6421A
Configuring and Troubleshooting a Windows Server® 2008 Network Infrastructure

Be sure to access the extended learning content on your Course Companion CD enclosed on the back cover of the book.
MICROSOFT LICENSE TERMS

OFFICIAL MICROSOFT LEARNING PRODUCTS COURSEWARE – BLENDED LEARNING COURSE - STUDENT EDITION

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. 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:**

© 2007 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.

4. 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.

5. 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;
- 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.

6. BACKUP COPY. You may make one backup copy of the licensed content. You may use it only to reinstall the licensed content.

7. TRANSFER TO ANOTHER DEVICE. You may uninstall the licensed content and install it on another device for your use. You may not do so to share this license between devices.

8. TRANSFER TO A THIRD PARTY. 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.

9. **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](http://www.microsoft.com/exporting).

10. **NOT FOR RESALE SOFTWARE/LICENSED CONTENT.** You may not sell software or licensed content marked as “NFR” or “Not for Resale.”

11. **TERMINATION.** Without prejudice to any other rights, Microsoft may terminate this agreement if you fail to comply with the terms and conditions of these license terms. Upon any termination of this agreement, you must destroy all copies of the licensed content and all of its component parts.

12. **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.

13. **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.

14. **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.

15. **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.
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 des consommateurs, que ce contrat ne peut modifier. La ou elles sont permises par le droit local, 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.
# Contents

## About This Course

### Module 1: Installing and Configuring Serve

- **Lesson 1:** Installing Windows Server 2008  
  1-3
- **Lesson 2:** Managing Server Roles and Features  
  1-12
- **Lesson 3:** Overview of the Server Core Installation Option  
  1-17
- **Lab:** Installing and Configuring Servers and Server Roles  
  1-25

### Module 2: Configuring and Troubleshooting DNS

- **Lesson 1:** Installing the DNS Server Role  
  2-3
- **Lesson 2:** Configuring the DNS Server Role  
  2-9
- **Lesson 3:** Configuring DNS Zones  
  2-20
- **Lesson 4:** Configuring DNS Zone Transfers  
  2-27
- **Lesson 5:** Managing and Troubleshooting DNS  
  2-32
- **Lab:** Configuring and Verifying a DNS Solution  
  2-39

### Module 3: Configuring and Managing WINS

- **Lesson 1:** Installing the Windows Internet Name Service  
  3-3
- **Lesson 2:** Managing the WINS Server  
  3-13
- **Lesson 3:** Configuring WINS Replication  
  3-22
- **Lesson 4:** Migrating from WINS to DNS  
  3-28
- **Lab:** Configuring a WINS Infrastructure  
  3-35

### Module 4: Configuring and Troubleshooting DHCP

- **Lesson 1:** Overview of the DHCP Server Role  
  4-3
- **Lesson 2:** Configuring DHCP Scopes and Options  
  4-11
- **Lesson 3:** Managing a DHCP Database  
  4-22
- **Lesson 4:** Monitoring and Troubleshooting DHCP  
  4-30
- **Lesson 5:** Securing DHCP  
  4-38
Lab: Configuring and Troubleshooting the DHCP Server Role 4-43

Module 5: Configuring and Troubleshooting IPv6 TCP/IP
Lesson 1: Overview of IPv6 5-3
Lesson 2: Coexistence with IPv6 5-17
Lesson 3: IPv6 Tunneling Technologies 5-25
Lab A: Configuring an ISATAP Router 5-32
Lesson 3: IPv6 Tunneling Technologies (continued) 5-39
Lesson 4: Transitioning from IPv4 to IPv6 5-44
Lesson 5: Troubleshooting IPv6 5-47
Lab B: Converting the Network 5-52

Module 6: Configuring and Troubleshooting Routing and Remote Access
Lesson 1: Configuring Network Access 6-3
Lesson 2: Configuring VPN Access 6-12
Lesson 3: Overview of Network Policies 6-22
Lesson 4: Overview of the Connection Manager Administration Kit 6-27
Lesson 5: Troubleshooting Routing and Remote Access 6-33
Lab: Configuring and Managing Network Access 6-41

Module 7: Installing, Configuring, and Troubleshooting the Network Policy Server Role Service
Lesson 1: Installing and Configuring a Network Policy Server 7-3
Lesson 2: Configuring RADIUS Clients and Servers 7-9
Lesson 3: NPS Authentication Methods 7-16
Lesson 4: Monitoring and Troubleshooting a Network Policy Server 7-22
Lab: Configuring and Managing Network Policy Server 7-27

Module 8: Configuring Network Access Protectio
Lesson 1: Overview of Network Access Protection 8-3
Lesson 2: How NAP Works 8-18
Lesson 3: Configuring NAP 8-27
Lesson 4: Monitoring and Troubleshooting NAP 8-34
Lab: Configuring NAP for DHCP and VPN 8-38

Module 9: Configuring IPsec
Lesson 1: Overview of IPsec 9-3
Lesson 2: Configuring Connection Security Rules 9-11
Lesson 3: Configuring IPsec NAP Enforcement 9-21
Lab: Configuring IPsec 9-26

Module 10: Monitoring and Troubleshooting IPsec
Lesson 1: Monitoring IPsec Activity 10-3
Lesson 2: Troubleshooting IPsec 10-8
Lab: Monitoring and Troubleshooting IPsec 10-12

Module 11: Configuring and Managing Distributed File System
Lesson 1: DFS Overview 11-3
Lesson 2: Configuring DFS Namespaces 11-15
Lesson 3: Configuring DFS Replication 11-25
Lab: Configuring DFS 11-39

Module 12: Configuring and Managing Storage Technologies
Lesson 1: Overview of Windows Server 2008 Storage Management 12-3
Lesson 2: Managing Storage Using File Server Resource Manager 12-8
Lesson 3: Configuring Quota Management 12-16
Lesson 4: Implementing File Screening 12-25
Lesson 5: Managing Storage Reports 12-31
Lab: Configuring and Managing Storage Technologies 12-36
Module 13: Configuring Availability of Network Resources and Content
  Lesson 1: Backing Up Data 13-3
  Lesson 2: Configuring Shadow Copies 13-13
  Lesson 3: Providing Server and Service Availability 13-20
  Lab: Configuring Availability of Network Resources 13-31

Module 14: Configuring Server Security Compliance
  Lesson 1: Securing a Windows Infrastructure 14-3
  Lesson 2: Using Security Templates to Secure Servers 14-11
  Lesson 3: Configuring an Audit Policy 14-17
  Lesson 4: Overview of Windows Server Update Services 14-22
  Lesson 5: Managing WSUS 14-30
  Lab: Configuring Server Security Compliance 14-35
About This Course

This section provides you with a brief description of the course, audience, suggested prerequisites, and course objectives.

Course Description

The purpose of this 5-day course is to teach Active Directory Technology Specialists how to implement and configure secure network access and implement fault tolerant storage technologies, understand the network technologies most commonly used with Windows Server 2008 and IP-enabled network, and how to secure servers and maintain update compliance. After completing this course, students will be able to configure and troubleshoot a Windows Server 2008 network infrastructure.

Audience

The primary audience for this course includes Active Directory technology specialists aspiring to be Enterprise Administrators (Tier 4 day-to-day network operations) or Network Administrators (Tier 2). Experienced Server Administrators aspiring to be Enterprise Administrators would also benefit from this course.

The secondary audience for this course includes Storage Area Network Administrators who need to understand this information to deploy or extend their current storage infrastructure. Operations Managers who need this information to support troubleshooting efforts and business decisions would also benefit from this course.

Student Prerequisites

This course requires that you meet the following prerequisites:

- Basic knowledge of Active Directory.
- An understanding of security concepts and methodologies (for example, corporate policies).
- Basic knowledge of DHCP.
- Basic knowledge of IPSec.
Course Objectives
After completing this course, students will be able to:

- Install and configure servers.
- Configure and troubleshoot DNS.
- Configure and manage WINS.
- Configure and troubleshoot DHCP.
- Configure and troubleshoot IPv6 TCP/IP.
- Configure and troubleshoot Routing and Remote Access.
- Install, configure, and troubleshoot the Network Policy Server Role service.
- Configure Network Access Protection.
- Configure IPSec.
- Monitor and troubleshoot IPSec.
- Configure and manage Distributed File System.
- Configure and manage storage technologies.
- Configure availability of network resources and content.
- Configure server security compliance.

Course Outline
This section provides an outline of the course:

Module 1: This module explains how to identify the appropriate usage scenario and installation type for a server and then install and configure appropriate server roles and features.

Module 2: This module explains how to configure, manage and troubleshoot DNS server and zone properties to be used in a secure environment.

Module 3: This module explains how to configure, manage and troubleshoot WINS servers.

Module 4: This module explains how to configure, manage and troubleshoot a DHCP environment supporting an IPV4 infrastructure.
Module 5: This module explains how to configure and troubleshoot static and dynamic IPv6 addresses, including subnet prefix lengths, gateways and DNS servers.

Module 6: This module explains how to configure and troubleshoot Routing and Remote Access Services.

Module 7: This module explains how to install, configure and troubleshoot the Network Policy Server Role service.

Module 8: This module explains how to configure and manage NAP for DHCP, VPN, and 802.1X.

Module 9: This module explains how to configure and test IPSec.

Module 10: This module explains how to monitor and troubleshoot IPSec.

Module 11: This module explains how to configure and manage Distributed File System.

Module 12: This module explains how to configure and troubleshoot file system storage technologies included with Windows Server 2008.

Module 13: This module explains how to describe and configure backup and recovery methods.

Module 14: This module explains how to configure and analyze server security and security update compliance.
Course Materials

The following materials are included with your kit:

- **Course handbook.** The Course handbook contains the material covered in class. It is meant to be used in conjunction with the Course Companion CD.

- **Course Companion CD.** The Course Companion CD contains the full course content, including expanded content for each topic pages, full lab exercises and answer keys, topical and categorized resources and Web links. It is meant to be used both inside and outside the class.

**Note** To access the full course content, insert the Course Companion CD into the CD-ROM drive, and then in the root directory of the CD, double-click StartCD.exe.

- **Course evaluation.** At the end of the course, you will have the opportunity to complete an online evaluation to provide feedback on the course, training facility, and instructor.

To provide additional comments or feedback on the course, send e-mail to support@mscourseware.com. To inquire about the Microsoft Certification Program, send e-mail to mcphelp@microsoft.com.

Virtual Machine Environment

This section provides the information for setting up the classroom environment to support the business scenario of the course.

Virtual Machine Configuration

In this course, you will use Microsoft Virtual Server 2005 to perform the labs.

**Important:** At the end of each lab, you must close the virtual machine and must not save any changes. To close a virtual machine without saving the changes, perform the following steps: 1. On the host computer, click **Start**, point to All **Programs**, point to **Microsoft Virtual Server**, and then click **Virtual Server Administration Website**. 2. Under **Navigation**, click **Master Status**. For each virtual machine that is running, point to the virtual machine name, and, in the context menu, click **Turn off Virtual Machine and Discard Undo Disks**. Click **OK**.
The following table shows the role of each virtual machine that this course uses:

<table>
<thead>
<tr>
<th>Virtual machine</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>6421A-NYC-DC1</td>
<td>Domain controller in the WoodgroveBank.com domain</td>
</tr>
<tr>
<td>6421A-NYC-SRV1</td>
<td>Member server</td>
</tr>
<tr>
<td>6421A-NYC-CL1</td>
<td>Windows Vista computer in the WoodgroveBank.com domain</td>
</tr>
<tr>
<td>6421A-NYC-CL2</td>
<td>Windows Vista computer in the WoodgroveBank.com domain</td>
</tr>
</tbody>
</table>

**Software Configuration**

The following software is installed on each virtual machine:

- Windows Server 2008 Enterprise; Windows Vista

**Classroom Setup**

Each classroom computer will have the same virtual machine configured in the same way.

**Course Hardware Level**

To ensure a satisfactory student experience, Microsoft Learning requires a minimum equipment configuration for trainer and student computers in all Microsoft Certified Partner for Learning Solutions (CPLS) classrooms in which Official Microsoft Learning Product courseware are taught. This course requires a computer that meets or exceeds hardware level 5, which specifies a 2.4–gigahertz (minimum) Pentium 4 or equivalent CPU, at least 2 gigabytes (GB) of RAM, 16 megabytes (MB) of video RAM, and a 7200 RPM 40-GB hard disk.
Module 1

Installing and Configuring Servers

Contents:

Lesson 1: Installing Windows Server 2008 1-3
Lesson 2: Managing Server Roles and Features 1-12
Lesson 3: Overview of the Server Core Installation Option 1-17
Lab: Installing and Configuring Servers and Server Roles 1-25
Module Overview

- Installing Windows Server 2008
- Managing Server Roles and Features
- Overview of the Server Core Installation Option

This module explains how to identify the appropriate usage scenario and installation type for a server and then install and configure appropriate server roles and features.
Lesson 1

Installing Windows Server 2008

- Windows Server 2008 Editions
- Windows Server 2008 Installation Requirements
- x64 Installation Considerations
- Common Installation Scenarios
- Preparing for the Installation of Windows Server 2008
- Process for Installing Windows Server 2008

Installing Windows Server® 2008 has changed somewhat from previous Windows Server versions. The options available vary from a simple DVD-based install, to using answer files created with Windows System Image Manager (SIM) and automating deployment using the Windows Automated Installation Kit (WAIK). The installation process no longer includes the text mode portion of setup and is completely GUI-based. Another difference is that the Standard, Enterprise, and DataCenter editions all are included on a single 32-bit or 64-bit DVD. The version that is installed depends on the installation key that you use during the installation process.
### Windows Server 2008 Editions

<table>
<thead>
<tr>
<th>Edition</th>
<th>Server Core</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2008 Standard</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows Server 2008 Enterprise</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows Server 2008 DataCenter</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows Web Server 2008</td>
<td>No</td>
</tr>
<tr>
<td>Windows Server 2008 for Itanium-based Systems</td>
<td>No</td>
</tr>
</tbody>
</table>

### Key Points

There are five available editions of Windows Server 2008. The edition that you choose will depend upon the business requirements that you need to address.

Windows Server 2008 helps information technology (IT) professionals increase the flexibility of their server infrastructure while offering developers a more robust Web and applications platform for building connected applications and services. Powerful new management tools and security enhancements offer more server and network control, and provide advanced protection for applications and data.
Windows Server 2008 Installation Requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| Processor                  | • Minimum: 1Ghz  
• Recommended: 2Ghz  
• Optimal: 3Ghz or faster |
| Memory                     | • Minimum: 512MB RAM  
• Recommended: 1GB RAM  
• Optimal: 2GB RAM (Full) or 1GB RAM (Server Core) or more  
• Maximum (32-bit): 4GB (Standard) or 64GB (Enterprise and Datacenter)  
• Maximum (64-bit): 32GB (Standard) or 2TB (Enterprise, Datacenter, and Itanium-based systems) |
| Available Disk Space       | • Minimum: 8GB  
• Recommended: 40GB (Full); 10GB (Core)  
• Optimal: 80GB (Full); 40GB (Core) |
| Optical Drive              | • DVD-ROM                                                                 |
| Display and Peripherals    | • Super VGA (800 x 600) or higher-resolution monitor  
• Keyboard  
• Microsoft mouse or compatible pointing device |

Key Points
Installation requirements for Windows Server 2008 vary between the different installation types, namely the full installation or the Server Core installation. Server Core requires less disk space for the operating system’s installation because, by default, only the modules that the assigned roles require are installed. Additionally, the GUI is not installed, which means that disk space utilization is lighter with the Server Core installation.

Note: If you are installing a 64-bit version, you must make sure that all kernel mode drivers are digitally signed prior to installing. The installation will fail if you use unsigned drivers.

Additional Resources:
• Windows Server 2008 Technical Library
x64 Installation Considerations

- Requires that all kernel-mode device drivers are digitally signed
- Device drivers are necessarily trusted because they have direct access to the system’s hardware
- May be able to mitigate some “rootkit” software

Key Points
You may have to include 64-bit versions of Windows Server 2008 in your infrastructure, depending on the company’s needs. For example, some network services, such as Exchange Server 2007, are supported only in a 64-bit production environment and therefore will be supported only for 64-bit versions of Windows Server 2008 running on 64-bit architecture.

Installing a 64-bit version may offer the ability to scale up (more CPUs and RAM) more than a 32-bit system allows, you must ensure that the kernel mode drivers that you will use are all digitally signed.

Additional Resources:
- Windows Server 2008 Technical Library
- Digital Signatures for Kernel Modules on x64-based Systems Running Windows Vista
Common Installation Scenarios

- Clean installations
- Upgrades
- Unattended installations

Key Points
Whether you choose to upgrade an existing server or perform a clean installation, you must decide how you will perform server installations in your environment. There are particular upgrade paths that you must follow, and you can perform unattended installations by using answer files, Windows SIM, and the Windows AIK.

Back up your servers before you upgrade. Your backup should include all data and configuration information that is necessary for the computer to function. It is important to perform a backup of server configuration information, especially for those servers that provide network infrastructure, such as Dynamic Host Configuration Protocol (DHCP) servers. When you perform the backup, be sure to include the boot and system partitions, and the system state data. Another way to back up configuration information is to create a backup set for Automated System Recovery.
Installing and Configuring Servers

Additional Resources:
• Windows Automated Installation Kit (WAIK) User's Guide for Windows Vista
• Windows Vista Deployment Step by Step Guide
• Windows Server 2008 Technical Library
Preparing for the Installation of Windows Server 2008

Key Points
Before installing Windows Server 2008, you must follow some general guidelines to ensure that the installation is as smooth as possible and that installation errors do not arise. Most of these guidelines are best practices for any installation of Microsoft operating systems, and therefore should be included in any build guides that are created for most environments.

Before you install Windows Server 2008, use the following guidelines to prepare for the installation:

- Check for application compatibility.
- Disconnect UPS devices.
- Back up your servers.
- Disable your virus protection software.
- Run the Windows Memory Diagnostic tool.
- Obtain mass storage drivers.
- Be aware of Windows Firewall installation defaults.
- Prepare Active Directory for the Active Directory Domain Services role.
• Provide mass storage drivers.
• Be aware that Windows Firewall is on by default.
• Prepare your Active Directory environment with Windows Server 2008 updates.

Additional Resources:
• Web Server
• Help and Support on the Install now page of Windows Server 2008 Setup wizard
Process for Installing Windows Server 2008

1. Provide language and preferences
2. Setup copies and installs Windows
3. Administrator configures the server using the Initial Configuration Tasks page at first logon

Key Points
The process for installing Windows Server 2008 is much the same as in previous versions of the operating system. However, there are differences that make the process more customizable and easier to accomplish than previous versions. One significant change is the volume licensing model that Microsoft uses with the server product. The license model for volume licensing is the same as the model that Windows Vista operating systems use.

Additional Resources:
- Windows Server "Longhorn" Beta 3 Server Manager Technical Overview
- Windows Server 2008: Server Manager
Lesson 2
Managing Server Roles and Features

- Tools Used for Administrative Tasks
- What Are Server Roles?
- What Are Server Features?
- Demonstration: Installing Server Roles and Features Using Server Manager

Microsoft has changed the way administrators manage the server environment. The operating system installs in a secure fashion and the administrator can choose among four different methods to configure the server according to desired functionality.

After the installation is complete and the administrator logs on to the server, the Initial Configuration Tasks window opens and allows the administrator to setup the server name, networking configuration, automatic updates and the Windows Firewall settings. After using this tool, the administrator can choose to use custom Microsoft Management Consoles (MMC)s to manage the server, use Server Manager to install and remove roles and features, and use Windows PowerShell for configuration tasks, if desired.
Tools Used for Administrative Tasks

Key Points
After you complete the installation of the operating system, you can manage the systems with four different tools.

On first logon, the Administrator must specify a password for the administrative account and then is presented with the Initial Configuration Tasks window. Subsequent management can be performed using Server Manager, typical Microsoft Management Console windows, and Windows PowerShell. The choice of tool depends on the task users wish to complete and the experience that they must have to work with each specific tool.

Additional Resources:
- Windows PowerShell 1.0 Documentation Pack
- Microsoft Management Console 3.0 for Windows XP (KB907265)
What Are Server Roles?

A server role describes the primary function of a server

- Administrators can dedicate an entire computer to one role or install multiple server roles on a single computer
- Each role can include one or more role services or sub-elements of a role
- Server Manager is the tool that is used to install, configure, and remove Server Roles

Key Points
Server roles in Windows Server 2008 describe a server’s primary function. For example, a server role might be as Active Directory Domain Services or a Web server. You can choose to install one or many roles on a Windows Server 2008 installation. The Server Manager administrative tool is used for the installation and removal of server roles in a Windows Server 2008 environment.

Additional Resources:
- Windows Server 2008 Technical Library
What Are Server Features?

Key Points

A feature does not generally describe the server’s primary function. Instead, it describes a server’s auxiliary or supporting function. Consequently, an administrator typically installs a feature not as the primary function of the server, but to augment the functionality of an installed role. For example, Failover Clustering is a feature that administrators can choose to install after installing specific roles, such as File Services, to make the File Services role more redundant.

Additional Resources:
- Windows Server "Longhorn" Beta 3 Server Manager Technical Overview
- Windows Server 2008 Technical Library
Demonstration: Installing Server Roles and Features Using Server Manager

In this demonstration, you will see how to use Server Manager to install roles and features.
Lesson 3
Overview of the Server Core Installation Option

- Benefits of a Server Core Installation
- Server Roles that a Server Core Installation Supports
- Features that a Server Core Installation Supports
- Managing a Server Core Installation

A new option in Windows Server 2008 is the Server Core option, which installs only what is required to have a manageable server for Active Directory Domain Services (AD DS), Active Directory Lightweight Directory Services (AD LDS), Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), File, Print, and/or Streaming Media Services. A graphical interface is not available with this option. Instead, you use the command-line or remote-management tools to configure and manage the server environment.

If you choose to install this option, the installation does not support upgrading from previous versions. Therefore, you must perform a clean installation. This option is beneficial to many environments because of the reduced management required, reduced attack surface, reduced maintenance needed, and smaller disk space requirements. The space difference realized by installing Server Core is that it only occupies approximately 25% of the disk space that a typical Standard installation uses.
Benefits of a Server Core Installation

Key Points
In Windows Server 2008, administrators now can choose to install a minimal environment that avoids extra overhead. Although this option limits the roles that the server can perform, it can improve security and reduce management. This type of installation is called a Server Core installation.

Server Core installations provide the following benefits:
- Reduced maintenance
- Reduced attack surface
- Reduced management
- Less disk space required

Additional Resources:
- Server Core Installation Option
Server Roles that a Server Core Installation Supports

Key Points
A Server Core installation is a minimal server installation option for Windows Server 2008. Server Core installations provide an environment for running the following server roles:

- Active Directory Domain Services (AD DS)
- Active Directory Lightweight Directory Services (AD LDS)
- Dynamic Host Configuration Protocol (DHCP) Server
- Domain Name System (DNS) Server
- File Services
- Print Server
- Streaming Media Services
The Server Core installation option installs only the subset of the binary files that are required by the supported server roles. For example, the Windows Explorer user interface (or ‘shell’) is not installed as part of a Server Core installation. Instead, the default user interface for a server running a Server Core installation is the command prompt.

**Additional Resources:**
- Server Core Installation Option
Features that a Server Core Installation Supports

<table>
<thead>
<tr>
<th>A Server Core installation supports the following features:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Backup</td>
</tr>
<tr>
<td>• Bitlocker Drive Encryption</td>
</tr>
<tr>
<td>• Failover Clustering</td>
</tr>
<tr>
<td>• Multipath I/O</td>
</tr>
<tr>
<td>• Network Load Balancing</td>
</tr>
<tr>
<td>• Removable Storage</td>
</tr>
<tr>
<td>• Simple Network Management Protocol</td>
</tr>
<tr>
<td>• Subsystem for UNIX-based applications</td>
</tr>
<tr>
<td>• Telnet Client</td>
</tr>
<tr>
<td>• WINS</td>
</tr>
</tbody>
</table>

**Key Points**
After the Server Core installation is complete and the server is configured, you can install one or more optional features. The Server Core installation of Windows Server 2008 supports the following optional features:

- Backup
- Bitlocker Drive Encryption
- Failover Clustering
- Multipath input/output (I/O)
- Network Load Balancing
- Removable Storage
- Simple Network Management Protocol (SNMP)
- Subsystem for UNIX-based applications
- Telnet client
- Windows Internet Name Service (WINS)

**Note:** Failover Clustering is not available in Windows Server 2008 Standard Edition.

**Additional Resources:**

- Server Core Installation Option of Windows Server "Longhorn" Step-By-Step Guide
Managing a Server Core Installation

A Server Core installation can be managed:

- Locally and remotely using a command prompt
- Remotely using Terminal Server
- Remotely using Windows Remote Shell
- Remotely using an MMC snap-in

Key Points

The Server Core installation option is designed for use in environments where high security requirements necessitate a minimal attack surface on a server, or in organizations that have many servers, only some of which need to perform dedicated tasks.

Because no graphical user interface is available for many Windows operations, using the Server Core installation option requires administrators to be experienced in using a command prompt or scripting techniques for local administration of the server. Alternatively, you can manage the Server Core installation with Microsoft Management Console (MMC) snap-ins from another computer running Windows Server 2008. To do this, select the computer running a Server Core installation as a remote computer to manage.
**Note:** Administrators managing a Server Core installation need to be aware that there is no graphical user interface (GUI). Although no changes are required to the configuration of your network, you might need to become familiar with command-line tools.

**Additional Resources:**
- Server Core Installation Option
- Installation and Configuration for Windows Remote Management
Lab: Installing and Configuring Servers and Server Roles

- Exercise 1: Identifying Server Types
- Exercise 2: Installing and Configuring Server Roles and Features
- Exercise 3: Configuring Server Core and Performing Basic Management Tasks

Logon information

<table>
<thead>
<tr>
<th>Virtual machines</th>
<th>NYC-DC1, NYC-SVR1, NYC-SVR2</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Administrator</td>
</tr>
<tr>
<td>Password</td>
<td>Pa$$w0rd</td>
</tr>
</tbody>
</table>

Estimated time: 60 minutes

Objectives
After completing this lab, you will be able to:

- Describe the appropriate server type needed for a usage scenario
- Install and configure server roles and features
- Configure Server Core and perform basic management tasks
Scenario
You have to install two new servers for your corporate infrastructure in the WoodgroveBank.com domain. The new servers are needed to increase DNS name-resolution services for a newly acquired company, Contoso.com, and to provide Terminal Services for some line-of-business applications that will be available to employees from their desktop computers and from their homes after hours. The Terminal Services server also will need to have backup capability installed for disaster recovery purposes.

For security purposes, the DNS service should be available on only one of the new servers and will be administered completely through remote management tools after initial configuration. Firewall configuration on the DNS server needs to be configured correctly for the ports required to respond to DNS name-resolution requests and for remote administration.

Lab Setup
For this lab you will use the available virtual machine environment. Before you begin the lab, you must:

1. Start the 6421A-NYC-DC1 and 6421A-NYC-SVR1 virtual machines.
2. Log on to 6421A-NYC-SVR1 with the user name Woodgrovebank\administrator and the password of Pa$$w0rd.
3. Close the Initial Configuration Tasks window that appears after log on.
4. Close the Server Manager window that appears.
Exercise 1: Identifying Server Types

Exercise Overview
In this exercise, you will analyze the scenario and answer the following questions related to a possible server type and role deployment.

**Question:** After reading the scenario, which installation type, Core or Standard, would be suitable for Terminal Services? Why?

**Question:** Would the Core installation be suitable for the Domain Name System (DNS) server? If so, are there any shortcomings to configuring the server to host this role?

**Question:** What benefits would you realize by using the Core installation option for the DNS server role?

**Question:** What roles and features are needed on the servers to meet the given scenario’s requirements?
Exercise 2: Installing and Configuring Server Roles and Features

In this exercise, you will install the Terminal Services role and Server Backup feature by using the Server Manager administrative tool.

The main tasks are as follows:
1. Ensure that you have completed the steps in the Lab Setup.
2. Start the Server Manager console.
3. From Server Manager, install the Terminal Services role.
4. View the installation results.
5. Install the Server Backup feature from the Server Manager console.
6. Verify the Terminal Services and Windows Server Backup tools are installed.

- Task 1: Ensure that you have completed the steps in the Lab Setup
  - Look in the Lab Setup section and ensure you have completed the steps before you continue with this lab.

- Task 2: Start the Server Manager console
  - On NYC-SVR1, start the Server Manager console.

- Task 3: From Server Manager, install the Terminal Services role
  1. Install the Terminal Services role using the following options:
     - Server Roles: Terminal Services
     - Role Services: Terminal Server
     - Authentication method: Do not require Network Level Authentication
     - Licensing Mode: Configure later
     - User Groups: Administrators
  2. Restart as required.
Task 4: View the Installation Results
1. Log on to NYC-SVR1 with the user name Woodgrovebank\administrator and the password Pa$$w0rd.

   Upon successful logon, Server Manager opens and the Terminal Services configuration resumes.

2. Once complete, **Installation succeeded** appears in the details pane. Click Close to exit the Installation Results page. Do not close Server Manager.

Task 5: Install the Server Backup feature from the Server Manager console
1. In the Server Manager list pane, right-click Features, and then click Add Features. The Add Features Wizard appears.

2. Install the **Windows Server Backup Features** option.

3. On the Installation Results page, verify **Installation succeeded** appears in the details pane, and then click Close. Do not close Server Manager.

   The Windows Server Backup feature is installed.

Task 6: Verify the Terminal Services and Windows Server Backup tools are installed
1. In the list pane of Server Manager, verify that Server Manager (NYC-SVR1) is selected.

2. Using the scroll bar in the details pane, scroll down until the Roles Summary is visible and verify that Terminal Services is listed.

3. Scroll down to Features Summary and verify that Windows Server Backup appears.

Exercise 3: Configuring Server Core and Performing Basic Management Tasks

In this exercise, you will configure a Core installation of Windows Server 2008 and install the DNS server role using command-line tools. You then will connect to the Core server from a remote Windows Server 2008 computer using a custom MMC to configure the DNS server role.

The 6421A-NYC-DC1 and 6421A-NYC-SVR1 virtual machines must be running to complete the exercise. Be sure to start the virtual machines prior to beginning this exercise.

The main tasks are as follows:
1. Start the 6421A-NYC-SVR2 virtual machine.
2. Log on to the Server Core installation.
3. Use command-line tools to set parameters in the Server Core virtual machine.
4. Connect the server to the WoodgroveBank.com domain.
5. Log on to the Server Core installation.
6. Verify the firewall configuration.
7. Use the `netsh` command to open ports.
8. View the current status of roles and install the DNS server role.
9. Manage the server by using DNS Manager from a remote computer.
10. Close all virtual machines and delete the changes.

▶ Task 1: Start the 6421A-NYC-SVR2 virtual machine
   - From the Virtual Machine Administration Website, start the 6421A-NYC-SVR2 virtual machine.

▶ Task 2: Log on to the Server Core installation
   - Log on to NYC-SVR2 as Administrator with a password of Pa$$w0rd.
Task 3: Use command line tools to set parameters in the Server Core virtual machine

- Computername=NYC-DNSSVR2
- IP address=10.10.0.12
- Mask=255.255.0
- Gateway=10.10.0.1
- DNS=10.10.0.10

1. To determine the current default assigned computer name, type `set` in the command window.

2. Locate the computer name attribute and write it down.

3. To change the computer name, type the following command and then press ENTER:
   
   Netdom renamecomputer NYC-SVR2 /NewName:NYC-DNSSVR2

4. When prompted, type `y` for yes, and then press ENTER.

5. In the command window, type the following command to set the static IP address: Netsh `interface ipv4 set address name= “local area connection” source=static address=10.10.0.12 mask=255.255.0.0 gateway=10.10.0.1` and then press ENTER.

6. In the command window, type the following command to set the primary DNS server and then press ENTER:
   
   Netsh interface ip set dns “local area connection” static 10.10.0.10 primary

7. At the command prompt, type `ipconfig /all` and then press ENTER to verify the IP address assignment.

8. On the keyboard, press RIGHT-ALT+DELETE.

9. Choose to restart the computer by clicking `Shutdown options` in the lower right-hand pane of the window, and then click Restart.

10. In the Shutdown Event Tracker window, click `Operating System: Reconfiguration (Planned)`, and then click OK. The server restarts.

11. Log on to the server with the user name Administrator and a password of Pa$$w0rd.
Task 4: Connect the server to the WoodgroveBank.com domain
1. In the command window type the following command and then press ENTER.
   ```bash
   ```
2. At the command prompt, type the following command and then press ENTER:
   ```bash
   Pa$$w0rd  
   ```
   **Note:** Your keystrokes will not be reflected on the screen. You will receive a message that the command completed successfully and that the computer needs to be restarted.
3. At the command prompt, press RIGHT-ALT+DELETE, click the **Shut down options** icon, and then click **Restart**. The **Shut Down Windows** dialog box appears.
4. In the **Option** box of the **Shut Down Windows** dialog box, click **Operating System: Reconfiguration (Planned)**, and then click **OK**.

Task 5: Log on to the Server Core installation
- Log on to the server with the user name **Administrator** and a password of **Pa$$w0rd**.

Task 6: Verify the firewall configuration
- Use the **netsh** command to view the current firewall configuration. Type the following command in the command window, and then press ENTER:
  ```bash
  Netsh firewall show state  
  ```
  **Note:** Notice that the Firewall status shows that the Operational mode is set to Enable This means that the Windows Firewall is enabled but no specific ports have been opened.
Task 7: Use the Netsh command to open ports

1. At the command prompt, type the following command and then press ENTER:
   \texttt{netsh firewall add portopening ALL 53 DNS-server}

2. At the command prompt, type the following command and then press ENTER:
   \texttt{netsh firewall add portopening TCP 135 remote-admin}

3. At the command prompt, type the following command and then press ENTER:
   \texttt{netsh firewall add portopening UDP 137 netbios-ns}

4. At the command prompt, type the following command and then press ENTER:
   \texttt{netsh firewall add portopening UDP 138 netbios-dgm}

5. At the command prompt, type the following command and then press ENTER:
   \texttt{netsh firewall add portopening TCP 139 netbios-ssn}

6. At the command prompt, type the following command and then press ENTER:
   \texttt{netsh firewall add portopening TCP 445 netbios-ns}

7. At the command prompt, type the following command and then press ENTER:
   \texttt{netsh firewall show config}

\textbf{Note:} Notice that in the Service configuration for Domain profile, File and Printer Sharing and Remote Desktop services are set to \textbf{enable}, and both TCP and UDP port 53 are open for the DNS server.
Task 8: View the current status of roles and install the DNS server role

1. In the command prompt window, at the command prompt, type the following command and then press ENTER:
   oclist

   **Note:** Verify that no server roles are installed.

2. Use the Ocsetup.exe and oclist commands to install the DNS server. To do this, type the following at the command prompt and then press ENTER:
   start /w ocsetup DNS-Server-Core-Role

   **Note:** The server role name is case sensitive.

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

   **Note:** Verify that the DNS-Server-Core-Role is installed.
Task 9: Manage the server by using DNS Manager from a remote computer

1. On NYC-DC1, open the DNS Manager console.
2. From the DNS console, connect to NYC-DNSSVR2.
3. Use the DNS console to create a forward lookup zone for Contoso.com:
   a. In the Console Root tree pane of the DNS Manager, expand NYC-DNSSVR2, and then click Forward Lookup Zones.
   b. Right-click Forward Lookup Zones, and then click New Zone.
   c. Click Next in the Welcome to the New Zone wizard.
   d. Click Next in the Zone Type dialog box, using the defaults to create a Primary zone.
   e. In the Zone Name window, type Contoso.com and then click Next.
   f. Click Next to accept the default name for the DNS zone file.
   g. In the Dynamic Update window, click Next to accept the defaults.
   h. In the Completing the New Zone Wizard dialog box, click Finish to create the new zone.
   i. Close the DNS Manager console.

Task 10: Close all virtual machines and discard undo disks

1. On the host computer, click Start, point to All Programs, point to Microsoft Virtual Server, and then click Virtual Server Administration Website.
2. Under Navigation, click Master Status. For each virtual machine that is running, click the Virtual Machine Name, and in the context menu, click Turn off Virtual Machine and Discard Undo Disks. Click OK.
Module Review and Takeaways

- Review Questions
- Considerations for Installing Windows Server 2008
- Best Practices
- Tools

Review Questions

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

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

3. You are responsible for many classrooms in an educational facility. Desktop operating system image refreshes take place on a weekly basis and involve approximately 300 computers. What type of volume-license scheme would work best – KMS Server or MAK, and why?

4. What is the difference between a role and a feature? How do you install each?
Considerations for Installing Windows Server 2008
Consider the following prior to installing Windows Server 2008:

- You can install Windows Server 2008 only on computers that use Advanced Configuration and Power Interface (ACPI).
- You cannot specify a custom hardware application layer (HAL) file with Windows Server 2008.
- Windows Firewall is enabled by default. Server applications that must receive unsolicited inbound connections will fail until you create inbound firewall rules to allow them.
- The mandatory kernel-mode code-signing policy applies to all kernel-mode software on x64-based systems running Windows Server 2008.
- You cannot upgrade a previous version of Windows Server to a Core installation. The installation must be clean.


- Always used signed kernel mode drivers when available. This is mandatory for x64 installations.
- Only install the Roles and Features required for the server’s intended purpose.
- Only allow inbound connections that are required for the installed Roles and Features on a given server.
- Enable Remote Desktop for Administrators on CORE installations. The shell will be the command prompt for terminal connections made.
## Tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Use for</th>
<th>Where to find it</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Management Console</td>
<td>Local and remote administration of all installed roles and features in Windows Server 2008.</td>
<td>Click <strong>Start</strong> and then point to <strong>Administrative Tools</strong>. Select a pre-configured tool or type <strong>MMC</strong> in the <strong>Run</strong> box to create a custom MMC console based on the snap-ins you specify.</td>
</tr>
<tr>
<td>Initial Configuration Tasks</td>
<td>Initial configuration of the server. Tasks include computername, automatic updates, roles, features, firewall configuration, and remote-desktop configuration.</td>
<td>ICT launches when the administrator logs on the installation of Windows Server 2008.</td>
</tr>
<tr>
<td>Server Manager</td>
<td>Management and maintenance of the installation and removal of roles and features.</td>
<td>Click <strong>Start</strong>, and then point to <strong>Administrative Tools. Select Server Manager</strong> from the available administrative tools.</td>
</tr>
</tbody>
</table>
Module 2

Configuring and Troubleshooting DNS

Contents:
Lesson 1: Installing the DNS Server Role 2-3
Lesson 2: Configuring the DNS Server Role 2-9
Lesson 3: Configuring DNS Zones 2-20
Lesson 4: Configuring DNS Zone Transfers 2-27
Lesson 5: Managing and Troubleshooting DNS 2-32
Lab: Configuring and Verifying a DNS Solution 2-39
Module Overview

- Installing the DNS Server Role
- Configuring the DNS Server Role
- Configuring DNS Zones
- Configuring DNS Zone Transfers
- Managing and Troubleshooting DNS

This module explains how to configure, manage, and troubleshoot Domain Name System (DNS) server and zone properties that you will use in a secure environment.
Lesson 1
Installing the DNS Server Role

- Overview of the Domain Name System Role
- Overview of the DNS Namespace
- DNS Improvements for Windows Server 2008
- Demonstration: Installing the DNS Server Role
- Considerations for Deploying the DNS Server Role

The DNS Server role is a critical component of a Windows Server® 2008 domain infrastructure. This lesson provides information about the DNS role and how the DNS name space works. This lesson also provides details about what has changed in the DNS role for Windows Server 2008 and identifies the considerations for deploying the DNS role.
Overview of the Domain Name System Role

Domain Name System is a hierarchical distributed database

- DNS is the foundation of the Internet naming scheme
- DNS supports accessing resources by using alphanumeric names
- InterNIC is responsible for managing the domain namespace
- DNS was created to support the Internet’s growing number of hosts

Key Points
DNS is a name-resolution service that resolves names to numbers. The DNS service is a hierarchical distributed database. This means that the database is separated logically, allowing many different servers to host the worldwide database of DNS names.

Additional Reading
- DNS Overview
- Understanding zones and zone transfer
Overview of the DNS Namespace

Key Points
The DNS Namespace facilitates how a DNS client locates a computer. It is organized hierarchically or in layers to distribute information across many servers.

Additional Reading
- DNS Namespace Planning
- Designing a DNS Namespace
DNS Improvements for Windows Server 2008

New or enhanced features in the Windows Server 2008 version of DNS include:

- Background zone loading
- IP version 6 support
- Support for read-only domain controllers
- Global single names

Key Points
You will realize some of the advantages of using Windows Server 2008 with the new features that it includes for the DNS server role. These features include background zone loading, support for IPv6 and for read-only domain controllers, and global single names.

Additional Reading
- What's New in DNS in Windows Server 2008
- AD DS: Read-Only Domain Controllers
- DNS Server Role
Demonstration: Installing the DNS Server Role

In this demonstration, you will see how to install the DNS Server role.
Considerations for Deploying the DNS Server Role

Key Points
The DNS Server role is critical in the configuration of Active Directory and Windows Network infrastructure. When planning to deploy DNS, there are several considerations that need to be reviewed:

- Server capacity planning
- Where to place DNS servers
- Service availability

Additional Reading
- Help topic: Planning DNS Servers
Lesson 2
Configuring the DNS Server Role

- What Are the Components of a DNS Solution?
- DNS Resource Records
- What are Root Hints?
- What is a DNS Query?
- What Are Recursive Queries?
- What Are Iterative Queries?
- What is a Forwarder?
- What is Conditional Forwarding?
- How DNS Server Caching Works
- Demonstration: Configuring the DNS Server Role

The DNS infrastructure is the basis for name resolution on the Internet and in Windows Server 2008 Active Directory domains. This lesson provides guidance and information about what is required to configure the DNS server role, and explains the basic functions of a DNS server.
What Are the Components of a DNS Solution?

Key Points
The components of a DNS solution include DNS servers, DNS servers on the Internet, and DNS clients.

Additional Reading
- DNS defined
- Server Features
- Client Features
- DNS Server Role
DNS Resource Records

DNS resource records include:

- SOA: Start of Authority
- A: Host Record
- CNAME: Alias Record
- MX: Mail Exchange Record
- SRV: Service Resources
- NS: Name Servers
- AAAA: IPv6 DNS Record

Key Points
The DNS zone file stores resource records. The next lesson examines zone files in more detail. Resource records specify a resource type and the IP address to locate the resource. The most common resource record is an A resource record. This is a simple record that matches a hostname to an IP address. The host can be a workstation, server, or another network device, such as a router.

Additional Reading
- Resource records reference
What are Root Hints?

Root hints are the list of the 13 servers on the Internet that the Internet Assigned Numbers Authority maintains and that the DNS server uses if it cannot resolve a DNS query by using a DNS forwarder or its own cache. The root hints are the highest servers in the DNS hierarchy and can provide the necessary information for a DNS server to perform an iterative query to the next lowest layer of the DNS namespace.

Key Points

Additional Reading
- Update root hints on the DNS server
- Disable recursion on the DNS server
What is a DNS Query?

A query is a request for name resolution and is directed to a DNS server

- Queries are recursive or iterative
- DNS clients and DNS servers both initiate queries
- DNS servers are authoritative or nonauthoritative for a namespace
- An authoritative DNS server for the namespace will either:
  - Return the requested IP address
  - Return an authoritative “No”
- A nonauthoritative DNS server for the namespace will either:
  - Check its cache
  - Use forwarders
  - Use root hints

Key Points
A DNS query is the method that you use to request name resolution in which a query is sent to a DNS Server. There are two types of DNS queries: authoritative and non-authoritative.

It is important to note that DNS servers also can act as DNS clients and send DNS queries to other DNS servers.
What Are Recursive Queries?

Key Points
A recursive query can have two possible results:
- It returns the IP address of the host requested
- The DNS server cannot resolve an IP address

For security reasons, it sometimes is necessary to disable recursive queries on a DNS server. In doing so, the DNS server in question will not attempt to forward its DNS requests to another server. This can be useful when you do not want a particular DNS server communicating outside its local network.
What Are Iterative Queries?

Key Points
Iterative queries provide a mechanism for accessing domain name information that resides across the DNS system, and enable servers to quickly and efficiently resolve names across many servers.

Additional Reading
- How DNS query works
What is a Forwarder?

A forwarder is a DNS server designated to resolve external or offsite DNS domain names.

Key Points
A forwarder is a network DNS server that forwards DNS queries for external DNS names to DNS servers outside that network. You also can use conditional forwarders to forward queries according to specific domain names.

Additional Reading
- Microsoft TechNet: Understanding forwarders
- Help topic: Understanding Forwarders
- Help topic: Using Forwarders
What is Conditional Forwarding?

Key Points
A conditional forwarder is a DNS server on a network that forwards DNS queries according to the query’s DNS domain name.
How DNS Server Caching Works

<table>
<thead>
<tr>
<th>DNS server cache</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
</tr>
<tr>
<td>ServerA.contoso.msft</td>
</tr>
</tbody>
</table>

Key Points

DNS caching increases the performance of the organization's DNS system by decreasing the time it takes to provide DNS lookups.

When a DNS server resolves a DNS name successfully, it adds the name to its cache. Over time, this builds a cache of domain names and their associated IP addresses for the most common domains that the organization uses or accesses.

Additional Reading

- Help topic: Install a Caching-only DNS Server
### Demonstration: Configuring the DNS Server Role

**In this demonstration, you will see how to:**

- Update root hints on a DNS server
- Configure a DNS server to use a forwarder
- Clear the DNS server cache by using the DNS console
- Clear the DNS server cache by using the DNSScmd command
Lesson 3
Configuring DNS Zones

- What Is a DNS Zone?
- What Are the DNS Zone Types?
- What Are Forward and Reverse Lookup Zones?
- What Are Stub Zones?
- Demonstration: Creating Forward and Reverse Lookup Zones
- DNS Zone Delegation

DNS zones are an important concept in DNS infrastructure. They allow for DNS domains to be logically separated and managed. This lesson provides the foundation for understanding how zones relate to DNS domains and information about the different types of DNS zones that are available in the Windows Server 2008 DNS role.
What Is a DNS Zone?

Key Points
A DNS zone hosts all or a portion of a domain and its subdomains. The slide illustrates how subdomains can belong to the same zone as their parents or be delegated to another zone. The Microsoft.com domain is separated into two zones. The first zone hosts www.microsoft.com and ftp.microsoft.com. Example.microsoft.com is delegated to a new zone, which hosts the example.microsoft.com and its subdomains ftp.example.microsoft.com and www.example.microsoft.com.

Additional Reading
- Understanding zones and zone transfer
What Are the DNS Zone Types?

<table>
<thead>
<tr>
<th>Zones</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>Read/write copy of a DNS database</td>
</tr>
<tr>
<td>Secondary</td>
<td>Read-only copy of a DNS database</td>
</tr>
<tr>
<td>Stub</td>
<td>Copy of a zone that contains only records used to locate name servers</td>
</tr>
<tr>
<td>Active Directory integrated</td>
<td>Zone data is stored in Active Directory rather than in zone files</td>
</tr>
</tbody>
</table>

Key Points
There are four DNS zone types:

- Primary
- Secondary
- Stub
- Active Directory integrated

Additional Reading
- Help topic: Understanding Zone Types
What Are Forward and Reverse Lookup Zones?

**Key Points**

The forward lookup zone resolves host names to IP addresses, and hosts the common resource records: A, CNAMEs, SRV, MX, SOA, and NS.

The reverse lookup zone resolves an IP address to a domain name, and hosts SOA, NS, and PTR records.

**Additional Reading**
- Help topic: Understanding Zone Types
What are Stub Zones?

Key Points
A stub zone is a copy of a zone that contains only those resource records necessary to identify that zone’s authoritative DNS servers. A stub zone resolves names between separate DNS namespaces, which may be necessary when a corporate merger requires that the DNS servers for two separate DNS namespaces resolve names for clients in both namespaces.

Additional Reading
- Help topic: Understanding Zone Types
Demonstration: Creating Forward and Reverse Lookup Zones

In this demonstration, you will see how to:

- Create a forward lookup zone
- Create a reverse lookup zone
DNS Zone Delegation

Key Points
DNS is a hierarchical system, and zone delegation connects the DNS layers together. A zone delegation points to the next hierarchical level down and identifies the name servers responsible for lower-level domain.

Additional Reading
- Delegating Zones
Lesson 4
Configuring DNS Zone Transfers

- What is a DNS Zone Transfer?
- How DNS Notify Works
- Securing Zone Transfers
- Demonstration: Configuring DNS Zone Transfers

DNS zone transfers are how the DNS infrastructure moves DNS zone information from one server to another. This lesson covers the different methods that the DNS Server role uses when transferring zones.
What is a DNS Zone Transfer?

**Key Points**

A zone transfer occurs when you transfer the DNS zone that is on one server to another DNS server.

Zone transfers keep primary DNS server zones and secondary DNS Server zones synchronized. This is how DNS builds its resilience on the Internet. It is important that DNS zones remain updated on primary and secondary servers. Discrepancies in primary and secondary zones can cause service outages and host names that are resolved incorrectly.

**Additional Reading**

- Understanding zones and zone transfer
- Initiate a zone transfer at a secondary server
- Reload or transfer a stub zone
- Adjust the refresh interval for a zone
- Adjust the retry interval for a zone
How DNS Notify Works

A DNS notify is an update to the original DNS protocol specification that permits notification to secondary servers when zone changes occur.

Key Points
DNS notify is an update to the original DNS protocol specification that permits notification to secondary servers when zone changes occur.

This is useful in a time-sensitive environment, where data accuracy is important.
Securing Zone Transfers

Key Points
Zone information provides organizational data, so you should take precautions to ensure it is secure from malicious access and that it cannot be overwritten with bad data (known as DNS poisoning). One way in which you can protect the DNS infrastructure is to secure the zone transfers and use secure dynamic updates.

Additional Reading
- Help topic: Checklist: Secure Your DNS Server
Demonstration: Configuring DNS Zone Transfers

In this demonstration, you will see how to:

- Configure DNS zone transfers
- Configure a secondary zone
Lesson 5
Managing and Troubleshooting DNS

- What is Time to Live, Aging, and Scavenging?
- Demonstration: Managing DNS Records
- Testing the DNS Server Configuration
- Tools That Identify Problems With DNS
- Demonstration: Testing the DNS Server Configuration
- Monitoring DNS using the DNS Event Log and Debug Logging

DNS is a crucial service in the Active Directory infrastructure. When the DNS service experiences problems, it is important to know how to troubleshoot them and identify the common issues that can occur in a DNS infrastructure. This lesson covers the common problems that occur in DNS, the common areas for gathering DNS information, and the tools that you can use to troubleshoot problems.
What is Time to Live, Aging, and Scavenging?

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time to Live (TTL)</td>
<td>Indicates how long a DNS record will remain valid</td>
</tr>
<tr>
<td>Aging</td>
<td>Occurs when records that have been inserted into the DNS server reach their expiration and are removed</td>
</tr>
<tr>
<td>Scavenging</td>
<td>Performs DNS server resource record grooming for old records in DNS</td>
</tr>
</tbody>
</table>

Key Points
Time to Live (TTL), aging, and scavenging help manage DNS resource records in the zone files. Zone files can change over time, so there needs to be a way to manage DNS records that are updated or which are not valid because the hosts they represent are no longer on the network.

Additional Reading
- Enable automatic scavenging of stale resource records
- Start immediate scavenging of stale resource records
- Use Aging and Scavenging
- Help topic: Use Aging and Scavenging
Demonstration: Managing DNS Records

In this demonstration, you will see how to:

- Configure TTL
- Enable Scavenging
- Configure Aging
Testing the DNS Server Configuration

You can test the DNS server configuration by using:

- A simple query to ensure that the DNS service is answering
- A recursive query to ensure that the DNS server can communicate with the upstream DNS service

Key Points
In the DNS server Monitoring tab, you can configure a test that allows the DNS server to determine whether it can resolve simple local queries and perform a recursive query to ensure that the server can communicate with upstream servers.
Tools That Identify Problems With DNS

<table>
<thead>
<tr>
<th>Tool</th>
<th>Used to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nslookup</td>
<td>Troubleshoot DNS problems</td>
</tr>
<tr>
<td>Dnscmd</td>
<td>Edit the DNS configuration</td>
</tr>
<tr>
<td>Dnslint</td>
<td>Diagnose common DNS issues</td>
</tr>
</tbody>
</table>

Key Points
Issues can occur when you do not configure the DNS server, and its zones and resource records, properly. When resource records are causing issues, it can sometimes be more difficult to identify the issue because configuration problems are not always obvious.

Additional Reading
- Description of the DNSLint utility
- Help topic: Troubleshooting DNS Servers
- Troubleshooting DNS
Demonstration: Testing the DNS Server Configuration

In this demonstration, you will see how to test the DNS server configuration by using:

- Simple queries
- Recursive queries
- Nslookup
- Dnscmd
- Dnslint
Monitoring DNS using the DNS Event Log and Debug Logging

- Monitor DNS events in the event log to:
  - Monitor zone transfer information
  - Monitor computer events
- Enable DNS debug logging to view granular verbose information about DNS activities

**Key Points**

The DNS server has its own category in the event log. As with any event log in Windows Event Viewer, you should review the event log periodically.

Sometimes it may be necessary to get more details about a DNS problem then the Event viewer provides. In this instance, you can use debug logging to provide additional information.
Lab: Configuring and Verifying a DNS Solution

- Exercise 1: Configuring a DNS Infrastructure
- Exercise 2: Monitoring and Troubleshooting DNS

Logon information

<table>
<thead>
<tr>
<th>Virtual machines</th>
<th>NYC-DC1, NYC-SVR1</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Administrator</td>
</tr>
<tr>
<td>Password</td>
<td>Pa$$wOrd</td>
</tr>
</tbody>
</table>

Estimated time: 60 minutes

Objectives:
- Configure a DNS Infrastructure to include a secondary zone, stub zone, and secure zone transfers
- Monitor DNS
Exercise 1: Implementing a DNS Infrastructure

Scenario
You are the primary DNS administrator for Woodgrove Bank. You have received a request to create two new DNS zones. The Nwtraders.msft zone is for a division in the bank that requires its own DNS domain. This division will also have a group of administrators that administer the zone’s resource records. Contoso is a company that Woodgrove Bank recently acquired. To begin integration testing, you must define a DNS domain called contoso.msft and test different zone configurations. You also need to test the zone to ensure it is resilient to failure.

Exercise Overview:
In this exercise, you will configure the DNS server role on a member server, and configure the contoso.msft and nwtraders.msft zones. You then will create secondary zones for each domain and create a stub zone for Nwtraders.msft.

The main tasks are as follows:
1. Start the 6421A-NYC-DC1 and 6421A-NYC-SVR1 virtual machines, and log on as administrator with a password of Pa$$w0rd.
2. Configure the DNS Server role on NYC-SVR1.
3. Configure the Contoso.msft zone on NYC-SVR1.
4. Configure the Nwtraders.msft zone on NYC-DC1.
5. Configure zone transfer security.
6. Configure secondary zones for each domain on NYC-SVR1 and NYC-DC1.
7. Configure a stub zone for Nwtraders.msft on NYC-SVR2.
8. Configure administrative options for the Nwtraders.msft domain.

▶ Task 1: Start the 6421A-NYC-DC1, and 6421A-NYC-SVR1 virtual machines
1. Start 6421A-NYC-DC1 and log on as Administrator using the password Pa$$w0rd.
2. Start 6421A-NYC-SVR1 and log on as Administrator using the password Pa$$w0rd.
Task 2: Configure the DNS Server role on NYC-SVR1

- On NYC-SVR1, in the Server Manager console, add the DNS Server role.

Task 3: Configure the Contoso.msft zone on NYC-SVR1

1. On NYC-SVR1, open the DNS console (found in Administrative Tools).
2. Create a primary forward lookup zone named Contoso.msft.
3. Use the default options in the New Zone Wizard.

Task 4: Configure the nwtraders.msft zone on NYC-DC1

1. On NYC-DC1, open the DNS console (found in Administrative Tools).
2. Create an Active Directory Integrated primary forward lookup zone named nwtraders.msft.
3. Use the default options in the New Zone Wizard.

Task 5: Configure zone transfers

1. On NYC-DC1 configure nwtraders.msft to allow zone transfers to NYC-SVR1:
   - NYC-SVR1 IP address is: 10.10.0.24.
2. On NYC-SVR1 configure contoso.msft to allow zone transfers to NYC-DC1.
   - NYC-DC1 IP address is: 10.10.0.10.
3. Answer the following question:

   Question: Why do you need to configure the zone transfers?
Task 6: Configure secondary zones for each domain
1. On NYC-DC1, use the DNS console to configure a secondary forward zone for Contoso.msft:
   - The address of the primary zone server for Contoso.msft: 10.10.0.24.
2. On NYC-SVR1, use the DNS console to configure a secondary forward zone for nwtraders.com:
   - The address of the primary zone server for nwtraders.com: 10.10.0.10.

Task 7: Configure a stub zone for WoodgroveBank.com
1. On NYC-SVR1, use the DNS console to configure a stub zone for WoodgroveBank.com:
   - The address of the primary zone server for WoodgroveBank.com: 10.10.0.10.
2. Click WoodgroveBank.com and take note of the records listed.
3. On NYC-DC1, in the DNS console, click WoodgroveBank.com and verify that there are additional records that are not included in a stub zone.
4. Answer the following question:

   Question: Why use a stub zone instead of conditional forwarders?

Task 8: Configure administrative options for the nwtraders.msft domain
1. On NYC-DC1, use the DNS console to add the DL Nwtraders DNS Admins group to the nwtraders.msft access control list.
2. Grant the Read, Write, Create all Child objects, and Delete all child objects permissions to the DL Nwtraders DNS Admins group.
Exercise 2: Monitoring and Troubleshooting DNS

Scenario
Some users have complained that they are having trouble resolving domain names. You have to analyze the DNS infrastructure to ensure that there are no problems.

Exercise Overview
In this exercise, you will perform several tests to ensure the DNS infrastructure is working properly. You will use several DNS troubleshooting tools to validate DNS configuration and responses.

The main tasks are as follows:
1. Test simple and recursive queries.
2. Verify SOA records by using Nslookup.
3. Use the Dnslint command to verify name server records.
4. View performance statistics by using the Performance console.
5. Verify DNS replication.
6. Close all virtual machines and discard undo disks.

▶ Task 1: Test simple and recursive queries
- On NYC-DC1, in the DNS console, use the DNS Server Monitoring function to perform A simple query against this DNS Server.

▶ Task 2: Verify SOA records by using Nslookup
1. On NYC-DC1, open a command prompt and type nslookup.exe.
2. Configure a query type of SOA (Start of Authority).
3. Look up the SOA resource records for nwtraders.msft and contoso.msft.
Task 3: Use the Dnslint command to verify name server records
1. On NYC-DC1, open a command prompt and run the dnslint.exe command for the nwtraders.msft domain on the 10.10.0.10 IP address:
   - The dnslint.exe file is located in d:\Labfiles\dnslint.
2. Generate a Dnslint report html file:
   - The /s switch specifies that Dnslint will not refer to the Internet for the specified domain.
   - The /d switch specifies the domain to be searched.

Note: Consult the Help documentation if you need guidance.

Task 4: View performance statistics by using the Performance console
1. On NYC-DC1, use the Computer Management console to open Performance Monitor.
2. Add the A simple query against this DNS Server and A recursive query against this DNS Server DNS counters.
3. Use the Monitoring feature in the DNS Server properties to generate requests to the DNS server.
4. Review the data that the requests generate in Performance Monitor. Alternate between the graph view and the report view.
▶ Task 5: Verify DNS replication
1. On NYC-DC1, use the DNS console to add an A resource record called Test to the nwtraders.msft zone. Use the IP address of 10.10.0.15.
2. Verify that the A resource record created on NYC-DC1 has replicated on NYC-SVR1.
3. If the A resource record does not appear, manually force replication to occur.

▶ Task 6: Close all virtual machines and discard undo disks
1. On the host computer, click Start, point to All Programs, point to Microsoft Virtual Server, and then click Virtual Server Administration Website.
2. Under Navigation, click Master Status. For each virtual machine that is running, click the Virtual Machine Name, and in the context menu, click Turn off Virtual Machine and Discard Undo Disks. Click OK.
Module Review and Takeaways

- Review Questions
- Common Issues and Troubleshooting Tips
- Real-world Issues and Scenarios
- Best Practices
- The DNS Console
- Command-line Tools
- Monitoring Tools

Review Questions

1. You are conducting a presentation for a potential client about the advantages of using Windows Server 2008. What are the new features that you would point out when discussing the Windows Server 2008 DNS server role?

2. 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?

3. What is the difference between recursive and iterative queries?

4. What must you configure before you can transfer a DNS zone to a secondary DNS server?
5. You are the administrator of a Windows Server 2008 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 DNS server and the Bind server. What is one possible reason for this?

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

Common Issues and Troubleshooting Tips
- To resolve DNS resource record resolution problems:
  - If the change to the resource record is recent, it may not be replicated to all DNS servers.
  - In larger organizations where DNS is integrated with Active Directory, convergence can take longer.
  - The client can sometimes cache invalid DNS records. Therefore, you should clear the local DNS cache.
  - Servers on the Internet may need additional time to update information in their own cache and organization before any changes you have made begin to work properly.
- To resolve issues with DNS zone transfers:
  - Ensure that the server trying to transfer the zone is permitted in the primary zone configuration.
  - Ensure that the server to which the zone is transferring supports the zone transfer features in Windows Server 2008. It may be necessary to turn off some features.
  - Ensure that a firewall or other port-management devices that reside between the two DNS servers are not blocking Port 53 UDP.
To resolve problems when the DNS Server responds slowly to requests:
  - Verify that other programs are not impacting the server with the DNS Server role.
  - Use Performance Monitor to identify the load on the server that DNS requests generate. It may be necessary to split the load or create additional subzones.
  - Ensure that there are not a large number of stale resource records.

Real-world issues and scenarios
  - Reverse DNS zones
    Typically, administrators do not create reverse DNS zones in their DNS infrastructure. This will not cause any obvious issues at first. However, many applications use reverse DNS to resolve name information about hosts on which they are running.
    Some applications require that a reverse zone and pointer resource records are defined. Many e-mail security devices and software routinely check for a reverse DNS record for the IP address communicating with it.
  - DNS and Active Directory trusts
    When creating trusts between two Active Directory domains, the ability for domain A to lookup records in domain B (and vice versa) is tied to the configuration of the DNS infrastructure. Active Directory domains are accessible rarely on the Internet. Therefore, you need conditional forwarders, stub zones, or secondary zones to replicate the DNS infrastructure across domains and forests.
  - Secure zones against zone dumping
    By default, zone transfers are disabled in Windows Server 2008. When configuring zone transfers, it is a best practice to specify the IP address of the servers to which you want to transfer zone data. We recommend strongly that the Allow zone transfer to Any Server is not selected, especially if the server is on the Internet. With this option enabled, it is possible to dump the entire zone, which can provide a significant amount of information about the network to possible attackers.
Best Practices

- Enter the correct e-mail address of the responsible person for each zone you add to, or manage on, a DNS server. Applications use this field to notify DNS administrators for a variety of reasons. For example, query errors, incorrect data returned in a query, and security problems are a few ways in which this field can be used. While most Internet e-mail addresses contain the “@” symbol to represent the word “at” in e-mail, this symbol must be replaced with a period (.) when entering an e-mail address for this field. For example, instead of “administrator@microsoft.com”, you would use “administrator.microsoft.com”.

For more information on configuring the responsible person for a zone, see Modify the start of authority (SOA) record for a zone at http://technet2.microsoft.com/WindowsServer/en/library/e1f77652-7e1f-4902-9107-6b863ccb43501033.mspx.

- Be conservative when adding alias records to zones

Avoid using CNAME resource records (RRs) to alias a host name used in a host (A) resource record if they are unnecessary. Also, ensure that no other RRs use any alias names you use.

DNS allows an owner name of a CNAME resource record to be used as the owner name of the other types of resource records, such as NS, MX, and TXT resource records.

For more information, see the Help topic: Managing resource records.

- If you are using Active Directory, use directory-integrated storage for your DNS zones. This offers increased security, fault tolerance, and simplified deployment and management.

By integrating zones, you can simplify network planning. For example, domain controllers for each of your Active Directory domains correspond in a direct one-to-one mapping to DNS servers. This can simplify planning and troubleshooting DNS and Active Directory replication problems because the same server computers are used in both topologies.
If you are using directory-integrated storage for your zones, you may select from the different replication scopes that replicate your DNS zone data throughout the directory. If your DNS infrastructure must support Windows 2000 DNS servers, you will use the directory-integrated storage method that replicates DNS zone data to all of a domain’s controllers. If your DNS infrastructure is composed of DNS servers running Windows Server 2003 only, you may also select from replication scopes that replicate your DNS zone data to all DNS servers in the Active Directory forest, all DNS servers in a specified Active Directory domain, or all domain controllers specified in a custom replication scope.

Any DNS server hosting a directory-integrated zone is a primary DNS server for that zone. This enables a multimaster model where multiple DNS servers may update the same zone data. A multimaster model eliminates a single point of failure associated with a conventional single-master DNS topology, where updates may be done only to a single DNS server for a given zone.

One of the important benefits of directory integration is the support for secure dynamic update of the names within a zone. For more information, see Dynamic update at http://technet2.microsoft.com/WindowsServer/en/library/e760737e-9e55-458d-b5ed-a1ae9e04819e1033.mspx.

- Consider the use of secondary zones to assist in off-loading DNS query traffic wherever appropriate.

You can use secondary servers as backups for DNS clients, which enables you to load balance DNS query traffic on your network and reserve your DNS-enabled primary servers for use only by those clients that need them to perform dynamic registration and updates of their A and PTR RRs.

Disable Recursion for servers that do not answer client queries or communicate using forwarders. As DNS servers communicate amongst themselves using iterative queries, this ensures that the server responds only to queries that are intended for it.

The DNS Console

The primary tool that you use to manage DNS servers is the DNS console, which is located in the Administrative Tools folder on the Start menu. You can use the DNS console alone or as a Microsoft Management Console (MMC), further integrating DNS administration into your total network management. It also is available in Server Manager on computers with the DNS Server role installed.
Command-Line Tools

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nslookup</td>
<td>Use to perform query testing of the DNS domain namespace.</td>
</tr>
<tr>
<td>Dnscmd</td>
<td>Use this command-line interface to manage DNS servers. This utility is useful in scripting batch files to help automate routine DNS management tasks or to perform simple unattended setup and configuration of new DNS servers on your network.</td>
</tr>
<tr>
<td>Ipconfig</td>
<td>Use this command to view and modify IP configuration details that the computer uses. This utility includes additional command-line options to provide help in troubleshooting and supporting DNS clients.</td>
</tr>
<tr>
<td>DNSlint</td>
<td>Provides several automated tests to verify that DNS servers and resource records are configured properly and pointing to valid services. You can download this command from Microsoft at <a href="http://support.microsoft.com/kb/321045">http://support.microsoft.com/kb/321045</a>.</td>
</tr>
</tbody>
</table>

Monitoring Tools

The Windows Server 2008 family includes the following options for monitoring DNS servers:

- Default logging of DNS server event messages to the DNS server log. DNS server event messages are separated and kept in their own system event log – the DNS server log – which you can view using the DNS console or Event Viewer.

- Optional debug options for trace logging to a text file on the DNS server computer. You also can use the DNS console to enable additional debug logging options for temporary trace logging of DNS server activity to a text-based file. The file that is created and used for this feature, Dns.log, is stored in the systemroot\System32\Dns folder.

- Windows Performance Monitor. You can monitor specific DNS performance counters in real time to diagnose DNS problems and resource-contention issues.
Module 3

Configuring and Managing WINS

Contents:
Lesson 1: Installing the Windows Internet Name Service 3-3
Lesson 2: Managing the WINS Server 3-13
Lesson 3: Configuring WINS Replication 3-22
Lesson 4: Migrating from WINS to DNS 3-28
Lab: Configuring a WINS Infrastructure 3-35
Module Overview

- Installing the Windows Internet Name Service
- Managing the WINS Server
- Configuring WINS Replication
- Migrating from WINS to DNS

This module explains how to configure, manage, and troubleshoot Microsoft® Windows® Internet Name Service (WINS) servers. WINS is a NetBIOS Name Server (NBNS) that you can use to resolve NetBIOS names to IP addresses.
Lesson 1
Overview of the Windows Internet Name Service

- When is WINS Required?
- Overview of WINS Components
- WINS Client Registration and Release Process
- What is Burst Handling?
- WINS Server Name Resolution Process
- What Are NetBIOS Node Types?
- Demonstration: Installing and Configuring a WINS Server

The purpose of WINS in a network infrastructure is to resolve NetBIOS names to IP addresses for effective communication between systems and applications that still make use of single names.
When is WINS Required?

WINS is required for the following reasons:

- Older versions of Microsoft operating systems rely on WINS for name resolution.
- Some applications, typically older applications, rely on NetBIOS names.
- When you need dynamic registration of single-label names.
- If users rely on the Network Neighborhood or My Network Places network browser features.
- If you are not using Windows Server 2008 as your DNS infrastructure.

Key Points

WINS resolves NetBIOS names to IP addresses, which can reduce NetBIOS broadcast traffic and enable clients to resolve the NetBIOS names of computers that are on different network segments (subnets).

WINS is required for the following reasons:

- Older versions of Microsoft operating systems rely on WINS for name resolution.
- Some applications, typically older applications, rely on NetBIOS names.
- You may need dynamic registration of single-label names.
- Users may rely on the Network Neighborhood or My Network Places network browser features.
- You may not be using Windows Server 2008 as your DNS infrastructure.
Additional Reading
• Windows 2000 Server Windows Internet Naming Service (WINS) Overview
• Why you still run Windows Internet Naming Service (WINS)
Overview of WINS Components

Key Points
To install and configure a WINS server properly, systems administrators must have a thorough understanding of the WINS components and the way in which they work together in a network environment.

The complete Windows Server 2008 WINS system includes the following components:

- WINS server
- WINS database
- WINS clients
- WINS proxy agent
**Note:** Windows Server 2008 enables you to migrate from WINS to a complete DNS solution when your infrastructure supports the prerequisites presented later in the module. This is made possible by utilizing a single-label name zone, called GlobalNames, in Windows Server 2008 DNS.

**Additional Reading**
- WINS Components
WINS Client Registration and Release Process

Key Points

Name registration is the process of a WINS client requesting and receiving the use of a NetBIOS name for the services that the client makes available on the network. The request may be for a unique (exclusive) name or a group (shared) name.

Name release is the process of a WINS client requesting a NetBIOS name deregistration from the WINS database.

Additional Reading

- Verify WINS registration of client NetBIOS names
What is Burst Handling?

Burst handling allows a WINS server to handle a high number of simultaneous name registration requests.

Key Points
Burst handling allows a WINS server to handle a high number of simultaneous name registration requests.

Burst handling allows the WINS server to respond positively and immediately to WINS clients without actually accepting the name registration request.

Additional Reading
- Burst handling
WINS Server Name Resolution Process

Key Points
Before clients can use a WINS server for name resolution, you first must configure them with the IP address of the WINS server.

You can configure WINS clients with a list of multiple WINS servers. The WINS client attempts to use only the first WINS server that its TCP/IP configurations list. If the first WINS server does not respond, the WNS clients contacts other WINS servers until it receives a response or it exhausts the list of usable WINS servers.

Additional Reading
- NetBIOS over TCP/IP Name Resolution and WINS
- Microsoft TCP/IP Host Name Resolution Order
What are NetBIOS Node Types?

A NetBIOS node type determines the method that a computer uses to resolve a NetBIOS name.

<table>
<thead>
<tr>
<th>Node type</th>
<th>Description</th>
<th>Registry value</th>
</tr>
</thead>
<tbody>
<tr>
<td>B-node</td>
<td>Uses broadcasts for name registration and resolution</td>
<td>1</td>
</tr>
<tr>
<td>P-node</td>
<td>Uses a NetBIOS name server, such as WINS, to resolve NetBIOS names</td>
<td>2</td>
</tr>
<tr>
<td>M-node</td>
<td>Combines B-node and P-node, but functions as a B-node by default</td>
<td>4</td>
</tr>
<tr>
<td>H-node</td>
<td>Combines P-node and B-node, but functions as a P-node by default</td>
<td>8</td>
</tr>
</tbody>
</table>

Key Points
A NetBIOS node type is a configurable setting that determines the method that a computer uses to resolve a NetBIOS name to an IP address.

Understanding how the various node types function will help you to configure your WINS solution properly. Windows Server 2008 supports the following node types:

- B-node (broadcast)
- P-node (peer to peer)
- M-node (mixed)
- H-node (hybrid)

Additional Reading
- NetBIOS over TCP/IP Name Resolution and WINS
Demonstration: Installing and Configuring a WINS Server

In this demonstration, you will see how to install the WINS server feature and configure burst handling.
Lesson 2
Managing the WINS Server

- Overview of Client Records
- Demonstration: Filtering and Viewing Records in WINS
- How Scavenging Works
- Deleting WINS Records
- Backing Up and Restoring the WINS Database
- Compacting the WINS Database
- Demonstration: Managing the WINS Server Database

For WINS to operate effectively in a Microsoft environment, the clients and servers must have their names registered with the WINS service. There may be instances when incorrect entries in the WINS server database create problems with NetBIOS name resolution.
Overview of Client Records

A WINS client record includes the following information:

<table>
<thead>
<tr>
<th>Record Name</th>
<th>Type</th>
<th>IP Address</th>
<th>State</th>
<th>Static</th>
<th>Owner</th>
<th>Version</th>
<th>Expiration</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>MBROWSE</em> [00h] WorkStation</td>
<td>Active</td>
<td>157.56.177.171</td>
<td>157.56.177.171</td>
<td>4</td>
<td>10/2/2002 11:32:50 AM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LEGACYPC [00h] File Server</td>
<td>Active</td>
<td>157.56.177.171</td>
<td>157.56.177.171</td>
<td>2</td>
<td>10/2/2002 11:32:50 AM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LEGACYPC [00h] Workgroup</td>
<td>Active</td>
<td>157.56.177.171</td>
<td>157.56.177.171</td>
<td>3</td>
<td>10/2/2002 11:32:50 AM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LEGACYPC [16h] Normal Group Name</td>
<td>Active</td>
<td>157.56.177.171</td>
<td>157.56.177.171</td>
<td>1</td>
<td>10/2/2002 11:32:50 AM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NWTRADER S [00h] WorkStation</td>
<td>Active</td>
<td>1.2.3.4</td>
<td>157.56.177.171</td>
<td>5</td>
<td>Infinite</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NWTRADER S [03h] Messenger</td>
<td>Active</td>
<td>1.2.3.4</td>
<td>157.56.177.171</td>
<td>6</td>
<td>Infinite</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VANCOUVER [20h] File Server</td>
<td>Active</td>
<td>1.2.3.4</td>
<td>157.56.177.171</td>
<td>7</td>
<td>Infinite</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Key Points

The WINS database is made up of client records. A client record contains detailed information for each NetBIOS-dependent service that runs on a WINS client.

WINS displays all records in the database and organizes WINS record information into the following columns:

- Record Name
- Type
- IP Address
- State
- Static
- Owner
- Version
- Expiration
Additional Reading
• View WINS Records
Demonstration: Filtering and Viewing Records in WINS

In this demonstration, you will see how to filter and view records in the WINS database.
How Scavenging Works

Scavenging removes extinct entries from the WINS database

Key Points
Scavenging is the process of deleting and removing expired entries from the WINS database.

Additional Reading
- Maintaining the WINS database
Deleting WINS Records

To delete obsolete records, you can update the WINS database by:

- Simple deletion. Records selected by using the WINS console are removed from the current local WINS server
- Tombstoned deletion. Records are marked for deletion, replicated to other WINS servers, and then removed during the next scavenging operation

Key Points
You can recover unused space by deleting obsolete records in the WINS database. The WINS Management console provides improved database management by supporting the following deletion operations:

- Simple deletion of WINS database records that are stored on a single-server database.
- Tombstoned deletion, which is the removal of records that are marked for deletion (tombstoned) from the WINS database only after they have been replicated to databases on other WINS servers.
- The ability to select multiple groups of displayed database records when performing either a simple deletion or tombstoned deletion.

Additional Reading
- Deleting and tombstoning records
Back up and restore a WINS database:
- Specify a backup directory
- Back up manually or configure automatic backups

To restore a WINS database:
- Stop the WINS service
- Manually delete and restore database files

Key Points
If you are unable to repair database corruption that results from a system failure, virus attack, power failure, or other disaster, you can restore the database from a backup.

The WINS Management console provides backup tools for the WINS database.

Additional Reading
- Maintaining the WINS database
Compacting the WINS Database

Compacting recovers unused space in a WINS database

Maintain WINS database integrity by using:
- Dynamic compacting. Automatically occurs while the database is in use
- Offline compacting. Administrator stops the WINS server and uses the Jetpack.exe command-line tool

Key Points
Recovering unused space in a WINS database helps maintain performance. By compacting the WINS database, you are able to recover unused space.

Dynamic compaction occurs as a background process during idle time as the database is updated. This reduces the need to perform offline compaction.

Note: WINS uses the Jet database format for storing its data. Jet produces J<n>.log and other files in the %systemroot%\System32\Wins folder.

Additional Reading
- How to Use Jetpack.exe to Compact a WINS or DHCP Database
Demonstration: Managing the WINS Server Database

In this demonstration, you will see how to configure a WINS Backup and compact a WINS Database
Lesson 3
Configuring WINS Replication

- What is Push Replication?
- What is Pull Replication?
- What is Push/Pull Replication?
- Demonstration: Configuring WINS Replication Partner Properties
- Checking WINS Database Consistency

By default, a WINS server contains information only about its own clients. To ensure effective NetBIOS name resolution in an environment with multiple WINS servers, each WINS server needs to be aware of all clients, regardless of the WINS server that registered the client.

WINS replication occurs between two WINS servers to maintain consistent data across multiple WINS servers.

The default configuration for WINS replication partners is the push/pull replication type.

**Note:** Rather than replicate the entire database, WINS servers replicate only the changes that are made to their databases.
What is Push Replication?

- A push partner notifies replication partners based on the number of changes in its database
- Push replication maintains a high level of synchronization

Key Points

Push replication is the process of copying updated WINS data from one WINS server to other WINS servers whenever the WINS server that contains the updated data reaches a specified threshold of changes.

You should configure a replication partner as a push partner if fast communication links connect the servers.

Additional Reading
- Push partners
What is Pull Replication?

Key Points
Pull replication is the process of copying updated WINS data from a WINS server to another WINS server at specific, configurable intervals.

You should configure a replication partner as a pull partner if slow communication links connect the WINS servers.

Additional Reading
- Pull partners
What is Push/Pull Replication?

Push/pull replication ensures that the databases on multiple WINS servers are nearly identical at any given time by:

- Notifying replication partners whenever the database reaches a set threshold of changes
- Requesting replication based on a set time

Key Points
In the push/pull replication process, a WINS server updates its records with new database entries from its replication partners, based on a replication threshold and interval.

You should configure a replication partner as a push/pull partner if you want to specify both a replication threshold and interval for the partner.

WINS replication partners are configured as push/pull partners by default.

Additional Reading
- WINS replication overview
Demonstration: Configuring WINS Replication Partner Properties

In this demonstration, you will see how to configure WINS Replication Partner properties
Checking WINS Database Consistency

Key Points
Checking WINS database consistency helps maintain database integrity among WINS servers in a large network.

When you initiate consistency checking at the WINS management console, records are verified based on each owner listed in the current server database, including other WINS servers that are indirect (not directly configured) replication partners.

Additional Reading
- Manually check database consistency
Lesson 4

Migrating from WINS to DNS

- Name Resolution for a Single-Label Name
- What is the GlobalNames Zone?
- How GlobalNames Zone Name Resolution Works
- Setup Requirements for Implementing the GlobalNames Zone
- Demonstration: Migrating From WINS to DNS Using the GlobalNames Zone

Today, numerous Microsoft customers deploy WINS technology and servers in their environment.

To help customers migrate to DNS for all name resolution, the DNS Server role in Windows Server 2008 supports a special GlobalNames Zone (GNZ) feature. GNZ is designed to enable the resolution of these single-label, static, global names for servers using DNS.

GNZ is intended to assist in the retirement of WINS. However, it is not a replacement for WINS.
Name Resolution for a Single-Label Name

Windows Server 2008 introduces a new zone type for DNS called GlobalNames Zone

- Resolves single-label names in the enterprise without using WINS
- Mitigates the management and maintenance of DNS suffix search lists
- Relies on static record creation
- Requires the zone be available on DNS servers throughout the forest

Key Points
By default, DNS clients append suffixes that they obtain from several sources to resolve a single-label name.

Additional Reading
- DNS Server GlobalNames Zone Deployment document
What is the GlobalNames Zone?

The GlobalNames zone:

- Enables Single-Label name resolution for IPV6 enabled networks
- Uses CNAME records to point to the FQDN of the computer that hosts the resource
- Is recommended to be integrated in Active Directory with forest-wide replication
- Can be a used as a method to decommission WINS servers
- Requires no additional client configuration because the client resolves the name in standard DNS query form

Key Points

The GlobalNames Zone is not a new zone type, but its reserved name distinguishes it. The name *GlobalNames* indicates to the DNS Server service running on Windows Server 2008 that the zone is to be used for single-name resolution.

The recommended GNZ deployment is by using an Active Directory Domain Services-integrated zone (named GlobalNames) that is distributed globally.

Additional Reading

- DNS Server GlobalNames Zone Deployment document
How GlobalNames Zone Name Resolution Works

Key Points
The GlobalNames Zone name resolution process is as follows:

1. A user types in http://mycontoso into the browser address bar on a computer that is joined to the engineering.corp.contoso.com domain.
2. The browser calls the GetAddrInfo() function to resolve the name mycontoso.
3. GetAddrInfo() invokes the DNS client to resolve the name.
4. The DNS client sends out the following qualified queries (based on the suffix search list):
   - mycontoso.engineering.corp.contoso.com ➔ Name Error
   - mycontoso.accounting.corp.contoso.com ➔ Name Error
   - mycontoso.itgroup.corp.contoso.com ➔ Name Error
5. If the qualified queries fail, the DNS server searches the GlobalNames zone, if configured, and tries to resolve that zone’s single-label name.
Additional Reading

- DNS Server GlobalNames Zone Deployment document
Setup Requirements for Implementing the GlobalNames Zone

- Requires authoritative name servers running Windows Server 2008
- Configure forest-wide, Active Directory-integrated replication of the GlobalNames zone
- Create static CNAME records that point to FQDN records
- Disable dynamic updates on the GlobalNames zone
- Enable single-label GlobalNames zone support on all DNS servers that host the zone

Use the following command to enable support for the GlobalNames zone on all DNS servers hosting the zone:

```
dnscmd /config /EnableGlobalNamessupport 1
```

Key Points
There are different methods for implementing the GlobalNames zone:

- Deploy multiple forests
- Deploy all domains and client computers in all forests
- Use a select set of DNS servers to host the GNZ

Additional Reading
- DNS Server GlobalNames Zone Deployment document
Demonstration: Migrating From WINS to DNS Using the GlobalNames Zone

In this demonstration, you will use the GlobalNames zone to migrate from WINS to DNS
Lab: Configuring a WINS Infrastructure

- Exercise 1: Installing WINS
- Exercise 2: Configuring WINS Burst Handling
- Exercise 3: Configuring WINS Replication
- Exercise 4: Migrating from WINS to DNS

Logon information

<table>
<thead>
<tr>
<th>Virtual machines</th>
<th>NYC-DC1 and NYC-SVR1</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Administrator</td>
</tr>
<tr>
<td>Password</td>
<td>Pa$$wOrd</td>
</tr>
</tbody>
</table>

Estimated time: 60 minutes

Objectives
- Install WINS
- Configure WINS burst handling
- Configure WINS replication
- Migrate from WINS to DNS

Scenario
You are tasked with installing a second WINS server for the Woodgrovebank domain for fault tolerance and use as a secondary WINS server resolver for domain clients. The database consistency and speed of convergence are of the utmost importance. Replication must be set up to make sure records replicate on change vector or time vector, whichever happens to occur first.
After successfully implementing the secondary WINS server, management wants you to test the new GlobalNames zone use in Windows Server 2008 DNS to help retire WINS servers that the Woodgrovebank domain uses. IT staff are finding the task of maintaining the domain name suffix-search list difficult, and Woodgrovebank domains still use single-label names for internal web server names. Install and verify that this new option in DNS will help in decommissioning the existing WINS servers.

**Lab Setup**
For this lab you will use the available virtual machine environment. Before you begin the lab, you must:

1. Start the 6421A-NYC-DC1 and 6421A-NYC-SVR1 virtual machines.
2. Log on to 6421A-NYC-SVR1 with the user name `Woodgrovebank\administrator` and the password `Pa$$w0rd`.
3. Close the Initial Configuration Tasks window.
4. Close the Server Manager window.
Exercise 1: Installing WINS

Exercise Overview:
In this exercise, you will install the WINS feature on 6421A-NYC-SVR1.
The main tasks are as follows:
1. Verify the lab setup.
2. Open the Server Manager console.
3. Install the WINS feature.

► Task 1: Ensure that you have completed the steps in the Lab Setup
   • Review the Lab Setup section and ensure you have completed the steps before you continue with this lab.

► Task 2: On 6421A-NYC-SVR1, launch the Server Manager console
   1. Open Administrative Tools.
   2. Launch Server Manager.

Note: The Server Manager console opens.
Task 3: From the Server Manager console, install the WINS feature

1. In Server Manager, use the Add Features Wizard to install the WINS feature on 6421A-NYC-SVR1.

2. On the Installation Results page, verify that the installation succeeded before closing the wizard.

Note: The WINS feature is installed on 6421A-NYC-SVR1.

Important: Do not log off or shut down the virtual machines at this point.
Exercise 2: Configuring WINS Burst Handling

Exercise Overview:
In this exercise, you will configure burst handling, create a static record, configure scavenging intervals, and configure clients to use the WINS servers for NetBIOS resolution.

The main tasks are as follows:
1. Configure the WINS server for burst handling.
2. Create a static entry in the WINS database.
3. Configure scavenging on the WINS server.
4. Configure NYC-DC1 to use the WINS server for NetBIOS resolution.
5. Test NetBIOS name resolution.

▶ Task 1: Configure the WINS server for burst handling
1. On NYC-SVR1, start the WINS console.
2. Configure Burst Handling with the option of Low.

▶ Task 2: Create a static entry in the WINS database
1. In the WINS console, create a New Static Mapping with the following properties:
   - Computer name of HRWEB
   - IP address of 10.10.0.10
2. Use Active Registrations to verify the new static entry exists.

Note: Do not close the WINS console.
Task 3: Configure scavenging on the WINS server to take place once every seven days
- In the WINS Properties dialog box for NYC-SVR1, use the Intervals tab to set the extinction timeout value to seven days.

Task 4: Configure 6421A-NYC-DC1 to use the WINS server for NetBIOS resolution
1. On NYC-DC1, open Network Connections and open the properties of the Local Area Connection.
2. In the Local Area Connection Properties dialog box, under This Connection Uses the Following Items, open the properties of TCP/IPv4.
3. Click Advanced and configure the computer to use the WINS server (IP address of 10.10.0.24).

Task 5: Test the NetBIOS name resolution capabilities
- On NYC-DC1, in a command window, type ping hrweb.
  The name resolution should be successful and resolve to 10.10.0.10.
Exercise 3: Configuring WINS Replication

Exercise Overview:
In this exercise, you will configure the WINS feature on 6421A-NYC-SVR1 and 6421A-NYC-DC1 to be push/pull replication partners to maintain the consistency of WINS records.

The main tasks are as follows:
1. Configure push and pull replication on NYC-DC1.
2. Configure push and pull replication on NYC-SVR1.
3. Verify replication.

► Task 1: Configure push and pull replication on NYC-DC1
1. Open WINS from the Administrative Tools menu.
2. In the WINS Administrative Tool window, use Replication Partners to select a new replication partner with the IP address of 10.10.0.24.
   The Replication Partners details pane lists NYC-SVR1 as a Push/Pull partner.

► Task 2: Configure push and pull replication on NYC-SVR1
1. Open WINS from the Administrative Tools menu.
2. In the WINS Administrative Tool window, use Replication Partners to select a new replication partner with the IP address of 10.10.0.10.
   The Replication Partners details pane lists NYC-DC1 as a Push/Pull partner.

► Task 3: Verify replication
1. On NYC-SVR1, force replication and then verify that records appear from both 10.10.0.10 and 10.10.0.11 as owners.
2. On NYC-DC1, force replication and then verify that records appear from both 10.10.0.10 and 10.10.0.24 as owners.
Exercise 4: Migrating from WINS to DNS

Exercise Overview:
In this exercise, you will migrate single-label name resolution from WINS to the GlobalNames zone in DNS.

The main tasks are as follows:
1. Create a GlobalNames zone and enable GNZ functionality.
2. Create an Alias record for a single-label name resource.
3. Decommission WINS.
4. Verify GlobalNames single-label name resolution.
5. Close all virtual machines and discard undo disks.

▶ Task 1: Create the GlobalNames zone in DNS
1. On NYC-DC1, open the DNS console from the Administrative Tools menu.
2. Create a new forward lookup zone with a name of GlobalNames, a replication scope that is forest wide and do not allow dynamic updates.
3. Open an administrative command prompt.
4. Type Dnscmd NYC-DC1 /config /Enableglobalnamessupport 1 and then press ENTER.

▶ Task 2: Create the Alias record for the single-label name resource
1. In the DNS Manager console, create a New Alias (CNAME) record in the GlobalNames forward lookup zone with an alias name of HRWEB and a FQDN of NYC-DC1.Woodgrovebank.com.
2. Close the DNS Manager console.
Task 3: Decommission WINS on NYC-DC1 and NYC-SVR1
1. On both **NYC-DC1** and **NYC-SVR1**, launch the Server Manager console from the **Administrative Tools** menu.
2. Remove the **WINS** feature from both NYC-DC1 and NYC-SVR1. Restart as necessary.

Task 4: Verify GlobalNames single-label name resolution
1. Log on to NYC-DC1 as **administrator** with a password of **Pa$$w0rd**.
2. Log on to NYC-SVR1 as **administrator** with a password of **Pa$$w0rd**.
3. Complete the WINS removal as required on both servers.
4. On NYC-DC1, open a command prompt and then type **ping hrweb**.
   The ping command is successful and resolves to nyc-dc1.woodgrovebank.com.

Task 5: Close all virtual machines and discard undo disks
1. On the host computer, click **Start**, point to **All Programs**, point to **Microsoft Virtual Server** and then click **Virtual Server Administration Website**.
2. Under **Navigation**, click **Master Status**. For each virtual machine that is running, click the Virtual Machine Name, and in the context menu, click **Turn off Virtual Machine and Discard Undo Disks**. Click **OK**.
Module Review and Takeaways

- Review Questions
- Considerations for WINS Services
- Best Practices
- Tools

Review questions

1. In the case of a corrupt database in WINS where a backup location was specified during configuration, what are the steps to repair the WINS server so it is in an operational state?

2. What are some of the benefits that you can realize by using the GNZ in DNS for single-label name resolution?

3. Your organization is thinking about decommissioning its WINS servers and use DNS entirely for name resolution. What steps should be taken to ensure that this is done successfully, if it can be done at all?

4. Can WINS be used in an IPv6 environment? What must be configured on Windows clients so that they may use the WINS server for NetBIOS resolution?
Considerations for WINS Services

Make sure you consider the following prior to installing WINS services:

- WINS is legacy technology. You should decommission WINS in your environment if at all possible.
- If you require dynamic registration of NetBIOS names in your environment, the GNZ option in DNS is not a good choice. WINS is required.
- If you are using WINS in your environment, make sure that all servers also have the IP addresses of the WINS servers to use in their IP configuration.

Best Practices

- Use default settings to configure WINS servers.
- Avoid using static WINS entries for anything other than mission-critical servers.
- Select Push/Pull when configuring replication partners.
- For best results in WINS replication and convergence time, use a hub-and-spoke design model.
- Use only as many WINS servers as you need.
- To maximize server performance, purchase hardware with optimal disk performance characteristics to handle WINS.
- Monitor and perform regular, offline compaction.
- Perform regular backups of the WINS database.
- Configure clients with more than one WINS server IP address.
- Configure each WINS server computer to point to itself.
- Use NBTSTAT -RR to register and troubleshoot client connectivity.
Tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Use for</th>
<th>Where to find it</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Management Console</td>
<td>Local and Remote administration of all installed Roles and Features in Server 2008.</td>
<td>Click <strong>Start</strong>, and then point to <strong>Administrative Tools</strong>. Select a pre-configured tool or type <strong>mmc</strong> in the <strong>Run</strong> box to create a custom MMC console based on the snap-ins that you specify.</td>
</tr>
<tr>
<td>WINS management tool</td>
<td>Configuration of the WINS service on remote servers and the local server.</td>
<td>Click <strong>Start</strong>, and then point to <strong>Administrative Tools</strong>. Select <strong>WINS</strong> from the available management tools.</td>
</tr>
<tr>
<td>Server Manager</td>
<td>Management and Maintenance of the installation and removal of Roles and Features.</td>
<td>Click <strong>Start</strong>, and then point to <strong>Administrative Tools</strong>. Select <strong>Server Manager</strong> from the available administrative tools.</td>
</tr>
<tr>
<td>DNS management tool</td>
<td>Configuration of the DNS service on remote servers or the local server.</td>
<td>Click <strong>Start</strong>, and then point to <strong>Administrative Tools</strong>. Select <strong>DNS</strong> from the available management tools.</td>
</tr>
</tbody>
</table>
Module 4

Configuring and Troubleshooting DHCP

Contents:
Lesson 1: Overview of the DHCP Server Role 4-3
Lesson 2: Configuring DHCP Scopes and Options 4-11
Lesson 3: Managing a DHCP Database 4-22
Lesson 4: Monitoring and Troubleshooting DHCP 4-30
Lesson 5: Securing DHCP 4-38
Lab: Configuring and Troubleshooting the DHCP Server Role 4-43
Module Overview

- Overview of the DHCP Server Role
- Configuring DHCP Scopes and Options
- Managing a DHCP Database
- Monitoring and Troubleshooting DHCP
- Securing DHCP

This module explains how to configure, manage, and troubleshoot Dynamic Host Configuration Protocol (DHCP) servers, and DHCP Scopes.
Lesson 1

Overview of the DHCP Server Role

- Benefits of Using DHCP
- New DHCP Features in Windows Server 2008
- How DHCP Allocates IP Addresses
- How DHCP Lease Generation Works
- How DHCP Lease Renewal Works
- DHCP Server Authorization
- Demonstration: Adding the DHCP Server Role

DHCP plays an important role in the Windows Server® 2008 infrastructure. It is the primary means of distributing important network information to network clients, and it includes important aspects of many other network-enabled tools, including Windows Deployment Services (WDS) and Network Access Protection (NAP).
Benefits of Using DHCP

DHCP reduces the complexity and amount of administrative work by using automatic TCP/IP configuration

<table>
<thead>
<tr>
<th>Manual TCP/IP Configuration</th>
<th>Automatic TCP/IP Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>• IP addresses are entered manually</td>
<td>• IP addresses are supplied automatically</td>
</tr>
<tr>
<td>• IP address could be entered incorrectly</td>
<td>• Correct configuration information is ensured</td>
</tr>
<tr>
<td>• Communication and network issues can result</td>
<td>• Client configuration is updated automatically</td>
</tr>
<tr>
<td>• Frequent computer moves increase administrative effort</td>
<td>• A common source of network problems is eliminated</td>
</tr>
</tbody>
</table>

Key Points

The DHCP protocol simplifies configuration of IP clients in a network environment.

With the DHCP Server role, you can ensure that all clients have the same configuration information, which eliminates human error during configuration.
New DHCP Features in Windows Server 2008

Key Points
The DHCP role on Microsoft Windows Server 2008 supports several new features.

- DHCPv6 stateful and stateless configuration is supported for configuring clients in an IPv6 environment.
- Network Access Protection (NAP) with DHCP helps isolate potentially malware-infected computers from the corporate network.
- DHCP can be installed as a role on a Windows Server 2008 Server Core installation.

Additional Reading
- DHCP Server
- The DHCPv6 Protocol
How DHCP Allocates IP Addresses

Key Points
DHCP allocates IP addresses on a dynamic basis, which is known as a lease. The lease value can be set to unlimited. However, the value typically is not more than a few hours or days. The default lease time is eight hours.

Additional Reading
- How DHCP Works
How DHCP Lease Generation Works

Key Points
The DHCP protocol lease-generation process includes four steps that enable a client to obtain an IP address. Understanding how each step works will help you to troubleshoot problems when clients cannot obtain an IP address:

1. The DHCP client broadcasts a **DHCPDISCOVER** packet.
2. Any DHCP Server in the subnet will respond by broadcasting a **DHCPOFFER** packet.
3. The client receives the **DHCPOFFER** packet.
4. The DHCP servers receive the **DHCPREQUEST**.

Additional Reading
- Request for Comments: 1531 Dynamic Host Configuration Protocol
- TCP/IP Fundamentals for Microsoft Windows: Chapter 6 - Dynamic Host Configuration Protocol
How DHCP Lease Renewal Works

Key Points
When the DHCP lease has reached 50 percent of the lease time, the client will attempt to renew the lease. This is an automatic process that occurs in the background. Computers may have the same IP address for a long period of time if they operate continually on a network without being shut down.

Additional Reading
• Request for Comments: 1531 Dynamic Host Configuration Protocol
DHCP Server Authorization

**Key Points**

DHCP allows a client computer to acquire configuration information about the network in which it is started up. DHCP communication occurs before any authentication of the user or computer, and because the DHCP protocol is based on IP broadcasts, an incorrectly configured DHCP server in a network can provide invalid information to clients. To avoid this, the server must be authorized.

**Additional Reading**

- DHCP Resources
- Networking Collection
Demonstration: Adding the DHCP Server Role

In this demonstration, you will see how to add and authorize the DHCP Server role
Lesson 2
Configuring DHCP Scopes and Options

- What are DHCP Scopes?
- What are Superscopes and Multicast Scopes?
- Demonstration: Configuring DHCP Scopes
- What are DHCP Options?
- What Are DHCP Class-Level Options?
- What Is a DHCP Reservation?
- How DHCP Options Are Applied
- DHCP Sizing and Availability
- Demonstration: Configuring DHCP Options

Administrators must configure the DHCP scopes after the DHCP role is installed on a server. A DHCP scope is the primary method by which you can configure options for a group of IP addresses. It is based on an IP subnet and can have settings specific to hardware or custom groups of clients. In this lesson, you will learn about superscopes, scope options, and managing scopes.
What are DHCP Scopes?

A scope is a range of IP addresses that are available to be leased.

Scope Properties
- Network ID
- Subnet mask
- Lease duration
- Network IP address range
- Scope name
- Exclusion range

Key Points
A DHCP scope is a range of IP addresses that are available for lease. A scope typically is confined to the IP addresses in a given subnet.
What are Superscopes and Multicast Scopes?

**Key Points**

A superscope is a collection of scopes that are grouped together into an administrative whole. This allows clients to receive an IP address from multiple logical subnets, even when they are on the same physical subnet.

A multicast scope is a collection of multicast addresses from the class D IP address range of 224.0.0.0 to 239.255.255.255. These addresses are used when applications need to efficiently communicate with numerous clients simultaneously.
Demonstration: Configuring DHCP Scopes

In this demonstration, you will see how to:

- Create and authorize a DHCP scope
- Configure a DHCP superscope
What are DHCP Options?

**DHCP options** are values for common configuration data that applies to the server, scopes, reservations, and class options.

<table>
<thead>
<tr>
<th>Common scope options are:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• DNS Servers</td>
</tr>
<tr>
<td>• DNS Name</td>
</tr>
<tr>
<td>• Default Gateway</td>
</tr>
<tr>
<td>• WINS Servers</td>
</tr>
</tbody>
</table>

**Key Points**

DHCP servers can configure more than just an IP address. They also provide information about network resources, such as DNS servers and the default gateway. You can apply DHCP options at the server, scope, user, and vendor levels.

An option code identifies the DHCP options, and most option codes come from the Request for Comments (RFC) documentation found on the Internet Engineering Task Force (IETF) website.

**Additional Reading**

- DHCP Tools and Settings
- Request for Comments: 2132 - DHCP Options and BOOTP Vendor Extensions
What Are DHCP Class-Level Options?

**DHCP class-level options are scope options that apply to a specific type of device**

<table>
<thead>
<tr>
<th>DHCP class-level option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor-class</td>
<td>Configured by vendors such as Microsoft, HP, and Sun</td>
</tr>
<tr>
<td>User-class</td>
<td>Set and viewed by the user</td>
</tr>
</tbody>
</table>

**Key Points**

DHCP options can be applied at several different levels, such as at the server and scope levels. You may need to apply scope options to custom types of computers or specific groups of users.

You specify class-level options when you need to configure a device belonging to a particular class in a specific way. A class is a logically defined group based on attributes of the IP-based device. This can be based on vendor-specific data or it may be user-defined.

Class-level options include:

- Vendor class
- User class
Additional Reading

- DHCP Resources
- Using option classes
What Is a DHCP Reservation?

**Key Points**

A DHCP reservation occurs when an IP address within a scope is set aside for use with a specific DHCP client.

Configuring reservations enables you to centralize management of fixed IP addresses.

You can configure custom DHCP options for reservations. These settings will override all other DHCP options that you configure at higher levels.
DHCP Sizing and Availability

Key Points
When configuring DHCP scopes and scope options, you must consider how many IP addresses to assign and how you will implement fault tolerance. It is a best practice to have more than one DHCP server in the network. In the event that one server fails, a backup server is in place to lease IP addresses.

Additional Reading
- Configuring scopes
- DHCP Best Practices
How DHCP Options Are Applied

Key Points
If you have configured DHCP options at multiple levels (server, scope, class, and reservation levels), DHCP applies options to client computers in the following order:

1. Server level
2. Scope level
3. Class level
4. Reserved-client level

It is important to understand these options when you are troubleshooting DHCP.

Additional Reading
- DHCP Resources
Demonstration: Configuring DHCP Options

In this demonstration, you will see how to configure DHCP server, scope, and class options.
Lesson 3
Managing a DHCP Database

- Overview of DHCP Management Scenarios
- What is a DHCP Database?
- How a DHCP Database is Backed Up and Restored
- How a DHCP Database is Reconciled
- Moving a DHCP Database
- DHCP Server Configuration Options
- Demonstration: Managing a DHCP Database

The DHCP database stores information about the IP address leases. It is important to understand how to backup the database and resolve database issues if there is a problem. In this lesson, you will learn how to manage the database and its data.
Overview of DHCP Management Scenarios

Key Points
The DHCP server database contains configuration data about the DHCP server and information about client IP leases. If this information becomes corrupt or inconsistent, it can lead to network configuration errors on clients’ computers. It also can lead to the same IP address being offered to multiple clients.

Management scenarios may include:

• Managing DHCP database growth.
• Backup and restore.
• DHCP database consistency.
• Moving the DHCP database.
• Adding clients.
• Adding new network service servers.
• Adding new subnets.
What is a DHCP Database?

The **DHCP database** is a dynamic database that contains configuration information

- The DHCP database contains DHCP configuration data such as:
  - Scopes
  - Address leases
  - Reservations

- Windows Server 2003 stores the DHCP database in the %Systemroot%\System32\Dhcp folder

- The DHCP database files include:
  - Dhcp.mdb
  - Tmp.edb
  - J50.log and J50*.log
  - Res*.log
  - J50.chk

Key Points

The DHCP database is the data file that stores the DHCP configuration information and the lease data for clients that have leased an IP address from the DHCP Server.

The DHCP server database is a dynamic database that is updated as DHCP clients are assigned or as they release their TCP/IP configuration parameters.
How a DHCP Database is Backed Up and Restored

Key Points
You can back up a DHCP database manually or configure it to backup automatically. An automatic backup is called a synchronous backup. A manual backup is called an asynchronous backup.

- Automatic (synchronous) backup. The DHCP database is backed up automatically every 60 minutes.
- Manual (asynchronous) backup. If you have an immediate need to create a backup, you can run the backup option in the DHCP console.

Additional Reading
- Backing up the DHCP database
- Restoring server data
How a DHCP Database is Reconciled

Key Points
Reconciling scopes can fix inconsistencies, such as incorrect or missing information, for client IP addresses that the scope lease information stores.

The DHCP Server service stores scope IP address-lease information in two forms:
- Detailed IP address lease information, which the DHCP database stores
- Summary IP address lease information, which the server’s Registry stores
Moving a DHCP Database

Key Points
In the event that you must move the DHCP Server role to another server, it is advisable to move the database to the new server, as well. This ensures that client leases are retained and reduces the likelihood of client-configuration issues.

You move the database initially by backing it up on the old DHCP server. Then, shut down the DHCP service on the old DHCP server. The DHCP database then is copied to the new server, where you can restore it using the normal database restore procedure.
DHCP Server Configuration Options

Key Points
The DHCP server-configuration options define server-wide behaviors. Certain configurations also affect the scopes that the server hosts.

- General options. These options enable the administrator to set DHCP debugging and troubleshooting statistics.

- DNS options. Configuring the DNS options is important if there are devices or operating systems that do not update their DNS information automatically.

- Network Access Protection options. These enable you to configure NAP to be enforced for one or more scopes.

- Advanced options. These options enable the administrator to force the DHCP server to check for IP conflicts when a DHCP client requests a particular IP address.
Demonstration: Managing a DHCP Database

In this demonstration, you will see how to manage a DHCP database.
Lesson 4
Monitoring and Troubleshooting DHCP

- Overview of Monitoring DHCP
- Common DHCP Issues
- What Are DHCP Statistics?
- What Is a DHCP Audit Log File?
- Monitoring DHCP Server Performance
- Demonstration: Monitoring DHCP

DHCP is a core service in modern network environments. If the DHCP service is not working properly, or if there is a situation that is causing problems with the DHCP server, it is important to know that an issue is occurring and how you can locate the problem. In this lesson, you will examine common DHCP issues and learn how to diagnose and fix them.
Overview of Monitoring DHCP

Key Points

DHCP is a dynamic protocol. Changes in the network environment usually result in DHCP server changes to accommodate the new environment.

DHCP has three sources of information that you can use for monitoring:

- DHCP statistics
- DHCP events
- DHCP performance data
Common DHCP Issues

The following table describes and provides examples of common DHCP issues:

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address conflicts</td>
<td>The same IP address is offered to two different clients.</td>
<td>An administrator deletes a lease. However, the client who had the lease still believes the lease is valid. If the DHCP server does not verify the IP, it may release the IP to another machine, causing an address conflict. This also can occur if two DHCP servers have overlapping scopes.</td>
</tr>
<tr>
<td>Failure to obtain a DHCP address</td>
<td>The client does not receive a DHCP address and instead receives an Automatic Private IP Addressing (APIPA) self-</td>
<td>If a client’s network card drive is configured incorrectly, it may cause a failure to obtain a DHCP address.</td>
</tr>
<tr>
<td>Issue</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Address obtained from incorrect scope</td>
<td>The client is obtaining an IP address from the wrong scope, causing it to</td>
<td>This often occurs because the client is connected to the wrong network.</td>
</tr>
<tr>
<td></td>
<td>experience communications problems.</td>
<td></td>
</tr>
<tr>
<td>DHCP database suffers data corruption or</td>
<td>The DHCP database become unreadable or is lost due to a hardware failure.</td>
<td>A hardware failure can cause the database to become corrupted.</td>
</tr>
<tr>
<td>loss</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP server exhausts its IP address pool</td>
<td>The DHCP server’s IP scopes have been depleted. Any new client requesting</td>
<td>All the IPs assigned to a scope are leased.</td>
</tr>
<tr>
<td></td>
<td>an IP address will be refused.</td>
<td></td>
</tr>
</tbody>
</table>
What Are DHCP Statistics?

DHCP statistics are collected at either the server level or scope level.

Key Points
DHCP statistics provide information about DHCP activity and usage. You can use this console to determine quickly whether there is a problem with the DHCP service or with the network’s DHCP clients.
What Is a DHCP Audit Log File?

A DHCP audit log is a log of service-related events

Key Points
The audit log provides a traceable log of DHCP server activity. You can use this log to track lease requests, grants, and denials, and this information allows you to troubleshoot DHCP server performance.

Additional Reading
- Audit logging
## Monitoring DHCP Server Performance

<table>
<thead>
<tr>
<th>Performance counters</th>
<th>What to look for after a baseline is established</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets received/second</td>
<td>Monitor for sudden increases or decreases, which could reflect network problems</td>
</tr>
<tr>
<td>Requests/second</td>
<td>Monitor for sudden increases or decreases, which could reflect network problems</td>
</tr>
<tr>
<td>Active queue length</td>
<td>Monitor for both sudden and gradual increases, which could reflect increased load or decreased server capacity</td>
</tr>
<tr>
<td>Duplicates dropped/second</td>
<td>Monitor for any activity that could indicate that more than one request is being transmitted on behalf of clients</td>
</tr>
</tbody>
</table>

### Key Points

DHCP performance counters become available after you install the DHCP Server role. You then can use Performance Monitor to load the performance counters.

A DHCP server typically should not come under a heavy network load. However, if you notice the queue lengths are logging consistently high values, you should check the server for bottlenecks that could be slowing DHCP performance.

### Additional Reading

- DHCP performance monitoring reference
Demonstration: Monitoring DHCP

In this demonstration, you will see how to monitor DHCP statistics and performance
Lesson 5
Securing DHCP

- Securing DHCP
- Preventing an Unauthorized User from Obtaining a Lease
- Restricting Unauthorized, Non-Microsoft DHCP Servers from Leasing IP Addresses
- Restricting DHCP Administration

DHCP protocol has no built-in method for authenticating users. This means that if you do not take precautions, IP leases could be granted to devices and users who have malicious intent. In this lesson, you will learn how to prevent unauthorized users from obtaining a lease, how to manage rogue DHCP servers, and how to configure DHCP servers so that a specific group can manage them.
Securing DHCP

Reasons for securing DHCP include:

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

Key Points

Reasons for securing DHCP include:

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

Key Points
DHCP by itself can be difficult to secure. This is because the protocol is designed to work before the necessary information is in place for a client computer to authenticate with a domain controller.

Basic precautions that you should take to limit unauthorized access include:

- Make sure that you reduce physical access.
- Enable audit logging on all DHCP servers.
- Authenticate users.
- Implement NAP.

Additional Reading
- Network Access Protection
- Step-by-Step Guide: Demonstrate DHCP NAP Enforcement in a Test Lab
Restricting Unauthorized, Non-Microsoft DHCP Servers from Leasing IP Addresses

Key Points

Many devices and network operating systems have DHCP server implementations. Networks are almost never homogeneous in nature, and therefore it is possible that at some point a DHCP server that does not check for Active Directory-authenticated servers will be enabled on the network. In this case, clients may obtain incorrect configuration data.

To eliminate an unauthorized DHCP server, you must locate and disable it from communicating on the network either physically or by disabling the DHCP service.

Additional Reading

- Manage Server Access
Restricting DHCP Administration

To restrict who can administer the DHCP service:

- Limit the members of the DHCP Administrators group
- Add users needing read-only access to the DHCP Users group

<table>
<thead>
<tr>
<th>Account</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Administrators group</td>
<td>Can view and modify any data about the DHCP server</td>
</tr>
<tr>
<td>DHCP Users group</td>
<td>Has read-only DHCP console access to the server</td>
</tr>
</tbody>
</table>

Key Points
The DHCP Administrators group is in the built-in groups on domain controllers or on local servers because the DHCP Administrators local group is used to restrict and grant access to administer DHCP servers.

Authorization of a DHCP service is only available to Enterprise administrators. If the need exists for a down-level administrator to authorize the domain, it can be done using Active Directory delegation.

Any user in the DHCP Administrators group can manage the server’s DHCP service.

Any user in the DHCP Users group can have read-only access to the console.

Additional Reading
- Manage Server Access
Lab: Configuring and Troubleshooting the DHCP Server Role

- Exercise 1: Installing and Authorizing the DHCP Server Role
- Exercise 2: Configuring a DHCP Scope
- Exercise 3: Troubleshooting Common DHCP Issues

Logon information

<table>
<thead>
<tr>
<th>Virtual machine</th>
<th>NYC-DC1, NYC-CL1</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Administrator</td>
</tr>
<tr>
<td>Password</td>
<td>Pa$$w0rd</td>
</tr>
</tbody>
</table>

Estimated time: 30 minutes
Exercise 1: Installing and Authorizing the DHCP Server Role

Scenario
You are the Network Administrator at Woodgrove Bank, which recently opened a new division that needs a DHCP service configured for approximately 200 clients. You must configure a DHCP server for the new division.

Exercise Overview
In this exercise, you will install the DHCP role and then authorize the server in the woodgrovebank.com domain.

The main tasks are as follows:
- Start the 6421A-NYC-DC1 and 6421A-NYC-CL1 virtual machines, and log on as Administrator with a password of Pa$$w0rd.
- Configure the DHCP Server role on NYC-DC1.
- Authorize the DHCP Server role on NYC-DC1.

Task 1: Start the 6421A-NYC-DC1 and 6421A-NYC-CL1 virtual machines and log on as Administrator
1. Open the Virtual Server Remote Control Client and then double-click 6421A-NYC-DC1.
2. Log on to NYC-DC1 as Administrator using the password Pa$$w0rd. Close the Initial Configuration Tasks window.
3. Open the Virtual Server Remote Control Client and then double-click 6421A-NYC-CL1.
4. Log on to NYC-CL1 as Administrator using the password Pa$$w0rd.
Task 2: Configure the DHCP Server Role on NYC-DC1

- On NYC-DC1, use Server Manager to add the DHCP Server role:
  - Bind the DHCP service to the IP: 10.10.0.10.
  - Use default values for all steps except: Disable DHCPv6 for Applications on this network.
  - Make sure to Skip Authorization of this DHCP server in AD DS.

Task 3: Authorize the DHCP Server Role on NYC-DC1

- On NYC-DC1, use the DHCP console to authorize the NYC-DC1.woodgrovebank.com DHCP server.
Exercise 2: Configuring a DHCP Scope

Scenario
You need to configure a DHCP scope for approximately 200 clients. The scope must provide information concerning the DNS server and the default gateway as part of the information that clients receive when they request a DHCP address.

Exercise Overview
In this exercise, you will configure a new DHCP scope, activate the scope, and configure scope options so that clients receive the correct information when they lease an IP address.

The main tasks are as follows:
- Configure a DHCP scope.
- Configure DHCP scope options.
- Test the scope using a client workstation.

Task 1: Configure a DHCP scope
1. On NYC-DC1, use the Server Manager console to create a new DHCP IPv4 scope:
   - Name of the scope: Head Office Network Scope
   - The IP address range for the scope: 10.10.0.1 - 10.10.0.254 using a subnet mask of: 255.255.0.0
   - An exclusions range of 10.10.0.1 - 10.10.0.30 should be added for servers and other devices that use a static IP address
   - Lease duration of one hour
   - Do not configure any additional scope options
2. On NYC-CL1, set the Local Area Connection properties for DHCP configuration on IPv4 properties for both IP address and DNS resolver configuration. Make sure the client computer can obtain an IP address. Verify that the client is configured with a default gateway.

**Question:** Why does the DHCP-configured Local Area Connection not have a default gateway?

**Task 2: Configure DHCP scope options**
- On NYC-DC1, use the DHCP console to configure the 003 Router DHCP scope option to point to 10.10.0.10.

  *Note: Make sure to configure the scope options and not the server options.*

**Task 3: Test the scope using a client workstation**
- On NYC-CL1, use the command prompt and the `ipconfig` utility to test whether the client is able to obtain an IP address and a default gateway, as the previous task specifies.
Exercise 3: Troubleshooting Common DHCP Issues

Scenario
The DHCP server has now been configured. To ensure minimal downtime, your department has requested that the DHCP administration team troubleshoot several potential configuration problem scenarios.

Exercise Overview
You will run a script that will configure the DHCP server so that it will not work properly. Using the available information, you will then fix the configuration problems that the script caused.

The main tasks are as follows:
• Verify DHCP lease information.
• Modify DHCP Server configuration using scripts to simulate configuration issues.
• Check the client’s ability to lease an IP address.
• Determine why the DHCP server is not allocating IP addresses.
• Identify information that has been changed.
• Configure the DHCP server with the correct router information.
• Configure the DHCP server with the correct DNS server information.
• Configure the DHCP with the proper lease period.
• Verify the information being leased to the client.
• Close all virtual machines and discard undo disks.

Task 1: Verify DHCP lease information
• On NYC-CL1, verify lease information and note the following settings:
  • IPv4 Address
  • Subnet Mask
  • Default Gateway
  • Lease Duration
Task 2: Modify DHCP Server configuration using scripts to simulate configuration issues
- At a command prompt, run the D:\Labfiles\Module4\DHCP.vbs script.

Task 3: Check the client’s ability to lease an IP address
- On NYC-CL1, use ipconfig to determine the most critical issue affecting the DHCP server.

Task 4: Determine why the DHCP server is not allocating IP addresses
- On NYC-DC1, determine if the DHCP scope is activated.

Task 5: Identify information that has changed
- On NYC-CL1, identify the information that has changed. Compare settings to those noted before running the DHCP.VBS script.

Task 6: Configure the DHCP server with the correct router information
- On NYC-DC1, verify the router information configured in the scope options.

Task 7: Configure the DHCP server with the correct DNS server information
- On NYC-DC1, verify the DNS server information configured in the scope options.

Task 8: Configure the DHCP with the proper lease period
- On NYC-DC1, check that the lease period configured in the scope properties is correct.
Task 9: Verify the information being leased to the client
- On NYC-CL1, use `ipconfig` to ensure that the client is configured as it was before running the `DHCP.VBS` script.

Task 10: Close all virtual machines and discard undo disks
1. On the host computer, click `Start`, point to `All Programs`, point to `Microsoft Virtual Server`, and then click `Virtual Server Administration Website`.
2. Under `Navigation`, click `Master Status`. For each virtual machine that is running, click the `virtual machine name`, and in the context menu, click `Turn off Virtual Machine and Discard Undo Disks`. Click `OK`. 


Module Review and Takeaways

- Review Questions
- Common Issues and Troubleshooting Tips
- Best Practices
- Tools

Review Questions
1. What is the main benefit of using DHCP?
2. With what new security feature does DHCP integrate to force client computers to be compliant with company security policies?
3. What are the four DHCP message broadcasts that are used when a successful address lease occurs?
4. At what point in a DHCP lease does the client usually renew the lease automatically?
5. Why would you use a superscope?
6. What are the three data sources for monitoring DHCP?
Common Issues and Troubleshooting Tips

DHCP authorization:
Windows-based DHCP servers will not lease IP addresses unless they are authorized. Make sure that when you authorize the DHCP service, you also activate the scope. It also is important to remember that stand-alone DHCP servers will take themselves offline if they detect another authorized DHCP server in the network.

DHCP and multiple subnets:
When using DHCP to provide addresses for multiple subnets, make sure that the server has an interface in the network in which the scope is defined. For example, if the scope is defined within the range of 10.10.0.50 to 10.10.0.100, the DHCP server should have an IP address in the subnet where the scope is defined. An alternative to having a DHCP server with multiple network interfaces is to configure a DHCP relay agent.

APIPA addresses:
Automatic Private IP Addressing (APIPA) is an address that a computer assigns itself when it is configured to use DHCP, but it cannot obtain an address lease. An APIPA address will start with 169.254. in the first two octets of the IP address. (This is a reserved IP space specified in RFC). For example, an APIPA address may be assigned if the media connecting the client is not working or when the DHCP server cannot be contacted. If a single client is experiencing issues, then the issue typically is client-related. However, if multiple clients are assigning themselves with APIPA addresses, the problem more likely is related to the DHCP server or the network configuration that the DHCP server is using.

Best Practices
• Use the 80/20 design rule for balancing scope distribution of addresses where multiple DHCP servers are deployed to service the same scope.

Using more than one DHCP server on the same subnet provides increased fault tolerance for servicing DHCP clients located on it. When you use two DHCP servers, if one server is unavailable, then the other server can take its place and continue to lease new addresses or renew existing clients.

A common practice when balancing a single network and scope range of addresses between two DHCP servers is to have 80 percent of the addresses distributed by one DHCP server and the remaining 20 percent provided by a second DHCP server.
• Use superscopes for multiple DHCP servers on each subnet in a LAN environment.

When started, each DHCP client broadcasts a DHCP discover message (DHCPDISCOVER) to its local subnet to attempt to find a DHCP server. Because DHCP clients use broadcasts during their initial startup, you cannot predict which server will respond to a client’s DHCP discover request if more than one DHCP server is active on the same subnet.

Use a new superscope that is configured similarly at all servers. The superscope should include all valid scopes for the subnet as member scopes. For configuring member scopes at each server, addresses must only be made available at one of the DHCP servers used on the subnet. For all other servers in the subnet, use exclusion ranges for the same scope ranges of addresses when configuring the corresponding scopes.

• Deactivate scopes only when removing a scope permanently from service. If the intent is only to affect temporary deactivation of scope addresses, editing or modifying exclusion ranges in an active scope achieves the intended results.

• Use server-side conflict detection on DHCP servers only when necessary.

Either DHCP servers or clients can use conflict detection to determine whether an IP address is in use already on the network before leasing or using the address.

Windows 2000, Windows XP, and Windows Vista detect IP conflicts using an APR request. By default, the DHCP service does not perform any conflict detection. To enable conflict detection, increase the number of ping attempts that the DHCP service performs for each address before leasing that address to a client.

Note that for each additional conflict-detection attempt that the DHCP service performs, additional seconds are added to the time needed to negotiate leases for DHCP clients.

Typically, if you use DHCP server-side conflict detection, you should set the number of conflict detection attempts that the server makes to use one or two pings at most. This provides the intended benefits of this feature without decreasing DHCP server performance.
You should create reservations on all DHCP servers that can potentially service the reserved client.

You can use a client reservation to ensure that a DHCP client computer always receives the same IP address lease at startup. If you have more than one DHCP server reachable by a reserved client, add the reservation at each of your other DHCP servers.

This allows the other DHCP servers to honor the client IP address reservation made for the reserved client. The client reservation is acted upon only by the DHCP server where the reserved address is part of the available address pool, but you can create the same reservation on other DHCP servers that exclude this address.

For server performance, note that DHCP is disk-intensive and purchase hardware with optimal disk performance characteristics.

The client reservation is acted upon only by the DHCP server where the reserved address is part of the available address pool, but you can create the same reservation on other DHCP servers that exclude this address.

When evaluating performance of your DHCP servers, you should evaluate DHCP as part of making a full performance evaluation of the entire server. By monitoring system hardware performance in the most demanding areas of utilization (CPU, memory, disk input/output), you obtain the best assessment of when a DHCP server is overloaded or in need of an upgrade.

Note that the DHCP service includes several System Monitor counters that you can use to monitor service.

Keep audit logging enabled for use in troubleshooting.

By default, the DHCP service enables audit logging of service-related events. Audit logging provides a long-term, service-monitoring tool that makes limited and safe use of server disk resources.

Reduce lease times for DHCP clients that use Routing and Remote Access service for remote access.
• Increase the duration of scope leases for large, stable, fixed networks if available address space is sufficient.

• Use the appropriate number of DHCP servers for the number of DHCP-enabled clients on your network.

In a small LAN (for example, one physical subnet not using routers), a single DHCP server can serve all DHCP-enabled clients. For routed networks, the number of servers needed increases, depending on several factors, including the number of DHCP-enabled clients, the transmission speed between network segments, speed of network links, whether you use DHCP service throughout your enterprise network or only on selected physical networks, and the network’s IP address class.

Tools

**DHCP console**

The primary method for managing DHCP is by using the DHCP console. The console is located in *Administrative Tools*. You also can use the console to manage server core instances of the DHCP Server role remotely.

**Command-line tools**

The following table describes the command-line tools that you can use to configure and manage DHCP:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netsh</td>
<td>Use the Netsh command to configure DHCP using the command line.</td>
</tr>
<tr>
<td>Ipconfig</td>
<td>Use this command to request and interact with the DHCP server from the client side.</td>
</tr>
<tr>
<td>DHCPLoc.exe</td>
<td>This tool is part of the Microsoft Resource Kit, and you can use it to locate active DHCP servers in the subnet.</td>
</tr>
</tbody>
</table>
Module 5

Configuring and Troubleshooting IPv6 TCP/IP

Contents:
Lesson 1: Overview of IPv6 5-3
Lesson 2: Coexistence with IPv6 5-17
Lesson 3: IPv6 Tunneling Technologies 5-25
Lab A: Configuring an ISATAP Router 5-32
Lesson 3: IPv6 Tunneling Technologies (continued) 5-39
Lesson 4: Transitioning from IPv4 to IPv6 5-44
Lesson 5: Troubleshooting IPv6 5-47
Lab B: Converting the Network 5-52
Module Overview

- Overview of IPv6
- Coexistence with IPv6
- IPv6 Tunneling Technologies
- Transitioning from IPv4 to IPv6
- Troubleshooting IPv6

Support for Internet Protocol version 6 (IPv6), a new suite of standard protocols for the Internet’s Network layer, is built into Windows Server 2008. IPv6 is a critical technology that will help ensure that the Internet can support a growing user base and the increasingly large number of IP-enabled devices. The current Internet Protocol Version 4 (IPv4) has served as the underlying Internet protocol for almost 30 years. Its robustness, scalability, and limited feature set now is challenged by the growing need for new IP addresses, due in large part to the rapid growth of new network-aware devices.
Lesson 1
Overview of IPv6

- Benefits of IPv6
- Differences between IPv4 and IPv6
- IPv6 Implementations Using Microsoft Technologies
- The IPv6 Address Space
- IPv6 Prefixes
- Unicast IPv6 Address Types
- IPv6 Addresses Assigned to Hosts and Routers
- Zone IDs
- Address Autoconfiguration for IPv6
- Demonstration: Configuring IPv6 Client Settings

IPv6 slowly is becoming more common. While adoption may be slow, it is important to understand how this technology will affect current networks and how to integrate IPv6 into those networks. The following lesson will cover the benefits of IPv6, how it compares to IPv4, and its basic types of IPv6 addresses. After completing this lesson, you should understand global, link-local, site-local, and unique-local addresses.
Benefits of IPv6

Benefits of IPv6 include:

- Large address space
- Hierarchical addressing and routing infrastructure
- Stateless and Stateful address configuration
- Built-in security
- Enhanced support for prioritized delivery
- New protocol for neighboring node interaction
- Extensibility

Key Points
The IPv6 protocol provides the following benefits:

- Large address space
- Hierarchical addressing and routing infrastructure
- Stateless and Stateful address configuration
- Built-in security
- Prioritized delivery
- Neighbor detection
- Extensibility

Additional Reading

- IPv6
### Differences Between IPv4 and IPv6

<table>
<thead>
<tr>
<th>Source and destination addresses</th>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>32 bits (4 bytes) in length</td>
<td>128 bits (16 bytes) in length</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IPSec support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optional</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Address Resolution Protocol</th>
<th>Broadcast ARP Request frames resolve IPv4 address to link layer address</th>
<th>ARP Request frames replaced with multicast Neighbor Solicitation messages</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Internet Group Management Protocol</th>
<th>Manages local subnet group membership</th>
<th>IGMP replaced with MLD messages</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>ICMP Router Discovery</th>
<th>Determines IPv4 address of default gateway</th>
<th>Replaced with ICMPv6 Router Solicitation and Router Advertisement messages</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Broadcast addresses</th>
<th>Sends traffic to all nodes on a subnet</th>
<th>Uses a link-local scope all-nodes multicast address instead of an IPv6 broadcast address</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Configured manually or through DHCP</th>
<th>Does not require manual configuration or DHCP</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Resource records</th>
<th>Uses A resource records in DNS to map host names to IPv4 addresses</th>
<th>Uses AAAA resource records in DNS to map host names to IPv6 addresses</th>
</tr>
</thead>
</table>

### Key Points

The following table highlights the differences between IPv4 and IPv6:

<table>
<thead>
<tr>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source and destination addresses are 32 bits (4 bytes) in length.</td>
<td>Source and destination addresses are 128 bits (16 bytes) in length.</td>
</tr>
<tr>
<td>IPSec support is optional.</td>
<td>IPSec support is required.</td>
</tr>
<tr>
<td>No identification of packet flow for Quality of Service (QoS) handling by routers is present within the IPv4 header.</td>
<td>Packet-flow identification for QoS handling by routers is included in the IPv6 header using the Flow Label field.</td>
</tr>
<tr>
<td>Fragmentation is done by both routers and the sending host.</td>
<td>Fragmentation is not done by routers, only by the sending host.</td>
</tr>
<tr>
<td>Header includes a checksum.</td>
<td>Header does not include a checksum.</td>
</tr>
<tr>
<td><strong>IPv4</strong></td>
<td><strong>IPv6</strong></td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>Header includes options.</td>
<td>All optional data is moved to IPv6 extension headers.</td>
</tr>
<tr>
<td>Address Resolution Protocol (ARP) uses broadcast ARP Request frames to resolve an IPv4 address to a link layer address.</td>
<td>ARP Request frames are replaced with multicast Neighbor Solicitation messages.</td>
</tr>
<tr>
<td>Internet Group Management Protocol (IGMP) is used to manage local subnet group membership.</td>
<td>IGMP is replaced with Multicast Listener Discovery (MLD) messages.</td>
</tr>
<tr>
<td>Internet Control Message Protocol (ICMP) Router Discovery, which is optional, is used to determine the IPv4 address of the best default gateway.</td>
<td>ICMP Router Discovery, which is required, is replaced with ICMPv6 Router Solicitation and Router Advertisement messages.</td>
</tr>
<tr>
<td>Broadcast addresses are used to send traffic to all nodes on a subnet.</td>
<td>There are no IPv6 broadcast addresses. Instead, a link-local scope all-nodes multicast address is used.</td>
</tr>
<tr>
<td>Must be configured either manually or through DHCP.</td>
<td>Does not require manual configuration or DHCP.</td>
</tr>
<tr>
<td>Uses host address (A) resource records in the Domain Name System (DNS) to map host names to IPv4 addresses.</td>
<td>Uses host address (AAAA) resource records in the Domain Name System (DNS) to map host names to IPv6 addresses.</td>
</tr>
<tr>
<td>Uses pointer (PTR) resource records in the IN-ADDR.ARPA DNS domain to map IPv4 addresses to host names.</td>
<td>Uses pointer (PTR) resource records in the IP6.ARPA DNS domain to map IPv6 addresses to host names.</td>
</tr>
<tr>
<td>Must support a 576-byte packet size (possibly fragmented).</td>
<td>Must support a 1280-byte packet size (without fragmentation).</td>
</tr>
</tbody>
</table>
IPv6 Implementations Using Microsoft Technologies

- Windows Server 2003 family
- The IPv6 protocol for Windows XP SP1 and Windows XP SP2
- The IPv6 protocol for Windows CE .NET versions 4.1 and later
- The Next Generation TCP/IP stack in Windows Vista and Windows Server 2008

Key Points
For all of the IPv6 implementations from Microsoft, you can use IPv6 without affecting IPv4 communications. Note that IPv6 is a dual stack implementation in Windows XP SP2 and Windows Server 2003, and a dual layer implementation for Windows Vista and Windows Server 2008.
The IPv6 Address Space

Key Points
The most obvious distinguishing feature of IPv6 is its use of much larger addresses. IPv4 IP addresses are expressed in four groups of decimal numbers, such as 192.168.1.1. Each grouping of numbers represents a binary octet. In binary, the preceding number is:

```
11000000.10101000.00000001.00000001 (4 octets = 32 Bits)
```

The size of an address in IPv6 is 128 bits, which is four times the larger than an IPv4 address. IPv6 addresses also are expressed as hexadecimal addresses in their “readable” format. For example, 2001:DB8:0:2F3B:2AA:FF:FE28:9C5A.

This may seem counterintuitive for end users, however the assumption is that average users will rely on DNS names to resolve hosts and will rarely manually type IPv6 addresses. The IPv6 address in hex also is easier to convert to binary and vice versa. This simplifies working with subnets, and calculating hosts and networks.
Additional Reading

- Introduction to IP Version 6
IPv6 Prefixes

<table>
<thead>
<tr>
<th>Allocation</th>
<th>Format prefix</th>
<th>Format prefix</th>
<th>Fraction of the address space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reserved</td>
<td>0000 0000</td>
<td>-</td>
<td>1/256</td>
</tr>
<tr>
<td>Reserved for NSAP allocation</td>
<td>0000 001</td>
<td>-</td>
<td>1/128</td>
</tr>
<tr>
<td>Aggregatable global unicast addresses</td>
<td>001</td>
<td>2 or 3</td>
<td>1/8</td>
</tr>
<tr>
<td>Link-local unicast addresses</td>
<td>1111 1110 10</td>
<td>FE8</td>
<td>1/1024</td>
</tr>
<tr>
<td>Site-local unicast addresses</td>
<td>1111 1110 11</td>
<td>FEC0</td>
<td>1/1024</td>
</tr>
<tr>
<td>Multicast addresses</td>
<td>1111 1111</td>
<td>FF</td>
<td>1/256</td>
</tr>
</tbody>
</table>

Key Points
Like the IPv4 address space, the IPv6 address space is divided by allocating portions of the available address space for various IP functions. The high-order bits (bits that are at the beginning of the 128-bit IPv6 address) are used to define areas statically in the IP space. The high-order bits and their fixed values are known as a format prefix.
Unicast IPv6 Address Types

Key Points
A unicast address identifies a single interface within the scope of the unicast address type. With the appropriate unicast routing topology, packets addressed to a unicast address are delivered to a single interface.

Unicast IPv6 address types include:

- Global unicast addresses
- Link-local addresses
- Site-local addresses
- Unique local IPv6 unicast addresses
- Special addresses
IPv6 Addresses Assigned to Hosts and Routers

**Key Points**
An IPv6 host, including those with only one interface, typically has multiple IPv6 addresses. By default, link-local addresses are configured automatically for each interface on each IPv6 host or router. To communicate with non-neighboring nodes, a host also must be configured with unicast site-local or global addresses. A host obtains these additional addresses either from router advertisements or by manual assignment. Use commands in the `netsh interface ipv6` context to configure IPv6 addresses manually.

In IPv6, hosts and routers are typically assigned the following addresses:
- **Unicast addresses**
- **Multicast addresses** (to listen for multicast traffic)

Additionally, IPv6 routers also have the following addresses:
- **Multicast addresses**
- **Anycast addresses**
Zone IDs

Unlike global addresses, you can reuse local-use addresses. Link-local addresses are reused on each link. Site-local addresses can be reused within each site of an organization. Link-local and site-local addresses are ambiguous because of this address-reuse capability.

You need an additional identifier to specify which link on which an address is assigned, located, or within which site an address is assigned or located. This additional identifier is a zone identifier (ID), also known as a scope ID, which identifies a connected portion of a network that has a specified scope. The syntax specified in RFC 4007 for identifying the zone associated with a local-use address is as follows:

Address@zone_ID
Address Autoconfiguration for IPv6

Key Points

The host can proceed through several states as it goes through the autoconfiguration process, and there are several ways to assign an IP address and information. Based on how the router is set up, a client may use stateless configuration (no DHCP service), or stateful with a DHCP server involved, to either assign an IP address and other network information, or just assign other network information. (Other information includes DNS servers and gateways.)

Autoconfigured addresses are in one or more of the following states:

- Tentative. The address is in the process of being verified as unique.
- Valid. The address has been verified as unique, and can send and receive unicast traffic.
- Preferred. The address enables a node to send and receive unicast traffic to and from it.
• Deprecated. The address is valid but its use is discouraged for new communication.

• Invalid. The address no longer allows a node to send or receive unicast traffic.

Types of autoconfiguration include:

• Stateless. Address configuration is based on the receipt of Router Advertisement messages with the Managed Address Configuration and Other Stateful Configuration flags set to 0 and one or more Prefix Information options.

• Stateful. Configuration is based on the use of a stateful address configuration protocol such as DHCPv6 to obtain addresses and other configuration options.

• Both. Configuration is based on receipt of Router Advertisement messages with Prefix Information options and the Managed Address Configuration or Other Stateful Configuration flags set to 1.

Additional Reading

• Introduction to IP Version 6
Demonstration: Configuring IPv6 Client Settings

In this demonstration, you will see how to configure IPv6 settings on a network client.
Lesson 2  
Coexistence with IPv6

- What are Node Types?  
- IPv4 and IPv6 Coexistence  
- What is a Dual Layer Architecture?  
- What is a Dual Stack Architecture?  
- How Does DNS Support IPv6?  
- Demonstration: Configuring DNS to Support IPv6  
- What Is IPv6 Over IPv4 Tunneling?

From its inception, IPv6 was designed based on the idea that it needs to have the ability to coexist, long term, with IPv4. This lesson provides an overview of the technologies that support the two IP protocols’ coexistence. After completing this lesson, you should understand, and be able to describe, different node types and IP stack implementations of IPv6, how DNS defines IPv6 addresses, and the various types of IPv6 tunneling technologies.
What are Node Types?

Key Points

When planning an IPv6 network, it is important to know what kind of nodes or hosts are on the network. By describing the nodes in the following ways, we can define their abilities on the network. This is important for tunneling because certain kinds of tunnels require specific node types, including:

- IPv4-only node. A node that implements only IPv4 (and has only IPv4 addresses) and does not support IPv6.
- IPv6-only node. A node that implements only IPv6 (and has only IPv6 addresses) and does not support IPv4.
- IPv4 node. A node that implements IPv4. It can be an IPv4-only node or an IPv6/IPv4 node.
- IPv6 node. A node that implements IPv6. It can be an IPv6-only node or an IPv6/IPv4 node.
IPv4 and IPv6 Coexistence

<table>
<thead>
<tr>
<th>Methods for providing coexistence of IPv4 and IPv6:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Dual IP layer architecture (Windows Vista and Windows Server 2008)</td>
</tr>
<tr>
<td>• Dual stack architecture (Windows Server 2003 and Windows XP)</td>
</tr>
<tr>
<td>• DNS Infrastructure requirements</td>
</tr>
<tr>
<td>• IPv6 over IPv4 tunneling</td>
</tr>
</tbody>
</table>

**Key Points**

To coexist with an IPv4 infrastructure and provide an eventual transition to an IPv6-only infrastructure, you can use the following mechanisms:

- Dual IP layer architecture (Windows Vista and Windows Server 2008).
- Dual stack architecture (Windows Server 2003 and Windows XP).
- DNS infrastructure requirements.
- IPv6 over IPv4 tunneling.

**Additional Reading**

- IPv6 Transition Technologies
What is a Dual Layer Architecture?

Key Points
A dual IP layer architecture contains both IPv4 and IPv6 Internet layers with a single implementation of transport layer protocols such as TCP and UDP. Dual stack allows for easier migration to IPv6. There are fewer files to maintain to provide IPv6 connectivity. IPv6 is also available without adding any new protocols in the network-card configuration.

Types of packets include:
- IPv4 packets
- IPv6 packets
- IPv6 over IPv4 packets (IPv6 packets encapsulated with an IPv4 header)
What is a Dual Stack Architecture?

Key Points
Dual stack architecture contains both IPv4 and IPv6 Internet layers with separate protocol stacks containing separate implementations of transport layer protocols, such as TCP and UDP.


Types of packets include:
- IPv4 packets
- IPv6 packets
- IPv6 over IPv4 packets
How Does DNS Support IPv6?

DNS support for IPv6:

- DNS Host records are classified as AAAA records
- Pointer Records are configured in the IP6.ARPA zone
- DNS tries to return the appropriate address (either IP 4 or IP 6 depending on the Address Selection rules)

Key Points
You need a DNS infrastructure for successful coexistence because of the prevalent use of names rather than addresses to refer to network resources. Upgrading the DNS infrastructure consists of populating the DNS servers with records to support IPv6 name-to-address and address-to-name resolutions. After you obtain the addresses using a DNS name query, the sending node must select which addresses to use for communication.
Demonstration: Configuring DNS to Support IPv6

*In this demonstration, you will see how to:*

- Configure an AAAA record
- Create an IPv6 PTR record (IP6.ARPA)
What Is IPv6 Over IPv4 Tunneling?

IPv6 over IPv4 tunneling is the encapsulation of IPv6 packets with an IPv4 header so that IPv6 packets can be sent over an IPv4 infrastructure. Within the IPv4 header:

- The **IPv4 Protocol** field is set to **41** to indicate an encapsulated IPv6 packet.
- The **Source** and **Destination** fields are set to IPv4 addresses of the tunnel endpoints. You can configure tunnel endpoints manually as part of the tunnel interface or they are derived automatically from the next-hop address of the matching route for the destination and the tunneling interface.

**Key Points**

**Note:** Unlike tunneling for the Point-to-Point Tunneling Protocol (PPTP) and Layer Two Tunneling Protocol (L2TP), there is no exchange of messages for tunnel setup, maintenance, or termination. Additionally, IPv6 over IPv4 tunneling does not provide security for tunneled IPv6 packets. This means that when you use IPv6 Tunneling, it does not need to establish a connection first. Also, the tunneling infers that it is only tunneling through IPv4 networks, and does not encrypt the tunnel.
Lesson 3
IPv6 Tunneling Technologies

- Tunneling Configurations
- Types of Tunnels
- Tunneling Technologies Usage
- What is ISATAP Tunneling?
- What is 6to4 Tunneling?
- What is Teredo Tunneling?
- What is Port Proxy?

An eventual successful transition to IPv6 requires interim coexistence of IPv6 nodes in today’s predominantly IPv4 environment. To support this, IPv6 packets are tunneled automatically over IPv4 routing infrastructures, enabling IPv6 clients to communicate with each other by using 6to4 or Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) addresses and tunneling IPv6 packets across IPv4 networks. This lesson provides information about the different tunneling technologies available in IPv6.
Tunneling Configurations

RFC 2893 defines the following tunneling configurations with which to tunnel IPv6 traffic between IPv6/IPv4 nodes over an IPv4 infrastructure:

- Router-to-Router
- Host-to-Router or Router-to-Host
- Host-to-Host
Types of Tunnels

<table>
<thead>
<tr>
<th>Tunnel</th>
<th>Key Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configured</td>
<td>Requires manual configuration of tunnel endpoints</td>
</tr>
<tr>
<td>Automatic</td>
<td>Tunnel endpoints are determined automatically by the use of logical tunnel interfaces, routes, and destination IPv6 addresses</td>
</tr>
</tbody>
</table>

Key Points

RFC 2893, “Transition Mechanisms for IPv6 Hosts and Routers,” defines the following types of tunnels:

- Configured
- Automatic

Additional Reading

- RFC 2893: Transition Mechanisms for IPv6 Hosts and Routers
Tunneling Technologies Usage

- Exercise 1: Configuring a New IPv6 Network and Client
- Exercise 2: Configuring an ISATAP Router to Enable Communications Between an IPv4 Network and an IPv6 Network

Logon information

<table>
<thead>
<tr>
<th>Virtual machine</th>
<th>6421A-NYC-DC1, 6421A-NYC-SVR1, and 6421A-NYC-CL1</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Administrator</td>
</tr>
<tr>
<td>Password</td>
<td>Pa$$w0rd</td>
</tr>
</tbody>
</table>

Estimated time: 30 minutes

Key Points
The tunneling technologies used for IPv6 over IPv4 tunneling include:
- ISATAP
- 6to4
- Teredo
PortProxy
To facilitate the communication between nodes or applications that cannot connect using a common Internet layer protocol (IPv4 or IPv6), the IPv6 protocol for Windows Server 2008 provides PortProxy, a component that allows proxying of the following traffic:

- IPv4 to IPv4
- IPv4 to IPv6
- IPv6 to IPv6
- IPv6 to IPv4

Additional Reading
- IPv6 Transition Technologies
What is ISATAP Tunneling?

- **Address assignment and automatic tunneling technology for unicast IPv6 traffic between IPv6/IPv4 nodes across an IPv4 intranet**

- **ISATAP addresses:**
  - [64-bit unicast prefix]:0:5EFE:w.x.y.z
  - w.x.y.z is a public or private IPv4 address
  - Example: FE80::5EFE:157.59.137.133

- **ISATAP treats an IPv4 infrastructure as a single link**

**Key Points**

ISATAP is an address-assignment and host-to-host, host-to-router, and router-to-host automatic tunneling technology that you can use to provide unicast IPv6 connectivity between IPv6/IPv4 hosts across an IPv4 intranet. ISATAP hosts do not require any manual configuration and can create ISATAP addresses using standard address autoconfiguration mechanisms.

**What is an ISATAP Router?**

ISATAP allows IPv6 clients in an IPv4 subnet to communicate without additional manual configuration. An ISATAP router allows the clients to communicate with other IPv6 clients in pure IPv6 or mixed subnets.
How ISATAP Tunneling Works
ISATAP tunneling can be initiated in several ways. The ISATAP router can be resolved by resolving the name “ISATAP” to an IPv4 Address or by using the **Netsh Interface IPv6 ISATAP set Router** command.

Additional Reading
- RFC 4214: Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
Lab A: Configuring an ISATAP Router

Objectives
- Configure a new IPv6 network and client
- Configure an ISATAP router to enable communications between an IPv4 network and an IPv6 network

Before you begin:
To be able to simulate multiple networks, you must configure the following before starting the virtual machines:

1. On the host machine, open the Virtual Server Administration Web site.
2. In the left pane, under Virtual Networks, click Add, click 6421A-NYC-VN1_IPv4.vnc, and then click Add again.
3. In the left pane, under Virtual Networks, click Add, click 6421A-NYC-VN2_IPv6.vnc, and then click Add again.
4. In the left pane, under Virtual Machines, point to Configure, and then click 6421A-NYC-SVR1.


6. Under Virtual network adapter 2, click the drop-down arrow, select 6421A-NYC-VN2_IPv6, and then click OK.

7. In the left pane, under Virtual Machines, point to Configure, and then click 6421A-NYC-CL1.


9. Under Virtual network adapter 1, click the drop-down arrow, select 6421A-NYC-VN2_IPv6, and then click OK.

Lab Setup

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must:

1. Start the 6421A-NYC-DC1, 6421A-NYC-SVR1, and 6421A-NYC-CL1 virtual machines.

2. Log on to the 6421A-NYC-DC1, 6421A-NYC-SVR1, and 6421A-NYC-CL1 virtual machines with the user name administrator and the password Pa$$w0rd.
Exercise 1: Configuring a New IPv6 Network and Client

Scenario
You must design and implement an IPv6 network. For your initial proof of concept, you must deploy only one client.

Exercise Overview
In this exercise, you will prepare the current environment to work with IPv6, and deploy an IPv6 client and IPv6 subnet.

The main tasks are as follows:
1. Start the 6421A-NYC-DC1, 6421A-NYC-SVR1, and 6421A-NYC-CL1 virtual machines.
2. Disable IPv4 on NYC-CL1.
3. Check the IP configuration on NYC-CL1. Make sure that it is not configured with an IPv4 IP address.
4. Disable IPv4 on NYC-SVR1 Interface 2.
5. Configure an IPv6 router advertisement for the global address 2001:db8:0:1::/64 network on NYC-SVR1.
6. Configure an IPv6 router advertisement for the site-local fec0:db8:0:1::/64 network on NYC-SVR1.
7. Check the IP configuration on NYC-CL1. Make sure it is configured with an IPv6 Global address and an IPv6 site-local address. Also, ensure that the IPv6 client can ping the IPv6 interface on NYC-SVR1.
8. Check the IP configuration on NYC-CL1. Make sure it is configured with an IPv6 site-local address, and make sure NYC-CL1 can communicate with NYC-SVR1.
Task 1: Start the 6421A-NYC-DC1, 6421A-NYC-SVR1, and 6421A-NYC-CL1 virtual machines
1. Start the 6421A-NYC-DC1, 6421A-NYC-SVR1, and 6421A-NYC-CL1 virtual machines.
2. Log on to the virtual machines with the user name administrator and the password Pa$$w0rd.

Task 2: Disable IPv4 on NYC-CL1
• On NYC-CL1 in the Manage Network Connections control panel, disable IPv4 connectivity.

Task 3: Check the IP configuration on NYC-CL1 and ensure that it is not configured with an IPv4 IP address
• Validate that the IP address on NYC-CL1 is a valid link-local IP address.

Task 4: Disable IPv4 on NYC-SVR1 for the Local Area Connection 2 network
• On NYC-SVR1, in the Manage Network Connections control panel, set Local Area Connection 2 to work only with IPv6.

Task 5: Configure an IPv6 router advertisement for the global address 2001:db8:0:1::/64 network on NYC-SVR1
1. On NYC-SVR1, using the command line and the netsh command, configure Local Area Connection 2 to forward packets and to advertise subnet prefixes.
2. Add a subnet prefix to Local Area connection 2 of: 2001:db8:0:1::/64. Make sure to publish this prefix.
Task 6: Check the IP configuration on NYC-CL1. Make sure that it is configured with an IPv6 global address in the 2001:db8:0:1::/64 network
- Validate that NYC-CL1 has configured itself using the global prefix assigned to the network.

Task 7: Configure an IPv6 router advertisement for the link-local fec0:db8:0:1::/64 network on NYC-SVR1
1. On NYC-SVR1, using the command line and the `netsh` command, configure Local Area Connection 2 to forward packets and to advertise subnet prefixes.
2. Add a subnet prefix to Local Area connection 2 of: fec0:db8:0:1::/64. Make sure to publish this prefix.

Task 8: Check the IP configuration on NYC-CL1 and ensure that it is configured with an IPv6 link-local address in the 2001:db8:0:1::/64 network
- Validate that NYC-CL1 has configured itself using the global prefix and the site-local prefix assigned to the network.
Exercise 2: Configuring an ISATAP Router to Enable Communications Between an IPv4 Network and an IPv6 Network

Scenario
Now that you have configured your IPv6 client, you must enable IPv4 client connectivity to the IPv6 network. Your evaluation of current IPv6 tunneling technologies has led you to choose to implement an ISATAP router.

Exercise Overview
In this exercise, you will enable and configure an ISATAP router interface that will allow two-way communications between the IPv4 and IPv6 networks.

The main tasks are as follows:
1. Add the ISATAP entry in the DNS zone.
2. Configure the ISATAP router on NYC-SVR.
3. Test connectivity with the IPv6 client.

▶ Task 1: Add the ISATAP entry into the woodgrovebank.com DNS zone on NYC-DC1
  • On NYC-SVR1, in the Woodgrovebank.com zone, create a new host record called ISATAP and configure it with the IPv4 address of NYC-SVR1 (10.10.0.24).

▶ Task 2: Configure the ISATAP router on NYC-SVR1
  1. On NYC-SVR1, identify the interface index (IDX) if the ISATAP local area connection (use the IPconfig and Netsh interface IPv6 show interface commands).
  2. Using the netsh command, enable forwarding and prefix advertise for the ISATAP interface.
  3. Using the netsh command, publish a new subnet prefix for the ISATAP subnet using 2001:db8:0:2::/64.
Task 3: Test connectivity with the IPv6 client

- Verify that you can ping NYC-DC1 from NYC-CL1, and that you can ping NYC-SVR1. Finally, verify that you can ping NYC-CL1 from NYC-DC1.

**Note:** If the IP addresses do not resolve, reboot the servers, starting with NYC-DC1, NYC-SVR1, and then NYC-CL1.

**Important:** Do not turn off the virtual machines at this time because you need them to complete the next lab.
What is 6to4 Tunneling?

**Key Points**

6to4 is an address-assignment and router-to-router, host-to-router, and router-to-host automatic tunneling technology that you can use to provide unicast IPv6 connectivity between IPv6 sites and hosts across the IPv4 Internet. 6to4 treats the entire IPv4 Internet as a single link.

**6to4 router functionality**

A 6to4 router:

- Enables IPv6 forwarding on both the 6to4 tunneling and private interfaces.
- Determines a 64-bit IPv6 subnet prefix to advertise on the private intranet.
- Sends router advertisement messages on the private interface.
**How 6to4 tunneling works**

Within a site, local IPv6 routers advertise 2002:WWXX:YYZZ:Subnet_ID::/64 subnet prefixes so that hosts autoconfigure 6to4 addresses. IPv6 routers within the site deliver traffic between 6to4 hosts. Hosts on individual subnets are configured automatically with a 64-bit subnet route for direct delivery to neighbors and a default route with the next-hop address of the advertising router. IPv6 traffic that does not match any of the subnet prefixes that the site uses is forwarded to a 6to4 router on the site border. The 6to4 router on the site border has a 2002::/16 route that forwards traffic to other 6to4 sites and a default route (::/0) that forwards traffic to a 6to4 relay.

**Additional Reading**

- RFC 3056: Connection of IPv6 Domains via IPv4 Clouds
What is Teredo Tunneling?

Key Points
Teredo tunneling enables you to tunnel across the IPv4 network when the clients are behind an IPv4 NAT. Teredo was created because many IPv4 routers use NAT to define a private address space for corporate networks.

Teredo components
The components of Teredo are:

- Teredo client
- Teredo server
- Teredo relay
- Teredo host-specific relay
How Teredo works

For two Windows-based Teredo clients, the most crucial Teredo processes are those that you use for initial configuration and communication with a different site’s peer.

• Initial Configuration
  • Teredo client:
    • Resolves the name teredo.ipv6.microsoft.com for Teredo servers
    • Sends multiple Teredo-encapsulated Router Solicitations to multiple Teredo servers
  • Based on responses, Teredo client determines:
    • Teredo server IPv4 address
    • Type of NAT
    • Externally mapped address and port for Teredo traffic

• Initial Communication Between Two Teredo Clients in Different Sites
  The set of packets sent during the initial communication between Teredo clients located in different sites depends on whether the Teredo clients are located behind cone NATs or restricted NATs.

Teredo: restricted NAT

The following process sends an initial communication packet from Teredo Client A to Teredo Client B:

1. Teredo Client A sends a bubble packet directly to Teredo Client B.
2. Teredo Client A sends a bubble packet to Teredo Client B through Teredo Server 2 (Teredo Client B’s Teredo server).
3. Teredo Server 2 forwards the bubble packet to Teredo Client B.
4. Teredo Client B responds to the bubble packet received from Teredo Client A with its own bubble packet, which is sent directly to Teredo Client A.
5. Upon the bubble packet’s receipt from Teredo Client B, Teredo Client A determines that source-specific NAT mappings exist for both NATs.
What is PortProxy?

PortProxy is a component that allows the proxying of the following traffic:

- **IPv4 to IPv4**: TCP traffic to an IPv4 address is proxied to TCP traffic to another IPv4 address
- **IPv4 to IPv6**: TCP traffic to an IPv4 address is proxied to TCP traffic to an IPv6 address
- **IPv6 to IPv6**: TCP traffic to an IPv6 address is proxied to TCP traffic to another IPv6 address
- **IPv6 to IPv4**: TCP traffic to an IPv6 address is proxied to TCP traffic to an IPv4 address

**Key Points**

You can use the PortProxy service as an application-layer gateway for nodes or applications that do not support IPv6. PortProxy facilitates the communication between nodes or applications that cannot connect using a common address type, Internet layer protocol (IPv4 or IPv6), and TCP port. This service’s primary purpose is to allow IPv6 nodes to communicate with IPv4 TCP applications.
Lesson 4

Transitioning from IPv4 to IPv6

The transition from IPv4 to IPv6 is expected to take many years. IPv4 remains the IP standard for the majority of applications and Internet services in use today. However, more and more networks and applications may function well in a purely IPv6 environment, as Windows Vista and Windows Server 2008 are adopted more widely. In this lesson, you will learn about the issues that you must consider when transitioning to IPv6 and review the necessary steps for transitioning to an IPv6-only installation.

- Discussion: Considerations for Migrating from IPv4 to IPv6
- Process For Transitioning to IPv6
Discussion: Considerations for Migrating from IPv4 to IPv6

- How might applications be affected?
- What kind of network infrastructure and network services need to be in place?
- What devices need to be upgraded?

Key Points
Answer the questions in a classroom discussion.
Process for Transitioning to IPv6

Key Points
The migration from IPv4 to IPv6 is expected to take considerable time. This was taken into consideration when designing IPv6 and as a result, the transition plan for IPv6 is a multistep process that allows for extended coexistence.

To achieve the goal of a pure IPv6 environment, use the following general guidelines.

- Upgrade your applications to be independent of IPv6 or IPv4.
- Update the DNS infrastructure to support IPv6 address and PTR records.
- Upgrade hosts to IPv6/IPv4 nodes.
- Upgrade routing infrastructure for native IPv6 routing.
- Convert IPv6/IPv4 nodes to IPv6-only nodes.
Lesson 5: Troubleshooting IPv6

- Methods Used to Troubleshoot IPv6
- Verifying IPv6 Connectivity
- Verifying DNS Name Resolution for IPv6 Addresses
- Verifying IPv6-based TCP Connections

This lesson describes the tools and techniques that you can use to identify a problem at successive layers of the TCP/IP protocol stack using an IPv6 Internet layer.
Methods Used to Troubleshoot IPv6

Key Points
To troubleshoot IPv6, depending on the problem, you can:

- Start at the bottom of the stack and move up.
- Start at the top of the stack and move down.

When starting at the top of the stack, the methods you can use to troubleshoot IPv6 include:

- Verify IPv6 connectivity.
- Verify DNS name resolution for IPv6 addresses.
- Verify IPv6-based TCP sessions.

Additional Reading
- TCP/IP Fundamentals for Microsoft Windows: Chapter 16 – Troubleshooting TCP/IP
Verifying IPv6 Connectivity

Key Points
You can use the following tasks to troubleshoot problems with IPv6 connectivity:

- Verify configuration
- Verify reachability
  - Check packet filtering
  - View and manage the IPv6 routing table
  - Verify router reliability
Verifying DNS Name Resolution for IPv6 Addresses

Key Points
When verifying network services connectivity, you use many of the same tools and software as with IPv4. When checking for DNS configuration and name resolution, you can verify the DNS configuration using the following tools:

- `Ipconfig/all`
- `Ipconfig/displaydns` and `Ipconfig/flushdns`
- `Ping`
- `Nslookup`
Verifying IPv6-based TCP Connections

Key Points
To verify IPv6-based TCP connections:
- Check for packet filtering.
- Verify TCP connection establishment (Telnet).
Lab B: Converting the Network

Exercise 1: Transitioning to an IPv6-Only Network

Logon information

<table>
<thead>
<tr>
<th>Virtual machine</th>
<th>6421A-NYC-DC1, 6421A-NYC-SVR1, and 6421A-NYC-CL1</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Administrator</td>
</tr>
<tr>
<td>Password</td>
<td>Pa$$w0rd</td>
</tr>
</tbody>
</table>

Estimated time: 30 minutes

Objective

- Transition the network into an IPv6-only network.

Lab Setup

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must:

1. Start the 6421A-NYC-DC1, 6421A-NYC-SVR1, and 6421A-NYC-CL1 virtual machines.
2. Log on to the NYC-DC1, NYC-SVR1, and NYC-CL1 virtual machines with the user name administrator and the password Pa$$w0rd.
Scenario
You are responsible for testing the IPv6 transition plan. To accomplish this, you will transition the computers from the previous network that uses both IPv4 and IPv6 and transition them to an IPv6-only network.
Exercise 1: Transitioning to an IPv6-Only Network

Exercise Overview
In this exercise, you will migrate the IPv4 network to be a fully capable IPv6 network.

The main tasks are as follows:
1. Disable the ISATAP router on NYC-SVR1.
2. Configure the native IPv6 router on NYC-SVR1.
3. Disable IPv4 connectivity.
4. Test connectivity between each IPv6 subnet.

► Task 1: Disable the ISATAP router on NYC-SVR1
- On NYC-SVR1, disable the ISATAP router and delete the static route subnet prefix that was defined previously for the ISATAP subnet.

► Task 2: Configure the native IPv6 router on NYC-SVR1
- Configure an IPv6 router in the Local Area Connection interface on NYC-SVR1. Make sure that forwarding and prefix advertising are enabled. Also add and publish the subnet prefix: 2001:db8:0:0::/64.

► Task 3: Disable IPv4 connectivity
- On NYC-SVR1 and NYC-DC1, disable all remaining IPv4 interfaces.

► Task 4: Test connectivity between each IPv6 subnet
- Make sure you can ping between NYC-DC1 and NYC-CL1. Also make sure that NYC-SVR1 is able to ping both servers.

Note: If the IP addresses do not resolve, reboot the servers starting with NYC-DC1, NYC-SVR1, and then NYC-CL1.
Task 5: Reconfigure the Network Adapters

To have the appropriate setup for future labs, you must configure the following before starting the virtual machines:

1. On the host machine, open the Virtual Server Administration Web site.
2. In the left pane, under Virtual Machines, point to Configure, and then click 6421A-NYC-SVR1.
4. Under Virtual network adapter 2, click the drop-down arrow, select Internal Network, and then click OK.
5. In the left pane, under Virtual Machines, point to Configure, and then click 6421A-NYC-CL1.
7. Under Virtual network adapter 1, click the drop-down arrow, select Internal Network, and then click OK.

Task 6: Close all virtual machines and discard undo disks

1. On the host computer, click Start, point to All Programs, point to Microsoft Virtual Server, and then click Virtual Server Administration Website.
2. Under Navigation, click Master Status. For each virtual machine that is running, click the virtual machine name, and in the context menu, click Turn off Virtual Machine and Discard Undo Disks. Click OK.
Module Review and Takeaways

• Review Questions
  • Command-Line Tools

Review Questions
1. What are the different types of unicast IPv6 addresses?
2. What are the main reasons why IPv6 is necessary?
3. What is the process called when a client configures itself with an IPv6 address?
4. What kind of IP address does every IPv6 client assign itself automatically?
5. How does the scope of an address affect its ability to communicate on the Internet?
6. What are the different tunneling technologies in IPv6?
7. What is the main purpose of a Teredo tunnel?
Command-Line Tools

The following table describes the command-line tools that you can use to configure and troubleshoot IPv6 TCP/IP:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPconfig</td>
<td>Provides overview data for IPv4 and IPv6.</td>
</tr>
<tr>
<td>Route</td>
<td>Provides basic information about IPv4 and IPv6 routing tables.</td>
</tr>
<tr>
<td>Netsh</td>
<td>Provides detailed information about the IPv6 configuration and is the primary tool used to configure IPv6 in Windows Server 2008 and Windows Vista. You also can use this command-line tool to configure an IPv6 router.</td>
</tr>
</tbody>
</table>
## Module 6

**Configuring and Troubleshooting Routing and Remote Access**

**Contents:**

<table>
<thead>
<tr>
<th>Lesson</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lesson 1: Configuring Network Access</td>
<td>6-3</td>
</tr>
<tr>
<td>Lesson 2: Configuring VPN Access</td>
<td>6-12</td>
</tr>
<tr>
<td>Lesson 3: Overview of Network Policies</td>
<td>6-22</td>
</tr>
<tr>
<td>Lesson 4: Overview of the Connection Manager Administration Kit</td>
<td>6-27</td>
</tr>
<tr>
<td>Lesson 5: Troubleshooting Routing and Remote Access</td>
<td>6-33</td>
</tr>
<tr>
<td>Lab: Configuring and Managing Network Access</td>
<td>6-41</td>
</tr>
</tbody>
</table>
Module Overview

- Configuring Network Access
- Configuring VPN Access
- Overview of Network Policies
- Overview of the Connection Manager Administration Kit
- Troubleshooting Routing and Remote Access

This module explains how to configure and troubleshoot Routing and Remote Access in Windows Server® 2008.
Windows Server 2008 includes Network Policy and Access Services, which offers scenario solutions for connectivity, such as:

- Network Access Protection (NAP). With NAP, system administrators can establish and automatically enforce health policies, which include software requirements, security update requirements, required computer configurations, and other settings.

- Secure wireless and wired solutions based on the 802.1X enforcement method.

- Remote access solutions, including virtual private network (VPN), traditional dial-up, and full-featured software routers.

- Central network policy management with Remote Authentication Dial-In User Service (RADIUS) server and proxy.
Components of a Network Access Services Infrastructure

Key Points
The underlying infrastructure in a complete Network Access Service in Windows Server 2008 typically includes the following components:

- VPN Server
- Active Directory® directory services
- Dynamic Host Configuration Protocol (DHCP) Server
- NAP Health Policy Server
- Health Registration Authority
- Remediation Servers

Additional Reading
- Help topic: Remote Access
What is the Network Policy and Access Services Role?

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Policy Server</td>
<td>The Microsoft implementation of Radius Server and proxy</td>
</tr>
<tr>
<td>Routing and Remote Access</td>
<td>Provides VPN and dial-up solutions for users, deploys full-featured software routers, and shares Internet connections across the intranet</td>
</tr>
<tr>
<td>Health Registration Authority</td>
<td>Issues health certificates to clients when using IPSec NAP enforcement</td>
</tr>
<tr>
<td>Host Credential Authorization Protocol</td>
<td>Integrates with Cisco network access control server</td>
</tr>
</tbody>
</table>

Key Points
The Network Policy and Access Services role in Windows Server 2008 provides the following network connectivity solutions:

- Network Access Protection (NAP)
- Secure wireless and wired access
- Remote access solutions
- Central network policy management with RADIUS server and proxy

Additional Reading
- Windows Server 2008 Technical Library
What is Routing and Remote Access?

- Used to provide remote users access to resources on a private network over Dial-up or VPN services
- Can be used to provide NAT services
- Can provide LAN and WAN routing services to connect network segments

Key Points
With Routing and Remote Access, you can deploy VPN and dial-up remote access services and multiprotocol LAN-to-LAN, LAN-to-wide area network (WAN), VPN, and network address translation (NAT) routing services.

You can deploy the following technologies during the installation of the Routing and Remote Access Service role:
- Remote Access Service
- Routing

Additional Reading
- Windows Server 2008 Technical Library
- Routing and Remote Access Service Help
Demonstration: How to Install Routing and Remote Access Services

In this demonstration, you will see how to install the Routing and Remote Access server role in Windows Server 2008.
Network Authentication and Authorization

Key Points
The distinction between authentication and authorization is important in understanding why connection attempts are accepted or denied:

- **Authentication** is the verification of the connection attempt’s credentials. This process consists of sending the credentials from the remote access client to the remote access server in either plaintext or encrypted form by using an authentication protocol.

- **Authorization** is the verification that the connection attempt is allowed. Authorization occurs after successful authentication.

Additional Reading
- Authentication vs. authorization
- Introduction to remote access policies
Types of Authentication Methods

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
<th>Security Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAP</td>
<td>Uses plaintext passwords. Typically used if the remote access client and remote access server cannot negotiate a more secure form of validation.</td>
<td>The least secure authentication protocol. Does not protect against replay attacks, remote client impersonation, or remote server impersonation.</td>
</tr>
<tr>
<td>CHAP</td>
<td>A challenge-response authentication protocol that uses the industry-standard MD5 hashing scheme to encrypt the response.</td>
<td>An improvement over PAP in that the password is not sent over the PPP link. Requires a plaintext version of the password to validate the challenge response. Does not protect against remote server impersonation.</td>
</tr>
<tr>
<td>MS-CHAPv2</td>
<td>An upgrade of MS-CHAP. Two-way authentication, also known as mutual authentication, is provided. The remote access client receives verification that the remote access server that it is dialing in to has access to the user’s password.</td>
<td>Provides stronger security than CHAP.</td>
</tr>
<tr>
<td>EAP</td>
<td>Allows for arbitrary authentication of a remote access connection through the use of authentication schemes, known as EAP types.</td>
<td>Offers the strongest security by providing the most flexibility in authentication variations.</td>
</tr>
</tbody>
</table>

Key Points
The authentication of access clients is an important security concern. Authentication methods typically use an authentication protocol that is negotiated during the connection establishment process. These protocols include:

- PAP
- CHAP
- MSCHAPv2
- EAP
- PEAP
Additional Reading

- Routing and Remote Access Service Help: Authentication
- Routing and Remote Access Service Help: Troubleshoot Remote Access
- Authentication Methods for use with IAS
Integrating DHCP Servers with the Routing and Remote Access Service

You can provide remote clients with IP configurations by using either:

- A static pool created on the Routing and Remote Access server for use with remote clients
- The corporate DHCP server located on the corporate LAN

DHCP servers running Windows Server 2008:

- Provide a predefined user class called the Default Routing and Remote Access Class
- Are useful for assigning options that are provided to Routing and Remote Access clients only

Key Points
You can deploy the DHCP Server service with the Routing and Remote Access service to provide remote access clients with a dynamically assigned IP address during connection. When you use these services together on the same server, the information provided during dynamic configuration is provided in a way that is different from typical DHCP configuration for LAN-based clients.

Additional Reading
Lesson 2

Configuring VPN Access

- What is a VPN Connection?
- Components of a VPN Connection
- Tunneling Protocols for a VPN Connection
- Configuration Requirements
- Demonstration: Configuring VPN Access
- Completing Additional Tasks
- Components of a Dial-up Connection

VPNs are point-to-point connections across a private or public network, such as the Internet. A VPN client uses special TCP/IP-based protocols, called tunneling protocols, to make a virtual call to a VPN server's virtual port.

In a typical VPN deployment, a client initiates a virtual point-to-point connection to a remote access server over the Internet. The remote access server answers the call, authenticates the caller, and transfers data between the VPN client and the organization’s private network.
What is a VPN Connection?

Key Points
To emulate a point-to-point link, data is encapsulated, or wrapped, with a header. The header provides routing information that enables the data to traverse the shared or public network to reach its endpoint. To emulate a private link, the data is encrypted for confidentiality. Packets that are intercepted on the shared or public network are indecipherable without encryption keys. The link in which the private data is encapsulated and encrypted is known as a VPN connection.

There are two types of VPN connections:
- Remote access VPN
- Site-to-site VPN
Components of a VPN Connection

Key Points
A VPN includes the following components:

- VPN client
- VPN server
- VPN tunnel
- Tunneled data
- Transit internetwork

Additional Reading
- Virtual Private Networks
Tunneling Protocols for a VPN Connection

<table>
<thead>
<tr>
<th>PPTP:</th>
<th>L2TP:</th>
<th>SSTP:</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP header</td>
<td>IP header</td>
<td>Encapsulates PPP frames in IP datagrams, and uses port 443 for tunnel management and PPP data frames</td>
</tr>
<tr>
<td>GRE header</td>
<td>L2TP header</td>
<td>Encryption is performed by the SSL channel of the HTTPS protocol</td>
</tr>
<tr>
<td>PPP trailer</td>
<td>PPP header</td>
<td></td>
</tr>
<tr>
<td>PPP payload (IPv4 packet)</td>
<td>PPP payload (IP diagram, IPX datagram, NetBEUI frame)</td>
<td></td>
</tr>
<tr>
<td>PPP frame</td>
<td>L2TP frame</td>
<td></td>
</tr>
<tr>
<td>encrypted</td>
<td>UDP message</td>
<td></td>
</tr>
</tbody>
</table>

**Key Points**

Tunneling enables the encapsulation of a packet from one type of protocol within a different protocol’s datagram. For example, VPN uses PPTP to encapsulate IP packets over a public network, such as the Internet. You also can configure a VPN solution based on PPTP, L2TP, or SSTP.

**Additional Reading**

- Routing and Remote Access Service Help: VPN Tunneling Protocols
Configuration Requirements

VPN server configuration requirements include:

- Two network interfaces (public and private)
- IP Address allocation (static pool or DHCP)
- Authentication provider (NPS/RADIUS or the VPN server)
- DHCP relay agent considerations
- Membership in the Local Administrators group or equivalent

Key Points
Before you configure a remote access VPN server, you must:

- Determine which network interface connects to the Internet and which network interface connects to your private network.
- Determine whether remote clients will receive IP addresses from a Dynamic Host Configuration Protocol (DHCP) server on your private network or from the remote access VPN server that you are configuring.
- Determine whether you want connection requests from VPN clients to be authenticated by a Remote Authentication Dial-In User Service (RADIUS) server or by the remote access VPN server that you are configuring.
- Determine whether VPN clients can send DHCP messages to the DHCP server on your private network.
- Verify that all users have user accounts that are configured for dial-up access.
**Additional Reading**

- Routing and Remote Access Service Help: Configure a Remote Access VPN Server
Demonstration: Configuring VPN Access

In this demonstration, you will see how to:

- Configure user dial-in settings
- Configure Routing and Remote Access as a VPN server
- Configure a VPN client
Completing Additional Tasks

Key Points
After you complete the steps in the Add Roles Wizard and complete the configuration in Routing and Remote Access, your server is ready for use as a remote access VPN server.

Additional tasks that you can perform on your remote access/VPN server include:

- Configure static packet filters
- Configure services and ports
- Adjust logging levels for routing protocols
- Configure the number of available VPN ports
- Create a Connection Manager profile for users
- Add Certificate Services
- Increase remote access security
- Increase VPN security
Additional Reading

- Network Policy and Access Services
- Routing and Remote Access Service Help: Configure a Remote Access VPN Server
Components of a Dial-Up Connection

Key Points
Dial-up remote access is a remote access technology that is available as part of the Routing and Remote Access service that Windows Server 2008 includes.

With dial-up remote access, a remote access client uses the telecommunications infrastructure to create a temporary physical circuit or a virtual circuit to a port on a remote access server. After the physical or virtual circuit is created, the rest of the connection parameters can be negotiated.

The physical or logical connection between the remote access server and the remote access client is facilitated by dial-up equipment installed at the remote access client, the remote access server, and the WAN infrastructure.

Additional Reading
- Routing and Remote Access Service Help: What is Dial-Up Networking?
Lesson 3
Overview of Network Policies

- What is a Network Policy?
- Process for Creating and Configuring a Network Policy
- How are Network Policies Processed?

When processing connection requests as a RADIUS server, Network Policy Server (NPS) performs both authentication and authorization for the connection request. NPS verifies the user’s or computer’s identity that is connecting to the network during the authentication process. NPS determines whether the user or computer is allowed to access the network during the authorization process.

To make this determination, NPS uses network policies that you configure in the NPS Microsoft Management Console (MMC) snap-in. To perform authorization, NPS also examines the dial-in properties of the user account in Active Directory.

Note: In Internet Authentication Service (IAS) in the Windows Server 2003 family of operating systems, network policies were called remote access policies.
What is a Network Policy?

A network policy consists of the following elements:

- Conditions
- Constraints
- Settings

Key Points

Network policies are sets of conditions, constraints, and settings that allow you to designate who is authorized to connect to the network and the circumstances under which they can, or cannot, connect. When you deploy Network Access Protection (NAP), health policy is added to the network policy configuration so that NPS performs client health checks during the authorization process.

Each network policy has four categories of properties:

- Overview
- Conditions
- Constraints
- Settings

Additional Reading

- Network Policy Server Help: Network Policy Properties
Process for Creating and Configuring a Network Policy

Key Points

NPS uses network policies, formerly named remote access policies, and the dial-in properties of user accounts, to determine whether to authorize a connection request to the network. You can configure a new network policy in either the NPS MMC snap-in or the Routing and Remote Access Service MMC snap-in.

To add a network policy using the Windows interface:

1. Open the NPS console and double-click Policies.
2. In the console tree, right-click Network Policies and then click New. The New Network Policy wizard opens.
3. Use the New Network Policy wizard to create a policy.
4. Configure the Network Policy properties.
Additional Reading

- Network Policy Server Help: Network Policies
- Network Policy Server Help: Add a Network Policy
How are Network Policies Processed?

Key Points
When NPS performs authorization of a connection request, it compares the request with each network policy in the ordered list of policies, starting with the first policy and moving down the list.

Additional Reading
- Network Policy Server Help: Add a Network Policy
Lesson 4
Overview of the Connection Manager Administration Kit

- What is the Connection Manager Administration Kit?
- Demonstration: Installing CMAK
- Process for Configuring a Connection Profile
- Demonstration: Creating a Connection Profile
- Distributing the Connection Profile to Users

The Connection Manager Administration Kit (CMAK) allows administrators to customize users’ remote-connection options by creating pre-defined connections to remote servers and networks. The CMAK wizard creates an executable file, which you can distribute in many ways or include during deployment activities as part of the operating-system image.
What is the Connection Manager Administration Kit?

**The Connection Manager Administration Kit:**

- Allows you to customize users’ remote connection experience by creating pre-defined connections on remote servers and networks
- Creates an executable file that can be run on a client computer to establish a network connection that you have designed
- Reduces Help Desk requests related to the configuration of RAS connections
- Assists in problem resolution because the configuration is known
- Reduces the likelihood of user errors when configuring their own connection objects

**Key Points**

The CMAK is a tool that you can use to customize the remote connection experience for users on your network by creating pre-defined connections to remote servers and networks. Use the CMAK wizard to create and customize a connection for your users.

**Additional Reading**

- CMAK Help: Welcome to the Connection Manager Administration Kit
Demonstration: Installing CMAK

In this demonstration, you will see how to use the Server Manager tool to install the Connection Manager Administration Kit.
Process for Configuring a Connection Profile

The CMAK Connection Profile Wizard assists in the process of creating custom connection profiles for users.

Use the CMAK Connection Profile Wizard to configure:

- The target operating system
- Support for VPN
- Support for Dial-up, including the custom phone book
- Proxy
- Custom Help file
- Custom support information

Key Points
You can configure a new or existing connection profile using the CMAK wizard. Each page of the wizard allows you to complete another step of the process.

Note: For complete information about creating a connection profile, see the CMAK Operations Guide.

Additional Reading
- CMAK Operations Guide
- Connection Manager Administration Kit Help: Run the CMAK Wizard to Create a Connection Profile
Demonstration: Creating a Connection Profile

In this demonstration, you will see how to use the Connection Manager Administration Kit to create a connection profile.
Distributing the Connection Profile to Users

The connection profile can be distributed to users in the following ways:

- As part of an image for new computers
- On removable media for the user to install manually
- With software distribution tools, such as Systems Management Server or System Center Configuration Manager 2007

Key Points
The CMAK wizard compiles the connection profile into a single executable file with an .exe file name extension. You can deliver this file to users through any method that is available to you. Some methods to consider are:

- Include the connection profile as part of the image included with new computers.
- Deliver the connection profile on removable media for the user to install manually.
- Deliver the connection profile with automated software distribution tools.

Additional Reading
- Connection Manager Administration Kit Help: Distribute Your Connection Profile to Your Users
Lesson 5
Troubleshooting Routing and Remote Access

- TCP/IP Troubleshooting Tools
- Authentication and Accounting Logging
- Configuring Remote Access Logging
- Configuring Remote Access Tracing
- Common Troubleshooting Solutions

Troubleshooting the Routing and Remote Access Service can be a very time-consuming task. The issues may be varied and not easily identified. Given that you may be using dial-up, dedicated, leased or public-based networks to satisfy your remote-connectivity solution, you must perform troubleshooting in a methodical, step-by-step process.
TCP/IP Troubleshooting Tools

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ipconfig</td>
<td>Displays current TCP/IP network configuration values, updates, or releases; DHCP allocated leases; and used to display, register, or flush DNS names</td>
</tr>
<tr>
<td>Ping</td>
<td>Sends ICMP Echo Request messages to verify that TCP/IP is configured correctly and that a TCP/IP host is available</td>
</tr>
<tr>
<td>Pathping</td>
<td>Displays a path of a TCP/IP host and packet losses at each router along the way</td>
</tr>
<tr>
<td>Tracert</td>
<td>Displays the path of a TCP/IP host</td>
</tr>
</tbody>
</table>

Key Points

Windows Server 2008 includes basic and advanced TCP/IP diagnostic tools that you can use to troubleshoot TCP/IP.

Basic TCP/IP diagnostic tools include:

- Network Diagnostics in Help and Support
- Network Connections folder
- Ipconfig command
- Ping command
Advanced TCP/IP diagnostic tools include:

- Hostname command
- Nbtstat command
- Pathping command
- Route command
- Tracert command

Additional Reading
- How to troubleshoot TCP/IP connectivity with Windows XP
Authentication and Accounting Logging

There are three types of logging for Network Policy Server:

- Event logging for auditing and troubleshooting connection attempts
- Logging authentication and accounting requests to a local file
- Logging authentication and accounting requests to a SQL server database

Key Points
You can configure NPS to perform RADIUS accounting for user authentication requests, Access-Accept messages, Access-Reject messages, accounting requests and responses, and periodic status updates. You can use this procedure to configure the log files in which you want to store the accounting data.

Additional Reading
- Help topic: Configure Log File Properties
Configuring Remote Access Logging

You can configure remote access logging to:

- Log errors only
- Log errors and warnings
- Log all events
- Not log any events
- Log additional routing and remote access information

Key Points
To configure remote-access logging, open the Routing and Remote Access Service console, right-click \textit{servername}, and then click Properties. Click the Logging tab to view the available options for, and the location of, the tracing log.

The four levels of event logging that Windows Server 2008 Routing and Remote Access Service makes available are:

- Log Errors Only
- Log Errors and Warnings
- Log all events
- Do not log any events

Additional Reading
- Routing and Remote Access Service Help: Server Properties – Logging Tab
Configuring Remote Access Tracing

You can configure remote access tracing by using:

- The Netsh command:
  - Netsh ras diagnostics set rastracing * enabled (enables tracing on all components in RAS)
- The Registry:
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing

Tracing consumes resources, so you should use it for troubleshooting only and then disable it

Key Points
The Routing and Remote Access service in Windows Server 2008 has an extensive tracing capability that you can use to troubleshoot complex network problems. You can enable the components in Windows Server 2008 to log tracing information to files using the Netsh command or through the Registry.

Additional Reading
- Help topic: VPN troubleshooting Tools
Common Troubleshooting Solutions

Common problems regarding remote access include:

- Error 800: VPN unreachable
- Error 721: Remote computer not responding
- Error 741/742: Encryption mismatch
- Unable to establish VPN connection
- L2TP/IPsec issues
- EAP-TLS issues

Key Points

Common issues that you may encounter when using Windows Server 2008 Remote Access include:

- Error 800: VPN server is unreachable
- Error 721: Remote computer is not responding
- Error 741/742: Encryption mismatch error
- Unable to establish a remote access VPN connection
- L2TP/IPsec authentication issues
- EAP-TLS authentication issues
- Connection attempt is accepted when it should be rejected
- VPN clients are unable to access resources beyond the VPN server
- Unable to establish tunnel
Additional Reading

- Help topic: Troubleshoot Remote Access
Lab: Configuring and Managing Network Access

- Exercise 1: Configuring Routing and Remote Access as a VPN Remote Access Solution
- Exercise 2: Configuring a Custom Network Policy
- Exercise 3: Configuring Logging
- Exercise 4: Configuring a Connection Profile

Logon information

<table>
<thead>
<tr>
<th>Virtual machine</th>
<th>6421A-NYC-DC1, 6421A-NYC-SVR1 and 6421A-NYC-CL1</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Administrator</td>
</tr>
<tr>
<td>Password</td>
<td>Pa$$w0rd</td>
</tr>
</tbody>
</table>

Estimated time: 60 minutes

Objectives

After completing this lab, you will be able to:

- Configure the Routing and Remote Access service as a VPN remote access solution.
- Configure a custom Network Policy.
- Configure logging.
- Configure a connection profile.
Scenario
Woodgrove Bank would like to implement a remote access solution for its employees so they can connect to the corporate network while away from the office. Woodgrove Bank requires a network policy that mandates that VPN connections are encrypted for security reasons.

The IT department of Woodgrove Bank does not want the Remote Access solution to cause a dramatic increase in support calls to the Help Desk for configuration issues regarding VPN connection objects that need to be created on the client computer.

Lab Setup
For this lab you will use the available virtual machine environment. Before you begin the lab, you must:

1. Start the NYC-DC1, NYC-SVR1, and NYC-CL1 virtual machines.
2. Log on to the NYC-SVR1 with the user name Woodgrovebank\administrator and the password Pa$$w0rd.
3. Close the Initial Configuration Tasks window that appears after log on.
4. Close the Server Manager window that appears.
Exercise 1: Configuring Routing and Remote Access Service as a VPN Remote Access Solution

Exercise Overview
In this exercise, you will configure the Routing and Remote Access Service role as a VPN Remote Access solution. The VPN server should use IP address allocation for clients from a static pool of IP addresses that is configured on the Remote Access server. The Remote Access server should only accept PPTP and L2TP connections, with 25 connections allowed for each.

The main tasks are as follows:
1. Ensure that you have completed the steps in the Lab Setup.
2. Install the Network Policy and Access Services role.
3. Configure 6421A-NYC-SVR1 as a VPN server with a static address pool for Remote Access clients.

► Task 1: Ensure that you have completed the steps in the Lab Setup
- Review the Lab Setup section and ensure you have completed the steps before you continue with this lab.

► Task 2: Install the Network Policy and Access Services role on 6421A-NYC-SVR1
1. Open Server Manager on 6421A-NYC-SVR1 and click Add Roles.
2. In Server Manager, on the Server Roles page, scroll down, select Network Policy and Access Services, and then click Next.
3. On the Select Role Services page, select Network Policy Server and Routing and Remote Access Services, and then click Next.
4. On the **Confirm Installation Selections** page, click **Install**.

5. On the **Installation Results** page, verify **Installation succeeded** appears in the details pane, and then click **Close**.

The **Network Policy** and **Routing and Remote Access Services** roles are installed on 6421A-NYC-SVR1.

---

**Note:** Do not log off or shut down the virtual machines at this point.

---

**Task 3: Configure 6421A-NYC-SVR1 as a VPN server with a static address pool for Remote Access clients**

1. From **Administrative Tools**, open **Routing and Remote Access**.

2. In the list pane, select and right-click **6421A-NYC-SVR1**, and then click **Configure and Enable Routing and Remote Access**.

3. Ensure that the default setting, **Remote Access (dial-up or VPN)**, is selected, and then on the **Remote Access** page, select the **VPN** option.

4. On the **VPN Connection** page, select the **Local Area Connection 2** interface.

5. On the **IP Address Assignment** page, select **From a specified range of addresses**.

6. Use the range of **192.168.1.100** with **75** available addresses for the static pool.

7. Accept the default settings for the remainder of the configuration process.

---

**Task 4: Configure available VPN ports on the Routing and Remote Access Service server to allow 25 PPTP and 25 L2TP connections**

1. In the **Routing and Remote Access** administrative tool interface, right-click **Ports** and then click **Properties**.

2. In the **Ports Properties** dialog box, configure **L2TP** and **PPTP** to have **25** available connectors. Specify **0** for **SSTP**.

3. In the **Ports Properties** dialog box, click **OK**.

Exercise 2: Configuring a Custom Network Policy

Exercise Overview
In this exercise, you will create a network policy to allow secure connections to the Routing and Remote Access Service server.

The main tasks are as follows:
2. Create a new network policy for Routing and Remote Access Service clients.

▶ Task 1: Open the Network Policy Server management tool on 6421A-NYC-SVR1
• From the Administrative Tools menu, click Network Policy Server.
  The Network Policy Server administrative tool appears.

▶ Task 2: Create a new network policy for Routing and Remote Access Service clients
1. In the list pane of the Network Policy Server administrative tool, expand Policies, right-click Network Policies, and then click New.
2. In the New Network Policy wizard, specify the following settings and accept the default values for all other settings:
   • Network Policy Name: Secure VPN
   • Type of network access server: Remote Access Server (VPN-Dial up)
   • Specify Conditions: Tunnel Type: PPTP and L2TP
   • Configure Authentication Methods: Deselect MS-CHAP
   • Configure Constraints: Day and Time: deny access Mon thru Fri 11PM to 6AM
   • Configure Settings: Under Encryption, clear all settings except Strongest encryption
Exercise 3: Configuring Logging

Exercise Overview
In this exercise, you will enable logging in Routing and Remote Access.

The main tasks are as follows:
1. Configure Routing and Remote Access Service logging on 6421A-NYC-SVR1 to log all events to the system log.
2. Test logging levels.

▶ Task 1: Configure Routing and Remote Access Service Logging on 6421A-NYC-SVR1 to log all events to the System log
1. Click Start, point to Administrative Tools, and then click Routing and Remote Access.
2. Right-click 6421A-NYC-SVR1 and then click Properties.
3. In the 6421A-NYC-SVR1 (local) Properties dialog box, click the Logging tab, click Log all events, and then click OK.

▶ Task 2: Test logging levels
1. Log on to NYC-CL1 with a user name of administrator and a password of Pa$$w0rd.
2. Click Start, click Network, and then in the Network window, click Network and Sharing Center.
3. Under Tasks, click Set up a connection or network to create a new VPN connection object.
4. In the Type the Internet address to connect to dialog box, specify an Internet address of 10.10.0.24 and a Destination Name of Woodgrovebank VPN.
5. Accept the defaults for the remainder of the wizard settings.
6. After the VPN connection object is created, connect to WoodgroveBank VPN from the Network Connections page.
7. Use the following information in the Connect Woodgrovebank VPN text boxes:
   - User name: Administrator
   - Password: Pa$$w0rd
   - Domain: Woodgrovebank

   The VPN connects successfully.

8. Right-click Woodgrovebank VPN and then click Disconnect. The VPN disconnects.

9. On 6421A-NYC-SVR1, click Start, point to Administrative Tools, and then click Event Viewer.

10. Use Event Viewer on 6421A-NYC-SVR1 and review the entries from the RemoteAccess source in the System log to see the logged data.

Exercise 4: Configuring a Connection Profile

Exercise Overview
In this exercise, you will configure a Connection Profile by using the Connection Manager Administration Kit (CMAK) tool to create connection objects for mobile computer users.

The main tasks are as follows:
1. Install the Connection Manager Administration Kit.
2. Use the CMAK to create a distributable executable that automates creation of connection objects for users.
3. Install and test the CMAK profile.
4. Close all virtual machines and delete the changes.

▶ Task 1: Install the Connection Manager Administration Kit
1. On 6421A-NYC-SVR1, click Start, and then click Server Manager.
2. Select the Connection Manager Administration Kit feature and then click Install.

▶ Task 2: Use the CMAK to create a distributable executable that automates creation of connection objects for users
1. Click Start, point to Administrative Tools, and then click Connection Manager Administration Kit.
2. On the Welcome page of the Connection Manager Administration Kit wizard, click Next. Specify the following settings in the wizard interface and accept the default values for the other settings:
   - On the Specify the Service Name and the File Name page, use WOODGROVEBANK VPN for the Service name and CORP_VPN for the File name.
• In Add Support for VPN Connections, select Phone book from this profile and specify to always use the same VPN server with an IP address of 10.10.0.24.

• In Add a custom Phone Book, deselect Automatically download phone book updates.

3. On the Your Connection Manager Profile is Complete and Ready to Distribute page, click Finish.

4. From NYC-SVR1, copy the CORP_VPN folder from the C:\Program Files\CMAK\Profiles\Vista\ location to the \NYC-DC1\Module6 location.

▶ Task 3: Install and test the CMAK profile

1. On 6421A-NYC-CL1, in the \NYC-DC1\module6\ share, run CORP_VPN.exe to create the VPN connection object.

   The WOODGROVEBANK VPN connection object opens.

2. In the WOODGROVEBANK VPN connection object, type the following credentials and then click Connect:
   • User name: Administrator
   • Password: Pa$$w0rd
   • Logon Domain: Woodgrovebank

3. Set the Network Location to Work.

4. Verify the VPN connects successfully in Network Connections. Right-click the connection icon and then click Disconnect.

▶ Task 4: Close all virtual machines and discard undo disks

1. On the host computer, click Start, point to All Programs, point to Microsoft Virtual Server, and then click Virtual Server Administration Website.

2. Under Navigation, click Master Status. For each virtual machine that is running, click the virtual machine name, and in the context menu, click Turn off Virtual Machine and Discard Undo Disks. Click OK.
Module Review and Takeaways

- Review Questions
- Best Practices
- Tools

Review Questions

1. You are adding Remote Access services to an existing infrastructure that uses non-RFC 1542 compliant routers. The DHCP server is not on the same subnet as the Remote Access server. What is one issue that might arise due to this configuration? How would you mitigate the issue?

2. You want to implement a VPN solution for users in your company, but the group that is responsible for security does not want to open the firewall to PPTP and L2TP traffic. Is it possible to create such a solution in Windows Server 2008? If so, what would you use?

3. Based on the scenario in the previous question, what encryption is used to secure traffic?
4. Is it possible to ignore the dial-in properties assigned to accounts in Active Directory with network policies? In what property category would this be set?

5. You have enabled full RADIUS logging on the Remote Access servers in your organization and verified that the logs are gathering the requested information. After a few weeks of logging, users begin to call the Help Desk because their connection attempts are failing. What is the most likely problem?

Best Practices
Decisions about the best method for providing remote access will vary depending on the tools you have chosen:

- Install and test servers running the Routing and Remote Access Service before configuring them as RADIUS clients.

- The RADIUS and Remote Access servers should be dedicated servers. This will minimize the likelihood of unauthorized users gaining network access and weakening the security configuration.

- Physically secure the RADIUS and Remote Access servers.

- Disable authentication protocols that you do not use. Do not use Password Authentication Protocol (PAP) unless you must support legacy systems.

- Determine the desired logging levels for auditing purposes and back up RADIUS logs.

- Secure remote administration sessions with IPSec or with VPNs if the sessions are initiated externally.
## Tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Use For</th>
<th>Where to find it</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing and Remote Access management tool</td>
<td>Managing and configuring the Routing and Remote Access service on the local server</td>
<td><strong>Routing and Remote Access</strong> on the Administrative Tools menu</td>
</tr>
<tr>
<td>Network Policy Server</td>
<td>Managing and creating network policy</td>
<td><strong>Network Policy Server</strong> on the Administrative Tools menu</td>
</tr>
<tr>
<td>Connection Manager Administration Kit</td>
<td>Creating customized, distributable connection objects for installation on client’s computers</td>
<td><strong>Connection Manager Administration Kit</strong> on the Administrative Tools menu</td>
</tr>
<tr>
<td>Event Viewer</td>
<td>Viewing logged information from application events, system events and security events</td>
<td><strong>Event Viewer</strong> on the Administrative Tools menu</td>
</tr>
</tbody>
</table>
Module 7

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

**Contents:**

- Lesson 1: Installing and Configuring a Network Policy Server 7-3
- Lesson 2: Configuring RADIUS Clients and Servers 7-9
- Lesson 3: NPS Authentication Methods 7-16
- Lesson 4: Monitoring and Troubleshooting a Network Policy Server 7-22
- Lab: Configuring and Managing Network Policy Server 7-27
Module Overview

- Installing and Configuring a Network Policy Server
- Configuring RADIUS Clients and Servers
- NPS Authentication Methods
- Monitoring and Troubleshooting a Network Policy Server

Lesson 1
Installing and Configuring a Network Policy Server

- What is a Network Policy Server?
- Network Policy Server Usage Scenarios
- Demonstration: How to Install the Network Policy Server
- Tools Used for Managing a Network Policy Server
- Demonstration: Configuring General NPS Settings

NPS allows you to configure and manage network policies centrally with the following three features: RADIUS server, RADIUS proxy, and NAP policy server.
What is a Network Policy Server?

Windows Server 2008 Network Policy Server (NPS):

- RADIUS server
- RADIUS proxy
- Network Access Protection

NPS allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization. You also can use NPS as a RADIUS proxy to forward connection requests to NPS or other RADIUS servers that you configure in remote RADIUS server groups.

Additional Reading

Network Policy Usage Scenarios

NPS is used for the following scenarios:

- **Network Access Protection**
  - Enforcement for IPsec traffic
  - Enforcement for 802.1x wired and wireless
  - Enforcement for DHCP
  - Enforcement for VPN

- **Secure Wired and Wireless Access**

- **RADIUS**

- **Terminal Server Gateway**

You can use NPS in Windows Server 2008 as either a RADIUS server or proxy.

- As a RADIUS server, NPS performs centralized connection authentication, authorization, and accounting for many types of network access, including wireless, authenticating switch, dial-up and VPN remote access, and router-to-router connections.

- As a RADIUS proxy, NPS forwards authentication and accounting messages to other RADIUS servers.

**Additional Reading**

- Network Policy Server Help: Network Policy Server Overview
Demonstration: How to Install the Network Policy Server

In this demonstration, you will see how to install the Network Policy Server
Tools Used for Managing a Network Policy Server

The following tools enable you to manage the Network Policy and Access Services server role:

- **NPS MMC snap-in.** Use the NPS MMC to configure a RADIUS server, RADIUS proxy, or NAP technology.
- **Netsh commands for NPS.** The netsh commands for NPS provide a command set that is fully equivalent to all configuration settings that are available through the NPS MMC snap-in.

**Additional Reading**
- Network Policy Server Help: Network Policy Server Overview
Demonstration: Configuring General NPS Settings

In this demonstration, you will see how to configure general NPS settings.
Lesson 2
Configuring RADIUS Clients and Servers

- What is a RADIUS Client?
- What is a RADIUS Proxy?
- Demonstration: Configuring a RADIUS Client
- Configuring Connection Request Processing
- What is a Connection Request Policy?
- Demonstration: Creating a New Connection Request Policy


The following components are part of the RADIUS authentication, authorization, and accounting infrastructure:

- Access clients
- Access servers (RADIUS clients)
- RADIUS proxies
- RADIUS servers
- User account databases
Demonstration: Configuring a RADIUS Client

In this demonstration, you will see how to:

- Add a new RADIUS client to NPS
- Configure Routing and Remote Access as a RADIUS client
What is a Connection Request Policy?

*Connection Request policies are sets of conditions and settings that designate which RADIUS servers perform the authentication and authorization of connection requests that NPS receives from RADIUS clients.*

**Connection Request policies include:**

- **Conditions, such as:**
  - Framed Protocol
  - Service Type
  - Tunnel Type
  - Day and Time restrictions

- **Settings, such as:**
  - Authentication
  - Accounting
  - Attribute Manipulation
  - Advanced settings

*Custom Connection Request policies are required to forward the request to another proxy or RADIUS server or server group for authorization and authentication, or to specify a different server for accounting information.*

Connection request policies are sets of conditions and settings that allow network administrators to designate which RADIUS servers perform authentication and authorization of connection requests that the NPS server receives from RADIUS clients. You can configure connection request policies to designate which RADIUS servers to use for RADIUS accounting.

**Additional Reading**

- Network Policy Server Help: Connection Request Policies
Demonstration: Creating a New Connection Request Policy

In this demonstration, you will see how to:

- Use the Connection Request Policy wizard to create a new connection request policy
- Disable or delete a connection request policy
Lesson 3
NPS Authentication Methods

- Password-Based Authentication Methods
- Using Certificates for Authentication
- Required Certificates for NPS Authentication Methods
- Deploying Certificates for PEAP and EAP

When users attempt to connect to your network through network access servers (also called RADIUS clients), such as wireless access points, 802.1X authenticating switches, dial-up servers, and VPN servers, NPS authenticates and authorizes the connection request before allowing or denying access.

Because authentication is the process of verifying the identity of the user or computer attempting to connect to the network, NPS must receive proof of identity from the user or computer in the form of credentials.
Password-Based Authentication Methods

<table>
<thead>
<tr>
<th>Authentication methods for an NPS server include:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• MS-CHAPv2</td>
</tr>
<tr>
<td>• MS-CHAP</td>
</tr>
<tr>
<td>• CHAP</td>
</tr>
<tr>
<td>• PAP</td>
</tr>
<tr>
<td>• Unauthenticated access</td>
</tr>
</tbody>
</table>

Each authentication method has advantages and disadvantages in terms of security, usability, and breadth of support. However, password-based authentication methods do not provide strong security and we do not recommend their use. We recommend that you use a certificate-based authentication method for all network access methods that support certificate use. This is especially true for wireless connections, for which we recommend the use of PEAP-MS-CHAP v2 or PEAP-TLS.

Additional Reading
- Help Topic: Password-Based Authentication Methods
Using Certificates for Authentication

**Certificate-based authentication in NPS:**

- **Certificate types:**
  - CA certificate: Verifies the trust path of other certificates
  - Client computer certificate: Issued to the computer to prove its identity to NPS during authentication
  - Server certificate: Issued to an NPS server to prove its identity to client computers during authentication
  - User certificate: Issued to individuals to prove their identity to NPS servers for authentication

- **Certificates can be obtained from public CA providers or you can host your own Active Directory certificate services**

- **To specify certificate-based authentication in a network policy, configure the authentication methods on the Constraints tab**

Certificates are digital documents that certification authorities (CAs) issue, such as Active Directory Certificate Services (AD CS) or the Verisign public CA. You can use certificates for many purposes, such as code signing and securing e-mail communication. However, with NPS, you use certificates for network access authentication because they provide strong security for authenticating users and computers, and eliminate the need for less secure, password-based authentication methods.

**Additional Reading**
- Help Topic: Certificates and NPS
Required Certificates for NPS Authentication Methods

All certificates must meet the requirements for X.509 and must work for connections that use SSL/TLS

<table>
<thead>
<tr>
<th>Type</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server certificates</strong></td>
<td>• Must contain a Subject attribute that is not NULL</td>
</tr>
<tr>
<td></td>
<td>• Must chain to a trusted-root CA</td>
</tr>
<tr>
<td></td>
<td>• Configured with Server Authentication purpose in EKU extensions</td>
</tr>
<tr>
<td></td>
<td>• Configured with required algorithm of RSA with a minimum 2048 key length</td>
</tr>
<tr>
<td></td>
<td>• Subject Alternative Name extension, if used, must contain the DNS name</td>
</tr>
<tr>
<td><strong>Client certificates</strong></td>
<td>• Issued by an Enterprise CA or mapped to an account in Active Directory</td>
</tr>
<tr>
<td></td>
<td>• Must chain to a trusted-root CA</td>
</tr>
<tr>
<td></td>
<td>• For computer certificates, the Subject Alternative Name must contain the FQDN</td>
</tr>
<tr>
<td></td>
<td>• For user certificates, the Subject Alternative Name must contain the UPN</td>
</tr>
</tbody>
</table>

The following table details the certificates that are required to successfully deploy each of the listed certificate-based authentication methods.

<table>
<thead>
<tr>
<th>Certificate</th>
<th>Required for EAP-TLS and PEAP-TLS?</th>
<th>Required for PEAP-MS-CHAP v2?</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA certificate in the Trusted Root Certification Authorities certificate store for the Local Computer and Current User</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Client computer certificate in the certificate store of the client</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Server certificate in the certificate store of the NPS server</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>User certificate on a smart card</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
Additional Reading

- Help Topic: Certificate Requirements for PEAP and EAP
- Help Topic: Certificates and NPS
Deploying Certificates for PEAP and EAP

- For Domain Computer and User accounts, use the auto-enrollment feature in Group Policy
- Non-domain member enrollment requires an administrator to request a user or computer certificate using the CA Web Enrollment tool
- The administrator must save the computer or user certificate to a floppy disk or other removable media, and manually install the certificate on the non-domain member computer
- The administrator can distribute user certificates on a smart card

All certificates that you use for network access authentication with EAP-TLS and PEAP must meet the requirements for X.509 certificates and work for connections that use Secure Sockets Layer-Transport Level Security (SSL/TLS). After this minimum requirement is met, both client and server certificates have additional requirements.

Additional Reading
- Help Topic: Certificates and NPS
- Help Topic: EAP and NPS
- Help Topic: PEAP and NPS
Lesson 4
Monitoring and Troubleshooting a Network Policy Server

- Methods Used to Monitor NPS
- Configuring Log File Properties
- Configuring SQL Server Logging
- Configuring NPS Events to Record in the Event Viewer

You can monitor NPS by configuring and using logging for events and user authentication and accounting requests. Event logging enables you to record NPS events in the system and security event logs. You can use request logging for connection analysis and billing purposes. The information that the log files collect is useful for troubleshooting connection attempts and for security investigation.
Methods Used to Monitor NPS

NPS monitoring methods include:

- **Event logging**
  - The process of logging NPS events in the System Event log
  - Useful for auditing and troubleshooting connection attempts

- **Logging user authentication and accounting requests**
  - Useful for connection analysis and billing purposes
  - Can be in a text format
  - Can be in a database format within a SQL instance

There are two types of accounting, or logging, that you can use to monitor NPS:

- Event logging for NPS. You can use event logging to record NPS events in the system and security event logs. You use this primarily for auditing and troubleshooting connection attempts.

- Logging user authentication and accounting requests. You can log user authentication and accounting requests to log files in text format or database format, or you can log to a stored procedure in a SQL Server 2000 database. Use request logging primarily for connection analysis and billing purposes, and as a security investigation tool, as it enables you to identify an attacker’s activity.

Additional Reading

- Help Topic: NPS Best Practices
Configuring Log File Properties

Use the NPS console to configure logging:

1. Open NPS from the Administrative Tools menu
2. In the console tree, click Accounting
3. In the details pane, click Configure Local File Logging
4. On the Settings tab, select the information to be logged
5. On the Log File tab, select the log type and the frequency or size attributes of the log files to be generated

Log files should be stored on a separate partition from the system partition:

If RADIUS accounting fails due to a full hard disk, NPS stops processing connection requests

You can configure NPS to perform RADIUS accounting for user authentication requests, Access-Accept messages, Access-Reject messages, accounting requests and responses, and periodic status updates.

Additional Reading

- Help Topic: Configure Log File Properties
- Help Topic: NPS Best Practices
Configure SQL Server Logging

You can use SQL to log RADIUS accounting data:

- Requires SQL to have a stored procedure named `report_event`
- NPS formats accounting data as an XML document
- Can be a local or remote SQL Server database

You can configure NPS to perform RADIUS accounting for user authentication requests, Access-Accept messages, Access-Reject messages, accounting requests and responses, and periodic status updates. You can use this procedure to configure logging properties and the connection to the server – running SQL Server – that stores your accounting data. The SQL Server database can be on the local computer or on a remote server.

**Additional Reading**

- Help Topic: Configure SQL Logging in NPS
Configuring NPS Events to Record in the Event Viewer

How do I configure NPS events to be recorded in Event Viewer?

- **NPS is configured by default to record failed connections and successful connections in the event log**
  - You can change this behavior on the **General** tab of the **Properties** sheet for the network policy
- **Common request failure events**
- **What information does the failure event record?**
- **What information does the success event record?**

What is Schannel logging and how do I configure it?

- **Schannel** is a security support provider that supports a set of Internet security protocols
- You can configure Schannel logging in the following Registry key:
  
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\EventLogging

You can configure NPS event logging to record connection-request failure and success events in the Event Viewer system log.

Additional Reading
- Help Topic: NPS Events and Event Viewer
- Help Topic: Configure NPS Event Logging
Lab: Configuring and Managing Network Policy Server

Logon information

<table>
<thead>
<tr>
<th>Virtual machine</th>
<th>6421A-NYC-DC1 and 6421A-NYC-SVR1</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Administrator</td>
</tr>
<tr>
<td>Password</td>
<td>Pa$$w0rd</td>
</tr>
</tbody>
</table>

Estimated time: 60 minutes

Objectives:
After completing this lab, you will be able to:

- Install the Network Policy Server role service and configure Network Policy Server settings
- Configure a RADIUS client
- Configure certificate auto-enrollment
Scenario
Woodgrove Bank is expanding its remote-access solution to all its branch office employees. This will require multiple Routing and Remote Access servers located at different points to provide connectivity for its employees. You will use RADIUS to centralize authentication and accounting for the remote-access solution.

The Windows Infrastructure Services Technology Specialist has been tasked with installing and configuring Network Policy Server into an existing infrastructure to be used for NAP, Wireless and Wired access, RADIUS, and RADIUS Proxy.

Lab Setup
For this lab, you will use the available virtual machine environment. Before you begin the lab, you must:

1. Start the NYC-DC1 and NYC-SVR1 virtual machines.
2. Log on to the NYC-SVR1 and NYC-DC1 virtual machines with the user name administrator and the password Pa$$w0rd.
3. Close the Initial Configuration Tasks window that appears after you log on.
4. Close the Server Manager window.
Exercise 1: Installing and Configuring the Network Policy Server Role Service

Exercise Overview
In this exercise, you will install and configure the Network Policy Server role. The main tasks are as follows:
1. Ensure that you have completed the steps in the Lab Setup.
2. Open the Server Manager tool on 6421A-NYC-DC1.
3. Install the Network Policy and Access Services role.
4. Register NPS in Active Directory.
5. Configure 6421A-NYC-DC1 to be a RADIUS server for dial-up or VPN connections.

Task 1: Ensure that you have completed the steps in the Lab Setup
• Review the Lab Setup section and ensure you have completed the steps before you continue with this lab.

Task 2: Open the Server Manager tool on 6421A-NYC-DC1
• On 6421A-NYC-DC1, open Server Manager from the Administrative Tools menu.

Task 3: Install the Network Policy and Access Services role
1. In the Server Manager list pane, right-click Roles and then click Add Roles.
2. Install the Network Policy Server role service from the Network Policy and Access Services role.
3. On the Installation Results page, verify Installation succeeded appears in the details pane and then click Close.
   The Network Policy Server role is installed on 6421A-NYC-DC1.
4. Do not log off or shut down the virtual PCs at this point.
Task 4: Register NPS in Active Directory
1. Open Network Policy Server from the Administrative Tools menu.
2. Using the NPS tool, register NPS in Active Directory.
   The Network Policy server is registered in Active Directory.

Task 5: Configure 6421A-NYC-DC1 to be a RADIUS server for dial-up or VPN connections
1. In the Network Policy Server management tool list pane, click NPS (Local).
2. In the details pane under Standard Configuration, click RADIUS server for Dial-Up or VPN Connections.
3. Under Radius server for Dial-Up or VPN Connections, click Configure VPN or Dial-Up and specify Virtual Private Network (VPN) Connections, and accept the default name.
4. In the RADIUS clients dialog box, add NYC-SVR1 as a RADIUS client with an address of 10.10.0.24.
5. In the New RADIUS Client dialog box, specify and confirm the shared secret of Pa$$w0rd and then click OK.
6. In the Specify Dial-Up or VPN Server dialog box, accept the default setting.
7. In the Configure Authentication Methods dialog box, select Extensible Authentication Protocol and MS-CHAPv2.
8. On the Specify User Groups page, accept the default settings.
9. On the Specify IP Filters page, accept the default settings.
11. On the Specify a Realm Name page, accept the default settings and finish the wizard.
Exercise 2: Configuring a RADIUS Client

Exercise Overview
In this exercise, you will configure 6421A-NYC-SVR1 to host Routing and Remote Access Services and configure 6421A-NYC-SVR1 as a RADIUS client.

The main tasks are as follows:
1. Open the Server Manager tool on 6421A-NYC-SVR1.
2. Install the Routing and Remote Access Services role.

► Task 1: Open the Server Manager tool on 6421A-NYC-SVR1
- On 6421A-NYC-SVR1, open Server Manager from the Administrative Tools menu.

► Task 2: Install the Routing and Remote Access Services role on 6421A-NYC-SVR1
1. Using Server Manager, install the Network Policy and Access Services role with the role service of Routing and Remote Access.
2. On the Installation Results page, verify Installation succeeded appears in the details pane, and then click Close.
   The Routing and Remote Access Services role is installed on 6421A-NYC-SVR1.
3. Do not log off or shut down the virtual PCs at this point.
Task 3: Configure 6421A-NYC-SVR1 as a VPN server with a static address pool for Remote Access clients and specify RADIUS authentication and accounting

1. Open the Routing and Remote Access Services administrative tool and click Configure and Enable Routing and Remote Access.
2. Configure the default Remote Access (dial-up or VPN), and on the Remote Access page, select the VPN option.
3. On the VPN Connection page, select the Local Area Connection 2 interface.
4. On the IP Address Assignment page, select From a specified range of addresses.
5. Use the range of 192.168.1.100 with 75 available addresses for the static pool.
6. On the Managing Multiple Remote Access Servers page, select Yes, set up this server to work with a RADIUS server, and then click Next.
7. Configure the following settings:
   - Primary RADIUS server: NYC-DC1
   - Shared secret for the RADIUS server: Pa$$w0rd
   - Accept the default settings for the remainder of the configuration process
Exercise 3: Configuring Certificate Auto-Enrollment

Exercise Overview
In this exercise, you will configure Certificate Auto-Enrollment for computers to use advanced authentication.

The main tasks are as follows:
1. Install and configure Certificate Services on NYC-DC1.
2. Open the Group Policy Management tool on 6421A-NYC-DC1 and configure automatic certificate enrollment.
3. Close all virtual machines and delete changes.

► Task 1: Install and Configure Certificate services on NYC-DC1
1. On NYC-DC1, start Server Manager from the Administrative Tools menu.
2. Install the Active Directory Certificate Services role using the defaults except for the following:
   - CA Name = WoodGroveBank-CA
3. On the Installation Results page, click Close.
4. From the Administrative Tools menu, open the Certification Authority management tool.
5. Right-click Certificate Templates, and then select Manage from the context menu.
6. Change the security on the Computer template to allow Authenticated Users the Enroll permission.
7. Close the Certificate Template and certsrv management consoles.
Task 2: Open the Group Policy Management tool on 6421A-NYC-DC1 and configure automatic certificate enrollment

1. On 6421A-NYC-DC1, open Group Policy Management from the Administrative Tools menu.


3. Right-click Default Domain Policy, and then click Edit.

4. Expand Computer Configuration, expand Window Settings, expand Security Settings, and then expand Public Key Policies.


6. Accept the default settings throughout the wizard.

7. Close the Group Policy Management Editor.


9. Start 6421A-NYC-CL1 and log on as Administrator with the password of Pa$$w0rd.

10. Create a new MMC console with the Certificates snap-in. Focus the snap-in to the Computer Account.

11. In the MMC console, verify that the computer account has enrolled the certificate from WoodGroveBank-CA.

Task 3: Close all virtual machines and discard undo disks

1. On the host computer, click Start, point to All Programs, point to Microsoft Virtual Server, and then click Virtual Server Administration Website.

2. Under Navigation, click Master Status. For each virtual machine that is running, click the virtual machine name, and in the context menu, click Turn off Virtual Machine and Discard Undo Disks. Click OK.
Module Review and Takeaways

- Review questions
- Best Practices
- Security Issues
- Tools

Review Questions
1. Why must you register the NPS server in Active Directory?
2. How can you make the most effective use of the NPS logging features?
3. What are the default authentication and accounting ports for RADIUS? What is the procedure for configuring NPS UDP port information using the Windows interface?
4. What other considerations are there if you choose to use a nonstandard port assignment for RADIUS traffic?
Best Practices
Perform the following tasks before installing NPS:

- Install and test each of your network access servers using local authentication methods before you make them RADIUS clients.

- After you install and configure NPS, save the configuration with the `netsh nps show config > path\file.txt` command. Save the NPS configuration with the `netsh nps show config > path\file.txt` command each time a change is made.


- Do not configure a server running NPS or Routing and Remote Access as a member of a Windows NT Server 4.0 domain if your user accounts database is stored on a Windows Server 2008 or Windows Server 2003 domain controller in another domain.

Security Issues
We recommend two methods for remote administration of NPS servers:

- Use Terminal Services to access the NPS server (remote desktop).

- Use Internet Protocol security (IPSEC) to encrypt confidential data.
Tools
The following describes the tools that you can use to configure, manage, monitor and troubleshoot NPS.

<table>
<thead>
<tr>
<th>Tool</th>
<th>Use For</th>
<th>Where to find it</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netsh command-line tool</td>
<td>Creating administrative scripts for configuring and managing the Network Policy Server role</td>
<td>From a command window, type <code>netsh nps</code> to administer from a command environment</td>
</tr>
<tr>
<td>Event Viewer</td>
<td>Viewing logged information from application, system, and security events</td>
<td>Event Viewer on the Administrative Tools menu</td>
</tr>
</tbody>
</table>
Module 8

Configuring Network Access Protection

Contents:
Lesson 1: Overview of Network Access Protection 8-3
Lesson 2: How NAP Works 8-18
Lesson 3: Configuring NAP 8-27
Lesson 4: Monitoring and Troubleshooting NAP 8-34
Lab: Configuring NAP for DHCP and VPN 8-38
Module Overview

- Overview of Network Access Protection
- How NAP Works
- Configuring NAP
- Monitoring and Troubleshooting NAP

Network Access Protection (NAP) ensures compliance with specific health policies for systems accessing the network. NAP assists administrators in achieving and maintaining a specific health policy. This module provides information about how NAP works, and how to configure, monitor, and troubleshoot NAP.
Lesson 1
Overview of Network Access Protection

- What is Network Access Protection?
- NAP Scenarios
- NAP Enforcement Methods
- NAP Platform Architecture
- NAP Architecture Interactions
- NAP Client Infrastructure
- NAP Server-Side Infrastructure
- Communication Between NAP Platform Components

NAP is a system health policy enforcement platform built into Windows Server 2008, Windows Vista™, and Windows® XP Service Pack 3 (which includes the NAP Client for Windows XP, now in beta testing), that allows you to better protect private network assets by enforcing compliance with system health requirements. With NAP, you can create customized health requirement policies to validate computer health before allowing access or communication, automatically update compliant computers to ensure ongoing compliance, and limit the access of noncompliant computers to a restricted network until they become compliant.
What is Network Access Protection?

Network Access Protection can:

- Enforce health requirement policies on client computers
- Ensure client computers are compliant with policies
- Offer remediation support for computers that do not meet the health requirements

Network Access Protection cannot:

- Enforce health requirement policies on client computers
- Ensure client computers are compliant with policies

NAP for Windows Server 2008, Windows Vista, and Windows XP Service Pack 3 provides components and an application programming interface (API) that help administrators enforce compliance with health requirement policies for network access or communication. With NAP, developers and administrators can create solutions for validating computers that connect to their networks, provide needed updates or access to needed health update resources, and limit the access or communication of noncompliant computers.

NAP has three important and distinct aspects:

- Health state validation
- Health policy compliance
- Limited access

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

- Introduction to Network Access Protection
NAP Scenarios

NAP benefits the network infrastructure by verifying the health state of:

- Roaming laptops
- Desktop computers
- Visiting laptops
- Unmanaged home computers

NAP helps provide a solution for the following common scenarios:

- Verifying the health state of roaming laptops
- Verifying the health state of desktop computers
- Verifying the health state of visiting laptops
- Verifying the health state of unmanaged home computer

Depending on their needs, administrators can configure a solution to address any or all of these scenarios for their networks.

**Question:** Have you ever had an issue with non-secure, unmanaged laptops causing harm to the network? Do you think NAP would have addressed this issue?

**Additional Reading**

- Network Access Protection
Components of the NAP infrastructure known as enforcement clients (ECs) and enforcement servers (ESs) require health state validation and enforce limited network access for noncompliant computers for specific types of network access or communication. Windows Vista, Windows XP Service Pack 3, and Windows Server 2008 include NAP support for the following types of network access or communication:

- Internet Protocol Security (IPSec)-protected traffic
- Institute of Electrical and Electronics Engineers (IEEE) 802.1X-authenticated network connections
- Remote access VPN connections
- Dynamic Host Configuration Protocol (DHCP) address configurations

Windows Vista and Windows Server 2008 also include NAP support for Terminal Services Gateway (TS Gateway) connections.
The following sections describe the IPSec, 802.1X, VPN, DHCP and TS Gateway enforcement methods.

- IPSec Enforcement
- 802.1X Enforcement
- VPN Enforcement
- DHCP Enforcement
- Terminal Services Gateway

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

**Additional Reading**
- Terminal Services
- Network Access Protection
The components of a NAP-enabled network infrastructure consist of the following:

- NAP clients
- NAP enforcement points

Examples of NAP enforcement points are the following:

- Health Registration Authority (HRA)
- VPN server
- DHCP server
- Network access devices
- NAP health policy servers
- Health requirement servers
• Active Directory® Domain Service
• Restricted network, which includes:
  • Remediation servers
  • NAP clients with limited access

**Question:** Does your environment presently use 802.1x authentication at the switch level? If so, would 802.1x NAP be beneficial considering remediation VLANs can be configured to offer limited access?

**Additional Reading**
• Network Access Protection Platform Architecture
The interactions for the computers and devices of a NAP-enabled network infrastructure are as follows:

- Between a NAP client and an HRA
- Between a NAP client and an 802.1X network access device (an Ethernet switch or a wireless access point)
- Between a NAP client and a VPN server
- Between a NAP client and a DHCP server
- Between a NAP client and a remediation server
- Between an HRA and a NAP health policy server
- Between an 802.1X network access device and a NAP health policy server
- Between a VPN server and a NAP health policy server
- Between a DHCP server and a NAP health policy server
- Between a NAP health policy server and a health requirement server
Additional Reading

- Network Access Protection Platform Architecture
NAP Client Infrastructure

The NAP client architecture consists of the following:

- A layer of NAP enforcement client (EC) components
- A layer of system health agent (SHA) components
- NAP Agent
- SHA application programming interface (API)
- NAP EC API

The NAP ECs for the NAP platform supplied in Windows Vista, Windows Server 2008, and Windows XP with SP2 (with the NAP Client for Windows XP) are the following:

- An IPSec NAP EC for IPSec-protected communications
- An EAPHost NAP EC for 802.1X-authenticated connections
- A VPN NAP EC for remote access VPN connections
- A DHCP NAP EC for DHCP-based IPv4 address configuration

**Question:** How would your organization deal with enabling the appropriate enforcement client (EC) on non-domain computers outside of the management scope?

**Additional Reading**
- Network Access Protection Platform Architecture
- Network Access Protection Platform Software Development Kit (SDK)
A Windows-based NAP enforcement point has a layer of NAP Enforcement Server (ES) components. Each NAP ES is defined for a different type of network access or communication. For example, there is a NAP ES for remote access VPN connections and a NAP ES for DHCP configuration. The NAP ES is typically matched to a specific type of NAP-capable client. For example, the DHCP NAP ES is designed to work with a DHCP-based NAP client. Third-party software vendors or Microsoft can provide additional NAP ESs for the NAP platform.

**Additional Reading**

- Network Access Protection Platform Architecture
Communication Between NAP Platform Components

The NAP Agent component can communicate with the NAP Administration Server component through the following process:

1. The NAP Agent passes the SSoH to the NAP EC.
2. The NAP EC passes the SSoH to the NAP ES.
3. The NAP ES passes the SSoH to the NPS service.
4. The NPS service passes the SSoH to the NAP Administration Server.

The NAP Administration Server can communicate with the NAP Agent through the following process:

1. The NAP Administration Server passes the SoHRs to the NPS service.
2. The NPS service passes the SSoHR to the NAP ES.
3. The NAP ES passes the SSoHR to the NAP EC.
4. The NAP EC passes the SSoHR to the NAP Agent.
An SHA can communicate with its corresponding SHV through the following process:
1. The SHA passes its SoH to the NAP Agent.
2. The NAP Agent passes the SoH, contained within the SSoH, to the NAP EC.
3. The NAP EC passes the SoH to the NAP ES.
4. The NAP ES passes the SoH to the NAP Administration Server.
5. The NAP Administration Server passes the SoH to the SHV.

The SHV can communicate with its corresponding SHA through the following process:
1. The SHV passes its SoHR to the NAP Administration Server.
2. The NAP Administration Server passes the SoHR to the NPS service.
3. The NPS service passes the SoHR, contained within the SSoHR, to the NAP ES.
4. The NAP ES passes the SoHR to the NAP EC.
5. The NAP EC passes the SoHR to the NAP Agent.
6. The NAP Agent passes the SoHR to the SHA.

Additional Reading
- Network Access Protection Platform Architecture
Lesson 2: How NAP Works

- NAP Enforcement Processes
- How IPSec Enforcement Works
- How 802.1X Enforcement Works
- How VPN Enforcement Works
- How DHCP Enforcement Works

NAP is designed so that administrators can configure it to meet the individual needs of their networks. Therefore, the actual configuration of NAP will vary according to the administrator’s preferences and requirements. However, the underlying operation of NAP remains the same.

When a client attempts to access the network or communicate on the network, it must present its system health state or proof of health compliance. If a client cannot prove it is compliant with system health requirements (for example, that it has the latest operating system and antivirus updates installed), its access to the network or communication on the network can be limited to a restricted network containing server resources so that health compliance issues can be remedied. After the updates are installed, the client requests access to the network or attempts the communication again. If compliant, the client is granted unlimited access to the network or the communication is allowed.
Network Access Protection (NAP) is a policy enforcement platform built into the Windows Vista, the Microsoft Windows XP, and the Windows Server 2008 operating systems that allows you to better protect network assets by enforcing compliance with system health requirements.

To validate access to a network based on system health, a network infrastructure needs to provide the following areas of functionality:

- **Health policy validation**: Determines whether the computers are compliant with health policy requirements.
- **Network access limitation**: Limits access for noncompliant computers.
- **Automatic remediation**: Provides necessary updates to allow a noncompliant computer to become compliant.
- **Ongoing compliance**: Automatically updates compliant computers so that they adhere to ongoing changes in health policy requirements.
Additional Reading

- Network Access Protection (NAP) for Windows Server 2008
How IPSec Enforcement Works

**Key Points of IPSec NAP Enforcement:**

- Comprised of a health certificate server and an IPSec NAP EC
- Health Certificate server issues X.509 certificates to quarantine clients when they are verified as compliant
- Certificates are then used to authenticate NAP clients when they initiate IPSec-secured communications with other NAP clients on an intranet
- IPSec Enforcement confines the communication on a network to those nodes that are considered compliant
- You can define requirements for secure communications with compliant clients on a per-IP address or a per-TCP/UDP port number basis

IPSec enforcement limits communication for IPSec-protected NAP clients by dropping incoming communication attempts that are sent from computers that cannot negotiate IPSec protection using health certificates. Unlike 802.1X and VPN enforcement, IPSec enforcement is performed by each individual computer, rather than at the point of entry into the network. Because you can take advantage of IPSec policy settings, the enforcement of health certificates can be done for all the computers in a domain, specific computers on a subnet, a specific computer, a specific set of Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) ports, or for a set of TCP or UDP ports on a specific computer.

IPSec enforcement defines the following logical networks:

- Secure network
- Boundary network
- Restricted network
Based on the definition of the three logical networks, the following types of initiated communications are possible:

- Computers in the secure network can initiate communications with computers in all three logical networks.
- Computers in the boundary network can initiate communications with computers in the secure or boundary networks that are authenticated with IPSec and health certificates or with computers in the restricted network that are not authenticated with IPSec.
- Computers in the restricted network can initiate communications with computers in the restricted and boundary networks.

**Question:** What types of computers in the secure network would you allow unsecure communication from computers in the restricted network to succeed?

**Answer:** IP filters can be created to allow certain communications to not be

**Additional Reading**

- Network Access Protection
IEEE 802.1X enforcement instructs an 802.1X-capable access point to use a limited access profile, either a set of IP packet filters or a VLAN ID, to limit the traffic of the noncompliant computer so that it can reach only resources on the restricted network. For IP packet filtering, the 802.1X-capable access point applies the IP packet filters to the IP traffic that is exchanged with the 802.1X client and silently discards all packets that do not correspond to a configured packet filter. For VLAN IDs, the 802.1X-capable access point applies the VLAN ID to all of the packets exchanged with the 802.1X client and the traffic does not leave the VLAN corresponding to the restricted network.

If the NAP client is noncompliant, the 802.1X connection has the limited access profile applied and the NAP client can only reach the resources on the restricted network.

**Question:** What must the network devices support to be able to implement 802.1x NAP?
Additional Reading

- Network Access Protection Platform Architecture
- Network Access Protection
How VPN Enforcement Works

Key Points of VPN NAP Enforcement:

- Computer must be compliant to obtain unlimited network access through a remote access VPN connection
- Noncompliant computers have network access limited through a set of IP packet filters that are applied to the VPN connection by the VPN server
- VPN enforcement actively monitors the health status of the NAP client and applies the IP packet filters for the restricted network to the VPN connection if the client becomes noncompliant

VPN enforcement consists of NPS in Windows Server 2008 and a VPN EC as part of the remote access client in Windows Vista, Windows XP with SP2 (with the NAP Client for Windows XP), and Windows Server 2008

VPN enforcement uses a set of remote access IP packet filters to limit the traffic of the VPN client so that it can only reach the resources on the restricted network. The VPN server applies the IP packet filters to the IP traffic that is received from the VPN client and silently discards all packets that do not correspond to a configured packet filter.

If the VPN client is noncompliant, the VPN connection has the packet filters applied, and the VPN client can only reach the resources on the restricted network.

**Question:** How does the VPN NAP enforcement method respond to non-compliant computers that make connection attempts?

**Additional Reading**

- Network Access Protection Platform Architecture
How DHCP Enforcement Works

DHCP address configuration limits network access for the DHCP client through its IPv4 routing table. DHCP enforcement sets the DHCP Router option value to 0.0.0.0, so the noncompliant computer does not have a configured default gateway. DHCP enforcement also sets the subnet mask for the allocated IPv4 address to 255.255.255.255, so that there is no route to the attached subnet.

To allow the noncompliant computer to access the remediation servers on the restricted network, the DHCP server assigns the Classless Static Routes DHCP option, which contains a set of host routes to the computers on the restricted network, such as the DNS and remediation servers.

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

Additional Reading
- Network Access Protection Platform Architecture
Lesson 3: Configuring NAP

- What Are System Health Validators?
- What is a Health Policy?
- What are Remediation Server Groups?
- NAP Client Configuration
- Demonstration: Using the Configure NAP Wizard to Apply Network Access Policies

This lesson provides information about configuring the client to interoperate with the server-side infrastructure of a NAP enforced environment.
What are System Health Validators?

System Health Validators are server software counterparts to system health agents

- Each SHA on the client has a corresponding SHV in NPS
- SHVs allow NPS to verify the statement of health made by its corresponding SHA on the client
- SHVs contain the required configuration settings on client computers
- The Windows Security SHV corresponds to the Microsoft SHA on client computers

Components of the NAP infrastructure known as system health agents (SHAs) and system health validators (SHVs) provide health state tracking and validation. Windows Vista and Windows XP Service Pack 3 include a Windows Security Health Validator SHA that monitors the settings of the Windows Security Center. Windows Server 2008 includes a corresponding Windows Security Health Validator SHV. NAP is designed to be flexible and extensible. It can interoperate with any vendor’s software that provides SHAs and SHVs that use the NAP API.

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

**Additional Reading**
- Network Access Protection Platform Architecture
- Introduction to Network Access Protection
What is a Health Policy?

Health policies consist of one or more system health validators (SHVs) and other settings that allow you to define client computer configuration requirements for the NAP-capable computers that attempt to connect to your network.

Question: Can you only use one System Health Validator (SHV) in a health policy?

Additional Reading
• Help Topic: Health Policies
What are Remediation Server Groups?

A remediation server group is a list of servers on the restricted network that provide resources required to bring noncompliant NAP-capable clients into compliance with administrator-defined client health policy.

**Question:** What services might a remediation server offer to update anti-virus signatures?

**Additional Reading**
- Help Topic: Remediation Server Groups
Use the following basic guidelines when performing NAP client configuration:

- Some NAP deployments that use Windows Security Health Validator require that Security Center is enabled.

- The Network Access Protection service is required when you deploy NAP to NAP-capable client computers.

- You must also configure the NAP enforcement clients on the NAP-capable computers.

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

- Help Topic: Enable Security Center in Group Policy
- Help Topic: Enable the Network Access Protection Service on Clients
- Help Topic: Configure NAP Enforcement Clients
Demonstration: Using the Configure NAP Wizard to Apply Network Access Policies

In this demonstration, you will see how to:

- Create DHCP NAP policies
- Configure DHCP enforcement on the DHCP server
- Use the NAP Client Management snap-in to enable EC

Additional Reading

- Help Topic: Create NAP Policies with a Wizard
- Help Topic: Checklist: Configure NAP Enforcement for DHCP
Lesson 4: Monitoring and Troubleshooting NAP

- What is NAP Tracing?
- Configuring NAP Tracing
- Demonstration: Configuring Tracing

Because of the differing levels of technology and the expertise and prerequisites for each of the NAP enforcement methods, troubleshooting and monitoring the NAP structure is an important administrative task. Trace logs are available for NAP, but are disabled by default. These logs serve two purposes: troubleshooting and evaluating the health and security of the network.
What is NAP Tracing?

- **NAP tracing identifies NAP events and records them to a log file based on the one of the following tracing levels:**
  - Basic
  - Advanced
  - Debug

- **You can use tracing logs to:**
  - Evaluate the health and security of your network
  - For troubleshooting and maintenance

- **NAP tracing is disabled by default, which means that no NAP events are recorded in the trace logs**

You can use NAP Client Configuration snap-in to configure NAP tracing. Tracing records NAP events in a log file and is useful for troubleshooting and maintenance. You can also use tracing logs to evaluate the health and security of your network. You can configure three levels of tracing: Basic, Advanced and Debug.

You should enable NAP tracing when:

- You are troubleshooting NAP problems.
- You want to evaluate the overall health and security of the computers in your organization.

**Additional Reading**

- Help and Support Topic: NAP tracing
Configuring NAP Tracing

There are two tools that are available for configuring NAP tracing. The NAP Client Configuration console is part of the Windows user interface, and `netsh` is a command-line tool.

To view the log files, navigate to the `%systemroot%\tracing\nap` directory and open the particular trace log that you want to view.

**Question:** What is the netsh command for enabling debug logging levels for NAP?

**Additional Reading**
- Help Topic: Enable and Disable NAP Tracing
- Help Topic: Specify Level of Detail in the NAP Trace Log
Demonstration: Configuring Tracing

In this demonstration, you will see how to:

- Configure tracing from the GUI
- Configure tracing from the command line
- View the log files

Question: What group must you be a member of to enable tracing for NAP?

Additional Reading

- Help Topic: Enable and Disable NAP Tracing
- Help Topic: Specify Level of Detail in the NAP Trace Log
Lab: Configuring NAP for DHCP and VPN

- Exercise 1: Configuring NAP for DHCP Clients
- Exercise 2: Configuring NAP for VPN Clients

Logon information

<table>
<thead>
<tr>
<th>Virtual machine</th>
<th>NYC-DC1, NYC-SVR1 and NYC-CL1</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Administrator</td>
</tr>
<tr>
<td>Password</td>
<td>Pa$$w0rd</td>
</tr>
</tbody>
</table>

Estimated time: 120 minutes

Objectives
- Configure NAP for DHCP clients
- Configure NAP for VPN clients

Logon Information
- Virtual Machines: 6421A-NYC-DC1, 6421A-NYC-SVR1, and 6421A-NYC-CL1
- User Name: WoodgroveBank\Administrator
- Password: Pa$$w0rd

Scenario
As the Woodgrove Bank Technology Specialist, you have been tasked with automatically bringing client computers into compliance by using Network Policy Server, creating client compliance policies and configuring a NAP server to check computers’ current health.
Exercise 1: Configuring NAP for DHCP Clients

In this exercise, you will configure and test NAP for DHCP clients.

The main tasks are as follows:

1. Ensure that you have completed the steps in the Lab Setup.
2. Open the Server Manager tool on 6421A-NYC-SVR1.
3. Install the DHCP and NPS server roles.
4. Configure NYC-SVR1 as a NAP health policy server.
5. Configure DHCP service for NAP enforcement.
6. Configure NYC-CL1 as a DHCP and NAP client.
7. Test NAP enforcement.
8. Shut down the virtual machines and do not save changes.

▶ Task 1: Ensure that you have completed the steps in the Lab Setup

- Review the Lab Setup section and ensure you have completed the steps before you continue with this lab.

▶ Task 2: Open the Server Manager tool on 6421A-NYC-SVR1

- On 6421A-NYC-SVR1, open Server Manager from the Administrative Tools menu.
Task 3: Install the NPS and DHCP server roles

1. On NYC-SVR1, open Server Manager.
2. Right-click Roles, and then click Add Roles.
4. On the Select Role Services page, select the Network Policy Server.
5. On the Select Network Connection Bindings page, verify that 10.10.0.24 is selected. Remove the check mark next to 192.168.1.10.
6. On the Specify DNS Server Settings page, verify that woodgrovebank.com is listed under Parent domain.
7. Type 10.10.0.10 under Preferred DNS server IP address, and click Validate. Verify that the result returned is Valid.
8. On the Specify WINS Server Settings page, accept the default setting.
9. On the Add or Edit DHCP Scopes page, click Add.
10. In the Add Scope dialog box, type NAP Scope next to Scope Name. Next to Starting IP Address, type 10.10.0.50, next to Ending IP Address type 10.10.0.199, and next to Subnet Mask type 255.255.0.0.
11. Select the Activate this scope check box, and then click OK.
12. On the Configure DHCPv6 Stateless Mode page, select Disable DHCPv6 stateless mode for this server.
13. On the Authorize DHCP Server page, select Use current credentials. Verify that Woodgrovebank\administrator is displayed next to Username, and then click Next.
15. Verify the installation was successful, and then click Close.
Task 4: Configure NYC-SVR1 as a NAP health policy server

1. Open the **Network Policy Server** administrative tool from the **Start Menu**, **Administrative Tools** location.

2. Configure SHVs:
   a. Expand **Network Access Protection**, and then click **System Health Validators**.
   b. Configure the System Health Validator. Clear all check boxes except **A firewall is enabled for all network connections**. You do not have to clear the **Windows Update** check box.

3. Configure remediation server groups:
   a. In the console tree, under **Network Access Protection**, right-click **Remediation Server Groups**, and then click **New**.
   b. Create a new remediation group with a group name of **Rem1** and add the IP address of **10.10.0.10**.

4. Configure health policies:
   a. Expand **Policies**.
   b. Right-click **Health Policies**, and then click **New**.
   c. Create a new health policy called **Compliant** that specifies the **Client passes all SHV checks** and uses the **Windows Security Health Validator**.
   d. Right-click **Health Policies**, and then click **New**.
   e. Create a new health policy called **NonCompliant** that specifies the **Client fails one or more SHV checks** and uses the **Windows Security Health Validator**.

5. Configure a network policy for compliant computers:
   a. In the console tree, under **Policies**, click **Network Policies**.
   b. Disable the two default policies under **Policy Name**.
   c. Create a new **Network Policy** called **Compliant-Full-Access**.
   d. In the **Specify Conditions** window, click **Add**.
   e. In the **Select condition** dialog box, double-click **Health Policies**, select **Compliant**, and then click **OK**.
8-42  Configuring Network Access Protection

f. In the **Specify Access Permission** window, verify that **Access granted** is selected.

g. In the **Configure Authentication Methods** window, select the **Perform machine health check only** check box. Clear all other check boxes.

h. In the **Configure Settings** window, click **NAP Enforcement**. Verify that **Allow full network access** is selected.

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

6. Configure a network policy for Noncompliant computers:

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

   b. Create a new **Network Policy** called **NonCompliant-Restricted**.

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

   d. In the **Select condition** dialog box, double-click **Health Policies**, select **Noncompliant**, and then click **OK**.

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

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

f. In the **Configure Authentication Methods** window, select the **Perform machine health check only** check box. Clear all other check boxes.

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

   h. In the **Configure Settings** window, click **NAP Enforcement**. Select **Allow limited access** and verify that **Enable auto-remediation of client computers** is selected.

   i. Click **Next**, and then click **Finish**. This completes configuration of your NAP network policies. Close the Network Policy Server console.
**Task 5: Configure DHCP service for NAP enforcement**

1. On NYC-SVR1, open the DHCP Management console by typing `dhcpmgmt.msc` in the Run box, and then pressing ENTER.

2. In the DHCP Management console, expand `NYC-SVR1.woodgrovebank.com`, and then expand IPv4.

3. Open the Properties for the Scope. On the Network Access Protection tab, verify Use default Network Access Protection profile is selected, and then click OK.

4. In the DHCP Management console, configure Scope Options.

5. On the Advanced tab, verify that Default User Class is chosen next to User class.

6. Under Available Options, select the 003 Router check box, type 10.10.0.1 in IP Address, select the 015 DNS Domain Name check box, type Woodgrovebank.com in String value, and then click OK. The Woodgrovebank.com domain is a full-access network assigned to compliant NAP clients.

7. In the DHCP Management console, configure Scope Options.

8. On the Advanced tab, next to User class, choose Default Network Access Protection Class.

9. Select the 006 DNS Servers check box, type 10.10.0.10 in IP Address, select the 015 DNS Domain Name check box, type restricted.Woodgrovebank.com in String value, and then click OK. The restricted.woodgrovebank.com domain is a restricted-access network assigned to noncompliant NAP clients.
Task 6: Configure NYC-CL1 as a DHCP and NAP client

1. On NYC-CL1, enable Security Center:
   a. Click Start, point to All Programs, click Accessories, and then click Run.
   b. Type gpedit.msc, and then press ENTER.
   d. Double-click Turn on Security Center (Domain PCs only), click Enabled, and then click OK.
   e. Close the console window. When prompted to save settings, click No.

2. Enable the DHCP enforcement client:
   a. Click Start, click All Programs, click Accessories, and then click Run.
   b. Type napclcfg.msc, and then press ENTER.
   c. In the console tree, click Enforcement Clients.
   d. Enable the DHCP Quarantine Enforcement Client.
   e. Close the NAP Client Configuration console.

3. Enable and start the NAP agent service:
   a. Click Start, point to All Programs, click Accessories, and then click Run.
   b. Type services.msc, and then press ENTER.
   c. In the services list, set Network Access Protection Agent Startup type to Automatic and start the service.
   d. Wait for the NAP agent service to start, and then click OK.
   e. Close the Services console.
4. Configure NYC-CL1 for DHCP address assignment:
   a. Click Start, and then click Control Panel.
   b. Click Network and Internet, click Network and Sharing Center, and then click Manage network connections.
   c. Configure Local Area Connection properties with the following:
      • Clear the Internet Protocol Version 6 (TCP/IPv6) check box.
      • Set properties of Internet Protocol Version 4 (TCP/IPv4) to Obtain an IP address automatically and Obtain DNS server address automatically.
   d. Click OK, and then click Close to close the Local Area Connection Properties dialog box.

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

Task 7: Test NAP Enforcement

1. Verify the DHCP assigned address and current Quarantine State:
   a. On NYC-CL1, open an administrative command prompt using the Run As Administrator command.
   b. At the command prompt, type ipconfig /all.
   c. Verify that the connection-specific DNS suffix is Woodgrovebank.com and the Quarantine State is Not Restricted.

2. Configure the System Health Validator policy to require antivirus software:
   a. On NYC-SVR1, in the Network Policy Server console, open NPS (Local), open Network Access Protection, and then open System Health Validators.
   b. Configure Windows Security Health Validator so that Virus Protection is set to An antivirus application is on.
   c. Click OK, and then click OK again to close the Windows Security Health Validator Properties window.
3. Verify the restricted network on NYC-CL1:
   a. On NYC-CL1, open an administrative command prompt using the Run As Administrator command.
   b. At the command prompt, type `ipconfig /release`.
   c. At the command prompt, type `ipconfig /renew`.
   d. Verify the connection-specific DNS suffix is now `restricted.woodgrovebank.com`.
   e. Close the command window and double-click the Network Access Protection icon in the system tray. Notice it tells you the computer is not compliant with requirements of the network.
   f. Click Close.

▶ Task 8: Shutdown virtual machines and do not save changes
   • Close all open windows, turn off all virtual machines and discard undo disks.
   • For Exercise 2, start NYC-DC1, NYC-SVR1 and NYC-CL1.
   • Log on to each as `WoodgroveBank\administrator` with a password of Pa$sw0rd.
Exercise 2: Configuring NAP for VPN Clients

In this exercise, you will configure NAP for VPN Clients. This exercise uses the Windows Security Health Agent and Windows Security Health Validator to require that client computers have Windows Firewall enabled and have an antivirus application installed.

You will create two network policies in this exercise. A compliant policy grants full network access to an intranet network segment. A noncompliant policy demonstrates network restriction by applying IP filters to the VPN tunnel interface that only allow client access to a single remediation server.

The main tasks are as follows:

1. Configure NYC-DC1 as an Enterprise Root CA
2. Configure NYC-SVR1 with NPS functioning as a health policy server
3. Configure NYC-SVR1 with the Routing and Remote Access service configured as a VPN server
4. Allow ping on NYC-SVR1
5. Configure NYC-CL1 as a VPN client and a NAP client
6. Close all virtual machines and discard undo disks.

- **Task 1: Configure NYC-DC1 as an Enterprise Root CA**

1. On NYC-DC1, click Start, point to Administrative Tools, and then click Server Manager.
2. Under Roles Summary, click Add Roles, and then click Next.
3. On the Before you Begin page, click Next.
4. Select the Active Directory Certificate Services check box and configure the wizard with the following:
   a. On the Specify Setup Type page, select Enterprise.
   b. On the Configure CA Name page, specify a name of Root CA.
   c. On the Confirm Installation Selections page, click Install.
5. On the Installation Results page, verify the installation succeeded, and then click Close.
6. Close the Server Manager window.
7. From the Administrative Tools menu, open the Certification Authority management tool.

8. Right-click Certificate Templates, and then choose Manage from the context menu.

9. Change the security on the Computer template to allow Authenticated Users the Enroll permission.


► Task 2: Configure NYC-SVR1 with NPS functioning as a health policy server

1. On NYC-SVR1, restart the server. After the computer restarts, log on as Woodgrovebank\administrator with a password of Pa$$w0rd.

2. Obtain a computer certificate on NYC-SVR1 for server-side PEAP authentication:
   a. Create a custom MMC console that includes the Certificates snap-in for Computer Account.
   b. In the console tree, double-click Certificates, right-click Personal, point to All Tasks, and then click Request New Certificate.
   c. The Certificate Enrollment dialog box opens. Click Next.
   d. Select the Computer check box, and then click Enroll.
   e. Verify the status of certificate installation as Succeeded, and then click Finish.
   f. Close the Console1 window.
   g. Click No when prompted to save console settings.

3. Install the NPS Server role:
   a. On NYC-SVR1, click Start, click Administrative Tools, and then click Server Manager.
   c. Verify the installation was successful, and then click Close.
   d. Close the Server Manager window.
4. Configure NPS as a NAP health policy server:
   a. Click **Start**, click **Run**, type **nps.msc**, and then press ENTER.
   b. Expand **Network Access Protection**, and then click **System Health Validators**.
   c. In the middle pane under **Name**, double-click **Windows Security Health Validator**.
   d. Configure the Windows Security Health Validator properties so all check boxes except **A firewall is enabled for all network connections** are cleared.
   e. Click **OK** to close the **Windows Security Health Validator** dialog box, and then click **OK** to close the **Windows Security Health Validator Properties** dialog box.

5. Configure health policies:
   a. Expand **Policies**.
   b. Create a new health policy called **Compliant**.
   c. Under **Client SHV checks**, verify that the **Client passes all SHV checks** check box is selected.
   d. Under **SHVs used in this health policy**, select the **Windows Security Health Validator** check box.
   e. Click **OK**.
   f. Create a new health policy called **Noncompliant**.
   g. Under **Client SHV checks**, select **Client fails one or more SHV checks**.
   h. Under **SHVs used in this health policy**, select the **Windows Security Health Validator** check box.
   i. Click **OK**.

6. Configure network policies for compliant computers:
   a. Expand **Policies**.
   b. Click **Network Policies**.
   c. Disable the two default policies under **Policy Name**.
   d. Create a new network policy called **Compliant-Full-Access**.
   e. In the **Specify Conditions** window, click **Add**.
f. In the **Select condition** dialog box, double-click **Health Policies**.

g. In the **Health Policies** dialog box, under **Health policies**, select **Compliant**.

h. In the **Specify Access Permission** window, verify that **Access granted** is selected.

i. In the **Configure Settings** window, click **NAP Enforcement**. Verify that **Allow full network access** is selected.

j. In the **Completing New Network Policy** window, click **Finish**.

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

   **Important:** A setting of **Access granted** does not mean that noncompliant clients are granted full network access. It specifies that clients matching these conditions should continue to be evaluated by the policy.

   g. In the **Configure Settings** window, click **NAP Enforcement**. Select **Allow limited access** and select **Enable auto-remediation of client computers**.

   h. In the **Configure Settings** window, click **IP Filters**.

   i. Under **IPv4**, create a new input filter for **Destination network** with the following values:
      - IP address: 10.10.0.10
      - Subnet mask: 255.255.255.255

This step ensures that traffic from noncompliant clients can only reach DC1.
j. Click OK to close the Add IP Filter dialog box, and then select Permit only the packets listed below in the Inbound Filters dialog box.

k. Under IPv4, create a new outbound filter with the following source network values:
   - IP address: 10.10.0.10
   - Subnet mask: 255.255.255.255

l. Click OK to close the Add IP Filter dialog box, and then select Permit only the packets listed below in the Outbound Filters dialog box. This step ensures that only traffic from DC1 can be sent to noncompliant clients.

m. In the Completing New Network Policy window, click Finish.

8. Configure connection request policies:
   a. Click Connection Request Policies.
   b. Disable the default CRP found under Policy Name.
   c. Create a new Connection Request policy called VPN connections.
   d. Under Type of network access server, select Remote Access Server (VPN-Dial up).
   e. In the Specify Conditions window, click Add.
   f. In the Select Condition window, double-click Tunnel Type, select PPTP and L2TP, and then click OK.
   g. In the Specify Connection Request Forwarding window, verify that Authenticate requests on this server is selected.
   h. In the Specify Authentication Methods window, select Override network policy authentication settings.
   i. Under EAP Types, click Add. In the Add EAP dialog box, under Authentication methods, click Microsoft: Protected EAP (PEAP).
   j. Under EAP Types, click Add. In the Add EAP dialog box, under Authentication methods, click Microsoft: Secured password (EAP-MSCHAP v2).
   k. Under EAP Types, click Microsoft: Protected EAP (PEAP), and then click Edit.
1. Verify that **Enable Quarantine checks** is selected, and then click **OK**.

m. Click **Next** twice, and then click **Finish**.

**Task 3: Configure NYC-SVR1 with the Routing and Remote Access service configured as a VPN server**

1. Click **Start**, click **Run**, type `rrasmgmt.msc`, and then press **ENTER**.

2. In the **Routing and Remote Access management** console, configure and enable Routing and Remote Access with the role **Remote access (dial-up or VPN)**.

3. Select the **VPN** check box, and then click **Next**.

4. Click the network interface with an IP address of **192.168.1.10**. Clear the **Enable security on the selected interface by setting up static packet filters** check box, and then click **Next**. This ensures that NYC-SVR1 will be able to ping NYC-DC1 when attached to the Internet subnet without having to configure additional packet filters for ICMP traffic.

5. On the **IP Address Assignment** page, select **From a specified range of addresses**, and on the **Address Range Assignment** page, specify a range of **10.10.0.100** to **10.10.0.110**.

6. On the **Managing Multiple Remote Access Servers** page, select **No, use Routing and Remote Access to authenticate connection requests**.

7. Click **Next**, and then click **Finish**.

8. Click **OK**, and wait for the Routing and Remote Access service to start.

9. Open the Network Policy Server console from the **Administrative Tools** menu, expand **Policies**, select **Connection Request Policies**, and then disable the **Microsoft Routing and Remote Access Service Policy** by right-clicking the policy and choosing **Disable**.

▶ Task 4: Allow ping on NYC-SVR1
1. Click Start, click Administrative Tools, and then click Windows Firewall with Advanced Security.
2. Create a custom inbound rule for All Programs with the protocol type of ICMPv4 and ICMP type of Echo Request for the default scope options.
3. In the Action window, verify that Allow the connection is selected, and then click Next.
4. Click Next to accept the default profile.
5. In the Name window, under Name, type ICMPv4 echo request, and then click Finish.

▶ Task 5: Configure NYC-CL1 as a VPN client and a NAP client
1. Configure NYC-CL1 so that Security Center is always enabled:
   a. Open the Local Group Policy Object Editor using the Run command with gpedit.msc.
   c. Double-click Turn on Security Center (Domain PCs only), click Enabled, and then click OK.
   d. Close the Local Group Policy Object Editor console.
2. Enable the remote access quarantine enforcement client:
   a. Launch the NAP Client Configuration tool using the Run command with napclcfg.msc.
   b. Enable the Remote Access Quarantine Enforcement Client.
   c. Close the NAP Client Configuration window.
3. Enable and start the NAP agent service:
   a. Open the Services console using services.msc in the Run command.
   b. In the Services list, double-click Network Access Protection Agent.
   c. Change the startup type to Automatic, and then click Start.
   d. Wait for the NAP agent service to start, and then click OK.
   e. Close the Services console.

4. Configure NYC-CL1 for the Internet network segment:
   a. Configure Local Area Connection Properties with Internet Protocol Version 4 (TCP/IPv4) set for the following:
      • IP address: 192.168.1.20
      • Subnet mask: 255.255.255.0
      • Remove Preferred DNS server setting of 10.10.0.10
   b. Click OK, and then click Close to close the Local Area Connection Properties dialog box.
   c. Close the Network Connections window.

5. Verify network connectivity for NYC-CL1:
   a. Open a command prompt and type ping 192.168.1.10.
   b. Verify that the response reads “Reply from 192.168.1.10.”
   c. Close the command window.

6. Configure a VPN connection:
   a. Using the Network and Sharing Center, create a new Connect to a workplace with the Use my Internet Connection (VPN) option.
   b. Click I’ll set up an Internet connection later.
   c. On the Type the Internet address to connect to page, next to Internet address, type 192.168.1.10. Next to Destination name, type Woodgrovebank. Select the Allow other people to use this connection check box, and then click Next.
   d. On the Type your user name and password page, type administrator next to User name, and type the password for the administrator account next to Password. Select the Remember this password check box, type Woodgrovebank next to Domain (optional), and then click Create.
e. In the Network and Sharing Center window, click Manage Network Connections.

f. Under Virtual Private Network, right-click the Contoso connection, click Properties, and then click the Security tab.

g. Select Advanced (custom settings), and then click Settings.

h. Under Logon security, select Use Extensible Authentication Protocol (EAP), and then choose Protected EAP (PEAP) (encryption enabled).

i. Click Properties.

j. Select the Validate server certificate check box. Clear the Connect to these servers check box, and then select Secured Password (EAP-MSCHAP v2) under Select Authentication Method. Clear the Enable Fast Reconnect check box, and then select the Enable Quarantine checks check box.

k. Click OK three times to accept these settings.

7. Test the VPN connection:

a. In the Network Connections window, use the Woodgrovebank connection object to initiate the VPN connection.

b. Verify that administrator account credentials are entered and that the Save this user name and password for future use check box is selected, and then click OK.

c. You are presented with a Validate Server Certificate window the first time this VPN connection is used. Click View Server Certificate, and verify Certificate Information states that the certificate was issued to NYC-SVR1.Woodgrovebank.com by Root CA. Click OK to close the Certificate window, and then click OK again.

d. Wait for the VPN connection to be made. Because NYC-CL1 is compliant, it should have unlimited access to the intranet subnet.

e. Open a command prompt and type `ipconfig /all` to view the configuration.

f. View the IP configuration. System Quarantine State should be Not Restricted.

The client now meets the requirement for VPN full connectivity.

g. Disconnect from the Woodgrovebank VPN.
8. Configure Windows Security Health Validator to require an antivirus application:
   b. Expand **Network Access Protection**, and then click **System Health Validators**.
   c. Configure the Windows Security Health Validator to require virus protection by selecting the check box next to **An antivirus application is on**.
   d. Click **OK**, and then click **OK** again to close the **Windows Security Health Validator Properties** window.

9. Verify the client is placed on the restricted network:
   a. On NYC-CL1, in the **Network Connections** window, right-click the **Woodgrovebank** connection, and then click **Connect**.
   b. Wait for the VPN connection to be made. You might see a message in the notification area that indicates the computer does not meet health requirements. This message is displayed because antivirus software has not been installed.
   c. Open a command prompt and type **ipconfig /all** to view the IP Configuration. **System Quarantine State** should be **Restricted**.
   
   The client does not meet the requirements for the network and therefore is put on the restricted network.
   
   Try to ping **10.10.0.24**. This should be unsuccessful.
   
   Try to ping **10.10.0.10**. This is the only server that the policy allows access to.
   
   d. Disconnect from **Woodgrovebank** VPN.

**Task 6: Close all virtual machines and discard undo disks**

1. On the host computer, click **Start**, point to **All Programs**, point to **Microsoft Virtual Server**, and then click **Virtual Server Administration Website**.

2. Under **Navigation**, click **Master Status**. For each virtual machine that is running, click the **virtual machine name**, and in the context menu, click **Turn off Virtual Machine and Discard Undo Disks**. Click **OK**.
Module Review and Takeaways

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

Consider the following best practices when implementing NAP:

- Use strong enforcement methods (IPSec, 802.1x and VPN). Strong enforcement methods provide the most secure and effective NAP deployment.

- Do not rely on NAP to secure a network from malicious users. NAP is designed to help administrators maintain the health of the computers on the network, which in turn helps maintain the network’s overall integrity. NAP does not prevent an authorized user with a compliant computer from uploading a malicious program to the network or disabling the NAP agent.

- Use consistent NAP policies throughout the site hierarchy to minimize confusion. Configuring a NAP policy incorrectly may result in clients accessing the network when they should be restricted or valid clients being erroneously restricted. The more complicated your NAP policy design, the higher the risk of incorrect configuration.

- Do not rely on NAP as an instantaneous or real-time enforcement mechanism. There are inherent delays in the NAP enforcement mechanism. While NAP helps keep computers compliant over the long run, typical enforcement delays may be several hours or more due to a variety of factors, including the settings of various configuration parameters.
Tools
The following table describes the tools that you can use to configure NAP.

<table>
<thead>
<tr>
<th>Tool</th>
<th>Use For</th>
<th>Where to find it</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>Enable and configure the NAP service on client computers</td>
<td>Click Start, click Control Panel, click System and Maintenance, click Administrative Tools, and then click double-click Services.</td>
</tr>
<tr>
<td>Netsh nap</td>
<td>Using netsh, you can create scripts to automatically configure a set of Windows Firewall with Advanced Security settings, create rules and rules, monitor connections, and display the configuration and status of Windows Firewall with Advanced Security.</td>
<td>Open a command window with administrative rights and type netsh nap. You can type help to get a full list of available commands.</td>
</tr>
<tr>
<td>Group policy</td>
<td>Some NAP deployments that use Windows Security Health Validator require that Security Center is enabled.</td>
<td>Enable the Turn on Security Center (Domain PCs only) setting in the Computer Configuration, Administrative Templates, Windows Components, and Security Center sections of Group Policy.</td>
</tr>
<tr>
<td>Configure NAP with a wizard</td>
<td>Used to create the health policies, connection request policies, and Network Access Protection (NAP) with Network Policy Server.</td>
<td>Open the NPS (Local) console. In Getting Started and Standard Configuration, select Network Access Protection (NAP) policy server. The text and links below the text change to reflect your selection. Click Configure NAP with a wizard.</td>
</tr>
</tbody>
</table>
Module 9

**Configuring IPsec**

**Contents:**

<table>
<thead>
<tr>
<th>Lesson</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lesson 1: Overview of IPsec</td>
<td>9-3</td>
</tr>
<tr>
<td>Lesson 2: Configuring Connection Security Rules</td>
<td>9-11</td>
</tr>
<tr>
<td>Lesson 3: Configuring IPsec NAP Enforcement</td>
<td>9-21</td>
</tr>
<tr>
<td>Lab: Configuring IPsec</td>
<td>9-26</td>
</tr>
</tbody>
</table>
Module Overview

- Overview of IPsec
- Configuring Connection Security Rules
- Configuring IPsec NAP Enforcement

Internet Protocol security (IPsec) is a framework of open standards for protecting communications over Internet Protocol (IP) networks through the use of cryptographic security services. IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. The Microsoft implementation of IPsec is based on standards developed by the Internet Engineering Task Force (IETF) IPsec working group.

IPsec is supported by the Microsoft Windows Vista, Windows Server 2008, Windows Server 2003, Microsoft Windows XP, and Windows 2000 operating systems and is integrated with the Active Directory directory service. IPsec policies can be assigned through Group Policy, which allows IPsec settings to be configured at the domain, site, or organizational unit level.
Lesson 1
Overview of IPsec

- Benefits of IPsec
- Recommended Uses of IPsec
- Tools Used to Configure IPsec
- What are Connection Security Rules?
- Demonstration: Configuring General IPsec Settings

IPsec is a set of protocols for helping to protect data over a network using security services and digital certificates with public and private keys. (A digital certificate assigns a public key to a person, a business, or a website.)

Because of its design, IPsec helps provide much better security than previous protection methods. Network administrators who use it don’t have to configure security for individual programs.
Benefits of IPsec

**IPsec** is a suite of protocols that allows secure, encrypted communication between two computers over an unsecured network.

- IPsec has two goals: to protect IP packets and to defend against network attacks.
- Configuring IPsec on sending and receiving computers enables the two computers to send secured data to each other.
- IPsec secures network traffic by using encryption and data signing.
- An IPsec policy defines the type of traffic that IPsec examines, how that traffic is secured and encrypted, and how IPsec peers are authenticated.

IPsec is typically used to attain confidentiality, integrity, and authentication in the transport of data across insecure channels.

IPsec provides the following benefits:

- Mutual authentication before and during communications.
- IPsec forces both parties to identify themselves during the communication process.
- Confidentiality through encryption of IP traffic and digital authentication of packets.

IPsec has two modes:

- Encapsulating Security Payload (ESP). Provides encryption by using one of a few different algorithms.
- Authentication Header (AH). Signs the traffic but does not encrypt it.
Additional Reading

- IPsec
Recommended Uses of IPsec

Some network environments are well suited to IPsec as a security solution and others are not. IPsec is recommended for the following uses:

- Packet filtering
- Securing host-to-host traffic on specific paths
- Securing traffic to servers
- Layer 2 Tunneling Protocol (L2TP)/IPsec for VPN connections
- Site-to-site (gateway-to-gateway) tunneling
- Enforcing logical networks

IPsec is not recommended for the following uses:

- Securing communication between domain members and their domain controllers
- Securing all traffic in a network
Additional Reading
- Overview of IPsec Deployment
- Windows Server 2008 Technical Library
Tools used to Configure IPsec

To configure IPsec, you can use:

- Windows Firewall with Advanced Security MMC (used for Windows Server 2008 and Windows Vista)
- IP Security Policy MMC (Used for mixed environments and to configure policies that apply to all Windows versions)
- Netsh command-line tool

There are several ways to configure Windows Firewall and IPsec settings and options, including the following:

- Using the Windows Firewall with Advanced Security Microsoft Management Console (MMC) snap-in
- Using the IP Security Policy MMC snap-in
- Using Netsh commands

Additional Reading

- Windows Firewall with Advanced Security Help Topic: Windows Firewall with Advanced Security
What are Connection Security Rules?

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

Firewall rules allow traffic through the firewall, but do not secure that traffic. To secure traffic with IPsec, you can create Computer Connection rules. However, the creation of a connection security rule does not allow the traffic through the firewall. You must create a firewall rule to do this, if the traffic is not allowed by the default behavior of the firewall. Connection security rules are not applied to programs and services. They are applied between the computers that make up the two endpoints.

Additional Reading

- Introduction to Windows Firewall with Advanced Security
- Windows Firewall with Advanced Security Help Topic: Connection Security Rules
Demonstration: Configuring General IPsec Settings

In this demonstration, you will see how to configure General IPsec settings in Windows Firewall with Advanced Security.
Lesson 2
Configuring Connection Security Rules

- Choosing a Connection Security Rule Type
- What are Endpoints?
- Choosing Authentication Requirements
- Authentication Methods
- Determining a Usage Profile
- Demonstration: Configuring a Connection Security Rule

You can use Connection Security rules to configure IPsec settings for specific connections between this computer and other computers. Windows Firewall with Advanced Security uses the rule to evaluate network traffic and then blocks or allows messages based on the criteria you establish in the rule. Under some circumstances Windows Firewall with Advanced Security will block the communication. If you have configured a settings that requires security for a connection (in either direction), and the two computers cannot authenticate each other, the connection will be blocked.
Choosing a Connection Security Rule Type

<table>
<thead>
<tr>
<th>Rule Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Isolation</td>
<td>Restricts connections based on authentication criteria that you define</td>
</tr>
</tbody>
</table>
| Authentication Exemption | • Exempts specific computers or a group or range of IP addresses from being required to authenticate.  
|                  | • Used to grant access to infrastructure computers that this computer must communicate with before authentications can be performed |
| Server-to-Server | Authenticates two specific computers, two groups of computers, two subnets, a specific computer and a group of computers or subnet |
| Tunnel          | Provides secure communications between two peer computers through tunnel endpoints (VPN or L2TP IPsec tunnels) |
| Custom          | Used rule to create a rule with special settings                            |

You can use the New Connection Security Rule wizard to create rules for the way in which Windows Firewall with Advanced Security authenticates the computers and users that match the rule criteria. Windows Firewall with Advanced Security uses IPsec to protect traffic using the settings in these rules.

The wizard provides four predefined types of rules. You can also create a custom rule that you can configure to suit your security needs.

- Isolation
- Authentication exemption
- Server-to-server
- Tunnel
- Custom
Additional Reading

- Windows Firewall with Advanced Security Help Topic: Choosing a Connection Security Rule Type
What are Endpoints?

Computer endpoints are the computers or the group of computers that form peers for the connection.

IPsec tunnel mode provides the protection of an entire IP packet by treating it as an AH or ESP payload. With tunnel mode, an entire IP packet is encapsulated with an AH or ESP header and an additional IP header. The IP addresses of the outer IP header are the tunnel endpoints, and the IP addresses of the encapsulated IP header are the ultimate source and destination addresses.

ESP encrypts packets and applies a new non-encrypted header to facilitate routing. Beyond providing encryption,

ESP functions in two modes:

- Transport mode
- Tunnel mode
Additional Reading
- Windows Firewall with Advanced Security Help Topic: Computer Endpoints
- Windows Firewall with Advanced Security Help Topic: Specify Tunnel Endpoints
Choosing Authentication Requirements

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Authentication for inbound and outbound connections</td>
<td>Ask that all inbound/outbound traffic be authenticated, but allow the connection if authentication fails</td>
</tr>
</tbody>
</table>
| Require authentication for inbound connections and request authentication for outbound connections | - Require inbound be authenticated or it will be blocked
- Outbound can be authenticated but will be allowed if authentication fails |
| Require authentication for inbound and outbound connections            | Require that all inbound/outbound traffic be authenticated or the traffic will be blocked |

While using the Connection Security Rule wizard to create a new rule, you can use the Authentication Requirements page of the wizard to specify how authentication is applied to inbound and outbound connections. Requesting authentication allows the communications when authentication fails; requiring authentication causes the connection to be dropped if authentication fails.

Additional Reading
- Windows Firewall with Advanced Security Help Topic: Authentication Requirements
Authentication Methods

<table>
<thead>
<tr>
<th>Method</th>
<th>Key Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Use the authentication method configured on the IPsec Settings tab</td>
</tr>
<tr>
<td>Computer and User (Kerberos V5)</td>
<td>You can request or require both the user and computer authenticate before communications can continue; Domain membership required</td>
</tr>
<tr>
<td>Computer (Kerberos V5)</td>
<td>Request or require the computer to authenticate using Kerberos V5</td>
</tr>
<tr>
<td>User (Kerberos V5)</td>
<td>Request or require the user to authenticate using Kerberos V5; Domain membership required</td>
</tr>
<tr>
<td>Computer certificate</td>
<td>• Request or require a valid computer certificate, requires at least one CA</td>
</tr>
<tr>
<td></td>
<td>• Only accept health certificates: Request or require a valid health certificate to authenticate, requires IPsec NAP</td>
</tr>
<tr>
<td>Advanced</td>
<td>Configure any available method; You can specify methods for First and Second Authentication</td>
</tr>
</tbody>
</table>

The Connection Security Rule wizard has a page where you can configure the Authentication Method to configure the credential used for authentication. If the rule already exists, you can use the Authentication tab of the Connection Security Properties dialog box of the rule you wish to edit.

Additional Reading

- Windows Firewall with Advanced Security Help Topic: Authentication methods
## Determining a Usage Profile

A firewall profile is a way of grouping settings, such as firewall rules and connection security rules that are applied to the computer depending on where the computer is connected. On computers running this version of Windows, there are three profiles for Windows Firewall with Advanced Security. Only one profile is applied at a time.

<table>
<thead>
<tr>
<th>Security Settings can change dynamically with the network location type</th>
</tr>
</thead>
</table>

### Windows supports three network types, and programs can use these locations to automatically apply the appropriate configuration options:

- **Domain**: selected when the computer is a member of the domain
- **Private**: networks trusted by the user (home or small office network)
- **Public**: default for newly detected networks, usually the most restrictive settings are assigned because of the security risks present on public networks

### The network location type is most useful on portable computers which are likely to move from network to network

---

BETA COURSEWARE. EXPIRES 4/11/2008
The following table describes the available usage profiles:

<table>
<thead>
<tr>
<th>Profile</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Applied when a computer is connected to a network in which the computer’s domain account resides.</td>
</tr>
<tr>
<td>Private</td>
<td>Applied when a computer is connected to a network in which the computer’s domain account does not reside, such as a home network. The private settings should be more restrictive than the domain profile settings.</td>
</tr>
<tr>
<td>Public</td>
<td>Applied when a computer is connected to a domain through a public network, such as those available in airports and coffee shops. The public profile settings should be the most restrictive because the computer is connected to a public network where the security cannot be as tightly controlled as within an IT environment.</td>
</tr>
</tbody>
</table>

Additional Reading

- Windows Firewall with Advanced Security Help Topic: Firewall Properties - Profiles
- Windows Firewall with Advanced Security
Demonstration: Configuring a Connection Security Rule

In this demonstration, you will see how to configure a Connection Security rule
Lesson 3
IPsec NAP Enforcement

- IPsec Enforcement for Logical Networks
- IPsec NAP Enforcement Processes
- Requirements to Deploy IPsec NAP Enforcement

Network Access Protection (NAP) enforcement for IPsec policies for Windows Firewall is deployed with a health certificate server, a Health Registration Authority (HRA) server, a computer running Network Policy Server (NPS), and an IPsec enforcement client. The health certificate server issues X.509 certificates to NAP clients when they are determined to be compliant. These certificates are then used to authenticate NAP clients when they initiate IPsec communications with other NAP clients on an intranet.

IPsec enforcement confines the communication on your network to compliant clients, and provides the strongest implementation of NAP. Because this enforcement method uses IPsec, you can define requirements for secure communications on a per-IP address or per-TCP/UDP port number basis.
IPsec enforcement divides a physical network into three logical networks. A computer is a member of only one logical network at any time. The logical networks are defined in terms of which computers have health certificates and which computers require IPsec authentication with health certificates for incoming communication attempts. The logical networks allow for limited network access and remediation and provide compliant computers with a level of protection from noncompliant computers.

Additional Reading
- Network Access Protection Platform Architecture
- Network Policy Server Help Topic: NAP Enforcement for IPsec Communications
To obtain a health certificate and become a member of the secure network, a NAP client using IPsec enforcement starts up on the network and performs the IPsec enforcement NAP process.

The NAP client removes any existing health certificates, if necessary, and adds the newly-issued health certificate to its computer certificate store. The IPsec NAP EC configures IPsec settings to authenticate using the health certificate for IPsec-protected communications and configures the host-based firewall to allow incoming communications from any peer that uses a health certificate for IPsec authentication. The NAP client is now a member of the secure network.

If the NAP client is noncompliant, the NAP client does not have a health certificate and cannot initiate communication with computers in the secure network. The NAP client performs a remediation process to become a member of the secure network.

**Additional Reading**
- Network Access Protection Platform Architecture
- IPsec
Requirements to Deploy IPsec NAP Enforcement

To deploy NAP with IPsec and HRA, you must configure the following:

- In NPS, configure connection request policy, network policy, and NAP health policy. You can configure these policies individually using the NPS console, or you can use the new Network Access Protection wizard.
- Enable the NAP IPsec enforcement client and the NAP service on NAP-capable client computers.
- Install HRA on the local computer or on a remote computer.
- Install and configure Active Directory Certificate Services (AD CS) and certificate templates.
- Configure Group Policy and any other settings required for your deployment.
- Configure the Windows Security Health Validator (WSHV) or install and configure other system health agents (SHAs) and system health validators (SHVs), depending on your NAP deployment.
If HRA is not installed on the local computer, you must also configure the following:

- Install NPS on the computer that is running HRA.
- Configure NPS on the remote HRA NPS server as a RADIUS proxy to forward connection requests to the local NPS server

**Additional Reading**

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

- Exercise 1: Preparing the Network Environment for IPsec NAP Enforcement
- Exercise 2: Configuring and Testing IPsec NAP Enforcement

Logon information

<table>
<thead>
<tr>
<th>Virtual machines</th>
<th>NYC-DC1, NYC-CL1, NYC-CL2</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Administrator</td>
</tr>
<tr>
<td>Password</td>
<td>Pa$$w0rd</td>
</tr>
</tbody>
</table>

Estimated time: 60 minutes

Objectives:
- Prepare the network environment for IPsec NAP enforcement
- Configure and test IPsec enforcement

Lab Setup
For this lab you will use the available virtual machine environment. Before you begin the lab, you must:

- Start the NYC-DC1, NYC-CL1 and NYC-CL2 virtual machines.
- Log on to the NYC-DC1, NYC-CL1 and NYC-CL2 virtual machines with the user name administrator and the password Pa$$w0rd.
- On the computers running Windows Server 2008, close the Initial Configuration Tasks window that appears after log on.
Scenario
Due to recent security related incidents on the internal network, Woodgrove Bank wants to implement IPsec policies to mitigate security risks through encryption and use Network Access Protection to verify the health of communicating parties prior to data transmission. The Woodgrove Bank IS Manager wants you to configure an IPsec Network Access Protection enforcement environment to mitigate any related future network security issues.
Exercise 1: Preparing the Network Environment for IPsec NAP Enforcement

Exercise Overview
In this exercise, you will prepare the environment for IPsec NAP enforcement.
The main tasks are as follows:
1. Ensure that you have completed the steps in the Lab Setup.
2. Open the Server Manager tool on 6421A-NYC-DC1.
3. Install the NPS, HRA and CA server roles.
4. Configure HRA with permissions.
5. Configure CA properties on HRA.
6. Configure NPS as a NAP health policy server.
7. Configure system health validators.
9. Configure NYC-CL1 and NYC-CL2 so that Security Center is always enabled.
10. Enable the IPsec enforcement client and configure client health registration settings.
11. Configure and start the NAP Agent service.
12. Allow ICMP through Windows Firewall.

► Task 1: Ensure that you have completed the steps in the Lab Setup
• Review the Lab Setup section and ensure you have completed the steps before you continue with this lab.

► Task 2: Open the Server Manager tool on 6421A-NYC-DC1
• On 6421A-NYC-DC1, open Server Manager from the Administrative Tools menu.
Task 3: Install the NPS, HRA and CA server roles

1. In Server Manager, add the Network Policy and Access Services role.

2. On the Select Role Services page, select the Health Registration Authority check box, and then click Add Required Role Services.

3. Select Install a local CA to issue health certificates for this HRA server with the allow anonymous requests for health certificates option.

4. Select Don’t use SSL or Choose a certificate for SSL encryption later.

5. On the Select Role Services page, verify that only the Certification Authority check box is selected.

6. Install Certificate Services as a Standalone Root CA.

7. Accept the default private key and cryptographic settings.

8. Name the CA Woodgrovebank-RootCA.

9. Accept the default settings for the remainder of the settings and then click Install.

10. On the Installation Results page, notice that the Network Policy and Access Services installation succeeded with errors. This is because the CA was installed after the role was installed, so it could not be reached. Verify that all other installations were successful, and then click Close.

Task 4: Configure HRA with permissions

1. Open the Certification Authority administrative tool.

2. Open the properties of the RootCA from the list pane.

3. Click the Security tab, click to add the Network Service account, and select the Issue and Manage Certificates, Manage CA, and Request Certificates check boxes.

4. On the Policy Module tab, click Properties and select Follow the settings in the certificate template, if applicable. Otherwise, automatically issue the certificate.

5. Restart the Certification Authority.

6. Close the Certification Authority console.
**Task 5: Configure CA properties on HRA**

1. On NYC-DC1, create a custom MMC and add the Health Registration Authority snap-in.

2. In the Health Registration console, right-click Certificate Authority, and add WoodGroveBank-RootCA by clicking Add Certificate authority.

3. Click Certificate Authority and verify that `\NYC-DC1.Woodgrovebank.com\Woodgrovebank-RootCA` is displayed in the details pane.

4. Right-click Certification Authority in the list pane and open the Properties to verify that Use standalone certification authority is selected.

5. Close the Health Registration Authority console.

**Task 6: Configure NPS as a NAP health policy server**

1. On NYC-DC1, open the Network Policy Server console.

2. Under Standard Configuration, click Configure NAP.

3. On the Select Network Connection Method for Use with NAP page, select IPsec with Health Registration Authority (HRA).


5. On the Define NAP Health Policy page, verify that the Windows Security Health Validator and Enable auto-remediation of client computers check boxes are selected, and then click Finish on the Completing New Network Access Protection Policies and RADIUS clients page.

6. Leave the NPS console open for the following task.
### Task 7: Configure system health validators

1. In the NPS console tree, click **Network Access Protection**, and then click **Configure System Health Validators** in the details pane.

2. In the details pane, under **Name**, double-click **Windows Security Health Validator**.

3. Click **Configure**.

4. Clear all check boxes except **A firewall is enabled for all network connections**.

5. Click **OK** twice to close the **Windows Security Health Validator** and the **Windows Security Health Validator Properties** dialog boxes.

6. Close the NPS console.

### Task 8: Configure Certificate Auto Enrollment in Default Domain Group Policy

1. On NYC-DC1, open the **Group Policy Management** console.

2. Edit the **Default Domain Policy**.


4. Double-click **Certificate Services Client – Auto-Enrollment**.

5. In the **Define Policy Settings** dialog box set the following:
   - Configuration Model: **Enabled**
   - Select **Renew expired certificates, update pending certificates, and remove revoked certificates**
   - Select **Update certificates that use certificate templates**

6. Click **OK** and close the Group Policy Management Editor.

7. Close the **Group Policy Management** console.
Task 9: Configure NYC-CL1/NYC-CL2 so that Security Center is always enabled
1. Log on to NYC-CL1 as Woodgrovebank\administrator with a password of Pa$$w0rd.
2. Open the Local Group Policy Editor by typing gedit.msc in the Start Search text box.
4. Double-click Turn on Security Center (Domain PCs only), click Enabled, and then click OK.
5. Close the Local Group Policy Object Editor console.
6. Repeat steps 1 through 5 on NYC-CL2.

Task 10: Enable the IPsec enforcement client and configure client health registration settings
1. On NYC-CL1, open the NAP Client Configuration console by typing napclcfg.msc in the Start Search text box.
2. Enable IPsec Relying Party in the Enforcement Clients details pane.
3. In the NAP Client Configuration console tree, double-click Health Registration Settings.
4. Add two new Trusted Server Groups, select do not require server verification, and then click New.
5. Under Add URLs of the health registration authority that you want the client to trust, type http://nyc-dc1.woodgrovebank.com/domainhra/hcsrvext.dll, and then click Add. Type http://nyc-dc1.woodgrovebank.com/nondomainhra/hcsrvext.dll, click Add, and then Finish.
6. In the console tree, click Trusted Server Groups and verify that the URLs are entered correctly.
7. Close the NAP Client Configuration window.
8. Repeat steps 1 through 7 on NYC-CL2.
Task 11: Configure and start the NAP Agent service

1. On NYC-CL1, open the Services console and set the startup properties of Network Access Protection Agent Properties to Automatic and then start the service.
2. Wait for the NAP agent service to start, and then click OK.
3. Close the Services console.
4. Repeat steps 1 through 3 for NYC-CL2.

Task 12: Allow ICMP through the Windows Firewall

1. On NYC-CL1, click Start and in the Start Search text box, type wf.msc and then press ENTER.
2. Create a new Custom Inbound Rule for All programs that specifies ICMPv4 Echo Request that uses the default scope with the Action of Allow the connection. Accept the default profile and name the rule ICMPv4 Echo Request.
4. Repeat steps 1 through 3 on NYC-CL2.
**Exercise 2: Configuring and Testing IPsec NAP Enforcement**

**Exercise Overview**
In this exercise, you will configure and test IPsec NAP Enforcement.

The main tasks are as follows:
1. Create an IPsec Secure Organizational Unit in Active Directory.
2. Create IPsec policies for secure health enforcement.
3. Move NYC-CL1 and NYC-CL2 to the IPsec Secure OU.
4. Apply group policies.
5. Verify health certificate status.
6. Verify clients can communicate securely.
7. Demonstrate Network Restriction.
8. Close all virtual machines and discard undo disks.

▶ **Task 1: Create an IPsec Secure Organizational Unit in Active Directory**

1. On NYC-DC1, open *Active Directory Users and Computers* and create a new root level Organization Unit named *IPsec Secure*.
2. Leave the *Active Directory Users and Computers* console open.
**Task 2: Create IPsec policies for the IPsec Secure OU**

1. On NYC-DC1, open the Group Policy Management console.

2. Create and link a new Group Policy Object for the **IPsec Secure** OU and name the policy **Secure Policy**.

3. Edit the **Secure Policy** to create IPsec policies for all profile states.
   a. Open **Secure Policy [nyc-dc1.woodgrovebank.com] Policy\Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security** and open the properties of **Windows Firewall with Advanced Security – LDAP**.

   b. On the **Domain Profile** tab, next to **Firewall state**, select **On** *(recommended)*. Next to **Inbound connections**, select **Block** *(default)*. Next to **Outbound connections**, select **Allow** *(default)*. The same settings will be used for the private and public profiles.

4. In the **Group Policy Management Editor** console tree, under **Windows Firewall with Advanced Security - LDAP**, right-click **Connection Security Rules**, and create a new rule that has **Isolation** and **Require authentication for inbound connections and request authentication for outbound connections** selected.

5. On the **Authentication Method** page, select **Computer certificate**, select the **Only accept health certificates** check box, and specify **RootCA**.

6. On the **Profile** page, verify that the **Private**, **Public**, and **Domain** check boxes are selected. On the **Name** page type **Secure Rule**, and then click **Finish**.

7. Right-click **Inbound Rules**, and then create a new rule using the predefined **File and Printer Sharing** rule with only the **Allow the connection if it is secure** option.

8. Close the **Group Policy Management Editor** console.

**Task 3: Move NYC-CL1 and NYC-CL2 into the IPsec Secure OU**

1. On NYC-DC1, open **Active Directory Users and Computers**.

2. Open the **Computers** container, select **NYC-CL1** and **NYC-CL2** and drag and drop into the **IPsec Secure** OU.

3. Close the **Active Directory Users and Computers** console.
Task 4: Apply group policies
1. On NYC-CL1 and NYC-CL2, use `gpupdate /force` to reapply the changed Group Policy settings.
2. Verify that the response reads **User Policy update has completed successfully** and Computer Policy update has completed successfully.
3. Leave the command windows open for the following procedures.

Task 5: Verify Health certificate status
1. On NYC-CL1, create a custom MMC tool that includes the **Certificates** snap-in with **Computer account** certificates specified for the **Local Computer**.
2. In the MMC console tree, double-click **Certificates (Local Computer)**, double-click **Personal**, and then click **Certificates**. In the details pane, under **Issued By**, verify that **WoodGroveBank-RootCA** is displayed. Verify that **Intended Purposes** shows **System Health Authentication**.
3. Close the MMC console and do not save changes.

Task 6: Verify clients can communicate securely
1. On NYC-CL1, click **Start**, in the **Start Search** text box, type `\NYC-CL2\` and then press ENTER.
2. Confirm that the command completed successfully.
3. Verify that you can view the contents of the share.
5. In the **Windows Firewall with Advanced Security** console list pane, expand **Monitoring**, expand **Security Associations** and select **Main Mode**.
6. In the details pane, you should see an entry for secure communications between NYC-CL1 and NYC-CL2. Double-click the entry and review at the contents of the **General** tab. You should see **Computer certificate for First Authentication**, **Encryption using AES-128** and **Integrity accomplished using SHA1**.
7. Close the dialog box, close **Windows Firewall with Advanced Security**.
Task 7: Demonstrate Network Restriction

**Note:** Automatic updates will be required for NAP compliance by enabling this system health check in the Windows Security Health Validator.

1. On NYC-DC1, open **Network Access Protection**, and then click **System Health Validators**.
2. Configure the **Windows Security Health Validator**, under **Automatic Updating**, select the **Automatic updating is enabled** check box, and then click **OK** twice.

**Note:** To demonstrate network restriction of noncompliant clients, auto-remediation of client computers must be disabled in the noncompliant network policy.

3. In the **Network Policy Server** console tree, click **Network Policies**.
4. In the details pane, double-click **NAP IPsec with HRA Noncompliant**.
5. Click the **Settings** tab, click **NAP Enforcement**, clear the **Enable auto-remediation of client computers** check box, and then click **OK**.
6. Close the **Network Policy Server** console.
7. On NYC-CL1, in the command window, type **ping -t NYC-CL2**, and then press ENTER. A continuous ping will run from NYC-CL1 to NYC-CL2. This should be successful.
8. On NYC-CL2, on the **Security** control panel, select **Turn automatic updating on or off**, select **Never check for updates (not recommended)**, and then click **OK**. This setting causes NYC-CL2 to be noncompliant with network health policy. Because auto-remediation has been disabled, NYC-CL2 will remain in a noncompliant state and will be placed on the restricted network.

**Note:** Do not close the Security control panel on NYC-CL2. It will be used to re-enable Windows Update in a step to follow.
9. On NYC-CL1, verify that the response in the command window has changed to Request timed out.

10. On NYC-CL1, click Start, and in the Start Search text box, type \NYC-CL2\ and verify the share is inaccessible.

11. On NYC-CL2, in the Security control panel under Windows Update, click Turn automatic updating on or off, select Install updates automatically (recommended), and then click OK. This setting will cause NYC-CL2 to send a new SoH that indicates it is compliant with network health requirements, and NYC-CL2 will be granted full network access.

12. On NYC-CL1, verify that the response in the command window changes to Reply from 10.10.0.60. It might take a minute before you see the change in status.

13. Verify that you can browse the share of NYC-CL2 (\NYC-CL2\).

14. Close all open windows.

▶ Task 8: Close all virtual machines and discard undo disks

1. On the host computer, click Start, point to All Programs, point to Microsoft Virtual Server, and then click Virtual Server Administration Website.

2. Under Navigation, click Master Status. For each virtual machine that is running, click the virtual machine name, and in the context menu, click Turn off Virtual Machine and Discard Undo Disks. Click OK.
Module Review and Takeaways

- Review Questions
- Common Misconceptions About IPsec
- IPsec Benefits
- Tools

**Review Questions**

1. What is the difference between the ESP protocol and the AH protocol when using IPsec?

2. What encryption algorithms are available for the ESP protocol in Windows Server 2008?

3. If you need secure communications to a particular domain server and must support connections from both domain and non-domain computers, and you want only a single authentication method, what authentication method would be best suited for this scenario?

4. Is it possible for a computer in the restricted logical network to access resources on a server in the secure logical network?

5. What types of computers would you typically find within the restricted logical network in an IPsec NAP environment?
Common Misconceptions About IPsec

The most common misconceptions about IPsec are:

- **IPsec is a virtual private network (VPN) technology.**

  Although IPsec is used for VPN connections across the Internet to connect remote clients to an intranet or remote sites to each other, IPsec was designed to protect both intranet and Internet traffic in a variety of scenarios.

  When using IPsec to protect IP traffic that is sent across the Internet, some VPN implementations use an additional mode of AH and ESP known as tunnel mode, in which an entire IP packet is encapsulated and protected. Computers running Windows Server 2008, Windows Vista, Windows Server 2003, or Windows XP can use Layer Two Tunneling Protocol (L2TP) with IPsec (L2TP/IPsec) for VPN connections. However, L2TP/IPsec does not use tunnel mode. Instead, L2TP provides encapsulation for an entire IP packet and the resulting IP packet payload is protected with ESP and encryption.

- **Using IPsec requires encryption.**

  IPsec only encrypts IP packet payloads when you choose to use ESP with encryption. Encryption is optional but recommended in many circumstances, including when sending private data across a public network (such as the Internet) or when sending highly sensitive data across an intranet (such as personal or financial data).

IPsec Benefits

IPsec support in Windows provides the following benefits:

- **Defense-in-depth against vulnerabilities in upper-layer protocols and applications.**

  IPsec protects upper layer protocols, services, and applications. With IPsec enabled, initial communication packets to access an application or service running on a server, for example, will not be passed to the application or service until trust has been established through IPsec authentication and the configured protection on packets for the application or service has been applied. Therefore, attempts to attack applications or services on servers must first penetrate IPsec protection.
IPsec offers no inbound application layer protocol protection to an authenticated peer. However once an application layer protocol session is encrypted between two peers using IPsec, it is protected from replay and Man-in-the-middle type attacks.

- Requiring peer authentication prevents communication with untrusted or unknown computers.
  
  IPsec security requires peers to authentication their computer-level credentials prior to sending any IP-based data. By requiring peer authentication using credentials based on a common trust model, such as membership in an Active Directory domain, untrusted or unknown computers cannot communicate with domain members. This helps protect domain member computers from the spread of some types of viruses and worms being propagated by untrusted or unknown computers.

- IP-based network traffic is cryptographically protected.
  
  IPsec provides a set of cryptographic protections for IP-based traffic based on your choice of AH, ESP without encryption, or ESP with encryption. Your IP-based network traffic is either tamper proofed (using AH or ESP with no encryption) or tamper proofed and encrypted (with ESP and encryption). Requiring cryptographic protection of IP traffic helps prevent many types of network attacks.

- Applications do not need to be changed to support IPsec.
  
  IPsec is integrated at the Internet layer of the TCP/IP protocol suite, providing security for all IP-based protocols in the TCP/IP suite. With IPsec, there is no need to configure separate security for each application that uses TCP/IP. Instead, applications that use TCP/IP pass the data to IP in the Internet layer, where IPsec can secure it. By eliminating the need to modify applications, IPsec can save application development time and costs.
## Tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Use For</th>
<th>Where to find it</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Firewall with Advanced Security MMC</td>
<td>Full control over firewall rules and IPsec properties on a single computer</td>
<td>Click Start, and point to Administrative Tools. Select the Windows Firewall with Advanced Security tool from the available administrative tools.</td>
</tr>
<tr>
<td>Netsh advfirewall</td>
<td>You can use the netsh command to create scripts that automatically configure Windows Firewall with Advanced Security settings, create rules, monitor connections, and display the configuration and status of Windows Firewall with Advanced Security.</td>
<td>Open a command window with administrative rights and type Netsh advfirewall. You can type help to get a full list of available commands.</td>
</tr>
<tr>
<td>Group policy</td>
<td>Group Policy provides access to the full feature set of Windows Firewall with Advanced Security, including profile settings, rules, and computer connection security rules for installation on client computers.</td>
<td>You can configure Group Policy settings for Windows Firewall with Advanced Security by opening the same snap-in through the Group Policy Object Editor.</td>
</tr>
<tr>
<td>IP Security Policy Management MMC</td>
<td>Used for mixed Windows version environments and to configure policies that apply to all Windows versions.</td>
<td>Click Start, click Run, type MMC, and then press ENTER. In the MMC window, click File, and then click Add/Remove Snap-in. From the list of available snap-ins, select IP Security Policy Management, click Add, and then click OK.</td>
</tr>
</tbody>
</table>
Module 10

Monitoring and Troubleshooting IPSec

Contents:
Lesson 1: Monitoring IPSec Activity 10-3
Lesson 2: Troubleshooting IPSec 10-8
Lab: Monitoring and Troubleshooting IPSec 10-12
Module Overview

- Monitoring IPsec Activity
- Troubleshooting IPsec

This module provides information about IPsec troubleshooting tasks and the troubleshooting tools that you can use to perform these tasks.
Lesson 1
Monitoring IPSec Activity

By monitoring IPSec activity, you can:
- View IPSec policy assignment information.
- View details about the active IPSec policy and IPSec statistics.
- Verify that security auditing is enabled.
- View IPSec-related events.
- Enable audit logging for Internet Key Exchange (IKE) events and view the events.
- View IPSec and other network communication.
- Change the IPSec configuration for troubleshooting.
Tools Used to Monitor IPSec

<table>
<thead>
<tr>
<th>Tool</th>
<th>Key Points</th>
</tr>
</thead>
</table>
| IP Security Monitor                       | • Used in Windows XP and higher  
• MMC snap-in  
• Administrators can monitor local and remote IPSec policy usage |
| IPSecmon                                  | • Only available in Windows 2000  
• Command-line tool  
• Reduced level of information available for troubleshooting |
| Detailed IKE tracing using Netsh          | • Trace file found in: systemroot\debug\oakley.log  
• Enabled in Windows XP and Windows 2000 through Registry modification |

**Key Points**

You can use the IP Security Monitor snap-in to view and monitor IPSec-related statistics and the IPSec policy applied to computers. This information can help you troubleshoot IPSec and test the policies you are creating. This snap-in can only be used for computers running Windows XP or Windows Vista.

Other tools that you can use to monitor IPSec include:

- IPSecmon
- The monitoring node of the Windows Firewall with Advanced Security snap-in
- The Netsh command

**Additional Reading**

- Help topic: Monitoring IPSec
- IPSec Troubleshooting Tools
Using IP Security Monitor to Monitor IPSec

**Options for using the IP Security Monitor:**

- **Modify IPSec data refresh interval to update information in the console at a set interval**
- **Allow DNS name resolution for IP addresses to provide additional information about computers connecting with IPSec**
- **Computers can monitored remotely**
  - To enable remote management editing, the HKLM\system\currentcontrolset\services\policyagent key must have a value of 1
- **To Discover the Active security policy on a computer, examine the Active Policy Node in the IP Security Monitoring MMC**
- **Main Mode Monitoring monitors initial IKE and SA**
  - Information about the Internet Key Exchange
- **Quick Mode Monitoring monitors subsequent key exchanges related to IPSec**
  - Information about the IPSec driver

**Key Points**

IP Security Monitor is implemented as a Microsoft Management Console (MMC) snap-in, and it includes enhancements that allow you to view details about an active IPSec policy that is applied by the domain or locally, as well as quick mode and main mode statistics, and active IPSec SAs. IP Security Monitor also enables you to search for specific main mode or quick mode filters. To troubleshoot complex IPSec policy designs, you can use IP Security Monitor to search for all matches for filters of a specific traffic type.

**Additional Reading**

- Help Topic: Monitoring IPSec
- Help Topic: Monitoring Main Mode
- Help Topic: Monitoring Quick Mode
Using Windows Firewall with Advanced Security to Monitor IPSec

Key Points
Windows Firewall with Advanced Security is a stateful, host-based firewall that blocks incoming and outgoing connections based on its configuration. While typical end-user configuration of Windows Firewall still takes place through the Windows Firewall Control Panel tool, advanced configuration now takes place in a Microsoft Management Control (MMC) snap-in named Windows Firewall with Advanced Security.
Demonstration: Monitoring IPSec

In this demonstration, you will see how to:

- Establish and monitor an IPSec connection
- Monitor an IPSec connection using the Windows Firewall with Advanced security MMC
Lesson 2
Troubleshooting IPSec

- IPSec Troubleshooting Process
- Troubleshooting IKE
- Troubleshooting IKE Negotiation Events

Successful troubleshooting of IPSec involves understanding the overall process for troubleshooting and monitoring IPSec, the common types of connectivity issues related to IPSec and IKE, and what to look for when troubleshooting IKE Negotiation events.
### Key Points

The IPSec troubleshooting process includes the following steps:

- Verify IP network configuration
- Verify appropriate local and external firewall configurations
- Verify Group Policy and IPSec policy
- Ensure policy compatibility

There are also additional considerations for troubleshooting IPSec, such as checking the firewall configuration and enabling logging in IKE.

### Additional Reading

- Server and Domain Isolation Using IPSec and Group Policy, Chapter 7: Troubleshooting IPSec
Troubleshooting IKE

Key Points
Successful troubleshooting of IKE involves the following guidelines:

- Troubleshoot Connectivity issues related to IPSec and IKE.
- Troubleshoot firewall and port issues.
- View the Oakley.log file for potential issues.
- Identifying Main Mode exchange issues.
Troubleshooting IKE Negotiation Events

**Common Security Event log codes:**

- **Success:**
  - 541 - IKE Main Mode or Quick Mode established
  - 542 - IKE Quick Mode was deleted
  - 543 - IKE Main Mode was deleted
- **Information Log Entries:**
  - Largely pertains to monitoring for denial of service attacks
  - There might not be any errors, however resources will run low which affects performance for legitimate clients
- **Quick Mode audit failures are denoted with 547 error message**

**Key Points**
When troubleshooting IKE Negotiation events, you must be able to identify the following:

- IKE negotiation success events.
- Information log entries.
- Quick mode audit failures.

**Additional Reading**

- Server and Domain Isolation Using IPSec and Group Policy, Chapter 7: Troubleshooting IPSec
- System Error Codes
Lab: Monitoring and Troubleshooting IPSec

- Exercise 1: Monitoring IPSec Connectivity
- Exercise 2: Configuring Connection Security
- Exercise 3: Troubleshooting IPSec

Logon information

<table>
<thead>
<tr>
<th>Virtual machine</th>
<th>6421A-NYC-DC1 and 6421A-NYC-SVR1</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Administrator</td>
</tr>
<tr>
<td>Password</td>
<td>Pa$$w0rd</td>
</tr>
</tbody>
</table>

Estimated time: 30 minutes

Objectives
- Monitor IPSec connectivity
- Configure connection security
- Troubleshoot IPSec

Lab Setup
For this lab you will use the available virtual machine environment. Before you begin the lab, you must:
1. Start the 6421A-NYC-DC1 and 6421A-NYC-SVR1 virtual machines.
2. Log on to 6421A-NYC-DC1 and 6421A-NYC-SVR1 with the user name administrator and the password Pa$$w0rd.
**Scenario:**

The Windows Infrastructure Services Technology Specialist has been tasked with extending an existing network infrastructure to include the functionality of IPSec. Using the IP Security Monitor snap-in and the Windows Firewall with Advanced Security snap-in, you will be able to view IP security statistics and policies and be able to determine if IPSec is failing negotiations and be able to monitor IPSec statistics. Escalations for troubleshooting are sent to you.
Exercise 1: Monitoring IPSec Connectivity

Exercise Overview
In this exercise, you will enable an IPSec policy and then view the connection using IP Security Monitor.

The main tasks are as follows:
1. Start the 6421A-NYC-DC1 and 6421A-NYC-SVR1 virtual machines.
2. Create an IPSec negotiation policy on NYC-DC1.
3. Export the policy from NYC-DC1.
4. Import the security policy to NYC-SVR1.
5. Validate that the negotiation policy is working by using the IP Security Monitor.

► Task 1: Start the 6421A-NYC-DC1 and 6421A-NYC-SVR1 virtual machines
1. Open the Virtual Server Remote Control Client, and then double-click 6421A-NYC-DC1.
2. Log on to NYC-DC1 as Administrator using the password Pa$$w0rd.
3. Open the Virtual Server Remote Control Client, and then double-click 6421A-NYC-SVR1.
4. Log on to NYC-SVR1 as Administrator using the password Pa$$w0rd.

► Task 2: Create an IPSec negotiation policy on NYC-DC1
1. Configure an IPSec policy that secures TCP/UDP traffic by using the Local Security Policy MMC found in Administrative Tools.
   - Source Port: 445
   - Destination Port: Any
2. Filter for IP traffic coming from any IP address going to any IP address.
Task 3: Export the policy from NYC-DC1
- In the Local Security Policy MMC console, export the IPSec policies to a file on NYC-SVR1 (save to D:\LabFiles\Module10\IPSecurityPolicy.ipsec).

Task 4: Import the security policy to NYC-SVR1
- On NYC-SVR1, import the IPSec policies using the Local Security Policy MMC.

Task 5: Validate that the negotiation policy is working by using the IP Security Monitor
1. Enable the IP Security Policies on both computers.
2. Using the Run command, load a blank console and add the IP Security Monitoring snap-in.
3. Establish a file connection share between NYC-SVR1 and NYC-DC1.
4. Monitor the secure connection information in the IP Security Monitoring console.
Exercise 2: Configuring Connection Security

Exercise Overview
In this exercise, you will configure a connection security rule in Windows Firewall and advanced security and then monitor the connection using the Security Associations node.

The main tasks are as follows:
1. Disable the IP Security Policy that was created in the previous exercise.
2. Configure a Security Association rule in the Windows Firewall with Advanced Security MMC.
3. Monitor the connection using the Security Association node.
4. Close all virtual machines and discard undo disks.

► Task 1: Disable the IP Security Policy that was created in the previous exercise

► Task 2: Configure a Security Association rule in the Windows Firewall with Advanced Security MMC
   1. On NYC-DC1, open Windows Firewall with Advanced Security.
   2. Create a new rule in Connection Security Rules.
   3. Select a Server-to-Server rule with Any IP Address for Endpoints.
   4. Select Require authentication for inbound and outbound connections.
   5. Select PreShared Key with a password of Pa$$w0rd.
   6. Apply the rule to the Domain, Private, and Public profiles.
   7. Create the same rule on NYC-SVR1 and use the same Preshared Key.
Task 3: Monitor the connection using the Security Association node.
1. Establish communication between NYC-SVR1 and NYC-DC1.
2. Review the Main Mode and Quick Mode nodes to view the status of the Connection Security rule.

Task 4: Close all virtual machines and discard undo disks
1. On the host computer, click Start, point to All Programs, point to Microsoft Virtual Server, and then click Virtual Server Administration Website.
2. Under Navigation, click Master Status. For each virtual machine that is running, click the virtual machine name, and in the context menu, click Turn off Virtual Machine and Discard Undo Disks. Click OK.
Exercise 3: Troubleshooting IPSec

Exercise Overview
In this exercise, you will review scenarios outlining common issues that can occur when troubleshooting IPSec, and then discuss possible solutions.

Scenario 1
An administrator is attempting to connect to a remote computer and monitor its IPSec connectivity. The administrator reports that he is unable to monitor the remote server. You ask him use the Event Viewer to identify the problem and in doing so, the administrator notes the following error: “The IPSec server is unavailable or incompatible with the IPSec monitor.”

Question: What can you do to resolve this issue?

Scenario 2
An administrator has configured and enabled an IPSec Security policy on a file server that stores sensitive data files. The administrator has also created an Active Directory-based policy and applied it to the organizational unit (OU) of clients that are permitted access to the secure server. The next day, the Backup Administrator, who is responsible for backing up the secure server, reports he was unable to access the server from the backup server. The backup server’s computer account is stored in an administrative OU separate from the client’s OU.

Question: Based on the information provided, why is the backup server unable to access the secure server?
Module Review and Takeaways

- Review Questions
- Best Practices

Review Questions
1. What is the name the log file that should be used to troubleshoot IKE problems?
2. What are the four main steps to follow when troubleshooting IPSec?
**Best Practices**

The following general recommended practices can help you enhance security and minimize the potential for problems when deploying IPSec:

- Establish an IPSec deployment plan. The deployment plan should address the following considerations: which deployment scenarios (such as server-to-server or remote access) require the use of IPSec, what level of security you require for each scenario, which types of data to secure, which computers to secure, which physical links to secure, who will manage IPSec policies, and how you will provide ongoing support and troubleshooting for end users after IPSec is deployed. This will allow for easier troubleshooting, and establish who is responsible for different areas of the IPSec infrastructure.

- Create and test IPSec policies for each deployment scenario. Before deploying IPSec in a production environment, test the IPSec policies in a realistic lab environment. To obtain realistic performance data, run standard workloads on programs. During initial tests, view packet contents with Network Monitor, or use Authentication Header (AH) or Encapsulating Security Payload (ESP) with null encryption to view packet contents for test environments.

- Do not use preshared keys. For enhanced security, the use of preshared key authentication is not recommended because it is a relatively weak authentication method. In addition, preshared keys are stored in plaintext. Preshared key authentication is provided for interoperability purposes and to adhere to IPSec standards. It is recommended that you use preshared keys only for testing and that you use certificates or Kerberos V5 instead in a production environment.

- Use the Triple Data Encryption Standard (3DES) algorithm for stronger encryption. For enhanced security, when configuring key exchange security methods for IPSec policies, use 3DES, which is a stronger encryption algorithm than DES.

- Create and assign a persistent IPSec policy for failsafe security. To enhance security, create and assign a persistent IPSec policy, so that computers can be secured if a local IPSec policy or an Active Directory-based IPSec policy cannot be applied. When you create and assign a persistent policy, it is applied before a local policy or an Active Directory-based policy, and it remains in effect regardless of whether the local policy or the Active Directory-based policy is applied (for example, an IPSec policy will not be applied if it is corrupted).
**Note:** You cannot configure this feature in the IP Security Policy Management console. To configure this feature, you must use the `Netsh IPSec` command-line tool.

- When applying the same IPSec policy to computers running different versions of the Windows operating system, test the policy thoroughly. To ensure that the same IPSec policy functions as expected, test the policy thoroughly on all relevant operating systems before deployment.

- Use Terminal Services to remotely manage and monitor IPSec on computers running different versions of the Windows operating system. Remote management and monitoring of IPSec is supported only for computers running the same version of the Windows operating system. To remotely manage and monitor IPSec on a computer that is running a different version of Windows than the version of Windows that is running on your computer, use Terminal Services.
Module 11

Configuring and Managing Distributed File System

Contents:
Lesson 1: DFS Overview 11-3
Lesson 2: Configuring DFS Namespaces 11-15
Lesson 3: Configuring DFS Replication 11-25
Lab: Configuring DFS 11-39
Module Overview

- DFS Overview
- Configuring DFS Namespaces
- Configuring DFS Replication

Many organizations have the challenge of maintaining a large number of users and servers that are often distributed throughout geographically dispersed locations. In these situations, administrators must find ways to ensure that users can locate files as quickly as possible. Managing multiple sites often introduces additional challenges, such as limiting network traffic over slow wide area network (WAN) connections, ensuring the availability of files during WAN or server failures, and backing up file servers that are located at smaller branch offices.

This module introduces the Distributed File System (DFS) solution that can be used to address these challenges by providing fault-tolerant access and WAN-friendly replication of files located throughout the enterprise.
Lesson 1
DFS Overview

- What is the Distributed File System?
- How DFS Namespaces and DFS Replication Work
- DFS Scenarios
- Types of DFS Namespaces
- What are Folders and Folder Targets?
- Namespace Server Requirements
- Demonstration: Installing DFS

Administrators who manage file servers throughout an enterprise require methods to provide efficient access to resources and ensure availability of files. DFS in Windows Server 2008 provides two technologies to help address these challenges; DFS Replication and DFS Namespaces. This lesson introduces these two technologies and provides scenarios and requirements for deploying a DFS solution within your network environment.
What is the Distributed File System?

The Distributed File System incorporates technologies that provide fault-tolerant access to geographically dispersed files.

DFS technologies include:

- **DFS Namespaces** - provide a virtual view of shared folders located on different servers
- **DFS Replication** - provides high-availability and fault-tolerance to files and folders
- **Remote Differential Compression** - provides a compression technology that is optimized for data transfers over limited-bandwidth networks

Key Points
DFS technologies in Windows Server 2008 provide a simplified way to access geographically dispersed files throughout an organization. DFS also provides WAN-friendly file replication between servers. Technologies provided with DFS include:

- DFS Namespaces
- DFS Replication
- Remote Differential Compression

**Question:** Which two technologies make up DFS?

**Question:** Which technology is used to replicate files within a Windows Server 2008 environment?
Additional Reading

- Distributed File System Technology Center
- Overview of the Distributed File System Solution in Microsoft Windows Server 2003 R2
- Microsoft Distributed File System - IT Value Card
- About Remote Differential Compression
- Optimizing File Replication over Limited-Bandwidth Networks using Remote Differential Compression
How DFS Namespaces and DFS Replication Work

Key Points

Even though DFS Namespaces and DFS Replication are separate technologies, both can be used together to provide high availability and redundancy of data.

The following process describes how DFS Namespaces and DFS Replication work together:

1. User accesses folder in the configured namespace.
2. Client computer accesses the first server in the referral.
Additional Reading

- Overview of the Distributed File System Solution in Microsoft Windows Server 2003 R2
- Distributed File System: Frequently Asked Questions
- Distributed File System Replication: Frequently Asked Questions
- Distributed File System Management Help: Overview of DFS Namespaces
DFS Scenarios

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sharing files across branch offices</td>
<td>Hub site → Branch office</td>
</tr>
<tr>
<td>Data collection</td>
<td>Hub site → Branch office</td>
</tr>
<tr>
<td>Data distribution</td>
<td>Hub site → Site 1 → Site 2</td>
</tr>
</tbody>
</table>

Key Points
There are a number of key scenarios that can benefit from DFS Namespaces and DFS Replication. These scenarios include:

- Sharing files across branch offices
- Data collection
- Data distribution

Question: How can you use DFS technologies within your organization?

Additional Reading
- Overview of the Distributed File System Solution in Microsoft Windows Server 2003 R2
Types of DFS Namespaces

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Domain-based</th>
<th>Stand-alone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td><code>\Domainname\Namespace</code></td>
<td><code>\Servername\Namespace</code></td>
</tr>
<tr>
<td>Location</td>
<td>Active Directory and memory cache</td>
<td>Server registry and memory cache</td>
</tr>
</tbody>
</table>
| Size           | • Up to 5,000 folders with targets in Windows 2000 mode  
                | • Up to 50,000 folders with targets in Windows Server 2008 mode | Up to 50,000 folders with targets          |
| Availability   | Namespace hosted on multiple servers              | Server cluster                                   |
| DFS Replication| Supported                                         | Supported                                        |

**Key Points**

When creating a namespace, you create either a domain-based namespace or a stand-alone namespace. Each type of namespace has different characteristics.

A domain-based namespace can be used when:

- High-availability of the namespace is required.
- You need to hide the name of the namespace servers from the users.

A stand-alone namespace is used when:

- Your organization has not implemented Active Directory® directory service.
- Your organization does not meet the requirements for a Windows Server 2008 mode domain-based namespace, and you have requirements for more than 5,000 DFS folders.
**Question:** How can you be sure that users are not traversing a slow WAN connection to access a DFS Namespace root?

**Additional Reading**
Help Topic: Distributed File System Management: Choosing a Namespace Type
What are Folders and Folder Targets?

### Key Points

Within a DFS namespace you create one or more folders. These folders contain one or more folder targets.

- **Folders.** Folders are the primary elements of a namespace.
- **Folder targets.** A folder target is a Universal Naming Convention (UNC) path to one of the following locations:
  - A shared folder.
  - A folder within a shared folder.
  - A path to another namespace.

**Question:** What is the DFS namespace hierarchy?

**Additional Reading**

- DFS Management
Namespace Server Requirements

A namespace server is:
- A domain controller or member server
- Windows Server 2003 or Windows Server 2008

Namespace server considerations:
- Must contain an NTFS volume to host the namespace
- Must be in the same domain if the namespace is domain-based
- Cannot be a clustered resource if the namespace is domain-based

Key Points

A namespace server is a domain controller or member server that hosts a DFS Namespace. The number of namespaces that a server can host is determined by the operating system running on the server.

Use the following guidelines for namespace server requirements:

<table>
<thead>
<tr>
<th>Server hosting stand-alone Namespaces</th>
<th>Server hosting Domain-Based Namespaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Must contain an NTFS volume to host the namespace</td>
<td>Must contain an NTFS volume to host the namespace</td>
</tr>
<tr>
<td>Can be a member server or a domain controller</td>
<td>Must be a member server or domain controller in the domain that the namespace is configured in.</td>
</tr>
<tr>
<td>Can be a clustered file server</td>
<td>Namespace cannot be a clustered resource in a sever cluster.</td>
</tr>
</tbody>
</table>
Additional Reading

- Help Topic: Prepare to Deploy DFS Namespaces: Review DFS Namespaces
  Server Requirements
Demonstration: Installing DFS

In this demonstration, you will see how to install the DFS services role

**Question:** You need to deploy DFS technology within your environment. Is DFS considered a role service or a feature?

**Question:** Is it possible to install DFS Replication without installing DFS Namespaces?
Lesson 2
Configuring DFS Namespaces

- Deploying Namespaces for Publishing Content
- Security Requirements for Creating and Managing a Namespace
- Demonstration: How to Create Namespaces
- Increasing Availability of a Namespace
- Options for Optimizing a Namespace
- Demonstration: Configuring Folder Targets

Configuring DFS Namespaces consists of a number of tasks which include creating the namespace structure, creating folders within the namespace, and adding folder targets. You may also choose to perform additional management tasks such as configuring the referral order and DFS replication. This lesson provides information on how to complete these configuration and management tasks to deploy an effective DFS solution.
Deploying Namespaces for Publishing Content

**Key Points**

Most DFS implementations primarily consist of content published within the DFS namespace. To configure a namespace for publication, perform the following procedures:

1. Create a namespace.
2. Create a folder in the namespace.
3. Add folder targets.
4. Set the ordering method for targets in referrals.

There are a number of optional tasks that you may want to consider, such as:

- Set target priority to override referral ordering.
- Enable client failback.
- Replicate folder targets using DFS-R.

You may also need to delegate the ability to create and manage namespaces.
Question: How can you ensure that a specific server is always placed first or last in the list of servers provided to the client when accessing a namespace?

Additional Reading
- Deploy a namespace for publishing content
- Help Topic: Distributed File System Management: Deploying DFS Namespaces
Security Requirements for Creating and Managing a Namespace

<table>
<thead>
<tr>
<th>Task</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a domain-based namespace</td>
<td>Domain Admins</td>
</tr>
<tr>
<td>Add a namespace server to a domain-based namespace</td>
<td>Domain Admins</td>
</tr>
<tr>
<td>Manage a domain-based namespace</td>
<td>Local Administrators on each namespace server</td>
</tr>
<tr>
<td>Create a stand-alone namespace</td>
<td>Local Administrators group on the namespace server</td>
</tr>
<tr>
<td>Manage a stand-alone namespace</td>
<td>Local Administrators group on the namespace server</td>
</tr>
<tr>
<td>Implement DFS replication</td>
<td>Domain Admins</td>
</tr>
</tbody>
</table>

Key Points
To perform namespace management tasks, a user either has to be a member of an administrative group, or has to be delegated specific permission to perform the task. You can right-click the namespace and then click Delegate Management Permissions to delegate the required permissions.

**Note:** You must also add the user to the Local Administrators group on the namespace server.
The following table describes the security requirements for creating and managing a DFS namespace:

<table>
<thead>
<tr>
<th>Task</th>
<th>Group Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a domain-based namespace</td>
<td>Domain Admins</td>
</tr>
<tr>
<td>Add a namespace server to a domain-based namespace</td>
<td>Domain Admins</td>
</tr>
<tr>
<td>Manage a domain-based namespace</td>
<td>Local Administrators on each namespace server</td>
</tr>
<tr>
<td>Create a stand-alone namespace</td>
<td>Local Administrators group on the namespace server</td>
</tr>
<tr>
<td>Manage a stand-alone namespace</td>
<td>Local Administrators group on the namespace server</td>
</tr>
<tr>
<td>Implement DFS replication</td>
<td>Domain Admins</td>
</tr>
</tbody>
</table>

**Question:** You need to manage a domain-based namespace. Do you require Domain Administrator privileges?

**Additional Reading**
- Delegate management permissions for an existing namespace
- Security requirements for creating and managing namespaces
Demonstration: How to Create Namespaces

In this demonstration, you will see how to:

- Create new namespaces
- Create a folder and folder target
- Delegate permissions

Question: You want to enable advanced scalability and access-based enumeration. Which option provides these features?
Increasing Availability of a Namespace

**Domain-based namespace:**
- Specify additional namespace servers

**Stand-alone namespace:**
- Create a stand-alone namespace as a cluster resource

**Folders:**
- Specify additional folder targets
- Replicate folders using DFS Replication

**Key Points**
For clients to connect to a DFS namespace, they must be able to connect to a namespace server. This means that it is important to ensure the namespace servers are always available. The process for increasing namespace availability varies for domain-based and stand-alone namespaces. Domain-based namespaces can be hosted on multiple servers. Stand-alone namespaces are limited to a single server.

- Domain-based namespaces. You can increase the availability of a domain-based namespace by specifying additional namespace servers to host it.
- Stand-alone namespaces. You can increase the availability of a stand-alone namespace by creating it as a shared resource in a server cluster.
- Folder targets. You can increase the availability of each folder in a namespace by adding multiple folder targets.
Question: What are the methods used to ensure content is available within a DFS namespace?

Additional Reading

- Increasing the Availability of a Namespace
Options for Optimizing a Namespace

### Key Points
Namespaces have a number of configuration options that can be used to optimize the usability and performance of a namespace. To optimize a namespace, you can:

- Rename or move a folder.
- Disable referrals to a folder.
- Specify referral cache duration.
- Configure namespace polling.

### Additional Reading
- Help Topic: Distributed File System Management: Tuning DFS Namespaces
Demonstration: Configuring Folder Targets

In this demonstration, you will see how to:
- Configure additional folder targets to provide availability
- Optimize a namespace

Question: Which types of paths can you use when creating a new folder target?

Question: What kind of permissions do you need to add folder targets?
Lesson 3
Configuring DFS Replication

- What is DFS Replication?
- What Are Replication Groups and Replicated Folders?
- DFS Replication Requirements
- Scalability Considerations for DFS Replication
- Process for Deploying a Multipurpose Replication Group
- Understanding the Initial Replication Process
- Generating Diagnostic Reports and Propagation Tests
- Demonstration: Deploying DFS Replication

To effectively configure DFS-R, it is important to understand the terminology and requirements associated with the feature. This lesson provides information on the specific elements, requirements, and scalability considerations related to DFS-R, and provides a process for configuring an effective replication topology.
What is DFS Replication?

**DFS-R** is a multimaster replication engine that supports replication scheduling and bandwidth throttling.

- Uses remote differential compression used to efficiently update files over a limited-bandwidth network
- Detects changes on the volume by monitoring the USN journal
- Uses a staging folder to stage a file before sending and receiving it
- Uses a version vector exchange protocol to determine which files need to be synchronized
- Uses a conflict resolution heuristic of last writer wins for files that are in conflict and earliest creator wins for name conflicts
- Is self-healing and can automatically recover from failure

**Key Points**

As stated previously, Distributed File System Replication (DFS-R) is a multimaster replication engine that supports replication scheduling and bandwidth throttling. DFS-R is the successor to the File Replication Service (FRS) that was introduced in Windows 2000 Server operating systems. It is important to take note of the following key points related to DFS-R:

- DFS-R uses a new compression algorithm known as remote differential compression (RDC).
- DFS-R detects changes on the volume by monitoring the update sequence number (USN) journal, and replicates changes only after the file is closed.
- DFS-R uses a staging folder to stage a file before sending or receiving it.
- DFS-R uses a version vector exchange protocol to determine which files need to be synchronized.
- When a file is changed, only the changed blocks are replicated, not the entire file.
• DFS-R uses a conflict resolution heuristic of “last writer wins” for files that are in conflict (that is, a file that is updated at multiple servers simultaneously) and “earliest creator wins” for name conflicts.

• DFS-R is self-healing and can automatically recover from USN journal wraps,

• DFS-R uses a Windows Management Instrumentation (WMI) provider that provides interfaces to obtain configuration and monitoring information from the DFS Replication service.

**Question:** Which two folders can help troubleshoot file replication issues when using DFS-R?

**Question:** What happens when two users simultaneously update the same file on different servers?

**Additional Reading**
- Introduction to DFS Replication
- Staging folders and Conflict and Deleted folders
What Are Replication Groups and Replicated Folders?

**Key Points**

A replication group consists of a set of member servers that participate in the replication of one or more replicated folders. There are two main types of replication groups:

- Multipurpose replication group.
- Replication group for data collection.

A replicated folder is a folder that is kept synchronized on each member server.

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

**Additional Reading**

- Replication groups and replicated folders
DFS Replication Requirements

Key Points
To use DFS-R, you must be aware of specific requirements. These requirements include:

- Ensure that the Active Directory schema has been updated to include the new DFS replication objects.
- The servers that will participate in DFS Replication must run a Windows Server 2003 R2 or Windows Server 2008 operating system.
- Servers in a replication group must be in the same forest.
- On server clusters, replicated folders must be located in the local storage of a node.
- Antivirus software must be compatible with DFS Replication.

DFS-R Requirements include:

- The Active Directory schema must include the DFS replication objects
- Servers must be Windows Server 2003 R2 or Windows Server 2008 and must have the DFS replication service installed
- Servers in a replication group must be in the same forest
- Replicated folders must be stored on NTFS volumes
- On server clusters, replicated folders must be located in the local storage of a node
- Antivirus software must be compatible with DFS Replication
Additional Reading

- DFS Replication requirements
- Distributed File System Replication: Frequently Asked Questions
Scalability Considerations for DFS Replication

Scalability considerations include:

- Each server can be a member of up to 256 replication groups
- Each replication group can contain up to 256 replicated folders
- Each server can have up to 256 connections
- The number of replication groups multiplied by the number of replicated folders multiplied by the number of simultaneously active connections must be kept to 1024 or fewer
- A replication group can contain up to 256 members
- A volume can contain up to 8 million replicated files, and a server can contain up to 1 terabyte of replicated files
- The maximum tested file size is 64 gigabytes

Key Points
Use the following scalability considerations when deploying DFS-R:

- Each server can be a member of up to 256 replication groups.
- Each replication group can contain up to 256 replicated folders.
- Each server can have up to 256 connections (for example, 128 incoming connections and 128 outgoing connections).
- On each server, the number of replication groups multiplied by the number of replicated folders multiplied by the number of simultaneously active connections must be kept to 1024 or fewer.
- A replication group can contain up to 256 members.
- A volume can contain up to 8 million replicated files, and a server can contain up to 1 terabyte of replicated files.
- The maximum tested file size is 64 gigabytes.
Additional Reading

- DFS Replication scalability guidelines
- Understanding DFS Replication limits
- More on DFS Replication limits
Process for Deploying a Multipurpose Replication Group

Key Points
A multipurpose replication group is used to replicate data between two or more servers for general content sharing or for data publishing. You can use the New Replication Group Wizard to complete the following steps:

1. Select the type of replication group to create.
2. Specify the name and domain.
3. Specify replication group members.
4. Select the topology. Choices include:
   - Hub and spoke
   - Full mesh
   - No topology
5. Specify replication group schedule and bandwidth.
6. Select the primary member server.
7. Select the folders to replicate.
8. Specify the local path on other members.

After an initial replication group is created, you can then modify the replicated folders, the connection, or topology. You can also delegate permissions to other administrators to allow for management of the replication group.

**Question:** What are the differences between selecting the Multipurpose replication group and the Replication group for data collection?

**Additional Reading**
- Deploying DFS Replication
Understanding the Initial Replication Process

When you first configure replication, you must choose a primary member that has the most up-to-date files to be replicated. This server is considered authoritative for any conflict resolution that occurs when the receiving members have files that are older or newer when compared to the same files on the primary member.

The following concepts will help you to better understand the initial replication process:

- Initial replication does not begin immediately.
- Initial replication always occurs between the primary member and the receiving replication partners of the primary member.
- When receiving files from the primary member during initial replication, the receiving members that contain files that are not present on the primary member move those files to their respective DfsrPrivate\PreExisting folder.
To determine whether files are identical on the primary member and receiving member, DFS replication compares the files using a hash algorithm.

After the initialization of the replicated folder, the “primary member” designation is removed.

Additional Reading
What to expect during initial replication
Generating Diagnostic Reports and Propagation Tests

Use the Diagnostic Report Wizard to:
- Create a health report
- Start a propagation test
- Create a propagation report

Key Points
To help maintain and troubleshoot DFS-R, you can generate diagnostic reports and perform propagation tests. You can use the Diagnostic Report Wizard to perform the following:
- Create a health report.
- Start a propagation test.
- Create a propagation report.

Additional Reading
- Create a diagnostic report for DFS Replication
Demonstration: Deploying DFS Replication

In this demonstration, you will see how to:

- Create a new replication group
- Add members to the group
- Determine the topology
- Set the replication schedule
- Configure folders to replicate
- Create a diagnostic report for DFS replication

Question: Where are you able to modify the path for the staging folder?

Question: Which tab shows the sending and receiving members of the replication group?
Lab: Configuring DFS

- Exercise 1: Installing the Distributed File System Role Service
- Exercise 2: Creating a DFS Namespace
- Exercise 3: Configuring Folder Targets and Folder Replication
- Exercise 4: Viewing Diagnostic Reports for Replicated Folders

Logon Information

<table>
<thead>
<tr>
<th>Virtual machines</th>
<th>NYC-DC1, NYC-SVR1</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Administrator</td>
</tr>
<tr>
<td>Password</td>
<td>Pa$$w0rd</td>
</tr>
</tbody>
</table>

Estimated time: 60 minutes

Objectives

- Install the Distributed File System Role Service
- Create a DFS Namespace
- Configure Folder Targets and Folder Replication
- View Diagnostic Reports

Logon Information

- Virtual Machines: NYC-DC1, NYC-SVR1
- User Name: WoodgroveBank\Administrator
- Password: Pa$$w0rd
Scenario
You are a Windows Infrastructure Services Technology Specialist for Woodgrove Bank. To simplify file access for users and provide high availability and redundancy, you will implement a DFS solution for a number of disparate file shares. For this project, you must complete the following tasks:

- Install the Distributed Files System role service to include DFS namespaces and DFS replication.
- Create a domain-based DFS namespace called CorpDocs with NYC-DC1 and NYC-SVR1 as host namespace servers.
- Add the following Folders to the CorpDocs namespace:
  - HRTemplates - folder target located on NYC-DC1
  - PolicyFiles - folder target located on NYC-SVR1
- Configure availability and redundancy by adding additional folder targets and replicating the folder targets in the CorpDocs namespace.
- Provide reports on the health of the CorpDocs folder replication.
Exercise 1: Installing the Distributed File System Role Service

In this exercise, you will install the Distributed File System Role Service on both NYC-DC1 and NYC-SVR1. This will provide redundancy for the CorpDocs namespace and allow clients to contact the namespace server within their own site.

The main tasks for this exercise are as follows:
1. Start each virtual machine and disable Local Area Connection 2 on NYC-SVR1.
2. Install the Distributed File System Role Service on NYC-DC1.
3. Install the Distributed File System Role Service on NYC-SVR1.

Task 1: Start each virtual machine and disable Local Area Connection 2 on NYC-SVR1
1. As indicated in the Logon Information section, start NYC-DC1 and NYC-SVR1 and log on as WoodgroveBank\Administrator using the password Pa$$w0rd.
2. On NYC-SVR1, disable the network adapter named Local Area Connection 2.

Task 2: Install the Distributed File System Role Service on NYC-DC1
1. On NYC-DC1, start Server Manager.
2. Use the Add Roles Wizard to add the Distributed File System Role Service including the DFS Namespaces and DFS Replication options.
3. Using the Server Manager Roles pane, verify that File Server, Distributed File System, DFS Namespaces, and DFS Replication are installed.

Task 3: Install the Distributed File System Role Service on NYC-SVR1
1. On NYC-SVR1, start Server Manager.
2. Use the Add Roles Wizard to add the Distributed File System Role Service including the DFS Namespaces and DFS Replication options.
3. Using the Server Manager Roles pane, verify that File Server, Distributed File System, DFS Namespaces, and DFS Replication are all installed.
Exercise 2: Creating a DFS Namespace

In this exercise, you will create the CorpDocs DFS namespace. You will also configure both NYC-DC1 and NYC-SVR1 to host the CorpDocs namespace to provide redundancy.

The main tasks for this exercise are as follows:

1. Raise the domain functional level.
2. Use the New Namespace Wizard to create a new namespace.
3. Add an additional namespace server to host the namespace.

► Task 1: Raise the domain functional level

- On NYC-DC1, open Active Directory Users and Computers and raise the domain functional level to Windows Server 2008.

► Task 2: Use the New Namespace Wizard to create a new namespace

1. On NYC-DC1, start the DFS Management console.
2. Use the New Namespaces Wizard to create a namespace with the following options:
   - Namespace Server: NYC-DC1
   - Namespace Name and Settings: CorpDocs
   - Namespace Type: Domain-based namespace (Windows Server 2008 mode)
3. In the left pane, click the plus sign next to Namespaces and then click \WoodgroveBank\CorpDocs.
4. Verify that the CorpDocs namespace has been created on NYC-DC1.
Task 3: Add an additional namespace server to host the namespace

1. On NYC-DC1, in the DFS Management console, use the Add Namespace Server Wizard to add a new namespace server with the following options:
   - Namespace server: NYC-SVR1
   - Click Yes to start the Distributed File System service.

2. In the left pane, click the plus sign next to Namespaces and then click \\WoodgroveBank\CorpDocs.
Exercise 3: Configuring Folder Targets and Folder Replication

In this exercise, you will initially create folder targets on two separate servers and then verify that the CorpDocs namespace functions correctly. You will then add availability and redundancy by creating additional folder targets and configuring replication.

The main tasks for this exercise are as follows:

1. Create the HRTemplates folder and configure a folder target on NYC-DC1.
2. Create the PolicyFiles folder and configure a folder target on NYC-SVR1.
3. Verify the functionality of the CorpDocs namespace.
4. Create additional folder targets for the HRTemplates folder and configure folder replication.
5. Create additional folder targets for the PolicyFiles folder and configure folder replication.

▶ Task 1: Create the HRTemplates folder and configure a folder target on NYC-DC1

1. On NYC-DC1, in the DFS Management console, right-click \WoodgroveBank\CorpDocs.
2. Create a new folder called HRTemplates.
3. Add a new folder target called HRTemplateFiles using the following options:
   - Click the New Shared Folder button.
   - Share Name: HRTemplateFiles
   - Local path of shared folder: C:\HRTemplateFiles
   - Shared Folder Permissions: Administrators have full access; other users have read-only permissions
4. In the console tree, click \WoodgroveBank.com\CorpDocs.
5. In the details pane, click the Namespace tab. Notice that HRTemplates is listed as an entry in the namespace.
6. In the console tree, expand `\WoodgroveBank.com\CorpDocs` and then click **HRTemplates**. In the details pane, notice that on the **Folder Targets** tab, one folder target is configured.

7. Click the **Replication** tab and notice that replication is not configured.

▶ **Task 2: Create the PolicyFiles folder and configure a folder target on NYC-SVR1**

1. On NYC-DC1, in the DFS Management console, right-click `\WoodgroveBank\CorpDocs`.

2. Create a new folder called **PolicyFiles**.

3. Add a new Folder target called **PolicyFiles** using the following options:
   - Click the **New Shared Folder** button.
   - **Share Name:** PolicyFiles
   - **Local path of shared folder:** C:\PolicyFiles
   - **Shared Folder Permissions:** Administrators have full access; other users have read-only permissions

4. In the console tree, expand `\WoodgroveBank.com\CorpDocs` and then click **PolicyFiles**. In the details pane, notice that on the **Folder Targets** tab, one folder target is configured.

▶ **Task 3: Verify the functionality of the CorpDocs namespace**

1. On NYC-DC1, click **Start** and then click **Run**.

2. Access the `\WoodgroveBank\CorpDocs` namespace and verify that both **HRTemplates** and **PolicyFiles** are visible. (If they are not visible, wait for approximately 5 minutes to complete.)

3. In the **HRTemplates** folder, create a new Rich Text Document file called **VacationRequest**.

4. In the **PolicyFiles** folder, create a new Rich Text Document file called **OrderPolicies**.
Task 4: Create additional folder targets for the HRTemplates folder and configure folder replication

1. On NYC-DC1, in the DFS Management console, add a folder target with the following options:
   - Path to folder target: \NYC-SVR1\HRTemplates
   - Create share: Yes
   - Local Path of shared folder: C:\HRTemplates
   - Shared folder permissions: Administrators have full access; other users have read-only permissions
   - Replication group: Yes
   - Replication Group name: woodgrovebank.com\corpdocs\hrtemplates
   - Replicated folder name: HRTemplates
   - Primary member: NYC-DC1
   - Topology: Full mesh
   - Replication schedule: default

2. In the console tree, expand the Replication node and then click woodgrovebank.com\corpdocs\hrtemplates.

3. In the details pane, on the Memberships tab, verify that both NYC-DC1 and NYC-SVR1 are listed and enabled.
Task 5: Create additional folder targets for the PolicyFiles folder and configure folder replication

1. On NYC-DC1, in the DFS Management console, add a folder target with the following options:
   - Path to folder target: \NYC-SVR1\PolicyFiles
   - Create share: Yes
   - Local Path of shared folder: C:\PolicyFiles
   - Shared folder permissions: Administrators have full access; other users have read-only permissions
   - Replication group: Yes
   - Replication Group name: woodgrovebank.com\corpdocs\policyfiles
   - Replicated folder name: PolicyFiles
   - Primary member: NYC-SVR1
   - Topology: Full mesh
   - Replication schedule: default

2. In the console tree, expand the Replication node and then click woodgrovebank.com\corpdocs\PolicyFiles.

3. In the details pane, on the Memberships tab, verify that both NYC-DC1 and NYC-SVR1 are listed and enabled.
Exercise 4: Viewing Diagnostic Reports for Replicated Folders

In this exercise, you will generate a diagnostic report to view the folder replication status.

The main task for this exercise is as follows:

• Create a diagnostic report for woodgrovebank.com\corpdocs\hrtemplates.
• Close all virtual machines and discard undo disks.

▶ Task 1: Create a diagnostic report for woodgrovebank.com\corpdocs\hrtemplates

1. On NYC-DC1, create a diagnostic report for woodgrovebank.com\corpdocs\hrtemplates based upon the following options:
   • Type of Diagnostic Report or Test: health report
   • Path and Name: default
   • Members to include: NYC-DC1 and NYC-SVR1
   • Options: Backlogged files enabled; Count replicated files enabled

2. Read through the report and take note of any errors or warnings. When you are finished, close the Internet Explorer window.

3. Create a diagnostic report for the policyfiles replication group. Read through the report and take note of any errors or warnings. When you are finished close the Internet Explorer window. Note that there may be errors reported if replication has not begun or finished yet.

▶ Task 2: Close all virtual machines and discard undo disks

1. On the host computer, click Start, point to All Programs, point to Microsoft Virtual Server, and then click Virtual Server Administration Website.

2. Under Navigation, click Master Status. For each virtual machine that is running, click the virtual machine name, and in the context menu, click Turn off Virtual Machine and Discard Undo Disks. Click OK.
Module Review and Takeaways

- Review Questions
- Network Ports Used by DFS
- Tools

Review Questions
1. How is DFS used in your File Services deployment?
2. What kind of compression technology is used by Windows Server 2008 DFS?
3. What are three main scenarios used for DFS?
4. What is the difference between a domain-based DFS namespace and a stand-alone DFS namespace?
5. What is the default ordering method for client referral to folder targets?
6. What does the Primary Member configuration do when setting up replication?
7. Which folder is used to cache files and folders where conflicting changes are made on two or more members?
Network ports used by DFS

The following table describes the network ports used by DFS.

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Relevant Computers</th>
<th>UDP</th>
<th>TCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetBIOS Name Service</td>
<td>Domain controllers; root servers that are not domain controllers; servers acting as folder targets; client computers acting as folder targets</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NetBIOS Datagram Service</td>
<td>Domain controllers; root servers that are not domain controllers; servers acting as folder targets; client computers acting as folder targets</td>
<td>137</td>
<td>137</td>
</tr>
<tr>
<td>NetBIOS Session Service</td>
<td>Domain controllers; root servers that are not domain controllers; servers acting as folder targets; client computers acting as folder targets</td>
<td></td>
<td>139</td>
</tr>
<tr>
<td>LDAP Server</td>
<td>Domain controllers</td>
<td>389</td>
<td>389</td>
</tr>
<tr>
<td>Remote Procedure Call (RPC) endpoint mapper</td>
<td>Domain controllers</td>
<td></td>
<td>135</td>
</tr>
<tr>
<td>Server Message Block (SMB)</td>
<td>Domain controllers; root servers that are not domain controllers; servers acting as folder targets; client computers acting as folder targets</td>
<td></td>
<td>445</td>
</tr>
</tbody>
</table>
Tools
The following table lists the tools that you can use to configure and manage DFS.

<table>
<thead>
<tr>
<th>Tool</th>
<th>Use For</th>
<th>Where to find it</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dfsutil</td>
<td>Performing advanced operations on DFS namespaces.</td>
<td>On a namespace server, type Dfsutil at a command prompt.</td>
</tr>
<tr>
<td>Dfscmd.exe</td>
<td>Scripting basic DFS tasks such as configuring DFS roots and targets.</td>
<td>On a namespace server, type Dfscmd at a command prompt.</td>
</tr>
<tr>
<td>DFS Management</td>
<td>Performing tasks related to DFS namespaces and replication.</td>
<td>Click <strong>Start</strong>, and then point to <strong>Administrative Tools, and then click DFS Management</strong>.</td>
</tr>
</tbody>
</table>
Module 12

Configuring and Managing Storage Technologies

Contents:
Lesson 1: Overview of Windows Server 2008 Storage Management 12-3
Lesson 2: Managing Storage Using File Server Resource Manager 12-8
Lesson 3: Configuring Quota Management 12-16
Lesson 4: Implementing File Screening 12-25
Lesson 5: Managing Storage Reports 12-31
Lab: Configuring and Managing Storage Technologies 12-36
File storage is an important aspect of managing Windows Server environments. There are significant challenges when analyzing, planning, and implementing storage solutions. Fortunately, Windows Server 2008 includes several tools to help you configure and manage storage technologies. This module provides information that will help you to understand common challenges for capacity and storage management. This module also describes how to analyze usage trends, and how to implement solutions to meet the requirements of users, while complying with company policy and industry and regulatory standards.
Lesson 1
Overview of Windows Server 2008 Storage Management

- Common Challenges to Capacity Management
- Common Challenges to Storage Management
- Addressing Capacity and Storage Management Challenges
- What Is File Server Resource Manager?

Windows Storage management tools were built to answer several challenges involved with managing storage systems in the enterprise environment. After this lesson, you should have a solid understanding of what these challenges are and how to address them.
Common Challenges to Capacity Management

Capacity management challenges include:

- Determining existing storage capacity and usage trends across the organization
- Determining whether usage effectively supports organizational goals
- Defining and implementing storage policies
- Adjusting the policies as capacity needs grow and as organizational needs change

Key Points
Capacity management is the process of planning, analyzing, sizing, and optimizing methods to satisfy an organization’s increase in data storage demands. As the amount of data that needs to be stored and accessed increases, so does the need for capacity management. Keeping track of how much storage capacity is available, how much storage space is needed for future expansion, and how the storage in the environment is being used allows administrators to adequately meet the storage capacity requirements of the organization.
Common Challenges to Storage Management

Storage management challenges include:

- Many organizations experience a growth in storage requirements from 60 to 100 percent per year
- Mission-critical data must be continuously available
- Organizations must comply with the latest regulatory requirements
- The number of storage-intensive applications on the market has increased

Key Points
After capacity management, the next challenge is managing what is stored in the given capacity. In many organizations, 60 to 100 percent of the data is stored. This data includes e-mail messages, office documents, and line-of-business application databases.

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

Question: Consider internal retention policies. Why are these policies in place, because of internal requirements or because of external requirements?

Question: Does the organization have regularly increasing storage requirements?
Addressing Capacity and Storage Management Challenges

Consider the following to help address capacity and storage management challenges:

- Analyze how storage is being used
- Define storage resource management policies
- Implement policies to attempt to slow storage growth
- Acquire tools to implement policies

Key Points

Business in the digital age is tied to information, which must be stored. As an IT professional, meeting the needs of the enterprise’s storage requirements poses a constant set of challenges. To address these challenges, several general tasks have been identified:

- Analyzing how storage is being used
- Defining storage resource management policies
- Acquiring tools to implement policies
What is File Server Resource Manager?

File Server Resource Manager (FSRM) is a File Services role that integrates:

- **Capacity Management**
  - Monitors usage patterns and utilization levels

- **Policy Management**
  - Restricts unauthorized files (file screening)

- **Quota Management**
  - Controls the amount of space used for a volume, folder, or share

- **Reports**
  - Provides extensive storage reports

### Key Points

File Server Resource Manager (FSRM) is a complete set of tools that allows administrators to address the following key challenges of file server management:

- **Capacity management.** Monitors usage patterns and utilization levels.
- **Policy management.** Restricts which files are stored on the server.
- **Quota management.** Limits how much data can be stored on the server.
- **Reports.** Provides reporting on storage capacity usage to meet regulatory requirements and reporting needs,
Lesson 2
Managing Storage Using File Server Resource Manager

- FSRM Functions
- Demonstration: Installing the FSRM Role Service
- Components of the FSRM Console
- FSRM Configuration Options
- Demonstration: Configuring FSRM Options

You can use File Server Resource Manager (FSRM) to configure quota management, implement file screening, and generate storage reports. This lesson provides information about how to manage storage by using FSRM.
FSRM Functions

Using FSRM, you can perform the following tasks:

- Create quotas to limit the space allowed for a volume or folder
- Have quotas automatically generated
- Create file screens
- Monitor attempts to save unauthorized files
- Define quota and file screening templates
- Generate scheduled or on-demand storage reports

Key Points
File System Resource Manager has several functions to accomplish storage management tasks. The following table describes FSRM functions.

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create quotas to limit the space allowed for a</td>
<td>Allows you to set the maximum amount of space allotted to a user. It also allows the administrator to be notified if the quota is exceeded.</td>
</tr>
<tr>
<td>volume or folder</td>
<td></td>
</tr>
<tr>
<td>Automatically generate quotas</td>
<td>Allows you to specify that quotas are dynamically generated upon the creation of subfolders. This allows the storage volume to be managed without having to apply quotas each time a directory structure is modified.</td>
</tr>
<tr>
<td>Create file screens</td>
<td>Enables the filtering of files based on file extension. Common file categories can be grouped together to create file groups.</td>
</tr>
<tr>
<td>Function</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Monitor attempts to save unauthorized files</td>
<td>Administrators can be notified when users are attempting to save a file that does not conform to the file screens in place</td>
</tr>
<tr>
<td>Define quota and file screening templates</td>
<td>Templates provide a high level of customization. This allows you to implement a detailed company storage policy.</td>
</tr>
<tr>
<td>Generate scheduled or on-demand storage reports</td>
<td>Allows you to create reports on a regular basis for review, or create reports on demand, which allows you to quickly generate a report for immediate consumption.</td>
</tr>
</tbody>
</table>

**Additional Reading**

Demonstration: Installing the FSRM Role Service

In this demonstration, you will see how to:

- Install the File Services role
- Install and configure the File Server Resource Manager Role Service
- View the FSRM console
Components of the FSRM Console

Key Points
The FSRM console enables you to view all their local storage resources from a single console, and create and apply policies that control these resources. The three tools included in The FSRM console are:

- Quota Management
- File Screening Management
- Storage Reports Management

Additional Reading
FSRM Configuration Options

FSRM configuration options include:

- Configuring e-mail notifications
- Configuring the default parameter for storage reports
- Changing report repository locations
- Configuring file screen audit

Key Points
Installing FSRM automatically configures the FSRM console, which is made available in the Administrative Tools folder and the Server Manager Console. When you open FSRM, three nodes are visible: Quota Management, File Screening Management, and Storage Reports Management.

The Quota Management node allows you to:

- Create, manage, and obtain information about quotas, which are used to set a space limit on a volume or folder.
- Create and manage quota templates to simplify quota management.
- Create and manage auto quotas.
The File Screening Management node allows you to:

- Create, manage, and obtain information about file screens, which are used to block selected file types from a volume or folder.
- Create file screening exceptions to override certain file screening rules.
- Create and manage file screen templates to simplify file screening management.
- Create and manage file groups.

The Storage Reports Management node is used to configure and schedule different types of storage reports and to create reports on demand.

Additional Reading

Demonstration: Configuring FSRM Options

In this demonstration, you will see how to configure FSRM options.
Lesson 3  
Configuring Quota Management

- What is Quota Management?  
- FSRM Quotas vs. NTFS Disk Quotas  
- What Are Quota Templates?  
- Creating and Modifying a Quota  
- Monitoring Quota Usage  
- Demonstration: How to Create and Manage Quotas

Quota management allows you to create quotas to limit the space allowed for a volume or folder and generate notifications when the quota limits are approached or exceeded. FSRM can define quota templates that can be easily applied to new volumes or folders and that can be used across an organization. You can also auto apply quota templates to all existing folders in a volume or folder, as well as to any new subfolders created in the future.
What is Quota Management?

**Limiting storage space via a hard or soft quota and generating notifications when the limits are approached or exceeded**

**Notification thresholds can be configured to:**
- Send e-mail notifications
- Log an event
- Run a command or script
- Generate storage reports

**Key Points**
You can create quotas to limit the space allowed for a volume or folder and generate notifications when the quota limits are approached or exceeded. By creating a quota for a volume or folder, you can limit the disk space that is allocated for it. The quota limit applies to the entire folder subtree.

**Additional Reading**
# FSRM Quotas vs. NTFS Disk Quotas

<table>
<thead>
<tr>
<th>Quota Features</th>
<th>NTFS Disk Quotas</th>
<th>FSRM Quotas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quota Tracking</td>
<td>Per user/per volume</td>
<td>By folder or by volume</td>
</tr>
<tr>
<td>Disk Usage Calculation</td>
<td>Logical file size</td>
<td>Actual disk space</td>
</tr>
<tr>
<td>Notification Mechanisms</td>
<td>Event logs only</td>
<td>E-mail, custom reports, command execution, event logs</td>
</tr>
</tbody>
</table>

## Key Points

The Windows 2000 Server, Windows Server 2003, and Windows Server 2008 operating systems support disk quotas, which are used to track and control disk usage on a per-user/per-volume basis.

The following table outlines the advantages of using the quota management tools in FSRM compared to NTFS disk quotas:

<table>
<thead>
<tr>
<th>Quota features</th>
<th>FSRM quotas</th>
<th>NTFS disk quotas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quota Tracking</td>
<td>By folder or by volume</td>
<td>Per user/per volume</td>
</tr>
<tr>
<td>Disk Usage Calculation</td>
<td>Actual disk space</td>
<td>Logical file size</td>
</tr>
<tr>
<td>Notification Mechanisms</td>
<td>E-mail, custom reports, command execution, event logs</td>
<td>Event logs only</td>
</tr>
</tbody>
</table>
Additional Reading

What Are Quota Templates?

A quota template defines:

- A space limit
- The type of quota (hard or soft quota)
- A set of notifications to be generated when the quota limit is approached

A number of default Quota Templates are provided in the Quota Management node of FSRM

Key Points

To simplify the tasks associated with quota management, it is recommended that you base your quotas on a quota template. If you base your quotas on a quota template and you later decide to change the quota configuration—for example, you want to allow each user additional space on the storage server—you can simply update the quota template and then choose to automatically update all quotas that are based on this template.

Additional Reading

Creating and Modifying a Quota

Key Points
You can use the Quota Management node in FSRM to create and modify quotas. By creating a quota for a volume or folder, you can limit the disk space that is allocated for that volume or folder. The Quota Management node of FSRM includes all the necessary options to work with quotas.

Additional Reading
Monitoring Quota Usage

Key Points
After configuring and applying quotas to your file shares or volumes, it is important to understand how to monitor disk usage to effectively meet the ongoing storage requirements of your organization.

In addition to the information included in notifications, you can monitor quota usage by:

- Viewing quota information.
- Generating a Quota Usage report.
- Creating soft quotas.

Note: Quotas reduce the input/output (I/O) per-second performance of the storage subsystem by a small amount (10 percent or less). Servers that apply quotas to more than 10,000 folders might experience a larger performance overhead.
Additional Reading

Demonstration: How to Create and Manage Quotas

**In this demonstration, you will see how to:**

- Create a new quota template
- Create a new quota based on a quota template
- Generate a quota notification
Lesson 4
Implementing File Screening

- What is File Screening?
- What Are File Groups?
- What Is a File Screen Exception?
- What Is a File Screen Template?
- Demonstration: Implementing File Screening

Your security policy might prohibit specific types of files from being placed on company servers, and you might want to be notified if a specific file type is saved on a file server. This lesson explains the concepts related to file screening that you can use to manage the types of files that users can save on corporate file servers.
What is File Screening?

A file screen provides a flexible method to control the types of files that are saved on company servers. For example, you can ensure that no music files are stored in personal folders on a server, yet allow storage of specific types of media files that support legal rights management or comply with company policies.

You can also implement a screening process to notify you by e-mail when an unauthorized file type has been stored on a shared folder.

Key Points

The File Screening Management node allows you to:

- Create file screens
- Define file screen templates
- Create file screen exceptions
- Create file groups

Additional Reading

What Are File Groups?

A file group is used to define a namespace for a file screen, file screen exception, or storage report.

The file group consists of a set of file name patterns, which are grouped into:

- Files to include
- Files to exclude

Key Points

A file group is used to define a namespace for a file screen, file screen exception, or storage report.

The file group consists of a set of file name patterns, which are grouped into files to include and files to exclude:

- Files to include. Files that belong in the group.
- Files to exclude. Files that do not belong in the group.

Additional Reading

What Is a File Screen Exception?

A file screen exception overrides any file screen that would otherwise apply to a folder, and all its subfolders, in a designated exception path.

Key Points
A file screen exception is a special type of file screen that overrides any file screening that would otherwise apply to a folder, and all its subfolders, in a designated exception path. In other words, the file screen exception creates an exception to any rules derived from a parent folder.

Additional Reading
What Is a File Screen Template?

A file screen template defines:

- Which file groups to block
- The type of screening to perform
- A set of notifications to be generated

Key Points
To simplify the management of file screens, it is recommended that you base your file screens on file screen templates. A file screen template defines:

- Which file groups to block.
- The type of screening to perform.
- A set of notifications to be generated.

FSRM provides several default file screen templates, which you can use to block audio and video files, executable files, image files, e-mail files and to meet some other common administrative needs.

Additional Reading
Demonstration: Implementing File Screening

**In this demonstration, you will see how to:**

- Create a file screen based on a file screen template
- Create a file screen exception based on a custom file group
Lesson 5
Managing Storage Reports

- What Are Storage Reports?
- What Is a Report Task?
- Generating On-Demand Reports

To assist in capacity planning, it is important to be able to configure and generate extensive reports based on current storage numbers. This lesson provides information about how to configure, schedule and generate storage reports by using FSRM. Error! Bookmark not defined.
What Are Storage Reports?

Key Points
The Storage Reports Management feature of FSRM allows you to generate storage reports on demand, as well as schedule periodic storage reports that help identify trends in disk usage. You can also create reports to monitor attempts to save unauthorized files by all users or a selected group of users.

The following table describes each storage report that is available in FSRM:

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large Files</td>
<td>Lists files that are larger than a specified size.</td>
</tr>
<tr>
<td>Files by Owner</td>
<td>Lists files, grouped by owner.</td>
</tr>
<tr>
<td>Files by File Group</td>
<td>Lists files that belong to specified file groups.</td>
</tr>
<tr>
<td>Duplicate Files</td>
<td>Lists files that appear to be duplicates.</td>
</tr>
<tr>
<td>Least Recently Used Files</td>
<td>Lists files that have not been accessed for a specified number of days.</td>
</tr>
<tr>
<td>Report</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Most Recently Used Files</td>
<td>Lists files that have been accessed within a specified number of days.</td>
</tr>
<tr>
<td>Quota Usage</td>
<td>Lists quotas for which the quota usage is higher than a specified percentage.</td>
</tr>
<tr>
<td>File Screening Audit</td>
<td>Lists file screening violations that have occurred on the server, for a specified number of days.</td>
</tr>
</tbody>
</table>

**Additional Reading**

What Is a Report Task?

Reports can be scheduled by creating a *Report Task*

A report task specifies:

- The volumes and folders to report on
- Which reports to generate
- What parameters to use
- How often to generate the reports
- Which file formats to save the reports in

**Key Points**

To generate a set of reports on a regular schedule, you schedule a report task. The report task specifies:

- The volumes and folders to report on.
- Which reports to generate.
- What parameters to use.
- How often to generate the reports.
- Which file formats to use when saving reports.

**Additional Reading**

Generating On-Demand Reports

Use the **Generate Reports Now** action to open Storage Reports Task Properties and select desired reports.

Key Points
During daily operations, you may want to generate reports on demand to analyze different aspects of current disk usage on the server. Use the **Generate reports now** action to generate one or more reports. Before the reports are generated, current data is gathered.

Additional Reading
Lab: Configuring and Managing Storage Technologies

Objectives
• Install the FSRM role service
• Configure storage quotas
• Configure file screening
• Generate storage reports using FSRM

Logon Information
• Virtual Machines: NYC-DC1, NYC-SVR1
• User Name: Administrator
• Password: Pa$$w0rd

Estimated time: 60 minutes
Scenario
As the Windows Infrastructure Services (WIS) Technology Specialist, you have been tasked with configuring storage on a server which will comply with corporate standards. You must create the storage with minimal long term management by utilizing file screening and quota management.
Exercise 1: Installing the FSRM Role Service
In this exercise, you will install the FSRM role service.
The main tasks for this exercise are as follows:
1. Start the NYC-DC1 and NYC-SVR1 virtual machines.
2. Install the FSRM server role on NYC-SVR1.

▶ Task 1: Start the NYC-DC1 and NYC-SVR1 virtual machines
   1. Open the Virtual Server Remote Control Client, and then double-click 6421A-NYC-DC1.
   2. Log on to NYC-DC1 as Administrator using the password Pa$$w0rd.
   3. Open the Virtual Server Remote Control Client, and then double-click 6421A-NYC-SVR1.
   4. Log on to NYC-SVR1 as Administrator using the password Pa$$w0rd.

▶ Task 2: Install the FSRM server role on NYC-SVR1
   • Using Server Manager, install the File System Resource Manager role service. It is a role service located under the File Services role.
Exercise 2: Configuring Storage Quotas

In this exercise, you must configure a quota template that allows users a maximum of 100MB of data in their user folders. When users exceed 85 percent of the quota or when they attempt to add files larger than 100MB, an event should be logged to the Event Viewer on the server.

The main tasks for this exercise are as follows:

1. Create a quota template.
2. Configure a quota based on the quota template.
3. Test that the quota is working by generating several large files.

▶ Task 1: Create a quota template

- In the File Server Resource Manager console, use the Quotas Templates node to configure a template that sets a hard limit on the maximum size of the folder to 100MB. Make sure this template also notifies the Event Viewer when the folder reaches 85 percent and 100 percent capacity.

▶ Task 2: Configure a quota based on the quota template

1. Use the File Server Resource Manager console and the Quotas node to create a quota in the D:\Labfiles\Module12\Users folder by using the quota template that you created in Task 1.
2. Create an additional folder named User4 in the D:\Labfiles\Module12\Users folder and ensure that the new folder is listed in the quotas list.
Task 3: Test that the Quota is working by generating several large files

1. Open a command prompt and use the `fsutil file createnew file1.txt 89400000` command to create a file in the `D:\Labfiles\Module12\Users\User1` folder.

2. Check the Event Viewer for an Event ID of 12325.

3. Test that the quota works by attempting to create a file that is 16400000 bytes, and then press ENTER.

4. Enable folder compression for the `D:\Labfiles\Module12\Users` folder. Check to see what affect this has in the Quota console. Try again to create a file that is 16400000 bytes.
Exercise 3: Configuring File Screening

In this exercise, you will configure file screening to monitor executable files.

The main tasks for this exercise are as follows:

1. Create a file screen.
2. Test and validate the file screen.

► Task 1: Create a file screen

1. In the File Server Resource Manager console, use the File Screens node to create a file screen that monitors executable files in the D:\Labfiles\Module12\Users folder. When an executable is dropped into the folder, the file screen will log an 8215 event in the Event Viewer.

2. Test the file screen by copying example.bat from D:\Labfiles\Module12 to the D:\Labfiles\Module12\Users\User1 folder. Verify that the file screen is working in the Event Viewer.
Exercise 4: Generating Storage Reports

In this exercise, you will generate an on-demand storage report.

The main tasks for this exercise are as follows:

- Generate an on-demand storage report.
- Close all virtual machines and discard undo disks.

▶ Task 1: Generate an on-demand storage report

- In the File Server Resource Manager console, use the Generate reports now option in the Reports node to generate a File Screening Audit and Quota Usage report on the D:\Labfiles\Module12\Users folder.

▶ Task 2: Close all virtual machines and discard undo disks

1. On the host computer, click Start, point to All Programs, point to Microsoft Virtual Server, and then click Virtual Server Administration Website.

2. Under Navigation, click Master Status. For each virtual machine that is running, click the virtual machine name, and in the context menu, click Turn off Virtual Machine and Discard Undo Disks. Click OK.
Module Review and Takeaways

- Review Questions
- Tools

Review Questions
What is the difference between a hard quota and soft quota?

When a common set of file types need to be blocked, what should you create to block them in the most efficient manner?

If you want to apply a quota to all subfolders in a folder, including folders that will be created in the future, what option must you configure in the quota policy?
Tools
The following table describes the tools that you can use to configure FSRM.

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dirquota.exe</td>
<td>Use to create and manage quotas and quota templates.</td>
</tr>
<tr>
<td>FileScrn.exe</td>
<td>Use to create and manage file screens, file screening exceptions, and file groups.</td>
</tr>
<tr>
<td>StorRept.exe</td>
<td>Use to configure report parameters and generate storage reports on demand. You can also create report tasks and then use Schtasks.exe to schedule the tasks.</td>
</tr>
<tr>
<td>Fsutil</td>
<td>Use the file system utility to configure NTFS Quotas, and create files to test quota behavior.</td>
</tr>
</tbody>
</table>
Module 13

Configuring Availability of Network Resources and Content

Contents:
Lesson 1: Backing Up Data 13-3
Lesson 2: Configuring Shadow Copies 13-13
Lesson 3: Providing Server and Service Availability 13-20
Lab: Configuring Availability of Network Resources 13-31
Module Overview

- Backing Up Data
- Configuring Shadow Copies
- Providing Server and Service Availability

This module provides the information necessary to configure availability of network resources and content. It explains the new backup infrastructure in Windows Server® 2008 and describes how to configure backup and recovery methods. This module also explains how to enable a shadow copy volume, which enables users to access previous versions of files and folders on a network. Finally, this module explains how failover clustering and Network Load Balancing can be used to facilitate greater data availability and workload scalability.
Lesson 1

Backing up Data

- Overview of Windows Server Backup
- New Features of Windows Server Backup
- Who Can Back Up Data?
- What is System State Data?
- Optimizing Backup Performance
- Specifying a Backup Time
- How Is Data Restored?
- Demonstration: Installing and Configuring Windows Server Backup

Windows Server Backup is a feature of the Windows Server 2008 operating system that provides a basic backup and recovery solution for the server that it is installed on. This version of Windows Server Backup replaces the Backup feature that was available with earlier versions of the Windows operating system.
Overview of Windows Server Backup

Windows Server Backup is a feature in Windows Server 2008 that you can use to back up and recover the operating system and restore files and folders that are stored on the server.

With Windows Server Backup, you can:
- Protect your entire server without using separate backup and recovery technology
- Back up an entire server or selected volumes
- Use the wizards and tools and the Complete PC Restore feature to assist in recovering a server
- Set up an automatic backup schedule
- Recover items or entire volumes

Key Points
Backup is an optional feature in Windows Server 2008 that helps you reliably back up and recover the operating system, and restore files and folders that are stored on the server. Backup consists of a Microsoft Management Console (MMC) snap-in and command-line tools.

Important: The MMC snap-in is not available on Windows Server 2008 Standard Edition and all core installations. To manage backups for a computer with Windows Server 2008 Standard Edition installed, you must use the snap-in on another computer to manage the backups remotely or use command-line tools on the local computer.
New Features of Window Server Backup

- Faster backup technology
- Simplified restoration
- Simplified recovery of your operating system
- Ability to recover applications
- Improved scheduling
- Offsite removal of backups for disaster protection
- Remote administration
- Automatic disk usage management
- Extensive command-line support
- Support for DVD media

Key Points
The Backup feature includes the following improvements:

- Faster backup technology
- Simplified restoration
- Simplified recovery of your operating system
- Ability to recover applications
- Improved scheduling
- Offsite removal of backups for disaster protection
- Remote administration
- Automatic disk usage management
- Extensive command-line support
- Support for DVD media
The Ntbackup.exe tool can be used to mount tapes from previous versions of backup in Windows 2000 and Windows 2003. You cannot, however, use it to create new backups on Windows Server 2008.

**Question:** Why would a company want to separate the Backup and Restore roles?

**Additional Reading**
- What’s New in AD DS Backup and Recovery?
- Windows Server 2008 Technical Library
Who Can Back Up Data?

Key Points
By default, members of the Backup Operators and Administrators groups have access to the Backup tool. This right can also be delegated to other groups or individuals.

- **By default, members in the following groups can backup and restore data on the server:**
  - Administrators
  - Server Operators
  - Backup Operators
- **Consider using custom groups that separate the backup and restore User Rights Assignments to increase security**
- **Limit the number users that belong to the default groups with backup/restore rights**

**Note:** Limit the number of users who belong to the Administrators or Backup Operators groups on the server. Members of these groups can use Backup.

Additional Reading
- What's New in AD DS Backup and Recovery?
What is System State Data?

<table>
<thead>
<tr>
<th>Component</th>
<th>When is this component included in System State?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registry</td>
<td>Always</td>
</tr>
<tr>
<td>COM+ Class Registration database</td>
<td>Always</td>
</tr>
<tr>
<td>Boot files, including the system files</td>
<td>Always</td>
</tr>
<tr>
<td>Active Directory Certificate Services database</td>
<td>If it is a Certificate Services server</td>
</tr>
<tr>
<td>Active Directory Domain Services database</td>
<td>If it is a domain</td>
</tr>
<tr>
<td>SYSVOL directory</td>
<td>Only if it is a domain controller</td>
</tr>
<tr>
<td>Cluster service information</td>
<td>If it is within a cluster</td>
</tr>
<tr>
<td>IIS Metadirectory</td>
<td>If it is installed</td>
</tr>
<tr>
<td>System files that are under Windows Resource Protection</td>
<td>Always</td>
</tr>
</tbody>
</table>

Key Points

Windows Server 2008 does not back up or recover system state data in the same manner as servers that run Windows Server 2003 or Windows 2000 Server. In Windows Server 2008, you must back up critical volumes rather than only backing up system state data.

In Windows Server 2008, the system components that make up system state data depend on the server roles that are installed on the computer and which volumes host the critical files that the operating system and the installed roles use.

Additional Reading

- What’s New in AD DS Backup and Recovery?
Optimizing Backup Performance

Key Points
You can optimize backup performance by choosing one of the following settings available under the **Configure Performance Settings** option in the **Actions** pane of Windows Server Backup:

- Always perform full backup
- Always perform incremental backup
- Custom

Additional Reading
- What's New in AD DS Backup and Recovery?
Specifying a Backup Time

Key Points
You can use the Backup Schedule Wizard from the Actions pane within Windows Server Backup to create a schedule and options for backup.

When you have a backup schedule in place, backups will run automatically each day. When you create a backup schedule, you can:

- Back up the entire server or specific volumes only.
- Run Backup daily or more often.

Question: Do you have any data in your organization for which you would need a customized schedule for backups? For example, a schedule that backs up data numerous times in a day?

Additional Reading
- Windows Server 2008 Backup and Recovery Step-by-Step Guide
How is Data Restored?

![Recovery Wizard]

**Key Points**

Data restoration is done through the Windows Server Backup tool. This tool is not installed by default; it is a feature that must be installed using the Initial Configuration Wizard or the Server Manager tool.

After you have successfully backed up data, you can use the Recover option in the Actions pane of the Windows Server Backup tool to recover volumes, folders and files on the local server or on a different server to which you connect remotely.

**Question:** Why would you consider a restoration of data to a different location other than the original location?

**Additional Reading**

- What’s New in AD DS Backup and Recovery?
Demonstration: Installing and Configuring Windows Server Backup

In this demonstration, you will see how to install and configure Windows Server Backup.
Lesson 2

Configuring Shadow Copies

- What are Shadow Copies?
- Shadow Copy Scheduling
- Demonstration: Configuring Shadow Copies
- Managing Shadow Copies from a Client Perspective
- Restoring Shadow Copies
- Demonstration: Restoring Shadow Copies

In Windows Server 2008 as in Windows Server 2003, you can enable shadow copies on a per volume basis which will monitor changes made to shares over the network, giving the user the opportunity to self help for file and folder recovery.
What are Shadow Copies?

- **Shadow copies provide iterative versions of network folders**
- **Use shadow copies to:**
  - Recover files
  - Review previous versions
- **Shadow copies are:**
  - Enabled per volume
  - Not a replacement for regular backups
  - Allocated storage limits versions

Key Points
You can use the Previous Versions feature in Windows Server 2008 to enable your users to access previous versions of files and folders on your network. This is useful because users can:

- Recover files that were accidentally deleted.
- Recover from accidentally overwriting a file.
- Compare versions of a file while working.

**Question:** If you were to deploy shadow copies of shared folders in your network environment, would you notice a decrease in calls from users needing restoration from backups?

**Additional Reading**
- Windows Server 2008 Help Topic: How do I use Previous Versions?
Shadow Copy Scheduling

Key Points
If you enable shadow copies of shared folders on a volume using the default values, tasks will be scheduled to create shadow copies at 7:00 A.M. and Noon. The default storage area will be on the same volume, and its size will be 10 percent of the available space.

If you decide that you want shadow copies to be made more often, verify that you have allotted enough storage space and that you do not make copies so often that it degrades server performance.

**Question:** How might you consider modifying the default schedule for your environment? Do you have data in shares that might require a more aggressive schedule?

**Additional Reading**
- Windows Server 2008 Help Topic: Enable and Configure Shadow Copies of Shared Folders
Demonstration: Configuring Shadow Copies

**In this demonstration, you will see how to configure shadow copies**
Managing Shadow Copies from a Client Perspective

Key Points
For previous versions of the Windows operating system, the Previous Versions client software must to be installed for the user to be able to make use of shadow copies. Microsoft Windows Vista has the Previous Versions client built-in to the operating system, so client configuration is not necessary.

Question: What might be the problem if a user calls the Help Desk and complains that the Previous Versions tab is missing from the shared folder/file properties?

Additional Reading
• Windows Server 2008 Help Topic: How do I use Previous Versions?
Restoring Shadow Copies

<table>
<thead>
<tr>
<th>If...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>No previous versions</td>
<td>The file was not modified after the last save</td>
</tr>
<tr>
<td>Restoring a folder</td>
<td>The current version is deleted</td>
</tr>
<tr>
<td>Restoring a file</td>
<td>File permissions are not changed</td>
</tr>
<tr>
<td>Properties dialog box does not include a Previous Versions tab</td>
<td>Shadow copies might not be enabled</td>
</tr>
<tr>
<td>Copying a file</td>
<td>File permissions are set to default</td>
</tr>
</tbody>
</table>

Key Points
After you enable shadow copies of shared folders and start creating shadow copies, you can use the Previous Versions feature to recover previous versions of files and folders, or files and folders that have been renamed or were deleted.

Additional Reading
- Windows Server 2008 Help Topic: How do I restore a previous version of a file or folder?
Demonstration: Restoring Shadow Copies

In this demonstration, you will see how to restore a shadow copy.
Lesson 3
Providing Server and Service Availability

- Network Load Balancing Manager Overview
- Demonstration: Installing Network Load Balancing
- Creating a Network Load Balancing Cluster
- Demonstration: Configuring a Network Load Balancing Cluster
- What Is a Failover Cluster?
- Hardware Requirements for a Failover Cluster

Network Load Balancing is a clustering technology offered by Microsoft. Network Load Balancing uses a distributed algorithm to load balance network traffic across a number of hosts, helping to enhance the scalability and availability of mission critical, IP-based services, such as Web, Virtual Private Networking (VPN), Streaming Media, Terminal Services, Proxy, and so on. It also provides high availability by detecting host failures and automatically redistributing traffic to operational hosts.
Network Load Balancing Manager Overview

Key Points
When Network Load Balancing is installed as a network driver on each of the member servers, or hosts, in a cluster, the cluster presents a virtual IP address to client requests. The client requests go to all the hosts in the cluster, but only the host to which a given client request is mapped accepts and handles the request. All the other hosts drop the request. Depending on the configuration of each host in the cluster, the statistical mapping algorithm, which is present on all the cluster hosts, maps the client requests to particular hosts for processing.

Using Network Load Balancing with Terminal Services offers the benefits of increased availability, scalability, and load-balancing performance, as well as the ability to distribute a large number of Terminal Services clients over a group of terminal servers.

Question: Do you have any servers hosting stateless information that would benefit from Network Load Balancing in your environment?
Additional Reading

- How Network Load Balancing Technology Works
- Windows Server 2008 Technical Library
Demonstration: Installing Network Load Balancing

In this demonstration, you will see how to install Network Load Balancing.
Creating a Network Load Balancing Cluster

Key Points
To configure the Network Load Balancing cluster, you must configure three types of parameters:

- Host parameters, which are specific to each host in a Network Load Balancing cluster.
- Cluster parameters, which apply to a Network Load Balancing cluster as a whole.
- Port rules, which control how the cluster functions.

You must be a member of the Administrators group on the host that you are configuring, or you must have been delegated the appropriate authority to use Network Load Balancing Manager. If you are configuring a cluster or host by running Network Load Balancing Manager from a computer that is not part of the cluster, you do not have to be a member of the Administrators group on that computer.
Additional Reading

- Windows Server 2008 Network Load Balancing Help topic: Create a new network load balancing cluster
Demonstration: Configuring a Network Load Balancing Cluster

In this demonstration, you will see how to configure a Network Load Balancing cluster.
What is a Failover Cluster?

A failover cluster is a group of independent computers that work together to increase the availability of applications and services.

Failover clusters include:

- A new validation feature to ensure that the system, storage, and network configuration is suitable for a cluster
- Improved cluster setup
- Simplified configuration interface
- Improved stability and security, which increases availability
- Improved cluster communication with storage, which improves the performance of a SAN or DAS
- Configuration options that eliminate the need for the quorum as a single point of failure
- Improvements to the software infrastructure, networking and security, which increase reliability and availability

Key Points

A failover cluster is a group of independent computers that work together to increase the availability of applications and services. The clustered servers (called nodes) are connected by physical cables and by software. If one of the cluster nodes fails, another node begins to provide service (a process known as failover). Users experience a minimum of service disruptions.

Note: The failover cluster feature is not available in Windows Web Server 2008 or Windows Server 2008 Standard editions.

Failover clusters include the following new functionality:

- New validation feature
- Support for globally unique identifier (GUID) partition table (GPT) disks in cluster storage
Improvements to existing failover cluster functionality include:

- Improved cluster setup
- Simplified management interfaces
- Improvements to stability and security, which can result in increased availability
- Improvements to the way a cluster works with storage
- Improvements to interfaces for working with shared folders
- Improvements to networking and security

Additional Reading

- Windows Server 2008 Technical Library
Hardware Requirements for a Failover Cluster

Key Points
Carefully review the hardware on which you plan to deploy a failover cluster to ensure that it is compatible with Windows Server 2008. This is especially necessary if you are currently using that hardware for a server cluster running Windows Server 2003. Hardware that supports a server cluster running Windows Server 2003 will not necessarily support a failover cluster running Windows Server 2008.

The following hardware is required in a failover cluster:

- Servers
- Network adapters and cable (for network communication)
- Device controllers or appropriate adapters for the storage
- Storage

**Question:** If you presently have a server cluster in a previous server version, can you do a rolling upgrade to Windows Server 2008 Failover Clustering?

**Additional Reading**

- Windows Server 2008 Technical Library
Lab: Configuring Availability of Network Resources

- Exercise 1: Configuring Windows Server Backup and Restore
- Exercise 2: Configuring Shadow Copying
- Exercise 3: Configuring and Testing Network Load Balancing

Logon information

<table>
<thead>
<tr>
<th>Virtual machine</th>
<th>NYC-DC1, NYC-SVR1 and NYC-CL1</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Administrator</td>
</tr>
<tr>
<td>Password</td>
<td>Pa$$w0rd</td>
</tr>
</tbody>
</table>

Estimated time: 60 minutes

Objectives

- Configure Windows Server Backup and Restore
- Configure shadow copies
- Configure and test Network Load Balancing
Lab Setup
For this lab you will use the available virtual machine environment. Before you begin the lab, you must:

- Start the NYC-DC1, NYC-SVR1 and NYC-CL1 virtual machines.
- Log on to the NYC-DC1, NYC-SVR1 and NYC-CL1 virtual machines with the user name administrator and the password Pa$$w0rd.
- On the Windows 2008 servers, close the Initial Configuration Tasks window that appears after log on.
- On the Windows 2008 servers, close the Server Manager window.

Scenario
The Windows Infrastructure Services Technology Specialist has been tasked with configuring disaster recovery restore and availability for all critical services.
Exercise 1: Configuring Windows Server Backup and Restore

In this exercise, you will configure Windows Server Backup.

The main tasks are as follows:
1. Ensure that you have completed the steps in the Lab Setup.
2. Open the Server Manager tool on 6421A-NYC-DC1.
3. Install the Windows Server Backup feature.
4. Create a share on 6421A-NYC-SVR1.
5. Manually back up files to a network location.
6. Restore files from a network location.

▶ Task 1: Ensure that you have completed the steps in the Lab Setup
   - Review the Lab Setup section and ensure you have completed the steps before you continue with this lab.

▶ Task 2: Open the Server Manager tool on 6421A-NYC-DC1
   - On 6421A-NYC-DC1, open Server Manager from the Administrative Tools menu.

▶ Task 3: Install the Windows Server Backup feature
   1. On NYC-DC1, open Server Manager.
   2. Using Server Manager, install the Windows Server Backup feature.
   3. On the Installation Results page, verify that the Windows Server Backup installation succeeded, and then click Close.
Task 4: Create a share on 6421A-NYC-SVR1

1. On NYC-SVR1, open the Computer Management administrative tool.
2. In the Computer Management list pane, expand Shared Folders, and then right-click Shares.
3. In the context menu that appears, click New Share.
4. Using the New Share Wizard, create a new share on the C:\ drive called NetBackup.
5. On the Shared Folder Permissions page, select Administrators have full access; other users have no access, and then click Finish.

Task 5: Manually back up files to a network location

1. On NYC-DC1, open the Windows Server Backup administrative tool from the Start menu, Administrative Tools location.
2. On the Actions pane of the Windows Server Backup (Local) window, select Backup Once.
3. On the Backup Options page of the Backup Once Wizard, click Next.
4. On the Specify backup type page, select Custom, and then click Next.
5. On the Select Backup Items page, clear the Enable System Recovery and Local Disk (C:), checkboxes, select Allfiles (D:), and then click Next.
6. On the Specify destination type page, select Remote Shared Folder, and then click Next.
7. On the Specify Remote Folder page, type a path of \NYC-SVR1\NetBackup, and then click Next.
8. On the Specify VSS backup type page, select VSS full backup, and then click Next.
10. On the Backup Progress page, verify the status is Backup Completed, and then click Close.
Task 6: Restore files from a network location

1. Click Start, click Computer, and then double-click Allfiles (D:).
2. In the details pane of the Allfiles (D:) window, delete the AllFiles directory, and then close the Allfiles (D:) window.
4. On the Recovery Wizard, Getting Started page, select Another Server, and then click Next.
5. On the Specify Location Type page, select Remote Shared Folder, and then click Next.
6. On the Specify Remote Folder page, type the URL of \NYC-SVR1\NetBackup, and then click Next.
7. On the Select backup date page, click today’s date (in bold), and then click Next.
8. On the Select Recovery Type page, accept the default of Files and Folders, and then click Next.
9. On the Select Items to Recover page, expand NYC-DC1, expand Allfiles (D:), select Labfiles, and then click Next.
10. On the Specify Recovery Options page, accept the default settings, and then click Next.
12. In the Recovery Progress window, verify the status is Restore of Files completed, and then click Close.
Exercise 2: Configuring and Testing Shadow Copies
In this exercise, you will configure and test shadow copies.
The main tasks are as follows:
1. Enable shadow copies on a volume.
2. Change a file in a share location.
3. Manually create a shadow copy.
4. View the previous versions of the file and restore to a previous version.

► Task 1: Enable shadow copies on a volume
1. On NYC-DC1, open the Computer Management console.
2. In the console tree of the Computer Management window, right-click Shared Folders, point to All Tasks, and then click Configure Shadow Copies.
3. In the Shadow Copies dialog box, select volume D:\, and then click Enable.
4. In the Enable Shadow Copies dialog box that appears, click Yes, and then click OK.
5. Leave the Computer Management console open.

► Task 2: Change a file in a share location
1. On NYC-CL1, click Start, and in the search text box type \NYC-DC1\shadow.
   A window should open with the contents of the Shadow share visible.
2. Open the shadowtest.txt file.
3. Add the following line of text to the end of the text file:
   This is my text that I am adding to the file.
4. Save and close the shadowtest.txt file.
Task 3: Manually create a shadow copy

1. On NYC-DC1, in the Computer Management console, right-click Shared Folders, point to All Tasks, and then click Configure Shadow Copies.

2. In the Shadow Copies dialog box, select volume D:\, and then click Create Now.
   
The shadow copies of selected volume should have two entries listed.


Task 4: View the previous versions of the file and restore to a previous version

1. On NYC-CL1, click Start, type \NYC-DC1\shadow in the Search text box, and then press ENTER.

2. Right-click shadowtest.txt and select Properties from the context menu.

3. In the Properties dialog box for the shadowtest.txt file, click the Previous Versions tab.

4. Under File Versions, you should see the last shadow copy that was created. Click Open to view the contents of the file. The file you are viewing should be the previous version of the file you modified with text.

5. Close the file and select Restore from the Previous Versions window to restore the file to its previous state before any changes were made.

6. In the Previous Versions dialog box, click OK.

7. Click OK to close the shadowtest.txt Properties dialog box.
**Exercise 3: Configuring Network Load Balancing**

In this exercise, you will configure Network Load Balancing.

The main tasks are as follows:

1. Install the Network Load Balancing feature on NYC-DC1 and NYC-SVR1.
2. Configure Network Load Balancing on NYC-DC1 and NYC-SVR1.
3. Install and share an IP-based printer on both NYC-DC1 and NYC-SVR1.
4. Use NYC-CL1 to connect to the shared printer object on the NLB virtual IP address.
5. Close all virtual machines and discard undo disks.

► **Task 1: Install the Network Load Balancing feature on NYC-DC1 and NYC-SVR1**

1. On NYC-DC1, open Server Manager.
2. In the Server Manager list pane, right-click Features, and install Network Load Balancing.
3. On the Results page, verify the installation succeeded, and then close the Add Features Wizard.
4. Repeat steps 1 through 3 for NYC-SVR1.
5. Close Server Manager on both NYC-DC1 and NYC-SVR1.

► **Task 2: Configure Network Load Balancing on NYC-DC1 and NYC-SVR1**

1. On NYC-DC1, open Network Load Balancing Manager.
2. In the Network Load Balancing Manager console, right-click Network Load Balancing Clusters in the list pane, and then click New Cluster.
3. In the New Cluster: Connect dialog box, type the hostname NYC-DC1, and then click Connect. You should see the Interface Name section populate with the Local Area Connection and IP address of that interface. Click Next.
4. In the New Cluster: Host Parameters dialog box, verify the default state is Started, and then click Next.
5. In the **New Cluster: Cluster IP Addresses** dialog box, click **Add** and specify an IPV4 cluster IP of **10.10.0.100** with a Subnet Mask of **255.255.0.0**, and then click **OK**.

6. In the **New Cluster: Cluster Parameters** dialog box, type a Full Internet Name of **printSVR.woodgrovebank.com**. Specify a cluster operation mode of **Multicast**, and then click **Next**.

7. In the **New Cluster: Port Rules** dialog box, click **Finish**.

8. In the **Network Load Balancing Manager** console list pane, right-click **printSVR.woodgrovebank.com**, and then click **Add Host to Cluster** from the context menu.

9. In the **Add Host to Cluster: Connect** dialog box, specify the host as **NYC-SVR1**, and then click **Connect**. In the **Interfaces available for configuring the cluster**, click **Local Area Connection**, and then click **Next**.

10. In the **Add Host to Cluster: Host Parameters** dialog box, accept the default settings, and then click **Next**.

11. In the **Add Host to Cluster: Port Rules**, accept the default settings, and then click **Finish**.

12. Close the **Network Load Balancing Manager** console window.

► **Task 3: Install and share an IP-based printer on both NYC-DC1 and NYC-SVR1**

1. On NYC-DC1, click **Start**, click **Control Panel**, and then double-click the **Printers** applet.

2. In the **Printers** console details pane, double-click **Add Printer**.

3. Add a local printer with a **Standard TCP/IP Port** with an address of **10.10.0.80**. Clear the **Query the printer and automatically select the driver to use** check box, and then click **Next**.

4. Wait for the detection of the TCP/IP port to complete, and then click **Next** in the **Additional Port information Required** dialog box.

5. In the **Install the printer driver** dialog box, specify the manufacturer of **HP** and the printer model of **LaserJet 6MP**, and then click **Next**.

6. In the **Type a printer name** dialog box, accept the default settings, and then click **Next**.
7. In the **Printer Sharing** dialog box, accept the default name, and then click **Next**.

8. In the **You’ve successfully added HP LaserJet 6MP** dialog box, click **Finish**.

9. Close the **Printers** control panel applet.

10. Repeat steps 1 through 9 on NYC-SVR1.

**Task 4: Use NYC-CL1 to connect to the shared printer object on the NLB virtual IP address**

1. On NYC-CL1, click **Start**, type `\printSVR.woodgroovebank.com` in the **Start Search** text box, and then press ENTER.

2. From the available resources on the `printSVR.woodgroovebank.com` cluster, double-click the **HP LaserJet 6MP** printer object to install it on NYC-CL1.

3. Close the **Printer Status** window and close the **printSVR** browse window.

   The HP 6MP is now installed using the NLB cluster as the host of the printer.

**Task 5: Close all virtual machines and discard undo disks**

1. On the host computer, click **Start**, point to **All Programs**, point to **Microsoft Virtual Server**, and then click **Virtual Server Administration Website**.

2. Under **Navigation**, click **Master Status**. For each virtual machine that is running, click the **virtual machine name**, and in the context menu, click **Turn off Virtual Machine and Discard Undo Disks**. Click **OK**.
Module Review and Takeaways

- Review Questions
- Best Practices

Review Questions
1. What are the benefits of using VSS and block-level technologies compared to traditional types of file-based backups?
2. What is the danger of choosing to restore a folder in Shadow Copies?
3. How is failover clusters different from Network Load Balancing?
Best Practices
Consider the following best practices for Network Load Balancing:

- Properly secure the Network Load Balancing hosts and the load-balanced applications.
  - Network Load Balancing does not provide additional security for the load balanced hosts and cannot be used as a firewall. It is important to properly secure the load balanced applications and hosts. Security procedures can typically be found in the documentation for each particular application. For example, if you are using Network Load Balancing to load balance a cluster of Internet Information Services (IIS) servers, you should follow the procedures and guidelines for securing IIS.
  - The Network Load Balancing subnet must be physically protected from intrusion by unauthorized computers and devices in order to avoid interference from unauthorized heartbeat packets.

- Use two or more network adapters in each cluster host whenever possible. Two network adapters, however, are not required.
  - If the cluster is operating in unicast mode (the default), Network Load Balancing cannot distinguish between single adapters on each host. Therefore, any communication among cluster hosts is not possible unless each cluster host has at least two network adapters.
  - You can configure Network Load Balancing on more than one network adapter. However, if you use a second network adapter to address this best practice, make sure that you install Network Load Balancing on only one adapter (called the cluster adapter).

- Use only the TCP/IP network protocol on the cluster adapter.
- Do not add any other protocols (for example, IPX) to this adapter.
• Enable Network Load Balancing Manager logging.

• You can configure Network Load Balancing manager to log each Network Load Balancing Manager event. This log can be very useful in troubleshooting problems or errors when using Network Load Balancing Manager. Enable Network Load Balancing Manager logging by clicking Log Settings in the Network Load Balancing Manager Options menu. Select the Enable logging check box and specify a name and location for the log file.

The Network Load Balancing Manager log file contains potentially sensitive information about the Network Load Balancing cluster and hosts, so it must be properly secured. By default, the log file inherits the security settings of the directory in which it is created, so you may need to change the explicit permissions on the file to restrict read and write access to those individuals who do not need full control of the file. Be aware that the individual using Network Load Balancing Manager does require full control of the log file.

• Verify that any given load-balanced application is started on all cluster hosts on which the application is installed.

• Network Load Balancing does not start or stop applications.

Additional Reading

• Network Load Balancing Best Practices
Module 14

Configuring Server Security Compliance

Contents:
Lesson 1: Securing a Windows Infrastructure 14-3
Lesson 2: Using Security Templates to Secure Servers 14-11
Lesson 3: Configuring an Audit Policy 14-17
Lesson 4: Overview of Windows Server Update Services 14-22
Lesson 5: Managing WSUS 14-30
Lab: Configuring Server Security Compliance 14-35
Module Overview

- Securing a Windows Infrastructure
- Using Security Templates to Secure Servers
- Configuring an Audit Policy
- Overview of Windows Sever Update Services
- Managing WSUS

This module explains how to secure servers and maintain update compliance. It explains how to secure a server role within a Windows infrastructure and how to secure servers using security templates. This module also explains how to configure an audit policy and manage updates using Windows Server Update Services.
Lesson 1
Securing a Windows Infrastructure

- Challenges of Securing a Windows Infrastructure
- Applying Defense-in-Depth to Increase Security
- Core Server Security Practices
- What is the Security Configuration Wizard?
- What is Windows Firewall?
- Demonstration: Using the Security Configuration Wizard to Secure Server Roles

This lesson explains how to secure a server role within a Windows infrastructure. As organizations expand the availability of network data, applications, and systems, it becomes more challenging to ensure the security of the network infrastructure. Security technologies in the Windows Server 2008 operating system enable organizations to better protect their network resources and organizational assets in increasingly complex environments and business scenarios.
Challenges of Securing a Windows Infrastructure

Challenges of securing a Windows infrastructure include:

- Implementing and managing secure configuration of servers
- Protecting against malicious software threats and intrusions
- Implementing effective identity and access control

Key Points
Each server role requires specific security configurations depending upon your deployment scenario and infrastructure requirements. The documentation that supports each server role contains security information and other security considerations. Additionally, some server roles have more of a security focus, such as Active Directory Rights Management Services (AD RMS) or Active Directory Certificate Services (AD CS), than others. For a complete list of available server roles, run the Server Manager Wizard from the Administrative Tools menu.

Additional Reading
Applying Defense-in-Depth to Increase Security

**Key Points**

After you have discovered and documented the risks your organization faces, the next step is to examine and organize the defenses you will use to provide your security solution. The defense-in-depth security model is an excellent starting point for this process. This model identifies seven levels of security defenses that are designed to ensure that any attempt to compromise the security of an organization will be met by a robust set of defenses. Each set is capable of deflecting attacks at many different levels.

**Question:** What is the most important part of the defense-in-depth security model?

**Additional Reading**

- Antivirus Defense-in-Depth Guide
Core Server Security Practices

Key Points
Without physical security, you have no security. Core server security practices are relatively easy to adopt and should be integrated into the standard security configuration of all servers. Some of the core server security practices should include:

- Apply the latest service packs and all available security and critical updates.
- Use the Security Configuration Wizard to scan and implement server security based on server roles.
- Use Group Policy and security templates to harden servers and lessen the attack footprint.
- Restrict scope of access for service accounts to lessen damage should the account be compromised.
- Restrict who can log on locally to server consoles by using security options.
- Restrict physical and network access to servers.
**Question:** Does your company have a detailed "build sheet" for all new installations that occur on new hardware? What can you do to lessen the attack footprint on your infrastructure?

**Additional Reading**
- Security and Protection
What is the Security Configuration Wizard?

SCW provides guided attack surface reduction

- Disables unnecessary services and IIS Web extensions
- Blocks unused ports and secure ports that are left open using IPsec
- Reduces protocol exposure
- Configures audit settings

SCW supports:

- Rollback
- Analysis
- Remote configuration
- Command-line support
- Active Directory integration
- Policy editing

Key Points

The Security Configuration Wizard (SCW) guides you through the process of creating, editing, applying, or rolling back a security policy. A security policy that you create with SCW is an .xml file that, when applied, configures services, network security, specific registry values, and audit policy.

SCW is a role-based tool that you can use to create a policy that enables services, firewall rules, and settings that are required for a selected server to perform specific roles. For example, a server might be a file server, a print server, or a domain controller.

Question: Does your organization use the Security Configuration Wizard for role-based security settings? How does a security template differ from the policy defined by SCW?

Additional Reading

What is Windows Firewall?

Windows Firewall is a stateful host-based application that provides the following features:

- Filters both incoming and outgoing network traffic
- Integrates both firewall filtering and IPsec protection settings
- Can be managed by the Control Panel tool or by the more advanced Windows Firewall with Advanced Security MMC console
- Provides Group Policy support
- Enabled by default in new installs

Key Points

Windows Firewall with Advanced Security combines a host firewall and IPsec. Unlike a perimeter firewall, Windows Firewall with Advanced Security runs on each computer running Windows Server 2008 and provides local protection from network attacks that might pass through your perimeter network or originate inside your organization. It also provides computer-to-computer connection security that allows you to require authentication and data protection for communications.

Question: How is Windows Firewall different from a perimeter firewall?

Additional Reading

- Windows Firewall with Advanced Security Help Topic: Windows Firewall with Advanced Security
Demonstration: Using the Security Configuration Wizard to Secure Server Roles

In this demonstration, you will see how to implement security using the Security Configuration Wizard
Lesson 2:
Using Security Templates to Secure Servers

- What is a Security Policy?
- What are Security Templates?
- Demonstration: Configuring Security Template Settings
- What is the Security Configuration and Analysis Tool?
- Demonstration: Analyzing Security Policy Using the Security Configuration and Analysis Tool

Security templates have existed since Windows NT 4.0 Service Pack 4. These security templates have become a popular method for applying security settings to not only servers, but also to the desktop environment. One reason for the success of security templates is that they provide a wide range of security settings and they are easy to implement in various environments. A single security template can configure a broad scope of security settings on a multitude of servers and desktop computers.
What is a Security Policy?

Key Points
A security policy in a Windows environment is a collection of security settings that are related and applied to different areas of the system.

Local policies can be useful in non-Active Directory Domain Services (AD DS) environments because they are applied at the local computer level. Domain policies tend to have more settings available to be configured and can use Group Policy as a means of deployment.

**Question:** Does your organization use security templates at the local computer level or domain-based GPO's with imported templates?

**Additional Reading**
- Windows Server 2008 Technical Library
What are Security Templates?

A security template is a collection of configured security settings used to apply a security policy.

**Security Templates:**
- Created and modified using the Security Templates MMC snap-in
- Default security templates stored in %SystemRoot%\Security\Templates
- Custom security templates are stored in local user profile folder

**Deployment Considerations:**
- Create templates based upon server role
- Deploy to individual computers using the SECDIT command
- Deploy to groups of computers using Group Policy

**Key Points**
A security template contains hundreds of possible settings that can control a single computer or multiple computers. The security templates can control areas such as user rights, permissions, and password policies. Security templates can be deployed centrally using Group Policy objects (GPOs). Finally, security templates can be customized to include almost any security setting on a target computer.

**Additional Reading**
- Predefined security templates
Demonstration: Configuring Security Template Settings

**In this demonstration, you will see how to:**

- Add the Security Templates snap-in and configure a custom security template for the DHCP server role
- Import a security template into Active Directory
What is the Security Configuration and Analysis Tool?

Key Points
You can use the Security Configuration and Analysis tool to analyze and configure local system security.

Regular analysis enables you to track and ensure an adequate level of security on each computer as part of an enterprise risk management program. You can tune the security levels and, most importantly, detect any security flaws that may occur in the system over time.

You can also use Security Configuration and Analysis to configure local system security.

Additional Reading
• Security Configuration and Analysis
Demonstration: Analyzing Security Policy using the Security Configuration and Analysis Tool

In this demonstration, you will see how to use the Security Configuration and Analysis Tool to analyze and configure local security policy settings.
Lesson 3
Configuring an Audit Policy

- What is Auditing?
- What is an Audit Policy?
- Types of Events to Audit
- Demonstration: How to Configure Auditing

You can configure an audit policy so that user or system activity in specified event categories is recorded. You can monitor security-related activity, such as who accesses an object, if a user logs on to or logs off from a computer, or if changes are made to an auditing policy setting.

As a best practice, you should create an audit plan before implementing audit policy.
What is Auditing?

**Key Points**

Auditing is the process that tracks the activities of users by recording selected types of events in the security log of a server or a workstation.

The most common types of events to be audited are:

- Access to objects, such as files and folders.
- Management of user accounts and group accounts.
- Users logging onto and logging off from the system.

**Question:** What are some reasons that you may want to audit certain areas of a system or a particular shared resource?

**Additional Reading**

- Auditing overview
What is an Audit Policy?

**Key Points**

An audit policy determines the security events to be reported to the network administrator. When you implement an audit policy:

- Specify the categories of events that you want to audit.
- Set the size and behavior of the security log.
- If you want to audit directory service access or object access, determine which objects to monitor access to and what type of access to monitor.

**Additional Reading**

- Auditing overview
Types of Events to Audit

- Account Logon
- Account Management
- Directory Service Access
  - Directory Service Changes
  - Directory Service Replication
  - Detailed Directory Service Replication
- Logon
- Object Access
- Policy Change
- Privilege Use
- Process Tracking
- System

Key Points
Before you implement an auditing policy, you must decide which event categories to audit. The auditing settings that you choose for the event categories define your auditing policy.

You can create an auditing policy that suits the security needs of your organization by defining auditing settings for specific event categories.

**Question:** What categories of events does your company presently audit? If your company is not auditing, what event categories would you like to see audited in your organization?

Additional Reading
- Auditing overview
Demonstration: How to Configure Auditing

In this demonstration, you will see how to:

- Enable auditing for various events
- Enable object access auditing
Lesson 4
Overview of Windows Server Update Services

- What is Windows Server Update Services?
- Windows Server Update Services Process
- Server Requirements for WSUS
- Automatic Updates Configuration
- Demonstration: Installing and Configuring WSUS

This lesson introduces Windows Server Update Services (WSUS), which is a tool for managing and distributing software updates that resolve security vulnerabilities and other stability issues.

WSUS enables you to deploy the latest Microsoft product updates to computers running the Windows operating system.
What is Windows Server Update Services?

Key Points

WSUS enables you to deploy the latest Microsoft product updates to computers running Windows Server 2003, Windows Server® 2008, Windows Vista™, Microsoft Windows® XP with Service Pack 2, and Windows 2000 with Service Pack 4 operating systems. By using WSUS, you can fully manage the distribution of updates that are released through Microsoft Update to computers in your network.

WSUS 3.0 provides improvements in the following areas:

- Ease of use
- Improved deployment options
- Better support for complex server hierarchies
- Better performance and bandwidth optimization
- The ability to extend WSUS 3.0 using improved APIs
Question: What Microsoft operating systems can make use of the WSUS services?

Additional Reading
- Microsoft Windows Server Update Services 3.0 Overview
- New in Windows Server Update Services 3.0
Key Points
The Microsoft recommended approach to the update management process consists of an ongoing set of four phases; assess, identify, evaluate and plan, and deploy. It is essential to repeat the update management process on an ongoing basis, as new updates become available that can enhance and protect the production environment.

Additional Reading
- Microsoft Windows Server Update Services 3.0 Overview
Server Requirements for WSUS

Key Points
Prerequisites for WSUS servers include:

- Windows Server 2003 SP1 or later, or Windows Server 2008
- Microsoft Internet Information Services (IIS) 6.0 or later
- Windows Installer 3.1 or later
- Microsoft .NET Framework 2.0
- SQL Server 2005 SP1 or later (optional)
- Microsoft Report Viewer Redistributable 2005

Hardware and database software requirements are driven by the number of client computers being updated in your organization. A WSUS server using the recommended hardware can support a maximum number of 20,000 clients. Both the system partition and the partition on which you install WSUS must be formatted with the NTFS file system.
**Question:** How do language options for updates effect the server requirements for WSUS 3.0?

**Additional Reading**
- Deploying Microsoft Windows Server Update Services 3.0
Key Points

You can use Group Policy or the registry to configure Automatic Updates. Configuring Automatic Updates involves pointing the client computers to the WSUS server, making sure that the Automatic Updates software is up to date, and configuring any additional environment settings.

How best to configure Automatic Updates and WSUS environment options depends upon your network environment. In an Active Directory environment, you use Group Policy, while in a non-Active Directory environment, you might use the Local Group Policy object or edit the registry directly.

**Question:** When would you use the registry-based configuration for client configuration of Automatic Updates as opposed to using Group Policy?

**Additional Reading**
- Deploying Microsoft Windows Server Update Services 3.0
Demonstration: Installing and Configuring WSUS

In this demonstration, you will see how to:

- Install WSUS
- Configure Automatic Update client settings using Group Policy
Lesson 5
Managing WSUS

- WSUS Administration
- Managing Computer Groups
- Approving Updates
- Demonstration: Managing WSUS

This lesson explains how to manage WSUS by performing administrative tasks using the WSUS 3.0 administration console, managing computer groups to target updates to specific computers, and approving the installation of updates for all the computers in your WSUS network or for different computer groups.
WSUS Administration

Key Points
The WSUS 3.0 administration console has changed from a Web-based console to a plug-in for Microsoft Management Console (MMC) version 3.0.

The WSUS 3.0 administration console also enables you to:

- Manage WSUS remotely.
- Configure post-setup tasks using a wizard.
- Generate multiple reports with improved precision.
- Maintain server health more easily.

Question: How do you manage the WSUS infrastructure remotely from another server or workstation?

Additional Reading
- Client Behavior with Update Deadlines
Managing Computer Groups

- Computers are automatically added
- Default computer groups
  - All Computers
  - Unassigned Computers
- Client-side targeting

Key Points
Computer groups are an important part of WSUS deployments, even a basic deployment. Computer groups enable you to target updates to specific computers. There are two default computer groups: All Computers and Unassigned Computers. By default, when each client computer initially contacts the WSUS server, the server adds that client computer to each of these groups.

You can create custom computer groups. One benefit of creating computer groups is that they enable you to test updates before deploying updates widely. If testing goes well, you can roll out the updates to the All Computers group. There is no limit to the number of custom groups you can create.

Question: What are some of the benefits of using computer groups in WSUS for deploying updates?

Additional Reading
- Release Notes for Microsoft Windows Server Update Services 3.0
Approving Updates

Key Points
After updates have been synchronized to your WSUS server, they are automatically scanned for relevance to the server’s client computers. However, you must approve the updates manually before they are deployed to the computers on your network. When you approve an update, you are specifying what WSUS does with it (the options are Install or Decline for a new update). You can approve updates for the All Computers group or for subgroups. If you do not approve an update, its approval status remains Not approved, and your WSUS server allows clients to evaluate whether or not they need the update.

Additional Reading
- Managing Windows Server Update Services 3.0
- Best Practices with Windows Server Update Services 3.0
Demonstration: Managing WSUS

In this demonstration, you will see how to:

- Add a computer to WSUS
- Approve an update
Lab: Configuring Server Security Compliance

- Exercise 1: Configuring and Analyzing Security
- Exercise 2: Analyzing Security Templates
- Exercise 3: Configuring Windows Software Update Services

Logon information

<table>
<thead>
<tr>
<th>Virtual machine</th>
<th>NYC-DC1, NYC-SVR1, and NYC-CL2</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Administrator</td>
</tr>
<tr>
<td>Password</td>
<td>Pa$$w0rd</td>
</tr>
</tbody>
</table>

Estimated time: 90 minutes

Objectives
- Configure and analyze security using the Security Configuration Wizard.
- Use the Security Configuration and Analysis Wizard to analyze security templates.
- Configure Windows Software Update Services.
Lab Setup
For this lab you will use the available virtual machine environment. Before you begin the lab, you must:

- Start the NYC-DC1, NYC-SVR1, and NYC-CL2 virtual machines.
- Log on to the NYC-DC1, NYC-SVR1, and NYC-CL2 virtual machines with the user name **administrator** and the password **Pa$$w0rd**.
- On the computers running Windows Server 2008, close the **Initial Configuration Tasks** window that appears after log on.
- On the computers running Windows Server 2008, close the **Server Manager** window.

Scenario
As the Windows Infrastructure Services Technology Specialist, you have been tasked with configuring and managing server and client security patch compliance. You must ensure systems maintain compliance with corporate standards.
Exercise 1: Configuring and Analyzing Security

In this exercise, you will configure and analyze security using the Security Configuration Wizard.

The main tasks are as follows:

1. Ensure that you have completed the steps in the Lab Setup section.
2. Open the Security Configuration Wizard on 6421A-NYC-SVR1 and use the wizard to configure security for a particular server role.

▶ Task 1: Ensure that you have completed the steps in the Lab Setup section

1. Start the NYC-DC1, NYC-SVR1, and NYC-CL2 virtual machines.
2. Log on to the NYC-DC1, NYC-SVR1, and NYC-CL2 virtual machines with the user name administrator and the password Pa$$w0rd.
3. On the computers running Windows Server 2008, close the Initial Configuration Tasks window that appears after log on.

▶ Task 2: Open the Security Configuration Wizard on NYC-SVR1

1. On NYC-SVR1, open the Security Configuration Wizard from the Administrative Tools menu.
3. On the Configuration Action page, under Select the action you want to perform, ensure that Create a new security policy is selected, and then click Next.
4. On the Select Server page, verify the server specified in the Server text box is NYC-SVR1, and then click Next.
5. On the Processing Security Configuration Database page, wait for the process to complete and then select View Configuration Database.
6. When the SCW Viewer opens, an Internet Explorer message box may appear asking for permission to allow an Active X control. Click Yes in this message box.
7. Scroll through and read the list of Server Roles, Client Features, Administration and Other Options, Services and Windows Firewall.

8. Close SCW Viewer, and then click Next.

9. On the Role-Based Service Configuration, Select Server Roles, Select Client Features, Select Administration and Other Options, and Select Additional Services pages, accept the default settings, and then click Next.

10. On the Handling Unspecified Services page, verify that Do not change the startup mode of the service is selected, and then click Next.

11. On the Confirm Service Changes page, scroll through the list and note which ones are being disabled, and then click Next.

12. On the Network Security page, click Next to start configuring network security.

13. On the Network Security Rules page, scroll through the list of ports that will be opened, and then click Next.

14. On the Registry Settings and Audit Policy pages, select Skip this section, and then click Next.


16. On the Security Policy File Name page, specify a name of NewMemberSVR.xml at the end of the C:\Windows\Security\mscw\Policies path that is listed, and then click Next.


19. When Application Complete appears above the status bar, click Next.

Exercise 2: Analyzing Security Templates

In this exercise, you will analyze security templates.

The main tasks are as follows:

1. Create a customized Microsoft Management Console (MMC).
2. Analyze current computer settings against secure template settings.
3. Configure the computer with the secure template settings.

**Task 1: Create a customized Microsoft Management Console (MMC)**

1. On NYC-SVR1, create a custom MMC with the Security Templates and Security Configuration and Analysis snap-ins.
2. Using the Console1 MMC created above, create a new template with a name of Secure.
3. Expand the Secure policy, expand Local Policies, and then select Security Options.
4. Double-click Interactive Logon: Do not display last user name.
5. Select the Define this policy setting in the template check box, click Enabled, and then click OK.
6. Save the Secure template.
7. Leave the Console1 MMC open for the next task.

**Task 2: Analyze current settings against secure template settings**

1. In the Console1 MMC list pane, right-click Security Configuration and Analysis, and then click Open Database.
2. In the Open Database dialog box, type a file name of Secure, and then click Open.
3. In the Import Template dialog box, select the Secure template, and then click Open.
4. In the Console1 MMC list pane, right-click Security Configuration and Analysis, and then click Analyze Computer Now.
5. In the Perform Analysis dialog box, click OK to accept the default log name.
6. When the analysis is complete, in the list pane, expand Security Configuration and Analysis, expand Local Policies, and then select Security Options.

7. Scroll down to Interactive Logon: Do not display last user name and compare the database setting to the computer setting. You should see a red “x” on the item, which indicates that the settings are different between the computer setting and the database setting.

8. Leave the Console1 MMC open for the next task.

Task 3: Configure the computer with the secure template settings

1. In the Console1 MMC window list pane, right-click Security Configuration and Analysis, and then select Configure Computer Now from the available options.

   The template is applied to the computer.

3. From the list pane of the Console1 MMC, right-click Security Configuration and Analysis, and then select Analyze Computer Now.

4. In the Perform Analysis dialog box, click OK to accept the default log.

5. When the analysis is complete, expand Local Policies, and then select Security Options.

6. Scroll down to Interactive Logon: Do not display last user name and verify that a check mark appears indicating that the database setting and computer setting are the same.

7. Close the Console1 MMC window.
Exercise 3: Configuring Windows Software Update Services

In this exercise, you will configure Windows Software Update Services (WSUS).

The main tasks are as follows:
1. Use the Group Policy Management Console to create and link a GPO to the domain to configure client updates.
2. Use the WSUS administration tool to configure WSUS properties.
3. Create a computer group and add NYC-CL2 to the new group.
5. Close all virtual machines and discard undo disks.

Task 1: Use the Group Policy Management Console to create and link a GPO to the domain to configure client updates

1. On NYC-DC1, open Group Policy Management from the Administrative Tools menu.
2. In the list pane, right-click WoodGroveBank.com, click Create a GPO in this domain, and Link it here, and name the GPO WSUS.
3. Right-click the WSUS GPO link under WoodGroveBank.com, and then click Edit.
4. In the Group Policy Management Editor window, expand Computer Configuration, expand Administrative Templates, expand Windows Components, and then click Windows Update.
5. In the details pane, double-click Configure Automatic Updates.
6. In the Configure Automatic Updates Properties dialog box, on the Settings tab, select Enabled. In the Configure automatic updating drop-down list, click 4 - Auto download and schedule the install, and then click Next Setting.
7. On the Specify intranet Microsoft update service location Properties page, on the Settings tab, select Enabled. Under Set the intranet update service for detecting updates and under Set the intranet statistics server, type http://NYC-SVR1 in the text boxes, and then click Next Setting.
8. On the Automatic Updates detection frequency Properties page, select Enabled, and then click OK.
9. Close the Group Policy Management Editor, and then close the Group Policy
   Management tool.
10. On NYC-CL2, open a command prompt.
11. At the command prompt, type `gpupdate /force`, and then press ENTER.
12. At the command prompt, type `wuauclt /detectnow`, and then press ENTER.
13. Close the command window on NYC-CL2.

► **Task 2: Use the WSUS administration tool to configure WSUS properties**
   1. On NYC-SVR1, open Microsoft Windows Server Update Services 3.0 from the
      Administrative Tools menu.
   2. In the Update Services administrative tool window, in the list pane under
      NYC-SVR1, click Options.
   3. Using the details pane, view the configuration settings available in WSUS, and
      click Cancel for each item when complete.

► **Task 3: Create a computer group and add NYC-CL2 to the new group**
   1. In the list pane, expand Computers, and then select All Computers.
   2. In the Actions pane, click Add Computer Group and name the group HO
      Computers.
   3. Change membership of the `nyc-cl2.woodgrovebank.com` computer object so
      that it is a part of the HO Computers group.

► **Task 4: Approve an update for Vista clients**
   1. In the Update Services administrative tool, in the list pane, expand Updates,
      and then click Critical Updates.
   2. In the details pane, change both the Approval and Status filters to Any. Notice
      all of the updates available.
   3. In the details pane, change the Status filter to Failed or Needed. A number of
      required updates are listed as reported by the computers within the network.
   4. In the Critical Updates details pane, right-click Update for Windows Vista
      (KB936357), and then select Approve from the context menu.
5. In the **Approve Updates** window that appears, click the arrow next to **All Computers**, select **Approved for Install**, and then click **OK**.

6. On the **Approval Progress** page, when the process is complete, click **Close**.

**Note:** Notice that a message appears stating that the update is approved but must be downloaded to complete.

7. In the Update Services console, click **Reports**.

8. View the various reports available in WSUS. Determine how many updates are required by NYC-CL2.

**Task 5: Close all virtual machines and discard undo disks**

1. On the host computer, click **Start**, point to **All Programs**, point to **Microsoft Virtual Server**, and then click **Virtual Server Administration Website**.

2. Under **Navigation**, click **Master Status**. For each virtual machine that is running, click the **virtual machine name**, and in the context menu, click **Turn off Virtual Machine and Discard Undo Disks**. Click **OK**.
Module Review and Takeaways

- Review Questions
- Best Practices

Review Questions

1. What kind of challenges might a small to medium-sized business experience that may not be as large an issue for a large enterprise?

2. What is one benefit of using the Security Configuration and Analysis tool to compare template settings against the settings presently being applied to the computer?

3. If you decide to put an audit policy in place, how should you configure the security log properties in Event Viewer?

4. What must an administrator do before any update is sent to clients and servers via WSUS?

5. What is the reason for setting a deadline for automatic installation to a past date?
Best Practices

Regardless of the operating system you are using, the basic steps for securing it are the same. Consider the following best practices for securing an operating system:

- Install all operating system patches.
- Verify user account security.
- Eliminate unnecessary applications and network services.
- Install and configure necessary applications and network services.
- Configure system logging to record significant events.
- Keep applications and operating system patches up to date.
Course Evaluation

Your evaluation of this course will help Microsoft understand the quality of your learning experience.

Please work with your training provider to access the course evaluation form.

Microsoft will keep your answers to this survey private and confidential and will use your responses to improve your future learning experience. Your open and honest feedback is valuable and appreciated.