Microsoft

OFFICIAL MICROSOFT LEARNING PRODUCT

20689D

Upgrading Your Skills to MCSA Windows® 8

Companion Content

Product Number: 20689D

Released: 05/2014

MICROSOFT LICENSE TERMS
MICROSOFT INSTRUCTOR-LED COURSEWARE

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

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

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

1. DEFINITIONS.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

a. **If you are a Microsoft IT Academy Program Member:**
   i. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
   ii. For each license you acquire on behalf of an End User or Trainer, you may either:
      1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User who is enrolled in the Authorized Training Session, and only immediately prior to the commencement of the Authorized Training Session that is the subject matter of the Microsoft Instructor-Led Courseware being provided, **or**
      2. provide one (1) End User with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
      3. provide one (1) Trainer with the unique redemption code and instructions on how they can access one (1) Trainer Content,

   provided you comply with the following:
   iii. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
   iv. you will ensure each End User attending an Authorized Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Authorized Training Session,
   v. you will ensure that each End User provided with the hard-copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,
   vi. you will ensure that each Trainer teaching an Authorized Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Authorized Training Session,

vii. you will only use qualified Trainers who have in-depth knowledge of and experience with the Microsoft technology that is the subject of the Microsoft Instructor-Led Courseware being taught for all your Authorized Training Sessions,
viii. you will only deliver a maximum of 15 hours of training per week for each Authorized Training Session that uses a MOC title, and
ix. you acknowledge that Trainers that are not MCTs will not have access to all of the trainer resources for the Microsoft Instructor-Led Courseware.

b. **If you are a Microsoft Learning Competency Member**:
i. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
ii. For each license you acquire on behalf of an End User or Trainer, you may either:
    1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User attending the Authorized Training Session and only immediately prior to the commencement of the Authorized Training Session that is the subject matter of the Microsoft Instructor-Led Courseware provided, **or**
    2. provide one (1) End User attending the Authorized Training Session with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
    3. you will provide one (1) Trainer with the unique redemption code and instructions on how they can access one (1) Trainer Content,

    provided you comply with the following:
iii. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
iv. you will ensure that each End User attending an Authorized Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Authorized Training Session,
v. you will ensure that each End User provided with a hard-copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,
vi. you will ensure that each Trainer teaching an Authorized Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Authorized Training Session,
vii. you will only use qualified Trainers who hold the applicable Microsoft Certification credential that is the subject of the Microsoft Instructor-Led Courseware being taught for your Authorized Training Sessions,
viii. you will only use qualified MCTs who also hold the applicable Microsoft Certification credential that is the subject of the MOC title being taught for all your Authorized Training Sessions using MOC,
ix. you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and
x. you will only provide access to the Trainer Content to Trainers.

c. **If you are a MPN Member**:

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

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

1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User attending the Private Training Session, and only immediately prior to the commencement of the Private Training Session that is the subject matter of the Microsoft Instructor-Led Courseware being provided, **or**
2. provide one (1) End User who is attending the Private Training Session with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
3. you will provide one (1) Trainer who is teaching the Private Training Session with the unique redemption code and instructions on how they can access one (1) Trainer Content,

provided you comply with the following:

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

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

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

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

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

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

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

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

d. **If you are an End User:**

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

e. **If you are a Trainer.**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

This limitation applies to

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

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

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

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

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

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

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

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

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

Revised July 2013

Module 1

Windows 8.1 in an Enterprise Environment

Contents:

Lesson 2

Overview of Windows 8.1

Contents:

Demonstration: Customizing the Windows 8.1 User Interface

Demonstration Steps

1. Sign in to LON-CL1 as **Adatum\Adam** with password **Pa$$w0rd**.
2. On the Start screen, click the **Photos** tile.
3. In the **Photos** app, move the pointer to the top of the screen, click, and then drag the pointer towards the bottom of the screen until the app closes.
4. From the Start screen, right-click the **Photos** tile, click **Resize**, and then click **Wide**.
5. Click and drag the **Photos** tile above the **Mail** tile.
6. Right-click the **Photos** tile, and then click **Unpin from Start**.
7. From the Start screen, move the pointer to the bottom of the screen, and then click the down-arrow icon.
8. Right-click the **Calculator** tile, and then click **Pin to Start**.
9. From the Start screen, click the **Desktop** tile.
10. On the desktop, right-click the **Start** button, and then click **Command Prompt**.
11. On the desktop, right-click the taskbar, and then click **Properties**.
12. On the **Taskbar and Navigation Properties** page, click the **Navigation** tab.
13. On the **Navigation** tab, in the Start screen section, select the **When I sign in or close all apps on a screen, go to the desktop instead of Start** check box, and then click OK.
14. Close all open windows.
15. Sign out of LON-CL1.
16. Leave all virtual machines running, as they will be used for the next demonstration.

Demonstration: Customizing Windows 8.1 Settings

Demonstration Steps

1. Sign in to LON-CL1 as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. From the Desktop, click the **Settings** charm, and then click **Change PC Settings**.
3. On the PC Settings screen, click **PC and devices**.
4. On the PC and devices screen, in the **Lock screen apps** section, click the **+** icon, click **Weather**, and then click the back arrow.
5. On the PC Settings screen, click **Accounts**, and then view the options available.
6. On the Accounts screen, click the back button.
7. On the PC Settings screen, click **Search and apps**.
8. On the Search and apps screen, click **Share**.
9. On the Frequent screen, change Items in list to **10**.
10. On the Search and apps screen, click **App sizes**.
11. In the app list, click **Finance**, click **Uninstall**, and then click **Uninstall**.
12. Click the back arrow.
13. On the PC Settings screen, click **Time and language**.

14. On the Time and Language screen, under **Time zone**, click the drop-down box, and then click **(UTC-6:00) Central Time (US & Canada)**.
15. Close the PC Settings screen.
16. Revert the 20689D-LON-CL1 and 20689D-LON-DC1 virtual machines.

Module Review and Takeaways

Review Question(s)

Question: What advantages does the domain environment provide for managing Windows 8.1–based computers?

Answer: Answers will vary, but students might mention centralized management and configuration with Group Policy, and centralized authentication with Active Directory® Domain Services. Domains also provide logical and security boundaries that can help an organization to provide a management structure for Windows 8.1–based computers.

Module 2

Installing and Upgrading to Windows 8.1

Contents:

Lesson 1

Preparing to Install and Deploy Windows 8.1

Contents:

Question and Answers

Planning Considerations for Windows 8.1 Installation

Question: Can you use the Client Hyper-V feature on 32-bit version of Windows 8.1 Enterprise?

Answer: No, you cannot use the Client Hyper-V feature on a 32-bit version of Windows 8.1 Enterprise. This feature is available only in the 64-bit version of Windows 8.1 Enterprise.

Question: Can you use Microsoft Office 2013 on Windows RT?

Answer: Yes, you can use Microsoft Office 2013 on Windows RT, because this app is part of Windows RT by default. Note that you can install only Windows Store apps on Windows RT.

Considerations for Deploying Windows 8.1 in the Enterprise Environment

Question: Why do enterprises not use the default Windows 8.1 DVD media to perform installations?

Answer: Installation from the default Windows 8.1 DVD media requires user interaction. You need to perform the installation locally, on one computer at a time. You can use Windows 8.1 DVD media for deploying Windows 8.1 in small branch offices. However, because of the manual intervention that is required, even small office environments typically use custom Windows 8.1 installation media.

Hardware Requirements for Installing Windows 8.1

Question: Do you have to create a virtual machine with at least 1 GB of memory if you want to install Windows 8.1 Pro on that virtual machine?

Answer: 1 GB of memory is the recommended minimum for installing Windows 8.1. However, you can install Windows 8.1 even if a computer or a virtual machine has less than 1 GB of memory—for example, 512 megabytes (MB). If you are installing Windows 8.1 on a virtual machine running on a Client Hyper-V virtualization platform, you can also use the Dynamic Memory feature.

Determining Device Driver Compatibility

Question: Can you use a device driver from a 64-bit version of Windows 8.1 with a 32-bit version of Windows 8.1?

Answer: A 32-bit version of Windows 8.1 can use only 32-bit device drivers, and a 64-bit version of Windows 8.1 can use only 64-bit device drivers. This means that you cannot use any device driver from a 64-bit version of Windows 8.1 with a 32-bit version of Windows 8.1.

Common Application Compatibility Issues

Question: Can you run a program that was developed for Windows XP on Windows 8.1?

Answer: Windows 8.1 is backward compatible with older versions of Windows operating systems. In general, you can run most programs that were developed for older versions of Windows operating systems on Windows 8.1. However, some changes in Windows 8.1 can cause compatibility issues. For example, if a program uses a component that is deprecated in Windows 8.1, you will not be able to run the program on Windows 8.1 by default, or sometimes, not at all.

Methods for Mitigating Common Application Compatibility Issues

Question: Consider a scenario where you have an application that can run on Windows XP but not on Windows 8.1. Also, you cannot use an application compatibility fix for the application. In this case, what will you do to mitigate the compatibility issue?

Answer: Client Hyper-V is one of the features in the 64-bit version of Windows 8.1. You can use Client Hyper-V to create a virtual machine, install Windows XP on the virtual machine, and then install the application on the virtual machine. You should ensure that you properly license the operating system that is running on the virtual machine.

Lesson 2

Installing Windows 8.1

Contents:

Question and Answers

Options for Installing Windows 8.1

Question: You bought a refurbished Windows 7 computer for your home office, and you plan to use it as a replacement for an existing computer. What type of Windows 8.1 installation should you perform?

> **Answer:** You should perform a clean installation of Windows 8.1 because you do not need the applications and data on the refurbished computer. After you install Windows 8.1, you can install the applications and migrate the settings and data from the computer you plan to replace.

Methods for Performing a Clean Installation

Question: What happens to the user settings, data, and installed applications if you perform a clean installation of Windows 8.1 on a computer that has Windows 7 installed on it?

> **Answer:** If you perform a clean installation of Windows 8.1, the existing users, their settings, data, and installed applications on the computer that is running Windows 7 are not migrated to Windows 8.1. If you did not format the volume, this information will be preserved in the Windows.old folder but will not be used in the Windows 8.1 environment.

Upgrading to Windows 8.1

Question: Can you upgrade Windows 7 Professional to Windows 8.1 Pro if you start the computer from Windows 8.1 DVD installation media?

> **Answer:** No, you can perform an upgrade to Windows 8.1 only if you run Setup.exe from the existing operating system. If you start the computer from the DVD, you can perform a clean installation of Windows 8.1, but you cannot upgrade the existing operating system to Windows 8.1.

Supported Windows 8.1 Upgrade Paths

Question: Can you upgrade a 32-bit version of Windows 8 Pro to a 64-bit version of Windows 8.1 Pro?

> **Answer:** No, cross-architecture upgrade to Windows 8.1 is not supported. Therefore, you cannot upgrade a 32-bit version of Windows 8 Pro to a 64-bit version of Windows 8.1 Pro.

Migrating to Windows 8.1

Question: You have a user who wants to upgrade a computer that is running Windows XP to Windows 8.1. The computer meets all of the hardware requirements for Windows 8.1, and the user wants to retain all of the existing user settings and use the same applications. The user has no time-related requirements and can be without the computer while you install Windows 8.1. How should you perform the Windows 8.1 installation?

> **Answer:** While most of the scenario would suggest an in-place upgrade, you cannot upgrade Windows XP directly to Windows 8.1. Therefore, in this scenario, you need to perform a migration, retain the user's settings, and reinstall applications.

Question: One of your users has been promoted to a new position, and the user has been given a new computer. The user would like to have the new applications that the job requires installed. The user would also like to have the documents and settings from the old Windows 7 computer transferred to the new computer. How should you perform the Windows 8.1 installation?

> **Answer:** You should perform a side-by-side migration in this scenario because a new computer and a new set of applications are being used. After installing Windows 8.1 on the new computer and installing new applications, you need to migrate the user's documents and settings, which are on the Windows 7 computer, to the new Windows 8.1 computer.

What Is Windows To Go?

Question: When would you use Windows To Go in your organization?

Answer: Answers may vary. You would typically use Windows To Go when you cannot or do not want to install Windows 8.1 on a physical computer. For example, you can use Windows To Go on personal devices that users bring to connect to organizational resources. With Windows To Go, users can start their devices to a customized Windows 8.1 environment, which can be domain-joined. This enables users to access company resources without modifying anything on the device, including the installed operating system and user data. The device must be Windows 8.1 compatible for you to use it with Windows To Go.

Starting a PC from a Native Boot Virtual Hard Disk

Question: Do you need to enable the Client Hyper-V feature if you want to use native boot from a virtual hard disk that contains Windows 8.1 Pro?

Answer: Native boot from a virtual hard disk uses physical hardware and does not require the Client Hyper-V feature. You can use native boot from a virtual hard disk even when the Client Hyper-V feature is not enabled.

Lesson 3

Volume Activation for Windows 8.1

Contents:

Question and Answers

Activation Options

Question: What is activation?

> **Answer:** Activation establishes a relationship between the product key that is used in Windows 8.1 installation and the computer hardware on which the installation was performed.

Volume Activation Technologies

Question: How can you determine if Windows 8.1 is activated? How you can activate Windows 8.1?

> **Answer:** You can determine if Windows 8.1 is activated by checking System properties, or by running the **slmgr –dli** script. You can activate Windows 8.1 by running the **slmg –ato** script or by using the Activate Windows settings page.

How KMS Activation Works

Question: Can a Windows 8.1 computer be a KMS host?

> **Answer:** Yes, a Windows 8.1 computer can be a KMS host. However, we do not recommend this configuration, because a computer that runs Windows 8.1 is not always connected to the network, and end users use it. It is recommended that one of the servers running Windows Server 2012 or a newer operating system also act as a KMS host.

How Active Directory–Based Activation Works

Question: What type of connection establishes between a Windows 8.1 computer and a Windows Server 2012 R2 domain controller when Active Directory–based activation is performed?

> **Answer:** When a Windows 8.1 computer wants to activate, it establishes Lightweight Directory Access Protocol (LDAP) communication with the domain controller. This is the same type of connection for other interactions between client computers and domain controllers, so you do not need to open any additional port on the firewall to allow Active Directory–based activation.

Tools Used to Manage Activation

Question: What is the main benefit that VAMT provides for an environment that does not have direct Internet connectivity?

> **Answer:** One of the features of VAMT is MAK Proxy Activation, which enables you to use VAMT for activating all the clients on a network at once, without requiring the clients to have Internet connectivity.

Troubleshooting Volume Activation

Question: Will the user be notified immediately if a Windows 8.1 computer cannot reactivate by using a KMS host?

> **Answer:** After Windows 8.1 is initially activated, it has up to 180 days for reactivation. During that time, it will try to contact the activation server every seven days, or even more often. If one of the attempts to reactivate is not successful—for example, if a KMS host is not available—the user will not be notified. You can find such events in the event log. The user will be notified only if Windows 8.1 is unable to activate in 180 days.

Lesson 4

Migrating User State and Settings

Contents:

Question and Answers

Tools for Migrating User Data and Settings

Question: You have been asked to replace ten 32-bit Windows 7 computers with 64-bit versions of Windows 8.1 in a small branch office. You also have been asked to show the local manager how to migrate user files and other data after installing Windows 8.1. Which tool should you demonstrate to the manager?

> **Answer:** Windows Easy Transfer is the best option in this scenario. A nontechnical user will perform the migration on a small number of computers only, so the Windows Easy Transfer wizard-based interface will be more familiar and easy to use.

Question: You have been asked to retain user settings for 200 users who are having their Windows 7 computers replaced with new Windows 8.1 computers. Which tool should you use for migrating user settings?

> **Answer:** USMT is the best option in this scenario. Migrating user states for 200 computers by using Windows Easy Transfer would be time-consuming. You can use the command-line tools for USMT in a script that can run on each computer.

Migrating User Settings by Using Windows Easy Transfer

Question: Can you use Windows Easy Transfer to migrate user settings and data between two Windows 8.1 computers?

> **Answer:** Windows Easy Transfer can migrate settings and data from a source computer that has an older Windows operating system installed to a Windows 8.1 destination computer. A Windows 8.1 computer cannot be a source computer for Windows Easy Transfer.

Migrating User Settings and Data by Using USMT

Question: Do you need to install Windows ADK on the source computer from which you plan to migrate user settings?

> **Answer:** No, you do not need to install Windows ADK on the source computer. However, you need to ensure that ScanState.exe and the XML files that you use during the capturing process are available on the source computer. USMT can be made available on a network share, and you can access the network share from the source computer and run USMT.

Capturing User State by Using ScanState

Question: Why would you use additional XML configuration files with ScanState.exe?

> **Answer:** When you want to include additional settings and data in the migration—for example, custom registry keys or folder structure—you can specify them in the additional XML configuration files. Be aware that data that is not captured on the source computer cannot be restored on the destination computer.

Restoring User State by Using LoadState

Question: How can you ensure that user data is safe during the migration?

> **Answer:** You can use encryption during the migration process. ScanState.exe can encrypt the data while it is capturing it, and LoadState.exe can decrypt it during the restoration process.

Module Review and Takeaways

Tools

Tool	Use for	Where to find it
ScanState.exe	Collecting user state data for migration	Windows ADK http://go.microsoft.com/fwlink/?LinkID=389939&clcid=0x409
LoadState.exe	Restoring user state data to newly installed operating systems	Windows ADK http://go.microsoft.com/fwlink/?LinkID=389939&clcid=0x409
USMTUtils.exe	Configuring and diagnosing the USMT environment	Windows ADK http://go.microsoft.com/fwlink/?LinkID=389939&clcid=0x409

Lab Review Questions and Answers

Lab A: Installing Windows 8.1

Question and Answers

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

Answer: You can export or copy the virtual machines from Client Hyper-V on Windows 8.1, and then import them to Windows Server 2012 R2 that is running the Hyper-V role in the production environment.

Question: Could you use Windows 8.1 Pro in the situation that the lab presents?

Answer: The 64-bit edition of Windows 8.1 Pro will run on the hardware that is specified and it will provide Client Hyper-V. However, Windows 8.1 Pro does not include the Windows To Go Creator Wizard, which is required for the lab. Therefore, you cannot use Windows 8.1 Pro in the situation that the lab presents.

Lab B: Migrating User State by Using USMT

Question and Answers

Question: Why did you need to create and customize a Config.xml file?

Answer: You use the custom Config.xml file to include or exclude additional settings and files in the migration. Your manager did not want several default folders to be migrated, so you had to create and customize the Config.xml file.

Question: Why did you use XML files with the ScanState.exe command?

Answer: XML files configure which settings and data to capture and which data should be included in the capture. If you do not specify the XML configuration files, only the default data will be captured.

Module 3

Configuring and Managing Windows 8.1

Contents:

Lesson 2

Using Windows PowerShell to Configure and Manage Windows 8.1

Contents:

Demonstration: Using Windows PowerShell ISE

Demonstration Steps

Prepare a computer to run scripts

1. On LON-CL1, on the Start screen, type **Admin**, and then click **Administrative Tools**.
2. In the Administrative Tools window, double-click **Windows PowerShell ISE**.
3. In Windows PowerShell Integrated Scripting Environment (ISE), at the Windows PowerShell command prompt, type **Get-ExecutionPolicy**, and then press Enter. Confirm that the execution policy is **Unrestricted**.

Open and review a script

1. In Windows PowerShell ISE, click **File**, and then click **Open**.
2. In the Open window, browse to **E:\Labfiles\Mod03**, click **Services.ps1**, and then click **Open**.
3. Read the script and explain what the script is doing. Note the following:
   - Comments are green.
   - Variables are red.
   - Cmdlets are bright blue.
   - Text in quotation marks is dark red.

Modify and test a script

1. Select line 3 in the script, and then press F8 to run the selection.
2. Read the output in the console pane. Notice that the line from the script appears in the console pane.
3. In the Console pane, type **$services**, and then press Enter.
4. Read the output in the console pane. Notice that a list of services displays.
5. Press F5 to run the script.
6. Read the output. Notice that it does not have multiple colors.
7. At the end of line 14, type **–ForegroundColor $color**.
8. Press F5 to run the script.
9. In the **Windows PowerShell ISE** dialog box, select the **In the future, do not show this message** check box, and then click **OK**.
10. Read the output. Notice that running services are green and services that are not running are red.
11. On line 16, type **Write-Host "A total of" $services.count "services were evaluated".**
12. Press F5 to run the script.
13. In the Commands pane, in the **Name** box, type **Write-Host**, and then click **Write-Host**.
14. In the **BackgroundColor** box, select **Gray**.
15. In the **ForegroundColor** box, select **Black**.
16. In the **Object** box, type **"Script execution is complete"**.
17. Click **Copy**, and then paste onto line 17 of the script.
18. Press F5 to run the script.
19. Press Ctrl+S to save the script.

20. Close Windows PowerShell ISE.

Run a script from the Windows PowerShell prompt

1. On the Start screen, type **PowerShell**, and then click **Windows PowerShell**.
2. At the Windows PowerShell command prompt, type **Set-Location E:\Labfiles\Mod03**, and then press Enter.
3. Type **.\Services.ps1**, and then press Enter.
4. Close the Windows PowerShell Command Prompt window.
5. Leave the virtual machines running for the next demonstration.

Demonstration: Using Windows PowerShell Remoting

Demonstration Steps

1. Ensure that you are signed in to LON-CL1 as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. To ensure that you have the correct execution policy in place, run the following command.

```
Set-ExecutionPolicy RemoteSigned
```

3. In the Execution Policy Change window, type **Y** to confirm the Execution Policy Change.
4. Run the following command.

```
Enable-PSremoting
```

   If you receive an error about a network connection being public, run the **Enable-PSremoting –SkipNetwork** cmdlet instead. Point out the error to students; it is an error they will see often.

5. Click **Yes** or press Y to confirm all dialog boxes.
6. To open a one-to-one connection to LON-DC1, type the following command, and then press Enter.

```
Enter-PSSession –ComputerName LON-DC1
```

7. To run the **Get-Process** command on LON-DC1, type the following command, and then press Enter.

```
Get-Process
```

8. To close the remote session, type the following command, and then press Enter.

```
Exit-PSSession
```

9. To run a cmdlet on multiple remote machines, type the following command, and then press Enter.

```
Invoke-Command –ComputerName LON-CL1,LON-DC1 –ScriptBlock { Get-EventLog –LogName
Security –Newest 10 }
```

10. Leave the virtual machines running for the next demonstration.

Lesson 3

Using Group Policy to Manage Windows 8.1

Contents:

Demonstration: Configuring Group Policy Settings

Demonstration Steps

Edit the local GPO to restrict use of registry editing tools

1. On LON-CL1, from the Start screen, type **group**, and then click **Edit group policy**.
2. In the Local Group Policy Editor, under User Configuration, expand **Administrative Templates**, click **System**, and then double-click **Prevent access to registry editing tools**.
3. In the Prevent Access to Registry Editing Tools window, click **Enabled**, and then click **OK**.
4. Close the Local Group Policy Editor.
5. On the Start screen, type **regedit**, and then click **regedit.exe**.
6. In the Registry Editor window, click **OK**.

Edit the local GPO to allow administrators to use registry editing tools

1. On the Start screen, type **mmc**, and then click **mmc.exe**.
2. In the MMC, click **File**, and then click **Add/Remove Snap-in**.
3. In the Add or Remove Snap-ins window, in the **Available snap-ins** box, click **Group Policy Object Editor**, and then click **Add**.
4. In the Select Group Policy Object window, click **Browse**.
5. In the Browse for a Group Policy Object window, click the **Users** tab, click **Administrators**, and then click **OK**.
6. In the Select Group Policy Object window, click **Finish**.
7. In the Add or Remove Snap-ins window, click **OK**.
8. In the MMC, expand **Local Computer\Administrators Policy**, expand **User Configuration**, expand **Administrative Templates**, click **System**, and then double-click **Prevent access to registry editing tools**.
9. In the Prevent Access to Registry Editing Tools window, click **Disabled**, and then click **OK**.
10. On the Start screen, type **regedit**, and then click **regedit.exe**.
11. Leave the virtual machines running for the next demonstration

Demonstration: Configuring Domain-Based GPOs

Demonstration Steps

Use the GPMC to create a new GPO

1. Switch to LON-DC1, and then sign in as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. In Server Manager, click **Tools**, and then click **Group Policy Management**.
3. If necessary, expand **Forest: Adatum.com**, expand **Domains**, and then expand **Adatum.com**.
4. Select and then right-click the **Group Policy Objects** folder, and then click **New**.
5. In the **New GPO** dialog box, in the **Name** box, type **Desktop**, and then click **OK**.

Configure Group Policy settings

1. In the GPMC, expand the **Group Policy Objects** folder, right-click the **Desktop** policy, and then click **Edit**.

2. In Group Policy Management Editor, under **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, expand **Local Policies**, and then click **Security Options**.
3. In the details pane, double-click **Interactive logon: Do not display last user name**.
4. In the **Interactive logon: Do not display last user name Properties** dialog box, select the **Define this policy setting** check box, click **Enabled**, and then click **OK**.
5. Under the Security Settings node, click **System Services**.
6. In the details pane, double-click **Windows Installer**.
7. In the **Windows Installer Properties** dialog box, select the **Define this policy setting** check box, and then click **OK**.
8. Under **User Configuration**, expand **Policies**, expand **Administrative Templates**, and then click **Start Menu and Taskbar**.
9. In the details pane, double-click **Remove Search link from Start Menu**.
10. In the **Remove Search link from Start Menu** dialog box, click **Enabled**, and then click **OK**.
11. Under the Administrative Templates folder, expand **Control Panel**, and then click **Display**.
12. In the details pane, double-click **Hide Settings tab**.
13. In the **Hide Settings tab** dialog box, click **Enabled**, and then click **OK**.
14. Close all open windows on LON-DC1.

Lesson 5

Configuring User State Virtualization

Contents:

Question and Answers

Overview of UE-V

Question: Can you use UE-V to synchronize application settings for a user who is already configured with Folder Redirection?

Answer: Yes, you can configure UE-V and Folder Redirection for the same user. We recommend using this method when you want to roam settings and user data between computers.

Module Review and Takeaways

Review Question(s)

Question: Your organization recently added computers running Windows 8.1 to the network. You have tried to connect to a remote computer running Windows 8.1 by using Event Viewer, but you cannot connect. You know that the remote computer is turned on. Why is this problem occurring, and how can you resolve it?

> **Answer:** By default, Windows Firewall does not allow remote management. You need to update Windows Firewall to allow remote management on the remote computer.

Question: One of the server administrators is complaining that he needs to use Remote Desktop and connect to a domain controller to manage user accounts. He wants to manage accounts without having to go through this process. In this case, what alternative will you suggest to administer user accounts from a computer running Windows 8.1?

> **Answer:** You can download and install the RSAT for Windows 8.1. RSAT includes the management tools found on Windows Server 2012 R2.

Question: You have configured a public-use computer in the lobby for visiting clients. This computer is not part of the AD DS domain. How can you secure this computer to prevent visiting clients from making changes to it and still allow administrators to have full access?

> **Answer:** As a first step, visiting clients should sign in with a standard user account. Then you can use a local Group Policy to restrict the standard user account further. To allow administrators to have full access, you can create a local Group Policy that removes restrictions from the items that are restricted for standard users.

Lab Review Questions and Answers

Lab A: Configure Windows 8.1 Settings by Using Management Tools

Question and Answers

Question: Why was Windows PowerShell remoting not enabled for LON-CL2?

Answer: When you set block inheritance on the MachineFloor organizational unit, you ensured that any GPOs that are applied to the domain will not be applied to computers in the MachineFloor organizational unit unless a policy at the domain-level is enforced. LON-CL2 was in the MachineFloor organizational unit.

Lab B: Configuring UE-V

Question and Answers

Question: After you copy the Settings Location Template to the settings location catalog, how long does it take for UE-V clients to update with the new Settings Location Template?

Answer: UE-V clients update with the settings from the settings location catalog once daily, at 3:30 A.M. by default, when the scheduled task triggers. If you want to update the UE-V client immediately with a new Settings Location Template, you should run ApplySettingsTemplateCatalog.exe.

Module 4

Implementing an Application Strategy for Windows 8.1

Contents:

Lesson 2

Managing Windows Store Apps

Contents:

Demonstration: How to Perform Sideloading of Windows Store Apps

Demonstration Steps

Enable Sideloading

To enable sideloading, you must first configure the appropriate Group Policy Object (GPO) settings:

1. Sign in to LON-CL1 as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. On the Start screen, type **gpedit.msc**, and then press Enter.
3. Under Local Computer Policy in the left navigation pane, expand **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then click **App Package Deployment**.
4. In the Results pane, double-click **Allow all trusted apps to install**.
5. In the **Allow all trusted apps to install** dialog box, click **Enabled**, and then click **OK**.
6. Close the **Local Group Policy Editor**.
7. Press the Windows logo key+**X**, and then on the **Administrative** menu, click **Windows PowerShell**.
8. In the Windows PowerShell® window, type **gpupdate /force**, and then press Enter.
9. Remain signed in on LON-CL1.

Install the root certificate

 **Note:** To sideload an app, Windows must trust the app. For purposes of this demonstration, the app will be signed with a self-signed certificate. You will need to install the root certificate on the client.

To install the root certificate, perform the following steps:

1. On LON-CL1, on the taskbar, click the **File Explorer** icon.
2. Expand drive **E:**, expand **Labfiles**, expand **Mod04**, expand **LeXProductsGrid**, right-click the **LeXProductsGrid81_1.1.0.2_AnyCPU.cer** file, and then click **Install Certificate**.
3. On the **Welcome to the Certificate Import Wizard** page, click **Local Machine**, and then click **Next**.
4. 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**.
5. In the **Certificate Import Wizard** dialog box, confirm that the import was successful, and then click **OK**.
6. Sign out of LON CL1.

 **Note:** Windows Store apps must be signed digitally. You can install them only on computers that trust the certification authority (CA) that provided the apps' signing certificate.

Install a Windows Store app

After you configure GPOs, you can install your apps. Apps are packaged in .appx files. To install a single app for a user, perform the following steps:

1. Sign in to LON-CL1 as **Adatum\Dan** with the password **Pa$$w0rd**.
2. On LON-CL1, on the Start screen, type **PowerShell**, and then press Enter.

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

```
add-appxpackage
E:\Labfiles\Mod04\LeXProductsGrid\LeXProductsGrid81_1.1.0.2_AnyCPU.appx
```

4. On the Start screen, type **TestAppTKL1**, and then press Enter.
5. Verify that the six groups of tiles display in the **TestAppTKL1** app.

Remove an installed Windows Store app

1. On LON-CL1, on the Start screen, type **TestApp**.
2. Right-click the **TestAppTKL1** tile, and then click **Uninstall** twice.
3. Sign out of LON-CL1.

Lesson 3

Configuring Internet Explorer Settings

Contents:

Question and Answers

Question: How does XSS Filter work to enhance security?

> **Answer:** XSS Filter has visibility into all requests and responses that are flowing through the browser. When the filter discovers a likely instance of XSS in a request, it identifies and neutralizes the attack if it is replayed in the server's response. XSS Filter helps protect users from website vulnerabilities. It does not ask difficult questions that users are unable to answer, and it does not harm the functionality on the website.

Demonstration: How to Configure Internet Explorer

Demonstration Steps

Enable Compatibility View for all websites

1. Sign in to the LON-CL1 as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. On the Start screen, click the **Desktop** tile.
3. On the desktop, on the taskbar, click the **Internet Explorer** icon.
4. Right-click the bar to the left of the home symbol, and then click **Menu bar**.
5. On the menu bar, click **Tools**, and then click **Compatibility View settings**.
6. In the **Compatibility View Settings** dialog box, select the **Display intranet sites in Compatibility View** check box, and then click **Close**.

Delete the browsing history

1. In Internet Explorer, in the address bar, type **http://LON-DC1**, and then press Enter.
2. Click the down arrow next to the address bar to confirm that the address you typed into it is stored.
3. In Internet Explorer, click **Tools**, and then click **Internet Options**.
4. Click the **General** tab. Under **Browsing history**, click **Delete**.
5. 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**.
6. Click **OK** to close Internet Options.
7. Confirm that there are no addresses stored in the address bar by clicking the down arrow next to the address bar.

Configure InPrivate Browsing

1. In Internet Explorer, on the **Tools** menu, click **InPrivate Browsing**.
2. In the address bar, type **http://LON-DC1**, and then press Enter.
3. To confirm the address you entered is not stored, click the down arrow next to the address bar.
4. Close the InPrivate Browsing window.

View the add-on management interface

1. In Internet Explorer, on the **Tools** menu, click **Manage Add-ons**.
2. In the left pane, click **Search Providers**.
3. In the right pane, click **Bing**.
4. In the left pane, click **Accelerators**.

5. In the left pane, click **Tracking Protection**.
6. Click **Close**.

Download a file

1. In the address bar, type **http://LON-DC1**, and then press Enter.
2. Click **Download Current Projects**.
3. In the **Internet Explorer** dialog box, click **Save**.
4. In the banner, click **View downloads**.
5. In the **View Downloads –Internet Explorer** dialog box, click **Open**.

   The file opens in Microsoft Excel®.
6. Close Excel and Internet Explorer, and then sign out from LON-CL1.

Lesson 4

Configuring Application Restrictions in an Enterprise

Contents:

Question and Answers

Question: What are some of the applications that you can use to apply an AppLocker rule?

> **Answer:** Answers will vary based on student experience.

Question: When testing AppLocker, you must consider carefully how you will organize rules between linked GPOs. What do you do if a GPO does not contain the default AppLocker rules?

> **Answer:** If a GPO does not contain the default rules, either add the rules directly to the GPO or add them to a GPO that links to it.

Question: What is the command to manually update the computer's policy, and where do you run it?

> **Answer:** The command to update a computer's policy manually is **gpupdate /force**, and you run it as an administrator at the command prompt or at a Windows PowerShell command prompt.

Demonstration: How to Configure AppLocker Rules

Demonstration Steps

Create a new executable rule

1. Sign in to LON-CL1 as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. On the Start screen, type **gpedit.msc**, and then press Enter.
3. In the Local Group Policy Editor, expand **Computer Configuration**, expand **Windows Settings**, expand **Security Settings**, expand **Application Control Policies**, and then double-click **AppLocker**.
4. Click and right-click **Executable Rules**, and then click **Create New Rule**.
5. On the **Create Executable Rules** page, click **Next**.
6. On the **Permissions** page, select **Deny**, and then click **Select**.
7. In the **Select User or Group** dialog box, in the **Enter the object names to select (examples)** box, type **Marketing**, click **Check Names**, click **OK**, and then click **Next**.
8. On the **Conditions** page, select **Path**, and then click **Next**.
9. Click **Browse Files**. In the **File name** box, type **C:\Windows\Regedit.exe**, and then click **Open**.
10. Click **Next** twice, and then click **Create**.
11. When prompted to create default rules, click **Yes**.

Automatically generate the script rules

1. Click and right-click **Script Rules**, and then click **Automatically Generate Rules**.
2. In the **Automatically Generate Script Rules** dialog box, on the **Folder and Permissions** page, click **Next** twice.
3. In the **Automatically Generate Script Rules** dialog box, click **Create**.
4. In the **AppLocker** dialog box, when prompted to create default rules, click **Yes**.

Demonstration: How to Enforce AppLocker Rules

Demonstration Steps

Enforce AppLocker rules

1. In the Local Group Policy Editor, click **AppLocker**, and then right-click and select **Properties**.

2. In the **Properties** dialog box, on the **Enforcement** tab, under **Executable rules**, click the **Configured** check box, and then select **Enforce rules**.
3. On the **Enforcement** tab, under **Script rules**, select the **Configured** check box, and then click **Audit only**, and then click **OK**.
4. Close the Local Group Policy Editor.

Confirm the executable rule enforcement

1. Press the Windows logo key+**X**, and on the **Administrative** menu, click **Windows PowerShell**.
2. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
gpupdate /force
```

3. Wait for the policy to update.
4. Press the Windows logo key+**X**, and then on the **Administrative** menu, click **Computer Management**.
5. In the Computer Management window, expand **Event Viewer**, expand **Windows Logs**, and then click **System**.
6. In the results pane, locate and click the latest event with the Event ID 1502.
7. On the **General** tab, review the event message details.
8. Expand **Services and Applications**, and then click **Services**.
9. Right-click the **Application Identity** service, and then click **Start**.
10. Sign out from LON-CL1.

Test the executable rule enforcement

1. Sign in to LON-CL1 as **Adatum\Adam** with the password **Pa$$w0rd**.
2. On the Start screen, type **cmd.exe**, and then press Enter.
3. At the command prompt, type the following command, and then press Enter:

```
Regedit.exe
```

4. Close the command prompt.
5. Sign out from LON-CL1.
6. Sign in to LON-CL1 as **Adatum\Administrator** with the password **Pa$$w0rd**.
7. Press the Windows logo key+**X**, and then on the **Administrative** menu, click **Computer Management**.
8. In the Computer Management window, expand **Event Viewer**, expand **Application and Services Logs**, expand **Microsoft**, expand **Windows**, expand **AppLocker**, and then double-click **EXE and DLL**.
9. Review the entries in the results pane. Locate Event ID 8004. This shows Adam's attempt to run Regedit.exe.
10. Close Computer Management.
11. Sign out of LON-CL1.

Module Review and Takeaways

Best Practices

Best Practices for AppLocker

- Before you create new rules manually or generate rules for a specific folder automatically, create the default rules. The default rules ensure that the key operating system files will be allowed to run for all users.
- When you test AppLocker, consider carefully how you will organize rules between linked GPOs. If a GPO does not contain the default rules, then either add the rules directly to the GPO, or add them to a GPO that links to it.
- After you create new rules, you must configure enforcement for the rule collections, and then refresh the computer's policy.
- By default, AppLocker rules do not allow users to open or run any files that are not specifically allowed. Administrators must maintain a current list of allowed applications.
- If AppLocker rules are defined in a GPO, only those rules are applied. To ensure interoperability between software restriction policies rules and AppLocker rules, define software restriction policies rules and AppLocker rules in different GPOs.
- When you set an AppLocker rule to Audit Only, the rule is not enforced. When a user runs an application that is included in the rule, the application is opened and runs normally, and information about that application is added to the AppLocker event log.

Best Practices for Internet Explorer 11

- Close all InPrivate tabs on Internet Explorer 11 to end your InPrivate session.
- Allow your Internet Explorer 11 favorites, history, and typed URLs to be synced across all Windows 8.1–based devices by signing in to Windows 8.1 with a Microsoft account.
- Change your default search provider by opening Internet Options, selecting the Programs tab, clicking Manage Add-ons, and selecting Search Providers.
- Do not turn off Enhanced Protected Mode in Internet Explorer 11 for the desktop.
- If Enhanced Protected Mode has been turned off, re-enable it under Security on the Advanced tab in Internet Options.
- Tracking protection is turned on by default for both versions of Internet Explorer 11.
- For optimal reliability and cross-browser compatibility, the best practices are to use standards-based technologies instead of critical plug-in functionality.
- When plug-in dependencies are removed, modern websites can benefit from better site interoperability.

Security Best Practices for IIS 8: Authentication

- When you use Windows authentication, turn on the extended protection feature, which helps protect from relaying of credentials and phishing attacks.
- Do not configure Anonymous authentication in addition to another authentication type for the same website, because this will likely cause authentication problems.
- Disable anonymous access to server directories and resources.
- Authenticate the user with a method that is not anonymous, prior to allowing write access to the website or File Transfer Protocol (FTP) site.

Review Question(s)

Question: What are some of the privacy features in Internet Explorer?

Answer: Microsoft InPrivate Browsing and Tracking Protection are two of the privacy features in Internet Explorer.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
AppLocker policies do not work correctly.	Before you can enforce AppLocker policies, you must start the Application Identity service.

Lab Review Questions and Answers

Lab A: Managing Windows Store Apps

Question and Answers

Question: Why do you think an organization would want to restrict users from accessing the Windows Store?

> **Answer:** Answers may vary. Organizations might have a corporate policy to restrict users from accessing the Windows Store. In addition, some organizations might want to provide access to the Windows Store only to the Bring Your Own Device (BYOD) users.

Lab B: Troubleshooting an Internet Explorer Issue

Question and Answers

Question: If a website states that it is secure, but there is no lock visible next to the address bar, what should you do?

> **Answer:** If there is no lock icon displayed next to the address bar, you will not be able to validate the safety of the website. Such a website is not secure, and you should not enter any personal or financial information on that website.

Lab C: Configuring AppLocker

Question and Answers

Question:

In the lab, you configured an executable path for the executable rule. What could you do if you wanted to allow users to run an earlier version of Windows Media Player?

> **Answer:** You can create a publisher executable rule and specify version 12.0.0.0 as the version to be restricted, citing Wmplayer.exe as the reference file. Different versions will then be able to run.

Question: Trevor has implemented AppLocker. Before he created the default rules, he created a custom rule that allowed all Windows processes to run except for Regedit.exe. Because he did not create the default rules first, he is blocked from performing administrative tasks. What does he need to do to resolve the issue?

> **Answer:** Trevor must restart the computer in safe mode, add the default rules, delete any Deny rules that are preventing access, and then refresh the computer policy.

Module 5

Managing Devices and Resource Access

Contents:

Lesson 1

Options for Managing Non-Domain Member Devices

Contents:

Question and Answers

Challenges of Managing Non-Domain Member Devices

Question: A company is using a client-server accounting app that cannot be installed on non-Microsoft operating systems. An employee wants to use the accounting app on his personal device, which is running a third-party operating system. How can the employee use the company accounting app from his device?

Answer: Because the accounting app cannot be installed locally on the employee's personal device, he or she can use the device to connect remotely to another computer that is running the app and use the app from that computer. For example, the employee can use Remote Desktop to connect to his or her domain member computer, which is running the app. Alternatively, the employee can connect to his or her virtual desktop if the company has deployed the Virtual Desktop Infrastructure (VDI) environment.

Comparing Domain Member and Non-Member Devices

Question: How can you manage non-domain member devices?

Answer: You cannot use Group Policies to manage devices that are not domain members. You must manage each non-domain member device individually, or use products, such as Windows Intune™ or System Center 2012 R2 Configuration Manager, to manage them centrally.

Security Enhancements for Devices That Are Not Joined to a Domain

Question: Can you use assigned access with an account that is a member of the Administrators group?

Answer: Assigned access allows you to limit user experience to a single Windows Store app. Therefore, you can use assigned access only with standard users. If the user is a member of the Administrators group, you cannot enable assigned access for him or her.

Question: How does remote business data removal enable you to comply with the company security policy?

Answer: Remote business data removal enables you to remotely wipe a local copy of company data from a user's device, while leaving user data on the device intact. By using this feature, you can remove company data from a lost device or from the device of an employee who has left the company.

Managing Non-Domain Member Devices by Using Windows Intune and Configuration Manager

Question: What must you do first before you can use Windows Intune to manage devices running Windows 8.1 by Windows Intune?

Answer: Before you can manage devices running Windows 8.1 by using Windows Intune, you must install the Windows Intune agent.

Lesson 2

Configuring Workplace Join

Contents:

Question and Answers

Workplace Join

Question: What is the difference between accessing company resources from a domain member device and accessing resources from a workplace-joined device?

> **Answer:** From domain member devices, you have a SSO experience when accessing domain resources, and you can access all domain resources to which you have permissions. From workplace-joined devices, you have a SSO experience when accessing company resources that support claims-based authentication only. For example, you can access internal company web apps with SSO, but you cannot access network shares on the company file server.

Scenarios for Using Workplace Join

Question: Can you join a Windows 8-based tablet to a workplace by using Workplace Join?

> **Answer:** No. Workplace Join is a Windows 8.1 feature, and it is not possible to use Workplace Join to join devices that are running previous versions of the Windows operating system.

Workplace Join Components

Question: What should you configure on a device to enable Workplace Join on it?

> **Answer:** To enable Workplace Join on a device, you must configure the device with network settings so that it can resolve company server names. You must also configure the device to trust the company CA.

Registering and Enrolling Devices

Question: What information do you need to join a device by using Workplace Join?

> **Answer:** When you want to join a device by using Workplace Join, you need to enter a user ID. A user ID looks like an email address, but it is actually a user principal name (UPN).

Demonstration: Enrolling Devices

Demonstration Steps

Configure Workplace Join on a device running Windows 8.1

1. On LON-CL4, on the taskbar, click the **Internet Explorer** icon.
2. In the Internet Explorer® address bar, type **https://lon-svr2.adatum.com/claimapp**, and then press Enter to access the company's internal web app.
3. In the **Windows Security** dialog box, in **User name** box, type **adatum\adam**, in the **Password** box, type **Pa$$w0rd**, and then click **OK**.
4. Confirm that the web page opens and Adam's claims display.
5. Close Internet Explorer.
6. On the taskbar, click the **Internet Explorer** icon.
7. In the Internet Explorer address bar, type **https://lon-svr2.adatum.com/claimapp**, and then press Enter.
8. Verify that the **Windows Security** dialog box displays again.
9. In the **Windows Security** dialog box, in the **User name** box, type **adatum\adam**, in the **Password** box, type **Pa$$w0rd**, and then click **OK**. This confirms that you will be asked for the credentials each time you access the company web app from the non-domain member device.

10. Close Internet Explorer.
11. On the Start screen, type **settings**, and then click **PC settings**.
12. On the PC settings screen, click **Network**.
13. On the Network screen, click **Workplace**. In the **Enter your user ID to get workplace access or turn on device management** box, type **adam@adatum.com**, and then click **Join**.
14. On the **Connecting to Adatum** page, verify that **adam@adatum.com** displays in the first box. In the second box, type **Pa$$w0rd**, and then click **Sign in**.
15. Verify that the device has joined your workplace network and that the label of the button changed from **Join** to **Leave**.
16. Move the pointer to the upper-left corner of the screen, and then click the **Desktop** tile.
17. On LON-DC1, on the Start screen, type **active**, and then click **Active Directory Users and Computers**.
18. In Active Directory Users and Computers, on the **View** menu, click **Advanced Features**. In the navigation pane, expand **Adatum.com**, and then click the **RegisteredDevices** node. Confirm that one object of type **msDS-Device** displays in the details pane. This object represents the LON-CL4 computer that you joined to the workplace network. Note the name of the **msDS-Device** object.
19. On LON-CL4, on the taskbar, click the **Internet Explorer** icon.
20. With the Internet Explorer window open, press the Alt key. On the **Tools** menu, click **Internet options**.
21. In the **Internet Options** dialog box, click the **Content** tab. In the **Certificates** section, click **Certificates**.
22. In the **Certificates** dialog box, on the **Personal** tab, verify that one certificate displays, and that it has a GUID in the **Issued To** box. This is the certificate that the Device Registration Service provided to the user when the device was joined to the workplace. Verify that the GUID is the same as the name of the **msDS-Device** object in Active Directory Users and Computers. Click **Close**, and then in the **Internet Options** dialog box, click **OK**.
23. In the Internet Explorer address bar, type **https://lon-svr2.adatum.com/claimapp**, and then press Enter to access the company's internal web app.
24. In the **Windows Security** dialog box, in the **User name** box, type **adatum\adam**. In the **Password** box, type **Pa$$w0rd**. Verify that the **Remember my credentials** check box is not selected, and then click **OK**.
25. Confirm that a web page opens and that Adam's claims display.
26. Verify that Claim Type **http://schemas.microsoft.com/2012/01/devicecontext/claims/identifier** has the same value as the name of the **msDS-Device** object in Active Directory Users and Computers.
27. Close Internet Explorer.
28. Re-open Internet Explorer, and then access the same company app at the **https://lon-svr2.adatum.com/claimapp** URL.
29. Verify that this time the web page opens without asking you for credentials. You are not asked for credentials because you accessed it from the workplace-joined device.
30. Close Internet Explorer.

Lesson 3

Configuring Work Folders and Remote Business Data Removal

Contents:

Question and Answers

Overview of Work Folders

Question: Can you share your Work Folders content with your coworkers?

Answer: By default, only a single user can access a Work Folder. However, one user can access a Work Folder from multiple devices. You cannot share your Work Folder, but you can make a copy of the Work Folder data and share the copy with coworkers. Note that the copy you make is a static copy, and it does not synchronize with the content of your Work Folder.

Components Required for Work Folders

Question: Can users access multiple Work Folders?

Answer: No. In Windows 8.1, users can access only a single Work Folder. Users can have sync access to multiple Work Folders, but only a single Work Folder will be used. They will not be able to synchronize other Work Folders, even if they have sync access permissions to them.

Configuring Work Folders

Question: Can you use Group Policy to set up Work Folders centrally to devices that are not domain joined?

Answer: No. By using Group Policy, you can set up Work Folders centrally only to domain member devices. If a device is not domain joined, you can use local Group Policy on the device to set up Work Folders.

Integrating Workplace Join and Work Folders

Question: Should a device be joined to a workplace for you to set up Work Folders on the device?

Answer: No. Workplace Join and Work Folders are two independent features. It is a bit easier to set up Work Folders on workplace-joined devices, because they already trust the company CA. However, you can set up Work Folders on any device that trusts the company CA.

Troubleshooting Work Folders

Question: Can you use either Work Folders Windows PowerShell cmdlets or Server Manager in Windows 8.1 by default?

Answer: No, because neither Server Manager nor Work Folders cmdlets are part of Windows 8.1. If you want to use them on computers running Windows 8.1, you need to install Remote Server Administration Tools (RSAT).

Comparing Work Folders with Other File Synchronization Technologies

Question: A user has three devices running Windows 8.1 and needs to keep files synchronized among all three devices. Two devices are domain member PCs running Windows 8.1. The other device is a tablet running Windows 8.1, and that is a workplace-joined device. The user's company has deployed two Windows Server 2012 R2 file servers. Which synchronization technology can the user use?

Answer: Because some of the devices are domain joined while others are not, the user cannot use Folder Redirection. The user cannot use OneDrive for Business because the company has not deployed Microsoft SharePoint® Server 2013. Therefore, the user could use either Work Folders or OneDrive. Because the user needs to synchronize work-related data, he or she should use Work Folders.

Demonstration: Configuring Work Folders

Demonstration Steps

Deploy Work Folders on a domain member device running Windows 8.1

1. On LON-DC1, in Server Manager, on the **Tools** menu, click **Group Policy Management**.
2. In Group Policy Management, in the navigation pane, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, and then select the **Marketing** organizational unit.
3. Right-click **Marketing**, and then click **Create a GPO in this domain, and Link it here**. In the **Name** box, type **Deploy Work Folders**, and then click **OK**.
4. In the navigation pane, expand **Marketing**. Right-click **Deploy Work Folders**, and then click **Edit**. The Group Policy Management Editor displays.
5. In Group Policy Management Editor, under **User Configuration**, in the navigation pane, expand **Policies**, expand **Administrative Templates**, expand **Windows Components**, and then click the **Work Folders** node.
6. In the details pane, right-click **Specify Work Folder settings**, and then click **Edit**.
7. In the **Specify Work Folder settings** dialog box, click **Enabled**. In the **Work Folders URL** box, type **https://lon-dc1.adatum.com**, select the **Force automatic setup** check box, and then click **OK**.
8. Close Group Policy Management Editor.
9. On LON-CL1, sign in as **adatum\adam** with the password **Pa$$w0rd**.
10. On the Start screen, click the **Desktop** tile.
11. On the desktop, on the taskbar, click the **File Explorer** icon.
12. In the This PC window, in the details pane, double-click **Work Folders**.
13. Right-click in the details pane, click **New**, click **Text Document**, and then name the file **On LON-CL1**.
14. On LON-CL4, on the taskbar, right-click the **Start** button, and then click **Control Panel**.
15. In Control Panel, in the **Search Control Panel** box, type **work**, and then click **Work Folders**.
16. On the **Manage Work Folders** page, click **Set up Work Folders**.
17. On the **Enter your work email address** page, click **Enter a Work Folders URL instead**.
18. On the **Enter a Work Folders URL** page, in the **Work Folders URL** box, type **https://lon-dc1.adatum.com**, and then click **Next**.
19. In the **Windows Security** dialog box, in the **User name** box, type **adatum\adam**. In the **Password** box, type **Pa$$w0rd**, and then click **OK**.
20. On the **Introducing Work Folders** page, review the local Work Folders location, and then click **Next**.
21. On the **Security policies** page, select the **I accept these policies on my PC** check box, and then click **Set up Work Folders**.
22. On the **Work Folders has started syncing with this PC** page, click **Close**.
23. In the Work Folders window, verify that the **On LON-CL1.txt** file displays.
24. In the WorkFolders window, right-click in the details pane, point to **New**, click **Text Document**, and then name the file **On LON-CL4.txt**.
25. On LON-CL1, in the Work Folders window, verify that only the **On LON-CL1** file displays.

26. In the details pane, right-click and click **Sync Now**. Press the F5 key to refresh the view, and verify that the **On LON-CL1** and **On LON-CL4** files display.

Lab Review Questions and Answers

Lab: Configuring Resource Access for Non-Domain Member Devices

Question and Answers

Question: Do you need to grant additional permissions to a domain user to be able to join his or her device to a workplace by using Workplace Join?

Answer: No, you do not need to grant the user any additional permissions. Domain users have sufficient permissions to join their devices to a workplace by using Workplace Join.

Question: How can you verify if a device is joined to a workplace?

Answer: On the device, you can open the PC Settings screen, navigate to the Network screen, and then select Workplace to verify if the device is joined to a workplace. You can also verify if the user has the digital certificate that was issued by the Device Registration Service. A domain administrator can find the certificate in the RegisteredDevices AD DS container.

Question: Can you join the same device to a workplace that your coworker already joined by using Workplace Join?

Answer: Yes. If you have a domain account, you can join a device to a workplace, even if it is already workplace-joined by somebody else. Workplace Join is performed once per user per device, and it associates the domain user account with the device. This means that each user who is using the device can join the device to the workplace by using Workplace Join. Workplace Join follows a different concept from joining a device to a domain, which is a system-wide configuration.

Question: Can a user access the same Work Folder from domain member devices and from workgroup devices?

Answer: Yes, the user can access the same Work Folder from all devices, regardless of his or her domain membership. If a user is accessing Work Folders by using the same domain credentials from all the devices, the user will access the same content.

Question: Can you access the content of Work Folders from a device that does not support Work Folders?

Answer: You can connect to Work Folders only from devices that support Work Folders. However, you can create an SMB share that points to the same folder on the Windows Server 2012 R2 file server. This will enable users to access the content from any device from which you can connect to the shared folder.

Question: Can you access Work Folders content on a PC without network connectivity?

Answer: A PC that supports Work Folders creates a local copy of the Work Folders content. If network connectivity is not available, you can still access and modify the local copy. When the network connectivity is restored, local changes will transparently synchronize with the Work Folder content on the file server.

Module 6

Securing Windows 8.1 Devices

Contents:

Lesson 1

Authentication and Authorization in Windows 8.1

Contents:

Question and Answers

The Process of Authentication and Authorization

Question: Which authentication method is used when a client computer that is running Windows 8.1 logs on to AD DS?

> **Answer:** Windows operating systems use the Kerberos v5 protocol unless an enterprise is using smart cards. In such cases, a Windows operating system uses the certificate mapping method for authentication.

Demonstration: Configuring a Picture Password or PIN for Authentication

Demonstration Steps

Create a picture password to sign in with gestures

1. Sign in to LON-CL4 as **Admin** with the password **Pa$$w0rd**.
2. On the Start screen, type **Picture**, and then click **Set up picture password**.
3. In the Sign-in Options window, under the **Picture password** option, click **Add**.
4. In the **Create a picture password** dialog box, type the password **Pa$$w0rd** to verify your account information, and then click **OK**.
5. In the Welcome to picture password window, click **Choose picture**.
6. After you have selected a picture, click **Open**.
7. Drag the picture to the correct position, and then click **Use this picture**.
8. Follow the onscreen instructions, and then draw three gestures on your picture.
9. Repeat the pattern to confirm, and then click **Finish**.
10. Swipe down from the top middle of the app to close the Sign-in account app.

Create a personal identification number (PIN) password to sign in

1. On the Start screen, type **PIN**, and then click **Set up PIN sign-in**.
2. In the Sign-in Options window, under the **PIN** option, click **Add**.
3. Type the password **Pa$$w0rd** to verify your account information.
4. On the **Create a PIN** page, follow the on-screen instructions, type a four-digit PIN password, and then click **Finish**.
5. Swipe down from the top middle of the app to close the Sign-in account app.

To prepare for the next demonstration

When you finish the demo, revert the virtual machines to their initial state.

1. On the host computer, start Hyper-V Manager.
2. In the **Virtual Machines** list, right-click **20689D-LON-CL4**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.

Lesson 2

Securing Data by Using BitLocker

Contents:

Question and Answers

BitLocker Modes

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

> **Answer:** Computers without TPM 1.2 or TPM 2.0 will not be able to use the system-integrity verification that BitLocker provides during the startup process.

Question: You just received a new batch of 10 laptops that do not have a TPM. Is it still possible to protect the contents of the hard drive by using BitLocker?

> **Answer:** Yes, but you must configure the startup to require a password or a startup key on a USB drive.

Microsoft BitLocker Administration and Monitoring 2.0 SP1

Question: How can you use Microsoft BitLocker Administration and Monitoring 2.0 to reduce the amount of time that the help desk needs to spend recovering a BitLocker unlock key for a remote user?

> **Answer:** You can enable the Microsoft BitLocker Administration and Monitoring 2.0 self-service portal to allow users to recover a BitLocker recovery password by themselves, without calling the help desk.

Configuring BitLocker

Question: When turning on BitLocker on a computer that has TPM 1.2, why should you save the recovery password?

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

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 the 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.

Comparing EFS and BitLocker

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

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

Lesson 3

Configuring UAC

Contents:

Question and Answers

How UAC Works

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

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

Configuring UAC Notification Settings

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

> **Answer:** UAC security settings configured in Local Security Policy and in the Action Center in Control Panel are the two configuration options that combine to produce the end-user elevation experience.

Configuring UAC with GPOs

Question: Which UAC setting detects when an application is being installed in Windows 8.1?

> **Answer:** The Detect Application Installations And Prompt for Elevation setting of User Account Control detects when an application is being installed in Windows 8.1.

Guidelines for Implementing UAC

Question: If a user approaches you and asks that you disable UAC on her computer because it is annoying her with frequent prompts, how would you respond?

> **Answer:** Answers may vary. However, you should try to understand what the user is doing to cause UAC to be displayed. Also, educate the user on the benefits of UAC and its ability to help keep the system secure from malicious attacks.

Demonstration: Configuring UAC with GPOs

Demonstration Steps

View the current User Account Control (UAC) settings

1. Sign in to LON-CL1 as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. Open the Administrative menu by pressing the Windows logo key+X, and then click **Run**.
3. In the **Open** box, type **gpedit.msc**, and then press Enter.
4. In the Local Group Policy Editor, expand **Computer Configuration**, expand **Windows Settings**, expand **Security Settings**, expand **Local Policies**, and then click **Security Options**.

Configure UAC settings

1. In the results pane, double-click **User Account Control: Behavior of the elevation prompt for standard users**.
2. In the **User Account Control: Behavior of the elevation prompt for standard users** dialog box, click **Automatically deny elevation requests**, and then click **OK**.
3. Close Local Group Policy Editor console.
4. Sign out.

Test the UAC settings

1. Sign in to LON-CL1 as **Adatum\Holly** with the password **Pa$$w0rd**.
2. On the Start screen, type **UAC**, and then select **Change User Account Control settings**.
3. In the **User Account Control Settings** dialog box click **OK** .
4. Sign out.

Reconfigure UAC settings

1. Sign in to LON-CL1 as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. On the Start screen, type **gpedit.msc**, and then press Enter.
3. In the Local Group Policy Editor, expand **Computer Configuration**, expand **Windows Settings**, 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, click **Prompt for credentials**, and then click **OK**.
6. Close Local Group Policy Editor console.
7. Sign out of LON-CL1.

Test these settings

1. Sign in to LON-CL1 as **Adatum\Holly** with the password **Pa$$w0rd**.
2. On the Start screen, type **UAC**, and then select **Change User Account Control settings**.

   Windows displays the User Account Control prompt.
3. In the **User name** box, type **Administrator**.
4. In the **Password** box, type **Pa$$w0rd**, and then click **Yes**.
5. Close the **User Account Control Settings** dialog box.
6. Sign out.

Lesson 4

Guarding Against Malware

Contents:

Question and Answers

Configuring Scanning Options in Windows Defender

Question:

What effect could malware such as a rootkit have on a computer? Additionally, if a user suspected malware in the form of a rootkit, what action should the user take?

> **Answer:** Answers may vary. The user should report the problem or suspicion to the help desk support team, or attempt to remove the malware by using the Windows Defender Offline tool.

Demonstration: Configuring Windows SmartScreen and Windows Defender Settings

Demonstration Steps

Configure Windows SmartScreen® settings

1. Sign in to the LON-CL1 as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. On the Start screen, type **action**, and then click **Action Center**.
3. Click **Change Windows SmartScreen settings**.
4. Review the available settings, close the **Windows SmartScreen** dialog box, and then close Action Center.

Configure Windows Defender settings to perform a quick scan

1. Press Windows logo key+X, and then on the Administrative menu, click **Control Panel**.
2. Click **View by**, select **Large Icons**, and then click **Windows Defender**.
3. On the **Home** tab, ensure the **Quick** scan option is selected.
4. Click **Scan now**.
5. Review the results.
6. Close Windows Defender.

Configure Windows Defender settings to test malware detection

1. Open File Explorer, and then browse to **E:\Labfiles\Mod06\Malware**.
2. In the Malware folder, open sample.txt in Notepad. The sample.txt file contains a text string that is used to test malware detection.
3. In the sample.txt file, delete both instances of **<remove>**, including the brackets and the leading space in the first line.
4. In Notepad, save the file, and then close the file. Immediately, Windows Defender detects a potential threat.
5. Shortly thereafter, the sample.txt will be removed from the Malware folder.

Examine the Windows Defender history

1. Click the **Settings** charm, and then click **Control Panel**.
2. Click **Windows Defender**.
3. In the Windows Defender window, click the **History** tab.
4. Click **View details**.

5. Review the results.
6. Select the check box for **Virus:DOS/EICAR_Test_File**, and then click **Remove**.
7. Close all open windows.

To prepare for the next demonstration

When you finish the demo, revert the virtual machines to their initial state.

1. On the host computer, start Hyper-V Manager.
2. In the **Virtual Machines** list, right-click **20689D-LON-CL1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20689D-LON-DC1** and **20689D-LON-CL2.**

Lesson 5

Configuring Windows Firewall

Contents:

Question and Answers

Windows Firewall with Advanced Security Settings

Question: What are the types of IPsec rules available and when would an organization configure IPsec rules?

> **Answer:** Answers may vary. IPsec rules should be used whenever an organization requires maximum security for connections between two computers that must be authenticated or encrypted. IPsec rules can be of the following types: Isolation rules, authentication exemption rules, server-to-server rules, tunnel rules or custom rules.

Demonstration: Configuring Inbound and Outbound Rules by Using GPOs

Demonstration Steps

Configure an inbound rule by using a GPO

1. Sign in to LON-DC1 as **Adatum\Administrator** with the password **Pa$$w0rd**
2. Right-click the **Start** button, click **Windows PowerShell (Admin)**, type **PING LON-CL1**, and then press Enter.

   Notice that ping is allowed.
3. Sign in to LON-CL1 as **Adatum\Administrator** with the password **Pa$$w0rd**.
4. Select **Run** from the Administrative menu by pressing the Windows logo key+X, and then type **gpedit.msc**.
5. In Local Group Policy Editor, navigate to **Computer Configuration/Windows Settings/Security Settings/Windows Firewall with Advanced Security/Windows Firewall with Advanced Security – Local Group Policy Object**.
6. In the navigation tree, click **Inbound Rules**, right-click **Inbound Rules**, and then click **New Rule**.
7. In the New Inbound Rule Wizard, select **Custom**, and then click **Next** twice.
8. On the **Protocol and Ports** page, select the ICMPv4 protocol type, and the click **Next** twice.
9. On the **Action** page, select **Block the connection**, and then click **Next** twice.
10. On the **Name** page, type **Deny ping** as the rule name, and then click **Finish** to exit the wizard.
11. Switch to LON-DC1, and then verify that you cannot now ping LON-CL1 by repeating the step 2 above.

Configure an outbound rule by using GPO

1. Sign in to LON-CL1 as **Adatum\Administrator** with the password **Pa$$w0rd.**
2. Right-click the **Start** button, click **Windows PowerShell (Admin)**, type **PING LON-DC1**, and then press Enter.

   Notice that ping is allowed.
3. Select **Run** from the Administrative menu by pressing Windows logo key+X, and then type **gpedit.msc**.
4. In Local Group Policy Editor, navigate to **Computer Configuration/Windows Settings/Security Settings/Windows Firewall with Advanced Security/Windows Firewall with Advanced Security – Local Group Policy Object**.
5. In the navigation tree, click **Outbound Rules**, right-click **Outbound Rules**, and then click **New Rule**.

6. In the New Inbound Rule Wizard, select **Custom**, and then click **Next** twice.
7. On the **Protocol and Ports** page, select the ICMPv4 protocol type, and then click **Next** twice.
8. On the **Action** page, select **Block the connection**, and then click **Next** twice.
9. On the **Name** page, type **Deny ping** as the rule name, and then click **Finish** to exit the wizard.
10. Right-click the **Start** button, click **Windows PowerShell (Admin)**, type **PING LON-DC1**, and then press Enter.

    Notice that ping is not allowed.
11. Sign out of LON-CL1.

To prepare for the next module

When you finish the demo, revert the virtual machines to their initial state.

1. On the host computer, start Hyper-V Manager.
2. In the **Virtual Machines** list, right-click **20689D-LON-CL1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20689D-LON-DC1**.

Module Review and Takeaways

Best Practice

Best Practices for User Account Control

- UAC Security Settings are configurable in the local Security Policy Manager (secpol.msc) or the Local Group Policy Editor (gpedit.msc). However, in most corporate environments, Group Policy is preferred because it can be centrally managed and controlled. There are nine GPO settings that you can configure for UAC.
- Because the user experience can be configured with Group Policy, there can be different user experiences, depending on policy settings. The configuration choices that are made in your environment affect the prompts and dialog boxes that standard users, administrators, or both, can view. For example, you may require administrative permissions to change the UAC setting to Always Notify Me or Always Notify Me and Wait For My Response. With this type of configuration, a yellow notification appears at the bottom of the User Account Control Settings page, indicating the requirement.
- Although UAC enables you to sign in by using an administrative user account to perform everyday user tasks, it is still good practice to sign in by using a standard user account for these everyday tasks. Sign in as an administrator only when necessary.

Best Practices for BitLocker

BitLocker stores its own encryption and decryption key in a hardware device that is separate from the hard disk, so you must have one of the following:

- A computer with TPM.
- A removable USB storage device, such as a USB flash drive. If your computer does not have TPM 1.2 or newer, BitLocker stores its key on the memory device.
- The most secure implementation of BitLocker takes advantage of the enhanced security capabilities of TPM 1.2.
- On computers that do not have TPM 1.2, you can still use BitLocker to encrypt the Windows operating system volume. However, this implementation will require the user to insert a USB startup key to start the computer or resume from hibernation and does not provide the prestartup system-integrity verification that BitLocker offers when it works with a TPM.
- Encrypt drives before adding data.

Best Practices for Configuring Windows Firewall with Advanced Security

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

- Configure a local or remote computer by using either the Windows Firewall with Advanced Security console or the cmdlets in the PowerShell NetSecurity module.
- Configure Windows Firewall with Advanced Security settings by using the Group Policy Management Console or the cmdlets in the Windows PowerShell NetSecurity module.
- If you are configuring the Windows Firewall with Advanced Security settings by using Group Policy, you need to ensure that the Windows Firewall service has the necessary NTFS write access permissions to application locations.
- If you deploy Windows Firewall with Advanced Security by using Group Policy and then block outbound connections, ensure that you enable the Group Policy outbound rules, and do full testing in a test environment before deploying. Otherwise, you might prevent all of the computers that receive the policy from updating the policy in the future, unless you intervene manually.

Best Practices for Windows Defender

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

- When you use Windows Defender, you must have current definitions.
- To help keep your definitions current, Windows Defender automatically installs new definitions as they are released. You also can set Windows Defender to check online for updated definitions before it scans.
- When scanning your computer, select the advanced option of Create a System Restore Point Before Applying Actions To Detected Items

Review Question(s)

Question: When you implement UAC, what happens to standard users and administrative users when they perform a task that requires administrative privileges?

> **Answer:** For standard users, UAC prompts the user for the credentials of a user with administrative privileges. For administrative users, UAC prompts the user for permission to complete the task.

Question: What are the requirements for BitLocker to store its own encryption and decryption key in a hardware device that is separate from the hard disk?

> **Answer:** This situation requires a computer with TPM or a removable USB flash drive. If your computer does not have TPM 1.2 or newer, BitLocker stores its key on the USB flash drive.

Question: An administrator configures Group Policy to require that data can be saved only on data volumes that are protected by BitLocker. Specifically, the administrator enables the Deny Write Access To Removable Drives Not Protected By BitLocker setting and deploys it to the domain. Meanwhile, an end user inserts a USB flash drive that is not protected with BitLocker. What will happen, and how can the user resolve the situation?

> **Answer:** Because the USB flash drive is not protected with BitLocker, Windows 8.1 displays an informational dialog box indicating that the device must be encrypted with BitLocker. From this dialog box, the user can choose to launch the BitLocker wizard to encrypt the volume, or continue working with the device as read-only.

Lab Review Questions and Answers

Lab B: Configuring Inbound and Outbound Firewall Rules

Question and Answers

Question: A user attempts to connect to their office computer by using his or her Microsoft Surface™ 2 Pro device from a meeting room, but the connection fails. What is the most likely cause of this problem?

Answer: Answers may vary. Windows Firewall blocks remote desktop connections by default. The office computer will need to be configured to allow remote connections.

Module 7

Configuring Remote Access

Contents:

Lesson 1

Overview of DirectAccess

Contents:

Demonstration: Running the Getting Started Wizard

Demonstration Steps

Add LON-CL1 to the DA_Clients group

1. On LON-DC1, in Server Manager, click **Tools**, and then click **Active Directory Users and Computers**.
2. In Active Directory® Users and Computers, double-click the **Users** container.
3. Right-click **DA_Clients**, and then click **Properties**.
4. In the **Properties** dialog box, click the **Members** tab, and then click **Add**.
5. Click **Object Types**, select **Computers**, and then click **OK**.
6. Type **LON-CL1**, and then click **OK**.
7. In the **DA_Clients Properties** dialog box, click **OK**.
8. Close Active Directory Users and Computers.

Configure DirectAccess by running the Getting Started Wizard

1. On LON-SVR2, in Server Manager, click **Tools**, and then select **Remote Access Management**.
2. In the Remote Access Management console, under Configuration, click **DirectAccess and VPN**.
3. Click **Run the Getting Started Wizard**.
4. On the **Configure Remote Access** page, click **Deploy DirectAccess only**.
5. Verify that **Edge** is selected, and in the **Type the public name or IPv4 address used by clients to connect to the Remote Access server** box, type **131.107.0.2**, and then click **Next**.
6. On the **Configure Remote Access** page, click the **here** link.
7. On the **Remote Access Review** page, verify that two Group Policy Objects (GPOs) have been created: DirectAccess Server Settings and DirectAccess Client Settings.
8. Next to Remote Clients, click **Change**.
9. In the Remote Access Setup window, click **Domain Computers (ADATUM\Domain Computers)**, and then click **Remove**.
10. Click **Add**.
11. In the Select Groups window, type **DA_Clients**, and then click **OK**.
12. Clear the **Enable DirectAccess for mobile computers only** check box, and then click **Next**.
13. On the **DirectAccess Client Setup** page, click **Finish**.
14. On the **Remote Access Review** page, click **OK**.
15. On the **Configure Remote Access** page, click **Finish** to finish the DirectAccess wizard.
16. In the **Applying Getting Started Wizard Settings** dialog box, click **Close**.
17. Restart LON-SVR2 and LON-CL1.

Demonstration: Identifying the Getting Started Wizard Settings

Demonstration Steps

1. On LON-SVR2, switch to the Server Manager console, click **Tools**, and then click **Remote Access Management**.
2. In the Remote Access Management console, in the left pane, click **DirectAccess and VPN**.

3. In the Remote Access Setup window, under the image of the client computer labeled as **Step 1 Remote Clients**, click **Edit**.
4. In the DirectAccess Client Setup window, click **Deployment Scenario** and review the default settings, click **Select Groups** and review the default settings, and then click **Network Connectivity Assistant** and review the default settings.
5. Click **Cancel**, and then click **OK**.
6. In the Remote Access Setup window, under the image of the client computer labeled as **Step 2 Remote Access Server**, click **Edit**.
7. In the Remote Access Server Setup window, click **Network Topology** and review the default settings, click **Network Adapters** and review the default settings, and then click **Authentication** and review the default settings.
8. Click **Cancel**, and then click **OK**.
9. In the Remote Access Setup window, under the image of the client computer labeled as **Step 3 Infrastructure Servers**, click **Edit**.
10. In the Infrastructure Server Setup window, click **Network Location Server** and review the default settings, click **DNS** and review the default settings, click **DNS Suffix Search List** and review the default settings, and then click **Management** and review the default settings.
11. Click **Cancel**, and then click **OK**.
12. In the Remote Access Setup window, under the image of the client computer labeled as **Step 4 Application Servers**, click **Edit**.
13. In the DirectAccess Application Server Setup window, review the default settings, click **Cancel**, and then click **OK**.
14. Close all open windows.

Lesson 2

Advanced DirectAccess Infrastructure

Contents:

Demonstration: Monitoring and Troubleshooting DirectAccess Connectivity

Demonstration Steps

Verify DirectAccess configuration for LON-SVR2

1. Sign in to LON-SVR2 as **Adatum\Administrator** with password **Pa$$w0rd**.
2. In Server Manager, click **Tools**, and then click **Remote Access Management**.
3. In the Remote Access Management console, click **Operations Status**.

All components should have a Status of Working and a green check mark beside them. If this is not the case, click **Refresh** to update the Operations Status view. You might have to do this several times. If Status does not show as working after 5-10 minutes, restart LON-SVR2 and repeat steps 1-3.

Verify DirectAccess Group Policy configuration settings for Windows 8.1 clients

1. Switch to LON-CL1 and sign in as **Adatum\Administrator** with a password of **Pa$$w0rd**.
2. On LON-CL1, open the Command Prompt window, and then type the following commands. Press Enter after each command.

```
gpupdate /force
gpresult /R
```

3. Verify that **DirectAccess Client Settings GPO** displays in the list of the Applied Policy objects for the Computer Settings.

Move the client computer to the Internet virtual network

1. Switch to LON-CL1.
2. From the Start screen, type **ncpa.cpl**, and then press Enter.
3. In the Network Connections window, right-click the **Ethernet** connection, and then click **Disable**.
4. In the Network Connections window, right-click the **Ethernet 2** connection, and then click **Enable**.
5. Close all open windows and restart LON-CL1

Verify connectivity to the DirectAccess server

1. Sign in to LON-CL1 as **Adatum\Administrator** with a password of **Pa$$w0rd**.
2. On LON-CL1, at a command prompt, type the following command.

```
ipconfig
```

3. Notice the IP address that starts with 2002. This is an Internet Protocol over Secure Hypertext Transfer Protocol (IP-HTTPS) address.
4. At the command prompt, type the following command, and then press Enter.

```
Netsh name show effectivepolicy
```

Monitoring DirectAccess connectivity

1. Switch to LON-SVR2.
2. On LON-SVR2, open the Remote Access Management console, and then in the left pane, click **Dashboard**.
3. Review the information in the central pane, under the **DirectAccess and VPN Client Status**.

4. In the left pane, click **Remote Client Status**, and then in the central pane, review the information under the **Connected Clients** list.
5. In the left pane, click **Reporting**, and then in the central pane, click **Configure Accounting**.
6. In the Configure Accounting window, under **Select Accounting Method**, click **Use inbox accounting**, click **Apply**, and then click **Close**.
7. In the central pane, under **Remote Access Reporting**, review the options for monitoring historical data.

Lesson 3

Configuring VPN Access

Contents:

Demonstration: Configuring a VPN Connection

Demonstration Steps

Create a new VPN connection

1. Switch to LON-CL1, and then sign in as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. Open Control Panel.
3. In Control Panel, under Network and Internet, click **View network status and tasks**.
4. In the Network and Sharing Center window, under Change your networking settings, click **Set up a new connection or network**.
5. In the **Choose a connection option** dialog box, click **Connect to a workplace**, and then click **Next**.
6. In the **Connect to a workplace** dialog box, click **Use my Internet connection (VPN)**, and then when prompted, select **I'll set up an Internet connection later**.
7. In the **Type the Internet address to connect to** dialog box, specify an **Internet address** of **172.16.0.10** and a **Destination name** of **HQ**, and then click **Create**.

Configure the VPN connection

1. In the Network and Sharing Center window, click **Change adapter settings**.
2. On the **Network Connections** page, right-click **HQ**, and then click **Properties**.
3. In the **HQ Properties** dialog box, click the **Security** tab, and then click **Allow these protocols**.
4. In the **Type of VPN** list, click **Point-to-Point Tunneling Protocol (PPTP)**, and then click **OK**.
5. On the **Network Connections** page, right-click **HQ**, and then click **Connect/Disconnect**.

Test the connection

1. In the **Networks** list on the right side, click **HQ**, and then click **Connect**.
2. Enter the following information in the **Network Authentication** boxes, and then click **OK**:
   - User name: **Adatum\Administrator**
   - Password: **Pa$$w0rd**
3. The VPN connects. Right-click **HQ**, and then click **Connect/Disconnect**.
4. Click **HQ**, and then click **Disconnect**.

Module Review and Takeaways

Question: What are the main benefits of using DirectAccess for providing remote connectivity?

Answer: The main benefits of using DirectAccess for providing remote connectivity are:

- Always-on connectivity. When a user is connected to the Internet, the user is also connected to the intranet.
- Same user experience, regardless of whether the user is connected locally or remotely.
- Bidirectional access. When a client computer accesses the intranet, the computer is also connected and managed.
- Improved security. Administrators can set and control the intranet resources that are accessible through DirectAccess.

Question: How do you configure DirectAccess clients?

Answer: To configure DirectAccess clients, use Group Policy. When you use the Getting Started Wizard to configure DirectAccess, two GPOs are created and linked to the domain. These two GPOs define DirectAccess-related settings and are applied to DirectAccess clients.

Question: What type of remote access VPN solutions can you provide to Windows 8.1–based clients?

Answer: You can configure the following remote access solutions by using VPN in Windows 8.1:

- Secure remote access to internal network resources for users who are on the Internet. Windows 8.1 computers act as VPN clients that connect to Windows Server 2012 R2, which acts as a VPN server.
- Secure communication between network resources that are located in different geographical locations or sites. This solution is called site-to-site VPN. In each site, Windows Server 2012 R2 acts as a VPN server that encrypts communication between the sites. This option does not require additional configuration for client computers, but it still provides VPN connectivity.
- Secure VPN connections from client computers to supported third-party VPN server solutions.

Lab Review Questions and Answers

Lab: Implementing DirectAccess by Using the Getting Started Wizard

Question and Answers

Question: How will you configure IPv6 addresses for client computers running Windows 8.1 to use DirectAccess?

Answer: Global unicast IPv6 addresses are automatically generated based on the network infrastructure. As a result, Windows 8.1–based clients can connect to an organization's intranet and the Internet by using DirectAccess, without requiring that you configure IPv6 addresses.

Module 8

Monitoring and Recovering Windows 8.1

Contents:

Lesson 1

Monitoring and Troubleshooting Performance in Windows 8.1

Contents:

Question and Answers

Discussion: Common Issues with System Performance

Question: What factors can influence system performance?

Answer: Answer will vary, but may include the following:

- Access speed of the physical hard disks.
- Memory available for all running processes.
- Fastest speed of the processor.
- Maximum throughput of the network interfaces.
- Application resource consumption.
- A faulty or poor configuration of the components mentioned above.

Demonstration: Using Performance Monitor to Gather Performance-Related Data

Demonstration Steps

Open Performance Monitor

1. On LON-CL1, on the Start screen, type **perfmon**, and then click the **perfmon.exe** tile.
2. In the Performance Monitor window, click the **Performance Monitor** node. Notice that only **% Processor Time** is displayed by default.

Add new values to the chart

1. Click the plus sign (**+)** in the toolbar to add an additional counter.
2. In the Available Counters area, expand **PhysicalDisk**, and then click **% Idle Time**.
3. In the **Instances of selected object** box, click **0 C:**, click **Add**, and then click **OK**.
4. Right-click **% Idle Time**, and then click **Properties**.
5. In the **Color** box, click **green**, and then click **OK**.

Create a data collector set

1. In the left pane, expand **Data Collector Sets**, and then click **User Defined**.
2. Right-click **User Defined**, point to **New**, and then click **Data Collector Set**.
3. In the **Name** box, type **CPU and Disk Activity**, and then click **Next**.
4. In the **Template Data Collector Set** box, click **Basic**, and then click **Next**. We recommend that you use a template.
5. Click **Next** to accept the default storage location for the data.
6. Click **Open properties for this data collector set**, and then click **Finish**. On the **General** tab, you can configure general information about the data collector set and the credentials that the data collector set uses when it is running.
7. Click the **Directory** tab. This tab lets you define information on how the collected data is stored.
8. Click the **Security** tab. This tab lets you configure which users can change this data collector set.
9. Click the **Schedule** tab. This tab lets you define when the data collector set is active and collecting data.

10. Click the **Stop Condition** tab. This tab lets you define when data collection is stopped, based either on time or data that is collected.
11. Click the **Task** tab. This tab lets you run a scheduled task when the data collector set stops.
12. Click **Cancel**. Notice that there are three kinds of logs in the right pane:
    - **Performance Counter** collects data that you can view in the Performance Monitor.
    - **Kernel Trace** collects detailed information about system events and activities.
    - **Configuration** records changes to registry keys.
13. In the right pane, double-click **Performance Counter**. Notice that all Processor counters are collected by default.
14. Click **Add**.
15. In the Available Counters area, click **PhysicalDisk**, click **Add**, and then click **OK**. All of the counters for the PhysicalDisk object are now added.
16. Click **OK**.
17. In the left pane, right-click **CPU and Disk Activity**, and then click **Start**.

Examine a report

1. Wait a few moments, and the data collector set will stop automatically.
2. Right-click **CPU and Disk Activity**, and then click **Latest Report**. This report shows the data that is collected by the data collector set.
3. Close the Performance Monitor window.

Lesson 2

Troubleshooting Windows 8.1 Startup

Contents:

Demonstration: Resolving Startup Problems

Demonstration Steps

Access Windows RE to perform startup repair options

1. On your host computer, in the **20689D-LON-CL1 on localhost - Virtual Machine Connection** dialog box, on the **Media** menu, point to **DVD Drive**, and then click **Insert Disk**.
2. In the **Open** dialog box, in the **File name** box, type **C:\Program Files\Microsoft Learning\20689\Drives\ Win81Ent_EVAL.iso**, and then click **Open**.
3. On LON_CL1, from the Desktop, right-click the **Start** button, click **Shut down or sign out**, and then click **Restart**.
4. When you see the **Press any key to boot from CD or DVD** message, press Spacebar. Setup loads.
5. When prompted in the **Windows Setup** dialog box, click **Next**.
6. On the **Windows Setup** page, click **Repair your computer**.
7. On the **Choose an option** page, click **Troubleshoot**.
8. On the **Troubleshoot** page, click **Advanced options**.
9. On the **Advanced Options** page, click **Command Prompt**.
10. At the command prompt, type **Bcdedit /enum**, and then press Enter.
11. At the command prompt, type **Bootrec /scanos**, and then press Enter. This command scans disks for installations that are compatible with Windows 8.1. This option displays installations that **Bcdedit /enum** does not list. You can use the **/RebuildBcd** switch to add the missing installations to the boot store.
12. At the command prompt, type **diskpart**, and then press Enter.
13. At the command prompt, type **list disk**, and then press Enter.
14. At the command prompt, type **list volume**, and then press Enter.
15. At the command prompt, type **exit**, and then press Enter.
16. At the command prompt, type **exit**, and then press Enter.
17. On the **Choose an option** page, click **Troubleshoot**.
18. On the **Troubleshoot** page, click **Advanced options**.
19. On the **Advanced Options** page, click **Startup Repair**.
20. On the **Startup Repair** page, click **Windows 8.1**. The automatic repair starts.
21. On the **Startup Repair** page, click **Advanced options**.
22. On the **Choose an option** page, click **Continue**. Windows starts normally.

Enable access to the Advanced Boot Options menu

1. On LON-CL1, sign in as **Adatum\administrator** with the password **Pa$$w0rd**.
2. On the Start screen, type **cmd**.
3. In the **Apps** list, right-click **Command Prompt**, and then click **Run as administrator**.
4. At the command prompt, type **Bcdedit /copy {current} /d "Duplicate boot entry"**, and then press Enter.
5. At the command prompt, type **Bcdedit /enum**, and then press Enter.

6. At the command prompt, type **shutdown /r**, and then press Enter.
7. When Windows restarts, wait until the **Choose an operating system** menu appears.
8. Click **Change defaults or choose other options**.
9. On the **Options** page, click **Choose other options**.
10. On the **Choose an option** page, click **Troubleshoot**.
11. On the **Troubleshoot** page, click **Advanced options**.
12. On the **Advanced options** page, click **Startup Settings**.
13. On the **Startup Settings** page, click **Restart**.
14. In the **Startup Settings** menu, type **4** to enable Safe Mode.
15. On LON-CL1, sign in as **Adatum\administrator** with the password **Pa$$w0rd**.

Module Review and Takeaways

Review Question(s)

Question: Your user adds a new hard disk to the computer, which changes the computer's partition numbering. To enable the computer to start, the user needs you to change the BCD store. What tool will you use?

> **Answer:** You can use **Bcdedit /enum** to view the entries in the store. Then use **Bcdedit** to edit the store to reflect the changes on the computer.

Question: After installing a new video driver, your user's computer becomes unstable and will not start correctly. What would you try first to resolve this problem?

> **Answer:** You would use System Restore, and then roll back the configuration to a previous point. If System Restore is unavailable, you could attempt a driver rollback.

Lab Review Questions and Answers

Lab A: Identifying Performance Problems

Question and Answers

Question: What was your approach to the scenario? How did your approach differ from the other members of the class?

Answer: Answers will vary. This question is intended to survey the students for their approach to the exercise, and allow them to discuss those approaches with each other. You can guide the discussion to highlight relevant points and connect student approaches to content covered in the topics in this lesson.

Lab B: Recovering Windows 8.1

Question and Answers

Question: In the lab, what was the problem?

Answer: A user's computer failed to start correctly because of a corrupted BCD store.

Question: How did you resolve the problem?

Answer: The product DVD was used to access Setup and then manually repair the BCD store.

Question: What other approach could you have taken?

Answer: Automatic repair might have been another successful approach.

Module 9

Implementing Client Hyper-V in Windows 8.1

Contents:

Lesson 1

Overview of Client Hyper-V

Contents:

Question and Answers

What Is Client Hyper-V?

Question: What must you do to be able to administer Client Hyper-V by using Windows PowerShell?

Answer: If you want to administer Client Hyper-V locally, you can use the Hyper-V module for Windows PowerShell, which is installed automatically when you turn on the Hyper-V Windows feature on a Windows 8.1–based computer. If you want to administer Client Hyper-V on a remote computer, you must first turn on the Hyper-V module for Windows PowerShell feature.

Scenarios for Using Client Hyper-V

Question: Can you run two virtual machines with the same name and TCP/IP network settings in the same Client Hyper-V environment?

Answer: Yes, you can run multiple virtual machines with the same name and TCP/IP settings in the same Client Hyper-V environment without a conflict. Each virtual machine is isolated from others and from the physical computer running Windows 8.1 by default, so there will not be any conflict if you configure operating systems in virtual machines with the same settings.

Overview of Client Hyper-V Networking

Question: Do you have to create a virtual switch on a computer running Client Hyper-V?

Answer: If there is no virtual switch on a computer running Client Hyper-V and you deploy multiple virtual machines on that computer, you will not be able to connect the virtual machines to a network. The virtual machines will be unable to communicate with other computers on the network or among themselves, even if they are running on the same physical computer. The physical computer will still have network connectivity because a virtual switch is not required to control its network traffic. However, as a best practice, always create one or more virtual switches on a computer running Client Hyper-V.

Virtual Switch Options in Client Hyper-V

Question: Can a virtual machine access the Internet if it is connected to an internal virtual switch?

Answer: If a virtual machine is connected to an internal virtual switch, its connectivity is generally limited to:

- The physical Windows 8.1–based computer itself.
- Other virtual machines that are running on the same physical computer and that are connected to the same internal virtual switch.

However, if the physical Windows 8.1–based computer has Internet connectivity and is configured with ICS, then the virtual machine could also have Internet connectivity.

Lesson 2

Creating Virtual Machines

Contents:

Question and Answers

Creating a Virtual Machine

Question: Can you convert a Generation 1 virtual machine that has Windows Server 2012 R2 installed to a Generation 2 virtual machine?

Answer: No. You can select a generation for the virtual machine only when you create the virtual machine. You cannot change the generation after you create the virtual machine. If you already have a Generation 1 virtual machine, you cannot convert it to a Generation 2 virtual machine, regardless of the operating system that is installed on that virtual machine.

Configuring Virtual Machine Settings

Question: Can you modify memory settings of a virtual machine while the virtual machine is running?

Answer: No, you cannot modify most of the virtual machine settings while the virtual machine is running. If the virtual machine has Dynamic Memory enabled, you can decrease the minimum RAM and increase the maximum RAM while the virtual machine is running. Irrespective of the state of a virtual machine, you can always modify the memory weight.

Running Virtual Machines

Question: Why is it preferable to import a virtual machine into Client Hyper-V rather than create a new virtual machine and configure it to use existing virtual hard disks?

Answer: When you import a virtual machine, its configuration (for example, the number of processors and memory settings) is preserved. Import also preserves checkpoints and TCP/IP settings of the network adapter. None of that is preserved when you create a new virtual machine and configure it with the existing virtual hard disk.

Question: Can you use the enhanced session mode to start a virtual machine from a USB flash drive?

Answer: Enhanced session mode is available only after the supported operating system is already running on the virtual machine. When the virtual machine is starting, enhanced session mode is not available. Therefore, you cannot use USB device redirection to start the virtual machine from the USB device.

Lesson 3

Managing Virtual Hard Disks

Contents:

Question and Answers

Virtual Hard Disk Options in Client Hyper-V

Question: Is there any difference between connecting a virtual hard disk to a virtual machine by using a virtual IDE controller and connecting a virtual hard disk to a virtual machine by using a virtual SCSI controller?

> **Answer:** Virtual hard disks have the same format, irrespective of the controller you use to connect them to a virtual machine. The only difference is how the virtual machine accesses those virtual hard disks and which options the controller offers. For example, you can add or remove virtual hard disks from a virtual SCSI controller while the virtual machine is running. However, you must first turn off the virtual machine if you want to add or remove a virtual hard disk from a virtual integrated device electronics (IDE) controller.

Question: Can Client Hyper-V allocate more storage space to a differencing virtual hard disk than to the parent disk to which it is linked?

> **Answer:** A differencing virtual hard disk is always linked to a parent disk, which can be a fixed-size virtual hard disk, a dynamically expanding virtual hard disk, or another differencing virtual hard disk. When a differencing virtual hard disk is linked to a dynamically expanding or differencing virtual hard disk, Client Hyper-V can allocate more space to it than it can to the parent disk to which it is linked.

Configuring a Virtual Hard Disk

Question: When would you use shared virtual hard disks?

> **Answer:** You would use shared virtual hard disks when you want to provide shared storage on a virtual machine, most likely to configure failover clustering.

Moving Virtual Machine Storage

Question: What virtual machine data can you move by using storage migration in Client Hyper-V?

> **Answer:** You can use storage migration to move all the virtual machine data files. This includes virtual hard disks, which are usually the largest virtual machine data files, checkpoints, current configuration, and Smart Paging files.

Question: Do you need to be a local administrator to use the Move Wizard?

> **Answer:** No, you do not need to be local administrator. You only need to be a member of the Hyper-V Administrators group to be able to use Move Wizard.

Lesson 4

Managing Checkpoints

Contents:

Question and Answers

What Are Checkpoints?

Question: Which checkpoint requires more space: a checkpoint of a running virtual machine or a checkpoint of a virtual machine that is turned off?

Answer: You can create checkpoints of virtual machines that are running and virtual machines that are turned off. However, the checkpoint of a virtual machine that is running includes memory content, whereas the checkpoint of a virtual machine that is turned off has no memory content. Therefore, the checkpoint of a virtual machine that is turned off will be smaller in size than the checkpoint of a running virtual machine.

Creating and Managing Checkpoints

Question: Can you modify the configuration of a virtual machine checkpoint if you created that checkpoint when the virtual machine was turned off?

Answer: A virtual machine must be turned off for you to be able to configure most of the virtual machine settings. However, you can never modify a virtual machine configuration in a checkpoint, regardless of whether the virtual machine was running or turned off when you created the checkpoint. Checkpoints contain virtual machine configurations from the past, which you cannot modify.

Considerations for Working with Checkpoints

Question: Can you prevent checkpoint creation from inside a virtual machine?

Answer: No, you cannot prevent checkpoint creation from inside a virtual machine.

Module Review and Takeaways

Review Question(s)

Question: Why would you deploy Client Hyper-V to a Windows-based client computer in a corporate environment?

Answer: Users can use Client Hyper-V to work with virtual machines that run in Hyper-V for troubleshooting and testing purposes. You also can use Client Hyper-V as an isolated test environment, or to run multiple operating systems on the same computer.

Question: Why should you not use virtual machine checkpoints for backup and disaster recovery?

Answer: Checkpoints enable you to apply earlier point-in-time snapshots to a virtual machine. However, checkpoints depend on the virtual machine files. If those files are not available, you cannot use checkpoints, even if checkpoint files are still available. Therefore, if the physical disk on which virtual machine files are stored fails, you will not be able to recover the virtual machine only by using checkpoint files.

Question: Can you create a checkpoint of a virtual machine that is turned off?

Answer: Yes, you can create a checkpoint of a virtual machine providing it is not in a Paused state. If you create a checkpoint of a virtual machine that is in an Off state, it will be smaller than a checkpoint of a running virtual machine, because the checkpoint will not contain virtual machine memory.

Question: When you opened Windows PowerShell and ran the **New-VM** cmdlet to create a new virtual machine, you received an error that **New-VM** was not recognized as the name of a cmdlet. What was the most probable reason for such an error?

Answer: New-VM is one of the cmdlets in the Windows PowerShell Hyper-V module. The most probable reason for the error is that the Hyper-V module is not available on the computer. If you want to use the cmdlet, you should turn on the Hyper-V Module for the Windows PowerShell feature.

Tools

Tool	Description	Where to find it
Hyper-V Manager	Management console for Client Hyper-V	Start screen
Hyper-V Virtual Machine Connection Tool	Allows you to connect directly to local or remote virtual machines without opening Hyper-V Manager	Start screen

Lab Review Questions and Answers

Lab: Configuring Client Hyper-V

Question and Answers

Question: Why did you have to use native boot from a Windows 8.1 virtual hard disk in order to complete this lab?

> **Answer:** An operating system that performs virtualization has to run directly on the computer's hardware. You cannot turn on the Client Hyper-V feature if Windows 8.1 is running on a virtual machine. Therefore, you had to use native boot from a virtual hard disk for this lab. However, if you want to manage Client Hyper-V remotely, you can turn on the Hyper-V Management tools feature in the virtual machine.

Question: In the lab, you created a private virtual switch to which to connect the virtual machine. Would a private virtual switch be the logical choice if you were using the virtual machine for testing Windows Updates? Why or why not?

> **Answer:** A private virtual switch would limit the virtual machine to connectivity with other virtual machines that are running on the same Windows 8.1 Client Hyper-V. This would not be a good choice for Windows Updates, because the computer will need Internet connectivity to download the updates. The external virtual switch would be best suited for a virtual machine that you are using to test Windows Updates.