Microsoft

OFFICIAL MICROSOFT LEARNING PRODUCT

20415B

Implementing a Desktop Infrastructure

Companion Content

Product Number: 20415B

Released: 04/2013

MICROSOFT LICENSE TERMS

OFFICIAL MICROSOFT LEARNING PRODUCTS COURSEWARE – STUDENT EDITION – Pre-Release and Final Versions

These license terms are an agreement between Microsoft Corporation and you. Please read them. They apply to the licensed content named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

- updates,
- supplements,
- Internet-based services, and
- support services

for this licensed content, unless other terms accompany those items. If so, those terms apply.

By using the licensed content, you accept these terms. If you do not accept them, do not use the licensed content.

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

1. **OVERVIEW.**

   Licensed Content. The licensed content includes software, printed materials, academic materials (online and electronic), and associated media.

   License Model. The licensed content is licensed on a per copy per device basis.

2. **INSTALLATION AND USE RIGHTS.**

   a. **Licensed Device.** The licensed device is the device on which you use the licensed content. You may install and use one copy of the licensed content on the licensed device.

   b. **Portable Device.** You may install another copy on a portable device for use by the single primary user of the licensed device.

   c. **Separation of Components.** The components of the licensed content are licensed as a single unit. You may not separate the components and install them on different devices.

   d. **Third Party Programs.** The licensed content may contain third party programs. These license terms will apply to your use of those third party programs, unless other terms accompany those programs.

3. **PRE-RELEASE VERSIONS.** If the licensed content is a pre-release ("beta") version, in addition to the other provisions in this agreement, then these terms also apply:

   a. **Pre-Release Licensed Content.** This licensed content is a pre-release version. It may not contain the same information and/or work the way a final version of the licensed content will. We may change it for the final, commercial version. We also may not release a commercial version. You will clearly and conspicuously inform any Students who participate in an Authorized Training Session and any Trainers who provide training in such Authorized Training Sessions of the foregoing; and, that you or Microsoft are under no obligation to provide them with any further content, including but not limited to the final released version of the Licensed Content for the Course.

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

   c. **Confidential Information.** The licensed content, including any viewer, user interface, features and documentation that may be included with the licensed content, is confidential and proprietary to Microsoft and its suppliers.

      i. **Use.** For five years after installation of the licensed content or its commercial release, whichever is first, you may not disclose confidential information to third parties. You may disclose confidential information only to your employees and consultants who need to know the information. You must have written agreements with them that protect the confidential information at least as much as this agreement.

      ii. **Survival.** Your duty to protect confidential information survives this agreement.

iii. **Exclusions**. You may disclose confidential information in response to a judicial or governmental order. You must first give written notice to Microsoft to allow it to seek a protective order or otherwise protect the information. Confidential information does not include information that

- becomes publicly known through no wrongful act;
- you received from a third party who did not breach confidentiality obligations to Microsoft or its suppliers; or
- you developed independently.

d. **Term**. The term of this agreement for pre-release versions is (i) the date which Microsoft informs you is the end date for using the beta version, or (ii) the commercial release of the final release version of the licensed content, whichever is first ("beta term").

e. **Use**. You will cease using all copies of the beta version upon expiration or termination of the beta term, and will destroy all copies of same in the possession or under your control.

f. **Copies**. Microsoft will inform Authorized Learning Centers if they may make copies of the beta version (in either print and/or CD version) and distribute such copies to Students and/or Trainers. If Microsoft allows to such distribution, you will follow any additional terms that Microsoft provides to you for such copies and distribution.

4. **ADDITIONAL LICENSING REQUIREMENTS AND/OR USE RIGHTS.**

a. **Media Elements and Templates.** You may use images, clip art, animations, sounds, music, shapes, video clips and templates provided with the licensed content solely for your personal training use. If you wish to use these media elements or templates for any other purpose, go to www.microsoft.com/permission to learn whether that use is allowed.

b. **Academic Materials.** If the licensed content contains academic materials (such as white papers, labs, tests, datasheets and FAQs), you may copy and use the academic materials. You may not make any modifications to the academic materials and you may not print any book (either electronic or print version) in its entirety. If you reproduce any academic materials, you agree that:

- The use of the academic materials will be only for your personal reference or training use
- You will not republish or post the academic materials on any network computer or broadcast in any media;
- You will include the academic material's original copyright notice, or a copyright notice to Microsoft's benefit in the format provided below:

Form of Notice:

© 2011 Reprinted for personal reference use only with permission by Microsoft Corporation. All rights reserved.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the US and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

c. **Distributable Code.** The licensed content may contain code that you are permitted to distribute in programs you develop if you comply with the terms below.

i. **Right to Use and Distribute.** The code and text files listed below are "Distributable Code."

- REDIST.TXT Files. You may copy and distribute the object code form of code listed in REDIST.TXT files.
- Sample Code. You may modify, copy, and distribute the source and object code form of code marked as "sample."
- Third Party Distribution. You may permit distributors of your programs to copy and distribute the Distributable Code as part of those programs.

ii. **Distribution Requirements**. For any Distributable Code you distribute, you must

- add significant primary functionality to it in your programs;
- require distributors and external end users to agree to terms that protect it at least as much as this agreement;
- display your valid copyright notice on your programs; and
- indemnify, defend, and hold harmless Microsoft from any claims, including attorneys' fees, related to the distribution or use of your programs.

iii. Distribution Restrictions. You may not

- alter any copyright, trademark or patent notice in the Distributable Code;
- use Microsoft's trademarks in your programs' names or in a way that suggests your programs come from or are endorsed by Microsoft;
- distribute Distributable Code to run on a platform other than the Windows platform;
- include Distributable Code in malicious, deceptive or unlawful programs; or
- modify or distribute the source code of any Distributable Code so that any part of it becomes subject to an Excluded License. An Excluded License is one that requires, as a condition of use, modification or distribution, that
  - the code be disclosed or distributed in source code form; or
  - others have the right to modify it.

5. **INTERNET-BASED SERVICES.** Microsoft may provide Internet-based services with the licensed content. It may change or cancel them at any time. You may not use these services in any way that could harm them or impair anyone else's use of them. You may not use the services to try to gain unauthorized access to any service, data, account or network by any means.
6. **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 allow you to use it in certain ways. You may not
   - disclose the results of any benchmark tests of the licensed content to any third party without Microsoft's prior written approval;
   - work around any technical limitations in the licensed content;
   - reverse engineer, decompile or disassemble the licensed content, except and only to the extent that applicable law expressly permits, despite this limitation;
   - make more copies of the licensed content than specified in this agreement or allowed by applicable law, despite this limitation;
   - publish the licensed content for others to copy;
   - transfer the licensed content marked as 'beta' or 'pre-release' to any third party;
   - allow others to access or use the licensed content;
   - rent, lease or lend the licensed content; or
   - use the licensed content for commercial licensed content hosting services.
   - Rights to access the server software that may be included with the Licensed Content, including the Virtual Hard Disks does not give you any right to implement Microsoft patents or other Microsoft intellectual property in software or devices that may access the server.
7. **BACKUP COPY.** You may make one backup copy of the licensed content. You may use it only to reinstall the licensed content.
8. **TRANSFER TO ANOTHER DEVICE.** You may uninstall the licensed content and install it on another device for your personal training use. You may not do so to share this license between devices.
9. **TRANSFER TO A THIRD PARTY.** You may not transfer those versions marked as 'beta' or 'pre-release' to a third party. For final versions, these terms apply: The first user of the licensed content may transfer it and this agreement directly to a third party. Before the transfer, that party must agree that this agreement applies to the transfer and use of the licensed content. The first user must uninstall the licensed content before transferring it separately from the device. The first user may not retain any copies.
10. **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.
11. **NOT FOR RESALE SOFTWARE/LICENSED CONTENT.** You may not sell software or licensed content marked as "NFR" or "Not for Resale."

12. **ACADEMIC EDITION.** You must be a "Qualified Educational User" to use licensed content marked as "Academic Edition" or "AE." If you do not know whether you are a Qualified Educational User, visit www.microsoft.com/education or contact the Microsoft affiliate serving your country.
13. **ENTIRE AGREEMENT.** This agreement, and the terms for supplements, updates, Internet-based services and support services that you use, are the entire agreement for the licensed content and support services.
14. **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.
15. **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.
16. **DISCLAIMER OF WARRANTY. THE LICENSED CONTENT IS LICENSED "AS-IS." YOU BEAR THE RISK OF USING IT. MICROSOFT 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 EXCLUDES THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.**
17. **LIMITATION ON AND EXCLUSION OF REMEDIES AND DAMAGES. YOU CAN RECOVER FROM MICROSOFT AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO U.S. $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, software, 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.

Module 1

Assessing and Determining Desktop Deployment Options

Contents:

Lesson 2

Assessing Hardware and Infrastructure Readiness for a Desktop Deployment

Contents:

Demonstration: Using Configuration Manager to Assess the Network Infrastructure

Demonstration Steps

1. Sign in to LON-CFG1 as **adatum\administrator** with a password of **Pa$$w0rd**.
2. On the taskbar, click **Configuration Manager Console**.
3. In the Configuration Manager console, click the **Administration** workspace.
4. In the Administration workspace, click **Client Settings**, and then click **Default Client Settings**.
5. On the **Home** tab, in the **Properties** group, click **Properties**.
6. In the **Default Settings** dialog box, click **Hardware Inventory**.
7. In the **Device Settings** list, configure the following:
   a. Enable hardware inventory on clients: **Yes**.
   b. Hardware inventory schedule: Specify the interval at which clients collect a Configuration Manager hardware inventory. Use the default value of **7 days**. Click **Schedule** to show how to set a custom interval.
8. Click **Cancel** to get back to the **Hardware Inventory** page.
9. Click **Set Classes** to open the Hardware Inventory Classes window. Review the different classes listed. Explain some of them to the students. Note that the classes come from the Windows Management Instrumentation (WMI) namespace. Point out the buttons below the list of classes: **Import**, **Export** and **Add**. You can use all of these functions, but to import, you have to have access to a Managed Object Format (MOF) file. When you export, you are creating a MOF file for the hardware classes listed and checked here. If you add, you will need to know the WMI nomenclature to add a value correctly. When you are finished, click **Cancel**.
10. Click **OK** to close the **Default Settings** dialog box.
11. Sign in to LON-CL1 as **adatum\administrator** with a password of **Pa$$w0rd**.
12. On the **Start** page, type **Control Panel**, and then press Enter.
13. In the Control Panel, click the **System and Security** hyperlink.
14. Scroll to the bottom, and then click **Configuration Manager**.
15. In the **Configuration Manager Properties** box, click the **Actions** tab.
16. Click **Hardware Inventory Cycle**, and then click **Run Now**.
17. A message displays that states that the selected cycle will run and might take several minutes to finish. Click **OK**, and then click **OK** to close the Configuration Manager Properties window.
18. Close all windows, and then sign out of LON-CL1.

Run Resource Explorer from the Configuration Manager console

1. On LON-CFG1, in the Configuration Manager console, click **Assets and Compliance**.
2. In the Assets and Compliance workspace, click **Devices**.
3. Click **LON-CL1** in the details pane, and in the **Home** tab, in the **Device** group, click **Start**, and then click **Resource Explorer**. The Resource Explorer window opens.
4. Expand the **Hardware** node in the console tree. You can select any hardware item in the console tree, right-click any item in the details pane of the Resource Explorer window, and then click **Properties** to

open the **Properties** dialog box. This can help you to view the collected inventory information in a more readable format.

5. Close the Resource Explorer window when you are finished.
6. Close all windows, and then sign out of LON-CFG1.

Lesson 3

Using MAP to Assess Deployment Readiness

Contents:

Demonstration: Using MAP to Assess Infrastructure Readiness

Demonstration Steps

1. Sign in to LON-CL1 as **adatum\administrator** with a password of **Pa$$w0rd**.
2. On the Start page, scroll to the right and double-click the **Microsoft Assessment and Planning Toolkit tile** to launch MAP. You may want to resize the application to full screen.
3. In the **Create or Select a Database** dialog box, click **Create an inventory database**, type **Demo** as a new database name, and then click **OK**.

Note: This database will be used to do a very small inventory of the LON-CL1 computer.

4. On the main menu, click **File,** and then click **Manage Databases** to launch the **Manage Databases** dialog box.
5. Select the Demo database, and then click **Export**.
6. Type Demo as the file name, and then click **Save**.
7. After successfully exporting the database, click **OK**.
8. Click **Import** on the **Manage Databases** dialog to launch the **To import a database…** dialog box.
9. Click **Browse** on the **To import a database…** dialog box, select the **MAP_SampleDB** demonstration database from the DatabaseBackups folder (C:\Program Files\Microsoft Assessment and Planning Toolkit) and then click **Open**.
10. Type the database name **MAP_SampleDB** in the **To import a database…** dialog box **Database Name** field, and then click **OK**.
11. If a message displays stating The imported database needs to be upgraded…, select **Yes**. In a few moments a Successfully imported and upgraded the database message will display. Click **OK**.
12. Observe that the database is present as a selection in the **Manage Databases** dialog box.
13. When finished, click **Close** on the **Manage Databases** dialog box.

Enable remote administration

1. Navigate to the **Start** page, type **Command Prompt**, right-click **Command Prompt**, and then click **Run As Administrator**.
2. Type the following command, and then press Enter:

   netsh advfirewall set currentprofile settings remotemanagement enable

3. To enable File and Printer Sharing in Windows 8, navigate to the **Start** page, type **Control Panel**, and then click Control Panel. Click **Network and Internet**, then click **Network and Sharing Center**, and then click **Change Advanced Sharing Settings**.
4. Turn on file and printer sharing, which will open TCP ports 139 and 445, and UDP ports 137 and 138.
5. Click the **Save Changes** button at the bottom of the window.
6. Close the Network and Sharing Center window.

Assess Windows 8

1. In the Microsoft Assessment and Planning Toolkit, select **File→Select a Database** from the main menu to launch the **Create or select a database to use** dialog box.

2. Click **Use an existing database**, select **MAP_SampleDB** from the **Databases** menu, and then click **OK**.
3. Click the **Desktop** scenario group in the navigation pane of the console, and then click the **Windows 8 Readiness** tile.
4. Inspect the scenario detail pane, and then observe that discovered machines are classified as

- Ready for Windows 8
- Can't run Windows 8.
- Insufficient data Collected

Generate Windows 8 Assessment Reports

1. Ensure that you have completed the previous procedure to assess Windows 8 Readiness.
2. Click the **Desktop** scenario group in the navigation pane of the console, and then click the **Windows 8 Readiness** tile.
3. Click **Generate Windows 8 Readiness Report & Proposal** at the top of the scenario detail pane to start generating the reports and proposals and to launch a status dialog box.
4. After the status dialog box reports that the generation has completed, click **Close**.
5. Select **View → Saved Reports and Proposals** from the main menu, or navigate to a previously opened File Explorer to launch a file browser on the directory where the generated files are stored.
6. Open the **Windows8Assessment-**<*date-and-time*> Excel report.
    i. If a **User Name** dialog box opens asking for initials for the administrator account, click **OK**.
    ii. If the Microsoft Office Activation Wizard pop up window appears, click Close.
7. Show the students the following tabs, and then explain the detailed information about the assessed computers and their relative readiness for Windows 8.
    - Summary

      Number of machines that are ready or are meeting the minimum or recommended requirements, the number that can be made ready with hardware upgrades, and the number that cannot be upgraded.
    - Assessment Values

      CPU, memory, free disk, DVD, audio and video, Microsoft minimum and recommended values, and the values used in the assessment.
    - Client Assessment

      Current operating system, upgrade assessment, reasons for the conclusion, and other information for each client surveyed.
    - After Upgrades

      Detailed list of computers that are not currently able to run Windows 8 and the hardware upgrades required to meet the minimum system requirements for a Windows 8 upgrade.
    - Device Summary

      Windows 8 compatibility with equipment attached to discovered client machines.
    - Device Details

      Windows 8 compatibility with equipment on each client.

- Discovered Applications

  Summary of applications installed on client computers with a count of the clients that have each application installed.

8. After viewing, close the report.
9. Open the **Windows8Proposal**-<*date-and-time*> Word document to view a customer-ready proposal containing detailed information on the assessed computers and their relative readiness for Windows 8. Explain that you can customize the generated documents and add text specific to your customer that complements the facts discovered in the environment.
10. Scroll down through the file and demonstrate the data presented in the proposal, as follows:
    a. Client computer readiness for Windows 8

       Number of machines that are ready, and the number that can be made ready.

    b. Windows 8 Ready Computers

       Number of machines that are ready, and the number that can be made ready.

    c. Client computer readiness for Windows 8 with hardware upgrades

       Number of computers that could run Windows 8 after upgrades.

    d. Windows 8 Ready Computers (with recommended hardware upgrades)

       Number of computers that could run Windows 8 after upgrades.

    e. Count of Computer Hardware Upgrades Recommended

       List of equipment upgrade categories.

    f. Count of Computers by the Number of Recommended Hardware Upgrades

       Roll-up list of equipment readiness by number of necessary upgrades.

    g. Operating Systems That the Assessment Found

       List of existing operating systems.

    h. Prevalent Software Installed on the Network

       List of most commonly installed software found.

    i. Web Browsers Installed

       List of installed web browsers.

    j. Web Browsers Installed by Operating System

       Table of installed web browsers by operating system.

    k. Microsoft and User Defined Thresholds

       Actual thresholds used for the Windows 8 readiness assessment.

11. After viewing, close the proposals and the file browser.

Generate a generic inventory report

1. Click the **Environment** scenario group in the navigation pane of the console, and then click the **Inventory Results** tile.
2. Click **Generate Inventory Results Report** at the top of the scenario detail pane to start generating the reports and to launch a status dialog box.
3. After the status dialog box reports that the generation has completed, click **Close**.

4. Select **View → Saved Reports and Proposals** from the main menu, or navigate to a previously opened File Explorer to launch a file browser on the directory where the generated files are stored.
5. Open the **InventoryResults-**<*date-and-time*> Excel report, and then review detailed information on every machine inventoried.
6. After viewing, close the reports and the file browser, and then sign out of LON-CL1.

Lesson 4

Overview of Enterprise Desktop Deployment Methods

Contents:

Resources

Selecting a Deployment Method for Enterprise Desktops

 **Additional Reading:** For more information about choosing a deployment strategy, go to http://go.microsoft.com/fwlink/?LinkId=286466

Providing a Remote Desktop Environment by Using VDI

 **Additional Reading:** For more information on VDI, refer to http://go.microsoft.com/fwlink/?LinkId=286467

Lesson 5

Volume Activation Technologies for Enterprise Desktops

Contents:

Resources

Volume Activation Technologies

 **Additional Reading:** For a volume activation overview, go to http://go.microsoft.com/fwlink/?LinkId=286471

Tools Used to Manage Activation

 **Additional Reading:** For more information on the procedure to import and export from VAMT, refer to http://go.microsoft.com/fwlink/?LinkId=286472

Module Review and Takeaways

Tools

Tools for Assessment and Deployment

Tool	Use for	Where to find it
MAP 7.0	Performing inventories, assessing, and reporting on your infrastructure so you can decide what Microsoft technology to deploy	http://go.microsoft.com/fwlink/?LinkId=286473
Windows ADK	Customizing, assessing, and deploying Windows operating systems to new computers	http://go.microsoft.com/fwlink/?LinkId=286474
ACT 6.0	Determining whether the applications, devices, and computers in your organization are compatible with Windows 8. ACT helps you obtain compatibility information from Microsoft and software vendors, identify compatibility issues, and share compatibility ratings with other ACT users	ACT is included with Windows ADK
MDT 2012	Accelerating and automating deployments of Windows 8, Windows Server 2012, Windows 7, Microsoft Office 2010, and Windows Server 2008 R2	http://go.microsoft.com/fwlink/?LinkId=286475

Tools for Volume Activation

Tool	Use for	Where to find it
VAMT 3.0	Automating and centrally managing the volume and retail activation process for Windows operating systems, Microsoft Office programs, and select other Microsoft products	You can install VAMT as part of the Windows ADK
The Volume Activation Services server role	Automating and simplifying the issuance and management of Microsoft software volume licenses for a variety of scenarios and environments	Installed from the Server Manager Add Roles Wizard on Windows Server 2012
Active Directory-based activation	Storing activation objects by using AD DS, which can further simplify the task of maintaining volume activation services for a network	Configured on any domain controller that runs Windows Server 2012
KMS	Enabling organizations to activate	Type **%WINDIR%\System32\slmgr.vbs /ipk**

Tool	Use for	Where to find it
	systems within their network from a server where a KMS host has been installed	**xxxxx-xxxxx-xxxxx-xxxxx-xxxxx** from a command prompt as administrator (x field is your KMS key)
Volume Activation Tools console snap-in	Managing activations and performing other activation-related tasks	Part of VAMT 3.0

Tools for Windows To Go

Tool	Use for	Where to find it
Windows ADK	Customizing, assessing, and deploying Windows operating systems to new computers	http://go.microsoft.com/fwlink/?LinkId=286477
ImageX	Capturing, modifying, and applying file-based disk images for rapid deployment	Part of Windows ADK
DISM	Servicing Windows images offline before deployment, installing, uninstalling, configuring, and updating Windows features, packages, drivers, and international settings. Subsets of the DISM servicing commands also are available for servicing a running operating system.	Part of Windows ADK

Tools for VDI

Tool	Use for	Where to find it
Remote Desktop Services service role	Enabling users to connect to virtual desktops, RemoteApp programs, and session-based desktops	Installed from the Server Manager Add Roles Wizard on Windows Server 2012
Hyper-V®	Creating and managing a virtualized computing environment by using virtualization technology that is built in to Windows 8 and Windows Server 2012	Installed from the Server Manager Add Roles Wizard on Windows Server 2012

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
When creating an inventory in MAP 7.0, some clients may not show any results or fail to communicate with the system	Make sure all systems are up and running, and that the domain account used in the MAP inventory configuration has administrator permissions on those systems. Additionally, ensure that WMI is allowed through the

Common Issue	Troubleshooting Tip
running MAP.	firewall on each client.

Lab Review Questions and Answers

Lab: Assessing and Determining Desktop Deployment Options

Question and Answers

Lab Review

Question: You need to create a hardware inventory throughout the enterprise. This might involve up to 800 computers plus peripherals. What is the best tool to accomplish this and why?

Answer: MAP collects hardware inventory throughout your network environment by using agentless collection methods such as WMI, the Remote Registry service, Simple Network Management Protocol, AD DS, and the Computer Browser service.

Question: You are deploying the Windows 8 client to 19 domain-joined computers. You have an existing KMS server. Which volume activation method do you use?

Answer: Active Directory-based activation is the best possible answer. A KMS server requires at least 25 client requests before it starts activating them. Active Directory-based activation does not have a minimum amount of clients or servers to activate. Since you have an existing KMS key, you can deploy that same key through Active Directory-based activation. MAK activation may be used, but this would require the purchase of specific MAK product licenses.

Module 2

Planning an Image Management Strategy

Contents:

Lesson 1

Overview of Windows Image Format

Contents:

Question and Answers

Discussion: Challenges of Maintaining Images in Your Organization

Question: Have you used sector-based imaging products in the past?

Answer: Answers will vary. Most likely, they have used a sector-based imaging product.

Question: How many images did you have to maintain?

Answer: Answer will vary. This part of the discussion could focus on the physical equipment challenges with sector-based imaging. Some common challenges include the need for a different hardware abstraction layer (HAL) for different model systems, different driver needs, possibly within the same model, or images due to drive size.

Question: What did you do about patching and updates?

Answer: Answers will vary. This discussion can focus on the difficulties of maintaining up-to-date software in the images and the need to create new images to capture changes in software.

Demonstration: Using Image Management Tools to View the Contents of a Windows Image File

Demonstration Steps

Using DISM to view Windows image file information

1. Sign in to the LON-CFG1 virtual machine as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. Open the **Start** screen.
3. Click on the **Deployment and Imaging Tools Environment** tile.
4. In the Administrator: Deployment and Imaging Tools Environment window, type the following command, and then press Enter.

```
DISM /Get-Wiminfo /WimFile:E:\Labfiles\Images\CustomWin8.wim
```

5. Review the results of the command.
6. In the Administrator: Deployment and Imaging Tools Environment window, type the following commands, and then press Enter after each command.

```
MD C:\Servicing
DISM /Mount-Wim /WimFile:E:\Labfiles\Images\CustomWin8.wim /Index:1
/MountDir:C:\Servicing
```

7. Review the results of the command.
8. In the taskbar, click **File Explorer**.
9. Open the Servicing folder on drive C, and discuss the files and folders.
10. Close File Explorer.
11. In the Administrator: Deployment and Imaging Tools Environment window, type the follow command, and then press Enter.

```
DISM /UnMount-Wim /MountDir:C:\Servicing /Discard
```

12. Review the results of the command.

Module Review and Takeaways

Review Question(s)

Question: What factors helped determine the image management strategy in your company?

Answer: Answers will vary. Some students may not be using imaging, and some students may be using different products, such as sector-based imaging.

Tools

Tool	Use to	Where to find it
DPInst	Add drivers for detected hardware	Windows Driver Kit available at: http://go.microsoft.com/fwlink/?LinkId=286477
PnPUtil	Add, remove, and enumerate drivers	Included with the Windows 8 operating system
Wusa.exe	Add service packs or other .msu files	Included with the Windows 8 operating system
Lpksetup	Add or remove language packs	Included with the Windows 8 operating system

Lab Review Questions and Answers

Lab: Planning an Image Management Strategy

Question and Answers

Lab Review

Question: What additional factors might you include in planning your image management strategy?

> **Answer:** Answer will vary, but could include determining whether to use additional products, such as the Microsoft Deployment Toolkit or Microsoft System Center 2012 Configuration Manager.

Question: How will moving applications out of the images affect the deployment time for an operating system?

> **Answer:** Answers will vary. Likely, the total deployment time will increase because the setup applications will need to run and perform the configuration changes that would have been included in the image without adding to the size of the image.

Module 3

Configuring Desktop Security

Contents:

Lesson 1

Implementing a Centralized Desktop Security Solution

Contents:

Question and Answers

Discussion: Applying Security Before or After Image Deployment

Question: What security settings would you configure to include in an image?

Answer: Answers will vary but could include:

- Configuring local policy settings
- Adding local accounts

Question: Many security settings can be set through Group Policy or through local policy. What do you consider are the pros and cons of configuring local security policies in an image?

Answer: Answers will vary but could include:

- Pro: Group Policy inheritance allows you to override any locally set polices with domain-based group policy.
- Con: If someone does not know a local policy is in place, it may be difficult to troubleshoot a problem.
- Pro: It allows you to apply policies to systems that will not join the domain.
- Con: It is difficult to manage systems centrally that are not on the domain.

Question: Considering your environment, what security options do you or would you configure for a desktop image?

Answer: Answers will vary. The discussion could include Group Policy, BitLocker, EFS, setting local permissions, or other security-related topics.

Resources

Device and Media Restriction Policies for Enterprise Desktops

 **Additional Reading:** For more information about GUIDs, go to http://go.microsoft.com/fwlink/?LinkId=286551

Demonstration: Configuring Audit Policies and User Account Control

Demonstration Steps

Use Group Policy to configure audit policies

1. Sign in to LON-DC1 as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. In the Server Manager window, click **Tools**, and then click **Group Policy Management**.
3. In the console tree, expand **Forest: Adatum.com**, **Domains**, **Adatum.com**, right-click the **Research** OU, and then click **Create a GPO in this domain, and Link it here**.
4. In the **New GPO** dialog box, type **Research Department Security** in the **Name** field, and then click **OK**.
5. Click **Research** OU, right-click **Research Department Security**, and then click **Edit**.
6. In the Group Policy Management Editor, under the **Computer Configuration** node, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, expand **Advanced Audit Policy Configuration**, expand **Audit Policies**, and then click **Object Access**. Discuss the available options under **Object Access**. Briefly explain when you would enable each of these options.

7. Double-click **Audit Handle Manipulation**, select the **Configure the following audit events** check box, select the **Success** check box, select the **Failure** check box, and then click **OK**.
8. Double-click **Audit Removable Storage**, select the **Configure the following audit events** check box, select the **Success** check box, select the **Failure** check box, and then click **OK**.
9. In the Group Policy Management Editor, collapse the **Advanced Audit Policy Configuration** node.

Use Group Policy to configure UAC settings

1. In the Group Policy Management Editor, under the **Computer Configuration\Policies\Windows Settings\Security Settings** node, expand **Local Policies**, and then click **Security Options**. Discuss the available options under the **Security Options** node. Concentrate on the UAC settings.
2. Double-click **User Account Control: Admin Approval Mode for the built-in Administrator account**, select the **Define this policy setting** check box, click **Enabled**, and then click **OK**.
3. Double-click **User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode**, select the **Define this policy setting** check box, click **Prompt for credentials on the secure desktop**, and then click **OK**.
4. Close the Group Policy Management Editor.
5. In the GPMC, expand the **Research** OU, and then click **Research Department Security**. In the Group Policy Management Console pop-up window, click **OK**.
6. On the **Research Department Security** policy, click the **Details** tab.
7. Change the **GPO Status** to **User configuration settings disabled**.
8. In the Group Policy Management pop-up window, click **OK**.
9. On the **Research Department Security** policy, click the **Settings** tab.
10. In the Internet Explorer Dialog box, click **Close**.
11. Review the configured settings.

Demonstration: Using Group Policy to Configure Device and Media Restrictions

Demonstration Steps

1. Sign in to LON-DC1 as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. In the Server Manager window, click **Tools**, and then click **Group Policy Management**.
3. In the console tree, expand **Forest: Adatum.com**, **Domains**, **Adatum.com**, right-click the **Research** OU, and then click **Create a GPO in this domain, and Link it here**.
4. In the **New GPO** dialog box, type **Research Department Device Restrictions** in the **Name** field, and then click **OK**.
5. Click the **Research** OU, right-click the **Research Department Device Restrictions** policy, and then click **Edit**.
6. In the Group Policy Management Editor, under the **Computer Configuration** node, expand **Policies**, expand **Administrative Templates**, expand **System**, expand **Device Installation**, and then click **Device Installation Restrictions**. Discuss the available options under **Device Installation Restrictions.** Briefly explain when you would enable each of these options.
7. Double-click the **Allow administrators to override Device Installation Restriction policies** policy, click **Enabled**, and then click **OK**.

8. Double-click the **Prevent installation of removable devices** policy, click **Enabled**, and then click **OK**.
9. In the Group Policy Management Editor, collapse the **Administrative Templates** node.
10. In the Group Policy Management Editor, under the **Computer Configuration\Policies** node, expand **Windows Settings**, expand **Security Settings**, expand **Advanced Audit Policy Configuration**, expand **Audit Policies**, and then click **Object Access**.
11. Double-click the **Audit Handle Manipulation** policy, select the **Configure the following audit events** check box, select the **Success** check box, select the **Failure** check box, and then click **OK**.
12. Double-click the **Audit Removable Storage** policy, select the **Configure the following audit events** check box, select the **Success** check box, select the **Failure** check box, and then click **OK**.
13. In the Group Policy Management Editor, collapse the **Advanced Audit Policy Configuration** node.
14. In the Group Policy Management Editor, under the **Computer Configuration\Policies\Windows Settings\Security Settings** node, expand **Local Policies**, and then click **Security Options**.
15. Double-click the **User Account Control: Admin Approval Mode for the built-in Administrator account** policy, select the **Define this policy setting** check box, click **Enabled**, and then click **OK**.
16. Double-click the **User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode** policy, select the **Define this policy setting** check box, click **Prompt for credentials on the secure desktop**, and then click **OK**.
17. Close the Group Policy Management Editor.
18. In the GPMC, expand the **Research** OU, and then click the **Research Department Device Restrictions** policy.
19. In the Group Policy Management Console pop-up window, click **OK**.
20. On the **Research Department Device Restrictions** policy, click the **Details** tab.
21. Change the **GPO Status** to **User configuration settings disabled**.
22. In the Group Policy Management pop-up window, click **OK**.
23. On the **Research Department Device Restrictions** policy, click the **Settings** tab.
24. In the Internet Explorer Dialog box, click **Close**.
25. Review the configured settings.

Lesson 2

Planning and Implementing BitLocker

Contents:

Resources

Planning and Deploying the MBAM Client

Reference Links: Time permitting, show one or more of the following videos:
Deploying the MBAM Agent with Group Policy: http://go.microsoft.com/fwlink/?LinkId=286497
Deploying the MBAM Agent with MDT: http://go.microsoft.com/fwlink/?LinkId=286550

Demonstration: Implementing the MBAM Server and Client Components

Demonstration Steps

Configure an MBAM GPO

1. On LON-DC1, from Server Manager, click **Tools**, and then click **Group Policy Management**.
2. In the GPMC, expand **Forest:Adatum.com**, expand **Domains**, right-click **Adatum.com**, and then click **Create a GPO in this domain, and link it here**.
3. In the **New GPO** dialog box, in the **Name** field, type **Research Department MBAM Policy**, and then click **OK**.
4. In the GPMC, expand **Adatum.com**, and then click the **Research Department MBAM Policy** GPO.
5. In the Group Policy Management Console pop-up window, click **OK**.
6. In the **Security Filtering** section, click **Authenticated Users**, and then click **Remove**.
7. In the Group Policy Management pop-up window, click **OK**.
8. In the **Security Filtering** section, click **Add**.
9. In the **Select User, Computer, or Group** dialog box, click **Object Types**.
10. In the **Object Types** dialog box, select the **Computers** check box, and then click **OK**.
11. In the **Enter the object name to select** field, type **LON-CL1**, and then click **OK**.

Note: In a production environment, this GPO would have been created at the nearest organizational unit (OU) above the computers it would apply to. Due to the structure of the Adatum domain, we are using security filtering to ensure this policy setting only applies to our Research department computer.

12. Right-click the **Research Department MBAM Policy** GPO, and then click **Edit**.
13. Under **Computer Configuration**, expand **Policies**, expand **Administrative Templates**, expand **Windows Components**, and then expand **MDOP MBAM (BitLocker Management)**.
14. In the console tree, click the **Client Management** container, and then double-click the **Configure MBAM services** policy.
15. Specify the following settings:
    - Click **Enabled**
    - MBAM Recovery service endpoint: **https://LON-MB1.adatum.com/MBAMRecoveryAndHardwareService/CoreService.svc**
    - MBAM Status reporting service endpoint: **https://LON-MB1.adatum.com/MBAMComplianceStatusService/StatusReportingService.svc**

16. In the **Configure MBAM services** policy, click **OK**.
17. In the console tree, click the **Operating System Drive** container, and then double-click the **Operating system drive encryption settings** policy.
18. Specify the following settings:
    - Click **Enabled**
19. In the **Operating system drive encryption settings** policy, click **OK**.
20. In the console tree, click the **Removable Drive** container, and then double-click the **Control Use of BitLocker on removable drives** policy.
21. Specify the following settings:
    - Click **Enabled**
22. In the **Control Use of BitLocker on removable drives** policy, click **OK**.
23. In the console tree, click the **Fixed Drive** container, and then double-click the **Choose how BitLocker-protected fixed drives can be recovered** policy.
24. Specify the following settings:
    - Click **Enabled**
25. In the **Choose how BitLocker-protected fixed drives can be recovered** policy, click **OK**.
26. Close the Group Policy Management Editor.
27. Close the GPMC.

Install the MBAM client

1. Sign in to the LON-CL1 virtual machine as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. On the **Start** screen, type **command**, right-click **Command Prompt**, and then click **Run as administrator**.
3. At the command prompt, type **GPUPDATE /force**, and then press Enter.
4. Close the Command Prompt window.
5. Open File Explorer.
6. Navigate to **\\LON-MB1\E$\Labfiles\MBAM\Client\x64**.
7. Right-click **MbamClientSetup.exe**, and then click **Run as administrator**.
8. On the End User License Agreement, click **I accept**, and then click **Next**. In the MDOP MBAM pop-up window, click **OK**. The MBAM client installs silently. Close File Explorer.

Lesson 3

Planning and Implementing EFS

Contents:

Demonstration: Configuring EFS in an Enterprise Environment

Demonstration Steps

Configure certificates for EFS

1. Sign in to LON-DC1 as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. Click to the **Start** screen, type **MMC.exe**, and then press Enter.
3. In Console 1, click **File**, and then click **Add/Remove Snap-in**.
4. In the **Add or Remove Snap-ins** dialog box, click **Certificate Templates**, and then click **Add**.
5. In the **Add or Remove Snap-ins** dialog box, click **OK**.
6. Click the **Certificate Templates** node.
7. Right-click the **Basic EFS** template, and then click **Duplicate Template**.
8. Click the **General** tab, and in the **Template display name** field, type **Adatum EFS**.
9. Click the **Security** tab, click **Authenticated Users**, and then select the **Allow** check box for **Autoenroll**.
10. In the **Properties for New Template** dialog box, click **OK**.
11. Close Console 1 without saving changes to the console.
12. In the Server Manager, click **Tools**, and then click **Certification Authority**.
13. Expand **Adatum-LON-DC1-CA**, and then click **Certificate Templates**.
14. Right-click the **Certificate Templates** node, point to **New**, and then click **Certificate Template to Issue**.
15. In the **Enable Certificate Templates** dialog box, click **Adatum EFS**, and then click **OK**.
16. Close the Certification Authority console.

Configure a GPO to support EFS

1. In the Server Manager window, click **Tools**, and then click **Group Policy Management**.
2. In the console tree, expand **Forest: Adatum.com**, **Domains**, right-click **Adatum.com**, and then click **Create a GPO in this domain, and Link it here**.
3. In the **New GPO** dialog box, type **Research Department EFS** in the **Name** field, and then click **OK**.
4. In the GPMC, expand **Adatum.com**, and then click the **Research Department EFS** GPO.
5. In the Group Policy Management Console pop-up window, click **OK**.
6. In the **Security Filtering** section, click **Authenticated Users**, and then click **Remove**.
7. In the Group Policy Management pop-up window, click **OK**.
8. In the **Security Filtering** section, click **Add**.
9. In the **Select User, Computer, or Group** dialog box, click **Object Types**.
10. In the **Object Types** dialog box, select the check box for **Computers**, and then click **OK**.
11. In the **Enter the object name to select** field, type **LON-CL1**, and then click **OK**.
12. Right-click the **Research Department EFS** policy, and then click **Edit**.
13. In the Group Policy Management Editor, under the **Computer Configuration** node, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, and then click **Public Key Policies**.

14. Right-click the **Encrypting File System** node, and then click **Properties**.
15. In the **Encrypting File System Properties** dialog box, on the **General** tab, click **Allow**.
16. Click the **Certificates** tab, and then click **Browse**.
17. Click the **Adatum EFS** certificate template, and then click **OK**.
18. Clear the **Allow EFS to generate self-signed certificates when a certification authority is not available** check box.
19. In the **Encrypting File System Properties** dialog box, click **OK**.
20. Right-click the **Encrypting File System** node, and then click **Create Data Recovery Agent**.
21. Close the Group Policy Management Editor.
22. On the **Research Department EFS** policy, click the **Details** tab.
23. Change the **GPO Status** to **User configuration settings disabled**.
24. In the Group Policy Management pop-up window, click **OK**.
25. On the **Research Department EFS** policy, click the **Settings** tab.
26. In the Internet Explorer Dialog box, click **Close**.
27. Review the configured settings.

Module Review and Takeaways

Best Practice

BitLocker Best Practices

- Provide end-user training before requiring the use of BitLocker.
- Use multifactor authentication methods, such as TPM and PIN, or TPM and USB drive.
- Store recovery data in either AD DS or MBAM.
- Suspend and resume BitLocker immediately after performing any operations that affect the boot drive. This will prevent the drive from locking on the next restart.
- Disable hibernation features on systems protected with BitLocker.
- Encrypt drives before adding data.

EFS Best Practices

- Provide end-user training on backing up the EFS certificate if using self-signed certificates.
- Encrypt folders, not individual files.
- Always configure a recovery agent.
- Do not destroy recovery certificates if a recovery agent is changed. New recovery agents are not added to previously encrypted files.
- Designate multiple recovery agents.
- Encrypt the print spooler folder(s).

Lab Review Questions and Answers

Lab A: Configuring Desktop Security

Question and Answers

Lab Review

Question: In your environment, do you use removable device restriction policies?

Answer: Answers will vary. The instructor should direct the discussion towards situations where it may be beneficial.

Question: In your environment, do you use BitLocker? If so, do you use MBAM?

Answer: Answers will vary. The instructor should direct the discussion to focus on the students' experience with the lab.

Lab B: Configuring File Encryption by Using EFS

Question and Answers

Question: Why was Ivan unable to open the Private file? Why was the Administrator account initially unable to open the Private file?

Answer: The Private file was encrypted using Ed's public key, from the certificate issued by LON-DC1. Neither Ivan nor the Administrator account had access to the private key needed to decrypt the file.

Question: Why was the Administrator account able to decrypt the Private file after the certificate import?

Answer: The file was encrypted with a file encryption key, and then the file encryption key was encrypted with Ed's public key and attached to the file. It was encrypted again with the Administrator's public key and published in AD DS from his EFS recovery certificate. Because the administrator was not using a roaming profile, the certificate had to be imported into the Administrators account on the machine where the file that needed to be recovered resided. Once this certificate was imported, the Administrator account then had the private key necessary to decrypt the file encryption key.

Module 4

Capturing and Managing a Desktop Operating System Image

Contents:

Lesson 2

Managing Windows PE

Contents:

Demonstration: Customizing a Windows PE Image

Demonstration Steps

Create the Windows PE environment to be customized

1. On LON-DC1, open the **Start** screen, right-click **Deployment and Imaging Tools Environment**, and then click **Run as administrator**.
2. In the Administrator: Deployment and Imaging Tools Environment window, type the following command, and then press Enter.

```
Copype amd64 E:\winpe_x64
```

When complete, the Administrator: Deployment and Imaging Tools Environment window should display a Success message.

3. Click **File Explorer** on the taskbar.
4. In the navigation pane, expand **Allfiles (E:)**, expand **WinPE_x64**, expand **Media**, and then click **Sources**.
5. Note the size of the Boot.wim file.
6. Close File Explorer.

Mount the base Windows PE image

1. In the Administrator: Deployment and Imaging Tools Environment window, type the following command, and then press Enter.

```
DISM /mount-image /imagefile:E:\winpe_x64\media\sources\boot.wim /index:1
/mountdir:E:\winpe_x64\mount
```

2. When complete, the Administrator: Deployment and Imaging Tools Environment window should display The operation completed successfully.

Add drivers and packages to Windows PE

1. To add the Hyper-V® drivers to the Windows PE image, type the following command, and then press Enter.

```
DISM /image:E:\winpe_x64\mount /add-Driver /driver:E:\Labfiles\IPx64_8.2  /recurse
/forceunsigned
```

2. When complete, the Administrator: Deployment and Imaging Tools Environment window should show that drivers have been installed, and you should have a message that The operation completed successfully.
3. To add support for Windows PowerShell® 3.0 command-line interface to the Windows PE image, type the following commands, pressing Enter after each. After each DISM command, check for The operation completed successfully message:

```
C:
CD C:\Program Files (x86)\Windows Kits\8.0\Assessment and deployment kit\Windows
preInstallation Environment\amd64\WinPE_OCs
DISM /image:E:\winpe_x64\mount /Add-Package /PackagePath:.\WinPE-NetFX4.cab
DISM /image:E:\winpe_x64\mount /Add-Package /PackagePath:.\WinPE-Scripting.cab
DISM /image:E:\winpe_x64\mount /Add-Package /PackagePath:.\WinPE-WMI.cab
DISM /image:E:\winpe_x64\mount /Add-Package /PackagePath:.\WinPE-PowerShell3.cab
E:
CD E:\winpe_x64
```

4. After you have completed the commands, verify that there are no error messages.

Commit changes to the Windows PE image

1. To save the changes and unmount the image, type the following command, and then press Enter.

```
DISM /unmount-image /mountdir:E:\winpe_x64\mount /commit
```

2. When complete, the Administrator: Deployment and Imaging Tools Environment window should display The operation completed successfully.

Demonstration: Creating Windows PE Media

Demonstration Steps

Create Windows PE media

1. The previous command modified the **E:\winpe_x64\Media\boot.wim** image. To create an ISO image that you can use to start media, run the following command.

```
MD E:\BootWims
Makewinpemedia /iso E:\winpe_x64 E:\BootWims\winpe_x64.iso
```

2. Click **File Explorer** on the taskbar.
3. In the navigation pane, expand **Allfiles (E:)**, and then click **BootWims**.
4. Right-click **WinPE_x64.iso**, and then click **Mount**.
5. In the DVD Drive (F:) DVD_ROM window, examine the contents of the WinPE_x64.iso file.
6. In the navigation pane, right-click **DVD Drive (F:) DVD_ROM**, and then click **Eject**.
7. Close the Administrator: Deployment and Imaging Tools Environment window.

Lesson 3

Building a Reference Image by Using Windows SIM and Sysprep

Contents:

Resources

Overview of Windows Setup

Additional Reading: For a complete list of the available command-line options, review http://go.microsoft.com/fwlink/?LinkId=286553

Demonstration: Creating Answer Files by Using Windows SIM

Demonstration Steps

Create an answer file

1. In your host system, in Hyper-V Manager, right-click the host name, point to **New**, and then click **Floppy Disk**.
2. Browse to **C:\Program Files\Microsoft Learning\20415**, type *your name* in the **File name** field, and then click **Create**.
3. Switch to the 20415B-LON-DC1 window, click **Media**, point to **Diskette Drive**, and then click **Insert Disk**.
4. Browse to the **C:\Program Files\Microsoft Learning\20415** folder, select the .vfd file you created, and then click **Open**.
5. On the taskbar, click **File Explorer**, and then click **Computer**.
6. Double-click **Floppy Disk Drive (A:)**, and then in the Microsoft® Windows prompt, click **Format disk**.
7. In the Format Floppy Disk Drive (A:) window, in the **Volume label** field, type **Answer File**, and then click **Start**.
8. In the Format Floppy Disk Drive (A:) warning, click **OK**.
9. In the Format Floppy Disk Drive (A:) Format Complete window, click **OK**.
10. In the Format Floppy Disk Drive (A:) window, click **Close**.
11. Close File Explorer.
12. Open the **Start** screen, and then click the **Windows System Image Manager** tile.
13. In the Windows System Image Manager, click **File**, and then click **Select Windows Image**.
14. In the **Select a Windows Image** dialog box, browse to the **E:\Labfiles\Windows8\sources** folder, select **install.wim**, and then click **Open**.
15. In the **Windows System Image Manager** message box, click **Yes**.
16. In the Answer File pane, right-click **Create or open an answer file**, and then click **Open Answer File**.
17. In the **Open** dialog box, browse to the **C:\Program Files (x86)\Windows Kits\8.0\Assessment and Deployment Kit\Deployment Tools\Samples\Unattend** folder, select **Autounattend_x64_BIOS_sample.xml**, and then click **Open**.

Note: Explain that you are using the sample file as a starting point and that you will be customizing it soon.

18. In the Windows System Image Manager pop-up window, click **Yes**.

19. In the Windows System Image Manager, click **File**, and then click **Save Answer File As**.
20. In the **Save As** dialog box, click **Computer**, and then double-click **Floppy Disk Drive (A:)**.
21. In the **File name** field, type **Autounattend**, and then click **Save**.

Note: Explain that Windows Setup looks for Autounattend in the root of removable drives when it runs.

Add and configure components

1. In the Answer File pane, under the Components node, explain the settings imported with the sample file as listed in the following three steps.
2. Expand **1 WindowsPE**, expand the **amd64_Microsoft-Windows-Setup_neutral** component, and then click **UserData**. In the **FullName** field, type *your name,* and then in the **Organization** field, type *your company*.

Note: Point out the AcceptEula setting on the UserData component.

3. In the Windows Image pane, under **Components**, expand **amd64_Microsoft-Windows-Shell-Setup_6.2.9200.16384_neutral**.
4. Right-click **OEMInformation**, and then select **Add Setting to Pass 7 oobeSystem**.
5. Expand **amd64_Microsoft-Windows-Shell-Setup_neutral**, select **OEMInformation**, and then in the **Manufacturer** field, type *your company*.
6. In the **Support Hours** field, type **6:00 am to 8:00 pm**.
7. In the **SupportPhone** field, type **555-436-6227**.
8. In the **SupportURL** field, type *your company url*.
9. In the Windows Image pane, expand **Packages**, expand **Foundation**, right-click **amd64_Microsoft-Windows-Foundation-Package_6.2.9200.16384_**, and then select **Add to Answer File**.
10. In the Answer File pane, expand **Packages**, expand **Foundation**, and then select **amd64_Microsoft-Windows-Foundation-Package_6.2.9200.16384_**.
11. In the Microsoft-Windows-Foundation-Package Properties pane, expand **Microsoft-Hyper-V-All**, click **Microsoft-Hyper-V-Tools-All**, and then enable **Microsoft-Hyper-V-Management-Clients** and **Tools-All**.

Validate and save the answer file

1. In the Windows System Image Manager, click **Tools**, and then click **Validate Answer File**.
2. In the Windows System Image Manager, click **File**, and then click **Save Answer File**.
3. Leave the Windows System Image Manager open.

Lesson 4

Capturing and Servicing a Reference Image

Contents:

Demonstration: Mounting and Servicing an Image by Using DISM

Demonstration Steps

Mount an image with DISM

1. On LON-DC1, click **File Explorer** on the taskbar.
2. Click on the **Allfiles (E:)** drive, right-click in the results pane, point to **New**, and then click **Folder**.
3. Name the new folder **Servicing**.
4. Open the **Start** screen, and then click the **Deployment and Imaging Tools Environment** tile.
5. Right-click the Command Prompt symbol on the Deployment and Imaging Tools Environment window, and then click **Properties**.
6. Click the **Layout** tab, and adjust the **Screen Buffer Size Height** to **1000**.
7. In the Administrator: Deployment and Imaging Tools Environment window, type the following command, and then press Enter.

```
DISM /Get-ImageInfo /ImageFile:E:\Labfiles\Windows8\sources\install.wim
```

8. Discuss the results of the command.
9. In the Administrator: Deployment and Imaging Tools Environment window, type the following command, and then press Enter.

```
DISM /Mount-Image /ImageFile:E:\Labfiles\Windows8\sources\install.wim /Index:1
/MountDir:E:\Servicing
```

Service an Image with DISM

1. In the Administrator: Deployment and Imaging Tools Environment window, type the following command, and then press Enter.

```
DISM /Image:E:\Servicing /Get-Packages
```

2. Briefly discuss the results of the command.
3. To retrieve detailed information about the Windows Foundation Package, type the following command, and then press Enter.

```
DISM /Image:E:\Servicing /Get-PackageInfo /PackageName:Microsoft-Windows-Foundation-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384
```

4. Briefly discuss the results of the command.
5. To enable the Scan Management Console feature in the image, type the following command, and then press Enter.

```
DISM /Image:E:\Servicing /Enable-Feature /FeatureName:ScanManagementConsole
```

6. To retrieve information about the Windows-based features installed, type the following command, and then press Enter.

```
DISM /Image:E:\Servicing /Get-Features
```

7. Scroll up and check the status of the ScanManagementConsole feature.
8. Click **File Explorer** on the taskbar, and then browse to **E:\Servicing**. Right-click in the results pane, point to **New**, and then click **Folder**.

9. Name the new folder **ImportantDocs**.
10. Close the File Explorer window.
11. To unmount the image and discard the changes, in the Administrator: Deployment and Imaging Tools Environment window, type the following command, and then press Enter.

Module Review and Takeaways

Best Practice

Best Practices for Creating Answer Files

- Always validate answer files in Windows SIM. Using Windows SIM to create and validate your answer files will lessen the likelihood of creating invalid answer files.
- Avoid unnecessary settings. Including settings that are not required can introduce deployment issues that can be hard to troubleshoot.
- Understand the configuration passes. Understanding what happens during each configuration pass is very important when creating answer files.
- Avoid creating empty elements. You can use Windows SIM to create empty values. However, not all settings will work with empty elements, and this may cause deployment issues.
- Use separate answer files for each architecture type. If an answer file contains settings for multiple architectures, the values may get applied multiple times, or with the wrong values.
- Use multiple answer files for specific customizations. To prevent the misconfiguration of values, create separate answer files for audit mode, OOBE mode, Copy Profile, or other custom scenarios you may have.
- Use the correct mechanisms to add updates to a Windows image. If you do not use DISM or Windows Update to add updates to an image, you may invalidate sections of your answer files.

Review Question(s)

Question: In your environment, what processes do you follow to keep your images current?

> **Answer:** Answers will vary but could include deploying the image to a computer and manually updating the image. Review what you can and cannot use DISM for.

Lab Review Questions and Answers

Lab A: Preparing the Imaging and Windows PE Environment

Question and Answers

Lab Review

Question: How would you add files to the Windows PE image in the E:\winpe_x64 folder?

Answer: You can add drivers with the **/Add-Driver** switch, and add packages with the **/Add-Package** switch. However, to add files and folders to a Windows PE image that is mounted, you can simply copy them to the location in the mounted file structure where you want the files to be.

Question: What additional files or components might you add to a Windows PE image?

Answer: Answers will vary but could include log file readers, such as CMTrace.exe, or any of the additional components discussed in class.

Lab B: Building a Reference Image by Using Windows SIM and Sysprep

Question and Answers

Question: When creating an answer file, several options could be added to multiple phases of the installation. Why would you use a component in multiple phases?

Answer: Some components, such as amd64_Microsoft-Windows-Shell-Setup_neutral, contain related settings that could be set in either phase of an installation. Certain settings in a component, such as ComputerName, can be used in only one of the phases.

Question: When working in audit mode, what kind of changes can you make? How could the CopyProfile setting help?

Answer: You can make changes such as adding applications, creating shortcuts, making changes to the administrator profile, and adding documents. When capturing the image, any programs or files added to the image would be captured. However, any profile changes are not captured unless the CopyProfile setting is used.

Question: Would you create a local administrative account in an image that will be joined to a domain when it is deployed? Why or why not?

Answer: Answers will vary. One reason to create a local account is to provide support personnel with an administrative account that they can use to sign in if the computer cannot communicate with the domain. One reason not to do it is that users could learn the password for the account and use it to install unauthorized software.

Lab C: Capturing and Servicing a Reference Image

Question and Answers

Question: What other types of software might you install in an offline image?

Answer: Answers will vary but could include .msu file format–based packages, or drivers for Plug and Play devices such as a corporate standard local printer.

Question: What would you do if you made a mistake while editing an image with DSIM?

Answer: You could use the **/Unmount-Wim /Discard** switches to unload the image without committing the changes.

Lab D: Configuring and Managing Windows DS

Question and Answers

Question: Why would you want to use an answer file with a Windows DS deployment?

Answer: You use the answer file for greater control over the image deployment.

Question: If you used Windows DS in your environment, would you use a Windows Deployment Services client unattend file?

Answer: Answers will vary. Using the Windows Deployment Services client unattend file allows you to automate the deployment process almost completely.

Module 5

Planning and Implementing User State Migration

Contents:

Lesson 1

Overview of User State Migration

Contents:

Question and Answers

Tools for User State Migration

Question: You have been asked to upgrade ten Windows 7 computers to Windows 8 in a small branch office. You also have been asked to perform a clean installation of Windows 8 and to show the local manager how to migrate user files and other data after Windows 8 has been installed. The manager will perform the Windows 8 installation and user state migration for the rest of the computers, as staff members make workstations available.

> **Answer:** Windows Easy Transfer is the best option in this scenario. A nontechnical user will perform the migration on a small number of computers, so Windows Easy Transfer's 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 Vista® desktop computers replaced with new Windows 8 computers.

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

Question: Your organization needs to move five employees from headquarters in London to the regional office in Toronto. The employees will not be taking their computers with them, but they want to access their files and settings in their new offices as soon as possible.

> **Answer:** In this scenario, you can use either of the tools. The information given for this scenario leaves the option open. You could use Windows Easy Transfer on their computers in London, place the exported user states on a USB drive, and then send the drive with them to Toronto, where they could run Windows Easy Transfer to import the settings stored on the drive. Alternatively, you could use Group Policy to set up a script to run for those five users, using ScanState in London and LoadState in Toronto.

Resources

 **Additional Reading:** For more information on Windows Easy Transfer, go to http://go.microsoft.com/fwlink/?LinkId=286556

 **Additional Reading:** For more information on USMT, go to http://go.microsoft.com/fwlink/?LinkId=286474

Features and Elements of USMT

 **Additional Reading:** For more information on USMTUtils Syntax, go to http://go.microsoft.com/fwlink/?LinkId=286557

Lesson 3

Migrating User State by Using USMT

Contents:

Question and Answers

Capturing User State by Using ScanState

Question: Using the example at the end of the topic, answer the following questions:

Where will the scanned results be stored?

What syntax controls the application settings and the user settings?

What does the **/ue** option do in this example?

Answer: Answers are as follows:

1. Results will be stored at \\LON-DC1\DesktopMigration.
2. The **/i:migapp.xml** and the **/i:miguser.xml** options control application and user settings.
3. The **/ue:Adatum\Don** option excludes the user account Don from migrating.

Restoring User State by Using LoadState

Question: Using the example at the end of the topic, answer the following questions:

Where will the user state be retrieved from?

What does the **/ui** option do in this example?

What would occur if the **/lae** switch was not provided in this example?

Answer: Answers are as follows:

1. The user state will be retrieved from \\LON-DC1\DesktopMigration.
2. The **/ui:DBService** command includes migrating an account named DBService.
3. The DBService account would be created and then disabled. The **/lae** switch enables the account.

Resources

Best Practices for Using USMT

 **Additional Reading:** For more information on USMT best practices, go to http://go.microsoft.com/fwlink/?LinkId=286558

Module Review and Takeaways

Review Question(s)

Question: Why would you choose to run ScanState and LoadState from the Windows Preinstallation Environment (PE), rather than from within the source operating system?

Answer: Generally, this is done because USMT tools are loaded into the copy of Windows PE that you are starting the computer with. Windows PE also loads independently of whatever operating system is installed on the computer and does not require you to sign in to the source operating system interactively. Windows PE typically loads faster than a standard installation of the Windows operating system.

Question: Why is USMT a better option than Windows Easy Transfer for large-scale user state migration scenarios?

Answer: Windows Easy Transfer must run interactively as a wizard-based process, which would be too time-consuming for a large number of computers. USMT's command line–based components can incorporate easily into scripts or other methods of automation.

Tools

Tool	Use for	Where to find it
ScanState.exe	Collecting user state data for migration	Windows Assessment and Deployment Kit (ADK) http://go.microsoft.com/fwlink/?LinkId=286474
LoadState.exe	Restoring user state data to newly installed operating systems	Windows ADK http://go.microsoft.com/fwlink/?LinkId=286474
USMTUtils.exe	Configuring and diagnosing the USMT environment	Windows ADK http://go.microsoft.com/fwlink/?LinkId=286474

Lab Review Questions and Answers

Lab A: Planning and Implementing User State Migration

Question and Answers

Lab Review

Question: In Exercise 1, why was it important to record which edition (32-bit or 64-bit) of the Windows operating system was being used on the source computer?

Answer: There are several differences between 32-bit and 64-bit editions of the Windows operating system, including driver support and available features. This was recorded to ensure that the destination version of Windows would be compatible with the settings migrated from the source version.

Question: Is ScanState used only to capture user state?

Answer: No. ScanState also can monitor user state migration information and can test migration scenarios.

Module 6

Planning and Deploying Desktops by Using the Microsoft Deployment Toolkit

Contents:

Lesson 2

Implementing MDT 2012 for LTI

Contents:

Demonstration: Configuring the Deployment Share

Demonstration Steps

Create an MDT deployment share

1. On LON-SVR1, in the 20415B-LON-SVR1 on localhost window, click **Media**, point to **DVD Drive**, and then click **Insert Disk**.
2. In the Open dialog box, browse to C:\Program files\Microsoft Learning\20415\Drives.
3. Click **Win8EntRTMEval.iso**, and then click **Open**.
4. On LON-SVR1, open the **Start** screen, and then click on the **Deployment Workbench** tile.
5. In the Deployment Workbench console, click on the **Deployment Shares** node.
6. Right-click the **Deployment Shares** node, and then click **New Deployment Share**.
7. In the New Deployment Share Wizard, on the **Path** page, in the **Deployment share path** field, type **C:\DeploymentShare**, and then click **Next**.
8. On the **Share** page, click **Next**.
9. On the **Descriptive Name** page, click **Next**.
10. Review the **Options** page, and then click **Next**.
11. On the **Summary** page, click **Next**.
12. On the **Confirmation** page, click **Finish**.

Examine the deployment share properties

1. In the Deployment Workbench, expand the **Deployment Share** node, and then expand **MDT Deployment Share**.
2. Briefly discuss each item shown.
3. Right-click **MDT Deployment Share**, and then click **Properties**.
4. Review the **General** tab, discuss the settings that were configured through the wizard, and then point out that the **Platforms Supported** settings are not configured through the wizard.
5. Click on the **Rules** tab, and then explain that the Rules are stored in the CustomSettings.ini file from the Control folder.
6. Click **Edit Bootstrap.ini**. Explain that this file also is in the Control folder.
7. Close Notepad.
8. Click the **Windows PE** tab. Explain that these settings control the creation of the boot media. Review the **Features** tab and the **Drivers and Patches** tab. Explain that the settings need to be configured separately for both platform types.
9. Click the **Monitoring** tab.
10. Close the **MDT Deployment Share Properties** dialog box.

Import operating system files into the deployment share

1. Right-click the **Operating Systems** node, and then click **Import Operating System**.
2. In the Import Operating System Wizard, on the **OS Type** page, select the **Full set of source files** option, and then click **Next**.
3. On the **Source** page, in the **Source directory** field, type **D:**, and then click **Next**.

4. On the **Destination** page, in the **Destination directory name** field, type **Windows8x64**, and then click **Next**.
5. On the **Summary** page, click **Next**.
6. On the **Confirmation** page, click **Finish**.

Create a subfolder in the Out-of-Box Drivers folder

1. Right-click the **Out-of-Box Drivers** node, and then click **New Folder**.
2. In the New Folder Wizard, on the **General Settings** page, in the **Folder name** field, type **Intellipoint Drivers**, and then click **Next**.
3. On the **Summary** page, click **Next**.
4. On the **Confirmation** page, click **Finish**.

Import device drivers into the deployment share

1. Right-click the **Intellipoint Drivers** folder, and then click **Import Drivers**.
2. In the Import Driver Wizard, on the **Specify Directory** page, in the **Driver source directory** field, type **\\LON-DC1\Labfiles\IPx64_8.2**, and then click **Next**.
3. On the **Summary** page, click **Next**.
4. On the **Confirmation** page, click **Finish**.

Demonstration: Configuring a Task Sequence and Updating the Deployment Share

Demonstration Steps

Create a standard client task sequence

1. On LON-SVR1, in the Deployment Workbench, in the **MDT Deployment Share**, right-click the **Task Sequences** item, and then click **New Task Sequence**.
2. In the New Task Sequence Wizard, on the **General Settings** page, in the **Task sequence ID** field, type **LON-001**.
3. In the **Task sequence name** field, type **Deploy Windows 8**, and then click **Next**.
4. On the **Select Template** page, select the **Standard Client Task Sequence** from the task sequence templates drop-down list, and then click **Next**.
5. On the **Select OS** page, click **Windows 8 Enterprise Evaluation in Windows8x64 install.wim**, and then click **Next**.
6. On the **Specify Product Key** page, select the **Do not specify a product key at this time** option, and then click **Next**.
7. On the **OS Settings** page, in the **Full Name** field, type **Administrator**. In the **Organization** field, type **Adatum**, and then click **Next**.
8. On the **Admin Password** page, in the **Administrator Password** and **Please confirm Administrator Password** fields, type **Pa$$w0rd**, and then click **Next**.
9. On the **Summary** page, click **Next**.
10. On the **Confirmation** page, click **Finish**.

Edit the standard client task sequence

1. In the navigation pane, click the **Task Sequences** node.

2. Right-click the **Deploy Windows 8** task sequence, and then click **Properties**.
3. Discuss the properties on the **General** tab.
4. Click the **Task Sequence** tab and briefly discuss the task steps in the task sequence.
5. Expand **Preinstall**, and then click **Inject Drivers**. From the **Choose a selection profile** drop-down list, choose the **Nothing** selection.
6. Click the **OS Info** tab and briefly discuss the information on the **OS Info** tab.
7. Click **OK** to close the Deploy Windows 8 Properties window.

Update a deployment share

1. Right-click the **MDT Deployment Share**, and then click **Update Deployment Share**.
2. In the Update Deployment Share Wizard, on the **Options** page, click **Next**.
3. On the **Summary** page, click **Next**.
4. On the **Progress** page, discuss the events being shown.

Module Review and Takeaways

Review Question(s)

Question: In your environment, if you were going to use the LTI method, how much information would you allow your users to input during the installation?

Answer: Answers will vary. You can customize the configuration files, Bootstrap.ini and CustomSettings.ini, to require the user to fill in several wizard pages or none at all.

Lab Review Questions and Answers

Lab: Planning and Deploying Desktops by Using MDT

Question and Answers

Lab Review

Question: How many task sequences would you need to create to deploy a client image if the client machine could join any one of four domains in a forest?

Answer: Because this is an LTI deployment, the user that initiates the deployment specifies the domain the computer will join. Therefore only one task sequence is required.

Question: In the lab, you edited the Bootstrap.ini file to show how the *%WDSServer%* variable worked. If you were using MDT in your environment, when would you use this configuration?

Answer: Answers will vary. However, you could include this configuration when using linked deployment shares, each with a local Windows DS server, and you want to maintain identical configuration files on all the deployment shares.

Module 7

Planning and Deploying Desktops by Using System Center 2012 Configuration Manager

Contents:

Lesson 1

Planning the ZTI Environment

Contents:

Demonstration: Configuring MDT Integration

Demonstration Steps

Install MDT

1. On LON-CFG1, on the taskbar, click **File Explorer**.
2. In the **Address** field, type **\\LON-DC1\Labfiles\MDT**, and then press Enter.
3. Right-click **MicrosoftDeploymentToolit2012_x64.msi**, and then click **Install**.
4. In the Microsoft Deployment Toolkit 2012 Update 1 Setup Wizard, on the **Welcome** screen, click **Next**.
5. On the **End-User License Agreement** page, select the **I accept the terms in the License Agreement** check box, and then click **Next**.
6. On the **Custom Setup** page, click **Next**.
7. On the **Customer Experience Improvement Program** page, click **Next**.
8. On the **Ready to Install Microsoft Deployment Toolkit 2012 Update 1** page, click **Install**.
9. On the **Completed the Microsoft Deployment Toolkit 2012 Update 1 Setup Wizard** page, click **Finish**.
10. Close File Explorer.

Integrate MDT with Configuration Manager

1. Open the **Start** screen, and then click **Configure ConfigMgr Integration**.
2. In the Configure ConfigMgr Integration wizard, on the **Options** page, click **Next**.
3. On the **Confirmation** page, click **Finish**.

Confirm MDT integration

1. On the taskbar, click **Configuration Manager Console**.
2. Click the **Software Library** workspace, expand the **Operating Systems** node, right-click **Task Sequences**, and confirm that **Create MDT Task Sequence** is in the shortcut menu.
3. Leave the Configuration Manager console open.

Lesson 2

Preparing the Site for Operating System Deployment

Contents:

Demonstration: Creating an Operating System Image Package

Demonstration Steps

Note: Explain that Configuration Manager 2012 SP1 uses an operating system image package in the build and capture task sequence, not the operating system installer package.

Create an operating system image package

1. In the Configuration Manager console, click the **Operating Systems Images** node.
2. On the ribbon, in the **Create** group, click **Add Operating System Image**.
3. In the Add Operating System Installer Wizard, on the **Data Source** page, in the **Path** box, type **\\LON-DC1\Labfiles\Windows8\Sources\Install.wim**, and then click **Next**.
4. On the **General** page, click **Next**.
5. On the **Summary** page, click **Next**.
6. On the **Completion** page, click **Close**.

Distribute an operating system image package

1. Right-click the **Windows 8 Enterprise Evaluation** image package, and then click **Distribute Content**.
2. In the Distribute Content Wizard, on the **General** page, click **Next**.
3. On the **Content Destination** page, click **Add**, and then click **Distribution Point**.
4. In the **Add Distribution Points** dialog box, select the **\\LON-CFG1.Adatum.com** check box, and then click **OK**.
5. On the **Content Destination** page, click **Next**.
6. On the **Summary** page, click **Next**.
7. On the **Completion** page, click **Close**.

Demonstration: Managing Device Drivers

Demonstration Steps

Create a share for the drivers

1. Click **File Explorer** in the taskbar.
2. Click the **All Files (E:)** drive, right-click in the details pane, point to **New**, and then click **Folder**. Name the new folder **Drivers**.
3. Select the **Drivers** folder, and then in the toolbar, click **Share**.
4. Click **Specific people**, in the **File Sharing** dialog box, click the drop-down list, select **Everyone**, and then click **Add**.
5. Click the drop-down list for the **Everyone** group, and then select **Read/Write**.
6. In the **File Sharing** dialog box, click **Share**, and then click **Done**.
7. Close File Explorer.

Import Intellipoint drivers

1. On LON-CFG1, click the **Software Library** workspace, expand the **Operating Systems** folder, and then click the **Drivers** node.
2. Right-click the **Drivers** node, and then click **Import Driver**.
3. On the **Locate Driver** page, click **Browse**.
4. In the **Select Folder** dialog box, in the **Folder** box, type **\\LON-DC1\Labfiles\IPx64_8.2**, and then click **Select Folder**.
5. On the **Locate Driver** page, click **Next**.
6. On the **Driver Details** page, click **Categories**, and then in the **Manage Administrative Categories** dialog box, click **Create**.
7. In the **Create Administrative Category** box, type **64-bit Drivers**, and then click **OK**.
8. In the **Manage Administrative Categories** dialog box, click **Create**.
9. In the **Create Administrative Category** box, type **Intellipoint Drivers**, and then click **OK**.
10. In the **Manage Administrative Categories** dialog box, click **OK**, and on the **Driver Details** page, click **Next**.
11. On the **Add Driver to Packages** page, click **New Package**.
12. In the **Create Driver Package** dialog box, in the **Name** box, type **Intellipoint Drivers**. In the **Path** box, type **\\LON-CFG1\Drivers**, and then click **OK**.
13. On the **Add Driver to Packages** page, click **Next**.
14. On the **Add Driver to Boot Images** page, click **Next**.
15. On the **Summary** page, click **Next**.
16. On the **Completion** page, click **Close**.

Distribute the Intellipoint driver package

1. Click the **Driver Packages** node.
2. Right-click the **Intellipoint Drivers** package, and then click **Distribute Content**.
3. In the Distribute Content Wizard, on the **General** page, click **Next**.
4. On the **Content Destination** page, click **Add**, and then click **Distribution Point**.
5. In the **Add Distribution Points** dialog box, select the **\\LON-CFG1.Adatum.com** check box, and then click **OK**.
6. On the **Content Destination** page, click **Next**.
7. On the **Summary** page, click **Next**.
8. On the **Confirmation** page, click **Close**.
9. Right-click the **Intellipoint Drivers** package, and then click **Refresh**. Repeat this step until the status shows Success. This should take about one minute.

Lesson 3

Building a Reference Image by Using a Configuration Manager Task Sequence

Contents:

Demonstration: Creating a Build and Capture Task Sequence

Demonstration Steps

Create a build and capture task sequence

1. On LON-CFG1, in the Configuration Manager console, click **Software Library**, expand **Operating Systems**, and then click the **Task Sequences** node.
2. On the ribbon, in the **Create** group, click **Create Task Sequence**.
3. In the Create Task Sequence Wizard, on the **Create New Task Sequence** page, click the **Build and capture a reference operating system image** option, and then click **Next**.
4. On the **Task Sequence Information** page, in the **Task sequence name** box, type **Build and Capture Windows 8**, and then click **Browse**.
5. In the **Select a Boot Image** dialog box, click **Boot image (x64) 6.2.9200.16384 en-US**, and then click **OK**.
6. On the **Task Sequence Information** page, click **Next**.
7. On the **Install Windows** page, click **Browse**.
8. In the **Select an Operating System Image** dialog box, click **Windows 8 Enterprise Evaluation en-US**, and then click **OK**.
9. On the **Install Windows** page, click the **Enable the account and specify the local administrator password** option, in the **Password** and **Confirm password** boxes, type **Pa$$w0rd**, and then click **Next**.
10. On the **Configure Network** page, in the **Workgroup** box, type **imaging**, and then click **Next**.
11. On the **Install Configuration Manager** page, click **Next**.
12. On the **Include Updates** page, click **Next**.
13. On the **Install Applications** page, click **Next**.
14. On the **System Preparation** page, click **Next**.
15. On the **Image Properties** page, in the **Created by** box, type *your name*, and then click **Next**.
16. On the **Capture Image** page, in the **Path** box, type **\\LON-CFG1\Labfiles\Images\MyWin8Capture.wim**.
17. In the area next to the **Account** box, click **Set**.
18. In the **Windows User Account** dialog box, in the **User name** box, type **Adatum\Administrator**, in the **Password** box, type **Pa$$w0rd**, in the **Confirm password** box, type **Pa$$w0rd**, and then click **OK**.
19. On the **Capture Image** page, click **Next**.
20. On the **Summary** page, click **Next**.
21. On the **Completion** page, click **Close**.

Demonstration: Deploying a Build and Capture Task Sequence

Demonstration Steps

1. Right-click **Build and Capture Windows 8**, and then click **Deploy**.
2. In the Deploy Software Wizard, on the **General** page, next to **Collection**, click **Browse**.

3. In the **Select Collection** dialog box, click **All Unknown Computers**, and then click **OK**.
4. On the **General** page, click **Next**.
5. On the **Deployment Settings** page, click the **Purpose** list, and then select **Available**.
6. In the **Make available to the following** drop-down list, select **Configuration Manager clients, media and PXE**, and then click **Next**.
7. On the **Scheduling** page, click **Next**.
8. On the **User Experience** page, click **Next**.
9. On the **Alerts** page, click **Next**.
10. On the **Distribution Points** page, click **Next**.
11. On the **Summary** page, click **Next**.
12. On the **Completion** page, click **Close**.

Lesson 4

Deploying Client Images by Using MDT Task Sequences

Contents:

Demonstration: Configuring and Deploying an MDT Task Sequence

Demonstration Steps

1. On LON-CFG1, in the Configuration Manager console, click **Software Library**, expand **Operating Systems**, and then click the **Task Sequences** node.
2. Right-click the **Task Sequences** node, and then click **Create MDT Task Sequence**.
3. In the Create MDT Task Sequence Wizard, on the **Choose Template** page, select **Client Task Sequence** from the drop-down list, and then click **Next**.
4. On the **General** page, in the **Task sequence name** box, type **Upgrade to Windows 8**, and then click **Next**.
5. On the **Details** page, select the **Join a domain** option, in the **Domain** field, type **Adatum.com**, and then click **Set**.
6. In the **Windows User Account** dialog box, in the **User name** field, type **Adatum\Administrator**, in the **Password** and **Confirm password** fields, type **Pa$$w0rd**, and then click **OK**.
7. On the **Details** page, in the **Windows Settings** section, in the **User name** field, type *your name*, in the **Organization name** field, type **Adatum**, and then click **Next**.
8. On the **Capture Settings** page, click **Next**.
9. On the **Boot Image** page, for **Specify an existing boot image package**, click **Browse**.
10. In the **Select a Package** dialog box, click **Boot image (x64) 6.2.9200.16384 en-US**, and then click **OK**.
11. On the **Boot Image** page, click **Next**.
12. On the **MDT Package** page, select the **Create a new Microsoft Deployment Toolkit Files package** option, in the **Package source folder to be created (UNCPath)** field, type **\\LON-CFG1\Labfiles\MDTPackage**, and then click **Next**.
13. On the **MDT Details** page, in the **Name** field, type **MDTPackage**, and then click **Next**.
14. On the **OS Image** page, for the **Specify an existing OS image** option, click **Browse**.
15. In the **Select a Package** dialog box, click **Windows 8 Enterprise Evaluation en-US**, and then click **OK**.
16. On the **OS Image** page, click **Next**.
17. On the **Deployment Method** page, click **Next**.
18. On the **Client Package** page, for the **Specify an existing client package** option, click **Browse**.
19. In the **Select a Package** dialog box, click **Microsoft Corporation Configuration Manager Client Package**, and then click **OK**.
20. On the **Client Package** page, click **Next**.
21. On the **USMT Package** page, for the **Specify an existing USMT package** option, click **Browse**.
22. In the **Select a Package** dialog box, click **Microsoft Corporation Configuration User State Migration Tool for Windows 8**, and then click **OK**.
23. On the **USMT Package** page, click **Next**.
24. On the **Settings Package** page, select the **Create a new settings package** option, in the **Package source folder to be created (UNCPath)** field, type **\\LON-CFG1\Labfiles\SettingsPackage**, and then click **Next**.

25. On the **Settings Details** page, in the **Name** field, type **SettingsPackage**, and then click **Next**.
26. On the **Sysprep Package** page, click **Next**.
27. On the **Summary** page, click **Next**.
28. On the **Confirmation** page, click **Finish**.

Module Review and Takeaways

Real-world Issues and Scenarios

Application Installation Issues

Blocked Executables

Problem: Installation source files downloaded from the Internet or that aren't in the Trusted\intranet site list can be marked with one or more NTFS file system data streams. The existence of NTFS file system data streams might cause an Open File – Security Warning prompt to display. The installation will not proceed until you click **Run** at the prompt.

Possible Solution 1: Right-click the installation source file, and then click **Properties**. Click **Unblock**, and then click **OK** to remove the NTFS file system data streams from the file. Repeat this process for each installation source file that was downloaded from the Internet.

Possible Solution 2: Use the Streams utility to remove the NTFS file system data streams from the installation source file. The Streams utility can remove NTFS file system data streams from multiple files or folders at the same time.

Possible Solution 3: Ensure all distribution points are in trusted or intranet sites.

Lost Network Connections

Problem: If a deployment installs device drivers or alters network configurations, the deployment could fail if network connectivity is interrupted.

Possible Solution: Run the ZTICacheUtil.vbs script to enable download and execution for the installation. This script is designed to modify the deployment to enable download and execution.

Task Sequence Issues

The Task Sequence Does Not Finish Successfully

Problem: The task sequence may not finish successfully or may have unpredictable behavior.

Possible Solution: If the Apply Operating System Image task sequence step for User Driven Installation and ZTI has been modified after the creation of the task sequence step, it is possible the change has caused the issue. When preparing to deploy a different operating system image, we recommend that you create a new task sequence.

Tools

Tool	Use to	Where to find it
Streams 1.56	Fix issues with blocked executables	http://go.microsoft.com/fwlink/?LinkId=286559

Lab Review Questions and Answers

Lab A: Preparing the Environment for Operating System Deployment

Question and Answers

Lab Review

Question: If you want to include the Windows Vista migration requirements in the plan, what additional steps would be required?

Answer: You would need to distribute the User State Migration Tool package.

Question: What additional components might you add to the MDT boot image?

Answer: Answer will vary but could include, scripting support, creating a folder with support tools such as CMTrace log viewer and importing those tools.

Lab B: Performing a ZTI by Using MDT and Configuration Manager

Question and Answers

Question: How would you do a bare-metal deployment as a ZTI deployment?

Answer: Answers will vary but could include:

- Allow PXE to respond only to known computers.
- Define the computers in Configuration Manager.
- Add the computers to a collection.
- Create an appropriate MDT task sequence.
- Deploy it to the collection containing the computers to be imaged as required.
- Turn on the computers.

Question: Why would you use the Install Application task step instead of capturing an image with all the applications already installed?

Answer: Answers will vary but could include:

- All applications might not be deployed to all computers.
- Adding applications into the captured image could necessitate having several operating system images for deployment. Additionally, besides keeping the operating system in the captured image updated, you also would need to be able to apply updates to the applications.
- An application that will not work after the sysprep /generalize process
- Licensing considerations for applications

Module 8

Planning and Implementing a Remote Desktop Services Infrastructure

Contents:

Lesson 1

Overview of Remote Desktop Services

Contents:

Resources

Overview of the Remote Desktop Client Experience

Reference Links: For complete details on hardware requirements for RemoteFX, see http://go.microsoft.com/fwlink/?LinkId=286560

Lesson 2

Planning the Remote Desktop Services Environment

Contents:

Resources

Implementing the RD Connection Broker

 **Reference Links:** For detailed instructions, see http://go.microsoft.com/fwlink/?LinkId=286561

Lesson 4

Configuring a Session-Based Desktop Deployment

Contents:

Demonstration: Creating a Session-Based Desktop Deployment

Demonstration Steps

1. On LON-SVR2, in Server Manager, click **Add roles and features**.
2. In the Add Roles and Features Wizard, click **Next**.
3. Click **Remote Desktop Services installation**, and then click **Next**.
4. Click **Standard Deployment**, and then click **Next**.
5. Click **Session-based desktop deployment**, and then click **Next**.
6. On the **Review role services** page, click **Next**.
7. On the **Specify RD Connection Broker server** page, click the arrow to select **LON-SVR2**, and then click **Next**.
8. On the **Specify RD Web Access server** page, click the arrow to select **LON-SVR2**, and then click **Next**.
9. On the **Specify RD Session Host servers** page, click the arrow to select **LON-SVR2**, and then click **Next**.
10. On the **Confirm selections** page, select the **Restart the destination server automatically if required** check box, and then click **Deploy**.
11. After the server restarts, sign in as **Adatum\Administrator** with the password **Pa$$w0rd**. Close the Add Roles and Features Wizard after completion.
12. Leave the virtual machines running for the next demonstration.

Demonstration: Creating and Configuring a Session Collection

Demonstration Steps

Create a session collection

1. On LON-SVR2, in the left pane in Server Manager, click **Remote Desktop Services**.
2. In the Remote Desktop Services details pane, click **Create session collections**.
3. In the Create Collection Wizard, click **Next**.
4. On the **Name the collection** page, in the **Name** field, type **Adatum Apps**, and then click **Next**.
5. On the **Specify RD Session Host servers** page, click the arrow to select **LON-SVR2**, and then click **Next**.
6. On the **Specify user groups** page, click **Next**.
7. On the **Specify user profile disks** page, clear the check box next to **Enable user profile disks**, and then click **Next**.
8. Click **Create**, and then close the wizard when complete.

View the properties of a session collection

1. In Server Manager, click the **Adatum Apps** collection.
2. In the middle pane, in the **Properties** section, click the **Tasks** drop-down arrow, and then click **Edit Properties**.
3. In the Adatum Properties window, click each of the session collection property pages and briefly describe the settings.

Demonstration: Configuring RemoteApp Publishing

Demonstration Steps

Publish RemoteApp programs

1. On LON-SVR2, in Server Manager, in **Remote Desktop Services**, click **Adatum Apps**.
2. In the RemoteApp Programs section, click the link to **Publish RemoteApp programs**.
3. In the Select RemoteApp programs window, select the check boxes for **WordPad**, **Paint**, and **Calculator**, and then click **Next**.
4. Click **Publish**, and then click **Close**.

Configure RemoteApp programs

1. Right-click **WordPad**, and then click **Edit Properties**.
2. In the Properties window, click **File Type Associations**.
3. Select the check box for .**docx**, and then click **OK**.
4. Right-click **Paint**, and then click **Edit Properties**.
5. Click **User Assignment**, click **Only specified users and groups**, and then click **Add**.
6. In the Select Users and Groups window, type **Domain Admins**, and then click **OK** twice.
7. Right-click **Calculator**, and then click **Edit Properties**.
8. In the General window, under Show the RemoteApp program in RD Web Access, click **No**, and then click **OK**.
9. Keep the virtual machines running for the next demonstration.

Lesson 5

Extending the Remote Desktop Services Environment to the Internet

Contents:

Demonstration: Configuring Deployment Properties for Using an RD Gateway Server

Demonstration Steps

Add an RD Gateway server

1. On LON-SVR2, click **Overview** in the Remote Desktop Services section.
2. In the Deployment Overview diagram, click the **RD Gateway** icon (the circled green plus sign).
3. On the **Add RD Gateway Servers** page, click the arrow to select **LON-SVR2.Adatum.com**, and then click **Next**.
4. On the **Name the self-signed SSL certificate** page, type **LON-SVR2.Adatum.com**, and then click **Next**.
5. On the **Confirm selections** page, click **Add**, and then click **Close**.

Configure deployment properties

1. In the Deployment Overview section, click the **Tasks** drop-down arrow, and then click **Edit deployment properties**. Ensure that the **RD Gateway** section is selected. Point out that the RD Gateway can be configured to be detected automatically or specified by name. Point out that the Bypass RD Gateway server for local addresses is **ON** by default. Point out that you can specify not to use an RD Gateway server.
2. Click **Certificates** in the left pane.
3. In the details pane, click **RD Gateway**, and then click **Create new certificate**.
4. In the Create New Certificate window, in the **Certificate name** field, type **LON-SVR2.adatum.com**. This is the common name that will appear on the certificate and must be the fully qualified domain name (FQDN) of the RD Gateway server.
5. In the **Password** field, type **Pa$$w0rd**.
6. Select the **Store this certificate** check box.
7. Click **Browse**, and then navigate to the **Desktop**.
8. In the **File name** field, type **RD Certificate**, and then click **Save**.
9. Select the **Allow the certificate to be added to the Trusted Root Certifications Authorities certificate store on the destination computers** check box, and then click **OK**. Note that the **State** field of the RD Gateway has changed to **Ready to apply**, but the **Level** field is **Not Configured** and the **Status** field is blank.
10. Select the **RD Gateway**, and then click **Apply**. In a few moments, the **Level** field now reads **Untrusted**, indicating a self-signed certificate, and the **Status** field is **OK**. Click **OK**.

Module Review and Takeaways

Best Practice

Implement the following best practices:

- Purchase public SSL certificates to support your SSL infrastructure.
- Whenever possible, choose applications that have been tested and certified by the vendor to run on a Windows Server 2012 deployment of Remote Desktop Services.
- Place your RD Session Host and RD Virtualization Host servers where they can be accessed readily by the clients who will be using them primarily.

Review Question(s)

Question: You discover that the RDS CALs that were purchased do not match the mode you configured for the RD Session Host. How can you change the mode on the RD Licensing server?

Answer: You must perform the following steps to edit the registry:

1. Stop the RD Licensing role service.
2. Use the Registry Editor to change the value of the LicensingMode key in HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control \Terminal Server\RCM \LicensingCore to either 2 or 4, whichever is appropriate.

Real-world Issues and Scenarios

The most common issue that prevents users from connecting to Remote Desktop Services deals with certificate naming. The common name on the certificate must match the FQDN of the RD Gateway and RD Web Access servers. If you use different servers for these roles, then both server names must be on the certificate, or you will need multiple certificates. Subject alternative name certificates can be purchased that allow multiple server names to be attached to a single certificate.

Common Issues and Troubleshooting Tips

Common Issue	Troubleshooting Tip
Users are unable to connect to the RD Gateway	Check that the name on the certificate matches the name of the RD Gateway server. During the SSL handshake process, the clients might drop connections because the CA is untrusted, or because the RD Gateway server was unable to produce a valid certificate. In either case, the user will be unable to launch a remote connection using the RD Gateway.

Lab Review Questions and Answers

Lab: Planning and Implementing a Remote Desktop Services Infrastructure

Question and Answers

Lab Review

Question: What ports need to be open on your external firewall to facilitate communications to the RD Web Access server?

Answer: Only port 443 needs to be open on the external firewall for SSL communications.

Question: How can you ensure that both managed and unmanaged computers, such as public computers, can connect to your RD Web Access server from the Internet?

Answer: Purchase a public SSL certificate. You are unable to distribute certificates to unmanaged computers.

Module 9

Managing User State Virtualization for Enterprise Desktops

Contents:

Lesson 1

Overview of User State Virtualization

Contents:

Question and Answers

Discussion: Challenges of User Profiles

Question: What are some of the major challenges of user profiles?

Answer: Answers will vary, depending on the experiences students have had.

Question: What happens when you upgrade a computer to a new Windows operating system?

Answer: Certain settings may no longer be available. For example, desktop settings such as wallpapers and icons may change. Start menu items no longer exist in Windows 8.

Question: What historic changes has the folder structure gone through?

Answer: Between Windows XP and Windows Vista®, the entire account location hierarchy changed from Documents and Settings, to Users. The My Documents structure changed as well. Subfolders such as My Pictures, My Videos, and My Music are now peer folders rather than subordinate folders. The AppData settings folder also was restructured extensively.

Question: If multiple profiles exist on a machine for the same user, can they be merged? If so, how would they be merged?

Answer: Use the User State Migration Tool (USMT) to migrate user data and settings. You can translate local profiles as a separate step from the user account migration process. Also, if you only need to merge data from one user's profile into another, you could sign in to the computer via a domain administrator account, and in the C:\Users folder, copy the files from one into the other.

Question: If users sign in locally and through their domain accounts, does this affect their profile data and settings?

Answer: Yes, they will have two separate profiles.

Lesson 2

Planning User State Virtualization

Contents:

Resources

 **Additional Reading:** For more information on the *Infrastructure Planning and Design* guide for User State Virtualization, go to http://go.microsoft.com/fwlink/?LinkId=286564

 **Additional Reading:** For more information on the *Infrastructure Planning and Design* guide for User State Virtualization, go to http://go.microsoft.com/fwlink/?LinkId=286564

Lesson 3

Configuring Roaming Profiles, Folder Redirection, and Offline Files

Contents:

Demonstration: Configuring Folder Redirection

Demonstration Steps

Create a network share

1. On LON-SVR1, on the taskbar, click the **File Explorer** button.
2. In the console tree, expand **Computer**, and then click **Local Disk (C:)**.
3. On the ribbon, click the **Home** tab.
4. In the New section, click **New Folder**, and name the new folder **UserData**.
5. In the details pane, right-click **UserData**, click **Share with**, and then click **Specific people**.
6. In the File Sharing pop-up window, under Type a name and then click add, type **Authenticated Users**, and then click the **Add** button.
7. Under the Permission Level column of Authenticated Users, click the drop-down arrow, click **Read/Write**, and then click the **Share** button. Click **Done**. Leave File Explorer open.

Create a group policy and apply it

1. On LON-DC1, in Server Manager, go to the **Tools** drop-down menu, and then select **Group Policy Management**.
2. In the console tree, expand **Forest: Adatum.com**, **Domains**, **Adatum.com**.
3. Right-click **Adatum.com**, and then click **Create a GPO in this domain, and Link it here**.
4. In the New GPO pop-up window, in the **Name** box, type **DocsRedirect**, and then click **OK**.

Redirect documents to a network share

1. In the console tree, under the **Adatum.com** node, right-click the **DocsRedirect** node, and then click **Edit**.
2. In the Group Policy Management Editor, in the console tree, expand **User Configuration**, expand **Policies**, expand **Windows Settings**, and then expand **Folder Redirection**.
3. Right-click **Documents**, and then click **Properties**.

 **Note:** Spend a few moments showing the various settings. In the **Target** tab, explain the differences between the **Basic** and **Advanced** settings. In larger enterprises, the **Advanced** setting enables administrators to load-balance user profiles over a large number of servers, usually by department or some other hierarchy.
In the **Settings** tab (be sure to explain that the **Target** tab has a specific setting named **Setting**, but that there is also a tab named **Settings**), explain the different choices, and what is set for defaults.
Inform the students that if they delete the policy that contained the Folder Redirection setting, then the machines will keep the setting as it has been set in the registry. Explain to students that they need to change the **Target** setting to **Not Configured**, and on the **Settings** tab, change the **Policy Removal** option to redirect the folder back to the local userprofile location. The registry setting for Folder Redirection is at:
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders. The default location will be %USERPROFILE%*foldername*, but if the folder remains redirected, it should say *servername**sharename**username**foldername*.

4. In the **Target** tab, under **Setting**, click **Basic-Redirect everyone's folder to the same location**. Under **Target** folder location, ensure that the **Create a folder for each user under the root path** drop-down is selected. In the **Root Path** box, type **\\LON-SVR1\UserData**, and then click **OK**.

Apply Group Policy to a domain

1. When a warning displays about the policy not applying to older versions of Windows operating systems displays, explain that the **Settings** tab has a check box labeled **Also apply redirection policies to…** that would prohibit getting this warning, but it may generate another warning specifying certain folders still would not be redirected, depending on the folder selected. Click **Yes**.
2. Close the Group Policy Management Editor. At this point, the Group Policy is applied to all the users in the domain.
3. Close Group Policy Management.

Test by signing in as a user, saving a document, and then signing out

1. Sign in to LON-CL1 as **Adatum\Hani** with the password **Pa$$w0rd**.
2. On the **Start** page, type **Command Prompt**, and then press Enter.
3. In the Command Prompt window, type the following command and then press Enter.

```
gpupdate.exe /Target:user /Force
```

4. The command will reply that the user must be signed out to apply, and presents you with an option to type either Yes (Y), or No (N). Type **Y**, and then press Enter.
5. After Hani is signed out, sign in again to LON-CL1 as **Adatum\Hani** with a password of **Pa$$w0rd**.
6. On the **Start** screen, type **Word**, and then click the **Microsoft Word 2010** icon. Click **OK** at the User Name box. On the Welcome screen, click **Don't make changes**, and then click **OK**.
7. Create a new document and type some text in it. Save it as **document1.docx** in the Documents folder.
8. Close Microsoft Word 2010, and then sign out of LON-CL1.
9. Switch back to LON-SVR1.
10. If not already open, open File Explorer, and browse to **C:\UserData**.
11. Right-click **UserData**, and then click **Properties**. On the **Security** tab, examine the discretionary access control list (DACL). Note that Authenticated Users have Full Control. After you have reviewed the options, click **Cancel**.
12. Expand **UserData**, expand **Hani**, click and then right-click **Documents**, and then click **Properties**.
13. Click the **Security** tab. Examine the DACL. You should see a message in the **Properties** dialog box stating that **You must have Read permissions to view the properties of this object. Click Advanced to continue.** Click **Advanced**.

 **Note:** Here, too, you do not have permissions to read. If necessary, an administrator could take ownership of this folder and change the permissions. However, by default, even the administrator is prohibited from seeing the user's documents.

14. Close all open windows.

Review new primary computers for Folder Redirection functionality

1. On LON-DC1, in Server Manager, click **Tools**, and then in the drop-down menu, click **Active Directory Administrative Center**.
2. In the console tree, click **Adatum (local)**, use the Navigate arrow, and then click the **Computers** container.
3. Right-click **LON-CL1**, and then click **Properties**.
4. In the console tree, click **Extensions**.
5. Click the **Attribute Editor** tab, scroll to and select **distinguishedName**, click **View**, and then right-click the value listed. Click **Copy**, click **OK**, and then click **Cancel**.
6. Navigate to the **Research** OU, right-click **Hani Loza**, and then click **Properties**.
7. In the navigation pane, click **Extensions**.
8. Click the **Attribute Editor** tab, click **msDs-PrimaryComputer**, and then click **Edit**.
9. In the **Multi-valued String Editor** dialog box, right-click in the text box, and then click **Paste**. Click **Add**, click **OK**, and then click **OK** again.
10. Close the Active Directory Administrative Center.

Enable primary computer support for Folder Redirection

1. In Server Manager, click **Tools**, and then in the drop-down list, click **Group Policy Management**.
2. In the Group Policy Management Console (GPMC), browse to **Adatum.com**, right-click the **DocsRedirect** Group Policy Object (GPO) that you created during the initial configuration of Folder Redirection, and then click **Edit**.
3. To enable primary computers support by using computer-based Group Policy, navigate to **Computer Configuration**. Alternatively, for user-based Group Policy, navigate to **User Configuration**.
   - Computer-based Group Policy applies primary computer support to all computers to which the GPO applies, affecting all users of the computers.
   - User-based Group Policy applies primary computer support to all user accounts to which the GPO applies, affecting all computers to which the users sign in.
4. Under User Configuration, navigate to **Policies**, expand **Administrative Templates**, expand **System**, and then click **Folder Redirection**.
5. Right-click **Redirect folders on primary computers only**, and then click **Edit**.
6. Click **Enabled**, and then click **OK**.
7. Review the other various settings with the class. Leave the DocsRedirect policy open.

Configure Group Policy to enable primary computer support for Roaming User Profiles

1. While still in the DocsRedirect Group Policy, Navigate to **Computer Configuration**, expand **Policies**, expand **Administrative Templates**, expand **System**, and then click **User Profiles**.
2. Right-click **Download roaming profiles on primary computers only**, and then click **Edit**.
3. Click **Enabled**, and then click **OK**.
4. Go over the other settings in User Profiles with the class.
5. Close the Group Policy Management Editor. At this point, the Group Policy is applied to all the users in the domain.

6. Close Group Policy Management.

Demonstration: Configuring and Managing Offline Files Settings

Demonstration Steps

Configure Offline Files

1. On LON-SVR1, on the taskbar, click the **File Explorer** button.
2. In the console tree, expand **Computer**, and then click **Local Disk (C:)**.
3. On the ribbon, click the **Home** tab.
4. In the New section, click **New Folder**, and name the new folder **CorpData**.
5. In the details pane, right-click **CorpData**, click **Share with**, and then click **Specific people**.
6. In the File Sharing pop-up window, under **Type a name and then click add**, type **Authenticated Users**, and then click **Add**.
7. Under the Permission Level column of Authenticated Users, click the drop-down arrow, and then click **Read/Write**. Click the **Share** button, and then click **Done**.
8. Right-click the **CorpData** folder, and then click **Properties**.
9. On the **Sharing** tab, click the **Advanced Sharing** button.
10. In the **Advanced Sharing** dialog box, click **Caching**.
11. In the **Offline Settings** dialog box, click the **All files and programs that users open from the shared folder are automatically available offline** option, and then ensure that the **Optimize for performance** check box is selected. Click **OK**.

 **Note:** Spend a few minutes describing the various options that display here. Explain that the **Optimize for performance** check box means that even executable files in the shared folder are cached offline.

12. In the **Advanced Sharing** dialog box, click **OK**.
13. Close all open windows.

Enable the Always Offline mode

1. If not already signed in, sign in to LON-DC1 as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. In Server Manager, click **Tools**, and in the drop-down menu, click **Group Policy Management**.
3. In the GPMC, in the console tree, expand **Forest: Adatum.com**, expand **Domains**, and then expand **Adatum.com**.
4. Right-click **Adatum.com**, and then click **Create a GPO in this domain, and Link it here**.
5. In the **New GPO** pop-up window, in the **Name** box, type **OfflineFilesPol**, and then click **OK**.
6. In the console tree, right-click **OfflineFilesPol**, and then click **Edit**. The Group Policy Management Editor displays.
7. In the console tree, under **Computer Configuration**, expand **Policies**, expand **Administrative Templates**, expand **Network**, and then click **Offline Files**.

8. Right-click **Configure slow-link mode**, and then click **Edit**. The Configure slow-link mode window displays. Click **Enabled**.
9. In the **Options** box, click **Show**. The Show Contents window displays.
10. In the **Value name** box, type **\\LON-SVR1\CorpData**. To enable Always Offline mode on all file shares, type *****.
11. In the **Value** box, type **1** to set the latency threshold to 1 millisecond (ms), and then click **OK** twice.

Enable background file synchronization on costed networks

1. In the Group Policy Management Editor, right-click **Enable file synchronization on costed networks**, and then click **Edit**. The Enable file synchronization on costed networks window displays.
2. Click **Enabled**, and then click **OK**.
3. Close all open windows.

Lesson 4

Implementing UE-V

Contents:

Resources

Creating Custom UE-V Settings Location Templates

Additional Reading: For more information or to download templates from the UE-V template gallery, go to http://go.microsoft.com/fwlink/?LinkId=286565

Demonstration: Managing the UE-V Agent with Group Policy

Demonstration Steps

Deploy the UE-V .admx template files and enable UE-V

1. On LON-DC1, open File Explorer, and then browse to **E:\Labfiles\UEV**.
2. Right-click the **.admx** file, and then copy it to **C:\Windows\PolicyDefinitions**.
3. Copy the **.adml** file to **C:\Windows\PolicyDefinitions\en-us**. Close the File Explorer window.

Note: On a local computer, copy the file to the C:\Windows\PolicyDefinitions directory. You can also copy to the Sysvol\PolicyDefinitions folder on the domain controller or in the ADMX central store. The .admx file must be placed in the PolicyDefinitions folder. The .adml file must be placed in the PolicyDefinitions\en-us folder.

4. In Server Manager, click **Tools**, and then in the drop-down menu, click **Group Policy Management**.
5. In the GPMC, in the console tree, expand **Forest: Adatum.com**, expand **Domains**, and then expand **Adatum.com**.
6. Right-click **Adatum.com**, and then click **Create a GPO in this domain, and Link it here**.
7. In the **New GPO** pop-up window, in the **Name** box, type **UEVPol**, and then click **OK**.
8. In the console tree, right-click **UEVPol**, and then click **Edit**. The Group Policy Management Editor displays.
9. In the Group Policy Management Editor, expand **Computer configuration**, expand **Policies**, expand **Administrative Templates**, expand **Windows Components**, and then click **Microsoft User Experience Virtualization**.
10. Double-click **Use User Experience Virtualization (UE-V)**. In the pop-up window, select the **Enabled** option, and then click **OK**. Explain the other settings here to the class, especially the Storage Settings, but do not set any. Leave the Group Policy Management Editor window open.

Deploy the UE-V agent with Group Policy

1. On LON-DC1, open File Explorer, and then browse to **E:\Labfiles\UEV**.
2. Return to the Group Policy Management Editor.
3. Navigate to **Computer Configuration\Policies\Software Settings**.
4. Right-click **Software Installation**, and then click **Properties**.
5. In the **Software installation Properties** pop-up window, in the **Default package location**, type **\\LON-DC1\labfiles\UEV**, and then click **OK**.
6. Right-click **Software Installation** again, click **New**, and then click **Package**.

7. In the Open window, navigate to **RC Release\X64**, click **AgentSetupx64**, click **Open**, click **Assigned**, and then click **OK**. After a time, the Microsoft User Experience Virtualization Agent will display in the details pane.
8. Close all open windows.

Module Review and Takeaways

Real-world Issues and Scenarios

When offering offline folders to users in your organization, always deploy the Enable file synchronization on costed networks option. As more users enhance their mobility and functionality with handheld and tablet devices, they run the risk of inadvertently running up unnecessary charges on 3G and 4G mobile network connections. The Enable file synchronization on costed networks option means that these users will not be synchronized until they resume using a wireless network, which for most Offline Files users is sufficient.

Tools

AD DS Users and Computers

AD DS Administrative Center; Attribute editor

GPOs in AD DS

UE-V agent and infrastructure.

Lab Review Questions and Answers

Lab: Managing User State Virtualization for Enterprise Desktops

Question and Answers

Lab Review

Question: What is the key difference between data saved in a roaming profile versus data saved in a redirected personal folder?

Answer: In roaming profiles, the data is saved on the network shared folder, and it also is copied to the local computer. Redirected folders keep the data on the network share only, until or unless the redirection is turned off or altered.

Question: In which scenario, or scenarios, should you use primary computers?

Answer: You should use primary computers in the Folder Redirection scenario. Primary computers is a new feature in Windows Server 2012 that lets you specify which computers a particular user has, and which of those computers will have access to the user's redirected folders. This is especially useful for users who might have a tablet and a laptop in addition to their desktop. All three devices would get the same access to data saved on any of them.

Module 10

Planning and Implementing an Updates Infrastructure to Support Enterprise Desktops

Contents:

Lesson 1

Planning an Updates Infrastructure for the Enterprise

Contents:

Resources

Overview of Update Classifications

Additional Reading: Point out that a good resource for information related to security updates is the Microsoft Security Response Center (MSRC), which is located at http://go.microsoft.com/fwlink/?LinkId=286566

Lesson 2

Supporting Software Updates with System Center 2012 Configuration Manager

Contents:

Demonstration: Installing the Software Update Point and Configuring Client Settings

Demonstration Steps

Configure site system prerequisites

1. On LON-SVR2, from Server Manager, click **Tools**, and then open the Computer Management console.
2. In the navigation pane, expand **System Tools**, expand **Local Users and Groups**, and then click **Groups**.
3. In the details pane, double-click **Administrators**. The **Administrators Properties** dialog box opens.
4. In the **Administrators Properties** dialog box, click **Add**.
5. In the **Select Users, Computers, Service Accounts, or Groups** dialog box, click **Object Types**.
6. In the **Object Types** dialog box, select the **Computers** check box, and then click **OK**.
7. In the **Select Users, Computers, Service Accounts, or Groups** dialog box, type **LON-CFG1**. Click **Check Names**, and then click **OK**.
8. Click **OK** to close the **Administrators Properties** dialog box.
9. Close the Computer Management console.
10. In Server Manager, in the navigation pane, verify that Windows Server Update Services (WSUS) has already been installed along with its prerequisites, such as Internet Information Services (IIS).
11. On LON-DC1, from Server Manager, click **Tools**, and then open the Group Policy Management console.
12. Expand **Forest:Adatum.com**, expand **Domains**, expand **Adatum.com**, and then click **Group Policy Objects**.
13. In the details pane, right-click **Default Domain Policy** and then click **Edit**. The Group Policy Management Editor opens.
14. Browse to Computer Configuration\Policies\Administrative Templates\Windows Components, and then click **Windows Update**.
15. In the details pane, double-click **Specify intranet Microsoft update service location**. Verify that **Not Configured** is selected, and then click **OK**. Point out that this setting should be modified if an existing WSUS implementation is in place.
16. Close the Group Policy Management Editor and the Group Policy Management console.

Add a new site system with the software update role

1. On LON-CFG1, open the System Center 2012 Configuration Manager console.
2. Click the **Administration** workspace, expand **Site Configuration**, and then click **Servers and Site System Roles**.
3. Right-click **Servers and Site System Roles**, and then click **Create Site System Server**.
4. In the Create Site System Server Wizard, on the **General** page, describe the options, configure the following settings, and then click **Next**:
   - Name: **LON-SVR2.Adatum.com**
   - Site code: **S01 – Adatum Site**
5. On the **Proxy** page, click **Next**.

6. On the **System Role Selection** page, select the **Software update point** check box, and then click **Next**.
7. On the **Software Update Point** page, configure the following settings, and then click **Next**:
   - WSUS is configured to use ports 8530 and 8531 for client communications (default settings for WSUS on Windows Server 2012): **Selected**
   - Client Connection Type: **Allow intranet-only client connections**
8. On the **Proxy and Account Settings** page, click **Next**.
9. On the **Synchronization Source** page, select the **Do not synchronize from Microsoft Update or upstream data source** option, and then click **Next**.
10. On the **Synchronization Schedule** page, configure the following settings, and then click **Next**:
    - Enable synchronization on a schedule: **Selected**
    - Simple schedule: **Selected**
    - Run every: **3 days**
    - Alert when synchronization fails on any site in the hierarchy: **Not selected**
11. On the **Supersedence Rules** page, select the **Immediately expire a superseded software update** option. Discuss the other options, and then click **Next**.
12. On the **Classifications** page, select the following software update classifications (clearing all other default selections), and then click **Next**:
    - **Critical Updates**
    - **Definition Updates**
    - **Security Updates**
13. On the **Products** page, select the following products (clearing all other default selections), and then click **Next**:
    - **Windows 7**
14. On the **Languages** page, ensure that only **English** is selected. Clear any other enabled languages, and then click **Next**.
15. On the **Summary** page, click **Next**.
16. On the **Completion** page, click **Close**.

Monitor site system component installation status

1. Click the **Monitoring** workspace, expand **System Status**, and then click **Component Status**.
2. In the results pane, scroll down, and then click **SMS_WSUS_CONTROL_MANAGER**.
3. Right-click **SMS_WSUS_CONTROL_MANAGER**, point to **Show Messages**, and then click **All**.
4. In the **Status Messages: Set Viewing Period** dialog box, click **OK**.
5. In the Configuration Manager Status Message Viewer, discuss the messages related to the component installation on LON-SVR2.
6. Close the Configuration Manager Status Message Viewer.

Configure the software update point component

1. Click the **Administration** workspace, expand **Site Configuration**, and then click **Sites**.

2. In the results pane, right-click **S01 – Adatum Site**, point to **Configure Site Components**, and then click **Software Update Point**.
3. In the **Software Update Point Component Properties** dialog box, click each tab, and then point out that this is how one would modify the initial software update point installation settings. Click **OK**.

Synchronize the software update point

1. Click the **Software Library** workspace, expand **Software Updates**, and then click **All Software Updates**.
2. Right-click **All Software Updates**, and then click **Synchronize Software Updates**.
3. In the **Configuration Manager** message box, click **Yes** to initiate a site-wide synchronization of software updates.
4. Click the **Monitoring** workspace, and then click **Software Update Point Synchronization Status**. Point out the information in the preview pane.
5. Click the **Administration** workspace, expand **Site Configuration**, and then click **Sites**.
6. In the results pane, right-click **S01 – Adatum Site**, point to **Configure Site Components**, and then click **Software Update Point**.
7. On the **Products** tab, click **Windows 8**.
8. Click **OK** to close the **Software Update Point Component Properties** dialog box.
9. Click the **Software Library** workspace, expand **Software Updates**, and then click **All Software Updates**.
10. Right-click **All Software Updates**, and then click **Synchronize Software Updates**. Click **Yes**. This will now include the Windows 8 updates during the synchronization.
11. Refresh the results pane. In the results pane, verify that updates are now listed.

Note: It may take a few minutes for the updates to appear. You will need to refresh the console a few times to view the results.

Configure the software update client settings

1. Click the **Administration** workspace, and then click **Client Settings**.
2. In the results pane, right-click **Default Client Settings**, and then click **Properties**.
3. In the **Default Settings** dialog box, click **Software Updates**. Verify that Software Updates is enabled, and then discuss other options as needed.
4. Click the **State Messaging** node, modify the value to have a reporting cycle of **5** minutes, and then click **OK** to close the **Default Settings** dialog box.

Run software updates scan on a client

- On LON-CL1, from Control Panel, open **Configuration Manager Properties**, and then initiate the **Machine Policy Retrieval & Evaluation Cycle** action and the **Software Updates Scan Cycle** action.

Create a new collection

1. On LON-CFG1, in the System Center 2012 Configuration Manager console, Click the **Assets and Compliance** workspace, and then click **Devices**.
2. In the results pane, right-click **LON-CL1**, point to **Add Selected Items**, and then click **Add Selected Items to a New Device Collection**.

3. In the **Create Device Collection Wizard** dialog box, type **All Windows 8 Workstations** for the **Name**.
4. Click **Browse**, and then select **All Systems** for the Limiting Collection. Click **Next**.
5. On the **Membership Rules** page, click **Next**.
6. On the **Summary** page, click **Next**, and then click **Close**.

Demonstration: Deploying Software Updates

Demonstration Steps

Create a software update group

1. On LON-CFG1, open the System Center 2012 Configuration Manager console.
2. Click the **Software Library** workspace, expand **Software Updates**, and then click **All Software Updates**.
3. In the results pane, click the **Update for Windows 8 for x64-based Systems (KB2768703)** update.

Note: If you do not see the update listed, right-click **All Software Updates**, and then click **Synchronize Software Updates**. It should appear once the console refreshes.

4. On the ribbon, select the **Home** tab, and then click **Create Software Update Group**.
5. In the **Create Software Update Group** dialog box, configure the following, and then click **Create**:
   - Name: **Critical Updates – Windows 8**
   - Description: **Critical Updates for Windows 8 Clients**
6. In the **Software Library** workspace, under **Software Updates**, click **Software Update Groups**. The Critical Updates – Windows 8 software update group is visible in the results pane.
7. Select **Critical Updates – Windows 8**, and then on the ribbon, click **Show Members**. Verify that the update that you added is displayed.
8. Under **Software Updates**, click **Software Update Groups**.
9. In the ribbon, click **Run Summarization**. In the **Configuration Manager** message box, click **OK**. Refresh the results pane. The preview pane displays the compliance statistics for the Critical Updates – Windows 8 software update group. Refresh the results pane as required.

Note: It may take time for the results to display. If results do not display, run the software update scan on the client, and then refresh the console. You can continue with the demonstration even with the results not showing.

Create a deployment package

1. In the navigation pane, expand **Software Updates**, and then click **Software Update Groups**.
2. In the list pane, right-click **Critical Updates – Windows 8**, and then click **Download**.
3. In the Download Software Updates Wizard, on the **Deployment Package** page, verify that **Create a new deployment package** is selected. Configure the following information, and then click **Next**:
   - Name: **Critical Updates – Win8**
   - Package source: **\\LON-CFG1\E$\labfiles\Updates**

4. On the **Distribution Points** page, click **Add**, and then click **Distribution Point**.
5. In the **Add Distribution Points** dialog box, select the **\\LON-CFG1.Adatum.com** check box, and then click **OK**.
6. In the Download Software Updates Wizard, click **Next**.
7. On the **Distribution Settings** page, click **Next**.
8. On the **Download Location** page, click **Download software updates from a location on my network**.
9. In the text box, type **\\LON-CFG1\E$\labfiles\Updates**, and then click **Next**.
10. On the **Language Selection** page, verify that only **English** is selected, and then click **Next**.
11. On the **Summary** page, click **Next**.
12. On the **Completion** page, verify that the package and software updates show success, which is indicated by a green circle with a white check mark. Click **Close**.
13. In the navigation pane, under **Software Updates**, click **Deployment Packages**.
14. In the preview pane, verify that the Distribution Point Status shows Success.

Deploy software updates

1. Click the **Software Library** workspace, expand **Software Updates**, and then click **Software Update Groups**.
2. In the results pane, click **Critical Updates – Windows 8**.
3. On the ribbon, click **Deploy**.
4. In the Deploy Software Updates Wizard, on the **General** page, configure the following settings, and then click **Next**:
   - Deployment Name: **Critical Updates – Win8**
   - Collection: **All Windows 8 Workstations**
5. On the **Deployment Settings** page, next to **Type of deployment**, click **Required**, and then click **Next**.
6. On the **Scheduling** page, click **Next**.
7. On the **User Experience** page, verify the following setting, and then click **Next**:
   - User notifications: **Display in Software Center and show all notifications**
8. On the **Alerts** page, select the **Generate an alert when the following conditions are met** check box, and then click **Next**.
9. On the **Download Settings** page, click **Next**.
10. On the **Summary** page, verify that the settings are correct, and then click **Save As Template**.
11. In the **Save As Template** dialog box, in the **Name** box, type **Critical Updates – Windows 8**, and then click **Save**.
12. On the **Summary** page, click **Next**.
13. On the **Completion** page, click **Close**.

Run software updates deployment on a client

1. Switch to LON-CL1, open the **Control Panel**, and then click **System and Security**.

2. Click **Configuration Manager**.
3. In the **Configuration Manager Properties** dialog box, click the **Actions** tab.
4. On the **Actions** tab, click **Machine Policy Retrieval & Evaluation Cycle**, and then click **Run Now**.
5. In the **Machine Policy Retrieval & Evaluation Cycle** message box, click **OK**.
6. On the **Actions** tab, click **Software Updates Deployment Evaluation Cycle**, and then click **Run Now**.
7. In the **Software Updates Deployment Evaluation Cycle** message box, click **OK**.
8. Click **OK** to close the **Configuration Manager Properties** dialog box, and then close the Control Panel. Within a few minutes, a prompt appears in the notification area.
9. On LON-CL1, switch to the **Start** screen, and then click **Software Center**.
10. In **Software Center**, on the **Installation Status** tab, take note of the installation status and details for the software updates.
11. Click **Update for Windows 8 for x64-based Systems (KB2768703)**, and then click **INSTALL**.
12. Close the Software Center.
13. In **System and Security**, click **Configuration Manager**.
14. In the **Configuration Manager Properties** dialog box, click the **Actions** tab.
15. On the **Actions** tab, click **Machine Policy Retrieval & Evaluation Cycle**, and then click **Run Now**.
16. In the **Machine Policy Retrieval & Evaluation Cycle** message box, click **OK**.
17. On the **Actions** tab, click **Software Updates Deployment Evaluation Cycle**, and then click **Run Now**.
18. In the **Software Updates Deployment Evaluation Cycle** message box, click **OK**.
19. Click **OK** to close the Configuration Manager Properties.

View software updates deployment status

1. On LON-CFG1, click the **Monitoring** workspace, and then click **Deployments**.
2. In the results pane, click **Critical Updates – Windows 8**, on the ribbon, click **Run Summarization**, and then click **OK**. Refresh the console. Describe the information in the preview pane. It may take several minutes for details to appear. You also may need to refresh the console.
3. In the results pane, right-click **Critical Updates – Windows 8**, and then click **View Status**. View the information displayed on the **Deployment Status** page.

Lesson 3

Managing Updates for Virtual Machines and Images

Contents:

Resources

Managing Software Updates for Virtual Machines

Additional Reading: Virtual Machine Servicing Tool 2012 is a free solution accelerator that you can download from http://go.microsoft.com/fwlink/?LinkId=286568

Updating VHDs Stored in the VMM Library

Additional Reading: You might want to point out that if the shared folder method is used, you can download updates from the Microsoft Update Catalog manually, which is accessible from http://go.microsoft.com/fwlink/?LinkId=286569

Infrastructure and Server Preparation to Support Virtual Machine Servicing Tool 2012

Additional Reading: Point out that the PsExec.exe tool can be downloaded from http://go.microsoft.com/fwlink/?LinkId=286570

Module Review and Takeaways

Best Practice

Consider the following best practices when you manage software updates in your environment:

- To help you determine which software updates are relevant for your organization, subscribe to the appropriate software update notification service.
- Maintain a consistent client hardware baseline for your organization.
- Deploy software updates in phased groups, so that you can minimize potential update issues.
- Educate users on the behavior of software update installations and restarts.

Review Question(s)

Question: When you are planning an update management process, what are some points that you may want to consider?

Answer: You will want to consider a number of points, such as which products and classifications you need to update, which types of computers need to be managed, how you will determine update requirements, and what your deployment requirements are.

Question: What is the purpose of the software update point in Configuration Manager?

Answer: The software update point role interacts with WSUS and provides software updates synchronization, assessment, and deployment to Configuration Manager clients.

Question: What are some of the important considerations related to the virtual machines that are managed by Virtual Machine Servicing Tool 2012?

Answer: Considerations include:

- All virtual machines must belong to the Active Directory® Domain Services (AD DS) domain.
- Determine and configure relevant firewall exceptions.
- Depending on the update management solution, the appropriate client must be installed on the virtual machine.

Question: Describe how the features of Windows Intune may benefit your organization.

Answer: Answers will vary. However, one possible answer includes the ability to manage computer devices that have Internet connections but rarely connect to the organization's network.

Lab Review Questions and Answers

Lab: Planning and Implementing an Updates Infrastructure to Support Enterprise Desktops

Question and Answers

Lab Review

Question: You need to add the Service Packs classification to be synchronized for software updates. Where can you make this modification?

Answer: You can make this modification on the Software Update Point Component Properties dialog box.

Question: In the lab, you had to run a summarization to view software update status. What can you do to minimize the manual summarization task?

Answer: You can modify the software update summarization schedule. By default, it runs once an hour. However, if summarization is set too low, it can cause performance issues.

Question: What are some of the advantages of using a software update group?

Answer: A software update group is an efficient way to organize, monitor, and deploy software updates. A number of the reports also are based on software update group settings.

Module 11

Protecting Enterprise Desktops from Malware and Data Loss

Contents:

Lesson 1

Overview of System Center 2012 Endpoint Protection

Contents:

Resources

Planning Sources for Definition Updates

Additional Reading: To download the latest definition files, visit the Malware Protection Center at http://go.microsoft.com/fwlink/?LinkId=286571
For more information, visit the MMPC at http://go.microsoft.com/fwlink/?LinkId=286478

Demonstration: Configuring System Center 2012 Endpoint Protection Server Settings and Antimalware Policies

Demonstration Steps

Configure System Center 2012 Endpoint Protection server settings

1. On LON-CFG1, on the taskbar, click the **Configuration Manager Console** option.
2. In the Configuration Manager console, click the **Administration** workspace.
3. In the navigation pane, expand **Site Configuration**, and then click **Servers and Site System Roles**.
4. In the results pane, right-click **LON-CFG1.adatum.com**, click **Add Site System Roles**, and then click **Next**.
5. In the **Specify internet proxy server** page, click **Next**.
6. Select the **Endpoint Protection Point** check box. In the Configuration Manager pop-up window informing you that Endpoint Protection uses software updates by default, click **OK**, and then click **Next**.
7. On the **Endpoint Protection** page, ensure that the **I accept the Endpoint Protection license terms** check box is selected, and then click **Next**.
8. On the **Microsoft Active Protection Service** page, click the **Basic membership** option, and then click **Next**.
9. On the **Confirm the settings** page, review the settings, ensuring that they are what you selected, and then click **Next**.
10. The Endpoint Protection point site system role should now install. You should get a success message on the **Completion** page. Click **Close**.

Create and deploy an antimalware policy

1. In the Configuration Manager console, click the **Assets and Compliance** workspace.
2. In the navigation pane, expand **Endpoint Protection**, and then click **Antimalware Policies**. In the results pane, double-click the **Default Antimalware Policy**, discuss a few of the settings you talked about in the previous slide, and then click **Cancel**.
3. On the ribbon, click the **Create Antimalware Policy** button.
4. On the **Endpoint Protection Antimalware Policy** page, in the **Name** box, type **Demo Client Policy**.
5. In the **Description** box, type **To demonstrate an antimalware policy for Endpoint Protection**.

Note: Describe what the policy is for and what it will do. Try to be succinct but descriptive. When you have numerous policies, the description helps you to identify the correct policy quickly.

6. Select the check boxes for all of the options in the **Options** box. As you do so, note how the options then are listed under **General** in the navigation pane to the left.
7. In the navigation pane, click **Scheduled scans**, which is the first item. Show the various settings but do not make any changes. Go through each of these options in the navigation pane, showing all of the settings that can be configured. When finished, click **OK**.

Note: Before you can deploy a policy, you must have a collection for it. You will not create a collection for this demonstration, but rather, you will use one of the default collections. Discuss with students the various available options and why they would create a new collection.

8. In the results pane, click the **Demo Client Policy** item you just made.
9. On the ribbon, in the **Deployment** section, click **Deploy**.
10. On the **Select Collection** page, click the **All Desktop and Server Clients** collection, and then click **OK**.
11. Note that the Demo Client Policy item in the results pane now shows a number 1 in the Deployments column.
12. Close all open windows, and then sign out of LON-CFG1.

Lesson 2

Configuring System Center 2012 Endpoint Protection Client Settings and Monitoring Status

Contents:

Resources

Client Settings for System Center 2012 Endpoint Protection

 **Additional Reading:** For more information about changes, go to http://go.microsoft.com/fwlink/?LinkId=286470

Demonstration: Configuring Client Settings for System Center 2012 Endpoint Protection

Demonstration Steps

Create a device collection for the two Windows 8 computers

1. On LON-CFG1, on the taskbar, click the **Configuration Manager Console** button.
2. Click the **Assets and Compliance** workspace.
3. In the navigation pane, click **Device Collections**. On the ribbon, click **Create Device Collection**.
4. In the Create Device Collection Wizard, on the **General** page, in the **Name** box, type **Windows 8 Devices**, and then in the **Description** box, type **London Windows 8 Operating Systems**.
5. In the **Limiting collection** section, click **Browse**. Click **All Systems**, and then click **OK**. Click **Next**.
6. On the **Membership Rules** page, click **Add Rule**, and then in the drop-down box, click **Direct Rule**.
7. In the Create Direct Membership Rule Wizard, on the **Welcome** page, click **Next**.
8. On the **Search for Resources** page, in the **Resource class** drop-down box, click **System Resource**. In the **Attribute name** drop-down box, click **Name**. In the **Value** box, type **Lon-CL%**, and then click **Next**.
9. On the **Select resources** page, select the **LON-CL1** and **LON-CL2** check boxes. Do not select **LON-CL3**, and then click **Next**.
10. On the **Summary** page, click **Next**.
11. When the direct membership rule is created successfully, click **Close**.
12. On the **Membership Rules** page, click **Next**.
13. On the **Summary** page, click **Next**.
14. When the Create Device Collection Wizard successfully completes, click **Close**.
15. Right-click the **Windows 8 Devices** collection that you just created, click **Update Membership**, and then in the pop-up window, click **Yes**. You should now have both computers in the collection.

Create a custom client settings policy for Endpoint Protection

1. Click the **Administration** workspace.
2. In the navigation pane, click **Client Settings**, and then on the ribbon, click **Create Custom Client Device Settings**.
3. In the Create Custom Client Device Settings Wizard, on the **Custom Device Settings** page, in the **Name** box, type **Windows 8 EP**, and in the **Description** box, type **Endpoint Protection settings for Windows 8 computers**.
4. On the **Custom Device Settings** page, select the **Endpoint Protection** check box.

5. Click **Endpoint Protection** in the navigation pane. This will bring up the **Device Settings** pane. Go over each setting with the students, but make no changes. Click **OK**.
6. With the **Windows 8 EP policy** selected in the results pane, go to the ribbon, and then click **Deploy** in the Client Settings section.
7. On the **Select Collection** page, click **Windows 8 Devices**, and then click **OK**.
8. The settings should now deploy to the Windows 8 clients, LON-CL1, and LON-CL2, at the next client policy retrieval cycle.

Lesson 4

Protecting Desktops by Using DPM

Contents:

Demonstration: Configuring Protection Groups for Client Computers

Demonstration Steps

Configure protection groups for client computers

1. Sign in to LON-DM1 as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. Open Server Manager, and then click **Tools**. In the drop-down list, click **Computer Management**.
3. In Computer Management, in the console tree, expand **Storage**, and then click **Disk Management**.
4. In the **Initialize Disk** pop-up window, click **OK**. Close the Computer Management window.
5. Click to the **Start** screen, and then click the **Microsoft System Center 2012 Data Protection Manager** tile.
6. Click the **Management** workspace below the console tree, and then in the console tree, click the **Disks** hyperlink.
7. On the ribbon above, click **Add**. In the Add Disks to Storage Pool window, click **Disk 1**, and then click the **Add** button. Click **OK**.
8. A pop-up message will inform you that you need to convert basic disks to dynamic. Click **Yes** to continue.

Note: The disk will now be in the DPM Storage Pool.

Add a client computer by using the Create New Protection Group Wizard

1. Click the **Protection** workspace below the console tree, and then on the ribbon above, click **New** in the **Protection Group** section.
2. On the **Welcome to the New Protection Group Wizard** page, click **Next**.
3. On the **Select Protection Group Type** page, click the **Clients** option, and then click **Next**.
4. On the **Select Group Members** page, click **LON-CL1** and **LON-CL2** while holding down the Ctrl key. Click **Add** to move the computers to the **Selected computers** list box, and then click **Next**.
5. On the **Specify Inclusions and Exclusions** page, to specify the folders to include, click the drop-down list, and then select **User Profiles**. In the **Rule** drop-down box, click **Include**.
6. Click the **Add Rows** button for each folder added, and then repeat step 5 for the **Program Files** and **My Documents** folders, selecting **Include** for both. Click **Next**.
7. On the **Select Data Protection Method** page, in the **Protection Group Name** box, type **Client 1 and 2 Demo**, and then click **Next** to continue.
8. On the **Specify Short-Term Goals** page, accept the defaults, and then click **Next**.
9. On the **Allocate Storage** page, note the default size specification of data to be protected is 5 gigabytes (GB), along with the space available on DPM. Change the **Data per computer** value to **3 GB**. Ensure that the **Co-locate client computers in DPM Storage Pool** and the **Automatically grow the volumes** check boxes are selected, and then click **Next**.
10. On the **Summary** page, review your selections, and then click **Create Group** to complete the wizard.
11. After successful completion of the Protection Group, review the **Status** page, and then click **Close**.
12. Close all windows, and then sign out of LON-DM1.

Module Review and Takeaways

Review Question(s)

Question: When using DPM, why should you stagger the delivery schedule for reports sent by email?

Answer:

The SQL Server Reporting Services (SSRS) memory thresholds might prevent some reports from actually being sent.

Real-world Issues and Scenarios

Keep in mind that you need to monitor disk consumption actively during your initial efforts at protecting client computers. Local storage expended by users can vary widely. For example, many users still use .pst files, though they consume a large amount of space and are being deprecated. You may wish to exclude .pst files from active protection.

Tools

Configuration Manager Administrator console

DPM administrator console

Lab Review Questions and Answers

Lab A: Implementing Client Endpoint Protection

Question and Answers

Lab Review

Question: When you created the London Windows 8 Devices collection, what was the purpose of the % sign in the direct membership rule?

Answer: The % sign is a wildcard. This means it will find one character at the end from all values containing LON-CL.

Question: Why does the initial Quick Scan of LON-CL1 take so long?

Answer: The first time it runs, it actually runs a Full Scan. This is to provide the antimalware application with a full list of values to compare later.

Lab B: Configuring Data Protection for Client Computer Data

Question and Answers

Question: What was the purpose of adding an additional drive at the beginning of Exercise 1?

Answer: A storage pool cannot be created until there is a sufficient number of storage devices present. A protection group cannot be created until there is a storage pool to assign to it.

Question: Why was no data returned in the Status report?

Answer: The Status report will only contain data after 24 hours.

Module 12

Monitoring the Performance and Health of the Desktop Infrastructure

Contents:

Lesson 1

Performance and Health Monitoring of the Desktop Infrastructure

Contents:

Demonstration: Configuring Auditing and Event Viewer Subscriptions

Demonstration Steps

Configure advanced auditing

1. On LON-CL1, click the **Start** screen, and then type **Admin**.
2. In the Search bar, click **Settings**, and then click **Administrative Tools**.
3. In the Administrative Tools window, double-click **Local Security Policy**.
4. In Local Security Policy, expand **Advanced Audit Policy Configuration**, and then expand **System Audit Policies – Local Group Policy Object**.
5. Click **Account Logon** and review the subcategories with the students.
6. Double-click **Audit Credential Validation**, and then click the **Explain** tab.
7. Read the content on the **Explain** tab.
8. In the Audit Credential Validation Properties window, click **Cancel**.
9. Click **Account Management** and review the subcategories with the students.
10. Click **Logon/Logoff** and review the subcategories with the students.
11. Double-click **Audit Logon**, and then click the **Explain** tab.
12. Click the **Policy** tab, and then select the **Configure the following audit events** check box.
13. Select the **Success** and **Failure** check boxes, and then click **OK**.
14. Click **Object Access** and review the subcategories with the students. Notice that this is where you would enable auditing of the file system or registry.
15. Close the Local Security Policy window.

Configure the source for an event subscription

1. In the Administrative Tools window, double-click **Computer Management**.
2. In the Computer Management window, expand **Local Users and Groups**, and then click **Groups**.
3. Double-click **Event Log Readers**.
4. In the Event Log Readers Properties window, click **Add**.
5. In the Select Users, Computers, Service Accounts, or Groups window, click **Object Types**, select the **Computers** check box, and then click **OK**.
6. Type **LON-CL2**, and then click **OK**.
7. In the Event Log Readers Properties window, click **Add**.
8. In the Select Users, Computers, Service Accounts, or Groups window, click **Locations**, click **LON-CL1**, and then click **OK**.
9. Type **Network Service**, and then click **OK**.
10. In the Event Log Readers Properties window, click **OK**.
11. Close the Computer Management window.
12. In the Administrative Tools window, double-click **Local Security Policy**.
13. In the Local Security Policy window, expand **Local Policies**, and then click **User Rights Assignment**.
14. In the list of policies, scroll down and double-click **Manage auditing and security log**.

15. In the Manage auditing and security log Properties window, click **Add User or Group**.
16. In the Select Users, Computers, Service Accounts or Groups window, click **Object Types**, select the **Computers** check box, and then click **OK**.
17. Type **LON-CL2**, and then click **OK**.
18. In the Manage auditing and security log Properties window, click **Add User or Group**.
19. In the Service Accounts or Groups window, click **Locations**, click **LON-CL1**, and then click **OK**.
20. Type **Network Service**, and then click **OK**.
21. In the Manage auditing and security log Properties window, click **OK**.
22. Close the Local Security Policy and the Administrative Tools windows.
23. On the **Start** screen, type **command**, and then click **Command Prompt**.
24. At the command prompt, type **winrm quickconfig**, and then press Enter.
25. Press **y**, and then press Enter to start the Windows Remote Management (WinRM) service and set the startup type to delayed auto start.
26. Press **y**, and then press Enter to create a WinRM listener and enable a firewall exception.
27. Close the Command Prompt window.
28. Restart LON-CL1 and then sign in as **Adatum\Administrator** with the password of **Pa$$w0rd**.

Configure an event subscription

1. On LON-CL2, click the **Start** screen, type **Event**, click **Settings**, and then click **View event logs**.
2. In Event Viewer, click **Subscriptions**.
3. In the pop-up window, click **Yes** to enable the Event Collector Service.
4. In the Actions pane, click **Create Subscription**.
5. In the **Subscription name** box, type **Security Events**.
6. In the **Destination log** box, select **Forwarded Events**.
7. Click **Collector initiated**, and then click **Select Computers**.
8. In the Computers window, click **Add Domain Computers**.
9. In the Select Computer window, type **LON-CL1**, and then click **OK**.
10. In the Computers window, click **Test**.
11. In the pop-up box that shows the test succeeded, click **OK**.
12. In the Computers window, click **OK**.
13. In the Subscription Properties window, click **Select Events**.
14. In the Query Filter window, In the **Event logs** box, click **Windows Logs\Security**, and then click **OK**.
15. In the Subscription Properties window, click **Advanced**.
16. In the Advanced Subscription Settings window, verify that the user account is **Machine Account**, and then click **OK**.
17. In the Subscription Properties window, click **OK**.

Verify functionality of an event subscription

1. In Event Viewer, click **Subscriptions**.

2. Review the status of the Security Events subscription. Notice that it has a green check mark.
3. Right-click **Security Events**, and then click **Runtime Status**.
4. In the Subscription Runtime Status – Security Events window, read the status for LON-CL1.Adatum.com. Notice that there is a green check mark and that the status is Active, and then click **Close**.
5. In the Event Viewer windows, expand **Windows Logs**, and then click **Forwarded Events**. There may be no events listed here because it can take up to 15 minutes for new security events to be collected.

Lesson 2

Monitoring VDI

Contents:

Demonstration: Monitoring Servers by Using Operations Manager

Demonstration Steps

Review the Operations Console

1. On LON-OM1, on the taskbar, click **Operations Console**.
2. In the Operations Console, click the **Monitoring** workspace. The Monitoring workspace is used to view the health of monitored infrastructure and to resolve alerts.
3. In the navigation pane, click **Active Alerts**. This node shows active alerts that you should troubleshoot and resolve.
4. In the navigation pane, click **Discovered Inventory**. This item shows the computers that are being monitored. Notice that only one computer is monitored at this time.
5. Click the **Authoring** workspace. The Authoring workspace is used to create custom management packs for your own applications.
6. Click the **Reporting** workspace. The Reporting workspace is used to generate and view reports that are included in management packs.
7. Click the **Administration** workspace. The Administration workspace is used to perform administrative tasks such as Operations Manager agent installation, security configuration, and notification configuration.
8. Click the **My Workspace** workspace. This workspace allows users to have a customized workspace where they can create their own views to see specific information.

Import management packs

1. On LON-OM1, on the taskbar, click **File Explorer**.
2. In File Explorer, browse to **\\LON-DC1\e$\Labfiles\ManagementPacks**, and then double-click **System Center Monitoring Pack-Windows Server Operating Systems.msi**.
3. On the **License Agreement** page, click **I accept**, and then click **Next**.
4. On the **Select Installation Folder** page, click **Next**.
5. On the **Confirm Installation** page, click **Install**.
6. On the **Installation Complete** page, click **Close**.
7. Close all open File Explorer windows.
8. In the **Operations console**, click the **Administration** workspace.
9. On the **Administration Overview** page, click **Required: Import management packs**.
10. In the Import Management Packs window, click **Add**, and then click **Add from disk**.
11. In the Online Catalog Connection window, click **No**.
12. In the Select Management Packs to Import window, browse to **C**:**Program Files (x86)\System Center Management Packs\System Center Monitoring Pack-Windows Server Operating System** folder, select all available management packs, and then click **Open**.
13. In the Import Management Packs window, note that management packs with a green checkmark are ready to install. Management packs with a blue information icon are already installed.
14. Select all management packs except **Windows Server 2012 Operating System (Discovery)** and **Windows Server 2012 Operating System (Monitoring),** and then click **Remove**.
15. Click **Install**. When the management pack imports are complete, click **Close**.

Install the Operations Manager agent on LON-SVR1

1. On LON-OM1, in the **Operations console**, in the **Administration** workspace, on the **Administration Overview** page, click **Required: Configure computers and devices to manage**.
2. In the Computer and Device Management Wizard, on the **What Would You Like to Manage** page, click **Windows computers**, and then click **Next**.
3. On the **Auto or Advanced** page, click **Advanced discovery**.
4. In the **Computer and Device Classes** box, select **Servers Only**, and then click **Next**.
5. On the **Discovery Method** page, click **Browse for, or type-in computer names**, and then click **Browse**.
6. In the Select Computers window, type **LON-SVR1**, and then click **OK**.
7. On the **Discovery Method** page, click **Next**.
8. On the **Administrator Account** page, click **Use selected Management Server Action Account**, and then click **Discover**.
9. On the **Select Objects to Manage** page, click **Select All**, and then click **Next**.
10. On the **Summary** page, click **Finish** to use the default agent installation directory and Local System as the Agent Action Account.
11. In the Agent Management Task Status window, click **Close**.

View the health of LON-SVR1

1. On LON-OM1, in the **Operations console**, click the **Monitoring** workspace.
2. In the navigation pane, click **Discovered Inventory**. This pane lists the computers that are being monitored. In a few minutes, LON-SVR1 will be listed here.

Module Review and Takeaways

Review Question(s)

Question: Your organization has decided that you should do a random sampling of reliability data on computers running Windows 8. This information will be used to determine if there are any systemic issues that have not been reported by users. A colleague suggests using Reliability Monitor to connect remotely to the selected remote systems and then to copy the data that is visibly displayed into a spreadsheet. What do you suggest?

Answer: It is not possible to use Reliability Monitor to connect to remote systems. However, you can write a script that uses the Win32_ReliabilityStabilityMetrics and Win32_ReliabilityRecords Windows Management Instrumentation (WMI) objects. These WMI objects provide the information that Reliability Monitor uses to display reliability.

You can collect and use this information by using many different scripting and programming languages, including Windows PowerShell® command-line interface.

Question: You have gathered baseline performance data from several computers running Windows 8. As you analyze the data, you notice that each computer has spikes in processor utilization where the %Processor Time counter reaches 100 percent. Does this indicate a need for faster processors in those computers?

Answer: No, it does not indicate a need for faster processors unless the %Processor Time counter has a sustained value of 100 percent for an extended period of time. Short periods of 100 percent processor time are normal as applications perform specific tasks or even when applications are started.

Question: Your organization has implemented a new VDI infrastructure with Remote Desktop Virtualization Host (RD Virtualization Host) role services. The RD Virtualization Hosts have advanced graphics cards with a high level of memory. How can you identify whether the hardware is sufficient for RemoteFX?

Answer: You can use the RemoteFX performance counters to identify whether there are frames being skipped or timeout detection and recovery incidents being generated. If these are occurring, you need to investigate to determine whether there is sufficient graphics processing capacity in the RD Virtualization Host.

Tools

You can use the following tools to monitor the performance and health of desktop infrastructure:

- Performance Monitor
- Advanced auditing
- Event subscriptions
- Reliability Monitor
- Operations Manager

Lab Review Questions and Answers

Lab: Monitoring the Performance and Health of the Desktop Infrastructure

Question and Answers

Lab Review

Question: Why is it necessary to configure WinRM for event log subscriptions?

Answer: Event Viewer gathers events from the remote computer by using WinRM. Therefore, you need to configure the WinRM listener, ensure that the WinRM service is started, and that WinRM communication is allowed through Windows Firewall.

Question: Is a computer available for monitoring immediately after installing the Operations Manager agent?

Answer: No. After installing the agent, the agent contacts the management server to download configuration information. The computer appears dimmed in monitoring views until the configuration is complete.