Microsoft®

OFFICIAL MICROSOFT LEARNING PRODUCT

6416C

Updating Your Network Infrastructure and Active Directory® Technology Skills to Windows Server® 2008

Companion Content

Product Number: 6416C

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

Installing and Configuring Windows Server® 2008

Contents:

Lesson 1

Installing Windows Server 2008

Contents:

Question and Answers

Windows Server 2008 Editions

Question: What are the advantages in special purpose editions such as Web or Hyper-V server?

Answer: Pricing and licensing would be a major advantage. Students may have other advantages.

Additional Reading

Windows Server 2008 Editions

- For more information about the differences between editions, see http://go.microsoft.com/fwlink/?LinkID=171094&clcid=0x409.
- To see the product information page for Windows Server 2008, go to http://go.microsoft.com/fwlink/?LinkID=171095&clcid=0x409.
- To see the Volume Activation Deployment Guide, go to http://go.microsoft.com/fwlink/?LinkID=171096&clcid=0x409.

Windows Server 2008 Installation Requirements

- For more information about system requirements, see http://go.microsoft.com/fwlink/?LinkID=171097&clcid=0x409.
- For a comparison of the editions by technical specifications, see http://go.microsoft.com/fwlink/?LinkID=171098&clcid=0x409.

X64 Installation Considerations

- For information on digital signatures for kernel modules on systems running Windows Vista®, see http://go.microsoft.com/fwlink/?LinkID=171099&clcid=0x409.
- For more information on kernel-mode code signing policy, see http://go.microsoft.com/fwlink/?LinkID=171100&clcid=0x409.

Common Installation Scenarios

- To see the Windows Automated Installation Kit (WAIK) User's Guide for Windows Vista, go to http://go.microsoft.com/fwlink/?LinkID=171101&clcid=0x409.
- To see the Windows Vista Deployment Step by Step Guide, go to http://go.microsoft.com/fwlink/?LinkID=171102&clcid=0x409.

Preparing to Install Windows Server 2008

- For more information on the Windows Server 2008 Setup Wizard, see Help and Support on the Install Now page of the Windows Server 2008 Setup Wizard.
- For more information on Windows Firewall, see http://go.microsoft.com/fwlink/?LinkID=171103&clcid=0x409.

Process for Installing Windows Server 2008

- For more information about Windows Server 2008 Server Manager, see http://go.microsoft.com/fwlink/?LinkID=171104&clcid=0x409.
- For more information about Server Management in Windows Server 2008, see http://go.microsoft.com/fwlink/?LinkID=171105&clcid=0x409.
- To see the Volume Activation Deployment Guide, go to http://go.microsoft.com/fwlink/?LinkID=171096&clcid=0x409.

Lesson 2

Managing Server Roles and Features

Contents:

Question and Answers

Demonstration: Installing Server Roles and Features by Using Server Manager

Question: How could you install a server role or feature on a remote server?

Answer: The Servermanagercmd utility could be used.

.

Detailed Demo Steps

Demonstration: Installing Server Roles and Features by Using Server Manager

Detailed demonstration steps

In this demonstration, you will see how to:

- Install the Print Services role on the domain controller.
- Install the Windows PowerShell feature.
- Install the ADLDS server role.

Server Manager starts automatically when an administrator logs on to a computer running Windows Server 2008. If you close Server Manager and want to start it again, you can start it from the following locations:

- On the **Start** menu, right-click **Computer,** and then click **Manage**.
- On the **Start** menu, point to **Administrative Tools**, and then click **Server Manager.**

On the **Quick Launch** toolbar available on the Windows taskbar.

Install the Print Service role

1. Ensure that LON-DC1 is running.
2. Log on as **Administrator** with a password of **Pa$$w0rd**.
3. Click the **Server Manager** icon in the quick launch bar.
4. Click **Roles**.
5. Click **Add Roles**.
6. In the Add Roles Wizard, click **Next.**
7. Select the **Print Services** check box, and then click **Next**.
8. On the **Print Services** page, click **Next.**
9. On the **Select Role Services page**, examine the options, and then click **Next**.
10. On the **Confirm Installation Selections** page, click **Install.**
11. Click **Close** to complete the installation.

Install the Windows PowerShell feature

1. In Server Manager, click **Features**.
2. Click **Add Features**.
3. In the Add Features Wizard, select the **Windows PowerShell** check box, and then click **Next.**
4. On the **Confirm Installation Selections** page, click **Install.**
5. Click **Close** to complete the installation.

Install the AD LDS server role by using servermanagercmd.exe

1. Click **Start**, and then click **Command Prompt**.
2. In the command prompt window, execute **Servermanagercmd –query.**

   Notice that AD LDS is not installed.
3. In the command prompt window, execute **Servermanagercmd –install ADLDS**.
4. When the command completes, execute **Servermanagercmd –query**.

   Notice that AD LDS is installed now.

Additional Reading

What Are Server Roles?

- For more information on roles, role services, and features, see http://go.microsoft.com/fwlink/?LinkID=171106&clcid=0x409.
- To see a comparison of server roles, go to http://go.microsoft.com/fwlink/?LinkID=171107&clcid=0x409.

What Is BitLocker Drive Encryption?

- To see the Windows BitLocker Drive Encryption Step-by-Step Guide, go to http://go.microsoft.com/fwlink/?LinkID=171108&clcid=0x409.
- For more information about the BitLocker Drive Preparation Tool, see http://go.microsoft.com/fwlink/?LinkID=171109&clcid=0x409.

Lesson 3

Configuring Windows Server 2008 Server Core

Contents:

Question and Answers

Features Supported By Server Core

Question: Why are features such as Windows PowerShell not available on Server Core?

Answer: Server Core does not support the .NET Framework, therefore any roles, features, or applications that rely on the .NET Framework are not supported by Server Core.

Detailed Demo Steps

Demonstration: Managing Server Core

Detailed demonstration steps

In this demonstration, you will see how to:

- Install the DNS server role.
- Open the firewall ports for file and print services and the DNS service.

Install the DNS server role

1. In the command prompt window, execute the following command to view the current state of roles.

   oclist

   Notice that no roles are currently installed.

2. In the command prompt window, execute the following command to install the DNS Server role:

   Start /w ocsetup DNS-Server-Core-Role

Note: The role name is case sensitive.

3. In the command prompt window, type the following command to view the state of roles, and then press ENTER.

   oclist

Notice that the DNS Server role is now installed.

Open the firewall ports for file and print and DNS service

1. In the command prompt window, execute the following command to open the appropriate ports for the file and print service:

   netsh firewall set service fileandprint enable all

2. In the command prompt window, execute the following command to open both the TCP and the UDP ports 53 for the DNS service:

   netsh firewall add portopening ALL 53 DNS-server

Additional Reading

Server Roles Supported By Server Core

- For more information on the Server Core Installation Option, see http://go.microsoft.com/fwlink/?LinkID=171110&clcid=0x409.
- To see the Server Core Installation Option Getting Started Guide, go to http://go.microsoft.com/fwlink/?LinkID=171116&clcid=0x409.

Managing a Server Core Installation

- For more information about installation and configuration for Windows Remote Management, see http://go.microsoft.com/fwlink/?LinkID=171111&clcid=0x409.

Module Reviews and Takeaways

Review questions

1. If your organization is planning a large-scale virtualization project to consolidate multiple servers on a few large-scale servers, what version of Windows would be best suited for this project and why?

   Answer: Datacenter Server is best suited for this project because of its unlimited virtual licensing scheme.

2. What are the primary benefits of using the Core Installation for a Windows Server 2008 version?

   Answer: Reduced administration, reduced maintenance, reduced attack footprint, and smaller installation footprint.

3. How often must a computer contact a KMS server for activation renewal?

   Answer: At least every 180 days.

Common issues related to installing and configuring Windows Server 2008

Identify the causes for the following common issues related to installing and configuring Windows Server 2008 and fill in the troubleshooting tips. For answers, refer to relevant lessons in the module.

Issue	Troubleshooting tip
Can't upgrade from Windows Server 2003 to Windows 2008 Server Core	Windows 2008 Server Core can only be installed as a clean installation.
Unable to install certain roles on a Server Core	Server Core does not support all the roles that a full install of Windows Server 2008 supports.
Unable to launch the Windows Server Backup utility from the Start menu	The Windows Server Backup must be installed as a feature.

Tools

Tool	Use for	Where to find it
Server Manager	General configuration and management of the server	In the Administrative Tools folder or on the Quick Launch toolbar
Initial Configuration Tasks	First configuration after installation	Launches automatically after an installation or by using the Oobe command
Netsh	Command-line server configuration	%systemroot%\System32 directory, Launched from a command prompt
Netdom	Manage domain and trust relationships from the command line	%systemroot%\System32 directory, Launched from a command prompt

Lab Review Questions and Answers

1. What must you do before you can use the Windows Server Backup?

   Answer: You must install the Windows Server Backup feature.

2. How can services be managed on a Server Core installation?

   Answer: Services can be managed remotely through an MMC or they can be managed via the command line.

3. What command-line utility is used to join a Server Core computer to the domain?

   Answer: The Netdom utility can be used to join a Server Core computer to the domain.

Module 2

Configuring Windows® Deployment Services

Contents:

Lesson 1

Overview of Windows Installation Technologies

Contents:

Additional Reading

What Is Windows Deployment Services?

To see the Windows Deployment Services Getting Started Guide, go to http://go.microsoft.com/fwlink/?LinkID=171132&clcid=0x409.

For more information about deploying earlier versions of Windows, see http://go.microsoft.com/fwlink/?LinkID=171133&clcid=0x409.

What Is Windows Imaging File Format?

Download the white paper "Windows Imaging File Format (WIM)" at http://go.microsoft.com/fwlink/?LinkID=171134&clcid=0x409.

Lesson 2

Creating Images for Windows Deployment Services

Contents:

Question and Answers

What Is the Windows System Image Manager?

Question: What is the format of answer files?

Answer: Answer files are in the XML format.

What Is Sysprep?

Question: Why is Sysprepping a computer an important step in the image process?

Answer: The reference machine must be prepared to avoid having computers deployed that have duplicate names and SIDs. This could prevent them from joining and participating in domain activities.

What Is Windows PE?

Question: Can Windows PE be used as a full operating system?

Answer: No, Windows PE was designed to be used for preinstallation environments and cannot be used to run traditional applications.

Windows PE Support Utilities

Question: What utility would you use to inject a third-party driver into an image?

Answer: The PEimg utility.

Additional Reading

What Is the Windows System Image Manager?

For more information on Windows System Image Manager, see http://go.microsoft.com/fwlink/?LinkID=171135&clcid=0x409.

Windows Setup Configuration Passes

For more information on how configuration passes work, see http://go.microsoft.com/fwlink/?LinkID=171136&clcid=0x409.

What Is Sysprep?

To see the Windows Vista Deployment Step-by-Step Guide, go to http://go.microsoft.com/fwlink/?LinkID=171137&clcid=0x409.

What Is Windows PE?

For more information on Windows PE 2.0 for Windows Vista, see http://go.microsoft.com/fwlink/?LinkID=171138&clcid=0x409.

Lesson 3

Deploying Images by Using Windows Deployment Services

Contents:

Additional Reading

Image Capture Process

For more information on creating custom install images, see http://go.microsoft.com/fwlink/?LinkID=171139&clcid=0x409.

What Is Multicasting?

For more information on Windows Deployment Services multicast servers, see http://go.microsoft.com/fwlink/?LinkID=171140&clcid=0x409.

Module Reviews and Takeaways

Review questions

1. What is the purpose of a capture image?

   Answer: A capture image is a boot image that contains Windows PE 2.0, which has been modified to launch an image capture utility instead of setup.

2. What are the prerequisites for installing Windows Deployment Services?

   Answer: AD DS, DNS, DHCP, NTFS Volume, Administrative rights.

3. What purpose does Sysprep serve?

   Answer: Sysprep removes machine-specific information from the reference computer to prepare it for the imaging process.

Common issues related to deploying an image

Identify the causes for the following common issues related to deploying an image, and fill in the troubleshooting tips. For answers, refer to relevant lessons in the module.

Issue	Troubleshooting tip
Computers fail to receive the Windows Deployment Services client.	Ensure that the computers are capable of PXE boot and that a functioning DHCP server is available.
Clients fail to receive an IP address from the DHCP server.	If the DHCP server is running on the Windows Deployment Services server, steps need to be taken to change the Windows Deployment Services service to not listen on port 67 and DHCP option 60 must be added to all DHCP scopes.
Answer files are not being applied.	Ensure that the answer files have been properly associated with the images in the Windows Deployment Services server. Use the Windows SIM to review settings. Refer to the built in help files in the Windows SIM.
Unable to assign an answer file to the Windows Deployment Services client.	Answer files for the Windows Deployment Services must be stored in the remote installation share.

Tools

Tool	Use	Where to find it
ImageX	Creating and managing WIM files	The Windows AIK
Sysprep	Preparing reference computers for imaging	%systemroot%\System32\Sysprep
Windows SIM	Creating XML-based answer files	The Windows AIK
Windows PE	Preinstallation environment for installing an operating system	The Windows AIK

Lab Review Questions and Answers

1. At the minimum, how many answer files are required for a fully automated installation to a bare-metal machine?

   Answer: Two answer files are required. One for the Windows Deployment Services client and one for the installation.

2. Where must the answer file for the Windows Deployment Services client be stored?

   Answer: The answer file for the Windows Deployment Services client must be stored in the Remote Installation shared folder.

3. What is the difference between an Auto-Cast and a Scheduled-Cast multicast transmission?

   Answer: An Auto-Cast starts sending clients the image on demand. Other clients can join the Auto-Cast at any time. A Scheduled-Cast waits until the specified number of clients have requested an image before transmitting the image.

Module 3

Configuring Networking and Network Services

Contents:

Lesson 1

Configuring IPv6 Addressing

Contents:

Additional Reading

The IPv6 Address Space

For more information, see the white paper "Introduction to IP Version 6" at http://go.microsoft.com/fwlink/?LinkId=99899&clcid=0x409.

Lesson 2

Migrating from IPv4 to IPv6

Contents:

Additional Reading

IPv4 and IPv6 Coexistence

For more information on IPv6 Transition Technologies, see http://go.microsoft.com/fwlink/?LinkID=112079&clcid=0x409.

Tunneling Technologies Usage

For more information on IPv6 Transition Technologies, see http://go.microsoft.com/fwlink/?LinkID=112079&clcid=0x409.

What Is ISATAP Tunneling?

For more information on RFC 4214: Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), see http://go.microsoft.com/fwlink/?LinkId=99900&clcid=0x409.

Lesson 3

Configuring DHCP and DNS

Contents:

Question and Answers

Demonstration: Configuring the GlobalNames Zone

Question: What is the recommended use for the GlobalNames zone?

Answer: The recommended use of a GlobalNamez zone (GNZ) is by using an AD DS integrated zone (named GlobalNames) that is distributed globally. The GNZ can hold DNS records to map a single-label name to a fully qualified domain name (FQDN) using a CNAME resource record, for example. The FQDN then allows the resolution of the name to an IP address.

Demonstration: Configuring DHCP

Question: What are some of the reasons for securing DHCP and requiring server authorization in Active Directory?

Answer: The reasons for securing DHCP servers include:

- Preventing an unauthorized user from obtaining a lease.
- Restricting unauthorized, non-Microsoft® DHCP servers from leasing IP addresses.
- Restricting DHCP administration.

Detailed Demo Steps

Demonstration: Configuring the GlobalNames Zone

Detailed demonstration steps

In this demonstration, you will see how to:

- Enable the GlobalNames Zone functionality.
- Create and configure the GlobalNames zone.
- Add an Alias (CNAME) Resource Record to the GlobalNames zone.
- Test the GlobalNames zone using the ping utility.

Enable the GlobalNames zone functionality

1. On LON-DC1, click **Start**, and then click **Command Prompt.**
2. Type the following in the command prompt, and then press ENTER:

   dnscmd lon-dc1 /config /EnableGlobalnamesSupport 1
3. Close the command prompt.

Create and configure the GlobalNames zone

1. On LON-DC1, open **Server Manager,** expand **Roles,** expand **DNS Server**, expand **DNS,** and then expand **LON-DC1**.
2. Right-click **Forward Lookup Zones**, and then click **New Zone**.
3. In the **New Zone Wizard**, click **Next.**
4. On the **Zone Type** screen, ensure that the **Primary zone** is selected and the **Store the zone in Active Directory** check box is selected, and then click **Next.**
5. Click **To all DNS servers in this forest: Contoso.com**, and then click **Next.**
6. Type **GlobalNames** in the **Zone name** field, and then click **Next.**
7. Click **Do not allow dynamic updates**, click **Next,** and then click **Finish.**

Add an alias (CNAME) resource record to the GlobalNames zone

1. On LON-DC1, click **Start**, and then click **Command Prompt**.
2. Type the following in the command prompt, and then press ENTER.

   dnscmd /RecordAdd GlobalNames DC CNAME lon-dc1.contoso.com

   This will add a CNAME record for a single-label name pointing to the FQDN of the Domain Controller.
3. Close the command prompt.

Test the GlobalNames zone by using the Ping utility

1. On LON-DC1, click **Start**, and then click **Command Prompt**.
2. Type the following in the command prompt, and then press ENTER:

   ping DC

You should receive a response back with the IP address and fully qualified domain name of lon-dc1.contoso.com.

Demonstration: Configuring DHCP

In this demonstration, you will see how to:

- Create DHCP IPv6 scope.
- Configure the client workstation to use DHCP-assigned IPv6 addresses.

Create DHCP IPv6 scope

1. On LON-DC1, click **Start,** point to **Administrative Tools**, and then click **Services.**
2. Right-click **DHCP Server**, and then click **Start**.
3. On LON-DC1, click **Start,** and then click **Server Manager**.
4. In the Server Manager console, expand **Roles**.
5. In the left pane, expand **DHCP Server**, and then expand **LON-DC1.contoso.com**.
6. Right-click the **IPv6 server** icon, and then click **New Scope**.
7. In the New Scope Wizard, on the **Welcome** page, click **Next.**
8. In the **Scope Name** dialog box, type **Contoso IPv6 Clients**. Click **Next**.
9. In the **Scope Prefix** dialog box, type **FC00:0:0:1::** into the **Prefix** field, leave the **Preference** setting at the default setting of **0**, and then click **Next**.
10. On the **Add Exclusions** page, enter **0:0:0:1** in the **Start IPv6 Address** field and **0:0:0:1** in the **End IPv6 Address** field, and then click **Add.**
11. Click **Next** to continue.
12. Review the default settings on the **Scope Lease** page, and then click **Next.**
13. Confirm the settings, ensure that **Yes** under **Activate Scope Now** is selected, and then click **Finish**.
14. Close **Server Manager** on LON-DC1.

Configure the client workstation to use DHCP-assigned addresses

1. On LON-CL1, click **Start**, right-click **Network**, and then click **Properties.** The Network and Sharing Center window appears.
2. Under **Tasks**, click **Manage network connections**. The Network Connections window appears.
3. Right-click **Local Area Connection 2,** and then choose **Properties** from the context menu.
4. In the **Local Area Connection 2 Properties** dialog box, click **Internet Protocol Version 4 (TCP/IPv4),** and then click **Properties.**
5. In the **Internet Protocol Version 4** dialog box, select **Obtain an IP address automatically** and **Obtain DNS server address automatically**, and then click **OK.**
6. In the **Local Area Connection Properties** dialog box, click **Internet Protocol Version 6 (TCP/IPv6),** and then click **Properties.**

7. In the **Internet Protocol Version 6** dialog box, select **Obtain an IPv6 address automatically** and **Obtain DNS server address automatically**, and then click **OK**.
8. In the **Local Area Connection 2 Properties** dialog box, click **Close.**
9. Close the **Network Connections** window, and then close the **Network and Sharing Center** window.
10. Click **Start**, click **All Programs**, click **Accessories**, and then click **Command Prompt**.
11. At the command prompt, type the following command:

    netsh int ipv6 show int

    The output from this command will list your interfaces and their respective index numbers. You will use this index value in the next command.
12. At the command prompt, type the following command to disable Router Discovery: **netsh int ipv6 set int [index] routerdiscovery=disabled.**
13. At the command prompt, type the following command to enable Managed Address: **netsh int ipv6 set int [index] managedaddress=enabled.**
14. Confirm your changes by using the following command to view the existing settings: **netsh int ipv6 show int [index].**
15. Restart **LON-CL1**. After the computer is restarted, log on as **Administrator** with the password **Pa$$w0rd**.
16. On LON-CL1, click **Start**, point to **All Programs**, point to **Accessories**, right-click **Command Prompt**, and then click **Run as Administrator**.
17. At the command prompt, type **ipconfig,** and then press ENTER.
18. At the command prompt, type **ipconfig /release,** and then press ENTER
19. At the command prompt, type **ipconfig /renew**, and then press ENTER.
20. At the command prompt, type **ipconfig /all**, and then press ENTER. Notice that both IPv4 and IPv6 addresses are assigned.
21. Close the command prompt.

Additional Reading

DNS Improvements in Windows Server 2008

- To see what's new in DNS in Windows Server 2008, go to http://go.microsoft.com/fwlink/?LinkId=99838&clcid=0x409.
- For more information on Read-Only Domain Controllers, see http://go.microsoft.com/fwlink/?LinkId=99839&clcid=0x409.
- For more information on the DNS Server Role, see http://go.microsoft.com/fwlink/?LinkId=99840&clcid=0x409.

DHCP Enhancements in Windows Server 2008

- For more information on DHCP Server, see http://go.microsoft.com/fwlink/?LinkId=99877&clcid=0x409.
- For more information on the DHCPv6 protocol, see http://go.microsoft.com/fwlink/?LinkId=99878&clcid=0x409.

Lesson 4

Configuring Windows Firewall

Contents:

Question and Answers

Demonstration: Configuring Windows Firewall with Advanced Security by Using Group Policy

Question: What features does Windows Firewall with Advanced Security combine?

Answer: Windows Firewall with Advanced Security combines a host firewall and IPsec.

Demonstration: Configuring Connection Security Rules in Windows Firewall with Advanced Security

Question: What is a connection security rule?

Answer: A connection security rule forces two peer computers to authenticate before they can establish a connection and to secure information transmitted between the two computers. Windows Firewall with Advanced Security uses IPsec to enforce these rules.

Detailed Demo Steps

Demonstration: Configuring Windows Firewall with Advanced Security by Using Group Policy

Detailed demonstration steps

In this demonstration, you will see how to:

- Create an organizational unit (OU) and put the client computer account in it.
- Create a new Group Policy object (GPO).
- Enable the firewall on client computers.
- Test the firewall settings.

Create an organizational unit and put the client computer account in it

1. On LON-DC1, click **Start**, and then click **Server Manager**.
2. Expand **Roles,** expand **Active Directory Domain Services**, and then expand **Active Directory Users and Computers.**
3. Right-click **Contoso.com**, click **New**, and then click **Organizational unit.**
4. Enter **Vista Clients** in the **Name** field, and then click **OK.**
5. Click the **Computers** container.
6. Right-click **LON-CL1**, and then click **Move.**
7. Select the **Vista Clients** OU, and then click **OK.**

Create a new Group Policy object (GPO)

1. On LON-DC1, in Server Manager, expand **Features**, expand **Group Policy Management**, expand **Forest: Contoso.com**, expand **Domains,** and then expand **contoso.com**.
2. Right-click the **Vista Clients** OU, and then click **Create a GPO in this domain, and link it here**.
3. Enter **Firewall Settings for Vista Clients** into the **Name** field, and then click **OK.**

Enable the firewall on client computers

1. In the main window, right-click **Firewall Settings for Vista Clients GPO**, and then click **Edit.**
2. In the Group Policy Management Editor, right-click the **Firewall Settings for Vista Clients [LON-DC1.contoso.com] Policy** icon, and then click **Properties.**
3. Select the **Disable User Configuration settings** check box, and then click **Yes** when prompted to confirm.
4. Click **OK** to close the window.
5. Expand **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, expand **Windows Firewall with Advanced Security**, and then expand **Windows Firewall with Advanced Security - LDAP://cn={GUID},cn=policies,cn=system,DC=contoso,DC=com**, where GUID is a unique number assigned to your domain.

6. Right-click **Windows Firewall with Advanced Security - LDAP://cn={GUID},cn=policies,cn=system,DC=contoso,DC=com,** where GUID is a unique number assigned to your domain., and then click **Properties**.
7. Click **Public Profile**.
8. Change the **Firewall state** to **On** (recommended), and then click **OK**.

Test the firewall settings

1. On LON-CL1, click **Start**, click **All Programs**, click **Accessories,** and then click **Command Prompt.**
2. Type the following command and then press ENTER: **gpupdate /force.**
3. Wait until the command finishes before moving to the next step.
4. To validate that the GPO was correctly applied, type the following command and then press ENTER: **gpresult /r /scope computer.**
5. In the output, look for the section **Applied Group Policy Objects**. Confirm that it contains entries for both **Firewall Settings for Vista Clients** and the **Default Domain Policy**.
6. On LON-CL1, click **Start**, type **wf.msc** into **the Start Search** box. and then press ENTER.
7. In Windows Firewall with Advanced Security, right-click **Windows Firewall with Advanced Security on Local Computer**, and then click **Properties**.
8. Note that the **Firewall State** setting on the **Public Profile** is **On** (recommended), and that the list control is disabled, preventing a local user, even an administrator, from modifying the setting.

Demonstration: Configuring Connection Security Rules in Windows Firewall with Advanced Security

Create a new connection security rule and review the available rule settings

1. On LON-CL1, click **Start,** type **wf.msc** into the **Start Search** box, and then press ENTER.
2. In Windows Firewall with Advanced Security, click **Connection Security Rules**.
3. Click **New rule** in the Actions pane.
4. Ensure that **Isolation** is selected in the **Rule Type** window, and then click **Next.**
5. Ensure that **Request authentication for inbound and outbound connections** is selected in the **Requirements** window, an d then click **Next.**
6. Select **Computer (Kerberos v5)** in the **Authentication method** window, and then click **Next.**
7. Select **Domain** in the **Profile** window, and then click **Next.**
8. Enter **Contoso computers** in the **Name** field, and then click **Finish.**
9. Right-click the **Contoso computers** rule, and then click **Properties.**
10. On the **Advanced** tab, click **Customize** next to **Interface types**.
11. Select **These interface types**, and then select **Remote access.**
12. Click **OK.**

13. Walk students through the other settings that can be changed in rule properties.
14. Click **OK** when finished.
15. Right-click the **Contoso computers** rule, and then click **Disable Rule**.

Additional Reading

Overview of IPsec

For more information on IPsec, see http://go.microsoft.com/fwlink/?LinkId=102229&clcid=0x409.

What Are Connection Security Rules?

- For an introduction to Windows Firewall with Advanced Security, go to http://go.microsoft.com/fwlink/?LinkId=102232&clcid=0x409.
- For more information on connection security rules see Windows Firewall with Advanced Security Help Topic: Connection Security Rules.

Choosing a Connection Security Rule Type

For more information on choosing a connection security rule, see Windows Firewall with Advanced Security Help: Choosing a Connection Security Rule Type.

Authentication Methods

For more information on authentication methods, see Windows Firewall with Advanced Security Help: Authentication methods.

Determining a Usage Profile

For more information on firewall profiles, see Windows Firewall with Advanced Security Help: Firewall Properties – Profiles.

For more information on Windows Firewall with Advanced Security, see http://go.microsoft.com/fwlink/?LinkId=102232&clcid=0x409.

Lesson 5

Configuring Wireless Networks

Contents:

Question and Answers

Demonstration: Configuring Wireless Network Settings with Group Policy

Question: Does the wireless policy for Windows Vista require each profile to specify a unique Service Set Identifier (SSID)?

Answer: No, the new Windows Vista Wireless Network Policies enable configuration and management of multiple wireless profiles that each use different profile names and different wireless settings while using the same SSID.

Detailed Demo Steps

Demonstration: Configuring Wireless Network Settings with Group Policy

Detailed demonstration steps

Create an organizational unit and put the client computer account in it

1. On LON-DC1, click **Start,** and then click **Server Manager**.
2. Expand **Roles,** expand **Active Directory Domain Services**, and then expand **Active Directory Users and Computers**.
3. Right-click **Contoso.com**, click **New**, and then click **Organizational unit.**
4. Enter **Wireless Clients** in the **Name** field, and then click **OK.**
5. Click the **Vista Clients** container.
6. Right-click **LON-CL1,** and then click **Move.**
7. Select the **Wireless Clients** OU, and then click **OK**.

Create a new Group Policy object (GPO) and configure the wireless settings for client computers

1. On LON-DC1, in Server Manager, expand **Features**, expand **Group Policy Management,** expand **Forest: Contoso.com**, expand **Domains,** and then expand **contoso.com.**
2. Right-click the **Wireless Clients** OU, and then click **Create a GPO in this domain, and link it here**.
3. Enter **Wireless Settings for Vista Clients** into the **Name** field, and then click **OK.**
4. In the main window, right-click the **Wireless Settings for Vista Clients** GPO, and then click **Edit.**
5. In the Group Policy Editor, right-click the **Wireless Settings for Vista Clients [LON-DC1.contoso.com] Policy** icon, and then click **Properties.**
6. Select the **Disable User Configuration settings** check box, and then click **Yes** when prompted to confirm**.**
7. Click **OK t**o close the window.
8. Expand **Computer Configuration**, expand **Policies,** expand **Windows Settings**, expand **Security Settings**, and then click **Wireless Network (IEEE 802.11) Policies**.
9. Right-click in the details pane on the right of the console with the **Wireless Network Policies** node highlighted, and then select **Create a New Windows Vista Policy.**
10. Enter **Contoso Wireless Network Policy** in the **Name** field.
11. Click **Add**, and then click **Infrastructure**.
12. Enter **Default Contoso profile** in the **Name** field.
13. Enter **Contoso** in the **Network Name(s) (SSID)** field, and then click **Add.**
14. Highlight **NEWSSID**, and then click **Remove.**
15. Click **OK.**

16. On the **Network Permissions** tab, select the **Prevent connections to ad-hoc networks** check box**.**
17. Click **OK.**

Test the wireless settings

1. On LON-CL1 click **Start,** click **All Programs**, click **Accessories**, and then click **Command Prompt**.
2. Type the following command and then press ENTER: **gpupdate /force.**
3. Wait until the command finishes before moving to the next step.
4. To validate that the GPO was correctly applied, type the following command and then press ENTER: **gpresult /r /scope computer.**
5. In the output, look for the **Applied Group Policy Objects** section. Confirm that it contains entries for both **Wireless Settings for Vista Clients** and the **Default Domain Policy.**

Module Reviews and Takeaways

Review questions

1. What is the primary benefit of using IPv6 addresses?

   Answer: The primary benefit of IPv6 is its increased addressing capacity. IPv6 addresses are 128 bits, compared to IPv4 32-bit addresses. This improvement provides for a radically expanded address space.

2. What does an IPv6 address look like?

   Answer: An IPv6 address has eight groups of hexadecimal characters (the numbers 0–9 and the letters A–H) separated by colons—for example, 3ffe:ffff:0000:2f3b:02aa:00ff:fe28:9c5a. The leading zeroes in a section can be suppressed—for example, 3ffe:ffff:0:2f3b:2aa:ff:fe28:9c5a.

3. Why do some IPv6 addresses contain double colons?

   Answer: A double colon indicates that part of the address containing only zeroes has been compressed, to help make the address shorter. For example, the IPv6 address fe80:0:0:0:2aa:ff:fe9a:4ca2 could be written like this: fe80::2aa:ff:fe9a:4ca2.

Common issues related to IPv6

Identify the causes for the following common issues related to IPv6 and fill in the troubleshooting tips. For answers, refer to relevant lessons in the module.

Issue	Troubleshooting tip
Connections to certain hosts are not working properly.	Check for packet filtering. This is the same process used for verifying IPv6 connectivity, but sometimes packet filtering will block one type of incoming connection. Also, verify TCP connection establishment with Telnet.
The Link Local address is not available.	Verify that the NIC is inserted correctly. Verify that you have IPv4 connectivity.
You can reach hosts using IPv6 addresses, but you can't reach hosts using the host names.	You might have a problem with host-name resolution. • Verify DNS configuration. • Display and flush the DNS client resolver cache. • Test DNS name resolution with the ping tool. • Use the Nslookup tool to view DNS server responses.

Real-world issues and scenarios

1. When migrating from IPv4 or IPv6, one of the common issues is that certain applications, even after they are ported to IPv6, do not turn on IPv6 support by default. You might have to configure these applications to turn on IPv6.
2. Adding an AAAA record for a service in DNS may result in some users losing connectivity and others experiencing unusually high latency. The root cause for connectivity loss is usually that the end user is on another network with IPv6 on their PC but no form of IPv6 connectivity.

Best practices related to IPv6

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

- When deploying IPv6 into an existing IPv4 environment, don't assume that in order to use it, you must immediately deploy native IPv6 addressing and routing. You can deploy tunneled IPv6 connectivity using the Intra-Site Automatic Tunnel Addressing Protocol (ISATAP). ISATAP traffic can traverse an IPv4-only intranet, so you can begin testing IPv6-capable applications immediately, without having to wait for a native IPv6 infrastructure.
- When planning migration from IPv4 to IPv6, consider the applications that you will use, your network devices, and potential device upgrades that may need to occur.

Tools

Tool	Use	Where to find it
IPconfig	Command-line utility that prints out the TCP/IP-related configuration data of a host	Included in the operating system
Ping	Sending ICMPv6 or ICMP Echo Request messages to perform network diagnostics and test reachability for a specific destination	Included in the operating system
Tracert	Sending ICMPv6 or ICMP Echo Request messages to produce command-line report information about each router that is crossed and the roundtrip time (RTT) for each hop	Included in the operating system
Netsh	Contains many commands that are useful for analyzing the current IPv6 configuration and troubleshooting problems; for example, displays general IPv6 settings, all DNS servers that have been configured for IPv6, etc.	Included in the operating system

Lab Review Questions and Answers

1. What does an ISATAP router allow an IPv6/IPv4 hybrid node to do?

   Answer: It allows the hybrid node to communicate with other IPv6 interfaces. It also allows IPv6 hosts to communicate with other IPv6 networks over an IPv4 subnet.

2. What do you need to define on the DNS server in order for an ISATAP router to function properly?

   Answer: You must define a DNS A record or host record named ISATAP, and then point it to the IPv4 address of the ISATAP router. This allows hosts to discover the ISATAP router on the IPv4 network. However, this can be done in one of two ways: 1.) Static Netsh configuration (see course 6421) 2.) DNS based automatic discovery. This is important because it is a fundamental setting to enable DirectAccess in Windows 7.

3. What does advertising a prefix do when a prefix in the IPv6 router is being defined?

   Answer: It allows clients to know between what prefixes the router will route. It also allows clients to configure themselves with the appropriate prefix.

Module 4

Configuring Network Policy Server and Remote Access Services

Contents:

Lesson 2

Configuring a Network Policy Server

Contents:

Question and Answers

Demonstration: Installing NPS

Question: Why does NPS server need to be registered in Active Directory?

Answer: NPS servers must be registered in Active Directory so that they have permission to read the dial-in properties of user accounts during the authorization process. Registering an NPS server adds the server to the RAS And IAS Servers group in Active Directory.

Demonstration: Configuring a RADIUS Client and a RADIUS Server

Question: Provide some examples of a RADIUS client.

Answer: RADIUS clients are network access servers—such as wireless access points, 802.1X authenticating switches, VPN servers, and dial-up servers.

Demonstration: Creating a Connection Request Policy

Question: How do connection request policies help manage RADIUS request messages?

Answer: With connection request policies, you can create a series of policies so that some RADIUS request messages sent from RADIUS clients are processed locally or forwarded to remote RADIUS servers.

Detailed Demo Steps

Demonstration: Installing NPS

Detailed demonstration steps

In this demonstration, you will see how to:

- Install the Network Policy Server (NPS) role service.
- Register NPS in Active Directory.

Install the Network Policy Server role service

1. Log on to **LON-DC1** as **Administrator**, and start **Server Manager**.
2. In the **Server Manager** list pane, right-click **Roles**, and select **Add Roles** from the context menu.
3. Select the **Network Policy and Access Services** role.
4. In **Select Role Services**, in **Role services**, select **Network Policy Server**
5. On the **Installation Results** page, verify that the installation was successful. The Network Policy Server role is installed on LON-DC1.
6. Close the Server Manager.

Register NPS in Active Directory

1. On LON-DC1, click **Start**, and then click **Administrative Tools**.
2. Start the **Network Policy Server** administrative tool.
3. In the list pane, select and right-click **NPS (Local)**, and then click **Register server in Active Directory**.

Demonstration: Configuring a RADIUS Client and a RADIUS Server

In this demonstration, you will see how to:

- Add a RADIUS Client in NPS.
- Configure a RADIUS server for dial-up or VPN connections.

Add a RADIUS client in NPS

1. On LON-DC1, click **Start**, click **Administrative Tools**, and then click **Network Policy Server**. The NPS console opens.
2. In the NPS console, expand **RADIUS Clients and Servers**. Right-click **RADIUS Clients**, and then click **New RADIUS Client**.
3. In **New RADIUS Client** dialog box, verify that the **Enable this RADIUS client** check box is selected.
4. In the **New RADIUS Client** dialog box, in the **Friendly name** field, type **LON-SVR1**. In the **Address (IP or DNS)** field, type **LON-SVR1**, and then click **Verify**.
5. Click **Resolve**, and then click **OK**.

6. In the **New RADIUS Client** dialog box, ensure that **Manual** is selected, and then in the **Shared secret** box, type **Pa$$w0rd**. Retype the shared secret in **Confirm shared secret** box.
7. Click **OK**. LON-SVR1 appears in the list of RADIUS clients configured on the NPS server.

Configure a RADIUS server for dial-up or VPN connections

1. In the Network Policy Server management tool list pane, click **NPS (Local)**.
2. In the Getting Started pane, in the list under **Standard Configuration**, click **RADIUS server for Dial-Up or VPN Connections**.
3. Under **Radius server for Dial-Up or VPN Connections**, click **Configure VPN or Dial-Up**.
4. In the **Configure VPN or Dial-Up** dialog box, select **Virtual Private Network (VPN) Connections**, accept the default name, and then click **Next**.
5. In the **Specify Dial-up or VPN Server** dialog box, click **Next**.
6. In the **Configure Authentication Methods** dialog box, select **Extensible Authentication Protocol and Microsoft Encrypted Authentication version 2** (**MS-CHAPv2)**, and then click **Next**.
7. On the **Specify User Groups** page, click **Add**, type **contoso\IT**, and then click **OK**.
8. On the **Specify IP Filters** page, click **Next**.
9. On the **Specify Encryption Settings** page, clear the **Basic encryption** and **Strong encryption** check boxes, and then click **Next**.
10. On the **Specify a Realm Name** page, click **Next**.
11. On the **Completing New Dial-Up or Virtual Private Connections and RADIUS clients** page, click **Finish**.
12. Close the **Network Policy Server** administrative tool.

Demonstration: Creating a Connection Request Policy

In this demonstration, you will see how to:

- Create a new Connection Request Policy and set up forwarding of RADIUS requests.

Create a connection request policy and forward RADIUS requests

1. On LON-DC1, click **Start**, click **Administrative Tools**, and then click **Network Policy Server**.
2. Expand **Policies** under **NPS (local)**.
3. Right-click **Connection request policies**, and then select **New**.
4. Enter **VPN** in the **Policy Name** field, and then select **Remote Access Server (VPN-Dial up)** from the menu.
5. Click **Add** to add a condition.
6. Scroll down, and double-click **Client IPv4 Address**. Then type **10.10.0.50** in the **Client IPv4 Address** dialog box, and click **OK**.
7. Click **Next**.
8. In the Specify Connection Request Forwarding window, click **New** to create a new RADIUS server group.

9. Enter **RADIUS** in the **Group name** field, and then click **Add**.
10. Enter **10.10.0.10** in the **Server** field, and then click **OK** twice.
11. Ensure that **RADIUS** is selected in the menu.
12. Select **Forward requests to the following remote RADIUS server group for authentication**, and then click **Next** twice.
13. Click **Finish**.

Additional Reading

Configuring NPS RADIUS Clients

For more information on RADIUS clients, see Network Policy Server Help: RADIUS Clients.

Configuring Connection Request Processing

For more information, see the following Help Topics:

- Network Policy Server Help: Connection Request Policies
- Network Policy Server Help: Configure NPS UDP Port information

Password-Based Authentication Methods

For more information on password-based authentication, see Help Topic: Password-Based Authentication Methods.

Using Certificates for Authentication

For more information on using certificates with NSP, see Help Topic: Certificates and NPS.

Administering and Monitoring NPS

For more information on NPS best practices, see Help Topic: NPS Best Practices.

Configuring Logging

For more information, see the following Help Topics:

- Help Topic: Configure Log File Properties
- Help Topic: NPS Best Practices

Lesson 3

Configuring Remote Access

Contents:

Question and Answers

Demonstration: Installing Routing and Remote Access Services

Question: What functionality is provided by configuring RRAS as a remote access server?

Answer: By configuring RRAS to act as a remote access server, you can connect remote or mobile workers to your organization's networks. Remote users can work as if their computers are directly connected to the network.

VPN Tunneling Protocols

Question: What are virtual private networks?

Answer: Virtual private networks are point-to-point connections across a private or public network such as the Internet.

Demonstration: Deploying SSTP Remote Access

Question: What are the RRAS server certificate requirements for SSTP VPN connections?

Answer: The computer certificate on the RRAS server must have either the Server Authentication or All-Purpose enhanced key usage (EKU) property. This computer certificate is used by the VPN client to authenticate the RRAS server when the session is established.

Demonstration: Creating a Connection Profile

Question: What format is the connection profile created in?

Answer: The CMAK wizard compiles the connection profile into a single executable file with an .exe file name extension. You can deliver this .exe file to your users through any method available to you, such as with software distribution tools.

Detailed Demo Steps

Demonstration: Installing Routing and Remote Access Services

Detailed demonstration steps

In this demonstration, you will see how to:

- Install the AD CS role.
- Configure automatic certificate enrollment.
- Install the RRAS role.

> **Note:** If configuring RRAS as an SSTP VPN server (we will cover it later in this lesson), the ADCS role needs to be installed before the RRAS role is installed.

Install and configure the AD CS role

1. On LON-DC1, click **Start**, point to **Administrative Tools,** and then click **Server Manager.**
2. In Server Manager, select and then right-click **Roles**, and then **click Add Roles** from the context menu.
3. In the Add Roles Wizard, click **Next.**
4. On the **Select Server Roles** page, **select Active Directory Certificate Services**, and then click **Next**.
5. On the **Introduction to Active Directory Certificate Services** page, click **Next**.
6. On the **Select Role Services** page, select **Certification Authority** and **Certification Authority Web Enrollment**.
7. Click **Add Required Role Services** when prompted, and then click **Next.**
8. On the **Specify Setup Type** page, click **Next**.
9. On the **Specify CA Type** page, click **Next.**
10. On the **Set Up Private Key** page, click **Next**.
11. On the **Configure Cryptography for CA** page, click **Next.**
12. On the **Configure CA Name** page, specify a name of **Contoso-CA,** and then click **Next**.
13. On the **Set Validity Period** page, click **Next.**
14. On the **Configure Certificate Database** page, click **Next.**
15. On the **Web Server (IIS)** page, click **Next**.
16. On the **Select Role Services** page, click **Next.**
17. On the **Confirm Installation Selections** page, review all selections, and then click **Install.**
18. On the **Installation Results** page, click **Close.**
19. Close **Server Manager**.
20. Click **Start**, point to **Administrative Tools,** and then click **Certification Authority.**
21. In the Certsrv management console, expand **Contoso-CA.**

22. Right-click **Certificate Templates**, and then select **Manage** from the context menu.
23. In the Certificate Templates Console pane, right-click **Computer,** and then choose **Properties** from the context menu.
24. In the **Computer Properties** dialog box, on the **Security** tab, select **Authenticated Users.**
25. In **Permissions for Authenticated Users**, select the **Allow** check box for the **Enroll** permission, and then click **OK.**
26. Close the **Certificate Template** console.
27. In the Certsrv management console, right click **Contoso-CA**, and select **Properties.**
28. Click **View Certificate**.
29. On the **Details** tab, click **Copy to File**.
30. Click **Next** twice, enter **\\lon-dc1\templates\lon-dc1.cer**, and then click **Next.**
31. Click **Finish,** and then click **OK** when prompted with the confirmation message.
32. Click **OK** to close **Certificate,** and then click **OK** to close **Contoso-CA Properties**.
33. Close the **certsrv** management console.

Configure automatic certificate enrollment

1. On LON-DC1, click **Start**, and then click **Administrative Tools**.
2. On the **Administrative Tools** menu, click **Group Policy Management**. The Group Policy Management tool appears.
3. In the Group Policy Management list pane, expand **Forest: Contoso.com**, expand **Domains,** and then expand **Contoso.com.**
4. In the list pane, under **Contoso.com**, right-click **Default Domain Policy**, and then click **Edit**.
5. On the **Group Policy Management Editor** page, under **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, and then expand **Public Key Policies.**
6. Right-click **Automatic Certificate Request Settings**, point to **New,** and then click **Automatic Certificate Request**.
7. In the **Welcome to the Automatic Certificate Request Setup Wizard**, click **Next.**
8. On the **Certificate Template** page, accept the default setting of **Computer**, and then click **Next**.
9. On the **Completing the Automatic Certificate Request Setup Wizard** page, click **Finish.**
10. Close the **Group Policy Management Editor.**
11. Close the **Group Policy Management** tool. Automatic certificate enrollment now is configured for domain computers in the Contoso domain.
12. On LON-CL1, click **Start,** type **cmd** in the **Search** box, and then press ENTER.
13. In the command window, type **gpupdate /force**, and then press ENTER. Wait for the policy processing to complete.

14. To verify automatic certificate enrollment on LON-SVR1: on LON-SVR1, click **Start**, type **cmd,** and then press ENTER.
15. In the Command Prompt window, type **gpupdate /force**, and then press ENTER. Wait for the policy processing to complete.
16. Click **Start,** type **MMC** in the **Search** box, and then press ENTER.
17. In the Console1 window, click **File,** and then click **Add/Remove Snap-in**.
18. In the **Add or Remove Snap-ins** box, select **Certificates**, and then click **Add.**
19. In the **Certificates snap-in** box, select **Computer account**, and then click **Next.**
20. In the **Select Computer** box, select **Local computer**, and then click **Finish**.
21. Click **OK** to close the **Add or Remove Snap-ins** box.
22. In the Console1 window, expand **Certificates (Local Computer).**
23. Expand **Personal,** and then click **Certificates.** Notice that LON-SVR1.Contoso.com is displayed. Also notice that Contoso-CA issued the certificate. You now can use this certificate as an authentication mechanism.

    Note: If the certificate is missing, follow the following steps:

24. Expand **Trusted Root Certification Authorities**, and then click **Certificates.**
25. Right-click **Certificates,** select **All Tasks**, and then select **Import.**
26. Click **Next,** type **\\LON-DC1\templates\lon-dc1.cer** in the **File Name** field, and then click **Next.**
27. Click **Next**, and then click **Finish** to close the wizard.
28. Click **OK**.
29. Expand **Certificates (Local Computer),** right-click **Personal**, click **All Tasks**, and then select **Request New Certificate.**
30. Click **Next**, select **Computer**, and then click **Enroll**.
31. Click **Finish.**
32. Close the **Console1** window.
33. Click **No** when prompted to save console settings.

Install the RRAS role

1. On LON-SVR1, start **Server Manager**.
2. In Server Manager, click **Roles**, and then click **Add Roles.**
3. Select **Network Policy and Access Services**, and then select **Routing and Remote Access Services** role service.
4. On the **Installation Results** page, verify **Installation succeeded** appears in the details pane, and then click **Close.** The RRAS role is installed on LON-SVR1.

Demonstration: Configuring a VPN Server

In this demonstration, you will see how to:

- Configure a VPN server with a static address pool for remote access clients.
- Specify RADIUS authentication and accounting.

Configure a VPN server with a static address pool for remote access clients, and specify RADIUS authentication and accounting

1. On LON-SVR1, start the **Routing and Remote Access** tool.
2. In the list pane, select and right-click the server, and then click **Configure and Enable Routing and Remote Access.**
3. On the **Configuration** page, leave the default **Remote access (dial-up or VPN)** selected.
4. On the **Remote Access** page, select the **VPN** option.
5. On the **VPN Connection** page, select the **Local Area Connection 2** interface.
6. On the **IP Address Assignment** page, select **From a specified range of addresses.**
7. On the **Address Range Assignment** page, click **New,** and in the **Start IP address** box, type **192.168.1.150.** In the **Number of addresses** box, type **50.**
8. On the **Managing Multiple Remote Access Servers** page, select **Yes, set up this server to work with a RADIUS server.**
9. On the **RADIUS Server Selection** page, specify **LON-DC1** for the Primary RADIUS server. Specify **Pa$$w0rd** as the shared secret for the RADIUS server.

   After completing, the Routing and Remote Access service starts. LON-SVR1 is configured as a VPN server with RADIUS configured.

Demonstration: Deploying SSTP Remote Access

In this demonstration, you will see how to:

- Configure a VPN connection.
- Configure and test an SSTP-based VPN connection.

Configure a VPN connection

1. On LON-CL1, click **Start**, and then click **Control Panel.**
2. Click **Network and Internet**, click **Network and Sharing Center**, and then click **Set up a connection or network.**
3. Click **Connect to a workplace**, and then click **Next**.
4. Click **Use my Internet connection (VPN).**
5. Click **I'll set up an Internet connection later**.
6. In **Internet address**, **type LON-SVR1.contoso.com**, and then click **Next.**
7. In the **Type your user name and password** dialog box, type the following information:

   In **User name**, type **Ed.**

   In **Password,** type **Pa$$w0rd.**

Click **Remember this password.**

In **Domain,** type **contoso.**

8. Click **Create,** and then click **Close.**

Configure and test an SSTP-based VPN connection

1. In the Network and Sharing Center, click **Manage network connections**.
2. Double-click **VPN Connection**, and then click **Properties.**
3. On the **Networking** tab, in the **Type of VPN** list, **select Secure Socket Tunneling Protocol (SSTP),** and then click **OK.**
4. In the **Connect VPN Connection** dialog box, click **Connect.**

Demonstration: Creating a Connection Profile

In this demonstration, you will see how to:

- Install CMAK.
- Create a new connection profile by using CMAK.

Install CMAK

1. On LON-SVR1, click **Start**, click **Administrative Tools**, and then click **Server Manager**.
2. In Server Manager, click **Features**, and then click **Add Features**.
3. In the list, select **Connection Manager Administration Kit.**
4. On the confirmation page, click **Install.**

Create a new connection profile by using CMAK

1. On LON-SVR1, click **Start,** click **Administrative Tools**, and then click **Connection Manager Administration Kit.**
2. On the **Welcome** page, click **Next.**
3. Select **Windows Vista**, and then click **Next.**
4. On the **Create or Modify a Connection Manager profile** page, click **Next.**
5. Type **Contoso Corporate** in the **Service name** field.
6. Type **contoso** in the **File name** field, and then click **Next**.
7. Click **Next** twice.
8. On the **Add Support for VPN Connections** page, select **Phone book from this profile**, and then enter **LON-SVR1.contoso.com** into the **Always use the same VPN server** field.
9. On the **Create or Modify a VPN Entry** page, accept the default value, **Contoso corporate Tunnel**, and click **Edit**.
10. On the **Security** tab, select **Only use Secure Socket Tunneling Protocol (SSTP)** from the **VPN strategy** list.
11. On the **Advanced** tab, enter **contoso.com** in the **DNS suffix for this connection's address in DNS** field, select both check boxes, and then click **OK.**

12. Click **Next.**
13. On the **Add a Custom Phone Book** page, clear the **Automatically download phone book updates** check box, and then click **Next.**
14. Click **Next** on the **Configure Dial-up Networking Entries** page.
15. Click **Next** on the **Specify Routing Table Updates** page.
16. On the **Configure Proxy Settings for Internet Explorer** page, click **Next.**
17. On the **Add Custom Actions** page, click **Next.**
18. On the **Display a Custom Logon Bitmap** page, click **Next.**
19. On the **Display a Custom Phone Book Bitmap** page, click **Next.**
20. On the **Display Custom Icons** page, click **Next.**
21. On the **Include a Custom Help File** page, click **Next.**
22. Enter **Please call your Helpdesk for support** in the **Support information** field, and then click **Next.**
23. On the **Display a Custom License Agreement** page, click **Next**.
24. On the **Install Additional Files with the Connection Manager profile** page, click **Next.**
25. Click **Next,** and then click **Finish** to complete the wizard.

Additional Reading

VPN Tunneling Protocols

For more information about RRAS, see Routing and Remote Access Service Help: VPN Tunneling Protocols.

VPN Server Configuration Requirements

For more information on configuring a remote access VPN server, see Routing and Remote Access Service Help: Configure a Remote Access VPN Server.

Configuring a Connection Profile with CMAK

For more information, see the following Help Topics:

- Connection Manager Administration Kit Help: Run the CMAK Wizard to Create a Connection Profile
- Connection Manager Administration Kit Help: Distribute Your Connection Profile to Your Users

Module Reviews and Takeaways

Review questions

1. How can you make the most effective use of the NPS logging features?

   Answer: You can make the most effective use of the NPS logging features by performing the following tasks:

- Turn on logging (initially) for both authentication and accounting records. Modify these selections after you determine what is appropriate for your environment.
- Ensure that you configure logging with sufficient capacity to maintain your logs.
- Back up all log files on a regular basis, because they cannot be recreated when damaged or deleted.
- To provide failover and redundancy with SQL Server logging, place two computers running SQL Server on different subnets. Use the SQL Server Create Publication Wizard to set up database replication between the two servers.

2. Is it possible to ignore the dial-in properties assigned to accounts in Active Directory with network policies? In what property category would this be set?

   Answer: Yes, in the Overview properties, you can specify to ignore the dial-in settings assigned to the account in Active Directory.

3. You want to evaluate the overall health and security of the NAP-enforced network. What do you need to do to start recording NAP events?

   Answer: NAP trace logging is disabled by default and you should enable it if you want to troubleshoot NAP-related problems or evaluate the overall health and security of your organization's computers. You can use the NAP Client Management console or the Netsh command-line tool to enable logging functionality.

Common issues related to NPS

Identify the causes for the following common issues related to NPS and fill in the troubleshooting tips. For answers, refer to relevant lessons in the module.

Issue	Troubleshooting tip
You have enabled RADIUS logging and verified that the logs are gathering the requested information. After a few weeks, users begin to call the Help Desk because their connection attempts are failing. What is the most likely problem?	If RADIUS accounting fails due to a full hard-disk drive or other reasons, NPS stops processing connection requests, which prevents users from accessing network resources. Make sure the logs do not fill up all available hard disk space.
You choose to use a nonstandard port assignment for RADIUS traffic. The RADIUS traffic cannot get through the firewall.	If you do not use the RADIUS default port numbers, you must configure exceptions on the firewall for the local computer to allow RADIUS traffic on the new ports.

Real-world issues and scenarios

1. You may not be able to open the firewall to PPTP and L2TP traffic due to security reasons. To create a VPN solution in Windows Server 2008, you can use SSTP—a new VPN protocol that can be used to create secure VPN tunnels over TCP port 443.

2. One scenario where NAP could be very useful is the enforcement of a security policy that calls for updates to Windows clients to be installed within a two-week period. You can use NAP to enforce the presence of each update on clients. After two weeks from the release of the update, any noncompliant clients could be prevented from connecting to the corporate network.

Best practices related to NPS

Some of the best practices include the following:

- Install and test servers running NPS or RRAS before configuring them as RADIUS clients.
- Disable authentication protocols that you do not use.
- Determine the desired logging levels for auditing purposes and back up RADIUS logs.
- After you install and configure NPS, save the configuration with the Netsh Nps Show Config > Path\File.txt command. Save the NPS configuration with the Netsh Nps Show Config > Path\File.txt command each time a change is made.
- Use strong enforcement methods (IPsec, 802.1x, and VPN). Strong enforcement methods provide the most secure and effective NAP deployment.

Tools

Tool	Use	Where to find it
Routing and Remote Access management tool	• Managing and configuring the Routing and Remote Access service on the local server	Routing And Remote Access on the Administrative Tools menu.
Network Policy Server	• Managing and creating network policy	Network Policy Server on the Administrative Tools menu.
Connection Manager Administration Kit	• Creating customized, distributable connection objects for installation on client's computers	Connection Manager Administrative Kit on the Administrative Tools menu. (CMAK is an optional Windows Server 2008 feature.)
Configure NAP wizard	• Creating the health policies, connection request policies, and NAP with Network Policy Server.	Open the NPS (Local) console. In Getting Started, under Standard Configuration, select Network Access Protection (NAP), and then click Configure NAP.

Lab Review Questions and Answers

1. What does a RADIUS proxy provide?

   Answer: When you use NPS as a RADIUS proxy, NPS forwards connection requests to NPS or other RADIUS servers for processing. Because of this, the domain membership of the NPS proxy is irrelevant. The proxy does not need to be registered in Active Directory because it does not need access to the dial-in properties of user accounts. Additionally, you do not need to configure network policies on an NPS proxy, because the proxy does not perform authorization for connection requests. The NPS proxy can be a domain member or it can be a stand-alone server with no domain membership.

2. What is a RADIUS client, and what are some examples of RADIUS clients?

   Answer: A network access server (NAS) is a device that provides some level of access to a larger network. A NAS using a RADIUS infrastructure also is a RADIUS client, sending connection requests and accounting messages to a RADIUS server for authentication, authorization, and accounting.

   Examples of network access servers are:

   - Network access servers that provide remote access connectivity to an organization network or the Internet. An example is a computer running Windows Server 2008 and the Routing and Remote Access service that provides either traditional dial-up or VPN remote access services to an organization intranet.
   - Wireless access points that provide physical layer access to an organization network, using wireless-based transmission and reception technologies.
   - Switches that provide physical-layer access to an organization's network, using traditional LAN technologies such as Ethernet.
   - RADIUS proxies that forward connection requests to RADIUS servers that are members of a remote RADIUS server group that is configured on the RADIUS proxy.

Module 5

Configuring Network Access Protection

Contents:

Lesson 1

Overview of Network Access Protection

Contents:

Question and Answers

What Is Network Access Protection?

Question: How would you use NAP enforcement in your environment, considering home users, roaming laptops, and outside business partners?

Answer: Answers may vary.

NAP Scenarios

Question: Have you ever had an issue with unsecure, unmanaged laptops causing harm to your network? Do you think NAP would have addressed this issue?

Answer: Answers may vary.

NAP Enforcement Methods

Question: Which of the NAP enforcement types would best suit your company? Can you see your organization using multiple NAP enforcement types? If so, which ones?

Answer: Answers may vary.

IPsec Enforcement

Question: For which computers in the secure network would you allow unsecure communication from computers in the restricted network to succeed?

Answer: You can create IP filters to allow certain communications to remain unauthenticated. A Web server might be such a server.

802.1x Enforcement

Question: What must the network devices support to implement 802.1x NAP?

Answer: Network devices must support 802.1x authentication.

DHCP Enforcement

Question: Does the DHCP NAP enforcement type work on IPv6 networks?

Answer: No. It is available only for IPv4 scopes

Demonstration: Configuring NAP Enforcement for DHCP

Question: What is client health and what are some of the health measurement examples?

Answer: Health is defined as information about a client computer that NAP uses to determine whether to allow or deny client access to a network. Some of the example measurements of health include:

- The operational status of Windows Firewall—whether it is enabled or disabled
- Status of an antivirus signature—is it the most recent one available?
- The installation status of security updates. Are the most recent security updates installed on the client?

Detailed Demo Steps

Demonstration: Configuring NAP Enforcement for DHCP

Detailed demonstration steps

In this demonstration, you will see how to:

- Install the Network Policy Server role service.
- Configure the Network Policy Server as a NAP health policy server.
- Configure DHCP service for NAP enforcement.
- Configure the client computer as a DHCP and NAP client.
- Test NAP enforcement.

Install the Network Policy Server role service

1. On LON-DC1, in Server Manager, right-click **Roles,** and then select **Add Roles** from the context menu.
2. On the **Before you Begin** page, click **Next.**
3. On the **Select Server Roles** page, select the **Network Policy and Access Services** check box, and then click **Next** twice.
4. On the **Select Role Services** page, select the **Network Policy Server** check box, and then click **Next**.
5. On the **Confirm Installation Selections** page, click **Install**.
6. Verify the installation was successful, and then click **Close.**
7. Close the Server Manager window.

Configure the Network Policy Server as a NAP health policy server

1. On LON-DC1, open the **Network Policy Server** Management console from the **Start** menu by clicking **Administrative Tools.**
2. Configure SHVs:
3. Expand **Network Access Protection**, and then click **System Health Validators**.
    a. In the middle pane under **Name**, double-click **Windows Security Health Validator**.
    b. In the **Windows Security Health Validator Properties** dialog box, click **Configure**.
    c. On the **Windows Vista** tab, clear all check boxes except **A firewall is enabled for all network connections**.
    d. Click **OK** to close the **Windows Security Health Validator** dialog box, and then click **OK** to close the **Windows Security Health Validator Properties** dialog box.
4. Configure remediation server groups:
    a. In the console tree, under **Network Access Protection**, right-click **Remediation Server Groups**, and then click **New**.
    b. Under **Group Name**, type **Rem1.**

c. Next to **Remediation Servers**, click **Add.**

d. In the **Add New Server** dialog box, under **IP address or DNS name**, type **10.10.0.10**, and then click **OK** twice.

5. Configure health policies:

a. Expand **Policies**.

b. Right-click **Health Policies**, and then click **New**.

c. In the **Create New Health Policy** dialog box, under **Policy Name**, type **Compliant**.

d. Under **Client SHV checks**, verify that **Client passes all SHV checks** is selected.

e. Under **SHVs used in this health policy**, select the **Windows Security Health Validator** check box, and then click **OK**.

f. Right-click **Health Policies**, and then click **New**.

g. In the **Create New Health Policy** dialog box, under **Policy Name**, type **Noncompliant**.

h. Under **Client SHV checks**, select **Client fails one or more SHV checks**.

i. Under **SHVs used in this health policy**, select the **Windows Security Health Validator** check box, and then click **OK**.

6. Configure a network policy for compliant computers:

a. In the console tree, under **Policies**, click **Network Policies**.

b. Disable the two default policies under **Policy Name** by right-clicking the policies, and then clicking **Disable** for each.

c. Right-click **Network Policies**, and then click **New**.

d. In the Specify Network Policy Name and Connection Type window, under **Policy name**, type **Compliant-Full-Access**, and then click **Next**.

e. In the **Specify Conditions** window, click **Add**.

f. In the **Select condition** dialog box, double-click **Health Policies**.

g. In the **Health Policies** dialog box, under **Health Policies**, select **Compliant**, and then click **OK**.

h. In the Specify Conditions window, verify that **Health Policy** is specified under **Conditions** with a value of **Compliant**, and then click **Next**.

i. In the Specify Access Permission window, verify that **Access granted** is selected, and then click **Next**.

j. In the Configure Authentication Methods window, select **Perform machine health check only**. Clear all other check boxes, and then click **Next**.

k. In the Configure Constraints window, click **Next**.

l. In the Configure Settings window, click **NAP Enforcement**. Verify that **Allow full network access** is selected, and then click **Next**.

m. In the Completing New Network Policy window, click **Finish** to complete configuration of your network policy for compliant client computers.

7. Configure a network policy for noncompliant computers:
    a. Right-click **Network Policies**, and then click **New**.
    b. In the Specify Network Policy Name and Connection Type window, under **Policy name**, type **Noncompliant-Restricted**, and then click **Next**.
    c. In the **Specify Conditions** window, click **Add**.
    d. In the **Select condition** dialog box, double-click **Health Policies**.
    e. In the **Health Policies** dialog box, under **Health policies**, select **Noncompliant**, and then click **OK**.
    f. In the Specify Conditions window, verify that **Health Policy** is specified under **Conditions** with a value of **Noncompliant**, and then click **Next**.
    g. In the Specify Access Permission window, verify that **Access granted** is selected, and then click **Next**.

    Note: A setting of Access Granted does not mean that noncompliant clients are granted full network access. It specifies that clients matching these conditions will be granted an access level that the policy determines.

    h. In the Configure Authentication Methods window, select **Perform machine health check only**. Clear all other check boxes, and then click **Next**.
    i. In the Configure Constraints window, click **Next**.
    j. In the Configure Settings window, click **NAP Enforcement**. Select **Allow limited access**, and verify that **Enable auto-remediation of client computers** is selected.
    k. Click **Next**, and then click **Finish**. This completes configuration of your NAP network policies. Close the Network Policy Server console.

Configure DHCP service for NAP enforcement

1. Click **Start**, point to **Administrative Tools**, and then click **DHCP**.
2. In the DHCP console, expand **LON-DC1.contoso.com**, and then expand **IPv4**.
3. Select and then right-click **Scope,** and then click **Properties**.
4. On the **Network Access Protection** tab, select **Enable for this scope**, verify that **Use default Network Access Protection profile** is selected, and then click **OK.**
5. In the DHCP console, expand **Scope**, select **Scope Options**
6. Confirm that the value for **003 Router** is set to **10.10.0.1**
7. Confirm that the value for **006 DNS Servers** is set to **10.10.0.10**
8. Confirm that the value for **015 DNS Domain Name** is set to **contoso.com**. The contoso.com domain is a full-access network assigned to compliant NAP clients.
9. In the DHCP console, right-click **Scope Options**, and then click **Configure Options**.
10. On the **Advanced** tab, next to **User class**, select **Default Network Access Protection Class**.
11. Select the **006 DNS Servers** check box, type **10.10.0.10** in **IP Address**, and then click **Add.**

12. Select the **015 DNS Domain Name** check box, type **restricted.contoso.com** in **String value**, and then click **OK**. The restricted.contoso.com domain is a restricted-access network assigned to noncompliant NAP clients.
13. Close the DHCP console.

Configure client computer as a DHCP and NAP client

1. On LON-CL1, enable Security Center:
    a. Click **Start**, point to **All Programs**, click **Accessories**, and then click **Run**.
    b. Type **mmc**, and then press ENTER.
    c. On the **File** menu, click **Add/Remove Snap-in**.
    d. In the **Add or Remove Snap-ins** dialog box, under **Available snap-ins**, **click** Group Policy Object Editor, and then click **Add**.
    e. In the **Select Group Policy Object** dialog box, click **Finish**, and then click **OK**.
    f. In the console tree, expand **Local Computer Policy/Computer Configuration/Administrative Templates/Windows Components/Security Center**.
    g. Double-click **Turn on Security Center (Domain PCs only)**, click **Enabled**, and then click **OK**.
    h. Close the console window. When prompted to save settings, click **No**.
2. Enable the DHCP enforcement client:
    a. Click **Start**, click **All Programs**, click **Accessories,** and then click **Run**.
    b. Type **napclcfg.msc**, and then press ENTER
    c. In the console tree, click **Enforcement Clients**.
    d. In the details pane, right-click **DHCP Quarantine Enforcement Client**, and then click **Enable.**
    e. Close the **NAP Client Configuration** console.
3. Enable and start the NAP agent service:
    a. Click **Start**, click **Control Panel**, click **System and Maintenance**, and then click **Administrative Tools**.
    b. Double-click **Services**.
    c. In the services list, double-click **Network Access Protection Agent**.
    d. In the **Network Access Protection Agent Properties** dialog box, change the **Startup** type to **Automatic**, and then click **Start**.
    e. Wait for the service to start, and then click **OK**.
    f. Close the Services console, and then close the Administrative Tools and System and Maintenance windows.
4. Configure LON-CL1 for DHCP address assignment:
    a. Click **Start,** and then click **Control Panel**.

b. Click **Network and Internet**, click **Network and Sharing Center,** and then click **Manage network connections**.

c. Right-click **Local Area Connection**, and then click **Properties**.

d. In the **Local Area Connection Properties** dialog box, clear the **Internet Protocol Version 6 (TCP/IPv6)** check box. This reduces the lab's complexity, particularly for those who are not familiar with IPv6.

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

f. Verify that **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.

g. Click **OK**, and then click **Close** to close the **Local Area Connection Properties** dialog box.

5. Close the Network Connections and Network and Sharing Center windows.

6. Restart LON-CL1. After the computer restarts, log on as **Administrator** with the password of **Pa$$w0rd**.

Test NAP Enforcement

1. Verify DHCP assigned address and current Quarantine State:

   a. On LON-CL1, click **Start,** click **All Programs**, click **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**.

   b. At the command prompt, type **ipconfig /all**, and then press ENTER.

   c. Verify the connection-specific DNS suffix of contoso.com and a Quarantine State of Not Restricted.

2. Configure the System Health Validator policy to require antivirus software:

   a. On LON-DC1, open the Network Policy Server console.

   b. Expand **Network Access Protection**, and then click **System Health Validators.**

   c. Under **Name, in the details pane**, double-click **Windows Security Health Validator.**

   d. In the **Windows Security Health Validator Properties** dialog box, click **Configure.**

   e. In the **Windows Security Health Validator** dialog box, under **Virus Protection**, select the **An antivirus application is on** check box.

   f. Click **OK**, and then click **OK** again to close the Windows Security Health Validator Properties window.

3. Verify the restricted network on LON-CL1:

   a. On LON-CL1, click **Start**, click **All Programs**, click **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**.

   b. At the command prompt, type **ipconfig /release.**

   c. At the command prompt, type **ipconfig /renew**.

   d. Verify the **Connection-specific DNS suffix** is now **restricted.contoso.com.**

4. Close the command window, and double-click the **Network Access Protection** icon in the system tray. Notice it tells you the computer is not compliant with requirements of the network.

5. Click **Close.**

Additional Reading

What Is Network Access Protection?

For more information on Network Access Protection, see http://go.microsoft.com/fwlink/?LinkId=102223&clcid=0x409.

NAP Scenarios

For more information on scenarios for implementing NAP, refer to the resources at http://go.microsoft.com/fwlink/?LinkId=102223&clcid=0x409.

NAP Components

For additional information on NAP components and the NAP architecture, see http://technet.microsoft.com/en-us/network/cc984186.aspx.

IPsec Enforcement

For more information on IPSec enforcement for NAP, download the white paper "Internet Protocol Security Enforcement in the Network Access Protection Platform," available at http://go.microsoft.com/fwlink/?LinkID=177453&clcid=0x409.

802.1x Enforcement

- For more information on 802.1x enforcement for NAP, refer to the relevant section in the white paper NAPArch.doc, which can be downloaded at http://go.microsoft.com/fwlink/?LinkId=102226&clcid=0x409.
- For additional information, refer to the resources available at http://go.microsoft.com/fwlink/?LinkID=177453&clcid=0x409.

VPN Enforcement

For more information on VPN enforcement for NAP, see the relevant section in the NAPArch.doc white paper, which is available at http://go.microsoft.com/fwlink/?LinkId=102226&clcid=0x409.

DHCP Enforcement

For more information on VPN enforcement for NAP, see the relevant section in the NAPArch.doc white paper, which is available at http://go.microsoft.com/fwlink/?LinkId=102226&clcid=0x409.

Lesson 2

Implementing NAP

Contents:

Question and Answers

What Are System Health Validators?

Question: Does NAP work only with Microsoft-supplied System Health Validators?

Answer: No. It is extensible, so you can use any vendor's System Health Agents and System Health Validators if they follow the NAP API.

What Is a Health Policy?

Question: Can you use only one SHV in a health policy?

Answer: No. You can specify any available SHVs.

NAP Client Configuration

Question: What Windows groups have the rights to enable Security Center in Group Policy, enable NAP service on clients, and enable/disable NAP enforcement clients?

Answer: The following groups have these rights: Enterprise Admins, Domain Admins, and Local Administrators.

Demonstration: Configuring NAP Clients

Question: Why do you need to manage NAP settings on client computers?

Answer: The client components are responsible for compiling health status statements on client computers, maintaining a client computer's health state, and communicating a client computer's health state to the server components. To make the server components and client components work together, you must configure NAP settings on both the servers and the client computers.

Demonstration: Configuring NAP Tracing

Question: What is NAP tracing used for and when does it need to be enabled?

Answer: Tracing records NAP events in a log file and is useful for troubleshooting and maintenance. NAP tracing is disabled by default, which means that no NAP events are recorded in the NAP tracing log files. You need to enable it if you want to evaluate the health and security of your network or troubleshoot any NAP problems.

Detailed Demo Steps

Demonstration: Configuring NAP Tracing

Detailed demonstration steps

In this demonstration you will:

- Enable Security Center in Group Policy.
- Enable the Network Access Protection Service on clients.
- Enable NAP enforcement clients.

Enable Security Center in Group Policy

1. On LON-CL1, open the **Group Policy Management** console, and then click **Add.**
2. In the **Select Group Policy Object** dialog box, click **Finish**, and then click **OK**.
3. In the console tree, double-click **Local Computer Policy**, double-click **Computer Configuration**, double-click **Administrative Templates**, double-click **Windows Components**, and then double-click **Security Center**.
4. Double-click **Turn on Security Center (Domain PCs only),** click **Enabled,** and then click **OK**.

Enable the Network Access Protection service on clients

1. On LON-CL1, click **Start**, click **Control Panel**, click **System and Maintenance,** click **Administrative Tools**, and then double-click **Services**.
2. In the services list, scroll down to, and double-click, **Network Access Protection**.
3. In the **Network Access Protection Agent Properties** dialog box, change **Startup Type** to **Automatic,** and then click **OK.**

Enable NAP enforcement clients

1. On LON-CL1, click **Start**, click **All Programs**, click **Accessories**, click **Run**, type **NAPCLCFG.MSC**, and then click **OK.**
2. Click **Enforcement Clients**. In the details pane, right-click the enforcement client that you want to enable or disable, and then click **Enable** or **Disable.**

Demonstration: Configuring NAP Tracing

In this demonstration you will:

- Configure NAP tracing by using a Windows Interface.
- Configure NAP tracing by using a command-line tool.
- View log files.

Configure NAP tracing by using a Windows interface

1. On LON-CL1, click **Start,** click **All Programs**, click **Accessories**, click **Run,** type **napclcfg.msc**, and then click **OK.**
2. In the console tree, right-click **NAP Client Configuration (Local Computer)**, and then click **Properties.**

3. In the **NAP Client Configuration (Local Computer) Properties** dialog box, choose **Enabled**.
4. Under **Specify the level of detail at which the tracing logs are written**, select **Debug**.

Configure NAP tracing by using a command-line tool

1. On LON-CL1, click **Start,** click **All Programs**, click **Accessories,** and then click **Command Prompt**.
2. To disable NAP tracing, type: **netsh nap client set tracing state=disable**.
3. To enable NAP tracing and configure for basic or advanced logging, type: **netsh nap client set tracing state=enable level =advanced**.

View the log files

1. On LON-CL1, click **Start,** click **All Programs**, click **Accessories**, then click **Windows Explorer**.
2. Navigate to the %systemroot%\tracing\nap directory.

Additional Reading

What Are System Health Validators?

- For additional information on SHVs, see the relevant section in the NAPArch.doc white paper, which is available at http://go.microsoft.com/fwlink/?LinkId=102226&clcid=0x409.
- For additional information, refer to the resources available at http://go.microsoft.com/fwlink/?LinkId=102223&clcid=0x409.

What Is a Health Policy?

For more information see the help topic, Health Policies.

What Are Remediation Server Groups?

For more information, see the help topic, Remediation Server Groups.

NAP Client Configuration

For more information, see the following help topics:

- Help Topic: Enable Security Center in Group Policy
- Help Topic: Enable the Network Access Protection Service on Clients
- Help Topic: Configure NAP Enforcement Clients

What Is NAP Tracing

For more information, see the following help topics:

- Help and Support Topic: NAP tracing
- Help Topic: Enable and Disable NAP Tracing
- Help Topic: Specify Level of Detail in the NAP Trace Log

Lesson 3

Implementing IPsec Enforcement for NAP

Contents:

Additional Reading

NAP with IPsec Enforcement Components

- Network Policy Server Help topic: NAP enforcement for IPsec communications

IPsec Enforcement for Logical Networks

For more information on IPsec enforcement for logical networks, refer to the following resources:

- Network Access Protection Platform Architecture: http://go.microsoft.com/fwlink/?LinkId=102226&clcid=0x409
- Network Policy Server Help Topic: NAP Enforcement for IPsec Communications

Module Reviews and Takeaways

Review questions

1. What are the three main client configurations that need to be configured for most NAP deployments?

   Answer: Some NAP deployments that use Windows Security Health Validator require that you enable Security Center. The Network Access Protection service is required when you deploy NAP to NAP-capable client computers. You also must configure the NAP enforcement clients on the NAP-capable computers.

2. You want to evaluate the overall health and security of the NAP enforced network. What do you need to do to start recording NAP events?

   Answer: NAP trace logging is disabled by default and should be enabled if you want to troubleshoot NAP-related problems or evaluate the overall health and security of your organization's computers. You can use the NAP Client Management console or the Netsh command-line tool to enable logging functionality.

Best practices related to NAP

Consider the following best practices when implementing NAP:

- Use strong enforcement methods (IPsec, 802.1x and VPN). Strong enforcement methods provide the most secure and effective NAP deployment.
- Do not rely on NAP to secure a network from malicious users. NAP is designed to help administrators maintain the health of the network's computers, which in turn helps maintain the network's overall integrity. NAP does not prevent an authorized user with a compliant computer from uploading a malicious program to the network or disabling the NAP agent.
- Use consistent NAP policies throughout the site hierarchy to minimize confusion. Configuring a NAP policy incorrectly may result in clients accessing the network when they should be restricted or in valid clients being erroneously restricted. The more complicated your NAP policy design, the higher the risk of incorrect configuration.
- Do not rely on NAP as an instantaneous or real-time enforcement mechanism. There are inherent delays in the NAP enforcement mechanism. Although NAP helps keep computers compliant over the long run, typical enforcement delays may last several hours or more due to a variety of factors, including the settings of various configuration parameters.

Tools

Tool	Use	Where to find it
Services	Enabling and configuring the NAP service on client computers.	Click Start, click Control Panel, click System And Maintenance, click Administrative Tools, and then click Services.
Netsh nap	Using Netsh, you can create scripts to automatically configure a set of Windows Firewall with Advanced Security settings, create rules, monitor connections, and display the configuration and status of Windows	Open a command window with administrative rights and type **netsh nap**. You can type **help** to get a full list of available commands.

	Firewall with Advanced Security.	
Group Policy	Some NAP deployments that use Windows Security Health Validator require that Security Center is enabled.	Enable the Turn on Security Center (Domain PCs only) setting in the Computer Configuration, Administrative Templates, Windows Components, and Security Center sections of Group Policy.

Lab Review Questions and Answers

1. Could you use the remote access NAP solution alongside the IPsec NAP solution?

   Answer: Yes. You can use one or all of the NAP solutions in an environment.

2. What benefit would be realized by using such a scenario?

   Answer: One benefit is that the communication on the intranet also would be secured with IPsec, not just the tunnel between the Internet host and the Routing and Remote Access server.

Module 6

Configuring Active Directory® Domain Services

Contents:

Lesson 1

Installing Domain Controllers

Contents:

Question and Answers

Requirements for Installing AD DS

Question: What permissions do you require to create a new forest?

Answer: You need local administrative rights on the computer that will become the first domain controller in the forest.

What Are Domain and Forest Functional Levels?

Question: What functional level must the forest be at to support forest trusts?

Answer: The forest must be at the Windows Server 2003 level.

AD DS Installation Process

Question: How many global catalogs are required in a forest?

Answer: At least one global catalog is required; you might configure others, depending on deployment and topolo

Advanced Options for Installing AD DS

Question: How do you access the advanced options of Dcpromo?

Answer: Use the **/adv** parameter with the Dcpromo executable.

Demonstration: Creating Installation Media

Question: When would you use the IFM option?

Answer: Answers will vary but will include situations where bandwidth is limited or situations where it would generate too much traffic to do a complete replication to a new domain controller.

Detailed Demo Steps

Demonstration: Creating Installation Media

Detailed demonstration steps

1. Log on to **LON-DC1** as **Administrator** with a password of **Pa$$w0rd**.
2. Click **Start**, and then click **Computer**.
3. Right-click drive **C:**, and create a new folder named **ADMedia**.
4. Click **Start**, right-click **Command Prompt**, and then click **Run as Administrator**.
5. Type **Ntdsutil**, and then press ENTER.
6. Type **activate instance ntds**, and then press ENTER.
7. Type **ifm**, and then press ENTER.
8. Type **create sysvol full C:\ADMedia**, and then press ENTER.
9. When the command completes, open the ADMedia folder and show the structure that was created.
10. Close the Command Prompt window.
11. Do not shut down the virtual machine (VM).

Additional Reading

Requirements for Installing AD DS

For more information on the requirements for installing AD DS, refer to the following topics:

- Active Directory Domain Services Help: Installing Active Directory Domain Services
- Requirements for Installing AD DS: http://go.microsoft.com/fwlink/?LinkId=99401

What Are Domain and Forest Functional Levels?

For more information on domain and forest functional levels, refer to the following resources:

- Active Directory Domain Services Help: Set the domain or forest functional level
- Appendix of Functional Level Features: http://go.microsoft.com/fwlink/?LinkId=99402
- Understanding Domain and Forest Functionality: http://go.microsoft.com/fwlink/?LinkID=177464&clcid=0x409
- Redirecting the users and computers containers in Active Directory domains: http://go.microsoft.com/fwlink/?LinkID=178006&clcid=0x409

AD DS Installation Process

For more information on installing AD DS, refer to the following resources:

- Active Directory Domain Services Help: Installing Active Directory Domain Services
- Installing a New Forest: http://go.microsoft.com/fwlink/?LinkId=99403

Advanced Options for Installing AD DS

For more information on advanced options for installing AD DS, refer to the following resources:

- Active Directory Domain Services Help: Use advanced mode installation
- What's New in AD DS Installation and Removal: http://go.microsoft.com/fwlink/?LinkId=99404
- Installing a New Windows Server 2008 Domain Tree by Using the Windows Interface: http://go.microsoft.com/fwlink/?LinkID=178007&clcid=0x409
- Configuring DNS client settings: Domain Name System (DNS): http://go.microsoft.com/fwlink/?LinkID=178008&clcid=0x409

Installing AD DS by Using IFM

For more information on installing AD DS by using IFM, refer to the following resources:

- Installing Active Directory Domain Services (AD DS) from Media: http://go.microsoft.com/fwlink/?LinkId=99405
- Create Installation Media by Using Ntdsutil: http://go.microsoft.com/fwlink/?LinkID=177465&clcid=0x409
- Active Directory Domain Services Help: Use advanced mode installation

Upgrading to Windows Server 2008 AD DS

- For more information on the options for installing AD DS, refer to the help topic Installing Active Directory Domain Services.
- For more information on installing a new forest in AD DS, see http://go.microsoft.com/fwlink/?LinkId=99407.
- For more information on the scenarios for installing AD DS, see http://go.microsoft.com/fwlink/?LinkId=99408.
- For more information on preparing your infrastructure for upgrade, go to http://go.microsoft.com/fwlink/?LinkID=177467&clcid=0x409.

Installing AD DS on a Server Core Computer

- To see an appendix of unattended installation parameters, see http://go.microsoft.com/fwlink/?LinkID=177468&clcid=0x409.
- For more information on how to use the unattended mode to install and remove AD DS on Windows Server 2008–based domain controllers, see http://go.microsoft.com/fwlink/?LinkID=177469&clcid=0x409.

Lesson 2

Configuring Read-Only Domain Controllers

Contents:

Question and Answers

Read-Only Domain Controller Features

Question: Can users get authenticated by an RODC if their passwords are not cached on the RODC?

Answer: If passwords are not cached, the RODC must forward the authentication request to a writable domain controller.

Question: A user in the branch office is unable to log on to the domain, even though there is an RODC at the branch office. What might be the cause?

Answer: If the RODC is not configured to cache passwords of the local users, and the WAN link to the site with the read/write domain controller is not available, then users may not be able to log on to the domain.

Detailed Demo Steps

Demonstration: Prestaging an RODC Account

Detailed demonstration steps

Create the RODC computer account

1. Log on to **LON-DC1** as **Administrator** with a password of **Pa$$w0rd**.
2. Click **Start**, and then execute **Dsa.msc** in the **Search** box.
3. Expand **Contoso.com**, right-click the **Domain Controllers** OU, and then click **Pre-create Read-only Domain Controller account**.
4. In the **Active Directory Domain Services Installation Wizard**, click **Next.**
5. On the **Operating System Compatibility** page, click **Next**.
6. On the **Network Credentials** page, click **Next.**
7. On the **Computer Name** page, type **RODC1** in the **Computer Name** field, and then click **Next.**
8. On the **Select a Site** page, click **Next**.
9. On the **Additional Domain Controller Options** page, click **Next.**
10. On the **Delegation of RODC Installation and Administration** page, click **Set.**
11. In the **Select User or Group** dialog box, type **Dylan**, click **OK,** and then click **Next.**
12. On the **Summary** page, click **Next**, and then click **Finish.**
13. Click the **Domain Controllers** OU, right-click the **RODC1** computer account, and click **Properties**.
14. Click the **Managed By** tab, notice that Dylan Miller is listed as having administrative rights, but that could be changed.

Create the password replication policy to allow the Research group to cache passwords

1. On the **Password Replication Policy** tab, notice that certain administrative groups are denied permission by default.

   Note: At this point you could add the research group to the Allowed RODC Password Replication Group, or you could add the Research global group specifically.

2. Click **Add.**
3. In the **Add Users and Computers** dialog box, click **Allow passwords for this account to replicate to the RODC** and then click **OK.**
4. Type **Research** in the **Select Users and Computers or Groups** dialog box, and then click **OK.**
5. Click **OK** to close the **RODC1 Properties** dialog box.

Additional Reading

What Is a Read-Only Domain Controller?

For more information on read-only domain controllers, refer to
http://go.microsoft.com/fwlink/?LinkId=99410

Preparing to Install the RODC

For more information on preparing to install RODCs, refer to the following resources:

- AD DS Help: Delegate read-only domain controller installation and administration
- AD DS: Read-Only Domain Controllers: http://go.microsoft.com/fwlink/?LinkId=99412
- Active Directory Replication Considerations:
  http://go.microsoft.com/fwlink/?LinkID=178009&clcid=0x409
- Read-only Domain Controllers (RODC) Step-by-Step Guide:
  http://go.microsoft.com/fwlink/?LinkId=99414

Delegating the RODC Installation

- AD DS Help: To see how to delegate read-only domain controller installation and administration, see AD DS Help.
- For information about AD DS and read-only domain controllers, see
  http://go.microsoft.com/fwlink/?LinkId=99412.
- To see a step-by-step guide on read-only domain controllers, see
  http://go.microsoft.com/fwlink/?LinkId=99414.
- For information on RODC features, see
  http://go.microsoft.com/fwlink/?LinkID=178010&clcid=0x409.

What Are Password Replication Policies?

- Go to AD DS Online Help for information about specifying password replication policy.
- For information about password replication policy administration, see
  http://go.microsoft.com/fwlink/?LinkID=177471&clcid=0x409.

Lesson 3

Configuring Fine-Grained Password Policies

Contents:

Question and Answers

Implementing Fine-Grained Password Policies

Question: What condition must be satisfied to implement fine-grained passwords?

Answer: All domain controllers must be running Windows Server 2008 and the domain levels must be raised to the highest level.

Additional Reading

What Are Fine-Grained Password Policies?

For more information on fine-grained password policies in AD DS, see http://go.microsoft.com/fwlink/?LinkID=177472&clcid=0x409.

Components of Fine-Grained Password Policies

For more information on the components of fine-grained password policies, refer to the following resources:

- http://go.microsoft.com/fwlink/?LinkID=177473&clcid=0x409
- Appendix A: Fine-Grained Password and Account Lockout Policy Review: http://go.microsoft.com/fwlink/?LinkID=177474&clcid=0x409

Implementing Fine-Grained Password Policies

For more information on AD DS policies, refer to: Active Directory Domain Services (AD DS) Fine-Grained Password and Account Lockout Policy Step-by-Step Guide at http://go.microsoft.com/fwlink/?LinkID=177475&clcid=0x409

Lesson 4

New Features in Group Policy

Contents:

Question and Answers

What Is a Starter GPO?

Question: When would Starter GPOs be appropriate for your organization?

Answer: Answers will vary.

Additional Reading

What Are ADM and ADMX Files?

To see a step-by-step guide on managing Group Policy ADMX files, see http://go.microsoft.com/fwlink/?LinkID=177476&clcid=0x409.

To see more information on the location of ADM (Administrative Template) files in Windows, see http://go.microsoft.com/fwlink/?LinkID=177477&clcid=0x409.

What Is the Central Store?

For more information on how to create a central store for Group Policy administrative templates in Window Vista, see http://go.microsoft.com/fwlink/?LinkID=177478&clcid=0x409.

What Are Multiple Local Group Policies?

To see a step-by-step guide to managing multiple Local Group Policy objects, see http://go.microsoft.com/fwlink/?LinkID=177479&clcid=0x409.

In Microsoft operating systems prior to Windows Vista, there was only one user configuration available in the local Group Policy. That configuration was applied to all users logged on from the local computer. This is still true, but Windows Vista and Windows Server 2008 have an added feature. In Windows Vista and Windows Server 2008, it is now possible to have different user settings for different local users. This is only available for the users' configurations in Group Policy. There is only one set of computer configurations available that affects all users of the computer. Windows Vista and Windows Server 2008 provide this ability with the following three layers of Local Group Policy objects:

- Local Group Policy (contains the computer configuration settings)
- Administrator and Non-Administrators Group Policy. These are not new security groups. They simply refer to users who are either in the administrators group or not.
- User-specific Local Group Policy. This refers to local users only, not domain users.

Lesson 5

Configuring Group Policy Preferences

Contents:

Question and Answers

Difference Between Group Policy Preferences and Settings

Question: Explain the difference between Group Policy Filtering and Item Level Targeting.

Answer: Group Policy Filtering can only be applied to the entire GPO. Item Level Targeting can be applied to individual settings.

Additional Reading

Difference Between Group Policy Preferences and Settings

For an overview of Group Policy preferences, see
http://go.microsoft.com/fwlink/?LinkID=177480&clcid=0x409.

Module Reviews and Takeaways

Review questions

1. What will happen if an RODC does not have cached passwords and a writable domain controller is unavailable?

   Answer: Authentications will fail.

2. Which two tools can you use to create a password setting object?

   Answer: LDIFDE and ADSI Edit

3. What Group Policy feature allows you to create GPO templates?

   Answer: Starter GPOs

Common issues related to configuring AD DS

Identify the causes for the following common issues related to a particular technology area in the module and fill in the troubleshooting tips. For answers, refer to relevant lessons in the module.

Issue	Troubleshooting tip
Users are unable to log on to an RODC at a branch office.	Ensure that a writable domain controller is available, or create a password replication policy on the RODC for local users.
Unable to create an RODC in the domain.	Ensure that there is a Windows Server 2008 domain controller installed in the domain.
Group Policy Preferences are not being applied.	Check the preference settings for item targeting or incorrect configuration.

Real-world issues and scenarios

1. You have a branch office in a remote location. The data link between Head Office and the branch is slow and unreliable. Logons often fail across the link. Security at the branch is low. You want to ensure that logons will always work for local users even when the data link is unavailable, but because of low security you do not want to put in a local domain controller.

   Solution: Implement an RODC in the branch and set up a password replication policy to cache the local user passwords on the RODC.

2. You have a number of logon scripts that map network drives for users. Not all users need these drive mappings so you must ensure that only the right users get the mappings. You want to move away from using these scripts.

   Solution: Use Group Policy Preferences to map the drives and use item-level targeting to ensure that only the right users receive the mappings.

Tools

Tool	Use	Where to find it
Ntdsutil	• Various AD DS activities	%SystemRoot%\System32

GPME	• Managing Group Policy	Installed as a feature on a server or from the RSAT tools for Windows Vista or later
ADSI Edit	• Lightweight Directory Access Protocol (LDAP) editor that you can use to manage objects and attributes in Active Directory	%SystemRoot%\System32 on Server or from the RSAT tools for Windows Vista or later
LDIFDE	• Exporting and importing data, allowing operations such as add, create, and modify to be performed against the Active Directory	%SystemRoot%\System32

Lab Review Questions and Answers

Lab A:

1. If no password replication policy is configured, how do users authenticate?

   Answer: Users must do pass-through authentication where their authentication request is sent to a read\write domain controller.

2. What rights do delegated administrators of an RODC have in Active Directory?

   Answer: None. Delegated administrators are local administrators and can perform server maintenance functions.

Lab B:

1. How would you ensure that any ADMX template files only need to be updated in a single location?

   Answer: Create a central store and put the ADMX file in the central store.

2. What is the main difference between a policy and a preference?

   Answer: Users can change preference settings, but they cannot change policy settings.

Module 7

Managing Active Directory Domain Services

Contents:

Lesson 1

Managing Events

Contents:

Question and Answers

What Are Subscriptions?

Question: Are you required to use the Forwarder Events log to hold events from subscriptions?

Answer: No, the Forwarder Events log is the default location, but any log could be used to hold events from subscriptions.

Additional Reading

New Features of Event Viewer

- For an overview of Event Viewer, see http://go.microsoft.com/fwlink/?LinkID=177415&clcid=0x409.
- For more information about Event Properties, see http://go.microsoft.com/fwlink/?LinkID=177416&clcid=0x40

Managing Event Logs on Server Core

For more information on Wevtutil, see http://go.microsoft.com/fwlink/?LinkID=177417&clcid=0x409.

What Are Custom Views?

For more information on creating and managing custom views, see http://go.microsoft.com/fwlink/?LinkID=177418&clcid=0x409.

What Are Subscriptions?

For more information about event subscriptions, and about configuring computers to forward and collect events, see http://go.microsoft.com/fwlink/?LinkID=177418&clcid=0x409.

Lesson 2

Configuring AD DS Auditing

Contents:

Question and Answers

What Is AD DS Auditing?

Question: What needs to be configured before you will see any results for object auditing?

Answer: The SACL for the object you want to audit must be configured before any auditing will take place.

Types of Events to Audit

Question: You want to track details about any modifications made to Active Directory objects for a particular organizational unit (OU) and any child OUs. Which ACE should you set to capture that information?

Answer: You should set the SACL for the Authenticated Users group to track successes for the Write All Properties ACE. You should ensure that the setting applies to This Object And All Descendant Objects.

Detailed Demo Steps

Demonstration: Enabling Directory Service Changes by Using Auditpol

Detailed demonstration steps

In this demonstration, you will see how to:

- View the current status of auditing.
- Enable the Directory Service Changes subcategory.

To complete this demonstration, you must have the LON-DC1 virtual machine running.

View the current status of auditing

1. Click **Start**, and then click **Command Prompt**.
2. Execute **auditpol /get /category:*** to display a listing of the current audit status of all categories.

   Notice that DS Access is set to Success and all others are set to no auditing.

Enable the Directory Service Changes subcategory

- Execute **auditpol /set /subcategory:"directory service changes" /success:enable**

View the new settings for just the directory service category

- Execute **auditpol /get /category:"DS Access"** to display the status of just the DS access category. Notice that Directory Service Changes is now set to audit successes.

Additional Reading

What Is AD DS Auditing?

To see a step-by-step guide on AD DS auditing, go to http://go.microsoft.com/fwlink/?LinkID=177419&clcid=0x409.

For more information on Auditpol, see http://go.microsoft.com/fwlink/?LinkID=177420&clcid=0x409.

Lesson 3

Monitoring AD DS

Contents:

Question and Answers

Reliability and Performance Monitor Features

Question: How would you create a reusable set of counters that you want to monitor?

Answer: You would create a Data Collector Set with the appropriate counters

Monitoring Service Availability with Reliability Monitor

Question: You want to see a historical record of software that has been added or removed from the computer. Where would you find that information?

Answer: The Software (Un)Installs category of events in the Reliability Monitor.

Monitoring AD DS by Using Data Collector Sets

Question: You want to create an alert to notify you when free disk space is low. How would you create one?

Answer: Create a new Data Collector Set manually and check the Performance Counter Alert. Add the %Free Space counter in the Logical Disk object and set the threshold as required.

Additional Reading

Reliability and Performance Monitor Features

For more information on Windows Reliability and Performance Monitor, see http://go.microsoft.com/fwlink/?LinkID=177421&clcid=0x409.

Monitoring AD DS by Using Performance Monitor

For more information on monitoring Active Directory, see http://go.microsoft.com/fwlink/?LinkID=177422&clcid=0x409.

Monitoring Service Availability with Reliability Monitor

To see the Windows Vista Performance and Reliability Monitoring Step-by-Step Guide, go to http://go.microsoft.com/fwlink/?LinkID=177423&clcid=0x409.

Monitoring AD DS by Using Data Collector Sets

For more information on creating Data Collector Sets, go to http://go.microsoft.com/fwlink/?LinkID=177424&clcid=0x409.

Lesson 4

Maintaining AD DS

Contents:

Question and Answers

Managing the Active Directory Database by Using Ntdsutil

Question: You have forgotten the directory services restore-mode password for your domain controller. How can you recover the password?

Answer: You cannot recover the password, but by using the Set DSRM password command in Ntdsutil, you can configure a new password for this account.

Demonstration: Performing AD DS Database Maintenance Tasks

Question: Why is it necessary to stop the AD DS before defragmenting?

Answer: The database needs to be closed completely before it can be overwritten. An online database may have locked records that are being written to, thus preventing file modification.

Question: Why is it necessary to compact the database to a temporary directory first?

Answer: Compacting the database actually creates a contiguous copy, which will be used to overwrite the fragmented original.

Backing Up AD DS

Question: What other process could you use to back up the system state data on a domain controller?

Answer: You could do a full server backup.

What Is the Database Mounting Tool?

Question: Can the Database Mounting Tool be used to view the attributes of objects?

Answer: No, the tool only exposes the data as an LDAP server. An LDAP tool has to be used to view the object information.

Detailed Demo Steps

Demonstration: Performing AD DS Database Maintenance Tasks

Detailed demonstration steps

In this demonstration, you will see how to:

- Start and stop AD DS Services.
- Perform an Offline Defrag of the Active Directory Database.

Stop or start the AD DS service

1. Ensure you are logged on to LON-DC1 as Administrator with a password of Pa$$w0rd
2. Click **Start**, click **Admin Tools,** and then click **Services.**
3. Right-click **Active Directory Domain Services**, and then select **Stop** from the **Context** menu.
4. In the **Also stop the following Services** dialog box, click **Yes**.

Perform an offline defrag of the Active Directory database

1. Click **Start**, click **Run**, type **CMD**, and then press ENTER.
2. In the command window, type **ntdsutil**, and then press ENTER.
3. At the **ntdsutil:** prompt, type **Activate Instance NTDS**, and then press ENTER.
4. At the **ntdsutil:** prompt, type **files**, and then press ENTER.
5. At the **file maintenance:** prompt, type **compact to C:\compact**, and then press ENTER.
6. Once complete, use Windows Explorer to copy the Ntds.dit file in the C:\compact directory and replace the C:\Windows\NTDS\ntds.dit.
7. Delete the old log files by typing **del C:\Windows\NTDS*.log** in a command window.
8. In the File Maintenance command window, type **integrity** to check the integrity of the new compacted database.
9. In the services mmc, right-click **Active Directory Domain Services**, and then click **Start**.

Additional Reading

What Are Restartable Active Directory Domain Services?

For more information on Restartable Active Directory Domain Services, see http://go.microsoft.com/fwlink/?LinkID=177425&clcid=0x409.

Locking Down Services on AD DS Domain Controllers

For more information, read the TechNet article Using SCW on Windows Server 2008 at http://go.microsoft.com/fwlink/?LinkID=177429&clcid=0x409.

Backing Up AD DS

To view the AD DS Backup and Recovery Step-by-Step Guide, go to http://go.microsoft.com/fwlink/?LinkID=177430&clcid=0x409.

What Is the Database Mounting Tool?

For more information on the Database Mounting Tool, see http://go.microsoft.com/fwlink/?LinkID=177426&clcid=0x409.

To view the step-by-step guide for using the Active Directory Database Mounting Tool in Windows Server 2008, go to http://go.microsoft.com/fwlink/?LinkID=177431&clcid=0x409.

Reanimating Tombstoned AD DS Objects

For more information on how to restore deleted user accounts and their group memberships in Active Directory, see http://go.microsoft.com/fwlink/?LinkID=177427&clcid=0x409.

Module Reviews and Takeaways

Review questions

1. What log shows you the audit results?

   Answer: The Security log displays the audit results.

2. How would you enable the tracking of failure events for the Directory Service Change subcategory?

   Answer: You must use the Auditpol.exe to enable failure tracking and set the appropriate ACEs for the objects being audited.

3. What service needs to be enabled on the source computers that forward events to subscriptions?

   Answer: The WinRM service needs to be enabled on the source computers.

4. How would you view event logs on a Server Core computer?

   Answer: You could use the Wevtutil.exe on the Server Core computer or you could create a subscription to forward events to a graphical installation of Windows Server or Windows Vista.

Common issues related to managing AD DS

Identify the causes for the following common issues related to managing AD DS and fill in the troubleshooting tips. For answers, refer to relevant lessons in the module.

Issue	Troubleshooting tip
No events appear in an event log.	Logging may be disabled on that log or the events may have been cleared by another user.
If a user account was deleted several weeks ago, but you are not sure which backup of AD DS has the most recent information about it.	View the snapshots of AD DS to see when the account was last available in AD DS. Then you can restore the backup of AD DS from that date.
You want to monitor the same set of performance monitor counters and log the results over a period of time.	Create a Data Collector Set containing the counters you need to measure.
You want to quickly see when a software application was installed on a server.	You can use the Reliability Monitor to quickly see the date that the software was installed.
Event Viewer cannot attach to a remote computer.	Ensure that the remote computer is available on the network. Next, ensure that the Remote Event Log Management firewall exception has been set on the remote computer. Finally, ensure that your user account has permission to access the remote computer.

Real-world issues and scenarios

1. Contoso, Ltd has a Web application that sometimes crashes. This application is critical and needs to be manually restarted. The administrator has attached a task to this event and has an e-mail message sent to the on-duty operator to restart the service.
2. Contoso, Ltd wants to capture certain events from all Microsoft SQL Servers throughout the organization. They want these events collected and forwarded to multiple locations throughout the country. The administrator has set up event subscriptions such that all Microsoft SQL servers forward certain events to multiple collector computers across the country.

Best practices

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

- Use subscriptions and custom views to aggregate event logs to a single workstation for reviewing.
- Use the operational logs for particular services to gain detailed information about events.
- A certain level of auditing should always be maintained on critical servers.
- AD DS should be backed up on a regular basis.

Tools

Tool	Use	Where to find it
Ntdsutil	• Various AD DS management tasks	%SystemRoot%\System32
DSAMain	• Exposes Active Directory data that is stored in a snapshot or backup as an LDAP server	%SystemRoot%\System32
Auditpol.exe	• Manages auditing settings	%SystemRoot%\System32
LDP	• LDAP client that allows users to perform operations (such as connect, bind, search, modify, add, delete) against any LDAP-compatible directory.	%SystemRoot%\System32
Wecutil	• Initializes the Windows Event Collector on a Collector computer	%SystemRoot%\System32
WinRM	• provides a secure way to communicate with local and remote computers using Web services	%SystemRoot%\System32
Wevtutil.exe	• Command-line management of event logs	%SystemRoot%\System32

Lab Review Questions and Answers

1. What steps must you take to remotely view event logs?

   Answer: You must create a firewall exception to allow remote management of event logs.

2. What service must be enabled on the collector computer for subscriptions?

   Answer: The Windows Event Collector Utility (WECUtil) must be enabled.

3. What command-line tool is used to control auditing?

   Answer: Auditpol.exe

4. What is the difference between restoring an AD DS object by undeleting it, and just recreating the object?

   Answer: When you restore an AD DS object by undeleting it, you restore the object with the same Security Identifier (SID). If you just recreate the object, the object may have the same name and attributes, but it will have a different SID.

Module 8

Configuring Active Directory® Lightweight Directory Services

Contents:

Lesson 1

Installing and Configuring AD LDS

Contents:

Question and Answers

What Is AD LDS?

Question: Does AD LDS require a domain environment?

Answer: No, AD LDS does not depend on the existence of a domain.

AD LDS Components

Question: Is an instance created automatically when the server role is installed?

Answer: No. After you add the AD LDS server role to your server, you create AD LDS instances using the AD LDS Setup Wizard.

Demonstration: Installing the AD LDS Server Role

Question: Can AD LDS be installed on a member server?

Answer: You can run AD LDS on member servers or stand-alone servers.

AD LDS Administration Tools

Question: What tool requires a Bind operation to authenticate before you can manage AD LDS?

Answer: The LDP.exe requires you to authenticate through a Bind operation.

Detailed Demo Steps

Demonstration: Installing the AD LDS Server Role

Detailed demonstration steps

In this demonstration, you will see how to install the AD LDS server role.

1. Start **LON-DC1**, and log on as **Contoso\Administrator**.
2. Start **Server Manager** by clicking the icon next to the **Start** menu.
3. Click the **Roles** node.
4. In the details pane, click **Add Roles**.
5. On the **Before You Begin** page, click **Next**.
6. Select the **Active Directory Lightweight Directory Services** check box, and then click **Next**.
7. On the **Introduction** page, click **Next**.
8. On the **Confirm Installation Selections** page, click **Install**.
9. On the **Installation Results** page, click **Close**.

Remember that installing the role does not create an instance. That is a separate action that can be done using the AD LDS Setup Wizard.

Note: If you have to remove the AD LDS server role, you must remove all instances of AD LDS through the Programs and Features applet in Control Panel.
Note: ADAM is automatically upgraded to AD LDS when the host operating system in upgraded from Windows Server 2003 to Windows Server 2008. All instances, data, and configuration will be backward-compatible without needing modification.

Also note, however, that if no ADAM instances have been defined prior to the operating system upgrade, the ADAM software will not be upgraded. In that case, first ensure that ADAM is uninstalled on the host server and then install AD LDS as normal.

AD LDS can be installed in a Windows Server 2008 Core configuration too.

Additional Reading

How Clients Connect to AD LDS

For more information on Service Connection Points (SCPs) and ADAM/AD LDS, see http://go.microsoft.com/fwlink/?LinkID=177987&clcid=0x409.

Lesson 2

Configuring AD LDS Instances

Contents:

Question and Answers

Demonstration: Modifying an AD LDS Schema

Question: What command-line tool is used to modify schema after the creation of the instance?

Answer: LDIFDE

Demonstration: Connecting to an AD LDS Instance and Application Partition

Question: Does each AD LDS instance have its own directory store?

Answer: Yes, each AD LDS instance has a separate directory store

Detailed Demo Steps

Demonstration: Modifying an AD LDS Schema

Detailed demonstration steps

In this demonstration, you will see how to modify an existing AD LDS installation to create an instance and import an LDIF file to modify the schema.

1. Ensure that **LON-DC1** is running and you are logged on as **Contoso\Administrator**.
2. Open **Server Manager** and expand the **Roles** node, and then click **Active Directory Lightweight Directory Services**.
3. In the details pane, under the **Advanced Tools** section, click **AD LDS Setup Wizard**.
4. On the **Welcome to the Active Directory Lightweight Directory Services Setup Wizard** page, click **next**.
5. On the **Setup Options** page, click **A unique instance**, and then click **Next**.
6. On the **Instance Name** page, in the **Instance name** box, type **ContosoApp1**, and then click **Next**.
7. On the **Ports** page click **Next**. Point out that because this is a domain controller, the default LDAP port is 50000 and 50001 for SSL. That is because the standard ports of 389 and 636 are being used by AD DS. If this were a member server, the wizard would suggest the standard ports. Also mention that any open ports are available to be used by AD LDS.
8. On the **Application Directory Partition** page, click **Yes, create an application directory partition**, in **Partition name** box, type **OU=App1,dc=contoso,dc=local** and then click **Next**.
9. On the **File Locations** page, accept the default data file locations, and then click **Next**.
10. On the **Service Account Selection** page, ensure that **Network service account** is selected, and then click **Next**.
11. On the AD LDS Administrators page, ensure that **Currently logged on user** is selected, and then click **Next**.
12. On the **Importing LDIF Files** page, select the **MS-User.LDF** check box, and then click **Next**.
13. On the **Ready to Install** page, review the selections and click **Next**.
14. Click **Finish**.

Demonstration: Connecting to an AD LDS Instance and Application Partition

In this demonstration, you will see how to configure an AD LDS instance and an application partition using ADSIEdit.exe.

1. Step through the following steps using the LON-DC1 virtual machine, logged on as **Contoso\Administrator**.
2. Open **Server Manager** and expand **Roles**, and then click **Active Directory Lightweight Directory Services**.

3. In the content pane, in the **Advanced Tools** section, click **ADSI Edit**. The ADSI Edit console appears.
4. In the ADSI Edit console, right-click **ADSI Edit**, and then click **Connect to**. The Connection Settings dialog box appears.
5. In the **Connection Settings** dialog box, in the **Name** box, type **ContosoApplication**.
6. Under **Connection Point**, in the **Select or type a Distinguished Name or Naming Context** box, type **OU=App1,dc=contoso,dc=local**.
7. Under **Computer**, select the **Select or type a domain or server** box:(Server | Domain **[:port])**, type **LON-DC1:50000**, and then click **OK**.

Optional demonstration: Manage and configure an AD LDS instance

1. Click **Start**, and then click **Server Manager**.
2. In the console tree, double-click **Roles**, and then click **Active Directory Lightweight Directory Services**.
3. In the details pane, under the **Advanced Tools**, click **Ldp.exe**.
4. On the **Connection** menu, click **Connect**.
5. In **Server**, type **LON-DC1** and in **Port**, type the LDAP port number **50000**, and then click **OK**.
6. On the **Connection** menu, click **Bind**, select **Bind as currently logged on user**, and then click **OK**.
7. When you are finished specifying the bind options, click **OK**.
8. On the **View** menu, click **Tree**, and then type **OU=App1,dc=contoso,dc=local**.
9. Scroll through the objects listed under the application partition and look through the right-click menu. Note the options you have in relation to configuring the application partition.

Optional demonstration: Create a partition by using LDP

1. While connected and in the LDP window, click the **Browse** menu, click **Add child**.
2. In the **Dn** field, type **CN=Partition2,dc**=**Contoso,dc**=**local**.
3. Under **Edit entry**, type **ObjectClass** in the **Attribute** field and **container** in the **Values** field, and then click ENTER.
4. Under **Edit entry**, type **instanceType** in the **Attribute** box and **5** in the **Values** box, and then click ENTER.
5. Click **Run**.
6. If the new application directory partition is added successfully, the following information appears in the details pane:
7. **Added {CN=Partition2,DC=Contoso}**
8. Click **Close**.

> **Note**: To refresh Ldp.exe and view your new directory partition, you must disconnect and then bind again to the AD LDS instance as follows:

9. On the **Connection** menu, click **Disconnect**.
10. Bind to your AD LDS instance as you did previously.
11. To view the directory tree in Ldp.exe, on the **View** menu, click **Tree**.
12. To view all directory partitions on the AD LDS instance, leave **BaseDN** blank, and then click **OK**.

Demonstration: Creating User Accounts and Groups in AD LDS

In this demonstration, you will see how to create user accounts and groups.

1. Log on to **LON-DC1**as **Contoso\Administrator.**
2. In the Server Manager console, expand **Roles,** and then click **Active Directory Lightweight Directory Services**.
3. In the content pane, in the **Advanced Tools** section, click ADSI Edit. The **ADSI Edit** console appears.
4. In the ADSI Edit console, right-click **ADSI Edit,** and then click **Connect to**. The Connection Settings dialog box appears.
5. In the **Connection Settings** dialog box, in the **Name** box, type **ContosoApplication**.
6. Under **Connection Point,** in the **Select or type a Distinguished Name or Naming Context** box, type **OU=App1,dc=contoso,dc=local.**
7. Under **Computer,** select the **Select or type a domain or server box:(Server | Domain [:port]),** type **LON-DC1:50000,** and then click **OK**.
8. In the ADSI Edit console, right-click **OU=App1,dc=CONTOSO,dc=local.**
9. Point to **New,** and then click **Object**. The Create Object dialog box appears.
10. In the **Create Object** dialog box, under **Select a class**, click **user**, and then click **Next**.
11. In the **Value** box, type **User1**, click **Next**, and then click **Finish**.
12. In the ADSI Edit console, expand **OU=App1,dc=CONTOSO,dc=local**, right-click **CN=Roles**, point to **New,** and then click **Object.** The Create Object dialog box appears.
13. In the **Create Object** dialog box, under **Select a class**, click **group**, and then click **Next**.
14. In the **Value** box, type **Group1**, click **Next**, and then click **Finish**. The ADSI Edit console appears.
15. Under **OU=App1,dc=CONTOSO,dc**=**local,** click **CN=Roles**, and then under **Name,** double-click **CN=Group1**. The CN=Group1 Properties dialog box appears.
16. In the **CN=Group1 Properties** dialog box, click **member**, and then click **Edit**. The Multivalued Distinguished Name With Security Principal Editor dialog box appears.
17. In the **Multivalued Distinguished Name With Security Principal Editor** dialog box, click **Add DN**.
18. In the **Enter a distinguished name (DN) for an object** box, type **CN**=**User1,OU**=**App1,dc**=**CONTOSO,dc**=**local,** and click **OK**. Then click **OK** twice.

Additional Reading

What Is an AD LDS Schema?

For more information on the AD LDS Schema, see
http://go.microsoft.com/fwlink/?LinkID=177988&clcid=0x409.

AD LDS Users and Groups

For more information on ADAM Security, see
http://go.microsoft.com/fwlink/?LinkID=177989&clcid=0x409.

Lesson 3

Configuring AD LDS Replication

Contents:

Question and Answers

How AD LDS Replication Works

Question: What tool would you use to create an AD LDS replica?

Answer: You can use the AD LDS setup wizard to create a replica of an existing instance.

Additional Reading

Why Implement AD LDS Replication?

For more information on AD LDS Replication and Configuration Sets, see http://go.microsoft.com/fwlink/?LinkID=177990&clcid=0x409.

Lesson 4

Configuring AD LDS Integration with AD DS

Contents:

Detailed Demo Steps

Demonstration: Adding AD DS Users to AD LDS Groups

Detailed demonstration steps

In this demonstration, you will see how to:

- Add AD DS users to AD LDS groups.
- Verify access permissions.

Add AD DS users to AD LDS groups

1. Use **LON-DC1**, logged on as **Contoso\Administrator**.
2. Start **ADSI Edit** (Administrative Tools/ADSI Edit) and navigate to the **OU=App1,dc=contoso,dc=local** section. Then click **CN=Roles**.
3. Right-click **CN=Readers**, and click **Properties**.
4. In the **Properties** dialog box, click **member**, and then click **Edit**.
5. Click **Add Windows Account**.
6. In the **Enter the object names to select** box, type **Ed**, and then click **OK** three times.

Verify access permissions

1. In ADSI Edit, in the console tree, right-click **ADSI Edit**, and select the **Connect to** check box.
2. In the **Connection Settings** dialog box, in the **Name** box, type **Windows User Test**.
3. Under **Connection Point**, in the **Select or type a Distinguished Name or Naming Context** box, type **OU=App1,dc=contoso,dc=local**.
4. Under **Computer**, in the **Select or type a domain or server** box, type **LON-DC1:50000**, and then click **Advanced**.
5. In the **Advanced** dialog box, select the **Specify Credentials** check box.
6. In the **Username** box, type **Contoso\Ed**. In the **Password** box, type **Pa$$w0rd,** and then click **OK** twice.
7. Verify that the **Ed Meadows** account has read access to objects in the App1 OU.

Additional Reading

Synchronizing AD DS Accounts to AD LDS

- For more information about Adamsync, see http://go.microsoft.com/fwlink/?LinkID=177991&clcid=0x409.
- For more information about the XML elements used in the Adamsync configuration file, see http://go.microsoft.com/fwlink/?LinkID=177992&clcid=0x409.
- For more information about ADSchemaAnalyzer, see http://go.microsoft.com/fwlink/?LinkID=177993&clcid=0x409.

Module Reviews and Takeaways

Review questions

1. What information do you require to create an AD LDS replica?

   Answer: You have to know the Domain Name System (DNS) name of the server that is running an AD LDS instance that belongs to the configuration set, as well as the Lightweight Directory Access Protocol (LDAP) port that was specified when the instance was created. You can also supply the distinguished names (also known as DNs) of specific application directory partitions that you want to copy from the configuration set to the AD LDS instance that you are creating.

2. Do the instances that are part of the same configuration set run on the same or separate computers?

   Answer: Instances that are part of the same configuration set can run on the same or separate computers

3. What tool provides the ability to create an AD LDS replica?

   Answer: The AD LDS setup wizard allows you to create a replica of an existing instance.

Common issues related to AD LDS

Identify the causes for the following common issues related to AD LDS, and fill in the troubleshooting tips. For answers, refer to relevant lessons in the module.

Issue	Troubleshooting tip
AD LDS replication not completing	If the instances in the configuration set are geographically separate, you may have to create site and schedule replication.
You cannot join an existing instance to a configuration set	Joining a configuration set can be done only at the time of creation of the instance.

Real-world issues and scenarios

1. An organization wants to expose a SharePoint portal site to external users who need to be authenticated, but will not be added to the Active Directory. This can be accomplished by using forms based authentication and storing the external user information in AD LDS.
2. An organization wants to expose a Web application through federated services. In this case, AD LDS can act as an identity provider for business scenarios that require an extranet directory to store customer user accounts and so on, where these accounts must be separate from the enterprise Active Directory Domain Services (AD DS) user account store.

Best practices related to AD LDS

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

- Use the highest level of replication security that your environment can support.
- In AD DS environments, run AD LDS on member servers, rather than on domain controllers, whenever possible.
- Use separate configuration sets for applications with strict isolation requirements.

Tools

Tool	Use	Where to find it
LDIFDE	• Performing batch operations against directories that conform to the LDAP standards	%systemroot%\System32
LDP	• Performing operations (such as connect, bind, search, modify, add, delete) against any LDAP-compatible directory, such as Active Directory	%systemroot%\System32
ADSIEdit	• Managing objects and attributes in LDAP directories. ADSI Edit provides a view of every object and attribute in the directory.	%systemroot%\System32

Lab Review Questions and Answers

1. What ports are used by default for AD LDS?

   Answer: On member servers, ports 389 and 636 for SSL. On a domain controller the default ports are 50000 and 50001 for SSL, but any ports can be used on any server as long as they are not being used by other services.

2. What type of input files are used to customize the schema?

   Answer: LDIF files are used to modify the schema.

3. What groups reside in the Roles container of each directory partition?

   Answer: Administrators, Readers, and Use

Module 9

Configuring Active Directory® Certificate Services

Contents:

Lesson 1

Deploying Active Directory Certificate Services

Contents:

Question and Answers

What Is New in AD CS in Windows Server 2008?

Question: Which new feature is most important for your organization?

Answer: Answers may vary. However, most organizations find Online Responder Restricted Enrollment Agent and Enterprise PKI as the most useful new features.

Types of CAs

Question: What is the main difference between a root CA and a subordinate CA?

Answer: Root CAs issue a self-signed certificate for itself while subordinate CA always receives a certificate from a root CA.

Upgrading Certification Authority to Windows Server 2008 AD CS

Question: What is the main difference between upgrade and migration of CA?

Answer: Whereas upgrade is performed along with operating system upgrade, migration of CA can be performed without this step, by moving functionality of CA to another machine.

Additional Reading

What Is New in AD CS in Windows Server 2008?

For more information on the Active Directory Certificate Services role, see http://go.microsoft.com/fwlink/?LinkID=178060&clcid=0x409.

Stand-Alone vs. Enterprise CAs

For more information about types of CAs and the roles they can play, visit http://go.microsoft.com/fwlink/?LinkID=178061&clcid=0x409.

Considerations for Installing Root and Subordinate CAs

- To learn how to install an enterprise root certification authority, visit http://go.microsoft.com/fwlink/?LinkID=178062&clcid=0x409.
- To learn how to install a stand-alone root certification authority, visit http://go.microsoft.com/fwlink/?LinkID=178063&clcid=0x409.
- To learn how to install an enterprise subordinate certification authority, visit http://go.microsoft.com/fwlink/?LinkID=178064&clcid=0x409.
- To learn how to install a stand-alone subordinate certification authority, visit http://go.microsoft.com/fwlink/?LinkID=178065&clcid=0x409.

Upgrading Certification Authority to Windows Server 2008 AD CS

For more information about AD CS upgrade and migration, read the Active Directory Certificate Services Upgrade and Migration Guide, available for download from http://go.microsoft.com/fwlink/?LinkId=116454.

Lesson 2

Managing Certificate Templates

Contents:

Question and Answers

Certificate Template Versions

Question: What should you do when you want to modify a certificate template that is version 1?

Answer: You should duplicate that template to make a template of version 2 or 3.

Configuring Certificate Template Permissions

Question: To which security principals will you give Full Control permission on Certificate templates?

Answer: Answers may vary. However, you will probably give Full Control permission to administrators that should be able to modify templates as well as assign permissions to other.

Methods for Updating a Certificate Template

Question: What is the difference between superseding and updating?

Answer: Superseding is a process in which one new certificate template replaces several other certificate templates with a similar purpose. Updating is a process where a single certificate template is changed.

Demonstration: Modifying and Enabling a Certificate Template

Question: Why would you need to modify a certificate template?

Answer: If you want to change any attribute or property in the template.

Detailed Demo Steps

Demonstration: Modifying and Enabling a Certificate Template

Detailed demonstration steps

In this demonstration, you will see how to:

- Create, modify, and supersede a template.
- Issue a certificate to be used by a CA.

Create, modify, and supersede a template; and issue a certificate to be used by a CA

1. Launch virtual machine **6416C-LON-DC1,** and log on as **Contoso\Administrator.**
2. Click **Start,** click **Administrative Tools,** and then click **Certification Authority.**
3. In the Certification Authority console, expand **ContosoCA,** right-click **Certificate Templates,** and then click **Manage.**
4. Review the list of default templates and examine them and their properties.
5. In the details pane, double-click **IPSec**.
6. Scroll through the tabs and note what you are able to modify on each tab. On the Security tab, you define permissions for enrollment. Close the template.

   You can create a template by duplicating an existing template and modifying it to suit your specific needs.
7. In the details pane, right-click the **Exchange User** certificate template, and then click **Duplicate Template**.
8. In the **Duplicate Template** dialog box, click **Windows Server 2008, Enterprise Edition**, and then click **OK**.
9. In the **Properties of New Template** dialog box, type **Exchange User Test** in the **Template display name** box.
10. On the **Superseded Templates** tab, click **Add.**
11. Click the **Exchange User** template, and then click **OK.**
12. On the **Security** tab, for **Authenticated Users**, click **Allow** for **Read, Enroll**, and **Autoenroll** permissions, and then click **OK.**
13. Close the **Certificate Templates** console.
14. In the Certification Authority console, right click **Certificate** templates, select **New**, and then click **Certificate Template to issue**.
15. From the list of templates, choose **Exchange User Test**, and then click **OK**.

Additional Reading

Certificate Templates in Windows Server 2008

For more information about implementing and administering certificate templates in Windows Server 2008, visit http://go.microsoft.com/fwlink/?LinkID=178066&clcid=0x409.

Certificate Template Versions

For more information about certificate templates, see http://go.microsoft.com/fwlink/?LinkID=178067&clcid=0x409.

Methods for Updating a Certificate Template

For more information on administering certificate templates, see http://go.microsoft.com/fwlink/?LinkID=178068&clcid=0x409.

Lesson 3

Managing Certificate Enrollment

Contents:

Question and Answers

Certificate Web Enrollment in Windows Server 2008

Question: Why can't you request computer certificates using Web Enrollment?

Answer: Internet Explorer cannot run in the local computer's security context; therefore, users can no longer request computer certificates by using Web enrollment.

Obtaining Certificates by Using Manual Enrollment

Question: In which scenarios will you use Web enrollment over Certificates console enrollment?

Answer: If you want to request a certificate from a non-domain computer, you will use Web Enrollment.

What Is NDES?

Question: How can NDES improve security?

Answer: By issuing and handling certificate for network devices, NDES can enable you to use encryption on these devices

Detailed Demo Steps

Demonstration: Configuring the Restricted Enrollment Agent

Detailed demonstration steps

In this demonstration, you will see how to:

- Configure the restricted enrollment agent.

Configure the restricted enrollment agent

1. Open the **Certification Authority** snap-in, right-click the name of the CA, and then click **Properties.**
2. On the **Enrollment Agents** tab, click **Restrict enrollment agents,** and then click **OK** on the message that appears.
3. Under **Enrollment agents,** click **Add,** type the names of the users or groups that you want to configure (for example, Don Roessler), and then click **OK**. Click **Everyone**, and then click **Remove.**
4. Under **Certificate Templates**, click **Add,** select the template for the certificates that you want this user or group to be able to enroll from (for example, EFS Recovery Agent), and then click **OK**. Repeat this step until you have selected all certificate templates that you want to enable for this enrollment agent. When you have finished adding the names of certificate templates, click **<All>**, and then click **Remove**.
5. Under **Permissions**, click **Add**, type the names of the users or groups (for example, Spencer Low) for whom you want the enrollment agent to manage the defined certificate types, and then click **OK.** Click **Everyone**, and then click **Remove**.
6. If you want to block the enrollment agent from managing certificates for a user, computer, or group, under **Permissions**, select this user, computer, or group, and then click **Deny**.
7. When you are finished configuring enrollment agent restrictions, click **OK** or **Apply**.

Additional Reading

Obtaining Certificates by Using Manual Enrollment

For information on advanced certificate enrollment and management, see http://go.microsoft.com/fwlink/?LinkID=178069&clcid=0x409.

What Is the Restricted Enrollment Agent?

For more information on the AD CS restricted enrollment agent, see http://go.microsoft.com/fwlink/?LinkID=178070&clcid=0x409.

Lesson 4

Managing Certificate Revocation

Contents:

Question and Answers

Reason Codes for Revoking a Certificate

Question: Why is it important to provide a reason when revoking certificates?

Answer: It is important for tracking certificate usage and management.

How Are CRLs Published?

Question: In which scenarios is it recommended to use delta CRL? What are the drawbacks?

Answer: If you have large CRLs, it is recommended to use delta CRLs. Delta CRLs are limited to Windows machines.

What Is an Online Responder?

Question: In which scenario will you deploy Online Responder?

Answer: If there are a large number of certificates used in organization, with high frequency of publishing new CRLs, it will be beneficial to use Online Responder.

Detailed Demo Steps

Demonstration: Configuring the Restricted Enrollment Agent

Detailed demonstration steps

In this demonstration, you will see how to:

- Configure an Online Responder.
- Install the Online Responder component on a Web server.
- Configure CA to include the Online Responder location in the AIA.
- Issue the OCSP Response Signing template.
- Configure the Online Responder.

Configure an Online Responder

1. In the Certification Authority console, open the **ContosoCA Properties** dialog box.
2. On the **Extensions** tab, examine the **CDPs**, and then close the **ContosoCA Properties** dialog box.
3. Right-click on **Revoked Certificates**, and then click **Properties.**
4. Set the **CRL Publication interval** to **1 Month.**
5. Set the **Publish Delta CRLs interval** to **5 Days.**

Install the Online Responder component on a Web server

- Use **Server Manager** to install the AD CS Online Responder role service.

Configure CA to include the Online Responder location in the AIA

1. In the Certification Authority console, open the **ContosoCA Properties** dialog box.
2. On the **Extensions** tab**,** add **http://LON-DC1/ocsp** as an AIA location. Also enable the **Include in the AIA extension of issued certificates** and the **Include in the online certificate status protocol (OSCP) extension** check boxes.
3. Close the **ContosoCA Properties** dialog box. Click **Yes** to restart AD CS.

Issue the OCSP Response Signing template

1. Use the **Certificate Templates** console to set the permissions on the **OCSP Response Signing template** so that you allow **Enroll** permission for the authenticated users.
2. Use the **Certification Authority** console to issue the OCSP Response Signing template.

Configure the Online Responder

1. Launch the **Online Responder Management** console.
2. Right-click **Revocation Configuration**, and then click **Add Revocation Configuration.**
3. Use the wizard to create a new revocation configuration named **ContosoCA. Online Responder.** Choose to **select a certificate for an Existing enterprise CA.** Browse to and select the **ContosoCA** certificate that is published in Active Directory. Choose to **Automatically select a signing certificate using AutoEnroll.**

After you run the wizard, the revocation configuration status will be set to Online.

4. Close the **Online Responder** console.

Additional Reading

What Is an Online Responder?

For more information about OCSP, see http://go.microsoft.com/fwlink/?LinkID=178071&clcid=0x409.

How Online Responders Work

To see the Online Responder Installation, Configuration, and Troubleshooting Guide, go to http://go.microsoft.com/fwlink/?LinkId=160643.

Lesson 5

Managing Certificate Recovery

Contents:

Question and Answers

Overview of Key Archival and Recovery

Question: What is a key recovery agent?

Answer: An individual to whom the role of key recovery agent is assigned within an organization, and to whom a KRA certificate is issued.

Configuring Automatic Key Archival

Question: Why is it important to keep KRA certificates secure?

Answer: Users with a KRA certificate are able to recover other users' private keys from the database.

Detailed Demo Steps

Demonstration: Configuring CA for Key Archival

Detailed demonstration steps

In this demonstration, you will see how to:

- Configure CA to archive private keys.
- Enroll for a Key Recovery Agent certificate.

Configure CA to archive private keys and enroll for a Key Recovery Agent certificate

1. On the LON-DC1 virtual machine, click **Start**, point to **Administrative Tools**, and then click **Certification Authority.** This opens the Certification Authority console.
2. In the Certificate Authority console, expand the **ContosoCA** node, right-click the **Certificates Templates** folder, and then click **Manage.**
3. In the details pane, right-click the **Key Recovery Agent** certificate, and then click **Properties.**
4. In the **Key Recovery Agent Properties** dialog box, on the **Issuance Requirements** tab, clear **the CA certificate manager approval** check box.

   Note: This is for test purposes only. In a production environment, you should not change this value.
5. On the **Security** tab, notice that Domain Admins and Enterprise Admins are the only groups that have the Enroll permission, and then click **OK**. Make no changes here.
6. Close the **Certificates Templates** console.
7. In the Certificate Authority console, configure a CA to issue certificates based on the **Key Recovery Agent** template: right-click **Certificate Templates**, click **New,** click **Certificate Template to issue**, click **Key Recovery Agent,** and then click **OK.**
8. Open **Run,** start **mmc.exe,** add the **Certificates** snap-in, and then click **My user account**.
9. Expand **Certificates,** expand **Current User**, expand **Personal,** and then expand **Certificates.** Right-click **Certificates,** select **All tasks**, and then click **Request New Certificate.**
10. Enroll for **Key Recovery Agent Certificate** by using a wizard.
11. Confirm that the new certificate is shown in the Certificates store. If it is shown, you have enrolled the Administrator to be the Key Recovery Agent. Minimize the **Certificates** console.
12. Open the properties of **ContosoCA.**
13. On the **Recovery Agents** tab, click **Archive the Key**, click **Add,** and then choose the **Administrator** certificate.
14. Click **OK** and confirm to restart AD CS.
15. Right-click **Certificate Templates**, and then click **Manage**.
16. -click the **Exchange User Test** certificate to open the **Properties** dialog box. On the **Request Handling** tab, click **Archive subject's encryption private key** and **Use advanced Symmetric algorithm to send key to the CA.** Close the template.

17. In the **Certificate Authority** console, configure a CA to issue certificates based on the **Exchange User Test** template: right-click **Certificate Templates,** click **New,** click **Certificate Template to issue,** click **Exchange User Test,** and then click **OK.**

Demonstration: Recovering a Lost Key

In this demonstration, you will see how to:

- Recover an archived certificate and a key from Active Directory.

Recover an archived certificate and a key from Active Directory

1. Open **Run**, start **mmc.exe**, add the **Certificates** snap-in, and then click **My user account**.
2. Expand **Certificates,** expand **Current User**, expand **Personal**, and then expand **Certificates.** Right-click **Certificates**, select **All tasks**, and then click **Request New Certificate.**
3. Enroll for the **Exchange User Test** certificate by using a wizard. When you select the **Exchange User Test** template in the wizard, click to open settings in a note to enter **Subject name.** Choose **Email** in the **Type** list, enter **administrator@contoso.com** as the value, and click **Add.** Click **OK,** and then click **Enroll.**
4. Verify that the certificate has appeared in the **Certificates** folder in the **Personal** store.
5. Simulate a lost private key by deleting the administrator@contoso.com certificate from the **Personal certificate** store. Minimize the **Certificates (Console1)** console.
6. In the Certification Authority console, in the Issued Certificates folder, double-click the certificate that you issued in an earlier step and record the serial number on the **Details** tab. (You can copy/paste it to Notepad, and then remove spaces between numbers.)
7. Open a **Command Prompt** window (with elevated privileges—right-click it on the **Start** menu, and then click **Run as Administrator).**
8. Switch to the root of drive C by typing **cd..** and then pressing ENTER. (You will probably have to do it twice,)
9. Select the certificate serial number from Notepad, right-click it, and then choose **Copy.**
10. In the **Command Prompt** window, type the following command: **Certutil -getkey serialnumber outputblob**, where *serialnumber* is a number that you paste from Notepad. (Note: If a question mark appears at the beginning of the number after pasting it, delete it.) Then press ENTER.
11. After the command is completed successfully, open drive C and verify that the Outputblob file has appeared.
12. At the command prompt, type: **Certutil -recoverkey outputblob recover.pfx**, and then press ENTER.
13. When prompted, type **Pa$$w0rd** as the new password, and then confirm the password.
14. Browse to drive C, and then verify that the Recover.pfx file—the recovered key—is created.
15. Double-click **recover.pfx.**
16. Click **Next** two times.
17. Enter the password **Pa$$w0rd**, click **Next** twice, click **Finish,** and then click **OK.**
18. Restore the Certificates console (Console 1). Refresh the Certificates store.

19. Verify that the **administrator@contoso.com** certificate has appeared.

Additional Reading

Configuring Automatic Key Archival

To see the Active Directory Certificate Services Longhorn Beta3 Key Archival and Recovery Whitepaper, go to http://go.microsoft.com/fwlink/?LinkID=178073&clcid=0x409.

Recovering a Lost Key

To see the Active Directory Certificate Services Longhorn Beta3 Key Archival and Recovery Whitepaper, go to http://go.microsoft.com/fwlink/?LinkID=178073&clcid=0x409.

Module Reviews and Takeaways

Review questions

1. What are some reasons that an organization would utilize PKI?

   Answer: Some reasons are: improving security, identity control, digital signing of code, and so on.

2. What are some reasons that an organization would use an enterprise root CA?

   Answer: If an organization wants to use only one CA and wants to use certificate templates and autoenrollment, then Enterprise RootCA will be the only choice.

3. What are some reasons that an organization would publish a CRL?

   Answer: CRLs must be published so that clients can verify certificates of their peers.

4. List the requirements to use autoenrollment for certificates.

   Answer: You must have Enterprise CA and you must configure Group Policy options.

5. For what is the DACL in a certificate template used?

   Answer: You use DACL on a certificate template to control permissions on the template, for example, who can enroll for a certificate based on that template.

6. Why would you use manual certificate enrollment?

   Answer: If you want to specify some additional options when enrolling for a certificate, you will use manual enrollment.

7. What are the steps to configure an Online Responder?

   Answer: You must create a Responder Configuration, and you must enroll for an OCSP Signing certificate. You must also add a Responder URL to AIA.

Common issues related to Active Directory certificate services

Issue	Troubleshooting tip
The location of the CA certificate specified in the authority information access extension is not configured to include the certificate name suffix. Clients may not be able to locate the correct version of the issuing CA's certificate to build a certificate chain, and certificate validation may fail.	Use the Certification Authority snap-in to configure the authority information access extension to include the certificate name suffix in each location.
CA is not configured to include CRL distribution point locations in the extensions of issued certificates. Clients may not be able to locate a CRL to check the revocation status of a certificate, and certificate validation may fail.	Use the Certification Authority snap-in to configure the CRL distribution point extension and specify the network location of the CRL. The default locations of the CRL are added to the CRL distribution point extension settings during CA installation, and the CA is configured to include the default locations in the extensions of all issued certificates.
CA was installed as an enterprise CA, but Group Policy settings for user autoenrollment have not been enabled. An enterprise CA can use	Use the Group Policy Management Console to configure user autoenrollment policy settings, and use the Certificate Templates snap-in to configure autoenrollment settings on

autoenrollment to simplify certificate issuance and renewal. If autoenrollment is not enabled, certificate issuance and renewal may not occur as expected.	the certificate template.

Real-world issues and scenarios

Contoso, Ltd wants to deploy PKI for supporting and securing several services, and they decided to use Windows Server 2008 Certificate Services as a platform for PKI. Certificates will be primarily used for EFS, digital signing, and for Web servers. Because documents that will be encrypted are very important, it is crucial to have a disaster recovery strategy in case of key loss. Also, clients that will access secure parts of the company Web site must not receive any warning in their browsers.

1. What kind of deployment should Contoso, Ltd choose?

   Answer: Contoso, Ltd should deploy an Enterprise CA, either as the root CA or as a subordinate issuing CA. This will enable automatic distribution of the root certificate to all clients.

2. What kind of certificates should be used for EFS and digital signing?

   Answer: The organization will need to deploy user certificates to enable EFS and digital signing.

3. What kind of certificates should be used for a Web site?

   Answer: The organization will need to deploy server certificates for the Web server.

4. How will Contoso, Ltd ensure that EFS encrypted data is not lost if a user loses a certificate?

   Answer: The organization will need to enable key archival and recovery.

Best practices related to Active Directory certificate services

- When deploying CA infrastructure, deploy Stand-Alone (non-domain joined) Root CA, and Enterprise Subordinate CA (issuing CA). After the Enterprise Subordinate CA gets a certificate from RootCA, take RootCA offline.
- Issue a certificate for RootCA for a long period of time.
- Use autoenrollment for certificates that are widely used.
- Use a Restricted Enrollment Agent whenever possible.

Lab Review Questions and Answers

1. Why is it not recommended to install just Enterprise Root CA?

   Answer: For security reasons, Root CA should be offline, without any network access. Enterprise RootCA can not be offline, so there is no maximum protection for its key.

2. What is the main benefit of OCSP over CRL?

   Answer: OCPS provides status for a single certificate that clients request instead of downloading the whole CRL. Also, responses are much faster and more reliable, because clients do not cache them.

3. What must you do in order to be able to recover private keys?

   Answer: You must configure CA to archive private keys for specific templates, and you must issue a Key Recovery Agent certificate.

Module 10

Configuring Active Directory® Federation Services

Contents:

Lesson 1

Overview of AD FS

Contents:

Question and Answers

Discussion: Identity Federation Business Requirements

Question: What are the business requirements that can lead to the deployment of an identity federation solution?

Answer: There are many possible answers to this question, but the root requirement will always be the secure exchange of information. Possible additional requirements include the need to:

- Share data and access to applications between organizations.
- Maintain local management of applications and user accounts.
- Maintain isolation between Active Directory forests.
- Maintain isolation between extranets and intranets.
- Reduce administrative efforts by managing only one user account for each user.

Additional Reading

What Is Identity Federation?

- For more information on the new features in AD FS in Windows Server 2008, see http://go.microsoft.com/fwlink/?LinkID=161012.
- For additional information on AD FS, refer to http://go.microsoft.com/fwlink/?LinkID=115969.

Identity Federation Scenarios

For more information on Federation scenarios, see http://go.microsoft.com/fwlink/?LinkID=161013.

Lesson 2

Deploying AD FS

Contents:

Question and Answers

Demonstration: How to Install the AD FS Server Role

Question: What are the available AD FS role services?

Answer: The server role and the federation server role

Question: Which are the two role services that cannot be installed on the same computer?

Answer: The Federation Service and the Federation Service proxy

Question: What services are required to install the AD FS server role?

Answer: AD DS and AD CS

Detailed Demo Steps

Demonstration: How to Install the AD FS Server Role

Detailed demonstration steps

1. On the LON-DC1 virtual machine, logged on as **Contoso\Administrator,** click **Start,** click **Administrative Tools,** and then click **Server Manager.** The Server Manager console appears.
2. In the console pane, click **Roles.**
3. In the Details pane, click **Add Roles.** The Add Roles Wizard appears.
4. On the **Before You Begin** page, click **Next.**
5. On the **Select Server Roles** page, select the **Active Directory Federation Services** check box, and then click **Next**.
6. On the **Active Directory Federation Services (AD FS)** introduction page, click **Next**.
7. On the **Select Role Services** page, select the **Federation Service** check box.
8. In the **Add Roles Wizard** box, click **Add Required Role Services.** This installs the Web Server (IIS) prerequisite. Click **Next.**
9. On the **Choose A Server Authentication Certificate for SSL Encryption** page, click **Create a self-signed certificate for SSL encryption**, and then click **Next**.
10. On the **Choose A Token-Signing Certificate** page, click Cre**ate a self-signed token-signing certificate**, and then click **Next**.
11. On the **Select Trust Policy** page, click **Next**.
12. On the **Web Server (IIS)** introduction page, click **Next** to accept the default path name for the trust policy.
13. On the **Select Role Services** page, click **Next** to accept the default settings for the Web server. Click **Install.** All specified roles, role services, and features will be installed.
14. On the **Installation Results** page, ensure that all tasks are successful, and then click **Close.**
15. In the Server Manager console, click the **Close** button.

Additional Reading

AD FS System Requirements

For more information on the requirements for deploying the AD FS role, see http://go.microsoft.com/fwlink/?LinkID=161014.

Demonstration: How to Install the AD FS Server Role

For more information on installing the AD FS role, see http://go.microsoft.com/fwlink/?LinkID=161012.

Lesson 3

Implementing AD FS Claims

Contents:

Question and Answers

Demonstration: How to Configure AD FS Claim Mapping

Question: What are claims?

Answer: Claims are used to identify users. A claim specifies information about users, including identity and group memberships.

Question: What is claim mapping?

Answer: Claim mapping is the act of mapping, removing or filtering, or passing inbound claims into outbound claims. Claim mapping may be different for each federation partner.

Question: Why do you need to define identical claims for both AD FS partners?

Answer: The claim effectively states who the user is and what they can do. It is important that the information be consistent among partners to ensure appropriate access to resources and to ensure claims are properly mapped.

Detailed Demo Steps

Demonstration: How to Configure AD FS Claim Mapping

Detailed demonstration steps

Note: Your instructor has already completed the demonstration in Lesson 2 and the LON-DC1 virtual machine is still running. To prepare for this demo, your instructor must additionally start the NWTDC01 virtual machine. Your instructor will have already performed some steps to put the virtual machines into the appropriate context for this demonstration.

Important: Either perform all tasks as part of the demonstration, or else complete tasks A-J prior to the demonstration, and complete only task K for the students.

A. Install the AD FS server role on the NWTDC01 virtual machine

1. On the NWTDC01 virtual machine, log on as **NORTHWINDTRADER\Administrator.**
2. Click **Start**, and then click **Server Manager.**
3. On the NWTDC01 virtual machine, in the Server Manager console, in the console pane, click **Roles.**
4. In the Details pane, click **Add Roles.** The Add Roles Wizard appears.
5. On the **Before You Begin** page, click **Next.**
6. On the **Select Server Roles** page, select the **Active Directory Federation Services** check box, and then click **Next.**
7. On the **Active Directory Federation Services (AD FS)** introduction page, click **Next.**
8. On the **Select Role Services** page, select the **Federation Service** check box.
9. In the **Add Roles Wizard** box, click **Add Required Role Services.** This installs the Web Server (IIS) prerequisite. Click **Next.**
10. On the **Choose a Server Authentication Certificate for SSL Encryption** page, click **Create a self-signed certificate for SSL encryption,** and then click **Next.**
11. On the **Choose a Token-Signing Certificate** page, click **Create a self-signed token-signing certificate,** and then click **Next.**
12. On the **Select Trust Policy** page, click **Next** to accept the default path and name for the trust policy.
13. On the **Web Server (IIS)** introduction page, click **Next.**
14. On the **Select Role Services** page, select the **ASP** check box, and then click **Next.**
15. Click **Install.** All specified roles, role services, and features will be installed.
16. On the **Installation Results** page, ensure that all tasks are successful, and then click **Close.**
17. In the Server Manager console, click **Close.**

B. Configure the SSL certificate for the LON-DC1 virtual machine

1. On the LON-DC1 virtual machine, click **Start,** click **Run,** type **mmc** in the **Open** box, and then click **OK.** The Console1 - [Console Root] appears.
2. In the Console1 - [Console Root], click **File,** and then click **Add/Remove Snap-in.**
3. Select **Certificates,** and then click **Add.** The Certificates snap-in window opens.
4. Click **Computer account,** and then click **Next.**
5. Click **Local computer,** click **Finish,** and then click **OK.**
6. In the tree pane, double-click the **Certificates (Local Computer)** icon, and then click **Personal.**
7. In the console pane, double-click **Certificates.**
8. Right-click the **LON-DC1.Contoso.com** certificate, and click **Copy.**
9. Expand the **Trusted Root Certification Authorities** node, right-click **Certificates,** and then click **Paste.**
10. Repeat steps 8 and 9 for the **Federation Server LON-DC1** certificate located in the **Personal\Certificates** node.
11. In the Console1 - [Console Root\Certificate(Local Computer)\Personal \Certificated] console, click the **Close** button. Do not save changes to the console.

C. Configure the SSL certificate for the NWTDC01 virtual machine

1. On the NWTDC01 virtual machine, click **Start**, click **Run,** type **mmc** in the **Open** box, and then click **OK.** The Console1 - [Console Root] appears.
2. In the **Console1 - [Console Root]**, click **File,** and then click **Add/Remove Snap-in.**
3. Select **Certificates,** click **Add,** click **Computer account,** and then click **Next.**
4. Click **Local computer: (the computer this console is running on)**, click **Finish**, and then click **OK.**
5. In the tree pane, double-click the **Certificates (Local Computer)** icon, and then double-click **Personal.**
6. In the console pane, click **Certificates.**
7. Right-click the **NWTDC01.NorthwindTraders.com** certificate, and click **Copy.**
8. Expand the **Trusted Root Certification Authorities** node, right-click **Certificates,** and then click **Paste.**
9. Repeat steps 7 and 8 for the **Federation Server NWTDC01** certificate located in the **Personal\Certificates** node.
10. In the Console1 - [Console Root\Certificate(Local Computer)\Personal \Certificated] console, click **Close.** Do not save the changes to the console.

D. Install the AD FS Web agent to support Windows token–based applications on the NWTDC01 virtual machine

1. On the NWTDC01 virtual machine, click **Start,** and then click **Server Manager.** The Server Manager console appears.

2. In the Server Manager console, in the console pane, click **Roles**.
3. In the Details pane, scroll down to the **Active Directory Federation Services** section, and then click **Add Roles Services**. The Add Roles Services Wizard appears.
4. On the **Select Role Services** page, select the **Windows Token-based Agent** check box, and then click **Next.**
5. On the **Specify Federation Server** page, in the **Federation Server** box, type **NWTDC01.NorthwindTraders.com**, and then click **Validate.** After successful validation, click **Next.**
6. On the **Confirm Installation Selections** page, click **Install**. The AD FS Web agent is installed.
7. On the **Installation Results** page, ensure that all tasks are successful, and then click **Close.**
8. In the Server Manager console, click the **Close** button.
9. Restart the **NWTDC01** virtual machine. After the server restarts, log on as **NORTHWINDTRADER\Administrator**, with the password **Pa$$w0rd.** Close the Server Manager window.

E. Ensure that the SSL certificate is bound to the default Web site on the NWTDC01 virtual machine

1. On the NWTDC01 virtual machine, click **Start**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**. The Internet Information Services Manager console appears.
2. In the tree pane of the Internet Information Services Manager console, expand the **NWTDC01 (NorthwindTraders\Administrator)** node, expand the **Sites** node, and then click **Default Web Site**.
3. In the Actions pane, click **Bindings**.
4. In the **Site Bindings** dialog box, click **https**, and then click **Edit**. Notice that the NWTDC01.NorthwindTraders.com certificate is bound to this Web site. Click **OK**, and then click **Close**.
5. In the details pane, double-click **SSL Settings**, select the **Require SSL** check box, and then click **Apply**.

F. Configure the token-based application

1. In the console pane of the Internet Information Services Manager console, right-click **Default Web Site**, and then click **Add Application**. The **Add Application** dialog box appears.
2. In the **Alias** box of the **Add Application** dialog box, type **tokenapp**, and then click **Select**.
3. Select **Classic .NET AppPool** from the list, and then click **OK**.
4. Click the ellipsis **(…)** button, and then click the **C:\inetpub\wwwroot** folder.
5. Click **Make New Folder**, name the folder **tokenapp**, click **OK**, and then click **OK** again.
6. Open a Windows Explorer window, and copy the contents of **\\LON-dc1\e$\Labfiles\Mod10\tokenapp** to **C:\inetpub\wwwroot \tokenapp**.

7. Cut the **blog.txt** file from the **tokenapp** folder, and paste it in **C:**.
8. In the Window Explorer window, click the **Close** button.

G. Configure the AD FS Web agent

1. In the tree pane of the Internet Information Services Manager console, click **NWTDC01(NorthwindTraders\Administrator).**
2. In the Details pane, double-click **Federation Service URL.**
3. In the Federation Service URL, ensure that the following URL is entered: **https://NWTDC01.northwindtraders.com/adfs/fs /federationserverservice.asmx.**

   Note: The Federation Service URL specified here, and also the Application and Return URLs, covered later, are case sensitive, and as such, they must all be identical. If they are not identical, you may receive an error when trying to connect later in the demo.
4. In the console pane, expand **Default Web Site**, and then click **tokenapp.**
5. In the Details pane, double-click **Authentication.**
6. Click **AD FS Windows Token-Based Agent**, and then click **Enable**.
7. If an error message appears, click **OK**.
8. Click **AD FS Windows Token-Based Agent**, and then click **Edit**. Under **Return URL** ensure that the following is entered: **https://NWTDC01.northwindtraders.com/tokenapp**/.
9. Click **Cancel** to close the **AD FS Windows Token-Based Agent** box.
10. If an error message appears, close the message box.
11. On the Internet Information Services Manager console, click the **Close** button.

H. Configure a forest trust between the intranet and the extranet forest

1. On the LON-DC1 virtual machine, click **Start**, point to **Administrative Tools**, and then click **Active Directory Domains and Trusts**. The Active Directory Domains And Trusts console appears.
2. In the console pane of the Active Directory Domains And Trusts console, right-click **Contoso.com**, and then click **Properties**.
3. On the **Contoso.com Properties** page, click the **Trusts** tab, and then click **New Trust**.
4. On the **Welcome To The New Trust Wizard** page, click **Next**.
5. On the **Trust Name** page, type **NorthwindTrader** in the **Name** field, and then click **Next**.
6. On the **Trust Type** page, click **Forest trust**, and then click **Next**.
7. On the **Direction Of Trust** page, select **One-way: incoming**, and then click **Next**.
8. On the **Sides Of Trust** page, select **Both this domain and the specified domain**, and then click **Next**.
9. In the **User Name** box, type **Administrator**. In the **Password** box, type **Pa$$w0rd**, and then click **Next**.
10. On the **Outgoing Trust Authentication Level-Specified Forest** page, ensure that **Forest-wide authentication** is selected, and then click **Next**.

11. On the **Trust Selections Complete** page, click **Next**.
12. On the **Trust Creation Complete** page, click **Next**.
13. On the **Confirm Incoming Trust** page, click **Yes, confirm the incoming trust**, and then click **Next**.
14. On the **Completing The New Trust Wizard** page, click **Finish**.
15. In the **Contoso.com Properties** dialog box, click **OK**.
16. In the Active Directory Domains And Trusts console, click the **Close** button.

I. Configure and export the trust policy on the NWTDC01 virtual machine

1. On the NWTDC01 virtual machine, click **Start**, point to **Administrative Tools**, and then click **Active Directory Federation Services**. The Active Directory Federation Services console appears.
2. In the console pane of the Active Directory Federation Services console, expand the **Federation Service** node, right-click **Trust Policy**, and then click **Export Basic Partner Policy**.
3. In the **Export Basic Partner Policy** box, click **Browse**.
4. In the **File name** box, type **C:\NWTPolicy**, and then click **Save.**
5. On the **Export Basic Partner Policy** page, click **OK**.
6. In the Active Directory Federation Services console, click the **Close** button.
7. On the **Start** menu, click **Run,** type **\\lon-dc1\c$** in the **Open** box, and then click **OK.**
8. Copy **C:\NWTPolicy.xml** from the NWTDC01 virtual machine to **C:** on LON-DC1.
9. In the Explorer window, click the **Close** button.

J. Configure and export the trust policy on the LON-DC1 virtual machine

1. On the LON-DC1 virtual machine, on the **Start** menu, point to **Administrative Tools**, and then click **Active Directory Federation Services.** The Active Directory Federation Services console appears.
2. In the console pane of the Active Directory Federation Services console, expand **Federation Service**, right-click **Trust Policy**, and then click **Export Basic Partner Policy**.
3. In the **Export Basic Partner Policy** box, click **Browse.**
4. In the **File name** box, type **C:\ContosoPolicy**, and then click **Save.**
5. On the **Export Basic Partner Policy** page, click **OK.**
6. In the Active Directory Federation Services console, click the **Close** button.

K. Configure claims

1. On the LON-DC1 virtual machine, click **Start**, point to **Administrative Tools**, and then click **Active Directory Federation Services**. The Active Directory Federation Services console appears.
2. In the Active Directory Federation Services console, expand the **Federation Service** node, the **Trust Policy** node, and the **My Organization** node.

3. Right-click **Organization Claims**, point to **New**, and then click **Organization Claim.**
4. In the **Create a New Organization Claim** box, under **Claim name**, type **TokenApp**.
5. Ensure that **Group claim** is selected, and then click **OK**.
6. In the console pane of the Active Directory Federation Services console, expand **Federation Service**, expand the **Trust Policy** node, expand the **My Organization** node, right-click **Account Stores**, point to **New,** and then click **Account Store.**
7. On the **Welcome To The Add Account Store Wizard** page, click **Next.**
8. On the **Account Store Type** page, ensure that **Active Directory Domain Services (AD DS)** is selected, and then click **Next.**
9. On the **Enable This Account Store** page, ensure that the **Enable this account store** check box is selected, and then click **Next**.
10. Click **Finish.** Under **Account Stores**, right-click **Active Directory**, point to **New**, and then click **Group Claim Extraction.**
11. On the **Create A New Group Claim Extraction** page, click **Add.** In the **Select Users or Groups** box, type **TokenAppGroup,** and then click **OK.**
12. Ensure that **TokenApp** is displayed under **Map to this Organization** claim, and then click **OK**.
13. In the console pane of the Active Directory Federation Services console, expand **Partner Organizations**, right-click **Resource Partners**, point to **New**, and then click **Resource Partner.**
14. On the **Welcome to the Add Resource Partners Wizard** page, click **Next.**
15. On the **Import Policy File** page, click **Yes.**
16. Under **Partner interoperatability policy** file, type **C:\NWTPolicy.xml,** and then click **Next.**
17. On the **Resource Partner Details** page, click **Next.**
18. On the **Federation Scenario** page, click **Federated Web SSO with Forest Trust,** and then click **Next.**
19. On the **Resource Partner Identity Claims** page, click **Next.**
20. On the **Select UPN Suffix** page, select the **Pass all UPN suffixes through unchanged** option, and then click **Next.**
21. On the **Enable This Resource Partner** page, select the **Enable this resource partner** check box, and then click **Next**.
22. On the **Completing the Add Resource Partner Wizard** page, click **Finish.**
23. In the AD FS console, right-click **NWTDC01.NorthwindTraders.com**, click **New**, and then click **Outgoing Group Claim Mapping.** The Create a New Outgoing Group Claim Mapping dialog box appears.
24. In the **Create a New Outgoing Group Claim Mapping** dialog box, select **TokenApp** from the **Organization group claims** list. In the **Outgoing group claim name** box, type **TokenAppMapping**, and then click **OK.**
25. Close the AD FS console.

Module Reviews and Takeaways

Review questions

1. What are some of the reasons organizations deploy AD FS?

   Answer: AD FS is deployed when organizations want to share information without creating new user accounts or trust relationships.

2. How would you describe an AD FS claim?

   Answer: An AD FS claim is the mechanism used to request authentication. The requestor "claims" to be an authorized entity, and the claim is then verified.

3. What is the purpose of an AD FS resource partner?

   Answer: The resource partner is the entity that contains the resources that are being used by the account partner.

4. Which two AD FS roles cannot be installed on the same server?

   Answer: The Federation Service and Federation Service Proxy cannot exist on the same physical machine.

Lab Review Questions and Answers

1. In the lab, which organization was the account partner and which was the resource partner?

   Answer: Contoso was the account partner and Northwind Traders was the resource partner.

2. In the lab, you implemented a self-signed certificate. If this was a real-world scenario, would that be appropriate?

   Answer: It might be difficult to distribute the certificate and users would otherwise receive security warnings and errors when accessing the application. A private CA might be suitable.

Module 11

Configuring Active Directory® Rights Management Services

Contents:

Lesson 1

Overview of AD RMS

Contents:

Question and Answers

What Is AD RMS?

Question: How can an organization benefit from AD RMS?

Answer: By using Active Directory Rights Management Services (AD RMS) and the AD RMS client, you can augment an organization's security strategy by protecting information through persistent usage policies, which remain with the information, no matter where it is moved.

When to Use AD RMS?

Question: What is the difference between providing permissions to access files using NTFS ACLs and using AD RMS?

Answer: By using RMS, you can provide more granular access control. For example, using ACL, you can allow or deny someone to access a file. Using AD RMS, you can provide someone the right to open a file but not to print it. Also, protection with AD RMS does not change when you move files.

Additional Reading

Components of AD RMS

For more information about AD RMS deployment components, see http://go.microsoft.com/fwlink/?LinkID=177609&clcid=0x409.

Lesson 2

Deploying AD RMS

Contents:

Question and Answers

Preinstallation Considerations

Question: What is the security risk of deploying AD RMS on Domain Controller?

Answer: The AD RMS service account must be a member of the Domain Admins group, which can pose a security risk.

Demonstration: Implementing an AD RMS Server

Question: What tool would you use to install the AD RMS server role?

Answer: The Server Manager Tool

Question: What are the various server roles that are required for the installation of the AD RMS server role?

Answer: AD DS, AD CS

Question: What servers can be included in an AD RMS cluster if Windows Internal Database is used?

Answer: The internal database does not accept remote connections, so you are limited to a single server.

What Is a Service Connection Point?

Question: Why is important to have Service Connection Point for AD RMS?

Answer: Active Directory Rights Management Services (AD RMS) clients use a service connection point (SCP) to automatically discover the AD RMS cluster.

Implementing an AD RMS Client

Question: What is the easiest way to deploy AD RMS client to operating systems that do not include it?

Answer: By using Group Policy

Detailed Demo Steps

Demonstration: Implementing an AD RMS Server

Configure a CNAME for the AD RMS cluster

1. Launch **LON-DC1**, and log on with the credentials **Contoso\Administrator** and password **Pa$$w0rd**.
2. Click **Start**, click **Administrative Tools**, and then click **DNS**.
3. In DNS Manager, expand **LON-DC1**, expand **Forward Lookup Zones**, and then expand **Contoso.com**.
4. Right-click **Contoso.com**, and then go to **New Alias (CNAME)**.
5. In the **Alias Name** box, type **RMS**, and in the **fully qualified domain name (FQDN) for target host** box, type **LON-DC1.contoso.com**.
6. Close the **DNS Manager**.

Install the AD RMS server role

1. On LON-DC1, open **Active Directory Users and Computers** from **Administrative Tools**.
2. In the **Users** container, create a user account with the username **ADRMSService** and password **Pa$$w0rd**. Select **Password never expires**. Add this account to the Server Operators group.

   Note: Tell students that you're doing this only for test purposes, since an account for the AD RMS service must be able to log on locally to validate the password during AD RMS setup. Because you're doing installation on Domain Controller, ordinary user accounts are not permitted to log on locally.
3. On LON-DC1, in the Server Manager, click the **Roles** node.
4. In the details pane, click **Add Roles**.
5. On the **Before You Begin** page, click **Next**.
6. On the **Select Server Roles** page, select the **Active Directory Rights Management Services** check box.
7. When prompted, click **Add Required Role Services**, and then click **Next**.
8. Click **Next** twice.
9. On the **Create or Join an AD RMS Cluster** page, select **Create a new AD RMS cluster**, and click **Next**.
10. On the **Select Configuration Database** page, select **Use Windows Internal Database on this server**, and then click **Next**.
11. On the **Specify Service Account** page, click **Specify**, type **Contoso\ADRMSService**, type **Pa$$w0rd** for the password, and click **OK** to provide a domain user account for the AD RMS service account. Then click **Next**.
12. On the **Configure AD RMS Cluster Key Storage** page, select **Use AD RMS centrally managed key storage**, and then click **Next**.

13. On the **Specify AD RMS Cluster Key Password** page, type **Pa$$w0rd** to confirm the AD RMS cluster key password, and then click **Next**.
14. On the **Select AD RMS Cluster Web Site** page, ensure that **Default Web Site** is selected, and then click **Next**.
15. On the **Specify Cluster Address** page, in the **Internal Address** box, type **rms.contoso.com**, select **Use an unencrypted connection (http://),** click **Validate**, and then click **Next**.

    Note: In the production environment, using SSL is highly recommended, but it invokes certificates.

16. On the **Server Licensor Certificate** page, accept the default value of **LON-DC1**, and click **Next**.
17. On the **Register AD RMS Service Connection Point** page, select **Register the AD RMS service Connection point now**, and then click **Next**.
18. On the **Web Server (IIS)** page, click **Next**.
19. On the **Select Role Services** page, click **Next**.
20. On the **Confirm Installation Selections** page, view the informational messages, and then click **Install** to complete the installation.
21. After the installation is complete, click **Close**.
22. Do not shut down LON-DC1. Just log off, and leave the virtual machine running, because you will need it for further demos.

Additional Reading

AD RMS Deployment Scenarios

For more information on AD RMS, see http://go.microsoft.com/fwlink/?LinkID=177610&clcid=0x409.

What Is a Service Connection Point?

For more information on AD RMS SCP registration, see
http://go.microsoft.com/fwlink/?LinkID=177611&clcid=0x409.

Lesson 3

Administering AD RMS Templates

Contents:

Question and Answers

Planning AD RMS Template Distribution

Question: In which scenario must you use manual template distribution?

Answer: If you have Windows XP or older clients, you must use manual distribution or use SMS or SCCM.

Demonstration: Creating a Rights Policy Template

Question: What are rights policy templates?

Answer: Rights policy templates are used to control the rights that a user or group has on a particular piece of rights-protected content.

Question: What is the purpose of archiving rights policy templates?

Answer: Archiving a template allows use licenses to continue to be granted but will not allow publishing new content.

Question: What is the difference between deployment of templates to Windows Vista released to manufacturing (RTM) and deployment of templates to the Windows Vista SP1 clients?

Answer: In Vista SP1 and later, Policy Templates are automatically updated through the use of a scheduled job. Previous versions did not perform the update, so you needed to replace the template when changes occurred.

Detailed Demo Steps

Demonstration: Creating a Rights Policy Template

Configure a distributed rights policy template

1. Log on to **LON-DC1** as **Administrator,** with the password of **Pa$$w0rd**. 2.
2. In Server Manager, expand the **Roles** node, and then expand the **Active Directory Rights Management Services** node. 3.
3. Expand **LON-DC1**. 4.
4. Browse to and click **Rights Policy Templates**. 5.
5. In the Actions pane, under **Rights Policy Templates**, click **Properties**. 6.
6. In the **Rights Policy Templates Properties** box, select **Enable export**. In the **Specify templates file location (UNC)** box, type **LON-DC1****Templates**, and then click **OK**.
7. In the details pane, click **Create Distributed Rights Policy Template**. Then, after the wizard is launched, click **Add**.
8. In the **Add New Template Identification Information** box, set **Language** to **English** (**United States**), set **Name** to **Confidential Projects**, set **Description** to **Contoso Pharmaceuticals IT Department**, and click **Add**. Then click **Next**.
9. On the **Add User Rights** page, click **Add**, and in the **Add User or Group** box, type **IT@Contoso.com**, and then click **OK**.
10. Under **Rights for IT@Contoso.com**, select the **Edit** check box.
11. Click **Add**, select **Anyone**, and then click **OK**.
12. Under **Rights for ANYONE**, select the **View** check box, and then click **Next**.
13. On the **Specify Expiration Policy** page, select **Expires after the following duration (days)** to specify content expiration, and type **14** as the value.
14. Click **Finish**.
15. Go to **\\LON-DC1\Templates** to view the template you just created.

Manage archived rights policy templates

1. In the distributed Rights Policy Template Information window, highlight the template you just created, **Confidential Projects**.
2. In the Actions pane, click **Archive this rights policy template**.
3. In the **Archive Rights Policy Template** dialog box, read the information, and then click **Yes**.
4. In the details pane, click the **Manage archived rights policy templates** link.
5. Highlight the **Confidential Projects** template, and in the Actions pane, click **Properties**. 6.
6. Step through the tabs to see what options are available.

Additional Reading

Planning AD RMS Template Distribution

For more information on template distribution, see
http://go.microsoft.com/fwlink/?LinkID=177612&clcid=0x409.

Lesson 4

Administering AD RMS Policies

Contents:

Question and Answers

Methods of Defining Trust Policies

Question: If you want to use AD RMS protected content on Internet, which was of defining trust policy is most convenient?

Answer: You can use Windows Live ID and configure trust to use it.

Overview of Trusted User Domain Interaction

Question: What must you do to make AD RMS issue licenses to users from other domains?

Answer: To configure AD RMS to issue these use licenses, you must import the Server Licensor Certificate (SLC) of the required user domain.

Demonstration: Configuring Trust Policies

Question: What is the purpose of setting up Trusted Publishing Domains (TPDs)?

Question: What is the format in which TPD certificates are created?

Question: What is the purpose of setting up trusted user domains?

Additional Reading

Deploying AD RMS with AD FS

To view the AD RMS with AD FS Identity Federation Step-by-Step Guide, go to http://go.microsoft.com/fwlink/?LinkID=156755.

Module Reviews and Takeaways

Review questions

1. What are some reasons to deploy AD RMS?

   Answer: AD RMS allows organizations to protect content through the use of XrML certificates and helps to secure information in a more flexible manner than using encrypted content.

2. What is the minimum OS and Service Pack level required to install AD RMS?

   Answer: Windows Server 2008 and SQL Server 2005. AD DCs must all be at least Windows 2000 SP3.

3. Can S/MIME be used to secure documents outside of e-mail?

   Answer: No

4. What is a lockbox?

   Answer: A lockbox is a dynamic link library (DLL) that can be used to increase the security of the environment in which an Active Directory Rights Management Services (AD RMS) application runs. The lockbox verifies all licenses and certificates used by the application and, for AD RMS clients, protects the process space by limiting access to required and optional modules identified in the application manifest.

5. What is a use license?

   Answer: The use license specifies what a user can do with protected content.

6. What special requirement must be met to install AD RMS on a domain controller?

   Answer: This is not a recommended solution. When AD RMS is installed on a domain controller, the service account must be a member of the Domain Administrators role.

7. What are some of the fields contained within a rights policy?

   Answer: Full Control, View, Save, Edit, Extract, Export, Print, Forward

Common issues related to AD RMS

Issue	Troubleshooting tip
Expired RMS Service Account Password.	If your RMS service account password expires, you must change the password on each RMS server that uses the account with the expired password, and then restart IIS. You can also configure a password on RMS account so that it does not expire.
Clients cannot open RMS-protected content due to expired permissions.	If a user's permissions have expired, the user cannot consume rights-protected content. If the system clock on the RMS server is ahead of the system clock on the RMS client, a user might also not be able to consume rights-protected content even when the permissions have not expired.
Clients cannot use AD RMS from applications.	E-mail attribute on user accounts is not set.
Clients are prompted for	AD RMS Cluster URL is not in Local intranet zone.

credentials when connecting to an AD RMS cluster URL from AD RMS–enabled application.	

Real-world issues and scenarios

Contoso Ltd wants to protect e-mail messages that are exchanged inside organization. They are using Microsoft Exchange Server 2007. They want to achieve the following result: When one of the managers sends an e-mail to all employees, only managers should be able to print, forward, and copy that e-mail. All other clients should only be able to view that e-mail, and the content must expire after 7 days. You are asked to propose a solution. Contoso has Windows Server 2008 Active Directory deployed. All client computers run Windows Vista SP1 and Office 2007.

1. Which solution will you propose?

   Answer: In this situation, AD RMS will be best solution.

2. How will you configure your solution?

   Answer: AD RMS should be installed on a member server running Windows Server 2008 in an existing domain. CNAME (alias) should be created in DNS and a URL for the AD RMS cluster will be added to Local intranet zone using Group Policy on a domain level. Required registry settings will also be deployed by using Group Policy. On the AD RMS side, right policy templates should be created to reflect requirements for content management. Users should be trained to use the AD RMS.

Best practices related to AD RMS

- Install AD RMS on a member server, not on a Domain Controller.
- Create an alias for the AD RMS cluster.
- Use SSL when connecting to the AD RMS cluster.
- Add the AD RMS cluster URL to the Local intranet zone for all clients.

Lab Review Questions and Answers

1. Why is it important to place the AD RMS cluster URL in the Trusted Sites zone?

   Answer: To use currently logged on user credentials while working with an AD RMS-enabled application, cluster URL must be in Trusted Sites zone.

2. Why do we create AD RMS templates?

   Answer: To make AD RMS easier to use for end users, administrators can pre-create templates with predefined permissions for documents.

3. What is the purpose of AD RMS policies?

   Answer: In order to be able to exchange ADRMS protected content with another organization, you must create trust policy.

Module 12

Software Maintenance Using Windows Server® Update Services

Contents:

Lesson 1

Introduction to Windows Server Update Services 3.0 SP1

Contents:

Question and Answers

What Is Windows Server Update Services?

Question: What is the main benefit of WSUS over Microsoft Update?

Answer: Centralizing update management and ability to approve or decline updates.

Question: What are other benefits of WSUS?

Answer: Ability to use Internet link more efficiently, control through Group policy, and so on.

Question: What are the components of WSUS solution?

Answer: WSUS server, WSUS Administration Console, Automatic Update client.

What's New in WSUS 3.0 SP1

Question: What is the most important new benefit of WSUS 3.0 SP1 for your environment?

Answer: Answers may vary depending on student environment. Usually, support for new client operating systems is most important to administrators.

WSUS Process

Question: What procedures must you perform to the client to get an update?

Answer: You must configure WSUS Server, configure the Automatic Updates component on client side by using registry or Group Policy to use WSUS, and define a schedule for update installation.

Additional Reading

WSUS Process

For more information about Windows Update, see the white paper "Windows Update Explained." This white paper can be found at http://go.microsoft.com/fwlink/?LinkID=177682&clcid=0x409.

Lesson 2

Installing and Configuring WSUS

Contents:

Question and Answers

Installing Components of WSUS 3.0 SP1

Question: Why is it important to install WSUS 3.0 SP1 by using Server Manager? What are the prerequisites to do that?

Answer: Installing through Server Manager, WSUS is secured by default, just as running Security Configuration Wizard after manual installation. Prerequisites are installing SP2 for Windows Server 2008.

Detailed Demo Steps

Demonstration: Automatic Updates Configuration Using Group Policy

Create a Group Policy object to control WSUS and Automatic Update settings

1. On LON-DC1, open the Group Policy Management Console from Administrative Tools.
2. Expand **Forest : Contoso.com**, and then navigate to Domains\Contoso.com\Group Policy Objects.
3. Right-click the **Group Policy Objects** item, and click **New**.
4. Type **WSUS** for the name of the GPO, and then click **OK**.
5. Right-click the **WSUS GPO**, and select **Edit**.
6. Expand Computer Configuration\Policies\Administrative Templates\ Windows Components\Windows Update node.

   Notice the available options and how they can be configured (for example, specify WSUS server, configure restart options)
7. Close the GPO Editor.
8. Right-click **Contoso.com** in GPMC, and click **Link an Existing GPO**.
9. Select **WSUS GPO**, and then click **OK**.

Additional Reading

Deployment Scenarios for WSUS

For more information on choosing a type of WSUS deployment, see http://go.microsoft.com/fwlink/?LinkID=177683&clcid=0x409.

WSUS 3.0 SP1 Post-Installation Configuration

For detailed instructions on how to configure the WSUS server, see http://go.microsoft.com/fwlink/?LinkID=177684&clcid=0x409.

Lesson 3

Managing WSUS

Contents:

Question and Answers

WSUS 3.0 SP1 Administration Console

Question: What is the main difference between Administration Console in WSUS 3.0 SP1 and earlier versions of WSUS?

Answer: WSUS 3.0 SP1 Administrator Console can be integrated into Server Manager. It also provides better administrative interface and better reporting.

Managing Computer Groups

Question: How would you use computer groups in your environment?

Answer: Answer may vary depending on student's environment. Usually, separate computer groups are created for test computers, and production computers.

Considerations for Managing Updates

Question: In which situations will it be reasonable to use automatic approval for updates? In which situations is this not recommended?

Answer: For new versions of earlier updates, it can be convenient to use auto approval.

Using and Managing Reports

Question: Which type of WSUS report is most important in your organization?

Answer: Answer may vary depending on type of environment that student has. Usually, computer status report and Sync report are most important.

Backing Up and Restoring WSUS

Question: What do you have to do after you restore your WSUS server data?

Answer: You should recycle IIS Pool and reset the database.

Additional Reading

Managing Updates

For more information about your options for storing updates, see http://go.microsoft.com/fwlink/?LinkId=79983.

Considerations for Managing Updates

For more information about managing updates, see http://go.microsoft.com/fwlink/?LinkID=177685&clcid=0x409.

Using and Managing Reports

For more information on reporting, see http://go.microsoft.com/fwlink/?LinkID=177686&clcid=0x409.

Backing Up and Restoring WSUS

For more information about WSUS backup and restore, see http://go.microsoft.com/fwlink/?LinkID=177687&clcid=0x409.

WSUS Best Practices

The full list of best practices is available at http://go.microsoft.com/fwlink/?LinkID=177688&clcid=0x409.

Module Reviews and Takeaways

Review questions

1. What is the main purpose of WSUS?

   Answer: The main purpose of WSUS is to centralize control over updates and to provide ability to approve, decline, and target updates to client computers.

2. What are the most important improvements in WSUS 3.0 SP1?

   Answer: Support for new operating systems, ability for installation on Windows Server 2008, new reporting

3. What are the most common scenarios of deploying WSUS?

   Answer: The most common scenario is deploying a single WSUS server for managing client updates in an organization. Also, deploying replica WSUS servers is common for larger organizations with multiple sites.

Common issues related to WSUS

Issue	Troubleshooting tip
WSUS 3.0 SP1 failed to install.	Check prerequisites. Check if the Microsoft .NET Framework is installed and active. Check setup logs.
WSUS fails to synchronize with Microsoft Update.	Check the error in the synchronization's details pane. Check proxy server settings by using the WSUS console. Check the firewall. Verify that users and the network service have Read permissions to the local update storage directory.
Client computers appear in the wrong groups.	Check if the client-side targeting is enabled in Options in the WSUS Administration Console. Verify that the target computer group names match groups on the WSUS server. Reset the Automatic Updates client using: wuauclt.exe /resetauthorization /detectnow

Real-world issues and scenarios

The organization Contoso, Ltd has a single domain on three locations in three different cities. Locations are connected with 1 Mbps links that are 90 percent used during work hours. You want to implement WSUS to manage updates. Internet link is available only at the central location. Also, administrators in the central location want to have control over approved updates in the whole organization.

1. How many WSUS servers will be deployed?

   Answer: Three, one at each location.

2. How will the WSUS hierarchy be deployed?

   Answer: Upstream server will be at the central location, and it will synchronize with the Microsoft Update site. At the other two locations, two replica servers will be deployed as downstream servers that will sync with WSUS at the central location.

3. How will you configure clients to use WSUS?

Answer: You will create three GPOs with appropriate WSUS settings and link it on site level for each site.

Tools

Tool	Use	Where to find it
WsusDBMaintenance script	Allows you to re-index any version of the SUSDB database, either SQL Server 2005 or Windows Internal Database.	http://go.microsoft.com/fwlink/?LinkId=87027

Lab Review Questions and Answers

1. What are the prerequisites for installation of WSUS 3.0 SP1??

   Answer: IIS 7.0 (Web Server role), Microsoft Report Viewer Redistributable 2005, Windows Internal Database (installed during setup), 2 GB of free space for database on the NTFS partition, 20 GB of free space for WSUS Content on NTFS partition.

2. How do you manage WSUS in Windows Server 2008?

   Answer: If WSUS is installed on Windows Server 2008, it appears as a Server role and it is managed using Server Manager.

3. What should the administrator do before updates are deployed to clients?

   Answer: Administrators should test updates on the test computer group in order to discover potential compatibility issues. After that, he should approve updates to target computer groups.

Module 13

Configuring Storage Technologies in Windows Server® 2008

Contents:

Lesson 1

Configuring Distributed File System

Contents:

Question and Answers

What Is DFS?

Question: Which two technologies make up DFS?

Answer: DFS Namespaces and DFS Replication.

Types of DFS Namespaces

Question: How can you prevent users from traversing a slow WAN connection to access a DFS Namespace root?

Answer: Implement a domain-based namespace root that will be replicated to a namespace server located close to the users.

What Are Folders and Folder Targets?

Question: What is the DFS namespace hierarchy?

Answer: A DFS namespace contains one or more folders. Each of these folders may contain one or more folder targets that link to various shared folders or other namespaces.

What Is DFS Replication?

Question: Which two folders can help troubleshoot file replication issues when using DFS Replication?

Answer: The DfsrPrivate\Staging folder and the DfsrPrivate\ConflictandDeleted folder can both be used to troubleshoot file replication issues.

What Are Replication Groups and Replicated Folders?

Question: What are the two types of groups that can be configured for replication?

Answer: Multipurpose and data collection.

Additional Reading

What Is DFS?

For more information on DFS management, see http://go.microsoft.com/fwlink/?LinkId=102243&clcid=0x409.

Generating Diagnostic Reports and Propagation Tests

For more information on how to create a diagnostic report for DFS Replication, see http://go.microsoft.com/fwlink/?LinkID=177454&clcid=0x409.

New Features in Windows Server 2008

- For more information on how to enable access-based enumeration on a namespace, refer to http://go.microsoft.com/fwlink/?LinkID=177455&clcid=0x409.
- For more information on comparing Dfsutil in Windows Server 2003 versus DFSUtil in Windows Server 2008, see http://go.microsoft.com/fwlink/?LinkID=177456&clcid=0x409.
- To see more examples of the functionality of Dfsdiag, see http://go.microsoft.com/fwlink/?LinkID=177561&clcid=0x409.

Lesson 2

Managing Storage with File System Resource Management

Contents:

Question and Answers

What Is Quota Management?

Question: Name and describe the two types of quotas.

Answer: Hard quotas enforce quota limits, and soft quotas are where quota limits are not enforced.

What Is File Screening?

Question: What criteria are used to determine whether a file should be blocked?

Answer: File extensions are used to determine whether a file should be blocked.

What Are Storage Reports?

Question: What report would you run to identify file-group usage patterns and to identify file groups that occupy large amounts of disk space?

Answer: The Files by File Group report will provide that information.

Additional Reading

What Is File Server Resource Manager?

For more information on how to use FSRM, refer to the Windows Server 2008 Step-by-Step Guides, which are available at http://go.microsoft.com/fwlink/?LinkId=113166.

What Are Quota Templates?

For more information on how to create a quota template, see http://go.microsoft.com/fwlink/?LinkID=112088&clcid=0x409.

What Is File Screening?

For more information on file screening management, go to http://go.microsoft.com/fwlink/?LinkID=112090&clcid=0x409.

What Are File Groups and File Screen Exceptions?

For more information on how to define file groups for screening, see http://go.microsoft.com/fwlink/?LinkID=112091&clcid=0x409.

What Is a File Screen Template?

For more information on how to create a file screen template, see: http://go.microsoft.com/fwlink/?LinkID=112093&clcid=0x409.

What Are Storage Reports?

For additional information on storage reports, refer to http://go.microsoft.com/fwlink/?LinkID=112094&clcid=0x409.

What Is a Report Task?

For more information on how to schedule a set of reports, refer to http://go.microsoft.com/fwlink/?LinkID=112095&clcid=0x409.

Lesson 3

Configuring Storage Area Network Connectivity

Contents:

Question and Answers

Differences Between a SAN and a NAS

Question: What communication protocol does a SAN use?

Answer: SCSI or iSCSI

SAN Terminology

Question: What is the function of the LUN?

Answer: The LUN identifies a SCSI logical unit.

Module Reviews and Takeaways

Review questions

1. What happens when two users simultaneously update the same file on different servers?

   Answer: When DFS Replication detects a conflict, it uses the version of the file that was saved last. It moves the other file into the DfsrPrivate\ConflictandDeleted folder.

2. How are initiators and targets identified in an iSCSI network?

   Answer: iSCSI qualified names (IQNs)

3. What is the default format when saving storage reports?

   Answer: DHTML

Common issues related to storage technologies

Identify the causes for the following common issues related to storage technologies and fill in the troubleshooting tips. For answers, refer to relevant lessons in the module.

Issue	Troubleshooting tip
DFS topology becomes disconnected	Use the Disconnected Topology dialog box in the error message to repair the topology.
DFS namespace is not accessible	Ensure that the DFS service is running. Ensure that the NetLogon service is running on all DFS hosts.
Unable to connect to data on the SAN	Verify that the switch can communicate with the server and storage device. Use diagnostic software to test switch connections. Check hardware such as the HBA or driver issues.

Real-world issues and scenarios

1. An organization wants to control the amount of disk space that a particular department is able to use on the file server. They implement quotas for the department shares on the file server.
2. An organization wants to prevent the network itself from becoming a single point of failure. They implement MPIO and invest in the hardware and cabling required to support multiple network paths to the SAN.
3. An organization wants to make software available to multiple branch offices. They set up a DFS and replicate the target folder to the DFS host in the branch offices. This way, the software and upgrades need only be maintained in the head office replica.

Best practices related to storage technologies

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

- Periodically perform a status check on common DFS targets to ensure that the targets are still accessible.
- Due to latency issues, do not create diagnostic reports for more than 50 servers at a time.

Tools

Tool	Use	Where to find it
Dfsdiag	Diagnosing DFS namespace issues	%systemroot%\System32
Dfsutil	Managing DFS Namespaces	%systemroot%\System32
Dirquota.exe	Quota management	%systemroot%\System32
Filescrn.exe	Creating and managing file screens, file-screening exceptions, and file groups	%systemroot%\System32
Storrept.exe	Configuring report parameters and generating storage reports on demand	%systemroot%\System32
Fsutil	Configuring NTFS Quotas and creating files to test quota behavior	%systemroot%\System32

Lab Review Questions and Answers

1. What is the difference between a domain-based DFS namespace and a stand-alone DFS namespace?

   Answer: A domain-based DFS namespace is hosted on multiple servers, whereas a stand-alone DFS namespace is only hosted on a single server. Users will connect to a domain-based namespace by using the domain name in the URL (ex: \\Contoso.com\corpfiles), whereas a user will connect to a stand-alone namespace by using the server name (\\SEA-SRV1\corpfiles)

2. What does the Primary Member configuration do when setting up replication?

   Answer: The Primary Member is used as the authoritative server during the initial replication. After initial replication is complete, the primary member designation is removed.

3. If you want to apply a quota to all subfolders in a folder, including folders that will be created in the future, what option must you configure in the quota policy?

   Answer: The auto quota option must be enabled. This will cause the quota to be applied to folders when they are created.

Module 14

Configuring High Availability in Windows Server® 2008

Contents:

Lesson 1

Configuring Network Load Balancing

Contents:

Question and Answers

Windows Server 2008 NLB Features

Question: Which new feature is most important to your environment?

Answer: Answers may vary; however, the most popular new features are the ability to have multiple network interface cards (NICs) per node, support for IPv6, and the ability to upgrade from Windows Server 2003.

Demonstration: Creating NLB Clusters

Question: What are the prerequisites for creating the NLB cluster?

Answer: You must install the NLB server feature on each computer. If the NLB cluster will support a Web-based application, you must also install and configure IIS and the Web application.

Detailed Demo Steps

Demonstration: Creating NLB Clusters

Preparation steps

1. Start **LON-DC1**, **LON-FS1**, and **LON-FS2**.
2. Log on to **LON-FS1** and **LON-FS2** as **Administrator** with the password **Pa$$w0rd**, and add the Network Load Balancing feature by using Server Manager on both computers.

Create a new NLB cluster

1. On LON-FS1, from the Server Manager console, click **Add Features**, and in the Add Features Wizard, add the Network Load Balancing feature.
2. Open the **Network Load Balancing Manager**, click **Start**, click **Administrative Tools**, and then click **Network Load Balancing Manager**. You can also open the Network Load Balancing Manager by typing **Nlbmgr** at a command prompt.
3. Right-click **Network Load Balancing Clusters**, and then click **New Cluster**.
4. To connect to the host that is to be a part of the new cluster, in the **Host** text box, type the name of the host, **LON-FS1**, and then click **Connect**.
5. Select the interface that you want to use with the cluster, **Local Area Network**, and then click **Next**. (The interface hosts the virtual IP address and receives the client traffic to load balance.)
6. In **Host Parameters**, select a value in **Priority (Unique host identifier)**. This parameter specifies a unique ID for each host. The host with the lowest numerical priority among the current members of the cluster handles all of the cluster's network traffic that is not covered by a port rule. Accept the default value of **1**.
7. You can override these priorities or provide load balancing for specific ranges of ports by specifying rules on the **Port rules** tab of the **Network Load Balancing Properties** dialog box.
8. In **Host Parameters**, you can also add dedicated IP addresses, if necessary.
9. Click **Next** to continue.
10. In **Cluster IP Addresses**, click **Add** and type the cluster IP address that is shared by every host in the cluster. NLB adds this IP address to the TCP/IP stack on the selected interface of all hosts that are chosen to be part of the cluster. Note that NLB does not support Dynamic Host Configuration Protocol (DHCP). NLB disables DHCP on each interface that it configures, so the IP addresses must be static. Click **Add**, and enter **10.10.0.100**, with a subnet mask of **255.255.255.0**, and then click **OK**.
11. Click **Next** to continue.
12. In **Cluster Parameters**, select values in **IP Address and Subnet mask** (for IPv6 addresses, a subnet mask value is not needed). Type the full Internet name that users will use to access this NLB cluster. You can type **contoso-NLB.contoso.com**.
13. In **Cluster operation mode**, click **Unicast** to specify that a unicast Media Access Control (MAC) address should be used for cluster operations. In unicast mode, the MAC address of the cluster is assigned to the network adapter of the computer, and the built-in MAC address of the network adapter is not used. We recommend that you accept the unicast default settings.

14. Click **Next** to continue.
15. In **Port Rules**, click **Edit** to modify the default port rules, if needed.
16. To add more hosts to the cluster, right-click the new cluster, and then click **Add Host to Cluster**. Configure the host parameters (including host priority, dedicated IP addresses, and load weight) for the additional hosts by following the same instructions that you used to configure the initial host. Because you are adding hosts to an already configured cluster, all the cluster-wide parameters remain the same.

Additional Reading

What Is NLB?

- For more information about network load balancing concepts, see http://go.microsoft.com/fwlink/?LinkID=178020&clcid=0x409.
- For more information about the key features of network load balancing, see http://go.microsoft.com/fwlink/?LinkID=178021&clcid=0x409.

Windows Server 2008 NLB Features

For an overview of network load balancing, see http://go.microsoft.com/fwlink/?LinkID=178022&clcid=0x409.

Configuring NLB Options

For more information on selecting the unicast or multicast method of distributing incoming requests, see http://go.microsoft.com/fwlink/?LinkID=178023&clcid=0x409.

Lesson 2

Overview of Windows Server 2008 Failover Clusters

Contents:

Question and Answers

Improvements in Failover Clustering in Windows Server 2008

Question: Why is the validation wizard important?

Answer: The validation wizard, a new feature of Windows Server 2008 failover clustering, provides a way to validate new or existing cluster configurations and prevent any errors or impaired functionality, before the cluster is created.

What Are Clustered Services and Resources?

Question: What is the difference between cluster services and cluster resources?

Answer: A resources is a basic configuration unit in failover clustering. Several resources are contained in one cluster service. A cluster service is a service or application that you want to make highly available.

Failover Clusters and Networks

Question: Why it is recommended to have separate networks for intra-cluster communication and communication with clients?

Answer: Separate networks are recommended because the public network (for communication with clients) can serve as a redundant network in case the private network fails. The recommendation for a separate private network is to eliminate the possible of the eviction of a node in the cluster, or even failure of the cluster due to lost quorum, during peak public network utilization periods due to lost heartbeats.

What Is Quorum?

Question: What is used to prevent problems caused by a split in a cluster?

Answer: Failover clusters use a voting algorithm to determine whether the cluster has enough votes to maintain quorum.

Types of Quorum Modes

Question: What is specific to the No Majority: Disk Only quorum mode?

Answer: In the No Majority: Disk Only mode, the quorum-shared disk can veto all other possible votes. In this mode, the cluster will continue to function as long as the quorum-shared disk and at least one node are available.

Additional Reading

Improvements in Failover Clustering in Windows Server 2008

To see what's new in failover clusters in Windows Server 2008, go to http://go.microsoft.com/fwlink/?LinkID=178024&clcid=0x409.

Failover Clustering Components

For more information about failover clusters, see http://go.microsoft.com/fwlink/?LinkID=178025&clcid=0x409.

What Is Quorum?

For more information on how to configure the quorum in a failover cluster, see http://go.microsoft.com/fwlink/?LinkID=178026&clcid=0x409.

Types of Quorum Modes

For more information on quorum modes, see http://go.microsoft.com/fwlink/?LinkID=178027&clcid=0x409.

Choosing a Quorum Mode

For more information on quorum modes, see http://go.microsoft.com/fwlink/?LinkID=178027&clcid=0x409.

Lesson 3

Preparing for Failover Clustering

Contents:

Question and Answers

Installing Failover Clustering

Question: When you install the failover clustering feature from the command line, what output is produced?

Answer: There is no output when you install the failover clustering feature. Therefore, when the installation is complete, it is important to use the sc command to verify that the failover cluster service is running.

Question: Why must you use the command line to manage a computer with a Server Core installation?

Answer: To reduce the overhead of the operating system, a Server Core installation does not provide a full graphical user interface (GUI). You must complete all tasks from the command line or from a remote server.

Demonstration: Running the Validate A Configuration Wizard

Question: What step is required before you run the Validate A Configuration Wizard?

Answer: You must install the failover clustering feature on each of the nodes in the cluster before you can run the Validate A Configuration Wizard.

Question: What are the benefits of the Validate A Configuration Wizard?

Answer: The Validate A Configuration Wizard helps to verify that the cluster configuration meets best practices, and will function optimally.

Detailed Demo Steps

Demonstration: Running the Validate A Configuration Wizard

Run the Validate A Configuration Wizard

Ensure that the LON-DC1, LON-FS1, LON-FS2, and LON-STR virtual machines are started and running. Log on to LON-FS1 using an Administrator account.

1. On LON-FS1, click **Start**, point to **Administrative Tools**, and then click **Failover Cluster Management**.
2. In the Failover Cluster Management snap-in, in the console tree, make sure **Failover Cluster Management** is selected, and then under **Management**, click **Validate a Configuration**.
3. Click **Next.**
4. In the **Enter Name** field, type **LON-FS1**.
5. Click **Add**.
6. In the **Enter Name** field, type **LON-FS2**.
7. Click **Add**, and then click **Next.**
8. Verify that **Run all tests (recommended)** is selected, and then click **Next.**
9. In the Confirmation window, click **Next**.
10. Wait for the validation tests to finish, and then, in the **Summary** window, click **View Report**.

Additional Reading

Failover Cluster Server Hardware Requirements

For more information on failover clustering requirements, see http://go.microsoft.com/fwlink/?LinkID=178028&clcid=0x409.

Failover Cluster Server Network Requirements

For more information on failover clustering requirements, see http://go.microsoft.com/fwlink/?LinkID=178028&clcid=0x409.

Failover Cluster Software Requirements

For more information on failover clustering requirements, see http://go.microsoft.com/fwlink/?LinkID=178028&clcid=0x409.

Lesson 4

Creating and Configuring Failover Clusters

Contents:

Question and Answers

Demonstration: Creating a Cluster

Question: Is there a reason why you might run the Create A Cluster Wizard from a server that is not part of the cluster?

Answer: Yes. You might run the Create A Cluster Wizard from another server to create Server Core clusters.

Demonstration: Clustering Print Services

Question: What corporate scenarios might benefit from clustering print services?

Answer: Because many corporations rely heavily on printing, it is easy to justify clustering print services. Server failures can cost a company money when employees cannot produce needed documents due to a server outage.

Configuring Cluster Properties

Question: When might it be important to change the quorum mode?

Answer: You might need to change the quorum mode when the number of cluster nodes changes.

Detailed Demo Steps

Demonstration: Creating a Cluster

Preparation steps

1. On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In the Virtual Machines pane, click **6416C-LON-DC1**, and then in the Actions pane, click **Start**.
3. To connect to the virtual machine, click **6416C-LON-DC1**, and then in the Actions pane, click **Connect**.
4. Repeat steps 2 and 3 to start the 6416C-LON-FS1, 6416C-LON-FS2, and 6416C-LON-STR virtual machines.
5. Log on to **LON-STR** as **Administrator** and open the command prompt with administrative privileges. Enter the following at the command prompt, and press ENTER after each command:

   netsh advfirewall firewall add rule name="Microsoft iSCSI Software Target Service-TCP-3260" dir=in action=allow protocol=TCP localport=3260

   netsh advfirewall firewall add rule name="Microsoft iSCSI Software Target Service-TCP-135" dir=in action=allow protocol=TCP localport=135

   netsh advfirewall firewall add rule name="Microsoft iSCSI Software Target Service-UDP-138" dir=in action=allow protocol=UDP localport=138

   netsh advfirewall firewall add rule name="Microsoft iSCSI Software Target Service" dir=in action=allow program="%SystemRoot%\System32\WinTarget.exe" enable=yes

   netsh advfirewall firewall add rule name="Microsoft iSCSI Software Target Service Status Proxy" dir=in action=allow program="%SystemRoot%\System32\WTStatusProxy.exe" enable=yes

Configure the iSCSI target software on LON-FS1

1. Log on to **LON-FS1** as **Administrator** using the password **Pa$$w0rd**.
2. Click **Start**, point to **Administrative Tools**, and then click **iSCSI Initiator**.
3. In the **Microsoft iSCSI** dialog box, click **Yes**.
4. In the second **Microsoft iSCSI** dialog box, click **Yes**.
5. On the **Discovery** tab, click **Add Portal**.
6. In the **IP address or DNS name** field, type **10.10.0.100**, and then click **OK**.
7. On the **Targets** tab, click **Refresh**.
8. Select **iqn.1991-05.com.microsoft:lon-str-lon-fs1-target** in the targets list, and then click **Log on**.
9. Select **Automatically restore this connection when the computer starts**, and then click **OK.**

Configure the iSCSI target software on LON-FS2

1. Log on to **LON-FS2** as **Administrator** using the password **Pa$$w0rd**.
2. Click **Start**, point to **Administrative Tools**, and then click **iSCSI Initiator**.

3. In the **Microsoft iSCSI** dialog box, click **Yes**.
4. In the second **Microsoft iSCSI** dialog box, click **Yes**.
5. On the **Discovery** tab, click **Add Portal**.
6. In the **IP address or DNS name** field, type **10.10.0.100**, and then click **OK**.
7. On the **Targets** tab, click **Refresh**.
8. Select **iqn.1991-05.com.microsoft:lon-str-lon-fs2-target** in the targets list, and then click **Log on**.
9. Select **Automatically restore this connection when the computer restarts**, and then click **Ok**

Configure the shared disks

1. On LON-FS1, open Server Manager.
2. Expand **Storage**, and click **Disk Management**.
3. Right-click **Disk 1**, and then click **Online**.
4. Right-click **Disk 1**, and then click **Initialize disk**. In the **Initialize Disk** dialog box, click **OK**.
5. Right-click the unallocated space beside Disk 1, and then click **New Simple Volume**.
6. On the **Welcome** page, click **Next**.
7. On the **Specify Volume Size** page, click **Next**.
8. On the **Assign Drive Letter or Path** page, click **Next**.
9. On the **Format Partition** page, in the **Volume Label** field, type **Data**. Select the **Perform a quick format** check box, and then click **Next**.
10. Click **Finish**.
11. On LON-FS2, open Server Manager.
12. Expand **Storage**, and then click **Disk Management**.
13. Right-click **Disk Management**, and then click **Refresh**.
14. Right-click **Disk 1**, and then click **Online**.

Validate the failover cluster

1. On LON-FS1, click **Start**, point to **Administrative Tools**, and then click **Failover Cluster Management**.
2. In the Failover Cluster Management action pane, click **Validate a Configuration**.
3. Click **Next**.
4. In the **Enter Name** field, type **LON-FS1**.
5. Click **Add**.
6. In the **Enter Name** field, type **LON-FS2**.
7. Click **Add**, and then click **Next**.
8. Verify that **Run all tests (recommended)** is selected, and then click **Next**.
9. In the Confirmation window, click **Next**.

10. Wait for the validation tests to finish, then, in the Summary window, click **View Report**.
11. Verify that all tests completed successfully.
12. Close Microsoft Internet Explorer®.
13. In the Summary window, click **Finish**.

Use the Create A Cluster Wizard to build a simple failover cluster

1. On LON-FS1, in **Failover Cluster Management,** in the **Management** section of the center pane, select **Create a Cluster**.
2. Read the Before You Begin information.
3. Click **Next**, type **LON-FS1**, and then click **Add**. Type **LON-FS2**, and then click **Add**.
4. Verify the entries, and then click **Next**.
5. In the **Access Point for Administering the Cluster** section, enter **Cluster1** for the cluster name.
6. Under **Address**, type **10.10.0.125** as the IP address, and then click **Next**.
7. In the **Confirmation** dialog box, verify the information, and then click **Next**.
8. On the **Summary** page, click **Finish** to return to the Failover Cluster Management snap-in.

Demonstration: Clustering Print Services

Add the Print Services role

1. On LON-FS1, open Server Manager.
2. Run the **Add Roles Wizard**.
3. Select the **Print Services** role and install it.
4. Repeat these steps on LON-FS2.

Configure the printer disk

1. On LON-FS1, open Server Manager.
2. Expand **Storage**, and then click **Disk Management**.
3. Right-click **Disk 2**, and then click **Online**.
4. Right-click **Disk 2**, and then click **Initialize disk**. In the **Initialize Disk** dialog box, click **OK**.
5. Right-click the unallocated space located beside Disk 2, and then click **New Simple Volume**.
6. On the **Welcome** page, click **Next**.
7. On the **Specify Volume Size** page, click **Next**.
8. On the **Assign Drive Letter or Path** page, click **Next**.
9. On the **Format Partition** page, in the **Volume Label** field, type **Printer1**. Select **Perform a quick format**, and then click **Next**.
10. Click **Finish**.
11. On LON-FS2, open Server Manager.
12. Expand **Storage**, and then click **Disk Management**.

13. Right-click **Disk Management**, and then click **Refresh**.
14. Right-click **Disk 2**, and then click **Online**. If a Disk Management error message appears, click **OK**.
15. Right-click **Disk 2**, and then click **Online**.

Cluster the Print Services role

1. On LON-FS1, click **Start**, click **Administrative Tools**, and then click **Failover Cluster Management**. If the **User Account Control** dialog box appears, confirm that the correct action displays, and then click **Continue**.
2. In the console tree, expand **CLUSTER1.contoso.com**, and then click **Storage**.
3. In the Actions pane, click **Add a disk**, and then click **OK**.
4. Click **Cluster1.contoso.com**, and in the Actions pane, click **Configure a Service or Application**.
5. Review the text on the first page of the wizard, and then click **Next**.
6. Click **Print Server**, and then click **Next**.
7. Type **Lon-Print** for the name and **10.10.0.108** as the IP address in the network specified as 10.10.0.0/16, and then click **Next**.
8. Select **Cluster Disk 2** as the storage volume for the print server, click **Next**, and then click **Next**.
9. After the wizard runs and the **Summary** page appears, you can view a report of the tasks the wizard performed by clicking **View Report**. Review the report, and then close Internet Explorer.
10. Click **Finish**.
11. In the console tree, expand **Services and Applications**, and verify that the clustered print server Lon-Print has been created.

Fail over the Lon-Print clustered service from LON-FS1 to LON-FS2

1. In the console tree, click **Lon-Print**. In the center pane, identify the service's current owner.
2. In the Actions pane, click **Move this service or application to another node**.
3. Click **Move to node *servername***, where ***servername*** is the cluster node that is not the current owner.
4. In the **Please confirm action** dialog box, click **Move Lon-Print to *servername***.
5. Wait for the service to move to the new owner. Then, in the center pane, verify that Lon-Print now shows the new current owner and that all components are online.

Demonstration: Configuring Failover Clusters

Modify the quorum mode of an established failover cluster

1. Log on to **LON-DC1**.
2. Using Windows Explorer, create a shared folder named **FSW** on a C drive. Give Authenticated Users full control permission.
3. Log on to **LON-FS1**.
4. Open the **Failover Clustering Management** console.

5. Right-click the cluster node, select **More Actions**, and then select **Configure Cluster Quorum Settings**. The Configure Cluster Quorum Wizard starts.
6. If this is the first time this wizard has been run in the cluster, the **Before You Begin** page appears. There is an option to hide this page on subsequent uses of the wizard, so the first page to appear might instead be the **Select Quorum Configuration** page. If the **Before You Begin** page is displayed, read the information on that page, and then click **Next** to continue.
7. On the **Select Quorum Configuration** page, select **Node and File Share Majority (for clusters with special configurations)**, and then click **Next**.
8. Enter the Universal Naming Convention (UNC) path to the file share, which is **\\LON-DC1\FSW**. After the **Shared Folder Path** field has been populated with the UNC path to the file share, click **Next**.
9. Permissions to the share are verified. If there are any problems accessing the share, an error message is displayed. If there are no problems accessing the share, the **Confirmation** page appears. Review the configuration changes that are about to be made and, if they are correct, click **Next** to make the changes.
10. After the cluster quorum settings have been changed to use a Node And File Share Majority quorum, the Summary page is displayed. Review the summary information, and then click **Finish** to close the wizard.

Module Reviews and Takeaways

Review questions

1. Which option in a port filtering rule defines which NLB node will respond to a client's second request?

   Answer: The affinity setting in a port filtering rule determines how subsequent requests are handled by the NLB nodes. With single affinity, a single NLB node handles all requests from a single client.

2. You are troubleshooting an eight-host NLB cluster, with four host members configured in multicast mode and four host members configured in unicast mode. Why would the cluster not function properly?

   Answer: The NLB service does not support a mixed unicast and multicast environment. All cluster hosts must be either multicast or unicast; otherwise, the cluster will not function properly.

3. What must you install before you can validate a cluster configuration?

   Answer: You must install the failover clustering feature before you can validate a cluster configuration.

Common issues related to failover clustering

Issue	Troubleshooting tip
When you create a new clustered service or application, a computer object (computer account) for that clustered service or application must be created in the Active Directory domain. This computer object is created by the computer object of the cluster itself. If the computer object of the cluster itself does not have the appropriate permissions, it cannot create or update the computer object for the clustered service or application.	Make sure that user and computer objects have appropriate permissions prior to creating a cluster.
The Cluster service is shutting down because quorum was lost. This could be due to the loss of network connectivity between some or all nodes in the cluster, or a failover of the disk witness.	Run the Validate A Configuration wizard to check your network configuration. If the condition persists, check for hardware or software errors related to the network adapter. Also check for failures in any other network components to which the node is connected, such as hubs, switches, or bridges.
The Cluster service is the essential software component that controls all aspects of failover cluster operation and manages the cluster configuration database. If the Cluster service fails to start on a failover cluster node, the node cannot function as part of the cluster.	Make sure that the Cluster service is running on all nodes.

Real-world issues and scenarios

The Contoso, Ltd company wants to implement a high-availability solution for their messaging system. They are currently using Microsoft Exchange Server 2007 installed on three Windows Server 2008 servers. They want to make Exchange Web services (the Client Access Server role) and Exchange Mailbox servers highly available. For that purpose, they are planning to add two more servers to the existing configuration. They have decided that Cluster Continuous Replication will be used for mailbox servers. You are hired as a consultant to design and implement a high availability solution for the messaging system.

1. Which high availability technology will be used for Exchange Web Services?

   Answer: Because Exchange Web services are based on IIS, Network Load Balancing is the recommended technology to use.

2. Which high availability technology will be used for Exchange Mailbox servers?

   Answer: Failover clustering will be used as the underlying technology for Exchange Cluster Continuous Replication.

3. If you decide to use failover clustering, which quorum settings will you use in this case?

   Answer: You should use Node and File Share Majority.

Best practices related to high availability solutions

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

- Make sure that you have the same hardware on all cluster nodes
- Combine failover clustering with Network Load Balancing (NLB) when you want to provide full redundancy and high availability to Web services that work with databases.
- Make sure you have exactly the same software on all failover clustering or NLB nodes.
- Always run the Validate A Configuration Wizard prior to creating a cluster.

Tools

Tool	Use	Where to find it
Failover Cluster Management Console	Creating and managing clusters	Administrative Tools
NLB Manager Console	Creating and managing NLB clusters	Administrative Tools
Disk Management	Configuring disks presented from the storage system	Server Manager

Lab Review Questions and Answers

1. What information will you need to gather as you plan a failover cluster implementation and choose the quorum mode?

   Answer: You will need to gather information such as:

   - How many applications or services will be deployed on the cluster.
   - Performance requirements and characteristics for each application or service.
   - How many servers must be available to meet the performance requirements.
   - Location of the users who use the failover cluster.
   - The type of storage used for the shared cluster storage.

2. After running the Validate A Configuration Wizard, how can you address the network communication single point of failure?

   Answer: You can address the network communication single point of failure by adding network adapters on a separate network to provide communication redundancy between cluster nodes.

3. In what situations might it be important to allow failback of a clustered application only during a specific time?

   Answer: Setting the failback to a preferred node at a specific time is important when you need to be sure that the failback does not interfere with client connections, backup windows, or other maintenance that a failback would interrupt.

Module 15

Configuring Virtualization in Windows Server® 2008

Contents:

Lesson 1

Overview of Hyper-V

Contents:

Question and Answers

Why Use Virtualization?

Question: Describe scenarios in your organization in which virtualization technologies would provide benefits.

Answer: Answers will vary depending on the specifics of each student's organization. In general, students should demonstrate an understanding of virtualization and the benefits that it brings.

What Is Hyper-V?

Question: What is the main difference between Hyper-V and older virtualization solutions such as Virtual PC?

Answer: Hyper-V runs on top of hardware, on hypervisor Type 1, whereas Virtual PC is a software-based virtualization solution. Machines in Hyper-V can perform much better and have less interference with the host operating system.

Hyper-V Architecture

Question: What is the main difference between parent and child partitions in Hyper-V?

Answer: A parent partition is a partition that is used to host the virtualization stack in support of virtual machine operation. Also, a parent partition is used by administrators to manage and create child partitions.

Hyper-V Versions

Question: What is the limitation of running Hyper-V on a virtualization server?

Answer: There is no support for failover clustering and there is a limitation of 32 GB per virtual machine.

Additional Reading

Hyper-V Versions

To learn more about Hyper-V Server 2008 and to download the product, go to http://go.microsoft.com/fwlink/?LinkID=177994&clcid=0x409.

Lesson 2

Installing Hyper-V

Contents:

Question and Answers

Requirements for Installing Hyper-V

Question: Why do you need an update for Hyper-V before you install it?

Answer: Because Windows Server 2008 RTM does not contain the final version of Hyper-V.

Considerations for Installing Hyper-V

Question: Why does the legacy adapter work even when you do not install a virtual machine driver?

Answer: Because the driver is already available on most operating systems.

Installing Hyper-V on a Server Core Installation

Question: What are the main benefits of running Hyper-V on a Server Core installation? What are the drawbacks?

Answer: A more secure platform, fewer resources used by parent partition, and easier patch management are some of the benefits of using Hyper-V on a Server Core installation. One of the drawbacks is lack of local administration tools.

Remote Management of Servers Running Hyper-V

Question: In which scenario is it necessary to use remote management of the Hyper-V environment?

Answer: You must use remote management if you installed Hyper-V on a Server Core installation or if you want to manage Hyper-V from your desktop machine.

Additional Reading

Requirements for Installing Hyper-V

For information about hardware considerations for Hyper-V, see http://go.microsoft.com/fwlink/?LinkID=177995&clcid=0x409.

Lesson 3

Configuring Hyper-V

Contents:

Question and Answers

Configuring Hyper-V Settings

Question: After Hyper-V is installed, what should you do before creating new virtual machines?

Answer: You should set up Hyper-V settings that control the location of virtual machine files.

Creating and Configuring Virtual Networks in Hyper-V

Question: What is the main difference between a private and an internal virtual network?

Answer: Private virtual networks do not create an adapter on the parent partition. Also, with a private network, the virtual machine cannot communicate with a parent partition.

Creating and Configuring Virtual Hard Disks

Question: In which scenarios is it useful to use differencing disks?

Answer: For testing and development, it is convenient to use differencing disks for creating multiple virtual machines with same base disk.

Considerations for Choosing a Hard Disk Type

Question: In what circumstances would you select a pass-through disk rather than a fixed-size disk?

Answer: When you need high performance on the disk side, a pass-through disk is a better choice.

Managing Hyper-V Snapshots

Question: I've taken multiple snapshots, and now my virtual machine pauses automatically. Hyper-V Manager shows the status as "Paused-Critical." How can I fix this?

Answer: This problem occurs when you have run out of space on the physical storage where the virtual machine snapshot files are stored. Note that this may be on a different drive than where the virtual hard disk is stored.

To fix the problem, create additional space on the drive by deleting unused data. For example, if you do not need to keep some of the snapshots, you can delete the snapshots individually. (Make sure to use Hyper-V Manager to delete the snapshots. Do not delete the .ahvd files directly.) Or, to delete all of the snapshots in one action, export the virtual machine and then import the virtual machine. If you delete snapshots, you must shut down, turn off, or save the state of the virtual machine to delete the snapshots from the physical storage.

Question: I've deleted some snapshots to free up storage space, but the space hasn't been recovered. What can I do?

Answer: Shut down the virtual machine—or, if that action is not available, turn off the virtual machine. Deleted virtual machine files are not removed from the physical storage until the virtual machine is shut down, turned off, or put into a saved state. Depending on the size and number of

snapshots, it may take awhile to delete the snapshot files. Hyper-V Manager displays the progress when deleting the snapshots.

Question: Should snapshots be used as a substitute for backups?

Answer: No, because virtual machine snapshots are not the same as backups created by a Volume Shadow Copy Service (VSS) writer. We do not recommend using virtual machine snapshots as a permanent data or system recovery solution. Even though virtual machine snapshots provide a convenient way to store different points of system state, data, and configuration, there are some inherent risks of unintended data loss if they are not managed appropriately. A backup solution helps provide protection that is not provided by snapshots.

One reason that snapshots are not an acceptable substitute for backups is that they do not protect against problems that may occur on the server running Hyper-V, such as a hardware malfunction on the physical computer or a software-related issue in the management operating system. Another reason is that applications that run in a virtual machine are not aware of the snapshot, and will not be able to adjust appropriately. For example, if you used a virtual machine snapshot to restore an Exchange server, the server would expect the same set of client connections that was present when the snapshot was taken.

Question: What is the difference between snapshots and undo disks in previous version of Microsoft virtualization platforms (such as Virtual PC or Virtual Server)?

Answer: The main difference between an undo disk and a differencing disk is that undo disks apply to all virtual hard disks associated with a virtual machine, and a differencing disk applies to one virtual hard disk only.

Detailed Demo Steps

Demonstration: Creating a Virtual Hard Disk

Create a new virtual hard disk

1. Open Hyper-V Manager. Click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In the Action pane, click **New**, and then click **Hard Disk**.
3. Proceed through the pages of the wizard to customize the virtual hard disk. You can click **Next** to move through each page of the wizard, or you can click the name of a page in the left pane to move directly to that page.
4. After you have finished configuring the virtual hard disk, click **Finish**.

Demonstration: Creating and Configuring Virtual Machines

Create and set up a virtual machine

1. Open Hyper-V Manager. Click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. From the Actions pane, click **New**, and then click **Virtual Machine**.
3. From the **New Virtual Machine Wizard**, click **Next**.
4. On the **Specify Name and Location** page, specify what you want to name the virtual machine and where you want to store it.
5. On the **Memory** page, specify enough memory to run the guest operating system you want to use on the virtual machine.
6. On the **Networking** page, connect the network adapter to an existing virtual network if you want to establish network connectivity at this point.

   Note: If you want to use a remote image server to install an operating system on your test virtual machine, select the external network.
7. On the **Connect Virtual Hard Disk** page, specify a name, location, and size to create a virtual hard disk so you can install an operating system on it.
8. On the **Installation Options** page, choose the method you want to use to install the operating system:
   - Install an operating system from a boot CD/DVD-ROM. You can use either physical media or an image file (.iso file).
   - Install an operating system from a boot floppy disk.
   - Install an operating system from a network-based installation server. To use this option, you must configure the virtual machine with a network adapter connected to the same network as the image server.
9. Click **Finish**.

Configure a virtual machine

1. Open Hyper-V Manager. Click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In the Results pane, under **Virtual Machines**, select the virtual machine that you want to configure.
3. In the Action pane, under the virtual machine name, click **Settings**.
4. In the navigation pane (left pane), click the item you want to configure.
5. Do one of the following:
    - To add another instance of an item, such as a SCSI controller, select the item, and then click **Add**. Some items, such as network adapters, may require additional configuration after you add them.
    - To modify an item, make your changes to the configuration and then click **OK**.
    - To remove an item, select it if necessary, and then click **Remove**.
6. To make more changes, click the next item that you want to configure, and repeat step 5. When you are finished with the configuration, click **OK**.

Additional Reading

Virtual Machine Integration Services

For more information on version compatibility for integration services, see
http://go.microsoft.com/fwlink/?LinkID=177997&clcid=0x409

Lesson 4

High Availability in a Hyper-V Environment

Contents:

Question and Answers

Why Make Virtual Machines Highly Available?

Question: What is the main reason for thinking about high availability in the context of virtualization in production?

Answer: Virtualization, when used for server consolidation, can present a great risk from a single point of failure if no high availability solution is deployed.

Supported Types of High Availability in Hyper-V

Question: When should you choose guest clustering over host clustering?

Answer: If you have a cluster-aware application that is hosted within the virtual machine, guest clustering is the better choice.

Requirements for Hyper-V Clustering

Question: What is the most important requirement when deploying Hyper-V in failover clustering?

Answer: You must have a storage device that is shared between Hyper-V nodes.

Virtual Machine Backup

Question: Describe some considerations for deciding whether to back up the contents of a virtual machine or the entire virtual machine.

Answer: Some important considerations include: disk space availability for backups, backup and recovery windows, time available to reconfigure a virtual machine after recovery, and application/service fragility (for example, in a domain with multiple domain controllers, it might be easier to re-create a failed domain controller by using a virtual machine template than to attempt to restore a failed domain controller).

Additional Reading

Why Make Virtual Machines Highly Available?

For more information about high availability for Hyper-V, see http://go.microsoft.com/fwlink/?LinkID=177998&clcid=0x409.

Supported Types of High Availability in Hyper-V

For more information on high availability for Hyper-V, see http://go.microsoft.com/fwlink/?LinkID=177998&clcid=0x409.

Module Reviews and Takeaways

Review questions

1. What are the main architectural changes in Hyper-V compared to Virtual PC or Virtual Server?

   Answer: Virtual Server and Virtual PC are considered Type 2 hypervisors because all virtual machine requests are still routed through the underlying Windows operating system. Type 1 hypervisors, such as Hyper-V, run directly on the hardware with no underlying operating system.

2. List the mandatory requirements for installation of the Hyper-V role.

   Answer: Requirements are an x64 processor, the enabling of DEP, support for hardware virtualization, and a 64-bit version of Windows Server 2008.

3. What types of high availability are supported in the Hyper-V environment?

   Answer: Host clustering and guest clustering are supported.

Common issues related to Hyper-V

Issue	Troubleshooting tip
When the user tries to control a virtual machine, he cannot use the mouse. He is using Remote Desktop Connection to connect to a server running Hyper-V.	The use of a virtual machine connection within a Remote Desktop Connection session is not supported until integration services are installed. Install integration services.
The Hyper-V role is installed and the user can create or import a virtual machine, but the virtual machine can't be started.	The hypervisor is not running. Check to make sure the hardware requirements are fulfilled.
The user cannot perform a network-based installation of a guest operating system.	The virtual machine is using a network adapter instead of a legacy network adapter, or the legacy network adapter is not connected to an appropriate external network. Ensure that the virtual machine is configured with a legacy network adapter that is connected to an external network that offers installation services.

Real-world issues and scenarios

A large company wants to consolidate its server workloads and the number of servers. Currently they have 20 servers, most of which are underutilized. On average, servers are used 40 percent of the time, except for two clustered Microsoft Exchange Server 2007 mailbox servers, which host 2000 users' mailboxes. The company has decided to implement a Hyper-V solution, and now they are making a plan of implementation. You are engaged as a consultant.

1. Which servers will you recommend to virtualize?

   Answer: It is recommended to virtualize all servers except the clustered mailbox servers.

2. Which server you will not virtualize?

   Answer: The Exchange 2007 mailbox servers should not be virtualized.

3. What kind of hardware will you use for the virtualization host?

   Answer: Use hardware that has the "Certified for Windows" logo.

4. What will you propose regarding high availability and backup?

   Answer: Propose host clustering with quick migration as a high availability solution, and VSS backup of VHD files for backup.

Best practices related to Hyper-V

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

- Avoid overloading the server.
- Ensure high-speed access to storage.
- Avoid mixing virtual machines that can and cannot use integration services.
- Configure anti-virus software to bypass Hyper-V processes and directories.
- Avoid storing system files on drives used for Hyper-V storage.
- Monitor performance to optimize and manage server loading.

Tools

Tool	Use	Where to find it
Remote Server Administration Tools	Managing Hyper-V on Server Core	http://go.microsoft.com/fwlink/?LinkID=178000&clcid=0x409

Lab Review Questions and Answers

1. What are snapshots?

   Answer: Virtual machine snapshots capture the state, data, and hardware configuration of a running virtual machine. Snapshots provide a fast and easy way to revert the virtual machine to a previous state

2. What different types of virtual hard disks does Hyper-V support?

   Answer: Dynamically expanding disks, Differencing disks, Fixed size disks, pass-through disks.

3. What are the integration services and why should they be installed?

   Answer: Integration services are special components that Hyper-V provides to guest operating systems. These services provide additional integration capabilities to operating systems that have been made aware of the fact they are running within a virtual environment.

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

- Volume Activation Deployment Guide
- System requirements
- Windows Vista Deployment Step by Step Guide
- Windows Firewall
- Windows Server 2008 Server Manager Technical Overview
- Roles, role services, and features
- Windows BitLocker Drive Encryption Step-by-Step Guide
- Server Core Installation Option Getting Started Guide
- Server Core Installation Option
- Windows Deployment Services Getting Started Guide
- Deploying earlier versions of Windows
- Managing answer files
- How configuration passes work
- Windows Vista Deployment Step-by-Step Guide
- Windows PE 2.0 for Windows Vista
- Creating custom install images
- Windows Deployment Services multicast servers
- Wdsutil
- Event Viewer
- Property details
- Wevtutil parameters
- Custom views, event subscriptions
- Auditing Step-by-Step Guide
- Auditpol
- Windows Reliability and Performance Monitor
- Monitoring Active Directory
- Windows Vista Performance and Reliability Monitoring Step-by-Step Guide
- Data Collector Sets
- Restartable AD DS
- Database Mounting Tool
- Using SCW on Windows Server 2008
- Backup and Recovery
- AD database mounting tool

- Active Directory Certificate Services Role
- Defining CA Types and Roles
- Install an enterprise root certification authority
- Install a stand-alone root certification authority
- Install an enterprise subordinate certification authority
- Install a stand-alone subordinate certification authority
- Certificate Templates Overview
- Administering Certificate Templates
- Advanced Certificate Enrollment and Management
- Restricted Enrollment Agent
- OCSP Support
- AD RMS Deployment Components
- AD RMS
- Connection Point Registration
- Template Distribution
- Choosing a type of WSUS deployment
- Using the WSUS 3.0 Configuration Wizard
- Managing updates
- Reports in Windows Server Update Services 3.0
- Backing Up Windows Server Update Services 3.0
- Best Practices
- Configuring Automatic Updates
- Network Load Balancing Concepts
- Network Load Balancing key features
- Overview of Network Load Balancing
- Selecting the Unicast or Multicast Method
- What's new
- Overview of Network Load Balancing
- Configuring the Quorum
- Quorum Modes
- Failover Cluster Requirements
- SPC-3 standard
- Summary of New or Expanded Group Policy Settings
- What does DFSDiag do?

- Service Connection Points (SCPs) and ADAM/AD LDS
- Understanding the AD LDS Schema
- ADAM Security
- Understanding AD LDS Replication and Configuration Sets
- Adamsync
- Adamsync Configuration File XML Reference
- ADSchemaAnalyzer
- "Hardware Considerations"
- Version Compatibility for Integration Services
- Achieving High Availability for Hyper-V
- Network Access Protection
- Create a Diagnostic Report for DFS Replication
- Enable Access-Based Enumeration on a Namespace
- DFSUtil in Windows Server 2003 VS DFSUtil in Windows Server 2008
- What does DFSDiag do?
- Storage Technology
- Understanding Domain and Forest Functionality
- Create Installation Media by Using Ntdsutil
- Read-only Domain Controllers Step-by-Step Guide
- Prepare Your Infrastructure for Upgrade
- Appendix of Unattended Installation Parameters
- Password Replication Policy Administration
- Reset the current credentials that are cached on an RODC if it is stolen
- AD DS: Fine-Grained Password Policies
- AD DS: Fine-Grained Password Policies
- Appendix A: Fine-Grained Password and Account Lockout Policy Review
- Active Directory Domain Services (AD DS) Fine-Grained Password and Account Lockout Policy Step-by-Step Guide
- Managing Group Policy ADMX Files Step-by-Step Guide
- Step-by-Step Guide to Managing Multiple Local Group Policy Objects
- Security Settings
- What's New in Group Policy in Windows Server 2008 R2 and Windows 7
- Web SSO Example
- Federated Web SSO Example

- Federated Web SSO with Forest Trust Example
- Identify the Type of Federated Application to Deploy
- Installing a New Windows Server 2008 Domain Tree by Using the Windows
- Configuring DNS client settings
- Active Directory Replication Considerations
- RODC Features
- Administering DNS Server
- Create a PSO
- What's New in AD DS: Active Directory PowerShell
- What's New in AD DS: Active Directory Web Services
- Group Policy Preferences
- Appendix B: PSO Attribute Constraints
- WinRM Service
- WinRM (Windows Remote Management) Troubleshooting
- Cryptography Next Generation
- Automated propagation through default job in Vista SP1
- Microsoft Hyper-V Server License Terms

MSDN

This section includes content from MSDN for this course.

- kernel-mode code signing policy
- Installation and configuration for Windows Remote Management

Communities

This section includes content from Communities for this course.

- Differences between editions
- Product information
- Comparison of the editions by technical specifications
- Digital signatures for kernel modules on systems
- Windows Automated Installation Kit (WAIK) User's Guide for Windows Vista
- Server Management in Windows Server 2008
- Redirecting the users and computers containers in Active Directory domains
- "Group Policy Preferences Overview"
- Location of ADM (Administrative Template) Files in Windows
- How to create a Central Store for Group Policy Administrative Templates in Window Vista
- How to use unattended mode to install and remove Active Directory Domain Services on Windows Server 2008-based domain controllers
- Simple SAN
- How to back up Hyper-V virtual machines from the parent partition on a Windows Server 2008-based computer by using Windows Server Backup
- Microsoft Remote Server Administration Tools for Windows Vista
- Quick Migration with Hyper-V: White Paper
- Microsoft® Hyper-V™ Server 2008 R2
- Microsoft Remote Server Administration Tools for Windows Vista
- Hyper-V Server 2008 R2
- Starter Group Policy Objects (GPOs)
- Installation package: Windows Server Update Services 3.0 Management Pack for Microsoft Operations Manager 2005
- Installation package: Microsoft Report Viewer Redistributable 2005 SP1 (Full Installation)
- White Paper: Windows Update Explained
- Active Directory Certificate Services Longhorn Beta3 Key Archival and Recovery Whitepaper: Installation & Configuration
- Key Archival and Recovery White Paper
- Certificate Templates in Windows Server 2008 implementation and administration
- Restore deleted user accounts and their group memberships
- Internal format of a Windows Imaging file format
- Windows Media Services 2008 for Windows Server 2008
- BitLocker Drive Preparation Tool
- Comparison of server roles
- Windows Server 2008 Security Guide
- PowerShell Management Library for Hyper-V
- Hyper-V Hosting Guidance: Using and Licensing Microsoft® Server Products in Hyper-V Virtual Hosting Scenarios

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.
