Microsoft®

OFFICIAL MICROSOFT LEARNING PRODUCT

# 6294A

# Planning and Managing Windows® 7 Desktop Deployments and Environments

*Companion Content*

Product Number: 6294A

Released: 12/2009

# 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**:

© 2008 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

## Preparing to Deploy Windows® 7 Business Desktops

### Contents:

# Lesson 1

## Overview of the Desktop Lifecycle

### Contents:

# Question and Answers

## Overview of the Client Lifecycle

**Question:** Provide a brief description of the activities in the Client Lifecycle's Management Phase.

**Answer:** Updates include facilities, software upgrade, and hardware transfer to a new user. Support includes training, IT support, and hardware servicing. The Microsoft Support Lifecycle policy applies to most products currently available through retail purchase or volume licensing, and most future release products.

## Overview of the Hardware Lifecycle

**Question:** What are the main reasons for upgrading or replacing hardware?

**Answer:** Hardware becomes outdated over time and upgrading the operating system or applications can require new hardware. One benefit of Windows 7 is that it has the same hardware requirements as Windows Vista®.

## Overview of the Desktop Deployment Lifecycle

**Question:** What are some of the benefits of having a pilot plan during the planning phase?

**Answer:** A pilot plan allows the IT Department to test a specific system configuration or application setup before deploying it to the entire enterprise. It is a risk mitigation tool.

## Lesson 2

# Desktop Deployment: Challenges and Considerations

### Contents:

# Question and Answers

## Guidelines for an Effective Business Desktop Deployment

**Question:** What is the purpose for creating a hardware and software baseline?

**Answer:** Implementing standard baselines allows you to more easily manage computing resources and roll out new software and hardware to users. This requires the adoption of a standard minimum hardware and software configuration for deployment.

## What Is the Infrastructure Optimization Model?

**Question:** What is the reason for adopting an optimization-level transition project?

**Answer:** Optimization-level transition projects exist to assist an organization in moving from a basic to a standardized level of optimization for the desktop, device, and server management capability within the Core Infrastructure Optimization model.

## Considering the Cost Savings of Automation

**Question:** What are the financial benefits of changing the optimization level?

**Answer:** Changing the optimization level results in reduced IT costs.

## Lesson 3

# Tools and Technologies Used in the Desktop Deployment Lifecycle

### Contents:

# Question and Answers

## Tools Used to Support the Planning Phase

**Question:** What is the purpose of the System Configuration Manager 2007?

**Answer:** Microsoft System Center Configuration Manager 2007 provides a comprehensive solution for change and configuration management for the Microsoft platform.

## Tools Used to Support the Deploying Phase

**Question:** You have decided to use the Windows AIK to deploy Windows 7. What do you use to create the images for the magazine development group?

**Answer:** ImageX is a tool used to create system images.

## Tools Used to Support the Deploying Phase

**Question:** You are deploying 500 new computers in the enterprise. What tool do you use to migrate user settings and user state to the new computers?

**Answer:** Use the USMT 4.0 when hardware and operating system upgrades are planned for a large number of computers.

## Lesson 4

# Assessing the Current Computing Environment for Deploying Windows 7

### Contents:

# Question and Answers

## Windows 7 Key Features

**Question:** What key feature of Windows 7 will help your organization to control the applications employees can install on their computers?

**Answer:** AppLocker allows IT professionals to more flexibly set software restriction policies.

## Editions of Windows 7

**Question:** Which edition of Windows 7 must you choose in the following scenarios?

Scenario 1: There are a few users in your organization. Currently, you do not have a centralized file server and all the computers are not joined to a domain.

Scenario 2: Your organization has more than one hundred users who are located in several offices across the country. In addition, you have several users that travel frequently.

**Answer:** Choose Windows 7 Professional for Scenario 1 and Windows 7 Enterprise for Scenario 2.

Scenario 1: For a business environment, choose either Windows 7 Professional or Windows 7 Enterprise. Windows 7 Home Premium, Windows 7 Home Basic, and Windows 7 Starter are targeted for home users. Because you only have a few users, Windows 7 Professional is the best fit.

Scenario 2: Choose Windows 7 Enterprise and take advantage of features such as BranchCache and DirectAccess to increase the productivity of your mobile users.

**Question:** What is the difference between the Enterprise and the Ultimate edition of Windows 7?

**Answer:** There is no difference in terms of features between the Enterprise and Ultimate editions. Windows 7 Enterprise is available through Microsoft Software Assurance with Volume Licensing and Windows 7 Ultimate is available through the retail channel. There is no upgrade path between the two.

## Hardware Requirements for Windows 7

**Question:** What is the typical computer specification within your organization? Contrast that specification to what was available when Windows Vista was released. Do you think Windows 7 can be deployed to the computers within your organization as they currently are?

**Answer:** The answer can vary. Several years ago, when Windows Vista was released, the hardware requirements were considered quite high. Since Windows 7 hardware requirements are the same as Windows Vista, computers in most organizations are able to install Windows 7.

## Assessment Features of the MAP Toolkit

**Question:** You need to create a hardware inventory throughout the enterprise. This can 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 using agent-less collection methods such as WMI, the Remote Registry Service, SNMP, AD DS, and the Computer Browser Service.

## Demonstration: Assessing the Computing Environment by Using the MAP Toolkit

**Question:** If your company is going to slowly migrate to Windows 7 how will you generate assessment reports for each planned deployment?

**Answer:** Depending on how your network is segmented you can Scan IP Subnets or use a specific list of systems.

## Overview of Collecting Inventory by Using Configuration Manager 2007

**Question:** You decide to use Configuration Manager 2007 to collect inventory data in the enterprise. Many of the computers are Windows 2003 Server and you are unable to collect data on those computers. What might be the problem?

**Answer:** Configuration Manager Client is explicitly not supported on the Windows Server 2003 with no service packs operating system version.

## Overview of Collecting Asset Inventory by Using MDOP

**Question:** You are responsible for deploying systems at sites in Germany, Japan, India, and the United States. Why is AIS a good inventory asset tool in this case?

**Answer:** AIS is a hosted solution and therefore is accessible from virtually anywhere.

## Considerations for Assessing the Current Network Infrastructure

**Question:** What is the best option for deployment if you have a large number of customizations at a location?

**Answer:** Work towards a single hardware and software configuration. If this is not possible, deploy the heavy customizations in a separate deployment from the zero customization deployment.

# Detailed Demo Steps

## Demonstration: Assessing the Computing Environment by Using the MAP Toolkit

## Detailed demonstration steps

There are several different scenarios the Microsoft Assessment and Planning Toolkit can help you with.

This demonstration shows how to use the Microsoft Assessment and Planning Toolkit.

### Configuring and running the Microsoft Assessment and Planning Toolkit

1. Log on to the LON-CL2 virtual machine as **Contoso\Administrator** with a password of **Pa$$w0rd**.
2. Click **Start**, point to **All Programs**, click **Microsoft Assessment and Planning Toolkit** and then click **Microsoft Assessment and Planning Toolkit**.
3. After the Microsoft Planning and Assessment Toolkit starts, on the Create or select a database to use dialog box, select the Create an inventory database radio button. Type Demonstration and then click OK.
4. In the Discovery and Readiness pane, click **Inventory and Assessment Wizard**.
5. Review the Computer Discovery Methods page and then click **Next**.
6. Fill in the Active Directory Credentials page with the following:
    - Domain: **Contoso.com**
    - Domain Account: **Contoso\Administrator**
    - Password: **Pa$$w0rd**

   Click **Next**.
7. Review the **Active Directory Options** page and then click **Next**.
8. On the Windows Networking Protocols page ensure the following:

   Workgroups and Windows domains to include in the inventory: **Contoso**

   Click **Next**.
9. On the WMI Credentials page, click **New Account**.
10. Fill in the **Inventory Account** page with the following:
    - Domain: **Contoso.com**
    - Domain Account: **Contoso\Administrator**
    - Password: **Pa$$w0rd**
    - Confirm password: **Pa$$w0rd**

    Click **Save**.
11. On the **WMI Credentials** page, click **Next**.
12. On the **Summary** page, click **Finish**.
13. Once the inventory is complete, on the **Status** page, click **Close**.

### Review the summary results

1. In the Inventory and Assessment pane, expand **Discovery and Readiness**.
2. In the Inventory and Assessment pane, click **Windows 7 Readiness**.
3. Review the **Windows 7 Readiness** Summary Results.
4. In the Inventory and Assessment pane, click **Windows Server 2008 R2 Readiness**.
5. Review the **Windows Server 2008 R2 Readiness** Summary Results.
6. In the Inventory and Assessment pane, click **Windows Vista Readiness**.
7. Review the **Windows Vista Readiness** Summary Results.
8. In the Inventory and Assessment pane, click **Windows Server 2008 Readiness**.
9. Review the **Windows Server 2008 Readiness** Summary Results.
10. In the Inventory and Assessment pane, click **Virtual Machine Discovery**.
11. Review the **Virtual Machine Discovery** Results.
12. In the Inventory and Assessment pane, click **Windows Server Roles Discovery**.
13. Review the **Windows Server Roles Discovery** Results.
14. In the Inventory and Assessment pane, click **Windows 7 Readiness**.
15. In the Actions pane; click **Generate report/proposal**.

# Lesson 5

## Overview of the Desktop Lifecycle

### Contents:

# Question and Answers

## Activation Options

**Question:** What methods of activation have you used at your company?

**Answer:** The answer will vary but will fall within Retail, OEM, and Volume licensing.

## Overview of Volume Activation Models

**Question:** You have already installed multiple instances of the Windows 7 client. Which Volume Licensing method do you use?

**Answer:** MAKs are not used to install Windows 7, but rather to activate it after installation. You can use MAKs to activate any Windows 7 volume edition.

## MAK Model

**Question:** You are deploying the Windows 7 client to 19 computers. Which volume activation method do you use?

**Answer:** The KMS method requires a minimum of 25 hosts, so MAK is the choice by default.

## KMS Model

**Question:** What are the hardware requirements for the KMS host?

**Answer:** KMS runs as a service on Windows Server 2008 or Windows Server 2003. It can be co-hosted with other services and even the largest enterprise requires only two KMS servers. This includes a backup KMS server.

# Module Reviews and Takeaways

## Review questions

1. What happens at a KMS host computer if the activation count is below 25?
2. What does Microsoft offer through the Support Lifecycle Policy for Operating Systems?
3. What is the main difference between the standardized information optimized infrastructure model and the rationalized optimized infrastructure model?
4. How does the Microsoft Assessment and Planning Toolkit assess your organization's readiness for Windows 7?
5. How does Windows XP Mode benefit Windows 7?

## Review answers

1. Clients that do not activate because the activation count is too low connect to the KMS host every two hours, by default, to receive a new count.
2. Ten (10) years of support (five (5) years Mainstream Support and five (5) years Extended Support) at the supported service pack level for Business and Developer products
3. The standardized model uses Lite Touch deployment services whereas the rationalized model uses the Zero Touch deployment services.
4. MAP uses several agent-less methods to connect to computers on the network, assesses their hardware and device compatibility with Windows 7, and then creates comprehensive Microsoft Office Word and Microsoft Office Excel reports.
5. New features in Windows Virtual PC make it easy to use and to help run many older Windows XP applications in Windows 7.

## Real-world issues and scenarios

1. If I am using Windows XP and have not looked at the Windows Vista and Windows Server 2008 imaging and deployment tools over the last few years, what do I need to know about Windows 7 deployment?

   If you have not looked at Windows Vista Deployment Enhancements and imaging, now is a great time to learn about the enhancements made around file-based, non-destructive imaging using the Windows® Imaging Format (WIM), and other advantages, including Hardware Abstraction Layer (HAL) independence and language neutrality in Windows Vista and Windows 7 images.

2. What is Hard-Link Migration, and how can I migrate user states from one operating system to another?

   The User State Migration Tool for Windows 7 now provides a new feature called Hard-Link Migration. This feature allows your customers to install Windows Vista or Windows 7 on an existing computer and retain data locally on that computer during operating system installation. Hard-Link Migration works by:

   - Discovering user files and settings.
   - Creating hard-links to each file in the system that constitutes the user profile, preferences, application settings, and documents.
   - Applying hard-links to the proper file locations in the new operating system.

Although the capability of storing user files locally has been available for some time, the process can take several hours and files are double-instanced on the local hard drive and require free disk space to accommodate them. With hard-links, the files do not move and the index of links can be created and remapped to the new operating system within a few minutes. The hard-link catalog also consumes little space on the hard drive since files are not double-instanced.

Hard-Link Migration can be performed before the operating system installation from within the legacy operating system. In that case, the index of links is stored in a protected folder while the operating system is installed and other folders are deleted as part of the install routine. The migration store protects files from deletion.

This process is how the Microsoft Deployment Toolkit 2010 Beta (http://go.microsoft.com/fwlink/?LinkID=108442) performs a default computer refresh. The second option is to perform a clean install of the operating system and by default the new operating system will create a "windows.old" folder with user files and settings and retain any legacy folders found in the root directory. Offline hard-link migration can be used to target files within "windows.old" and map them to the appropriate locations in the Windows Vista or Windows 7 operating system.

This process takes only a few minutes and the risk for data loss using this solution is minimal. After migration has occurred from "windows.old," the user can use the disk cleanup utility to remove "windows.old," and hard-link migrated files are protected from deletion.

3. Are there any changes in the Windows Deployment Services server role in Windows Server 2008 R2?

   Windows Deployment Services in Windows Server 2008 R2 enables network deployments of WIM images or Virtual Hard Disks (VHD) as files used for operating system deployments. The previous release of Windows Deployment Services (WDS) in Windows Server 2008 included the capability of multicast for image transmission to computers in the deployment pool.

   This can reduce network bandwidth consumption and increase deployment capacity by using a single-image transmission to multiple clients; instead of one 5-GB image passing to 100 clients and consuming 500 GB of network bandwidth. The same deployment using multicast can consume as little as five (5) to ten (10) GB of network bandwidth.

   One consequence of using multicast in Windows Server 2008 is that the slowest client determined the transfer rate for all client machines. In Windows Server 2008 R2, multicast now supports the use of Multiple Stream Transfer of two to three speeds to ensure that the fastest clients can receive deployment images faster. Additionally, using standard multicast (not with Multiple Stream Transfer), you can set minimum transfer thresholds and automatically remove slow clients from the multicast pool.

   Windows Server 2008 R2 with WDS also enables Dynamic Driver Provisioning. With Dynamic Driver Provisioning, driver files can be stored centrally and outside the image and only the required drivers are installed at the time of deployment using Plug and Play device matching. For organizations now including large driver payloads into standard network-installed images, Dynamic Driver Provisioning can help to reduce image size and ease driver management routines.

## Best practices

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

## Standard desktop strategy

This best practice involves deploying a standardized desktop by minimizing hardware and software configurations and implementing a three- to four-year PC lifecycle strategy. It helps organizations move from a basic to a standardized level of optimization for desktop, device, and server management in the Core Infrastructure Optimization model.

## Centrally managed PC settings and configuration

This best practice involves keeping deployed PCs standardized by preventing users from making changes that compromise security, reliability, and the application portfolio. It helps organizations move from a standardized to a rationalized level of optimization for desktop, device, and server management in the Core Infrastructure Optimization model.

## Comprehensive PC security

This best practice involves proactively addressing security with antivirus software, antispyware software, patching, and quarantine. It helps organizations move from a basic to a standardized, and then from a standardized to a rationalized, level of optimization for security and networking in the Core Infrastructure Optimization model.

## Comprehensive directory solution

This best practice requires a single directory for authentication, single sign-on capability for all computing resources, and automated password reset. It helps organizations move from a basic to a standardized level of optimization for identity and access management in the Core Infrastructure Optimization model.

## PCs managed by Group Policy Objects (GPOs)

This best practice requires PCs to authenticate into Active Directory and individual PCs to receive configuration, software installation, and desktop configuration through GPOs. It helps organizations move from a standardized to a rationalized level of optimization for identity and access management in the Core Infrastructure Optimization model.

## Reduction of third-party application directories

This best practice requires the use of a single directory service for both operating system management and application directory services. It helps organizations move from a standardized to a rationalized level of optimization for identity and access management and desktop, device, and server management in the Core Infrastructure Optimization model.

## Automated user provisioning

This best practice requires a single directory, or synchronized directories with a metadirectory service, and IT processes for automated user provisioning. Users are provisioned (including adds, removes, and changes) only once in a primary directory, and the changes are propagated to all related directories. It helps organizations move from a standardized to a rationalized level of optimization for identity and access management in the Core Infrastructure Optimization model.

## Automated packaging tools and software distribution

This best practice involves the use of tools to maintain software inventories, automate software packaging, and automate software distribution. It helps organizations move from a basic to a standardized level of optimization for security and networking in the Core Infrastructure Optimization model.

## Single systems management tool

This best practice involves the use of a single software tool for managing software inventory, hardware inventory, and automated software distribution. It helps organizations move from a basic to a standardized level of IT optimization for security and networking in the Core Infrastructure Optimization model.

## Centrally managed PC applications

This best practice involves keeping deployed PC applications standardized by generating software inventory reports for auditing versus standards and de-installing non-compliant software. It helps organizations move from a standardized to a rationalized level of optimization for security and networking in the Core Infrastructure Optimization model.

## Tools

| Tool | Use for | Where to find it |
|---|---|---|
| Windows System Image Manager (Windows SIM) | • The tool used to open Windows images, create answer files, and manage distribution shares and configuration sets. | http://go.microsoft.com/fwlink/?LinkId=162632 |
| ImageX | • The tool used to capture, create, modify, and apply Windows images. | http://go.microsoft.com/fwlink/?LinkId=162633 |
| Deployment Image Servicing and Management (DISM) | • The tool used to apply updates, drivers, and language packs to a Windows image. DISM is available in all installations of Windows 7 and Windows Server 2008 R2. | http://go.microsoft.com/fwlink/?LinkId=162634 |
| Windows Pre-installation Environment (Windows PE) | • A minimal operating system environment used to deploy Windows. The AIK includes several tools used to build and configure Windows PE environments. | http://go.microsoft.com/fwlink/?LinkId=162635 |
| User State Migration Tool (USMT) | • A tool used to migrate user data from a previous Windows operating system to Windows 7. USMT is installed as part of the AIK in the %PROGRAMFILES%\Windows AIK\Tools\USMT directory. For more information about USMT, refer to the User State Migration Tool User's Guide (%PROGRAMFILES%\Windows AIK\Docs\Usmt.chm) | http://go.microsoft.com/fwlink/?LinkId=140374 |

# Lab Review Questions and Answers

## Lab A: Assessing the Computing Environment by Using the Microsoft Assessment and Planning Toolkit

**Question**: What are the requirements for deploying the Microsoft Assessment and Planning Toolkit?

**Answer**: Windows XP or above, NET Framework v3.5SP1, Windows Installer v4.5, Microsoft Word 2003 SP2 or above (Microsoft Word 2007 recommended), Microsoft Excel 2003 SP2 or above (Microsoft Excel 2007 recommended), Microsoft Office Primary Interop Assemblies, SQL Server 2008 Express Edition (or above) and installation of all updates for the operating system and Microsoft Office.

**Question**: What are the Remote Computer configuration requirements for using the MAP Toolkit?

**Answer**: In order to run the MAP Toolkit wizards, the only required configuration is to configure the Windows Firewall (where appropriate) to enable remote access to WMI. The Remote Registry service is used to find the roles installed on a server. It is also required for running the Gather Performance Metrics Wizard.

**Question**: What discovery methods are available for the MAP Toolkit?

**Answer**: MAP can discover computers in your environment or you can specify which computers to inventory using one of the following methods:

Active Directory® Domain Services (AD DS), Windows networking protocols, Import computer names from a file, Scan an IP address range, or Manually enter computer names.

**Question**: In addition to the Hardware Analysis, what information is available in a Windows 7 proposal generated by the MAP Toolkit?

**Answer**: Software Analysis, including a summary of devices and how to obtain drivers discovered on client computers, current client operating system, and a summary of the most prevalent applications discovered on client computers.

## Lab B: Recommending an Activation Strategy

**Question**: What are some of the key decision points between using a Multiple Activation Key or Key Management System for Volume licensing?

**Answer**: There are several differences including:

A MAK can only activate the Windows editions within its specific product group. A KMS key can activate the Windows editions within its specific product group as well as editions in “lower” product key groups.

KMS requires a minimum number of physical computers in a network environment, called the activation threshold, to activate KMS client machines. The activation threshold for Windows Vista remains at twenty-five (25) physical computers. However the activation threshold for Windows Server 2008 is five (5) physical computers.

**Question**: From the client computer how can an Administrator determine the type of license in use?

**Answer**: Use the SLMGR.vbs script with a –dli or -dlv switch. Amongst the information displayed is last 5 digits of the product key, the License Status and the Description which shows the Windows Product Group, i.e. Retail, MAK, MAK_B, KMS, KMS_C etc.

**Question**: How long are Windows Clients activated for once they contact a KMS server?

**Answer**: KMS clients are activated for 180 days.

**Question**: How many KMS hosts can be activated from a single KMS Key?

**Answer**: Each KMS key can activate 6 KMS hosts up to 10 times each.

**Question**: What tools are available to manage MAK activation and report current activation state?

**Answer**: The Volume Activation Management Tool (VAMT) and the Operations Manager KMS Management Pack.

# Module 2

## Assessing Application Compatibility

### Contents:

# Lesson 1

## Overview of Application Compatibility

### Contents:

# Question and Answers

## Discussion: Which Applications Must Be Tested for Compatibility?

**Question:** Which standard desktop core applications must be tested within your environment?

**Answer:** Answers will vary. However, common core applications can include office productivity suites, such as the 2007 Microsoft® Office system.

**Question:** Which line-of-business applications must be tested within your environment?

**Answer:** Answers will vary. However, common line-of-business applications can include enterprise resource-planning suites, customer relationship management systems, and financial applications. For example, this may include applications such as Microsoft Dynamics® AX, Microsoft Dynamics® NAV, Microsoft Dynamics® GP, Microsoft Dynamics® SL, and Microsoft Dynamics® CRM.

**Question:** Which types of administrative tools or desktop utilities must be tested within your environment?

**Answer:** Types of administrative tools or desktop utilities to test include antivirus applications, compression utilities, personal backup applications, virtual private network clients, and remote-control applications. You must also test services and applications that use service accounts and special permissions to enable operation.

**Question:** Which custom tools must be tested within your environment?

**Answer:** Types of custom tools to test include logon scripts, original equipment manufacturer (OEM) utilities, power management tools, and hardware-specific drivers.

**Question:** Can you name any other applications that must be tested?

**Answer:** Answers will vary. Low-level applications, such as kernel-mode drivers and filter drivers, are especially likely to pose problems. An organization must also ensure that its server applications are compatible with client computers running Windows 7.

## Guidelines for Testing Commercial Applications

**Question:** Why is it recommended that you install an application while logged on as a standard user and again as an administrator?

**Answer:** To identify how User Access Control (UAC) affects the installation options.

## What Are Common Application Compatibility Problems?

**Question:** How can you mitigate the application compatibility issues related to User Account Control?

**Answer:** Applications needing to run as administrators can use RunAsAdmin or RunAsHighestAvailable.

## What Are Common Mitigation Methods?

**Question:** You have an application that fails to run in Windows 7. What mitigation process can be considered if all the other recommended processes are tried on the application and none of them worked?

**Answer:** Consider running the application in a virtualized environment that uses the earlier Windows version that successfully ran the application.

# Lesson 2

## Assessing and Resolving Application Compatibility Issues by Using ACT 5.5

### Contents:

# Question and Answers

## What Is the Application Compatibility Toolkit?

**Question:** How does the Application Compatibility Toolkit reduce the cost and time involved in resolving application compatibility issues?

**Answer:** By analyzing, rationalizing, and prioritizing application compatibility efforts, which assist in deploying Windows 7 more quickly and efficiently.

## Features of ACT 5.5

**Question:** What is the benefit provided by running the ACM tool?

**Answer:** The ACM tool collects and inventories compatibility information from network clients. The tool also analyzes and reports on application compatibility status within each client.

**Question:** What is the benefit provided by running the SUA tool?

**Answer:** The SUA tool monitors and determines issues related to running an application as a standard user in Windows 7.

## ACT 5.5 Architecture Overview

**Question:** What is the purpose of the Application Compatibility Manager (ACM)?

**Answer:** The purpose of the ACM is to configure, collect, and analyze data used so you can fix any issues before deploying a new operating system or deploying a Windows® update in your organization.

## Compatibility Evaluators for Windows 7

**Question:** What information does the Update Compatibility Evaluator collect?

**Answer:** The UCE collects information about the modules loaded, the files opened, and the registry entries accessed by the applications currently running on the computers.

## How Application Compatibility Manager Helps in Collecting and Analyzing Application Data

**Question:** After configuring your data collection package, you can save and distribute it to your network clients. What are some methods you can use to distribute the DCP to your clients?

**Answer:** Possible methods include: from a network share or from removable media such as a CD or portable USB drive. Enterprise environments can also use Active Directory Group Policy to deploy the DCP.

## Using the Standard User Analyzer

**Question:** The Standard User Analyzer Wizard provides a step-by-step process to locate and mitigate UAC issues. However, the wizard provides limited functionality when compared to the Standard User Analyzer Tool. What is this limitation?

**Answer:** The Standard User Analyzer Wizard does not include advanced analysis features that are available with the Standard User Analyzer Tool.

# Module Reviews and Takeaways

## Review questions

1. You have just installed ACT and configured the initial settings. What final task must be completed to ensure that inventory collection occurs?

   Answer: You must open the Services console to ensure that the Log Processing Service has started.

2. What are some examples of common application categories or considerations to use when organizing your application inventory?

   Answer: Answers can vary. However, consider the following:

   - Determine if there are applications specific to particular departments or geographies.
   - Analyze the hardware platforms that are used in the environment, and determine whether there are there dependencies.
   - Determine whether any applications require special hardware devices or peripherals.
   - Calculate the the percentage of ISV applications versus custom line-of-business applications.

3. How can assigning application priorities help in your subsequent application compatibility analysis tasks?

   Answer: Assigning priorities helps to determine which applications are tested first due to business criticality. Priorities can also be assigned to computers (for example, computers that handle payroll) to designate which computers are considered high priority to ensure application compatibility mitigations are in place.

4. What are some examples of applications that might be rationalized out of the priority application list?

   Answer: Examples of applications that might be candidates for rationalizing out of the priority application list include:

   - Applications most likely to be replaced automatically during a deployment, such as operating system applications like Notepad, or operating system utilities.
   - Hardware-specific applications actually used in the planned deployment area.
   - ISV applications that the community and ISVs have marked as compatible.
   - Applications that are not in a geography or department planned for upgrade.

5. During your application analysis, what is the main advantage of adding issue details or certifying applications using ACT?

   Answer: The main advantage is that your application information is synchronized with the Microsoft Compatibility Exchange and shared with other IT Professionals in the ACT community. ACT community members are able to quickly obtain information on how to mitigate issues to ensure compatibility with operating system upgrades or Windows updates.

6. After analyzing your compatibility issues, what are some examples of ways to mitigate any issues discovered?

   Answer: Answers can vary, but some examples include:

- Reinstall the application.
- Install a service pack or update to the application.
- Create application fixes by modifying the registry or file structure.
- Turn off operating system features that are causing the application compatibility issue.

7. Can a computer or application be deleted from your ACT database?

   Answer: Computers or applications cannot be deleted from the ACT database; however, your obsolete data can be assigned to a category that can be filtered out of your reports.

8. Must the client computer be restarted to get a DCP to collect data?

   Answer: The only time the client computer must be restarted is if the DCP includes the Update Compatibility Evaluator (UCE) and if the client computer is running Windows 2000. All other evaluators and supported operating systems do not require a restart.

## Real-world issues and scenarios

1. Last year, your customer upgraded its client computers from Windows XP to Windows Vista. The organization has since decided to deploy Windows 7, but management has indicated that it does not want to test applications twice for Windows Vista and then Windows 7. What are the implications of this decision?

   Answer: The majority of application incompatibilities are identified when moving from Windows XP or earlier operating systems to Windows Vista, and these incompatibilities apply in the same way to Windows 7. Investments made to remediate applications for Windows Vista will carry forward to Windows 7. While Microsoft is making the best effort to ensure that applications running on Windows Vista continue to run on Windows 7, some things have changed as evidenced by the information mentioned earlier in this module.

   Compatibility testing is recommended for any major configuration change, which can mean introducing applications, updates, service packs or complete operating systems to your computers. As a design goal, Windows 7 fundamentally does not change application compatibility requirements compared to Windows Vista when moving from Windows XP. Therefore, while the testing pass is still recommended, the effort required for additional application remediation will be much less after applications are certified for Windows Vista.

2. You have just installed Windows 7 on your organization’s client computers. How do you ensure that the new Windows 7 features work as expected with your current application portfolio?

   Answer: Deploy your data collection package to a Windows 7 test machine that contains all your approved business applications. Ensure the data collection package has the Internet Explorer and User Account Control Compatibility Evaluators enabled. Run the applications and access Web sites as a standard user and complete routine business tasks. The application compatibility information will be uploaded to your monitoring server.

3. You plan to use the Application Compatibility Toolkit to determine whether your organization’s applications are compatible with Windows 7. However, you are concerned that the data collection and inventory process will cause performance issues on your client workstations. What can you do to minimize performance issues?

   Answer: Configure the data collection package to only monitor application usage at specific times of the day and for a specified duration. Communicate with users about the monitoring so that users are aware if a performance issue does appear.

## Best practices related to implementing the application compatibility toolkit

1. In organizations that employ a large number of client computers, it is usually impossible and impractical to deploy data collection packages (DCPs) to every computer. The following guidelines can assist in determining which computers to deploy the DCPs to:

    - Ensure that all device drivers are captured so the proper impact can be assessed during an operating system or security upgrade, in addition to locating potential issue and solution data provided by Microsoft Corporation, Independent Software Vendors (ISVs), and the ACT Community.

    - Sample each unique hardware configuration so that you can synchronize with the Microsoft Compatibility Exchange and obtain the relevant driver compatibility issues.

2. The Application Compatibility Manager is used to restrict access for the testing and remediation processes being done by the various application owners throughout your organization. Perform the following steps to enable restricted access:

    a. Provide read and write access to the database for any users that require access to the compatibility reports.

    b. Start the Application Compatibility Manager for the first time, and then select the **View and manage reports only** option from the **Configuration Type Selection** page of the ACT Configuration Wizard.

       Selecting this option creates an instance of the ACT that cannot connect to the ACT Log Processing Service, but enables users to create data collection packages and to analyze their data.

    The users provided with read and write access will now be able to record their assessment ratings, their issue reproduction steps, and their solutions. In addition, you can create queries for each group and enable them to review only the relevant information for their specific applications.

3. After compatibility analysis using the Application Compatibility Toolkit, vendor and community assessment, and manual application-to-operating system testing, you can perform the following best practices to remediate applications:

    - The first priority is to locate a compatible version of the application with vendor support for third party applications. This ensures the application will work as intended and support for that application is available.

    - For in-house developed applications, the best practice is to recode the application for native compatibility or in the cases where it exists, use the compatible version. Guidance for recoding applications can be found in the Application Quality Cookbook for Windows 7.

    - For third party applications without support (for example, the vendor is no longer in business) or for in-house developed applications where recoding is not an option, compatibility fixes (or shims) can be used to assist the incompatible application for use with Windows 7. The Compatibility Administrator tool is part of ACT and can be used to create and edit shim database (SDB) files to mitigate compatibility issues.

      The Standard User Analyzer also creates SDB files to correct issues it detects where administrative privilege (or elevation) is required. SDB files are created to include fixes for as many applications as possible, not one for each application. They can be serviced through scripted commands if and when updates and additions are needed.

  - After exhausting ways of making applications run natively in Windows 7 or with the help from Compatibility Fixes, legacy operating system virtualization (Microsoft Enterprise Desktop Virtualization or Windows XP mode) or Remote Desktop Services can be used as a last resort or transitional path while applications are in the process of compatibility remediation.

4. Establish the Application Lifecycle for ongoing management of application versions. When companies stay up-to-date on applications and utilities, they usually can avoid these issues.

   Application Life-Cycle Management (ALM) is a practice whose primary objective is to turn an organization's IT function from a basic cost center that delivers brittle, unconnected applications and platforms to a strategic asset capable of:

   - Delivering a service oriented application platform that supports the organization's core business functions.
   - Delivering new services to drive business forward.
   - Adapting as your business evolves.
   - Keeping your business ahead of the competition.

   Staying up-to-date on applications and utilities is essential to delivering a service oriented application platform that supports an organization's core business functions.

5. Maintain application inventory for future Operating System and Service Pack testing. This is not disposable work to be used only once.

# Lab Review Questions and Answers

## Lab A: Evaluating Application Compatibility Using the Microsoft Application Compatibility Toolkit

**Question**: What are the benefits of joining the ACT community?

**Answer**: The ACT Community provides the ability to synchronize your local inventory and analysis results with an online collection from other IT Professionals, ISVs, and Microsoft. You will then be able to analyze application compatibility, and view detailed information on possible mitigation strategies as experienced by others using the same types of applications .

**Question**: How do would you ensure that the new Windows Vista features work as expected with your current application portfolio?

**Answer**: Deploy your data collection package to a Windows 7 test machine that contains all of your approved business applications. Make sure that the data collection package has the Compatibility Evaluators enabled. Run the applications as a standard user, and complete routine business tasks. The application compatibility information will be uploaded to your monitoring server.

**Question**: You are concerned that the data collection and inventory process will cause performance issues on your client workstations. What can you do to minimize performance issues?

**Answer**: Configure the data collection package to only monitor application usage at specific times of the day, and for a specified duration. Communicate with users about the monitoring so that users are aware if a performance issue does appear .

## Lab B: Creating Application Compatibility Fixes

**Question**: Provide a summary of the issues that you discovered when running StockViewer

**Answer**: Standard permission errors, unhandled exception errors, and an unsupported version error.

**Question**: Why did most of the application features work when you elevated the privileges? What did not work even with elevated privileges?

**Answer**: The application seems to require administrative permissions to specific file and registry locations. The Show Me a Star feature only supports Windows XP.

**Question**: What might be your next step after testing the fixed application and having successful results?

**Answer**: Your next step will be to deploy the StockViewerFix shim to target computers. You will need to run the Sdbinst.exe command to register the new shim on each computer that requires the application.

# Module 3

## Evaluating Windows® 7 Deployment Methods

### Contents:

# Lesson 2

## Evaluating Side-by-Side Deployment

### Contents:

# Question and Answers

## Discussion: Determining a Deployment Scenario

**Question:** How might you determine the deployment scenarios in your organization?

**Answer:** In this case, you have the following categories of users:

- Users who run Windows XP and have hardware more than three years old.
- Users who run Windows Vista with computers less than three years old.
- Users who run Windows Vista with newer computers.
- New users coming in the next month.

**Question:** How might you determine the deployment scenarios in your organization?

**Answer:** Your organization infrastructure fully supports all deployment scenarios. You can choose your deployment strategy to use all deployment scenarios as follows:

- Perform a side-by-side deployment for the 50 new computers for the managers. Ensure migration of user settings and data. You can automate this migration by using USMT with hard-link migration to minimize migration time and discard the need for storage space.
- Perform a clean installation of Windows 7 for the old computers. Despite using older computers, this will be a new computer scenario, where no migration is needed.

# Lesson 3

## Evaluating Lite-Touch Deployment Method

### Contents:

# Question and Answers

## Discussion: Determining the Feasibility of Using Lite-Touch Deployment Method

**Question:** How do you determine the feasibility of using the Lite-Touch deployment method to deploy Windows 7 to workstations in your head office and your remote offices, without bringing down the network at the same time?

**Answer:** Your organization already has a managed network, with Active Directory and Group Policy, and the users are already running Windows operating systems. This fulfills the infrastructure requirement for Lite-Touch deployment, which only requires file servers and managed networks.

# Lesson 4

## Evaluating Zero-Touch Deployment Method

### Contents:

# Question and Answers

## Discussion: Determining the Feasibility of Using Zero-Touch Deployment Method

**Question:** How do you determine the feasibility of using Zero-Touch deployment method to deploy Windows 7 to workstations in your head office and your remote offices, without bringing down the network at the same time?

**Answer:** To deploy Windows by using Zero-Touch deployment, you must ensure that the required infrastructure supports Zero Touch Installation (ZTI). Your organization already has a managed network, with Active Directory and Group Policy, and the users are already running Windows operating systems. But to implement ZTI, you must have System Center Configuration Manager, in addition to Microsoft Deployment Toolkit (MDT) and Windows Deployment Services (WDS). In this case, you must invest in Configuration Manager and training for the IT staff.

# Module Reviews and Takeaways

## Tools

| Tool | Use for | Where to find it |
|---|---|---|
| Microsoft® Deployment Toolkit (MDT) 2010 | • Deploying Microsoft products to desktops and servers<br>• Creating a single path for image creating and automated installation | Microsoft Download Center |
| System Center Configuration Manager 2007 SP2 | Assessing, deploying, and updating servers, clients, and devices across a physical, virtual, distributed, and mobile environment | Microsoft Download Center |
| Windows Deployment Services | Deploying Windows over the network | Microsoft Download Center for Windows Server 2003® SP1 Server Role in Windows Server 2008® and Windows Server 2008 R2 |
| Microsoft Assessment and Planning Toolkit | Assessing organization readiness for Windows 7 | Microsoft Download Center |
| Application Compatibility Toolkit | Inventorying and analyzing organization application compatibility | Microsoft Download Center |
| Windows Automated Installation Kit (Windows AIK) | Supporting the deployment of Windows operating system | Microsoft Download Center |
| ImageX | Capturing, creating, modifying, and applying the WIM file | Windows AIK |
| Windows Setup | Installing Windows or upgrading previous Windows versions | Windows 7 Product DVD |
| Answer file | Configuring Windows settings | |
| User State Migration Tool | Migrating user settings and data for a large number of computers | Windows AIK |
| Windows Easy Transfer | Migrating user settings and data in side-by-side migration for a single or few computers | Windows 7 Windows 7 Product DVD |

# Lab Review Questions and Answers

**Question**: What are the requirements for deploying a WDS server?

**Answer**: The WDS computer must be a member of an Active Directory domain.

The computer cannot be a Server Core computer.

The DHCP and DNS roles must be accessible to client computers using the WDS service.

The client computers must support PXE-boot to access the WDS service.

**Question**: Which command-line tool can be used to capture, modify, and apply WIM images?

**Answer**: ImageX.exe.

**Question**: What are the additional requirements for implementing ZTI deployments over those for LTI deployments?

**Answer**: ZTI deployments require SMS or SCCM in addition to the requirements of LTI deployments.

# Module 4

## Designing Standard Windows® 7 Images

### Contents:

# Lesson 3

## Determining the Image Strategy

### Contents:

# Question and Answers

## Determining the Language Packs to be Added to an Image

**Question:** Why might you add language packs to your image?

**Answer:** Language packs enable a multilingual Windows environment. Windows is language-neutral, and all language and locale resources are added to Windows with language packs. By adding one or more language packs to a Windows image, you can enable one or more languages in the final Windows operating system. This enables organizations to deploy the same Windows image to regions with multiple languages and locale settings, reducing the number of images that you have to maintain.

## Lesson 4

# Selecting the Image Servicing Methods

### Contents:

# Question and Answers

## Why Image Servicing?

**Question:** Why might you service an image using Windows Setup?

**Answer:** You may want to service an image using the settings in an answer file because the answer file installs updates and configures packages in a specific order, which makes it simpler for you to ensure that dependencies are satisfied. For example, you need a language pack installed before configuring international settings, and a Windows feature must be enabled before configuring settings for it. In addition, you may have a boot-critical driver that must be installed before the operating system boots.

When you use an unattended answer file with Windows Setup, customizations are made during the various configuration passes of Windows Setup. Setup calls the answer file during the deployment process, and the settings in the answer file are applied during the appropriate configuration pass.

## Considerations for Choosing Offline Servicing

**Question:** Why might you perform offline servicing to a Windows image?

**Answer:** If you have already created and customized your primary deployment image and discover that you have to apply an update, add a new driver, change the settings, or support multiple languages, these changes can be made without deploying the image and recapturing it, by performing offline servicing. Offline servicing is an efficient way to manage existing images that are stored on a server because it eliminates the need for deploying and recapturing the updated image. In addition, when servicing an image offline, you are not required to run the Sysprep tool, and therefore are not required to use a rearm.

## Considerations for Choosing Online Servicing

**Question:** Why might you perform online servicing to a Windows image?

**Answer:** In a typical scenario, you have a customized Windows image. Some of the packages and drivers that were added or removed offline might be in a pending state. This is usually because a reboot is required to complete online actions. Starting the image in audit mode will satisfy the reboot requirement and enable you to take inventory of your image, verify the installation state of drivers and other packages, and also service the running operating system.

# Module Reviews and Takeaways

## Review questions

1. Describe some of the benefits of using modularization when deploying a sector-based disk imaging system.
2. There are a few options to apply updates and determine how you add updates to your images. List some of the different approaches.
3. What is an important key to developing your Windows deployment strategy?

## Review answers

1. Benefits include: adding device drivers and updates to the imaged file offline, without actually deploying the image on a computer; when Microsoft releases an update for one of the features, you only have to update that feature in the installation image without re-creating the entire image; customization of optional features; deploying multiple Windows 7 language versions with a single image file.
2. The different approaches to add updates are as follows: slipstreaming updates to the install source; adding updates to the master image; adding updates post deployment.
3. Configuration passes are the key to the Windows deployment strategy. Configuration passes are the phases of a Windows installation, during which you can customize an image. These phases determine the appropriate modifications that you can make at each point in the installation process.

## Best practices related to scenarios and migration store size

- Use a single image strategy to reduce the number of images to maintain and service.
- Use a multilingual strategy to add multiple language packs to your image to reduce the number of language-specific images that you support.
- Run the **sysprep /generalize** command when preparing the Windows image to be captured, even if all computers have the same hardware configuration.
- Do not deploy the default image (install.wim) file that is included with the Windows product DVD directly by using ImageX. You can use the default image only with Windows Setup (setup.exe).
- Use the **imagex /flags** option when capturing a Windows image to create the metadata to apply to the image that you are capturing.
- Do not duplicate features for different architecture types in an answer file, if you are performing cross-platform deployments.
- Create architecture-specific settings for each configuration pass in an answer file for cross-platform deployments.

### Tools

| Tool | Use for | Where to find it |
|---|---|---|
| Windows Automated Installation Kit | Collection of tools that provide the conceptual and procedural information required for an unattended installation of | http://go.microsoft.com/fwlink/?LinkId=136976 |

| | | |
|---|---|---|
| (Windows AIK) | Windows operating systems, including:<br>• Windows® Preinstallation Environment (Windows PE)<br>• Deployment Image Servicing and Management (DISM)<br>• Windows System Image Manager (Windows SIM)<br>• ImageX<br>• User State Migration Tool (USMT) | |
| Windows® Pre-installation Environment (Windows PE) | A minimal operating system environment that is part of Windows AIK. It is used to deploy Windows. | Windows AIK |
| Deployment Image Servicing and Management (DISM) | A command-line tool that is part of Windows AIK. It can be used to service a Windows image or to prepare a Windows PE image. (DISM is available in all installations of Windows 7 and Windows Server® 2008 R2.) | Windows AIK Windows 7 |
| Windows Optional Component Setup (OCSetup) | Use the Ocsetup.exe tool at the command prompt to install or remove Windows optional elements and system features. | http://go.microsoft.com/fwlink/?LinkId=163072 |
| Driver Package Installer (DPInst) | Tool used to non boot critical drivers on a running operating system. (DPInst is a part of Driver Install Frameworks (DIFx) version 2.1 which is available in the Windows Driver Kit (WDK). | http://go.microsoft.com/fwlink/?LinkId=163073 |
| Plug and Play Utility (PNPUtil) | Tool used to add, remove, and enumerate drivers when updating Windows 7 operating system. | Windows 7 |
| Windows Update Standalone Installer (WUSA) | This tool uses the Windows Update Agent API to install update packages. Update packages must have a.msu file extension name. | http://go.microsoft.com/fwlink/?LinkId=163074 |
| Language Pack Setup (LPKSetup) | Tool used to add or remove language packs. | Windows 7 |

# Lab Review Questions and Answers

**Question**: In Exercise 1, how might your imaging strategy have changed had storage space not been at such a premium on the Hammersmith file server?

**Answer**: Answers will vary, but without the constraint of disk space on the server, students must envision using thick images to support the two distinct builds in the Hammersmith branch office.

**Question**: In Exercise 2, if network traffic was already excessive, might that have made any difference to the imaging strategy you selected?

**Answer**: Answers will vary, but with network traffic becoming a problem, use of hybrid images will seem more appropriate. This reduces the quantity of applications and updates that must be applied after the image is deployed.

# Module 5

## Deploying Windows® 7 by Using Windows AIK

### Contents:

# Lesson 1

## Overview of Windows AIK 2.0

### Contents:

# Question and Answers

## Overview of Tools Included in Windows AIK 2.0

**Question:** Which Windows AIK 2.0 tool enables OEMs and corporations to capture, modify, and apply file-based disk images for rapid deployment?

**Answer:** ImageX

## Overview of the Hardware Lifecycle

**Question:** What are the main reasons for upgrading or replacing hardware?

**Answer:** Hardware becomes outdated over time and upgrading the operating system or applications can require new hardware. One benefit of Windows 7 is that it has the same hardware requirements as Windows Vista®.

## Overview of the Desktop Deployment Lifecycle

**Question:** What are some of the benefits of having a pilot plan during the planning phase?

**Answer:** A pilot plan allows the IT Department to test a specific system configuration or application setup before deploying it to the entire enterprise. It is a risk mitigation tool.

# Lesson 2

## Building a Reference Windows 7 Image by Using Windows SIM and Sysprep

### Contents:

# Question and Answers

## Demonstration: Using Windows SIM

**Question:** Why use an answer file rather than manually completing the installation of Windows 7?

**Answer:** An answer file is used to automate the installation process for speed and consistency. Using an answer file assures that each installation is the same. Automating the installation process is more efficient when multiple computers are configured at once.

## Using Sysprep

**Question:** What is the purpose of running Sysprep with the **/audit** option?

**Answer:** The **/audit** option restarts the computer in audit mode. This enables you to add drivers or applications to Windows 7 and to test an installation of Windows 7 before it is sent to an end user.

# Detailed Demo Steps

## Demonstration: Using Windows SIM

### Build an answer file by using Windows SIM

1. Log on to the LON-CL2 virtual machine as **Contoso\Administrator** with a password of **Pa$$w0rd**.
2. Click Start, point to All Programs, click Microsoft Windows AIK, and then click Windows System Image Manager.
3. In the Windows Image area, right-click Select a Windows image or catalog file, and then click Select Windows Image.
4. Browse to \\LON-DC1\Labfiles\Source\Sources\Install_Windows 7 ENTERPRISE.clg and then click Open.

> **Note:** If a catalog file does not exist for this edition of Windows 7, follow the prompts to create a catalog file. The creation process takes several minutes. In this demonstration, there are no prompts to create a catalog file because one already exists.

5. In the Answer File area, right-click Create or open an answer file, and then click New Answer File.
6. In the **Windows Image** area, expand **Components** and scroll down and expand **x86_Microsoft-Windows-Setup**. This group of settings is primarily used in the Windows PE stage of an unattended installation. Notice that it includes Disk Configuration.
7. Expand **UserData** and right-click **ProductKey**. Notice that this setting can only be applied in the Windows PE stage. This is used for an unattended installation where Windows 7 is installed from the install.wim file on the Windows 7 installation DVD.
8. Scroll down and click **x86_Microsoft-Windows-Shell-Setup**. Notice that the option for the product key is available here and also in the Properties area.
9. Right-click **x86_Microsoft-Windows-Shell-Setup** and click **Add setting to Pass 4 specialize**. These settings are applied after an operating system is generalized by using Sysprep.
10. In the **Microsoft-Windows-Shell-Setup Properties** area, in the **ProductKey** box, type **11111-22222-33333-44444-55555** and press Enter. Placing a product key in this answer file prevents the need to enter the product key during the installation of a new image.
11. In Windows SIM, click **Tools**, and then click **Validate Answer File**.
12. Close **Windows System Image Manager** and do not save any changes.

# Lesson 3

## Managing the Windows Pre-Installation Environment

### Contents:

# Question and Answers

## What Is Windows PE?

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

**Answer:** You can use Windows PE to replace system files, recover data before installing Windows, and run diagnostic and configuration tools.

## Windows PE 3.0 Support Utilities

**Question:** Which Windows PE tool adds out-of-box drivers to a Windows PE image?

**Answer:** Drvload.

# Detailed Demo Steps

## Demonstration: Customizing a Windows PE Boot Disk

This demonstration shows how to customize a Windows PE boot disk.

1. Log on to the LON-CL2 virtual machine as **Contoso\Administrator** with a password of **Pa$$w0rd**.
2. Click **Start**, point to **All Programs**, click **Microsoft Windows AIK**, and then right-click **Deployment Tools Command prompt**. Click **Run as Administrator**.

### The following steps create a basic Windows PE environment for an x86 based system.

1. At the command prompt, type **Copype.cmd x86 c:\winpe_x86** and press **Enter**.
2. At the command prompt, type **copy c:\winpe_x86\winpe.wim c:\winpe_x86\ISO\sources\boot.wim** and press **Enter**.

> **Note:** Adding customizations involves copying folders and files into the Windows PE structure created with the previous commands. Some customizations are not loaded into memory when started in the Windows PE environment, such as ImageX.

3. To add ImageX, type: **copy "C:\program files\Windows AIK\Tools\x86\imagex.exe C:\winpe_x86\iso\** and press **Enter**.
4. At the command prompt, type **oscdimg -n -bC:\winpe_x86\etfsboot.com C:\winpe_x86\ISO C:\winpe_x86\winpe_x86.iso** and press **Enter**.

# Lesson 4

## Capturing, Applying, and Servicing a Windows 7 Image

### Contents:

# Question and Answers

## What Is ImageX?

**Question:** ImageX provides the ability to store multiple images in a single WIM file. What benefit does this provide?

**Answer:** Storing multiple images in a single WIM file minimizes the image file size. This simplifies your ability to deploy multiple images across a slower network connection, or by using removable media.

# Module Reviews and Takeaways

## Review questions

### Real-world issues and scenarios

1. Joseph is project managing the deployment of Windows 7 across Fabrikam's network of client computers. He wants to improve upon the deployment experience that they previously had with Windows XP several years ago by ensuring that the client installations are fast and consistent, and that multiple computers can be duplicated quickly.

   Since Fabrikam is giving its users a choice from a standardized range of applications that can be deployed along with Windows 7, Joseph wants to stage all of these applications in the reference installation. Based on these requirements, what deployment method does Joseph need to employ?

   Answer: Deploy an image of a custom Windows installation using a network.

2. Manisha is the IT Manager for a small wholesale distributor. She wants to deploy Windows 7 across the eight client computers in the organization's warehouse. She has the computers set up on an internal network, but she is not familiar with creating images. Which deployment method do you recommend Manisha use, and why?

   Answer: Manisha needs to use the Deploy from Media method and manually install Windows 7 on each client computer. This methodology is ideal for small corporate organizations that do not use images and employ a small number of computers.

3. You have installed Windows 7 on your company's client computers. However, you are later informed that one of the computers has a corrupted system file and will not start. From the list of tools covered in this module, which tool can you use to help fix the computer?

   Answer: Use Windows PE to start the computer, and then replace the corrupted system file from the Windows 7 media.

4. Paul is the lead technologist at London-based Tailspin Toys Inc. He is assigned the task of deploying Windows 7 across each of the organization's client computers. In an effort to decrease costs and scheduling risks, Paul plans to install Windows as rapidly as possible, including all relevant updates, applications, and settings.

   To accomplish this objective, he has decided to use ImageX to capture Windows Image (.wim) files for later deployment. What steps must Paul perform to prepare for the image capture?

   Answer: Paul must perform the following steps to prepare for the image capture:

   i. Create a Windows PE disk with the ImageX tool.

   ii. Create an ImageX configuration file.

   iii. Create a reference computer by deploying Windows 7 and then removing the computer-specific information from the system.

5. In Paul's hurry to get his Windows 7 image deployed as quickly as possible at Tailspin Toys, he failed to consider any security threats to his images. Why is this concern a serious shortcoming in his planning efforts?

   Answer: The files used to set up and deploy Windows 7 contain sensitive data. Unattended installation answer files contain passwords and product keys. Distribution shares contain intellectual property, licensed applications, custom applications, and other data. Windows images can contain an aggregate of this sensitive data. Paul needed to review safety measures to improve the security of his deployment infrastructure.

### Best practices related to the Windows AIK

1. When building your deployment environment, it is recommended that you create a lab environment dedicated to developing and testing your Windows 7 deployment. The lab must mirror the production environment as closely as possible to ensure that all aspects of this environment can be accounted for in the development process.

2. Deploying Windows 7 images from a network is ideal for corporate deployments. Using an image-based deployment over a network ensures that your installations are faster and consistent across all your systems. This method provides maximum flexibility and enables you to duplicate multiple computers quickly.

   After creating a base image, you can install it on multiple computers so that all clients end up with identical configurations. You can also customize the base image to meet the requirements of a specific user or group of users.

### Best practices related to the servicing Windows images

1. **Elevate Permissions for Command-Line tools**: All deployment command-line tools, including Deployment Image Servicing and Management (DISM), require elevated permissions. To ensure that you have elevated permissions, click **Start**, point to **All Programs**, point to **Windows OPK (or Windows AIK)**, right-click **Deployment Tools Command Prompt**, and then select **Run as administrator**. This must be done even if you are logged on as an administrator.

2. **Servicing an Image**: The best way to service a Windows image is offline with the DISM tool. DISM can be used to install, uninstall, configure, and update drivers, features, and packages in Windows images and Windows Pre-installation Environment (Windows PE) images without starting the image.

3. **Package Locations**: Do not put a package you intend to install directly at the root of a partition on a Windows 7 installation.

4. **Use Log Files**: By default, DISM will log verbose information to **%WINDIR%\Logs\Dism\Dism.log**. You can also specify a name and location of your choice for the log file and set the **/loglevel** parameters so that only the information you are interested in is logged.

   When an error occurs, the console will display the error code, error message, and the location of the log file. The log file will automatically be archived. The archived log file will be saved with .bak appended to the file name, and a new log file will be generated.

   Each time the log file is archived, the .bak file will be overwritten. The log file provides the history of the operations performed, which can help you troubleshoot problems.

## Tools

The following table provides a consolidated list of the tools covered in this module.

| Tool | Use for | Where to find it |
|---|---|---|
| Windows Pre-installation | Windows PE is a compact, special-purpose Windows operating system | Located in the Windows AIK, which is installed to the **C:\Program Files\Windows** |

| | | |
|---|---|---|
| Environment (Windows PE) | that prepares and initiates a computer for Windows Setup, maintenance, or imaging tasks, and recovers operating systems such as Windows 7. With Windows PE, a subset of Windows 7 can be started from a network or removable medium, which provides network and other resources necessary to install and troubleshoot Windows 7. Windows PE can also start a computer that has no functioning operating system installed, and act as a replacement for MS-DOS®–based boot disks that were utilized in previous Windows operating system versions. | **AIK** directory. |
| System Preparation tool (Sysprep) | Sysprep prepares a Windows image for disk imaging, system testing, and delivery to an end user. Sysprep can remove any system-specific data from a Windows image, such as the security identifier (SID). After removing unique system information from an image, you can capture that Windows image and use it to deploy on multiple systems. In addition, Sysprep can configure the Windows image to start to audit mode. Audit mode enables you to test the integrity of the system and install additional applications and device drivers. Sysprep is also used to configure Windows to start to Windows Welcome the next time the system starts. | Windows command line tool. Syntax: sysprep.exe [/oobe \| /audit] [/generalize] [/reboot \| /shutdown \| /quit] [/quiet] [/unattend:answerfil] |
| Windows System Image Manager (Windows SIM) | Windows SIM is a tool used for customizing and automating Windows 7 installations. Windows SIM enables you to create and manage unattended Windows Setup answer files. These answer files are used during the Windows Setup installation phases to apply additional configurations and customizations to the default installation. | Located in the Windows AIK, which is installed to the **C:\Program Files\Windows AIK** directory. |
| ImageX | ImageX is a command-line tool that enables the creation, modification, and deployment of file-based images by using a shared imaging format across operating system images, including applications. ImageX works with Windows image | Located in the Windows AIK, which is installed to the **C:\Program Files\Windows AIK** directory. |

| | | |
|---|---|---|
| | (.wim) files for copying to a network. The .wim files contain one or more volume images for a Windows operating system. A volume image represents the captured volume or partition of a Windows operating system. The primary purpose of the ImageX tool is to capture, modify, and apply images for deployment in a manufacturing or corporate IT environment. | |
| Deployment Image Servicing and Management tool (DISM) | DISM is a new command-line tool in Windows 7 and Windows Server 2008 R2. DISM consolidates the core image management functions of multiple tools found in the Windows Automated Installation Kit (AIK). DISM enables IT professionals to view components of an applied or mounted operating system image and add or remove packages, software updates, and drivers. DISM can service Windows images offline before deployment or to prepare a Windows Pre-installation Environment (Windows PE) image. | Located in the Windows AIK, which is installed to the **C:\Program Files\Windows AIK** directory. |

The following table describes the documentation resources available on the Windows AIK DVD and installed with the Windows AIK tools. Additional documentation can be included on the Windows AIK DVD but not listed in this table.

| **Documentation** | **Description** |
|---|---|
| Windows Automated Installation Kit (Windows AIK) User's Guide (Windows AIK.chm) | Provides the conceptual and procedural information required for unattended installation of Windows operating systems. This user's guide includes information on:<br>• Planning<br>• Preparing the deployment environment<br>• Creating and customizing an image<br>• Capturing, modifying, and testing the image<br>• Deploying, maintaining, and servicing the image |
| Imaging APIs for Windows (Wimgapi.chm) | Provides comprehensive coverage of all the Windows imaging application programming interfaces (APIs). |
| Windows Pre-installation Environment (Windows PE) User's Guide (Winpe.chm) | Provides instructions on creating a customized version of Windows PE and enabling Windows PE to start from different types of media. |
| Component Platform Interface (CPI) Reference (Cpiapi.chm) | Documents the APIs that are used in Windows SIM. |

| | |
|---|---|
| Windows® Unattended Setup Reference (Unattend.chm) | Provides comprehensive coverage of all the customizable settings in the Windows Unattend.xml file. |
| Step-by-Step: Basic Windows Deployment for IT Professionals (stepbystep_itpro) | Provides basic instructions on building an end-to-end deployment. This guide is ideal for new users who want to learn the basics of Windows deployment. |

# Lab Review Questions and Answers

## Lab A: Installing the Windows Automated Installation Kit

**Question**: What are the tools that comprise the Windows Automated Installation Kit?

**Answer**: Windows System Image Manager (Windows SIM), ImageX, Deployment Image Servicing and Management (DISM), Windows Pre-installation Environment (Windows PE), Windows Setup, Sysprep, and the User State Migration Tool (USMT).

**Question**: What is the function of the Windows System Image Manager?

**Answer**: The tool is used to open Windows images, create answer files, and manage distribution shares and configuration sets.

**Question**: What is ImageX used for?

**Answer**: The tool is used to capture, create, modify and apply Windows images.

**Question**: What is the Windows Pre-installation Environment?

**Answer**: A minimal operating system environment used to deploy Windows. The Windows AIK includes several tools used to build and configure Windows PE environments.

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

**Question**: What information is in a catalog file?

**Answer**: A binary file that contains the state of all the settings and packages in a Windows image. When a catalog is created, it queries the Windows image for a listing of all the settings in that image. Because the contents of a Windows image can change over time, it is important torecreate the catalog file whenever you update a Windows image.

**Question**: What are the Benefits of using Windows SIM?

**Answer**: Windows SIM provides the following benefits that allow you to:

- Create an unattended answer file quickly.
- Validate the settings of an answer file against a Windows image (.wim) file.
- View all the configurable component settings in a .wim file.
- Update an answer file simply.
- Create a configuration set that contains a complete set of portable folders with Setup files.
- Add third-party drivers, applications, or other packages to an answer file.

**Question**: What is the purpose of the Generalize switch with Sysprep?

**Answer**: It prepares the Windows installation to be imaged. If this option is specified, all unique system information is removed from the Windows installation. The security ID (SID) resets, any system restore points are cleared, and event logs are deleted. The next time the computer starts, the specialize configuration pass runs. A new security ID (SID) is created, and the clock for Windows activation resets, if the clock is not already reset three times.

## Lab C: Creating Windows PE Boot Media

**Question**: You added the entry \Temp to your WIMScript.ini file, however files were imaged in the C:\Windows\Temp folder, what caused this to happen?

**Answer**: This happened because using the preceding \ character only excludes folder in relation to the root directory. In our example using \temp excludes C:\Temp or E:\Temp etc but would not exclude C:\Windows\Temp.

**Question**: What is created by default you are building a Windows PE Image?

**Answer**: Just the Windows PE environment. Additional modules can be loaded, such as ImageX, Scripting Support, recovery Environment features and other optional packages.

## Lab D: Capturing and Applying a Windows 7 Image Using ImageX

**Question**: Why do you need to create a C: drive before deploying an image?

**Answer**: ImageX is a file-level imaging tool and does not work at the sector level therefore the partition must exist before the files can be laid down.

**Question**: How can you further automate the deployment process?

**Answer**: Include the scripting module in the Windows PE build and create scripts for partition creation and formatting.

## Lab E: Servicing Images by Using DISM

**Question**: How do you add a windows package to an offline image?

**Answer**: "DISM /Image:C:\Servicing /Add-Package /PackagePath:Z:\Package.cab"

**Question**: What kind of packages can be added to an offline image?

**Answer**: Updates in .CAB or .MSU files.

# Module 6

## Deploying Windows® 7 by using Windows Deployment Services

### Contents:

# Lesson 1

## Overview of WDS

### Contents:

# Question and Answers

## Types of Images Supported by WDS

**Question:** How is an install image different from a boot image?

**Answer:** An install image has the operating system to be deployed to the client. The boot image has an application in a Windows PE computer to be deployed.

## Process of Deploying Windows 7 by Using WDS

**Question:** You want to transmit data by using multicasting, but do not want to incorporate all of WDS. Which server role do you select?

**Answer:** Transport Server

# Lesson 2

## Designing and Configuring WDS for Windows 7 Deployment

### Contents:

# Question and Answers

## Considerations for Designing a WDS Environment

**Question:** What are the image requirements for Windows 7 in WDS?

**Answer:** All the images must be WIM files.

## Demonstration: Configuring the WDS Server Role

**Question:** What is the difference between the Deployment Server and the Transport Server?

**Answer:** The Deployment Server is the server that is used for most Windows Deployment implementation scenarios. It contains the images and configuration for client connections. The Transport Server is used to provide multicasting features to the WDS server.

## Creating a Custom Install Image by Using the Image Capture Wizard

**Question:** What are the prerequisites for creating custom install images?

**Answer:** Disk space availability and local administrator credentials.

## Demonstration: Provisioning Drivers by Using WDS

**Question:** You have a driver package for a specific manufacturer that needs be deployed. Which type of filter do you configure?

**Answer:** You can configure a Manufacturer filter type that matches the manufacture name.

## Configuring WDS to Manage Client Computer Requests

**Question:** You want to configure properties on the computer account to control the installation for the client. What do you need to do to the client?

**Answer:** This is called prestaging the client.

## Deploying VHD Images by Using WDS

**Question:** In general, .vhd images are deployed in the same way that .wim images are deployed. What WDS command-line tool must be used to do this?

**Answer:** The only way to import and configure these images is through the WDSUTIL command-line tool.

# Detailed Demo Steps

## Demonstration: Configuring the WDS Server Role

## Detailed demonstration steps

This demonstration shows how to install and configure the WDS server role.

### Install the WDS Server role

1. Log on to **LON-DC1** as **Contoso\Administrator** using the password **Pa$$w0rd**.
2. In the task bar, click **Server Manager**.
3. In the **Server Manager** console, in the left-hand console pane, click **Roles**. The **Roles** node is used to add and remove server roles on a Windows Server 2008 server.
4. In the details pane, in the **Roles Summary** section, click **Add Roles**. The **Add Roles Wizard** starts.
5. On the **Before You Begin** page, click **Next**.
6. On the **Select Server Roles** page, select the check box next to **WDS** and then click **Next**. The **Select Server Roles** page provides a list of all the server roles available in Windows Server 2008.
7. On the **Overview of WDS** page, click **Next**.
8. On the **Select Role Services** page, ensure that both **Deployment Server** and **Transport Server** are selected and then click **Next**.

   The Deployment Server is the server that is used for most Windows Deployment implementation scenarios. It contains the images and configuration for client connections. The Transport Server is used to provide multicasting features to the WDS server.
9. On the **Confirm Installation Selections** page, click **Install**.
10. On the **Installation Results** page, click **Close**.
11. Close the **Server Manager** console.

### Configure the WDS Server role

1. On LON-DC1, click **Start**, point to **Administrative Tools** and then click **WDS**.
2. In the WDS console, in the left-hand console pane, click the plus sign to expand the **Servers** node and then click **LON-DC1.Contoso.com**.
3. Right-click **LON-DC1-Contoso.com** and then click **Configure Server**. The **WDS Configuration Wizard** starts.
4. On the **Before you Begin** page, click **Next**.
5. On the **Remote Installation Folder Location** page, under **Path**, type **E:\RemoteInstall** and then click **Next**.

   The remote install folder is used to store the boot and install images. It is automatically shared and configured to allow for remote clients to connect and download images.
6. On the **DHCP Option 60** page, select the following options and then click **Next**:
   - Do not listen on port 67

  - Configure DHCP option 60 to 'PXEClient'

7. The **Do not listen on port 67** setting is required if you are installing the WDS server role on a server that also hosts the DHCP server role. The option 60 provides DHCP scope information for locating the PXE server.
8. On the **PXE Server Initial Settings** page, select **Respond to all client computers (Known and unknown)**. Select the check box next to **Require administrator approval for unknown computers**. Click **Next**.

   There are three options on this page. Selecting **Do not respond to any clients** disables the PXE services from providing boot or install images to clients.

   If you select **Respond only to known clients**, only clients that are pre-staged into Active Directory are able to use PXE services.

   The final option responds to both unknown and known clients. This option is often secured by requiring administrator approval for unknown computers.
9. On the **Operation Complete** page, clear the **Add images to the server now** check box and then click **Finish**.
10. In the WDS console, in the left-hand pane, right-click **LON-DC1.Contoso.com** and then click **Properties**.
11. Take note of the following tabs:
    - **General**: information about the Computer name, location of the Remote installation folder, and the Server mode.
    - **PXE Response**: options for configuring the PXE Response Policy.
    - **AD DS**: options for defining how to name unknown computers and for specifying where computer accounts need to be created.
    - **Boot**: options for providing default PXE boot settings and default boot image selections.
    - **Client**: options for providing an unattend file, joining a domain, and client logging.
    - **DHCP**: options for configuring DHCP integration.
    - **Multicast**: options for configuring multicast IP Addresses and Transfer settings.
    - **Advanced**: options for integrating with domain controllers and DHCP authorization.
    - **Network**: options for configuring the UDP Port Range.

## Demonstration: Provisioning Drivers by Using WDS

## Detailed demonstration steps

This demonstration shows how to add and filter drivers using WDS.

### Add drivers to WDS

1. In the left-hand console pane, expand **LON-DC1.Contoso.com** and then click **Drivers**.
2. Right-click **Drivers** and then click **Add Driver Package**. The **Add Driver Package Wizard** starts.
3. On the **Driver Package Location** page, click the **Select all driver packages from a folder** option.

4. In the **Location** text box, type **E:\Labfiles\Drivers\VX6000** and then click **Next**.
5. On the **Available Driver Packages** page, accept the default selections and then click **Next**.
6. On the **Summary** page, click **Next**. The driver packages are added to WDS.
7. On the **Task Progress** page, click **Next**.
8. On the **Driver Groups** page, select **Create a new driver group named:** and then type **VX 6000 Lifecam**. Click **Next**.
9. On the **Task Complete** page, remove the check mark next to **Modify the filters for this group now** and then click **Finish**.

### Create a driver deployment filter

There might be a number of scenarios that require different drivers. For example, you can have laptops that require specific multimedia drivers that are different than your desktop images. You can create filters to ensure that only systems that meet specific requirements receive drivers from WDS.

1. In the left-hand console pane, expand **LON-DC1.Contoso.com** and then expand **Drivers**.
2. Click the **VX 6000 Lifecam node**.
3. Right-click **VX 6000 Lifecam** and then click **Modify Filters for this Group**.
4. In the **VX 6000 Lifecam Properties** box, on the Filters tab, click **Add**.
5. In the **Add Filter** box, configure the following and then click **Add**:
    - Filter Type: **Chassis Type**
    - Operator: **Equal to**
    - Value: **Laptop**
6. In the **Add Filter** box, click **OK**.
7. In the **VX 6000 Lifecam Properties** box, click **OK**.

# Module Reviews and Takeaways

## Review questions

1. Windows 7 needs to be deployed to a variety of clients in a heterogeneous computer environment. How do you handle the creation of multiple images for deployment to each kind of client?
2. You are tasked with deploying Windows 7 to clients in several countries. Is it necessary to create a different install image for each language?
3. How does drive provisioning assist the WDS project?
4. What type of an image must be used to capture the operating system of a client as a .wim file?

## Review answers

1. Windows 7 images are not HAL specific, so only two images are needed: one for 32-bit architecture clients and one for 64-bit architecture clients.
2. Languages are installed by using external language packs, and applications are downloaded by using Configuration Manager 2007.
3. Driver provisioning enables you to add and configure driver packages on the server and then deploy them to client computers during installations based on their hardware.
4. A type of boot image called a Capture Image.

## Troubleshooting performance problems

| Issue | Troubleshooting Tip |
|---|---|
| **Performance decreases**: WDS can handle several hundred network boot requests per second in sustained throughput. Slight performance decreases can occur if the domain controller is located across a latent network link or is overloaded. | In larger environments, consider locating DHCP and WDS roles on separate physical computers. |
| You diagnose long download times (observed from the client computer as a progress bar below an IP address). | Look at the average response time between the client and the server it is downloading from. To do this, in Windows PE, open the Command Prompt window, type **ping** *<server's IP address>*, and then note the average latency measured. If the average latency is less than 1 millisecond, that is good. To improve this performance, consider doing one or more of the following: Use a WDS server that is closer to each client. Remove stress and load from the network segment. If the client connects to the server after multiple network hops, use the output from the **tracert** command to identify the latent segment, and consider rerouting TFTP traffic to avoid the hop. |
| Multicast transmissions are running slowly | A typical cause of this issue occurs in environments that contain computers with different hardware configurations and architectures. In this case, some clients can run multicast transmissions faster than others. Because each transmission can be run only as fast as the slowest client, the entire |

| | |
|---|---|
| | transmission is slow if there is one slow client. To resolve this issue, first determine the client that is holding back the transmission (this is called the master client). To do this, view the output of the following command: WDSUTIL /Get-AllMulticastTransmissions /Show:Clients Next, disconnect the master client by using the following command, where <ID> is the client ID: WDSUTIL /disconnect-client /ID:<ID> Disconnecting the master client forces it to run the transmission by using the Server Message Block (SMB) protocol, and then other clients' multicast performance speeds up. If the multicast performance does not speed up, there is a problem with the client's hardware (for example, a slow hard drive) or a network problem. |
| After enabling multicasting, there is excessive traffic on the network | A common cause of this is if Internet Group Membership Protocol (IGMP) snooping is not enabled on all devices. IGMP snooping enables your network hardware to forward multicast packets only to those devices that are requesting data. If IGMP snooping is turned off, multicast packets are treated as broadcast packets and are sent to every device in the subnet. In cases where IGMP snooping cannot be enabled, adjust the multicast packet time-to-live (TTL), which is 32 by default. Change this by modifying the registry key of the network profile at: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WDSServer\Providers\Multicast\Profiles\ The value 32 is sufficient for most network topologies. |

## Best practices

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

**Reduce the size of the boot image to speed up TFTP downloads:**

- Use the tools in the Windows AIK to create a custom boot image that contains the Windows Setup binary files and Windows PE. Ensure that this image is prepared by using PEIMG.exe /prep.
- Ensure that the.wim file that contains the boot image does not contain extra space. A best practice is to use the ImageX /export command to export your boot image to a clean .wim file before adding the image to the WDS server.
- Ensure that the .wim file that contains the boot image is using the maximum compression format, LZX. To do this, run ImageX /info ImageFile <ImageNumber|ImageName>.
- In situations where a server is overburdened, configure a network boot referral to direct starting clients to different WDS servers for TFTP downloads.
- Alter your physical network topology by doing one or more of the following:
    - Add a WDS server closer to the client computer.
    - Move the client computer closer to the WDS server.
    - Repair the existing network infrastructure (in the case of high-packet loss).
    - Upgrade to better cabling (Cat 5e is recommended).
    - Check the condition of the switches between the client computer and the WDS server to ensure that packets are not being dropped.

**Reduce network congestion or inadequate resources on the server or client:**

- **Create more bandwidth on the network**: This might mean upgrading your network infrastructure to support greater bandwidth and higher throughput.

For example, moving from 100 Mb to 1 Gb, upgrading cabling, replacing hubs with routers or switches, or reducing the number of clients that can access a particular network segment simultaneously.

- **Add additional WDS servers to the network to handle the network demand**: This means segmenting network infrastructure so that smaller groups of clients are answered by each server.
- **Balance the server load by adding dedicated image servers**.
- **Reduce image size**: Because larger images mean longer installation times and greater network strain, consider creating images that contain minimum customization, drivers, and applications; or consider creating specialized images for each department, hardware type, or function.

### Use Performance Monitoring

Windows Reliability and Performance Monitor can be a powerful tool for identifying resource issues on services associated with WDS. The following are useful counters for diagnosing WDS performance:

- Network Interface (Bytes Sent/sec)
- PhysicalDisk (Avg. Disk sec/Read, Avg. Disk sec/Write, and Current Disk Queue Length )
- Process (Page Faults/sec)
- Processor (% Processor Time)
- WDS Multicast Server (all counters)
- WDS TFTP Server (all counters)
- WDS Server (all counters)

### Use deployment logs

You can enable tracing and logging for all WDS components for troubleshooting purposes. The installation logs are stored at %windir%\logs\cbs\cbs.log. Other than displaying a message that indicates whether the operation succeeded or failed, WDSUTIL shows minimal screen output (by default).

However, you can specify two additional options to enable more output. You can specify */Verbose* to show detailed information about a task, and specify */Progress* to use ellipses to indicate that a long-running process (for example, adding an image) is running and is not stalled. When these options are being used, it is still possible to redirect the WDSUTIL output to a file.

### Use dyamic driver provisioning in Windows 7 to reduce the size of the images and reduce the number of images to maintain

- It is not necessary to update images when you introduce new hardware into the environment. By storing drivers centrally on deployment servers, separate from images, you can install drivers dynamically or assign sets of drivers based on information contained in the BIOS.
- If you choose to install drivers dynamically, Windows 7 enumerates Plug and Play devices during installation. Then, it chooses drivers based on the Plug and Play IDs of the actual devices on the PC.
- Reducing the number of drivers on individual PCs reduces the number of potential driver conflicts. This helps streamline installation and setup times, and helps improve the reliability of the PC.

### Avoid performance and scalability problems

- Ensure that the network interface between the server and client has sufficient bandwidth.
- Use high-quality Ethernet cabling.
- Use network switches.
- Partition network segments to distribute the load across multiple servers.
- Keep network latency to a minimum to optimize TFTP transfers.
- Ensure that the disk that contains the remote install folder has enough throughput to meet the client demand.
- Ensure that there is sufficient memory on the server to handle the demands.
- Ensure that there is enough processor bandwidth on the server to handle the demands.

### Configure the server for performance and scalability

A key benefit of using WDS is the ability to deploy to several clients simultaneously. Again, many factors influence the solution's ability to scale, but the most important ones are the following (in order from most to least influential):

- **Network bandwidth**: WDS performs best using a 1Gb-per-second network adapter.
- **RAM on the server**: If the computer has enough available memory, it is possible to cache an entire image into memory.

  This reduces the number of disk read/write operations and, in turn, speeds up the process. If several different images are being deployed concurrently, you may need more RAM.
- **Disk speed on the server**: The install image must be read from the disk at least once, and a faster disk speed can accelerate this process.
- **Disk speed on the client**: A bottleneck in the client computer's disk may keep it from achieving the shortest possible installation times.

# Lab Review Questions and Answers

**Question**: What is the difference between a boot image, a capture image, and an install image?

**Answer**: A boot image is a Windows PE image used to boot the PXE client. A capture boot image also launches the client, but will then start the Windows Deployment Services Image Capture Wizard . An install image is the image that will be deployed and installed on the client workstation.

**Question**: How can you minimize the need to approve client computers that are being installed over the network?

**Answer**: Prestage the client computers by adding them to Active Directory Domain Services before the PXE deployment.

# Module 7

## Deploying Windows® 7 by Using Lite Touch Installation

### Contents:

# Lesson 1

## Designing the Lite Touch Installation Environment

### Contents:

# Question and Answers

## Discussion: Designing a Lite Touch Installation Environment for a Given Scenario

**Question:** What elements in your current infrastructure support Lite Touch Installations?

**Answer:** LTI requires minimal infrastructure. In this scenario, you already have the required infrastructure to deploy Windows 7 using LTI, in terms of file servers and a managed network. In addition, your corporate head office has already prepared a standardized image, so you do not need to create a custom image of Windows 7. You only need to focus on how to deploy this image efficiently and effectively.

**Question:** How might you use your current resources to perform LTI deployment?

**Answer:** You have two servers that you can use for this deployment project. Ideally, you will designate one as a build server, install MDT 2010 on it, and create a deployment share. However, you can also install MDT 2010 on the technician computer and manage your build server from your technician computer. Populate the build server deployment share with the custom Windows 7 image provided by the corporate head office. Because most of the users have fairly new computers, it is typically best to select the refresh computer scenario. Create task sequences for the deployment scenario.

**Question:** What deployment method do you choose for the three offices?

**Answer:** You need to deploy to three offices. For deployment to the Copenhagen and Paris office, you can use WDS to initiate the destination computer and install the image from the deployment share. You can install Windows Server 2008 R2 on the other available server, and configure the WDS server role. This is because the server is located in the Copenhagen office, and the Paris office has a high-speed connection to Copenhagen office.

For the London office, use the LTI deployment media. You can prepare this media at your office and ship it to the London office, or ask the IT support in London to download it from your file server. The IT support in London can then use this LTI deployment media to start the deployment process and install Windows 7 to the computers in the London office.

**Question:** How do you optimize the user data migration in this scenario?

**Answer:** In this scenario, you are performing the refresh computer scenario. In the refresh computer scenario, you can use the USMT with a hard-link migration to help migrate user data on the local computer. When you do this, you do not require temporary storage for user data and you can take advantage of the performance benefits of hard-link migration store with offline migration.

## Lesson 2

# Implementing MDT 2010 for Deploying Windows 7

### Contents:

# Question and Answers

## Demonstration: Configuring a Deployment Share

**Question:** How do you create a deployment share on a Server (such as LON-DC1) if the MDT was deployed to a workstation (such as LON-CL2)?

**Answer:** If the user has administrative rights to the server, he or she can specify the UNC to the folder. The appropriate subfolders will then be created.

## Demonstration: Creating a Task Sequence

**Question:** How do you deploy Windows 7 to three different departments with different application needs?

**Answer:** Answer will vary. One way is to create three task sequences to deploy a single operating system image using the Standard Client Task Sequence and then customize the applications added by that task sequence.

## Demonstration: Updating a Deployment Share

**Question:** When might you decide to completely regenerate the boot images when updating a deployment share?

**Answer:** If you have made changes to the WinPE settings of an existing deployment share.

# Detailed Demo Steps

## Demonstration: Configuring a Deployment Share

## Detailed demonstration steps

This demonstration shows you how to create a deployment share, how to add an operating system to the deployment share, and how to add device drivers to the deployment share.

### Create an MDT 2010 deployment share

You can create a deployment share by using the New Deployment Share Wizard in the Deployment Workbench.

1. On LON-CL2, open the **MDT 2010 Deployment Workbench** from the Start Menu.
2. In the Deployment Workbench console tree, right-click **Deployment Shares**, and then click **New Deployment Share**; the New Deploym**ent Wizard opens.**
3. On the **Path** page, click **Browse**.
4. Expand **Computer** and select **Local Disk**.
5. Click **Make New Folder. The folder can be created earlier. The only requirement for the deployment share is that it starts with an empty folder.**
6. Type **DeploymentShare** and then click **OK**. The folder can be named anything.
7. On the **Path** page, click **Next**. The f**older must exist before you continue.**
8. On the **Share** page, click **Next**. Regardless of the folder name specified, the default share is \\<Computer_name>\DeploymentShare$.
9. On the **Descriptive Name** page, click **Next. This name is used to identify the share in the Deployment Workbench console.**
10. On the **Allow Image Capture** page, click **Next. Typically, you are prompted to capture an image from systems installed into a workgroup. Clearing this check box allows you to skip this step.**
11. On the **Allow Admin Password** page, click **Next. You can select this check box to allow users to set the Local Administrator password when an image is deployed from this share.**
12. On the **Allow Product Key** page, click **Next. Selecting this check box will allow the users to specify an installation key.**
13. Review the **Summary** page and then click **Next. Review the summary information and continue with the creation of the deployment share.**
14. Review the **Confirmation** page and then click **Finish. Review the log file for errors that occurred during the creation of the deployment share. In addition, you can view the PowerShell code used to create the deployment share.**
15. Right-click **Deployment Workbench/Deployment Shares/MDT Deployment Share (C:\DeploymentShare)** and then click **Properties**.

    On the **General** tab, there is a check box to enable multicast support on this deployment share. This requires the deployment share to be created on a Windows 2008 server with WDS installed.

16. Select the **Rules** tab. This tab allows you to adjust the behavior of this deployment share. You can see some of the settings specified earlier such as SkipAdminPassword=YES. Refer to the MDT Documentation for the available options on this tab.
17. Select the **Windows PE x86 Settings** tab. This tab allows you to configure the boot images created for this deployment share. The **Windows PE x64 Settings** tab contains the same settings for the 64-bit environment.
18. Select the **Windows PE x86 Components** tab. This tab allows you to specify additional components for the Windows PE boot environment. The **Windows PE x64 Components** tab contains the same settings for the 64-bit environment.
19. Close the properties dialog box.

### Add Operating System Files to the Deployment Share

1. Before an Operating System can be deployed, the deployment share must contain the Operating System files. You can add the operating system files by using the Import Operating System Wizard in the Deployment Workbench.
2. On the host computer, in the **Hyper-V Manager, right-click 6294A-LON-CL2 and select Settings**.
3. In the Settings for 6294A-LON-CL2 dialog box, click **DVD Drive**.
4. Select the **Image File:** check box and specify the "C:\Program Files\Microsoft Learning\6294\Drives\Windows7_32Bit.iso" image file.
5. In the **Settings for 6294A-LON-CL2** dialog box, click **OK**.
6. In LON-CL2, close the Autoplay window.
7. In the Deployment Workbench console tree, locate Deployment Workbench/Deployment Shares/MDT Deployment Share (C:\DeploymentShare)/Operating Systems.
8. In the Actions pane, click **Import Operating System**; the Import Operating System Wizard opens.
9. On the **OS Type** page, select the **Full set of source files** and then click **Next**. The option selected depends on the type of installation to be performed.

   For example, to build a new reference computer you may want to start with the full set of source files. After capturing a customized installation, import the Custom image for deployment. You can also import images from a previous WDS deployment.
10. On the **Source** page, type **D:\** and then click **Next**. Because you choose to import the full set of source files, you are prompted for the source files location. If you choose to import a custom image file, this step is skipped and you are prompted for the image location instead.
11. On the **Destination** page, click **Next**. This creates the folder within the deployment share for the operating system files.
12. Review the **Summary** page and then click **Next. Review the summary information and continue with the import of the operating system files.**
13. Review the **Confirmation** page and then click **Finish. Review the log file for any errors that occurred during the import of operating system files**. Similar to the other Wizards, this page allows you to view the PowerShell code that is run to complete the previous steps.

### Add device drivers to the deployment share

Device driver packages that include an .inf file can be imported to the Deployment Workbench and installed automatically as a part of the deployment process. To implement this, first add the device driver to the Deployment Workbench.

1. In the Deployment Workbench console tree, locate **Deployment Workbench/Deployment Shares/MDT Deployment Share (C:\DeploymentShare)/Out-of-Box Drivers**.
2. In the Actions pane, click **Import Drivers**; the Import Driver Wizard opens.
3. On the **Specify Directory** page, type \\LON-DC1\Labfiles\Mod05\LabE\IPoint and click **Next**.
4. Review the **Summary** page and click **Next**. Review **the summary information and continue with the import of the device driver.**
5. Review the **Confirmation** page and click **Finish**. Review **the log file for any errors that occurred during the import of the device driver.** Similar to the other Wizards, this page allows you to view the PowerShell code that is run to complete the previous steps.

> **Note:** For more information, refer to the Microsoft Deployment Toolkit Documentation library.

## Demonstration: Creating a Task Sequence

## Detailed demonstration steps

This demonstration shows you how to create a task sequence for a deployment share.

### Create a task sequence for the reference computer

1. In the Deployment Workbench console tree, locate **Deployment Workbench/Deployment Shares/MDT Deployment Share (C:\DeploymentShare)/Task Sequences**.
2. In the Actions pane, click **New Task Sequence**; the New Task Sequence Wizard opens.
3. On the **General Settings** page, set the following: Task sequence ID: **WIN7_REFERENCE** Task sequence name: **Deploy Windows 7 to LON-IMG1** Click **Next**.

   The Task Sequence ID must be unique in a deployment share. Plan your Task Sequence ID carefully because it cannot be modified later. The task sequence name and comments are displayed by the deployment wizard and can be modified at a later time if necessary.
4. On the **Select Template** page, select **Standard Client Task Sequence**, and then click **Next**.

   There are seven available templates. This template is selected because this task involves deploying an OS to a client system. Carefully choose each template and review their purpose.
5. On the **Select OS** page, specify the **Windows 7 Enterprise in Windows 7 x86 install.wim**, and then click **Next**. You can only install Operating Systems that have been previously imported.
6. On the **Specify Product Key** page, click **Next**. The options depend on how the organization is licensed.
7. On the **OS Settings** page, set the following: Full Name: **Admin** Organization: **Contoso LTD**. Click **Next**.

8. On the **Admin Password** page, select the **Do not specify an Administrator password at this time**, and click **Next**. In this case, you are building a reference computer and will not use it in production. If this system is to be deployed into production, you may want to specify a password here or in a custom setup file.
9. On the **Summary** page, click **Next**.
10. On the **Confirmation** page, click **Finish**.

**Note:** For more information, refer to the Microsoft Deployment Toolkit Documentation library.

## Demonstration: Updating a Deployment Share

## Detailed demonstration steps

This demonstration shows you how to update a deployment share.

### Update the deployment share

Updating a deployment share creates the Windows PE boot images (WIM and ISO files) necessary to start the LTI deployment process.

1. In the Deployment Workbench console tree, go to **Deployment Workbench/Deployment Shares/MDT Deployment Share (C:\DeploymentShare)**.
2. In the Actions pane, click **Update Deployment Share**; the Update Deployment Wizard opens.
3. Review the **Options** page and then click **Next**. There are two options available when updating a deployment share. You only need to completely regenerate the boot images if you have changed the Windows PE settings in the deployment share properties.
4. In the Update Deployment Share Wizard, on the **Summary** page, click **Next**.
5. In the Update Deployment Share Wizard, on the **Confirmation** page, click **Finish**. The update takes approximately 10 to 15 minutes.

**Note:** For more information, refer to the Microsoft Deployment Toolkit Documentation library.

# Module Reviews and Takeaways

## Review questions

### Best practices for implementing Lite Touch Installation

- Ensure that you have met the requirements for implementing LTI, which includes a managed network and a file server, and all the software requirements for MDT 2010.
- Ensure that you have sufficient storage space for deployment shares and migration data.
- Use WDS to deploy to network computers and deployment media for computers with slow or no network connectivity.
- For highly scalable LTI environments, implement replication using MDT Database, SQL Server, and Distributed File System (DFS) technologies.

### Best practices for user data considerations

- When you use the refresh computer scenario and have determined the storage requirements for the user state migration data, store your data on the local computer. This reduces the time it takes to deploy Windows and reduces network utilization.
- Consider the security and privacy of the user data and profile in the temporary storage location.

### Tools

| Tool | Used to | Where to find it |
|---|---|---|
| Microsoft Deployment Toolkit (MDT) 2010 | • Deploy Microsoft products to desktops and servers<br>• Create a single path for image creating and automated installation | Microsoft Download Center |
| Microsoft Windows Deployment Services (WDS) | Store both boot and installation images for deployment | Microsoft Download Center |
| Windows Preinstallation Environment (Windows PE) | A minimal operating system environment used to deploy Windows. The AIK includes several tools used to build and configure Windows PE environments. | Microsoft Download Center |
| Deployment Workbench | Administration console for MDT 2010 | Microsoft Deployment Toolkit |
| Windows PowerShell | Provides an environment for performing administrative tasks using cmdlets | Microsoft Deployment Toolkit Windows 7 |
| User State Migration Tool (USMT) | Migrate user settings and data for a large number of computers | Windows AIK |
| Windows Automated Installation Kit (Windows AIK) | Support the deployment of Windows operating system | Microsoft Download Center |

| | | |
|---|---|---|
| Windows 7 installation files | Install Windows or upgrade previous Windows versions | Windows 7 Product DVD |

# Lab Review Questions and Answers

## Lab A: Planning and Configuring MDT 2010

**Question**: What additional components do need to be installed to support Multi-Cast deployments?

**Answer**: Windows Deployment Services. With the release of Windows Server 2008, Windows Deployment Services was enhanced to support the deployment of images using multicast transmissions. MDT 2010 also includes updates to integrate MDT with Windows Deployment Services multicasting.

**Question**: Can a deployment share be created on a remote server?

**Answer**: The deployment share is configured in the MDT with the UNC path to the share. With appropriate rights, the deployment share can be created on a remote server and the local system.

## Lab B: Deploying Windows 7 by Using Lite Touch Installation

**Question**: What are the available Task Sequences and what are they used for?

**Answer**: The default Task Sequences are:

- Standard Client Task Sequence: The default task sequence for deploying operating systems images to client computers.
- Standard Client Replace Task Sequence: Used to performs a system back up, the user state and wipe the disk.
- Custom Task Sequence: Used to create customized Task Sequences that do not install an operating system.
- Standard Server Task Sequence: The default task sequence for deploying operating systems images to server computers.
- Lite-Touch OEM Task Sequence: Used by OEM to deploy Operating Systems in a staging environment.

**Question**: What's the difference between the LTI Bootable Media and the WinPE environment that is created from the WAIK?

**Answer**: The MDT-created WinPE boot media automatically includes all the optional components necessary for imaging. With the WAIK, the administrator is responsible for installing the correct components.

**Question**: What types of applications can be installed with the MDT?

**Answer**: Any application that supports a silent install.

# Module 8

## Deploying Windows® 7 by Using Zero Touch Installation

### Contents:

# Lesson 1

## Designing the Zero Touch Installation Environment

### Contents:

# Question and Answers

## Process of Deploying Windows 7 by Using ZTI

**Question:** What is the main benefit of integrating MDT2010 and Configuration Manager?

**Answer:** The process of creating and implementing new task sequences for deploying operating systems is greatly enhanced by the Import Microsoft Deployment Task Sequence Wizard. MDT 2010 adds new scripts to Configuration Manager.

## Packages and Images Required by the Task Sequence Process

**Question:** What is the purpose of the boot image?

**Answer:** To start the client computer to begin the Zero Touch deployment project.

## Considerations for Designing a ZTI Environment

**Question:** Your network manager is concerned about the over-subscription rate on the closet switches to support your deployment. What technology do you use to ease this concern?

**Answer:** A distribution point stores software packages that are distributed to network clients.

## Discussion: Designing a Zero Touch Installation Environment for a Given Scenario

**Question:** What must you consider when designing your ZTI deployment infrastructure to deploy Windows 7 to all employees in the European offices?

**Answer:** ZTI requires a rationalized or dynamic network infrastructure. In this scenario, you already have the required infrastructure to deploy Windows 7 using ZTI in terms of file servers and a managed network. In addition, your corporate head office has already prepared a standardized image, so you do not need to create a custom image of Windows 7. You need to focus on how to deploy this image efficiently and effectively.

**Question:** How do you deploy the image effectively to the Berlin office to mitigate the slow connection?

**Answer:** Multicasting is a new feature in Configuration Manager. Multicast allows for image deployment with a much reduced network load.

# Lesson 2

## Performing Zero Touch Installation by Using MDT 2010 and Configuration Manager 2007

### Contents:

# Question and Answers

## Demonstration: The Configuration Manager Console

**Question:** To create an Operating System Install Package, what must you first import into the Configuration Manager environment?

**Answer:** You must import the Operating System Images that are to be included in Operating System Install Packages.

## Demonstration: Installing Prerequisite Components for ZTI

**Question:** What are ways that you can help ensure security within your Operating system deployment solution?

**Answer:** You can disable unknown computer support and also require a password for computers to start using PXE.

## Demonstration: Configuring Deployment Packages and Images

**Question:** What other types of packages do you deploy from the Software Distribution node?

**Answer:** Any software that is not specifically part of the Operating System Deployment nodes have to be deployed using software distribution, for example, Microsoft Office.

## Demonstration: Configuring and Advertising Task Sequence

**Question:** What are the final tasks after creating the MDT task sequence?

**Answer:** You need to advertise the task sequence and then make sure that all software distribution packages have been distributed to the required distribution points.

# Detailed Demo Steps

## Demonstration: The Configuration Manager Console

## Detailed demonstration steps

Configuration Manager 2007 is a collection of features that helps you fulfill business requirements. After you deploy the site and install the clients, you must enable Configuration Manager features. Some features can be used individually with little or no dependence on other features. For example, after you enable remote control, start using the Configuration Manager console to control Configuration Manager client computers without additional configuration. Then, configure at least one Configuration Manager distribution point and enable the hardware inventory client agent.

This demonstration provides an introduction to the Configuration Manager Console.

### Overview of the Configuration Manager Console

1. Log on to **LON-SVR1** as **Contoso\Administrator** using the password **Pa$$w0rd**.
2. Click **Start**, point to **All Programs**, click **Microsoft System Center**, and then click **ConfigMgr Console**.
3. In the **Configuration Manager Console**, in the left-hand console pane, expand **Site Database\Site Management\S01 – Contoso\Site Settings** and then click **Boundaries**. Describe the following nodes:
    - **Boundaries**: used to define IP subnets, Active Directory sites, IPv6 prefixes, or IP ranges that must be assigned to the Configuration Manager site. Only clients that are within the Boundary can be managed by Configuration Manager 2007.
    - **Client Agents**: client components that can be enabled, disabled, and configured to perform various tasks within the Configuration Manager environment. For example, the Hardware and Software Inventory Client Agents specify settings related to collecting hardware and software installed on each Configuration Manager client.
    - **Site Systems**: displays the site system roles installed on a specific server. You can add or remove site systems as needed.
4. In the **Configuration Manager Console**, expand **Computer Management** and then click **Collections**. Collections are used to target tasks such as software or software update deployment.
5. In the **Configuration Manager Console**, expand **Operating System Deployment**. Describe the following nodes:
    - **Boot Images**: displays a list of Operating System boot images that have been created. These are Windows PE based images that are used to boot computers during operating system deployment tasks. By default, an x86 and an x64 images is provided. You can add your own custom images as needed.
    - **Computer Association**: helps with two main tasks: migrating user state and settings from a source computer to a destination computer and importing unknown computers into the Configuration Manager database.

- **Operating System Images**: displays a list of the Operating System images that have been added to the Configuration Manager environment. You can add the default WIM file from the Windows media or you can add your own customized WIM files as needed.
- **Operating System Install Packages**: lists the installation packages that have been configured to be deployed to client workstations.
- **Task Sequences**: provides a list of the task sequences that have been created.
- **Drivers**: provides a list of the drivers that have been imported into the Configuration Manager environment.
- **Driver Packages**: provides a list of driver packages that can be deployed to clients. These packages refer to the drivers listed in the Drivers node.
- **Unprovisioned Computers**: lists computers that have been discovered by Configuration Manager as an unknown computer and that do not have the Configuration Manager Client installed.

## Demonstration: Installing Prerequisite Components for ZTI

## Detailed demonstration steps

To prepare the deployment environment to run ZTI with Configuration Manager, complete the following steps:

- Install the PXE Service Point
- Install Configuration Manager
- Install MDT 2010
- Enable Microsoft Deployment integration with the Configuration Manager console in Configuration Manager 2007

### Install the PXE Service Point

During deployment to the target computers, the deployment scripts connect to the deployment point shares and shared folders. Create accounts for the scripts to use when accessing these resources.

Installation of the PXE Service Point occurs in the Distribution Share of the Deployment Workbench. Expand this item to view the operating systems, applications, operating system packages, and out-of-box (OOB) drivers that the distribution share contains. Click any item beneath Distribution Share to view its contents in the details pane.

### Install Configuration Manager

The following checklist is intended to provide a high-level list of items to consider and outlines the steps to take to install the Configuration Manager 2007 R2:

1. Ensure that your computing environment meets the supported configurations required for installing the Configuration Manager 2007 R2 feature update release.
2. Verify that you do not have any unresolved operational issues with the site by checking the site status messages.
3. Install any critical Windows updates on the site server and site systems.
4. Install any critical Microsoft SQL Server updates on the site database server.
5. If you are using SQL Server Database Replication, disable it before upgrading.

6. Back up the site to be upgraded.
7. No additional schema updates are required for Configuration Manager 2007 R2. However, if you have not already extended your schema for Configuration Manager 2007, consider the benefits of extending it.
8. Restart the site server and site systems to ensure that there are no pending actions from installing updates or prerequisites.
9. Run Configuration Manager 2007 R2 Setup from the Configuration Manager installation media from a copy of the installation media located on a network shared folder, or other storage media, to start the Configuration Manager R2 Setup Wizard.

After installing the Configuration Manager 2007 R2 feature update release on the primary site server, Configuration Manager 2007 R2 Setup must be run on secondary site server computers and on any associated Configuration Manager consoles to allow Configuration Manager 2007 R2 features to be displayed.

### Install MDT

In most instances, MDT will already be installed on the deployment server. In instances where this task has not yet been completed, install MDT. For integrated Configuration Manager support with Deployment Workbench, install MDT on each computer that is running the Configuration Manager console. This allows you to run the Configuration Manager 2007 Integration option and specify data for MDT packages.

Configure the appropriate processing rules based on the environment in the MDT database. The ZTI deployment process uses rules defined in the MDT database to configure target computers.

### Enable the Configuration Manager Console integration

Before the deployment team can use the Configuration Manager integration features of Microsoft Deployment, run the Configure Configuration Manager 2007 Integration script. The script copies the appropriate Configuration Manager integration files to the Configuration Manager root (where Configuration Manager root is the folder in which Configuration Manager is installed). The script also adds Windows Management Instrumentation (WMI) classes for MDT custom actions. The classes are added by compiling a new Managed Object Format (MOF) file that contains the new class definitions.

This demonstration shows how to install and configure MDT 2010 and the PXE Service Point.

### Install MDT 2010

MDT is available for x86 and x64 environments. The 64-bit version is used in this demonstration. The setup includes tools and documentation on how to use the tool.

1. Log on to **LON-SVR1** as **Contoso\Administrator** using the password **Pa$$w0rd**.
2. Click **Start**, and then click **Run**.
3. In the **Run** box, type **\\LON-DC1\Labfiles\MDT\**, and then click **OK**.
4. In the **MDT** window, double-click **MicrosoftDeploymentToolkit2010_x64**.
5. In the **Open File – Security Warning** box, click **Run**. The **Setup Wizard** starts.
6. On the **Welcome** page, click **Next**.
7. On the **End-User License Agreement** page, click the option next to **I accept the terms in the License Agreement**, and then click **Next**.
8. On the **Custom Setup** page, accept the default settings, and then click **Next**.

9. On the **Ready to Install** page, click **Install**.
10. On the **Completing the Microsoft Deployment Toolkit 2010 Setup Wizard** page, click **Finish**.
11. Close the **MDT** window.
12. On **LON-SVR1**, click **Start**, point to **All Programs**, click **Microsoft Deployment Toolkit**, and then click **Configure ConfigMgr Integration**. The ConfigMgr extension files are used to provide MDT functionality to the Configuration Manager console.
13. On the **Options** box, ensure that **Install the ConfigMgr extensions** is selected with the following options, and then click **Next**.
    - Site Server Name**: LON-SVR1**
    - Site code**: S01**

### Install the WDS server role

WDS is required to provide the PXE boot capabilities of ZTI. You can install the server role using the Server Manager in Windows Server 2008. Once WDS is installed, all configuration settings take place from within Configuration Manager 2007. You do not configure any WDS settings from within the WDS console.

1. On **LON-SVR1**, click **Server Manager** in the task bar.
2. In the **console** pane, click **Roles**.
3. In the **details** pane, click **Add Roles**; the **Add Roles Wizard** starts.
4. On the **Before You Begin** page, click **Next**.
5. On the **Select Server Roles** page, select **WDS check box**, and then click **Next**.
6. On the **Overview of WDS** page, click **Next**.
7. On the **Select Role Services** page, accept the default selections, and then click **Next**.
8. On the **Confirm Installation Selections** page, click **Install**.
9. On the **Installation Results** page, click **Close**.
10. Close the **Server Manager**.

### Configure the PXE Service Point role

The PXE Service point role takes over the WDS installation and provides PXE boot services for clients.

1. On **LON-SVR1**, click **Start**, point to **All Programs**, click **Microsoft System Center**, click **Configuration Manager 2007**, and then click **ConfigMgr Console**.
2. In the **console** pane, expand **Site Database (S01 – SEA-SVR1, Contoso)**, and then expand **Site Management\S01 - Contoso\Site Settings**.
3. In the **console** pane, expand the **Site Systems** node.
4. In the **console** pane, click **\\LON-SVR1**, and then take note of the configured roles on the server. The PXE service point role needs to be installed to support PXE boot requests.
5. In the **console** pane, right-click **\\LON-SVR1** and then click **New Roles**; the New Site Role Wizard starts.

6. On the **General** page, ensure that **Specify a fully qualified domain name** is selected, and that **LON-SVR1.CONTOSO.COM** is entered in the **Intranet FQDN** text box. Leave all other default selections, and then click **Next**.
7. On the **System Role Selection** page, select the check box next to **PXE service point**, and then click **Next**.
8. On the **PXE Service Point Configuration** box, click **Yes** to open the required ports.
9. On the **PXE – General** page, configure the following, and then click **Next**:
    - Allow this PXE service point to respond to incoming requests: **Enabled This option enables and disables the PXE service point.**
    - Enable unknown computer support: **Enabled This option provides the ability for computers that have not been imported into the Configuration Manager database to still be installed.** If you do not turn on this feature, use the Computer Association node to import computer names and references.
    - Require a password for computers to boot using PXE: **Not Enabled This option enables or disables the requirement to need a password before computers can use PXE.**
    - Respond to PXE requests on all network interfaces: **Selected**
    - Delay (seconds): **0**
10. On the **PXE – Database** page, leave all default settings and then click **Next**.
11. On the **Summary** page, click **Next**.
    - On the **Wizard Completed** page, click **Close**.

## Demonstration: Configuring Deployment Packages and Images

## Detailed demonstration steps

Zero Touch deployment uses a number of images and packages during the deployment process. The images that are used by the ZTI process include:

- Boot images that are used to initiate the ZTI deployment process.
- Images of the operating system to be deployed to the target computers

Additional packages may be needed, depending on your ZTI scenario. These packages include:

- **Deployment files package**: the files used from the distribution share directory are the scripts and control files
- **Client package**: Configuration Manager client installation files
- **Device driver package**: distribution of drivers to distribution points
- **USMT package**: files used to capture and restore user state
- **Custom settings package**: unattended files and customsettings.ini
- **Sysprep files package**: Sysprep files

### Add boot and operating system images and packages

The operating system WIM files you import can be used as part of an operating system deployment task sequence. You can add operating system install packages for use with your setup-initiated operating system deployments. The operating system install packages can be copied to distribution points so that they are available for Configuration Manager 2007 computers to install them.

Configuration Manager R2 SP2 provides two initial boot images that can be used for basic operating system deployments. You can also import your own custom boot images and deploy them as required.

For both boot images, you have to ensure that they are available on all distribution points, including the WDS-related distribution point.

The steps for deploying a boot image with the Configuration Manager Console are as follows:

1. In the **console** pane, expand **Computer Management\Operating System Deployment**, and then click **Boot Images**. Notice that default boot images are already available for x86 and x64 installations.
2. In the **console** pane, expand the **Boot Images** node, and then expand the **Boot image (x86)** node.
3. Under the **Boot image (x86)** node, right-click **Distribution Points**, and then click **New Distribution Points**; the **New Distribution Points Wizard** starts.
4. On the **Welcome** page, click **Next**.
5. On the **Copy Package** page, select the check box next to **LON-SVR1** and **LON-SVR1\SMSPXEIMAGES$**, and then click **Next**.
6. On the **Wizard Completed** page, click **Close**.
7. Repeat steps 2-6 for **Boot image (x64)**.
8. Under **Boot image (x86)** expand **Package Status** and then click the **Package Status** folder. This folder is used to provide details on the state of the package distribution.

### Add drivers and driver packages

You can import device drivers for use in your Configuration Manager 2007 site. Imported device drivers can be added to boot image packages or driver packages and can be installed as part of an Operating System Deployment task sequence using the Auto Apply Driver and Apply Driver Package task sequence steps.

Configuration Manager 2007 reads the provider, class, version, signature, supported hardware, and supported platform information associated with the device as part of the import process. By default, the driver is named after the first hardware device it supports, however the device driver can be renamed later. The supported platforms list is determined based on the device driver's definition. However, the accuracy of this can vary; therefore, manually verify if the device driver is supported after it has been imported.

A driver package contains the content associated with one or more device drivers. Device drivers must to be added to a driver package and copied to a distribution point before Configuration Manager 2007 clients can install them.

Driver packages that are made available to Microsoft Windows 7-based Configuration Manager 2007 clients must not contain more than 150 device drivers in a single driver package.

You can view the associated general, data source, distribution point, data access, and security information for the driver package by right-clicking the driver package and then clicking Properties. You can add Windows device drivers that have been imported into the driver catalog to an existing driver package.

You can add new device drivers to an existing operating system image by using the task sequence editor. To allow Configuration Manager 2007 to search in the driver catalog for the new device drivers, add the Auto Apply Drivers task sequence step to an existing task sequence. The Auto Apply Driver task sequence step searches existing driver categories for the most appropriate device driver to install with the operating system deployment. Configuration Manager 2007 looks in all available categories for the device driver. The Configuration Manager 2007 system account must have read/write permissions to the specified driver package source location.

### Configuration Manager client package

The client package contains Configuration Manager client installation files. You can install Configuration Manager 2007 client software on desktop and laptop computers. In addition, you can install Configuration Manager 2007 client software on server computers and manage them as clients of Configuration Manager 2007. While servers often have specific operational requirements, for example, the times you are allowed to restart server computers might be more limited than desktop computers, Configuration Manager 2007 makes no functional distinction between server or client computers.

Client computers typically connect into the organization network directly, either by being attached directly to the network or by using VPN or dial-up access. In Configuration Manager 2007, client computers can also be managed by Configuration Manager 2007 sites if they have a connection to the Internet but never connect directly to the organization network. For example, a home-based worker can be managed by Configuration Manager 2007 without ever dialing into the corporate network. These clients are called Internet-based clients, and they require additional infrastructure support.

Use the CCMSetup.exe command to manually install the Configuration Manager 2007 client software onto computers in your enterprise.

### Add operating system images

Before deploying an operating system, add the operating system images to Configuration Manager. You can either add the default WIM from the Windows media or add your own custom WIM files.

1. In the **console** pane, right-click **Operating System Images**, and then click **Add Operating System Image**; the **Add Operating System Image Wizard** starts.
2. On the **Data Source** page, under **Path**, type **\\LON-DC1\Labfiles\Source\sources\install.wim**, and then click **Next**.
3. On the **General** page, fill in the following information, and then click **Next**:
    - Name: **Windows 7 ENTERPRISE**
    - Version: **RTM**
    - Comment: <Current date>
4. On the **Summary** page, click **Next**.
5. On the **Wizard Completed** page, click **Close**.
6. After adding the operating system image, you need to deploy the image to the distribution points. You only need to deploy the image to the standard distribution point. There is no need to deploy the image to the WDS distribution point.
7. In the **console** pane, expand the **Operating System Images** node, and then expand the **Windows 7 ENTERPRISE** node.

8. Under the **Windows 7 ENTERPRISE** node, right-click **Distribution Points**, and then click **New Distribution Points**; the **New Distribution Points Wizard** starts.
9. On the **Welcome** page click **Next**.
10. On the **Copy Package** page, select **LON-SVR1**, and then click **Next**. (Do not select LON-SVR1\SMSPXEIMAGES$ because this is the PXE boot distribution point.)
11. On the **Wizard Completed** page, click **Close**.

### Add operating system install packages

To deploy an operating system that is available in the Operating System Images node, you need to create an Operating System Install Package.

1. In the **console** pane, click the **Operating System Install Packages** node.
2. Right-click **Operating System Install Packages**, and then click **Add Operating System Install Package**; the **Add Operating System Install Package Wizard** starts.
3. On the **Data Source** page, under Source Directory, type **\\LON-DC1\Labfiles\Source\**, and then click **Next**.
4. On the **General** page, fill in the following information, and then click **Next**:
    - Name: **Windows 7 ENTERPRISE**
    - Version: **RTM**
    - Comment: <*Current date*>
5. On the **Summary** page, click **Next**.
6. On the **Wizard Completed** page, click **Close**. Again, you need to deploy the package to all standard distribution points.
7. In the **console** pane, expand the **Operating System Install Packages** node, and then expand the **Windows 7 ENTERPRISE** node.
8. Under the **Windows 7 ENTERPRISE** node, right-click **Distribution Points**, and then click **New Distribution Points**; the **New Distribution Points Wizard** starts.
9. On the **Welcome** page, click **Next**.
10. On the **Copy Package** page, select **LON-SVR1**, and then click **Next**. (Do not select **LON-SVR1\SMSPXEIMAGES$** because this is the PXE boot distribution point.)
11. On the **Wizard Completed** page, click **Close**.

    If you have any additional drivers that need to be deployed to the operating system, you can add the drivers to the **Drivers** node and then create a **Driver Package**. The process is similar to what has been demonstrated for the other packages.

### Adding the Configuration Manager client package

There may be some packages that you need to deploy as standard software distribution packages. One such package is the Configuration Manager Client Package:

1. On **LON-SVR1**, in the **Configuration Manager Console**, expand **Computer Management\Software Distribution**, and then click **Packages**.
2. Right-click **Packages**, point to **New**, and then click **Package from Definition**.

3. On the **Welcome** page, click **Next**.
4. On the **Package Definition** page, select **Configuration Manager Client Upgrade**, and then click **Next**.
5. On the **Source Files** page, select **Always obtain files from a source directory**, and then click **Next**.
6. On the **Source Directory** page, under **Source directory**, type **\\LON-SVR1\SMS_S01\Client**, and then click **Next**.
7. On the **Summary** page, click **Finish**. The Configuration Manager Client Upgrade package is now visible in the **details** pane.
8. In the **console** pane, expand the **Packages** node, and then expand the **Microsoft** Configuration Manager **Client Upgrade 4.0 ALL** node.
9. Under the **Configuration Manager Client Upgrade 4.0 ALL** node, right-click **Distribution Points**, and then click **New Distribution Points**; the **New Distribution Points Wizard** starts.
10. On the **Welcome** page, click **Next**.
11. On the **Copy Package** page, select **LON-SVR1**, and then click **Next**. (Do not select **LON-SVR1\SMSPXEIMAGES$** because this is the PXE boot distribution point.)
12. On the **Wizard Completed** page, click **Close**.

## Demonstration: Configuring and Advertising Task Sequence

## Detailed demonstration steps

You can create a task sequence to deploy an existing operating system image to a target computer, and you can modify the task sequence after it is created. The boot image you specify must match the chip architecture installed on the target computer or the task sequence fails.

### Type of task sequence templates

Task sequences are created by the Task Sequence Editor and consist of a combined series of steps that are designed to complete an action. Task sequences can operate across a computer restart and can be configured to automate tasks on a computer without requiring user intervention. In addition, task sequence steps can be added to a task sequence group, which help keep similar task sequence steps together for better organization and error control. The following Task Sequence Templates are available for Zero Touch Deployment:

- **Apply Network Settings**: configures the network adapter on the target computer.
- **Configure ADDS**: configures the target computer as an Active Directory directory service domain controller.
- **Enable BitLocker**: configures BitLocker™ Drive Encryption on the target computer.
- **Format and Partition Disk**: partitions and formats disks on the target computer.
- **Gather**: gathers data and processing rules for the target computer.
- **Install Application**: installs applications on the target computer.
- **Install Operating System**: installs an operating system on the target computer.
- **Install Roles**: installs the selected roles and features on the target computer.

- **Install Updates Offline**: installs updates to the image on the target computer after the operating system has been deployed, but before the target computer has been restarted.
- **Restart Computer**: restarts the target computer.
- **Run Command Line**: runs the specified command line on the target computer.
- **Run Command Line As**: runs the specified command line on the target computer and does so while impersonating the specified user.
- **Set Task Sequence Variable**: sets the specified task sequence variable to the specified value.
- **Validate**: validates that the target computer meets the specified deployment prerequisite conditions.

Task sequence template files that can be imported into Configuration Manager from MDT include:

- **Standard Client Task Sequence**: use for deploying client operating systems.
- **Standard Server Task Sequence**: use for deploying server operating systems.
- **Standard Client Replace Task Sequence**: use to capture the user state data from an existing computer so that it can be restored on a user's new destination computer.
- **Custom Task Sequence**: use to install applications and can be customized to perform additional actions.

## Advertize task sequences

Configuration Manager Task Sequences must be advertised explicitly for initiating deployments. This is unlike MDT task sequences, which can be advertised as the last step of the wizard that is used to configure them. In Configuration Manager, advertise task sequences to collections by using the New Advertisement wizard.

Before you run the New Advertisement Wizard, know the collections and desired run-time behavior you want for the advertisement. Read access to the task sequence is required and the task sequence must exist prior to creating the advertisement. When you have created a successful advertisement, it is located under the Software Distribution/Advertisements node.

> **Note:** Task sequence advertisement names do not need to be unique; you can assign the same name to more than one task sequence advertisement.

This demonstration shows how to configure boot and operating system images and packages.

## Overview of Configuration Manager task sequence options

The Task Sequence Wizard provides a number of task sequence types that can be created.

1. In the **console** pane, expand **Computer Management\Operating System Deployment**, and then click **Task Sequences**.
2. Right-click **Task Sequences**, point to **New** and then click **Task Sequence**.
3. Explain the following as you click each option:
    - **Install an existing image package**: provides default steps to install and configure an image. Notice the high-level tasks in the wizard step list on the left-hand side of the dialog box.

- **Build and capture a reference operating system image**: provides defaults for installing and then capturing a reference operating system. Use this reference image to deploy to other clients.
- **Create a new custom task sequence**: opens the task sequence editor and allows you to create your own task sequences.

### Creating the Microsoft deployment task sequence

This option uses the integrated MDT functionality to create task sequences based upon the ones available from within MDT 2010. The Wizard automatically does the following:

- Associates a boot image
- Creates a package that contains the required MDT files
- Associates an operating system image
- Associates or creates a client package
- Associates and creates a USMT package
- Configures Sysprep options

1. In the **console** pane, expand **Computer Management\Operating System Deployment**, and then click **Task Sequences**.
2. Right-click **Task Sequences**, and then click **Create Microsoft Deployment Task Sequence**.
3. On the **Choose Template** page, select **Client Task Sequence**, and then click **Next**.
4. On the **General** page, fill in the following information, and then click **Next**:
   - Task sequence name: **Windows 7**
   - Task sequence comments: <*Current Date*>
5. On the **Details** page, fill in the following information, and then click **Next:**
   - Join a domain: **Selected**
   - Domain: **Contoso.com**
   - Account: Username: **Contoso\Administrator** Password: **Pa$$w0rd**
     - User name: **Client1**
     - Organization name: **Contoso**
6. On the **Capture Settings** page, select **This task sequence may be used to capture an image**, configure the following settings, and then click Next:
   - Capture destination: **\\LON-DC1\Labfiles\Source\Win7.wim**
   - Capture account: Username: **Contoso\Administrator** Password: **Pa$$w0rd**
7. On the **Boot Image** page, ensure that **Specify an existing boot image package** is selected, and then click **Browse**.
8. On the **Select a Package** dialog box, select **Boot image (x86)**, click **OK**, and then click **Next**.
9. On the **MDT Package** page, select **Create a new Microsoft Deployment Toolkit Files package**.

10. In the **Package source folder to be created** field, type **\\LON-DC1\Labfiles\MDTFiles**, and then click **Next**.
11. On the **MDT Details** page, fill in the following information, and then click **Next**:
    - Name: **MDT Source Files**
    - Version: **1.0**
    - Language: **English**
    - Manufacturer: **Microsoft**
    - Comments: **<Current date>**
12. On the **OS Image** page, select **Specify an existing OS install package**, and then click **Browse**.
13. On the **Select a Package** dialog box, select **Windows 7 ENTERPRISE**, click **OK**, and then click **Next**.
14. On the **Client Package** page, ensure that **Specify an existing ConfigMgr client package** is selected, and then click **Browse**.
15. On the **Select a Package** dialog box, select **Configuration Manager Client Upgrade**, click **OK**, and then click **Next**.
16. On the **USMT Package** page, select **Create a new USMT package**.
17. Under **Path to USMT executables and related files**, ensure that **C:\Program Files\Windows AIK\tools\USMT** is entered.
18. Under **Package source folder to be created**, type **\\LON-DC1\Labfiles\USMT**, and then click **Next**.
19. On the **USMT Details** page, fill in the following information, and then click **Next**:
    - Name: **MDT USMT Package**
    - Version: **1.0**
    - Language: **English**
    - Manufacturer: **Microsoft**
    - Comments: <*Current date*>
20. On the **Settings Package** page, select **Create a new settings package**.
21. In the **Package source folder to be created** field, type **\\LON-DC1\Labfiles\MDTFiles**, and then click **Next**.
22. On the **Settings Details** page, fill in the following information, and then click **Next:**
    - Name: **MDT Settings Files**
    - Version: **1.0**
    - Language: **English**
    - Manufacturer: **Microsoft**
    - Comments: <*Current date*>
23. On the **Sysprep Package** page, select **No Sysprep package is required**, and then click **Next**.

24. On the **Summary** page, click **Next**.
25. After the wizard is finished, click the **Task Sequences** node, and then right-click **Windows 7**. Click **Edit and** take note of—but do not change—the various tasks that make up the Windows Vista task sequence.
26. Click **Cancel** to close the Windows Vista Task Sequence Editor.

# Module Reviews and Takeaways

## Review questions

1. You have decided to migrate user settings and data, but you need to determine how much storage is required for the migration data. What tool do you use to do this?
2. How can you run the Configuration Manager 2007 Integration option and specify data for MDT packages?
3. What kind of infrastructure model is required by Zero Touch?

## Review answers

1. Run **Scanstate.exe** in the USMT with the **/p** option to estimate the size of the user state migration data. By using the **/p** option, you can estimate the disk space requirements without actually performing the migration.
2. For integrated Configuration Manager support with Deployment Workbench, install MDT 2010 on each computer that is running the Configuration Manager console.
3. A ZTI solution requires an in-place rationalized or dynamic network infrastructure which includes the prerequisite components.

### Common issues related to Zero Touch Deployment

Identify the causes for the following common issues related to Zero Touch Deployment.

| Issue | Troubleshooting tip |
|---|---|
| The Operating System Images Zero Touch deployment is pushing out to the clients at a new division do not recognize the video card in the target computers. | Update the Video Driver in the Device Drivers Package |
| You have obtained the correct drivers for the video card but you are unable to update the distribution point from the Configuration Manager Console. | To update a package on its associated distribution points, you must have Distribute permission for the Package Security object type or for the specific package instance. |
| You have configured Zero Touch deployment to a hardware refresh at a division in the enterprise. Users report that the deployed image cannot start. | You must assign the PXE service point site role to a server that is supported by Configuration Manager 2007 operating system deployment. |
| You need to configure a Zero Touch deployment using a remote Configuration Manager Console. You are unable to access the Console. | You must have Local Administrator credentials on the Remote Configuration Manager Console |

### Best practices related to zero touch deployment

The TechNet Desktop Deployment Center is structured around the Microsoft Solution Accelerator for Business Desktop Deployment (BDD) 2007. BDD 2007 is the recommended best practice methodology for consistent, repeatable, and cost-effective deployments. BDD delivers end-to-end guidance to efficiently plan, build, test, and deploy operating systems and applications. Microsoft has been working with leading deployment partners to enhance and develop this industry guidance in addition to providing Microsoft's implementations of BDD methodology.

While Configuration Manager provides technology for performing desktop deployment, its larger focus is on methodology and best practices. Microsoft solutions, such as System Center Configuration Manager, are implementations of industry-standard methodologies and best practices. These solutions provide opportunities for Microsoft partners and independent software vendors (ISVs) to learn how to build their own solutions too. Deployment is not just a Microsoft standard but is also becoming an industry standard with the input that Microsoft partners and ISVs provide.

By following the guidance in System Center Configuration Manager, you are implementing these methodologies and best practices to manage complex projects. Configuration Manager enables you to build best practice oriented solutions to do the following:

- Manage teams and processes to produce a comprehensive and integrated deployment based on technology solutions.
- Set up lab and test environments that the development teams share.
- Create software and hardware inventories for deployment planning.
- Test applications for compatibility with Windows 7 and mitigate the compatibility issues discovered during the process.
- Automate applications' installations, customize their configurations, and repackage applications, if necessary, to achieve a fully automated installation.
- Develop strategies and solutions for migrating users' documents and settings.
- Create an automated process for developing and deploying computer images.
- Develop an imaging strategy that requires fewer flexible images to deploy dynamic builds to destination computers.
- Deploy computer images using Lite Touch and Zero Touch solutions; deploy computer images remotely to branch offices and mobile users.
- Harden deployment servers and computer images against security threats.
- Disable antivirus programs on the lab computer before capturing an image of the lab computer's disk.

  Antivirus programs can interfere with the configuration of the image and installation of applications during deployment.

  After deployment, enable the antivirus program. Test the interaction of antivirus programs with System Center Configuration Manager.

### Decide whether clients must download content if they are on a slow or unreliable network boundary

The default for every Configuration Manager 2007 advertisement and software update deployment is to not download software packages and software updates when the client is connected within a slow or unreliable network boundary. This default assumes that you do not want clients downloading content over slow or unreliable network connections, thereby saving network bandwidth.

However, in some scenarios, this default setting might unexpectedly prevent clients from installing the software packages and software updates that you want them to have. Consider changing this default if you want to ensure that clients always install software packages and software updates when requested and if any of the following scenarios apply:

- Clients are not within a configured boundary for their assigned site because boundaries are not configured correctly or because the clients have been incorrectly assigned.

  In this scenario, clients never install the software package or software updates. For these clients to install the software package or software update with the default configuration, all boundaries must be configured correctly.

- Clients are within a boundary that is configured as slow or unreliable, such as a virtual private network (VPN) or wireless network.

  In this scenario, clients are not able to install the software package or software updates unless their network location changes to a fast and reliable boundary. Alternatively, reconfigure the slow or unreliable boundary to be fast and reliable.

- Clients have roamed into another site that does not host the content.

  In this scenario, clients are not able to install the software package or software updates until they return to their assigned site.

### Choose between updating and refreshing a package

Updating and refreshing Microsoft System Center Configuration Manager 2007 packages are two different operations. Use the following table to help decide when to update and when to refresh a package.

| Criterion | Package Update | Package Refresh |
|---|---|---|
| Use when | You make a modification to the package source, such as adding, changing, or deleting a file or folder. | You need to repair a package at a specific distribution point. |
| What it does | Builds a new, complete, compressed package file and a delta compressed package file from the updated package source files. The delta file is passed to all distribution points. | Recopies the compressed package from the local site server to the distribution point but does not copy files from the package source. |
| Resets access control list (ACL) | No. | Yes, if you have made changes to the Package Access Accounts. |
| Resets the Virtual Directory | Yes, if you have enabled or disabled BITS on the distribution point since the last package update. | Yes, if you have enabled or disabled BITS on the distribution point since the last package refresh. |
| Updates the package source version | Yes. | No. |
| Increments package version in client policy | Yes | No |

## Tools

| Tool | Use for | Where to find it |
|---|---|---|
| MDT 2010 | Integration to Configuration Manger 2007 and provision of deployment templates | http://go.microsoft.com/fwlink/?LinkID=160877 |
| Configuration Manager 2007 | Manages Zero Touch deployment projects | http://go.microsoft.com/fwlink/?LinkID=162645 |
| USMT 4.0 | Migrates user profiles to a new computer | http://go.microsoft.com/fwlink/?LinkID=140374 |
| Sysprep | Prepares files for a package | http://go.microsoft.com/fwlink/?LinkID=156807 |
| AD DS | Finds the Configuration Manager management points and stores metadata for the deployment | http://go.microsoft.com/fwlink/?LinkID=162646 |

# Lab Review Questions and Answers

**Question**: When do you use the SMSPXEIMAGES$ distribution point option?

**Answer**: You only need to use this option when distributing the boot images and boot image packages. Standard packages do not have to be placed on this location.

**Question**: What is the PXE service point and what is it used for?

**Answer**: The PXE service point is required if you want to enable computers to start over the network. It uses the Windows Deployment Services components to allow PXE booting.

**Question**: You attempt to import the Microsoft Deployment Task Sequence, and cannot see the option in Configuration Manager. What do you do?

**Answer**: Run the **Configure ConfigMgr Integration** command from the **Microsoft Deployment Toolkit** Program Group.

# Module 9

## Migrating User State by Using WET and USMT 4.0

### Contents:

# Lesson 1

## Designing the Zero Touch Installation Environment

### Contents:

# Question and Answers

## Tools for Migrating User State

**Question:** How do you migrate applications to Windows 7?

**Answer:** You can migrate application settings, but you cannot migrate the application itself. You have to re-install your applications on the destination computer before you restore the application settings on that computer.

# Lesson 3

## Planning User State Migration (USMT 4.0)

### Contents:

# Question and Answers

## Determining What to Migrate

**Question:** How do you decide which application settings to migrate?

**Answer:** The answer may vary. Generally, you must migrate settings for all supported applications in your organization. But this may not always be possible, or even practical. Refer to the “Identify Application Settings” topic and further discuss what application settings you will migrate in your organization.

## Choosing a Migration Store Type and Location

**Question:** Which migration store best suits your organization?

**Answer:** The answer may vary, but generally, if the scenario and other conditions permit, use the new hard-link migration store to take advantage of the storage space and the migration performance.

## Lesson 4

# Migrating User State by Using USMT 4.0

### Contents:

# Question and Answers

## Capturing User State by Using ScanState

**Question:** Where will the scanned user state results be stored?

**Answer:** Results will be stored at \\SEA-DC1\DesktopMigration.

**Question:** Which parts of the syntax controls application settings and user settings?

**Answer:** The **/i:migapp.xml** and the **/i:miguser.xml** control application and user settings.

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

**Answer:** The **/ue:Contoso\Don** excludes the user account Don from migrating.

## Restoring User State by Using LoadState

**Question:** Where will the user state be retrieved from?

**Answer:** The user state will be retrieved from \\SEA-DC1\DesktopMigration.

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

**Answer:** The **/ui:DBService** command includes migrating an account named DBservice.

**Question:** What will happen if the **/lae** switch was not provided in this example?

**Answer:** The DBService account will be created and then disabled. The /**lae** switch enabled the account.

# Module Reviews and Takeaways

## Review questions

1. List three main considerations when you are planning a user state migration task.
2. You must estimate the size of the stored user state on the network server. Which USMT tool can provide this estimate?
3. You must modify the operating system elements that are transferred from a Windows XP computer to a Windows Vista computer. Which USMT file do you modify?
4. You must secure the data store that is generated with USMT. What can you do to accomplish this task?
5. Which files can be modified during a user state migration by using USMT 4.0?
6. You migrated a user account to a new computer by using the /lac option. However, when attempting to log on, the user receives an error message and is prevented from logging on to the computer. What is the most likely cause of the issue?

## Review answers

1. Planning considerations may include: which settings and features to migrate, how much space is required to store and migrate the data, and how the data will be secure.
2. You can use the ScanState tool with the /p switch to generate an estimate of the transferred used state.
3. You must create and modify a custom Config.xml file. Windows Vista does not use the MigSys.xml file.
4. You can use ScanState to encrypt the store by using the /encrypt option.
5. You can modify MigUser.xml, MigApp.xml, and MigDoc.xml. In addition, you can create and modify a Config.xml or custom XML file if you want to exclude some elements from the migration, and/or if you want to modify files and folders that are to be migrated to a computer that is running Windows 7.
6. You most likely migrated the account as a disabled account. Use the /lae option to ensure that the account is enabled during the migration.

## Best practices related to scenarios and migration store size

1. **Local store versus remote store**: if you select the refresh computer scenario and there is enough space on the local computer, the best option is to store the user state data on a local device. This reduces server storage costs and eliminates network performance issues. If you select the replace computer scenario, or have insufficient space on the local computer, then you must store the user state data remotely.
2. **Estimate migration store size**: a good method for determining how much space you have to store the migrated data is to base your calculations on the volume of e-mail, personal documents, and system settings for each user. You can survey several computers to arrive at an average for the size of the store that you will need.

## Best practices related to the use of USMT 4.0

- Install applications before you run the LoadState tool

- Do not use MigUser.xml and MigDocs.xml together
- Close all applications before running either the ScanState or LoadState tools
- Log off after running the LoadState tool
- Create a managed environment
- Run Chkdsk.exe before running the ScanState and LoadState tools
- Migrate in groups and phases if users are using the network

## Summary of security best practices

Best practices for maintaining privacy and security of your users during migration are summarized in the following:

- **Encrypting File System (EFS)**: migrate encrypted files with caution, because the end-user does not have to be logged on to capture the user state. (By default, USMT 4.0 fails if an encrypted file is found.)
- **Encrypt the store**: consider using the **/encrypt** option with the ScanState command and the **/decrypt** option with the LoadState command. However, be careful with these options, because anyone who has access to the ScanState command-line script also has access to the encryption key.
- **Virus scan**: run an antivirus utility on the source and destination computers before migration.
- **Maintain security of the file server and the deployment server**: transmit data over a secure Internet connection, such as a virtual private network.
- **Password migration**: be sure end-users know their passwords because USMT does not migrate passwords to ensure user privacy.

## Tools

| Tool | Use for | Where to find it |
|---|---|---|
| Windows® Easy Transfer (WET) | Use to perform migration for a single computer or only a few computers. | Windows 7 product DVD |
| Windows Pre-installation Environment (Windows PE) | A minimal operating system environment used to deploy Windows. | Windows AIK |
| User State Migration Tool (USMT) | Use to migrate user data from previous Windows operating system to Windows 7 for multiple computers. | Windows AIK |

# Lab Review Questions and Answers

## Lab A: Migrate User State by Using WET (Optional)

**Question**: You decide to use WET to migrate application settings from an old computer to a new Windows 7 computer. After the migration, you cannot find the application on your new computer. What do you need to do?

**Answer**: WET only migrates application settings, not the application itself. Install the application on the new computer before performing the user state migration.

**Question**: After migrating the user state of a local user account, the user discovers that he or she cannot log on using the old password. What is wrong?

**Answer**: Local user account passwords are not migrated. The user will be forced to change the password during the logon.

## Lab B: Migrating User State by Using USMT 4.0

**Question**: You migrated a user account to a new computer using the /lac option. However, when attempting to log on, the user receives an error message and is prevented from logging on to the computer. What is the most likely cause of the issue?

**Answer**: You most likely migrated the account as a disabled account. Use the /lae option to ensure that the account is enabled during the migration.

**Question**: You must secure the data store that is generated with USMT. What can you do to accomplish this task?

**Answer**: You can use ScanState to encrypt the store by using the /encrypt option.

**Question**: You must estimate the size of the stored user state on the network server. Which USMT tool can provide this estimate?

**Answer**: You can use the ScanState tool with the /p switch to generate an estimate of the transferred user state.

## Lab C: Migrating User State Using Hard-Link Migration

**Question**: Which command-line option is used to specify a hard-link migration?

**Answer**: The /hard-link command line option is used to specify a hard-link migration store.

**Question**: Which migration scenario supports hard-link migration?

**Answer**: Only the computer refresh scenario supports hard-link migration.

# Module 10

## Designing, Configuring, and Managing the Client Environment

### Contents:

# Lesson 1

## Overview of Planning Client Configuration

### Contents:

# Question and Answers

## Methods for Implementing Client Configuration

**Question:** Which type of settings provides an unmanaged method of client configuration that allows users to change system settings?

**Answer:** Group Policy Preferences

## Discussion: Advantages and Disadvantages of Client Configuration Implementation Methods

**Question:** Your organization recently modified its virtual private networking (VPN) connection. You are asked to automatically modify the VPN connection information for each laptop to reflect this corporate change. Which client configuration method is best suited for accomplishing this task?

**Answer:** Group Policy preferences provide the best method for configuring VPN connections. The Network Options preference extension can be used to configure Virtual Private Network (VPN) connections, including their options, security settings, and connection type.

**Question:** Your organization has several stand-alone Windows 7 client workstations that are not part of its Active Directory domain. You are asked to set the Account Lockout Threshold setting for each of these workstations to three invalid logon attempts. Which client configuration method is best suited to address this request?

**Answer:** Local Group Policy is the best method for configuring standalone workstations. The Account Lockout Threshold is a security setting located under the Windows Settings category in the Local Group Policy Editor.

**Question:** For each of your organization's user accounts, you are asked to perform the following tasks based on the user's group membership: If the user belongs to the Engineering, Finance, or Human Resources group, then map the user's G drive to the group shared drive, and set the user's default printer to be the group printer. Which client configuration method is best suited to accomplish this request?

**Answer:** Setting a default printer and mapping a computer drive for specific user accounts is best suited to Group Policy Settings instead of Group Policy Preferences. By using Group Policy Settings, these domain-based policies cannot be changed by the end users.

# Lesson 2

## Designing and Configuring Standard System Settings

### Contents:

# Question and Answers

## Demonstration: Configuring the Standard System Settings by Using Local Policies

**Question:** The Local Group Policy Editor is used in this demonstration. What other tool can you use to configure multiple computers in a single step?

**Answer:** Group Policy Management Console (GPMC) from a domain controller.

# Detailed Demo Steps

## Demonstration: Configuring the Standard System Settings by Using Local Policies

## Detailed demonstration steps

This demonstration examines how to configure standard system settings by using the Local Group Policy Editor. This demonstration does not cover every standard setting; instead, it provides an introduction into local group policy configuration by updating a few group policy settings.

### Start the Virtual Machines and log on

1. Start the 6294A-LON-DC1 virtual machine. When the virtual machine has started, then start the 6294A-LON-CL1 virtual machine.
2. Switch to the LON-CL1 computer. Log on to the LON-CL1 virtual machine as **CONTOSO\administrator** with a password of **Pa$$w0rd**.

### Open the Local Policy Editor

1. Click **Start**.
2. In the **Search programs and files** box, type **gpedit.msc**, and then press ENTER

### Configure computer-related standard settings

1. In Local Group Policy Editor, in the navigation tree, click **Computer Configuration**. There are no Preferences available in the local policy editor.
2. Navigate to **Administrative Templates/Control Panel/ Regional and Language Options**. In the results pane, double-click **Restricts the UI language Windows uses for all logged users**. This setting, if enabled, restricts the user interface to the specified language for computers with more than one language installed. Click **Cancel**.
3. In the navigation tree, expand **Network**, and then click **Offline Files**. In the results pane, double-click **Allow or Disallow use of the Offline Files** feature. This setting enables or disables offline file caching; by selecting Disabled, offline caching is unavailable. Click **Cancel**.
4. In the navigation tree, click **Printers**, and in the results pane, double-click **Pre-populate printer search location text**. This setting enables users to quickly locate adjacent printers. It requires that Active Directory objects, such as Sites and Subnets, be configured with location strings. Click **Cancel**.
5. In the navigation tree, expand **System**, and then click **User Profiles**. These settings are used by an administrator to control user profile behavior. In the results pane, double-click **Only allow local user profiles**. This setting can be used on a computer in a public area, such as a library, to prevent use of roaming profiles. Click **Cancel**.
6. In the navigation tree, expand **Windows Components**, expand **Backup**, and then click **Client**. In the results pane, double-click **Prevent backing up to optical media (CD/DVD)**. This setting can be used to prevent users from archiving to optical media. Click **Cancel**.

### Configure user-related standard settings

1. In Local Group Policy Editor, in the navigation tree, navigate to **User Configuration/ Windows Settings/ Internet Explorer Maintenance/URLS**. In the results pane, double-click **Important**

**URLs**. These settings can be used to configure the default home page, search pages, and other URLs for users.

2. Select the **Customize Home page URL** check box, and in the **Home page URL:** box, type **http://lon-dc1** and then click **OK**. On the Quick Launch bar, click **Internet Explorer**. The Contoso Web site automatically opens. Close Internet Explorer, and switch to the Local Group Policy Editor.
3. In the navigation tree, expand **Administrative Templates**, expand **Control Panel**, and then click **Personalization**. In the results pane, double-click **Load a specific theme**. Click **Enabled**, and in the **Path to theme** file box, type **C:\windows\Globalization\MCT\MCT-US\Theme\US.Theme**. This setting is used to configure the desktop theme. Click **Cancel**.
4. Close the editor.

# Lesson 3

## Designing and Configuring Internet Explorer Settings

### Contents:

# Question and Answers

## Discussion: The Need for Configuring IE Settings

**Question:** Why is it important that an organization configure Internet Explorer settings on its client computers?

**Answer:** Organizations need to configure Internet Explorer settings on its client computers for a variety of reasons, including:

- Businesses place a great deal of effort into protecting computer assets and resources. Phishing attacks, otherwise known as social engineering attacks, can evade those protections and result in users giving up personal information. This can lead to a variety of problems for users, including:
    - Web sites can locate users in the physical world, profile them in the virtual world, and correlate this information to form a "complete" identity.
    - Web sites share their personal data with other parties, such as marketing contacts, for unexpected purposes like online behavior analysis. The problem is exacerbated by the fact that many users are often unaware of such data collection practices.
    - The majority of phishing scams target individuals in an attempt to extort money or perform identity theft.
- Configuring IE settings can help organizations avoid these kind of attacks. For example:
    - The new SmartScreen filter in Internet Explorer 8 can help protect users from malicious sites that conduct phishing attacks or attempt to download malicious software.
    - By configuring the **Prevent bypass** setting, you can prevent users from inadvertently ignoring SmartScreen warnings for known-malicious sites.
- To reduce application and Web site compatibility issues, or to reduce the learning curve for users as they encounter new features, you can implement IE compatibility settings to make your current version of Internet Explorer behave as closely as possible to previous versions.

## Privacy Features of IE 8.0

**Question:** Describe the difference between InPrivate Browsing and InPrivate filtering.

**Answer:** InPrivate Browsing helps protect data and privacy by preventing browsing history, temporary Internet files, form data, cookies, usernames, and passwords from being stored or retained locally by the browser. InPrivate Filtering is designed to monitor the frequency of all third-party content as it appears across all Web sites visited by the user.

## Demonstration: Security Features of IE 8.0

**Question:** Which sites does a user typically add to his or her trusted sites list, and what are the implications?

**Answer:** Users typically add sites that are known to be safe, that they regularly visit, and that contain elements that are inhibited by the more stringent security of the Internet zone. Caution must be exercised when adding sites to this list.

## Discussion: Compatibility Features in Internet Explorer 8.0

**Question:** What compatibility issues can you encounter when updating Internet Explorer?

**Answer:** Do you envision your organization implementing ACT as a means to identify potential compatibility issues? Why or why not?

## Discussion: Determining the IE 8.0 Settings

**Question:** How can you prevent users' personal information from being collected while they are browsing the Internet?

**Answer:** By implementing InPrivate Browsing, which helps protect data and privacy by preventing browsing history, temporary Internet files, form data, cookies, usernames, and passwords from being stored or retained locally by the browser. This leaves virtually no evidence of browsing or search history since the browsing session does not store session data.

**Question:** Which new IE 8.0 feature do you implement that blocks user access to malicious sites? What must you do to prevent users from disregarding notifications that a site has been blocked and must not be accessed?

**Answer:** You must enable the SmartScreen Filter, which blocks Web sites known to be unsafe and notifies users with a SmartScreen blocking page that offers guidance to help avoid known, unsafe Web sites. One of the options on this blocking page enables users to disregard the notice and continue displaying the site. To prevent users from selecting this option, you can disable it in Group Policy. This removes the users' ability to ignore the warning.

**Question:** What recommendation must you make to the buyers in the Purchasing Department to address the compatibility issues related to the six vendor sites that do not render as expected?

**Answer:** The buyers need to use the **Compatibility View** button to fix sites that render differently than expected. Internet Explorer 8 remembers sites that are set to Compatibility View so that the button only needs to be pressed once for a site. After that, the site is always rendered in Compatibility View unless it is removed from the list.

## Discussion: Configuring IE 8.0 Settings

**Question:** Do you always need to enable SmartScreen? Explain why.

**Answer:** No. Some third-party products provide this kind of filtering as part of a security suite.

# Detailed Demo Steps

## Demonstration: Configuring the Standard System Settings by Using Local Policies

## Detailed demonstration steps

This demonstration examines how to configure standard system settings by using the Local Group Policy Editor. This demonstration does not cover every standard setting; instead, it provides an introduction into local group policy configuration by updating a few group policy settings.

### Start the Virtual Machines and log on

1. Start the 6294A-LON-DC1 virtual machine. When the virtual machine has started, then start the 6294A-LON-CL1 virtual machine.
2. Switch to the LON-CL1 computer. Log on to the LON-CL1 virtual machine as **CONTOSO\administrator** with a password of **Pa$$w0rd**.

### Open the Local Policy Editor

1. Click **Start**.
2. In the **Search programs and files** box, type **gpedit.msc**, and then press ENTER

### Configure computer-related standard settings

1. In Local Group Policy Editor, in the navigation tree, click **Computer Configuration**. There are no Preferences available in the local policy editor.
2. Navigate to **Administrative Templates/Control Panel/ Regional and Language Options**. In the results pane, double-click **Restricts the UI language Windows uses for all logged users**. This setting, if enabled, restricts the user interface to the specified language for computers with more than one language installed. Click **Cancel**.
3. In the navigation tree, expand **Network**, and then click **Offline Files**. In the results pane, double-click **Allow or Disallow use of the Offline Files** feature. This setting enables or disables offline file caching; by selecting Disabled, offline caching is unavailable. Click **Cancel**.
4. In the navigation tree, click **Printers**, and in the results pane, double-click **Pre-populate printer search location text**. This setting enables users to quickly locate adjacent printers. It requires that Active Directory objects, such as Sites and Subnets, be configured with location strings. Click **Cancel**.
5. In the navigation tree, expand **System**, and then click **User Profiles**. These settings are used by an administrator to control user profile behavior. In the results pane, double-click **Only allow local user profiles**. This setting can be used on a computer in a public area, such as a library, to prevent use of roaming profiles. Click **Cancel**.
6. In the navigation tree, expand **Windows Components**, expand **Backup**, and then click **Client**. In the results pane, double-click **Prevent backing up to optical media (CD/DVD)**. This setting can be used to prevent users from archiving to optical media. Click **Cancel**.

### Configure user-related standard settings

1. In Local Group Policy Editor, in the navigation tree, navigate to **User Configuration/ Windows Settings/ Internet Explorer Maintenance/URLS**. In the results pane, double-click **Important**

**URLs**. These settings can be used to configure the default home page, search pages, and other URLs for users.

2. Select the **Customize Home page URL** check box, and in the **Home page URL:** box, type **http://lon-dc1** and then click **OK**. On the Quick Launch bar, click **Internet Explorer**. The Contoso Web site automatically opens. Close Internet Explorer, and switch to the Local Group Policy Editor.
3. In the navigation tree, expand **Administrative Templates**, expand **Control Panel**, and then click **Personalization**. In the results pane, double-click **Load a specific theme**. Click **Enabled**, and in the **Path to theme** file box, type **C:\windows\Globalization\MCT\MCT-US\Theme\US.Theme**. This setting is used to configure the desktop theme. Click **Cancel**.
4. Close the editor.

## Demonstration: Security Features of IE 8.0

## Detailed demonstration steps

This demonstration examines how to configure the security zones in Internet Explorer.

### Open Internet Explorer and locate the security settings

1. On the LON-CL1 computer, access **Internet Options**.
2. Click the **Security** tab. The default site, **http://lon-dc1**, has been identified as part of the Local intranet.

### View the security zones

1. In the **Select a zone to view or change security settings** list, click **Internet**. Notice the zone template is Medium-high, and that this zone operates in Protected Mode.
2. In the **Select a zone to view or change security settings** list, click **Local intranet**. Notice the zone template is Medium-low, and that this zone does not operate in Protected Mode.
3. In the **Select a zone to view or change security settings** list, click **Trusted sites**. Notice that the zone template is customized. Click **Default level**, and now notice that the zone template is **Medium**. Notice that the zone does not operate in **Protected Mode**. Click **Sites**. Trusted sites can be added to the sites list, but by default, sites must implement HTTPS, although this can be changed. Click **Close**.

### Add a site to the restricted sites list

1. In the **Select a zone to view or change security settings** list, click **Restricted sites**. Notice the zone template is High, and that this zone operates in Protected Mode. Click **Sites**, and in the **Restricted sites** dialog box, in the **Add this website to the zone** box, type **http://lon-dc1**, click **Add**, and then click **Close**. Click **OK**.
2. In Internet Explorer, press F5. On the Contoso Intranet Home Page, click **Current Projects**. Notice the Security Warning at the top of the page. The ActiveX control required by this page cannot load due to the security settings on the Restricted sites zone. Close the current Web page, and return to the Contoso Intranet Home Page.

### Add a site to the trusted sites list

1. Open **Internet Options** and click the **Security** tab. Select **Trusted sites**, and then click **Sites**. In the **Trusted sites** dialog box, clear the **Require server verification (https( for all sites in this**

**zone** check box, and in the **Add this website to the zone** box, type **http://lon-dc1**, click **Add**, and then click **Close**. Click **OK**, and in **Internet Explorer**, press **F5**. On the **Contoso Intranet Home** Page, click **Current Projects**. Notice the ActiveX control required by this page loads without warning.

### Change the zone template for the trusted sites zone

1. Access **Internet Options** and then click the **Security** tab. Select **Trusted sites**, and then click **Custom level**. Notice that you can configure individual elements of the security settings.
2. Scroll down the **Settings** list and beneath **Run ActiveX controls and plug-ins**, click **Prompt**. Click **OK**, and then click **Yes**. Click **OK**, and in the **Contoso Intranet Home Page**, click **Current Projects**. Notice the prompt for the ActiveX control required by the Web page on this site?
3. In the **Internet Explorer** dialog box, click **Yes**. Close the Current Projects Web page, and then close Internet Explorer.

## Demonstration: Configuring IE 8.0 Settings

## Detailed demonstration steps

This demonstration examines how to configure Internet Explorer settings by using the Local Group Policy Editor.

### Open the Local Policy Editor

1. On the LON-CL1 computer, click **Start**.
2. In the **Search programs and files** box, type **gpedit.msc**, and then press ENTER. Local policies are enforced first, and then group policies applied subsequently with a higher priority.

### Configure Compatibility View settings

1. Compatibility View determines how Internet Explorer identifies itself to a Web server and how content is rendered. This can help ensure that some Web sites display properly in Internet Explorer 8. In Local Group Policy Editor, navigate to **Computer Configuration/ Administrative Templates/ Windows Components/Internet Explorer/ Compatibility View**. These settings can also be configured on the User Configuration folder.
2. Open Internet Explorer. Click **Tools**. Notice that the local intranet site is being viewed in compatibility mode (Compatibility View is grayed-out).
3. Click **Compatibility View Settings**. Add or remove sites, and configure intranet sites settings from here. Click **Close**, and then close Internet Explorer. Switch to Local Group Policy Editor.
4. In the results pane, double-click **Turn off Compatibility View**. This policy controls the Compatibility View feature. If this setting is enabled, users will not be able to use Compatibility View. Click **Cancel**.

### Configure InPrivate settings

1. Open Internet Explorer, click **Safety**, and then click **InPrivate Filtering Settings**. When visiting Web sites, some information about your visit is collected by the content provider. InPrivate Filtering is used to control which providers receive information about the Web sites that are visited. Click **Cancel**.

2. Switch to Local Group Policy Editor. In the navigation tree, click **InPrivate**. In the results pane, double-click **Turn off InPrivate Filtering**. If this policy is enabled, then InPrivate Filtering is not available. Click **Cancel**.
3. Switch to Internet Explorer. Click **Safety**, and then click **InPrivate Browsing**. InPrivate Browsing prevents Internet Explorer from storing session data such as cookies, temporary Internet files, and history.
4. Close Internet Explorer, and then switch to **Local Group Policy Editor**. In the results pane, double-click **Turn off InPrivate Browsing**. If this policy is enabled, InPrivate Browsing is unavailable. Click **Cancel**.

### Configure SmartScreen settings

1. Open Internet Explorer. Click **Safety**, and then click **SmartScreen Filter**. SmartScreen filtering warns the user if the Website being visited is known for fraudulent attempts to gather personal information – known as phishing sites – or if the site is known to contain malicious software.
2. Switch to Local Group Policy Editor, and in the navigation tree, click **Internet Explorer**. In the results pane, click **Turn off Managing SmartScreen Filter**. Use this to control SmartScreen Filtering.

### Configure search providers

1. In Local Group Policy Editor, navigate to **User Configuration/ Windows Settings/Internet Explorer Maintenance/URLS**. In the results pane, double-click **Important URLs**. Aside from the default home page, search provider URLs can be configured here. Click **Cancel**.
2. In the navigation tree, navigate to **Computer Configuration/Administrative Templates/ Windows Components/Internet Explorer**, and in the results pane, double-click **Restrict search providers to a specific list of providers**. This setting can also be used to control search providers. Click **Cancel**.

### Configure accelerators

1. Switch to Internet Explorer. In the Web page, highlight and then right-click any text. The new Accelerators in Internet Explorer 8 help users quickly perform everyday browsing tasks without navigating to other Web sites to get things done.

   Highlight text from any Web page, and then click the **blue Accelerator** icon that appears above the selection to obtain driving directions, translate and define words, e-mail content to others, search with ease, and more. For example, with the “Map with Live Search” Accelerator in Internet Explorer 8, an in-place view of a map can be displayed directly on the page. Close Internet Explorer.
2. Switch to Local Group Policy Editor, and in the result pane, double-click **Accelerators**. Accelerators can be configured by using these Group Policy settings.

### Configure security settings

1. In Local Group Policy Editor, in the navigation tree, click **Security Features**. The following range of folders and policies can be added to configure all the security settings in Internet Explorer 8.
2. Close Local Group Policy Editor.

# Lesson 4

## Designing and Configuring Security Settings

### Contents:

# Question and Answers

## Determining the AppLocker Rules

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

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

## Demonstration: Configuring and Enforcing AppLocker Rules

**Question:** What are the advantages of using a published rule for executable AppLocker rules?

**Answer:** Use the slider bar to enforce a restriction on multiple versions rather than a single exact matching executable.

## Determining the BitLocker Settings

**Question:** What is the advantage of encrypting the Windows operating system drive when a TPM microchip is installed on the computer?

**Answer:** TPM enables BitLocker to validate that the boot components, such as the system BIOS, the hardware profile, and the operating system, have not been modified from the configuration that was present when the drive was locked.

## Determining the Firewall Rules and Settings

**Question:** Why are host-based firewalls that run on individual computers needed in an organization?

**Answer:** Network perimeter firewalls cannot provide protection for traffic generated inside a trusted network.

## Demonstration: Configuring Firewall Settings

**Question:** What can you use to configure authentication besides the Connection Security Rules?

**Answer:** IPsec.

## Demonstration: Determining and Configuring Windows Defender Settings

**Question:** Does Windows Defender provide for antivirus protection?

**Answer:** Only indirectly; some malicious software detected by Defender can also carry an infectious payload. Even with Windows Defender installed, you must still implement antivirus protection on your computers.

# Detailed Demo Steps

## Demonstration: Configuring and Enforcing AppLocker Rules

## Detailed demonstration steps

This demonstration examines how to create the default AppLocker rules and a custom AppLocker rule.

### Open the Group Policy Management editor

1. Switch to the LON-DC1 computer, and log on to the virtual machine as **CONTOSO\administrator** with a password of **Pa$$w0rd**.
2. Open **Group Policy Management**. Open the Default Domain Policy for editing.

### Configure an executable rule

1. In Group Policy Management Editor, navigate to **Computer Configuration/ Policies/Windows Settings/ Security Settings/ Application Control Policies/AppLocker**. In the results pane, under **Overview**, click **Executable Rules**.
2. In the navigation tree, right-click **Executable Rules**, and then click **Create New Rule**. In the **Create Executable Rules wizard**, on the **Before You Begin** page, click **Next**.
3. Configure the action to deny or allow, and specify which users or groups are affected. Click **Deny**, and then click **Next**.
4. Select an application from a known publisher, from a designated path, or from a file hash. Click **Publisher**, and then click **Next**. On the **Publisher** page, click **Browse**. In the **Open** dialog box, double-click **Internet Explorer**, and then double-click **iexplore.exe**. If necessary, target and identify a specific version of a specific program from a specific publisher. Use the slider bar to make the rule slightly less specific. For example, slide the bar up, rather than impose a restriction for Internet Explorer 8.0, to look for any version. Click **Next**.
5. Configure exceptions, if necessary. Click **Next** and then click **Create**.
6. Enable the default rules at this point. In the **AppLocker** dialog box, click **Yes**. Notice that the default rules allow members of the Everyone group to run programs located in Program Files and Windows.

### Configure enforcement

1. In the navigation tree, click **AppLocker**, and in the results pane, click **Configure rule enforcement**.
2. In the **AppLocker Properties** dialog box, under **Executable rules**, select the **Configured** check box, and then click **OK**. Select the option **Audit only**, if necessary. Do this to determine which applications users are running before locking down the application environment.

### Start services and refresh group policy

1. Start the **Application Identity** service. Without this service running on the client computer, AppLocker will not function correctly. Use Group Policy to configure this service to automatically start.
2. Force a refresh of the group policy.

**Note:** Sometimes it is necessary to refresh the policy twice.

### Testing the rule

1. Load **Internet Explorer**.
2. In the warning dialog box, click **OK**. In the **Windows** dialog box, click **No**.

### Creating and testing a script rule

1. Switch to the LON-DC1 computer and navigate to C:\users\Public. Create a file called test.vbs in this folder.
2. Edit the file and type **msgbox “Test script”**, and save the file. Close notepad.
3. Switch to Group Policy Management Editor. In the navigation tree, right-click **Script Rules**, and then click **Create New Rule**.
4. Create a script rule that denies permissions to the Everyone group. Use a file hash and browse and locate the script file just created. Activate the default rules when prompted.
5. On the LON-CL1 computer, force a refresh of the group policy.
6. On the LON-CL1 computer, from a Command Prompt, type **\\lon-dc1\users\public\test.vbs** and press ENTER. In the **Windows Scripting Host** dialog box click **OK**.

### Allowing the script to run

1. Switch to the LON-DC1 computer and delete the script rule previously created.
2. On the LON-CL1 computer, force a refresh of the group policy.
3. At the Command Prompt, type **\\lon-dc1\users\public\test.vbs** and press ENTER. In the **un-named** dialog box click **OK**.

## Demonstration: Configuring BitLocker Settings

## Detailed demonstration steps

This demonstration examines how to configure BitLocker settings. The virtual environment does not provide for a TPM platform. Consequently, the demonstration will show the settings, but they will not be changed.

### Open the Local Policy

1. On the LON-CL1 computer, open the Local Group Policy Editor.
2. Navigate to **Computer Configuration/Administrative Templates/Windows Components/BitLocker Drive Encryption.**

### View BitLocker policies

1. In the results pane, click **Store BitLocker recovery information in Active Directory Domain Services (Windows Server 2008 and Windows Vista)**. Use this setting to backup recovery information to AD DS to help prevent data loss due to lack of key information.

2. In the results pane, click **Choose drive encryption method and cipher strength**. Use this setting to configure the algorithm used to encrypt specified drives. In the results pane, double-click **Operating System Drives**.
3. In the results pane, click **Choose how BitLocker-protected operating system drives can be recovered**. Use this setting to define the way in which operating system drives can be recovered in the absence of key information; for example, to specify that a data recovery agent can be used in these circumstances.
4. Close Local Group Policy Editor.

## Demonstration: Determining and Configuring the UAC Settings

## Detailed demonstration steps

This demonstration examines two of the UAC group policy settings in the Local Group Policy Editor.

### Create a UAC Group Policy setting preventing access elevation

1. On the LON-CL1 computer, open the Local Group Policy Editor.
2. Navigate to **Computer Configuration/ Windows Settings/ Security Settings/Local Policies/ Security Options**.
3. In the results pane, double-click User Account Control: Behavior of the elevation prompt for standard users. Select Automatically deny elevation requests then click OK.
4. Close **Local Group Policy Editor** and log off. Log on to the LON-CL1 as **Contoso\Ryan** with a password of **Pa$$w0rd**.
5. Click **Start**, and in the **Search programs and files** box, type **services.msc**, and in the **Program(1)** list, right-click **services**, and then click **Run as administrator**. Notice that it is not possible to elevate the program. In the error dialog box, click **OK** and then log off.

### Create a UAC Group Policy setting prompting for credentials for administrator users

1. Log on to the LON-CL1 as **Contoso\Administrator** with a password of **Pa$$w0rd** and open the Local Group Policy Editor.
2. Navigate to **Computer Configuration/ Windows Settings/ Security Settings/Local Policies/ Security Options**.
3. In the results pane, double-click **User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode**. Select **Prompt for credentials** and then click **OK**. Log off.
4. Log on to the LON-CL1 as **LON-CL1\Admin** with a password of **Pa$$w0rd**. Click **Start**, and in the **Search programs and files** box, type **services.msc**, and in the **Program(1)** list, right-click **services**, and then click **Run as administrator**. Notice that the prompts are for credentials rather than for consent.
5. In the **User Account Control** dialog box, click **No** and then log off.

# Demonstration: Configuring Firewall Settings

## Detailed demonstration steps

This demonstration examines how to configure Windows Firewall with Advanced Security by using Group Policy settings.

### Configure an inbound rule

1. Switch to the LON-DC1 virtual machine and ping lon-cl1. Notice that ping is blocked by default.
2. Log on to the LON-CL1 as **Contoso\Administrator** with a password of **Pa$$w0rd**.
3. Open the **Local Group Policy Editor**, and navigate to **Computer Configuration/Windows Settings/Security Settings/ Windows Firewall with Advanced Security/ Windows Firewall with Advanced Security – Local Group Policy Object**. In the navigation tree, click **Inbound Rules**, and then right-click **Inbound Rules**. Click **New Rule**.
4. Create a new custom rule that allows ICMPv4 packets for all profiles. Call the rule “Allow ping”.
5. Switch to the LON-DC1 virtual machine and verify that you can now ping lon-cl1.
6. Switch to the LON-CL1 computer and modify the properties of the Allow Ping rule. On the **General** page, click **Allow the connection if it is secure**, and then click **OK**.
7. Switch to the LON-DC1 virtual machine and verify that you cannot ping LON-CL1. You can see that ping is now prevented again because there is no way to authenticate.

### Configure a connection security rule

1. Switch to the LON-CL1 computer.
2. In Local Group Policy Editor, in the navigation tree, click **Connection Security Rules**.
3. Create a new custom security rule that Requests authentication for inbound and outbound connections. Specify that the rule applies only to ICMPv4 traffic, and that the default authentication mechanism be used. The rule needs to apply to all profiles. Call the rule “Authenticate ping.”
4. Switch to the LON-DC1 computer. Open the Local Group Policy Editor, and navigate to **Computer Configuration/Windows Settings/Security Settings/ Windows Firewall with Advanced Security/ Windows Firewall with Advanced Security – Local Group Policy Object** and then repeat steps 2 and 3.
5. Try to ping LON-CL1. Notice that ping is now enabled again because of the connection security rule. Close all open windows.

### Monitoring the rules

1. Switch to the LON-CL1 computer. Open Windows Firewall with Advanced Security and navigate to **Monitoring/ Security Associations/ Main Mode**. Notice that the two computers are authenticating with Computer (Kerberos V5) authentication. Click **Quick Mode**. View the protocol being used in ICMPv4.
2. Close all open windows.

# Demonstration: Determining and Configuring Windows Defender Settings

## Detailed demonstration steps

This demonstration examines how to use Group Policy settings to configure Windows Defender.

### Configure Windows Defender options with Group Policy

1. On the LON-CL1 computer open Local Group Policy Editor and navigate to **Computer Configuration/ Administrative Templates/ Windows Components/ Windows Defender**.
2. In the results pane, click **Turn off Windows Defender**. If this setting is enabled, Windows Defender does not run and your computer will not be scanned for malicious software.
3. In the results pane, click **Turn off Real-Time Monitoring**. If this setting is enabled, Windows Defender does not prompt you when it discovers malicious software.
4. In the results pane, click **Turn on definition updates through both WSUS and Windows Update**. Enable this option if you want Windows Defender to be able to obtain definition updates even during the temporary absence of a local WSUS server. Close Local Group Policy Management.

# Lesson 5

## Designing and Implementing Group Policy

### Contents:

# Question and Answers

## How Are GPOs Processed

**Question:** When a client computer is connected to a domain, which GPO takes precedence – the local GPO or the domain-based GPOs?

**Answer:** Settings in domain GPOs always take precedence because they are processed after the local GPO.

## Group Policy Inheritance

**Question:** You created a GPO that is linked to a container. How do you prevent the settings in this GPO from being overwritten by settings linked to GPOs in child containers (which generally have a higher precedence)?

**Answer:** By setting the GPO link to **Enforced**.

## Group Policy Planning Considerations

**Question:** What are two of the most important considerations that must be taken into account when designing an organization's Active Directory structure?

**Answer:** Ease of administration and delegation. OU design requires balancing requirements for delegating administrative rights, independent of Group Policy needs, and the need to scope the application of Group Policy.

## Demonstration: Configuring Group Policy Settings and Preferences

**Question:** What does using Preference targeting do?

**Answer:** Determines Preference conditions.

# Detailed Demo Steps

## Demonstration: Configuring Group Policy Settings and Preferences

## Detailed demonstration steps

This demonstration examines how to configure Group Policy and Preference settings by using Group Policy Management console.

### Create and link a GPO

1. Switch to the LON-DC1 computer and open **Group Policy Management**.
2. Create a new GPO called "Contoso Standard Settings" and link it to the Contoso.com domain.

### Edit the settings and preferences in the GPO

1. In the Group Policy Management Editor, navigate to **User Configuration/ Policies/ Windows Settings/ Scripts (Logon/Logoff)**.
2. Create a new logon script called Logon.vbs with the following content:
   - Set oNet=Wscript.CreateObject("Wscript.Network")
   - oNet.Mapnetworkdrive "L:", "\\lon-dc1\data"
3. Rather than use a policy setting for configuring a drive mapping, a user preference can also be used. Open the new policy for editing, and navigate to **User Configuration/Preferences/ Windows Settings/ Drive Maps**.
4. Create a new drive mapping with the following properties:
   - Location: \\lon-dc1\data
   - Reconnect: select
   - Drive letter: K
5. Click the **Common** tab and select the **Item-level targeting** check box, and then click **Targeting**. In the **Targeting Editor** dialog box, click New Item. Use targeting to specify a condition, or conditions, that must be met for the preference to be applied. In the list, click **Domain**. For example, to specify domain level targeting which applies the preference only when the user is logged onto the domain. Click **Computer in domain**. Or when the computer is part of a domain. Click **Cancel**. Click **OK**.
6. Close Group Policy Management Editor.
7. Switch to the LON-CL2 computer and force refresh the group policy settings.
8. Restart the computer and then log on to the virtual machine as **CONTOSO\administrator** with a password of **Pa$$w0rd**.
9. Click **OK** to the logon script welcome message. Click **Start**, and then click **Computer**. Notice the drive mapping?

# Lesson 6

## Troubleshooting Group Policy

### Contents:

# Question and Answers

## Discussion: Reasons for Group Policy Application Failures

**Question:** What are the potential reasons for Group Policy application failures?

Some of the most common reasons for Group Policy application failures relate to network, processes, scope, or infrastructure. Present and discuss your ideas with the class.

**Answer:** Possible reasons for Group Policy application failures include:

- GPOs are included in the Denied List.
- The required services and components, such as the Group Policy Service, are not running and configured as expected.
- The core configuration of the computer is not implemented correctly. For example, the computer may not be connected to the network or joined to the domain, or the computer does not have the correct system time.
- Group Policy exceptions such as security filtering, WMI filters, block inheritance, enforcement, loopback processing, and slow link settings are affecting usual GPO processing.
- CSEs are unable to start because core Group Policy processing fails to complete.

## Group Policy Troubleshooting Tools

**Question:** What is the purpose of GPOTool.exe?

Some of the most common reasons for Group Policy application failures relate to network, processes, scope, or infrastructure. Present and discuss your ideas with the class.

**Answer:** GPOTool.exe is a command-line tool to be used in replicated domains that contain more than one domain controller. It traverses all of your domain controllers and checks each for consistency between the Group Policy container and the Group Policy template. The tool also determines whether the policies are valid and consistent between all domain controllers and displays detailed information about the GPOs that are replicated between the domain controllers.

## Process for Resolving Group Policy Application Failures

**Question:** When resolving Group Policy application failures, what is the purpose of running **GPResult**?

**Answer:** GPResult pays attention to the order in which the GPOs are applied. If the same setting is specified in multiple GPOs, those applied later in the process (lower in the log files) are authoritative and override settings in GPOs higher in the list.

# Module Reviews and Takeaways

## Review questions

1. **Question**: What benefit does implementing Multiple Local Group Policy Objects (MLGPO) in Windows provide over previous Windows versions? What are the three layers of local GPOs provided by MLGPO (for bonus points, list them in the order in which they are applied)?

   **Answer**: Multiple Local Group Policy objects allow an administrator to apply different levels of Local Group Policy to local users on a stand-alone computer. This technology is ideal for shared computing environments where domain-based management is not available, such as shared library computers or public Internet kiosks. The three layers of GPOs supported by MLPGO are (in the order in which they are applied): Local Group Policy, Administrator and Non-Administrators Group Policy, and User-specific Local Group Policy.

2. **Question**: What are some of the advantages to configuring Windows 7 clients using Group Policy Settings?

   **Answer**: Advantages include (and are not limited to):

   - Enable centralized desktop management.
   - Decrease total cost of ownership.
   - Over 2500 Group Policy settings enable you to standardize almost every specific computer feature.
   - Reduce losses in productivity by defining policy settings and allowed actions for users and computers.
   - Settings are enforced, so end users cannot change settings.
   - Settings are refreshed, and original settings are not changed.

3. **Question**: When configuring IE8.0 settings, what benefit is provided when you enable InPrivate Browsing, and what improvement does it provide over the Delete Browsing History option?

   **Answer**: InPrivate Browsing helps protect data and privacy by preventing browsing history, temporary Internet files, form data, cookies, usernames, and passwords from being stored or retained locally by the browser. This leaves virtually no evidence of browsing or search history as the browsing session does not store session data.

   From the enterprise and IT professional perspective, InPrivate Browsing is inherently more secure than using Delete Browsing History to maintain privacy because there are no logs kept or tracks made during browsing. InPrivate Browsing is a proactive feature because it enables IT professionals to control what is tracked in a browsing session.

4. **Question**: What are the two main firewall types, and how are they different from one another?

   **Answer**: The two main firewall types are network firewalls and host-based firewalls. Network firewalls are located at the network's perimeter, and host-based firewalls are located on individual hosts within the network. Network firewalls provide management and control of network traffic, stateful connection analysis, and VPN gateway functionality. However, network perimeter firewalls cannot provide protection for traffic generated inside a trusted network. For this reason, host-based firewalls that run on individual computers are needed. Host-based firewalls, such as Windows Firewall with Advanced Security, protect a host from unauthorized access and attack, and can often be configured to block specific types of outgoing traffic.

5. **Question**: When implementing AppLocker, what must you do before manually creating new rules or automatically generate rules for a specific folder, and why?

   **Answer**: You must create the default AppLocker rules. Without the default rules in place, critical system files might not run and you can be blocked from performing administrative tasks.

6. **Question**: What are the two modes in which you can run BitLocker? Which is the most secure, and why?

   **Answer**: BitLocker can run on two types of computers: those running TPM 1.2, and those without TPM 1.2 that have a removable USB memory devise. The most secure implementation of BitLocker leverages the enhanced security capabilities of TPM version 1.2. The TPM is a hardware feature installed in many newer computers by the computer manufacturers. It works with BitLocker to help protect user data and to ensure that a computer running Windows 7 is not been tampered with while the system is offline.

7. **Question**: How does the SmartScreen Filter work in Internet Explorer 8?

   **Answer:** With the SmartScreen Filter enabled, Internet Explorer 8 performs a detailed examination of the entire URL string and compares the string to a database of sites known to distributed malware, then the browser checks with the Web service. If the Web site is known to be unsafe, it is blocked and the user is notified with a bold SmartScreen blocking page that offers clear language and guidance to help avoid known-unsafe Web sites.

8. **Question**: What network firewall shortcoming does the Windows Firewall with Advanced Security address?

   **Answer:** Network firewalls cannot provide protection for traffic generated inside a trusted network.

9. **Question**: GPO A is linked to Organizational Unit (OU) 1 and GPO B is linked to OU 2. OU 2 is nested under OU 1 in the domain. Computer policy setting X is defined in GPO A and B with different values, and computer policy setting Y is defined only in GPO A. What will be the result of setting X and Y on the following computers:

   - Computer K is located on OU 1.
   - Computer L is located on OU 2.

   **Answer:** Policy setting Y will be applied to Computer K and L as defined in GPO A. Depending on what is the computer policy setting X, but generally setting X on computer K will follow the one that is defined in GPO A and setting X on computer L will follow the one that is defined in GPO B.

## Real-world issues and scenarios

1. An administrator configures Group Policy to require that data can only be saved on data volumes protected by BitLocker. Specifically, the administrator enables the **Deny write access to removable data drives not protected by BitLocker** policy and deploys it to the domain. Meanwhile, an end user inserts a USB flash drive that is not protected with BitLocker. What happens, and how can the user resolve the situation?

   **Answer:** Since the USB flash drive is not protected with BitLocker, Windows 7 displays an informational dialog indicating that the device must be encrypted with BitLocker. From this dialog, the user chooses to launch the BitLocker Wizard to encrypt the volume or continues working with the device as read-only.

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

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

3. A server has multiple network interface cards (NICs), but one of the NICs is not connected. In Windows Vista, this caused the machine to be stuck in the public profile (the most restrictive rule). How is this issue resolved in Windows 7?

   **Answer:** The new multiple active firewall profile feature in Windows 7 solves the problem by applying the appropriate rules to the appropriate network; in this case, the profile associated with the connected NIC will be applied.

4. Peter recently upgraded to Internet Explorer 8. Ever since the upgrade, he has noticed that several of the sites that he normally visits are no longer being rendered as expected. What action does Peter need to take?

   **Answer:** Peter needs to use the **Compatibility View** button to fix sites that render differently than expected.

5. John’s organization is interested in implementing the Group Policy loopback feature across a series of computers in their Production Department. During their pilot project, they configured different settings for two managers based on the computers in their Assembly, Fabrication, and Warehouse Departments. They discovered during their testing that the same policy settings were applied to both managers at each computer, when in fact, each manager needed to experience different settings at the same computer. What might be the probable cause for this error?

   **Answer**: When implementing the loopback processing policy setting in a GPO, ensure that the computer and user sections of the GPO are enabled. If the computer section of the GPO is enabled but not the user section, then the policy setting will apply to any user of the computer.

6. Paul modified several Group Policies, but during his testing he noticed that his changes did not take effect immediately. Working from a domain connected client, Paul had to wait approximately 90 minutes for his policy changes to take effect. What can Paul do to remedy this situation?

   **Answer**: For domain members such as Paul, the default refresh interval is 90 minutes. To view the immediate effect of Group Policy changes, Paul must open a command prompt and run **gpupdate**.

### Common issues related to Internet Explorer 8 security settings

IT professionals must familiarize themselves with the common issues that are related to Internet Explorer 8 security settings.

| Issue | Troubleshooting tip |
|---|---|
| Diagnose Connection Problems Button | The **Diagnose Connections Problems** button helps users find and resolve issues potentially without involving the Helpdesk. When Internet Explorer 8 is unable to connect to a Web site, it shows a **Diagnose Connection Problem** button. Clicking the button helps the user resolve the problem by providing information to troubleshoot the problem. This option is available in Internet Explorer 7 but is now easier to find in Internet Explorer 8. |

| | |
|---|---|
| Resetting Internet Explorer 8 Settings | If Internet Explorer 8 on a user's computer is in an unstable state, use the Reset Internet Explorer Settings (RIES) feature in Internet Explorer 8 to restore the default settings of many browser features. These include the following:<br>• Search scopes<br>• Appearance settings<br>• Toolbars<br>• ActiveX controls (reset to opt-in state, unless they are pre-approved)<br>• Branding settings created by using IEAK 8<br>Reset personal settings by using the **Delete Personal Settings** option for the following:<br>• Home pages<br>• Browsing history<br>• Form data<br>• Passwords<br>RIES disables all custom toolbars, browser extensions, and customizations that are installed with Internet Explorer 8. To use any of these disabled customizations, you must selectively enable each customization through the **Manage Add-ons** dialog box. RIES does not do the following:<br>• Clear the Favorites list.<br>• Clear the RSS Feeds.<br>• Clear the Web Slices.<br>• Reset connection or proxy settings.<br>• Affect Administrative Template Group Policy settings that are applied.<br>**Note:** Unless the Group Policy setting titled "Internet Explorer Maintenance policy processing" is enabled, Normal mode settings on the browser created by using IEM are lost after using RIES.<br>1. Perform the following steps to use RIES in Internet Explorer 8:<br>2. Click the **Tools** menu and then click **Internet Options**.<br>3. On the **Advanced** tab, click **Reset**.<br>4. In the **Reset Internet Explorer Settings** dialog box, click **Reset**. To remove personal settings, select the **Delete Personal Settings** check box. To remove branding, select the **Remove Branding** check box.<br>5. When Internet Explorer 8 finishes restoring the default settings, click **Close**, and then click **OK** twice.<br>6. Close Internet Explorer 8. The changes take effect the next time Internet Explorer 8 is opened.<br>**Note:** To prevent users from using the RIES feature, enable the **Do not allow resetting Internet Explorer settings** policy in Group Policy Administrative Templates. |

## Best practices for User Account Control

- UAC Security Settings are configurable in the local Security Policy Manager (secpol.msc) or the Local Group Policy Editor (gpedit.msc). However, in most corporate environments, Group Policy is preferred because it can be centrally managed and controlled. There are nine Group Policy object (GPO) settings that can be configured for UAC.

- Because the user experience can be configured with Group Policy, there can be different user experiences, depending on policy settings. The configuration choices made in your environment affect the prompts and dialog boxes that standard users, administrators, or both, can view.

  For example, you might require administrative permissions to change the UAC setting to "Always notify me" or "Always notify me and wait for my response." With this type of configuration, a yellow notification appears at the bottom of the User Account Control Settings page indicating the requirement.

### Best practices for Windows BitLocker

- Because BitLocker stores its own encryption and decryption key in a hardware device that is separate from the hard disk, you must have one of the following:
  - A computer with Trusted Platform Module (TPM).
  - A removable Universal Serial Bus (USB) memory device, such as a USB flash drive. If your computer does not have TPM version 1.2 or higher, BitLocker stores its key on the memory device.
- The most secure implementation of BitLocker leverages the enhanced security capabilities of Trusted Platform Module (TPM) version 1.2.
- On computers that do not have a TPM version 1.2, you can still use BitLocker to encrypt the Windows operating system volume. However, this implementation will require the user to insert a USB startup key to start the computer or resume from hibernation and does not provide the pre-startup system integrity verification offered by BitLocker that is working with a TPM.

### Best practices for Windows AppLocker

- Before manually creating new rules or automatically generating rules for a specific folder, create the default rules. The default rules ensure that the key operating system files are allowed to run for all users.
- When testing AppLocker, carefully consider how you will organize rules between linked GPOs. If a GPO does not contain the default rules, then either add the rules directly to the GPO or add them to a GPO that links to it.
- After creating new rules, enforcement for the rule collections must be configured and the computer's policy refreshed.
- By default, AppLocker rules do not allow users to open or run any files that are not specifically allowed. Administrators must maintain a current list of allowed applications.
- If AppLocker rules are defined in a Group Policy Object (GPO), only those rules are applied. To ensure interoperability between Software Restriction Policies rules and AppLocker rules, define Software Restriction Policies rules and AppLocker rules in different GPOs.
- When an AppLocker rule is set to Audit only, the rule is not enforced. When a user runs an application that is included in the rule, the application is opened and runs normally and information about that application is added to the AppLocker event log.
- At least one Windows Server 2008 R2 domain controller is required to host the AppLocker rules.

### Best practices for Windows Defender

- When using Windows Defender, you must have current definitions.
- To help keep your definitions current, Windows Defender works with Windows Update to automatically install new definitions as they are released. You can also set Windows Defender to check online for updated definitions before scanning.
- When scanning your computer, it is recommended that you select the advanced option to **Create a restore point before applying actions to detected items.** Because Windows Defender can be set to automatically remove detected items, selecting this option allows system settings to be restored if software that is unintentionally removed needs to be used.

# Lab Review Questions and Answers

## Lab A: Designing and Configuring the Client Environment

**Question**: If all users needed drive mappings, the same applications, how will that change your GPO strategy?

**Answer**: You can implement an application deployment GPO at the domain-level. However, some other settings remain that are departmental specific – such as folder redirection and AppLocker; these would need to be implemented at OU level GPOs.

**Question**: Which takes precedence – an enforced GPO or the block inheritance setting on an OU?

**Answer**: Enforcement

## Lab B: Troubleshooting GPO Issues

**Question**: If the LON-CL1 computer was not online when you wanted to perform the tests you undertook in the lab, which tool must you use to perform the analysis?

**Answer**: Group Policy Modeling does not require the computers to be online; rather, it performs a what-if analysis.

# Module 11

## Planning and Deploying Applications and Updates to Windows® 7 Clients

### Contents:

# Lesson 1

## Determining the Application Deployment Method

### Contents:

# Question and Answers

## Software Distribution in Configuration Manager 2007

**Question:** What is the purpose of advertisements in the Configuration Manager deployment method?

**Answer:** Advertisements make the presence of new applications known to the client. They alert clients that the specific package is available for them to download and install, and they provide the administrator with a means to push a mandatory program to clients.

## Software Deployment by Using GPOs

**Question:** You are tasked with creating a GPO object for Office deployment. Where do you create the GPO for the deployment?

**Answer:** On a **domain controller that has access** to the GPMC.

## Application Virtualization and TS RemoteApp

**Question:** How does application virtualization affect application access?

**Answer:** It decouples applications from the operating system and enables them to run as network services.

# Lesson 2

## Deploying the 2007 Microsoft Office System

### Contents:

# Question and Answers

## Demonstration: Using the Office Customization Tool

**Question:** You need to customize your Microsoft Office installation so that it does not install Microsoft® Office Publisher. Which Office Customization Tool category do you configure?

**Answer:** You configure the **Set feature installation states** section found under the **Features** category.

## Methods to Deploy the 2007 Office System

**Question:** List some reasons why you might choose to precache the local installation source during a 2007 Office system deployment.

**Answer:** Precaching the local installation source may decrease network traffic during the install process. You may also be able to better control the exact time-period when users install and start using the 2007 Office release.

**Question:** List two methods that can be used to precache the local installation source.

**Answer:** Configure the **<LIS CACHEACTION="CacheOnly" />** option in the Config.xml file and then deploy the setup command using either a logon script or by using Configuration Manager.

## Troubleshooting a 2007 Office System Deployment

**Question:** When you try to upgrade the Microsoft Office 2003 Multilanguage User Interface Pack (MUI) to the Office Language Pack, you learn that the **Upgrade** button is unavailable in the 2007 Office Setup program. Instead, the **Install Now** button is available. How do you correct this situation?

**Answer:** Remove the Office 2003 MUI when you install, or after you install, the 2007 Office programs.

**Question:** You have deployed the 2007 Office system to end-users at your enterprise who have many documents in Microsoft Office 2003 files. How do you move these files to the new format?

**Answer:** Using the Office File Conversion Tool, desktop administrators can convert documents saved in Microsoft Office 97 through Microsoft Office 2003 formats to the new Office Open XML Formats.

# Detailed Demo Steps

## Demonstration: Using the Office Customization Tool

## Detailed demonstration steps

In this demonstration, you are introduced to the OCT.

### Overview of the Office Customization Tool setup category

1. Log on to LON-DC1 with the user name **Administrator** and the password **Pa$$w0rd**.
2. On the **Start** menu, click **Run**.
3. In the **Open** box, type **E:\Labfiles\Office2007\setup.exe /admin**, and then click **OK**. The OCT starts.
4. In the **Select Product** box, ensure that **Create a new Setup customization file for the following product** is selected and that **Microsoft Office Professional Plus 2007** is shown as the **Product**, and then click **OK**.

   If you have multiple products available on the network installation point, each customizable product is listed. If you have an existing Setup customization file to modify, you can select it from this dialog box.
5. In the OCT, in the left-hand console pane, notice that there are four main sections. These sections include:
   - **Setup**: provides a number of options related to general setup of the Office system.
   - **Features**: configure user settings and to select the Office features that are to be installed.
   - **Additional content**: provides options for adding or removing custom files and registry entries during the installation.
   - **Outlook**: customize the default Microsoft® Office Outlook 2007 profile and set Office Outlook 2007 and Microsoft® Exchange Server 2007 options.
6. In the left-hand pane, click **Install location and organization name**. This option is used to specify the default folder in which to install Microsoft Office on the user's computer. The default setting is to have it install in the **Program Files** folder. This option is recognized only when you first install Office on a user's computer; you cannot change the installation path without uninstalling and reinstalling Office.
7. Under **Organization name** type **Contoso**. This name appears in the **About** box (Help menu) and on the banner pages of Office applications.
8. In the left-hand pane, click **Additional network sources**. You can use this setting to specify additional servers that have a copy of the network installation point. Setup looks for servers in this list, in the order specified, if it is installing a feature on demand or repairing Office and the original network installation point is unavailable. This demonstration does not configure an additional network source.
9. In the left-hand pane, click **Licensing and user interface**. Use this setting to enter the product key and accept the end-user license agreement (EULA) on behalf of each user who installs Office

with this Setup customization file. You can also use this setting to select how the user interface is displayed during installation. The options include:

- **Full (default)**: Setup displays all of the user interface and messages.
- **Basic**: Setup displays the **Welcome** screen, prompts for the product key and end-user license agreement (if needed), and displays a progress bar and the completion notice.
- **None**: Setup runs quietly, which means that it does not display any user interface or messages.

10. The **Completion notice** option provides the ability to enable or disable the display of a message to the user when installation is complete.
11. The **Suppress Modal** option can be selected if you do not want Setup to display error messages and other dialog boxes that might interrupt the installation. If you set **Display level** to **Full**, error messages and other dialog boxes are displayed regardless of the state of this check box.
12. The No cancel option can be selected if you want to disable the **Cancel** button on the **Progress** dialog box. This applies only if **Display** level is set to **Full** or **Basic**.
13. In the left-hand pane, click **Remove previous installations**. This option allows you to specify which previous versions of Microsoft Office programs to keep or remove.
14. In the left-hand pane, click **Add installation and run programs**. Use this option to run additional programs before or after the Office installation is complete. A program file can have one of the following extensions: .exe, .com, .bat, .scr, or .msi.
15. In the left-hand pane, click **Office security settings**. Use this option to configure security settings such as trusted sources for digitally signed macros, add-ins, Microsoft ActiveX® controls, and other executable code. You can also configure a list of trusted locations from which any file can be opened without being checked by the Trust Center security feature.
16. In the left-hand pane, click **Modify Setup properties**. This option provides the ability to set properties to be applied during the Office installation. You can customize Setup properties only when you first install Office on a user's computer; properties configured in a setup customization file do not take effect if you apply the file to an existing installation. The following properties can be used when you customize a 2007 Office release installation:
    - **HIDEUPDATEUI**: If set to **True**, this property hides the **Check for Updates** button on the completion dialog. This property is ignored if the completion dialog is not displayed. The default value is **False**.
    - **PRIMARYFOLDER**: Designates a primary folder for the installation.
    - **ROOTDRIVE**: Specifies the default drive for the destination folder of the installation. The value for this property must end with '****'.
        - **SETUP_REBOOT**: Determines how Setup restarts the computer after installation.
            - **AutoAlways**: Always initiate a reboot. Do not prompt the user.
            - **Always**: Always prompt for a reboot at the end of setup.
            - **IfNeeded**: Prompt for a reboot at the end of setup if setup requires a reboot. (Default).
            - **AutoIfNeeded**: Initiate a reboot if setup requires a reboot. Do not prompt the user.

- **Never**: Never initiate or prompt for a reboot.

### Overview of the Office Customization Tool features category

1. In the left-hand pane, click **Modify user settings**. Use this setting to specify the default values of Office application settings for users who install Office with this customization file. Click **Show All Settings** to display all available user settings. Click **Show Configured Settings** to display only those settings that you have configured.

2. In the details pane, expand **Microsoft Office 2007 system\File Open/Save** dialog box and then click **Places Bar Locations**. For example, you may want to configure specific save locations to be available on the **Places** bar in the Microsoft Office applications, this option allows you to configure custom settings for the installation.

3. In the left-hand pane, click **Set feature installation states**. Use this setting to customize how the 2007 Office release features are installed on the user's computer. Options include:

    - **Run from My Computer**: Setup copies files and writes registry entries and shortcuts associated with the feature to the user's hard disk, and the application or feature runs locally.

    - **Run All from My Computer**: The same as the **Run from My Computer** option, except that all child features belonging to the feature are also set to this state.

    - **Installed on First Use**: Setup leaves components for the feature and all its child features on the installation source until the user attempts to use the feature for the first time, at which time the components are copied to the local hard disk. This is also known as an advertised feature.

    - **Not Available**: The components for the feature, and all of the child features belonging to this feature, are not installed on the computer.

    - **Hidden**: Setup does not display the feature in the feature tree during installation if Setup is run interactively. The feature is not hidden when Setup is run in maintenance mode after Office is installed.

    - The best use of this setting is to simplify the feature tree for users. For example, you might hide the **Office Tools** branch of the feature tree so that users do not have to decide which tools they need; only the tools that you select are installed.

    - **Locked**: The installation state you choose for this feature cannot be changed by the user during installation or in maintenance mode after Office is installed.

    - **Reset**: The feature is returned to its default installation state.

### Overview of the Office Customization Tool additional content category

1. In the left-hand pane, click **Add files**. The Add files and Remove files sections are used to add or remove files to users' computers when Office is installed. When you add files to an Office installation, the files are copied into the Setup customization file when you save the customization file and exit the OCT. Large files increase the size of the Setup customization file.

2. In the left-hand pane, click **Add registry entries**. The Add registry entries and Remove registry entries sections are used to add, modify, or remove registry entries on users' computers when Office is installed.

3. In the left-hand pane, click **Configure shortcuts**. Use this setting to modify or remove default shortcuts to installed Office applications and to add shortcuts to any files installed with the 2007

Office release or already on the user's computer. You can configure shortcuts only when you first install Office on a user's computer; this option is ignored if you apply the Setup customization file to an existing installation.

## Overview of the Office Customization Tool Outlook category

1. In the left-hand pane, click **Outlook profiles**. Use this setting to customize a user's default Office Outlook profile. Options include:

    - **Use existing profile**: Use the profile already configured on the user's computer or prompt the user to create a profile the first time Office Outlook is started. Choosing this option disables the other Office Outlook sections of the OCT.
    - **Modify profile**: Modify the default profile on the user's computer or define changes to existing profiles located on the local computer. If no default profile exists or there is no profile by the name that you specify, Office Outlook creates a profile based on the options you choose in the other Office Outlook sections of the OCT. Office Outlook uses the default profile name (Outlook) or uses the profile name you have specified.
    - **New profile**: Create a new profile on the user's computer and make it the default profile; any existing profiles are not removed and remain available to users. You must type a name in the **Profile name** box. This name appears in the **E-mail Accounts** dialog box in Office Outlook. Office Outlook creates the profile based on the options you choose in the other Office Outlook sections of the OCT.
    - **Apply PRF**: Import an Office Outlook profile file (PRF file) to create a new default profile. Selecting this option disables the other Office Outlook sections of the OCT but does not update the OCT with the settings in the PRF file.

    You can use any profile created for Office Outlook 2007. Type a name and path for the profile in the **Apply The Following Profile (PRF File)** box. If you created a PRF file for a previous version of Office Outlook, you can import it to Office Outlook 2007, provided that the profile uses only MAPI services.

2. In the details pane, click **Modify Profile**. Only new or modified default profiles can have Exchange settings configured in the next section.

3. In the left-hand pane, click **Specify Exchange Server settings**. Use this option to configure an Exchange Server connection for new or existing profiles. You can also configure the default behavior for Cached Exchange Mode, which is used to create a local cached copy of your Outlook profile on your workstation.

4. In the left-hand pane, click **Add accounts**. Use this option to include new Office Outlook e-mail accounts in the user's profile.

5. In the left-hand pane, click **Remove accounts & export settings**. Use this option to remove existing Lotus cc:Mail or Microsoft Mail accounts. This option is also used to export Office Outlook settings to a PRF file.

6. In the left-hand pane, click **Specify Send/Receive groups**. Set up Send/Receive groups for Exchange accounts and folders, and specify the tasks that are performed on each group during a Send/Receive operation in Office Outlook.

    A Send/Receive group contains a collection of Office Outlook accounts and folders. You can specify different options for Send/Receive groups for when Office Outlook is online and offline.

7. Click the **File** menu and then click **Save As**. Browse to **E:\Labfiles\Office2007\Updates**. The file is saved in the **Updates** folder as with an MSP file extension. When Office is installed from this network installation point, the MSP file is automatically applied.

# Lesson 3

## Planning and Configuring Desktop Updates by Using WSUS

### Contents:

# Question and Answers

## Considerations for Managing Updates

**Question:** An end-user at your company is repairing an installation of Office, when the user is prompted for the original installation media or network location of the original installation files. Why is this happening?

**Answer:** If the product to be updated was deployed using Windows Installer, the Windows Installer may require access to original installation files.

## Demonstration: Configuring the Automatic Updates Client by Using Group Policy

**Question:** Which setting is required to ensure that client computers contact a local WSUS server?

**Answer:** The **Specify intranet Microsoft update service location** setting is required and is the basis for most of the other settings available for Windows Update.

## Demonstration: Managing Updates by Using the WSUS Administration Console

**Question:** From the Windows Update page, how do you know if the updates are coming from the Internet or being managed from your IT department?

**Answer:** On the **Windows Update** page, next to **You receive updates:**, it states **Managed by your system administrator**.

# Detailed Demo Steps

## Demonstration: Configuring the Automatic Updates Client by Using Group Policy

## Detailed demonstration steps

In this demonstration, you will see how to use Group Policy Settings to configure the Automatic Updates feature on network clients.

### Use Group Policy to deploy Automatic Updates client settings

The GPMC is used to either create a new GPO or edit an existing GPO with the required settings. For this demonstration, create a new GPO that contains the Automatic Updates configuration settings and link it to the Research department.

1. On LON-DC1, click **Start**, point to **Administrative Tools**, and then click **Group Policy Management**. The Group Policy Management console opens.
2. Expand **Forest: Contoso.com**, expand **Domains**, expand **Contoso.com**, and then click **Group Policy Objects**.
3. Right-click **Group Policy Objects** and then click **New**.
4. In the **New GPO** dialog box, under **Name**, type **Research Dept Automatic Update Settings**, and then click **OK**.
5. Right-click **Research Dept Automatic Update Settings** and then click **Edit**.
6. Under **Computer Configuration**, expand **Policies**, expand **Administrative Templates**, expand **Windows Components**, and then click **Windows Update**.
7. Discuss the following settings:
    - Do not display ‘Install Updates and Shut Down’ option in Shut Down Windows dialog box
    - Do not adjust default option to ’Install Updates and Shut Down’ in Shut Down Windows dialog box
    - Enabling Windows Update Power Management to automatically wake up the system to install scheduled updates
    - Configure Automatic Updates
    - Specify intranet Microsoft update service location
    - Automatic Updates detection frequency
    - Allow non-administrators to receive update notifications
    - Allow Automatic Updates immediate installation
    - Turn on recommended updates through Automatic Updates
    - No auto-restart with logged on users for scheduled automatic updates installations
    - Re-prompt for restart with scheduled installations
    - Delay Restart for scheduled installations

- Reschedule Automatic Updates scheduled installations
- Enable client-side targeting
- Allow signed updates from an intranet Microsoft update service location

8. In the details pane, double-click **Configure Automatic Updates**.
9. In the **Configure Automatic Updates** dialog box, click **Enabled**.
10. Under **Options**, configure the following and then click **OK**:
    - Configure automatic updating: 4 – Auto download and schedule the install
    - Scheduled install day: 0 – Every day
    - Scheduled install time: 03:00
11. In the details pane, double-click **Specify intranet Microsoft update service location**.
12. In the **Specify intranet Microsoft update service location** dialog box, click **Enabled**.
13. Under **Options** configure the following and then click **OK**:
    - Set the intranet update service for detecting updates: http://LON-DC1
    - Set the intranet statistics server: http://LON-DC1
14. In the details pane, double-click **Enable client-side targeting**.
15. In the **Enable client-side targeting** dialog box, click **Enabled**.
16. Under **Options** configure the following and then click **OK**:
    - Target group name for this computer: Research
17. Close the Group Policy Management Editor.
18. In the Group Policy Management console, right-click the **Research** OU and then click **Link an Existing GPO**.
19. In the **Select GPO** dialog box, click **Research Dept Automatic Update Settings**, and then click **OK**.
20. Close Group Policy Management.
21. Open Active Directory Users and Computers and move LON-CL1 from the **Computers** container to the **Research** OU.
22. To prepare for the next demonstration, start (or restart if it is already running) LON-CL1 and log on as **Administrator** with the password of **Pa$$w0rd**.

## Demonstration: Managing Updates by Using the WSUS Administration Console

## Detailed demonstration steps

In this demonstration, you will see how to use WSUS to view and approve updates for network clients.

### Use WSUS to approve and deploy updates to network clients

WSUS is used to view, approve, and deploy updates to network clients. For this demonstration, determine if LON-CL1 requires any updates. Then, approve and deploy any required updates. Note that WSUS has already been configured to manage the Research computer group.

1. On LON-DC1, click **Start**, point to **Administrative Tools**, and then click **Windows Server Update Services**.
2. In the left-hand pane, expand **Computers**, expand **All Computers**, and then click **Research. LON-CL1.contoso.com** appears in the details pane.
3. Double-click **lon-cl1.contoso.com**. A report is generated to show which updates are required on this computer.
4. Click the **Next Page** button. Notice that four critical updates are reported. Close the report.
5. In the left-hand pane, expand **Updates** and then click **Critical Updates**. Notice the critical updates that are listed.
6. Right-click **Update for the Office System (KB967642)** and then click **Approve**.
7. In the **Approve Updates** dialog box, click the arrow next to **Research** and then click **Approved for Install**. Click **OK**.
8. In the **Approval Progress** dialog box, click **Close**.
9. Right-click **Update for Microsoft Office Outlook 2007 Junk Email Filter (KB70012)** and then click **Approve**.
10. In the **Approve Updates** dialog box, click the arrow next to **Research** and then click **Approved for Install**. Click **OK**.
11. In the **Approval Progress** dialog box, click **Close**.
12. Close the **Update Services** console.
13. On LON-CL1, click **Start**, and then in the **Search programs and files** box, type **Windows Update**.
14. In the search results, under **Programs**, click **Windows Update**.
15. On the **Windows Update** page, click **Check for updates**. Notice that Windows update states that two important updates are available.

# Module Reviews and Takeaways

## Review questions

1. Within Configuration Manager, packages provide one of the foundations of distributing software to clients. What is the purpose of the package?
2. What must an administrator do before any update is sent to clients and servers by using WSUS?
3. What is the reason for setting a deadline for an automatic installation to a past date?

## Review answers

1. The package provides a wrapper that dictates where source files are stored on the site server and distribution points, on what schedule the package is updated on the distribution points, and other settings related to the overall package.
2. Configure automatic approval of certain types of updates or manually specify that the update is approved for installation. Also configure Group Policy settings to enable clients to contact the WSUS server.
3. The update is applied immediately at the next interval when the computer contacts the WSUS server.

## Best practices

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

### Best practices for deploying software through group policy

- Test all software installation packages before you deploy them.
- Use and enforce standard configurations for applications, if possible
- It is recommended that you deploy software as high in the Active Directory hierarchy or tree as you can. Software must be deployed close to the root in the Active Directory tree because it allows you to use one GPO to deploy software to multiple users.
- A Windows Installer package must be assigned and published only once in the identical GPO.
- Create application categories when you have a large quantity of published applications within your organization. This simplifies a user's ability to find applications in Add or Remove Programs in Control Panel.

### Best practices for securing an operating system

- Install all operating system patches
- Verify user account security
- Eliminate unnecessary applications and network services
- Install and configure necessary applications and network services
- Configure system logging to record significant events
- Keep applications and operating system patches up to date

### Best practices to help secure the network installation point for office

- Make sure that access to source files is read-only.

- The Setup.xml and Package.xml files are digitally signed and cannot be modified.
- Save all customization files that you create, including Setup customization files and custom Config.xml files, as read-only.
- If you are centralizing log files on the network, make sure that users have read/write access to that location.

## Tools

| Tool | Use for | Where to find it |
|---|---|---|
| Group Policy Management Console (GPMC) | Provides unified management of all aspects of Group Policy across multiple forests in an organization. | http://go.microsoft.com/fwlink/?LinkId=154249 |
| Office Customization Tool (OCT) | Use to customize an installation of the Office system. The OCT is part of the Setup program and is the recommended tool for most customizations | http://go.microsoft.com/fwlink/?LinkId=162306 |
| Windows Server Update Services (WSUS) | Use for managing and distributing software updates that resolve security vulnerabilities and other stability issues. | http://go.microsoft.com/fwlink/?LinkId=159626 |

# Lab Review Questions and Answers

## Lab A: Planning an End to End Windows 7 LTI Deployment

**Question**: What MDT additional components do you install to support a migration from versions of Windows prior to Windows Vista SP1?

**Answer**: USMT 3.01.

**Question**: When do you allow users to choose the applications to be installed?

**Answer**: Answers will vary. One possible answer is when performing an LTI deployment and there are applications that are not run on all systems.

**Question**: When do you customize a task sequence?

**Answer**: Answers will vary. One possible answer is when certain steps need to be skipped or controlled such as specifying which applications will be available to a particular task sequence.

## Lab B: Deploying Windows 7 Using the LTI Deployment Plan

**Question**: When creating a Reference Computer can you include programs that do not have a silent install option?

**Answer**: Yes, the reference computer can be installed and the image captured as separate tasks.

**Question**: What is the best way to handle deploying custom application with the MDT?

**Answer**: Answers will vary. One way is to create separate installations packages for the applications to be added to images that are deployed.

**Question**: When additional resources do you need to perform a fully automated installation?

**Answer**: Zero Touch installation requires a SCCM 2007 infrastructure.

# Resources

## Contents:

# Microsoft Learning

This section describes various Microsoft Learning programs and offerings.

- Microsoft Skills Assessments

  Describes the skills assessment options available through Microsoft.

- Microsoft Learning

  Describes the training options available through Microsoft — face-to-face or self-paced.

- Microsoft Certification Program

  Details how to become a Microsoft Certified Professional, Microsoft Certified Database Administrators, and more.

- Microsoft Learning Support
- To provide comments or feedback about the course, send e-mail to support@mscourseware.com.
- To ask about the Microsoft Certification Program (MCP), send e-mail to mcphelp@microsoft.com

# Technet and MSDN Content

- Prescriptive guidance has been updated externally on TechNet and IT Springboard. Go to http://go.microsoft.com/fwlink/?LinkId=162631
- This process is how the Microsoft Deployment Toolkit 2010 Beta http://go.microsoft.com/fwlink/?LinkID=108442
- Windows System Image Manager (Windows SIM)
- ImageX
- Deployment Image Servicing and Management (DISM)
- User State Migration Tool (USMT)
- Driver Package Installer (DPInst)
- For more information on Image types, go to: http://go.microsoft.com/fwlink/?LinkId=162642
- MDT 2010
- Configuration Manager 2007
- USMT 4.0
- AD DS
- For complete information on new features of USMT 4.0, refer to "What's New in USMT 4.0"
- For more information about specific features and application settings that are migrated, refer to What Does USMT Migrate?
- For more information on rerouting files and settings, refer to http://go.microsoft.com/fwlink/?LinkID=163077
- For more information on planning user state migration, refer to: http://go.microsoft.com/fwlink/?LinkID=163078
- For more information about Software Distribution in Configuration Manager click the following link http://go.microsoft.com/fwlink/?LinkId=119690
- TS RemoteApp Step-by-Step Guide
- Terminal Services RemoteApp
- For more information, click the link to the Office Deployment Quick-Start Guide and Checklist
- Use Group Policy Software Installation to deploy the 2007 Office system
- Using enterprise deployment tools for the 2007 Office system:
- Create a network installation point for the 2007 Office system
- Troubleshooting resources for the 2007 Office system:
- Microsoft Windows Server Update Services
- Windows Server Update Services 2.0 with Service Pack 1 Product Overview
- WSUS and the Update Management Process:
- Update Management Process
- Office Customization Tool (OCT)

- Windows Server Update Services (WSUS)

# MSDN

There is no MSDN content in this course.

# Communities

- For more information on Windows 7 hardware requirements, refer to:http://go.microsoft.com/fwlink/?LinkID=154215
- Windows Pre-installation Environment (Windows PE)
- Windows Automated Installation Kit (Windows AIK)
- Windows Optional Component Setup (OCSetup)
- Windows Update Standalone Installer (WUSA)
- Sysprep
- How to use Group Policy to remotely install software in Windows Server 2003
- Microsoft Application Virtualization Technical Overview
- Microsoft Application Virtualization
- Group Policy Management Console (GPMC)

# Send Us Your Feedback

You can search the Microsoft Knowledge Base for known issues at Microsoft Help and Support before submitting feedback. Search using either the course number and revision, or the course title.

**Note** Not all training products will have a Knowledge Base article – if that is the case, please ask your instructor whether or not there are existing error log entries.

## Courseware Feedback

Send all courseware feedback to support@mscourseware.com. We truly appreciate your time and effort. We review every e-mail received and forward the information on to the appropriate team. Unfortunately, because of volume, we are unable to provide a response but we may use your feedback to improve your future experience with Microsoft Learning products.

## Reporting Errors

When providing feedback, include the training product name and number in the subject line of your e-mail. When you provide comments or report bugs, please include the following:

- Document or CD part number
- Page number or location
- Complete description of the error or suggested change

Please provide any details that are necessary to help us verify the issue.

**Important** All errors and suggestions are evaluated, but only those that are validated are added to the product Knowledge Base article.