Microsoft®

OFFICIAL MICROSOFT LEARNING PRODUCT

6421B

Configuring and Troubleshooting a Windows Server® 2008 Network Infrastructure

Product Number: 6421B

Part Number: X17-66521

Released: 5/2011

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

Planning and Configuring IPv4

Contents:

Lesson 1

Planning an IPv4 Network Infrastructure

Contents:

Question and Answers

Plan an IPv4 Addressing Scheme

Question: What is the subnet address for the following host: 192.168.16.17/28?

Answer: 192.168.16.16. The 28 signifies that only 4 host bits are available. With four bits in the significant octet for the subnet mask, the mask would be 255.255.255.240. 240 yields up the first subnet of 16, with the next subnet of 32, 48 and 64… The first host in subnet 16 is 17. Thus, 192.168.16.17 is the first host. The last host in this subnet is 30, because 192.168.16.31 is the broadcast address for subnet 16.

Discussion: Selecting an Appropriate Addressing Scheme

Question: Contoso.com has implemented IPv4 throughout the organization. It is currently implementing a new head office building. The office will host 5,000 computers that are distributed fairly evenly across 10 floors of these offices. What address class would suit this scenario?

Answer: Any class would be suitable with CIDR; however, a class B network with subnetting is the most logical choice.

Question: Analysis of the network traffic at the existing head office shows that the maximum number of hosts for each subnet should be around 100. How many subnets are required, and assuming a network address for the whole site of 172.16.0.0/16, what mask should you use to ensure sufficient support for the required subnets?

Answer: At least 50 subnets are needed. To express 50 subnets, you will need 6 bits in the mask. 2^6 yields 64, while 2^5 provides only 32 subnets.

Question: Assuming the network address for the head office is 172.16.0.0/19, what mask would you assign to each subnet?

Answer: The mask would be 25 bits, and would be expressed in decimal as 255.255.255.128.

Question: How many hosts can you have in each subnet based on your selected mask?

Answer: There are 7 bits remaining for hosts, which allows for 2^7-2 hosts, which is 126. If the subnet mask was 26 bits, that would provide for only 62 hosts and the requirement is for a maximum of 100. However, a mask of 26 bits would support 128 subnets and can be considered as a valid configuration.

Question: Assuming you implement the mask that you determined for each subnet, what would the first subnet address be?

Answer: With a 6 bit subnet mask, the actual decimal mask would be 255.255.255.128. The first subnet would be 172.16.0.0/26. If you opted for a 7 bit mask, then again, the first subnet would be 172.16.0.0/27, but the decimal mask would be 255.255.255.192.

Question: What are the first and last host addresses for the first subnet?

Answer. With a 6 bit subnet mask, the first host in the first subnet would be 172.16.0.1/26 and the last host would be 172.16.0.126/26. Using a 7 bit mask, the first host would be 172.16.0.1/27, while the last host would be 172.16.0.62/27.

Lesson 2

Overview of Name Resolution Services in an IPv4 Network Infrastructure

Contents:

Additional Reading

Name Resolution with WINS

- DNS Server GlobalNames Zone Deployment documentation from Microsoft

Lesson 3

Configuring and Troubleshooting IPv4

Contents:

Detailed Demonstration Steps

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

Demonstration Steps

Note You require the 6421B-NYC-DC1, 6421B-NYC-SVR1, and 6421B-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**. Start the domain controller and the client virtual machine, but do not start the server until prompted to do so.

▶ 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 the **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 **6421B-NYC-SVR1**, and in the Actions pane, click **Start**.
8. In the Action spane, click **Connect**. Wait until the virtual machine starts.
9. Log on using the following credentials:User name: **Administrator**
   - Password: **Pa$$w0rd**
   - Domain: **Contoso**
10. Click **Start**, and in the **Search** box, type **cmd.exe** and press ENTER.
11. In the Command Prompt, type ping **NYC-DC1** and press ENTER.

▶ 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).

▶ 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 read **("contoso")** and then click **Apply**.
5. Several frames should be returned. Go through each in turn and describe the contents.

▶ 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 to their original state for the subsequent modules.

Module Reviews and Takeaways

Review questions

Question: Your organization intends to use IPv4 for its branch offices. There are a large number of hosts and subnets required. Which private network address would you recommend?

Answer: 10.0.0.0/8 or 172.16.0.0/12.

Question: Your organization has a line of business application that uses NetBIOS names. A relatively few people use this application and you are reluctant to implement WINS. What alternative does Windows Server 2008 provide?

Answer: Implement the GlobalNames zone in DNS.

Question: Your Windows 7 client is unable to properly connect to a Windows Server. You suspect a name resolution problem. What two utilities enable you to troubleshoot name resolution from a client computer?

Answer: ipconfig.exe and nslookup.exe.

Lab Review Questions and Answers

Question: In the lab, you used the graphical interface to configure the IPv4 address on NYC-CL2. What else could you have used?

Answer: Netsh

Question: What syntax would you have used to achieve this?

Answer: Netsh interface ipv4 set address name="Local Area Connection" source=static addr=172.16.16.3 mask=255.255.255.0 gateway=172.16.16.1 gwmetric=1.

Module 2

Configuring and Troubleshooting DHCP

Contents:

Lesson 1

Overview of the DHCP Server Role

Contents:

Detailed Demonstration Steps

Demonstration: How to Add the DHCP Server Role

Demonstration Steps

Note You require the 6421B-NYC-DC1, 6421B-NYC-SVR1, and 6421B-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**.

▶ Install and authorize the DHCP Server role

1. Switch to the NYC-SVR1 computer.
2. On the **Taskbar**, click **Server Manager**.
3. In Server Manager, in the navigation pane, click **Roles**, and then in the right-pane, click **Add Roles**.
4. In the Add Roles Wizard, click **Next**.
5. On the **Select Server Roles** page, select the **DHCP Server** check box and then click **Next**.
6. On the **Introduction to DHCP Server** page, click **Next**.
7. On the **Select Network Connection Bindings** page, click **Next**.
8. On the **Specify IPv4 DNS Server Settings** page, click **Next**.
9. On the **Specify IPv4 WINS Server Settings** page, click **Next**.
10. On the **Add or Edit DHCP Scopes** page, click **Next**.
11. On the **Configure DHCPv6 Stateless Mode** page, click **Disable DHCPv6 stateless mode for this server**, and then click **Next**.
12. On the **Authorize DHCP Server** page, click **Next**.
13. On the **Confirm Installation Selections** page, click **Install**.
14. On the **Installation Results** page, click **Close** and then close Server Manager.

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

Additional Reading

How DHCP Allocates IP Addresses

- Microsoft TechNet: DHCP Resources

How DHCP Lease Generation Works

- Microsoft TechNet: How DHCP Technology Works

How DHCP Lease Renewal Works

- Microsoft TechNet: How DHCP Technology Works

DHCP Server Authorization

- Microsoft TechNet: DHCP Resources
- Microsoft TechNet: Networking Collection

Lesson 2

Configuring DHCP Scopes

Contents:

Detailed Demonstration Steps

Demonstration: How to Configure DHCP Scopes

Demonstration Steps

Note You require the 6421B-NYC-DC1, 6421B-NYC-SVR1, and 6421B-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**. The virtual machines should still be running from the preceding demonstration.

▶ Create an IPv4 scope

1. Switch to the NYC-SVR1 computer.
2. Click **Start**, point to **Administrative Tools**, and then click **DHCP**.
3. In DHCP, in the navigation pane, expand **nyc-svr1.consoto.com**, expand **IPv4**, right-click **IPv4**, and then click **New Scope**.
4. In the New Scope Wizard, click **Next**.
5. On the **Scope Name** page, in the **Name** box, type **Head Office Scope 1** and then click **Next**.
6. On the **IP Address Range** page, complete the page using the following information and then click **Next:**
   - Start IP address: **10.10.0.50**
   - End IP address: **10.10.0.100**
   - Length: **16**
   - Subnet mask: **255.255.0.0**
7. On the **Add Exclusions and Delay** page, click **Next**.
8. On the **Lease Duration** page, click **Next**.
9. On the **Configure DHCP Options** page, click **No, I will configure these options later** and then click **Next**.
10. On the **Completing the New Scope Wizard** page, click **Finish**.

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

Additional Reading

What Are DHCP Scopes?

- Microsoft TechNet: Setting Up Scopes

What Are Superscopes and Multicast Scopes?

- Microsoft TechNet: Setting Up Scopes

What Is a DHCP Reservation

- Microsoft TechNet: DHCP Resources

DHCP Sizing and Availability

- Technet: Configuring Scopes
- Technet: DHCP Best Practices

Lesson 3

Configuring DHCP Options

Contents:

Detailed Demonstration Steps

Demonstration: How to Configure DHCP Options

Demonstration Steps

Note You require the 6421B-NYC-DC1, 6421B-NYC-SVR1, and 6421B-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**. The virtual machines should still be running from the preceding demonstration.

▶ Configure scope options

1. In the DHCP console, in the navigation pane, expand **Scope [10.10,0.0] Head Office Scope 1**.
2. Click **Scope Options**.
3. Right-click **Scope Options** and then click **Configure Options**.
4. In the **Scope Options** dialog box, in the **Available Options** list, select the **003 Router** check box.
5. Under **Data entry**, in the **IP address** box, type **10.10.0.1**, click **Add**, and then click **OK**.

▶ Configure server options

1. In the navigation pane, click **Server Options**.
2. Right-click **Server Options** and then click **Configure Options**.
3. In the **Server Options** dialog box, in the **Available Options** list, scroll down the list to show the two configured options and then click the **Advanced** tab.
4. In the **Vendor class** list, click **DHCP Standard Options** to show the available options.
5. In the **User class** list, click **Default User Class** to display the available options.
6. Click **OK**.

▶ Create a user class for options

1. In the navigation pane, right-click **IPv4** and then click **Define User Classes**.
2. In the **DHCP User Classes** dialog box, click **Add**.
3. In the **New Class** dialog box, in the **Display name** box, type **Laptop**.
4. In the **ID** box, type **ABCD** and then click **OK**.
5. In the **DHCP User Classes** dialog box, click **Close**.
6. In the navigation pane, click **Server Options**.
7. Right-click **Server Options** and then click **Configure Options**.
8. In the **Server Options** dialog box, click the **Advanced** tab.
9. In the **User class** list, click **Laptop**.
10. In the **Server Options** dialog box, in the **Available Options** list, select the **044 WINS/NBNS** Servers check box.
11. Under **Data entry**, in the **IP address** box, type **10.10.0.10**, click **Add**, and then click **OK**.

▶ Enable scope and configure client computer user class

1. In the navigation pane, right-click **Scope [10.10.0.0] Head Office Scope 1** and then click **Activate**.
2. Switch to the NYC-CL1 computer.
3. Click **Start**, and in the **Search** box, type **cmd.exe** and press ENTER.
4. At the command prompt, type **ipconfig /setclassid "Local Area Connection" laptop** and press ENTER.

Note The LAN connection might be called Local Area Connection 2 or even 3.

5. At the command prompt, type **ipconfig /renew** and press ENTER.
6. At the command prompt, type **ipconfig /all** and press ENTER

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

Additional Reading

What Are DHCP Options?

- Request for Comments 2132
- Microsoft TechNet: DHCP Resources

What Are DHCP Class-Level Options?

- Microsoft TechNet: DHCP Resources
- Microsoft TechNet: Using option classes

How DHCP Options Are Applied

- Microsoft TechNet: DHCP Resources

Lesson 4

Managing a DHCP Database

Contents:

Detailed Demonstration Steps

Demonstration: How to Manage a DHCP Database

Demonstration Steps

Note You require the 6421B-NYC-DC1, 6421B-NYC-SVR1, and 6421B-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**. The virtual machines should still be running from the preceding demonstration.

▶ Examine the backup interval

1. Switch to NYC-SVR1.
2. Click **Start**, and in the **Search**box, type **Regedit.exe** and press ENTER.
3. In Registry Editor, navigate to **HKLM\System\CurrentControlSet\Services\DHCPServer\Parameters**.
4. In the right pane, double-click **BackupInterval**.
5. In the **Edit DWORD (32-bit) Value** dialog box, click **Decimal** and then click **Cancel**.
6. Close the Registry Editor.

▶ Back up the DHCP database

1. Switch to DHCP.
2. In the navigation pane, right-click **nyc-svr1.contoso.com** and then click **Backup**.
3. In the **Browse For Folder** dialog box, click **OK**.

▶ Reconcile the scope data

1. Right-click **Scope [10.10.0.0] Head Office Scope 1** and then click **Reconcile**.
2. In the **Reconcile** dialog box, click **Verify**.
3. In the **DHCP** dialog box, click **OK**.
4. In the **Reconcile** dialog box, click **Cancel.**

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

Additional Reading

What Is a DHCP Database

- Microsoft TechNet: DHCP Resources

How a DHCP Database Is Backed Up and Restored

- Microsoft TechNet: Backing up the DHCP database

Lesson 5

Monitoring and Troubleshooting DHCP

Contents:

Detailed Demonstration Steps

Demonstration: How to Monitor DHCP

Demonstration Steps

Note You require the 6421B-NYC-DC1, 6421B-NYC-SVR1, and 6421B-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**. The virtual machines should still be running from the preceding demonstration.

▶ View server statistics

1. In DHCP, in the navigation pane, right-click **IPv4** and then click **Display Statistics**.
2. In the **Server nyc-svr1.contoso.com Statistics** dialog box, view the data and then click **Close**.

▶ View the log files

1. Click **Start**, and in the **Search** box, type **c:\windows\system32\dhcp** and then press ENTER.
2. In Explorer, double-click the **DhcpSrvLog-DAY.log** file, where DAY is an abbreviation for today's day name.
3. Examine the log, and then close notepad and Explorer.

▶ Use Network Monitor to monitor DHCP

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 the **New capture** tab.
5. On the **Capture 1** tab, on the menu bar, click **Start**.
6. Click **Start**, and in the **Search** box, type **cmd.exe** and then press ENTER.
7. At the command prompt, type **ipconfig /release** and then press ENTER.
8. At the command prompt, type **ipconfig /renew** and then press ENTER.
9. In Microsoft Network Monitor 3.4, on the menu, click **Stop**.
10. In the Frame Summary window, examine the captured frames that relate to DHCP.
11. Click **Load Filter**, point to **Standard Filters**, point to **Basic Examples**, and then click **Protocol Filter – DNS**.
12. In the **Display Filter** text box, locate the text that reads **DNS** and change it to **DHCP**. Click **Apply**.
13. Now examine the captured frames.
14. Double-click each frame and expand and discuss the contents.

Note Revert all virtual machines.

Additional Reading

What Is a DHCP Audit Log File?

- Microsoft TechNet: Audit logging

Monitoring DHCP Server Performance

- Microsoft TechNet: DHCP performance monitoring reference

Module Reviews and Takeaways

Review questions

Question: You have two subnets in your organization and want to use DHCP to allocate addresses to client computers in both subnets. You do not want to deploy two DHCP Servers. What factors must you consider?

Answer: The router that interconnects the two subnets must support DHCP relaying, or else you must place a relay on the subnet that does not host the DHCP server. Additionally, you should consider the impact on service availability if your single DHCP server fails.

Question: Your organization has grown and your IPv4 scope has almost run out of addresses. What could you do?

Answer: Implement a superscope by combining the existing scope and a new scope.

Question: What information do you require to configure a DHCP reservation?

Answer: The MAC address of the client that will lease the reservation.

Question: Is it advisable to configure options 003 – Router as a Server-level DHCP scope option?

Answer: No; in a multi-scope environment, all clients would obtain the same gateway setting. This is only appropriate where all clients are in the same subnet.

Lab Review Questions and Answers

Question: In the lab, you configured the router with the DHCP Relay agent. What does the agent do?

Answer: The relay passes the DHCP broadcast messages to a configured DHCP server on the other side of the router.

Question: In the lab, you configured a scope for the branch office computers on each of two DHCP servers to provide for fault tolerance. What would happen to clients that renewed when both DHCP servers were unavailable?

Answer: If the clients could not renew, but the lease of their IP configuration had not expired, they would continue to use their address. If the lease had expired, however, the clients would fall back to use either APIPA or alternate IP configuration (if configured).

Module 3

Configuring and Troubleshooting DNS

Contents:

Lesson 1

Installing the DNS Server Role

Contents:

Detailed Demonstration Steps

Demonstration: How to Install the DNS Server Role

Demonstration Steps

Note You require the 6421B-NYC-DC1, 6421B-NYC-SVR1, and 6421B-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**.

▶ Install the DNS server role

1. Switch to NYC-SVR1, and on the **Taskbar**, click **Server Manager.**
2. In Server Manager, in the navigation pane, click **Roles**, and in the right pane, click **Add Roles**.
3. In the Add Roles Wizard, on the **Before You Begin** page, click **Next**.
4. On the **Select Server Roles** page, in the **Roles** list, select the **DNS Server** check box and then click Next.
5. On the **DNS Server** page, click **Next**.
6. On the **Confirm Installation Selections** page, click **Install**.
7. Once the role is installed, click **Close**.

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

Additional Reading

Overview of the Domain Name System Role

- DNS Overview
- Understanding zones and zone transfer
- Help Topic: Understanding Active Directory Domain Services Integration

DNS Improvements for Windows Server 2008

- What's New in DNS in Windows Server 2008

DNS Improvements for Windows Server 2008 R2

- What's New in DNS in Windows Server 2008 R2

Considerations for Deploying the DNS Server Role

- Help topic: Planning DNS Servers

Lesson 2

Configuring the DNS Server Role

Contents:

Detailed Demonstration Steps

Demonstration: How to Configure the DNS Server Role

Demonstration Steps

Note You require the 6421B-NYC-DC1, 6421B-NYC-SVR1, and 6421B-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**. The virtual machines should still be running from the preceding demonstration.

▶ Configure DNS server properties

1. Switch to NYC-DC1.
2. Click **Start**, point to **Administrative Tools**, and then click **DNS**.
3. In DNS Manager, expand **NYC-DC1**, select and then right-click **NYC-DC1**, and then click **Properties**.
4. In the **NYC-DC1 Properties** dialog box, click the **Forwarders** tab.
5. On the **Forwarders** tab, click **Edit**. You can configure forwarding here. Click **Cancel**.
6. Click the **Advanced** tab. You can configure options including securing the cache against pollution.
7. Click the **Root Hints** tab. You can see the configuration for the root hints servers here.
8. Click the **Debug Logging** tab and select the **Log packets for debugging** check box. You can configure debug logging options here.
9. Clear the **Log packets for debugging** check box and then click the **Event Logging** tab.
10. Click **Errors and Warnings** and then click the **Trust Anchors** tab. You can configure DNSSEC here.
11. Click the **Monitoring** tab. You can perform simple and recursive tests against the server using the **Monitoring** tab. Select the **A simple query against this DNS server** check box and then click **Test Now**.
12. Click the **Security** tab. You can define permissions on the DNS infrastructure here. Click **OK**.

▶ Configure conditional forwarding

1. In the navigation pane, expand **Conditional Forwarders**.
2. Right-click **Conditional Forwarders** and then click **New Conditional Forwarder**.
3. In the **New Conditional Forwarder** dialog box, in the **DNS Domain** box, type **nwtraders.msft**.
4. Click in the **<Click here to add an IP Address or DNS Name>** box. Type **131.107.1.2** and press ENTER. Validation will fail.
5. Click **OK**.

▶ Clear the DNS cache

1. In the navigation pane, right-click **NYC-DC1** and the click **Clear Cache.**

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

Additional Reading

What Are the Components of a DNS Solution?

- Microsoft TechNet: DNS defined
- Microsoft TechNet: Server features
- Microsoft TechNet: Client features

DNS Resource Records

- Help topic: Adding Resource Records

What Is Forwarding?

- Microsoft TechNet: Understanding Forwarders
- Help topic: Understanding Forwarders
- Help topic: Using Forwarders

How DNS Server Caching Works

- Help topic: Install a Caching-only DNS Server

Lesson 3

Configuring DNS Zones

Contents:

Detailed Demonstration Steps

Demonstration: How to Create Zones

Demonstration Steps

Note You require the 6421B-NYC-DC1, 6421B-NYC-SVR1, and 6421B-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**. The virtual machines should still be running from the preceding demonstration.

▶ Create a reverse lookup zone

1. On NYC-DC1, in DNS Manager, in the navigation pane, click **Reverse Lookup Zones**.
2. Right-click **Reverse Lookup Zones** and click **New Zone**.
3. In the New Zone Wizard, click **Next**.
4. On the **Zone Type** page, click **Primary zone** and then click **Next**.
5. On the **Active Directory Zone Replication Scope** page, click **Next**.
6. On the **Reverse Lookup Zone Name** page, click **IPv4 Reverse Lookup Zone** and click **Next**.
7. On the second **Reverse Lookup Zone Name** page, in the **Network ID**: box, type **10.10.0** and click **Next**.
8. On the **Dynamic Update** page, click **Next**.
9. On the **Completing the New Zone Wizard** page, click **Finish**.

▶ Create a forward lookup zone

1. Switch to NYC-SVR1.
2. Click **Start**, point to **Administrative Tools**, and then click **DNS**.
3. In DNS Manager, in the navigation pane, expand **NYC-SVR1** and then click **Forward Lookup Zones**.
4. Right-click **Forward Lookup Zones** and click **New Zone**.
5. In the **New Zone Wizard**, click **Next**.
6. On the **Zone Type** page, click **Secondary zone** and then click **Next**.
7. On the **Zone Name** page, in the **Zone name**: box, type **Contoso.com** and then click **Next**.
8. On the **Master DNS Servers** page, in the **Master Servers** list, type **10.10.0.10** and press ENTER.
9. Click **Next**, and on the **Completing the New Zone Wizard** page, click **Finish**.

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

Additional Reading

What Is a DNS Zone?

- Help topic: Planning DNS zones
- Microsoft TechNet: Understanding zones and zone transfer

What Are the DNS Zone Types?

- Help topic: Understanding Zone Types

What Are Forward and Reverse Lookup Zones?

- Help topic: Understanding Zone Types

What Are Stub Zones?

- Help topic: Understanding Zone Types

DNS Zone Delegation

- Microsoft TechNet: Delegating Zones

Lesson 4

Configuring DNS Zone Transfers

Contents:

Detailed Demonstration Steps

Demonstration: How to Configure DNS Zone Transfers

Demonstration Steps

Note You require the 6421B-NYC-DC1, 6421B-NYC-SVR1, and 6421B-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**. The virtual machines should still be running from the preceding demonstration.

▶ Enable DNS zone transfers

1. Switch to NYC-DC1.
2. In DNS Manager, in the navigation pane, expand **Forward Lookup Zones**.
3. Right-click **Contoso.com** and then click **Properties**.
4. In the **Contoso.com Properties** dialog box, click the **Zone Transfers** tab.
5. Select the **Allow zone transfers** check box and then click **Only to servers listed on the Name Servers tab**.
6. Click **Notify**, and in the **Notify** dialog box, click **Servers listed on the Name Servers tab**. Click **OK**.
7. Click the **Name Servers** tab and click **Add**.
8. In the **New Name Server Record** dialog box, in the **Server fully qualified domain name (FQDN)** box, type **NYC-SVR1.Contoso.com** and click **Resolve**. Click **OK**.
9. In the **Contoso.com Properties** dialog box, click **OK**.

▶ Update the secondary zone from the master server

1. Switch to NYC-SVR1.
2. In DNS Manager, in the navigation pane, expand **Forward Lookup Zones**.
3. Press F5 to refresh the display, right-click **Contoso.com** and then click **Transfer from Master**.

Note You might need to repeat step 3 a number of times before the zone transfers. Also note that the transfer might occur automatically before you manually perform these steps.

▶ Update the primary zone and verify the change on the secondary zone

1. Switch to NYC-DC1.
2. In DNS Manager, right-click **Contoso.com** and then click **New Alias (CNAME)**.
3. In the **New Resource Record** dialog box, in the **Alias name (uses parent domain if left blank)** box, type **intranet**.
4. In the **Fully qualified domain name (FQDN) for target host** box, type **nyc-dc1.contoso.com** and click **OK**.
5. Switch to NYC-SVR1.
6. In DNS Manager, right-click **Contoso.com** and then click **Transfer from Master**.

Note The record might take some time to appear. You might need to press F5 to refresh the display.

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

Additional Reading

What Is a DNS Zone Transfer?

- Microsoft TechNet: Understanding zones and zone transfer

Lesson 5

Managing and Troubleshooting DNS

Contents:

Detailed Demonstration Steps

Demonstration: How to Manage DNS Records

Demonstration Steps

Note You require the 6421B-NYC-DC1, 6421B-NYC-SVR1, and 6421B-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**. The virtual machines should still be running from the preceding demonstration.

▶ Configure TTL

1. Switch to NYC-DC1.
2. In DNS Manager, right-click **Contoso.com** and click **Properties**.
3. In the **Contoso.com Properties** dialog box, click the **Start of Authority (SOA)** tab.
4. In the **Minimum (default) TTL** box, type **2** and then click **OK**.

▶ Enable and configure scavenging

1. Right-click **NYC-DC1** and then click **Set Aging/Scavenging for All Zones**.
2. In the **Set Aging/Scavenging Properties** dialog box, select the **Scavenge stale resource records** check box and click **OK**.
3. In the **Server Aging/Scavenging Confirmation** dialog box, select the **Apply these settings to the existing Active Directory-integrated zones** check box and then click **OK**.

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

Demonstration: How to Test the DNS Server Configuration

Demonstration Steps

Note You require the 6421B-NYC-DC1, 6421B-NYC-SVR1, and 6421B-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**. The virtual machines should still be running from the preceding demonstration.

▶ Capture DNS network traffic

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 the **New capture** tab.

5. On the **Capture 1** tab, on the menu bar, click **Start**.
6. Click **Start**, and in the **Search** box, type **cmd.exe** and then press ENTER.
7. At the command prompt, type **ipconfig /flushdns** and then press ENTER.
8. At the command prompt, type **ping intranet** and then press ENTER.
9. At the command prompt, type **ipconfig /displaydns** and then press ENTER.
10. In Microsoft Network Monitor 3.4, on the menu, click **Stop**.

▶ Filter and analyze captured traffic

1. In the Frame Summary window, examine the captured frames that relate to DNS.
2. Click **Load Filter**, point to **Standard Filters**, point to **DNS**, and then click **DnsAllNameQuery**.
3. Click **Apply**.
4. Now examine the captured frames.
5. Double-click each frame and then expand and discuss the contents.

▶ Use Nslookup to test DNS

1. At the command prompt, type **nslookup –d2 nyc-svr1.contoso.com. > file.txt** and press ENTER.
2. At the command prompt, type **notepad file.txt** and press ENTER.

Note Revert all virtual machines.

Additional Reading

What Is Time to Live, Aging, and Scavenging?

- Microsoft TechNet: Use Aging and Scavenging

Tools That Identify Problems With DNS

- Microsoft Help and Support Center: Description of the DNSLint utility
- Help Topic: Troubleshooting DNS Servers
- Microsoft TechNet: Troubleshooting DNS

Module Reviews and Takeaways

Review questions

Question: You are presenting to a potential client about the advantages of using Windows Server 2008 R2. What are the new features that you would point out when discussing the Windows Server 2008 R2 DNS server role?

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

Question: You are deploying DNS servers into an Active Directory domain, and your customer requires that the infrastructure is resistant to single points of failure. What must you consider while planning the DNS configuration?

Answer: You must ensure that more than one DNS domain controller is deployed into the network.

Question: What is the difference between recursive and iterative queries?

Answer: A client issues a recursive query to a DNS server. It can have only two possible replies: 1) the IP address of the domain requested, or 2) host not found. An iterative query resolves IP addresses through the hierarchal DNS name space. An iterative query returns an authoritative answer or the IP address of a server the next level down in the DNS hierarchy.

Question: What must you configure before a DNS zone can be transferred to a secondary DNS server?

Answer: You must configure DNS zone transfers to allow the secondary zone server to transfer from the primary zone.

Question: You are the administrator of a Windows Server 2008 R2 DNS environment. Your company recently acquired another company. You want to replicate their primary DNS zone. The acquired company is using Bind 4.9.4 to host their primary DNS zones. You notice a significant amount of traffic between the Windows Server 2008 R2 DNS server and the Bind server. What is one possible reason for this?

Answer: Bind 4.9.4 does not support IXFR. Each time a change occurs in the Bind zone, it has to replicate the entire zone to a computer that is running Windows Server 2008 R2 to remain updated.

Question: You must automate a DNS server configuration process so that you can automate the deployment of Windows Server 2008 R2. What DNS tool can you use to do this?

Answer: You can use dnscmd.exe.

Lab Review Questions and Answers

Question: In the lab, you were required to deploy a secondary zone because no additional domain controllers were going to be deployed. If this condition changed, that is, NYC-SVR1 was a domain controller, how would that change your implementation plan?

Answer: You could install the AD DS and DNS roles and you would not need to configure any zones or configure zone transfers.

Module 4

Configuring and Troubleshooting IPv6 TCP/IP

Contents:

Lesson 2

IPv6 Addressing

Contents:

Detailed Demonstration Steps

Demonstration: How to Configure IPv6 Client Settings

Demonstration Steps

Note: You require the 6421B-NYC-DC1 and 6421B-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as Contoso\Administrator with the password of Pa$$w0rd.

▶ Configure a DHCP Scope for IPv6 Clients

1. Switch to NYC-DC1.
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 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:e1a2**.
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. Click **Start**, point to **Administrative** Tools, and then click **DHCP**.
12. In DHCP, in the navigation pane, expand **NYC-DC1.Contoso.com** and then click **IPv6**.
13. Right-click **IPv6** and then click **New Scope**.
14. In the New Scope Wizard, click **Next**.
15. On the **Scope Name** page, in the **Name** box, type **Contoso IPv6 Scope** and then click **Next**.
16. On the **Scope Prefix** page, in the **Prefix** box, type **2001:db8:0:1**:: and then click **Next**.
17. On the **Add Exclusions** page, click **Next**.
18. On the **Scope Lease page**, click **Next**.
19. On the **Completing the New Scope Wizard** page, click **Finish**.
20. In the navigation pane, click **Server Options** and then double-click **00023 DNS Recursive Name Server IPV6 Address List**.
21. In the **Server Options** dialog box, click **Remove** twice.
22. In the **New IPv6 address** box, type **2001:db8:0:1:1a81:f438:3222:e1a2**, click **Add**, and then click **OK**.

▶ 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**, and 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 demonstration.

Additional Reading

Address Autoconfiguration for IPv6

- Introduction to IP Version 6

Lesson 3

Coexistence with IPv6

Contents:

Detailed Demonstration Steps

Demonstration: How to Configure DNS to Support IPv6

Demonstration Steps

Note You require the 6421B-NYC-DC1 and 6421B-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**. These two computers are already running.

▶ 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, right-click **NYC-DC1** and then click **Properties**.
4. On the **Interfaces** tab, verify that the **2001:db8:0:1:1a81:f438:3222:e1a2** check box is selected and then click **OK**.

▶ 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. Close DNS Manager.

Note Revert all virtual machines.

Additional Reading

What Are Node Types?

- Introduction to IP Version 6

IPv4 and IPv6 Coexistence

- IPv6 Transition Technologies

Lesson 4

IPv6 Transition Technologies

Contents:

Additional Reading

What Is Teredo?

- IPv6 Transition Technologies

What Is PortProxy?

- IPv6 Transition Technologies

Lesson 5

Transitioning from IPv4 to IPv6

Contents:

Additional Reading

Discussion: Considerations for Migrating from IPv4 to IPv6

- IPv6 Transition Technologies

Process for Transitioning to IPv6-only

- IPv6 Transition Technologies

Troubleshooting IPv6

- The Cable Guy - March 2005

Module Reviews and Takeaways

Review questions

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

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

Question: What are the main reasons why IPv6 is 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 a Teredo tunnel?

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

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.

Question: What does advertising a prefix do when you are defining a prefix in the IPv6 router?

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

Question: Why must you disable the ISATAP router when transitioning to IPv6?

Answer: The ISATAP router is needed only when communicating over IPv4 subnets.

Module 5

Configuring and Troubleshooting Routing and Remote Access

Contents:

Lesson 2

Configuring VPN Access

Contents:

Detailed Demonstration Steps

Demonstration: How to Configure VPN Access

Demonstration Steps

Note You require the 6421B-NYC-DC1, 6421B-NYC-EDGE1, and 6421B-NYC-CL1 virtual machines to complete this demonstration. Log on to 6421B-NYC-DC1 and 6421B-NYC-EDGE1 as **Contoso\Administrator** with the password of **Pa$$w0rd**. Do not log on to 6421B-NYC-CL1 until directed to do so.

▶ Configure 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. 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.

▶ Configure Routing and Remote Access as a VPN server

1. On NYC-EDGE1, click **Start** and then click **Administrative Tools**.
2. From the **Administrative Tools** menu, click **Server Manager**. The Server Manager opens.
3. In the **Server Manager (NYC-EDGE1)** list pane, right-click **Roles** and click **Add Roles** from the context menu. The Add Roles Wizard appears. Click **Next**.
4. On the **Select Server Roles** page, select **Network Policy and Access Services**, and then click **Next**.
5. On the **Network Policy and Access Services** introduction page, click **Next**.
6. On the **Select Role Services** page, select the **Network Policy Server** and **Routing and Remote Access Services** check boxes and then click **Next**.
7. On the **Confirm Installation Selections** page, click **Install**.
8. On the **Installation Results** page, verify that **Installation succeeded** appears in the details pane and then click **Close**.
9. Close the Server Manager. The Network Policy and Routing and Remote Access Services roles are installed on 6421B-NYC-EDGE1.
10. On NYC-EDGE1, click **Start** and then click **Administrative Tools**.
11. From the **Administrative Tools** menu, click **Routing and Remote Access**. The Routing and Remote Access administrative tool appears.

12. In the list pane, select and right-click **NYC-EDGE1 (local)**, and then click **Configure and Enable Routing and Remote Access**.
13. Click **Next** on the wizard **Welcome** page.
14. On the **Configuration** page, leave the default **Remote Access (dial-up or VPN)** selected and click **Next**.
15. On the **Remote Access** page, select the **VPN** check box and click **Next**.
16. On the **VPN Connection** page, select the **Public** interface and then click **Next**.
17. On the **IP Address Assignment** page, select **From a specified range of addresses** and then click **Next**.
18. On the **Address Range Assignment** page, click **New**, and in the **Start IP address** box, type the value of **10.10.0.60**. In the **Number of addresses** box, type the value of **25** and click **OK**. Click **Next**.
19. On the **Managing Multiple Remote Access Servers** page, leave the default selection **No, use Routing and Remote Access to authenticate connection requests** and then click **Next**. Click **Finish**.
20. In the **Routing and Remote Access** dialog box, click **OK**.
21. In the **Routing and Remote Access** dialog box regarding the DHCP Relay agent, click **OK**. The Routing and Remote Access service starts. Close the Routing and Remote Access console.
22. On NYC-EDGE1, click **Start** and then click **Administrative Tools**.
23. On the **Administrative Tools** menu, click **Network Policy Server**. The Network Policy Server administrative tool appears.
24. In the list pane, expand **Policies** and then click **Network Policies**.
25. Right-click the **Connections to Microsoft Routing and Remote Access server** policy and then click **Disable**.
26. Repeat for any remaining policies.

▶ Configure a VPN Client

1. Switch to the NYC-CL1 computer and log on as **Contoso\Adam** with the password of **Pa$$w0rd**.
2. Click **Start** and then click **Control Panel**.
3. In the Control Panel window, under Network and Internet, click **View network status and tasks**.
4. In the Network and Sharing Center window, click **Change adapter settings**.
5. Right-click **Local Area Connection 3** and then click **Properties**. In the **User Account Control** dialog box, provide Administrator with the password of **Pa$$w0rd**.
6. Select **Internet Protocol Version 4 (TCP/IPv4)** and then click **Properties**.
7. Configure the following IP address settings and then click **OK**:
   - IP Address: **131.107.0.20**
   - Subnet mask: **255.255.255.0**
   - Default gateway: **131.107.0.1**
8. Click **Close** and then click the **Back** button to return to the Network and Sharing Center.

9. 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**.
10. 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**.
11. In the **Type the Internet address to connect to** dialog box, specify an Internet address of **131.107.0.2** and a Destination Name of **HQ**, and then click **Next**.
12. On the **Type your user name and password** page, leave the user name and password blank and then click **Create**.
13. Click **Close** in the **Connect to a Workplace** dialog box.
14. In the Network and Sharing Center window, click **Change adapter settings**.
15. On the **Network Connections** page, right-click **HQ** and then click **Connect**.
16. Use the following information in the **Connect HQ** text boxes and then click **Connect**:
    - User name: **Adam**
    - Password: **Pa$$w0rd**
    - Domain: **Contoso**

    The VPN does not connect as no matching policy exists.
17. Click **Close**.

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

Lesson 3

Overview of Network Policies

Contents:

Detailed Demonstration Steps

Demonstration: How to Create a Network Policy

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.

▶ Create a VPN policy based on Windows Groups condition

1. On NYC-EDGE1, switch to the **Network Policy Server** console.
2. In the list pane, expand **Policies**, right-click **Network Policies**, and then click **New**.
3. On the **New Network Policy – Specify Network Policy Name and Connection Type** page, type **VPN** in the **Policy name** text box, and in the **Type of network access server** drop-down list, click **Remote Access Server (VPN-Dial up)** and then click **Next**.
4. On the **Specify Conditions** page, click **Add**. On the **Select condition** dialog box, double-click **Windows Groups**.
5. Click **Add Groups**, and in the **Enter the object name to select** box, type **Marketing**, click **Check Names**, click **OK** twice, and then click **Next**.
6. On the **Specify Access Permission** page, leave the default of **Access granted** and then click **Next**.
7. On the **Configure Authentication Methods** page, click **Next**.
8. On the **Configure Constraints** page, under **Constraints**, in the right pane, select the **Disconnect after the maximum idle time** check box and then click **Next**.
9. In the **Configure Settings** dialog box, click **Next** and then click **Finish**.
10. In the list pane of the **Network Policy Server** tool, click the **Network Policies** node.

▶ Test the VPN

1. On NYC-CL1, right-click **HQ** and then click **Connect**.
2. Use the following information in the **Connect HQ** text boxes and then click **Connect**:
   - User name: **Adam**
   - Password: **Pa$$w0rd**
   - Domain: **Contoso**

   The VPN connects.

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

Lesson 4

Overview of the Connection Manager Administration Kit

Contents:

Detailed Demonstration Steps

Demonstration: How to Create a Connection Profile 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.

▶ 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.

▶ 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 **131.107.0.2** 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**.

▶ 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 created for the profile.

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

Note Revert all virtual machines.

Lesson 6

Configuring DirectAccess

Contents:

Detailed Demonstration Steps

Demonstration: How to Install and Configure DirectAccess

Demonstration Steps

This demonstration shows how to:

- Configure the AD DS domain controller and DNS
- Configure the PKI environment
- Configure the DirectAccess clients and test Intranet and Internet access
- Configure the DirectAccess server
- Verify DirectAccess Functionality

Note To observe how to perform these tasks, download and extract the supplemental content file 6421B-ENU-Companion.zip from the http://www.microsoft.com/learning /en/us/training/companionmoc.aspx site and view the following media files:
6421B_DirectAccessDemo_Task1.WMV
6421B_DirectAccessDemo_Task2.WMV
6421B_DirectAccessDemo_Task3.WMV
6421B_DirectAccessDemo_Task4.WMV
6421B_DirectAccessDemo_Task5.WMV

To view the transcript for the demonstration, see 6421B_DirectAccessDemo_Transcript_and_Steps.PDF.

Module Reviews and Takeaways

Review questions

1. Your organization wants to implement a cost effective solution that interconnects two branch offices with your head offices. In what way could VPNs play a role in this scenario?

Answer: You could implement VPNs in a site-to-site configuration over the Internet to provide the necessary routing capabilities.

2. The IT manager at your organization is concerned about opening too many firewall ports to facilitate remote access from users that are working from home through 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.

3. 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 had 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 else to change the policy order so that the administrator policy is first in the list.

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: Why did you create the DA_Clients group?

Answer: To enable the application of DirectAccess security settings to DirectAccess computers that are a member of this security group.

Question: What is the purpose of the nls.contoso.com DNS host record that you associated with an internal IP address?

Answer: To enable intranet-based DirectAccess clients to locate the Network Location Server while in the intranet.

Question: What is the purpose of the certificate revocation list?

Answer: To enable DirectAccess clients and servers to determine whether issued certificates (used for authentication) have been revoked.

Question: Why do you make the CRL available on the DirectAccess server in the perimeter network?

Answer: So that Internet DirectAccess clients can access the CRL.

Question: Why would you use GPO to configure certificate deployment?

Answer: To more quickly and effortlessly deploy the required certificates to DirectAccess client computers.

Question: Why did you install a certificate on the client computer?

Answer: Without a certificate, the client cannot identify and authenticate itself to the DirectAccess server.

Module 6

Installing, Configuring, and Troubleshooting the Network Policy Server Role Service

Contents:

Lesson 1

Installing and Configuring a Network Policy Server

Contents:

Detailed Demonstration Steps

Demonstration: How to Install the Network Policy Server

Demonstration Steps

Note You require the 6421B-NYC-DC1 and 6421B-NYC-SVR1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**.

▶ 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.

▶ 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.

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

Demonstration: How to Configure General NPS Settings

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.

▶ 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.

▶ 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.

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

Lesson 2

Configuring RADIUS Clients and Servers

Contents:

Detailed Demonstration Steps

Demonstration: How to Configure a RADIUS Client

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.

▶ 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 the **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 the subsequent demonstration.

Demonstration: How to Create a New Connection Request Policy

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.

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 Revert all virtual machines.

Module Reviews and Takeaways

Review questions

1. 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 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.

2. 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 generates, is unique for each request, duplicate records might exist in cases where the reply to the access server is lost and the request is resent. 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 running SQL Server on different subnets. Use the SQL Server Create Publication Wizard to set up database replication between the two servers..

3. 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.

Lab Review Questions and Answers

Question: What does a RADIUS proxy provide?

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

Question: What is a RADIUS client, and what are some examples of RADIUS clients?

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

Examples of network access servers are:

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

Module 7

Implementing Network Access Protection

Contents:

Lesson 3

Configuring NAP

Contents:

Detailed Demonstration Steps

Demonstration: How to Configure Network Access Protection

Demonstration Steps

Note You require the 6421B-NYC-DC1 and 6421B-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**.

▶ Install the NPS server role

1. On NYC-DC1, click **Start**, click **Administrative Tools**, and then click **Server Manager**.
2. Click **Roles**, and then under **Roles Summary**, click **Add Roles** and then click **Next**.
3. Select the **Network Policy and Access Services** check box and then click **Next** twice.
4. Select the **Network Policy Server** check box, click **Next**, and then click **Install**.
5. Verify that the installation was successful and then click **Close**.
6. Close the Server Manager window.

▶ Configure NPS as a NAP health policy server

1. 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 the **A firewall is enabled for all network connections** check box.
5. Click **OK** to close the **Windows Security Health Validator** dialog box.

▶ 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**.

▶ 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**.

▶ 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 remove the check box next to **Enable auto-remediation of client computers**.
11. Click **Next** and then click **Finish**.

▶ Configure the DHCP server role for NAP

1. Click **Start**, point to **Administrative Tools**, and then click **DHCP**.
2. In **DHCP**, expand **NYC-DC1.contoso.com**, expand **IPv4**, right-click **Scope [10.10.0.0] NYCScope**, and then click **Properties**.
3. In the **Scope [10.10.0.0] NYCScope Properties** dialog box, click the **Network Access Protection** tab, click **Enable for this scope**, and then click **OK**.
4. In the navigation pane, click **Scope Options**.
5. Right-click **Scope Options** and then click **Configure Options**.
6. In the **Server Options** dialog box, click the **Advanced** tab.
7. In the **User class** list, click **Default Network Access Protection Class**.
8. In the **Available Options** list, select the **006 DNS Servers** check box.
9. In the **IP address** box, type **10.10.0.10** and then click **Add**.
10. In the **Available Options** list, select the **015 DNS Domain Name** check box.
11. In the **String value** box, type **restricted.contoso.com** and then click **OK**.
12. Close **DHCP**.

▶ Configure client NAP 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 expand **Security Center**.
12. Double-click **Turn on Security Center (Domain PCs only)**, click **Enabled**, and then click **OK**.
13. Close the console window. When prompted to save settings, click **No**.
14. Click **Start**, and in the **Search** box, type **Network and in the Control Panel (28)** list, click **Network and Sharing Center**.
15. In **Network and Sharing Center**, in the left-pane, click **Change adapter settings**.
16. Right-click **Local Area Connection 2** and then click **Properties**.

17. In the **Local Area Connection 2 Properties** dialog box, double-click **Internet Protocol Version 4 (TCP/IPv4)**.
18. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, click **Obtain an IP address automatically**.
19. Click **Obtain DNS server address automatically** and then click **OK**.
20. In the **Local Area Connection 2 Properties** dialog box, click **OK**.

▶ Test NAP

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

```
Ipconfig
```

3. Switch to services.
4. In **Services**, in the Results pane, double-click **Windows Firewall**.
5. In the **Windows Firewall Properties (Local Computer)** dialog box, in the **Startup** type list, click **Disabled**.
6. Click **Stop** and then click **OK**.
7. At the command prompt, type the following command and press ENTER:

```
Ipconfig /release
```

8. At the command prompt, type the following command and press ENTER:

```
Ipconfig /renew
```

9. At the command prompt, type the following command and press ENTER:

```
Ipconfig /all
```

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

Lesson 4

Monitoring and Troubleshooting NAP

Contents:

Detailed Demonstration Steps

Demonstration: How to Configure NAP Tracing

Demonstration Steps

Note You require the 6421B-NYC-DC1 and 6421B-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**. The virtual machines should still be running from the preceding demonstration

▶ Configure tracing from the GUI

1. Switch to NYC-CL1.
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, right-click **NAP Client Configuration (Local Computer)** from the console tree and then click **Properties**.
4. On the **General** tab, click **Enabled**, and in the **Basic** list, click **Advanced** and then click **OK**.

▶ Configure tracing from the command-line

1. Switch to the command prompt.
2. At the Command Prompt, type the following command and then press ENTER:

```
netsh nap client set tracing state = enable.
```

Note Revert all virtual machines.

Module Reviews and Takeaways

Review questions

1. 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.

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

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

3. On a client computer, what steps must you perform to ensure that it can be assessed for health?

Answer: Enable the NAP enforcement client. Enable the Security Center. Start the NAP agent service.

Lab Review Questions and Answers

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? Why or why not?

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 8

Increasing Security for Windows Servers

Contents:

Lesson 1

Windows Security Overview

Contents:

Question and Answers

Discussion: Identifying Security Risks and Costs

Question: What are some of the risks and associated costs to Windows-based networks?

Answer: Some of the risks and associated costs to Windows-based networks are:

- Malware is one of the biggest risks to Windows-based networks. As a popular operating system, Windows is targeted frequently by malware writers. Malware can be used to steal passwords and other useful information from your organization. Malware can also begin to use your computer to send out spam. The most sophisticated malware might be written specifically to target your organization.
- Stolen data is a risk for a computer system. Data that is stolen can be used by a competitor or used to embarrass your organization.
- Deleted data, whether deleted by a user with inappropriate permissions or malware, can result in costs for data recovery.
- Legal issues are a concern if confidential or private data are stolen. This is particularly true for customer data.

Lesson 2

Configuring Windows Firewall with Advanced Security

Contents:

Question and Answers

Discussion: Why Is a Host-Based Firewall Important?

Question: Why is it important to use a host-based firewall like 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. This 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 do respond to ping requests.
- When outbound rules are enabled, it can prevent malware from spreading by preventing the malware from communicating on the network. In the case of a virus outbreak, you could 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

Demonstration Steps

Note You require the 6421B-NYC-DC1 virtual machine to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**.

▶ Configure firewall profiles

On NYC-DC1, click **Start**, point to **Administrative Tools**, and click **Windows Firewall with Advanced Security**.

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

Module Reviews and Takeaways

Review questions

Question: Does the defense-in-depth model prescribe specific technologies that should be used to protect Windows servers?

Answer: No, the defense-in-depth model is used to organize your thinking about defense rather than prescribe specific technologies.

Question: Your company is concerned about security and has implemented Windows Firewall to block outbound communication by default on client computers. You are implementing a new program that randomly selects a port number for communication on the network. How can you allow this program to function without opening up ports that are unnecessary?

Answer: The firewall rule for the new application should be based on a program rather than a port. Then, the program is allowed to access the network regardless of the port that is being used.

Question: You are creating a GPO with standardized firewall rules for the servers in your organization. You tested the rules on a standalone server in your test lab. The rules appear on the servers after the GPO is applied, but they are not taking effect. What is the most likely cause of this problem?

Answer: The firewall rules are most likely not being applied to the correct firewall profile. It is possible that you did not apply them to the domain profile as would be required for member servers. To test rules on a standalone server, they would have been applied to the public or private firewall profiles.

Question: A colleague has argued that all Windows updates should be applied automatically when they are released. Do you have an alternative process that you recommend?

Answer: All updates should be tested before they are applied in a production environment. It is simple to deploy updates to a set of test computers by using WSUS.

Lab Review Questions and Answers

Question: Why was it appropriate to deploy the firewall rule by using Group Policy?

Answer: In this scenario, many computers needed the rule to be applied. Group Policy is the best way to apply changes to many computers quickly and easily.

Question: Is the use of wuauclt.exe typically required when implementing WSUS?

Answer: No. In this lab, it was used to for automatic updates to query the WSUS server and register the computer. Typically, this would happen automatically the next time automatic updates is scheduled to download updates.

Module 9

Increasing Security for Network Communication

Contents:

Lesson 1

Overview IPsec

Contents:

Detailed Demonstration Steps

Demonstration: How to Configure IPsec Settings (optional)

Demonstration Steps

Note You require the 6421B-NYC-DC1, 6421B-NYC-SVR1, and 6421B-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**.

▶ View existing IPsec policies in Group Policy

1. Switch to NYC-DC1.
2. Click **Start**, point to **Administrative Tools**, and then click **Group Policy Management**.
3. In Group Policy Management, expand **Forest: Contoso.com**, expand **Domains**, expand **Contoso.com**, and then click **Default Domain Policy**. In the **Group Policy Management Console** dialog box, click **OK**.
4. Right-click **Default Domain Policy** and click **Edit**.
5. In Group Policy Management Editor, under **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, and then click **IP Security Policies on Active Directory (CONTOSO.COM)**.
6. In the right pane, view the three existing policies.

▶ Create a custom IPsec policy

1. Right-click **IP Security Policies on Active Directory (CONTOSO.COM)** and then click **Create IP Security Policy**.
2. In the IP Security Policy Wizard, click **Next**.
3. On the **IP Security Policy Name** page, in the **Name** box, type **DNS Zone Transfer policy** and then click **Next**.
4. On the **Requests for Secure Communication** page, click **Next**.
5. On the **Completing the IP Security Policy Wizard** page, click **Finish**. The DNS Zone Transfer policy Properties dialog box opens.

▶ Create a security rule

1. In the **DNS Zone Transfer policy Properties** dialog box, click **Add**.
2. In the **Security Rule Wizard**, click **Next**.
3. On the **Tunnel Endpoint** page, click **Next**.
4. On the **Network Type** page, click **Next**.

▶ Create a new IP filter

1. On the **IP Filter List** page, click **Add**.
2. In the **IP Filter List** dialog box, in the **Name** box, type **DNS zone traffic** and then click **Add**.

3. In the IP Filter Wizard, click **Next**.
4. On the **IP Filter Description and Mirrored Property** page, click **Next**.
5. On the **IP Traffic Source** page, in the **Source Address** list, click **A specific DNS Name**.
6. In the **Host name** box, type **NYC-DC1.Contoso.com** and click **Next**.
7. In the **Security Warning** dialog box, click **Yes**.
8. On the **IP Traffic Destination** page, in the **Destination address** list, click **A specific DNS Name**.
9. In the **Host name** box, type **NYC-SVR1.Contoso.com** and then click **Next**.
10. In the **Security Warning** dialog box, click **Yes**.
11. On the **IP Protocol Type** page, in the **Select a protocol type** list, click **TCP** and then click **Next**.
12. On the **IP Protocol Port** page, under **Set the IP protocol port**, click **From this port** and in the box, type **53**. Click **To this port**, and in the box type **53**. Click **Next**.
13. On the **Competing the IP Filter Wizard** page, click **Finish**.
14. In the **IP Filter List** dialog box, click **OK**.

▶ Completing the Security Rule Wizard

1. In the Security Rule Wizard, on the **IP Filter List** page, click **DNS zone traffic** and then click **Next**.
2. On the **Filter Action** page, click **Require Security** and then click **Next**.
3. On the **Authentication Method** page, click **Next**.
4. On the **Completing the Security Rule Wizard** page, click **Finish**.

▶ Completing the IP Security Rule Wizard

1. In the**DNS Zone Transfer policy Properties**dialog box, click **OK**
2. InGroup Policy Management Editorin the right pane, right-click **DNS Zone Transfer policy**

Important Do not assign the policy. Just show your students that this step is required to activate the rule that you created.

3. Close all open windows

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

Additional Reading

Ways to Use IPsec

- Determining Your IPsec Needs

Tools Used to Configure IPsec

- Help Topic: Windows Firewall with Advanced Security

Lesson 2

Configuring Connection Security Rules

Contents:

Detailed Demonstration Steps

Demonstration: How to Configure a Connection Security Rule

Demonstration Steps

Note You require the 6421B-NYC-DC1, 6421B-NYC-SVR1, and 6421B-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**. The virtual machines should still be running from the preceding demonstration.

▶ Enable ICMP traffic on NYC-SVR1

1. Switch to NYC-SVR1.
2. Click **Start**, and in the **Search** box, type **Windows Firewall with Advanced Security** and press ENTER.
3. 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 **Programs** page, click **Next**.
6. On the **Protocols 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**.

▶ Create a server to server rule on NYC-SVR1

1. 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 click **Finish**.

▶ Create a server to server rule on NYC-CL1

1. Switch to NYC-CL1.
2. Click **Start**, and in the **Search** box, type **Windows Firewall with Advanced Security** and press ENTER.
3. Right-click **Connection Security Rules** and then click **New Rule**.
4. In the New Connection Security Rule Wizard, click **Server-to-Server** and then click **Next**.
5. On the **Endpoints** page, click **Next**.
6. On the **Requirements** page, click **Require authentication for inbound and outbound connections** and then click **Next**.
7. On the **Authentication Method** page, click **Advanced** and then click **Customize**.
8. In the **Customize Advanced Authentication Methods** dialog box, under **First authentication**, click **Add**.
9. In the **Add First Authentication Method** dialog box, click **Preshared Key**, type **secret**, and then click **OK**.
10. In the **Customize Advanced Authentication Methods** dialog box, click **OK**.
11. On the **Authentication Method** page, click **Next**.
12. On the **Profile** page, click **Next**.
13. On the **Name** page, in the **Name** box, type **Contoso-Server-to-Server** and click **Finish**.

▶ Test the rule

1. Click **Start**, and in the **Search** box, type **cmd.exe** and press ENTER.
2. At the command prompt, type **ping 10.10.0.24** and press ENTER.
3. Switch to Windows Firewall with Advanced Security.
4. Expand **Monitoring**, expand **Security Associations**, and then click **Main Mode**.
5. In the right pane, double-click the listed item.
6. View the information in **Main Mode** and then click **OK**.
7. Expand **Quick Mode**.
8. In the right pane, double-click the listed item.
9. View the information in **Quick Mode** and then click **OK**.

Note Revert all virtual machines.

Additional Reading

What Are Connection Security Rules?

- Help Topic: Connection Security Rules

What Are Tunnel and Transport Modes?

- Help Topic: Specify Tunnel Endpoints
- Help Topic: IPsec Tunneling

Choosing Authentication Requirements

- Help Topic: Authentication Requirements

Choosing an Authentication Method

- Help Topic: Authentication Methods
- Windows Firewall with Advanced Security

Lesson 3

Configuring IPsec NAP Enforcement

Contents:

Additional Reading

IPsec Enforcement for Logical Networks

- Network Access Protection Platform Architecture

How IPsec NAP Enforcement Works

- Introduction to Network Access Protection
- Step-by-Step Guide: Demonstrate NAP IPsec Enforcement in a Test Lab

Lesson 4

Monitoring and Troubleshooting IPsec

Contents:

Additional Reading

Monitoring IPsec by Using Windows Firewall with Advanced Security

- Help Topic: Monitoring Windows Firewall with Advanced Security

Monitoring IPsec by Using IP Security Monitor

- Help Topic: Monitoring IPsec
- Help Topic: Monitoring Main mode
- Help Topic: Monitoring Quick mode

Module Reviews and Takeaways

Review questions

1. You need to ensure that traffic passing between a computer in the perimeter network and one deployed in the internal network is both encrypted and authenticated. The computer in the perimeter is not a member of your AD DS forest. What authentication methods could you use if you attempted to establish a Connection Security rule between these two computers?

Answer: You could NOT use Kerberos as the perimeter computer is not in the forest. Therefore, you could use: Certificates or a Preshared key.

2. To enable NAP with IPsec enforcement, what policies must you configure on your NPS server?

Answer: A connection request policy, network policy, and NAP health policy.

3. are responsible for monitoring computers participating in an IPsec-secured network. You wish to do this remotely, but are having difficulty in connecting to remote computers from the IP Security Monitor console. What do you need to do?

Answer: You can monitor computers remotely from a single console, but you must modify a Registry key so that the remote system accepts a console connection. Setting the EnableRemoteMgmt Registry key to 1 prevents the “IPsec service is not running” error when you manage a computer remotely. You can disable this ability by setting the following key to zero (0): HKLM\system\currentcontrolset\services\policyagent.

Lab Review Questions and Answers

Question: In the lab, you created an OU-specific policy for a specific application. If Contoso wanted to create a domain isolation rule, how would you go about it?

Answer:

1. Create a new GPO linked to the domain (or modify the default domain policy).
2. Create a connection security rule for domain isolation within this GPO

Question: What method of authentication would you select?

Answer: Kerberos would be easiest as all the computers are part of the same forest.

Module 10

Configuring and Troubleshooting Network File and Print Services

Contents:

Lesson 1

Configuring and Troubleshooting File Shares

Contents:

Question and Answers

Troubleshooting Network File Access Permissions

Question: If a user is assigned Full Control share permission and Read NTFS permission, what permission will the user have to access data in the share?

Answer: The user will have Read access to files in the share.

Detailed Demonstration Steps

Demonstration: How to Create a File Share

Demonstration Steps

Note You require the 6421B-NYC-DC1, 6421B-NYC-SVR1, and 6421B-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**.

▶ Create a file share by using the simplified interface

1. On NYC- DC1, click **Start** and then click **Computer**.
2. In Windows Explorer, in the left pane, click **Local Disk (C:)**.
3. In the menu bar, click **New folder**.
4. To set the folder name, type **Share1** and press ENTER.
5. Right-click **Share1** and click **Properties**.
6. In the **Share1 Properties** window, on the **Sharing** tab, click **Share**.
7. In the **File Sharing** window, in the **Add** box, type **Marketing** and press ENTER. Notice that the Marketing group is added with Read permission.
8. Click **Marketing** to show the available options for permission levels. Notice that owner is not available. Only Read and Read/Write can be assigned. Mention that this is configuring NTFS permissions rather than share permissions. The share permission defined for this share will be Full Control for the Everyone Group.
9. Click **Share**.
10. Note the UNC path for the share and point it out to students. Click **Done**.
11. In the **Share1 Properties** window, click **Close**.

▶ Create a file share by using advanced sharing

1. In Windows Explorer, in the menu bar, click **New folder**.
2. To set the folder name, type **Share2** and press ENTER.
3. Right-click **Share2** and click **Properties**.
4. In the **Share2 Properties** window, on the **Sharing** tab, click **Advanced Sharing**.
5. In the **Advanced Sharing** window, select the **Share this folder** check box and click **Permissions**.
6. In the **Permissions for Share2** window, read the default permissions that are assigned.
7. With the **Everyone** group selected, select the **Allow Full Control** check box and click **OK**.
8. In the **Advanced Sharing** window, click **Apply**.

▶ Task 3: Configure advanced sharing for a file share

1. In the **Advanced Sharing** window, click the **Add** button.

2. In the **New Share** window, in the **Share name** box, type **Accounting** and click **OK**. This folder is now shared with two share names and independent configuration for share permissions.
3. In the **Advanced Sharing** window, click **Caching**. Note the available options for students.

Note BranchCache is covered in Module 9: Optimizing Data Access for Branch Offices.

4. In the **Offline Settings** window, click Cancel.
5. In the **Advanced Sharing** window, click **OK**.
6. In the **Share2 Properties** window, click **Close**.
7. Close Windows Explorer.

Demonstration: How to Configure NTFS Permissions

Demonstration Steps

Note You require the 6421B-NYC-DC1, 6421B-NYC-SVR1, and 6421B-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as Contoso\Administrator with the password of Pa$$w0rd.

▶ Configure NTFS permissions

1. On NYC- DC1, click **Start** and click **Computer**.
2. In Windows Explorer, in the left pane, click **Local Disk (C:)**.
3. Right-click **Share1** and click **Properties**.
4. In the **Share1 Properties** window, on the **Security** tab, review the groups and users that are listed. These are the NTFS permissions that are created by the simplified file sharing in the previous demonstration.
5. In the **Group or user names** box, click **Marketing** and read the permissions that are listed.
6. Click **Edit**.
7. In the **Permissions for Share1** window, click **Marketing**.
8. In the **Permissions for Marketing** area, select the **Allow Modify** permission check box and click **OK**.

▶ View Advanced NTFS Permissions

1. In the **Share1 Properties** window, click **Advanced**.
2. In the **Advanced Security Settings for Share1** window, click **Change Permissions**.
3. In the **Advanced Security Settings for Share1** window, click **Marketing** and then click **Edit.**
4. In the **Permission Entry for Share1** window, review the available options and then click **Cancel**.
5. In the **Advanced Security Settings for Share1** window, click **Cancel**.
6. In the **Advanced Security Settings for Share1** window, click the **Auditing** tab. Auditing can be used to track which users are accessing and modifying files.
7. Click the **Owner** tab. This tab allows you to change the owner of a file or folder.

8. Click the **Effective Permissions** tab. This tab allows you to view the effective NTFS permissions for a user or group when all group memberships are taken into account.
9. Click **Cancel**.
10. In the **Share1 Properties** window, click **Cancel.**

▶ View inherited permissions

1. In Windows Explorer, double-click **Share1**.
2. In the menu bar, click **New folder**.
3. To set the folder name, type **Subfolder** and press ENTER.
4. Right-click **Subfolder** and click **Properties**.
5. On the **Security** tab, click **Marketing** and review the permissions. Notice that the check marks that indicate the permissions are greyed out because they are inherited.

Lesson 2

Encrypting Network Files with EFS

Contents:

Detailed Demonstration Steps

Demonstration: How to Encrypt a File by Using EFS

Demonstration Steps

Note You require the 6421B-NYC-DC1 and 6421B-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of Pa$$w0rd unless otherwise noted.

▶ Verify that a computer account supports EFS on a network share

1. On NYC-DC1, click **Start**, point to **Administrative Tools**, and click **Active Directory Users and Computers**.
2. If necessary, expand **Contoso.com** and click **Domain Controllers**.
3. Right-click **NYC-DC1** and click **Properties**.
4. On the **Delegation** tab, verify that **Trust this computer for delegation to any service (Kerberos only)** is selected and then click **Cancel**. This setting is on by default for domain controllers, but needs to be enabled for most file servers to support EFS.
5. Close Active Directory Users and Computers.

▶ Use EFS to encrypt a file on a network share

1. On NYC-CL1, log on as Contoso**Adam** with a password of **Pa$$w0rd**.
2. Click **Start**, type **\\NYC-DC1\Share1**, and press ENTER.
3. In Windows Explorer, right-click an open area, point to **New**, and click **Microsoft Office Word Document**.
4. Type **MyEncryptedFile** and press ENTER to name the file.
5. Double-click **MyEncryptedFile** to open it.
6. If necessary, click **OK** to close the error message.
7. If necessary, click **OK** to set the user name.
8. In the document, type **My secret data** and click the **Save** button.
9. Close Word.
10. Right-click **MyEncryptedFile** and click **Properties**.
11. In the **MyEncryptedFiles Properties** window, on the **General** tab, click **Advanced**.
12. In the **Advanced Attributes** window, select the **Encrypt content to secure data** check box and click **OK**.
13. In the **MyEncryptedFiles Properties** window, click **OK**.

▶ View the certificate that is used for encryption

1. On NYC-DC1, click **Start** and click **Computer**.

2. Browse to **C:\Users**. Notice that Adam has a profile on the computer. This is where the self-signed certificate is stored. It cannot be viewed in the MMC Certificates snap-in unless Adam logs on locally to the server.
3. Browse to **C:\Users\Adam\roaming\Microsoft\SystemCertificates\My\Certificates**. This is the folder that stores the self-signed certificate for Adam.

▶ Test access to an encrypted file

1. On NYC-CL1, log on as **Don** with a password of **Pa$$w0rd**.
2. Click **Start**, type **\\NYC-DC1\Share1**, and press ENTER.
3. Double-click **MyEncryptedFile**.
4. If necessary, click **OK** to set the user name.
5. Click **OK** to clear the access denied message.
6. Close Word.

Lesson 3

Encrypting Partitions with BitLocker

Contents:

Detailed Demonstration Steps

Demonstration: How to Encrypt a Partition by Using BitLocker

Demonstration Steps

Note You require the 6421B-NYC-DC1, 6421B-NYC-SVR1, and 6421B-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**.

▶ Preparing for the demonstration

1. On the virtual host, if necessary, open **Hyper-V Manager**.
2. Right-click **6421B-NYC-DC1** and click **Settings**.
3. In the list of hardware, verify that **BitLocker.vfd** is listed. This is the virtual floppy disk that will be used as an alternative to a TPM.
4. If BitLocker.vfd is not listed, click the **Diskette Drive**, click **Browse**, select b Files\Microsoft **Learning\6421\Drives\6421B-NYC-DC1\Virtual Hard Disks\BitLocker.vfd**, and click **OK**.

▶ Install the BitLocker feature

1. On NYC-DC1, click **Start**, point to **Administrative Tools**, and click **Server Manager**.
2. In Server Manager, click **Features** and then click **Add Features**.
3. In the list of features, select the **BitLocker Drive Encryption** check box and click **Next**.
4. On the **Confirm Installation Selections** page, click **Install**.
5. On the **Results** page, click **Close**.
6. In the popup window, click **Yes** to restart.
7. When the restart is complete, log on as **Administrator** with a password of **Pa$$w0rd**.
8. Wait until installation completes, and then click **Close** and close Server Manager.

▶ Configure Bitlocker to not require a TPM

1. On NYC-DC1, click **Start**, type **gpedit.msc**, and press ENTER.
2. In the Local Group Policy Editor window, browse to **Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives**.
3. Double-click **Require additional authentication at startup**.
4. In the **Require additional authentication at startup** window, click **Enabled**.
5. Verify that the **Allow BitLocker without a compatible TPM** check box is selected and click **OK**.
6. Close the Local Group Policy Editor window.

▶ Enable BitLocker when a TPM is unavailable

1. On NYC-DC1, click **Start** and click **Control Panel**.
2. In Control Panel, click **System and Security** and click **BitLocker Drive Encryption**.

3. In the BitLocker Drive Encryption window, beside C:, click **Turn On BitLocker**. This is the window you would typically use to turn on BitLocker.

Note In the Hyper-V environment that is used for the labs, there is no way to use a virtual USB flash drive. Therefore, BitLocker must be enabled at a command prompt.

4. Close the BitLocker Drive Encryption window.
5. Click **Start**, point to **All Programs**, click **Accessories**, and click **Command Prompt**.
6. At the command prompt, type **manage-bde.exe -on C: -rp -sk A:** and press ENTER. You are required to do this at a command line because the graphical interface for BitLocker does not allow you to select a floppy disk for storing the key.
7. Restart NYC-DC1 to complete the encryption process for C:.

▶ Access the recovery password

1. Log on as **Administrator** with a password of **pa$$w0rd**.
2. Click **Start** and click **Control Panel**.
3. In Control Panel, click **System and Security** and click **BitLocker Drive Encryption**.
4. Read the status of the C: drive. Note that it is encrypting.
5. Click **Manage BitLocker**.
6. Click **Save or print recovery key again**.
7. Click **Save the recovery key to a file**, browse to **D:\Labfiles**, and click **Save**.
8. Click **Yes** to save the file in this location.
9. Close all open windows.
10. Click **Start** and click **Computer**.
11. Browse to **D:\Labfiles** and double-click the Bitlocker Recovery Key text file.
12. Review the 48-digit recovery key.
13. Close all open windows.

Lesson 4

Configuring and Troubleshooting Network Printing

Contents:

Question and Answers

Discussion: Troubleshooting Network Printing

Question: What are some common network printing problems and their resolution?

Answer: Some common network printing problems are:

- **Print jobs not displaying correctly:** This is typically caused by incorrect drivers. Try updating the driver on the server with the latest version from the manufacturer. When you update the driver for the shared printer on the server, it will be pushed out to the client.
- **Corrupted print job blocking the queue:** Sometime print jobs become corrupted and prevent other print jobs from printing. To resolve this issue, you should delete the corrupted print job. If you cannot delete the corrupted print job in the graphical interface, you may need to stop the spooler service and the delete the job manually from C:\Windows\System32\spool\PRINTERS.
- **User unable to install drivers:** You can avoid this issue by installing printer drivers for all operating systems on the print server. When a network printer is installed, the user does not need permission to install the drivers. If local printers need to be installed, the drivers can be prestaged by using pnputil to load them into the driver cache.

Detailed Demonstration Steps

Demonstration: How to Create Multiple Configurations for a Print Device

Demonstration Steps

Note You require the 6421B-NYC-DC1, 6421B-NYC-SVR1, and 6421B-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**.

▶ Task 1: Create a shared printer

1. On NYC-DC1, click **Start** and click **Devices and Printers**.
2. In the Devices and Printers window, click **Add a printer**.
3. In the Add Printer window, click **Add a local printer**.
4. On the **Choose a printer port** page, click **Next**. In a real life scenario, you would select a Standard TCP/IP port to communicate with a network printer.
5. On the **Install the printer driver** page, click **Next** to accept the default selection. In a real life scenario, you would select the driver for your printer.
6. On the **Type a printer name** page, in the **Printer name** box, type **AllUsers** and click **Next**.
7. On the **Printer Sharing** page, click **Next** to share the printer with the default settings.
8. On the **You've successfully added All Users** page, click **Finish**.

▶ Task 2: Create a second printer using the same port

1. In the Devices and Printers window, click **Add a printer**.
2. In the Add Printer window, click **Add a local printer**.
3. On the **Choose a printer port** page, click **Next**. This is the same port as was selected for the printer that was created in the previous task.
4. On the **Install the printer driver** page, click **Next** to accept the default selection, which is the same printer driver that was used for the printer that was created in the previous task.
5. On the **Which version of the driver do you want to use** page, click **Next** to reuse the same printer driver.
6. On the **Type a printer name** page, in the **Printer name** box, type **Executives** and click **Next**.
7. On the **Printer Sharing** page, click **Next** to share the printer with the default settings.
8. On the **You've successfully added Executives** page, click **Finish**.
9. In the **Devices and Printers** window, review the list of devices. Notice that only the Executives printer is listed.

▶ Task 3: Increase the priority of the second printer

1. In the **Devices and Printers** window, right-click **Executives**, point to **Printer properties**, and click **Executives**.

2. On the **Advanced** tab, in the **Priority** box, type **10** and click **OK**. Now jobs submitted to the Executives printer have higher priority that those submitted to the AllUsers printer and will be printed first.

Module Reviews and Takeaways

Review questions

Question: You are planning the configuration of NTFS and share permissions on new file server. One of your colleagues suggests that share permissions should be limited to the minimum possible rather than assigning the EVERYONE group Full Control. Why is this not a concern when NTFS permissions are used?

Answer: When NTFS permission are used to secure the data on a file share, they cannot be overridden, but more permissive share permissions. As long as NTFS permissions are configured properly, share permissions can be configured as full control. If share permissions are limited it increase the complexity of managing share permissions.

Question: Your organization has a mix of roaming users with Windows XP and Windows 7 laptops. Roaming users use a VPN to access files remotely. A user that was recently upgraded to Windows 7 remarked that file access over the VPN is much faster now. Why is this occurring?

Answer: Windows 7 and Windows Server 2008 R2 include SMB 2.1 for file sharing. This is a much faster protocol that SMB 1 in Windows XP.

Question: You are planning to enable BitLocker on the servers located in remote offices to increase security. One of your colleagues is concerned that this will increase complexity for users accessing file shares on those servers. Why is this not a valid concern?

Answer: BitLocker is completely transparent to user and applications when it is enabled. It will not increase complexity for users.

Question: Some users have been starting to encrypt files stored on network shares to protect them from other departmental users with NTFS permissions to those files. Is this an effective way to prevent users from viewing and modifying those files?

Answer: Yes. An EFS encrypted file cannot be opened or modified by unauthorized users. By default only the user that encrypted a file and the recovery agent can decrypt the file.

Question: One department in your organization has been manually adding printers on computers that perform direct IP printing to the physical printer. They are doing this so that all users automatically get access to the printer after it is installed. Can you configure a printer server and still make printers available to all users?

Answer: Yes. If you use Group Policy preferences or configured a GPO in Print Management, a printer distributed to the computer will be available to all users on that computer.

Lab Review Questions and Answers

Question: In Exercise 1, why did Adam only see the Marketing folder?

Answer: Access-based enumeration limited Adam's view of folder to only those that he has permission to access. Adam did not have permission to access the Production folder, so it was hidden.

Question: In Exercise 2, why was the Administrator account able to open the encrypted file?

Answer: The certificate that was added as the recovery agent was generated by the CA and added to the Administrator account at the same time it was added to the GPO.

Question: When two ports are enabled for a printer, how do you know where a print job will be directed?

Answer: It is not possible to predict which port will be used. That is why both physical printers should be in the same physical location.

Module 11

Optimizing Data Access for Branch Offices

Contents:

Lesson 1

Branch Office Data Access

Contents:

Question and Answers

Discussion: Challenges of Branch Office Data Access

Question: Why are network connections between branch offices and the head office relatively slow and unreliable?

Answer: The network links that provide WAN connectivity are expensive. One way that most organizations minimize costs is by purchasing the slowest acceptable speed of connectivity. Also, the distance of WAN connectivity increases latency. Finally, not all WAN connectivity is unreliable, but it typically less reliable than the internal network at the head office.

Question: How does slow and unreliable network connectivity affect the users in branch offices?

Answer: If data logon services are provided by head office, then slow and unreliable network connectivity prevents users in the branch offices from working. If connectivity to head office is not available, it prevents users from accessing data or logging on to the network. Slow connectivity prevents users from performing their work as quickly as they would like and results in lower productivity.

Question: How does management of computers systems in branch offices compare to management of computer systems in the head office?

Answer: Remote offices typically have less management of computer systems than a head office. In the smallest offices, there might be no onsite staff to assist users and perform management tasks.

Question: How does system security in branch offices compare to system security in the head office?

Answer: Often, branch offices have poor security for computer systems. In some cases, servers are not in a locked room.

Lesson 2

DFS Overview

Contents:

Detailed Demonstration Steps

Demonstration: How to Install the DFS Role

Demonstration Steps

Note You require the 6421B-NYC-DC1 and 6421B-NYC-SVR1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**.

▶ Install the DFS role

1. Switch to NYC-DC1.
2. On the task bar, click **Server Manager**.
3. In the console pane, click **Roles**.
4. In the details pane, click **Add Roles**.
5. In the Add Roles Wizard, click **Next**.
6. On the **Select Server Roles** page, select the **File Services** check box and then click **Next**.
7. On the **File Services** page, click **Next**.
8. On the **Select Role Services** page, select the check box next to **Distributed File System**. Click **Next**.
9. On the **Create a DFS Namespace** page, select the **Create a namespace later using the DFS Management snap-in in Server Manager** option and then click **Next**.
10. On the **Confirm Installation Selections** page, click **Install**.
11. On the **Installation Results** page, click **Close**.
12. Close **Server Manager**.
13. Switch to NYC-SVR1.
14. On the task bar, click **Server Manager**.
15. In the console pane, click **Roles**.
16. In the details pane, under **File Services**, click **Add Role Services**.
17. On the **Select Role Services** page, select the check box next to **Distributed File System**. Click **Next**.
18. On the **Create a DFS Namespace** page, select the **Create a namespace later using the DFS Management snap-in in Server Manager** option and then click **Next**.
19. On the **Confirm Installation Selections** page, click **Install**.
20. On the **Installation Results** page, click **Close**.
21. Close **Server Manager**.

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

Lesson 3

Configuring DFS Namespaces

Contents:

Detailed Demonstration Steps

Demonstration: How to Create Namespaces

Demonstration Steps

Note You require the 6421B-NYC-DC1 and 6421B-NYC-SVR1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**. The virtual machines should still be running from the preceding demonstration

▶ Create a new namespace

1. Switch to NYC-SVR1.
2. Click **Start**, point to **Administrative Tools**, and then click **DFS Management**.
3. In the **DFS Management** console, in the console pane, click **Namespaces**.
4. Right-click **Namespaces** and then click **New Namespace**. The New Namespace Wizard starts.
5. On the **Namespace Server** page, under **Server**, type **NYC-SVR1**. Click **Next**.
6. On the **Namespace Name and Settings** page, under **Name**, type **Research**. Click **Next**.
7. On the **Namespace Type** page, ensure that **Domain-based namespace** is selected. Also, ensure that **Enable Windows Server 2008 mode** is selected and then click **Next**.
8. On the **Review Settings and Create Namespace** page, click **Create**.
9. On the **Confirmation** page, verify that the create namespace task is successful and then click **Close**.
10. In the console pane, expand the **Namespace** node and then click **\\Contoso.com\Research**. Describe the four tabs in the details pane.
11. In the console pane, right-click **\\Contoso.com\Research** and then click **Properties**. Describe the **General**, **Referrals**, and **Advanced** tab options.
12. Click **OK** to close the **\\Contoso.com\Research Properties** dialog box.

▶ Create a new folder and folder target

1. Switch to NYC-SVR1.
2. In the DFS Management console, right-click **\\Contoso.com\Research** and then click **New Folder**.
3. In the **New Folder** dialog box, under **Name**, type **Proposals**.
4. In **New Folder** dialog box, under **Folder targets**, click **Add**.
5. In the **Add Folder Target** dialog box, type **\\NYC-SVR1\Proposal_docs** and then click **OK**.
6. In the **Warning** dialog box, click **Yes** to create the shared folder.
7. On the **Create Share** dialog box, configure the following and then click **OK**.
   - Local path of shared folder: **C:\Proposal_docs**
   - Shared folder permissions: **Administrators have full access; other users have read and write permissions**
8. In the **Warning** dialog box, click **Yes** to create the folder.

9. Click **OK** to close the **New Folder** dialog box.
10. In the console pane, expand **\\Contoso.com\Research** and then click **Proposals**. Explain that currently there is only one Folder Target. To provide redundancy, a second folder target can be added with DFS Replication configured. Also explain that this process would be repeated for each folder that is to be hosted within the namespace.
11. To test the namespace, click **Start**, and in the **Search programs and files** box, type **\\Contoso.com\Research**. Press ENTER. The **Proposals** folder is displayed.

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

Lesson 4

Configuring and Troubleshooting DFS Replication

Contents:

Detailed Demonstration Steps

Demonstration: How to Configure DFS Replication

Demonstration Steps

Note You require the 6421B-NYC-DC1 and 6421B-NYC-SVR1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**. The virtual machines should still be running from the preceding demonstration

▶ Create a new folder target for replication

1. Switch to NYC-SVR1.
2. In **DFS Management**, right-click the **Proposals** folder and then click **Add Folder Target**.
3. In the **New Folder Target** dialog box, **type \\NYC-DC1\Proposal_docs** and then click **OK**.
4. In the **Warning** dialog box, click **Yes** to create the shared folder.
5. On the **Create Share** dialog box, configure the following and then click **OK**.
   - Local path of shared folder: **C:\Proposal_docs**
   - Shared folder permissions: **Administrators have full access; other users have read and write permissions**
6. In the **Warning** dialog box, click **Yes** to create the folder.
7. At the **Replication** dialog box, click **Yes** to create a replication group. The Replicate Folder Wizard starts.

▶ Create a new replication group

1. In the Replicate Folder Wizard, on the **Replication Group and Replicated Folder Name** page, accept the default entries for **Replication group name** and **Replicated folder name**. Click **Next**.
2. On the **Replication Eligibility** page, take note that NYC-DC1 and NYC-SVR1 are eligible as DFS replication members. Click **Next**.
3. On the **Primary Member** page, select **NYC-SVR1** as the primary member. Click **Next**.
4. On the **Topology Selection** page, leave the default selection of **Full mesh**, which will replicate all data between all members of the replication group. If you had three or more members within the replication group, you can also choose **Hub and spoke**, which allows you to configure a publication scenario where data is replicated from a common hub to the rest of the members. You can also choose **No topology**, which allows you to configure the topology at a later time. Click **Next**.
5. On the **Replication Group Schedule and Bandwidth** page, leave the default selection of **Replicate continuously**. Then, configure the setting to use Full bandwidth. Note that you can also choose a specific schedule to replicate during specified days and times. Click **Next**.
6. On the **Review Settings and Create Replication Group** page, click **Create**.
7. On the **Confirmation** page, ensure that all tasks are successful and then click **Close**. Take note of the **Replication Delay** warning and then click **OK**.

8. In the console pane, expand **Replication**.
9. Under **Replication**, click **contoso.com\research\proposals**. Click and discuss each of the tabs in the details pane.

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

Lesson 5

Configuring BranchCache

Contents:

Detailed Demonstration Steps

Demonstration: How to Configure BranchCache Mode

Demonstration Steps

Note You require the 6421B-NYC-DC1, 6421B-NYC-SVR1, and 6421B-NYC-CL1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**. The virtual machines should still be running from the preceding demonstration.

▶ Enable BranchCache on a File Server

1. Switch to NYC-DC1.
2. Click **Start**, point to **Administrative Tools**, and click **Server Manager**.
3. In the left pane, expand **Roles** and click **File Services**.
4. If necessary, scroll down to **Role Services** and click **Add Role Services**.
5. On the **Select Role Services** page, select the **BranchCache for network files** check box and click **Next**.
6. On the **Confirm Installation Selections** page, click **Install**.
7. On the **Installation Results** page, click **Close**.
8. Close Server Manager.
9. Click **Start**, type **gpedit.msc**, and press ENTER.
10. Browse to **Computer Configuration\Administrative Templates\Network\Lanman Server** and double-click **Hash Publication for BranchCache**.
11. In the **Hash Publication for BranchCache** window, click **Enabled**.
12. In the **Options** box, select **Allow hash publication only for shared folder on which BranchCache is enabled** and then click **OK**.
13. Close the Local Group Policy Editor.
14. Open Windows Explorer from the taskbar and browse to **C:**.
15. Click **New Folder**, type **Share**, and then press ENTER
16. Right-click **Share** and click **Properties**.
17. In the Share Properties window, click the **Sharing** tab and click **Advanced Sharing**.
18. In the Advanced Sharing window, click **Caching**.
19. In the Offline Settings window, select the **Enable BranchCache** check box and then click **OK**.
20. Close all open windows.

Note Revert all virtual machines.

Module Reviews and Takeaways

Review questions

1. How can you use DFS in your File Services deployment?

Answer: You can use DFS to provide DFS namespaces and file replication. DFS namespaces provide a virtual view of shared folders on different servers. DFS replication provides high-availability and fault-tolerance to files and folders.

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

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

3. What kind of compression technology is used by Windows Server 2008 DFS?

Answer: Windows Server 2008 uses Remote Differential Compression to help optimize data transfers over limited-bandwidth networks.

4. How does BranchCache differ from DFS?

Answer: BranchCache only caches files that users in a remote location have accessed. DFS replicates files between head office and a remote location so that all files exist in both locations.

5. Why would you want to implement BranchCache in hosted cache mode rather than distributed cache mode?

Answer: When distributed cache mode is used, the cache is distributed among all Windows 7 computers. However, it is likely that Windows 7 computers will be turned off or laptop computers will be removed from the office. This means that a cached file might not be available, forcing the file to be downloaded across the WAN link again. Hosted cache mode keeps the cached files on a file server that will always be available.

Lab Review Questions and Answers

Question: What are the requirements for deploying a namespace in Windows Server 2008 mode?

Answer: The domain must use Windows Server 2008 domain functional level, and all namespace servers must be running Windows Server 2008.

Question: What are the benefits of hosting a namespace on several namespace servers?

Answer: Hosting a namespace on several namespace servers increases availability in the event that a namespace server fails. Users will still be able to access the namespace by using one of the remaining namespace servers.

Question: In the lab, you moved NYC-SVR1 to its own OU. Why?

Answer: The client configuration settings were configured in the Default Domain Policy that is linked to the root of the domain. Those Group Policy settings prevent hosted mode from being configured on NYC-SVR1. By moving NYC-SVR1 to its own OU enabled you to block inheritance of Group Policy to that OU and prevent those settings from applying to NYC-SVR1.

Module 12

Controlling and Monitoring Network Storage

Contents:

Lesson 1

Monitoring Network Storage

Contents:

Question and Answers

Discussion: Storage Management Challenges

Question: What are some of the storage management challenges in your organization?

Answer: Some storage management challenges are:

- Determining existing storage use. Many organizations do not have an automated method for identifying how much storage is in use, and just as importantly, how much storage is free.
- Establishing and enforcing storage use policies. Many organizations have no way to control the amount of storage used by individual users or departments other than the size of the disk.
- Anticipating future requirements. If an organization does not track storage use over time, they cannot identify usage trends and plan to expand storage in a timely way.

Detailed Demonstration Steps

Demonstration: How to Install and Configure FSRM

Demonstration Steps

Note You require the 6421B-NYC-DC1 and 6421B-NYC-SVR1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**.

Install FSRM

1. On NYC-SVR1, click **Start**, point to **Administrative Tools**, and click **Server Manager**.
2. In Server Manager, in the left pane, expand **Roles**, click **File Services**, and then click **Add Role Services**.
3. In the Add Role Services window, select the **File Server Resource Manager** check box and click Next.
4. On the **Configure Storage Usage Monitoring** page, click **Next**.
5. On the **Confirmation** page, click **Install**.
6. On the **Results** page, click **Close**.

View FSRM Configuration Options

1. On NYC-SVR1, click **Start**, click **Administrative Tools**, and then click **File Server Resource Manager**.
2. In the left hand pane in the File Server Resource Manager window, right-click on **File Server Resource Manager (Local)** and then click **Configure Options**.
3. Click on each of the tabs in the File Server Resource Manager Options window, observing the options that are available in each tab. Close the File Server Resource Manager Options window.
4. In the left-hand pane in the File Server Resource Manager, expand each of the components and view the details for each sub-node.

Lesson 2

Controlling Network Storage Utilization

Contents:

Detailed Demonstration Steps

Demonstration: How to Create and Configure a Quota

Demonstration steps

Note You require the 6421B-NYC-DC1 and 6421B-NYC-SVR1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password **Pa$$w0rd**.

▶ Prepare for the demonstration

1. Click **Start**, type **cmd**, and press ENTER.
2. At the command prompt, type **md C:\Projects** and press ENTER.
3. At the command prompt, type **net share Projects=C:\Projects** and press ENTER.
4. Close the command prompt.

▶ 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 **Project Folders 1 GB**.
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. In the **Notification thresholds** area, 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 the **Send warning to event log** check box and then click **OK**. Click **Yes** to dismiss the warning about SMTP server configuration. If students are interested, show them how to configure the SMTP server that is 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.

▶ Create a new quota based on a quota template

1. In the details pane, right-click **Project Folders 1 GB** and then click **Create Quota from Template**.
2. In the **Quota path** field, type **C:\Projects** and click **Auto apply template and create quotas on existing and new subfolders**.
3. Click **Create**.

▶ Generate a quota notification

1. Click **Start**, type **cmd**, and then press ENTER.
2. Type **md C:\Projects\Project1** and then press ENTER.
3. Type **cd C:\Projects\Project1** and then press ENTER.
4. Type **fsutil file createnew largefile.txt 1300000000** and then press ENTER.
5. Click **Start**, click **Administrative Tools**, and then click **Event Viewer**.
6. In Event Viewer, expand **Windows Logs** and then click **Application**.
7. Note the event with Event ID of 12325.
8. Close all open windows on NYC-SVR1.

Lesson 3

Managing File Types on Network Storage

Contents:

Detailed Demonstration Steps

Demonstration: How to Implement File Screening

Demonstration steps

Note You require the 6421B-NYC-DC1 and 6421B-NYC-SVR1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password **Pa$$w0rd**.

▶ 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**. These are typically media files such as mp3.
6. In the **Files to exclude** field, type ***.mpp** and then click **Add**. These are Microsoft Project files.
7. Click **OK**.

▶ Create a File Screen Template

1. In the File Server Resource Manager console tree, click on **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, click the check box to select the **MPx Media Files** File Group.
6. Click the **Event Log** tab.
7. Click the check box to select **Send warning to event log** and then click **OK**.

▶ Create a File Screen

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 **C:\Projects** 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.

▶ Test the File Screen

1. Click **Start**, and then click **Computer**.
2. Browse to the **Documents** library.
3. In the right hand pane, right-click the empty space, point to **New**, and click **Text Document**.
4. Rename **New Text Document.txt** to **musicfile.mp3**.
5. Right-click **musicfile.mp3** and then click **Copy**.
6. Browse to **C:\Projects**.
7. In the right hand pane, right-click the empty space and then click **Paste**.
8. A warning appears that the destination folder access is denied. Click **Cancel** and then close Windows Explorer.

Demonstration: How to Configure File Classification

Demonstration steps

Note You require the 6421B-NYC-DC1 and 6421B-NYC-SVR1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password **Pa$$w0rd**.

▶ 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 on **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**.

▶ Create a Classification Rule

1. Click on the **Classification Rules** node.
2. Right-click the **Classification Rules** node and then click **Create a New Rule**.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** area, click the **Add** button.
6. In the Browse for Folder window, expand **Local Disk (C:)**, click **Projects**, 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**.

▶ Create a File Containing the Word Payroll

1. Click **Start** and click **Computer**.
2. Browse to **C:\Projects**.
3. Right-click an open area, point to **New**, and click **Text Document**.
4. Type **January** and press ENTER to rename the file January.txt.
5. Double-click **January.txt** to open it.
6. In Notepad, type **Payroll information for January**.
7. Close Notepad and save the changes.
8. Close Windows Explorer.

▶ Modify the Classification Schedule

1. In File Server Resource Manager, right-click the **Classification Rules** node and then click **Configure Classification Schedule**.
2. In the File Server Resource Manager Options window, ensure that 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. Close all open windows on NYC-SVR1.

Module Reviews and Takeaways

Review questions

Question: You want to use file classification and file management to expire certain documents on all the file servers in your organization. Are there any limitations on where you can file classifications and file management?

Answer: Yes, file classification and file management are only available in Windows Server 2008 R2. It cannot be used on Windows Server 2008 file servers.

Question: You want to use file management to expire old documents on departmental file shares. A colleague is concerned that deleting files without authorization will generate complaints from the departments.

Answer: Your colleague is correct. Departments must be consulted before a policy like this is put into place. The departments must play a role in defining how files will be selected for removal and any requirements for archiving.

Question: You have implemented file screening to prevent users from storing video files on in the shared data volume that contains departmental folders. However, the Marketing department needs to store video files in their departmental folder. How can you allow this?

Answer: Create a file screening exception for the Marketing department's folder that allows video files. A file screening exception overrides a file screen.

Question: You have proposed that FSRM quotas be used to control the size of departmental file shares. A colleague has experience with NTFS quotas and does not think that quotas are practical to use because they are based on file ownership. What can you tell your colleague about FSRM quotas to overcome this objection?

Answer: FSRM quotas are not based on file ownership. FRSM quotas can be applied directly to a folder to limit the size of that folder, regardless of which users are owners of the files.

Question: The data in a departmental file share has grown by 10 GB in a single day. Typically, growth is less than 1 GB. You are concerned that a user has placed several large files in the departmental file share. How can you confirm this?

Answer: You can use the Large Files storage report to identify large files in the share. You can also use the Most Recently Accessed Files storage report to identify recently created files.

Lab Review Questions and Answers

Question: When you created the quota on the Home share, why did you select the option **Auto apply template and create quotas on existing and new subfolders**?

Answer: That option configures the quota to apply to subfolders. By selecting that option, the quota is applied to each user's home folder.

Question: What is the difference between active screening and passive screening?

Answer: Active screening prevents users from saving files that match the file screen. Passive screening allows the file to be saved and only sends a notification.

Question: Why is it important to schedule file management tasks?

Answer: If a file management task is not scheduled, then it is likely that the task will never be run or run irregularly. Automating the process ensures that file management is performed in a timely way.

Module 13

Recovering Network Data and Servers

Contents:

Lesson 1

Recovering Network Data with Shadow Copies

Contents:

Detailed Demonstration Steps

Demonstration: How to Configure Shadow Copies

Demonstration steps

Note You require the 6421B-NYC-DC1 virtual machine to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**.

▶ Enable shadow copies on C:

1. On NYC-DC1, click **Start** and click **Computer**.
2. In Windows Explorer, right-click **Local Disk (C:)** and click **Configure Shadow Copies**.
3. In the Shadow Copies window, click **C:** and click **Enabled**.
4. In the Enable Shadow Copies window, click **Yes**.

▶ View settings for shadow copies

1. In the Shadow Copies window, click **Settings**.
2. Point out that the maximum size allocated is 10 percent of the disk space.
3. Click **Schedule** and click the drop down list to show that shadow copies will be created at 07:00 A.M. and noon.
4. Close all open windows.

Demonstration: How to Restore Data from a Shadow Copy

Demonstration steps

Note You require the 6421B-NYC-DC1 virtual machine to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**.

▶ Create a new file

1. On NYC-DC1, click **Start** and click **Computer**.
2. Browse to **C:** and click **New folder**.
3. Type **Data** and press ENTER to rename the new folder.
4. Browse to **C:\Data**.
5. Right-click an open area, point to **New**, and click **Text Document**.
6. Type **TestFile** and press ENTER to rename the file.
7. Double-click **TestFile.txt** to open the document.
8. In Notepad, type **Version 1**.
9. Close Notepad and click **Save** to save the changes.

▶ Create a shadow copy

1. In Windows Explorer, right-click **Local Disk (C:)** and click **Configure Shadow Copies**.
2. In the Shadow Copies window, click **Create Now**.
3. When the shadow copy is complete, click **OK**.

▶ Modify the file

1. In Windows Explorer, double-click **TestFile.txt** to open the document.
2. In Notepad, type **Version 2**.
3. Close Notepad and click **Save** to save the changes.

▶ Restore a previous version

1. In Windows Explorer, right-click **TestFile.txt** and click **Restore previous versions**.
2. In the TestFile.txt Properties window, on the **Previous Versions** tab, click the most recent file version and click **Restore**.
3. In the warning window, click **Restore**.
4. Click **OK** to close the success message.
5. Click **OK** to close the TestFile.txt Properties window.
6. Double-click **TestFile.txt** to open the document and verify that the previous version is restored.
7. Close all open windows.

Module Reviews and Takeaways

Review questions

Question: All of the file servers in your organization are using the default configuration for shadow copies. A user accidentally deleted content from a file and then saved it at 11:00. Can you restore the correct version from a shadow copy?

Answer: The default configuration for shadow copies takes a snapshot at 07:00 and noon. You can restore a version of the file from 07:00. Any changes made since 07:00 would be lost.

Question: All of the file servers in your organization are using the default configuration for shadow copies. A user accidentally deleted a file several weeks ago, but did not realize it until today. Is it possible to recover this file from a shadow copy?

Answer: Possibly. Shadow copies are allocated a specific amount of disk space. If the changes since the time those files were deleted are less the amount of disk space that has been allocated, then the files are recoverable from a shadow copy. There is not a specific time period that a shadow copy is valid for.

Question: Your organization has determined that four hours each week are used restoring user files from backup or shadow copy. A colleague has suggested training users to perform restores from shadow copies to reduce the workload of the help desk. Is this a good idea?

Answer: It is possible for user to perform restores from a shadow copy. However, users must be aware of the ramifications of restoring files from a shadow copy, including the potential loss of current data in a file. Many organizations prefer to let the help desk or administrators perform this task.

Question: Your organization has opened a new branch office with a single server. The server has a SQL database that is used by a local application. Can Windows Server Backup be used to back up and restore the database?

Answer: Yes, Windows Server Backup has the ability to perform backups of applications including SQL Server. It uses the SQL VSS writer to ensure that backups are consistent and to truncate transaction logs.

Question: You have configured a new server to perform a daily backup to a network share on another server. This is a temporary solution until your standard backup software is in place. After several days, you need to restore a file, but there is only the most recent backup to select from, not multiple days as you expected. Why did this occur?

Answer: When backing up to a network share, Windows Server Backup cannot use the shadow copy capability to keep multiple backup versions; that can only be performed on a local disk or external hard drive.

Lab Review Questions and Answers

Question: Why did you need to go to the properties of the share to restore a deleted file from a shadow copy?

Answer: To restore a deleted file, you do so from the properties of the folder that contained the file. In this case, the file was in the root folder of the share. Therefore, the deleted file is restored from the properties of the share.

Question: When you performed the second backup, why did the disk space in use not increase on the destination drive?

Answer: Windows Server Backup is able to keep track of which data has changed and only the changed data is added to the destination drive. In this case, minimal data had changed on the disk between the two backups.

Module 14

Monitoring Windows Server 2008 Network Infrastructure Servers

Contents:

Lesson 2

Using Performance Monitor

Contents:

Detailed Demonstration Steps

Demonstration: How to Capture Counter Data with a Data Collector Set

Demonstration steps

Note You require the 6421B-NYC-DC1 and 6421B-NYC-SVR1 virtual machines to complete this demonstration. Log on to both virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**.

▶ Create a data collector set

1. Switch to the NYC-SVR1 computer.
2. Click **Start**, point to **Administrative Tools,** and then click **Performance Monitor**.
3. In **Performance Monitor**, in the navigation pane, expand **Data Collector Sets** and then click **User Defined**.
4. Right-click **User Defined**, point to **New,** and then click **Data Collector Set**.
5. In the **Create New Data Collector Set** wizard, in the **Name** box, type **NYC-SVR1 Performance**.
6. Click **Create manually (Advanced)** and then click **Next**.
7. On the **What type of data do you want to include?** page, select the **Performance counter** check box and then click **Next**.
8. On the **Which performance counters would you like to log?** page, click **Add**.
9. In the **Available counters** list, expand **Processor**, click **% Processor Time**, and then click **Add >>**.
10. In the **Available counters** list, expand **Memory**, click **Pages/sec**, and then click **Add >>.**
11. In the **Available counters** list, expand **PhysicalDisk**, click **% Disk Time**, and then click **Add >>**.
12. Click **Avg. Disk Queue Length** and then click **Add >>**.
13. In the **Available counters** list, expand **System**, click **Processor Queue Length**, and then click **Add >>**.
14. In the **Available counters** list, expand **Network Interface**, click **Bytes Total/sec**, click **Add >>**, and then click **OK.**
15. On the **Which performance counters would you like to log?** page, in the **Sample interval** box, type **1** and then click **Next**.
16. On the **Where would you like the data to be saved?** page, click **Next**.
17. On the **Create the data collector set?** page, click **Save and close** and then click **Finish**.
18. In Performance Monitor, in the Results pane, right-click **NYC-SVR1 Performance** and then click **Start**.

▶ Create a disk load on the server

1. On the Windows Taskbar, click **Start**, and in the **Search** box, type **cmd.exe** and press ENTER.
2. At the command prompt, type the following command and press ENTER:

```
Fsutil file createnew bigfile 104857600
```

3. At the command prompt, type the following command and press ENTER:

```
Copy bigfile \\nyc-dc1\c$
```

4. At the command prompt, type the following command and press ENTER:

```
Copy \\nyc-dc1\c$\bigfile bigfile2
```

5. At the command prompt, type the following command and press ENTER:

```
Del bigfile*.*
```

6. At the command prompt, type the following command and press ENTER:

```
Del \\nyc-dc1\c$\bigfile*.*
```

7. Close the command prompt.

▶ Analyze the resulting data in a report

1. Switch to Performance Monitor.
2. In the navigation pane, right-click **NYC-SVR1 Performance** and then click **Stop**.
3. In Performance Monitor, in the navigation pane, click **Performance Monitor**.
4. On the toolbar, click **View log data**.
5. In the **Performance Monitor Properties** dialog box, on the **Source** tab, click **Log files** and then click **Add**.
6. In the **Select Log File** dialog box, double-click **Admin**.
7. Double-click **NYC-SVR1 Performance**, double-click the **NYC-SVR1_date-00001** folder and then double-click **DataCollector01.blg**.
8. Click the **Data** tab and then click **Add**.
9. In the **Add Counters** dialog box, in the **Available counters** list, expand **Memory**, click **Pages/sec** and then click **Add >>**.
10. Expand **Network Interface**, click **Bytes Total/sec**, and then click **Add >>**.
11. Expand **PhysicalDisk**, click **%Disk Time**, and then click **Add >>**.
12. Click **Avg. Disk Queue Length** and then click **Add >>**.
13. Expand **Processor**, click **%Processor Time**, and then click **Add >>**.
14. Expand **System**, click **Processor Queue Length**, click **Add >>**, and then click **OK**.
15. In the **Performance Monitor Properties** dialog box, click **OK**.
16. On the toolbar, click the down arrow and then click **Report**.

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

Demonstration: How to Configure an Alert

Demonstration steps

Note You require the 6421B-NYC-DC1 and 6421B-NYC-SVR1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**. The virtual machines should still be running from the preceding demonstration

▶ Create a data collector set with an alert counter

1. Switch to the NYC-SVR1 computer.
2. In Performance Monitor, in the navigation pane, expand **Data Collector Sets** and then click **User Defined**.
3. Right-click **User Defined**, point to **New,** and then click **Data Collector Set**.
4. In the Create New Data Collector Set Wizard, in the **Name box**, type **NYC-SVR1 Alert**.
5. Click **Create manually (Advanced)** and then click **Next**.
6. On the **What type of data do you want to include?** page, click **Performance Counter Alert** and then click **Next**.
7. On the **Which performance counters would you like to monitor?** page, click **Add**.
8. In the **Available counters** list, expand **Processor**, click **%Processor Time**, click **Add >>**, and then click **OK**.
9. On the **Which performance counters would you like to monitor?** page, in the **Alert when** list, click **Above**.
10. In the **Limit** box, type **10** and then click **Next**.
11. On the **Create the data collector set?** page, click **Finish**.
12. In the navigation pane, expand the **User Defined** node and then click **NYC-SVR1 Alert**.
13. In the Results pane, right-click **DataCollector01** and then click **Properties**.
14. In the **DataCollector01 Properties** dialog box, in the **Sample interval box**, type **1** and then click the **Alert Action** tab.
15. Select the **Log an entry in the application event log** check box and then click **OK**.
16. In the navigation pane, right-click **NYC-SVR1** Alert and then click **Start**.

▶ Generate a load on the server to exceed configured threshold

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

```
C:

Cd\Labfiles
```

3. At the command prompt, type the following command and press ENTER:

```
StressTool 95
```

4. Wait for one minute to allow for alerts to be generated.
5. Press CTRL+C.
6. Close the command prompt.

▶ Examine event log for resulting event

1. Click **Start**, point to **Administrative Tools**, and then click **Event Viewer**.
2. In Event Viewer, in the navigation pane, expand **Windows Logs** and then click **Application**.
3. Examine the log for performance-related messages.

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

Demonstration: How to View Performance Monitor Reports

Demonstration steps

Note You require the 6421B-NYC-DC1 and 6421B-NYC-SVR1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**. The virtual machines should still be running from the preceding demonstration

▶ View a performance report

1. In the navigation pane, expand **Reports**, expand **User Defined**, and then click **NYC-SVR1 Performance**.
2. Expand the folder beneath NYC-SVR1 Performance. This was the report that was generated by the previous Data Collector Set collection process. You can change from the chart view to any other supported view.
3. Close all open windows.

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

Lesson 3

Monitoring Event Logs

Contents:

Detailed Demonstration Steps

Demonstration: How to Create a Custom View

Demonstration Steps

Note You require the 6421B-NYC-DC1 and 6421B-NYC-SVR1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**. The virtual machines should still be running from the preceding demonstration

▶ View Server Roles custom views

1. Switch to Event Viewer.
2. In the navigation pane, expand **Custom Views**, expand **Server Roles**, and then click on **File Server**. This is the File Server role-specific custom view.

▶ Create a custom view

1. In the navigation pane, right-click **Custom Views** and then click **Create Custom View**.
2. In the **Create Custom View** dialog box, select the **Critical**, **Warning**, and **Error** check boxes.
3. In the **Event logs** list, expand **Windows Logs** and then select the **System** and **Application** check boxes. Click the mouse back in the **Create Custom View** dialog box and then click **OK**.
4. In the **Save Filter to Custom View** dialog box, in the **Name** box, type **Errors and warnings** and then click **OK**.
5. In Event Viewer, in the right pane, view the events that are visible within your Custom View.

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

Demonstration: How to Configure an Event Subscription

Demonstration Steps

Note You require the 6421B-NYC-DC1 and 6421B-NYC-SVR1 virtual machines to complete this demonstration. Log on to the virtual machines as **Contoso\Administrator** with the password of **Pa$$w0rd**. The virtual machines should still be running from the preceding demonstration

▶ Configure the source computer

1. Switch to NYC-DC1.
2. Click **Start**, and in the **Search** box, type **cmd.exe** and press ENTER.
3. At the command prompt, type the following command and then press ENTER:

```
winrm quickconfig
```

4. When prompted, type **Y** and press ENTER.

5. Click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
6. In Active Directory Users and Computers, in the navigation pane, click **Builtin**.
7. In the results pane, double-click **Administrators**.
8. In the **Administrators Properties** dialog box, click the **Members** tab.
9. Click **Add**, and in the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, click **Object Types**.
10. In the **Object Types** dialog box, select the **Computers** check box and then click **OK**.
11. In the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, in the **Enter the object names to select** box, type **nyc-svr1** and then click **OK**.
12. In the **Administrator Properties** dialog box, click **OK**.

▶ Configure the collector computer

1. Switch to NYC-SVR1.
2. Click **Start**, and in the **Search** box, type **cmd.exe** and press ENTER.
3. At the command prompt, type the following command and then press ENTER.

```
Wecutil qc
```

4. When prompted, type **Y** and press ENTER.

▶ Create and view the subscribed log

1. In the Event Viewer, in the navigation pane, click **Subscriptions**.
2. Right-click **Subscriptions** and then click **Create Subscription**.
3. In the **Subscription Properties** dialog box, in the **Subscription name** box, type **NYC-DC1 Events**.
4. Click **Collector Initiated** and then click **Select Computers**.
5. In the **Computers** dialog box, click **Add Domain Computers**.
6. In the **Select Computer** dialog box, in the **Enter the object name to select** box, type **NYC-DC1** and then click **OK**.
7. In the **Computers** dialog box, click **OK**.
8. In the **Subscription Properties – NYC-DC1 Events** dialog box, click **Select Events**.
9. In the **Query Filter** dialog box, select the **Critical**, **Warning**, **Information**, **Verbose**, and **Error** check boxes.
10. In the **Logged** list, click **Last 30 days**.
11. In the **Event logs** list, select **Windows Logs**. Click the mouse back in the **Query Filter** dialog box and then click **OK**.
12. In the **Subscription Properties – NYC-DC1 Events** dialog box, click **OK**.
13. In Event Viewer, in the navigation pane, expand **Windows Logs**.
14. Click **Forwarded Events**.

Note Revert all virtual machines.

Module Reviews and Takeaways

Review questions

1. What significant counters should you monitor in Windows Server Performance Monitor?

Answer: Processor>% Processor Time

System>Processor Queue Length

Memory>Pages/sec

Physical Disk>%Disk time

Physical Disk>Average Disk Queue Length

2. Why is it important to monitor server performance periodically?

Answer: Helps you to perform capacity planning, identify and remove performance bottlenecks, and assist with server troubleshooting.

3. Why use Performance alerts?

Answer: Using alerts enables you to react more quickly to emerging performance-related problems, perhaps before they have a chance to impinge on users' productivity.

Lab Review Questions and Answers

Question: During the lab, you collected data in a data collector set. What is the advantage of collecting data in this way?

Answer: By collecting data in data collector sets, you can analyze and compare the data against historical data and draw conclusions over server capacity.

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 msupport@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.