Microsoft

OFFICIAL MICROSOFT LEARNING PRODUCT

6416D

Updating Your Windows Server® 2003 Technology Skills to Windows Server® 2008

Companion Content

Product Number: 6416D

Released: 10/2011

MICROSOFT LICENSE TERMS

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

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

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

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

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

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

1. **OVERVIEW.**

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

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

2. **INSTALLATION AND USE RIGHTS.**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Form of Notice:

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

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

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

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

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

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

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

iii. Distribution Restrictions. You may not

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

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

12. **ACADEMIC EDITION.** You must be a "Qualified Educational User" to use licensed content marked as "Academic Edition" or "AE." If you do not know whether you are a Qualified Educational User, visit www.microsoft.com/education or contact the Microsoft affiliate serving your country.
13. **ENTIRE AGREEMENT.** This agreement, and the terms for supplements, updates, Internet-based services and support services that you use, are the entire agreement for the licensed content and support services.
14. **APPLICABLE LAW.**
    a. **United States.** If you acquired the licensed content in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.
    b. **Outside the United States.** If you acquired the licensed content in any other country, the laws of that country apply.
15. **LEGAL EFFECT.** This agreement describes certain legal rights. You may have other rights under the laws of your country. You may also have rights with respect to the party from whom you acquired the licensed content. This agreement does not change your rights under the laws of your country if the laws of your country do not permit it to do so.
16. **DISCLAIMER OF WARRANTY. THE LICENSED CONTENT IS LICENSED "AS-IS." YOU BEAR THE RISK OF USING IT. MICROSOFT GIVES NO EXPRESS WARRANTIES, GUARANTEES OR CONDITIONS. YOU MAY HAVE ADDITIONAL CONSUMER RIGHTS UNDER YOUR LOCAL LAWS WHICH THIS AGREEMENT CANNOT CHANGE. TO THE EXTENT PERMITTED UNDER YOUR LOCAL LAWS, MICROSOFT EXCLUDES THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.**
17. **LIMITATION ON AND EXCLUSION OF REMEDIES AND DAMAGES. YOU CAN RECOVER FROM MICROSOFT AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO U.S. $5.00. YOU CANNOT RECOVER ANY OTHER DAMAGES, INCLUDING CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT OR INCIDENTAL DAMAGES.**

    This limitation applies to

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

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

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

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

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

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

Cette limitation concerne:

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

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

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

Module 1

Installing and Configuring Windows Server 2008

Contents:

Lesson 3: Managing Server Roles and Features **8**

Lesson 4: Configuring and Managing Windows Server 2008 Server Core **11**

Lesson 5: Choosing a Deployment Technology **16**

Lesson 6: Deploying Windows Server 2008 **18**

Module Reviews and Takeaways **21**

Lab Review Questions and Answers **23**

Lesson 3

Managing Server Roles and Features

Contents:

Question and Answers 9

Additional Reading 10

Question and Answers

What Are Server Roles?

Question: How do server roles and role-based configuration make it easier to configure functionality on a Windows Server 2008 server? Are there ways that role-based configuration makes configuration more difficult?

Answer: Role based configuration allows the operating system to enable and configure individual components based on the role you select, rather than forcing you to configure those components individually. One aspect that some admins may find challenging with role-based configuration is determining the role to which a specific component belongs if they require only the individual component enabled.

Additional Reading

Infrastructure and Application Services Roles

- Windows Server 2008 R2 Edition Comparison by Server Role

Lesson 4

Configuring and Managing Windows Server 2008 Server Core

Contents:

Question and Answers 12

Detailed Demonstration Steps 13

Question and Answers

When to Choose Server Core

Question: In which situations would you use a Server Core installation, instead of a full installation of Windows Server 2008?

Answer: Answers will vary, but situations like remote branches, single role servers, or locations where the physical security of the server may be compromised are ideal for Server Core installations.

Detailed Demonstration Steps

Demonstration: How to Configure Post-Installation Settings on Server Core

Detailed demonstration steps

Note You require 6416D-NYC-DC1 and 6416D-NYC-CORE virtual machines to complete this demonstration. Log on to NYC-DC1 as **Contoso\Administrator,** with the password, **Pa$$w0rd**.Log on to NYC-CORE as **Administrator**, with the password, **Pa$$w0rd.**

▶ Task 1: Configure network settings.

1. On NYC-CORE, at the command prompt, type the following command, and then press Enter.

```
netsh interface ipv4 show interfaces
```

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

```
netsh interface ipv4 set address name="Local Area Connection" source=static
address=10.10.10.30 mask=255.255.0.0 gateway=10.10.10.1
```

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

```
netsh interface ipv4 add dnsserver name="Local Area Connection" address=10.10.0.10
index=1
```

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

```
Ipconfig /all
```

5. Verify the configuration.

▶ Task 2: Change the computer name.

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

```
Netdom renamecomputer %computername% /NewName:NYC-SVR-CORE
```

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

```
Y
```

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

```
Shutdown /r
```

4. Log on by using the following credentials:
   - User name: Administrator
   - Password: Pa$$w0rd

▶ Task 3: Add the computer to the Contoso.com domain.

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

```
netdom join %computername% /domain:Contoso.com /userd:Administrator /passwordD:Pa$$w0rd
```

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

```
Shutdown /r
```

3. Log on by using the following credentials:
   - User name: Administrator
   - Password: Pa$$w0rd
   - Domain: Contoso

▶ Task 4: Enable remote desktop.

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

```
sconfig
```

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

```
7
```

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

```
E
```

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

```
2
```

5. In the Remote Desktop dialog box, click OK.

▶ Task 5: Configure remote management.

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

```
4
```

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

```
2
```

3. In the Restart dialog box, click Yes.
4. Log on by using the following credentials:
   - User name: Administrator
   - Password: Pa$$w0rd
   - Domain: Contoso
5. At the command prompt, type the following command, and then press Enter.

```
sconfig
```

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

```
4
```

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

```
3
```

8. In the Enabled dialog box, click OK.
9. At the command prompt, type the following command, and then press Enter.

```
1
```

10. In the Enabled dialog box, click OK.
11. At the command prompt, type the following command, and then press Enter.

```
5
```

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

```
13
```

▶ Task 6: Verify remote management functionality.

1. Switch to the NYC-DC1 domain controller.
2. Click Start, point to Administrative Tools, and then click Server Manager.
3. In Server Manager, in the navigation pane, right-click Server Manager (NYC-DC1), and then click Connect to Another Computer.
4. In the Connect to Another Computer dialog box, in the Another computer box, type NYC-SVR-CORE, and then click OK.
5. Verify that you have connected to NYC-SVR-CORE and then close all windows.

 **Note** Revert all virtual machines.

Lesson 5

Choosing a Deployment Technology

Contents:

Question and Answers 17

Question and Answers

Image-Based Deployment

Question: Considering your choices for image deployment, how would you implement imaging within your organization?

Answer: Answers will vary, depending upon the students' organizations' requirements.

Lesson 6

Deploying Windows Server 2008

Contents:

Question and Answers 19

Question and Answers

High-Touch Retail Media Deployments

Question: What do you see as the key limitations in the preceding deployment method?

Answer: Answers will vary, but might include the following:

- IT professionals are required to initiate interactive installations.
- USB memory sticks with individual answer files are inefficient.
- Multiple copies of the retail media are required.
- The method does not scale well, but suits small, one-off deployments.

High-Touch Standard Image Deployments

Question: How does this deployment method address your comments regarding the high-touch retail media deployment method?

Answer: Although you still need a technician to initiate the installation, you do not require multiple copies of the retail media. The solution still does not scale well because of the interaction required.

Discussion: Choosing a Deployment Topology

Question: How would you use Windows Deployment Services to aid deployment?

Answer: Answers may vary, but important points to consider are:

- Use answer files to automate the image selection process during deployment.
- Use answer files to automate the responses during setup, including domain-joining.
- Create a custom image.
- Capture the image and upload to Windows Deployment Services.
- Distribute the image to the servers across the network.

Question: Which elements in your current infrastructure support Lite-Touch Installations?

Answer: LTI requires minimal infrastructure. In this scenario, you already have the required infrastructure to deploy Windows Server 2008 R2 by using LTI, in terms of file servers and a managed network. In addition, your corporate head office has already prepared a standardized image, so you do not need to create a custom image of Windows Server 2008 R2. You only need to focus on how to deploy this image efficiently and effectively.

Question: Which deployment method would you choose for the three offices?

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

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

the deployment process and install Windows Server 2008 R2 to the server computers in the London office.

Module Reviews and Takeaways

Review questions

Question: From which version of Windows Server can you upgrade to Windows Server 2008 R2 Enterprise Server Core?

Answer: Server Core installation of Windows Server 2008 Standard with or without SP2 or Server Core installation of Windows Server 2008 Enterprise with or without SP2.

Question: Which new program is provided to enable simpler post-installation configuration of Server Core?

Answer: Sconfig.cmd makes post-installation configuration of Server Core easier

Question: Which command can be used on all editions of Windows Server 2008 R2, both Server Core and Full, to install additional server roles from the command line?

Answer: Dism.exe.

Question: How is Windows AIK useful with Windows Deployment Services deployments?

Answer: Windows AIK provides tools such as ImageX.exe, Sysprep.exe, and Windows SIM that enable you to manage images for use by Windows Deployment Services. For example, you can use Windows SIM to create and configure answer files to automate Windows Deployment Services deployments; you can use Sysprep to generalize a capture image for Windows Deployment Services; additionally, Windows AIK provides a number of Windows PE images and management tools.

Question: Which management tool would you recommend for a new junior administrator who has been asked to manage a Server Core installation of Windows Server 2008 R2?

Answer: The most likely solution would be to use Server Manager remotely to manage the server. While Server Manager does not have the flexibility and power of managing the server by using the local command line or remotely by using PowerShell, it does allow the junior administrator to view the general structure of the server and use a familiar, graphical management tool until he or she is ready or required to move on to more robust tools like PowerShell.

Tools

Tool	Use for	Where to find it
Windows AIK	• Managing image files • Configuring answer files	Download from Microsoft website
WDSUtil.exe	• Command-line management of Windows Deployment Services	Part of Windows Deployment Services
Dism.exe	• Offline and online servicing of images	Part of Windows AIK
Netsh.exe	• Command-line tool for managing network-related settings	Part of Windows Server

Tool	Use for	Where to find it
Ocsetup.exe	• Adding and removing Server Core roles and features	• Command-line
Sconfig.exe	• Managing a Server Core installation of Windows Server 2008 (R2 only)	• Type Sconfig.exe at the command line
Microsoft Assessment and Planning(MAP) Toolkit	• Simplifying and streamlining the IT infrastructure planning by assessing existing environments	• http://go.microsoft.com/fwlink/?LinkID=228324
Server Manager	• Managing a Windows Server 2008 server	• Start Menu

Lab Review Questions and Answers

Question: In the lab, you configured the domain membership of the server by using netdom. Which additional command could you have used

Answer: Sconfig.cmd enables you to change domain/workgroup membership.

Question: What is the importance of enabling remote MMC management of Server Core servers

Answer: The Server Core provides a command prompt interface, which is suitable for many administrative tasks; sometimes, however, it is quicker and easier to perform management by using a graphical interface. This can be achieved on Server Core by enabling remote MMC management and connecting from another full server installation to perform management.

Question: In the lab, you used Dism.exe to install roles. Which other command could you use on server core?

Answer: You could also use **start /w ocsetup** to install roles on server core.

Question: Which command-line tools can you use to install roles on full installations of Windows Server 2008 R2?

Answer: Dism.exe works on full installations.

Question: In the lab, the DHCP server and Windows Deployment Services server roles were co-hosted on one server. What issues did this present?

Answer: Both services listen on UDP port 67. You must configure Windows Deployment Services to not do so by configuring options in the initial configuration wizard.

Question: In the lab, you created a capture image. How is this used?

Answer: You can use a capture image to boot a reference computer, capture its installed operating system, and then upload it back to Windows Deployment Services.

Module 2

Server Management in Windows Server 2008

Contents:

Lesson 1: Managing Windows Server with Server Manager **25**

Lesson 2: Managing Server Updates by Using WSUS **27**

Lesson 3: Managing Backup and Restore by Using Windows Server Backup **32**

Lesson 5: Performance and Resource Management **36**

Module Reviews and Takeaways **38**

Lab Review Questions and Answers **40**

Lesson 1

Managing Windows Server with Server Manager

Contents:

Detailed Demonstration Steps 26

Detailed Demonstration Steps

Demonstration: Using Server Manager

Detailed demonstration steps

Note You require the 6416D-NYC-DC1 virtual machine to complete this demonstration. Log on to the virtual machine as **Contoso\Administrator** with the password **Pa$$w0rd**.

1. On **NYC-DC1**, log on as **Contoso\Administrator** with the password **Pa$$w0rd**.
2. Run **Server Manager** from the task bar.
3. Expand all nodes in the left pane and show the available options and tools that can be run from Server Manager.
4. In left pane, click **Server Manager (NYC-DC1)**, and then in right pane, in the **Security Information** section, click **Configure IE ESC**. Show how can you configure this feature separately for Administrators and Users. Click **OK**.
5. At the lower part of the Server Manager console, click **Configure refresh**. Show how can you configure refresh interval for status of server roles. Click **OK**.
6. In the left pane, expand **Roles** (if they are not already expanded) and click **Active Directory Domain Services**.
7. In the right pane, show the filtered Event log for the AD DS role and services that are related to that role.
8. Run the **Best Practices Analyzer for Active Directory Domain Services** role and show results that it produces.
9. Close the **Server Manager** console.

Lesson 2

Managing Server Updates by Using WSUS

Contents:

Question and Answers 28

Detailed Demonstration Steps 29

Additional Reading 31

Question and Answers

Deploying Updates with WSUS

Question: What is the update approval process at your organization?

Answer: Many organizations do not have an approval process, though one or two students in each class have complicated and involved approval processes. Ask if anyone has to sign off on updates or if it is up to administrator discretion.

Question: What types of updates would you consider approving automatically?

Answer: Anti-malware definitions are one type of update where there is little risk in automatic approval.

Question: When was the last time you deployed an update that caused a problem with an existing configuration?

Answer: This will depend on the organization. Depending on the experience of the group, you may have students that have never experienced problems with the deployment of updates.

Detailed Demonstration Steps

Demonstration: Managing WSUS Groups in WSUS Management Console

Detailed demonstration steps

Note You require the 6416D-NYC-DC1 and 6416D-NYC-SVR1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password **Pa$$w0rd**.

1. Switch to NYC-SVR1 and open the Windows Server Update Services console from the **Administrative Tools** menu.
2. Expand the **NYC-SVR1\Computers** node and click **All Computers**.
3. On the **Action** menu, click **Add Computer Group**.
4. In the **Add Computer Group** dialog box, in the **Name** field, type **Update_Testing**, and then click **Add**.
5. Ensure that the **NYC-SVR1\Computers** node is still selected. On the **Action** menu, click **Add Computer Group**.
6. In the **Add Computer Group** dialog box, in the **Name** field, type **Australia** and click **Add**.
7. Expand **All Computers**, and then click the **Australia** computer group. In the **Actions** pane, click **Add Computer Group**.
8. In the **Add Computer Group** dialog box, in the **Name** field, type **Melbourne_Sales** and then click **Add**.
9. Repeat steps 7 and 8 and create the computer group **Melbourne_Marketing**.
10. Switch to NYC-DC1.
11. From the **Administrative Tools** menu, open the **Group Policy Management** console.
12. Navigate to the **Forest: Contoso.com\Domains\Contoso.com\Group Policy Objects** node.
13. From the **Action** menu, click **New**. In the **New GPO** dialog box, enter the name **WSUS_Policy** and then click **OK**.
14. Right-click **WSUS_Policy** and then click **Edit**.
15. Navigate to the **Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update** node and then double-click **Enable client-side targeting**.
16. In the **Enable client-side targeting** policy, set the policy to **Enabled** and set the **Target group name for this computer** to **Melbourne_Marketing**. Click **OK**.

Demonstration: Configuring Automatic Approval Rule

Detailed demonstration steps

Note You require the 6416D-NYC-DC1 and 6416D-NYC-SVR1 virtual machines to complete this demonstration. Log on to the virtual machines as Contoso\Administrator with

the password of Pa$$word.

This demonstration assumes that you have created the computer groups Update_Testing, Australia, Melbourne_Marketing and Melbourne_Sales during the previous demonstration.

1. On **NYC-SVR1**, open the Windows Server Update Services console from the **Administrative Tools** menu.
2. Click the **Options** node and then click **Automatic Approvals**.
3. Review the properties of the Default Automatic Approval Rule.
4. Click **New Rule**. In the **Add Rule** dialog box, select the **When an update is in a specific classification**, **When an update is in a specific product**, and **Set a deadline for the approval** check boxes.
5. Click the underlined **all computers** text and then ensure that only the **Update_Testing** group is selected. Click **OK**.
6. Click **7 days after the approval at 3:00am text**. In the **Choose Deadline** dialog box, change the update approval deadline to **1** day and then click **OK**.
7. In the **Specify a name** box, type **Automatic_To_Test_Computers** and then click **OK**.
8. Click New Rule. In the Add Rule dialog box select the When an update is in a specific classification, When an update is in a specific product, and Set a deadline for the approval checkboxes.
9. Click the underlined **any classification** text and then ensure that only **Critical Updates** and **Security Updates** are selected and click OK.
10. Click 7 days after the approval at 3:00am text. In the Choose Deadline dialog, change the update approval deadline to 10 days and then click OK.
11. Click the underlined **all computers** text and ensure that only the Melbourne_Marketing group is selected and click OK.
12. In the **Specify a name** text box, enter **Melbourne_Marketing_Security_Critical** and then click OK.
13. Click the Advanced tab. Discuss the following settings:
    - Automatically Approve Updates To The WSUS Product Itself
    - Automatically Approve New Revisions Of Updates That Area Already Approved
    - Automatically Decline Updates When A New Revision Causes Them To Expire

Additional Reading

WSUS Reporting

- Reports in Windows Server Update Services 3.0

Lesson 3

Managing Backup and Restore by Using Windows Server Backup

Contents:

Detailed Demonstration Steps 33

Additional Reading 35

Detailed Demonstration Steps

Demonstration: Overview of the Windows Server Backup Features

Detailed demonstration steps

Note You require the 6416D-NYC-DC1 and 6416D-NYC-SVR1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$word**.

Use the backup wizard to schedule a backup

1. On NYC-DC1, click **Start**, click **Administrative Tools**, and then click **Windows Server Backup**. Point out the elements of the MMC such as **Status** and **Actions**.
2. In the **Actions** pane, click **Backup Schedule**.
3. In the **Backup Schedule Wizard**, click **Next.**
4. On the **Select Backup Configuration** page, click **Custom**, and then click **Next**.
5. On the **Select Items for Backup** page, click **Add Items**. Point out and describe the available items.
6. Select the checkbox for **C:** and click **OK**.
7. Click **Advanced Settings.**
8. In the **Advanced Settings** dialog box, click **Add Exclusion.**
9. Ensure that drive C is selected and click **OK.**
10. Click into the **File Type** field and type **.TMP.**
11. Click **Add Exclusion.**
12. Expand **C:** drive and click **pagefile.sys** and click **OK.**
13. In the **Advanced Settings** dialog box, click **OK**.
14. Click **Next**.
15. On the **Specify Backup Time** page, click the drop-down arrow and select **1:00 AM** as the time of day and click **Next**.
16. On the Specify Destination Type page, click the **Back up to a shared network folder** and click **Next**. In the **Windows Server Backup** dialog box, click **OK**.
17. In the location field, type **\\NYC-SVR1\backup** and click **Next.**
18. In the **Register Backup Schedule** dialog box, type **Contoso\Administrator.**
19. In the password field, type **Pa$$w0rd** and click **OK**.
20. Click **Finish** and then click **Close**. Note that to modify the scheduled backup settings, you must run the wizard again.

Use the backup wizard to back up a folder.

1. In the Actions pane click **Backup Once**.

2. On the Backup Options page click **Different options** and click **Next**.
3. On the Select Backup Configuration page click **Custom** and click **Next**.
4. On the Select Items for Backup page click **Add Items**.
5. Expand drive C, select the **MarketingTemplates** check box, click **OK**, and then click **Next**.
6. On the **Specify Destination Type** page click **Remote shared folder** and click **Next**.
7. On the **Specify Remote Folder** page, type **\\NYC-SVR1\Backup** and then click **Next**.
8. On the **Confirmation** page click **Backup**.
9. On the **Backup Progress** page click **Close** after the backup completes.

Use the Recovery wizard to restore the folder

1. On NYC-DC1, navigate to **C:** and delete the **MarketingTemplates** folder.
2. On the **Windows Server Backup** page, in the Actions pane, click **Recover**.
3. On the **Getting Started** page, click **A backup stored on another location**, and click **Next.**
4. On the **Specify Location type** page, click **Remote shared folder**, and click **Next**.
5. On the **Specify Remote Folder** page, type **\\NYC-SVR1\Backup,** and click **Next**.
6. On the **Select Backup Date** page, click **Next**.
7. On the **Select Recovery Type** page, click **Next**.
8. On the **Select Items to Recover** page expand **NYC-DC1** and click **Local Disk (C:)** drive and on the right panel select **Marketing Templates** and click **Next**.
9. On the **Specify Recovery Options** page, under **Another Location**, type **C:\,** and click **Next**.
10. On the **Confirmation** page, click **Recover**.
11. On the **Recovery Progress** page, click **Close**.
12. Navigate to **C:** and ensure that folder **MarketingTemplates** has been restored to drive C.

Additional Reading

Advantages of Full Server Backup

- Backing Up Your Server

Recovering Data

- Recover Riles and Folders
- Recover Volumes

Lesson 5

Performance and Resource Management

Contents:

Question and Answers 37

Question and Answers

Reasons for Monitoring Windows Servers

Question: Can you list four troubleshooting procedures that would benefit from server monitoring.

Answer: There are many troubleshooting procedures that benefit from server monitoring. Some include:

- Establishing baseline metrics to determine normal operating conditions for servers.
- Improving server performance by detecting anomalies.
- Simplifying troubleshooting through early identification of malfunctioning components.
- Making server management proactive through early identification of potential problems.
- Predicting requirements for future server capacity.
- Reallocating underused resources.

Module Reviews and Takeaways

Review questions

Question: In what situations is it better to plan to use an upstream server as the source of a WSUS server's update files than using Microsoft Update?

Answer: When you've got a good connection to the upstream server and it makes more sense to source those updates over a link rather than to pull them directly over the Internet.

Question: Which types of computers should you include in a test group?

Answer: You should include computers that reflect common configurations. It is better to use a test group that has live computers as you are more likely to find conflicts if the computers are being used for everyday tasks than just if an administrator spends half an hour ensuring that no obvious errors have occurred.

Question: What is the limitation of using network shares as a centralized backup solution?

Answer: Backup to a network share can only hold a single day's worth of backups.

Question: What is the difference between an incremental backup in Windows Backup in Windows Server 2003 and an incremental backup in Windows Server Backup in Windows Server 2008 R2?

Answer: Incremental backups in Windows Server 2003 backed up changed files, incremental backups in Windows Server Backup back up blocks that have changed since the last backup.

Question: Give two reasons to centralize event log management.

Answer: A single location to review event log entries. Second, forwarded event logs from remote computers are available to review, even if the remote computer is not.

Question: What is the primary purpose for creating custom views in Event Viewer?

Answer: A custom view can provide you with instant results from frequently used filters or searches applied to events that are saved as a custom view.

Common Issues related to a server management

Issue	Troubleshooting tip
Cannot connect to remote machine by using Server Manager	Check if remote server is running Windows Server 2008 R2 and that remote management is allowed.
WSUS doesn't sync with Microsoft Update	Check if proxy settings are configured properly
You cannot select specific folders to backup in Windows Server Backup software	Folder selection is only supported in Windows Server 2008 R2
Event Subscription does not work	Check firewall and check if you enable this in command prompt.

Best Practices related to a server management

- Use Server Manager for day to day server administration
- Use Windows Server Backup schedules for period backups

- As your organization moves towards operating systems such as Windows 7 and Windows Server 2008 R2, you can consider retiring local branch office WSUS servers in favor of using BranchCache.
- Use performance monitoring for critical server components before planning to upgrade

Tools

Tool	Use for	Where to find it
Server Manager	Centralized Server Management	Start – Administrative Tools
Window Server Update Service	Update Management	Start – Administrative Tools (should be installed first)
Windows Server Backup	Simple backup and restore procedures	Start – Administrative Tools (should be installed first)
Event Viewer	Viewing and manipulating Windows event logs	Start – Administrative Tools
Task Scheduler	Creating and managing scheduled and programmed tasks	Start – Administrative Tools
Winrm.exe	Configuring the Windows Remote Management service	Command line

Lab Review Questions and Answers

Question: When you add a replica WSUS server, where do you approve the updates?

Answer: You approve updates on main (source) WSUS server

Question: What's the advantage of storing backups in VHD files?

Answer: You can easily mount such backup by using Disk Management, without performing restore procedure

Question: How can you configure a program to run when a specific event appears in Event Log?

Answer: By attaching a task to a specific event.

Module 3

Configuring Networking and Network Services

Contents:

Lesson 1: Configuring IPv6 Addressing **42**

Lesson 2: Migrating from IPv4 to IPv6 **45**

Lesson 3: DHCP and DNS Enhancements in Windows Server 2008 **47**

Lesson 4: Configuring and Managing Windows Firewall with Advanced Security **49**

Lesson 5: Configuring Routing and Networking with Windows Server 2008 **54**

Module Reviews and Takeaways **59**

Lab Review Questions and Answers **61**

Lesson 1

Configuring IPv6 Addressing

Contents:

Detailed Demonstration Steps 43

Detailed Demonstration Steps

Demonstration: How to Configure IPv6 Client Settings

Detailed demonstration steps

Note You require the 6416D-NYC-DC1, 6416D-NYC-SVR1, and 6416D-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator**, with the password, **Pa$$w0rd**.

▶ Task 1: Configure a DHCP scope for IPv6 clients.

1. Switch to NYC-DC1.
2. Click **Start**, in the Search box, type **network and sharing center**, and then press Enter.
3. In Network and Sharing Center, click **Change adapter settings**.
4. In Network Connections, right-click **Local Area Connection 2**, and then click **Properties**.
5. In the Local Area Connection 2 Properties dialog box, double-click **Internet Protocol Version 6 (TCP/IPv6)**.
6. In the Internet Protocol Version 6 (TCP/IPv6) Properties dialog box, click **Use the following IPv6 address**.
7. In the IPv6 address box, type **2001:db8:0:1:1a81:f438:3222:e1b3**.
8. In the Subnet prefix length box, type **64**.
9. In the Preferred DNS server box, type **::1** and then click **OK**.
10. In the Local Area Connection 2 Properties dialog box, click **OK**.
11. Switch to NYC-SVR1.
12. Click **Start**, in the Search box, type **network and sharing center**, and then press Enter.
13. In Network and Sharing Center, click **Change adapter settings**.
14. In Network Connections, right-click **Local Area Connection 2** and then click **Properties**.
15. In the Local Area Connection 2 Properties dialog box, double-click **Internet Protocol Version 6 (TCP/IPv6)**.
16. In the Internet Protocol Version 6 (TCP/IPv6) Properties dialog box, click **Use the following IPv6 address**.
17. In the IPv6 address box, type **2001:db8:0:1:1a81:f438:3222:e1a2**.
18. In the Subnet prefix length box, type **64**.
19. In the Preferred DNS server box, type **2001:db8:0:1:1a81:f438:3222:e1b3** and then click **OK**.
20. In the Local Area Connection 2 Properties dialog box, click **OK**.
21. Switch to NYC-DC1.
22. Click **Start**, point to **Administrative Tools**, and then click **DHCP**.
23. In DHCP, in the navigation pane, expand **NYC-DC1.Contoso.com**, and then click **IPv6**.
24. Right-click **IPv6** and then click **New Scope**.

25. In the New Scope Wizard, click **Next**.
26. On the Scope Name page, in the Name box, type **Contoso IPv6 Scope** and then click **Next**.
27. On the Scope Prefix page, in the Prefix box, type **2001:db8:0:1::** and then click **Next**.
28. On the Add Exclusions page, click **Next**.
29. On the Scope Lease page, click **Next**.
30. On the Completing the New Scope Wizard page, click **Finish**.
31. In the navigation pane, right-click **Server Options** and then click **Configure Options**.
32. In Server Options, select the **00023 DNS Recursive Name Server IPV6 Address List** check box.
33. In the New IPv6 address box, type **2001:db8:0:1:1a81:f438:3222:e1b3**, click **Add**, and then click **OK**.

▶ Task 2: Configure the client computer.

1. Switch to NYC-CL1.
2. Click **Start**, and in the Search box, type **network and sharing center** and then press **Enter**.
3. In Network and Sharing Center, click **Change adapter settings**.
4. In Network Connections, right-click **Local Area Connection 3** and then click **Properties**.
5. In the Local Area Connection 3 Properties dialog box, clear the Internet Protocol Version 4 (TCP/IPv4) check box and then click **OK**.
6. Click **Start**, in the Search box, type **cmd.exe** and then press Enter.
7. At the command prompt, type **ipconfig.exe** and then press Enter.

Note Leave all virtual machines in their current state for the subsequent demonstrations.

Lesson 2

Migrating from IPv4 to IPv6

Contents:

Detailed Demonstration Steps 46

Detailed Demonstration Steps

Demonstration: How to Configure DNS to Support IPv6

Detailed demonstration steps

Note You require the 6416D-NYC-DC1 and 6416D-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator**, with the password, **Pa$$w0rd**. These two machines are already running.

▶ Task 1: Configure the bindings for the DNS service.

1. Switch to NYC-DC1.
2. Click **Start**, point to **Administrative Tools**, and then click **DNS**.
3. In DNS Manager, select and then right-click **NYC-DC1**, and then click **Properties**.
4. On the Interfaces tab, verify that the **2001:db8:0:1:1a81:f438:3222:e1b3** check box is selected, and then click **OK**.

▶ Task 2: Verify the presence of AAAA records in Contoso.com.

1. In DNS Manager, in the navigation pane, expand **NYC-DC1**, expand **Forward Lookup Zones**, and then click **Contoso.com**.
2. Notice that there are several AAAA host records. Leave DNS Manager open.

Note Leave all virtual machines in their current state for the subsequent demonstrations.

Lesson 3

DHCP and DNS Enhancements in Windows Server 2008

Contents:

Detailed Demonstration Steps 48

Detailed Demonstration Steps

Demonstration: How to Configure the GlobalNames Zone

Detailed demonstration steps

Note You require the 6416D-NYC-DC1 virtual machine to complete this demonstration. Log on to the virtual machine as **Contoso\Administrator**, with the password, **Pa$$w0rd**. This virtual machine is already running.

▶ Task 1: Enable the GlobalNames zone functionality.

1. On NYC-DC1, click **Start**, in the Search box, type **cmd.exe** and then press Enter.
2. At the command prompt, type the following, and then press Enter.

dnscmd nyc-dc1 /config /EnableGlobalnamesSupport 1

▶ Task 2: Create and configure the GlobalNames zone.

1. On NYC-DC1, switch to DNS Manager, expand DNS, and then expand NYC-DC1.
2. Right-click **Forward Lookup Zones**, and then click **New Zone**.
3. In the New Zone Wizard, click **Next**.
4. In 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 running on domain controllers in this forest: Contoso.com**, and then click **Next**.
6. In the Zone name field, type **GlobalNames**, and then click **Next**.
7. Click **Do not allow dynamic updates**, click **Next**, and then click **Finish**.

▶ Task 3: Add an alias (CNAME) resource record to the GlobalNames zone.

1. On NYC-DC1, switch to the Command Prompt window.
2. Type the following at the command prompt, and then press Enter.

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

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

▶ Task 4: Test the GlobalNames Zone by using the ping utility.

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

```
ping DC
```

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

Note Leave all virtual machines in their current state for the subsequent demonstrations.

Lesson 4

Configuring and Managing Windows Firewall with Advanced Security

Contents:

Question and Answers 50

Detailed Demonstration Steps 51

Question and Answers

What Is Windows Firewall with Advanced Security?

Question: Why is it important to use a host-based firewall such as Windows Firewall with Advanced Security?

Answer: Windows Firewall with Advanced Security is important for the following reasons:

- Computers are protected from attacks on the internal network. Host-based firewall such as Windows Firewall with Advanced Security can prevent malware from moving through the internal network by blocking unsolicited inbound traffic.
- Inbound rules prevent network scanning to identify hosts on the network. The simplest network scanners ping hosts on a network in an attempt to identify them. Windows Firewall with Advanced Security prevents member servers from responding to ping requests. Domain controllers, however, do respond to ping requests.
- When outbound rules are enabled, they can prevent malware from spreading by preventing the malware from communicating on the network. In the case of a virus outbreak, you can configure computers with a specific outbound rule that prevents the virus from communicating over the network.
- Connection Security rules allow you to create sophisticated firewall rules that use computer and user authentication information to limit communication with high security computers.

Detailed Demonstration Steps

Demonstration: How to Configure Firewall Profiles

Detailed demonstration steps

Note You require the 6416D-NYC-DC1 virtual machine to complete this demonstration. Log on to the virtual machine as **Contoso\Administrator**, with the password, **Pa$$w0rd**. This virtual machine is already running.

▶ Task 1: Configure firewall profiles.

1. On NYC-DC1, click **Start**, point to **Administrative Tools**, and then click **Windows Firewall with Advanced Security**.
2. In Windows Firewall with Advanced Security, point out which profile is active (Domain).
3. In the left pane, right-click the Windows Firewall with Advanced Security node, and then click **Properties**.
4. Mention that inbound connections are blocked by default.
5. Mention that outbound connections are allowed by default.
6. In the Settings area, click the **Customize** button.
7. Mention that the rule merging section is only relevant when rules are being applied through Group Policy.
8. Click **Cancel**.
9. In the Logging area, click the **Customize** button.
10. Mention that no logging is enabled by default.
11. Click **Cancel**.
12. Click each profile tab to show that they all contain the same settings.
13. Click **Cancel**.
14. Click the **Inbound Rules** node.
15. Point out the column that identifies which profiles a rule applies to. Most rules at the top of the list are enabled for all profiles.
16. Scroll down the list and identify a rule that is not applied to only the domain profile.
17. Close Windows Firewall with Advanced Security.

 **Note** Leave all virtual machines in their current state for the subsequent demonstrations.

Demonstration: How to Configure a Connection Security Rule

Detailed demonstration steps

Note You require the 6416D-NYC-DC1, 6416D-NYC-SVR1, and 6416D-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator**, with the password, **Pa$$w0rd**. The virtual machines should still be running from the preceding demonstration.

▶ Task 1: Enable ICMP traffic on NYC-SVR1.

1. Switch to NYC-SVR1.
2. Click **Start**, in the Search box, type **Windows Firewall with Advanced Security**, and then press Enter.
3. Click **Inbound Rules**, right-click **Inbound Rules**, and then click **New Rule**.
4. In the **New Inbound Rule Wizard** dialog box, click **Custom**, and then click **Next**.
5. On the Program page, click **Next**.
6. On the Protocol and Ports page, in the Protocol type list, click **ICMPv4**, and then click **Next**.
7. On the Scope page, click **Next**.
8. On the Action page, click **Allow the connection if it is secure**, and then click **Next**.
9. On the Users page, click **Next**.
10. On the Computers page, click **Next**.
11. On the Profile page, click **Next**.
12. On the Name page, in the **Name** box, type **ICMPv4 allowed**, and then click **Finish**.

▶ Task 2: Create a server-to-server rule on NYC-SVR1.

1. Click **Connection Security Rules**, right-click **Connection Security Rules**, and then click **New Rule**.
2. In the New Connection Security Rule Wizard, click **Server-to-server**, and then click **Next**.
3. On the Endpoints page, click **Next**.
4. On the Requirements page, click **Require authentication for inbound and outbound connections**, and then click **Next**.
5. On the Authentication Method page, click **Advanced**, and then click **Customize**.
6. In the Customize Advanced Authentication Methods dialog box, under First authentication, click **Add**.
7. In the Add First Authentication Method dialog box, click **Preshared key**, type **secret**, and then click **OK**.
8. In the Customize Advanced Authentication Methods dialog box, click **OK**.
9. On the Authentication Method page, click **Next**.
10. On the Profile page, click **Next**.
11. On the Name page, in the **Name** box, type **Contoso-Server-to-Server**, and then click **Finish**.

▶ Task 3: Create a server-to-server rule on NYC-CL1.

1. Switch to NYC-CL1.
2. Switch to Network Connections.
3. Right-click **Local Area Connection 3**, and then click **Properties**.
4. In the **Local Area Connection 3 Properties** dialog box, select the **Internet Protocol Version 4 (TCP/IPv4)** check box, and then click **OK**.
5. Click **Start**, in the **Search** box, type **Windows Firewall with Advanced Security**, and then press Enter.
6. Click **Connection Security Rules**, right-click **Connection Security Rules**, and then click **New Rule**.
7. In the New Connection Security Rule Wizard, click **Server-to-server**, and then click **Next**.
8. On the Endpoints page, click **Next**.
9. On the Requirements page, click **Require authentication for inbound and outbound connections**, and then click **Next**.
10. On the Authentication Method page, click **Advanced**, and then click **Customize**.
11. In the **Customize Advanced Authentication Methods** dialog box, under First authentication, click **Add**.
12. In the **Add First Authentication Method** dialog box, click **Preshared Key**, type **secret**, and then click **OK**.
13. In the **Customize Advanced Authentication Methods** dialog box, click **OK**.
14. On the Authentication Method page, click **Next**.
15. On the Profile page, click **Next**.
16. On the Name page, in the **Name** box, type **Contoso-Server-to-Server**, and click **Finish**.

▶ Task 4: Test the rule.

1. At the command prompt, type **ping 10.10.0.11**, and then press Enter.
2. Switch to Windows Firewall with Advanced Security.
3. Expand Monitoring, expand Security Associations, and then click **Main Mode**.
4. In the right-pane, double-click the listed item.
5. View the information in Main Mode, and then click **OK**.
6. Click **Quick Mode**.
7. In the right-pane, double-click the listed item.
8. View the information in Quick Mode, and then click **OK**.

Note Revert all virtual machines.

Lesson 5

Configuring Routing and Networking with Windows Server 2008

Contents:

Question and Answers 55

Detailed Demonstration Steps 56

Question and Answers

Common Routing Protocols

Question: A subsidiary of Fabrikam, Inc. has a medium-sized network consisting of around 500 nodes. These nodes are distributed across several floors in their headquarters building. Additionally, there are about a dozen branch offices each with around ten nodes. Routers have been deployed within the network to interconnect the networks. Would you recommend static or dynamic routing?

Answer: It depends on the number of routers involved. Static routing has the advantage of being entirely predictable. It does not change unless you change it. However, there might be twenty or more networks in this organization. Because some are remotely connected, there is the possibility of link failure. A routing protocol would be useful in this respect.

Question: Is the use of a routing protocol indicated? If so, which one would you recommend?

Answer: The use of OSPF would be sensible. The network is not too large to implement RIP. However, the presence of remote links with their potential for failure would better suit a link-state, rather than a distance vector protocol. Hence, use OSPF, rather than RIP.

Question: Tailspin Toys has a small network consisting of around 100 nodes. Recently, network throughput has been affected by network traffic. You decide to install routers to help manage the network traffic. Initially, there will be three networks connected by two routers. Would you recommend static or dynamic routing?

Answer: With a small number of routers, there is no need for dynamic routing. Static routing tables would be quick and easy to configure.

Question: How else can you configure these routers?

Answer: You can configure each router to use the other router as its default gateway. There would then be no need for routing tables at all.

Question: Tailspin Toys implements an Internet connection by using a router. How does this change the router configuration you have selected?

Answer: The default gateway method would no longer work; two routers in sequence is the maximum possible. Implementation of either static routing or RIP would now be appropriate.

Detailed Demonstration Steps

Demonstration: How to Configure Wireless Network Settings with Group Policy

Detailed demonstration steps

Note You require the 6416D-NYC-DC1 and 6416D-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator**, with the password, **Pa$$w0rd**.

▶ Task 1: Create an organizational unit and put the client computer account in it.

1. On NYC-DC1, click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. Right-click **Contoso.com**, click **New**, and then click **Organizational unit**.
3. In the **Name** field, enter **Wireless Clients**, and then click **OK**.
4. Click the **Computers** container.
5. Right-click **NYC-CL1**, and then click **Move**.
6. Select the Wireless Clients OU, and then click **OK**.

▶ Task 2: Create a new Group Policy object (GPO) and configure the wireless settings for client computers.

1. On NYC-DC1, click **Start**, point to **Administrative Tools**, and then click **Group Policy Management**.
2. Expand **Forest: Contoso.com**, expand **Domains**, and then expand **contoso.com**.
3. Right-click **Wireless Clients**, and then click **Create a GPO in this domain, and Link it here**.
4. In the **Name** field, enter **Wireless Settings for Windows 7 Clients**, and then click **OK**.
5. Click **Group Policy Objects**, in the main window, right-click **Wireless Settings for Windows 7 Clients**, and then click **Edit**.
6. In the Group Policy Management Editor, right-click the Wireless Settings for Windows 7 Clients [NYC-DC1.contoso.com] Policy icon, and then click **Properties**.
7. Select the Disable User Configuration settings check box, and then click **Yes** when prompted to confirm.
8. Click **OK** to close the window.
9. Expand **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, and then click **Wireless Network (IEEE 802.11) Policies**.
10. 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 Wireless Policy for Windows Vista and Later Releases**.
11. In the **Policy Name** field, enter **Contoso Wireless Network**.
12. Click **Add**, and then click **Infrastructure**.
13. In the **Profile Name** field, enter **Default Contoso profile**.

14. In the **Network Name(s) (SSID)** field, enter **Contoso**, and then click **Add**.
15. Click **OK**.
16. On the Network Permissions tab, select the **Prevent connections to ad-hoc networks** check box.
17. Click **OK**.

▶ Task 3: Test the wireless settings.

1. On NYC-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 Windows 7 clients, and the Default Domain Policy.

Note Leave both the virtual machines running for the final demonstration.

Demonstration: How to Capture and Analyze Network Traffic by Using Network Monitor

Detailed demonstration steps

Note You require the 6416D-NYC-DC1, 6416D-NYC-SVR1, and 6416D-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator**, with the password, **Pa$$w0rd**. Both NYC-DC1 and NYC-CL1 are already running, but do not start NYC-SVR1 until prompted to do so.

▶ Task 1: Capture traffic with Network Monitor.

1. Switch to NYC-CL1.
2. From the Desktop, double-click **Microsoft Network Monitor 3.4**.
3. In the Microsoft Update Opt-In dialog box, click **No**.
4. In Microsoft Network Monitor 3.4, in the Recent Captures pane, click **New capture tab**.
5. On the Capture 1 tab, on the menu bar, click **Start**.
6. On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
7. In Hyper-V Manager, click **6416D-NYC-SVR1**, and in the Actions pane, click **Start**.
8. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
9. Log on as **Contoso\administrator**, with the password, **Pa$$w0rd**.
10. Click Start, and in the Search box, type **cmd.exe** and press Enter.
11. Atthe command prompt, type **ping NYC-DC1**, and then press Enter.

▶ Task 2: Analyze the captured traffic.

1. Switch to NYC-CL1.
2. In Microsoft Network Monitor 3.4, on the menu, click **Stop**.
3. Click the third frame (or whichever frame is the first ARP frame) in the Frame Summary pane.
4. Click in the Frame Details pane and expand **Ethernet**.
5. Discuss the content of the frame with the students. Mention the DestinationAddress and SourceAddress fields.
6. Expand **Arp**.
7. Identify the requested IP address. Which address is this? (This is the local IP address; that is, the IP address of NYC-SVR1).

▶ Task 3: Filter the traffic.

1. In the Display Filter pane, click **Load Filter**.
2. Click **Standard Filters**, point to **NetBios**, and then click **NetBiosNameQuery**.
3. In the **Display Filter** text box, locate the text line that reads NbtNs.NbtNsQuestionSectionData.QuestionName.Name.contains ("www.server.com").
4. Change ("**www.server.com**") to ("**contoso**") and then click **Apply**.
5. Several frames should be returned. Go through each in turn and describe the contents.

▶ Task 4: Save the captured data.

1. On the menu, click **Save As**.
2. Click Desktop, and then, in the **File name** box, type **NYC-SVR1 startup**, and then click **Save**.

Note Revert all virtual machines for the next module.

Module Reviews and Takeaways

Review questions

Question: You are presenting to a potential client the advantages of using Windows Server 2008. What are the new features that you would point out when discussing the Windows Server 2008 DNS server role?

Answer: Background Zone Loading, Support for IPv6, Support for Read-Only Domain Controllers, and Global single names.

Question: What are the different types of unicast IPv6 addresses?

Answer: The different types are link-local, unique-local, and global.

Question: Why is IPv6 necessary?

Answer: It is necessary because of IPv4 address-space depletion, and because it offers more manageable router addressing and better security integration.

Question: What is the process called when a client configures itself with an IPv6 address?

Answer: Autoconfiguration.

Question: What kind of IP address does every IPv6 client automatically assign itself?

Answer: A link-local IP address.

Question: How does the scope of an address affect its ability to communicate on a locally attached subnet?

Answer: The scope limits the networks over which a packet might be routed. A data packet sent in the link-local scope cannot be forwarded beyond the link-local subnet by an IPv4 router. Similarly, a site-local packet will not be forwarded beyond the defined site-local subnets that are defined for a given site. Only global IPv6 addresses can be used to transmit on the public Internet. Tunneling technologies are ISATAP, 6to4, and Teredo.

Question: What is the main purpose of Teredo?

Answer: A Teredo tunnel provides the ability for IPv6 to communicate across IPv4 NATs.

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 cannot 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.

Issue	Troubleshooting tip
	• Test DNS name resolution with the ping tool. • Use the Nslookup tool to view DNS server responses.

Real-World Issues and Scenarios

- 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.
- 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 computer, 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, do not assume that to use it, you must immediately deploy native IPv6 addressing and routing. You can deploy tunneled IPv6 connectivity by using 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 for	Where to find it
IPconfig	Provides overview data for IPv4 and IPv6.	Command-line
Route	Provides basic information about IPv4 and IPv6 routing tables.	Command-line
Netsh	Provides detailed information about IPv6 configuration. It is the primary tool used to configure IPv6 in Windows Server 2008 and Windows Vista. You can use this command-line tool to configure an IPv6 router.	Command-line
DHCP console	Managing DHCP.	Administrative Tools
DNS Manager	Managing a DNS server.	Administrative Tools
Ping	Verifying network connectivity.	Command-line
Gpresult	Verifying and testing the application of GPOs.	Command-line
Network Monitor	Capturing and analyzing network traffic.	Download from the TechNet website

Lab Review Questions and Answers

Question: 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.

Question: What do you need to define on the DNS server 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 6421B)

2.) DNS-based automatic discovery.

This is important because it is a fundamental setting to enable DirectAccess in Windows 7.

Question: 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 **63**

Lesson 3: Configuring Remote Access **68**

Lesson 6: Configuring VPN Enforcement by Using NAP **72**

Module Reviews and Takeaways **76**

Lab Review Questions and Answers **80**

Lesson 2

Configuring a Network Policy Server

Contents:

Detailed Demonstration Steps 64

Detailed Demonstration Steps

Demonstration: How to Configure the NPS Role

Detailed demonstration steps

Note You require the 6416D-NYC-DC1 and 6416D-NYC-SVR1 virtual machines to complete this demonstration. Log on to the virtual machines as Contoso\Administrator with the password Pa$$w0rd.

▶ Task 1: Install the NPS role

1. Switch to NYC-DC1.
2. On the Taskbar, click **Server Manager**.
3. In the Server Manager navigation pane, click **Roles**,
4. In the right pane, click **Add Roles**
5. In the Add Roles Wizard, click **Next**.
6. On the **Select Server Roles** page, select the **Network Policy and Access Services** check box, and then click **Next**.
7. On the **Network Policy and Access Services** welcome page, click **Next**.
8. On the **Select Role Services** page, select the **Network Policy Server** check box, and then click **Next**.
9. On the **Confirm Installation Selections** page, click **Install**.
10. On the **Installation Results** page, click **Close**.
11. Close Server Manager.

▶ Task 2: Register NPS in AD DS

1. Click **Start**, point to **Administrative Tools**, and then click **Network Policy Server**.
2. In the navigation pane, right-click **NPS (Local)**, and then click **Register server in Active Directory**.
3. In the **Network Policy Server** message box, click **OK**.
4. Click **OK** again in the subsequent Network Policy Server message box.

▶ Task 3: Configure a RADIUS server for VPN connections

1. In the Network Policy Server management tool, in the Getting Started details pane, open the drop-down list under Standard Configuration, and then click **RADIUS server for Dial-Up or VPN Connections**.
2. Under Radius server for Dial-Up or VPN Connections, click **Configure VPN or Dial-Up**.
3. In the Configure VPN or Dial-Up wizard, click **Virtual Private Network (VPN) Connections**, accept the default name, and then click **Next**.
4. On the **RADIUS clients** page, click **Add**.

5. In the **New RADIUS Client** dialog box, in the **Friendly Name** box, type NYC-SVR1 and then click **Verify**.
6. In the **Verify Address** dialog box, in the address box, type NYC-SVR1, click **Resolve**, and then click **OK**.
7. In the **New RADIUS Client** dialog box, in the **Shared secret** and **Confirm shared secret** boxes, type Pa$$w0rd, and then click **OK**.
8. On the **Specify Dial-Up or VPN Server** page, click **Next**.
9. On the **Configure Authentication Methods** page, select the **Microsoft Encrypted Authentication version 2 (MS-CHAPv2)** check box, and then click **Next**.
10. On the **Specify User Groups** page, click **Next**.
11. On the **Specify IP Filters** page**,** click **Next**.
12. On the **Specify Encryption Settings** page, click **Next**.
13. On the **Specify a Realm Name** page, click **Next**.
14. On the **Completing New Dial-Up or Virtual Private Network Connections and RADIUS clients** page, click **Finish**.
15. Close the Network Policy Server administrative tool.

▶ Task 4: Save the configuration

1. Click **Start**, and in the **Search** box, type cmd.exe and press Enter.
2. At the command prompt, type the following command, and then press Enter.

```
netsh nps show config> file.txt
```

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

```
Notepad file.txt
```

4. Scroll through the file and discuss the contents.

▶ Task 5: Configure a RADIUS client

1. Switch to NYC-SVR1.
2. On the Taskbar, click **Server Manager**.
3. In the Server Manager navigation pane, click **Roles**, and then in the right pane, click **Add Roles**.
4. On the **Before You Begin** page, click **Next**.
5. On the **Select Server Roles** page, select the **Network Policy and Access Services** check box, and then click **Next**.
6. On the **Network Policy and Access Services** page, click **Next**.
7. On the **Select Role Services** page, select the **Routing and Remote Access Services** check box, and then click **Next**.
8. On the **Confirm Installation Selections** page, click **Install**.
9. On the **Installation Results** page**,** click **Close**.

10. Close the Server Manager window.
11. Click **Start**, point to **Administrative Tools**, and then click **Routing and Remote Access**.
12. In the navigation pane, select NYC-SVR1 (local).
13. Right-click **NYC-SVR1 (Local)**, and then click **Configure and Enable Routing and Remote Access**.
14. In the Routing and Remote Access Server Setup Wizard, on the **Welcome** page, click **Next**.
15. On the **Configuration** page, click **Custom configuration** and click **Next**.
16. On the **Custom Configuration** page, select the **VPN access** check box, and click **Next**.
17. On the **Completing the Routing and Remote Access Server Setup Wizard** page, click **Finish**.
18. In the **Routing and Remote Access** dialog box, click **Start service**.
19. Right-click **NYC-SVR1 (Local)**, and then click **Properties**.
20. In the **NYC-SVR1 (local) Properties** dialog box, click the **IPv4** tab.
21. Click **Static address pool**, and then click **Add**.
22. In the **New IPv4 Address Range** dialog box, in the **Start IP** address box, type 10.10.0.60. In the **Number of addresses** box, type the value of 25, and click **OK**.
23. In the **NYC-SVR1 (local) Properties** dialog box, click the **Security** tab.
24. In the **Authentication provider** list, click **RADIUS Authentication** and then click **Configure**.
25. In the **RADIUS Authentication** dialog box, click **Add**.
26. In the **Add RADIUS Server** dialog box, in the **Server name** box, type NYC-DC1.
27. Click **Change**, and in both **New secret** and **Confirm new secret** check boxes, type Pa$$w0rd, and then click **OK**.
28. Click **OK** three times.

Note Leave all virtual machines in their current state for subsequent demonstrations.

Demonstration: How to Create a Connection Request Policy

Detailed demonstration steps

You must have completed the preceding demonstration and all virtual machines must still be running and in the exact state as at the end of the preceding demonstration.

▶ Task 1: Create a VPN connection request policy

1. Switch to the NYC-DC1 computer.
2. Click **Start**, point to **Administrative Tools**, and then click **Network Policy Server**.
3. In Network Policy Server, expand **Policies**, and then click **Connection Request Policies**. Notice the presence of the Virtual Private Network (VPN) Connections policy; this was created automatically by the wizard when you specified the NPS role of this server.
4. Right-click **Connection Request Policies** and then click **New**.
5. In the **New Connection Request Policy** wizard, in the **Policy name** box, type **Contoso VPN**.

6. In the **Type of network access server** list, click **Remote Access Server (VPN-Dial up)**, and then click **Next**.
7. On the **Specify Conditions** page, click **Add**.
8. In the **Select condition** dialog box, select **NAS Port Type** and click **Add**.
9. In the **NAS Port Type** dialog box, select the **Virtual (VPN)** check box, and then click **OK**. Click **Next**.
10. On the **Specify Connection Request Forwarding** page, click **Next**.
11. On the **Specify Authentication Methods** page, click **Next**.
12. On the **Configure Settings page**, click **Next**.
13. On the **Completing Connection Request Policy Wizard** page, click **Finish**.
14. In the **Connection Request Policies** list, right-click **Contoso VPN** and click **Move Up**.

Note Leave all virtual machines running for the next demonstration. You will also need 6416D-NYC-CL1, so start it now.

Lesson 3

Configuring Remote Access

Contents:

Detailed Demonstration Steps 69

Detailed Demonstration Steps

Demonstration: How to Configure VPN Access

Detailed demonstration steps

Note You require the 6416D-NYC-DC1, 6416D-NYC-SVR1, and 6416D-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as Contoso\Administrator with the password Pa$$w0rd. Both 6416D-NYC-DC1 and 6416D-NYC-SVR1 should be running. Now, start 6416D-NYC-CL1.

▶ Task 1: Verify user dial-in settings

1. Switch to the NYC-DC1 virtual machine.
2. Click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
3. In the navigation pane, expand **Contoso.com** and then click **Marketing**.
4. In the results pane, double-click **Adam Carter**.
5. In the **Adam Carter Properties** dialog box, click the **Dial-in** tab.
6. Notice that the Network Access Permission defaults to **Control access through NPS Network Policy**. Click **OK**.
7. In the right pane, double-click **Marketing** and then click the **Members** tab.
8. Notice that Adam Carter is a member of the group. Click **OK**.
9. Close **Active Directory Users and Computers**.

▶ Task 2: Configure the Network Policies

1. On NYC-DC1, click **Start** and then click **Administrative Tools**.
2. On the **Administrative Tools** menu, click **Network Policy Server**. The Network Policy Server administrative tool appears.
3. In the list pane, expand **Policies** and then click **Network Policies**.
4. Right-click the **Connections to Microsoft Routing and Remote Access server** policy and then click **Disable**.
5. Disable the **Connections to other access servers** policy.
6. Double-click the **Virtual Private Network (VPN) Connections** policy.
7. In the **Virtual Private Network (VPN) Connections** dialog box, click the **Conditions** tab.
8. The existing condition was created in the last demonstration. Click **OK**.

▶ Task 3: Configure a VPN client

1. Switch to the NYC-CL1 computer and log on as **Contoso\administrator** with the password of **Pa$$w0rd**.
2. Click **Start** and then click **Control Panel**.

3. In the Control Panel window, under **Network and Internet**, click **View network status and tasks**.
4. In the **Network and Sharing Center** window, under **Change your networking settings**, click **Set up a new connection or network**. In the **Choose a connection option** dialog box, click **Connect to a workplace** and then click **Next**.
5. In the **Connect to a workplace** dialog box, select the **Use my Internet connection (VPN)** option. When prompted, select **I'll set up an Internet connection later**.
6. In the **Type the Internet address to connect to** dialog box, specify an Internet address of **10.10.0.11** and a **Destination Name** of **HQ**.
7. Select the **Allow other people to use this connection** check box and then click **Next**.
8. On the **Type your user name and password** page, leave the **user name** and **password** blank and then click **Create**.
9. Click **Close** in the **Connect to a Workplace** dialog box.

Demonstration: How to Create a Connection Profile

Detailed demonstration steps

Note You must have completed the preceding demonstration and all virtual machines must still be running and in the exact state as at the end of the preceding demonstration.

▶ Task 1: Install the CMAK Feature.

1. Switch to the NYC-DC1 computer.
2. On the Taskbar, click Server Manager.
3. In Server Manager, in the navigation pane, click Features.
4. In the right pane, click Add Features.
5. In the Add Features Wizard, on the **Select Features** page, select the **Connection Manager Administration Kit** check box and then click Next.
6. On the **Confirm Installation Selections** page, click **Install**.
7. On the **Installation Results** page, click **Close**.
8. Close Server Manager.

▶ Task 2: Create a Connection Profile

1. On NYC-DC1, click **Start**, point to **Administrative Tools**, and then click **Connection Manager Administration Kit**.
2. In the Connection Manager Administration Kit Wizard, click **Next**.
3. On the **Select the Target Operating System** page, click **Windows 7 or Windows Vista**, and then click **Next**.
4. On the **Create or Modify a Connection Manager profile** page, click **New profile**, and then click **Next**.
5. On the **Specify the Service Name and the File Name** page, in the **Service name** box, type Contoso HQ, in the **File name** box, type Contoso, and then click **Next**.

6. On the **Specify a Realm Name** page, click **Do not add a realm name to the user name**, and then click **Next**.
7. On the **Merge Information from Other Profiles** page, click **Next**.
8. On the **Add Support for VPN Connections** page, select the **Phone book from this profile** check box.
9. In the **VPN server name or IP address** box, type 10.10.0.11 and then click **Next**.
10. On the **Create or Modify a VPN Entry** page, click **Next**.
11. On the **Add a Custom Phone Book** page, clear the **Automatically download phone book updates** check box and then click **Next**.
12. On the **Configure Dial-up Networking Entries** page, click **Next**.
13. On the **Specify Routing Table Updates** page, click **Next**.
14. On the **Configure Proxy Settings for Internet Explorer** page, click **Next**.
15. On the **Add Custom Actions** page, click **Next**.
16. On the **Display a Custom Logon Bitmap** page, click **Next**.
17. On the **Display a Custom Phone Book Bitmap** page, click **Next**.
18. On the **Display Custom Icons** page, click **Next**.
19. On the **Include a Custom Help File** page, click **Next**.
20. On the **Display Custom Support Information** page, click **Next**.
21. On the **Display a Custom License Agreement** page, click **Next**.
22. On the **Install Additional Files with the Connection Manager profile** page, click **Next**.
23. On the **Build the Connection Manager Profile and Its Installation Program** page, click **Next**.
24. On the **Your Connection Manager Profile is Complete and Ready to Distribute** page, click **Finish**.

▶ Task 3: Examine the profile

1. Click **Start**, and in the **Search** box, type C:\Program Files\CMAK\Profiles\Windows 7 and Windows Vista\Contoso, and then press Enter.
2. Verify that you can see the executable file that was created for the profile.

Note The profile you created is for 64-bit editions of Windows 7. The client virtual machine is 32-bit.

Note Leave all virtual machines in their current state for the subsequent demonstrations.

Lesson 6

Configuring VPN Enforcement by Using NAP

Contents:

Detailed Demonstration Steps 73

Detailed Demonstration Steps

Demonstration: How to Configure NAP

Detailed demonstration steps

Note You require the 6416D-NYC-DC1 and 6416D-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as Contoso\Administrator with the password of Pa$$w0rd. They should already be running from the previous demonstrations.

Note During the demonstration, when you configure access for noncompliant computers, mention that organizations often allow network access for noncompliant computers during the initial deployment of NAP; this enables a reporting mode rather than a strict enforcement mode.

▶ Task 1: Configure NPS as a NAP health policy server

1. On NYC-DC1, click **Start**, point to **Administrative Tools**, and then click **Network Policy Server**.
2. Expand **Network Access Protection**, expand **System Health Validators**, expand **Windows Security Health Validator**, and then click **Settings**.
3. In the right pane under **Name**, double-click **Default Configuration**.
4. On the Windows 7/Windows Vista selection, clear all check boxes except **A firewall is enabled for all network connections**.
5. Click **OK** to close the **Windows Security Health Validator** dialog box.

▶ Task 2: Configure health policies

1. Expand **Policies**.
2. Right-click **Health Policies**, and then click **New**.
3. In the **Create New Health Policy** dialog box, under **Policy name**, type Compliant.
4. Under **Client SHV checks**, verify that **Client passes all SHV checks** is selected.
5. Under SHVs used in this health policy, select the **Windows Security Health Validator** check box.
6. Click **OK**.
7. Right-click **Health Policies**, and then click **New**.
8. In the **Create New Health Policy** dialog box, under **Policy Name**, type Noncompliant.
9. Under **Client SHV checks**, select **Client fails one or more SHV checks**.
10. Under SHVs used in this health policy, select the **Windows Security Health Validator** check box.
11. Click **OK**.

▶ Task 3: Configure network policies for compliant computers

1. Ensure Policies is expanded.
2. Click **Network Policies**.

3. Disable the two default policies found under Policy Name by right-clicking the policies, and then clicking **Disable**.
4. Right-click **Network Policies**, and then click New.
5. In the Specify Network Policy Name and Connection Type window, under **Policy name**, type Compliant-Full-Access, and then click **Next**.
6. In the Specify Conditions window, click **Add**.
7. In the **Select condition** dialog box, double-click **Health Policies**.
8. In the **Health Policies** dialog box, under **Health policies**, select **Compliant**, and then click **OK**.
9. In the Specify Conditions window, verify that Health Policy is specified under Conditions with a value of Compliant, and then click **Next**.
10. In the Specify Access Permission window, verify that Access granted is selected and then click **Next**.
11. On the **Configure Authentication Methods** page, clear all check boxes, select the **Perform machine health check only** check box and then click **Next**.
12. Click **Next** again.
13. In the Configure Settings window, click **NAP Enforcement**. Verify that Allow full network access is selected, and then click **Next**.
14. In the Completing New Network Policy window, click **Finish**.

▶ Task 4: Configure network policies for noncompliant computers

1. Right-click **Network Policies**, and then click **New**.
2. In the Specify Network Policy Name and Connection Type window, under **Policy name**, type Noncompliant-Restricted, and then click **Next**.
3. In the Specify Conditions window, click **Add**.
4. In the **Select condition** dialog box, double-click **Health Policies**.
5. In the **Health Policies** dialog box, under **Health policies**, select **Noncompliant**, and then click **OK**.
6. In the Specify Conditions window, verify that Health Policy is specified under Conditions with a value of Noncompliant, and then click **Next**.
7. In the Specify Access Permission window, verify that Access granted is selected and then click **Next**.
8. On the **Configure Authentication Methods** page, clear all check boxes, select the **Perform machine health check only** check box and then click **Next**.
9. Click **Next** again.
10. In the Configure Settings window, click **NAP Enforcement**. Select Allow limited access, and clear the **Enable auto-remediation of client computers** check box.
11. Click **Next** and then click **Finish**.

Note We will not proceed with configuring any specific enforcement methods. The module is quite long and time does not permit.

▶ Task 5: Configure NAP client settings

1. Switch to the NYC-CL1 computer.
2. Click **Start**, and in the **Search** box, type napclcfg.msc and then press Enter.
3. In napclcfg – [NAP Client Configuration (Local Computer)], in the navigation pane, click **Enforcement Clients**.
4. In the Results pane, right-click **DHCP Quarantine Enforcement Client**, and then click **Enable**.
5. Close napclcfg – [NAP Client Configuration (Local Computer)].
6. Click **Start**, and in the **Search** box, type Services.msc and press Enter.
7. In Services, in the Results pane, double-click **Network Access Protection Agent**.
8. In the **Network Access Protection Agent Properties (Local Computer)** dialog box, in the **Startup** type list, click **Automatic**.
9. Click **Start** and then click **OK**.
10. Click **Start**, and in the **Search** box, type gpedit.msc and press Enter.
11. In the console tree, expand **Local Computer Policy**, expand **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then click **Security Center**.
12. Double-click **Turn on Security Center (Domain PCs only)**, click **Enabled**, and then click **OK**.
13. Close the console window.

Note Revert all virtual machines.

Module Reviews and Takeaways

Review questions

Question: 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.

Question: The IT manager in your organization is concerned about opening too many firewall ports to facilitate remote access from users working from home via a VPN. How could you meet the expectations of your remote users while allaying your manager's concerns?

Answer: Implement SSTP as the tunneling protocol. This implements a connection by using HTTPS; this protocol relies on TCP port 443, a port that is typically already open on corporate firewalls to facilitate connections to other applications and services; for example, Outlook Web App and Web services.

Question: You have a VPN server with two configured network policies. The first has a condition that grants access to members of the Contoso group, to which everyone in your organization belongs, but has a constraint of day and time restrictions for office hours only. The second policy has a condition of membership of the Domain Admins group and no constraints. Why are administrators being refused connections out of office hours and what can you do about it?

Answer: Administrators are also members of the Contoso group, and therefore the first policy condition is met. The second policy is not processed. The solution is either to remove the administrators from the Contoso group or to change the policy order so that the 'administrator' policy is first in the list.

Question: Why must you register the NPS server in Active Directory?

Answer: When NPS is a member of an Active Directory domain, NPS performs authentication by comparing user credentials that it receives from network access servers with the credentials that Active Directory stores for the user account. NPS authorizes connection requests by using network policy and by checking user account dial-in properties in Active Directory. You must register the NPS server in Active Directory to have permission to access user-account credentials and dial-in properties.

Question: 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 event 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.

- Use the RADIUS Class attribute to track usage and simplify the identification of which department or user to charge for usage. Although the Class attribute, which is automatically generated, is unique for each request, duplicate records might exist in cases where the reply to the access server is lost and the request is re-sent. You might need to delete duplicate requests from your logs to track usage accurately.
- To provide failover and redundancy with SQL Server logging, place two computers that are running SQL Server on different subnets. Use the SQL Server Create Publication Wizard to set up database replication between the two servers.

Question: What considerations are there if you choose to use a nonstandard port assignment for RADIUS traffic?

Answer: 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.

Question: What are the three main client configurations that you need to configure 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.

Question: 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.

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 **NetshNps Show Config> Path\File.txt** command. Save the NPS configuration with the **NetshNps 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.
Services.msc	Managing Windows services	Administrative Tools. Otherwise, launch from Run.
Gpedit.msc	Editing the Local Group Policy	Launch from Run.
Mmc.exe	Management Console creation and management	Launch from Run.
Gpupdate.exe	Managing group policy application	Run from command-line.

Tool	Use	Where to find it
Napclcfg.msc	Manage client computer NAP enforcement settings	Launch from Run.
Netsh command-line tool	Creating administrative scripts for configuring and managing the Network Policy Server role	Ina command window, type ***netsh –c nps*** to administer from a command prompt
Event Viewer	Viewing logged information from application, system, and security events	**Event Viewer** on the **Administrative Tools** menu

Lab Review Questions and Answers

Question: In the lab, you configured the VPN server to allocate an IP address configuration by using a static pool of addresses. What alternative is there?

Answer: You could use a DHCP server on the internal network to allocate addresses.

Question: If you use the alternative, how many addresses are allocated to the VPN server at one time?

Answer: The DHCP server allocates the VPN server blocks of ten addresses at a time to allocate to remote clients.

Question: In the lab, you configured a policy condition of tunnel type and a constraint of a day and time restriction. If there were two policies – the one you created plus an additional one that had a condition of membership of the Domain Admins group and a constraints of tunnel type (PPTP or L2TP) – why might your administrators be unable to connect out of office hours?

Answer: The administrators are affected by the first policy because they are using the tunnel type of either PPTP or L2TP. Change the policy order.

Question: The DHCP NAP enforcement method is the weakest enforcement method in Microsoft Windows Server 2008. What makes it less preferable than other ways?

Answer: It is less preferable because a manually assigned IP address on the client machine circumvents the DHCP NAP enforcement altogether.

Question: Could you use the remote access NAP solution alongside the IPsec NAP solution? What benefit would be realized by using such a scenario?

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

Question: Could you have used DHCP NAP enforcement for the client? Give reasons.

Answer: No. It would not have worked, because the IP addresses assigned to the Routing and Remote Access client are coming from a static pool on the Routing and Remote Access server itself.

Module 5

Configuring and Managing Active Directory Domain Services

Contents:

Lesson 1: Active Directory Enhancements in Windows Server 2008 and 2008 R2 **82**

Lesson 2: Installing and Configuring Domain Controllers **84**

Lesson 3: Configuring Read-Only Domain Controllers **88**

Lesson 4: Configuring Fine-Grained Password Policies **92**

Lesson 5: Managing Active Directory Objects with Windows PowerShell **95**

Lesson 6: Active Directory Database Management **101**

Module Reviews and Takeaways **107**

Lab Review Questions and Answers **109**

Lesson 1

Active Directory Enhancements in Windows Server 2008 and 2008 R2

Contents:

Additional Reading 83

Additional Reading

Infrastructure Enhancements

- Windows Server 2003 with SP1 to Windows Server 2008

Administrative Enhancements

- Windows Server 2008 to Windows Server 2008 R2

Domain and Forest Functional Levels

- Understanding Active Directory Domain Services (AD DS) Functional Levels

Lesson 2

Installing and Configuring Domain Controllers

Contents:

Question and Answers 85

Detailed Demonstration Steps 86

Additional Reading 87

Question and Answers

Unattended Installation Options and Answer Files

Question: How can you manage a domain controller installed on Server Core?

Answer: You can do it from another Windows Server 2008 R2 or Windows 7 computerby using Remote Server Administration Tools.

Detailed Demonstration Steps

Demonstration: Creating Installation Media

Detailed demonstration steps

To complete this demonstration, you must have the 6416D-NYC-DC1 virtual machine running.

1. Log on to **NYC-DC1** as **Contoso\Administrator**, with thepassword,**Pa$$w0rd**.
2. Click **Start**, and then click **Computer**.
3. Double-click **Local Disk (C:)** and create a new folder named,**ADMedia**.
4. Click **Start**, click **All Programs**, click **Accessories**, 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.

Additional Reading

Installing AD DS by Using IFM

- Installing Active Directory Domain Services (AD DS) from Media
- Create Installation Media by Using Ntdsutil

Preparing to Install the RODC

- AD DS: Read-Only Domain Controllers

Lesson 3

Configuring Read-Only Domain Controllers

Contents:

Question and Answers 89

Detailed Demonstration Steps 90

Question and Answers

What Is a Read-Only Domain Controller?

Question: Can you compare the RODC concept with a somewhat similar concept from earlier versions of Windows Server?

Answer: In some way, RODC can be compared to Backup Domain Controllers in Windows NT.

Detailed Demonstration Steps

Demonstration: Managing RODC Account and Password Replication Policy

Detailed demonstration steps

To complete this demonstration, you must have the 6416D-NYC-DC1 virtual machine running.

1. Log on to **NYC-DC1** as **Contoso\Administrator**, with the password **Pa$$w0rd**.
2. Click **Start**, and then run **Dsa.msc** in the **Search** box.
3. Right click **Contoso.com** and select **Raise Domain functional level…**
4. Click **Raise** and then click **OK** twice. Leave **Active Directory Users and Computers** console open
5. Click **Start**, point to **Administrative Tools** and select **Active Directory Domains and Trusts**
6. Right click **Active Directory Domains and Trusts [NYC-DC1.Contoso.com]** and select **Raise Forest Functional Level…**
7. Click **Raise** and click **OK** twice. Close **Active Directory Domains and Trusts** console
8. Restore **Active Directory Users and Computers** console.
9. Expand **Contoso.com**, right-click the **Domain Controllers** OU, and then click **Pre-create Read-only Domain Controller account**.
10. In the **Active Directory Domain Services Installation Wizard**, click **Next**.
11. On the **Operating System Compatibility** page, click **Next**.
12. On the **Network Credentials** page, click **Next**.
13. On the **Specify the Computer Name** page, type **RODC2** in the **Computer Name** field, and then click **Next**.
14. On the **Select a Site** page, click **Next**.
15. On the **Additional Domain Controller Options** page, click **Next**.
16. On the **Delegation of RODC Installation and Administration** page, click **Set**.
17. In the **Select User or Group** dialog box, type **Ed,** click **OK**, and then click **Next**.
18. On the **Summary** page, click **Next**, and then click **Finish**.
19. Click the **Domain Controllers** OU, right-click the **RODC2** computer account, and then click **Properties**.
20. On the **Managed By** tab, notice that Ed Meadows is listed as having administrative rights, but that can 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 can add the Research group to the Allowed RODC Password Replication Group, or you can add the Research global group specifically.

2. Click **Add**.
3. On the **Add Groups, Users and Computers** dialog box, click **Allow passwords for the account to replicate to this RODC,** and then click **OK**.
4. In the **Select Users, Computers or Groups** dialog box, type **Marketing**, and then click **OK**.
5. Click **OK** to close the RODC2 properties dialog box.

Lesson 4

Configuring Fine-Grained Password Policies

Contents:

Detailed Demonstration Steps 93

Detailed Demonstration Steps

Demonstration: Implementing Fine-Grained Password Policies

Detailed demonstration steps

Note You require the 6416D-NYC-DC1 virtual machine to complete this demonstration. Log on to the virtual machine as **Contoso\Administrator**, with the password, **Pa$$w0rd**.

1. On NYC-DC1, click **Start**, click **Run**, type **adsiedit.msc** into the **Run...** dialog box, and then press Enter.
2. In the **ADSI Edit** window, in the console pane, right-click **ADSI Edit**, and then click **Connect to**.
3. In the **Connection Settings** dialog box, click **OK**.
4. In the console pane, expand **Default naming context [NYC-DC1.Contoso.com]**, expand **DC=Contoso, DC=com,** expand **CN=System**, right-click **CN=Password Settings Container**, point to **New**, and then click **Object**.
5. In the **Create Object** dialog box, click **msDS-PasswordSettings**, and then click **Next**.
6. On the **Attribute: cn** page, in the **Value** field, type **Administrator**, and then click **Next**.
7. On the **Attribute: msDS-PasswordSettingsPrecedence** page, in the **Value** field, type **10**, and then click **Next**.
8. On the **Attribute: msDS-PasswordReversibleEncryptionEnabled** page, in the **Value** field, type **false**, and then click **Next**.
9. On the **Attribute: msDS-PasswordHistoryLength** page, in the **Value** field, type **30**, and then click **Next**.
10. On the **Attribute: msDS-PasswordComplexityEnabled** page, in the **Value** field, type **true**, and then click **Next**.
11. On the **Attribute: msDS-MinimumPasswordLength** page, in the **Value** field, type **10**, and then click **Next**.
12. On the **Attribute: msDS-MinimumPasswordAge** page, in the **Value** field, type **06:00:00:00**, and then click **Next**.
13. On the **Attribute: msDS-MaximumPasswordAge** page, in the **Value** field, type **07:00:00:00**, and then click **Next**.
14. On the **Attribute: msDS-LockoutThreshold** page, in the **Value** field, type **3**, and then click **Next**.
15. On the **Attribute: msDS-LockoutObservationWindow** page, in the **Value** field, type **00:00:30:00**, and then click **Next**.
16. On the **Attribute: msDS-LockoutDuration** page, in the **Value** field, type **00:00:30:00**, click **Next**, and then click **Finish**.
17. In the **ADSI Edit** window, select **CN=Password Settings Container** and then double-click **CN=Administrator** in the middle pane.

18. In the **CN=Administrator Properties** window, scroll down and then double-click **msDS-PSOAppliesTo**.
19. In the **Multi-valued Distinguished Name With Security Principal Editor** window, click the **Add Windows Account** button.
20. In the **Select Users**, **Computers, or Groups** window, type **Domain Admins**, click **Check Names**, and then click **OK**.
21. In the **Multi-valued Distinguished Name With Security Principal Editor** window, click **OK**.
22. In the **CN=Administrator Properties** window, click **OK**.
23. Close the **ADSI Edit** window.

Lesson 5

Managing Active Directory Objects with Windows PowerShell

Contents:

Question and Answers 96

Detailed Demonstration Steps 97

Additional Reading 100

Question and Answers

Demonstration: AD DS Database Maintenance

Question: Why is it necessary to stop 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.

Detailed Demonstration Steps

Demonstration: Managing Users and Groups by Using Windows PowerShell

Detailed demonstration steps

Note You require the 6416D-NYC-DC1 virtual machine to complete this demonstration. Log on to the virtual machine as **Contoso\Administrator**, with the password, **Pa$$w0rd**.

1. On NYC-DC1, click **Start**, point to **Administrative Tools**, and then click **Active Directory Module for Windows PowerShell**.
2. To create a new OU, type the following command.

```
new-adorganizationalunit Test1
new-adorganizationalunit Test2
```

3. To create a new user, type the following:

```
new-aduser -name TestUser1 -department IT -city "New York" -organization "Contoso"
```

4. To move the user to another OU, type the following command.

```
get-aduser -filter 'Name -eq "TestUser1"' | move-adobject -targetpath
"ou=Test2,dc=contoso,dc=com"
```

5. To get a group and view its members, type the following command.

```
get-adgroup -filter "Name -eq 'Domain Admins'"

get-adgroup -filter "Name -eq 'Domain Admins'" | get-adgroupmember
```

6. To add a new user to a group, type the following command.

```
add-adgroupmember "Marketing" testuser1
```

7. To set the password and enable a user account, type the following command.

```
Set-ADAccountPassword testuser1 -Reset -NewPassword (ConvertTo-SecureString -AsPlainText
"POwerShellTe$ting1" -Force)

get-aduser -filter 'Name -eq "TestUser1"' | enable-adaccount
```

Demonstration: Restore Deleted Objects with Active Directory Recycle Bin

Detailed demonstration steps

Enable the Active Directory Recycle Bin feature.

1. Click **Start**, click **Administrative Tools**, and then right-click **Active Directory Module for Windows PowerShell**. Click **Run as administrator**.

2. Type the following command, and then press Enter.

```
Enable-ADOptionalFeature –Identity ‘CN=Recycle Bin Feature,CN=Optional
Features,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,
DC=contoso,DC=com’ –Scope ForestOrConfigurationSet –Target ‘contoso.com’
```

3. Type **y**, and then press **Enter**,
4. After the command prompt is returned to you, close the PowerShell window.

Delete an object.

1. Open the **Active Directory Users and Computers** console from **Administrative Tools**.
2. Expand **Contoso.com**, and then expand **IT** organizational unit.
3. In the central pane, right-click **Candy Spoon**, and then select **Delete**.
4. In the confirmation window, click **Yes**.
5. Close Active Directory Users and Computers.

Restore the deleted object by using LDP.exe.

1. To open Ldp.exe, click **Start**, and in the search box, type **ldp.exe**. Under **Programs**, right-click **ldp.exe**, and then click **Run as administrator**.
2. On the **Options** menu, click **Controls**.
3. In the **Controls** dialog box, expand the **Load Predefined** menu, click **Return deleted objects**, and then click **OK**.
4. To verify that the **Deleted Objects** container is displayed:
   - To connect and bind to the server that hosts the forest root domain of your AD DS environment, under **Connection**, click **Connect**, click **OK**, and then, under **Connection**, click **Bind**, and then click **OK**.
   - Click **View**, click **Tree**, and in **BaseDN**, type **DC=contoso,DC=com**, and then click **OK**
   - In the console tree, double-click the root distinguished name (also known as DN) and locate the **CN=Deleted Objects**, **DC=contoso,DC=com** container. Expand that object and ensure that **Candy Spoon** object appears below it.
5. Right-click the **CN=Candy Spoon**,... object, and then click **Modify**
6. In the **Edit Entry Attribute** box, type **isDeleted**.
7. Under **Operation**, click **Delete**, and then click **Enter**.
8. In the **Edit Entry Attribute** box, type **distinguishedName**.
9. In the **Values box**, type the original distinguished name, which is **CN=Candy Spoon, OU=IT,DC=contoso,DC=com**.
10. Under **Operation**, click **Replace**.
11. Ensure that the **Extended** check box is selected, click **Enter**, and then click **Run**.
12. Click **Close**.
13. From **Administrative Tools**, open the **Active Directory Users and Computers** console
14. Expand **Contoso.com**, and then expand **IT** organizational unit.

15. Ensure that the **Candy Spoon** user object exists and that all attributes such as group membership are retained.

Additional Reading

Demonstration: AD DS Database Maintenance

- Compact the Directory Database File (Offline Defragmentation)

Active Directory Snapshots

- Active Directory Domain Services Database Mounting Tool (Snapshot Viewer or Snapshot Browser) Step-by-Step Guide

Lesson 6

Active Directory Database Management

Contents:

Question and Answers 102

Detailed Demonstration Steps 103

Additional Reading 106

Question and Answers

Active Directory Database Files and Modification Process

Question: Which other Microsoft services use a transactional model for making database changes? How does the AD DS model compare to these other services?

Answer: Both Microsoft Exchange Server and Microsoft SQL Server® use the transaction model. The AD DS model is very similar in all cases, although some details, such as the size of the transaction logs, vary. For example, in Exchange Server 2007, the transaction logs are only 1 MB in size.

Demonstration: AD DS Database Maintenance

Question: Why is it necessary to stop 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.

Detailed Demonstration Steps

Demonstration: AD DS Database Maintenance

Detailed demonstration steps

1. If it is not already started, start the virtual machine **6416D-NYC-DC1**and log on as **Contoso\Administrator,** with the password, **Pa$$w0rd**
2. Click **Start**, click **Administrative Tools**, and then click **Services**.
3. Right-click **Active Directory Domain Services**, and then select **Stop** from the context menu.
4. In the **Stop Other Services** dialog box, click **Yes**.

To perform an offline defragmentation of the Advanced Directory database while in an AD DS stopped state:

1. Click **Start**, click **Run**, type **CMD**, and then press Enter.
2. In the Command Prompt 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:\backup**, and after few seconds press **Ctrl+C** to break the process. It takes too long to demonstrate.
6. Copy **C:\windows\ntds\NTDS.dit** to a **C:\backup** folder, along with the logs (*.log), and then delete the logs (*.log).
7. In the Command Prompt window, type **ntdsutil**, and then press Enter.
8. At the **ntdsutil:** prompt, type **Activate Instance NTDS**, and then press Enter.
9. At the **ntdsutil:** prompt, type **files**, and then press Enter.
10. Type **integrity** to check the integrity of the newly compacted database, but press **Ctrl+C** to break the process. Delete the content of folder **C:\backup**.

To move the AD DS database:

1. In the Command Prompt window, type **ntdsutil**, and then press Enter.
2. At the **ntdsutil:** prompt, type **Activate Instance NTDS**, and then press Enter.
3. At the **ntdsutil:** prompt, type **files**, and then press Enter.
4. In the **File Maintenance** Command Prompt window, type **move db to C:\backup**, and then press **Ctrl+C** to break the process. Explain that the NTDS.dit file would be moved to the new location and permissions would be set accordingly

To restart AD DS**:**

1. In the Services MMC, right-click **Active Directory Domain Services**, and then click **Start**.

Demonstration: Restore Deleted Objects with Active Directory Recycle Bin

Detailed demonstration steps

Enable the Active Directory Recycle Bin feature.

1. Click **Start**, click **Administrative Tools**, and then right-click **Active Directory Module for Windows PowerShell**. Click **Run as administrator**.
2. Type the following command, and then press Enter.

```
Enable-ADOptionalFeature –Identity ‘CN=Recycle Bin Feature,CN=Optional
Features,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,
DC=contoso,DC=com’ –Scope ForestOrConfigurationSet –Target ‘contoso.com’
```

3. Type **y**, and then press **Enter**,
4. After the command prompt is returned to you, close the PowerShell window.

Delete an object.

1. Open the **Active Directory Users and Computers** console from **Administrative Tools**.
2. Expand **Contoso.com**, and then expand **IT** organizational unit.
3. In the central pane, right-click **Candy Spoon**, and then select **Delete**.
4. In the confirmation window, click **Yes**.
5. Close Active Directory Users and Computers.

Restore the deleted object by using LDP.exe.

1. To open Ldp.exe, click **Start**, and in the search box, type **ldp.exe**. Under **Programs**, right-click **ldp.exe**, and then click **Run as administrator**.
2. On the **Options** menu, click **Controls**.
3. In the **Controls** dialog box, expand the **Load Predefined** menu, click **Return deleted objects**, and then click **OK**.
4. To verify that the **Deleted Objects** container is displayed:
   - To connect and bind to the server that hosts the forest root domain of your AD DS environment, under **Connection**, click **Connect**, click **OK**, and then, under **Connection**, click **Bind**, and then click **OK**.
   - Click **View**, click **Tree**, and in **BaseDN**, type **DC=contoso,DC=com**, and then click **OK**
   - In the console tree, double-click the root distinguished name (also known as DN) and locate the **CN=Deleted Objects**, **DC=contoso,DC=com** container. Expand that object and ensure that **Candy Spoon** object appears below it.
5. Right-click the **CN=Candy Spoon**,... object, and then click **Modify**
6. In the **Edit Entry Attribute** box, type **isDeleted**.
7. Under **Operation**, click **Delete**, and then click **Enter**.
8. In the **Edit Entry Attribute** box, type **distinguishedName**.
9. In the **Values box**, type the original distinguished name, which is **CN=Candy Spoon, OU=IT,DC=contoso,DC=com**.

10. Under **Operation**, click **Replace**.
11. Ensure that the **Extended** check box is selected, click **Enter**, and then click **Run**.
12. Click **Close**.
13. From **Administrative Tools**, open the **Active Directory Users and Computers** console
14. Expand **Contoso.com**, and then expand **IT** organizational unit.
15. Ensure that the **Candy Spoon** user object exists and that all attributes such as group membership are retained.

Additional Reading

Infrastructure and Application Services Roles

- Compact the Directory Database File (Offline Defragmentation)

Active Directory Snapshots

- Active Directory Domain Services Database Mounting Tool (Snapshot Viewer or Snapshot Browser) Step-by-Step Guide

Module Reviews and Takeaways

Review questions

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

Answer: Authentication will fail.

Question: Why is it necessary to stop 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: Which two tools can you use to create a password setting object?

Answer: You can use ADSI Edit and LDIFDE.

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.

Question: What should you do before starting to use Active Directory Recycle Bin?

Answer: You should check if your forest functional level is on Windows Server 2008 R2, and you must enable the Active Directory Recycle Bin feature by using Windows PowerShell or by using Ldp.exe.

Question: What kind of restore can you perform with Active Directory?

Answer: You can perform authoritative restore, nonauthoritative restore and single object restore with Active Directory Recycle Bin.

Question: Is the Active Directory Administrative Center based on Microsoft Management Console(MMC)?

Answer: No, it is based on Windows PowerShell.

Common issues related to configuring and managing AD DS

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.
You are unable to create an RODC in the domain.	Ensure that there is a Windows Server 2008 domain controller installed in the domain.
You cannot enable Active Directory Recycle Bin.	Check if the forest functional level is Windows Server 2008 R2.
You cannot restore an object by using Active Directory Recycle Bin.	Check if the object was deleted before Active Directory Recycle Bin was enabled.

Best practices related to configuring and managing AD DS

- Deploy Read-Only Domain Controllers on locations where physical security is not good.

- Use fine-grained password policies to specify different password requirements, instead of creating multiple domains.
- Use the ability to stop and start AD DS when a domain controller is online, instead of restarting to the Directory Service Restore Mode.
- Back up the Active Directory database as often as possible.
- Use Active Directory Recycle Bin for object restoration, instead authoritative restore.

Tools

Tool	Use for	Where to find it
ADSI Edit	• Objects and attributes management in Active Directory	%SystemRoot%\System32 on the server or from the RSAT tools for Windows Vista or later
Active Directory with PowerShell Module	• Active directory administration	Administrative Tools
Active Directory Administrative Center	• Active Directory domain management	Administrative Tools

Lab Review Questions and Answers

Question: What is the purpose of Password Replication Policy? If a user is not defined in the Password Replication Policy, which component will process its logon request?

Answer: Password Replication Policy defines groups of users that will have cached or not cached their credentials on Read Only Domain Controllers. If a user is not affected by the Password Replication Policy, and the user's credentials are not cached, then the logon request is processed by writable domain controller.

Question: What is the purpose of creating Shadow Groups in the context of fine-grained password policies?

Answer: Shadow groups are being used to update group membership based on membership in an organizational unit. In the context of a fine-grained password policy, they are used to simulate applying the password setting object to the organizational unit.

Question: Will it be possible to restore the deleted objects if they were deleted before Active Directory Recycle Bin has been enabled?

Answer: Yes, but only as tombstone objects, without most of attributes, or by performing an authoritative restore of AD DS.

Question: In which scenarios is Windows PowerShell a more appropriate method for object restoration?

Answer: If we were restoring multiple objects, PowerShell is a more convenient method because of the possibility to pipeline commands so we can restore multiple objects with just one command.

Module 6

Managing Group Policy in Active Directory Domain Services

Contents:

Lesson 1: Group Policy Enhancements in Windows Server 2008 **111**

Lesson 2: Managing Security with Group Policy **113**

Lesson 3: Managing Clients with Group Policy Preferences **116**

Module Reviews and Takeaways **118**

Lab Review Questions and Answers **120**

Lesson 1

Group Policy Enhancements in Windows Server 2008

Contents:

Additional Reading 112

Additional Reading

What Are ADM and ADMX Files?

- To see a step-by-step guide on managing Group Policy ADMX files, see
- To see more information on the location of ADM (Administrative Template) files,

What Are Multiple Local Group Policies?

- To see a step-by-step guide to managing multiple Local Group Policy objects, see

Lesson 2

Managing Security with Group Policy

Contents:

Detailed Demonstration Steps 114

Detailed Demonstration Steps

Demonstration: How to Configure Application Control Policies

Detailed demonstration steps

Note You require the 6416D-NYC-DC1 and 6416D-NYC-CL1 virtual machines to complete this demonstration. Log on to the 6416D-NYC-DC1 as Contoso\Administrator, with the password, Pa$$w0rd. Do not start NYC-CL1 until directed to do so.

Create a GPO to enforce the default AppLocker Executable rules.

1. On NYC-DC1, click **Start**, click **Administrative Tools**, and then click **Group Policy Management**.
2. Expand **Forest: Contoso.com**, and then expand **Domains**.
3. Expand **Contoso.com**.
4. Click **Group Policy Objects**.
5. Right-click **Group Policy Objects**, and then click **New**.
6. Name the new GPO **WordPad Restriction Policy**, and then click **OK**.
7. Right-click **WordPad Restriction Policy**, and then click **Edit**.
8. Expand **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, expand **Application Control Policies**, and then expand **AppLocker**.
9. Select **Executable Rules**, and then right-click and select **Create New Rule**.
10. Click **Next**.
11. On the **Permissions** screen, select **Deny**, and then click **Next**.
12. On the **Conditions** screen, select **Publisher**, and then click **Next**.
13. Click **Browse**, and then click **Computer**.
14. Double click **Local Disk (C:)**.
15. Double-click **Program Files**, double click **Windows NT**, double-click **Accessories**, select **wordpad.exe**, and then click **Open**.
16. Move the slider up to the **File name:** position, and then click **Next**.
17. Click **Next** again, and then click **Create**.
18. Click **Yes** if prompted to create default rules.
19. In **Group Policy Management Editor**, expand **Computer Configuration**, expand **Windows Settings**, and then expand **Security Settings**.
20. Expand **Application Control Policies**.
21. Click **AppLocker**, and then right-click and select **Properties**.
22. On the **Enforcement** tab, under **Executable rules**, select the **Configured** check box, and then select **Enforce rules**.
23. Click **OK**.

24. In the **Group Policy Management Editor**, expand **Computer Configuration**, expand **Policies**, expand **Windows Settings**, and then expand **Security Settings**.
25. Click **System Services** and then double-click **Application Identity**.
26. In the **Application Identity Properties** dialog box, select the **Define this policy setting** check box.
27. Select **Automatic** under **Select service startup mode**, and then click **OK**.
28. Close **Group Policy Management Editor**.

Apply the GPO to the Contoso.com domain.

1. In the **Group Policy Management** window, expand **Forest: Contoso.com**.
2. Expand **Domains**.
3. Expand **Contoso.com**.
4. Expand **Group Policy Objects**.
5. Drag the **WordPad Restriction Policy** GPO on top of the **Contoso.com** domain container.
6. Click **OK** to link the GPO to the domain.
7. Close the **Group Policy Management** console.
8. Click **Start**, in the **Search programs and files** box, type **cmd**, and then press Enter.
9. In the Command Prompt window, type **gpupdate /force**, and then press Enter. Wait for the policy to be updated.

Test the AppLocker rule.

1. Start and then log on to the **NYC-CL1** as **Contoso\Alan**, with the password, **Pa$$w0rd**.
2. Click **Start**, in the **Search programs and files** box, type **cmd**, and then press Enter.
3. In the Command Prompt window, type **gpupdate /force**, and press Enter. Wait for the policy to be updated.
4. Click **Start**, click **All programs**, click **Accessories**, and then click **WordPad**.
5. Click **OK** to the **This program is blocked by group policy. For more information, contact your system administrator** error message.

Note Revert all virtual machines.

Lesson 3

Managing Clients with Group Policy Preferences

Contents:

Additional Reading 117

Additional Reading

Comparing Group Policy Settings and Preferences

- For an overview of Group Policy preferences, see

Module Reviews and Takeaways

Review questions

Question: You want to place an application control policy on a new type of executable file. What must you do before you can create a rule for this executable code?

Answer: You must add the file extension to the list of Designated Files Types.

Question: Can PowerShell scripts be used as Startup scripts?

Answer: Only Windows Server 2008 R2 or Windows 7 can run PowerShell scripts.

Question: Why must AppLocker rules be defined in a GPO separate from SRP rules?

Answer: AppLocker rules are completely separate from SRP rules and cannot be used to manage pre-Windows 7 computers. The two policies are also separate. If AppLocker rules have been defined in a GPO, only those rules are applied. Therefore, define AppLocker rules in a separate GPO to ensure interoperability between SRP and AppLocker policies.

Question: Your organization currently has a number of Windows 2000 workstations in the organization. You wish to use Group Policy preferences to map printers for all users. What steps must you take to support the Windows 2000 clients?

Answer: You cannot deploy Group Policy preferences to Windows 2000 clients. These clients must be upgraded to at least Windows XP and then have the Group Policy preferences client-side extensions installed.

Question: How can you configure Group Policy preferences from a Windows 7 system?

Answer: Install the Remote Server Administration Tools (RSAT) on the Windows 7 system to access the Group Policy Management Console.

Question: You need to configure a service to start automatically at computer startup. You do not want local users to be able to change this behavior. How should you proceed?

Answer: You should configure a group policy settings for this task. A preference would allow the user to change the behavior.

Question: You have mapped a drive by using preferences, but the user reports that though the drive appears, the user cannot access the drive. What might be the issue?

Answer: The Run in logged-on user's security context setting might be disabled; in which case, the System (computer) account is the account being used to access the resource and it might not have permission.

Best Practices Related to Group Policy

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

- Use Group Policy preferences to perform configurations instead of using scripts
- Use the central store to provide for consistency for administrators that edit GPOs from multiple Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2 computers

Tools

Tool	Use	Where to find it
GPME	Editing Group Policy	Installed as a feature on a server or from the RSAT tools for Windows Vista or later
GPMC	Managing Group Policy	Installed as a feature on a server or from the RSAT tools for Windows Vista or later
Auditpol.exe	Manages auditing settings	%SystemRoot%\System32

Lab Review Questions and Answers

Question: 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.

Question: How could you permit access to only a specific set of applications for a set of computers in your environment?

Answer: Place the computers in an OU, create a GPO, and link it to the OU. In the GPO, configure the default AppLocker rules to block applications. Then whitelist the applications you want the computers to have access to.

Question: You have created Group Policy Preferences to configure new power options. How can you ensure that they will only be applied to laptop computers?

Answer: Use item-level targeting to apply the preference to Portable Computers. Then the preference will be applied if the hardware profile of the computer identifies it as a portable computer.

Module 7

Configuring Active Directory Certificate Services

Contents:

Lesson 1: Active Directory Certificate Services Overview **122**

Lesson 2: Deploying Active Directory Certificate Services **124**

Lesson 3: Managing Certificate Templates **127**

Lesson 4: Managing Certificate Enrollment **131**

Lesson 5: Managing Certificate Revocation **134**

Lesson 6: Managing Certificate Recovery **137**

Module Reviews and Takeaways **142**

Lab Review Questions and Answers **145**

Lesson 1

Active Directory Certificate Services Overview

Contents:

Additional Reading 123

Additional Reading

Components of AD CS in Windows Server 2008

- Active Directory Certificate Services Role

Lesson 2

Deploying Active Directory Certificate Services

Contents:

Question and Answers 125

Additional Reading 126

Question and Answers

Types of CAs

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

Answer: RootCA has the self-signed certificate, while subordinate CA has a certificate issued by RootCA. Also, RootCA usually does not issue any other certificates.

Additional Reading

Stand-Alone vs. Enterprise CAs

- http://go.microsoft.com/fwlink/?LinkID=228340

Upgrading Certification Authority to Windows Server 2008 AD CS

- http://go.microsoft.com/fwlink/?LinkId=116454

Lesson 3

Managing Certificate Templates

Contents:

Question and Answers 128

Detailed Demonstration Steps 129

Additional Reading 130

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 it and upgrade to version 2 or 3, which allows modification.

Configuring Certificate Template Permissions

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

Answer: Only to people who will manage DACL of certificate template. For all other purposes, Write permission is sufficient.

Detailed Demonstration Steps

Demonstration: Modifying and Enabling a Certificate Template

Detailed demonstration steps

1. Launch virtual machine **6416D-NYC-DC1**, and then log on as **Contoso\Administrator** with the password of **Pa$$w0rd**.
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 2008Enterprise**, 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 **CertificateTemplates**, 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 Template Versions

- http://go.microsoft.com/fwlink/?LinkID=228341

Lesson 4

Managing Certificate Enrollment

Contents:

Question and Answers 132

Detailed Demonstration Steps 133

Question and Answers

Obtaining Certificates by Using Manual Enrollment

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

Answer: For example, if you want to enroll non-domain member for a certificate or provide certificate enrollment in isolated environments.

What Is Network Device Enrollment Service (NDES)?

Question: How NDES improve security?

Answer: By providing you a way to distribute certificate for network devices for authentication or encryption

Detailed Demonstration Steps

Demonstration: Configuring the Restricted Enrollment Agent

Detailed demonstration steps

1. On **NYC-DC1**, open the **Certification Authority** snap-in, right-click **ContosoCA**, 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, Candy Spoon), 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, Ed Meadows) 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**.

Lesson 5

Managing Certificate Revocation

Contents:

Detailed Demonstration Steps 135

Detailed Demonstration Steps

Demonstration: Configuring an Online Responder

Detailed demonstration steps

Configure an Online Responder

1. In the Certification Authority console on NYC-DC1, open the **ContosoCA Properties** dialog box.
2. On the **Extensions** tab, examine the **CDPs**, and then close the **ContosoCA Properties** dialog box.
3. Open the **Revoked Certificates** folder properties dialog box.
4. Set the **CRL Publication interval** to **1 Month**.
5. Set the **Publish Delta CRLs interval** to **5 Days**.
6. Click OK

Install the Online Responder component

1. Open **Server Manager** on NYC-DC1
2. Expand **Roles**
3. Click **Active Directory Certificate Services**
4. In the right pane click **Add Role Services**
5. Select **Online Responder** and click **Next**
6. Click **Install**
7. Click Close

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, choose **Authority Information Access(AIA)** in the drop down list of **SelectExtension**:. Add **http://NYC-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. Click **OK** to close the **ContosoCA Properties** dialog box. Click **Yes** to restart AD CS.

Issue the OCSP Response Signing template

1. In the **Certificate Authority** console right-click **Certificate Templates**and select **Manage**.
2. In the list of templates, find**OCSP Response Signing** template, right click it and open **Properties**.
3. Click the **Security** tab
4. Click **Authenticated Users** and then select **Enroll** permission. Click **OK**.
5. Close the **Certificate Templates** console
6. In the **Certification Authority** console right-click **Certificate Templates**, point to **New** and then click **Certificate Template to Issue**.

7. In the list of templates, select **OCSP Response Signing** and click **OK**

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**.
4. After you run the wizard, the revocation configuration status will be set to Online.
5. Close the **Online Responder** console.

Lesson 6

Managing Certificate Recovery

Contents:

Question and Answers 138

Detailed Demonstration Steps 139

Question and Answers

Configuring Automatic Key Archival

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

Answer: You should keep KRA certificate in a secure place, because this certificate can be used to retrieve private key for any archived certificate.

Detailed Demonstration Steps

Demonstration: Configuring CA for Key Archival

Detailed demonstration steps

1. On NYC-DC1, 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**, type **mmc**.**exe**, and press Enter.
9. In **Console 1** window click **File** and select **Add/remove Snap-In**
10. On the **Add/Remove Snap-ins** page, select **Certificates** and click **Add**
11. Select **My user account**, click **Finish** and then click **OK**
12. Expand **Certificates**- **Current User**, expand **Personal**, and then click **Certificates**. Right-click **Certificates**, select **All tasks**, and then click **Request New Certificate**.
13. In **Certificate Enrollment** wizard click **Next** twice.
14. In the **Request Certificates** window, select **Key Recovery Agent** and click **Enroll**.
15. Click **Finish**
16. 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.
17. In the **Certification Authority** console, right-click the **ContosoCA**, and click **Properties**.
18. On the **Recovery Agents** tab, click **Archive the Key**, click **Add**, and then choose the **Administrator** certificate.
19. Click **OK** and confirm to restart AD CS.
20. Right-click **Certificate Templates**, and then click **Manage**.

21. Double-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**. Click OK to close the template.

    When finished with the demonstration, you can leave the virtual machine running because you will need it for subsequent demos in this module.

Demonstration: Recovering a Lost Key

Detailed demonstration steps

1. Open **Run**, start **mmc.exe**, click **File**, and then click **Add/Remove Snap-in**.Select**certificates** in the available snap-ins, and click **Add**. Click **My User Account**, and click **Finish**.
2. Expand **Certificates-Current User**, expand **Personal**, and then click **Certificates**. Right-click **Certificates**, select **Alltasks**, and then click **Request New Certificate**.
3. Enroll for the **Exchange User Test** certificate by using the 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 **Personal->Certificates** 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. Also ensure that you remove all spaces from the serial number, or enclose the serial number in quotation marks.) 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.

Module Reviews and Takeaways

Review questions

Question: 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.

Question: 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.

Question: 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.

Question: List the requirements to use autoenrollment for certificates.

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

Question: 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.

Question: 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.

Question: 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.

Question: What are the steps to configure an Online Responder?

Answer: You must create 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

Issue	Troubleshooting tip
	certificates.
CA was installed as an enterprise CA, but Group Policy settings for user autoenrollment have not been enabled. An enterprise CA can use autoenrollment to simplify certificate issuance and renewal. If autoenrollment is not enabled, certificate issuance and renewal may not occur as expected.	Use the Group Policy Management Console to configure user autoenrollment policy settings, and use the Certificate Templates snap-in to configure autoenrollment settings on the certificate template.
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.

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?
2. What kind of certificates should be used for EFS and digital signing?
3. What kind of certificates should be used for a Web site?
4. How will Contoso ensure that EFS encrypted data is not lost if a user loses a certificate?

Best practices related to a particular technology area in this module

- When deploying CA infrastructure, deploy Stand-Alone (non-domain joined) Root CA, and Enterprise Subordinate CA (issuing CA). After 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.

Tools

Tool	Use for	Where to find it
Certificate Authority Console	Managing CA and certificates	Administrative Tools
Certificate Templates Console	Managing certificate templates	MMC snap-in or run from CA console
Certificates Console	Enrollment and management of locally installed certificates	MMC snap-in

Tool	Use for	Where to find it
Certutil	CA and certificate management	Command line utility

Lab Review Questions and Answers

Question: 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.

Question: 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.

Question: 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 8

Configuring Active Directory Identity and Access Solutions

Contents:

Lesson 1: Installing and Configuring AD LDS **147**

Lesson 4: Installing and Configuring AD RMS **150**

Module Reviews and Takeaways **153**

Lab Review Questions and Answers **156**

Lesson 1

Installing and Configuring AD LDS

Contents:

Detailed Demonstration Steps 148

Detailed Demonstration Steps

Demonstration: How to Install the AD LDS Server Role

Detailed demonstration steps

▶ Task 1: Install the AD LDS server role.

1. On NYC-DC1, click **Start**, point to **Administrative Tools**, and then click **Server Manager**.
2. Click the **Roles** node.
3. In the **Details** pane, click **Add Roles**.
4. On the **Before You Begin** page, click **Next**.
5. Select the **Active Directory Lightweight Directory Services** check box, and then click **Next**.
6. On the **Introduction to Active Directory Lightweight Directory Services** page, click **Next**.
7. On the **Confirm Installation Selections** page, click **Install**.
8. On the **Installation Results** page, click **Close**.

Mention that AD LDS can be installed in a server core installation of Windows Server 2008.

▶ Task 2: Run the AD LDS Setup Wizard to configure AD LDS.

1. On NYC-DC1, click **Start**, point to **Administrative Tools**, and then click **Active Directory Lightweight Directory Services Setup Wizard**.
2. Click **Next** at the first screen of the wizard.
3. On the **Setup Options** page, ensure that **A unique instance** type is selected, and then click **Next**.
4. On the **Instance Name** page, enter **test1** as the **Instance name**. Keep the default **Description**, and then click **Next**.
5. If a Windows Firewall warning appears, click **Allow**.
6. On the **Ports** page, enter **6389** as the **LDAP port number** and **6636** as the **SSL port number**. Click **Next**.
7. On the **Application Directory Partition** page, click the **Yes, create an application directory partition option.** Enter **ou=test1,dc=contoso,dc=local** as the Partition name, and then click **Next**.
8. On the **File Locations** page, keep the default paths, and then click **Next**.
9. On the **Service Account Selection** page, ensure that the **Network service account** option is selected, and then click **Next**.
10. On the **AD LDS Administrators** page, ensure that the **Currently logged on user: CONTOSO\Administrator** option is selected, and then click **Next**.
11. On the **Importing LDIF Files** page, select **MS-User.LDF**, and then click **Next**.
12. On the **Ready to Install** page, click **Next**.
13. When the installation is complete, a message indicating a successful installation appears. Click **Finish**.
14. Close all open windows.

Note Leave all virtual machines in their current state for the subsequent demonstrations.

Lesson 4

Installing and Configuring AD RMS

Contents:

Detailed Demonstration Steps 151

Detailed Demonstration Steps

Demonstration: How to Install the First Server of an AD RMS Cluster

Detailed demonstration steps

Note You require the 6416D-NYC-DC1 and 6416D-NYC-SVR1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator**, with the password, **Pa$$w0rd**. These should still be running from the preceding demonstration.

▶ Task 1: Use DNS to add a CNAME for the AD RMS cluster.

1. Switch to NYC-DC1.
2. Click **Start**, point to **Administrative Tools**, and then click **DNS**.
3. In DNS Manager, expand **NYC-DC1**, expand **Forward Lookup Zones**, and then expand **Contoso.com**.
4. Right-click **Contoso.com**, and then click **New Alias (CNAME)**.
5. In the **Alias** name box, type **RMS**. In the Fully qualified domain name (FQDN) for the target host field, type **NYC-SVR1.contoso.com**, and then click **OK**.
6. Close the DNS Manager.

▶ Task 2: Install the AD RMS server role.

1. Switch to NYC-SVR1.
2. Click **Start**, point to **Administrative Tools**, and then click **Server Manager**.
3. Click **Roles**, then, in the Details pane, click **Add Roles**.
4. On the Before You Begin page, click **Next**.
5. On the Select Server Roles page, select the **Active Directory Rights Management Services** check box.
6. When prompted, click **Add Required Role Services**, and then click **Next**.
7. Click **Next** twice.
8. On the Create or Join an AD RMS Cluster page, select **Create a new AD RMS cluster**, and then click **Next**.
9. On the Select Configuration Database page, select **Use Windows Internal Database on this server**, and then click **Next**.
10. On the Specify Service Account page, click **Specify**, type **CONTOSO\adrms-svc**, type **Pa$$w0rd** for the password. Click **OK** to provide a domain user account for the AD RMS service account. Click **Next** to continue.
11. On the Configure AD RMS Cluster Key Storage page, select **Use AD RMS centrally managed key storage**, and then click **Next**.
12. On the Specify AD RMS Cluster Key Password page, type **Pa$$w0rd** to confirm the AD RMS cluster key password, and then click **Next**.

13. On the Select AD RMS Cluster Web Site page, ensure that **Default Web Site** is selected, and then click **Next**.
14. 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**.
15. On the Name the Server Licensor Certificate page, accept the default value of **NYC-SVR1**, and then click **Next**.
16. On the Register AD RMS Service Connection Point page, select **Register the AD RMS service Connection point now**, and then click **Next**.
17. On the Web Server (IIS) page, click **Next**.
18. On the Select Role Services page, click **Next**.
19. On the Confirm Installation Selections page, view the informational messages, and then click **Install** to complete the installation.
20. After the installation is complete, click **Close**.

Note Revert all virtual machines.

Module Reviews and Takeaways

Review questions

Question: How can you configure intersite replication for AD LDS?**Answer**: Use AD Sites and Services.

Question: What are your options for high availability for AD LDS?**Answer**: Load balancing is one option and adding additional replicas is another option.

Question: If you want to run multiple instances of AD LDS on a single server, which networking pieces are needed?**Answer**: Ports. Each instance requires a unique port.

Question: You are troubleshooting an AD FS 2.0 user reported issue. You have checked the AD FS 2.0 Admin log but enough information to diagnose the issue is unavailable. What are two other options for gathering additional troubleshooting information?**Answe**r: Enable the debug log and enable auditing. Both give you a substantial amount of additional information, which should help narrow down the problem.

Question: You are reviewing your design options for an upcoming AD FS 2.0 deployment. What are the two supported AD FS 2.0 designs?**Answer**: Web SSO and federated web SSO**Question**: What are some reasons to deploy AD RMS?**Answer**: Reasons include providing persistent protection to sensitive information, providing the ability for users to communicate securely by using email, and automatically protecting document libraries in SharePoint.

Question: Which special requirement must be met to install AD RMS on a domain controller? You run across an AD RMS-protected document that you cannot open. You were able to open it a couple of months ago, so you are positive that you had the proper authorization. What might cause this?**Answer**: The content is expired. The content author put an expiration on the content and it has now expired. The content is not viewable by anybody.

Common Issues related to Active Directory Rights Management Services

Issue	Troubleshooting tip
Unable to exchange AD RMS protected email messages with partner company	Look at other IDA roles that can extend AD RMS.
Windows XP client computer not able to protect documents by using AD RMS	Client computer issue.
In multi-domain environment, AD RMS protected email sent to group cannot be opened by group members	Look at group types in cross-domain environments.
Unable to protect Microsoft Office documents by using Windows SharePoint Services	Always ensure that your application is AD RMS-aware.

Real-world Issues and Scenarios

1. Fabrikam has a development team working at two locations. The development team is working on the same directory-aware application. Currently, AD LDS is deployed at one location. Because of bandwidth constraints, the development team at the other location has reported poor performance when working with the application. What can you do to improve the performance?
2. The IT team at Contoso deployed AD LDS for their development team. To keep things simpler at that time, the team deployed AD LDS on an existing domain controller. The development team has asked for administrative access to perform tasks such as installing SSL certificates, stopping and starting services, and managing the AD LDS database. How should you proceed?
3. Tailspin Toys is deploying a new claims-based web application on the perimeter network. The application relies on a back-end SQL database for data storage. The company wants to give a partner company access to the web application. However, in initial testing, the partner company's users are reporting issues when they attempt to use the web application to request data from the database. Which AD FS 2.0 technology can solve this problem?
4. Fabrikam is examining the requirements for AD FS 2.0. The company wants to use a federation proxy server for maximum security. Currently, Fabrikam has an internal network with internal DNS servers. Their Internet-facing DNS is hosted by a hosting company. The perimeter network uses the hosting company's DNS servers for DNS resolution. What must the company do to prepare for the deployment?
5. An organization wants to offer employees persistent protection for Microsoft Office Word documents. In addition, the organization wants to enable employees to be able to send confidential messages to anybody on the Internet. Which technology or technologies should this organization use?
6. Fabrikam runs AD DS, AD RMS, and Exchange Server 2010. The company wants to ensure that when employees send other employees an email message that contains the phrase, "Top Secret", the email message is automatically protected with AD RMS. How should they accomplish this?

Tools

Tool	Use for	Where to find it
Adamsync.exe	Replicating between AD LDS and AD DS	Available on AD LDS server after importing user class
Dsdbutil.exe	Changing AD LDS service account, viewing instance information, and snapshots	%systemroot%\system32
Ldifde.exe	Importing data into AD LDS and updating the schema	%systemroot%\system32
AD RMS Bulk Protection Tool	Protecting files in bulk	http://go.microsoft.com/fwlink/?LinkID=212934
Windows PowerShell®	Installing, configuring, and administering AD RMS	Import AD RMS PowerShell modules: Import-Module AdRmsAdmin Import-Module AdRms
Rights Management Services Administration	Miscellaneous AD RMS administrative tools	http://go.microsoft.com/fwlink/?LinkId=98961

Tool	Use for	Where to find it
Toolkit with SP2		

Lab Review Questions and Answers

Question: Which ports are used by default for AD LDS?

Answer: On member servers, ports 389 and 636 for Secure Sockets Layer (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.

Question: Which type of input files are used to customize the schema?

Answer: LDAP directory interchange format files are used to modify the schema.

Question: Which groups reside in the Roles container of each directory partition?

Answer: Administrators, Readers, and Users.

Question: 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, the cluster URL must be in Trusted Sites zone.

Question: 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.

Module 9

Installing and Configuring Remote Desktop Services

Contents:

Lesson 1: Overview of Remote Desktop Services **158**

Lesson 2: Implementing RemoteApp Infrastructure **162**

Lesson 3: Implementing Remote Desktop Gateway **167**

Module Reviews and Takeaways **172**

Lab Review Questions and Answers **174**

Lesson 1

Overview of Remote Desktop Services

Contents:

Question and Answers 159

Detailed Demonstration Steps 160

Additional Reading 161

Question and Answers

What Are Remote Desktop Services?

Question: How is RDS different from Remote Desktop?

Answer: You can enable Remote Desktop on a Windows client and server operating system, while RDS is a server role, and you can add it only to the Windows Server 2008 R2 operating system. Remote Desktop allows up to three remote sessions, which includes two remote desktop sessions and a console redirection, while RDS supports as many connections as you have licenses. RDS provides many additional features, such as RemoteApp programs, RD Web Access, RD Gateway, or VDI. These features are not available when you enable only Remote Desktop.

Client Experience Features with RDS

Question: Are enhanced features that RDP 7.0 provides available just on Windows 7 and Windows Server 2008 R2 clients?

Answer: To benefit from new and enhanced RDP 7.0 features, you must use Remote Desktop Connection (RDC) 7.0 client or newer. This client is part of Windows 7 and Windows Server 2008 R2, but you can download it for Windows XP Service Pack 3 (SP3), Windows Vista SP1, or a newer operating system. When you use RDC 7.0 client, most of the new and enhanced features are available on the client, but some of them, such as Aero Glass support, work only on Windows 7 and Windows Server 2008 R2 clients.

Detailed Demonstration Steps

Demonstration: Establishing a Remote Desktop Connection Client

Detailed Demonstration Steps

For this demonstration, start 6416D-NYC-DC1 and 6416D-NYC-CL1. Log on to all virtual machines as **Contoso\Administrator** with the password **Pa$$w0rd**.

1. On NYC-DC1, click **Start**, right-click **Computer**, click **Properties**, and then click **Remote settings**.
2. On the **Remote** tab, select the **Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)** option. Click **OK** at the Remote Desktop Connection prompt. Click **OK** to close the System Properties box.
3. On NYC-CL1, click **Start**, point to **All Programs**, click **Accessories**, and then click **Remote Desktop Connection**.
4. In **Remote Desktop Connection**, click **Options**.
5. On the **General** tab, enter **NYC-DC1** in the **Computer** field.
6. Click the **Display** tab, and then set **Display configuration** to **800x600**.
7. On the **Local Resources** tab, clear the **Printers** check box from the Local devices and resources section and review the rest of available options.
8. Click the **Programs** tab and review available options.
9. Click the **Experience** tab and review available options.
10. Click the **Advanced** tab, click **Settings**, review available options and then click **Cancel**.
11. Click the **General** tab, click **Save as**, and then save the settings on the **Desktop**.
12. On the Desktop, right-click the saved file, and open it in Notepad.
13. Review the settings in Notepad, and then close Notepad.
14. Click **Connect** in Remote Desktop Connection, click **Connect** again, and then provide **Contoso\Administrator** with the password of **Pa$$w0rd** to establish a connection with NYC-DC1.
15. In the NYC-DC1 – Remote Desktop Connection window, click **Start**, and then click **Log off**.

Additional Reading

What Are Remote Desktop Services?

- Additional reading can be found at Windows Server 2008 R2: Remote Desktop Services,

What Is RemoteFX?

- Additional reading can be found at Microsoft RemoteFX,

Lesson 2

Implementing RemoteApp Infrastructure

Contents:

Question and Answers 163

Detailed Demonstration Steps 164

Additional Reading 166

Question and Answers

What Is Remote Desktop Web Access?

Question: Why would you use RD Web Access?

Answer: Answers will vary, but may include following reasons: List available RemoteApp programs, remote desktops, and virtual desktops at one place, Start RemoteApp programs easily, without distributing shortcuts to client computers, and integrate a list of available RemoteApp programs with the Start menu on Windows 7 clients.

What Is RemoteApp User Assignment?

Question: Why would you use RemoteApp User Assignment?

Answer: The main reason for configuring RemoteApp User Assignment is to limit who can see published RemoteApp programs and to reduce the number of unnecessary applications that users see. If you do not configure RemoteApp User Assignment, all authenticated users can see published RemoteApp programs.

Detailed Demonstration Steps

Demonstration: How to Publish RemoteApp Programs

Detailed Demonstration Steps

For this demonstration, start 6416D-NYC-DC1, 6416D-NYC-SVR1, and 6416D-NYC-CL1. Log on to all virtual machines as **Contoso\Administrator** with the password **Pa$$w0rd**. You also need to complete the steps of Exercise 1 in the Lab, before you perform this demonstration.

1. On the **Start** menu of the NYC-SVR1 server, point to **Administrative Tools**, **Remote Desktop Services**, and **Remote Desktop Web Access Configuration**. The Internet Explorer window opens. Click **Continue to this website**.
2. In Internet Explorer, enter **contoso\administrator** as Domain\user name, **Pa$$w0rd** as Password, and then click **Sign in**.
3. Select the **One or more RemoteApp sources** radio button, enter **NYC-DC1.contoso.com; NYC-SVR1.contoso.com** in **Source name**, and then click **OK**. The source setting configures the **Remote Desktop Web Access** page to retrieve the aggregated list of RemoteApp programs from both RD Session Host servers.
4. On the **Start** menu of the NYC-DC1 server, point to **Administrative Tools**, point to **Remote Desktop Services**, and then click **RemoteApp Manager**. The RemoteApp Manager window opens.
5. In the Actions pane of **RemoteApp Manager**, click **Add RemoteApp Programs**.
6. Click **Next** in the Welcome to the RemoteApp Wizard.
7. Select the **Calculator** and **Paint** check boxes, and then click **Next**. Calculator and Paint represent applications that are available on a Remote Desktop Session Host Server. However, in reality, any business application could be in the list.
8. Click **Finish** in the Review Settings window. Calculator and Paint are added to the list of available RemoteApp Programs.
9. On the **Start** menu of the NYC-SVR1 server, point to **Administrative Tools**, point to **Remote Desktop Services**, and then click **RemoteApp Manager**. The RemoteApp Manager window opens.
10. In the Actions pane of **RemoteApp Manager**, click **Add RemoteApp Programs**.
11. Click **Next** in the Welcome to the RemoteApp Wizard.
12. Click **Browse**, select **Notepad** in the **Windows\System32** folder, and then click **Open**.
13. Select the **WordPad** check box, and then click **Next**. WordPad and Notepad represent applications that are available on a Remote Desktop Session Host Server. However, in reality, any business application could be in the list.
14. Click **Finish** in the Review Settings window. Notepad.exe and WordPad are added to the list of available RemoteApp Programs.
15. On NYC-SVR1, refresh the page in Internet Explorer. If popup window appears click Retry. Verify that all four RemoteApp published applications are displayed on the **RemoteApp Programs** web page.
16. On the NYC-SVR1 server, switch to RemoteApp Manager, right-click **WordPad** in the **RemoteApp Programs** list, and then select **Properties**.

17. On the **User Assignment** tab, select the **Specified domain users and domain groups** radio button, and then click **Add**. Enter **contoso\ruser**, and then click **OK**. This allows only ruser to view RemoteApp icon for WordPad. Click **OK** in the **RemoteApp Properties** dialog box.
18. On the NYC-SVR1 server, switch to Internet Explorer, and then refresh the page. Because **Administrator** does not have permissions for **WordPad** RemoteApp program any longer, the WordPad icon is no longer available, and there are only three RemoteApp programs available on the **Remote Desktop Services Default Connection** web page.

Additional Reading

What Are RemoteApp Programs?

- Additional reading can be found at Overview of RemoteApp,

What Is Remote Desktop Web Access?

- Additional reading can be found at Overview of Remote Desktop Web Access (RD Web Access),

Lesson 3

Implementing Remote Desktop Gateway

Contents:

Question and Answers 168

Detailed Demonstration Steps 169

Additional Reading 171

Question and Answers

Remote Desktop Gateway Overview

Question: In which situations would you use RD Gateway?

Answer: You would use RD Gateway if you need to provide access to RDS hosts to remote users over Internet. Local users can access RDS hosts directly, but remote users first need to establish a connection to local network. Previously, users had to establish a VPN connection, but with RD Gateway, users can access internal RDS hosts without first establishing a VPN connection

Detailed Demonstration Steps

Demonstration: Configuring RD Gateway

Detailed Demonstration Steps

For this demonstration, start 6416D-NYC-DC1 and 6416D-NYC-SVR1. Log on to all virtual machines as **Contoso\Administrator** with the password **Pa$$w0rd**. You also need to install the Remote Desktop Gateway role service on NYC-SVR1.

1. On the NYC-SVR1 server, open **Server Manager**, expand **Roles,** click **Remote Desktop Services** in the left pane, and then click **Add Role Services** in the right pane.
2. On the **Select Role Services** page, select **Remote Desktop Gateway**. When the **Add Role Services** window pops up, click **Add Required Role Services**. Click **Next**.
3. On the **Choose a Server Authentication Certificate for SSL Encryption** page, select **Create a self-signed certificate for SSL encryption** and click **Next.**
4. On the **Create Authorization Policies for RD Gateway** page, click **Later**, and click **Next** five times.
5. On the **Confirm Installation Selections** page, click **Install**.
6. On the **Installation Results** page click **Close.**
7. Click **Start**, point to **Administrative Tools**, point to **Remote Desktop Services**, and then click **Remote Desktop Gateway Manager**.
8. Expand **RD Gateway Manager**, expand **NYC-SVR1 (Local)**, expand **Policies**, and then click **Connection Authorization Policies**.
9. In the Actions pane, click **Create New Policy**, and then click **Wizard**.
10. Click **Next** in the **Create Authorization Policies for RD Gateway Wizard**.
11. Enter **Authorized Remote Users** as name for the RD CAP, and then click **Next**.
12. On the **Select Requirements** page, next to **User group membership**, click **Add Group,** type **RD Users**, click **OK**, and then click **Next**. In the lab environment, all RD Users are allowed access through RD Gateway. In a production environment, you would have separate groups.
13. Click **Next** to accept the default settings for device redirection.
14. On the **Set Session Timeouts** page, click **Next**, and on the **RD CAP Settings Summary** page, click **Finish**.
15. Click **Close** to confirm the creation of authorization policies.

Configuring a RAP

1. On NYC-SVR1, in RD Gateway Manager, expand **NYC-SVR1 (Local)**, expand **Policies**, and then click **Resource Authorization Policies**.
2. In the Actions pane, click **Create New Policy**, and then click **Wizard**.
3. Click **Next** in the Create Authorization Policies for RD Gateway Wizard.
4. Enter **Authorized Target Computers** as name for the RD RAP, and then click **Next**.

5. On the **Select User Groups** page, click **Add Group**, add **RD Users**, click **OK**, and then click **Next**. In the lab environment, all RD Users are allowed access through RD Gateway. In the production environment, you would have a separate group for that.
6. On the **Select Network Resources** page, leave the option Select an Active Directory Domain Services network resource group selected, click **Browse**, type **RD Computers**, click OK, and then click **Next**.
7. Click **Next** to accept the default **Allowed TCP Ports**.
8. Click **Finish** on the **RD RAP Settings Summary** page. Click **Close** to confirm the creation of authorization policies.

Additional Reading

Remote Desktop Gateway Overview

- Additional reading can be found at Remote Desktop Gateway,

Module Reviews and Takeaways

Review questions

Question: Do you need to install the RDS role if you only want to provide Remote Desktop access for remote administration?

Answer: No, if you want just Remote Desktop for remote administration, you can simply enable Remote Desktop. It will allow up to three sessions (two sessions and console redirection) and you will not need any additional CAL licenses for that.

Question: Is the RD Web Access role service required if you want to provide RemoteApp program access for your clients?

Answer: It depends. If you copy the .rdp file for publishing RemoteApp to your clients, or if you deploy a Windows Installer package for a RemoteApp program to your clients, you do not need RD Web Access. However, if you want to list the available RemoteApp programs on a Web page, or if you want to deploy RemoteApp and Desktop Connections to your Windows 7 clients, you must implement RD Web Access in your environment.

Question: Can you connect from Windows Vista SP1 client to RD Session Host server on Windows Server 2008 R2?

Answer: Yes, you can connect from Windows Vista SP1 client to RD Session Host server on Windows Server 2008 R2. But if you want to benefit from new and improved features that are provided by RDP 7.0 protocol, you need to install RDC 7.0 on Windows Vista SP1 computer.

Question: How can you control who sees the RemoteApp program link on the RD Web Access web page?

Answer: By default, when you publish a RemoteApp program, all authenticated users will see the link to that RemoteApp program on the RD Web Access Web page. You can hide the link to specific RemoteApp programs on the RD Web Access page for all users, and you then can use RemoteApp User Assignment to assign a link to specific users or groups. This enables you to ensure that only users that you specify can see the RemoteApp program link on the RD Web Access Web page.

Question: What benefits does SSO provide when you run RemoteApp programs and where can you configure it?

Answer: SSO enables you to start RemoteApp program with the same credentials as the currently logged on user, without providing these credentials again. With SSO, user experience when starting RemoteApp program is similar to starting a local application, as in both cases users do not have to enter their credentials again. You configure SSO in the Credentials Delegation part of Computer settings in Group Policy.

Question: Does RD Gateway provide full end-to-end protection of RDP traffic?

Answer: No, RD Gateway protects RDP traffic just between the RD client and RD Gateway. From RD gateway to RDS, RDP transmits host traffic, so RD Gateway does not provide additional protection. However, you should be aware that RDP itself uses encryption, and that it is a local network between RD Gateway and the RDS host, not a public network, such as the Internet.

Common Issues Related to Remote Desktop Services

Issue	Troubleshooting tip
Users can connect to the RD Session Host server from Windows 7 and Windows Vista clients, but they cannot connect from Windows XP clients.	You configure an RD Session Host with Network Level Authentication, which is available in Windows 7 and Windows Vista. However, you must enable it specifically on Windows XP SP3 clients.
When users establish a Remote Desktop session with RD Session Host, they cannot use any of the Windows 7 features, like desktop themes and photo management.	This is the default behavior. To enable Windows 7 features in RD sessions, you must add the Desktop Experience feature on the RD Session Host server, and then enable Windows 7 features.
When users establish an RD session from a Windows 7 client, they can see the Aero Glass effect in the session. However, when the same users establish an RD session from a Windows Vista client, the Aero Glass effect is not available.	This behavior is by design, as even with RDC 7.0 client, the Aero Glass effect in RD session is available on Windows 7 and Windows Server 2008 R2 clients only. It is not available on older client operating systems.
Several users can see a published RemoteApp program on the RD Web Access Web page, while other users cannot.	The most probable reason for this is the RemoteApp User Assignment configuration. It is likely that it is configured so that some users have the RemoteApp program assigned and others do not.
When users start RemoteApp programs, they always receive prompts for their credentials.	This is the default behavior when you are running RemoteApp programs. You can avoid this by configure SSO.
Users can open data files in a RemoteApp program, but when they double-click on the same file in Windows Explorer, the RemoteApp program does not start.	When creating the Windows Installer package for the RemoteApp program, you should associate client extensions with the RemoteApp program.

Best Practices Related to Remote Desktop Services

- Use RemoteApp programs instead of classic terminal applications to provide better user experience
- Deploy RemoteApp programs as .msi packages as they provide more options
- Use RD Gateway instead VPN
- Always work with dedicated groups when managing CAPs and RAPs in RD Gateway

Lab Review Questions and Answers

Question: Which RDS role service must you install first before you can publish RemoteApp programs?

Answer: You can publish RemoteApp programs on the RD Session Host server, so you must install at least this role service before you can publish RemoteApp programs.

Question: Which group enables the user to access Remote Desktop or published RemoteApp program?

Answer: Before users can connect to Remote Desktop or published RemoteApp program, they must be members of the Remote Desktop Users group. This is a local group on member servers and a domain group for accessing RD Session Host on domain controllers.

Question: How can you consolidate a list of available RemoteApp programs from multiple servers on the same RD Web Access Web page?

Answer: You can either use RD Connection Broker as a source and configure it with RD Session Hosts or configure RD Web Access to use multiple RD Session Host servers as the sources.

Question: How can you avoid additional prompts when you start a RemoteApp program?

Answer: If you want to avoid additional prompts when you start RemoteApp program, you should configure digital signing for the .rdp file, a trusted .rdp publisher, and single sign-on.

Question: Can you use RemoteApp and Desktop Connections for enabling access to RemoteApp programs from all your clients?

Answer: You can use RemoteApp and Desktop Connections only with the Windows 7 and Windows Server 2008 R2 operating systems. You cannot use it with older operating systems, but you can instruct users to visit the RD Web Access Web site and start RemoteApp programs from there.

Module 10

Managing Remote Desktop Services

Contents:

Lesson 1: Managing RD Session Host and Connection Broker **176**

Lesson 2: Configuring and Managing Remote Desktop Licensing **181**

Lesson 3: Managing Remote Desktop Client Connections **184**

Module Reviews and Takeaways **189**

Lab Review Questions and Answers **191**

Lesson 1

Managing RD Session Host and Connection Broker

Contents:

Question and Answers 177

Detailed Demonstration Steps 178

Additional Reading 180

Question and Answers

What Is RD Connection Broker?

Question: If the user's network connection is lost and the user attempts to reconnect, will he or she get reconnected to their previous session?

Answer: Yes, in a nutshell, that is one of the main purposes of RD Connection Broker. If a user with an existing session reconnects, RD Connection Broker Load Balancing redirects the user to the RD Session Host server where the user's existing session resides.

Configuring an RD Session Host Farm with RD Connection Broker

Question: What is the farm name used for?

Answer: The farm name is the virtual name that clients will use to connect to the RD Session Host server farm.

Detailed Demonstration Steps

Demonstration: Configuring an RD Connection Broker Managed Farm

Detailed Demonstration Steps

For this demonstration, start 6416D-NYC-DC1, 6416D-NYC-SVR1, and 6416D-NYC-SVR2. Log on to all virtual machines as **Contoso\Administrator** with the password **Pa$$w0rd**. You also need to complete the steps of Exercise 1, Task 1 and then Exercise 3 Task 1 (Steps 1-8) in the Lab, before you perform this demonstration.

1. On the **Start** menu of NYC-DC1, point to **Administrative Tools**, and then click **Active Directory Users and Computers**. The Active Directory Users and Computers console appears.
2. In the left pane, click **Users**.
3. In the result pane, right-click the **Session Broker Computers** group, and then click **Properties**. The **Session Broker Computers Properties** dialog box appears**.**
4. On the **Members** tab, click **Add**.
5. In the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, click **Object Types**.
6. Select the **Computers** check box, and then click **OK**.
7. In the **Enter the object names to select** box, type **NYC-SVR1;NYC-SVR2,** click **Check Names,** and then click **OK**.
8. In the **Session Broker Computers Properties** dialog box, click **OK.**
9. Close the **Active Directory Users and Computers** console.

Configure RD Connection Broker settings.

1. On the **Start** menu of NYC-SVR1, point to **Administrative Tools**, point to **Remote Desktop Services**, and then click **Remote Desktop Session Host Configuration**. The **Remote Desktop Session Host Configuration** console appears.
2. On the **Configuration for Remote Desktop Session Host server** page, in the **Edit settings** area, under **RD Connection Broker**, double-click **Member of farm in RD Connection Broker**. The **Properties** dialog box appears.
3. On the **RD Connection Broker** tab, click **Change Settings**. The **RD Connection Broker Settings** dialog box appears.
4. Under **Remote Desktop Services**, click **Farm member**.
5. In the **RD Connection Broker** server name box, type **NYC-DC1**.
6. In the Farm name box, type **DemoRDFarm**, and then click **OK.**
7. On the **RD Connection Broker** tab, select the **Participate in Connection Broker Load-Balancing** check box. Notice that the Relative weight of this server in the farm is set to 100, by default.
8. Under **Select IP addresses to be used for reconnection**, click **10.10.0.11**, and then click **OK**.
9. Repeat the steps 1–8 on NYC-SVR2. In step 8, use the IP address of NYC-SVR2 (10.10.0.12).

Create a new Host named DemoRDFarm by using the DNS Manager.

1. On the **Start** menu of **NYC-DC1**, point to **Administrative Tools**, and then click **DNS**. The **DNS Manager** console appears.
2. In the console tree, expand **NYC-DC1,** expand **Forward Lookup Zones**, and then click **contoso.com**.
3. In the console tree, right-click **contoso.com**, and then click **New Host (A or AAAA**). The New Host dialog box appears.
4. In the **Name** box, type **DemoRDFarm**.
5. In the **IP Address** box, type **10.10.0.11**, and then click **Add Host.**
6. In the **DNS** message box, click **OK**.
7. In the **New Host** dialog box, click **Done**.
8. Repeat steps 3–7. In step 5, use the IP address,**10.10.0.12.**
9. Close all the windows.

Additional Reading

Installation and Configuration Considerations for RD Session Host Server

- about configuring RD Session Host server settings, go to

Lesson 2

Configuring and Managing Remote Desktop Licensing

Contents:

Question and Answers 182

Additional Reading 183

Question and Answers

Remote Desktop Services Client Access Licenses

Question: What is the main difference between Per Device and Per User CALs?

Answer: Per device CALs are issued to a client computer while per user CALs are issued to users. Also, unlike per device CALs, user CALs are not enforced.

Additional Reading

Overview of Remote Desktop Licensing

- about Remote Desktop Licensing, go to

Lesson 3

Managing Remote Desktop Client Connections

Contents:

Question and Answers 185

Detailed Demonstration Steps 186

Question and Answers

What Is SSO?

Question: What is the advantage of using SSO when you start a RemoteApp program?

Answer: By default, when you run a RemoteApp program on the RD Session Host server, you must provide credentials, even if you are already logged on to the client computer with the same credentials. By using single sign-on, you avoid this step and you can start the RemoteApp program without typing the user credentials again. Single sign-on is configured by using Group Policy and you can configure it to make the user experience of starting a RemoteApp program very similar to starting a locally installed application.

What Is Device Redirection?

Question: Can you redirect only the devices that are connected locally when you establish a remote connection?

Answer: You can redirect devices that are connected locally when you establish a remote connection, and devices to which you connect later after establishing a remote connection. You can achieve this by enabling the Devices that I plug in later option in Remote Desktop Connection client.

Detailed Demonstration Steps

Demonstration: Configuring Authentication and Encryption Parameters

Detailed Demonstration Steps

For this demonstration, start 6416D-NYC-DC1, 6416D-NYC-SVR1, and 6416D-NYC-SVR2. Log on to all virtual machines as **Contoso\Administrator** with the password **Pa$$w0rd**. You also need to complete the previous demonstrations, before you perform this demonstration.

1. On NYC-SVR1, click **Start**, click **Administrative Tools**, point to **RemoteDesktopServices**, and then click **Remote Desktop Session Host Configuration**. The **Remote Desktop Session Host Configuration** window appears.
2. On the **Configuration for Remote Desktop Session Host** server page, under **Connections**, right-click **RDP-Tcp**, and then click **Properties**. The **RDP-TcpProperties** dialog box appears.
3. On the **General** tab, in the **Encryptionlevel** list, click **High**.
4. To select a certificate, under **Certificate**, click **Select**. The **Windows Security** dialog box appears.
5. Under **Confirm Certificate**, click **NYC-SVR1.contoso.com**, and then click **OK**.
6. Select the **Allow connections only from computers running Remote Desktop with Network Level Authentication** check box. The **Remote Desktop Session Host Configuration** message box appears.
7. In the **Remote Desktop Session Host Configuration** message box, click **OK**.
8. In the **RDP-Tcp Properties** dialog box, click **OK**.
9. On the **Configuration for Remote Desktop Session Host server page**, under **Connections**, right-click **RDP-Tcp**, and then click **Properties**. The **RDP-Tcp Properties** dialog box appears.
10. On the **Log on Settings** tab, ensure that **Use client provided log on information** is selected, and then select the **Always prompt for password** check box.
11. In the **RDP-Tcp Properties** dialog box, click the **Security** tab.
12. In the **Remote Desktop Session Host Configuration** message box, click **OK**.
13. In the **Group or user names** list, click **Remote Desktop Users (NYC-SVR1\Remote Desktop Users)**.
14. Notice that the User Access and Guest Access is allowed for the Remote Desktop users. To select special permissions, click **Advanced**. The **Advanced Security Settings for RDP Tcp** dialog box appears.
15. On the **Permissions** tab, under **Permission entries**, double-click **Remote Desktop Users (NYC-SVR1\Remote Desktop Users)**. The **Permission Entry for RDP-Tcp** dialog box appears.
16. Notice that the Query Information, Log on, and Connect permissions are granted to the Remote Desktop users. Click **Cancel**.
17. In the **Advanced Security Settings for RDP-Tcp** dialog box, click **Cancel**.
18. In the **RDP-Tcp Properties** dialog box, click **Cancel**.

Demonstration: Configuring and Monitoring RD Resources with WSRM

Detailed Demonstration Steps

For this demonstration, start 6416D-NYC-DC1, 6416D-NYC-SVR1, and 6416D-NYC-SVR2. Log on to all virtual machines as **Contoso\Administrator** with the password **Pa$$w0rd**. You also need to complete the previous demonstrations, before you perform this demonstration.

1. On the **Start menu** of **NYC-SVR1**, point to **AdministrativeTools**, and then click **Windows SystemResource Manager**. The **Windows System Resource Manager** appears.
2. In the **Connect to Computer** dialog box, ensure that **This computer** is selected, and then click **Connect**.
3. In the console tree, right-click **Process Matching Criteria**, and then click **New Process Matching Criteria**.
4. In the **Criteria name** text box, type **RDGateway.**
5. Click **Add**
6. On **Add Rule** page, click **Select**.
7. On the **Add Registered Service** page, select **TS Gateway** from the list, and then click **OK** three times.
8. In the console tree, right-click **Resource Allocation Policies**, and then click **New Resource AllocationPolicy**. The **New Resource Allocation Policy** dialog box appears.
9. In the **Policy n**ame box, type **ResourceAllocation1**, and then click **Add**. The **Add or Edit ResourceAllocation** dialog box appears.
10. To create a CPU target resource allocation, on the **General** tab, in the **Process matching criteria** list, click **RDGateway**.
11. In the **Percentage of processor allocated for this resource** box, type **50**.
12. On the **Memory** tab, click **Use maximum committed memory for each process.**
13. In the **Maximum committed memory limit per process** box, type **100**.
14. In the **Add or Edit Resource Allocation** dialog box, click **OK**.
15. In the **New Resource Allocation Policy** dialog box, click **OK**.
16. Close the WSRM– [Windows System Resource Manager (Local)\Resource Allocation Polices] console.
17. In the Microsoft Management Console message box, click **No** to close the console without saving any changes.

Demonstration: Using Device Redirection

Detailed Demonstration Steps

For this demonstration, start 6416D-NYC-DC1, 6416D-NYC-SVR1and 6416D-NYC-CL1. Log on to all virtual machines as **Contoso\Administrator** with the password **Pa$$w0rd**. You also need to complete the previous demonstrations, before you perform this demonstration.

1. On NYC-CL1, click **Start**, point to **All Programs**, click **Accessories**, and then click **Remote Desktop Connection**.
2. In **Remote Desktop Connection**, click **Options**.

3. On the **General** tab, enter **NYC-SVR1** in the **Computer** field.
4. On the **Local Resources** tab, clear the **Printers** check box from the Local devices and resources section.
5. Click **More**, expand **Drives**, click **Local Disk (C:)**, and then click **OK**.
6. Click **Connect** in **Remote Desktop Connection**.
7. Click **Connect** again, and then enter the user credentials: **CONTOSO\administrator** and **Pa$$w0rd**.
8. Open Windows Explorer in the RD session, and then view the redirected local drive (drive C on NYC-CL1).
9. On NYC-CL1, view local drive C in Windows Explorer.
10. On NYC-CL1, in RD Session to NYC-SVR1, in Windows Explorer, point out that the files on the local computer are visible inside the session.
11. On NYC-CL1, log off from the RD Session, from NYC-SVR1.

Module Reviews and Takeaways

Review questions

Question: You installed RDS in a testing environment. After 120 days, you are no longer able to connect to the RDS server. What is the most probable reason for this?

Answer: The grace period has expired. You must activate the Licensing server and install CAL licenses.

Question:Can users access published RemoteApps from the Internet or from outside the internal network?

Answer: Yes. You can deploy RD Gateway together with RemoteApp programs. If you do that, users will have the same experience when running Remote App from internal and external networks.

Question: How is the use of RemoteApp and Desktop Connection different from simply accessing RemoteApp from RD Web Access?

Answer: RemoteApp and Desktop Connection is specific to Windows 7. You are configuring it from Control Panel, and it is dynamically updated from Remote Session Host server. Also, it installs shortcuts on the Start menu.

Question: What is the main purpose of Remote Desktop Connection Broker?

Answer: RD Connection Broker is a role service to allow a user to reconnect to an existing session in a load-balanced terminal server farm.

Common Issues Related to a Remote Desktop Services

Issue	Troubleshooting tip
RD Session Hosts in an RD Farm are not load balanced.	Check if DNS round robin is enabled in DNS Manager.
You cannot add RD Session Host server as a member of a farm managed by Remote Desktop Connection Broker.	Check if RD Session Host is a member of the Session Broker Computers group on RD Connection Broker.
Single sign-on for RDP sessions is not working.	Check if the certificate installed on Remote Desktop Session Host is valid and issued to a name that the client is using to connect.
Device redirection is not working.	Check if it is disabled on RD Session Host or in Group Policy.

Best Practices Related to a Remote Desktop Services

- If you have more than one RD Session Host server with same purpose, create a farm and manage it with RD Connection Broker.
- Restrict each user to one session on RD Session Host server to better control resources.
- Use the grace period for RD licensing to better evaluate license needs.
- Configure SSO for RemoteApp programs to enhance user experience.
- Consider security before allowing users to use device redirection.

Tools

Tool	Use for	Where to find it
RemoteApp and Desktop Connection	GUI tool for integrating RemoteApps and Desktop Connection with the Start menu	Control Panel
Remote Desktop Services Manager	GUI tool for administering Remote Desktop Services	Administrative Tools on the Start menu
Remote Desktop Session Host configuration tool	GUI tool for administering Remote Desktop Session Host servers	Administrative Tools on the Start menu
Remote Desktop Licensing Manager	GUI tool for administering Remote Desktop Licensing	Administrative Tools on the Start menu

Lab Review Questions and Answers

Question: What prevented you from activating RD Licensing Manager in Exercise 1?

Answer: To be able to activate RD Licensing Manager, you must have an Internet connection with Microsoft Clearinghouse or a telephone connection.

Question: What is the purpose of creating Process Matching criteria in WSRM?

Answer: With Process Matching Criteria, you are can identify a service that you want to use when you create the Resource Allocation Policy.

Question: Why did you get prompt for password when initiating the RDP connection, although you configured SSO on NYC-CL1?

Answer: Because the certificate on NYC-SVR1 and NYC-SVR2 is not configured with the name, RDFarm.contoso.com, and it is not on a trust list for NYC-CL1, the prompt appears.

Module 11

Installing and Configuring Web Servers and Applications with Internet Information Services 7.5

Contents:

Lesson 2: Configuring Web Applications and Sites **193**

Module Reviews and Takeaways **195**

Lab Review Questions and Answers **197**

Lesson 2

Configuring Web Applications and Sites

Contents:

Additional Reading 194

Additional Reading

What Is an Application Pool?

- Managing Application Pools in IIS 7
- Metabase Compatibility with IIS 7.0

Module Reviews and Takeaways

Review Questions

Question: What type of authentication is most commonly used on the Internet?

Answer: Anonymous. Most websites are accessible by any client and do not prompt for credentials.

Question: You have deployed nine web applications on the same server. Five of these applications are in one site, while four are in a different site. You have not modified the default application pool settings. One of the applications runs in classic mode. What is the minimum number of application pools you must configure?

Answer: Two. While it may be desirable to isolate each application, or site, by application pool, the restricting requirement is classic versus integrated mode, assuming that all of the integrated mode applications run the same .NET framework version.

Question: You want to remove an application pool from your server. What must you do before you remove the application pool?

Answer: You must assign applications or sites currently assigned to the application pool to other application pools before you can remove it.

Question: A developer wants to add a shopping component to a website. What should you do to ensure confidence and security for users to enter their credit card numbers into a web form?

Answer: Obtain and install a security certificate from a certification authority and employ an SSL-secured webpage.

Best Practices Related to Managing Web Servers and Websites

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

- The domain name restrictions rules restrict access by domain name. This rule significantly affects server performance because it requires a DNS lookup for every request.
- Employ minimal install to install only the bare minimum number of components. With fewer components installed, there is a smaller surface area available to attackers and there are fewer components to manage and maintain.
- Locate the log file on a secure, reliable drive. It should be stored in a directory other than %systemroot%.
- Monitor and manage the maximum number of log files to keep and the maximum size of the log files.

Tools

This is an optional section.

Tool	Use for	Where to find it
Internet Information Services (IIS) Manager	Editing IIS configuration	Administrative Tools
Appcmd.exe	Editing IIS configuration	Command-line

Tool	Use for	Where to find it
LogParser 2.2	Viewing IIS log files	Microsoft Download website
Internet Information Services (IIS) 6.0 Manager	Editing SMTP configuration	Administrative Tools
Netsh.exe	Configuring networking components	Command-line
Certificates snap-in	Managing certificates	Management console

Lab Review Questions and Answers

Question: In the lab, you enabled logging, but no user name was recorded in the log when a user accessed the website. Why?

Answer: Anonymous authentication has been configured, which is the default.

Question: How can you resolve this?

Answer: Enable another type of authentication, such as Integrated Windows Authentication (as this is an internal website).

Question: What should you do to make this change?

Answer: Install the Windows Authentication role service; it is not selected by default.

Question:If you deploy the SMTP Server feature to a computer that is Internet-facing, what should you be aware of?

Answer: The SMTP Virtual Server that is created by default is configured for anonymous authentication, but also for the setting that any computer that can successfully authenticate can relay, regardless of any specific relay settings.

Question: What should you do?

Answer: You should either change the authentication method, or deselect the option that allows relay after successful authentication, or both.

Question: Why was it necessary to obtain a certificate with the subject name of www.contoso.com?

Answer: Because the default server name, NYC-DC1.contoso.com, is not the name users will use to navigate to the intranet site. Consequently, they will receive a warning in their browsers that the subject name does not match that of the host.

Module 12

Configuring Storage Technologies in Windows Server® 2008

Contents:

Lesson 1: Configuring Distributed File System **199**

Lesson 2: Managing Storage with File System Resource Management **201**

Lesson 3: Implementing Classification Management and File Management Tasks **205**

Module Reviews and Takeaways **208**

Lab Review Questions and Answers **210**

Lesson 1

Configuring Distributed File System

Contents:

Additional Reading 200

Additional Reading

New Features in Windows Server 2008

- Enable Access-Based Enumeration on a Namespace
- Windows Server 2003 versus DFSUtil in Windows Server 2008
- Functionality of Dfsdiag

Lesson 2

Managing Storage with File System Resource Management

Contents:

Detailed Demonstration Steps 202

Detailed Demonstration Steps

Demonstration: How to Configure FSRM

Detailed demonstration steps

Note You require the 6416D-NYC-DC1 and 6416D-NYC-SVR1 virtual machines to complete this demonstration. Log on to the virtual machines as Contoso\Administrator with the password of Pa$$w0rd.

▶ Task 1: Use Server Manager to install the FSRM role service.

1. On NYC-SVR1, click **Start**, click **Administrative Tools**, and then click **Server Manager**.
2. In the Server Manager window, click Roles.
3. Under File Services, click Add Role Services.
4. On the Select Role Services page, select the **File Server Resource Manager** check box, and then click Next.
5. On the **Configure Storage Usage Monitoring** page, click the check box to select Local Disk (C:), and then click Next.
6. On the **Set Report Options** page, click **Next**.
7. On the **Confirm Installation Selections** page, click **Install**.
8. After the installation completes, click Close.
9. Close the Server Manager window.

▶ Task 2: View FSRM configuration options.

1. Click **Start**, click **Administrative Tools**, and then click **File Server Resource Manager**.
2. In the left pane in the File Server Resource Manager window, right-click File **Server Resource Manager (Local)**, and then click **Configure Options**.
3. Click each of the tabs in the File Server Resource Manager Options window, observing the options available in each tab. Close the File Server Resource Manager Options window.
4. In the left pane in the File Server Resource Manager window, expand each of the components and view the details for each sub-node.

▶ Task 3: Create a new quota template.

1. On NYC-SVR1, click **Start**, click **Administrative Tools**, and then click **File Server Resource Manager**.
2. In the **File Server Resource Manager** console tree, expand **Quota Management**, and then click **Quota Templates**.
3. Right-click **Quota Templates** and select **Create Quota Template**.
4. In the **Template name** field, type Monitor D: for Large Files
5. In the **Limit** field, type 1.
6. In the drop-down box to the right of the Limit field, select GB.

7. Select Soft quota. Allow users to exceed limit (use for monitoring).
8. Click **Add**.
9. On the **E-mail Message** tab, select both check boxes, and then click the **Event Log** tab. Click **Yes** at the File Server Resource Manager warning.
10. Select **Send warning to event log**, and then click **OK**. Again, click **Yes** to dismiss the warning about SMTP server configuration. If students are interested, show them how to configure the SMTP server used for sending notifications after this demonstration by setting File Server Resource Manager Options.
11. Click **OK** to close the **Create Quota Template** dialog box.

▶ Task 4: Create a new quota based on a quota template

1. In the details pane, right-click Monitor D: for Large files, and then click **Create Quota from Template**.
2. In the **Quota path** field, type D:\
3. Click Create.

▶ Task 5: Generate a quota notification.

1. Click **Start**, type cmd.exe in the Search programs and files field, and then press Enter.
2. Type d: and then press Enter.
3. Type fsutil file createnew largefile.txt 1300000000, and then press Enter.
4. Click **Start**, click **Administrative Tools**, and then click **Event Viewer**.
5. In Event Viewer, expand **Windows Logs**, and then click **Application**.
6. There should be an event with Event ID of 12325. Examine this event if it is listed. Otherwise, continue.
7. Close all open windows on NYC-SVR1.

▶ Task 6: Create a file group.

1. On NYC-SVR1, click **Start**, click **Administrative Tools**, and then click **File Server Resource Manager**.
2. In the **File Server Resource Manager** console tree, expand **File Screening Management**, and then click **File Groups**.
3. Right-click **File Groups** and then click **Create File Group**.
4. In the Create File Group Properties window, enter MPx Media Files into the File group name field.
5. In the Files to include field, type *.mp*, and then click Add.
6. In the Files to exclude field, type *.mpp, and then click Add.
7. Click OK.

▶ Task 7: Create a file screen template.

1. In the **File Server Resource Manager** console tree, click **File Screen Templates**.
2. Right-click **File Screen Templates**, and then click **Create File Screen Template**.
3. In the Create File Screen Template window, type Block MPx Media files into the **Template** name field.

4. Under Screening type, ensure that **Active screening. Do not allow users to save unauthorized files** is selected.
5. In the **File groups** section, select the **MPx Media Files File Group** check box.
6. Click the **Event Log** tab.
7. Select the **Send warning to event log** check box and then click OK.

▶ Task 8: Create a file screen using a file screen template

1. In the File Server Resource Manager, select and then right-click **File Screens**, and then click **Create File Screen**.
2. In the Create File Screen window, type D:\Labfiles\Mod12 in the File screen path field.
3. In the Create File Screen window, click the drop-down box under Derive properties from this file screen template (recommended), and click **Block MPx Media Files**.
4. Click **Create**.
5. Close File Server Resource Manager.

▶ Task 9: Test the file screen.

1. Click Start, and then click Computer.
2. In the left pane, click Allfiles (D:)
3. In the right pane, right-click the empty space, point to New, and select Text Document.
4. Rename New Text Document.txt to musicfile.mp3.
5. Right-click **music file.mp3** and then click **Copy**.
6. In the left pane, expand **All files (D:)**, expand **Labfiles**, right-click **Mod12**, and then click **Paste**.
7. A warning appears that the destination folder access is denied. Click **Cancel** and then close the explorer window.

Note Leave all virtual machines in their current state for the subsequent demonstrations.

Lesson 3

Implementing Classification Management and File Management Tasks

Contents:

Detailed Demonstration Steps 206

Detailed Demonstration Steps

Demonstration: How to Configure Classification Management

Detailed demonstration steps

Note You require the 6416D-NYC-DC1 and 6416D-NYC-SVR1 virtual machines to complete this demonstration. Log on to the virtual machines as Contoso\Administrator with the password Pa$$w0rd. These should be running from the previous demonstration.

▶ Task 1: Create a Classification Property.

1. On NYC-SVR1, click **Start**, click **Administrative Tools**, and then click **File Server Resource Manager**.
2. Expand the Classification Management node, and then click **Classification Properties**.
3. Right-click **Classification Properties** and then click **Create Property**.
4. In the Create Classification Property Definition window, type Confidential in the Property name field, and type Assigns a confidentiality value of Yes or No in the Description field.
5. Under Property type, click the drop-down box, and select **Yes/No**.
6. Click **OK**.

▶ Task 2: Create a Classification Rule.

1. Click the **Classification Rules** node.
2. Right-click the **Classification Rules** node, and then click **Create a New Rule**.
3. In the **Rule name** field, type Confidential Payroll Documents.
4. In the **Description** field, type Classify documents containing the word "payroll" as confidential.
5. In the **Scope** section, click the Add button.
6. In the Browse for Folder window, expand **Allfiles (D:)**, expand **Labfiles**, click **Mod12**, and then click **OK**.
7. In the Classification Rule Definitions window, click the **Classification** tab.
8. In the Classification mechanism area, click the drop-down box, and click **Content Classifier**.
9. In the Property name section, choose a Property name of Confidential and a Property value of Yes, and then click the Advanced button.
10. In the Additional Rule Parameters window, click the **Additional Classification Parameters** tab.
11. On the **Additional Classification Parameters** tab, double-click in the blank cell below the Name column and type String.
12. Double-click in the Value column and type payroll.
13. Click OK.
14. In the Classification Rule Definitions window, click **OK**.

▶ Task 3: Modify the Classification Schedule.

1. Right-click the **Classification Rules** node and then click **Configure Classification Schedule**.
2. In the File Server Resource Manager Options window, ensure the **Automatic Classification** tab is selected, and click the **Create** button.
3. In the Schedule window, click the **New** button.
4. In the **Start time** field, type 8:30 AM and click **OK**.
5. In the File Server Resource Manager Options window, click **OK**.
6. Right-click the **Classification Rules** node, and then click **Run Classification With All Rules Now**.
7. In the Run Classification window, select Wait for classification to complete execution, and then click **OK**.
8. View the report and ensure that January.txt is listed at the bottom of the report.
9. Navigate to the D:\Labfiles\Mod12\Data folder and view the contents of January.txt.
10. Close all open windows on NYC-SVR1.

 **Note** Revert all virtual machines.

Module Reviews and Takeaways

Review Questions

Question: 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.

Question: What are the primary benefits of a SAN over DAS?

Answer: Highly effective resource sharing; better storage utilization; hardware consolidation and availability.

Question: What is the primary advantage of a domain-based DFS namespace?

Answer: Fault tolerance of the namespace can be provided without the need to implement clustering of the file services role.

Question: How can fault tolerance of the content in a DFS namespace be provided?

Answer: By adding multiple namespace targets and configuring replication.

Question: In what ways can Classification Management and File Management Tasks decrease administrative overhead when dealing with a complex file and folder structure?

Answer: Classification Management and File Management Tasks can allow administrators to automate the manual classification and modification of files on a file server. Rather than manually inspecting files and performing manual file operations, administrators can set up a file classification infrastructure to classify files and then perform the necessary operations on those files with file management tasks to ensure that capacity issues do not occur on those volumes.

Common Issues Related to Storage Technologies

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
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.

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 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

This is an optional section.

Tool	Use for	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

Question: 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)

Question: 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.

Question: 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 13

Configuring High Availability in Windows Server 2008

Contents:

Lesson 1: Configuring Network Load Balancing **212**

Lesson 2: Overview of Windows Server 2008 Failover Clusters **217**

Lesson 3: Preparing for Failover Clusters **220**

Lesson 4: Creating and Configuring Failover Clusters **224**

Module Reviews and Takeaways **229**

Lab Review Questions and Answers **231**

Lesson 1

Configuring Network Load Balancing

Contents:

Question and Answers 213

Detailed Demonstration Steps 214

Additional Reading 216

Question and Answers

What Is Network Load Balancing?

Question: Are you already using Network Load Balancing? If yes, for what purpose?

Answer: Answers may vary. If some students already use NLB, most probably, it will be for web servers.

Detailed Demonstration Steps

Demonstration: Implementing Network Load Balancing

Detailed Demonstration Steps

1. Start the virtual machines, **6416D**-**NYC-DC1**,**6416D**-**NYC-SVR1**, and**6416D**-**NYC-SVR2.**
2. Log on to all three machines by using the following credentials:
   - User name: **Administrator**
   - Password: **Pa$$w0rd**
   - Domain: **Contoso**
3. On NYC-SVR1, click **Start**, point to **Administrative Tools**, and then click **ServerManager**.
4. In the navigation pane, click **Features**. In the results pane, click **Add Features**, and in the **Add Features Wizard**, select the **Network Load Balancing** check box. Click **Next**, click **Install**, and then click **Close**.
5. Repeat steps 3 and 4 on NYC-SVR2.
6. Switch back to NYC-SVR1.
7. Click **Start**, click **Administrative Tools**, and then click **Network Load Balancing Manager**.
8. Right-click **Network Load Balancing Clusters**, and then click **New Cluster**.
9. 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, **NYC-SVR1**, and then click **Connect**.
10. Select the interface that you want to use with the cluster, **Local Area Connection 2,** and then click **Next**. (The interface hosts the virtual IP address and receives the client traffic to load balance.)
11. In **New Cluster: 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**.
12. Click **Next** to continue.
13. In **New Cluster :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. Enter **10.10.0.100**, with a subnet mask of **255.255.0.0**, and then click **OK**.
14. Click **Next** to continue.
15. In **New Cluster:Cluster Parameters**, type the Full Internet name that users will use to access this NLB cluster. You can type **contoso-NLB.contoso.com**.
16. Under **Cluster operation mode**, click **Multicast** to specify that a multicast Media Access Control (MAC) address should be used for cluster operations.
17. Click **Next** to continue.
18. In New Cluster: Port Rules, click **Finish**.

19. In Network Load Balancing Manager, expand Network Load Balancing Clusters, right-click **Contoso-NLB.contoso.com (10.10.0.100)**, and then click **Add Host to Cluster**.
20. In Add Host to Cluster: Connect, in the Host box, type **NYC-SVR2**, and then click **Connect**.
21. Click **Next** to continue.
22. In **Add Host to Cluster : Host Parameters**, click **Next**.
23. In the **Add Host to Cluster : Port Rules**, click **Finish**.

Remove the Network Load Balancing cluster.

1. In Network Load Balancing Manager, right-click **NYC-SVR1 (Local Area Connection 2)**,and then click **Delete Host**.
2. In the **Network Load Balancing Manager** dialog box, click Yes.
3. Repeat for NYC-SVR2 (Local Area Connection 2).
4. Close all open windows.

Additional Reading

What Is Network Load Balancing?

- about Network Load Balancing, go to:
- about Network Load Balancing, go to:

Windows Server 2008 NLB Features

- about NLB features, go to:

Configuring Network Load Balancing

- about configuring NLB, go to:

Lesson 2

Overview of Windows Server 2008 Failover Clusters

Contents:

Question and Answers 218

Additional Reading 219

Question and Answers

Improvements in Failover Clustering in Windows Server 2008

Question: Why is the validation wizard important?

Answer: The validation wizard minimize the chance for incorrect cluster configuration. It performs a series of tests to ensure that the node satisfies the conditions for creating a cluster.

Failover Clusters and Networks

Question: Why it is recommended to have separate networks for intra-cluster communication and communication with clients?

Answer: To maintain redundancy for cluster communication.

Types of Quorum Modes

Question: What is specific to the No Majority: Disk Only quorum mode?

Answer: In this quorum mode, the quorum-shared disk can veto all other possible votes, no matter how many nodes are in the cluster.

Additional Reading

Improvements in Failover Clustering in Windows Server 2008

- about improvements in failover clustering, go to:

What Is Quorum?

- about quorum, go to:

Choosing a Quorum Mode

- about quorum modes, go to:

Lesson 3

Preparing for Failover Clusters

Contents:

Question and Answers 221

Detailed Demonstration Steps 222

Additional Reading 223

Question and Answers

Demonstration: Running the Validate a Configuration Wizard

Question: Which 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.

Detailed Demonstration Steps

Demonstration: Running the Validate a Configuration Wizard

Detailed Demonstration Steps

For this demonstration, start 6416D-NYC-DC1, 6416D-NYC-SVR1, 6416D-NYC-SVR2, and 6416D-NYC-RTR. Log on to all virtual machines as **Contoso\Administrator** with the password **Pa$$w0rd**.

1. On both NYC-SVR1 and NYC-SVR2, open Server Manager and install the **Failover Clustering** feature.
2. On NYC-SVR1, click **Start**, point to **Administrative Tools**, and then click **Failover Cluster Manager**.
3. In the **Failover Cluster Manager** snap-in, in the console tree, ensure that Failover Cluster Manager is selected, and then, under **Management**, click **Validate a Configuration**.
4. Click **Next**.
5. In the **Enter Name** field, type **NYC-SVR1**.
6. Click **Add**.
7. In the **Enter Name** field, type **NYC-SVR2**.
8. Click **Add**, and then click **Next**.
9. Verify that **Run all tests (recommended)** is selected, and then click **Next**.
10. In the Confirmation window, click **Next**.
11. Wait for the validation tests to finish, and then, in the **Summary** window, click **View Report**.

Note Point out to students that the group of tests that deal with disk storage has failed, but that is expected because you have not configured any storage disks yet.

Additional Reading

Failover Cluster Server Hardware Requirements

- about Server Hardware Requirements, go to:

Lesson 4

Creating and Configuring Failover Clusters

Contents:

Detailed Demonstration Steps 225

Detailed Demonstration Steps

Demonstration: Creating a Cluster

Detailed Demonstration Steps

For this demonstration, start 6416D-NYC-DC1, 6416D-NYC-SVR1, 6416D-NYC-SVR2, and 6416D-NYC-RTR. Log on to all virtual machines as **Contoso\Administrator** with the password **Pa$$w0rd**.

1. On **NYC-RTR** 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 local port=3260

   netsh advfirewall firewall add rule name="Microsoft iSCSI Software Target Service-TCP-135" dir=in action=allow protocol=TCP local port=135

   netsh advfirewall firewall add rule name="Microsoft iSCSI Software Target Service-UDP-138" dir=in action=allow protocol=UDP local port=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
2. On NYC-SVR1, click **Start**, point to **Administrative Tools**, and then click **iSCSI Initiator**.
3. In the Microsoft iSCSI dialog box, click **Yes**.
4. On the Discovery tab, click **Discover Portal**.
5. In the **IP address or DNS name** field, type **10.10.0.1**, and then click **OK**.
6. On the **Targets** tab, click **Refresh**.
7. Select iqn.1991-05.com.microsoft:NYC-rtr-lun-01-target in the targets list, and then click **Connect**.
8. Select **Add this connection to the list of Favorite Targets**, and then click **OK**.
9. On NYC-SVR2, click **Start**, point to **Administrative Tools**, and then click **iSCSI Initiator**.
10. In the **Microsoft iSCSI** dialog box, click **Yes**.
11. On the **Discovery** tab, click **Discover Portal**.
12. In the **IP address or DNS name** field, type **10.10.0.1**, and then click **OK**.
13. On the **Targets** tab, click **Refresh**.
14. Select iqn.1991-05.com.microsoft:NYC-RTR-LUN-02-target in the targets list, and then click **Connect**.
15. Select **Add this connection to the list of Favorite Targets**, and then click **OK**.
16. On NYC-SVR1, open Server Manager.
17. Expand **Storage**, and then click **Disk Management**.
18. Right-click **Disk 2**, and then click **Online**.
19. Right-click **Disk 2**, and then click **Initialize disk**. In the **Initialize Disk** dialog box, click **OK**.

20. Right-click the unallocated space next to Disk 2, and then click **New Simple Volume**.
21. On the **Welcome** page, click **Next**.
22. On the **Specify Volume Size** page, click **Next**.
23. On the **Assign Drive Letter or Path** page, click **Next**.
24. On the **Format Partition** page, in the **Volume Label** field, type **Data**. Select the **Perform a quick format** check box, and then click **Next**.
25. Click **Finish**.
26. On NYC-SVR2, open Server Manager.
27. Expand **Storage**, and then click **Disk Management**.
28. Right-click **Disk Management**, and then click **Refresh**.
29. Right-click **Disk 2**, and then click **Online**.
30. On NYC-SVR1, click **Start**, point to **Administrative Tools**, and then click **Failover Cluster Manager**.
31. In the Failover Cluster Manager action pane, click **Validate a Configuration**.
32. Click **Next**.
33. In the **Enter Name** field, type **NYC-SVR1**.
34. Click **Add**.
35. In the **Enter Name** field, type **NYC-SVR2**.
36. Click **Add**, and then click **Next**.
37. Verify that **Run all tests (recommended)** is selected, and then click **Next**.
38. In the Confirmation window, click **Next**.
39. Wait for the validation tests to finish, and then, in the Summary window, click **View Report**.
40. Verify that all tests completed successfully.
41. Close Microsoft Internet Explorer.
42. In the Summary window, click **Finish**.
43. On NYC-SVR1, in **Failover Cluster Management,** in the **Management** section of the center pane, select **Create a Cluster**.
44. Read the Before You Begin information.
45. Click **Next**, type **NYC-SVR1**, and then click **Add**. Type **NYC-SVR2**, and then click **Add**.
46. Verify the entries, and then click **Next**.
47. In the Access Point for Administering the Cluster section, enter **Cluster1** for the cluster name.
48. Under **Address**, type **10.10.0.125** as the IP address, and then click **Next**.
49. In the **Confirmation** dialog box, verify the information, and then click **Next**.
50. On the **Summary** page, click **Finish** to return to the Failover Cluster Management snap-in.

Demonstration: Clustering Print Services

Detailed Demonstration Steps

1. On NYC-SVR1, open Server Manager.
2. Run the **Add Roles Wizard**.
3. Select the **Print and Document Services** role and install it.
4. Repeat these steps on NYC-SVR2.
5. On NYC-SVR1, open Server Manager.
6. Expand **Storage**, and then click **Disk Management**.
7. Right-click **Disk 3**, and then click **Online**.
8. Right-click **Disk 3**, and then click **Initialize disk**. In the **Initialize Disk** dialog box, click **OK**.
9. Right-click the unallocated space located next to Disk 3, and then click **New Simple Volume**.
10. On the **Welcome** page, click **Next**.
11. On the **Specify Volume Size** page, click **Next**.
12. On the **Assign Drive Letter or Path** page, click **Next**.
13. On the **Format Partition** page, in the **Volume Label** field, type **Printer1**. Select **Perform a quick format**, and then click **Next**.
14. Click **Finish**.
15. On NYC-SVR2, open Server Manager.
16. Expand **Storage**, and then click **Disk Management**.
17. Right-click **Disk Management**, and then click **Refresh**.
18. Right-click **Disk 3**, and then click **Online**. If a Disk Management error message appears, click **OK**.
19. On NYC-SVR1, click **Start**, click **Administrative Tools**, and then click **Failover Cluster Management**. If the **User Account Control** dialog box appears, confirm that the correct action is displayed, and then click **Continue**.
20. In the console tree, expand **Cluster1**, and then click **Storage**.
21. In the Actions pane, click **Add a disk**, and then click **OK**.
22. Click **Cluster1.contoso.com**, and then, in the Actions pane, click **Configure a Service or Application**.
23. Review the text on the first page of the wizard, and then click **Next**.
24. Click **Print Server**, and then click **Next**.
25. Type **NYC-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**.
26. Select **Cluster Disk 2** as the storage volume for the print server, click **Next**, and then click **Next**.
27. 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.
28. Click **Finish**.

29. In the console tree, expand **Services and Applications**, and verify that the clustered print server NYC-Print has been created.
30. In the console tree, click **NYC-Print**. In the center pane, identify the current owner of the service.
31. In the Actions pane, click **Move this service or application to another node**.
32. Click **Move to node *servername***, where ***servername*** is the cluster node that is not the current owner.
33. In the **Please confirm action** dialog box, click **Move NYC-Print to *servername***.
34. Wait for the service to move to the new owner. Then, in the center pane, verify that NYC-Print now shows the new current owner and that all components are online.

Demonstration: Configuring Failover Clusters

Detailed Demonstration Steps

1. Log on to **NYC-DC1**.
2. Using Windows Explorer, create a shared folder named **FSW** on drive C. Give Authenticated Users full control permission.
3. Log on to **NYC-SVR1**.
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 **\\NYC-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

Question: 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.

Question: 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.

Question: 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. If the computer object of the cluster does not have the appropriate permissions, it cannot create or update the computer object for the clustered service or application.	Ensure 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.	Ensure that the cluster service is running on all nodes.

Best Practices Related to Failover Clustering

- Ensure 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.

- Ensure that 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 for	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

Question: 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.

Question: After running the Validate a Configuration Wizard, how can you resolve the network communication single point of failure?

Answer: You can resolve the network communication single point of failure by adding network adapters on a separate network to provide communication redundancy between cluster nodes.

Question: In which 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 ensure that the failback does not interfere with client connections, backup windows, or other maintenance that a failback would interrupt.

Module 14

Configuring Virtualization in Windows Server® 2008

Contents:

Lesson 1: Hyper-V™ Overview **233**

Lesson 2: Installing and Configuring Hyper-V and Virtual Machines **235**

Lesson 4: High Availability in a Hyper-V Environment **240**

Lesson 5: Implementing Virtual Desktop Infrastructure **242**

Module Reviews and Takeaways **244**

Lab Review Questions and Answers **246**

Lesson 1

Hyper-V™ Overview

Contents:

Question and Answers 234

Question and Answers

What Is Hyper-V?

Question: What is the main benefit of using a Type 1 hypervisor versus previous Microsoft virtualization solutions that used Type 2 hypervisors?

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 Features and Benefits

Question: Which features of Hyper-V are most important for your production environment? Why?

Answer: Answers may vary.

Lesson 2

Installing and Configuring Hyper-V and Virtual Machines

Contents:

Question and Answers 236

Detailed Demonstration Steps 237

Question and Answers

Overview of User Settings for Hyper-V

Question: Why should you clear saved credentials?

Answer: You should clear saved credentials for security considerations. Only authorized personnel should be able to access Hyper-V virtual machines.

Virtual Network Settings for Hyper-V

Question: Which type of network allows a virtual machine to access a physical network? In what scenarios would you use this type of network?

Answer: External network enables a virtual machine to access a physical network. In this case, this enables the virtual machine to communicate on the physical network or outside the corporate environment.

Creating and Configuring Virtual Hard Disks

Question: What's the appropriate scenario for using differencing hard disks?

Answer: Differencing virtual hard disks should be used when you want to perform testing and save various configurations in separate systems.

Detailed Demonstration Steps

Demonstration: Configuring Virtual Networks

Detailed Demonstration Steps

Create a new internal virtual network

1. On a host machine, in **Hyper-V Manager**, in the Actions pane, click **Virtual Network Manager**.
2. In the Virtual Network Manager window, click **Internal** and then click **Add**.
3. In the **Name** field, type **Internal Network 2**, and then click **OK**.
4. Click **Start**, right-click **Network**, and then click **Properties**.
5. In the Network and Sharing Center window, click **Change adapter settings**.
6. Right-click the **Local Area Connection** that is connected to the Internal Network 2, and then click **Properties**.
7. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**. Verify that no IP address is configured, and then click **Cancel**. In order for the host computer to communicate with the virtual machines using this network, you need to configure the network adapter with an IP address configuration that is able to communicate with the virtual machines.
8. Close the **Local Area Connection** dialog box, and then close the **Network Connections** window.

Configure the MAC address range

1. In **Hyper-V Manager**, in the Actions pane, click **Virtual Network Manager**.
2. In the Virtual Network Manger window, click **MAC Address Range**.
3. Beside **Maximum**, increase the value of the fifth pane by one, and then click **OK**.

Demonstration: Managing Virtual Hard Disks

Detailed Demonstration Steps

Create a new virtual hard disk

1. On the host machine, 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. Show students all options for creating a new virtual hard drive. Finally, create a 1GB fixed size disk named TestVHD.vhd and place it to : C:\Program Files\Microsoft Learning\6416\Drives
4. After you have finished configuring the virtual hard disk, click **Finish**.

Attach a virtual hard disk to a running virtual machine

1. Open the Hyper-V Manager console. Make sure that NYC-CL1 virtual machine is not running.
2. Right click **6416D-NYC-CL1** virtual machine and click **Settings**
3. In the left pane click **Add Hardware**, and in the right pane click **SCSI Controller** and click **Add**.

4. Click **OK**.
5. Start the 6416D-NYC-CL1 virtual machine. Log on as Contoso\Administrator with password Pa$$w0rd.
6. In Hyper-V Manager, right-click 6416D-NYC-CL1, and then click **Settings**. Click **SCSI Controller**, and in the right pane, click **Hard Drive**, and then click **Add**.
7. Click **Browse**, navigate to C:\Program Files\Microsoft Learning\6416D\Drives, select **TestVHD.vhd**, and then click **Open**.
8. Click **OK**.
9. Switch to the 6416D-NYC-CL1 virtual machine desktop, click **Start**, right-click **Computer**,and click **Manage**.
10. Click **Disk Management**.
11. In the Initialize Disk window, click **OK**
12. Right-click new disk drive and select **New Simple Volume**. Click **Next** four times,and then click **Finish**
13. Open **Windows Explorer** on **NYC-CL1** and verify that disk is present.
14. Open a new disk in **Explorer** and create a new text file on it.
15. Switch to the Hyper-V Manager console.
16. Right-click 6416D-NYC-CL1, and then click **Settings**. Expand **SCSI Controller**, click **Hard Drive** under the SCSI Controller node, click **Remove** in the right pane, and then click **OK**.
17. Switch to Disk Management on the host computer. Right-click **Disk Management**, and then click **AttachVHD**. Browse to, and select, **C:\Program Files\Microsoft Learning\6416\Drives\TestVHD.vhd**, click **Open**, and then click **OK**.
18. In Windows Explorer, open the new drive, and ensure that it contains all of the files.

Demonstration: Creating and Configuring Virtual Machines

Detailed Demonstration Steps

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**.

Lesson 4

High Availability in a Hyper-V Environment

Contents:

Question and Answers 241

Question and Answers

Options for Providing High Availability for Virtualization

Question: You are planning to provide high availability to the following applications: Intranet site, Microsoft Exchange Server® 2010 Hub Transport server, and an Active Directory® Domain Services (AD DS) domain controller. Which of the high availability options can you use for each application?

Answer: For the intranet website, you could use NLB or guest clustering. For the Exchange Server, you could use host clustering. For the AD DS domain controller, you could use host clustering.

Lesson 5

Implementing Virtual Desktop Infrastructure

Contents:

Question and Answers 243

Question and Answers

Types of VDI Deployment

Question: What is the main difference between personal virtual desktops and pooled virtual desktops?

Answer: Personal virtual desktops are virtual machines that you assign to a user within your organization, and users always access the same virtual machine. Pooled virtual desktops are groups of virtual machines that you configure identically, and users can connect to any virtual machine in the pool.

Module Reviews and Takeaways

Review questions

Question: What are the main architectural changes in Hyper-V compared with Virtual PC or Virtual Server?

Answer: Hyper-V is using Hypervisor Type-1 while older solutions, such as Virtual PC and Virtual Server, are using Hypervisor Type-2. Hyper-V is a hardware-based virtualization solution, and Virtual PC is software-based solution that uses hardware emulation

Question: List the mandatory requirements for installation of the Hyper-V role.

Answer: You must have 64-bit processor, hardware support for virtualization, execute disable bit functionality configured in BIOS, and supported version of Windows Server 2008.

Question: What types of high availability are supported in the Hyper-V environment?

Answer: Hyper-V environment supports Failover Clustering (on host and guest level) and Network Load Balancing (on guest level)

Question: List some of the most important improvements to Hyper-V in Windows Server 2008 R2

Answer: Some of the most important improvements include Live Migration support for jumbo frames, and dynamic virtual machine storage

Question: Can you assign the same virtual machine to more than one user?

Answer: No, you can assign one virtual machine to only one user at a time

Question: How do you preserve user data in the virtual desktop pool scenario?

Answer: By using technologies such as Roaming Profiles and Folder Redirection.

Common Issues related to a Hyper-V

Issue	Troubleshooting tip
The virtual machine uses too much memory with Dynamic Memory enabled	If a virtual machine with Dynamic Memory–enabled appears to use too much memory, or does not release memory when the physical computer does not have enough available memory, you can limit the amount of memory used by the virtual machine by setting a lower value for the Maximum RAM setting. You may notice that the amount of RAM reported by Task Manager in the guest operating system does not decrease when a virtual machine uses less RAM. This occurs because the driver reports the maximum amount of memory that the guest operating system has used since it was started.
Available memory is too low in the management operating system	Hyper-V automatically calculates an amount of memory to reserve for exclusive use by the management operating system. This memory is used to run virtualization services. If the computer is part of a failover cluster, Hyper-V also reserves enough memory to run the failover cluster services. However, if the management operating system sums other roles or features, the amount of

Issue	Troubleshooting tip
	reserved memory might be too low. You can specify a larger amount of memory by modifying the registry.
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.

Best Practices related to a Hyper-V

- Use high availability technologies, such as Live Migration for Hyper-V.
- Configure personal virtual desktops to go in saved state mode after the user logs off. This optimizes usage of system resources.
- 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.

Tools

Tool	Use for	Where to find it
Hyper-V Manager	Creating and Managing virtual machines	Administrative Tools
Remote Server Administration Tools	Remote Management of Windows Servers	Microsoft Download Center

Lab Review Questions and Answers

Question: 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

Question: What different types of virtual hard disks does Hyper-V support?

Answer: Dynamically expanding disks, Differencing disks, Fixed size disks, pass-through disks.

Question: 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.

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:

1. Document or CD part number
2. Page number or location
3. 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.