Test the new entry

1. At the Windows PowerShell command prompt, type **test-connection intranet**, and then press Enter.

2. At the Windows PowerShell command prompt, type **Get-DnsClientCache | fl**, and then press Enter.

3. View the intranet record in the cache.

Test name resolution

1. At the Windows PowerShell command prompt, type **nslookup lon-dc1.adatum.com**, and then press Enter.

2. At the Windows PowerShell command prompt, type **Resolve-Dnsname LON-DC1 | fl**, and then press Enter.

3. At the Windows PowerShell command prompt, type **nslookup –d1 lon-dc1.adatum.com > file.txt**, and then press Enter.

4. Type **notepad .\file.txt**, and then press Enter.

5. Review the information, and then close Notepad. Note that you must scroll to the section starting with **Got answer**.

6. Close Windows PowerShell.

Lesson 5
Troubleshooting network connectivity

Contents:

Question and Answers

Question: If clients complain that they are unable to connect to a server, which of the following steps would help you to resolve the problem?

(   ) Restart the server.

(   ) Verify that the client has a valid IP address.

(   ) Verify the client received the proper APIPA address.

(   ) Check the IP configuration of the servers to which the client is trying to connect.

(   ) All of the above.

> **Answer:**
>
> (   ) Restart the server.
>
> (√) Verify that the client has a valid IP address.
>
> (   ) Verify the client received the proper APIPA address.
>
> (   ) Check the IP configuration of the servers to which the client is trying to connect.
>
> (   ) All of the above.

Demonstration: Troubleshooting network connections

Demonstration Steps

Test connectivity

1. If necessary, open Windows PowerShell.

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

    ```
    test-connection LON-DC1
    ```

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

    ```
    netstat –n
    ```

    Observe and describe the active connections to 172.16.0.10. Most connections to services are transient.

4. If no connections appear, create a connection. To create a connection, in the **Ask me anything** text box, type **\\LON-DC1**, and then press Enter.

5. In **File Explorer**, double-click **NETLOGON**.

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

    ```
    netstat –n
    ```

    Identify the services to which **LON-CL1** had connections on **LON-DC1**.

Lesson 6
Implementing wireless network connectivity

Contents:

Question and Answers

Discussion: Considerations for wireless connectivity

Question: What are some considerations for enabling Wi-Fi access for your users?

> **Answer:** Answers will vary, but could include:

- Potential security issues. Any user within range of a wireless hub can potentially connect.

- Convenience. By definition, wireless connections eliminate the need for physical wiring between users' devices and the network.

- Management issues. More users might wish to connect more devices through wireless connections, particularly their own devices, such as cellphones and tablets. These are probably unmanaged devices, which can pose problems for the IT department.

Discussion: Troubleshooting wireless connectivity

Question: How will you verify that these problems are occurring?

> **Answer:** You should go to the Cambridge location to attempt to reproduce the problem.

Question: What do you suspect is causing these problems?

> **Answer:** Answers will vary, but might include:

- Interference from electronic devices can cause connection failures.

- Clients might fail to connect because their computers are not configured with the appropriate wireless settings.

- Some wireless access points might be in the wrong place, enabling connections from the parking lot.

Question: How will you resolve these issues?

> **Answer:** Answers might vary, but will include:

- Examine the location for sources of interference and, where possible, move the wireless access points from these areas.

- Suggest implementing Group Policy Objects (GPOs) to configure appropriate wireless settings.

- Consider moving the wireless access points. In addition, consider the selected wireless channel, antennas, use of wireless repeaters, and updating drivers or firmware. Also, ensure that they are using certificate-based authentication and a high level of encryption to help increase security.

Module Review and Takeaways

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 not available.

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:** To clear the DNS resolver cache, you can use the Windows PowerShell cmdlet **Clear-DnsClientCache**. You can also use **IPConfig /flushdns**.

Question: How does an incorrect default gateway configuration affect the network communication?

> **Answer:** A host with an incorrect default gateway is unable to communicate with hosts on a remote network. However, this does not affect communication on the local network.

Lab Review Questions and Answers

Lab A: Implementing network connections

Question and Answers

Question: In the lab, you tested name resolution. If a user notices that she cannot access normal enterprise websites, but she knows that she has a valid IP address, what tool can she use to troubleshoot her computer's DNS access?

> **Answer:** She can use **NSLookup** to troubleshoot DNS access issues.

Question: In the lab, you configured the Windows 10 device to obtain its IPv4 configuration automatically. What might happen if you did this and no DHCP server was available?

> **Answer:** The likely outcome would be that the device would obtain an APIPA address in the 169.254.X.Y range.

Lab B: Troubleshooting network connections

Question and Answers

Question: What was your approach to the first scenario? How did your approach differ from the class?

> **Answer:** Answers will vary.

Question: What was your approach to the second scenario? How did your approach differ from the class?

> **Answer:** Answers will vary.

Module 4

Implementing network security

Contents:

Lesson 1
Implementing Windows Defender Firewall

Contents:

Question and Answers

Question: You need to open a firewall port to allow Lightweight Directory Access Protocol (LDAP) traffic. Which port would you open to accomplish this task?

( ) 143

( ) 389

( ) 443

( ) 161

> **Answer:**
>
> ( ) 143
>
> (√) 389
>
> ( ) 443
>
> ( ) 161
>
> **Feedback:** LDAP uses Port 389.

Demonstration: Configuring inbound and outbound firewall rules

Demonstration Steps

Test Remote Desktop connectivity

1. On LON-CL1, click **Start**, and then type **Remote Settings**.

2. In the **Best match** list, click **System**.

3. In **System**, click **Remote settings**.

4. In the **System Properties** dialog box, on the **Remote** tab, under Remote Desktop, click **Allow remote connections to this computer** and then click **OK**.

5. On LON-DC1, right-click **Start**, and then click **System**.

6. In **System**, click **Remote settings**.

7. In the **System Properties** dialog box, on the **Remote** tab, under Remote Desktop, click **Allow remote connections to this computer**, and then click **OK**.

8. On **LON-CL2**, in the **Ask me anything** box, type **mstsc.exe**, and then press Enter.

9. In the Remote Desktop Connection dialog box, in the **Computer** box, type **LON-CL1**, and then press Enter.

10. Sign in to **LON-CL1** as **Adatum\Administrator** with the password **Pa55w.rd**.

11. In the Remote Desktop session, right-click **Start**, point to **Shut down or sign out**, and then click **Sign out**.

Configure an inbound rule

1. On **LON-CL1**, sign in to **LON-CL1** as **Adatum\Administrator** with the password **Pa55w.rd**.

2. Click **Start**, type **Control Panel**, and then press Enter.

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

4. In the left pane, click **Advanced settings**, click and then right-click **Inbound Rules**, and then click **New Rule**.

5. In the **New Inbound Rule Wizard** window, select **Predefined**, click the drop-down list, click **Remote Desktop**, and then click **Next**.

6. On the **Predefined Rules** page, select all available rules, and then click **Next**.

7. On the **Action** page, **select Block the connection**, and then click **Finish**.

8. Minimize the **Windows Defender Firewall with Advanced Security** window.

Test the inbound rule

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

2. In the **Ask me anything** box on the taskbar, type **mstsc**, and then click **mstsc**. This opens a **Remote Desktop Connection**.

3. In the **Computer** box, type **LON-CL1**, and then press Enter.

4. Verify that the connection attempt fails, and then click **OK**.

Test outbound Remote Desktop connectivity

1. Switch to **LON-CL1**.

2. In the **Ask me anything** box on the taskbar, type **mstsc**, and then click **mstsc**. This opens a **Remote Desktop Connection**.

3. In the **Computer** box, type **LON-DC1**, and then press Enter.

4. Sign in to **LON-DC1** as **Adatum\Administrator** with the password **Pa55w.rd**.

5. In the Remote Desktop session, right-click **Start**, point to **Shut down or sign out**, and then click **Sign out**.

Configure an outbound rule

1. On **LON-CL1**, on the taskbar, click the **Windows Defender Firewall with Advanced Security** window, and then click **Outbound Rules**.

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

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

4. On the **Program** page, click **This program path**, type **C:\Windows\System32\mstsc.exe**, and then click **Next**.

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

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

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

8. 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**.

9. Click the **Scope** tab, and then, under the **Remote IP address** heading, click **These IP addresses**.

10. Under the **Remote IP address** heading, click **Add**, in the **This IP address or subnet** box, type **172.16.0.10**, and then click **OK**.

11. In the **Block Outbound RDP to LON-DC1 Properties** dialog box, click **OK**.

Test outbound Remote Desktop connectivity

1. On **LON-CL1**, in the **Ask me anything** box on the taskbar, type **mstsc**, and then click **mstsc**. This opens a **Remote Desktop Connection**.

2. In the **Computer** box, type **LON-DC1**, and then press Enter.

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

4. Close all open windows.

Lesson 2
Connection security rules

Contents:

Question and Answers

Question: Which of the following authentication options allows you to use a pre-shared key when configuring a connection security rule?

(   ) Computer and User (Kerberos V5)

(   ) Computer (Kerberos V5)

(   ) User (Kerberos V5)

(   ) Computer Certificate

(   ) Advanced

> **Answer:**
>
> (   ) Computer and User (Kerberos V5)
>
> (   ) Computer (Kerberos V5)
>
> (   ) User (Kerberos V5)
>
> (   ) Computer Certificate
>
> (√) Advanced
>
> **Feedback:** Only the **Advanced** option allows the use of a pre-shared key.

Demonstration: Creating and configuring connection security rules

Demonstration Steps

Enable PING through the firewall

1. On **LON-CL1**, click **Start**, type **Control Panel**, and then press Enter.

2. Click **System and Security**, and then click **Windows Defender Firewall**.

3. In the left pane, click **Advanced settings**, click and right-click **Inbound Rules**, and then click **New Rule**.

4. In the **New Inbound Rule Wizard** window, select **Custom**, and then click **Next**.

5. On the **Program** page, click **Next**.

6. On the **Protocol and Ports** page, in the **Protocol type** list, click **ICMPv4** and then click **Next**.

7. On the **Scope** page, click **Next**.

8. On the **Action** page, select **Allow the connection**, and then click **Next**.

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

10. On the **Name** page, in the **Name** box, type **Inbound ICMPv4** and then click **Finish**.

11. Minimize the **Windows Defender Firewall with Advanced Security** window.

12. Switch to LON-CL2 and repeat steps 1 through 11.

Test connectivity between LON-CL2 and LON-CL1

1. On **LON-CL2**, in the **Ask me anything** box on the taskbar, type **Windows PowerShell**, and then press Enter.

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

3. Verify that the ping generated four "Reply from 172.16.0.40: bytes=32 time=$x$ms TTL=128" messages. Please note, the times that the message lists may vary from the example.

4.   Switch to **Windows Defender Firewall with Advanced Security**.

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

6.   Click **Main Mode**, and then examine the information in the center pane. No information should be present.

7.   Click **Quick Mode**, and then examine the information in the center pane. No information should be present.

8.   Switch to **LON-CL1**.

9.   In the **Ask me anything** box on the taskbar, type **PowerShell**, and then press Enter.

10. To examine the Main Mode SAs, at the command prompt, type the following command, and then press Enter:

```
Get-NetIPsecMainModeSA
```

11. To examine the Quick Mode SAs, at the command prompt, type the following command, and then press Enter:

```
Get-NetIPsecQuickModeSA
```

12. Running each command should produce no result.

Create a connection rule

1.   Switch to **Windows Defender Firewall with Advanced Security**.

2.   In the left pane, click **Connection Security Rules**.

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

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

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

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

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

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

9.   Switch to LON-CL2.

10. On LON-CL2, and switch to **Windows Defender Firewall with Advanced Security**.

11. In the left pane, click **Connection Security Rules**.

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

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

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

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

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

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

Test connectivity between LON-CL2 and LON-CL1

1. On LON-CL2, in the **Administrator: Windows PowerShell** window, type **ping LON-CL1**, and then press Enter.

2. Verify that the ping generated four "Reply from 172.16.0.40: bytes=32 time=$x$ms TTL=128" messages. Please note, the times that the message lists may vary from the example.

3. In **Windows Defender Firewall with Advanced Security**, in the left pane, expand **Monitoring**, and then expand **Security Associations**.

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

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

6. Close all open windows.

7. Switch to LON-CL1.

8. To examine the Main Mode SAs, at the command prompt, type the following command in the **Administrator: Windows PowerShell** window, and then press Enter:

```
Get-NetIPsecMainModeSA
```

9. Review the result.

10. To examine the Quick Mode SAs, at the command prompt, type the following command, and then press Enter:

```
Get-NetIPsecQuickModeSA
```

11. Review the result.

12. Close all open windows.

Lesson 3
Implementing Windows Defender Antivirus

Contents:

Demonstration: Using Windows Defender Antivirus

Demonstration Steps

1. Switch to LON-CL1.

2. Click **Start**, and then click **Windows Defender Security Center**.

3. In Windows Defender Security Center, on the **Home** tab, click **Scan now**.

4. Click **Quick scan**, and then review the results.

5. Open **File Explorer**, and then browse to **E:\Labfiles\Mod04**.

6. In the Mod04 folder, open **sample.txt** in Notepad. The **sample.txt** file contains a text string to test malware detection.

7. In the **sample.txt** file, delete both instances of **<remove>**, including the brackets and any extra lines or blank spaces.

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

9. Windows Defender then removes **sample.txt** from the **Mod04** folder.

10. Switch to **Windows Defender Security Center**.

11. On the **Virus & threat protection** page, click **Scan history**.

12. Under the **Virus:DOS/EICAR_Test_File** heading, click **Severe**.

13. Click **Remove**.

14. Close and reopen **Windows Defender Security Center**.

15. Click **Virus & threat protection**.

16. Click **Virus & threat protection settings**.

17. Review the following settings:

    o **Real-time protection**

    o **Cloud-delivered Protection**

    o **Automatic sample submission**

    o **Controlled Folder Access**

    o **Exclusions**

    o **Notifications**

18. Right-click **Start**, and then click **Run**.

19. In the **Run** dialog box, type **gpedit.msc** and press Enter.

20. Expand **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then click **Windows Defender Antivirus**.

21. Review the Group Policy items present, and explain how you can use Group Policy to configure Windows Defender settings.

22. Close all open windows.

Module Review and Takeaways

Question: Why is it important to have a firewall on the host *and* a firewall on the perimeter network?

Answer: Answers will vary, but the main reason is that having multiple firewalls provides stronger defense-in-depth, as compared to a single firewall on a perimeter network or just on the host.

Lab Review Questions and Answers

Lab: Implementing network security

Question and Answers

Question: In what way does a connection security rule protect network traffic?

>**Answer:** Connection security rules protect network traffic from interception and modification by malicious users.

Question: You want to block users from utilizing a particular application on computers that use a specific port to connect to an Internet server. What type of rule should you configure?

>**Answer:** You should configure an outbound rule to block the application from sending traffic on that port.

Module 5

Managing Windows 10 with Group Policy

Contents:

Lesson 1
Overview of Group Policy

Contents:

Question and Answers

Question: To which types of Active Directory objects can you link a GPO? Select all that apply.

(   ) User

(   ) Domain

(   ) Security group

(   ) Site

(   ) OU

> **Answer:**
>
> (   ) User
>
> (√) Domain
>
> (   ) Security group
>
> (√) Site
>
> (√) OU
>
> **Feedback:** You can link a GPO only to a site, domain, and OU. With security filtering, you can limit the application of a GPO to group members only, and you can prevent other users or computers who might have an account in the same part of Active Directory Domain Services (AD DS) from applying the GPO.

Question: Which of the following tools can you use for Group Policy troubleshooting? Select all that apply.

(   ) GPRefresh

(   ) GPUpdate

(   ) GPReport

(   ) GPResult

(   ) RSoP.msc

> **Answer:**
>
> (   ) GPRefresh
>
> (√) GPUpdate
>
> (   ) GPReport
>
> (√) GPResult
>
> (√) RSoP.msc

Feedback: In Windows 10, you can use GPUpdate, GPResult, and RSoP.msc for Group Policy troubleshooting. Windows 10 has no built-in tools named GPRefresh and GPReport.

Resources

Managing Group Policy inheritance

Additional Reading: The only way to configure password policies in a domain is in the GPO with the highest link order in the domain. To learn more about password policies, refer to: http://aka.ms/wtsi9c

Demonstration: Configuring GPOs

Demonstration Steps

Start the Group Policy Management Console (GPMC)

1.   In the **Server Manager** window, click **Tools**, and then click **Group Policy Management**.

2.   Switch to the **Group Policy Management** window.

Create a GPO

1.   In the **Group Policy Management** window, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, right-click the **Group Policy Objects** node, and then click **New**.

2.   In the **New GPO** dialog box, in the **Name** text box, type **Desktop Settings GPO**, and then press Enter.

Link a GPO

1.   Right-click the **Research** OU, and then click **Link an Existing GPO**.

2.   In the **Select GPO** dialog box, click **Desktop Settings GPO**, and then click **OK**.

3.   Click the **Research** OU, and then click the **Group Policy Inheritance** tab.

Note: Notice that both the Desktop Settings GPO and the Default Domain Policy apply to the Research OU.

Configure Block Inheritance

•   Right-click the **Research** OU, and then click **Block Inheritance**.

Note: Notice the exclamation mark (!), which denotes that inheritance has been blocked on the Research OU. Notice that only the Desktop Settings GPO displays on the **Group Policy Inheritance** tab.

Configure security filtering

1.   Click the **Group Policy Objects** node, and then double-click the **Desktop Settings GPO**.

2.   Click the **Delegation** tab, and then click the **Advanced** button.

3.   In the **Desktop Settings GPO Security Settings** dialog box, click **Add**.

4.   In the **Select Users, Computers, Service Accounts, or Groups** dialog box, type **IT**, and then click **OK**.

5.   In the **Desktop Settings GPO Security Settings** dialog box, next to **Apply group policy**, select the **Deny** check box, and then click **OK**.

6.   In the **Windows Security** dialog box, click **Yes**.

Create an RSoP report

1.   Right-click the **Group Policy Results** node, and then click **Group Policy Results Wizard**.

2.   In the **Group Policy Results Wizard** window, click **Next**.

3.   On the **Computer Selection** page, click **Next**.

4.   On the **User Selection** page, click **Next**.

5. On the **Summary of Selections** page, click **Next**.

6. On the **Completing the Group Policy Results Wizard** page, click **Finish**.

7. Examine the **Summary**, **Details** and **Policy Events** tabs.

8. On the **Details** tab, click **show all**, right-click somewhere in the text of the **Details** tab, and then click **Save Report**.

9. In the **Save GPO Report** dialog box, click **Documents**, and then click **Save**.

10. On the desktop, on the taskbar, click the **File Explorer** icon.

11. In File Explorer, double-click the **Documents** folder, and then double-click the **Administrator on LON-DC1.htm** file.

12. In the warning message box, click **Allow blocked content**.

13. Click **show all**.

📋   **Note:** Notice that the contents of the file are the same as the report shown in the GPMC.

14. Close Internet Explorer.

15. Close File Explorer.

Lesson 2
Configuring Windows 10 devices with GPOs

Contents:

Question and Answers

Question: Which of the following are new settings that you can configure in Windows 10 **Administrative Templates**?

( ) Microsoft Edge

( ) Windows Hello

( ) Windows Insider

( ) Storage Sense

( ) Command prompt

> **Answer:**
>
> (√) Microsoft Edge
>
> (√) Windows Hello
>
> (√) Windows Insider
>
> ( ) Storage Sense
>
> ( ) Command prompt
>
> **Feedback:** You have previously been able to configure access to the command prompt, so this is not a new setting. Some of the new settings that you can configure in Windows 10 **Administrative Templates** include Microsoft Edge, Windows Hello, and Windows Insider.

Resources

New administrative template settings in Windows 10

Reference Links: When Microsoft releases a new version of the Windows operating system, a Microsoft Excel spreadsheet with all the settings that you can configure in administrative templates is also released. You can download this Group Policy Settings Reference spreadsheet from the Microsoft Download Center at https://aka.ms/qvk02m.
The **Windows10andWindows2016PolicySettings.xlsx** spreadsheet details all the available settings, and you can use the filtering capabilities that are included in this spreadsheet to view specific settings. For example, you can filter the **Supported On** column to view a list of settings that are specific to Windows 10 or Windows Server 2016.

Demonstration: Configuring Group Policy settings

Demonstration Steps

1. On **LON-DC1**, in the **Group Policy Management** window, click the **Group Policy Objects** node, right-click **Desktop Settings GPO**, and then click **Edit**.

2. In the **Group Policy Management Editor** window, under **User Configuration**, expand **Policies**, expand **Administrative Templates**, expand **System**, and then click **Logon**.

3. In the **details** pane, double-click **Run these programs at user logon**.

4. In the **Run these programs at user logon** dialog box, select the **Enabled** option, and then click the **Show** button.

5. In the **Show Contents** dialog box, in the **Value** column, type **notepad.exe**, and then click **OK**.

6. In **Run these programs at user logon** dialog box, click **OK**.

7. Close the **Group Policy Management Editor** window.

8. In the **Group Policy Management** window, right-click the **Group Policy Objects** node, and then click **New**.

9. In the **New GPO** dialog box, type **Computer Settings GPO**, and then press Enter.

10. Click the **Group Policy Objects** node, right-click **Computer Settings GPO**, and then click **Edit**.

11. In the **Group Policy Management Editor** window, under **Computer Configuration**, expand **Policies**, expand **Administrative Templates**, and then click **System**.

12. In the details pane, double-click **Display highly detailed status messages**.

13. In the **Display highly detailed status messages** dialog box, select the **Enabled** option, and then click **OK**.

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

15. In the details pane, double-click **Interactive logon: Message title for users attempting to log on**.

16. In the **Interactive logon: Message title for users attempting to log on Properties** dialog box, select the **Define this policy setting** check box, in the text box, type **Welcome to the Adatum corporate domain**, and then click **OK**.

17. In the details pane, double-click **Interactive logon: Message text for users attempting to log on**.

18. In the **Interactive logon: Message text for users attempting to log on Properties** dialog box, select the **Define this policy setting in the template** check box, in the text box, type **You are not allowed to use this computer for inappropriate behavior**, and then click **OK**.

19. Close the **Group Policy Management Editor** window.

20. In the navigation pane, right-click the **Adatum.com** domain, and then click **Link an Existing GPO**.

21. In the **Select GPO** dialog box, click **Computer Settings GPO**, and then click **OK**.

22. On the host computer, switch to **Hyper-V Manager**.

23. In **Hyper-V Manager**, click **20698B-LON-CL1**, and then in the **Actions** pane, click **Start**.

24. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.

25. Switch to **LON-CL1**.

26. On **LON-CL1**, click **OK** to accept the message, and then click the **Other user** icon.

27. Sign in as **Adatum\Claire** with the password **Pa55w.rd**.

28. Notice the terms and conditions that you had to accept before signing in.

📋   **Note:** Because this is the first time Claire signed in, her profile is being created. Instead of the welcome message, different texts display that refer to the different actions the Group Policy client is performing.

Notice that Notepad opens.

29. Sign out of **LON-CL1**.

Module Review and Takeaways

Best Practices

Best practices related to Group Policy management

- Include comments on GPO settings to document settings and to make it easier to find configured settings later.
- Use a Central Store for administrative templates.
- Use Group Policy preferences to eliminate settings that are configured in logon scripts.

Review Questions

Question: What is the benefit of having a Central Store?

> **Answer:** A Central Store is a single folder in SYSVOL that holds all the ADMX and ADML files that are required for administering Group Policy. After you have set up the Central Store, the **Group Policy Management Editor** recognizes it and then loads all administrative templates from the Central Store instead of from the local computer. This is beneficial if you edit GPOs from several computers. By using a Central Store, you only need to update ADMX and ADML files in one location.

Question: Have you extended the set of administrative templates in your organization? If yes, did you download them from the Internet, or did you develop them in your organization?

> **Answer:** Answers will vary. You can download ADMX files for applications including Office, Skype, Adobe Reader, Mozilla Firefox, 7-Zip, and Java.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Group Policy settings are not applying to all users or computers in an OU where a GPO is applied.	- Check security filtering on the GPO. - Check WMI filters on the GPO.
Group Policy preferences are not applying.	Check the preference settings for item-level targeting.

Lab Review Questions and Answers

Lab: Configuring Group Policy Objects and settings

Question and Answers

Question: Which policy settings do you deploy by using Group Policy in your organization?

> **Answer:** Answers will vary.

Question: Many organizations rely heavily on security group filtering to scope GPOs rather than linking GPOs to specific OUs. In these organizations, GPOs typically are linked high in the Active Directory logical structure—usually to the domain itself or to a first-level OU. What advantages do you gain by using security group filtering rather than GPO links to manage a GPO's scope?

> **Answer:** The fundamental problems with relying on organizational units (OUs) to scope the application of GPOs is that an OU is a fixed, inflexible structure within AD DS, and a single user or computer can only exist within one OU. As organizations grow larger and more complex, configuration requirements are difficult to match in a one-to-one relationship with any container structure. With security groups, a user or computer can exist in as many groups as necessary, and you can add or remove them easily without affecting the security or management of the user or computer account.

Module 6

Implementing remote management

Contents:

Lesson 1
Using Remote Desktop

Contents:

Question and Answers

Question: What protocol does Remote Desktop use and over which TCP port does it communicate?

> **Answer:** Remote Desktop uses the Remote Desktop Protocol (RDP) protocol over Transmission Control Protocol (TCP) port 3389.

Lesson 2
Using Remote Assistance

Contents:

Question and Answers

Question: With Remote Assistance, the local user is required to sign out.

( ) True

( ) False

> **Answer:**
>
> ( ) True
>
> (√) False
>
> **Feedback:** An important difference between Remote Desktop and Remote Assistance is that with Remote Assistance, the local user is not required to sign out. This enables the remote helper to interact with the local user and the local user to observe the actions of the remote helper.

Lesson 3
Remoting with Windows PowerShell

Contents:

Question and Answers

Question: What does the **Invoke-Command** Windows PowerShell cmdlet do when it is used to manage a computer remotely?

> **Answer:** This cmdlet enables you to run the subsequent commands on the named computer. For example, the following command runs the hostname command on the computer named **LON-CL1**:

```
Invoke-Command -ComputerName LON-CL1 -ScriptBlock {hostname}
```

Demonstration: Using Windows PowerShell remoting

Demonstration Steps

1. Switch to **LON-CL1**.

2. Right-click **Start**, and then click **Windows PowerShell (Admin)**.

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

```
Winrm quickconfig
```

4. When prompted, press **Y**, and then press Enter.

5. Press **Y**, and then press Enter again.

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

```
Enable-PSRemoting -Force
```

7. Switch to **LON-CL2**.

8. Right-click **Start**, and then click **Windows PowerShell (Admin)**.

9. Repeat steps 3 through 6.

10. Switch to **LON-DC1**.

11. Right-click **Start**, and then click **Windows PowerShell (Admin)**.

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

```
Invoke-Command -ComputerName LON-CL1 -ScriptBlock {Get-EventLog -log system}
```

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

```
$s = New-PSWorkflowSession -ComputerName LON-CL1
```

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

```
Enter-PSSession $s
```

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

```
Get-Command
```

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

```
exit
```

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

```
Invoke-Command -Session $s -ScriptBlock {$c = Get-command}
```

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

```
Invoke-Command -Session $s -ScriptBlock {$c.count}
```

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

```
Invoke-Command -ComputerName LON-CL1, LON-CL2 -ScriptBlock {Get-Culture}
```

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

```
$s = New-PSWorkflowSession -ComputerName LON-CL1, LON-CL2
```

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

```
Invoke-Command -Session $s -ScriptBlock {$c = Get-command}
```

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

```
Invoke-Command -Session $s -ScriptBlock {$c.count}
```

23. On **LON-DC1**, click **Start**, scroll down, expand **Windows PowerShell**, right-click **Windows PowerShell ISE**, point to **More**, and then click **Run as administrator**.

24. In the **Administrator: Windows PowerShell ISE** window, click **File**, and then click **New Remote PowerShell Tab**.

25. In the **New Remote PowerShell Tab** window, in the **Computer** text box, type **LON-CL1**, in the **User name** box, type **administrator**, and then click **Connect**.

26. In the **Windows PowerShell credential request** dialog box, in the **Password** box, type **Pa55w.rd**, and then click **OK**.

27. In the **LON-CL1** window, type the following command, and then press Enter:

```
Get-Service | Where-Object {$_.Status –eq "Running"}
```

28. In the **LON-CL1** window, type the following command, and then press Enter:

```
Get-NetIPConfiguration
```

29. In the **LON-CL1** window, type the following command, and then press Enter:

```
Restart-Computer -Force
```

30. Verify that **LON-CL1** has restarted.

Module Review and Takeaways

Question: You need to forcibly restart a user's computer remotely. The user is not currently in front of the computer. What methods can you use to do this?

> **Answer:** You can restart the user's computer remotely using a remote Windows PowerShell session. You also could connect by using Remote Desktop and then restart the computer.

Question: What is the difference between solicited and offered Remote Assistance?

> **Answer:** With solicited Remote Assistance, the computer user forwards an invitation to the helper. With offered Remote Assistance, an authorized user offers Remote Assistance to the user.

Question: What cmdlet can you use from a remote Windows PowerShell session to view the IP address configuration of the remote computer?

> **Answer:** You can use the **Get-NetIPConfiguration** cmdlet to view the IP address configuration of the remote computer.

Lab Review Questions and Answers

Lab: Implementing remote management

Question and Answers

Question: What are some of the differences between Remote Desktop and Remote Assistance?

> **Answer:** Remote Assistance enables invitations to be sent to a remote user, and enables a remote user to interact with the session of a user who is signed-on. Remote Desktop connections require membership of the Administrators or Remote Desktop Users group.

Question: Which cmdlets can you run against a remote computer if the computer has not been configured to support remoting?

> **Answer:** You can run cmdlets that support the –*ComputerName* parameter.

Module 7

Managing storage

Contents:

Lesson 1
Overview of storage options

Contents:

Question and Answers

Question: What are the advantages of using virtual hard disks?

( ) Backup

( ) Performance

( ) Portability

( ) Availability

( ) Physical failures

Answer:

(√) Backup

( ) Performance

(√) Portability

( ) Availability

( ) Physical failures

Feedback: Advantages of using virtual hard disks include:

- Portability. Virtual hard disk files might be easier to move between systems, particularly when you use shared storage.
- Backup. A .vhd file represents a single file for backup purposes.

Lesson 2
Managing disks, partitions, and volumes

Contents:

Question and Answers

Question: What are the features of a GPT-initialized disk?

( ) Supports up to four partitions

( ) Supports up to 128 partitions

( ) Supports a maximum size of 2 TB

( ) Supports a maximum size of 18 exabytes

( ) Provides redundancy

> **Answer:**
>
> ( ) Supports up to four partitions
>
> (√) Supports up to 128 partitions
>
> ( ) Supports a maximum size of 2 TB
>
> (√) Supports a maximum size of 18 exabytes
>
> (√) Provides redundancy
>
> **Feedback:** MBR disks support only four partitions and 2-TB maximum size. The partition table is duplicated and therefore redundant on GPT disks.

Question: You can shrink a volume to the size of the used storage space on the volume.

( ) True

( ) False

> **Answer:**
>
> ( ) True
>
> (√) False
>
> **Feedback:** You can shrink a volume only to the size where unmovable files are stored.

Demonstration: Creating volumes

Demonstration Steps

Initialize disks

1. On **LON-CL2**, right-click **Start**, and then click **Windows PowerShell (Admin)**.

2. In the **Administrator: Windows PowerShell** window, type the following command, and then press Enter:

```
Get-Disk | Where partitionstyle -eq 'raw' | Initialize-Disk -PartitionStyle MBR
```

Create a simple volume by using Disk Management

1. In the **Ask me anything** box on the taskbar, type **diskmgmt.msc**, and then press Enter.

2. In Disk Management, right-click the unallocated part of **Disk 1**, and then click **New Simple Volume**.

3. In the **New Simple Volume Wizard** window, click **Next**.

4. On the **Specify Volume Size** page, type **5120**, and then click **Next**.

5. In the **Assign Drive Letter or Path** window, make sure that drive **E** is selected, and then click **Next**.

6. On the **Format partition** page, type **Simple** in the **Volume Label** text box, and then click **Next**.

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

8. If a Windows dialog box opens, click **Cancel**.

9. If File Explorer opens, close the window.

Create simple volume by using Windows PowerShell

1. Switch to the **Windows PowerShell** window.

2. In the **Administrator: Windows PowerShell** window, type the following command, and then press Enter:

```
Get-Disk -Number 2
```

3. In the **Administrator: Windows PowerShell** window, type the following command, and then press Enter:

```
New-Partition –Size 5350879232 –Disknumber 2| Format-Volume -Confirm:$false –
FileSystem NTFS –NewFileSystemLabel Simple2
```

4. In the **Administrator: Windows PowerShell** window, type the following command, and then press Enter:

```
Get-Partition –DiskNumber 2
```

Note the partition number that you just created, because you will use that in the next step.

5. In the **Administrator: Windows PowerShell** window, type the following command, replacing **<NumberFromBefore>** with the partition number you recorded in the preceding step, and then press Enter:

```
Set-Partition -DiskNumber 2 -PartitionNumber <NumberFromBefore> -NewDriveLetter F
```

6. If File Explorer opens, close the window.

Create a spanned volume

1. Switch to the **Disk Management** window.

2. Right-click the unallocated part of **Disk 2**, and then click **New Spanned Volume**.

3. In the **New Spanned Volume** wizard window, click **Next**.

4. On the **Select Disks** page, click **Disk 3**, and then click **Add**. In the **Selected** list, click each disk, and then in the **Select the amount of space in MB** text box, type **2048**. Click **Next**.

5. On the **Assign Drive Letter or Path** page, make sure that drive **G** is selected, and then click **Next**.

6. On the **Format partition** page, in the **Volume Label** text box, type **Spanned**, and then click **Next**.

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

8. In the **Disk Management** dialog box, click **Yes** to convert the disks to dynamic disks.

9. If File Explorer opens, close the window.

Create a striped volume

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

2. In the **New Striped Volume** wizard window, click **Next**.

3. On the **Select Disks** page, click **Disk 3**, and then click **Add**. Click **Next**.

4. On the **Assign Drive Letter or Path** page, make sure that drive **H** is selected, and then click **Next**.

5. On the **Format partition** page, in the **Volume Label** text box, type **Striped**, and then click **Next**.

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

7. If File Explorer opens, close the window.

Demonstration: Resizing a volume

Demonstration Steps

Shrink partition in Windows PowerShell

1. On **LON-CL2**, switch to Windows PowerShell.

2. In the **Windows PowerShell** command prompt window, type the following command, and press Enter:

```
Resize-Partition –DiskNumber 1 -PartitionNumber 1 –Size 3GB
```

Extend a partition by using Disk Management

1. Switch to the **Disk Management** window.

2. Right-click the **Simple (E:)** part of **Disk 1**, and then click **Extend Volume**. You might need to refresh the console to view the **Simple (E)** partition. (If necessary, close and reopen Disk Management).

3. In the **Extend Volume Wizard** window, click **Next**.

4. On the **Select Disks** page, click **Next**.

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

6. If you receive an error message indicating that the RPC server is not available, close the **Disk Management** console. Then, click **Start**, type **diskmgmt.msc**, and then press Enter. Repeat steps 2 to 5.

Lesson 3
Maintaining disks and volumes

Contents:

Question and Answers

Question: Which features in Windows 10 will work on both FAT-formatted and NTFS-formatted volumes?

( ) Storage

( ) Defragmenting disks

( ) Folder compression

( ) ZIP compression

( ) Disk quotas

> **Answer:**
>
> (√) Storage
>
> (√) Defragmenting disks
>
> ( ) Folder compression
>
> (√) ZIP compression
>
> ( ) Disk quotas
>
> **Feedback:** Folder compression and disk quotas will only work on NTFS-formatted volumes.

Question: By default, defragmentation runs on a monthly basis.

( ) True

( ) False

> **Answer:**
>
> ( ) True
>
> (√) False
>
> **Feedback:** By default, disks are defragmented weekly.

Demonstration: Using Storage

Demonstration Steps

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

2. Click **Start**, and then click the **Settings** icon.

3. In the **Settings** window, click **System**, and then click **Storage**.

4. On the **Storage** page, click **This PC (C:)**.

5. On the **Storage usage** page, click **Apps & games**.

6. On the **Apps & games** page, in the **Search this list** text box, type **Solitaire**, and then click the **Microsoft Solitaire Collection** app.

7. Click **Uninstall**. Click **Uninstall** in the window that opens.

8. Click the back arrow to return to **Storage usage**.

9. On the **Storage usage** page, click **Temporary files** in the category list.

10. On the **Temporary files** page, select the **Temporary files** check box.

11. Click **Remove files**.

12. Click the back arrow to return to **Storage usage**.

13. Click the back arrow to return to **Storage**.

14. On the **Storage** page, click **Change where new content is saved**.

15. Click the drop-down list for **New documents will save to**, and then select **Simple (E:)**.

16. Click **Apply**.

17. Click **File Explorer** on the taskbar.

18. In the **File Explorer** window, expand **This PC**, and then click **Simple (E:)**.

19. Double-click the **Administrator** folder.

20. Notice the **Documents** folder where new documents will be saved.

Demonstration: Performing disk maintenance

Demonstration Steps

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

2. In the **File Explorer** window, click **This PC**, right-click **Local Disk (C:)**, and then click **Properties**.

3. In the **Local Disk C: Properties** window, click the **Tools** tab, and then click **Optimize**.

4. In the **Optimize Drives** window, verify that **(C:)** is selected, and then click **Analyze**. Click **Optimize**. This should not take very long.

5. In the **Optimize Drives** window, click **Change settings**.

6. In the window that opens, click the **Frequency** drop-down list, and then select **Monthly**.

7. Clear the **Notify me if three consecutive scheduled runs are missed** check box, and then click **OK**.

8. In the **Optimize Drives** window, click **Close**.

9. In the **Local Disk C: Properties** window, click **OK**.

Demonstration: Compressing files and folders

Demonstration Steps

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

2. In **File Explorer**, navigate to the **C:\Users** folder.

3. Right-click the **Admin** folder, and then click **Properties**.

4. On the **General** tab, note the **Size on disk** in megabytes:_____

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

6. In the **Advanced Attributes** dialog box, click **Compress contents to save disk space**, and then click **OK**.

7. Click **Apply**, and then in the **Confirm Attribute Changes** dialog box, click **OK**.

8. If you see an **Access Denied** window, click **Continue**.

9. In the **Error Applying Attributes** window, click **Ignore All**.

10. After the compression finishes, note the **Size on disk** in megabytes:_____, and then click **OK**.

Demonstration: Configuring disk quotas

Demonstration Steps

Enable disk quotas

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

2. In the **File Explorer** window, right-click **Simple (E:)**, and then click **Properties**.

3. In the **Simple (E:) Properties** dialog box, click the **Quota** tab, and then select the **Enable quota management** check box.

4. In the **Simple (E:) Properties** dialog box, select the **Deny disk space to users exceeding quota limit** check box.

5. Click **Limit disk space to**, in the **Limit disk space to** text box, type **200**, and then in the **Set warning level to** text box, type **100**.

6. Select **MB** as the unit for both values.

7. In the **Simple (E:) Properties** dialog box, click **OK**.

8. If a **Disk Quota** dialog box opens, click **OK**.

9. Right-click **Start**, point to **Shut down or sign out**, and then click **Sign out**.

Create files

1. Sign in as the local user **.\Admin** with the password **Pa55w.rd**.

2. Click **Start**, type **cmd.exe**, right-click **Command Prompt**, and then click **Run as administrator**.

3. In the **User Account Control** dialog box, click **Yes**.

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

    ```
    E:
    ```

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

    ```
    MKDIR files
    ```

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

    ```
    CD files
    ```

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

    ```
    Fsutil file createnew file1.txt 104857600
    ```

8. In the command prompt window, type the following command, and then press Enter:

    ```
    Fsutil file createnew file2.txt 104857600
    ```

9. Right-click **Start**, point to **Shut down or sign out**, and then click **Sign out**.

Check disk quotas usage

1. Sign in as **Adatum\Administrator** with the password **Pa55w.rd**.

2. Click the **File Explorer** icon on the taskbar.

3. In the **File Explorer** window, right-click **Simple (E:)**, and then click **Properties**.

4. In the **Simple (E:) Properties** dialog box, click the **Quota** tab, and then click **Quota Entries**.

5. Notice the entry for **LON-CL2\Admin** for the disk space used.

6. Close the **Quota Entries for Simple (E:)** window.

7. Click **OK** to close the **Simple (E:) Properties** window**.**

Lesson 4
Managing Storage Spaces

Contents:

Question and Answers

Question: Which types of storage spaces can you create in Windows 10?

( ) Simple

( ) Advanced

( ) Two-way mirror

( ) Three-way mirror

( ) Parity

> **Answer:**
>
> (√) Simple
>
> ( ) Advanced
>
> (√) Two-way mirror
>
> (√) Three-way mirror
>
> (√) Parity
>
> **Feedback:** There is no such thing as an Advanced storage space.

Question: You need three disks to create a three-way mirror storage space.

( ) True

( ) False

> **Answer:**
>
> ( ) True
>
> (√) False
>
> **Feedback:** You need at least five disks to create a three-way mirror storage space.

Features of Storage Spaces

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

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

Demonstration: Configuring Storage Spaces

Demonstration Steps

Clear disks in Windows PowerShell

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

2. On the taskbar, in the **Ask me anything** box, type **Diskmgmt.msc** and press Enter.

3. In the **Disk Management** window, in the right side of **Disk 1**, right-click **Simple**, and then click **Delete Volume**.

4. In the **Delete simple volume** window, click **Yes**.

5. In the **Disk Management** dialog box, click **Yes**.

6. In the **Disk Management** window, in the right side of **Disk 2**, right-click **Simple2**, and then click **Delete Volume**.

7. In the **Delete simple volume** window, click **Yes**.

8. In the **Disk Management** window, in the right side of **Disk 2**, right-click **Spanned**, and then click **Delete Volume**.

9. In the **Delete spanned volume** window, click **Yes**.

10. In the **Disk Management** window, in the right side of **Disk 2**, right-click **Striped**, and then click **Delete Volume**.

11. In the **Delete striped volume** window, click **Yes**.

12. Right-click **Start**, and then click **Windows PowerShell (Admin)**.

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

```
Get-Disk | Clear-Disk -RemoveData
```

14. Press A to do this on all disks. Notice the error message "clear-disk: Operation not supported on a critical disk." This command does not reset the disk with the Windows installation.

15. Switch to the **Disk Management** window, and then verify that Disks 1, 2, and 3 are not initialized.

Create a storage space

1. In the **Ask me anything** box on the taskbar, type **storage spaces**, and then press Enter.

2. In the **Storage Spaces** window, click **Create a new pool and storage space**.

3. On the **Select drives to create a storage pool** page, verify that Disks 1, 2, and 3 are selected. Click **Create pool**.

4. On the **Enter a name, resiliency type, and size for the storage space** page, click the **Resiliency type** drop-down list, and then select **Parity**.

5. Click **Create storage space**.

6. If necessary, open File Explorer and click **This PC**.

   Notice that the size of **Storage Space (E:)** is 15.8 GB.

7. Close the **File Explorer** window.

Modify an existing storage space

1. In **Storage Spaces**, on the **Manage Storage Spaces** page, click **Change**.

2. On the **Enter a new name and size for the storage space** page, change the **Storage space size** to **50 GB**.

   Notice the information text, which states that you can add more drives when the capacity is low.

3. Click **Change storage space**.

4. Click **File Explorer** on the taskbar.

5. Click **This PC**.

   Notice that the size of **Storage Space (E:)** is now 49.8 GB.

Lesson 5
Implementing and managing OneDrive

Contents:

Question and Answers

Question: Which features do you get with OneDrive in Windows 10?

( ) 5 GB free storage

( ) Synchronization of selected folders

( ) Automatic synchronization of all folders

( ) Built-in universal app

( ) Manually installed app to get OneDrive integration

       Answer:

       (√) 5 GB free storage

       (√) Synchronization of selected folders

       ( ) Automatic synchronization of all folders

       (√) Built-in universal app

       ( ) Manually installed app to get OneDrive integration

Lesson 6
Working with virtual hard disks

Contents:

Question and Answers

Question: When might you use virtual hard disks in your environment?

Answer: Answers might vary based on students' experience and organizational needs.

Module Review and Takeaways

Question: You are implementing 64-bit Windows 10 and need to partition the disk to support 25 volumes, some of which will be larger than 2 terabytes (TB). 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 TB. Additionally, you can boot a computer with 64-bit Windows 10 installed from a GPT disk.

Question: Can administrators manage the content stored in both OneDrive and OneDrive for Business, provided the computer is a domain member?

>**Answer:** No, administrators cannot manage content in OneDrive. Because OneDrive is a consumer-based service, it does not allow any delegated management.

Lab Review Questions and Answers

Lab: Managing storage

Question and Answers

Question: When would you use a spanned volume instead of a simple volume? Is there a better solution in Windows 10?

> **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 an operating system. A better solution in Windows 10 could be to use Storage Spaces.

Module 8

Managing files and resources

Contents:

Lesson 1
Overview of file systems

Contents:

Question and Answers

Question: Which two of the following file systems can you use on a 100-GB simple volume that you created on a single disk?

(   ) FAT

(   ) FAT32

(   ) exFAT

(   ) NTFS

(   ) ReFS

> **Answer:**
>
> (   ) FAT
>
> (   ) FAT32
>
> (√) exFAT
>
> (√) NTFS
>
> (   ) ReFS
>
> **Feedback:** Only exFAT, NTFS, and ReFS support large enough partitions. However, Windows 10 has limited support for ReFS. You can only use it in storage spaces.

Question: You can convert a partition with the NTFS file system to the FAT32 file system.

(   ) True

(   ) False

> **Answer:**
>
> (   ) True
>
> (√) False
>
> **Feedback:** You cannot convert from the NTFS file system back to FAT or FAT32. You must format the volume for FAT32.

Lesson 2
Configuring and managing file access

Contents:

Question and Answers

Question: On which two file systems can you assign permissions in Windows 10?

( ) FAT

( ) FAT32

( ) exFAT

( ) NTFS

( ) ReFS

> **Answer:**
>
> ( ) FAT
>
> ( ) FAT32
>
> ( ) exFAT
>
> (√) NTFS
>
> (√) ReFS
>
> **Feedback:** In Windows 10, you cannot assign permissions on the FAT file system.

Question: You can modify inherited permissions on a file without disabling the inheritance.

( ) True

( ) False

> **Answer:**
>
> ( ) True
>
> (√) False
>
> **Feedback:** You can modify only explicit permissions set on the file. To modify inherited permissions, you must disable the inheritance or modify the permissions at the higher level, on the folder on which they were set.

Demonstration: Securing files and folders with file permissions

Demonstration Steps

1. On **LON-CL1**, on the taskbar, click **File Explorer**.

2. In File Explorer, in the navigation pane, under **This PC**, click **Local Disk (C:)**.

3. In the details pane, right-click the empty space, point to **New**, and then click **Folder**.

4. Type **Data**, and then press Enter.

5. Right-click **Data**, and then click **Properties**.

6. In the **Data Properties** dialog box, click the **Security** tab, and then click **Edit**. Explain why the check boxes in the **Permissions for Authenticated Users** section are dimmed.

7. In the **Permissions for Data** dialog box, verify that **Authenticated Users** is selected in the **Group or user names** section, and then click **Remove**. Explain that you cannot remove **Authenticated Users** because this is an inherited permission. Click **OK**, and then click **Add**.

8. In the **Select Users, Computers, Service Accounts, or Groups** dialog box, in the **Enter the object names to select (examples)** text box, type **managers**, and then click **OK**. Explain why permissions for **Managers** are not dimmed.

9. In the **Permissions for Managers** section, clear the **Read & execute** and **List folder contents** check boxes, and then click **OK**.

10. In the **Data Properties** dialog box, click **Advanced**.

11. In the **Advanced Security Settings for Data** dialog box, in the **Permission entries** section, click **Managers**, and then click **Edit**.

12. In **Permission Entry for Data**, in the **Basic permissions** section, verify that only the **Read** check box is selected.

13. Click **Show advanced permissions**, and then explain that the basic Read permission contains multiple advanced permissions. Click **OK** three times.

14. In File Explorer, in the details pane, double-click **Data**.

15. In the details pane, right-click the empty space, point to **New**, and then click **Text Document**.

16. Type **File1**, and press Enter.

17. Right-click **File1.txt**, click **Properties**, click the **Security** tab, and then click **Advanced**.

18. In the **Advanced Security Settings for File1.txt** dialog box, verify that the permissions for **Managers** are inherited from **C:\Data** and all other permissions are inherited from **C:**.

19. Click the entry for **Managers**, click **Remove**, note the message, and then click **OK**.

20. In the **Advanced Security Settings for File1.txt** dialog box, click **Disable inheritance**. Review the options in the **Block Inheritance** dialog box, and then click **Convert inherited permissions into explicit permissions on this object**.

21. In the **Advanced Security Settings for File1.txt** dialog box, verify that all permissions entries are set explicitly on **File1.txt**, because their permission inheritance is set to **None**.

22. Verify that **Managers** is selected, click **Remove**, and then explain that now you can modify permissions, because they are no longer inherited. Click **OK** twice.

Lesson 3
Managing shared folders

Contents:

Question and Answers

Question: You can configure advanced permissions for a shared folder.

( ) True

( ) False

> **Answer:**
>
> ( ) True
>
> (√) False
>
> **Feedback:** For a shared folder, you can configure only the Read, Change, or Full Control permission. You can configure advanced permissions only at the file-system level, not at the share-folder level.

Question: You cannot configure access-based enumeration for shares on a Windows 10 computer.

( ) True

( ) False

> **Answer:**
>
> ( ) True
>
> (√) False
>
> **Feedback:** You can configure access-based enumeration for Windows 10 shares by using the **Set-SmbShare** Windows PowerShell cmdlet.

Demonstration: Sharing folders

Demonstration Steps

1. On **LON-CL1**, in File Explorer, in the navigation pane, click **Local Disk (C:)**.

2. In the details pane, right-click the **Data** folder, select **Properties**, select the **Security** tab, and then point out that **Managers** have permissions on the **C:\Data** folder.

3. Click the **Sharing** tab, note that the folder is not shared, and then click **OK**.

4. In the details pane, right-click **Data** folder, point to **Give access to**, and then click **Specific people**.

5. In the **File Sharing** dialog box, select **Managers**, click **Custom** in the **Permission Level** column, and then click **Remove**.

6. Next to the **Add** button, click the drop-down arrow, and then click **Find people**.

7. In the **Select Users or Groups** dialog box, in the **Enter the object names to select (examples)** text box, type **IT**, and then click **OK**.

8. Verify that **IT** is added and selected. Click **Read** in the **Permission Level** column, click **Read/Write**, click **Share**, and then click **Done**.

9. In File Explorer, in the navigation pane, right-click **Data**, and then select **Properties**.

10. Click the **Security** tab, point out that **Managers** no longer have permissions on the folder, but **IT** does, and then click the **Sharing** tab.

11. In the **Data Properties** dialog box, verify that the folder is shared, and then click **Advanced Sharing**.

12. In the **Advanced Sharing** dialog box, note that the share name is **Data**, which is the same as the folder name.

13. In the **Limit the number of simultaneous users to** text box, type **5**, and then click **Permissions**.

14. In the **Permissions for Data** dialog box, point out that **Everyone** and **Administrators** have Full Control permissions to the share, click **OK**, and then click **Apply**.

15. In the **Advanced Sharing** dialog box, click **Add**, in the **Share name** text box, type **IT Data**, and then click **Permissions**.

16. Select the **Full Control** check box in the **Allow** column, click **OK** three times, and then click **Close**.

17. In File Explorer, click the arrow in the **Address** bar, type **\\LON-CL1**, and then press Enter. Point out that you can see the **Data** and **IT Data** shares in the details pane.

18. Double-click **IT Data**, and then point out that you can see **File1.txt**, which you created in the previous demonstration.

19. Right-click **Start**, and then click **Computer Management**.

20. In **Computer Management**, in the navigation pane, expand **Shared Folders**.

21. Click **Shares**, and then point out that in the details pane, you can see the **Data** and **IT Data** shares. Close **Computer Management**.

22. Right-click **Start**, and then click **Windows PowerShell (Admin)**.

23. In Windows PowerShell, type **Get-SmbShare**, and then press Enter. Point out that shares on **LON-CL1** are listed, including **Data** and **IT Data**.

24. Close the **Windows PowerShell** window.

25. Sign out of **LON-CL1**.

Lesson 4
Work Folders

Contents:

Question and Answers

Question: You can use Work Folders on a Windows 10 device only if it is a member of AD DS.

( ) True

( ) False

> **Answer:**
>
> ( ) True
>
> (√) False
>
> **Feedback:** You can use Work Folders regardless of the domain membership of the Windows 10 device.

Question: A user can have a single Work Folder in Windows 10.

( ) True

( ) False

> **Answer:**
>
> (√) True
>
> ( ) False

Demonstration: Enabling Work Folders

Demonstration Steps

1. On **LON-CL1**, on the taskbar, click **File Explorer**.

2. In File Explorer, in the navigation pane, click **Work Folders**.

3. Right-click in the details pane, point to **New**, click **Text Document**, type **On LON-CL1**, and then press Enter.

> 📋 **Note:** If you do not see **Work Folders** in File Explorer, sign out and sign back in to **LON-CL1**, and then repeat steps 1 through 3.

4. On **LON-CL4**, click **Start**, type **Control Panel**, and then press Enter.

5. In Control Panel, in the **Search Control Panel** text box, type **work**, and then click **Work Folders**.

6. On the **Manage Work Folders** page, click **Set up Work Folders**, and then on the **Enter your work email address** page, click **Enter a Work Folders URL instead**.

7. On the **Enter a Work Folders URL** page, in the **Work Folders URL** text box, type **https://lon-dc1.adatum.com**, and then click **Next**.

8. In the **Windows Security** dialog box, in the **User name** text box, type **adatum\Annie**, in the **Password** text box, type **Pa55w.rd**, and then click **OK**.

9. On the **Introducing Work Folders** page, review the local Work Folders location, and then click **Next**.

10. On the **Security policies** page, select the **I accept these policies on my PC** check box, and then click **Set up Work Folders**.

11. On the **Work Folders has started syncing with this PC** page, click **Close**.

12. In the **Work Folders** window, verify that the **On LON-CL1.txt** file displays.

13. Sign out of **LON-CL4**.

Lesson 5
Managing printers

Contents:

Question and Answers

Question: Which tool would you use to manage printers on multiple Windows 10–based computers in an Active Directory environment?

( ) Device Manager

( ) Printers & Scanners

( ) Print Management

( ) Computer Management

( ) Connected Devices

> **Answer:**
>
> ( ) Device Manager
>
> ( ) Printers & Scanners
>
> (√) Print Management
>
> ( ) Computer Management
>
> ( ) Connected Devices

Question: You can add multiple printers in Windows 10 for a single printing device that connects to your computer.

( ) True

( ) False

> **Answer:**
>
> (√) True
>
> ( ) False

Demonstration: Installing and sharing a printer

Demonstration Steps

1. On **LON-CL1**, sign in as **Adatum\Administrator**.

2. Click **Start**, type **Control Panel**, and then press Enter.

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

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

5. In the **Add a device** dialog box, 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, verify that **Use an existing port** is selected, and then click **Next**.

8. On the **Install the printer driver** page, in the **Manufacturer** list, select **Microsoft**. In the **Printers** list, select **Microsoft PCL6 Class Driver**, and then click **Next**.

9. On the **Type a printer name** page, in the **Printer name** text box, type **Managers Printer**, and then click **Next**.

10. On the **Printer Sharing** page, click **Next**, and then click **Finish**.

11. In **Devices and Printers**, right-click **Managers Printer**, click **Printer properties**, and then click the **Security** tab**.**

12. In the **Managers Printer Properties** dialog box, verify that **Everyone** is selected, and then click **Remove**.

13. Click **Add**, in the **Enter the object names to select (examples)** dialog box, type **Marketing**, and then click **OK**.

14. In the **Permissions for Marketing** section, verify that the **Print** check box in the **Allow** column is selected, and then click **OK**.

Module Review and Takeaways

Question: On which objects can you set file-level permissions?

Answer: You can set file-level permissions on volumes, folders, and files.

Question: Robin recently created a spreadsheet and assigned it file permissions that restricted file access to her alone. Following the system reorganization, the file moved to a folder on a different NTFS volume, and Robin discovered that other users could open the spreadsheet. What is the probable cause of this situation?

Answer: Because the spreadsheet moved across partitions, the moved file inherited file permissions from the new parent. When the file moved, it lost all explicit permissions that Robin configured.

Question: Can you access the Work Folders content on a computer without network connectivity?

Answer: A computer that supports Work Folders creates a local copy of the Work Folders content. If network connectivity is not available, you will still be able to access and modify the local copy. When network connectivity is available again, local changes will sync transparently with the Work Folder content on a file server.

Lab Review Questions and Answers

Lab A: Creating, securing, and sharing a folder

Question and Answers

Question: When you share a folder, what is the difference between using **Network File and Folder Sharing** and using the **Advanced Sharing** feature?

> **Answer:** If you are sharing a folder by using **Network File and Folder Sharing**, you will be modifying local file permissions and share permissions. You will configure local file permissions on the **File Sharing** page, while share permissions will allow full control to administrators and the **Everyone** group. If you are sharing a folder by using the **Advanced Sharing** feature, local file permissions do not change. The **Advanced Sharing** feature only sets share permissions.

Question: Can you view effective access permissions on NTFS and FAT32 volumes?

> **Answer:** You can view effective access permissions on the **Advanced Security Settings** page for the file or folder on an NTFS volume or for the entire NTFS volume. You can access this page on the **Security** tab in the volume, folder, or file properties dialog box. FAT32 volumes do not support security, so you cannot access effective access permission information on a FAT32 volume. Therefore, because you cannot configure security on a FAT32 volume, everyone has unlimited access to that volume's content.

Lab B: Implementing Work Folders

Question and Answers

Question: Can a user access the same Work Folders from domain-joined devices and workgroup devices?

> **Answer:** Yes. Users can access the same Work Folders from all devices, regardless of their domain membership. A user's user account is the most important factor. If users access Work Folders from their devices by using the same domain credentials, they will access the same content.

Question: Can the same user connect to multiple Work Folders?

> **Answer:** No. Although you can grant the user sync access to multiple sync shares, the user can connect only to a single Work Folder.

Lab C: Managing printers

Question and Answers

Question: How can you list printers with a connection to a computer?

> **Answer:** You can list printers with a connection to a computer in several different ways. You can use the Devices and Printers feature, the **Print Management** console, or the **Get-Printer** Windows PowerShell cmdlet.

Question: By default, who can print on a newly created printer?

> **Answer:** By default, everyone has the Print permission on a newly created printer, which means that anyone can print on that printer.

Question: How can you determine which printer is the default printer?

> **Answer:** When you view printers in **Devices and Printers**, the default printer has a green check mark next to its name.

Module 9

Deploying and managing apps

Contents:

Lesson 2
The Microsoft Store and Microsoft Store for Business

Contents:

Question and Answers

Question: To install Microsoft Store apps by using sideloading, you must first configure GPOs to enable the Windows 10 sideloading feature.

( ) True

( ) False

> **Answer:**
>
> ( ) True
>
> (√) False
>
> **Feedback:** In Windows 8.1, it is necessary to enable sideloading by using registry edits or by using GPOs. However, in Windows 10 you can enable this feature through the device settings.

Demonstration: Sideloading Microsoft Store apps

Demonstration Steps

Enable sideloading

1. On **LON-CL1**, sign in as **.\Admin** with the password **Pa55w.rd**.

2. In the notification area, click **Notifications**, and then click **All settings**.

3. Click **Update & Security**.

4. On the **For developers** tab, in the **Use developer features** section, click **Sideload apps**.

5. In the **Use developer features** dialog box, click **Yes**.

6. Close **Settings**.

Install the root certificate

1. On **LON-CL1**, click File Explorer on the taskbar.

2. Navigate to **\\lon-dc1\apps**.

3. In the **Windows Security** dialog box, enter the user name **Administrator** and the password **Pa55w.rd**, and then click **OK**.

4. Right-click **LeXProductsGrid81_1.1.0.2_AnyCPU.cer**, and then click **Install Certificate**.

5. On the **Certificate Import Wizard** page, click **Local Machine**, and then click **Next**.

6. In the **User Account Control** dialog box, click **Yes**.

7. On the **Certificate Store** page, click **Place all certificates in the following store**, click **Browse**, click **Trusted Root Certification Authorities**, click **OK**, click **Next**, and then click **Finish**.

8. In the **Certificate Import Wizard** dialog box, confirm that the import was successful, and then click **OK**.

9. Sign out of **LON-CL1**.

Install a Microsoft Store app

1. Sign in to **LON-CL1** as **Adatum\Claire** with the password **Pa55w.rd**.

2. Right-click **Start**, and then click **Windows PowerShell**.

3. To install the package, at the Windows PowerShell command prompt, type the following command, and then press Enter:

```
add-appxpackage \\lon-dc1\apps\app1.appx
```

4. Click **Start**, scroll down, and then click **TestAppTKL1**.

5. Close the app.

Remove an installed Microsoft Store app

1. Click **Start**, scroll down, right-click **TestAppTKL1** tile, and then click **Uninstall**.

2. In the **This app and its related info will be uninstalled** dialog box, click **Uninstall**.

3. Close all open windows.

4. Sign out of **LON-CL1**.

Lesson 3
Automating app deployment

Contents:

Question and Answers

Question: Which of the following statements about installing apps in Windows 10 is true? (Choose all that apply.)

(   ) Desktop apps are installed with either .exe or .appx installer files.

(   ) Microsoft Store apps are installed with .appx files.

(   ) RemoteApp apps allow users of Windows RT computers to run apps that are designed for 64-bit versions of Windows 10.

(   ) Desktop apps must be signed digitally.

(   ) Microsoft Store apps must be signed digitally.

> **Answer:**
>
> (   ) Desktop apps are installed with either .exe or .appx installer files.
>
> (√) Microsoft Store apps are installed with .appx files.
>
> (√) RemoteApp apps allow users of Windows RT computers to run apps that are designed for 64-bit versions of Windows 10.
>
> (   ) Desktop apps must be signed digitally.
>
> (√) Microsoft Store apps must be signed digitally.

Question: What are the different methods that you can use to deploy software via Group Policy? (Select all that apply.)

(   ) Assign to a computer

(   ) Assign to a user

(   ) Publish to a user by using Programs and Features

(   ) Publish to a computer by using Programs and Features

(   ) Publish to a user by using Extension activation

> **Answer:**
>
> (√) Assign to a computer
>
> (√) Assign to a user
>
> (√) Publish to a user by using Programs and Features
>
> (   ) Publish to a computer by using Programs and Features
>
> (√) Publish to a user by using Extension activation
>
> **Feedback:** You can use four different methods to deploy software via Group Policy:
>
> - Assign to a computer.
> - Assign to a user.
> - Publish to a user by using Program and Features.
> - Publish to a user by using Extension activation.
>
> You cannot publish software to a computer.

Demonstration: Deploying a universal app by using Windows Configuration Designer

Demonstration Steps

Create a package

1. On **LON-CL1**, sign in as **Adatum\Administrator** with the password **Pa55w.rd**.

2. Click **Start**, expand **Windows Kits**, and then click **Windows Imaging and Configuration Designer**.

3. In Windows Imaging and Configuration Designer, on the **Start page**, click **Advanced provisioning**.

4. In the **New project** wizard, on the **Enter project details** page, in the **Name** box, type **App1**, and then click **Next**.

5. On the **Choose which settings to view and configure** page, click **All Windows desktop editions**, and then click **Next**.

6. On the **Import a provisioning package (optional)** page, click **Finish**.

Configure the app

1. On **LON-CL1**, in Windows Imaging and Configuration Designer, on the **App1** page, in the **View** list, click **Common IT Pro settings**.

2. Expand **Runtime settings**.

3. In the navigation pane, expand **UniversalAppInstall**, and then click **DeviceContextApp**.

4. In the details pane, in the **PackageFamilyName** box, type **App1**, and then click **Add**.

5. In the navigation pane, click **PackageFamilyName: App1**.

6. In the details pane, click **Browse**.

7. In the **Open** dialog box, in the **File name** box, type **\\lon-dc1\apps** and then press Enter.

8. In the **Open** dialog box, double-click **App1.appx**.

9. On the menu, click **File**, and then click **Save**.

10. Click **OK**.

Build the package

1. On **LON-CL1**, in Windows Imaging and Configuration Designer, on the menu, click **Export**, and then click **Provisioning package**.

2. In the **Build** wizard, on the **Describe the provisioning package** page, click **Next**.

3. On the **Select security details for the provisioning package** page, click **Next**.

4. On the **Select where to save the provisioning package** page, click **Next**.

5. On the **Build the provisioning package** page, click **Build**.

5. On the **All done!** page, click the **Output location** link. These are the customization files.

6. In Windows Imaging and Configuration Designer, on the **All done!** page, click **Finish**.Close Windows Configuration Designer.

Lesson 4
Configuring web browsers

Contents:

Question and Answers

Discussion: Which browser should you use?

Question: How well suited is Microsoft Edge to your environment?

> **Answer:** Answers will vary based on the students' own experiences and the web-based apps that users are utilizing within their organizations.

Demonstration: Configuring and using Internet Explorer 11

Demonstration Steps

Configure Compatibility View

1. Switch to **LON-CL1**.

2. Sign in to **LON-CL1** as **Adatum\Claire** with the password **Pa55w.rd**.

3. Click **Start**, scroll down, and then click **Windows Accessories**.

4. Right-click **Internet Explorer**, point to **More**, and then click **Pin to taskbar**.

5. On the taskbar, click **Internet Explorer**.

📄   **Note:** If you receive a prompt, click **Use recommended security and compatibility settings**, and then click **OK**.

6. In the address bar, type **http://LON-DC1**, and then press Enter.

7. Right-click the home symbol, and then click **Menu bar**.

8. On the menu bar, click **Tools**, and then click **Compatibility View settings**.

9. In the **Compatibility View Settings** dialog box, click **Add** to add the LON-DC1 website to Compatibility View, and then click **Close**.

Delete the browsing history

1. In Internet Explorer, click the down arrow next to the address bar to confirm that the address that you typed is stored.

2. In Internet Explorer, on the **Tools** menu, click **Internet options**.

3. Click the **General** tab. Under **Browsing history**, click **Delete**.

4. In the **Delete browsing history** dialog box, clear the **Preserve Favorites website data** check box, select the **Temporary Internet files and website files**, **Cookies and website data**, and **History** check boxes, and then click **Delete**.

5. Click **OK** to close the **Internet Options** dialog box.

6. Confirm that there are no addresses stored in the address bar by clicking the down arrow next to the address bar.

📄   **Note:** You can ignore Bing.com.

Configure InPrivate Browsing

1. On the **Tools** menu, click **InPrivate Browsing**.

2. In the address bar, type **http://LON-DC1**, and then press Enter.

3. Confirm that the address that you entered is not stored by clicking the down arrow next to the address bar.

📝   **Note:** You can ignore Bing.com

4. Close the **InPrivate Browsing** window.

View the add-on management interface

1. On the **Tools** menu, click **Manage add-ons**.

2. In the left navigation pane, click **Search Providers**.

3. In the right navigation pane, click **Bing**.

4. In the left navigation pane, click **Accelerators**.

5. In the left navigation pane, click **Tracking Protection**.

6. Click **Close**.

Download a file

1. In the address bar, type **http://LON-DC1**, and then press Enter.

2. In the browser window, click **Download Current Projects**.

3. In the **Internet Explorer** dialog box, click **Save**.

4. In the banner, click **View downloads**.

5. Click **Open**.

6. The file opens in Microsoft Excel.

📝   **Note:** If you receive a prompt from Office, in the **Microsoft Office Activation Wizard** dialog box, click **Close**.

7. Close Excel, and then close Internet Explorer.

Demonstration: Configuring and using Microsoft Edge

Demonstration Steps

Open a webpage

1. On **LON-CL1**, on the taskbar, click **Microsoft Edge**.

2. In the **Where to next** text box, type **http://lon-dc1**, and then press Enter.

Pin a tab

1. In Microsoft Edge, right-click the **A Datum Intranet** tab, and then click **Pin**.

2. Close and reopen Microsoft Edge. Verify that the pinned tab still displays.

Load a webpage that requires an ActiveX control

1. In Microsoft Edge, on the **A Datum Intranet Home Page**, click **Current Projects**. A new tab opens with columns displayed for **Project** and **Project Lead**. No data displays.

2. Click the **More actions** button (**…**).

3. Click **Open with Internet Explorer**. The same webpage displays, but with the data extracted from the comma-separated value (CSV) file and displayed in the appropriate columns.

4. Close Internet Explorer.

Configure settings

1. In Microsoft Edge, click **More actions**, and then click **Settings**.

2. In the Choose a theme list, click **Dark**.

3. Click **View advanced settings**.

4. Scroll down the list of options, and then highlight the **Help protect me from malicious sites and downloads with SmartScreen Filter**. Do not change the setting.

5. Click **<< Advanced settings**.

6. Click outside the **SETTINGS** pane to close **SETTINGS**.

Download a file

1. In Microsoft Edge, on the **A Datum Intranet** tab, click **Download Current Projects**.

2. In the banner, click **Save**.

3. In the banner, click **Open**.

4. The file opens in Excel.

📝   **Note:** If you receive a prompt from Office, in the **Microsoft Office Activation Wizard** dialog box, click **Close**.

5. Close Excel.

6. Switch to Microsoft Edge.

Make a web note

1. In the notification area, click **Notifications**, and then click **Tablet mode**.

2. In Microsoft Edge, on the **A Datum Intranet** tab, on the menu bar, click **Add Notes**.

3. On the webpage, draw a square.

4. Click the **Highlighter** tool.

5. Highlight two of the hyperlinks on the webpage.

6. Click **Add a note**, and then click the cursor somewhere on the webpage.

7. Type **This is my note**, and then, on the menu, click **Save Web Note**.

8. Click **Favorites**, and then click **Save**.

9. Click **Exit**.

10. In Microsoft Edge, click **Hub**, and then click **Favorites**.

11. Click the **Web Notes – A Datum Intranet** link. Your web note opens.

12. In the notification area, click **Notifications**, and then click **Tablet mode**.

13. Close Microsoft Edge.

Module Review and Takeaways

Question: What does Internet Explorer 11 display when a browser detects that a website does not adhere to HTML5 or CSS3 standards?

> **Answer:** Internet Explorer 11 will display the webpage in compatibility mode, which enables the browser to continue to attempt to display the webpage correctly.

Question: You are installing apps from the Microsoft Store on a tablet that has a small internal hard disk. However, you have added a micro SD card with 64 GB of space. How can you utilize this storage for your apps?

> **Answer:** Use Windows 10 to move apps to external storage by performing the following steps: open **Settings**, select **System**, and then tap **Apps & features**. Your apps are listed. Tap each app that you want to move, and then tap **Move**.

Question: You want to know which apps you have previously installed or purchased on your Windows devices, regardless of whether they are installed on your current device. How can you access this information in Windows 10?

> **Answer:** You can access a list of all your apps from the Microsoft Store **Settings** menu by tapping **My Library**. A list of your apps displays. These apps might not be installed currently on this device, but you have previously installed them on one of the devices associated with your Microsoft account.

Lab Review Questions and Answers

Lab A: Deploying and managing Microsoft Store apps

Question and Answers

Question: In the lab, you used a self-signed certificate for validating the source of the app that you wanted to sideload. What is wrong with using a self-signed certificate?

> **Answer:** When you use a self-signed certificate, you cannot verify the integrity of the software vendor that produced the app that you intend to install. This is not a problem if you are testing internally developed apps, but it is a security concern if you are using third-party apps. In production environments, only install apps from trusted sources.

Lab B: Deploying apps with Windows Configuration Designer

Question and Answers

Question: Why was it necessary to deploy a certificate with the app?

> **Answer:** This step was necessary because the app is a Microsoft Store app and is from an untrusted source. The certificate provides the necessary trust information.

Lab C: Configuring Microsoft Edge

Question and Answers

Question: In the lab, you were unable to get complete functionality from the A. Datum Intranet website by using Microsoft Edge. What was the reason? What was the solution?

> **Answer:** The A. Datum Intranet site uses an ActiveX control for tabulating data retrieved from a CSV file. ActiveX controls do not work in Microsoft Edge. You were able to view the website correctly by switching to Internet Explorer to view the appropriate page.

Module 10

Securing Windows 10

Contents:

Lesson 1
Managing user accounts

Contents:

Demonstration: Managing user accounts

Demonstration Steps

Create a local user account

1. Switch to **LON-CL1**.

2. On **LON-CL1**, sign in as **.\Admin** with the password **Pa55w.rd**.

3. Click **Start**, and then click **Settings**.

4. In **Settings**, click **Accounts**.

5. In **Accounts**, click the **Other people** tab, and then click **Add someone else to this PC**.

6. On the **Create an account for this PC** page, in the **Who's going to use this PC?** text box, type **Claire**.

7. In the **Enter password** and **Re-enter password** text boxes, type **Pa55w.rd**.

8. In the **Password hint** text box, type **Usual**, and then click **Next**.

9. Right-click **Start**, and then click **Computer Management**.

10. In **Computer Management**, expand **Local Users and Groups**, and then click **Users**.

11. In the details pane, double-click **Claire**.

12. In the **Claire Properties** dialog box, in the **Full name** box, type **Claire Roberson**, and then click **OK**.

13. Sign out.

14. Sign in as **.\Claire** with the password **Pa55w.rd**. This is a local account.

15. Sign out.

Delete a domain user account

1. Switch to **LON-DC1**.

2. On LON-DC1, in **Server Manager**, click **Tools**.

3. Click **Active Directory Administrative Center**.

4. In **Active Directory Administrative Center**, click **Adatum (local)**, and then double-click **Managers**.

5. In Managers, right-click **Holly Spencer**, and then click **Delete**.

6. In the **Delete Confirmation** dialog box, click **Yes**.

Create a new domain user account

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

2. In the **Create User** dialog box, in the **Full name** text box, type **Holly Spencer**.

3. In **User UPN logon** text box, type **Holly**.

4. In **Password** and **Confirm password** text boxes, type **Pa55w.rd**, and then click **OK**.

Move the domain user account

1. Right-click **Holly Spencer**, and then click **Move**.

2. Click the **IT** organizational unit (OU), and then click **OK**.

3. In the navigation pane, click **Adatum (local)**.

4. In the results pane, double-click **IT**.

5. Verify that Holly's account is listed.

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

7. Sign in as **Adatum\Holly** with the password **Pa55w.rd**.

8. At the prompt to change the user's password, click **OK**, and in the **New password** and **Confirm password** boxes, type **Pa55w.rd2**, and then press Enter.

9. Click **OK**, and then click **Sign in**.

10. Sign out.

Lesson 2
Configuring UAC

Contents:

Question and Answers

Categorize Activity

Question: Categorize each item below.

	Items
1	Change the desktop background for the current user
2	Install a driver for a device, such as a digital camera driver
3	Install updates from Windows Update
4	Configure accessibility options
5	Configure Automatic Updates
6	Install drivers from Windows Update or those that the operating system includes
7	Use Remote Desktop to connect to another computer
8	Configure Remote Desktop access
9	View Windows settings
10	Establish and configure a wireless connection
11	Open Windows Firewall in Control Panel
12	Pair Bluetooth devices with the computer
13	Configure battery-power options
14	Schedule Automated Tasks
15	Reset the network adapter
16	Restore a user's backup files
17	Restore system-backup files
18	Perform network-repair tasks

Category 1		Category 2		Category 3
Tasks that a standard user can perform		Tasks that require elevation to an administrator account		Tasks that the default User Account Control (UAC) setting allows a standard user to perform without receiving a UAC prompt

Answer:

Category 1		Category 2		Category 3
Tasks that a standard user can perform		Tasks that require elevation to an administrator account		Tasks that the default User Account Control (UAC) setting allows a standard user to perform without receiving a UAC prompt
Change the desktop background for the current user Configure accessibility options Use Remote Desktop to connect to another computer Establish and configure a wireless connection Configure battery-power options Restore a user's backup files		Install a driver for a device, such as a digital camera driver Configure Automatic Updates Configure Remote Desktop access Open Windows Firewall in Control Panel Schedule Automated Tasks Restore system-backup files		Install updates from Windows Update Install drivers from Windows Update or those that the operating system includes View Windows settings Pair Bluetooth devices with the computer Reset the network adapter Perform network-repair tasks

Question: Which of the following is the default setting for the UAC elevation prompt?

( ) Never notify me

( ) Notify me only when apps try to make changes to my computer (do not dim my desktop)

( ) Notify me only when apps try to make changes to my computer (default)

( ) Always notify me

> **Answer:**
>
> ( ) Never notify me
>
> ( ) Notify me only when apps try to make changes to my computer (do not dim my desktop)
>
> (√) Notify me only when apps try to make changes to my computer (default)
>
> ( ) Always notify me
>
> **Feedback:** The default User Account Control setting is **Notify me only when apps try to make changes to my computer (default)**. When you configure this setting, UAC notifies a user when apps attempt to make changes to computer settings.

Demonstration: Configuring UAC

Demonstration Steps

View the current UAC settings

1. Sign in to **LON-CL1** as **Adatum\Administrator** with the password **Pa55w.rd**.

2. In the **Ask me anything** box on the taskbar, type **gpedit.msc**, and then press Enter.

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

4. Scroll down and review the options that start **User Account Control**.

Configure the 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, in the drop-down list, click **Automatically deny elevation requests**, and then click **OK**.

3. Close **Local Group Policy Editor**.

4. Sign out.

Test the UAC settings

1. Sign in to **LON-CL1** as **Adatum\Holly** with the password **Pa55w.rd2**.

2. In the **Ask me anything** box on the taskbar, type **gpedit.msc**, and then press Enter.

3. The Windows operating system does not display the **Local Group Policy Editor** snap-in. Instead, you see a **Group Policy Error** dialog box that states **You do not have permission to perform this operation**.

4. Close **Local Group Policy Editor** and then sign out.

Reconfigure the UAC settings

1. Sign in to **LON-CL1** as **Adatum\Administrator** with the password **Pa55w.rd**.

2. In the **Ask me anything** box on the taskbar, type **gpedit.msc**, and then press Enter.

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

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

5. In the **User Account Control: Behavior of the elevation prompt for standard users** dialog box, in the drop-down list, click **Prompt for credentials**, and then click **OK**.

6. Close **Local Group Policy Editor**.

7. Sign out.

Test the UAC settings again

1. Sign in to **LON-CL1** as **Adatum\Holly** with the password **Pa55w.rd2**.

2. Click **Start**, type **cmd.exe**, right-click **Command Prompt**, and then click **Run as administrator**. The Windows operating system displays the User Account Control prompt.

3. In the **User Account Control** dialog box, type **Administrator** in the **User name** box, type **Pa55w.rd** in the **Password** box, and then click **Yes**.

4. Close the **Administrator: Command Prompt** window.

5. Sign out.

Lesson 3
Implementing and managing BitLocker

Contents:

Question and Answers

Categorize Activity

Question:

Categorize each item below.

Items	
1	Encrypts the entire operating-system volume, including Windows system files and the hibernation file.
2	Encrypts files.
3	Does not require user certificates.
4	Requires user certificates.
5	Protects the operating system from modification.
6	Does not protect the operating system from modification.

Category 1		Category 2
BitLocker		EFS

Answer:

Category 1		Category 2
BitLocker		EFS
Encrypts the entire operating-system volume, including Windows system files and the hibernation file.		Encrypts files.
Does not require user certificates.		Requires user certificates.
Protects the operating system from modification.		Does not protect the operating system from modification.

BitLocker modes

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

> **Answer:** Computers without TPMs will not be able to use the system-integrity verification during startup that BitLocker can provide.

Using Group Policy settings to configure BitLocker

Question: How can you use Microsoft BitLocker Administration and Monitoring 2.5 Service Pack 1 (SP1) to reduce the time that the help desk spends recovering a BitLocker unlock key for a remote user?

> **Answer:** Administrators can enable the Microsoft BitLocker Administration and Monitoring 2.5 SP1 Self-Service Portal to allow users to recover a BitLocker recovery password without having to call their organization's help desk.

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 that is unique to a computer name. You can find the password ID under a computer's properties, which you can use to locate recovery passwords that are stored in AD DS.

Demonstration: Configuring and using BitLocker

Demonstration Steps

1. Sign in to **LON-CL1** as **Adatum\Administrator** with the password **Pa55w.rd**.

2. In the **Ask me anything** box on the taskbar, type **gpedit.msc**, and then press Enter.

3. In **Local Group Policy Editor**, under **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then expand **BitLocker Drive Encryption**.

4. Click **Operating System Drives**, and then double-click **Require additional authentication at startup**.

5. In the **Require additional authentication at startup** dialog box, click **Enabled**, and then click **OK**.

6. Close **Local Group Policy Editor**.

7. Click **Start**, type **cmd.exe**, right-click **Command Prompt**, and then click **Run as administrator**.

8. At the command prompt, type **gpupdate /force**, and then press Enter.

9. Close all open windows.

10. In the **Ask me anything** box, type **bitlocker** and then click **Manage BitLocker**.

11. Click **Allfiles (E:) BitLocker off**, and then click **Turn on BitLocker**.

12. In the **BitLocker Drive Encryption (E:)** dialog box, click **Use a password to unlock the drive**.

13. In the **Enter your password** and **Reenter your password** boxes, type **Pa55w.rd**, and then click **Next**.

14. On the **How do you want to back up your recovery key?** page, click **Save to a file**.

15. In the **Save BitLocker recovery key as** dialog box, click **Local Disk (C:)**.

16. On the File Explorer toolbar, click **New folder**, type **BitLocker**, and then press Enter

17. In the **Save BitLocker recovery key as** dialog box, click **Open**, click **Save**, click **Yes**, and then click **Next**.

18. On the **Choose which encryption mode to use** page, ensure that **New encryption mode (best for fixed drives on this device)** is selected, and then click **Next**.

19. On the **BitLocker Drive Encryption (E:)** page, click **Start encrypting**.

20. After the encryption process is complete, restart **LON-CL1**.

21. Sign in to **LON-CL1** as **Adatum\Administrator** with the password **Pa55w.rd**.

22. On the taskbar, click **File Explorer**.

23. In the Navigation pane, click **This PC**.

24. Right-click **Local Disk (E:)**, click **Open**, verify that the drive is listed as not accessible and that access is denied, and then click **OK**.

25. In the **Ask me anything** box on the taskbar, type **bitlocker** and then click **Manage BitLocker**.

26. Click **E: BitLocker on (Locked)**, and then click **Unlock drive**.

27. Enter the password **Pa55w.rd**, press Enter to unlock the drive, and then verify access to the drive contents.

28. Close all open windows.

Module Review and Takeaways

Question: Your coworker lost his USB drive, which contained confidential information about a new project. Which security feature could prevent unauthorized users from accessing that data?

Answer: BitLocker To Go

Lab Review Questions and Answers

Lab A: Configuring user accounts

Question and Answers

Question: In the lab, you configured UAC to switch to the secure desktop. What advantage does this offer?

> **Answer:** The secure desktop presents the configure UAC prompt, and restricts functionality and access to the system until the user satisfies sign-in requirements. This helps make Windows 10 more secure.

Lab B: Managing data security

Question and Answers

Question: In the lab, you implemented BitLocker. Why was it necessary to configure the GPO settings?

> **Answer:** This step was required because the virtual machine does not have a TPM.

Module 11

Implementing remote connectivity

Contents:

Lesson 1
Overview of remote connectivity options

Contents:

Question and Answers

Discussion: When to use remote access

Question: Do you allow users to connect to your network resources remotely? If so, how?

> **Answer:** Answers might vary but could include:

- Access to the company´s VPN server.
- Access to company resources via DirectAccess.
- Access to company resource by using RDS.

Question: What are your business requirements for using remote access?

> **Answer:** Answers might vary but could include:

- Allowing your administrators to work from home.
- Fix issues that arise during weekends.
- Allow users access to company resources while traveling.

Lesson 2
Implementing VPNs

Contents:

Question and Answers

Question: The default NPS network policies enable remote access automatically.

(   ) True

(   ) False

> **Answer:**
>
> (   ) True
>
> (√) False
>
> **Feedback:** The two default NPS network policies deny access.

Question: Which VPN tunneling protocol supports VPN Reconnect?

> **Answer:** The IKEv2 VPN tunneling protocol supports VPN Reconnect.

Demonstration: Creating a VPN connection

Demonstration Steps

Configure the VPN server role

1. Switch to **LON-RTR**.

2. On **LON-RTR**, click **Start** and then click **Server Manager**.

3. In Server Manager, click the **Tools** menu, and then click **Remote Access Management**.

4. In the **Configuration** pane, click **DirectAccess and VPN**.

5. In the details pane, under **Configure Remote Access**, click the link **Run the Getting Started Wizard**.

6. In the **Configure Remote Access** wizard, click **Deploy VPN only**. This brings up a separate **Routing and Remote Access** console.

7. In the **Routing and Remote Access** console, right-click **LON-RTR**, and then select **Configure and Enable Routing and Remote Access**.

8. In the **Routing and Remote Access Server Setup Wizard**, click **Next**.

9. On the **Configuration** page, ensure that **Remote access (dial-up or VPN)** is selected, and then click **Next**.

10. On the **Remote Access** page, select the **VPN** check box, and then click **Next**.

11. On the **VPN Connection** page, select the **Internet** interface value that has the 131.107.0.200 address, and then click **Next**.

12. On the **IP Address Assignment** page, click **Next**.

13. On the **Managing Multiple Remote Access Servers** page, click **Next**, and then click **Finish**.

14. In the **Routing and Remote Access** dialog box, click **OK**.

15. In the next **Routing and Remote Access** dialog box, click **OK**.

> **Note:** If you receive an error during startup of the service, click **OK**. The service sometimes starts with a delay.

16. In **Server Manager**, click the **Tools** menu item, and then click **Network Policy Server**.

17. In Network Policy Server, in the navigation pane, expand **Policies**, and then click **Network Policies**.

18. Right-click **Connections to Microsoft Routing and Remote Access server**, and then click **Properties**.

19. In the **Connections to Microsoft Routing and Remote Access server Properties** dialog box, in the **Access Permission** section, click **Grant access**, and then click **OK**.

20. Close all open windows.

21. Right-click **Start**, and then click **Windows PowerShell (Admin)**.

22. In the **Administrator: Windows PowerShell** window, type the following command, and then press Enter:

```
Restart-Computer
```

Move the client from the intranet to the public network

1. Switch to **LON-CL1**.

2. Click **Start**, type **Control Panel**, and then press Enter.

3. Click **View network status and tasks**.

4. Click **Change adapter settings**.

5. Right-click **Ethernet**, and then click **Disable**.

6. Right-click **Internet**, and then click **Enable**.

7. Right-click **Internet**, and then click **Properties**.

8. In the **Internet Properties** dialog box, double-click **Internet Protocol Version 4 (TCP/IPv4)**.

9. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, verify that the following displays, and then click **OK**:

   o   IP address: **131.107.0.40**

   o   Subnet mask: **255.255.0.0**

   If no changes are required, then in the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, click **Cancel**.

10. In the **Internet Properties** dialog box, click **OK**.

11. Close Network Connections.

Create and test a new VPN connection

1. On **LON-CL1**, on the **Start** menu, select **Settings**.

2. In the Settings app, click the **Network & Internet** category.

3. In the **Network & Internet** console tree, select **VPN**.

4. In the **details** pane, click the **Add a VPN connection** plus sign (**+**).

5. In the **Add a VPN connection** window, provide the following values, and then click **Save**:

   o   VPN provider: **Windows (built-in)**

   o   Connection name: **Adatum HQ VPN**

   o   Server name or address: **131.107.0.200**

6. In the **Network & Internet Settings** app, click **Adatum HQ VPN**, and then click **Connect**.

7. Sign in as **Adatum\Administrator** with the password **Pa55w.rd**, and then click **OK**.

8. In the **Network & Internet Settings** app, the Adatum HQ VPN should show a status of Connected.

Verify that the VPN server can monitor and manage the client VPN connection

1. Switch to **LON-RTR**, and then sign in as **Adatum\Administrator** with the password **Pa55w.rd**.

2. In Server Manager, click **Tools**, and then click **Remote Access Management**.

3. In the navigation pane, click **Remote Client Status**.

4. Verify that the details pane shows the **Adatum\Administrator** connection. Review the **Access Details** and **Connection Details** boxes below the details pane.

5. In the navigation pane, click **VPN**.

6. In the **Tasks** section on the right, click **Open RRAS Management**.

7. In the **Routing and Remote Access** window, expand **LON-RTR**, and then select **Remote Access Clients (1)**.

8. In the navigation pane, click **Ports**, and then in the details pane, click the **Status** column name once. This should show the Active connection. Right-click it, and then select **Status**.

9. Explain the **Port Status** window. Note how it provides much of the information we saw previously in the **Remote Client Status** window of the **Remote Access Management** console.

10. In the **Port Status** window, click **Close**.

11. Close the **Routing and Remote Access** console.

12. In the **Remote Access Management Console** navigation pane, click **Remote Client Status**.

13. In the **Tasks** pane on the far right, click **Disconnect VPN Clients**, and then click **OK** twice.

14. Switch to **LON-CL1**, click **Start**, type **Control Panel**, and then press Enter.

15. Click **View network status and tasks**.

16. Click **Change adapter settings**.

📋 **Note:** Note the new connection object titled Adatum HQ VPN, but also note that it is disconnected.

17. Close the **Network Connections** window.

18. Close all open windows on **LON-RTR** and **LON-CL1**, and then sign out of both.

Lesson 3
Implementing DirectAccess

Contents:

Question and Answers

Question: Which of the following are mandatory requirements for a DirectAccess deployment? Select all that apply.

( ) DirectAccess server

( ) AD DS forest

( ) DNS

( ) Group Policies

( ) PKI

> **Answer:**
>
> (√) DirectAccess server
>
> (√) AD DS forest
>
> (√) DNS
>
> (√) Group Policies
>
> ( ) PKI
>
> **Feedback:** A PKI is optional. It is used when the self-signed certificate in the Getting Started Wizard is insufficient for your organization's security needs.

Demonstration: Configuring DirectAccess

Demonstration Steps

Create a security group for DirectAccess client computers

1. On **LON-DC1**, in **Server Manager**, in the upper-right corner, click **Tools**, and then click **Active Directory Users and Computers**.

2. In the **Active Directory Users and Computers** navigation pane, right-click **Adatum.com**, click **New**, and then click **Organizational Unit**.

3. In the **New Object – Organizational Unit** dialog box, in the **Name** text box, type **Special Accounts**, and then click **OK**.

4. In the **Active Directory Users and Computers** navigation pane, right-click **Special Accounts**, point to **New**, and then click **Group**.

5. In the **New Object - Group** dialog box, in the **Group name** text box, type **DirectAccessClients**.

6. Under the **Group** scope, ensure that **Global** is selected. Under the **Group** type, ensure that **Security** is selected, and then click **OK**.

7. In the details pane, right-click **DirectAccessClients**, and then click **Properties**.

8. In the **DirectAccessClients Properties** dialog box, click the **Members** tab, and then click **Add**.

9. In the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, click **Object Types**, select the **Computers** check box, and then click **OK**.

10. In the **Enter the object names to select (examples)** text box, type **LON-CL1**, click **Check Names**, and then click **OK**.

11. Verify that **LON-CL1** displays under **Members**, and then click **OK**.

12. Close the **Active Directory Users and Computers** console.

Configure DirectAccess by running the Getting Started Wizard

1. Switch to **LON-RTR**.

2. Click **Start**, and then click **Server Manager**.

3. In **Server Manager**, click **Tools**, and then click **Remote Access Management**.

4. In the **Remote Access Management** console, under **Configuration**, click **DirectAccess and VPN**, and then click **Run the Getting Started Wizard**.

5. In the **Getting Started Wizard**, on the **Configure Remote Access** page, click **Deploy DirectAccess only**.

6. On the **Network Topology** page, verify that **Edge** is selected, in the **Type the public name or IPv4 address used by clients to connect to the Remote Access server** text box, type **131.107.0.200**, and then click **Next**.

7. On the **Configure Remote Access** page, click the **here** link.

8. On the **Remote Access Review** page, verify that two GPO objects are created: **DirectAccess Server Settings**, and **DirectAccess Client Settings**.

9. Next to **Remote Clients**, click the **Change** link.

10. Click **Domain Computers (ADATUM\Domain Computers)**, and then click **Remove**.

11. Click **Add**. In **Enter the object names to select (examples)** text box, type **direct**, and then click **Check Names**.

12. Verify that **DirectAccessClients** displays, and then click **OK**.

13. Clear the **Enable DirectAccess for mobile computers only** check box, and then click **Next**.

14. On the **DirectAccess Client Setup** page, complete the following information, and then click **Finish**:

    o   Helpdesk email address: **DAHelp@adatum.com**

    o   DirectAccess connection name: **A. Datum DirectAccess**

15. On the **Remote Access Review** page, click **OK**.

16. On the **Configure Remote Access** page, click **Finish**, and then wait for the configuration to finish.

17. In the **Applying Getting Started Wizard Settings** dialog box, verify that the configuration was successful, and then click **Close**.

Verify client configuration

1. On your host, in **Hyper-V Manager**, right-click **20698B-LON-CL1**, and then click **Start**.

2. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts

3. Switch to **LON-CL1**.

4. Sign in as **Adatum\Administrator** with the password **Pa55w.rd**.

5. Click **Start**, type **cmd.exe**, right-click **Command Prompt**, and then click **Run as administrator**.

6. In the **Administrator: Command Prompt** window, type the following command, and then press Enter:

```
gpresult /R
```

7. In the **Administrator: Command Prompt** window, review the displayed output of the command that you executed in the previous step. Under the **COMPUTER SETTINGS** section, verify that the **DirectAccess Client Settings** GPO is applied.

📋   **Note:** If the DirectAccess Client Settings GPO is not applied, restart **LON-CL1**, and then sign in as **Adatum\Administrator** by using the password **Pa55w.rd**.

8. At the **Administrator: Command Prompt** windows, type the following command, and then press Enter:

```
netsh name show effectivepolicy
```

9. Verify that the following message displays: **DNS Effective Name Resolution Policy Table Settings**.

📋   **Note:** DirectAccess settings are inactive when this computer is inside a corporate network.

10. Close the **Command Prompt** window.

Module Review and Takeaways

Question: What type of remote access solutions can you provide by using VPN in Windows 10?

Answer: You can configure the following remote access solutions by using VPN in Windows 10:

- Secure remote access to internal network resources for users located on the Internet. The users act as VPN clients that are connecting to Windows Server 2016, which acts as a VPN server.

- Secure communication between network resources that are located on different geographical locations or sites. This solution is called *site-to-site VPN*. In each site, Windows Server 2016 acts as a VPN server that encrypts communication between the sites.

Question: What are the primary benefits of using DirectAccess for providing remote connectivity?

Answer: The primary benefits of using DirectAccess for providing remote connectivity are as follows:

- Always-on connectivity. When the user is connected to the Internet, the user is also connected to the intranet.

- Users have the same experience regardless of whether they are connected locally or remotely.

- Bidirectional access. When the client computer is accessing the intranet, the computer can be managed by the administrators.

- Improved security. Administrators can set and control the intranet resources that are accessible through DirectAccess.

Lab Review Questions and Answers

Lab: Implementing a VPN

Question and Answers

Question: How can you determine which VPN protocol the connections that you established in this lab exercise are using?

> **Answer:** You can view a list of used ports in the Routing and Remote Access console on the VPN server, which list the VPN protocol. Additionally, you can look at the adapter settings on the client computer, which also display the VPN protocol that is in use currently.

Question: You used a network policy with a condition of membership of a Windows Group during the lab. What would have happened if Claire had not belonged to the Research group?

> **Answer:** The short answer is that Claire could not connect the VPN if she did not belong to the Research group. The longer answer is that any other policies would then be processed because Claire's attempt to connect did not meet the policy conditions of the first policy in the list of policies on the NPS server.

Module 12

Maintaining Windows 10

Contents:

Lesson 1
Updating Windows 10

Contents:

Question and Answers

Question: Aside from using WSUS to apply updates, what other technologies could you use to help keep your Windows 10 devices up to date? (Select all that apply.)

( ) Intune

( ) Microsoft System Center 2012 R2 Configuration Manager

( ) Windows Update for Business

> **Answer:**
>
> (√) Intune
>
> (√) Microsoft System Center 2012 R2 Configuration Manager
>
> (√) Windows Update for Business
>
> **Feedback:** You can use all three of these Microsoft technologies to keep your Windows 10 devices up to date.

Question: You can use Windows Update for Business to update all editions of Windows 10.

( ) True

( ) False

> **Answer:**
>
> ( ) True
>
> (√) False
>
> **Feedback:** Windows Update for Business is for Windows 10 Pro, Windows 10 Education, and Windows 10 Enterprise editions. Windows Update for Business does not support Windows 10 Home.

Demonstration: Configuring Windows Update

Demonstration Steps

Configure Windows Update manually

1.   Switch to **LON-CL1**.

2.   Click **Start**, and then click the **Settings** icon.

3.   In **Settings**, click **Update & Security**.

4.   On the **Windows Update** tab, click **Advanced options**.

5.   On the **Advanced options** page, clear the **Give me updates for other Microsoft products when I update Windows** check box.

6.   Click **Back**.

7.   Click **Change active hours**.

8.   In the **End time** drop-down list, click **8 00 PM**, and then click the check mark.

9.   Click **Save**.

Configure Windows Update by using GPOs

1.   In the **Ask me anything** box, type **gpedit.msc**, and then in the list of returned items, click **gpedit.msc**.

2. In **Local Group Policy Editor**, navigate to **Computer Configuration/Administrative Templates/Windows Components/Data Collection and Preview Builds**.

3. In the right pane, double-click **Toggle user control over Insider builds**.

4. In the **Toggle user control over Insider builds** dialog box, click **Disabled**, and then click **OK**.

5. In **Local Group Policy Editor**, navigate to **Computer Configuration/Administrative Templates/Windows Components/Windows Update/Windows Update for Business**.

6. In the right pane, double-click **Select when Preview Builds and Feature Updates are received**.

7. In the **Select when Preview Builds and Feature Updates are received** dialog box, click **Enabled**.

8. In the **Select the Windows readiness level for the updates you want to receive** list, click **Semi-Annual Channel**.

9. In the **After a Preview Build or Feature Update is released, defer receiving it for this many days** text box, type **90**, and then click **OK**.

10. In the navigation pane, click **Windows Update**.

11. In the right pane, double-click **Turn off auto-restart for updates during active hours**.

12. In the **Turn off auto-restart for updates during active hours** dialog box, click **Enabled**, and then click **OK**.

13. In the right pane, double-click **Configure Automatic Updates**.

14. In the **Configure Automatic Updates** dialog box, click **Enabled**, in the **Configure automatic updating** drop-down list, click **2 – Notify for download and auto install**, and then click **OK**.

15. Close the Local Group Policy Editor.

16. Right-click **Start**, and then click **Windows PowerShell (Admin)**.

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

```
gpupdate /force
```

18. Restart **LON-CL1**.

19. Sign in as **Adatum\Administrator** with the password **Pa55w.rd**.

20. Click **Start**, and then click the **Settings** icon.

21. In **Settings**, click **Update & Security**.

22. On the **Windows Update** tab, click **Advanced options**.

23. Notice that the branch readiness level and feature update deferment options are dimmed.

24. Close all open apps and windows.

Note: If the settings are not as documented, repeat steps 16 through 24.

Lesson 2
Monitoring Windows 10

Contents:

Question and Answers

Question: When monitoring Windows 10–based computers to optimize their performance, which key system components should you monitor? (Select all that apply.)

( ) Processor

( ) System

( ) Disk

( ) Memory

( ) Network

> **Answer:**
>
> (√) Processor
>
> ( ) System
>
> (√) Disk
>
> (√) Memory
>
> (√) Network
>
> **Feedback:** The system is not a key resource component, but it is a Performance Monitor object.

Demonstration: Monitoring Windows with Event Viewer

Demonstration Steps

Explore custom views

1. On **LON-CL1**, click **Start**, expand **Windows Administrative Tools**, and then click **Event Viewer**.

2. In the navigation pane, expand **Custom Views**, and then click **Administrative Events**.

Create a custom view

1. In the navigation pane, right-click **Custom Views**, and then click **Create Custom View**.

2. In the **Create Custom View** dialog box, select the **Critical**, **Warning**, and **Error** check boxes.

3. In the **Event logs** list, expand **Windows Logs**, and then select the **System** and **Application** check boxes. Click in the **Create Custom View** dialog box, and then click **OK**.

4. In the **Save Filter to Custom View** dialog box, in the **Name** box, type **Adatum Custom View**, and then click **OK**.

5. In **Event Viewer**, in the right pane, view the events that are visible within your custom view.

Demonstration: Monitoring performance

Demonstration Steps

Open Performance Monitor

1. On **LON-CL1**, in the **Ask me anything** text box, type **perfmon**, and then press Enter.

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. On the toolbar, click the plus (**+**) symbol 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. To accept the default storage location for the data, click **Next**.

6. Click **Open properties for this data collector set**, and then click **Finish**.

7. In the **CPU and Disk Activity Properties** dialog box, 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.

8. Click the **Directory** tab. This tab lets you define information about how to store collected data.

9. Click the **Security** tab. This tab lets you configure which users can change this data collector set.

10. Click the **Schedule** tab. This tab lets you define when the data collector set is active and collecting data.

11. Click the **Stop Condition** tab. This tab lets you define when to stop data collection, based on time or collected data.

12. 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.

13. Click **Cancel**. Notice that there are three kinds of logs in the right pane:

    o **Performance Counter** collects data that you can view in Performance Monitor.

    o **Configuration** records changes to registry keys.

    o **Kernel Trace** collects detailed information about system events and activities.

14. In the right pane, double-click **Performance Counter**. Notice that all **Processor** counters are collected, by default.

15. Click **Add**.

16. In the **Available counters** area, click **PhysicalDisk**, click **Add**, and then click **OK**. All the counters for the **PhysicalDisk** object are now added. 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 for the data collector set to stop automatically.

2. Right-click **CPU and Disk Activity**, and then click **Latest Report**.

3. Review the report, which shows the data that the data collector set collects.

4. Close Performance Monitor.

Module Review and Takeaways

Question: What is the benefit of configuring Windows Update by using Group Policy rather than by using **Settings**?

Answer: By using Group Policy, you can apply configuration settings to multiple computers by performing a single action. It also prevents users from overriding the settings.

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

Answer: You should monitor the following counters:

- **Processor > % Processor Time**

- **System > Processor Queue Length**

- **Memory > Pages/sec**

- **Physical Disk > % Disk Time**

- **Physical Disk > Avg. Disk Queue Length**

Question: If 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 manually by using the counters in the Performance Monitor or by using a template.

Lab Review Questions and Answers

Lab: Maintaining Windows 10

Question and Answers

Question: In the lab, you collected performance data for specific system objects. Which object(s) and counter(s) in Performance Monitor indicate how busy the computer's CPU is?

Answer: The **Processor\% Processor Time** counter and the **System\Processor Queue Length** counter together provide the best indication of how busy or overloaded the computer's CPU is.

Module 13

Recovering Windows 10

Contents:

Lesson 1
Recovering files

Contents:

Question and Answers

Question: Which location can **File History** use to store backup data?

(   ) C:\

(   ) D:\Backup

(   ) \\172.16.10.256\Share1

(   ) E:\

(   ) https://azure.microsoft.com/backup

> **Answer:**
>
> (   ) C:\
>
> (   ) D:\Backup
>
> (   ) \\172.16.10.256\Share1
>
> (√) E:\
>
> (   ) https://azure.microsoft.com/backup
>
> **Feedback: File History** cannot store backups on the volume on which the operating system is installed. You also cannot create backups in the subfolders or use the HTTPS protocol to connect to the shared folder on the network on which a backup will be performed. 172.17.10.256 is not a valid IP address. The only correct option is to use the root of the local drive, which could be E:\.

Question: You can use the **Backup and Restore (Windows 7)** tool to back up data that a Resilient File System (ReFS) volume is storing.

(   ) True

(   ) False

> **Answer:**
>
> (   ) True
>
> (√) False
>
> **Feedback:** By using the **Backup and Restore (Windows 7)** tool, you can only back up data that an NTFS volume is storing. You cannot use it to back up data that is on the FAT file system, FAT32, exFAT, or ReFS volumes.

Question: You can use the **Previous Versions** feature only with files that NTFS volumes are storing.

(   ) True

(   ) False

> **Answer:**
>
> (   ) True
>
> (√) False
>
> **Feedback:** You can use the **Previous Versions** feature with any file, regardless of the file system on the volume that is storing it. However, if the file system is not NTFS, **Previous Versions** can come only from **File History.**

File recovery methods in Windows 10

Question: Does Windows 10 include a backup tool?

Answer: Yes. Windows 10 includes two backup tools:

- **Wbadmin.exe**, which is a backup command-line tool.

- **Backup and Restore (Windows 7)**, which you can use to schedule backups of individual folders, users' libraries, and a complete Windows 10–based computer.

Question: What is the simplest way to recover a locally stored document that a user accidentally deleted in Windows 10?

Answer: After you set it up, **File History** is the easiest and most user-friendly way to restore previous versions of files.

File History

Question: Is **File History** turned on by default?

Answer: No. Before you can use **File History**, you must configure it with a local drive, a removable drive, or a network location, and then turn on **File History**.

Question: Can you protect additional folders by using **File History**?

Answer: Yes. You can add additional folders to one of the libraries that **File History** is protecting. Alternatively, you can use the **Backup** option in the **Recovery** section in the Settings app. When you do so, **File History** also protects the folders that you add.

Previous Versions

Question: What must you configure if you want the **Previous Versions** tab in File Explorer to list previous versions of files?

Answer: Previous versions of files come from **File History** or from restore points. If you want the **Previous Versions** tab in File Explorer to list previous versions of files, you must protect those files by using **File History** or including them in the backup that the **Backup and Restore (Windows 7)** tool creates.

Question: When will the **Previous Versions** tab include the previous versions of a file that the **Backup and Restore (Windows 7)** tool backs up?

Answer: As soon as the **Backup and Restore (Windows 7)** tool creates a backup, the previous version will be available on the **Previous Versions** tab. The same is true if **File History** is protecting the file. When **File History** runs, previous versions of the file become available on the **Previous Versions** tab.

Demonstration: Using File History to recover files

Demonstration Steps

Configure File History

1. On **LON-CL1**, on the taskbar, click **File Explorer**.

2. In File Explorer, in the navigation pane, expand **This PC**, and then click **Documents**.

3. In the details pane, right-click an empty space, point to **New**, click **Text Document**, type **Report**, and then press Enter.

4. Double-click **Report.txt**, and then in Notepad, type **This is a report**.

5. Close Notepad, and then click **Save** to save the changes.

6. On the taskbar, in the **Ask me anything** box, type **file history**, and then click **Restore your files with File History**.

7. In the **Home – File History** window, click **Configure File History settings**.

8. In the **File History** dialog box, in the navigation pane, click **Select drive**.

9. In the **Select Drive** dialog box, click **Add network location**, in the **Folder** box, type **\\LON-DC1\Backup2**, click **Select Folder**, and then click **OK**.

10. In the **File History** dialog box, in the details pane, click **Turn on**.

11. In the navigation pane, click **Advanced settings**, point out the default values, and then click **Cancel**.

12. In File Explorer, in the navigation pane, click **Documents**, right-click **Report.txt**, and then click **Delete**.

13. In File Explorer, click the **Home** tab, and then click **History**.

14. In the **Documents – File History** window, right-click **Report.txt**, and then click **Preview**.

📝   **Note:** Point out that you can see the text that you typed earlier.

15. Click the round green button with the arrow to restore the file to the original location.

16. File Explorer opens. Point out that the **Report.txt** file has been recovered. Double-click **Report.txt**, point out that it has the content that you typed earlier, close Notepad, and then close File Explorer.

17. In the **Report.txt – File History** window, to the left of the address box, click the upward-pointing arrow twice.

📝   **Note:** Point out the folders and libraries that **File History** is protecting, and then verify that the **Data** folder is currently not among the protected folders.

18. Close the **Home – File History** window.

19. In File Explorer, in the navigation pane, expand **Local Disk (C:)**, and then click **Data**.

20. In the details pane, right-click **Sales.txt**, click **Properties**, and then click the **Previous Versions** tab.

📝   **Note:** Point out that there are no previous versions available.

21. Click **OK**.

Add an additional folder to File History

1. On the taskbar, in the **Ask me anything** box, type **file history**, and then click **Backup settings**.

2. In the **Settings** dialog box, in the **Back up using File History** section, click **More options**.

3. In the **Backup options** window, in the **Back up these folders** section, click **Add a folder**.

4. In the **Folder** box, type **C:\Data**, and then click **Choose this folder**.

📝   **Note:** Point out that the **C:\Data** folder is added. Show and discuss other settings, such as backup frequency, how long to keep files, and which folders are excluded.

5. Close the **Backup options** window.

6. In the **File History** dialog box, click **Run now**.

Use File History to recover a deleted file

1. In File Explorer, in the details pane, right-click **Sales.txt**, click **Properties**, and then click the **Previous Versions** tab.

📋   **Note:** Point out that there is now one previous version available, which was created when you ran **File History**.

2. Click **OK**. In File Explorer, click the **Home** tab, and then click **History**.

3. In the **Sales.txt – File History** window, at the left of the address box, click the upward-pointing arrow until the window title changes to **Home – File History**.

📋   **Note:** Point out that the **Data** folder is now among the folders and libraries that **File History** is protecting.

4. Close the **Home – File History** and **File History** windows.

Demonstration: Using Previous Versions to recover files

Demonstration Steps

1. On **LON-CL1**, in File Explorer, in the navigation pane, verify that **Data** is selected.

2. In the details pane, right-click **Sales.txt**, click **Properties**, click the **Previous Versions** tab, point out that there is one previous version, explain that it was created when **File History** ran in the previous demonstration, and then click **OK**.

3. Double-click **Sales.txt**. In Notepad, type **Before restore point**, close Notepad, and then click **Save** to save the changes.

4. Right-click **Sales.txt**, click **Properties**, click the **Previous Versions** tab, point out that there is still only one previous version, and then click **OK**.

5. Click **Start**, type **Control Panel**, press Enter, and then click **Backup and Restore (Windows 7)**.

6. In the **Backup and Restore (Windows 7)** window, click **Set up backup**.

7. In the **Set up backup** window, click **Save on a network**.

8. In the **Network location** text box, type **\\lon-dc1\Backup2**, in the **Username** text box, type **Adatum\Administrator**, in the **Password** text box, type **Pa55w.rd**, click **OK**, and then click **Next**.

9. On the **What do you want to back up?** page, select **Let me choose**, and then click **Next**.

10. Clear the **Include a system image of drives: System Reserved, (C:)** check box, expand **Local Disk (C:)**, select **Data**, point out that the **Misc** folder is not selected, and then click **Next**.

11. On the **Review your backup settings** page, click **Save settings and run backup**, and then wait until the backup finishes.

12. In File Explorer, right-click **Sales.txt**, click **Properties**, click the **Previous Versions** tab, point out that there are now two previous versions because the second previous version was added when the backup was created, and then click **OK**.

13. Right-click **Sales.txt**, and then click **Delete**.

14. In the details pane, right-click the empty space, click **Properties**, click the **Previous Versions** tab, click the first **Data** folder listed under **Folder versions**, click **Restore**, and then click **OK**.

15. In File Explorer, in the details pane, double-click **Data**, and then point out that the **Sales.txt** file is restored.

16. In File Explorer, in the navigation pane, expand **Local Disk (C:)**, and then click **Misc**.

17. In the details pane, right-click **Temp.txt**, click **Properties**, and then click the **Previous Versions** tab. Point out that no previous version is available because the backup did not include the folder.

18. Click **OK**, close File Explorer, and then close the **Backup and Restore (Windows 7)** window.

Lesson 2
Performing system recovery

Contents:

Question and Answers

Question: Which of the following tools cannot preserve user data that is stored on drive C?

( ) **Reset this PC**

( ) **System Image Recovery**

( ) **Startup Repair**

( ) **Diskpart.exe**

( ) **Go back to the previous build**

> **Answer:**
>
> ( ) **Reset this PC**
>
> (√) **System Image Recovery**
>
> ( ) **Startup Repair**
>
> ( ) **Diskpart.exe**
>
> ( ) **Go back to the previous build**
>
> **Feedback:** If you use **System Image Recovery**, it will replace all the data with that of the system image. You can select the **Keep my files** option with **Reset this PC**. **Startup Repair** does not modify user data. Using **Go to the previous build** will also preserve user data. You can use **Diskpart.exe** to create a new partition, which does not affect existing user data.

Question: System Image Recovery is the easiest and fastest tool for repairing startup problems in Windows 10.

( ) True

( ) False

> **Answer:**
>
> ( ) True
>
> (√) False
>
> **Feedback: Startup Repair** is the easiest and fastest tool for repairing startup problems in Windows 10.

Question: You can use **System Restore** even if your Windows 10–based computer has startup problems.

( ) True

( ) False

> **Answer:**
>
> (√) True
>
> ( ) False
>
> **Feedback:** If your computer has startup problems, you can start it from Windows 10 installation media, select **Repair**, and then select **System Restore.**

Question: From which tool or tools can you perform a driver rollback operation for printers?

( ) Device Manager

( ) Devices and Printers

( ) Devices in Windows 10 Settings

( ) All of the above

( ) None of the above

> **Answer:**
>
> ( ) Device Manager
>
> ( ) Devices and Printers
>
> ( ) Devices in Windows 10 Settings
>
> ( ) All of the above
>
> (√) None of the above
>
> **Feedback:** You cannot perform driver rollback for printers (print queues).

Overview of system recovery procedures

Question: Can you run the **Reset this PC** feature from a computer that is running Windows 10 in the normal mode?

> **Answer:** No. You can select the **Reset this PC** option only from the recovery environment. To start a computer in the recovery environment, you should select the option to change advanced startup options while Windows 10 is running, or you should start the computer from Windows 10 installation media and then select **Recovery**.

Question: Why would you use **Startup Repair** instead of **System Image Recovery** if the Boot Configuration Data (BCD) store is damaged on a Windows 10–based computer?

> **Answer:** If the BCD store is damaged, Windows 10 will not start. Both **Startup Repair** and **System Image Recovery** can resolve the issue, but **Startup Repair** is much faster and is a nondestructive operation.

Driver rollback

Question: Why is the **Roll Back Driver** option unavailable for some devices?

> **Answer:** The **Roll Back Driver** option reverts the device driver to the previously used device driver. If the device is using the first and only version of the device driver, the **Roll Back Driver** option is unavailable for that device.

Question: Can you roll back device drivers for printers in Device Manager?

> **Answer:** No. Device Manager does not provide an option to roll back device drivers for printers (print queues). This is because you manage printers in **Devices and Printers**, not in Device Manager.

System Protection and restore points

Question: How can you configure Windows 10 to create restore points automatically?

> **Answer: System Protection** creates a scheduled task named SR that can schedule the creation of restore points automatically. You can add a new trigger to the task and configure the frequency for creating restore points.

Question: Can you enable **System Protection** on an ReFS volume?

> **Answer:** No. You can only turn on **System Protection** on NTFS volumes. You cannot enable it on FAT or ReFS volumes.

Advanced startup options

Question: Can you access startup settings options by pressing F8 during computer startup?

> **Answer:** No. You cannot use keyboard shortcuts during the Windows 10 startup process, and you cannot access startup settings options by pressing any key during computer startup. You can access startup options by:

- Changing advanced startup options in Windows 10.

- Pressing the Shift key while selecting the **Restart** option.

- Restarting the computer by running the **shutdown.exe /r /o** command.

Question: How can you access the **Last Known Good Configuration** startup option in Windows 10?

> **Answer:** The **Last Known Good Configuration** startup option is not available in Windows 10.

Tools available in Windows RE

Question: Can you use **System Image Recovery** without any previous preparation?

> **Answer:** No. **System Image Recovery** restores a system image on your computer. To be able to use this option, you must first create the system image while Windows 10 is running.

Question: What are the options for the **Reset this PC** tool?

> **Answer:** If you start the **Reset this PC** tool, you can first choose between the **Keep my files** and **Remove everything** options. If you select **Remove everything**, you can further choose between the **Just remove my files** and **Fully clean the drive** options.

Discussion: Recovering devices

Question: Can you start **System Recovery** only from Windows 10 that is running in normal mode?

> **Answer:** No. You can also start **System Recovery** in safe mode or in recovery mode.

Question: When would you use **System Image Recovery**?

> **Answer:** If your device has failed, you should probably use **System Image Recovery** as the last option. This method requires you to prepare a system image in advance, and it completely replaces device data with the content of the system image.

Demonstration: Using a restore point to roll back device configuration

Demonstration Steps

1. On **LON-CL1**, in File Explorer, in the navigation pane, right-click **This PC**, click **Properties**, and then click **System protection**.

2. In the **System Properties** dialog box, in the **Protection Settings** section, select **Local Disk (C:) (System)**, click **Configure**, select **Turn on system protection**, move the **Max Usage** slider between **5 GB** and **10 GB**, and then click **OK**.

3. In the **System Properties** dialog box, click **Create**.

4. In the **System Protection** dialog box, type **Initial settings**, click **Create**, and then click **Close**.

5. Right-click the desktop, point to **New**, click **Text Document**, type **My document**, and then press Enter.

6. Right-click the **Start** icon, and then click **Device Manager**.

7. In Device Manager, expand **Keyboards**, right-click **Microsoft Hyper-V Virtual Keyboard**, and then select **Update Driver**.

8. In the **Update Drivers – Microsoft Hyper-V Virtual Keyboard** dialog box, click **Browse my computer for driver software**. Click **Let me pick from a list of available drivers on my computer**, and then clear the **Show compatible hardware** check box.

9. In the **Model** section, select **Microsoft Wireless Keyboard 700 v2.0 (106/109)**, click **Next**, in the **Update Driver Warning** box, click **Yes**, and then click **Close**.

10. Point out that in Device Manager, **Microsoft Wireless Keyboard 700 v2.0 (106/109)** appears with an exclamation point (!).

11. In the **System Properties** dialog box, in the **System Restore** section, click **System Restore**, and then click **Next**.

12. Select the **Initial settings** restore point, click **Next**, click **Finish**, and then click **Yes**. Wait until **LON-CL1** has restarted and **System Restore** has restored files and settings.

13. Sign in to **LON-CL1** as **Adatum\Administrator** with the password **Pa55w.rd**.

14. In the **System Restore** dialog box, click **Close**. Point out that **My document.txt** is still on the desktop.

15. Right-click the **Start** icon, and then click **Device Manager**.

16. In Device Manager, expand **Keyboards**, and then verify that Microsoft Hyper-V Virtual Keyboard is present. Microsoft Wireless Keyboard 700 v2.0 (106/109) was removed because you added it after creating the restore point.

17. Close **Device Manager**.

18. On the taskbar, click **File Explorer**.

19. In File Explorer, in the navigation pane, right-click **This PC**, click **Properties**, and then click **System protection**.

20. In the **System Properties** dialog box, click **System Restore**.

21. In the **System Restore** dialog box, select **Choose a different restore point**, and then click **Next**.

22. In the **System Restore** dialog box, verify that the additional restore point with the description **Restore Operation** and the type **Undo** was created.

23. Click **Cancel**, click **OK** in the **System Properties** dialog box, and then close the **System** window.

Demonstration: Using advanced startup options

Demonstration Steps

1. On **LON-CL1**, sign out, and then sign in as **.\Admin** with the password **Pa55w.rd**.

2. On the taskbar, in the **Ask me anything** box, type **service**, and then click **View local services**.

3. In the **Services** window, click the **Status** column to sort the services, scroll down, point out that more than 75 services are running, and then close the **Services** window.

4. Click **Start**, click **Settings**, and then click **Update & Security**.

5. On the **Recovery** tab, in the **Advanced startup** section, click **Restart now**, and then wait a few seconds.

6. On the **Choose an option** page, discuss the available options, and then click **Troubleshoot**.

7. On the **Troubleshoot** page, explain the **Reset this PC** options, and then click **Advanced options**.

8. On the **Advanced options** page, discuss the available options, click **Startup Settings**, and then click **Restart**.

9. Discuss the available **Startup** options, and then press 4 to select **Enable Safe Mode**.

10. When the computer starts, type **Pa55w.rd** as the password for **Adatum\Administrator**, and then press Enter.

11. Point out that the words "Safe Mode" appear in all four corners of the desktop. Right-click the **Start** icon, and then select **Device Manager**.

12. In Device Manager, right-click **Generic PnP Monitor**, select **Properties**, and then point out that the status of the device is not available when running in safe mode.

13. Click the **Driver** tab, and then point out that you can still update or uninstall drivers while running in safe mode. Mention that you can also perform driver rollback if a previous version of the driver exists, and then click **OK**.

14. Right-click the **Start** icon, and then click **Computer Management**.

15. In **Computer Management**, in the navigation pane, expand **Services and Applications**, and then click **Services**. In the details pane, click the **Status** column to sort the services, scroll down, and then point out that less than 30 services are running when you are in safe mode, while more than 75 services were running in normal mode.

16. On your host computer, in the **20698B-LON-CL1 on localhost – Virtual Machine Connection** dialog box, on the **Media** menu, point to **DVD Drive**, and then click **Insert Disk**.

17. In the **Open** dialog box, in the **File name** text box, type **C:\Program Files\Microsoft Learning\20698\Drives\Win10_1709_Eval.iso**, and then click **Open**. If virtual machines extract to a different location than drive C, use that drive letter instead.

18. On **LON-CL1**, right-click the **Start** icon, select **Shut down or sign out**, and then select **Restart**.

19. When you see the "Press any key to boot from CD or DVD" message, press the spacebar, and then wait while Windows Setup loads.

20. When prompted, in the **Windows Setup** dialog box, click **Next**.

21. On the next Windows Setup page, click **Repair your computer**.

22. On the **Choose an option** page, explain that you have the same available options even though you started the computer from DVD media this time, and then select **Troubleshoot**.

23. On the **Advanced options** page, point out that the only option that is missing is **Startup Settings**, because you started the recovery environment from DVD media.

24. Click **System Restore**, and then click **Windows 10**.

25. In the **System Restore** window, click **Next**. Point out that you can view and use restore points in **System Restore** even when you start the computer from installation media.

Module Review and Takeaways

Question: The help desk recently installed a new device driver on a computer. A stop code is generated, and you see a blue screen during computer startup. What recovery mechanism would you try first?

> **Answer:** You could try starting the computer in safe mode and using a driver rollback if the computer is able to start from the hard drive. Alternatively, you can use Windows 10 media and Windows RE to apply a **System Restore** point. You could also use **Reset this PC** as one of the last recovery options.

Question: Which Windows 10 features can help end users restore previous versions of their files?

> **Answer:** Windows 10 includes several features that can help end users restore previous versions of their files. The easiest way is to use the **Previous Versions** feature, which sources previous versions from **File History** and from restore points that **Backup and Restore (Windows 7)** creates.

Question: Can a non-administrative user use **System Restore** from the recovery environment?

> **Answer:** If a user starts the recovery environment from a computer that is running Windows 10 in normal mode by changing the advanced startup options, then the user will need to provide administrative credentials to run **System Restore**. However, if the user starts the recovery environment from Windows 10 installation media, then they can use **System Restore** without providing administrative credentials.

Lab Review Questions and Answers

Lab: Troubleshooting and recovery

Question and Answers

Question: What must you do if you want to use the **Previous Versions** feature in Windows 10?

> **Answer:** If you want to use the **Previous Versions** feature in Windows 10, you must configure **File History**, **Backup and Restore (Windows 7)**, or both.

Question: In Windows 10, how can you access advanced startup settings such as safe mode?

> **Answer:** If you want to access advanced startup settings such as safe mode, you must click the **Change advanced startup options** option while Windows 10 is running.

Question: Where can you access the **Refresh your PC** option in Windows 10?

> **Answer:** The **Refresh your PC** option is not available in Windows 10. It was only available in Windows 8 and Windows 8.1. In Windows 10, **Reset this PC** integrates the functionality of the **Refresh your PC** option.