Exam
Manual

LearnSmart

Upgrading **MCSA 2003** to Server 2008

(70-648) Microsoft Certified IT Professional (MCITP)

This LearnSmart exam manual covers all the necessary concepts with which you must be familiar in order to successfully complete the Upgrading MCSA 2003 to Server 2008 exam (70-648). By studying this manual, you will become familiar with an array of exam-related content, including:

- Configuring Additional Active Directory Server Roles
- Maintaining the Active Directory Environment
- Configuring Active Directory Certificate Services
- Configuring Network Access
- And more!

Give yourself the competitive edge necessary to further your career as an IT professional and purchase this exam manual today!

Upgrading MCSA 2003 to Server 2008 (70-648) LearnSmart Exam Manual

Product ID: 012466
Production Date: July 12, 2011

Warning and Disclaimer

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or fitness is implied. The publisher and authors assume no responsibility for errors or omissions. The information provided is on an "as is" basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this document.

Volume, Corporate, and Educational Sales

Favorable discounts are offered on all products when ordered in quantity. For more information, please contact us directly:

1-800-418-6789
solutions@preplogic.com

International Contact Information

International: +1 (813) 769-0920

United Kingdom: (0) 20 8816 8036

Table of Contents

Abstract

The Upgrading Your Server 2003 MCSA to Windows Server 2008, 70-648 Exam Manual is designed to provide you with exactly the information you need to ensure your valuable server administration skills are completely up to date. We have designed this Exam Manual with you, the working technician, in mind. Only the most information most pertinent to the 70-648 exam and, of course, to updating your already extensive Windows Server skill set is included in this manual. Rather than take the approach that assumes you are a complete novice to the world of Microsoft Server technologies, we are delivering just what you need to get ready for the all important MCITP certifications.

What to Know

As with most of Microsoft's newest line of certification exams, you are required to have quite a bit of hands-on experience with Server 2008 before attempting the exam. Microsoft recommends at least a year of experience with Server 2008, on top of any accumulated experience with Server 2003. In specific, you should be highly aware of the changes to Active Directory between server 2003 and Server 2008 and the changes to the day-to-day monitoring tasks, such as Event Viewer and Performance Monitor.
The specific objectives for this exam are:

- Configuring Additional Active Directory Server Roles
- Maintaining the Active Directory Environment
- Configuring Active Directory Certificate Services
- Configuring IP Addressing and Services
- Configuring Network Access
- Monitoring and Managing a Network Infrastructure

Tips

If you don't already have experience working with Server 2008, it's a good idea to download a trial of the software and either create a full install of it on your home machine or virtualize a Server 2008 environment. Virtualizing the environment gives you the opportunity to play with some of the Network Access and WSUS features (such as creating downstream update servers) you wouldn't normally have access to outside of a professional environment. Additionally, if your practical experience with Server, in general, is a few years old, you may want to consider a more comprehensive training experience, such as CBTs or video. Also, before you sit the exam, always take a practice exam.

Domain 1: Configuring Additional Active Directory Server Roles

Configure Active Directory Lightweight Directory Service (AD LDS)

Follow the steps below to install AD LDS:

1. Click **Start**, and then click **Server Manager**.
2. In the console tree, right-click **Roles**, and then click **Add Roles**.
3. Review the information on the **Before You Begin** page of the Add Roles Wizard, and click **Next**.
4. On the **Select Server Roles** page in the **Roles** list, select the **Active Directory Lightweight Directory Services** check box, and click **Next**.
5. Finish adding the AD LDS server role by following the instructions in the wizard.

Once you have installed the AD LDS server role to a server, you must create an AD LDS instance. Follow the steps below to create an AD LDS instance:

1. Click **Start**; point to **Administrative Tools**, and click **Active Directory Lightweight Directory Services Setup Wizard**.
2. On the **Welcome to the Active Directory Lightweight Directory Services Setup Wizard** page, click **Next**.
3. On the **Setup Options** page, click **A unique instance**, and then click **Next**.
4. On the **Instance Name** page, provide a name for the AD LDS instance that you are installing. This name is used on the local computer to uniquely identify the AD LDS instance.
5. On the **Ports** page, specify the communications ports that the AD LDS instance uses to communicate. AD LDS can communicate using both LDAP and Secure Sockets Layer (SSL); therefore, you must provide a value for each port.
   - **NOTE**: If you install AD LDS on a computer where either of the default ports is in use, the Active Directory Lightweight Directory Services Setup Wizard automatically locates the first available port, starting at 50000. For example, Active Directory Domain Services (AD DS) uses ports 389 and 636, as well as ports 3268 and 3269 on global catalog servers. Therefore, if you install AD LDS on a domain controller, the Active Directory Lightweight Directory Services Setup Wizard provides a default value of 50000 for the LDAP port and 50001 for the SSL port.
6. On the **Application Directory Partition** page, you can create an application directory partition (or naming context) by clicking **Yes, create an application directory partition**. Or, you can click **No, do not create an application directory partition**, in which case you must create an application directory partition manually after installation.
   - **NOTE**: AD LDS supports both X.500-style and Domain Name System (DNS)–style distinguished names for top-level directory partitions
7. On the **File Locations** page, you can view and change the installation directories for AD LDS data and recovery (log) files. By default, AD LDS data and recovery files are installed in %ProgramFiles%\Microsoft ADAM*instancename*\data, where *instancename* represents the AD LDS instance name that you specified on the **Instance Name** page. Click **Next**.

8. On the **Service Account Selection** page, select an account to be used as the service account for AD LDS. The account that you select determines the security context in which the AD LDS instance runs. The Active Directory Lightweight Directory Services Setup Wizard defaults to the **Network Service account**. Click **Next**.
9. On the **AD LDS Administrators** page, you select a user or group to become the default administrator for the AD LDS instance. The user or group that you select will have full administrative control of the AD LDS instance. By default, the Active Directory Lightweight Directory Services Setup Wizard specifies the currently logged on user. You can change this selection to any local or domain account or group on your network. Click **Next.**
10. On the **Importing LDIF Files** page, you can import schema .ldf files into the AD LDS instance. The following table details some of the available files:

LDIF File Name	Description
MS-InetOrgPerson.ldf	Contains the definition of the **inetOrgPerson** LDAP object class.
MS-User.ldf	Contains **user** and related classes object definitions.
MS-UserProxy.ldf	Contains the simple **userProxy** class object definition.
MS-UserProxyFull.ldf	Contains the full **userProxy** class object definition.
MS-ADLDS-DisplaySpecifiers.ldf	Contains display specifiers. This .ldf file is required for snap-in operations. If you are planning to connect to your AD LDS instance and then manage it through the Active Directory Sites and Services snap-in, import this file now with the Active Directory Lightweight Directory Services Setup Wizard.

Figure 1: LDIF Files

NOTE: AD LDS also allows you to make custom LDAP Data Interchange Format (LDIF) files available during AD LDS setup by adding them to the %systemroot%\ADAM directory. You can create custom LDIF files by using ADSchema Analyzer. Store the custom LDIF file in the %systemroot%\ADAM directory and then run the AD LDS Setup Wizard to create a new AD LDS instance. Your custom LDIF file will be available in the list of LDIF file names on the **Importing LDIF Files** page.

1. The **Ready to Install** page gives you an opportunity to review your installation selections. After you click **Next**, the Active Directory Lightweight Directory Services Setup Wizard copies files and sets up AD LDS on your computer.
2. When the Active Directory Lightweight Directory Services Setup Wizard finishes installing AD LDS, it displays this message: "You have successfully completed the Active Directory Lightweight Directory Services Setup Wizard." When the **Completing the Active Directory Lightweight Directory Services Setup Wizard** page appears, click **Finish** to close the wizard. If any problems occur during the setup, you may view error messages on the Summary page of the wizard. Text based log files may also be viewed at:
    i. **%windir%\Debug\ADAMSsetup.log**
    ii. **%windir%\Debug\ADAMSsetup_loader.log**

AD LDS is supported on Windows Server 2008 Server Core. To install the AD LDS role, type the following at a command prompt:

```
start /w ocsetup DirectoryServices-ADAM-ServerCore
```

Ldifde

You can use the *Ldifde* command to create, modify, and delete directory objects. *Ldifde* can also be used to extend the schema, export Active Directory user and group information to other applications or services, and populate AD DS with data from other directory services. This command is available once you have the AD DS or AD LDS server role installed. You must be at an elevated command prompt to run this command.

The command syntax of *Ldifde* is:

```
Ldifde [-i] [-f <FileName>] [-s <ServerName>] [-c <String1>
<String2>] [-v] [-j <Path>] [-t <PortNumber>] [-d <BaseDN>]
[-r <LDAPFilter>] [-p <Scope>] [-l <LDAPAttributeList>] [-o
<LDAPAttributeList>] [-g] [-m] [-n] [-k] [-a
<UserDistinguishedName> <Password>] [-b <UserName> <Domain>
<Password>] [-?]
```

The following table details the parameters of the *Ldifde* command:

Parameter	Description
-i	Specifies to use the import mode. The default mode is export.
-f <FileName>	Identifies the import or export file name.
-s <ServerName>	Specifies the domain controller to perform the import or export operation. By default, **ldifde** runs on the domain controller on which **ldifde** is installed.
-c <String1> <String2>	Replaces all occurrences of <String1> with <String2>. Generally, you use this parameter when you import data from one domain to another and you must replace the distinguished name of the export domain (<String1>) with the distinguished name of the import domain (<String2>).
-v	Sets verbose mode.
-j <Path>	Sets the log file location. The default location is the current path.
-t <PortNumber>	Specifies a Lightweight Directory Access Protocol (LDAP) port number. The default LDAP port number is 389. The global catalog port number is 3268.
-d <BaseDN>	Sets the distinguished name of the search base for data export.
-r <LDAPFilter>	Creates an LDAP search filter for data export. For example, to export all users with a surname that you specify, you can use the following filter: **-r (and(objectClass=User)(sn=Surname))**
-p <Scope>	Sets the search scope. The search scope options are **Base**, **OneLevel** or **SubTree**.
-l <LDAPAttributeList>	Sets the list of attributes to return in the results of an export query. If you do not specify this parameter, the search returns all attributes.
-o <LDAPAttributeList>	Sets the list of attributes to omit from the results of an export query. This is typically used when exporting objects from AD DS and then importing them into another LDAP-compliant directory. If attributes are not supported by another directory, you can omit the attributes from the result set using this option.

-g	Omits paged searches.
-m	Omits attributes that apply only to Active Directory objects, such as the **ObjectGUID**, **objectSID**, **pwdLastSet** and **samAccountType** attributes.
-n	Omits the export of binary values.
-k	Ignores errors during an import operation and continues processing. This parameter ignores all of the following errors: • The object is already a member of the group. • The operation has an object class violation. • This violation means that the specified object class does not exist, if the object being imported has no other attributes. • The object already exists. • The operation has a constraint violation. • The attribute or value already exists. • The operation found no such object.
-a <UserDistinguishedName> <Password>	Sets the command to run using the distinguished name (<UserDistinguishedName>) and password (<Password>) that you supply. By default, the command uses the credentials of the user who is currently logged on to the network.
-b <UserName> <Domain> <Password>	Sets the command to run using the supplied <UserName> <Domain> <Password>. By default, the command will run using the credentials of the user currently logged on to the network.
/?	Displays help at the command menu.

Figure 2: LDIFDE Command Line Options

Syntax examples:

- To import directory objects, at the command prompt, type the following command, and then press **ENTER**:

```
ldifde -i -f <filename> -s <servername>:<port> -m -a <username>
<domain> <password>
```

- To export directory objects, at the command prompt, type the following command, and then press **ENTER**:

```
ldifde -e -f <filename> -s <servername>:<port> -m -a <username>
<domain> <password>
```

Windows Server 2008 Hyper-V

Follow the steps below to install Hyper-V:

1. Click **Start**, and then click **Server Manager**.
2. In the **Roles Summary** area of the Server Manager main window, click **Add Roles**.
3. On the **Select Server Roles** page, click Hyper-V.

4. On the **Create Virtual Networks** page, click one or more network adapters if you want to make their network connection available to virtual machines.
5. On the **Confirm Installation Selections** page, click **Install**.
6. The computer must be restarted to complete the installation. Click **Close** to finish the wizard, and then click **Yes** to restart the computer.
7. After you restart the computer, log on with the same account you used to install the role. After the Resume Configuration Wizard completes the installation, click **Close** to finish the wizard.

Once you have installed the Hyper-V role, you will need to create and set up a virtual machine. Before proceeding you should consider the following:

- Are the installation media available for the operating system you want to install on the virtual machine? You can use physical media, a remote image server, or an .ISO file. The method you want to use determines how you should configure the virtual machine.
- How much memory will you allocate to the virtual machine?
- Where do you want to store the virtual machine, and what do you want to name it?

Follow the steps below to create and set up a virtual machine:

1. Open Hyper-V Manager. Click **Start**; point to **Administrative Tools**, and click **Hyper-V Manager**.
2. From the **Action** pane, click **New**, and then click **Virtual Machine**.
3. From the **New Virtual Machine Wizard**, click **Next**.
4. On the **Specify Name and Location** page, specify what you want to name the virtual machine and where you want to store it.
5. On the **Memory** page, specify enough memory to run the guest operating system you want to use on the virtual machine.
6. On the **Networking** page, connect the network adapter to an existing virtual network if you want to establish network connectivity at this point.
   - **NOTE:** If you want to use a remote image server to install an operating system on your test virtual machine, select the external network.
7. On the **Connect Virtual Hard Disk** page, specify a name, location and size to create a virtual hard disk so you can install an operating system on it.
8. On the **Installation Options** page, choose the method you want to use to install the operating system:
   a. Install an operating system from a boot CD/DVD-ROM. You can use either physical media or an image file (.iso file).
   b. Install an operating system from a boot floppy disk.
   c. Install an operating system from a network-based installation server. To use this option, you must configure the virtual machine with a network adapter connected to the same network as the image server.
9. Click **Finish**.
10. You are now ready to start the virtual machine and install an operating system.

Configure Active Directory Rights Management Service (AD RMS)

Follow the steps below to install the AD RMS role:

1. Click **Start**; point to **Administrative Tools**, and click **Server Manager**.
2. In the **Roles Summary** box, click **Add Roles**. The **Add Roles Wizard** opens.
3. Verify the options in the **Before You Begin** section, and click **Next**.
4. On the **Select Server Roles** page, select the **Active Directory Rights Management Services** check box.
5. The **Role Services** page appears, informing you of the AD RMS dependent role services and features. Make sure that Web Server (IIS), Windows Process Activation Service (WPAS), and Message Queuing are listed, and then click **Add Required Role Services**. Click **Next**.
6. Read the AD RMS introduction page, and click **Next**.
7. On the **Select Role Services** page, verify that the **Active Directory Rights Management Server** check box is selected, and click **Next**.
8. Click the **Create a new AD RMS cluster** option, and click **Next**.
9. Click the **Use a different database server** option.
10. Click **Select**; type **ADRMS-DB** in the **Select Computer** dialog box, and click **OK**.
11. In **Database Instance**, click **Default**, and then click **Validate**. Click **Next**.
12. Click **Specify**; type <*domain*>\<*account*>; type the password for the account; click **OK**, and then click **Next**.
13. Ensure that the **Use AD RMS centrally managed key storage** option is selected, and click **Next**.
14. Type a strong password in the **Password** box and in the **Confirm password** box, and click **Next**.
15. Choose the Web site where AD RMS will be installed, and click **Next**. In an installation that uses default settings, the only available Web site should be **Default Web Site**.
16. Click the **Use an SSL-encrypted connection (https://)** option.
17. Type the FQDN in the **Fully-Qualified Domain Name** box, and click **Validate**. If validation succeeds, the **Next** button becomes available. Click **Next**.
18. Click the **Choose an existing certificate for SSL encryption** option; click the certificate that has been imported for this AD RMS cluster, and then click **Next**.
19. Type a name that will help you identify the AD RMS cluster in the **Friendly name** box, and click **Next**.
20. Ensure that the **Register the AD RMS service connection point now** option is selected, and click **Next** to register the AD RMS service connection point (SCP) in Active Directory during installation.
21. Read the **Introduction to Web Server (IIS)** page, and click **Next**.
22. Keep the Web server default check box selections, and click **Next**.
23. Click **Install** to provision AD RMS on the computer. It can take up to 60 minutes to complete the installation. Click **Close**.
24. Log off the server, and then log on again to update the security token of the logged-on user account. The user account that is logged on when the AD RMS server role is installed is automatically made a member of the AD RMS Enterprise Administrators local group. A user must be a member of that group to administer AD RMS.

AD RMS Rights Policy Template

Follow the steps below to create a new AD RMS rights policy template:

1. Open the Active Directory Rights Management Services Administration console. Click **Start**; point to **Administrative Tools**, and click **Active Directory Rights Management Services**.
2. In the Active Directory Rights Management Services Administration console, expand the cluster name.
3. Right-click **Rights Policy Templates**, and then click **Properties**.
4. Select the **Enable export** check box; type the UNC path in the **Specify templates file location (UNC)** box, and click **OK**.
5. In the **Actions** pane, click **Create Distributed Rights Policy Template** to start the Create Distributed Rights Policy Template wizard. Click **Add**.
6. In the **Language** box, choose the appropriate language for the rights policy template.
7. Type the template name in the **Name** box.
8. Type a description for the template in the **Description** box, and click **Add**. Click **Next**.
9. Click **Add**; type an e-mail address in **The e-mail address of a user or group** box, and click **OK**.
10. Select the **View** check box to grant the selected e-mail address group Read access to any document created, by using this AD RMS rights policy template. Click **Finish.**

Configure the Read-Only Domain Controller (RODC)

Before you can deploy an RODC, you must ensure that the *Forest Functional Level* is set to Windows Server 2003 or higher. Follow the steps below to verify the domain functional level:

1. Open Active Directory Domains and Trusts.
2. In the console tree, right-click the name of the forest, and then click **Properties**.
3. Under **Forest functional level**, verify that the value is **Windows Server 2003** or **Windows Server 2008**.
4. If it is necessary to raise the forest functional level, in the console tree, right-click **Active Directory Domains and Trusts,** and then click **Raise forest functional level**.
5. In **Select an available forest functional level**, click **Windows Server 2003**, and then click **Raise**.

If you are in a mixed environment with both Windows Server 2003 and Windows Server 2008 domain controllers, you will need to update the permissions on all the DNS application directory partitions in the forest. This step allows them to be replicated successfully by all RODCs that are also DNS servers. You do not need to complete this step if you only have Windows Server 2008 domain controllers.

1. Log on to a domain controller as a member of the Enterprise Admins group.
2. Copy the contents of the \sources\adprep folder on the Windows Server 2008 installation DVD to the schema master.
3. Open a command prompt; change directories to the adprep folder; type the following command, and press ENTER:

   adprep /rodcprep

NOTE: An RODC must replicate domain updates from a writable domain controller that runs Windows Server 2008. Before you install an RODC, be sure to install a writable domain controller that runs Windows Server 2008 in the same domain. The domain controller can run either a full installation or a Server Core installation of Windows Server 2008. In Windows Server 2008, the writable domain controller does not have to hold the primary domain controller (PDC) emulator operations master role.

Follow the steps below to install an RODC on a full installation of Windows Server 2008:

1. Click **Start**; type **dcpromo**, and press ENTER to start the Active Directory Domain Services Installation Wizard. The server can belong to a workgroup. Alternatively, if you are not delegating the installation, the server can already be joined to the domain in which you want it to be an RODC.
2. On the **Choose a Deployment Configuration** page, click **Existing forest**; click **Add a domain controller to an existing domain**, and then click **Next**.
3. On the **Network Credentials** page, type the name of a domain in the forest where you plan to install the RODC. If necessary, also type a user name and password for a member of the Domain Admins group, and click **Next**.
4. Select the domain for the RODC, and click **Next**.
5. Click the Active Directory site for the RODC, and then click **Next**.
6. Select the **Read-only domain controller** check box. By default, the **DNS server** check box is also selected.
7. To use the default folders that are specified for the Active Directory database, the log files and SYSVOL, click **Next**.
8. Type and then confirm a Directory Services Restore Mode password, and click **Next**.
9. Confirm the information that appears on the Summary page, and click **Next** to start the AD DS installation. You can select the **Reboot on completion** check box to make the rest of the installation complete automatically.

Configure Password Replication

Follow the steps below to configure the password replication policy for the RODC:

1. Click **Start**; click **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. Ensure that Active Directory Users and Computers points to the writable domain controller that is running Windows Server 2008, and click **Domain Controllers**.
3. In the details pane, right-click the RODC computer account, and then click **Properties**.
4. Click the **Password Replication Policy** tab.
5. The **Password Replication Policy** tab lists the accounts that, by default, are defined in the Allowed List and the Denied List on the RODC. To add other groups that should be included in either the Allowed List or the Denied List, click **Add.** To add other accounts that will *not* have credentials cached on the RODC, click **Deny**. To add other accounts that will have credentials cached on the RODC, click **Allow**.

NOTE: Accounts that will not have credentials cached on the RODC can still use the RODC for domain logon. The credentials, however, will not be cached for subsequent logon using the RODC.

Credential Caching

Follow the steps below to prepopulate the password cache for an RODC by using Active Directory Users and Computers:

1. Click **Start**; click **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. Ensure that Active Directory Users and Computers points to the writable domain controller that is running Windows Server 2008, and click **Domain Controllers**.
3. In the details pane, right-click the RODC computer account, and then click **Properties**.
4. Click the **Password Replication Policy** tab.
5. Click **Advanced**.
6. Click **Prepopulate Passwords**.
7. Type the name of the accounts whose passwords you want to prepopulate in the cache for the RODC, and click **OK**.
8. When asked if you want to send the passwords for the accounts to the RODC, click **Yes**.

Follow the steps below to prepopulate the password cache for an RODC by using the command-line:

1. Log on to a writable domain controller that is running Windows Server 2008.
2. Click **Start**; right-click **Command Prompt**, and then click **Run as administrator**.
3. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and click **Continue**.
4. Type the following command, and press ENTER:

```
repadmin /rodcpwdrepl [DSA_List] <Hub DC> <User1 Distinguished
Name> [<Computer1 Distinguished Name> <User2 Distinguished Name> …]
```

The following table details the parameters in the *Repadmin* command:

Placeholder	Value
DSA_List	The name of the RODC whose password cache you want to prepopulate.
Hub DC	The name of the writable Windows Server 2008 domain controller that is the replication partner of the RODC.
User1, Computer1, ….	The names of the users and computers whose passwords you want to cache on the RODC. You must add the computer accounts of the users or they cannot log on.

Figure 3: RepAdmin Command Line Parameters

Administrator Role Separation

Follow the steps below to configure Administrator Role Separation for an RODC:

1. Click **Start**; click **Run**; type **cmd**, and press ENTER.
2. At the command prompt, type **dsmgmt.exe**, and press ENTER.
3. At the DSMGMT prompt, type **local roles**, and press ENTER.
4. For a list of valid parameters, type **?**, and press ENTER.
   - By default, no local administrator role is defined on the RODC after AD DS installation. To add the local administrator role, use the **Add** parameter.
5. Type **add** <*DOMAIN*>\<*user*> <*administrative role*>

The following table lists the parameters that are available for Administrator Role Separation:

Parameter	Description
Add %s1 %s2	Adds an account %s1 to the local role %s2.
Connections	Connects to a specific Active Directory domain controller or an AD LDS instance.
Help	Shows pertinent Help information.
List Roles	Lists defined local roles.
Quit	Returns to the previous menu.
Remove %s1 %s2	Removes an account %s1 from the local role %s2.
Show Role %s	Shows local role members.

Figure 4: Parameters for Administrator Role Separation

Configure Active Directory Federation Services (AD FS)

Follow the steps below to install AD FS:

1. Click **Start**; point to **Administrative Tools**, and click **Server Manager**.
2. Right-click **Roles**, and click **Add Roles** to start the Add Roles Wizard.
3. On the **Before You Begin** page, click **Next**.
4. On the **Select Server Roles** page, click **Active Directory Federation Services**. Click **Next** two times.
5. On the **Select Role Services** page, select the **Federation Service** check box. If you are prompted to install additional Web Server (IIS) or Windows Process Activation Service role services, click **Add Required Role Services** to install them, and then click **Next**.
6. On the **Choose a Server Authentication Certificate for SSL Encryption** page, click **Create a self-signed certificate for SSL encryption**, and then click **Next**.
7. On the **Choose a Token-Signing Certificate** page, click **Create a self-signed token-signing certificate**, and then click **Next**.
8. On the **Select Trust Policy** page, click **Create a new trust policy**, and then click **Next** twice.
9. On the **Select Role Services** page, click **Next** to accept the default values.
10. Verify the information on the **Confirm Installation Selections** page, and click **Install**.
11. On the **Installation Results** page, verify that everything installed correctly, and click **Close**.

Follow the steps below to configure IIS to require SSL on your federation servers:

1. Click **Start**; point to **Administrative Tools**, and click **Internet Information Services (IIS) Manager**.
2. In the console tree, double-click **ADFSACCOUNT** or **ADFSRESOURCE**; double click **Sites**, and then click **Default Web Site**.
3. In the center pane, double-click **SSL Settings**, and select the **Require SSL** check box.
4. Under **Client certificates**, click **Accept**, and then click **Apply**.

Follow the steps below to install the AD FS Web Agent:

1. Click **Start**; point to **Administrative Tools**, and click **Server Manager**.
2. Right-click **Roles**, and then click **Add Roles** to start the Add Roles Wizard.
3. On the **Before You Begin** page, click **Next**.
4. On the **Select Server Roles** page, click **Active Directory Federation Services**. Click **Next** two times.
5. On the **Select Role Services** page, select the **Claims-aware Agent** check box. If you are prompted to install additional Web Server (IIS) or Windows Process Activation Service role services, click **Add Required Role Services** to install them, and then click **Next**.
6. On the **Web Server (IIS)** page, click **Next**.
7. On the **Select Role Services** page, in addition to the pre-selected check boxes, select the **Client Certificate Mapping Authentication** and **IIS Management Console** check boxes, and click **Next**.
   - **NOTE**: **The Client Certificate Mapping Authentication** check box installs the components that IIS needs to create a self-signed server authentication certificate which is required for this server.
8. After verifying the information on the **Confirm Installation Selections** page, click **Install**.
9. On the **Installation Results** page, verify that everything installed correctly, and click **Close**.

Creating, Exporting, and Importing Certificates

Follow the steps below to create a certificate on AD FS:
Click **Start**; point to **Administrative Tools**, and click **Internet Information Services (IIS) Manager**.

1. In the console tree, select the AD FS server.
2. In the center pane, double-click **Server Certificates**.
3. In the **Actions** pane, click **Create Self-Signed Certificate**.
4. In the **Create Self-Signed Certificate** dialog box, type the server name, and click **OK**.

Follow the steps below to export a certificate from AD FS to a file:

1. Click **Start**; point to **Administrative Tools**, and click **Active Directory Federation Services**.
2. Right-click **Federation Service**, and then click **Properties**.
3. On the **General** tab, click **View**.
4. On the **Details** tab, click **Copy to File**.
5. On the **Welcome to the Certificate Export Wizard** page, click **Next**.

6. On the **Export Private Key** page, click **No, do not export the private key**, and then click **Next**.
7. On the **Export File Format** page, click **DER encoded binary X.509 (.CER)**, and then click **Next**.
8. On the **File to Export** page, type the path and name of the export folder, and click **Next**.
9. On the **Completing the Certificate Export Wizard**, click **Finish**.

Follow the steps below to configure a Web server to trust the AD FS server:

1. Click **Start**; point to **Administrative Tools**, and click **Internet Information Services (IIS) Manager**.
2. In the console tree, select the AD FS server.
3. In the center pane, double-click **Server Certificates**.
4. In the center pane, right-click the certificate name, and then click **Export**.
5. In the **Export Certificate** dialog box, click the **…** button.
6. In **File name**, type the path and file name, and click **Open**.
   - **NOTE:** This certificate must be imported to the Web server in the next procedure. Therefore, make this file accessible over the network to that server.
7. Type a password for the certificate; confirm it, and click **OK**.

Domain 2: Maintaining the Active Directory Environment

Configure Backup and Recovery

To access backup and recovery tools for Windows Server 2008, you must install the **Windows Server Backup**, **Command-line Tools**, and **Windows PowerShell** items that are available in the Add Features Wizard in Server Manager. This installs the following tools:

- Windows Server Backup Microsoft Management Console (MMC) snap-in.
- **Wbadmin** command-line tool, which replaces the **ntbackup** command that was used with previous versions of Windows.
- Windows Server Backup *cmdlets* (Windows PowerShell commands).

Follow the steps below to install the backup and recovery tools:

1. Click **Start**; click **Server Manager**; in the left pane, click **Features**, and then in the right pane, click **Add Features** to open the *Add Features Wizard*.
2. In the Add Features Wizard, on the **Select Features** page, expand **Windows Server Backup Features**, and select the check boxes for **Windows Server Backup** and **Command-line Tools**.
   a. You will receive a message that Windows PowerShell is also required to be installed with these features.
   b. If you just want to install the snap-in and the **Wbadmin** command-line tool, expand **Windows Server Backup Features**, and select the **Windows Server Backup** check box. In this case, Windows PowerShell is not required.
3. Click **Add Required Features**, and then click **Next**.

4. On the **Confirm Installation Selections** page, review the choices that you made, and click **Install**. If there is an error during the installation, it will be noted on the **Installation Results** page.
5. Then, to access these backup and recovery tools, do the following:
    a. To access the Windows Server Backup snap-in, click **Start**; click **Administrative Tools**, and then click **Windows Server Backup**.
    b. To access and view the syntax for **Wbadmin**, click **Start**; right-click **Command Prompt**, and then click **Run as administrator**. At the prompt, type: **wbadmin /?**

Follow the steps below to create a backup schedule using the Windows Server Backup user interface:

1. Click **Start**; click **Administrative Tools**, and then click **Windows Server Backup**.
2. In the **Actions** pane of the snap-in default page, under **Windows Server Backup**, click **Backup Schedule**. This opens the Backup Schedule Wizard.
3. On the **Getting started** page, click **Next**.
4. On the **Select backup configuration** page, do one of the following, and click **Next**:
    a. Click **Full Server** to back up all volumes on the server. This is the recommended option.
    b. Click **Custom** to back up just certain volumes. On the **Select backup items** page, select the check boxes for the volumes that you want to back up and clear the check boxes for the volumes that you want to exclude.
    c. **IMPORTANT**: Volumes that contain operating system components are included in the backup by default and cannot be excluded.
5. On the **Specify backup time** page, do one of the following, and click **Next**:
    a. Click **Once a day**, and enter the time to start running the daily backup.
    b. Click **More than once a day**. To select a start time, under **Available time**, click the time that you want the backup to start, and then click **Add** to move the time under **Scheduled time**. Repeat for each start time that you want to add.
6. On the **Select destination disk** page, select the check box for the disk that you attached for this purpose, and click **Next**.
7. A message informs you that the selected disk will be formatted and any existing data will be deleted. Click **Yes** if you do not need the data on that disk; otherwise, click **No**, and select a different disk under **Available disks**.
8. On the **Label destination disk** page, the disk that you selected is listed. A label that includes your computer name, the current date, the current time, and a disk name is assigned to the disk. Click **Next**.
9. On the **Confirmation** page, review the details, and click **Finish**. The wizard formats the disk, which may take several minutes depending on the size of the disk.
10. On the **Summary** page, click **Close**.

Wbadmin

The **Wbadmin** command is used to back up and restore your operating system, volumes, files, folders, and applications from a command prompt. This command must be run from an elevated command prompt.

The following table lists the subcommands available with the **Wbadmin** command:

Subcommand	Description
Wbadmin enable backup	Configures and enables a daily backup schedule. This subcommand applies only to Windows Server 2008.
Wbadmin disable backup	Disables your daily backups. This subcommand applies only to Windows Server 2008.
Wbadmin start backup	Runs a one-time backup. If used with no parameters, uses the settings from the daily backup schedule.
Wbadmin stop job	Stops the currently running backup or recovery operation.
Wbadmin get versions	Lists details of backups recoverable from the local computer or, if another location is specified, from another computer.
Wbadmin get items	Lists the items included in a specific backup.
Wbadmin start recovery	Runs a recovery of the volumes, applications, files, or folders specified. This subcommand applies only to Windows Server 2008.
Wbadmin get status	Shows the status of the currently running backup or recovery operation.
Wbadmin get disks	Lists disks that are currently online. This subcommand applies only to Windows Server 2008.
Wbadmin start systemstaterecovery	Runs a system state recovery. This subcommand applies only to Windows Server 2008.
Wbadmin start systemstatebackup	Runs a system state backup. This subcommand applies only to Windows Server 2008.
Wbadmin delete systemstatebackup	Deletes one or more system state backups. This subcommand applies only to Windows Server 2008.
Wbadmin start sysrecovery	Runs a recovery of the full system (at least all the volumes that contain the operating system's state). This subcommand applies only to Windows Server 2008, and it is only available if you are using the Windows Recovery Environment.
Wbadmin restore catalog	Recovers a backup catalog from a specified storage location in the case where the backup catalog on the local computer has been corrupted. This subcommand applies only to Windows Server 2008.
Wbadmin delete catalog	Deletes the backup catalog on the local computer. Use this subcommand only if the backup catalog on this computer is corrupted and you have no backups stored at another location that you can use to restore the catalog. This subcommand applies only to Windows Server 2008.

Figure 5: WBAdmin Sub-Commands

Follow the steps below to perform a non-authoritative restore of AD DS:

NOTE: To perform a non-authoritative restore of AD DS, you need at least a critical-volume backup. However, you can use a full server backup for non-authoritative restore if you do not have a critical-volume backup.

1. At the **Windows** logon screen, click **Switch User**, and then click **Other User**.
2. Type **.\administrator** as the user name; type the DSRM password for the server, and press ENTER.
3. Click **Start**; right-click **Command Prompt**, and then click **Run as Administrator**.
4. At the command prompt, type the following command, and press ENTER:
   wbadmin get versions -backuptarget:<targetDrive>**:**
   -machine:<BackupComputerName>
   Where:
   - <targetDrive>: is the location of the backup that you want to restore.
   - <BackupComputerName> is the name of the computer where you want to recover the backup. This parameter is useful when you have backed up multiple computers to the same location, or you have renamed the computer since the backup was taken.
5. Identify the version that you want to restore.
   - You must enter this version exactly in the next step.
6. At the **Sources** prompt, type the following command, and press ENTER:
   wbadmin start systemstaterecovery -version:<MM/DD/YYYY-HH:MM>
   -backuptarget:<targetDrive>**: -machine:<**BackupComputerName>
   -quiet
   Where:
   - <MM/DD/YYYY-HH:MM> is the version of the backup that you want to restore.
   - <targetDrive>: is the volume that contains the backup.
   - <BackupComputerName> is the name of the computer where you want to recover the backup. This parameter is useful when you have backed up multiple computers to the same location, or you have renamed the computer since the backup was taken.

NOTE: If you do not specify the -quiet parameter, you are prompted to press Y to proceed with the restore process and press Y to confirm that the replication engine for SYSVOL has not changed since you created the backup.

7. After the recovery operation has completed, restart the server. By default, the logon security context is for the DSRM administrator account when you try to log on to the server after it restarts. Click **Switch User** to logon with a domain account.

Performing an Authoritative Restore of AD DS

To perform an authoritative restore of Active Directory objects, you must first perform a non-authoritative restore. However, you must not restart the domain controller normally following the non-authoritative restore procedure. Instead, you use the **ntdsutil authoritative restore** command to mark an object or objects as authoritative. Then you restart the domain controller normally and perform additional tasks as needed. The **ntdsutil** command must be run from an elevated command prompt.

NOTE: Before you can run the authoritative restore subcommand, you need to set NTDS or an AD LDS instance as the active instance for ntdsutil. For example, if the AD LDS instance that you want to restore is named instance 1, type the following command at the ntdsutil prompt before you run the authoritative restore subcommand:

ac in instance 1

The sub-command syntax for the **ntdsutil** command is:

{create ldif file(s) from %s | list nc crs | restore object %s | restore object verinc %d |restore subtree %s | restore subtree %s verinc %d}

The following table defines the parameters of the **ntdsutil** sub-commands:

Parameter	Description
create ldif file(s) from %s	This option creates an LDIF file of link updates from the Ntdsutil-generated text file that is named in *%s*. This file can be used to update backlinks on objects in a domain other than the domain of the restored object. For example, this file can be used to restore group membership for a user when the group belongs to a different domain than the user.
List nc crs	Lists partitions and cross-references. You need the cross-reference of an application directory partition to restore it.
%d	A numeric value that overrides the default value of 100,000. The version number of the object or database being authoritatively restored will be increased by this value times the number of days since backup.
restore object %s	Marks object *%s* as being authoritative. This option also generates a text file that contains the distinguished name of the restored object and an LDIF file that can be used to restore backlinks for objects that are being authoritatively restored (such as group memberships of users).
restore object %s verinc %d	Marks object *%s*as being authoritative and updates links as described in **restore object** *%s*, and also increments the version number by *%d* times the number of days since backup. Use this option only to authoritatively restore over a previous, incorrect, authoritative restore, such as an authoritative restore from a backup that contains the problem that you want to restore.
restore subtree %s	Marks subtree *%s* (and all children of the subtree) as being authoritative. This option also generates a text file that contains the distinguished names of the restored objects and an LDIF file that can be used to restore backlinks for objects that are being authoritatively restored (such as group memberships of users).
restore subtree %s verinc %d	Marks subtree *%s* (and all children of the subtree) as being authoritative, and updates links as described in **restore subtree** *%s*, and also increments the version number by *%d* times the number of days since backup. Use this option only to authoritatively restore over a previous, incorrect, authoritative restore, such as an authoritative restore from a backup that contains the problem that you want to restore.
%s	An alphanumeric variable, either a distinguished name for a restored object or subtree, or a file name for a text file that is used to create an LDIF file.
quit	Takes you back to the previous menu or exits the utility.

Figure 6: NTDSUtil Sub-Commands

Directory Services Restore Mode (DSRM)

This mode (or state) is unchanged from Windows Server 2003 with one exception. In Windows Server 2008, you can run the **dcpromo /forceremoval** command to forcefully remove AD DS from a domain controller that is started in Directory Services Restore Mode, just as you can in the AD DS Stopped state.

Use the **ntdsutil** command to reset the DSRM password on a domain controller. The sub-command syntax is:

Reset Password on server %s

The following table defines the parameters of the **Reset DSRM Administrator Password** sub-command:

Parameter	Description
Reset Password on server %s	Prompts for a new DSRM password for a domain controller. Use NULL as the domain controller name to reset the DSRM password on the current server. After entering this parameter, the **Please type password for DS Restore Mode Administrator Account:** prompt appears. At this prompt, type the desired new DSRM password.
%s	An alphanumeric variable, such as a domain or domain controller name.
quit	Takes you back to the previous menu or exits the utility.

Figure 7: Resetting the DSRM Administrator Password

Perform Offline Maintenance

Follow the steps below to perform offline defragmentation of the directory database:

1. In Directory Services Restore Mode, compact the database file to a local directory or remote shared folder, as follows:
   a. **Local directory:** Go to step 2.
   b. **Remote directory:** If you are compacting the database file to a shared folder on a remote computer, establish a network connection to the shared folder as shown below. Because you are logged on as the local administrator, unless permissions on the shared folder include the built-in Administrator account, you must provide a domain name, user name, and password for a domain account that has Write permissions on the shared folder. In the example below, \\SERVER1\NTDS is the name of the shared folder, and K: is the drive that you are mapping to the shared folder. After typing the first line and pressing ENTER, Ntdsutil.exe prompts you for the password. Type the password, and press ENTER.
      i. **H:\>net use K: \\SERVER1\NTDS /user:***domainName\userName* ***
      ii. Type the password for **\\SERVER1\NTDS:**
      iii. Drive K: is now connected to **\\SERVER1\NTDS**
      iv. The command completed successfully.
2. Type the following command at a command prompt, and press ENTER: **ntdsutil**
3. At the **ntdsutil:** prompt, type **files**, and press ENTER.

4. At the **file maintenance:** prompt, type **compact to** *drive:\ LocalDirectoryPath* (where *drive:\ LocalDirectoryPath* is the path to a location on the local computer), and press ENTER.
   a. If you have mapped a drive to a shared folder on a remote computer, type the drive letter only (for example, **compact to K:**).
   b. **NOTE:** When compacting to a local drive, you must provide a path. If the path contains any spaces, enclose the entire path in quotation marks (for example, compact to "c:\new folder"). If the directory does not exist, Ntdsutil.exe creates it and creates the file named Ntds.dit in that location.
5. If defragmentation completes successfully, type **quit**, and press ENTER to quit the **file maintenance:** prompt. Type **quit** again, and press ENTER to quit Ntdsutil.exe. Go to step 6. If defragmentation completes with errors, go to step 9.
   • **IMPORTANT**: Do not overwrite the original Ntds.dit file or delete any log files.
6. If defragmentation succeeds with no errors, then follow the Ntdsutil.exe onscreen instructions to Delete all of the log files in the log directory by typing: **del** *drive***:***pathToLogFiles****.log**
   a. **NOTE**: You do not need to delete the Edb.chk file.
   b. If space allows, either rename the original Ntds.dit file to preserve it, or copy it to a different location. Avoid overwriting the original Ntds.dit file.
   c. Manually copy the compacted database file to the original location, as follows: **copy** *temporaryDrive***:\ntds.dit** *originalDrive***:***pathToOriginalDatabaseFile***\ntds.dit**
7. Type **ntdsutil**, and press ENTER.
8. At the **ntdsutil:** prompt, type **files**, and press ENTER.
9. At the **file maintenance:** prompt, type **integrity**, and press ENTER.
   • If the integrity check fails, the likely cause is that an error occurred during the copy operation in step 6.3. Repeat steps 6.3 through step 9. If the integrity check fails again, do one of the following:
      a. Contact Microsoft Product Support Services.
      b. Copy the original version of the Ntds.dit file that you preserved in step 6.2 to the original database location and repeat the offline defragmentation procedure.
10. If the integrity check succeeds, proceed as follows:
    a. If the initial compact to command failed, go back to step 4 and perform steps 4 through 9.
    b. If the initial compact to command succeeded, type **quit**, and press ENTER to quit the **file maintenance:** prompt, and then type **quit** and press ENTER again to quit Ntdsutil.exe.
11. Restart the domain controller normally. If you are connected remotely through a Terminal Services session, be sure that you have modified the Boot.ini file for normal restarting before you restart the domain controller.

Follow the steps below to change the garbage collection logging level:

1. Click **Start**; click **Run**; type **regedit**, and press ENTER.
2. In Registry Editor, navigate to the **Garbage Collection** entry in **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics**.
3. Double-click **Garbage Collection**, and for the **Base**, click **Decimal**.
4. In the **Value data** box, type **1**, and click **OK**.

Relocating Active Directory Database Files

The following conditions require relocating AD database files:

- Hardware maintenance: If the physical disk on which the database or log files are stored requires upgrading or maintenance, the database files must be moved, either temporarily or permanently.
- Low disk space: When free disk space is low on the logical drive that stores the database file (Ntds.dit), the log files, or both, first verify that no other files are causing the problem. If the database file or log files are the cause of the growth, then provide more disk space by taking one of the following actions:
    - Expanding the partition on the disk that currently stores the database file, the log files, or both. This procedure does not change the path to the files and does not require updating the registry.
    - Use Ntdsutil.exe to move the database file, the log files, or both to a larger existing partition. If you are not using Ntdsutil.exe when moving files to a different partition, you will need to manually update the registry.

Follow the steps below to relocate the database files:

1. Determine the size and location of the Active Directory database.
2. Compare the size of the directory database files to the volume size.
3. Back up system state.
4. Restart the domain controller in Directory Services Restore Mode.
5. Move or copy the directory database and log files, either to a local drive or a remote share.
    - The shared folder on a remote drive must have enough free space to hold the database file (Ntds.dit) and log files. Create separate subdirectories for copying the database file and the log files.
6. Back up system state.

Monitor Active Directory

The following table lists the events that may be found in Event Viewer when monitoring Active Directory:

Application Directory Partition Default Security		
Event ID	**Source**	**Message**
1979	Microsoft-Windows-ActiveDirectory_DomainService	AD_TERM was unable to correctly create the default security descriptor for the following application directory partition. User Action Review the access control list (ACL) on the newly created application directory partition. Ensure the Replication Get Changes All access right is assigned to both the Enterprise Domain Controllers group and the Enterprise Read-only Domain Controllers group, and remove the right from the domain Domain Controllers group.
1980	Microsoft-Windows-ActiveDirectory_DomainService	The default access control list (ACL) on the following Domain-DNS object class has been previously removed. All subsequently created domain and application directory partitions will permit insecure access. User Action To secure access to domain and application directory partitions created in the future, revert the default security descriptor on the Domain-DNS object class in the schema back to the default setting.
1981	Microsoft-Windows-ActiveDirectory_DomainService	AD_TERM was unable to access the security identifier (SID) associated with the Enterprise Domain Controllers group or the Enterprise Read-only Domain Controllers group.
1982	Microsoft-Windows-ActiveDirectory_DomainService	AD_TERM was unable to delete the access control entry (ACE) for the domain Domain Controllers security group on the newly created application directory partition. This ACE gave the domain Domain Controllers security group the Replication Get Changes All right for the following newly created application directory partition. User Action Review the access control list (ACL) on the newly created application directory partition. Ensure the right Replication Get Changes All is given to both the Enterprise Domain Controllers group and the Enterprise Read-only Domain Controllers group, and remove that right from the domain Domain Controllers group.

1983	Microsoft-Windows-ActiveDirectory_DomainService	AD_TERM failed to create an access control entry (ACE) for the Enterprise Domain Controllers group or the Enterprise Read-only Domain Controllers group on a newly created application directory partition. User Action Review the access control list (ACL) on the newly created application directory partition. Ensure the Replication Get Changes All access right is assigned to both the Enterprise Domain Controllers group and the Enterprise Read-only Domain Controllers group, and remove the right from the domain Domain Controllers group.
KCC Initialization		
Event ID	**Source**	**Message**
1008	Microsoft-Windows-ActiveDirectory_DomainService	Sample Event: The Knowledge Consistency Checker (KCC) did not initialize. Consistency updates to the replication topology on the local domain controller have been disabled. The previous replication topology will be used until the local domain controller is restarted.
Replication Changes		
Event ID	**Source**	**Message**
1084	Microsoft-Windows-ActiveDirectory_DomainService	Preferred bridgehead servers have been selected to support inter-site replication with the following site using the following transport. However, none of these preferred bridgehead servers can replicate the following directory partition. User Action Using Active Directory Sites and Services, do the following: • Configure a domain controller that can support replication of this directory partition as a preferred bridgehead server for this transport. You can do this by modifying the corresponding server. • Verify that the corresponding Server objects have a network address for this transport. For example, domain controllers that replicate using the SMTP transport must have a mailAddress attribute. This attribute is normally configured automatically after the SMTP service is installed. Until this is rectified, the Knowledge Consistency Checker (KCC) will consider all domain controllers in this site as possible bridgehead domain controllers for this directory partition.

1188	Microsoft-Windows-ActiveDirectory_DomainService	A thread in AD_TERM is waiting for the completion of an RPC made to the following directory service. User Action If this condition continues, restart the directory service.
1567	Microsoft-Windows-ActiveDirectory_DomainService	Preferred bridgehead servers have been selected to support inter-site replication with the following site using the following transport. However, none of these preferred bridgehead servers can replicate the following directory partition. User Action • Configure a directory server that can support replication of this directory partition as a preferred bridgehead server for this transport. • Verify that the corresponding Server objects have a network address for this transport. For example, directory servers that replicate using the SMTP transport must have a mailAddress attribute. This attribute is normally configured automatically after the SMTP service is installed. • Until this is rectified, the Knowledge Consistency Checker (KCC) will consider all directory servers in this site as possible bridgehead servers for this directory partition.
1645	Microsoft-Windows-ActiveDirectory_DomainService	AD_TERM did not perform an authenticated remote procedure call (RPC) to another directory server because the desired service principal name (SPN) for the destination directory server is not registered on the Key Distribution Center (KDC) domain controller that resolves the SPN. User Action Verify that the names of the destination directory server and domain are correct. Also, verify that the SPN is registered on the KDC domain controller. If the destination directory server has been recently promoted, it will be necessary for the local directory server's account data to replicate to the KDC before this directory server can be authenticated.
1964	Microsoft-Windows-ActiveDirectory_DomainService	The local directory service has denied a replication attempt on the following directory partition. The following directory service requested to replicate one or more objects from an unauthorized directory partition and the attempt failed. This might pose a security risk.

1977	Microsoft-Windows-ActiveDirectory_DomainService	The following directory service made a replication request for a writable directory partition that has been denied by the local directory service. The requesting directory service does not have access to a writable copy of this directory partition. User Action If the requesting directory service must have a writable copy of this partition, verify that the security descriptor on this directory partition has the correct configuration for the Replication Get Changes All access right. You may also get this message during the transition period after a child partition has been removed. This message will cease when knowledge of the child partition removal has replicated throughout the forest.
SPN Generation		
Event ID	**Source**	**Message**
1411	Microsoft-Windows-ActiveDirectory_DomainService	Active Directory failed to construct a mutual authentication service principal name (SPN) for the following domain controller. The call was denied. Communication with this domain controller might be affected.
Schema Operations (partial list)		
Event ID	**Source**	**Message**
1016	Microsoft-Windows-ActiveDirectory_DomainService	AD_TERM could not be initialized because the schema could not be loaded. User Action Restart the directory service, and try this task again. If this error continues to occur, restore the directory service from backup media.
1135	Microsoft-Windows-ActiveDirectory_DomainService	The search for objects in the schema directory partition failed during the following phase.
1136	Microsoft-Windows-ActiveDirectory_DomainService	AD_TERM failed to create an index for the following attribute. A schema cache update will occur 5 minutes after the logging of this event and will attempt to create an index for the attribute.
1137	Microsoft-Windows-ActiveDirectory_DomainService	AD_TERM successfully created an index for the following attribute.
1140	Microsoft-Windows-ActiveDirectory_DomainService	AD_TERM could not allocate the following amount of memory while caching the schema. User Action Restart the local computer. If this event continues to occur, increase the physical memory or virtual memory.

1157	Microsoft-Windows-ActiveDirectory_DomainService	Internal event: AD_TERM is in the process of creating a new index for the following attribute.
1180	Microsoft-Windows-ActiveDirectory_DomainService	AD_TERM could not delete the following column from the database. This column is no longer used. It was previously used by the following attribute, which has been deleted.
1208	Microsoft-Windows-ActiveDirectory_DomainService	An internal asynchronous attempt to update the schema cache failed with an error. AD_TERM will not retry the operation again. Recent schema updates may not be available until this cache is updated. User Action Perform an explicit synchronous schema cache update or restart the directory service.
1315	*Microsoft-Windows-ActiveDirectory_DomainService*	AD_TERM schema cache failed to inherit all attributes for the following class. The schema cache is incomplete. User Action Refresh the schema cache.
Group Policy Reporting		
Event ID	**Source**	**Message**
1089	Microsoft-Windows-GroupPolicy	Windows failed to record Resultant Set of Policy (RSoP) information, which describes the scope of Group Policy objects applied to the computer or user. This could be caused by RSoP being disabled or Windows Management Instrumentation (WMI) service being disabled or stopped, or other WMI errors. Group Policy settings successfully applied to the computer or user; however, management tools may not report accurately.
1091	Microsoft-Windows-GroupPolicy	Windows could not record the Resultant Set of Policy (RSoP) information for the Group Policy extension %8. Group Policy settings successfully applied to the computer or user; however, management tools may not report accurately.
1095	Microsoft-Windows-GroupPolicy	Windows encountered an error while recording Resultant Set of Policy (RSoP) information, which describes the scope of Group Policy objects applied to the computer or user. Group Policy settings successfully applied to the computer or user; however, management tools may not report accurately.

Figure 8: Common Active Directory-related Event IDs

Repadmin

The **Repadmin** command enables administrators to diagnose Active Directory replication problems between domain controllers running Microsoft Windows operating systems. **Repadmin** is used to view the replication topology, as seen from the perspective of each domain controller. In addition, you can use **Repadmin** to manually create the replication topology, to force replication events between domain controllers, and to view both the replication metadata and up-to-dateness vectors (UTDVECs). You can also use **Repadmin** to monitor the relative health of an AD DS forest. The **Repadmin** command must be run from an elevated command prompt.

The syntax of the **Repadmin** command is:

```
repadmin <cmd> <args> [/u:{domain\user}] [/pw:{password | *}]
[/retry[:<retries>][:<delay>]] [/csv]
```

Most **Repadmin** commands take their parameters in the following order:

1. "Destination or Target DSA_LIST"
2. "Source DSA_NAME", if required
3. <Naming Context> or Object distinguished name, if required

Consider the following example:

```
repadmin /showrepl <DSA_LIST> <Source_DSA_NAME> <Naming Context>
```

<DSA_NAME> is a Directory Service Agent binding string, as is <DSA_LIST>. For AD DS, this string is a network label.

The following table lists the available **Repadmin** commands:

Parameter	Description
Repadmin /kcc	Forces the Knowledge Consistency Checker (KCC) on targeted domain controllers to immediately recalculate the inbound replication topology.
Repadmin /prp	Specifies the Password Replication Policy (PRP) for read-only domain controllers (RODCs).
Repadmin /queue	Displays inbound replication requests that the domain controller must issue to become consistent with its source replication partners.
Repadmin /replicate	Triggers the immediate replication of the specified directory partition to a destination domain controller from a source domain controller.
Repadmin / replsingleobj	Replicates a single object between any two domain controllers that have common directory partitions.
Repadmin / replsummary	Identifies domain controllers that are failing inbound replication or outbound replication, and summarizes the results in a report.
Repadmin / rodcpwdrepl	Triggers replication of passwords for the specified users from the source domain controller to one or more read-only domain controllers. (The source domain controller is typically a hub-site domain controller.)
Repadmin /showattr	Displays the attributes of an object.

Repadmin / showobjmeta	Displays the replication metadata for a specified object that is stored in AD DS, such as attribute ID, version number, originating and local update sequence numbers (USNs), globally unique identifier (GUID) of the originating server, and date and time stamp.
Repadmin /showrepl	Displays the replication status when the specified domain controller last attempted to perform inbound replication on Active Directory partitions.
Repadmin / showutdvec	Displays the highest, committed USN that AD DS, on the targeted domain controller, shows as committed for itself and its transitive partners.
Repadmin /syncall	Synchronizes a specified domain controller with all replication partners.

Figure 9: RepAdmin Commands

Windows System Resource Manager (WSRM)

WSRM is used to control how CPU and memory resources are allocated to applications, services, and processes on the computer.

Follow the steps below to install WSRM:

1. Open Server Manager. Click **Start**; point to **Administrative Tools**, and click **Server Manager**.
2. Under **Features Summary**, click **Add features.**
3. On the **Select Features** page, select the **Windows System Resource Manager** check box.
4. A dialog box will appear informing you that Windows Internal Database also needs to be installed for WSRM to work properly. Click **Add Required Features**, and then click **Next**.
5. On the **Confirm Installation Selections** page, verify that Windows Internal Database and Windows Server Resource Manager will be installed, and click **Install**.
6. On the **Installation Results** page, confirm that the installation of Windows Internal Database and Windows Server Resource Manager succeeded, and click **Close**.

After installing WSRM, you will need to start the Windows System Resource Manager service:

1. Open the Services snap-in. To open the Services snap-in, click **Start**; point to **Administrative Tools**, and click **Services**.
2. In the **Services** dialog box, in the **Name** column, right-click **Windows System Resource Manager**, and click **Start**.

Reliability and Performance Monitor

The following counters are useful when monitoring AD DS:

- NTDS\ DRA Inbound Bytes Total /sec
- NTDS\ DRA Inbound Object
- NTDS\ DRA Outbound Bytes Total /sec
- NTDS\ DRA Pending Replication Synchronizations
- NTDS\ Kerberos Authentications /sec
- NTDS\ NTLM Authentications

Gpresult

The **Gpresult** command is used to display the Resultant Set of Policy (RSoP) information for a remote user and computer.

The syntax of the **Gpresult** command is as follows:

```
gpresult [/s <Computer> [/u [<Domain>\]<UserName>
[/p [<Password>]]]] [/user [<TargetDomain>\]<TargetUser>]
[/scope {user | computer}] [/r | /v | /z] [[/x | /h] <FileName>
[/f]]
```

The following table describes the parameters of the **Gpresult** command:

Parameter	Description
/s <Computer>	Specifies the name or IP address of a remote computer. Do not use backslashes. The default is the local computer.
/u [<Domain>\]<UserName>	Runs the command with the credentials of the specified user. The default user is the user who is logged on to the computer that issues the command.
/p [<Password>]	Specifies the password of the user account that is provided in the **/u** parameter. If **/p** is omitted, **gpresult** prompts for the password. **/p** cannot be used with **/x** or **/h**.
/user [<TargetDomain>\]<TargetUser>	Specifies the remote user whose RSoP data is to be displayed.
/scope {user | computer}	Displays RSoP data for either the user or the computer. If **/scope** is omitted, **gpresult** displays RSoP data for both the user and the computer.
[/x | /h] <FileName>	Saves the report in either XML (**/x**) or HTML (**/h**) format at the location and with the file name specified by the *FileName* parameter. Cannot be used with **/u**, **/p**, **/r**, **/v**, or **/z**.
/f	Forces **gpresult** to overwrite the file name specified in the **/x** or **/h** option.
/r	Displays RSoP summary data.
/v	Displays verbose policy information, including additional detailed settings that have been applied with a precedence of 1.
/z	Displays all available information about Group Policy, including detailed settings that have been applied with a precedence of 1 and higher.

Figure 10: GPResult Command-line Switches

Domain 3: Configuring Active Directory Certificate Services

Install Active Directory Certificate Services

Follow the steps below to install an enterprise root CA:

1. Click **Start**; point to **Administrative Tools**, and click **Server Manager**.
2. In the **Roles Summary** section, click **Add roles**.
3. On the **Select Server Roles** page, select the **Active Directory Certificate Services** check box. Click **Next** two times.
4. On the **Select Role Services** page, select the **Certification Authority** check box, and click **Next**.
5. On the **Specify Setup Type** page, click **Enterprise**, and then click **Next**.
6. On the **Specify CA Type** page, click **Root CA**, and then click **Next**.
7. On the **Set Up Private Key** and **Configure Cryptography for CA** pages, you can configure optional configuration settings, including cryptographic service providers. Click **Next**.
8. In the **Common name for this CA** box, type the common name of the CA, and click **Next**.
9. On the **Set the Certificate Validity Period** page, accept the default validity duration for the root CA or specify a different duration, and click **Next**.
10. On the **Configure Certificate Database** page, accept the default values or specify other storage locations for the certificate database and the certificate database log, and click **Next**.
11. After verifying the information on the **Confirm Installation Options** page, click **Install**.

Follow the steps below to install a stand-alone root CA:

1. Click **Start**; point to **Administrative Tools**, and click **Server Manager**.
2. In the **Roles Summary** section, click **Add roles**.
3. On the **Select Role Services** page, select the **Certification Authority** check box, and click **Next**.
4. On the **Specify Setup Type** page, click **Standalone**, and then click **Next**.
5. On the **Specify CA Type** page, click **Root CA**, and then click **Next**.
6. On the **Set Up Private Key** and **Configure Cryptography for CA** pages, you can configure optional settings, including cryptographic service providers. Click **Next**.
7. In the **Common name for this CA** box, type the common name of the CA, and click **Next**.
8. On the **Set the Certificate Validity Period** page, accept the default validity duration for the root CA, and click **Next**.
9. On the **Configure Certificate Database** page, accept the default values or specify other storage locations for the certificate database and the certificate database log, and click **Next**.
10. After verifying the information on the **Confirm Installation Options** page, click **Install**.

Follow the steps below to set up a subordinate issuing CA:

1. Click **Start**; point to **Administrative Tools**, and click **Server Manager**.
2. In the **Roles Summary** section, click **Add roles**.
3. On the **Select Role Services** page, select the **Certification Authority** check box, and click **Next**.
4. On the **Specify Setup Type** page, click **Standalone** or **Enterprise**, and then click **Next**.
5. On the **Specify CA Type** page, click **Subordinate CA**, and then click **Next**.
6. On the **Set Up Private Key** and **Configure Cryptography for CA** pages, you can configure optional settings, including cryptographic service providers. Click **Next**.
7. On the **Request Certificate** page, browse to locate the root CA, or if the root CA is not connected to the network, save the certificate request to a file so that it can be processed later. Click **Next**.
   - The subordinate CA setup will not be usable until it has been issued a root CA certificate and this certificate has been used to complete the installation of the subordinate CA.
8. In the **Common name for this CA** box, type the common name of the CA.
9. On the **Set the Certificate Validity Period** page, accept the default validity duration for the CA, and click **Next**.
10. On the **Configure Certificate Database** page, accept the default values or specify other storage locations for the certificate database and the certificate database log, and click **Next**.
11. After verifying the information on the **Confirm Installation Options** page, click **Install**.

Configure CA Server Settings

The basic steps for configuring a CA for key archival are:

1. Create a key recovery agent account or designate an existing user to serve as the key recovery agent.
2. Configure the key recovery agent certificate template and enroll the key recovery agent for a key recovery agent certificate.
3. Register the new key recovery agent with the CA.
4. Configure a certificate template, such as Basic EFS, for key archival, and enroll users for the new certificate. If users already have EFS certificates, ensure that the new certificate will supersede the certificate that does not include key archival.
5. Enroll users for encryption certificates based on the new certificate template.
   - Users are not protected by key archival until they have enrolled for a certificate that has key recovery enabled. If they have certificates that were issued before key recovery was enabled, data encrypted with these certificates will not be covered by key archival.

Follow the steps below to back up a CA by using the Certification Authority snap-in:

1. Open the Certification Authority snap-in.
2. In the console tree, click the name of the CA.
3. On the **Action** menu, point to **All Tasks**, and click **Back Up CA**.
4. Follow the instructions in the CA Backup Wizard.

Follow the steps below to back up a CA by using the *Certutil* command-line tool:

1. Open a command prompt.
2. Type **certutil -backup <BackupDirectory>**, where *BackupDirectory* is the path used to store the backup data.
3. Press **Enter**.

Follow the steps below to restore a CA from a backup copy by using the Certification Authority snap-in:

1. Open the Certification Authority snap-in.
2. In the console tree, click the name of the CA.
3. On the **Action** menu, point to **All Tasks**, and click **Restore CA**.
4. Follow the instructions in the Certification Authority Restore Wizard.

Follow the steps below to restore a CA by using the *Certutil* command-line tool:

1. Open a command prompt.
2. Type **certutil -restore <*BackupDirectory*>**, where *BackupDirectory* specifies the path where the backup data is located.
3. Press **Enter**.

Manage Certificate Templates

The following table lists and defines the different certificate templates available in Windows Server 2008:

Name	Description	Key Usage	Applications used for extended key usage (EKU)
Administrator	Allows trust list signing and user authentication	Signature and encryption	Microsoft Trust List Signing EFS Secure Email Client Authentication
Authenticated Session	Allows subject to authenticate to a Web server	Signature	Client Authentication
Basic EFS	Used by Encrypting File System (EFS) to encrypt data	Encryption	EFS
CA Exchange	Used to protect private keys as they are sent to the CA for private key archival	Encryption	Private Key Archival
CEP Encryption	Allows the holder to act as a registration authority (RA) for simple certificate enrollment protocol (SCEP) requests. (The Windows Server 2008 NDES uses this template, by default, for its key exchange certificate to keep communications with devices secret.)	Encryption	Certificate Request Agent
Code Signing	Used to digitally sign software	Signature	Code Signing
Computer	Allows a computer to authenticate itself on the network	Signature and encryption	Client Authentication Server Authentication

Cross-Certification Authority	Used for cross-certification and qualified subordination.	Signature Certificate signing CRL signing	
Directory E-mail Replication	Used to replicate e-mail within Active Directory	Signature and encryption	Directory Service E-mail Replication
Domain Controller	All-purpose certificates used by domain controllers (Superseded by two separate templates: Domain Controller Authentication and Directory E-mail replication)	Signature and encryption	Client Authentication Server Authentication
Domain Controller Authentication	Used to authenticate Active Directory computers and users	Signature and encryption	Client Authentication Server Authentication Smart Card Logon
EFS Recovery Agent	Allows the subject to decrypt files previously encrypted with EFS	Encryption	File Recovery
Enrollment Agent	Used to request certificates on behalf of another subject	Signature	Certificate Request Agent
Enrollment Agent (Computer)	Used to request certificates on behalf of another computer subject	Signature	Certificate Request Agent
Exchange Enrollment Agent (Offline request)	Used to request certificates on behalf of another subject and supply the subject name in the request (The Windows Server 2008 NDES uses this template for its enrollment agent certificate, by default.)	Signature	Certificate Request Agent
Exchange Signature Only	Used by Microsoft Exchange Key Management Service to issue certificates to Exchange users for digitally signing e-mail	Signature	Secure E-mail
Exchange User	Used by Exchange Key Management Service to issue certificates to Exchange users for encrypting e-mail	Encryption	Secure E-mail
IPSec	Used by IPSec to digitally sign, encrypt, and decrypt network communication	Signature and encryption	IPSec Internet Key Exchange (IKE) intermediate
IPSec (Offline request)	Used by IPSec to digitally sign, encrypt, and decrypt network communication when the subject name is supplied in the request. (The Windows Server 2008 SCEP service uses this template, by default, for device certificates.)	Signature and encryption	IPSec IKE intermediate
Kerberos Authentication	New in Windows Server 2008, this template is similar to the "Domain Controller Authentication" template and offers enhanced security capabilities for Windows Server 2008 domain controllers authenticating Active Directory users and computers.	Signature and Encryption	Client Authentication Server Authentication Smart Card Logon KDC Authentication
Key Recovery Agent (KRA)	Recovers private keys that are archived on the CA.	Encryption	Key Recovery Agent

OCSP Response Signing	New in Windows Server 2008, this template issues certificates used by the OCSP Service Provider to sign OCSP responses. (By default, these certificates contain a special "OCSP No Revocation Checking" extension and no AIA or CDP extensions.)	Signature	OCSP Signing
Remote Access Service (RAS) and Internet Authentication Service (IAS) Server	Enables RAS and IAS servers to authenticate their identity to other computers	Signature and Encryption	Client Authentication Server Authentication
Root CA	Used to prove the identity of the root CA	Signature Certificate signing CRL signing	
Router (Offline request)	Used by a router when requested through SCEP from a CA that holds a CEP Encryption certificate	Signature and encryption	Client Authentication
Smart Card Logon	Allows the holder to authenticate using a smart card	Signature and encryption	Client Authentication Smart Card Logon
Smart Card User	Allows the holder to authenticate and protect e-mail using a smart card	Signature and encryption	Secure E-mail Client Authentication Smart Card Logon
Subordinate CA	Used to prove the identity of the subordinate CA. It is issued by the parent or root CA.	Signature Certificate signing CRL signing	
Trust List Signing	Allows the holder to digitally sign a trust list	Signature	Microsoft Trust List Signing
User	Used by users for e-mail, EFS, and client authentication	Signature and encryption	EFS Secure E-mail Key Usage
User Signature Only	Allows users to digitally sign data	Signature	Secure E-mail Client Authentication
Web Server	Proves the identity of a Web server	Signature and encryption	Server Authentication
Workstation Authentication	Enables client computers to authenticate their identity to servers	Signature and encryption	Client Authentication

Figure 11: Server 2008 Certificate Templates

Follow the steps below to add a certificate template to a CA:

1. Open the Certification Authority snap-in, and double-click the name of the CA.
2. Right-click the Certificate Templates container; click **New**, and then click **Certificate Template to Issue**.
3. Select the certificate template, and click **OK**.

Follow the steps below to set CA administrator and certificate manager security permissions for a CA:

1. Open the Certification Authority snap-in.
2. In the console tree, click the name of the CA.
3. On the **Action** menu, click **Properties**.
4. Click the **Security** tab, and specify the security permissions.

Follow the steps below to define permissions to allow a specific security principal to enroll for certificates based on a certificate template:

1. Log on as a member of the Enterprise Admins or the forest root domain's Domain Admins group, or as a user who has been granted permission to perform this task.
2. Open the **Certificate Templates** MMC (*Certtmpl.msc*).
3. In the details pane, right-click the certificate template you want to change, and then click **Properties**.
4. On the **Security** tab, ensure that **Authenticated users** is assigned **Read** permissions.
   - This ensures that all authenticated users on the network can see the certificate templates.
5. On the **Security** tab, click **Add**. Add a global group or universal group that contains all security principals requiring Enroll permissions for the certificate template, and click **OK**.
6. On the **Security** tab, select the newly added security group, and then assign **Allow** permissions for the **Read and Enroll** permissions.
7. Click **OK**.

Follow the steps below to configure a key recovery agent:

1. Log on as Administrator of the server or CA Administrator, if role separation is enabled.
2. On the **Administrative Tools** menu, open **Certification Authority**.
3. In the console tree, select the CA.
4. Right-click the CA name, and then click **Properties**.
5. Click the **Recovery Agents** tab.
6. To enable key archival, click **Archive the key**.
7. By default, the CA will only use one KRA. However, a KRA certificate must first be selected for the CA to begin archival. To select a KRA certificate, click **Add**.

The system will find valid KRA certificates and display the available KRA certificates.

KRA certificates are normally published to Active Directory by an Enterprise CA when enrollment occurs. KRA certificates are stored under the KRA container in the Public Key Services branch of the configuration partition in Active Directory. Since a CA may issue multiple KRA certificates, each KRA certificate will be added to the multi-valued userAttribute attribute of the CA object.

1. Select one certificate and click **OK**. You may view the highlighted certificate to ensure that you have selected the intended certificate.
2. After one or more KRA certificates have been added, click **OK** to enable key archival on the CA. However, Certificate Services must be stopped and started to enable the use of the selected KRAs. KRA certificates are only processed at service start.

Manage Enrollments

Follow the steps below to configure the default action for certificate requests:

1. Open the Certification Authority snap-in.
2. In the console tree, click the name of the CA.
3. On the **Action** menu, click **Properties**.
4. On the **Policy Module** tab, click **Properties**.
5. Click the option you want:
   a. To have the CA administrator review every certificate request before issuing a certificate, click **Set the certificate request status to pending**.
   b. To have the CA issue certificates based on the configuration of the certificate template, click **Follow the settings in the certificate template, if applicable. Otherwise, automatically issue the certificate**.
6. Stop and restart the CA.

Follow the steps below to set up and configure the Network Device Enrollment Service (NDES):

1. Click **Start**; point to **Administrative Tools**, and click **Server Manager**.
2. In the **Roles Summary** section, click **Add roles**.
3. On the **Select Role Services** page, clear the **Certification Authority** check box, and select **Network Device Enrollment Service**.
   - Unless already installed on the selected server, you are prompted to install IIS and Windows Activation Service.
4. Click **Add Required Role Services**, and then click **Next** three times.
5. On the **Confirm Installation Options** page, click **Install**.
6. When the installation is complete, review the status page to verify that the installation was successful.
7. If this is a new installation with no pending SCEP certificate requests, click **Replace existing Registration Authority (RA) certificates**, and then click **Next**.
   - **NOTE**: When the Network Device Enrollment Service is installed on a computer where a registration authority already exists, the existing registration authority, and any pending certificate requests, are deleted.
8. On the **Specify User Account** page, click **Select User**, and type the user name and password for this account, which the Network Device Enrollment Service will use to authorize certificate requests. Click **OK**, and then click **Next**.
9. On the **Specify CA** page, select either the **CA name** or **Computer name** check box; click **Browse** to locate the CA that will issue the Network Device Enrollment Service certificates, and then click **Next**.
10. On the **Specify Registry Authority Information** page, type computer name in the **RA name** box. Under **Country/region**, select the check box for the country/region you are in, and click **Next**.
11. On the **Configure Cryptography** page, accept the default values for the signature and encryption keys, and click **Next**.
12. Review the summary of configuration options, and click **Install**.

Follow the steps below to configure the autoenrollment options in Group Policy:

1. On a domain controller running Windows Server 2008, click **Start**; point to **Administrative Tools**, and click **Group Policy Management**.
2. In the console tree, double-click **Group Policy Objects** in the forest and domain containing the **Default Domain Policy** Group Policy object (GPO) that you want to edit.
3. Right-click the **Default Domain Policy** GPO, and then click **Edit**.
4. In the Group Policy Management Console (GPMC), go to **User Configuration**, **Windows Settings**, **Security Settings**, and click **Public Key Policies**.
5. Double-click **Certificate Services Client - Auto-Enrollment**.
6. Select the **Enroll certificates automatically** check box to enable autoenrollment. If you want to block autoenrollment from occurring, select the **Do not enroll certificates automatically** check box.
7. If you are enabling certificate autoenrollment, you can select the following check boxes:
   a. Renew expired certificates, update pending certificates, and remove revoked certificates
   b. Update certificates that use certificate templates
8. Click **OK** to accept your changes.

Follow the steps below to install Web enrollment support:

1. Click **Start**; point to **Administrative Tools**, and click **Server Manager**.
2. Click **Manage Roles**. Under **Active Directory Certificate Services**, click **Add role services**. If a different AD CS role service has already been installed on this computer, select the **Active Directory Certificate Services** check box in the **Role Summary** pane, and click **Add role services**.
3. On the **Select Role Services** page, select the **Certification AuthorityWeb Enrollment Support** check box.
4. Click **Add required role services**, and then click **Next**.
5. On the **Specify CA** page, if a CA is not installed on this computer, click **Browse** to select the CA that you want to associate with Web enrollment; click **OK**, and then **Next**.
6. Click **Next**; review the information listed, and click **Next** again.
7. On the **Confirm Installation Options** page, click **Install**.
8. When the installation is complete, review the status page to verify that the installation was successful.

Follow the steps below to configure an Enterprise CA to issue a KRA certificate for use with smart card enrollment:

1. On the **Administrative Tools** menu, open the **Certification Authority** snap-in.
2. In the console tree, expand **Certification Authority**, and click **Certificate Templates**.
3. Right-click the **Certificate Templates** node; click **New**, and then click **Certificate Template to Issue**.
4. In the **Select Certificate Template** dialog box, click **Key Recovery Agent**, and then click **OK.**
5. Close the **Certification Authority** MMC snap-in.

Follow the steps below to define permissions to allow a specific security principal to enroll for certificates based on a certificate template

1. Log on as a member of the Enterprise Admins or the forest root domain's Domain Admins group, or as a user who has been granted permission to perform this task.
2. Open the **Certificate Templates** MMC (Certtmpl.msc).
3. In the details pane, right-click the certificate template you want to change, and then click **Properties**.
4. On the **Security** tab, ensure that **Authenticated users** is assigned **Read** permissions.
   - This ensures that all authenticated users on the network can see the certificate templates.
5. On the **Security** tab, click **Add**. Add a global group or universal group that contains all security principals requiring Enroll permissions for the certificate template, and click **OK**.
6. On the **Security** tab, select the newly added security group, and then assign **Allow** permissions for the **Read and Enroll** permissions.
7. Click **OK**.

Manage Certificate Revocations

Follow the steps below to install the Online Responder:

1. Ensure that IIS has already been installed on the Windows Server 2008 computer.
2. Click **Start**; point to **Administrative Tools**, and click **Server Manager**.
3. Click **Manage Roles**. In the **Active Directory Certificate Services** section, click **Add role services**.
4. On the **Select Role Services** page, select the **Online Responder** check box.
5. You are prompted to install IIS and Windows Activation Service.
6. Click **Add Required Role Services**, and then click **Next** three times.
7. On the **Confirm Installation Options** page, click **Install**.

Follow the steps below to configure the CA for OCSP Response Signing certificates:

1. Log on to the server as a CA administrator.
2. Open the Certificate Templates snap-in.
3. Right-click the **OCSP Response Signing** template, and then click **Duplicate Template**.
4. Type a new name for the duplicated template.
5. Right-click the new certificate template, and then click **Properties**.
6. Click the **Security** tab. Under **Group or user name**, click **Add**, and type the name or browse to select the computer that will be hosting the Online Responder service.
7. Click the computer name, and in the **Permissions** dialog box, select the **Read** and **Autoenroll** check boxes.
8. While you have the Certificate Templates snap-in open, you can configure certificate templates for users and computers by substituting the desired templates in step 3, and repeating steps 4 through 7 to configure additional permissions for the server and your user accounts.

Follow the steps below to configure a CA to support the Online Responder service:

1. Open the Certification Authority snap-in.
2. In the console tree, click the name of the CA.
3. On the **Action** menu, click **Properties**.
4. Click the **Extensions** tab. In the Select extension list, click **Authority Information Access (AIA)**.
5. Select the **Include in the AIA extension of issue certificates** and **Include in the online certificate status protocol (OCSP)** extension check boxes.
6. Specify the locations from which users can obtain certificate revocation data.
7. In the console tree of the Certification Authority snap-in, right-click **Certificate Templates**, and then click **New Certificate Templates to Issue**.
8. In **Enable Certificate Templates**, select the **OCSP Response Signing** template and any other certificate templates that you configured previously, and click **OK**.
9. Open **Certificate Templates**, and verify that the modified certificate templates appear in the list.

Follow the steps below to create a revocation configuration:

1. Open the Online Responder snap-in.
2. In the **Actions** pane, click **Add Revocation Configuration** to start the Add Revocation Configuration wizard, and then click **Next**.
3. On the **Name the Revocation Configuration** page, type a name for the revocation configuration, and click **Next**.
4. On the **Select CA certificate Location** page, click **Select a certificate from an existing enterprise CA**, and then click **Next**.
5. On the following page, the name of the CA should appear in the **Browse CA certificates published in Active Directory** box.
    a. If it appears, click the name of the CA that you want to associate with your revocation configuration, and then click **Next**.
    b. If it does not appear, click **Browse for a CA by Computer name** and type the name of the computer, or click **Browse** to locate this computer. When you have located the computer, click **Next**.
    c. You might also be able to link to the CA certificate from the local certificate store or by importing it from removable media in step 4.
6. View the certificate and copy the CRL distribution point for the parent root CA. To do this:
    a. Open the Certificate Services snap-in. Select an issued certificate.
    b. Double-click the certificate, and then click the **Details** tab.
    c. Scroll down and select the **CRL Distribution Points** field.
    d. Select and copy the URL for the CRL distribution point that you want to use.
    e. Click **OK**.
7. On the Select Signing Certificate page, accept the default option, **Automatically select signing certificate**, and click Next.
8. On the Revocation Provider page, click **Provider**.
9. On the **Revocation Provider Properties** page, click **Add**; enter the URL of the CRL distribution point, and click **OK**.
10. Click **Finish**.

Using the Online Responder snap-in, select the revocation configuration, and then examine the status information to verify that it is functioning properly. You should also be able to examine the properties of the signing certificate to verify that the Online Responder is configured properly.

Follow the steps below to revoke a certificate:

1. Open the Certification Authority snap-in.
2. In the console tree, click **Issued Certificates**.
3. In the details pane, click the certificate you want to revoke.
4. On the **Action** menu, point to **All Tasks**, and click **Revoke Certificate**.
5. Select the reason for revoking the certificate; adjust the time of the revocation, if necessary, and then click **Yes**. Available reason codes are:
   a. Unspecified
   b. Key Compromise
   c. CA Compromise
   d. Change of Affiliation
   e. Superseded
   f. Cease of Operation
   g. Certificate Hold. This is the only reason code that can be used when you might want to unrevoke the certificate in the future.

Follow the steps below to configure the Authority Information Access (AIA) extension:

1. Open the Certification Authority snap-in; right-click the name of the issuing CA, and then click **Properties**.
2. Click the **Extensions** tab.
3. In the **Select extension** list, click **Authority Information Access (AIA)**, and then click **Add**.
4. In the **Add Location** dialog box, type the full URL of the Online Responder, which should be in the following form: http://<*DNSServerName*>/<*vDir*>
   • NOTE: When installing the Online Responder, the default virtual directory used in IIS is OCSP.
5. Click **OK**.
6. Select the location from the **Location** list.
7. Select the **Include in the online certificate status protocol (OCSP) extension** check box, and click **OK**.

Domain 4: Configure IP Addressing and Services

In the 70-648 Exam, addressing a given topology plays a large portion in your overall score on the exam and whether or not you will succeed. To do well, you need to be familiar with the concepts of subnetting, Addressing, and IPv4 and IPv6. We'll start with IPv4.

Configuring IPv4 and IPv6 Addressing

IPv4 Addressing

32 bit addressing is the most common form of addressing and comes in three forms: APIPA, Static, and Dynamic.

- **APIPA Addressing** – a mechanism that Windows Server uses to address a logical device, even if a DHCP server or manual address is unavailable. These addresses are placed in the 168.254.0.0/16 range. These are usually addresses that are given as "temporary" addresses so that a logical device is always given a logical address.

- **Static Addresses** – manually configured addresses on devices in order to manually assign the network topology of a given interface. This is done by administrators to specify addresses that they will always be able to remember.

- **Dynamic Addressing** – a technique that takes advantage of the Dynamic Host Configuration Protocol (DHCP) role that can be added to a Windows Server. DHCP is a mechanism that we'll discuss in depth in this section of your Exam Manual.

Address Ranges

When designing a network, we need to decide how to address a network in a manner that is large enough to encompass the entirety of our organization, allocate for room to for growth, but not be so large that it doesn't overtake the organization with its sheer mass of extra address space and actually *inhibit* the process of growth.

IPv4 address ranges are developed by determining an address class and a subnet range. You can determine these by determining figure out how many hosts you require, roughly doubling the number to account for growth, and picking the address based on the expected number of hosts.

ADDRESS CLASS	NUMBER OF NETWORK BITS	AVAILABLE HOST BITS	MAXIMUM HOSTS
Class A	8	24	16,777,214
Class B	16	16	65,534
Class C	24	8	254

Figure 12: IPv4 Address Class Specifications

Furthermore, each of these network classes is assigned certain ranges that will be predefined for your network design. These ranges are broken down into several portions by the first octet (0-255) of your network. These break down as follows:

- Class A 1.0.0.0 to 126.255.255.255
- Class B 128.0.0.0 to 191.255.255.255
- Class C 192.0.0.0 to 223.255.255.255

The only exceptions to these are **private IP addresses**, which are defined for each class of address:

- Class A: **10.0.0.0 to 10.255.255.255**
- Class B: **172.16.0.0 to 172.31.255.255**
- Class C: **192.168.0.0 to 192.168.255.255**
- Localhost**: 127.0.0.1**

These addresses will function on internal networks, but will not function on the Internet. Most organizations will use Network Address Translation (NAT) to allow their users to access the Internet despite the use of private addresses on the internal network. This is covered in more detail, later in the manual.

Subnetting IPv4

Subnetting is a complicated process that involves using binary math to subdivide a range of provided addresses within a network into smaller subnetworks (thus the "sub" in subnetting). This succeeds in separating a network into different collision domains, improving the overall efficiency of hosts within larger networks. The process also helps to alleviate some of the limitations of classful addressing.

The Subnetting Process:

1. Determine how many addresses you need per network.
2. Find a power of two that is greater than your address needs. For example, if you need **28 addresses**, you would use $\mathbf{2^5}$, because $\mathbf{2^5 = 32}$, four more addresses than your network's requirements.
3. Use the **power of two** to find intervals of the address up to 256.
4. Let's use the example we started with: subnetting the 192.168.0.X subnet into equal subnetworks, housing 28 address each:

   Find the **power of two**…

   25 = 32. The official formula is **2N-2**. (The -2 takes into account the broadcast and subnet ID addresses).

   Take the 192.168.0.X address and **replace the X with multiples of 32**…

   192.168.0.0
   192.168.0.32
   192.168.0.64
   192.168.0.96
   192.168.0.128
   192.168.0.160
   192.168.0.192
   192.168.0.224
   192.168.0.256

   Each IP address above represents **the Subnet ID** address, which are unusable by hosts. Additionally, we can't use the **192.168.0.0** or **192.168.0.224** ranges.

   Next we find the **broadcast addresses**, which are the **last usable** IP Address in each range:

   192.168.0.31
   192.168.0.63
   192.168.0.95
   192.168.0.127
   192.168.0.159
   192.168.0.191

Our **host address ranges** are everything not reserved by subnet IDs, broadcast addresses or unusable subnets:

Subnet .32: 192.168.0.32 - 192.168.0.62
Subnet .64: 192.168.0.65 - 192.168.0.94
Subnet .96: 192.168.0.97 - 192.168.0.126
Subnet .128: 192.168.0.129 - 192.168.0.158
Subnet .160: 192.168.0.161 - 192.168.0.190
Subnet .192: 192.168.0.193 - 192.168.0.222

SuperNetting

A supernet is a collection of subnets that are routed by a router. The way to think of them is that they are collections of smaller subnets that are contained within a larger subnet. This is done so that fewer calls are made to the router for the purpose of routing between subnets that are contained within the supernet. This way, more traffic can be handled by switches and managed switches.

IPv6 Addressing

IPv6 addresses are 128 bit addresses that make use of a 64 bit host and 64 bit network portion.

Address Ranges

IPv6 doesn't actually work much like 32 bit IPv4. The address ranges are not infinite, but the amount of IPv6 addresses is so large that you won't have to worry about subnetting as much. This said, IPv6 does support standard subnet masks.

IPv6 Shorthand Addressing

Using IPv6, you can shorten addresses by using the :: and : convention. A standard IPv6 address looks something like this:

2001:cdba:0000:0000:0000:0000:3257:9652

With shorthand, you can shrink each section of four zeros down to ":0" and then multiple sections of zeros to "::," like so:

2001:cdba:0:0:0:0:3257:9652
2001:cdba::3257:9652

IPv6 Broadcast

IPv4 Broadcast is pretty simple and can be defined in a single sentence: IPv4 broadcasts to a subnet. Ipv6 is quite different, in that it has three scope methods where it broadcasts: **Unicast**, **Multicast** and **Anycast**.

Unicast – in IPv6, addresses can deliver a single address to a single specified interface by using a unicast address. You can think of this a lot like a router border. It is a specific area that only receives broadcast from one place to another, specified by a network administrator. The key point here is that they can only go to one place.

Multicast – a multicast address is sort of like a unicast address that broadcasts to a group of unicasts for the purpose of saving bandwidth. Alternatively, you'd have to send a unicast to each individual address, which would be time consuming. Think of it like this: One address says "Hey, you bunch of unicasts!" Sounds kind of silly, but it's a good way of looking at it. Except just to mix things up, multicast address have different scopes:

- **Global –** has a completely global scope
- **Organizational-Local –** are confined to one custom build scope for an organization
- **Site-Local –** these sites have the scope of an entire site or organization, and can be addressed without the need for a public prefix
- **Link-Local –** Link Local addresses are assigned to a specific link and can't go outside this link. They can be used to for address configuration and neighbor discovery
- **Node-Local –** Confined only to a node scope

The last thing to note about them is that Multicast addresses can be easily identified because they start with the binary 1111 1111 (FF). Thus, FF00:0:0:0:0:0:0:1 is a multicast address.

Anycast – an anycast address is an address that is not as commonly used, but is infinitely more flexible than other IPv6 addresses. It's not assigned a specific interface, but instead is assigned to a specific router function. An anycast address is an address that can go from anywhere specified by an administrator to anywhere else specified by an administrator. The way it works is that a single address can send from its own address to any single member of a given group. This differs from multicasts, who send from one address to the whole group. Unicast addresses send from one address to another single address. The advantage of anycast addresses is that they will be delivered to whatever address is nearest.

Transitional Techniques

IPv6 makes use of several transitional techniques to translate from IPv4 to IPv6. These techniques are:

- **Teredo –** a method to translate IPv6 to IPv4 through IPv6 NAT unaware devices. Effectively what happens with teredo tunneling is that an IPv6 packet encapsulates through a UDP datagram that can be routed through IPv4 across WAN links. In other words, IPv6 gets mutated into IPv4 and then passed along into IPv6.
- **ISATAP –** Intra-Site Automatic Tunnel Addressing Protocol creates an IPv6 address stack on top of an IPv4 stack. This is done so both the IPv4 and IPv6 stacks are able to access data through one local network device. ISATAP uses a virtual, non-broadcast, multiple-access data link layer that allows it to support multicasting. ISATAP addresses can come in multiple forms, depending on their scope:
  - Link-Local – FE80
  - Site-Local – FEC0

Configuring Dynamic Host Configuration Protocol (DHCP)

The DHCP process is the flow of automatically assigning addresses from a DHCP client to a DHCP server. The process works as illustrated below:

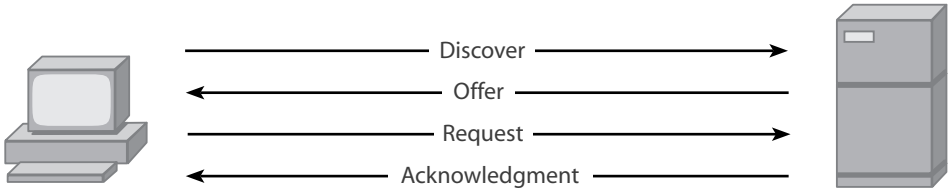

Figure 13: The DHCP Process

The server discovers the clients, the server offers an address, the client requests and address, and then the server confirms that address.

Configuring DHCP

Configuring DHCP on Windows Server 2008 is an easy and straight forward process using Server Manager. To configure DHCP, perform the following steps:

1. Open the **Server Manager.**
2. Select **Roles** and then select **Add Roles.**
3. Choose **DHCP Server** in the **Server Roles Manager** and click **Next.**
4. After reading through the introduction page, click **Next**.
5. On the address you see below, make *sure* that the address is the address of your server.

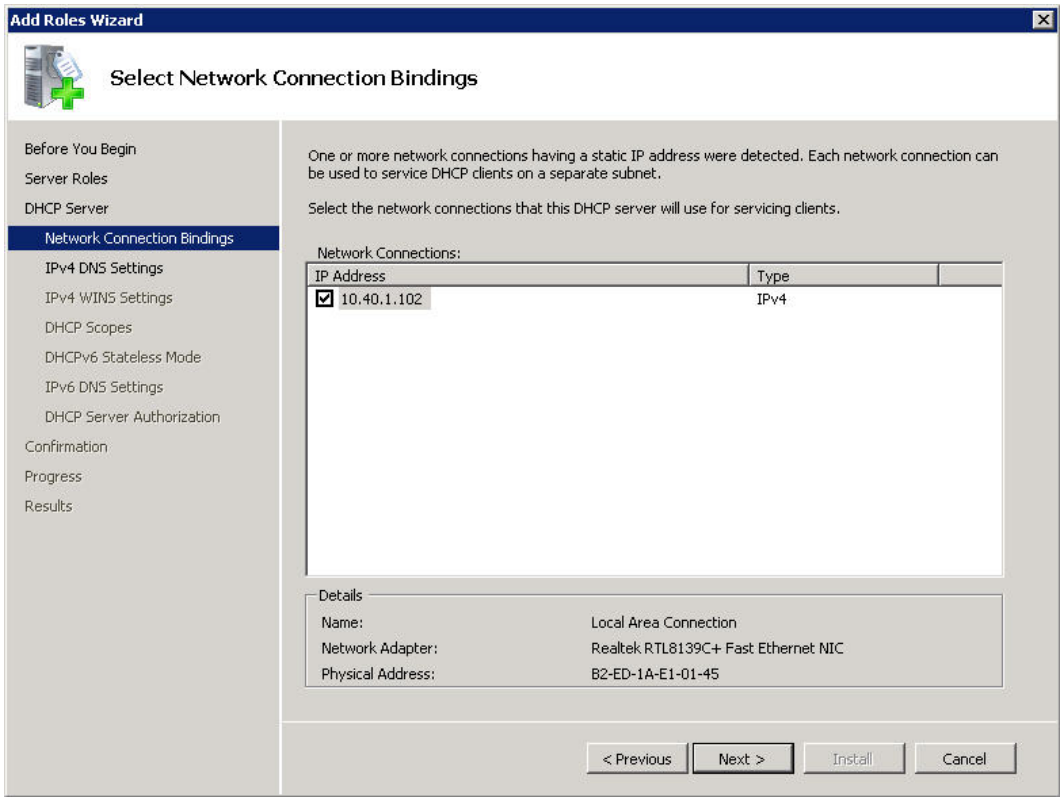

Figure 14: Configuring a DHCP Server Role

6. Click **Next**.
7. In the next screen, shown below, make sure the parent domain is the name of your domain and specify the DNS address of your DNS server (usually your domain controller) and an alternate DNS server, if one is available. If not, you can use a free, public DNS server. Click **Next**

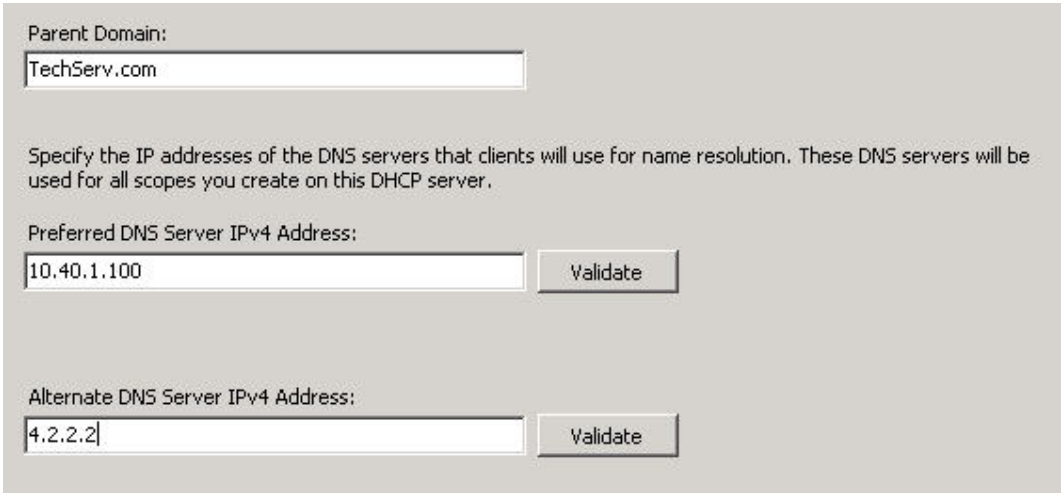

Figure 15: Entering DNS Information

8. In the next box, select whether or not you would like to use **WINS** and click **Next**. Unless you know you'll need WINS for your network, we strongly recommend clicking "WINS is not required for applications on this network".
9. Under the scopes section click **Add**. Depending on the class range of your address, you'll want to enter the IP address range of addresses you would like your server to address. If you don't know, enter something similar to what we have below and click **Next.**

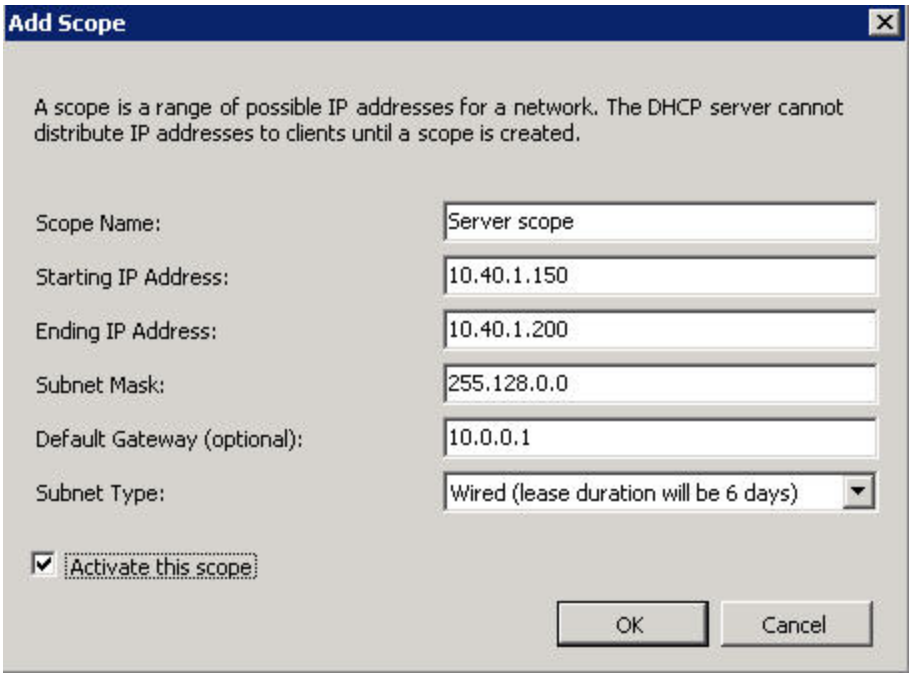

Figure 16: Adding IP Address Scopes

10. Click **OK**, then click **Next**.
11. In DHCP mode, disable **stateless mode** unless you would like to use IPv6, in which case you'll need to enter your IPv6 DNS information in the next screen. Click **Next.**
12. On the following screen, keep the settings default unless you would like to use different credentials to authorize your addresses and click **Next**.
13. Click **Install**.
14. Click **Finish** when the process completes.
15. Enabling a DHCP server on Windows Server 2008 Server Core edition is actually quite easy.

DHCP can be enabled through **Server Core** by executing the following command:

start /w ocsetup DHCPServerCore.

Follow the onscreen instructions to configure a scope and then authorize it.

To uninstall the DHCP server role, enter the following command:

start /w ocsetup DHCPServerCore /uninstall

The DHCP Server role can be started by entering the following commands:

1. sc config dhcpserver start= auto
2. net start dhcpserver

PXE Boot

The **Pre-boot Execution Environment** (PXE Boot) is a configurable option with Windows Server 2008 that will allow you to boot from a network service. Effectively, what happens is PXE asks DHCP for an address and then speaks to a network boot program service and gets fed information that will allow clients to boot from windows services. To enable this, you must have a DHCP server running, as well as Windows Deployment Services. Typically, Microsoft will not require you to set this up on the this exam, because it involves Windows Deployment Services, which are mostly covered on the 70-643 and 70-649 exams. For this exam, you will just need to memorize the process, which is as follows:

1. A client sends a PXE request.
2. The PXE server forwards the request to a deployment services provider.
3. The PXE provider inspects the server and the address and either succeeds or fails.
4. If it fails, the process stops, if it succeeds, the request is fed to the deployment server and the process is begun through the trivial file transfer protocol (TFTP), a simple file protocol that passes through port 20.

Default User Profiles

Default user profiles are created whenever a Domain User or local user logs on to a local box. On Windows XP, profiles are created in the C:\Documents and Settings\ directory. In Windows Vista or later operating systems, they are created in a virtually linked directory called the Users directory, under C:\Users. Whenever users are logged in, Windows will create default user profiles for any logged in user. Alternatively, you can make roaming profiles that follow users around wherever they go. However, the entirety of the profile must be stored in the Windows Domain and transferred to wherever a user is logging in.

For example, if a user logs in to a Windows XP machine which they have never used before, the user will have their "roaming profile" transferred. And, if they have a lot of large files in their profile (like mp3s or huge database files, for example) this may take quite a while.
In Windows, a profile consists of the following information:

- Contacts
- Desktop
- Downloads
- Favorites
- Links
- My Documents
- <Other added files>
- Searches* - Windows Vista+

It also contains tons of other information, like customizations to start menus and background for the desktop and other customization features.

Relay Agents

DHCP relay agents are used to forward requests for DHCP from server to server or subnet to subnet, which are not normally forwarded. You can enable a DHCP relay agent by performing the following actions:

1. Install **DHCP**, as we explained, above.
2. Under **IPv4/6** in **Routing and Remote Access**, right click **General** and click **New Routing Protocol.**
3. Select **DHCP relay Agent** from the dropdown.
4. Right click the agent that is created underneath IPv4 and select **New Interface**.
5. Choose the interface you'd like to use as a relay agent, and then dynamically assign it an IP from the menu.

Exclusions

DHCP exclusions are exclusions of IP addresses that you can manually make in the DHCP routing and remote access area by manually entering them in as excluded addresses. For example, if you were using the 192.168.0.X subnet, you could exclude the address of 192.168.0.100 if that address is manually assigned to your server. To do this, you just need to follow this procedure:

1. Navigate to the **DHCP MMC** from **Administrative Tools** in the **Start Menu**.
2. **Double-click** your DHCP server.
3. **Double-click** IPv4.
4. Right-click **Address Pool** and add a **New Exclusions Range**.
5. Enter the starting and ending IP address range that you would like to exclude, and then click **Close**.

Authorizing a Server in Active Directory

Servers in DHCP are authorized (or unauthorized, as the case may be) to give addresses based on the Active Directory domain and forest information. This means that an unauthorized DHCP server cannot give random IP addresses out to anyone that isn't in the domain. This way, you don't have issues if you have something like two clients from different domains on the same subnet getting fed different requests for DHCP addresses because there are two servers on the domain. Instead, they have to be authorized for that domain. To authorize a server, you can do this when you first install DHCP, like we did above, or you can pretty simply do it by navigating to the DHCP MMC and adding an authorization.

Scopes

DHCP Scopes are the definable address range associated with DHCP. For instance, if you want to run a scope from 192.168.0.1 to 192.168.0.255, you're effectively running a scope from the class C 192.168.0.X 255.255.255.0 range. Putting it more complicated than that just confuses things, and makes it harder to pass the test. When you're being asked about scopes, just think of it like this: A DHCP scope is the range of addresses that your server is allowed to use. There can be more than just one, or just one. What does matter is that when your DHCP server runs out of usable ranges in one scope, it will attempt to use another. You can define scopes in the DHCP MMC.

Windows Server Hyper-V

What you need to know about Windows Server 2008 Hyper-V and DHCP is pretty straight forward, although Microsoft will both have you think that it's really complicated, and also ask you a ton of questions on it. To get through it all, just know the following:

1. Hyper-V can run as a DHCP server
2. Hyper-V can receive a DHCP address, so long as a network interface is assigned to the VM
3. Hyper-V supports IPv6
4. Hyper-V plays friendly with active directory domain building

Configuring Routing

The process of configuring routing and remote access on Windows Server 2008 is not as difficult as it seems. First, configuring routing is done through the Server Manager. And second, you have to install Network Policy and Access Services, as shown in the steps below, to get to it:

1. Start **Server Manager**.
2. Select **Roles.**
3. Click **Add Roles.**
4. Select **Network Policy and Access Services.**
5. Click **Next** at the intro screen.
6. Select **Routing and Remote Access Services**, and then click **Next**.
7. Click **Install**.
8. Once it's installed, click **Close**.

Set Up Routing

The most important thing we need to understand about is the difference between classful and classless routing protocols. RIPv1 is a classful routing protocol that uses a "hop" based metric system to count distances between routing points and RIPv2 and OSPF (which is no longer supported by Windows Server 2008) are classless. To set up routing protocols (RIP):

1. Navigate to **Routing and Remote Access** from **Administrative Tools** and **right-click** on your server.
2. Select **Configure and Enable Routing and Remote Access.**
3. The wizard will open; click **Next**.
4. Select **Custom Configuration**, click **Next**.
5. Select the **LAN Routing** checkbox, click **Next**.
6. Click **Finish**. If you're asked to start the service, start the service.
7. Your server should now have a green up arrow next to it. **Expand** your Server and **expand IPv4**, then **right-click General** and select **New Routing Protocol**. You can select either **RIPv2** or **IGMP**. Select RIPv2. **Note:** This is the same spot where you'd enable a DHCP relay agent.
8. Now you'll see RIP listed under IPv4. **Right-click** it, and select **New Interface…**
9. Select your interface.
10. Press **OK**.

Configuring IPSec

IPSec is an example of a security mechanism that determines how a local security policy handles a group of computers network traffic. It is a suite of protocols that provides encryption that can be configured through group policy, and managed through a filter list that allows certain types of traffic. Effectively, IPSec is like an overriding "yes/no" filter that sits across you entire server infrastructure. With Windows Server 2008, all IPSec is managed through a single section with the Group Policy Editor, which can only be accessed through the Group Policy Management Console. Effectively, IPSec should be assigned in this fashion:

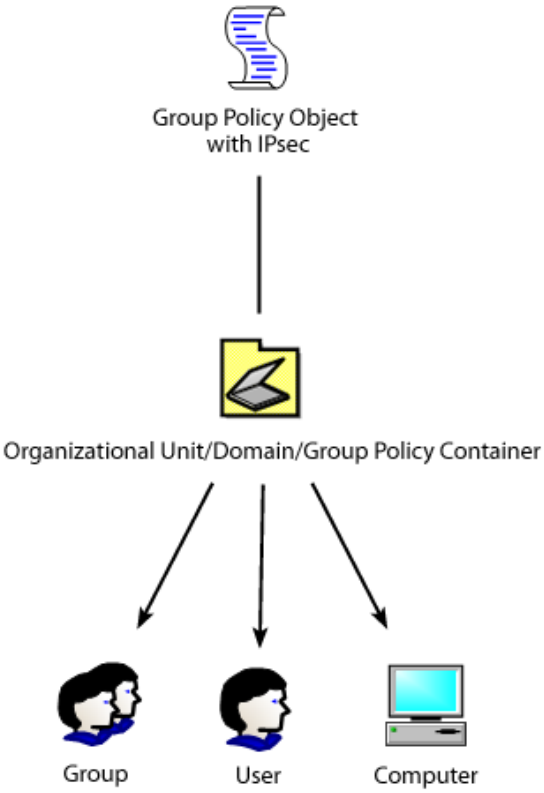

Figure 17: Group Policy with IPSec

The group Policy Object is linked to the container and the container contains active directory objects, such as users, groups, computers, printers, and so forth.

To configure IPSec:

1. Navigate to the **Group Policy Management Console** (GPMC) by going to **Administrative Tools** and then **Group Policy Management.**
2. Select a group policy object and **right-click** it, then select **Edit**.
3. This will bring up the **Group Policy Management Editor**.
4. Expand **Windows Settings** and then **Observe IP Security Policies on Active Directory**.
5. Create a new **IPSec Policy** by **right-clicking** and selecting **Create IP Security Policy.**

6. Name the policy something appropriate.
7. Leave the default response for secure communication blank, unless you're dealing with external client authentication. Click **Next**.
8. From **IPSec Properties**, you can select **Edit** and choose from one of three options:
   a. **Kerberos –** the most secure method that uses a complicated security algorithm to authenticate network paths.
   b. **Certificates –** a method of using certificate authorities to validate network paths.
   c. **Prehared Keys –** the ability to house a preshared key to decrypt and encrypt data.
9. To add more filters, click the **Add** button, and then click **Next** when the wizard pops up.
10. You can either specify the rule for a specific tunnel in the IPSec policy or, if you do not wish to use an IP tunnel, select "This rule does not specify a tunnel."
11. Click **Next.**
12. Select **All Network Connections**, **LAN**, or **Remote Access,** depending on what type of filter you'd like to setup and click **Next.**
13. On the next screen, shown below, you can filter traffic on either **ICMP** or **All IP Traffic.** Select the appropriate radio button and click **Edit**.

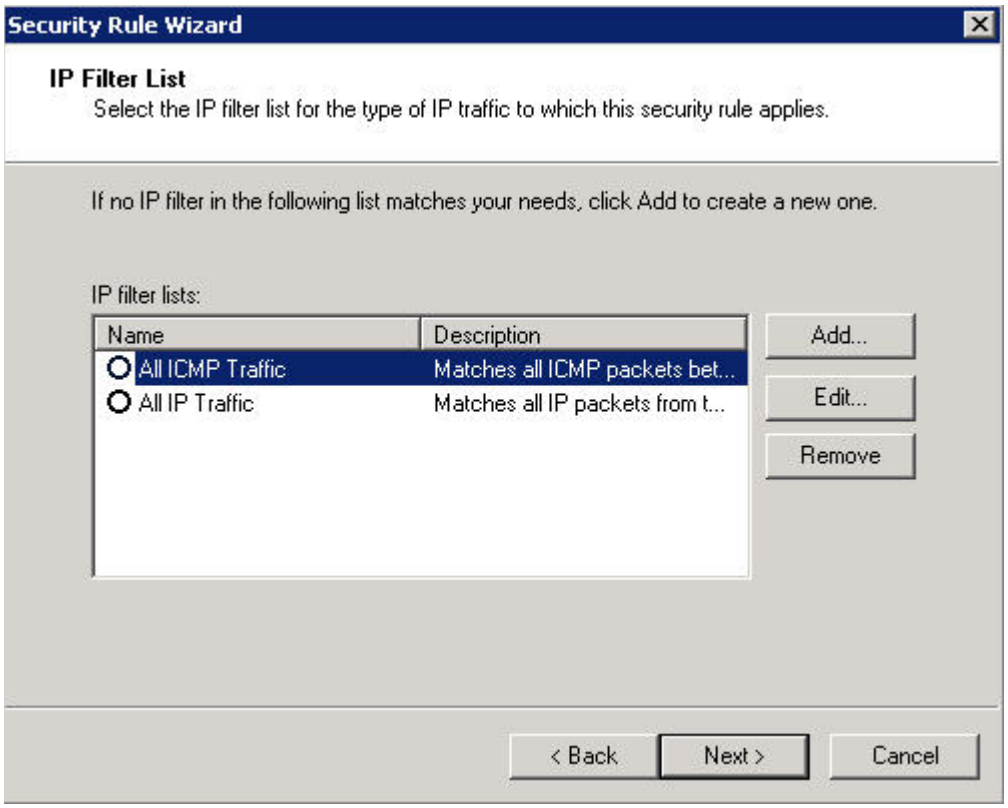

Figure 18: Creating an IPSec Filter

14. Name the filter something, such as "**RDP Traffic**".
15. Click **Edit**.

16. On the addresses page, you can specify addresses you'd like to restrict. The choices are My IP address, a specified address, DNS, WINS, DHCP, or Default Gateway. Choose appropriately.
17. On the protocol page, you can specify the type of traffic you'd like to filter. For example, you could choose RDP.
18. Click **OK.**
19. On the filter page, you can choose to **Permit**, **Request Security**, or **Require Security**. For example, if you wanted to restrict RDP, you could choose "Require Security."
20. Click **Next**.
21. At this point, you can choose Kreberos, Certificates, or Preshared Keys. Kerberos is recommended, as it's extremely secure.
22. Click **Next**, and then click **Finish**.

Authentication Headers

Authentication headers are simple 32 bit protocols that define authentication and integrity in an IPSec filter. The specific data determining what these headers do depends entirely on the location of the authentication header. For the Microsoft exam, you should know the following fields:

- 0 – 7: Sends the field to search for the next header, which contains that type of payload it will distribute.
- 8 – 15: The length of the payload that will be sent.
- 16 – 31: The payload itself, which will process the data in the Authentication header.

You can setup authentication headers from within the Group Policy Managed Editors on the IPSec policy. You'll find them in the security section of the IPSec policy.

Encapsulating Security Payload

Another optional protocol available with IPSec in the policy editor is the Encapsulating Security Payload method. It's another method to try and keep the contents of your data secure. However, the big difference between Authentication headers and Payload Encapsulation is that just the payload is encapsulated with ESP, but AH contains packet header authentication, as well as payload. Administrators typically implement ESP when the data is critically important to security, but the origination and destination IP is not particularly of concern.

Domain 5: Configuring Network Access

The Windows Server architecture has been designed to allow clients from all over the globe to connect to a Windows Server 2008 server running wide area network and remote access features with ease. When Microsoft created these policies, the philosophy behind them was to create a centralized server that provided every feature that a client could possibly want in terms of remote access, all from a single platform. With Windows Server 2008, a single server is capable of supporting:

1. Routing and Remote Access
2. Network Access Protection
3. Network Authentication
4. Wireless Clients
5. Application-level firewalls

In this section of the Exam Manual, we're going to explore all parts of network access. We'll begin by reviewing how to configure your server as a network access server role. To configure your server to support network policy and access services:

1. Launch the Server Manager.
2. Select **Roles**, and then click **Add Roles.**
3. Choose Network Policy and Access Services.
4. Click **Next**, then **Next** again at the information screen.
5. For the sake of simplicity, select every service at the Role Services screen and then click **Next**.
6. At the "Choose Certificate Authority to use with Health Registration Authority" page, choose to install a local certificate authority. Alternatively, you could also use an existing remote CA or select it later. But for the sake of this exercise, installing one remotely will be just fine.
7. Click **Next**.
8. At the **Choose Authentication Requirements for the Health Registration Authority** page, choose "Yes, require requestors to be authenticated as members of the domain." This is because you probably don't want your server to just randomly issue certificates to just anyone.
9. Click **Next**.
10. The next screen will start the installation process for Active Directory Certificate Services. Click **Next.**
11. At the next **eight** screens, click **Next**. At the last screen, you will need to click **Install**.

Configuring Remote Access

The term "remote access" is slightly ambiguous in that the Microsoft definition of Remote Access includes both how to access your server via remote connections, and also how to translate addresses from wide area addresses to local area network addresses.

To start, we will begin by discussing dial-up access for accounts using dial-up modems. You will note that the initial configuration steps for any given remote access connection is essentially the same, up to a point. We'll cover the whole process in the Dial-Up section, below. Afterward, we'll cover the configuration routines unique to subsequent remote access connections.

Dial-Up

To configure a dial-up connection, complete the following steps:

1. Navigate to Start → Administrative Tools → Routing and Remote Access.
2. Right-click on your server and select Configure and Enable Remote Access.

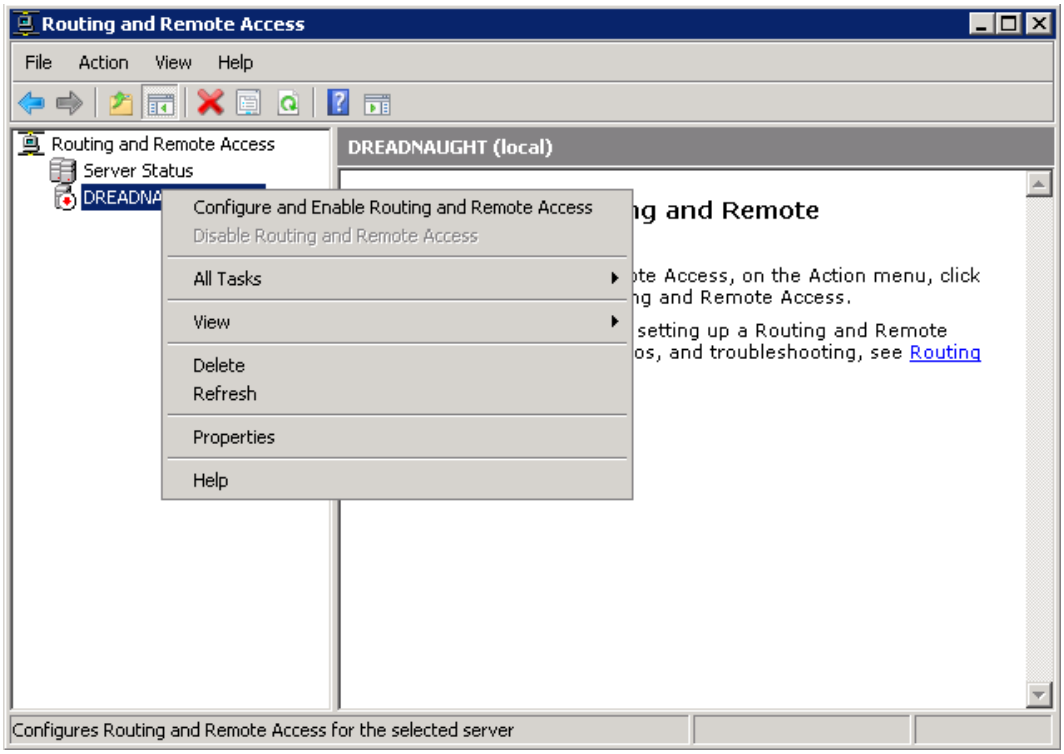

Figure 19: Enabling Routing and Remote Access

3. This will bring up the Routing and Remote Access Server Setup Wizard.
4. Select Remote Access (Dial up or VPN).
5. Click **Next**.
6. Select the **Dial-Up** checkbox; click **Next**.
7. At the next screen, you can either choose a range of IPs; specifically or automatically assign them.
8. Click **Next**.
9. You can choose to either enter a RADIUS server (discussed later) or allow your server to accept direct connections.
10. Click **Next**.
11. Click **Finish**.

RADIUS

RADIUS is a protocol used to communicate between Network Access Servers and Network Policy Servers. This is done because a Network Access Server acts as a liaison between a user and a Network Policy Server.

Conceptually, it's a lot like this:

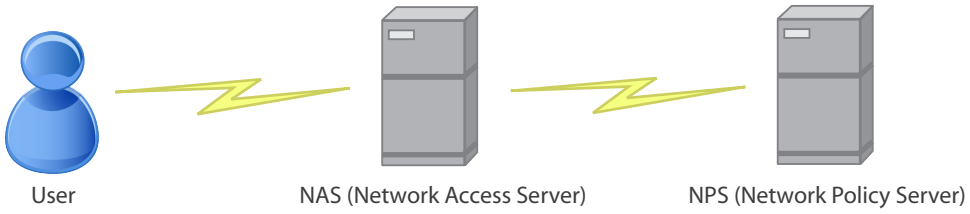

Figure 20: How RADIUS Works

A user connects to an NAS, which connects to an NPS. And the NPS translates requests from the NAS (which are called "Authentication Requests)" and then responds based on what the NPS says back to it. Here's a step by step scenario:

1. A user decides to authenticate from a Dial-up/External source.
2. The user dials into the NAS.
3. The NAS uses RADIUS to talk to the NPS.
4. The NPS authenticates the user, then sends data back to the NAS
5. The NAS provides network server.

The key points here are that the user uses a protocol to connect to the NAS (PPP, for example), the NAS then talks to the NPS and authenticates; the authentication then defines the user behavior.

Remote Access Policy

With a remote access policy, you can choose to connect via a dial up connection through a secure protocol. What this means is that with Remote Access, you can choose to do the same actions with dial-up or VPN. However, because there is a more expansive VPN section in another area of the remote access server, we highly recommend that you configure it in that area.

Network Address Translation (NAT)

Network access translation is the process of converting public IP addresses to private IP address and vice versa. For example, a global IP address like 63.41.16.68 could easily be converted to a more common private convention, like 192.168.0.2. The reason this is done is two-fold: first, it allows more IP addresses, and second, it provides layers of security. The reason we would want to set this up in this area of our server is that we might be in a situation where we need to create a public address to connect to the internet.

We'd normally do this if we were connected to a router. As you can see from the image below, in this section we have two radio buttons, one of which is grayed out in our scenario.

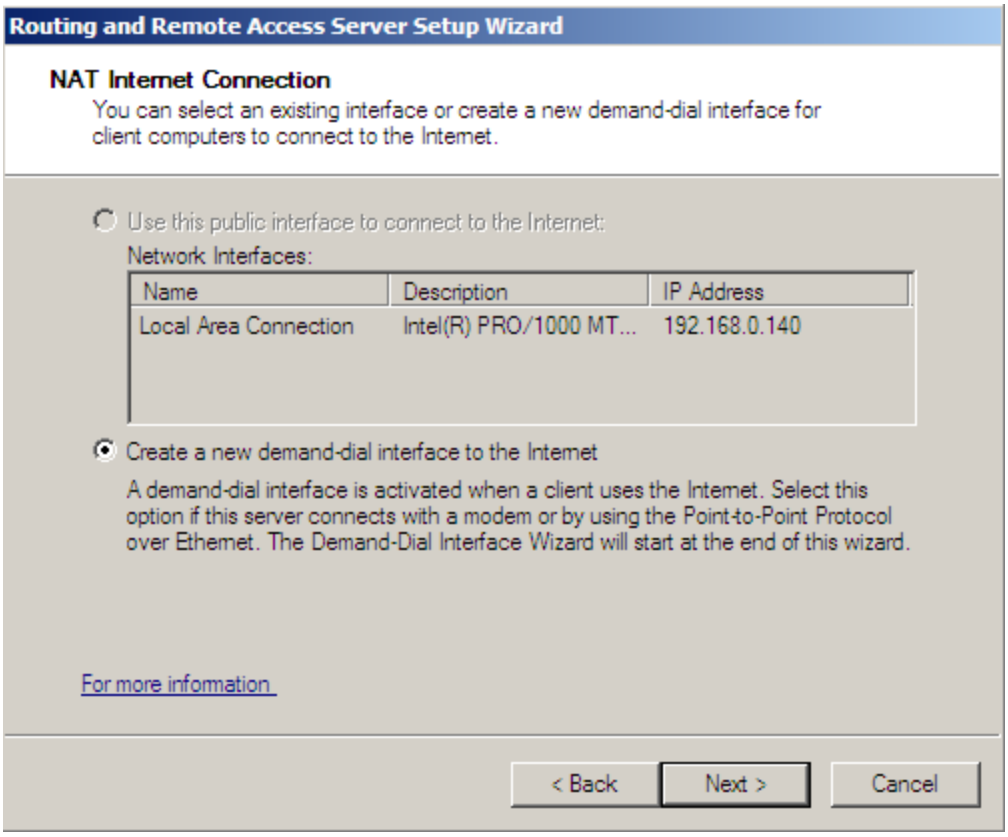

Figure 21: Configuring a Demand-Dial Interface

The grayed out option would be available to us if we had assigned a public IP address to our server. In this case, the wizard would assume that we were going to be using NAT to convert from a given public IP address to an internal IP address.

The second radio button allows us to create a demand-dial interface to the internet. As you can see from the text description, demand-dial (as in, "on demand") interfaces work when the client connects to the internet. You should use this if the server is using a modem to access the internet. In this case, the demand-dial wizard will open up.

Note: Because modems and slow analog connections have mostly become a thing of the past, we're going to skip this section. However, the setup is fairly straight- forward. All you have to do is click next and choose the options for your setup during the initial wizard. The options will be very straight- forward - , just simple questions like what you see in the figure below.

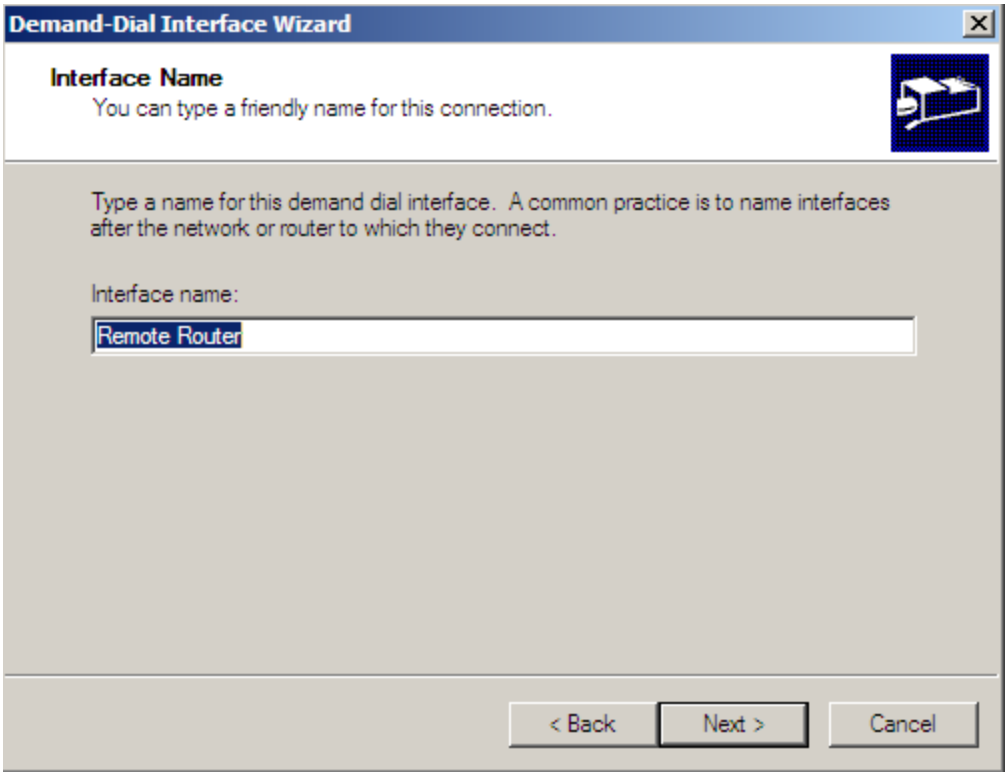

Figure 22: Naming the Demand-Dial Interface

Internet Connection Sharing (ICS)

Internet connection sharing is the process of allowing multiple servers to access one shared internet connection through multiple network interfaces. The theory is that one computer holds the internet connection on one network card, and then passes off the connection to other computers by handing out DHCP addresses and using NAT. Unlike the other types of connections we have discussed, this type is done through the control panel. To access ICS settings, do the following:

1. Open **Control Panel.**
2. If **Network and Internet** is there, click it, otherwise click **Network and Sharing Center** and then click **Manage Network Connections.**
3. **Right-click** your connection and select **Properties.**
4. Click the **Sharing Tab**.

VPN

Virtual Private Networks are the most common reason that this area of Windows Server is enabled. Through Windows Virtual Private Networks, you can secure your server so that the resources can only be accessed through secured connections over wide area networks. To begin this setup process, start the Remote Access configuration process, discussed earlier, and choose VPN and NAT, rather than Dial-Up, at the main selection screen.

Note: You will need at least two Network Interface Cards to complete this section.

1. At the main screen, make sure you see both of your network cards and click **Next**.
2. In the IP address assignment area, choose to either automatically assign addresses for your VPN, or choose from a specific range.
3. Normally, users will choose to have them automatically assigned for the sake of flexibility. However, the option is there if you would like to manually pick IP addresses to be reserved for your VPN connection.

For the next part of our configuration, we'll need to move to the VPN and NAT section of the **Routing and Remote Access** wizard.

4. To access this, you will need to choose **VPN and NAT**, then to have your addresses automatically assigned.
5. At the next screen, you'll be presented with the image you see below:

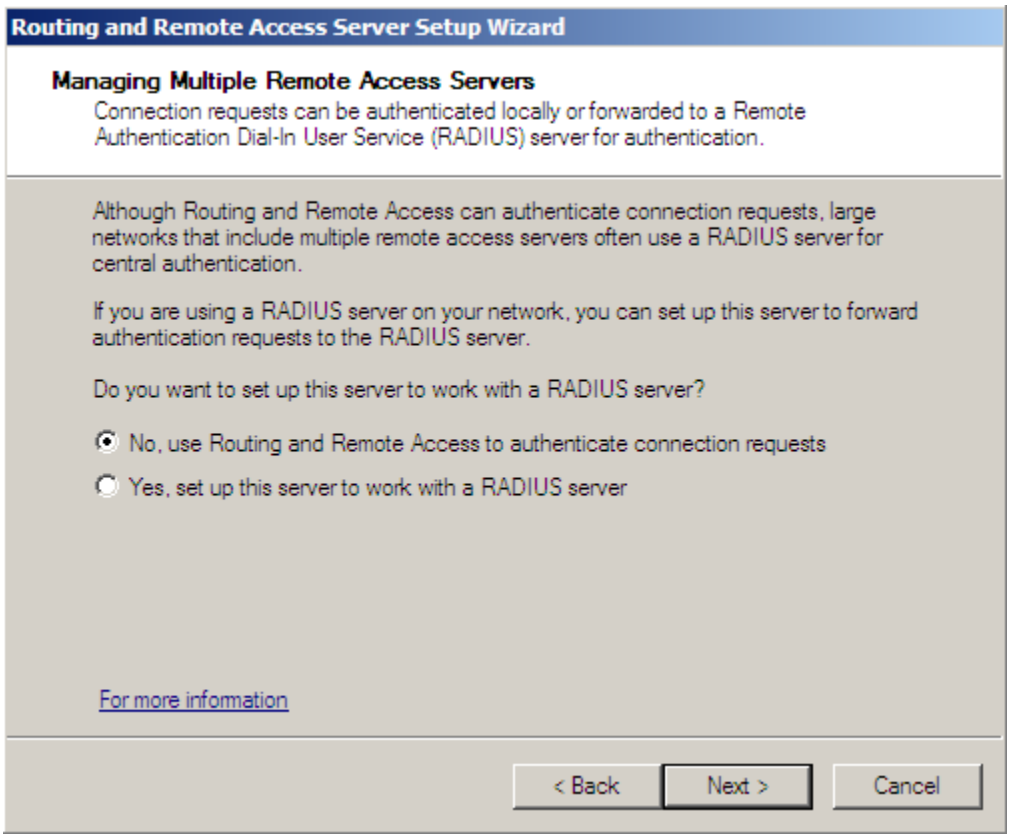

Figure 23: Configuring VPN Access for RADIUS

6. Choose YES to configure, and then click **Next**.
7. At the next screen, you will need to enter your **Primary and Alternate RADIUS Servers** for remote access, and then click **Next**.
8. The system will then authenticate and complete setup automatically.

Routing and Remote Access Services (RRAS)

The Routing and Remote Access portions of Windows Server 2008 expand to the extent that they include Network Policy and Access filters. This is accomplished through the Network Policy Server portion of Windows Server 2008. You can access this by going to **Start → Administrative Tools → Network Policy Server**. Additionally, this section will cover further refinement of the Routing and Remote Access portions of Windows Server 2008.

Inbound and Outbound Filters

You can setup inbound and outbound filters through the NAT portion of your Routing and Remote Access server by navigating the Routing and Remote Access (R&RS) snap-in and expanding the IP routing section. Inbound and Outbound filters monitor traffic that goes in and out of your network. For example, if someone has traffic going outbound, the outbound filters would apply. And vice versa; inbound filters apply to inbound traffic.

Note: This does require you to have setup NAT already.

If you right-click on the NAT/Basic Firewall section, you'll be able to expand its properties. As you can see in the figure below, there will be an inbound and outbound filter setting. This will allow you to refine traffic based on your own criteria, including which addresses or protocols are acceptable in your environment.

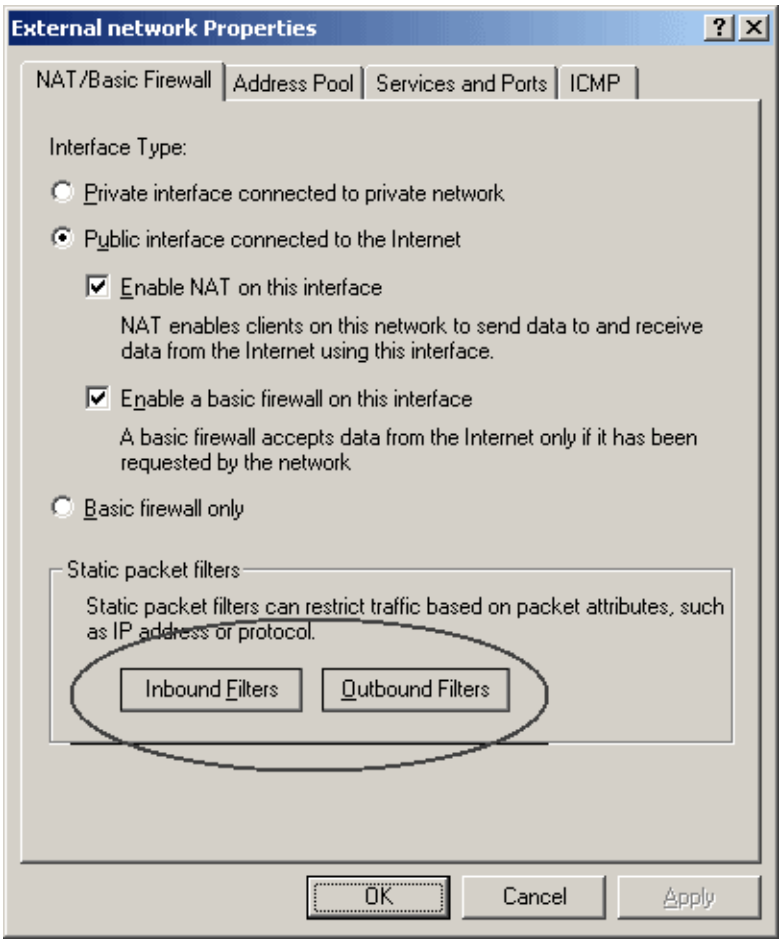

Figure 24: Creating Inbound and Outbound Filters

Remote Access Protocols

Remote Access Protocols allow us to further refine how are network is accessed (and when it is accessed) by allowing security methods that will authenticate how clients connect. With this exam, we are specifically concerned about is the encryption methods that are available to administrators when connecting across remote access mechanisms. Some of these encryptions include:

PAP

Password Authentication Protocol (PAP) is a weak authentication mechanism that takes use of an unencrypted channel to pass a password back and forth. It is widely considered highly insecure, but it is supported by almost every single remote server type.

CHAP

Challenge-Handshake Authentication Protocol (CHAP) is an encrypted protocol which uses a plaintext password that is known by both parties. For the exam, you just need to know that it's highly associated with Microsoft's implementation of CHAP – MS-CHAP.

MS-CHAPv2

MS-CHAPv2 is a version of CHAP implemented by Microsoft. It uses the CHAP algorithm to connect between the two connections, but it does not require the plaintext password to be known like CHAP. Additionally, it provides a peer challenging mechanism that's built-in to the protocol.

PPP

Point to Point protocol (PPP) is a protocol that exists on layer 2 of the OSI model and is used to connect between two points on any given network. It is currently the most common connection protocol used in the world and provides good to excellent encryption. Through PPP, a connection can connect over virtually any network connection type (Dial-Up, Cable, DSL, any type of ISP) and connect to another node through synchronous or asynchronous connection mechanisms. Typically, PPP is used for virtual private networks.

PPTP

Point to Point Tunneling Protocol (PPTP) is another VPN encryption mechanism that provides PPP connection, as well as encapsulation of the PPP packets through a dedicated tunnel. PPTP is more secure than PPP, because it encrypts the connection and also conceals it through an additional tunneling layer.

L2TP

Layer 2 Tunnel Protocol (L2TP) takes advantage of a tunneling layer like PPTP, but does not provide any encryption. It's basically like a second layer implementation of the Data Link Layer, which can be encrypted using other authentication methods, like IPSec or PPP.

Configure Network Access Protection (NAP)

Network Access Protection allows you to use a Network Policy Server to secure access authentication to your clients, no matter what their location is. Through NAP, you can access a local network by external means and connect to it with proper access and rights. A Network Access Protection server is designed to be the front-end authentication mechanism that allows users to authenticate to the rest of your network. NAP supports many connection mechanisms, but in order to use any of them, you must ensure that:

- Your Windows Server 2008 server is a domain controller
- It is running DHCP
- It is running DNS

This will allow you to use one of the many mechanisms that NAP uses to allow authentication.

Network Policy Server

A network policy server connects to the back-end of a Network Access Protection server and serves as the portion of our network access model that determines the rules and procedures associated with authenticated accounts. When accounts connect, they connect to a Network Access Server, and then they authenticate through a Network Policy Server.

Additionally, Network Policy servers can provide:

1. VPN Services
2. Dial-up access
3. 802.11 protected access
4. Routing & Remote Access
5. Active Directory Authentication
6. Network Access Policy Services

DHCP Enforcement

DHCP enforcement of a Network Policy is designed to support the implementation of network protection when a client receives a DHCP lease. This is particularly useful if you want to restrict behavior of clients that will authenticate via DHCP; more accurately put, deciding where certain clients should be registered on the network. However, it will not work on clients that have static IP addresses.

To enforce NAP DHCP, you must do the following:

1. Configure an NPS policy with the NAP wizard on your Network Policy Server.
2. Enable the policy.
3. Ensure DHCP is operating properly.
4. Enable the NAP with the DHCP snap-in.

VPN enforcement

VPN Enforcement forces computers authenticating to a VPN to use network policies to control the behavior of clients externally authenticated through a WAN connection. In order to use VPN enforcement you must, obviously, have an active VPN connection that has already been setup somewhere in your environment, as we covered earlier, in the VPN section.

You must enable the VPN connection to use NPS. If you select the **Allow full network access for a limited time** option, this will allow clients to connect to the VPN and then be automatically disconnected after the time has expired.

IPSec Enforcement

IPSec allows you to define the behavior of your NAP policy based on TCP/IP and IPSec compatible clients. With IPSec, any client that is compatible with NPS (XP, Vista, 7, Windows Server 2008) will authenticated based on IPSec settings defined in the NPS.

To deploy NAP with IPSec and a Healthy Registration Authority responsible for obtaining certificates for the NAP in the NPS-NAP model, you must do the following:

1. Configure an NPS policy using the NPS console.
2. Enable NAP IPSec enforcement.
3. Install HRA on the local computer.
4. Install **Active Directory Certificate Services** and **Certificate Templates.**
5. Configure the **Windows Security Health Vendor,** or you can install system health agents, which are agents installed by default in Windows Server 2008 that can monitor various aspects of the Windows Security Center (Firewall/Antivirus/Updates and Security Updates).
6. Install NPS on the client computer.

802.1x Enforcement

802.1X is an implementation method that takes advantage of 802.1X compatible hardware (switches, for example) and that is capable of authenticating based on 802.1X encryption standards, which are a series of standards meant to pair with 802.11 wireless authentication. They provide an authentication mechanism for 802.11 using Extensible Authentication Protocol (EAP). The end result is that users have to identify themselves. And with the 802.1X enforcement method, clients are forced to either authenticate with this protocol or be placed upon a remedial network with fewer privileges.

802.1X Wired and Wireless Requirements

The installation requirements for 802.1X (in either a wired or wireless network) are very similar to the policy requirements for other situations. In each case, you will need to configure an NPS on your server, configure group policy to deploy it, and use 802.1X as the authentication method for the network. Lastly, you will need to setup health validators, System health validators allow specific requirements to be placed on the clients on your network. For example, you could declare that clients connecting to your network must have an AntiVirus product associated with the Windows Security Center.

To setup a health validator, you can do as follows:

1. Open the NPS console.
2. Expand **Network Access Protection**.
3. Choose **System Health Validators.**
4. Right-Click the **Windows Security Health Validator** and go to **Properties**.
5. Hit **Configure.**
6. There, for both VISTA and XP, you could set client authentication rules regarding the security center and push **OK**. Take a look at the screenshot below.

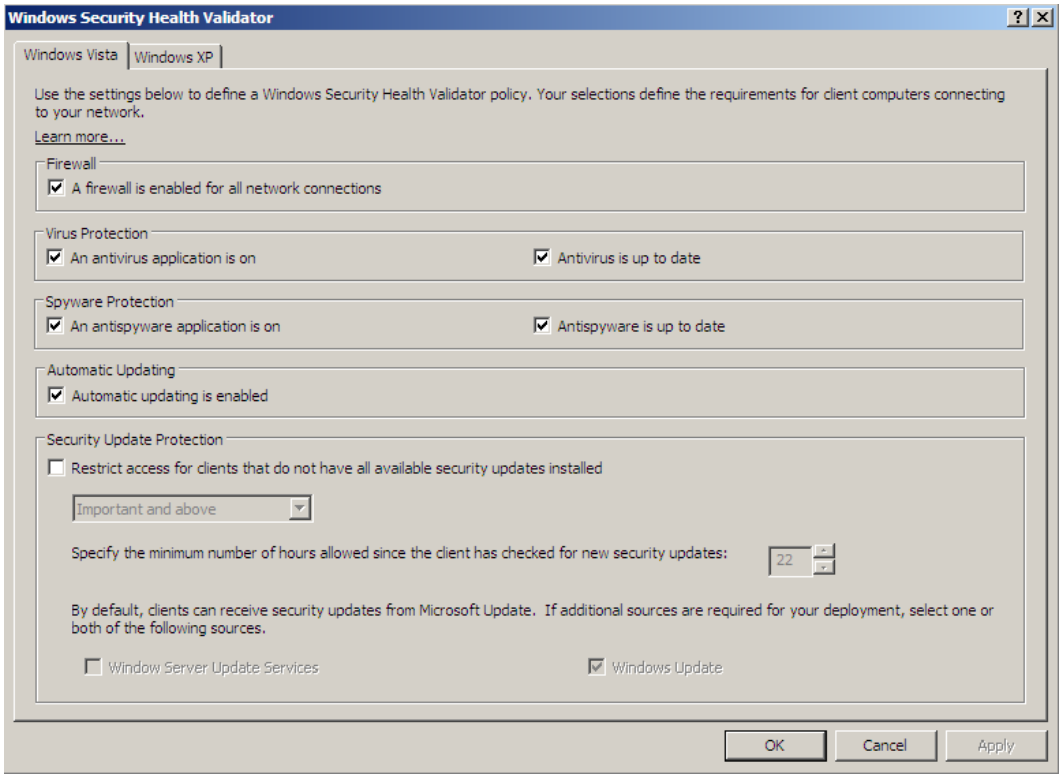

Figure 25: A health validator set to require all aspects of the windows security center.

7. Next, you would need to switch all of the compliances for your health vendor to compliant, based on your restrictions. As you can see below, I've set everything to compliant.

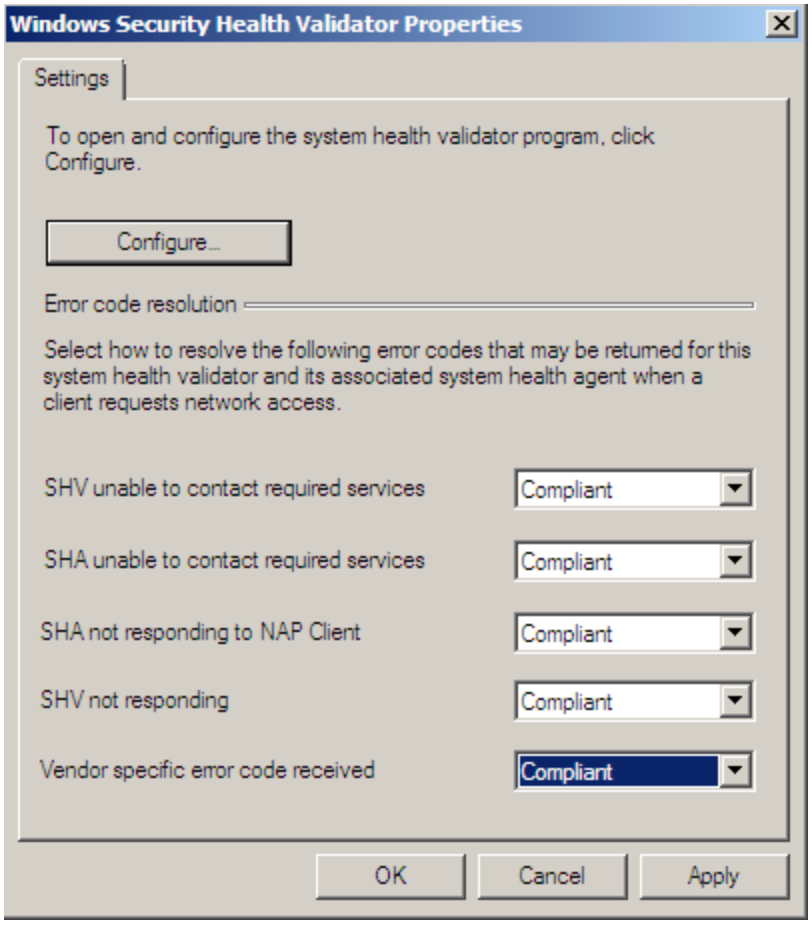

Figure 26: Configuring Health Validator Compliance

Configuring Network Authentication

Network Authentication in Windows Server 2008 allows you to ensure that your server's resources are protected from outside intervention by securing the connection between Windows Servers and Windows Clients with extra encryption.

When clients log on, the method which the server uses to connect is set, by default, to settings that are less secure that what Windows Server is capable of accomplishing. In this section, we will briefly cover how to set up these authentication protocols in such a way that you can completely customize your server's authentication security. This section covers:

- LAN authentication by using NTLMv2 and Kerberos
- WLAN authentication by using 802.1x
- RAS authentication by using MS-CHAP
- MS-CHAP v2
- EAP

To alter your network authentication settings, complete these steps:

1. Open **Group Policy Management.**
2. Select your Domain's GPO (or the GPO that you wish to enforce these authentication settings to). **Right-click** it and select **Edit.**
3. Expand **Computer Configuration** → **Windows Settings** → **Security** → **Windows Firewall with Advanced Security.**
4. Select **Firewall Properties** in the detail menu.

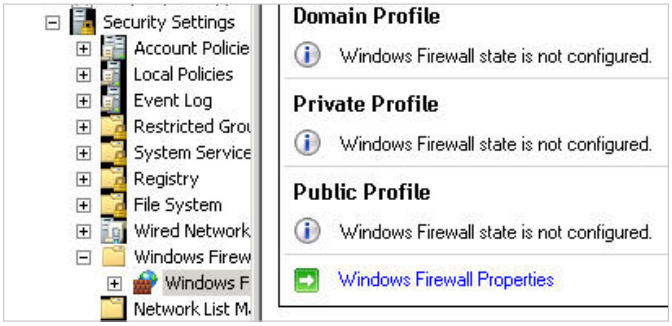

Figure 27: Windows Firewall Properties

5. Select the **IPSec** tab.
6. You should see the results below:

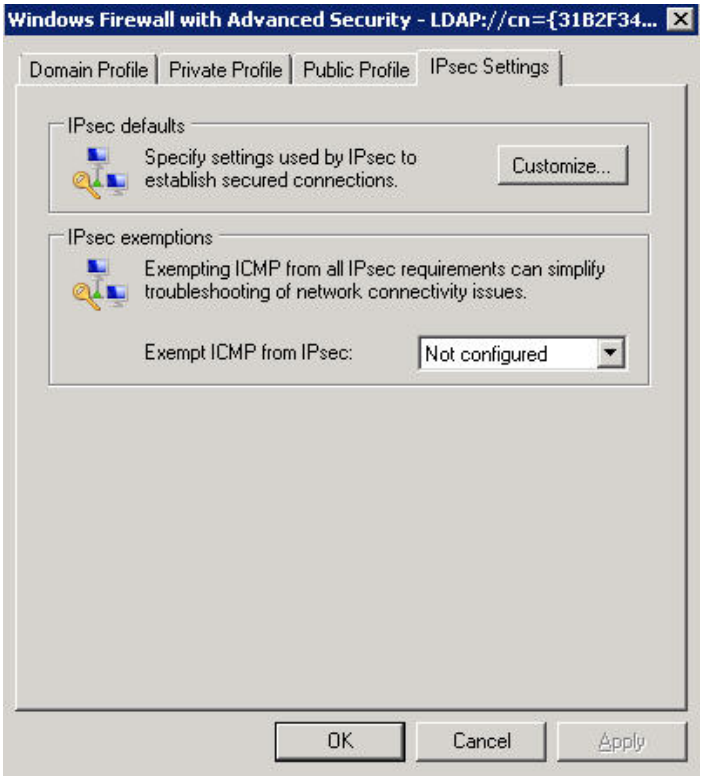

Figure 28: Windows Firewall with Advanced Security

7. Click the **Customize** button.

From this menu, you will be able to alter the various authentication settings that your server utilizes. You can discover the advantages of each by reading them in the help menu or looking them up online.

To configure all of the forms of authentication, you can choose the Advanced menu from the Key Exchange, Data Protection, and Authentication Methods. Each of these buttons will bring up a customize menu.

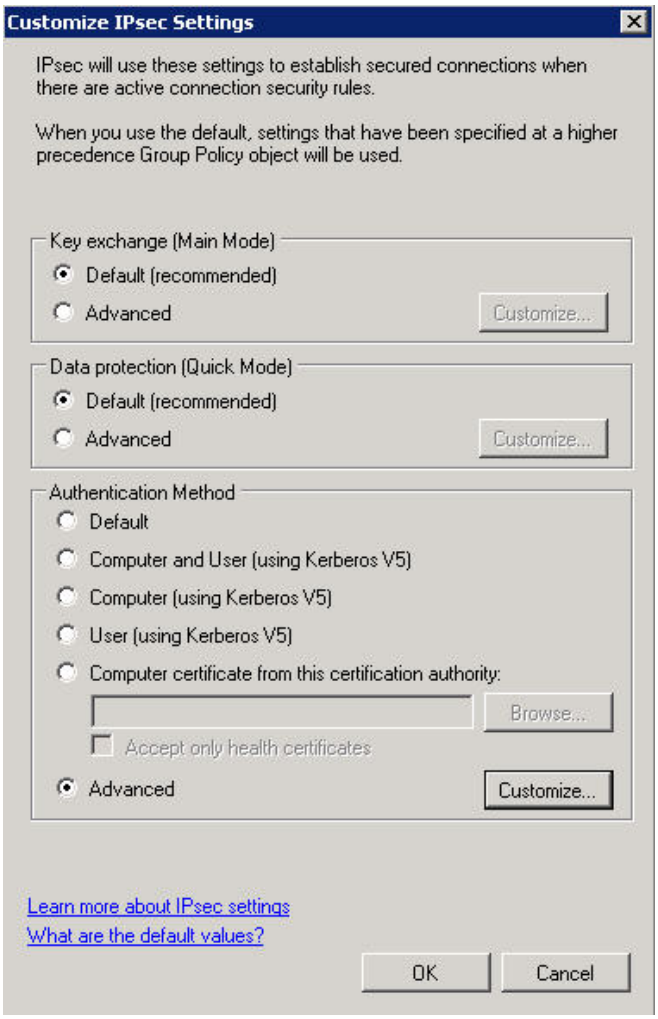

Figure 29: Customizing IPSec Settings

The customize menu will provide you with options to select the exact type of authentication you would like to use. For example, here is the Data Protection menu, which lets you select various forms of encryption:

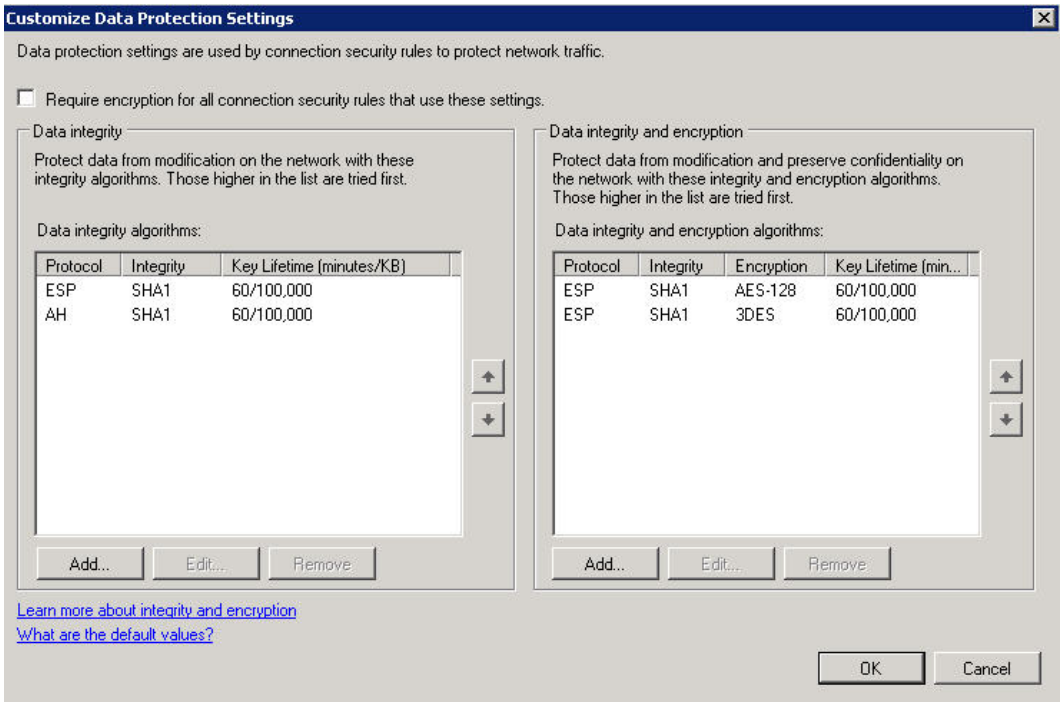

Figure 30: Choosing an Encryption Algorithm

And here is the advanced key section, which will let you pick the exact type of encryption algorithm you will use when sharing keys, then click **OK.**

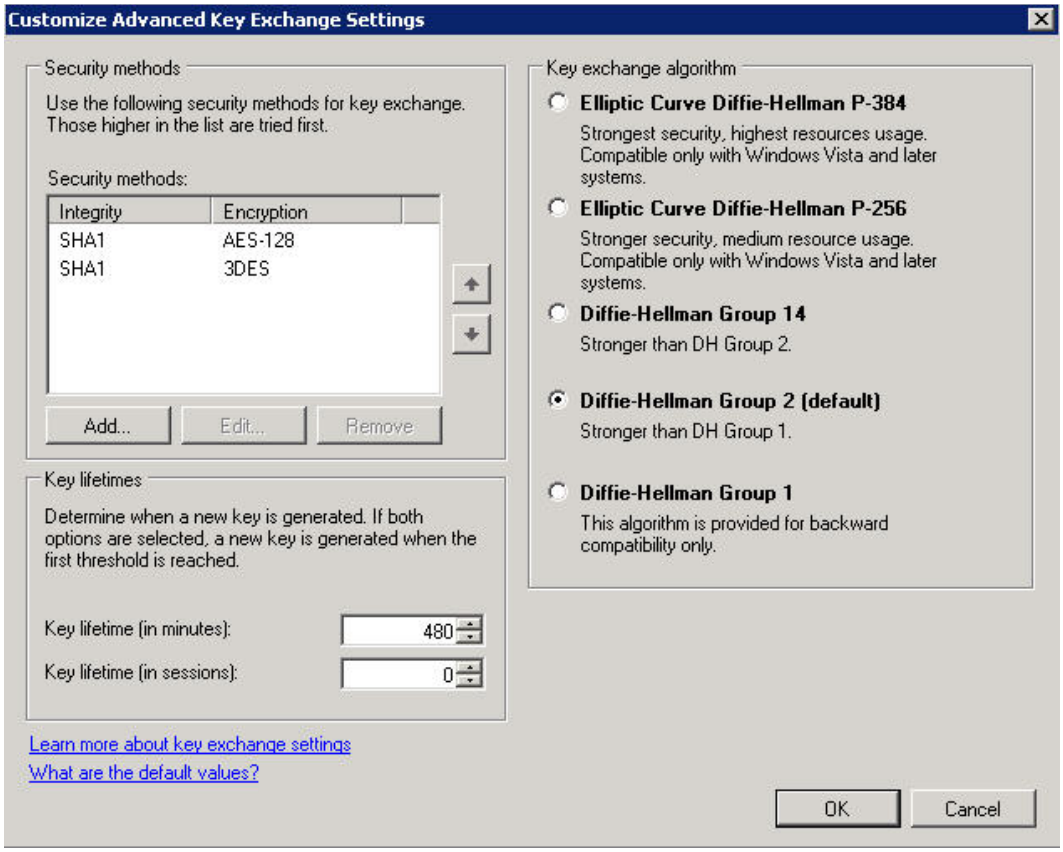

Figure 31: Advanced Key Exchange Settings

Configuring Wireless Access

The trick with wireless networking and Windows Server 2008 is that Windows Server itself is not responsible for the process of creating a routed Wireless Network with access points. Instead, Windows is capable of using authentication methods alongside a Wireless Network. In this section, we will purely define these terms, as well as how they apply to your exam. Keep in mind that the governing body behind Wireless Network Communication as it pertains to wireless networks as we know them is the IEEE (the Institute for Electronic and Electrical Engineers).

Service Set Identifier (SSID)

The Set Service Identifier is the name which your organization broadcasts along with its wireless network signal. For example, a Wireless Network dubbed "George's Network" could broadcast the SSID of **George's Network**, along with its signal. This way, users could look for George's network and then authenticate to it with their credentials.

Because of the open nature of SSIDs, it's recommended that you disable broadcasting of SSIDs on your network. If you do so, users will be required to manually enter in their network credentials in order to access your wireless access point.

Wired Equivalent Privacy (WEP)

WEP is the least secure of all wireless WEP is the most insecure of all wireless encryptions. It uses a Hexadecimal preshared key to encrypt the signal on both the client and server end. WEP comes in 40, 64, and 128 bit forms. However, no matter the bit rate, it is considered highly insecure because it is easily crackable. Still, many companies use this because some protection is better than no protection at all. In addition, almost all wireless routers support WEP.

Wi-Fi Protected Access (WPA and WPA2)

WPA and WPA2 are the second most and most powerful encryptions available on the market today. Through WPA, a preshared key is sent between the client and server in an advanced algorithm that takes advantage of an advanced encryption system. In the case of WPA, WPA uses TKIP (Temporal Key Integrity Protocol) encryption. And in the case of WPA2, WPA2 uses government grade AES (Advanced Encryption Standard) or both AES and TKIP. These are very advanced encryption algorithms that are exceptionally difficult to break.

In addition, WPA2 supports two forms: Personal and Enterprise. WPA2 can take advantage of the powerful AES encryption, while WPA2 can use this as well as 802.1X authentication using RADIUS. This means that you get the strong encryption of AES, as well as the user account based authentication or 802.1X.

Ad Hoc vs. Infrastructure Mode

An Ad Hoc wireless network is just an access point that exists without a routing point to provide infrastructure. Ad hoc networks are useful for just the sole purpose of transferring data between two computers "over the air." You might use this if you had two wireless laptops and wanted to get data from one place to another, without using any additional hardware. However, there is a danger involved. Ad Hoc networks are usually utilized by hackers in order to gain access to your machine. Normally, malicious users will broadcast SSIDs of commonly named networks such as "Public Network" and easily authenticate clients, only to hope that they broadcast or attempt to broadcast personal information on them, such as their email or bank account numbers. Because of this, ad hoc networks are generally not used at the infrastructure level.

An infrastructure level network is a network that is designed to support multiple clients over a larger area by joining together networks through the use of access points of network bridges. All access point in an infrastructure network share the same SSID, and connect in serial to cover a larger area.

Group Policy for Wireless

For the exam, you should know that Group Policy does support wireless networks and that you should place your group policy clients into a dedicated OU. This way, you can apply GPOs to them in an isolated manner.

Configuring Firewall Settings

Windows Server 2008 contains a very modular firewall that can filter both incoming and outgoing traffic based on particular rules. To navigate to firewall settings, open up Windows Firewall with Advanced Security by typing it into the Windows Server 2008 search field.

Incoming and Outgoing Traffic Filtering

Creating incoming or outgoing rule in Windows Server 2008 is a very simple process. First, select **Inbound or Outbound** in the Windows Server firewall properties. Then select **New Rule**. In the Wizard, you can refine your policy based on several fields, including port, protocol, and application. Make sure to practice setting up filters in your home lab.

Active Directory Account Integration

The Windows Firewall supports the ability to apply Firewall rules based on where a computer is located. Imagine you have a good deal of laptops that are frequently going out on- site. When they are locally joined to a domain, there is no reason to filter what traffic comes inbound or outbound. As long as they are within the trusted LAN, the network traffic should be fine. However, if they are out in the wild and not connected to their trusted network, they need to be more closely guarded. This is at the root of the Windows Firewall's three profile levels:

- Domain
- Private
- Public

A domain profile is used when joined and authenticated to a domain. A private profile is used when joined to a private network, and a public profile is used when connected directly to the internet via a WAN address.

The whole idea in a nutshell is this:

- You create a GPO that determines how clients firewalls should behave based on their Domain, Private or Public profile.
- You link the GPO where you want it, based on the OU, Domain, or Site.
- You place computers into the appropriate active directory container that they should go, and they receive the firewall settings that they should, as based on Active Directory.

Identify Ports and Protocols

You should be familiar with the following ports and protocols:

Note: Protocols are TCP unless otherwise noted.

Protocol Name	Port Number	Description
File Transfer Protocol	20	UDP protocol used to transmit Files
File Transfer Protocol	21	TCP version of FTP used to transmit files more quickly and accurately
SSH (Secure Shell)	22	Protocol used to establish command shells over distances securely
Telnet	23	Used to establish insecure shells over distances
SMTP (Send Mail Transfer Protocol)	25	Used to transport mail
whois	43	Used to lookup IP/name information
DNS (Domain Name Service)	53	Used to support transmission of IP/Name conversion information
DHCP (Dynamic Host Control Protocol)	68	Used to automatically obtain IP addresses
HTTP (HyperText Transfer Protocol)	80	Used to transmit data over the world wide web / Internet
POP3 (Post Office Protocol, version 3)	110	Used to receive email from an email server
SFTP (Secure File Transfer Protocol)	115	Security version of FTP
NTP (Network Time Protocol)	123	UDP protocol used to transmit network time
IMAP (Internet Message Access Protocol)	143	Protocol used to access email from a server, similar to POP3
SNMP (Simple Network Management Protocol)	161	UDP protocol used to monitor network attached devices
LDAP (Lightweight Directory Access Protocol)	389	Used to query active directory information via a network, even with Non-Windows based platforms.
SSL (Secure Socket Layer)	443	Security protocol used to exchange SSL certificates

Figure 32: TCP and UDP Ports

Microsoft Windows Firewall versus Windows Firewall with Advanced Security

The main differences between the basic Windows Firewall and the Windows Firewall with Advanced security are:

- Windows Firewall supports simple off and on functions, which the advanced security menu does not.
- The Windows Firewall with Advanced Security allows you to define protocols for inbound and outbound connections much more granularly. Second, the Windows Firewall with Advanced Security allows you to define protocols for inbound and outbound connections much more specifically and granularly than the standard Windows Firewall.

Configuring the Firewall through Group Policy

You can configure the Windows Firewall through group policy by opening the GPME (Group Policy Management Editor) and navigating to **Computer Configuration → Policies → Windows Settings → Windows Firewall with Advanced Security**. There, you can modify the policy just as you would with the normal Windows Firewall. Depending on where you link the policy, it will propagate to the remaining fields.

Isolation Policy

An isolation policy ensures that all computers connected to a Windows Server 2008 Domain Controller are utilizing IPSec in order to identify and manage the other computers on the network. The process for this is rather involved, so we won't be going into complete detail, but we will highlight the steps necessary to achieve this:

- **Plan for all computers to use IPSec** – usually this involves Windows workstations above Windows XP (Vista/7), but Windows XP can support this. However, it will fall back to plain text.
- **Create a GPO IPSec rule that allows for isolation** – deploy the rule via group policy.
- **Test the rule** – attempt to authenticate with a non-member server or workstation.

Create a GPO IPSec isolation Policy:

1. Open Group Policy Management.
2. Create a new GPO and name it "Isolation."
3. Edit the GPO by right-clicking it and selecting **Edit**.
4. Right-click your GPO and click **Properties**.
5. Check the **Disable User Configuration Setting** checkbox.
6. Click **Yes** when asked to confirm disable, then click **OK**.
7. Go to **Computer Configuration → Policies → Window Settings → Security Settings → Windows Firewall with Advanced Security → Windows Firewall with Advanced Security →** LDAP://cn={guid},cn=policies,cn=system,DC=yourdomain,DC=com
8. Right-click **Connection Security Rules** and choose **New Rule**.
9. Choose **Isolation** on the **Type** page.
10. Confirm **Request authentication for inbound and outbound connections** selected.

11. Choose **Computer and User** (Kerberos v5).
12. Choose **Private and Public.**
13. Request **inbound,** request **outbound**.

Domain 6: Monitoring and Managing a Network Infrastructure

So far, we have covered the process of setting up a network infrastructure and ensuring that the infrastructure is well-designed and can support our current number of users and any future employees we may acquire. Next, we come to one of the most important parts of any network design: **maintenance**. Or, more specifically, we come to the portion where we will address how to monitor the behavior of our network and determine if maintenance needs to be done. In this section, we're going to learn about Server updates, Group Policy designs, performance data, events, and network information.

Configuring Windows Server Update Services (WSUS)

Windows Server Update Services is a software update method utilized by Microsoft to automatically deploy updates from a server to its child servers and workstations. This ensures easy, centralized administration and management of any Microsoft update to every system on your enterprise network.

Properly implementing this feature requires a mix of group policy, targeting specific clients, testing the implementation, and preparing for when networks may disconnect from time to time. As a first step, we need to install WSUS.

To Install WSUS, do the following:

1. Confirm that your Server contains at least 1 GB of RAM per 500 clients.
2. Download WSUS with the latest services pack from TechNet. You will need to chose either the x86 or x64 version, depending on your server hardware.
3. Add the **Application Server** and **Web Server (IIS)** roles to your server. You can do this by doing the following:
4. Start Server Manager.
5. Select **Roles** and then **Add Roles**.
6. Choose **Application Server** and **Web Server (IIS)** and agree to any additional prerequisites.
7. Ensure that **IIS6 Compatibility** is checked when you install IIS.
8. Either **double-click** the download or use the **Server Manager** to install WSUS 3.0. To use the server manager, do the following:
9. Start Server Manager.
10. Click Add Roles.
11. Choose Windows Server Update Services.
12. Confirm the selections and click install.

Once WSUS has installed, you will need to configure it by doing the following:

1. Accept the license agreement.
2. Agree to install any additional or missing components.
3. Select an **Update Source** location, as you see in the following screen:

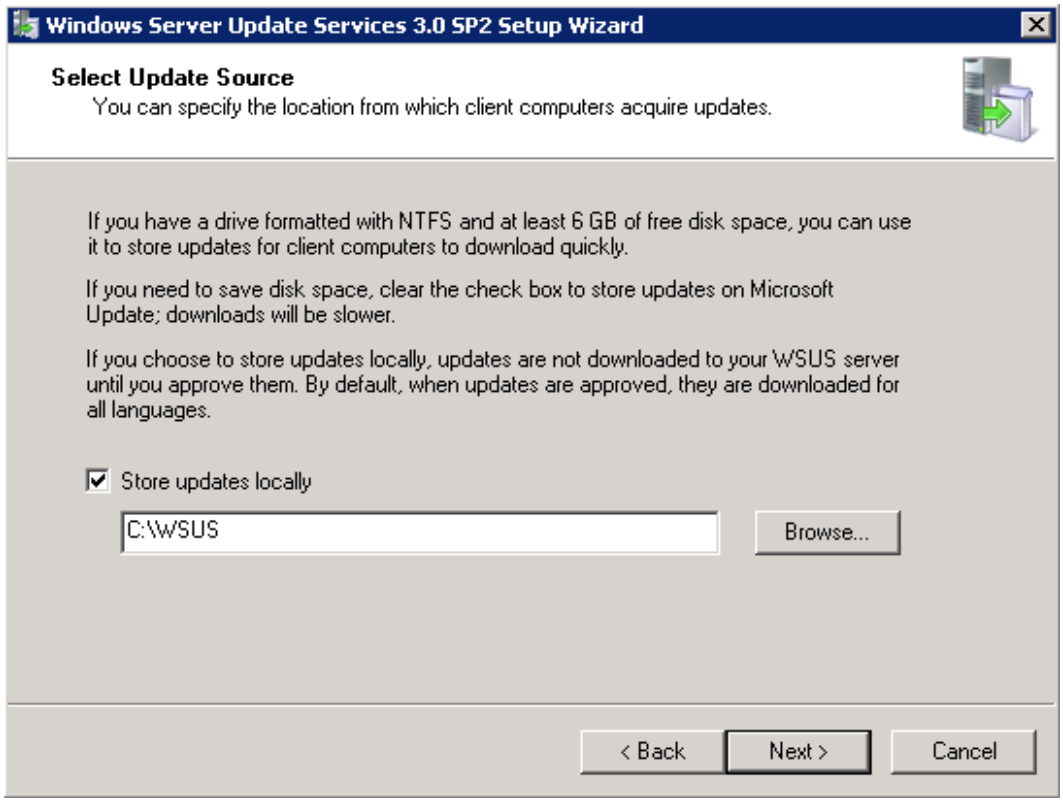

Figure 33: Choosing a WSUS Update Source

4. Choosing the default location is usually sufficient. If you like, you can specify a folder somewhere on your server or an NFS/SMB location.
5. Next, choose where to keep an internal database, as you see in the screen below. It's highly recommended that you pick the same directory that you stored the physical updates in. (**Note:** This database is not an SQL database. To select an SQL database, you will need to select either the existing database or another existing database and provide the **machinename\instancename**.)

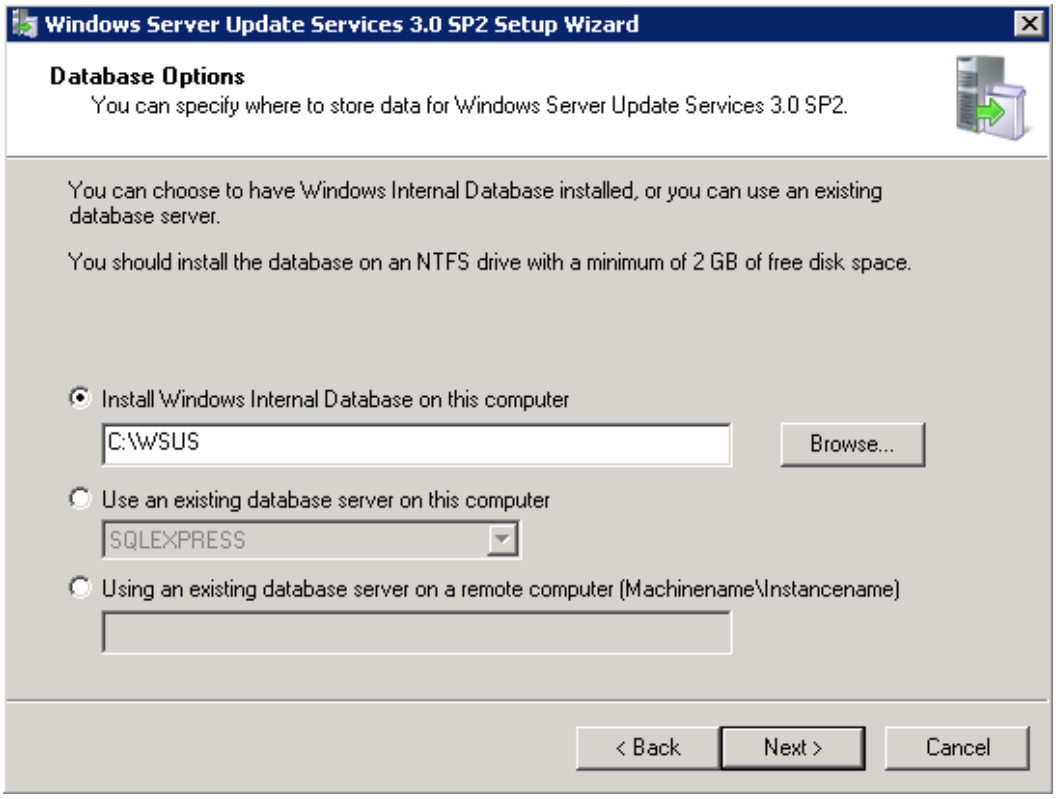

Figure 34: Choosing an Internal Database for WSUS

6. At the **Web Site Selection** screen, you will want to choose to either create a new website or choose from an existing website. As a best practice, you should create a new website by selecting the new web site radio button. This is a best practice because it exercises one of the fundamental aspects of good administration: separation. It also practices another great habit: dedication. It's always good to have a dedicated, separated server for a specific task.

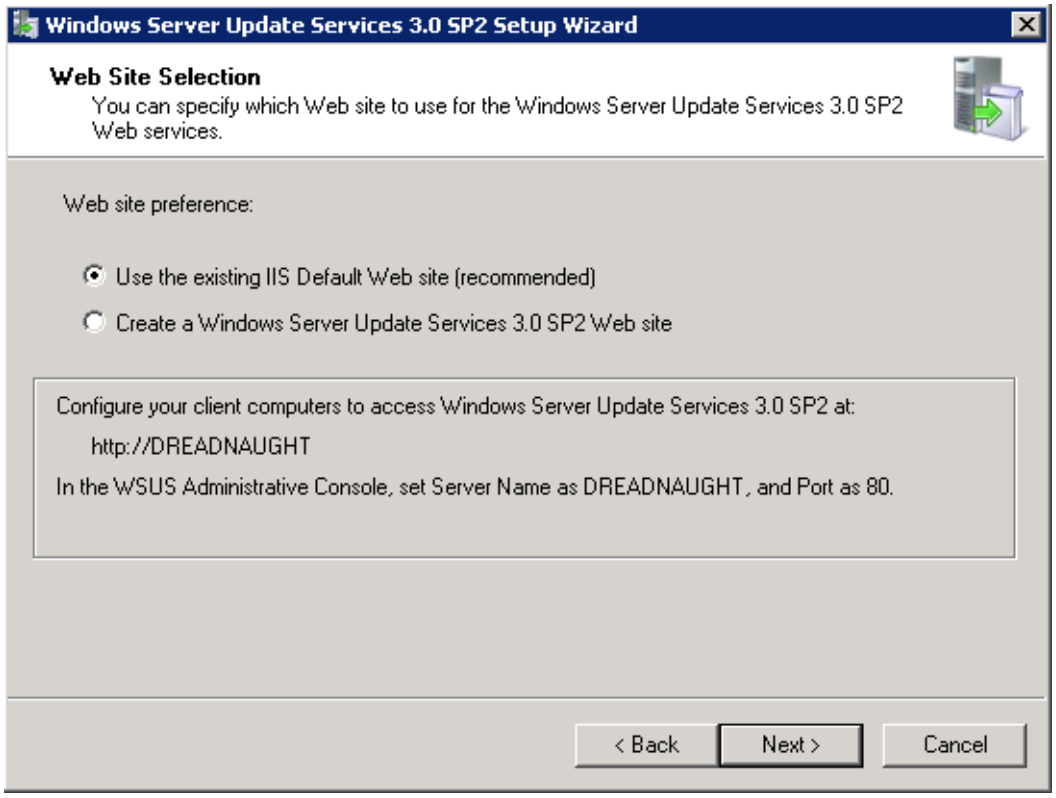

Figure 35: Choosing a Web Site for WSUS

7. Click **Next** at the following two screens and wait for the components to install.
8. Click **Finish**.

Now you will need to configure WSUS to apply server updates to your infrastructure. To do so, follow these instructions:

9. Click **Next** at the opening wizard.
10. The next screen will ask you to participate in Microsoft's improvement program, you can choose to participate or to not. Click **Next**.
11. At the next screen, shown below, you can choose to **Synchronize from Microsoft Update** or to Synchronize from another Windows Server Update Server.

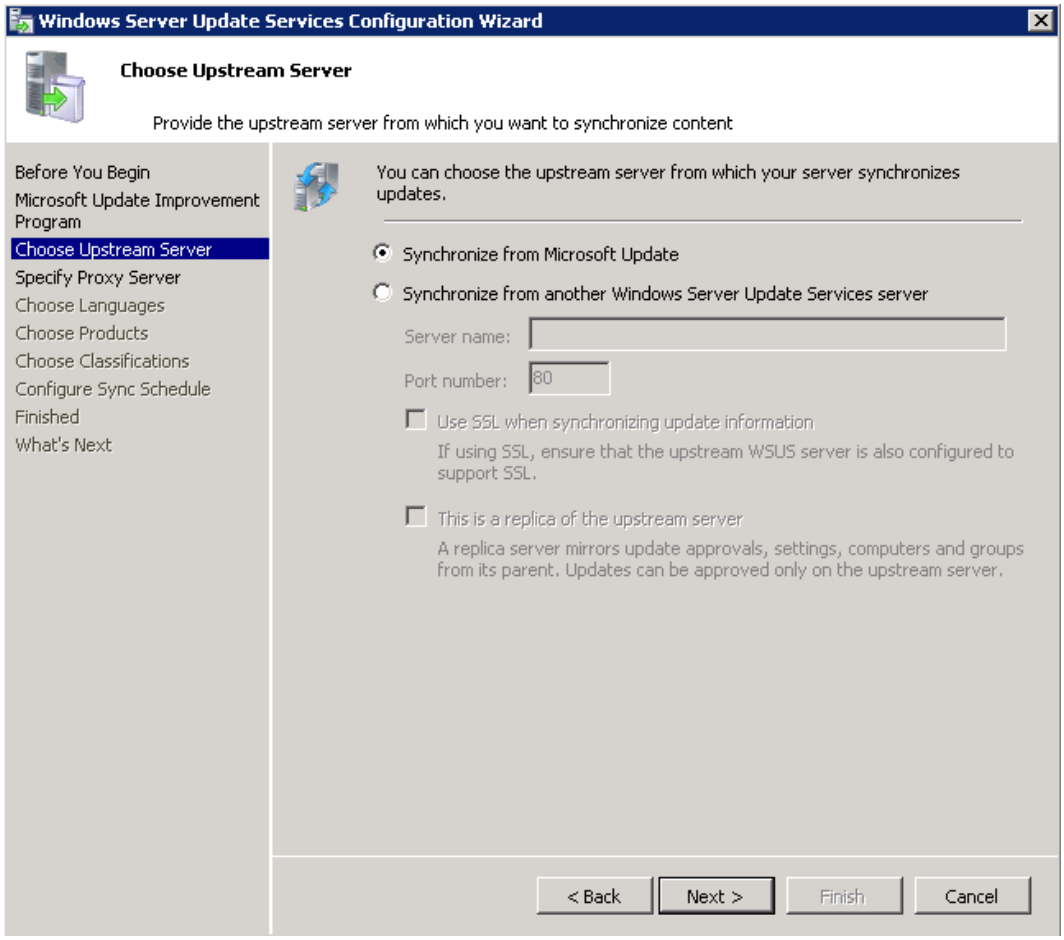

Figure 36: Choosing the Upstream WSUS Server

This portion of the WSUS service is designed to give you the ability to tier updates. You can think of it like this: imagine having one server that received updates from Microsoft Update. Then, you could have that server "downstream" updates to other servers in your organization, choosing which updates you would like to install to the rest of your infrastructure. For the purposes of this example, we will use Microsoft Update, thus creating the upstream server for our organization. On subsequent servers, you can fill in the server name and port at this step.

Take note of the choices provided under the server name and port number fields:

Using **Secure Sockets Layer (SSL)**, you can force client computers and downstream servers to authenticate the WSUS server before taking updates. Additionally, SSL will encrypt any metadata passed between client and server computers.

You may also mark the server as a **replica**, which mirrors updates, settings and groups from the original (parent) update server, providing high availability.

1. If you have a **proxy server**, you will need to enter it on the next screen. If not, just click **Next**.
2. At the next screen, you'll choose the types of updates available and the languages you will make your updates available in.
3. Click **Start Connecting**. The portion in the updates area may take some time.
4. Once the process completes, click **Next**.
5. In the language options menu, shown below, you can choose the languages you would like to receive updates in. If you're an organization with employees who natively speak another language, you will want to choose languages for these individuals here. Once you have made your selections, click next.

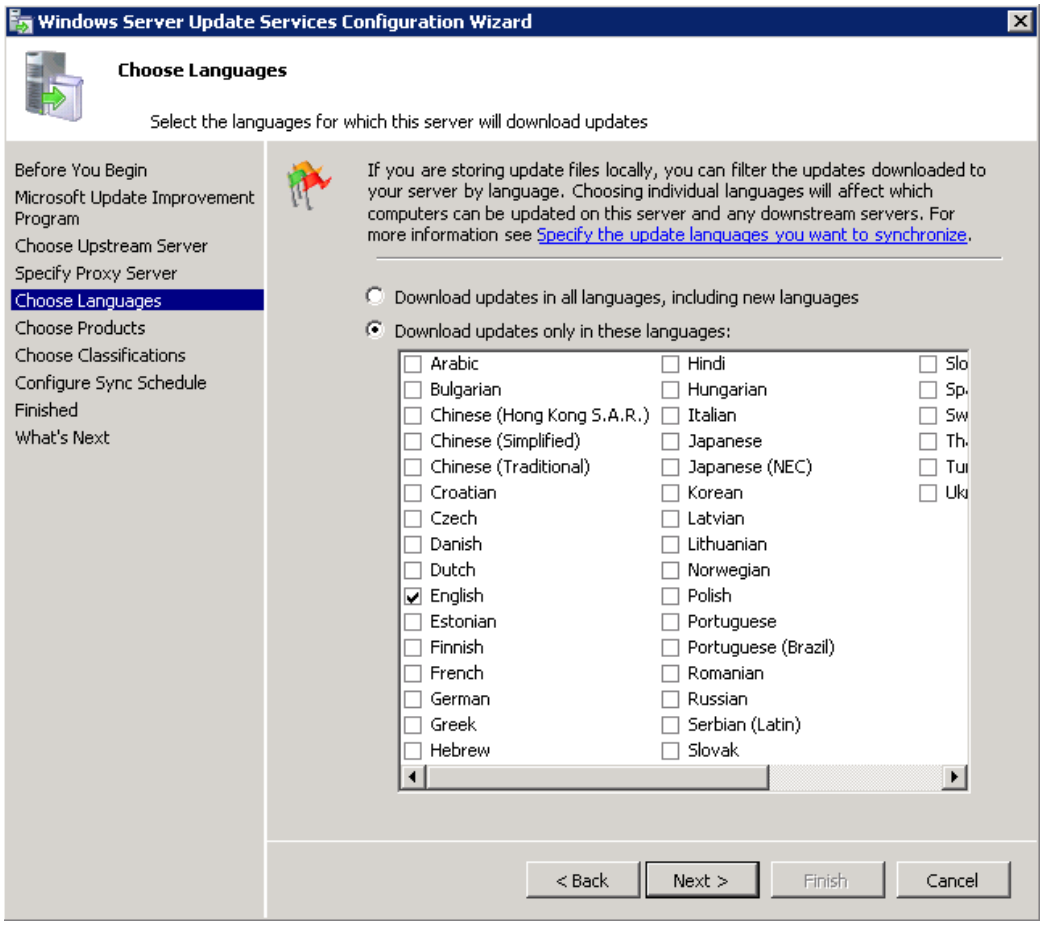

Figure 37: Choosing Update Languages

6. The next screen allows you to select the products you would like to receive updates for. This includes non-operating system products, like Office and SharePoint. According to Microsoft, WSUS can update everything in your organization easily. Make your selections and click **Next**.

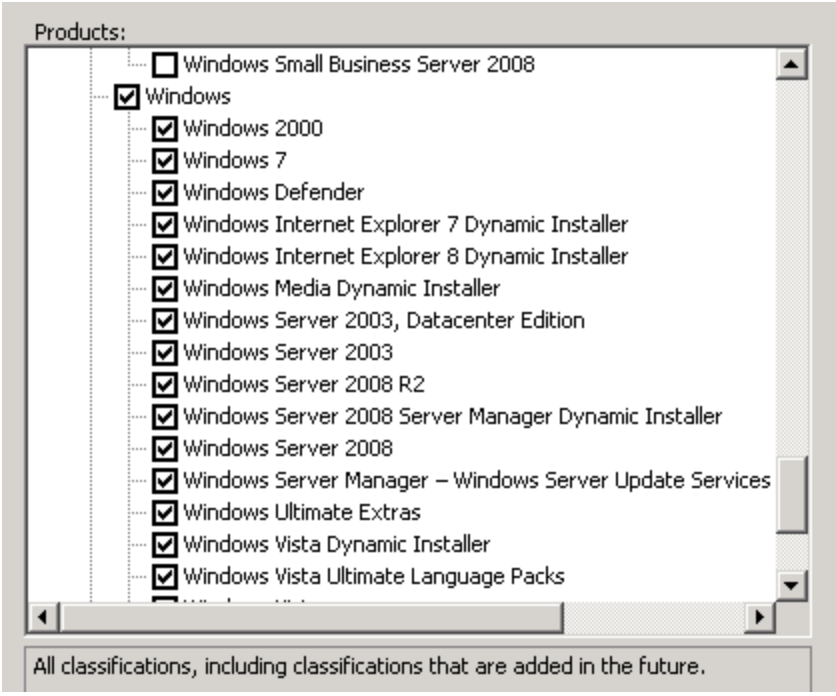

Figure 38: Choosing Updates for Specific Products

7. The next screen, shown below, allows you to choose classes of updates. Best practices dictate that you enable critical updates, definition updates, and security updates, at least. Make your selections and click **Next**.

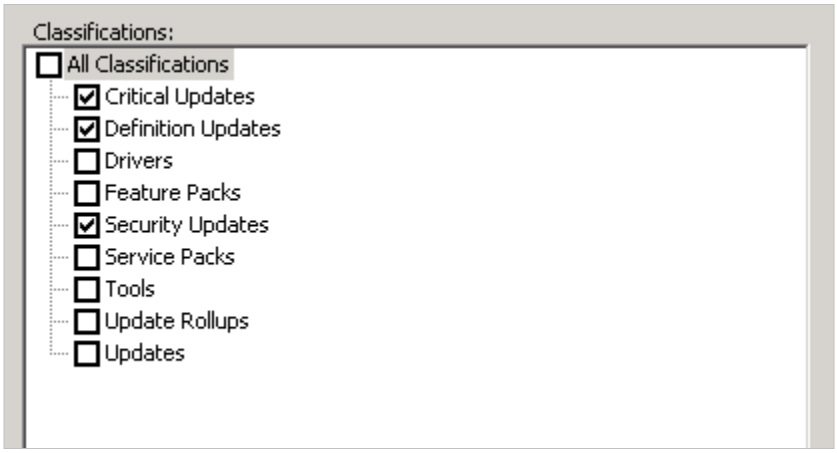

Figure 39: Selecting Update Classifications

8. At the next screen, you can choose to manually or automatically sync your updates. Manually synching will allow you to choose when your servers check in for updates. The servers will download updates depending on your approval. Automatically synching will cause them to update automatically. In this example, we've chosen automatic updates at 4:17:08AM, once per day.

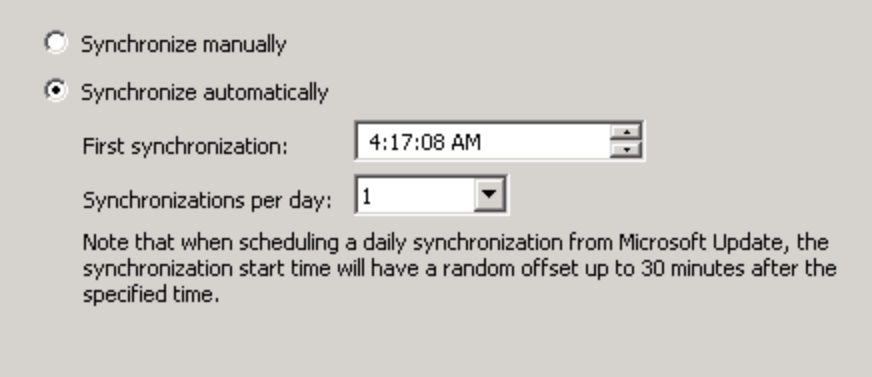

Figure 40: Configuring WSUS Synchronizations with Microsoft

9. Click **Next**.
10. At the next screen, you will begin your initial synchronization. Run this now. You can either click **Finish** and go to the next screen or click **Next**.
11. If you click next, you will see more advanced options, including the following:
12. **Using SSL with WSUS** – Configuring your updates to be sent from a secure location. Remember that you will need two ports: one for encrypting metadata and one for clear HTTP transmission.
13. **Create Computer Groups** – Create security groups to deploy WSUS to.
14. Assign Computers to Groups using Group Policy – Configure group policy for WSUS groups.
15. **Configure Auto-Approval Rules** – Configure rules to auto-approve update pushes for your clients.
16. In the next section, we will walk through some of these submenus that pertain to the exam.

Creating a Computer Group

Selecting the Create a Computer Group button will take you to the Microsoft Help Menu file, which will take you through the steps of creating a computer group:

12. From the updates services tree, expand your server and then expand computers.
13. Under **All Computers**, choose the group where you would like to create a new computer group.
14. Right-click your node and select **Add Computer Group**.
15. Type the name of your group and hit OK.

Assigning Clients through Group Policy

To ensure that clients are now looking for the WSUS for updates instead of Microsoft Update, we will need to configure our associated computers with a group policy rule to look for our new WSUS Server. To do this, you will need to perform the following steps:

1. Open **Group Policy Management**.
2. **Right-click** the OU containing the computers in your organization and create a GPO. Edit the GPO.

3. Expand **Computer Configuration** → **Administrative Templates** → **Windows Components**, and select **Windows Update**.
4. Double-click **Enable Client-side targeting.**
5. Click **Enabled**.
6. Type the name of the computer group in the "Target Group name for this computer" box.
7. Click OK.

Auto-Approval Rules

Auto-approval rules allow you to choose certain types of updates to be automatically approved without administrative approval. If you were a particularly risky administrator, you could automatically approve all security updates without review. If you'd like to configure your server to auto-approve updates for your client workstations, follow these steps:

1. In the **WSUS Update Services** tree, expand the section where you'd like to approve updates and click **Options**.
2. Click **Automatic Approvals.**
3. Select **Default Automatic** approval and then click **Edit**.
4. Click **New Rule** to create a new rule.
5. Edit the **Properties** of the rule and select where you would like to approve updates.
6. Click **OK**.

Managing a Disconnected Network

In order to provide updates to machines that are no longer attached to your network, you need to manually place updates on removable media that can be transported to machines for manual installation. Once we have reached this point, we typically have WSUS already setup. Thus, you only need to consider the following:

1. Have I determined the updates that are necessary to send to my disconnected network?
2. Are the updates compatible?

Necessary updates that we know are going to do good, and need to be applied. Now, just to be clear, you won't see this on the exam. But, it's important that you realize that on a disconnected network, it really isn't necessary to deploy every single update – just those that you require. That said, there are three steps to actual deployment of WSUS updates to a disconnected network:

1. Ensure compatibility.
2. Copy the updates to a file system.
3. Copy from the file system to the server.
4. Run wsusutil.exe with the "/export" switch from C:\Program Files\Update Services\Tools.
5. Export the data to a package.
6. Import the data on your destination server with WSUS installed by running the /import switch with the same tool.

Capturing Performance Data

An important part of any maintenance plan is the consistent gathering of network and system performance data for use in baselines and comparison studies. Through Windows Server 2008, administrators are given access to many tools that can be used to determine the overall health of systems, and whether or not they are performing at the ideal level.

Additionally, as problems begin to arise in your infrastructure (as they inevitably do in even the best laid environments with the most ideal hardware), you will want to collect data sets that will allow you to realize what is happening's going on and where.

Performance Monitor

Performance Monitor, or "PerfMon" for short, is a performance analysis tool that is used in organization to monitor the overall performance of our server. To launch PerfMon in Windows Server 2008, you can type **perfmon** in the Windows Start menu. This will launch the **Reliability and Performance Monitor**, shown below.

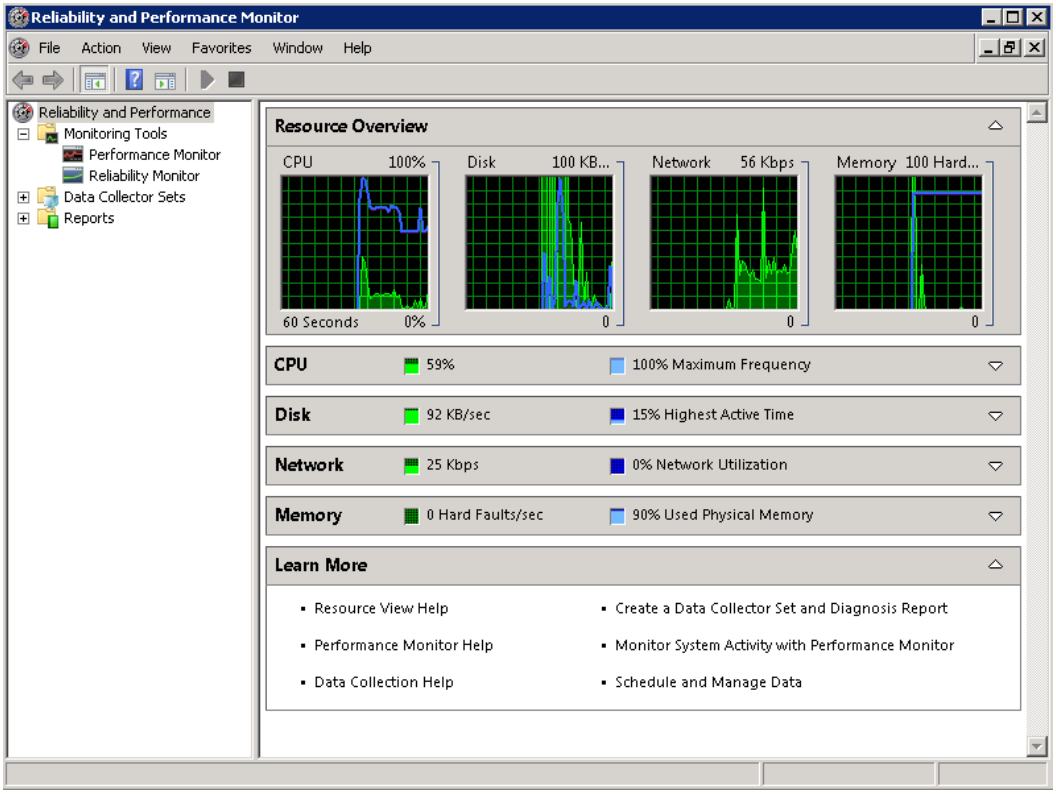

Figure 41: Windows Server 2008 Reliability and Performance Monitor

From the home screen, Perfmon creates an analysis of overall CPU, Disk, Memory and Network use. Here, we can get a quick overview of our system. In the screenshot above, we can see the following:

- Our Current CPU load is 59%.
- The Disk I/O is only 92Kbps.
- The Network usage is only 25kbps.
- There are no memory faults, but 90% of the memory is used.

The performance monitor section of the Reliability and Performance monitor can be accessed by selecting Performance Monitor from the main menu. Here, in this section, we can create a number of fields to analyze based on our custom inputs. To create a counter, you can click the plus sign. Here, we can add many different fields to monitor.

For example, on a server in the infrastructure, we are interested in monitoring the performance of SQL. Thus, in the add counters area, you can select the **MSSQL$SQLEXPRESS:Databases** section and all the submenus beneath the plus sign. Then, we can click **Add** and receive the added counters menu, as you see below.

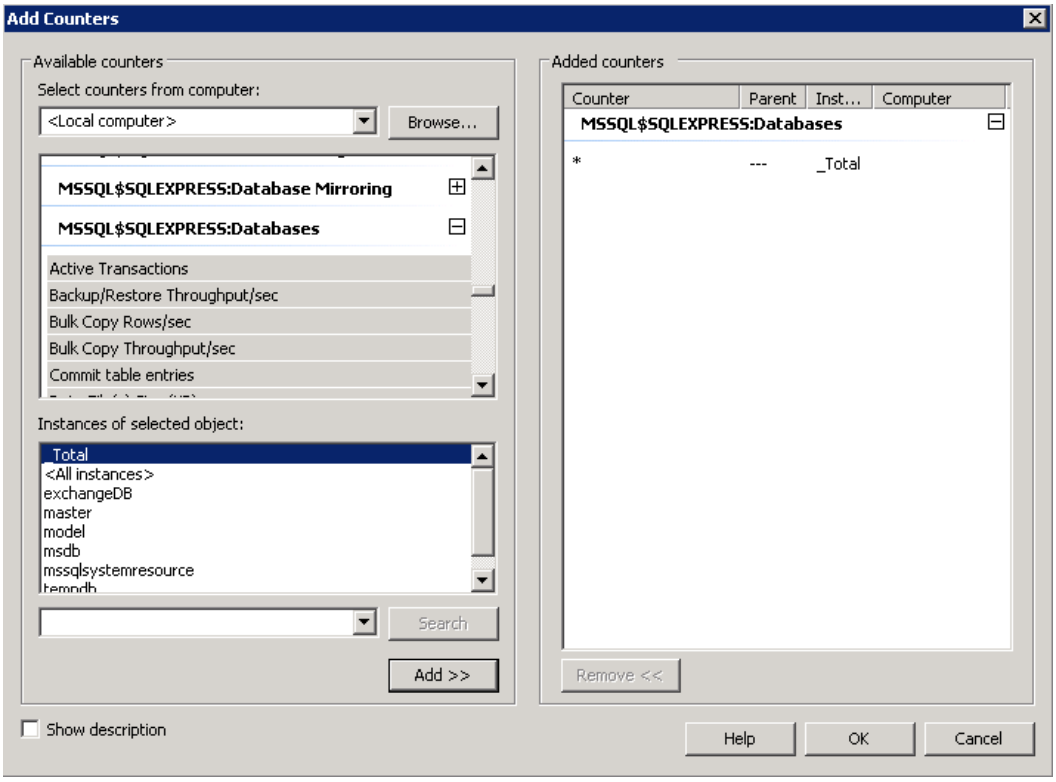

Figure 42: Adding a PerfMon Counter

Now, when we hit **OK**, we will see the perfmon counter that has been added, along with all the data fields associated with it. These will appear in the main screen, where we can watch their progress.

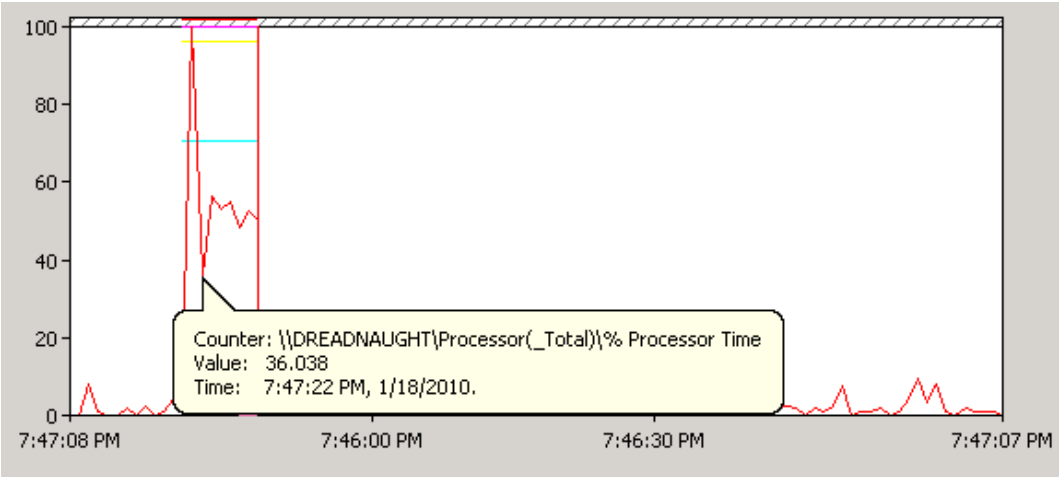

Figure 43: A Counter in Action

On the other hand, the reliability monitor will give you an overall view of your server's health. Below, we have included a screenshot of the average performance of a server over time.

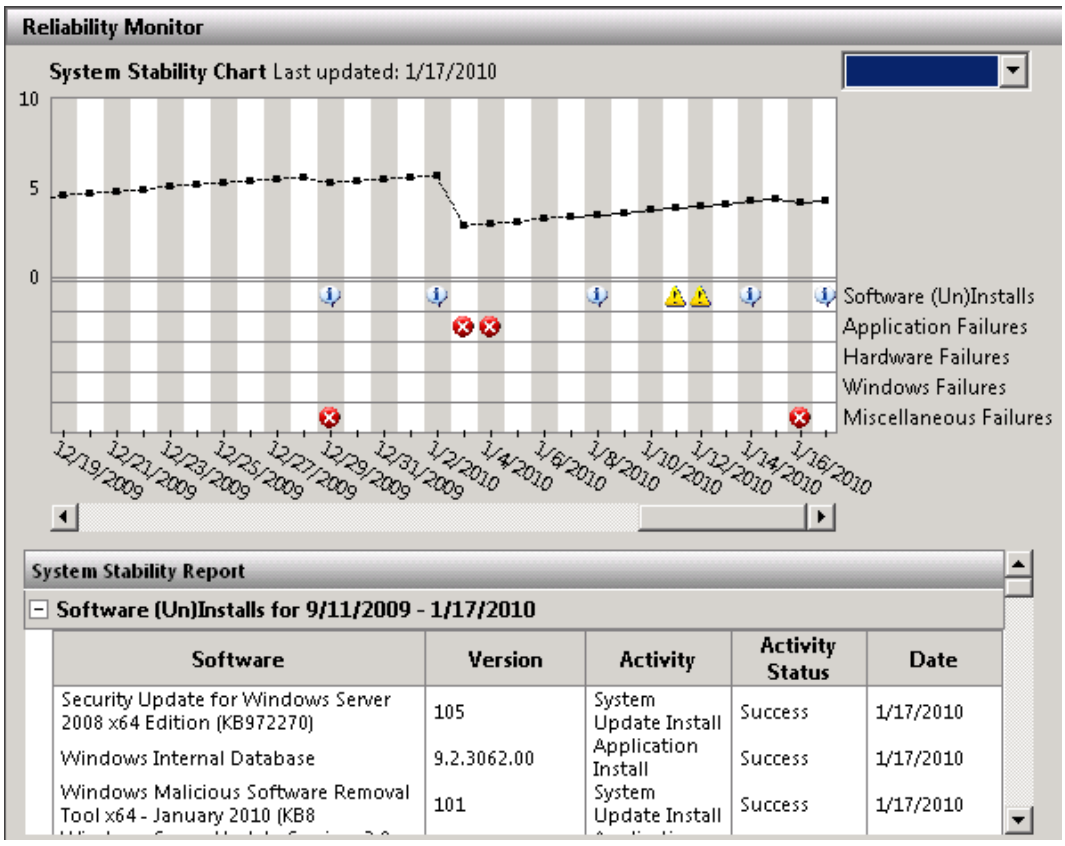

Figure 44: The System Stability Chart

Here, the reliability monitor shows application failures, hardware failures, and other information pertaining to the server. From the drop down menu, you can choose a date range or select all.

Data Collectors Sets

Data Collector Sets allow administrators to create predefined rules that allow the collection of data related to the performance monitor and its reliability. To collect a data set, do the following:

1. Under Data Collector Sets in PerfMon, choose User Defined.
2. Right-click and select New → Data Collector Set.
3. Name the data collector set. You can either create a collector set from a template or manually. It's much easier to choose a template, because most actions are predefined.

From the templates, you can choose:

4. Active Directory Diagnostics
5. Basic
6. System Diagnostics
7. System Performance
8. Health Registration Authority
9. LAN Diagnostics
10. For this example, we will choose system performance.
11. Click **Next.**
12. Keep the root directory default, unless you want to specify another directory, and click **Finish**.
13. This will monitor system events and collect them in the directory we defined in the previous step.
14. When the set appears in the user defined area, **right-click it** and select **Start**.
15. The set will begin to collect data and output it to the defined directory.

You can choose to view any of the pre-defined sets whenever you feel it is necessary. Each set allows you to pick various resources to view any time you wish. For example, if your LAN is acting strangely, choose LAN diagnostics, start it, and then monitor the results in the output directory.

Monitoring Event Logs

The Event Viewer is another powerful monitoring tool in Windows Server 2008. Through it, you can view a wide variety of events, from Administrative Events to Windows logon events. Additionally, you can view serve role events, or. Additionally, you can monitor Windows Log events, including Application, Security, Setup, System, and forwarded events.

The event log, shown below, is a very simple system to use. It can export data to XML files and "Event Files" (EVTX). XML files are serialized files that contain data separated by tags. EVTX files are specifically formatted log files that house XML data, as well as event viewer data. EVTX also contains data associated with the Windows Event Viewer. With the Event Viewer, you can log windows activities on five different levels:

- Application
- Security
- Setup
- System
- Forwarded Events

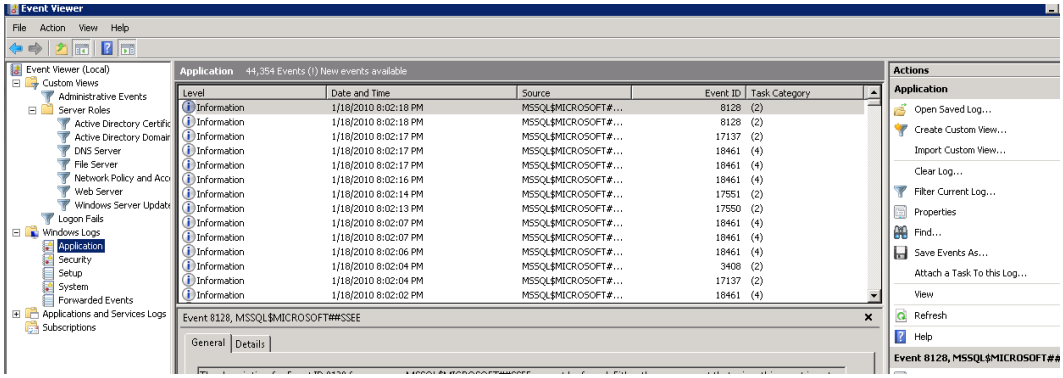

Figure 45: Windows Server 2008 Event Viewer

Regardless of which you choose, you can create custom views by clicking the **Create Custom View…** button and then configuring them from the very simple launch wizard. Additionally, you can export these views by choosing "**Save Events As**…" and exporting them.

Gathering Network Data

For the exam, network monitoring requires knowledge of Network Monitor configuration and practical use of the Simple Network Management Protocol (SNMP).

SNMP

This is a network protocol used by TCP/IP to monitor routers, bridges computers and wireless access points. Really, any TCP/IP devices with SNMP support. You should also know that SNMP can be used to configure devices remotely, monitor network performance, and detect network faults.

You should also know (though you don't necessarily need to know how to set it up) that SNMP works through management systems and SNMP agents. Management systems monitor agents and determine if they have any system events that need to be reported to the administrative platform that is controlling them.

Network Monitor

Network monitor is a downloadable tool available through Microsoft. The Monitor is a port and protocol analyzer designed to view and analyze network performance data. You would want to analyze network protocols because it is very helpful for an administrator to know exactly what type of data is being passed through their network. For example, you may not realize that you have a large amount of FTP traffic going to and fro on a server you have setup as an SMB server. It could mean that the server is being exploited for personal use by an employee (like serving files).

Launching the Network monitor will create a series of parsers (programs that search text via tokens) that will allow you to capture data. To capture data, you will need to select your network card, as shown in the figure below, and then click **New Capture.**

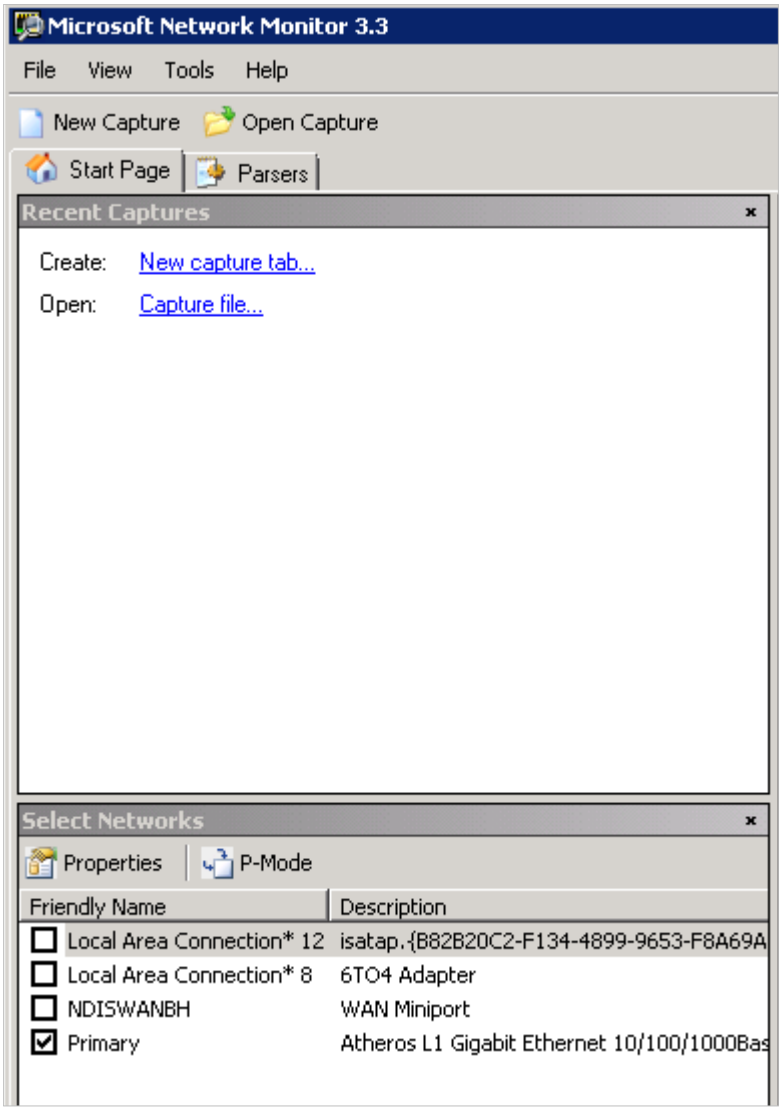

Figure 46: Starting a New Network Monitor Capture

Once you click **Capture**, this will launch the network capture wizard. You will then need to click **Start**. At this point, network traffic will start to fly past the "All Traffic" monitor. You will then be able to see the executables that are accessing TCP/IP traffic, as well as inbound traffic bound for no specific destination (which could potentially be quite bad!). Once you have monitored the network data you are after, you can export this data by choosing the "**Save As**" button. This will export the data as a CAP file that you can open with network monitor at another point.

Practice Questions

Chapter 1

1. Stephanie is the systems administrator for Meley Enterprises, a marketing firm based out of Miami. In an effort to save money on hardware, Stephanie has decided to install Hyper-V on four Windows 2008 Enterprise servers instead of having to purchase four extra servers. All the servers have x64-based processors and run on Intel VT-enabled machines. Stephanie installs Windows Server 2003 SP2 for the guest operating systems on the four servers. After installation, the guest OS will not boot and the servers receive an error in the system event log that states: "Hypervisor launch failed; at least one of the processors in the system does not appear to support the features required by the hypervisor." What action does Stephanie need to take to get the guest operating systems to function properly? Select the best answer.

   - ❍ A. Stephanie needs to install Windows Server 2008 for the guest operating systems since Server 2003 is not supported.
   - ❍ B. Stephanie needs to make sure that the Execute Disable feature is enabled in the BIOS.
   - ❍ C. In order for the hypervisor to boot, the Execute Disable feature in the BIOS must be disabled.
   - ❍ D. Stephanie needs to enable her PXE compliant NIC to be enabled in the BIOS. This allows the guest OS to boot properly.

2. Kevin is the network administrator for Gearing Up Racing, Inc., a motorcycle manufacturing company in Seattle. Kevin has recently migrated the company's network to a Windows 2008 Active Directory from Windows 2003. Kevin's company also recently purchased 30 laptops for salesmen that will be traveling for the company, trying to create contacts and make clients. Because of all these new mobile users needing access to the network while on the road, Kevin is worried about his network's security. Kevin wants to be able to manage network security policies, and he wants to ensure that all mobile users comply with a certain set of security standards before they are allowed to authenticate on the network. These standards will include: patches, virus definitions, and hardware configurations. What Windows Server 2008 technology would allow Kevin to accomplish what he needs? Select the best answer.

   - ❍ A. Network Access Protection would allow Kevin to manage security policies and ensure that mobile users have to comply with standards before being allowed onto the network.
   - ❍ B. If Kevin used WSUS, he would be able to ensure that all computers had the most recent Microsoft updates before logging on to the network.
   - ❍ C. IPSec, built into Windows Server 2008, would allow Kevin to control the mobile computers that log onto his network.
   - ❍ D. Active Directory Certificate Server (AD CS) would allow mobile users to be verified before logging onto Kevin's network.

3. Sharon is the network administrator for Gantly Incorporated, a clothing manufacturing company in Miami. Sharon is in charge of the entire network which consists of one domain running Windows Server 2008 Active Directory. The company is comprised of three offices all in Miami. One of the offices does not have very many employees and only has one IT person on staff. Because of this, Sharon has decided to perform a staged installation of a Read-Only Domain Controller. Sharon runs the Pre-create Read-only Domain Controller account wizard and then delegates permission to install the RODC to the security group that contains the IT staff person at the other office. What command does the IT staff person need to run on the RODC to start the installation wizard?Select the best answer.

   - ❍ A. The IT staff person needs to run the command: dcpromo /UseExistingAccount:Attach
   - ❍ B. The command: dcpromo /startRODC needs to be run on the RODC by the delegated administrator.
   - ❍ C. The IT staff member at the other office needs to run the adprep /domainprep to prepare the domain for the installation of the new RODC.
   - ❍ D. The staff member needs to run the command: dcpromo /delegate:Attach

4. You are the network administrator for your company. You have three web servers running Windows 2000 Server that you are getting ready to upgrade to Windows Server 2008. These servers are running Web-based applications using ASP.NET and Web Distributed Authoring and Versioning (WebDAV). You use Server Manager on 2008 to configure the servers as application servers. You install the Web-based application on the web servers. Now when you attempt to navigate to the application using a URL, it says that the page cannot be found, with an HTTP Error 404 - File or Directory not found. What do you need to do to ensure the Web-based application works properly? Select the best answer.

   - ❍ A. You need to use IIS Manager to allow Active Server Pages Web service extension.
   - ❍ B. You need to disable anonymous access.
   - ❍ C. You need to enable reversible encryption.
   - ❍ D. You need to restart the default web site in IIS manager.

Chapter 2

1. Henry is the systems administrator for his company. The company has a total of 20 servers running Windows Server 2008 Enterprise and 100 workstations running Windows Vista. Although every machine on the network is running antivirus software, one of the users inadvertently downloaded a Trojan virus which spread through the network to one of the servers. After removing both the server and the workstation from the network, Henry runs a removal tool and is able to completely remove the virus from both machines. Now, when either machine is booted up, both of them have the Task Manager option disabled from the Ctrl+Alt+Del screen. When Henry tries to run the Task Manager from Windows Explorer, it says that the Task Manager has been disabled by the administrator. How can Henry re-enable the Task Manager for the server and the workstation? Select the best answer.

   - ❍ A. Henry must re-apply the latest service packs for both Windows Server 2008 and Windows Vista for the Task Manager to be enabled.
   - ❍ B. Henry must open the Local Computer Policy first from the command line. He then needs to go to Computer Configuration, Administrative Templates, System, Ctrl+Alt+Del Options and disable the setting that states "Remove Task Manager".
   - ❍ C. Henry must open the Local Computer Policy first from the command line. He then needs to go to User Configuration, Windows Settings, System, Ctrl+Alt+Del and enable the setting that states "Enable Task Manager".
   - ❍ D. To re-enable the Task Manager, Henry must open the Local Computer Policy from the command line. Then, he needs to navigate to User Configuration, Administrative Templates, System, Crtl+Alt+Del Options and disable the "Remove Task Manager" setting.

2. Katy is the systems administrator for Goodness Manufacturing, a candy-making company in Pennsylvania. The company's network is currently running a Windows Server 2003 Active Directory environment. All workstations are running Windows XP. Katy is the sole person responsible for updating and maintaining the servers. Katy normally has to wait till after normal working hours to perform any application or Windows updates, since they require a reboot. She also performs offline defragmentation of the Active Directory database after hours, since it requires a reboot as well. Katy is trying to convince her boss that migrating to Windows Server 2008 would be very beneficial and would save him from paying her so much overtime from working after hours. What feature in Windows Server 2008 would allow Katy to perform updates and offline defragmentation without rebooting? Select the best answer.

   - ❍ A. There are no features built into Server 2008 that would allow this. If Katy migrates, she will still have to perform reboots after updates and after performing offline defragmentation of the Active Directory database.
   - ❍ B. Offline caching, a new feature in Server 2008, will allow updates and database defragmentation without server reboots.
   - ❍ C. The use of Hyper-V for the host operating systems in Server 2008 will allow Katy to install Windows updates and perform database defragmentation without having to restart the servers.
   - ❍ D. The Active Directory Domain Service can now be restarted which does not necessitate restarting the entire server.

3. Yancey is the systems administrator for his company. The entire company's network consists of one 2008 Active Directory domain, with 20 servers running Windows Server 2008, and 250 workstations running Windows Vista. Of the 20 servers, 4 of them hold the operations master roles. SVR1 holds the schema master and domain naming master role. SVR2 holds the RID master role. SVR3 holds the infrastructure master role. SVR4 holds the PDC emulator role. One of Yancey's junior administrators is planning to take SVR2 down for maintenance over a two day span. During that same time, another junior administrator is scheduled to add a number of user accounts to the domain for recently hired employees. Yancey needs to make sure that the junior administrator can add user accounts to the domain while SVR2 is down and also that user account creation will be possible after SVR2 is brought back online. What does Yancey need to do to accomplish this? Choose TWO.

   - ❍ A. He needs to use Ntdsutil to connect to SVR2.
   - ❍ B. He needs to use Ntdsutil to connect to SVR1.
   - ❍ C. He needs to transfer the RID master role from SVR2 to SVR1.
   - ❍ D. He needs to seize the RID master role from SVR2.

4. You are the systems administrator for your company. The network consists of one Windows Server 2008 Active Directory domain with two sites. The system state for every domain controller is backed up every night. You delete an Organizational Unit (OU) called Graphics, since there is nothing in that container. At about the same moment, a network administrator in the other Active Directory Site moves 15 computer and user accounts to that OU. The network administrator finds out that the OU was deleted and now cannot see the computer and user accounts that were moved to that OU. You need to re-create the Graphics OU and add the 15 accounts to that OU without affecting those accounts' network resources.
   What do you need to do? Select the best answer.

   - ❍ A. You should create another OU called Graphics and move the accounts from the DeletedObjects container to this new OU.
   - ❍ B. You should create a new OU named Graphics. Then, you should re-create all the user and computer accounts in that OU. Finally, you should use ADSI edit to change the SID of the accounts to their original value.
   - ❍ C. You should perform an authoritative restore for the Graphics OU to restore the computer and user accounts.
   - ❍ D. You should first create an OU called Graphics. Then, you should move the accounts from the LostAndFound container to this new OU.

5. You are the network administrator for your company. The network is comprised of one Active Directory domain called Stanton.com and three sites, called headquarters, westernbranch, and easternbranch. Each site has three domain controllers and 200 client computers. One server in the westernbranch site is called SVR10. All DNS servers have Active Directory-integrated zones. Some junior administrators say they cannot connect to SVR10 when trying to perform Active Directory administration. They are able to perform these tasks locally. You have verified that SVR10 is operational and that file and print resources are accessible by using the servers host name. You need to ensure that administrators can perform tasks on SVR10 without needing to have physical access to the server. What do you need to do? Select the best answer.

- ❍ A. You should install DNS on SVR10.
- ❍ B. You should force registration of DNS host resource records on SVR10.
- ❍ C. You should configure SVR10 as a local bridgehead server for the westernbranch site.
- ❍ D. You should restart the Net Logon service on SVR10.

Chapter 3

1. You are the systems administrator for your company. You administer the entire network, which consists of one 2008 Active Directory forest with three domains. The root domain has a domain controller with Active Directory Certificate Services (AD CS) installed to serve as the company's Enterprise root CA. You have set up online responders in the company branch offices to help with certificate validation. You have noticed that the OCSP clients in the branch offices are caching responses for too long of a period, so you need to change that. What command line utility can you use to change the OCSP client caching time? Select the best answer.

- ❍ A. You should use the cacheutil command line utility to change the OCSP client caching time.
- ❍ B. You should use the certutil tool to adjust the OCSP client response caching time.
- ❍ C. You should use ADSI edit to change the OCSP client response caching time.
- ❍ D. Wbadmin should be used, since it can change the OCSP client response caching time.

2. You are the IT manager for a large company. Your company's network is comprised of one 2008 Active Directory domain. You have installed Active Directory Certificate Services (AD CS) on one of the servers. For recovery purposes, you have assigned one of the systems administrators the ability to decrypt users' archived private keys but not the ability to retrieve these keys from the Certificate Authority's database. What role have you assigned to this administrator? Select the best answer.

- ❍ A. You have assigned the Key Recovery Agent Role to this administrator.
- ❍ B. You have assigned the Root Recovery Agent to this administrator.
- ❍ C. You have assigned the Certificate Manager role to this administrator.
- ❍ D. You have assigned the Certificate Auditor role to this administrator.

3. You are the systems administrator for your company. You oversee the entire network, which consists of one 2008 Active Directory domain. You have implemented Active Directory Certificate Services (AD CS) for EFS and S/MIME throughout the network. You have assigned the CA Officer and Key Recovery Agent (KRA) roles to two different systems administrators. After a user accidentally deleted his private key, you have the CA Officer retrieve the key from the database. The KRA has decrypted the private key, and now you need to import it back into the user's certificate store. This user's name is Helen. How can you accomplish this using a command line tool? Select the best answer.

   - ❍ A. You should type in the command: C:\certutil.exe -getkey Helen.pfx
   - ❍ B. You should type in the command: C:\Certutil.exe -storepersonal -Helen
   - ❍ C. You should type in the command: C:\CertImport -personal Helen.pfx
   - ❍ D. You should type in the command: C:\certutil.exe -user -importPFX Helen.pfx

Chapter 4

1. Your organization contains a Windows Server 2008 member server that is configured with the RRAS server role. Its two network adapters are named LAN1 and LAN2. You need to configure the network adapters such that outbound network traffic is favored toward LAN2. What action should you perform? Select the best answer.

   - ❍ A. Set the interface metric of LAN1 to 1 and the interface metric of LAN2 to 2.
   - ❍ B. Set the interface metric of LAN1 to 2 and the interface metric of LAN2 to 1.
   - ❍ C. Install the Microsoft Loopback Adapter and set its interface metric to 1.
   - ❍ D. Install the Microsoft Loopback Adapter and set its interface metric to 2.

2. Your organization consists of a single Active Directory domain in which all servers run Windows Server 2008 and all clients run Windows Vista. You need to configure your client computers' TCP/IP settings to provide IPv6 support in networks within your organization that support only IPv4 and NAT. What action should you perform? Select the best answer.

   - ❍ A. Ensure that the IPv6 protocol is enabled in the network card properties of all client workstations.
   - ❍ B. Ensure that at least one IPv6 scope is created on the networks' DHCP server.
   - ❍ C. Run the command netsh interface ipv6 set teredo on all client workstations.
   - ❍ D. Run the command netsh interface ipv6 set state on all client workstations.

3. Your organization includes a newly deployed Windows Server 2008 e-mail server that is configured with the following IP configuration information:

   IP Address: 172.16.16.3
   Subnet mask: 255.255.224.0

   You receive complaints from users who state that they are unable to connect to the e-mail server. What action should you perform? Select the best answer.

   - ❍ A. Change the server's IP address to 172.16.0.3.
   - ❍ B. Change the server's IP address to 172.16.32.3.
   - ❍ C. Configure the server to use a /20 subnet mask.
   - ❍ D. Configure the server to use the subnet mask 255.255.128.0.

4. Your organization's single Active Directory domain consists of a mixed IPv4/IPv6 environment. All servers run Windows Server 2008, and all client workstations run Windows Vista. You need to ping a file server named FS01.BIRCO.LAN that uses an IPv6 address. What actions should you perform? Choose TWO. (Each correct answer represents an independent solution.)

   - ❍ A. Ping the site-local address of the server.
   - ❍ B. Ping the link-local address of the server.
   - ❍ C. Issue the command ping -6 fs01.birdco.lan from your administrative workstation.
   - ❍ D. Issue the command ping -426 fs01.birdco.com from your administrative workstation.

5. Your organization consists of a single Active Directory domain in which all servers run Windows Server 2008 and all client computers run Windows Vista. You are planning to migrate from IPv4 and IPv6 and need to educate yourself as to how IPv6 addressing works. Which of the following represents an invalid IPv6 address? Select the best answer.

   - ❍ A. 2001:cdba:0000:0000:0000:0000:3257:9656
   - ❍ B. 2001:cdba:0:0:0:0:3257:9655
   - ❍ C. 2001:cdba::3257:9651
   - ❍ D. 2001:cgba::3257:9654

Chapter 5

1. Your network consists of a single Active Directory domain in which all servers run Windows Server 2008. You are planning a secure remote access infrastructure that includes three servers: WINNPS: Network Policy Server, HEALTH01: System Health Validation Server, Remediation Server, VPN01: VPN Server. You need to ensure that VPN client computers are screened by network health policies. What action should you perform to complete the configuration?

   - ❍ A. Configure VPN01 as a System Health Validator.
   - ❍ B. Configure VPN01 as a RADIUS server.
   - ❍ C. Configure VPN01 as a RADIUS client of HEALTH01.
   - ❍ D. Configure VPN01 as a RADIUS client of WINNPS.

2. You need to secure Remote Desktop sessions between your company's Windows Vista-based administrative workstations and your company's Windows Server 2008-based domain controller. What actions should you perform? Choose TWO. (Each correct choice represents a part of a single solution.)

   - ❍ A. Enable a security layer for RDP connections in Group Policy.
   - ❍ B. Disable Single Sign-On for Terminal Services.
   - ❍ C. Ensure that terminal servers are placed in the same Active Directory OU as other servers on the network.
   - ❍ D. Change the default RDP port on the server and the client computers.

3. Your network consists of a single Active Directory domain in which all servers run Windows Server 2008 and all client computers run Windows Vista with Service Pack 1. You need to support VPN connections from remote clients to an RRAS server named VPN01. However, network security policy mandates that the VPN connections use only standard Web protocols. What action should you perform? Select the best answer.

   - ❍ A. Define SSTP connections on VPN01.
   - ❍ B. Define L2TP connections on VPN01.
   - ❍ C. Define PPTP connections on VPN01.
   - ❍ D. Define IPSec connections on VPN01.

4. You are the IT manager for a small network. You need to configure a Windows Server 2008 member server named RRAS01 to support IP routing and VPN services. What action should you perform? Select the best answer.

- ❍ A. Install the Terminal Services role.
- ❍ B. Install the Network Policy and Access Services role.
- ❍ C. Install the Network Policy Server role service.
- ❍ D. Install the Health Registration Authority role service.

5. Your Windows Server 2008 Active Directory domain includes an application server named FS01 that stores highly confidential data. You need to configure Windows Firewall in Group Policy such that all Windows Vista clients who are authorized to access FS01 only do so by using IPSec packet encryption. What action should you perform? Select the best answer.

- ❍ A. Create a program rule that contains the action "Allow The Connection if it is Secure" and is associated with the Domain profile.
- ❍ B. Create a port rule that contains the action "Allow The Connection" and is associated with the Private profile.
- ❍ C. Create a custom rule that contains the action "Allow The Connection if it is Secure" and is associated with the Public profile.
- ❍ D. Create a predefined rule that contains the action "Allow the connection" and is associated with the Domain profile.

6. You manage a single Active Directory domain in which all servers run Windows Server 2008 and all client computers run Windows XP with Service Pack 2. You configure a member server named VPN01 to support incoming VPN connections that use SSTP. However, remote access users are unable to connect to the VPN server. What action should you perform? Select the best answer.

- ❍ A. Configure the RRAS server to issue a static pool of IP addresses instead of using DHCP.
- ❍ B. Open port UDP 500 on your corporate firewall.
- ❍ C. Upgrade the client computers to Windows XP Professional Service Pack 3.
- ❍ D. Upgrade the client computers to Windows Vista SP1.

7. Your network consists of a single Active Directory domain in which all servers run Windows Server 2008 and all client computers run Windows Vista SP1. You are configuring a member server named RRAS01 to support remote access connections. In particular, you need to allow IT staff to establish RDP connections to internal server resources without the overhead of building and tearing down VPN connections. RRAS01 possesses a Web server certificate that was issued by Verisign. What action should you perform? Select the best answer.

   - ❍ A. Configure RRAS01 to support SSTP connections.
   - ❍ B. Configure RRAS01 as a TS Gateway server.
   - ❍ C. Install the Network Policy Server role on RRAS01.
   - ❍ D. Install Active Directory Certificate Services on RRAS01.

8. You are planning to upgrade a Windows Server 2003 Routing and Remote Access (RRAS) server to Windows Server 2008. Your manager asks if any RRAS protocols have been removed in Windows Server 2008; you need to know this information to prevent a loss of functionality post-upgrade. Which of the following remote access protocols have been removed in Windows Server 2008 RRAS? Choose TWO.

   - ❍ A. OSPF.
   - ❍ B. BAP.
   - ❍ C. RIPv2.
   - ❍ D. CHAP.

Answers & Explanations

Chapter 1

1. Answer: B

Explanation A. Incorrect. Windows Server 2003 is supported.

Explanation B. Correct. This setting must be changed so that the guest operating systems can boot properly.

Explanation C. Incorrect. This feature must be enabled in the BIOS for the hypervisor to boot.

Explanation D. Incorrect. The NIC has nothing to do with the guest operating system booting properly.

2. Answer: A

Explanation A. Correct. Network Access Protection (NAP) is new in Windows Vista and Windows Server 2008 and allows for the creation of security policies and standards that computers must comply with to gain access to a network.

Explanation B. Incorrect. While WSUS helps computers stay up-to-date with Microsoft patches, it does not ensure that they are compliant with security policies before logging onto a network.

Explanation C. Incorrect. IPSec is used to create secure tunnels between devices, not to ensure whether devices are secure enough to allow onto a network.

Explanation D. Incorrect. While using certificates to verify user or computer accounts is a good security policy, it would not check for current patches or virus updates.

3. Answer: A

Explanation A. Correct. This is the appropriate command for the delegated administrator to run on the RODC.

Explanation B. Incorrect. There is no such dcpromo command.

Explanation C. Incorrect. The adprep /domainprep command is used to extend the schema, not to prepare a domain for an RODC.

Explanation D. Incorrect. There is no such option used with the dcpromo command.

4. Answer: A

Explanation A. Correct. You need to enable ASP pages.

Explanation B. Incorrect. This would not help display the Web-based application.

Explanation C. Incorrect. Authentication has nothing to do with the page not displaying.

Explanation D. Incorrect. Restarting the web site will not help display the application.

Chapter 2

1. Answer: D

Explanation A. Incorrect. Running the service packs will do nothing to re-enable the Task Manager.

Explanation B. Incorrect. This setting is not available in the Computer Configuration settings; it is in the User Configuration settings.

Explanation C. Incorrect. There is no such option available in the User Configuration, Windows Settings area.

Explanation D. Correct. This is the local policy that allows the Task Manager to be enabled or disabled. Some viruses have been known to change this setting when they infect a computer.

2. Answer: D

Explanation A. Incorrect. This is not normally necessary in Server 2008. The Active Directory Domain Services can be stopped and restarted without actually rebooting the server.

Explanation B. Incorrect. There is no such thing as offline caching in Server 2008.

Explanation C. Incorrect. Hyper-V is a new technology that allows for virtual machines, not for performing updates without having to reboot.

Explanation D. Correct. The AD DS can now be stopped and restarted after performing Windows updates or defragmenting the Active Directory database, eliminating the need to restart the server.

3. Answers: B, C

Explanation A. Incorrect. Yancey needs to connect to the server he will be transferring the role to, not from.

Explanation B. Correct. He needs to first use Ntdsutil to connect to the server he will transfer the role to.

Explanation C. Correct. If he transfers the role from SVR2 to SVR1, the junior administrator will be able to create user accounts on the domain while SVR2 is down.

Explanation D. Incorrect. If he seizes the role from SVR2, he will have to re-install windows on that server before bringing it back online.

4. Answer: D

Explanation A. Incorrect. There is no such object as the DeletedObjects container in Active Directory.

Explanation B. Incorrect. The accounts are not actually deleted, and this procedure would not work anyway.

Explanation C. Incorrect. The accounts were not actually deleted, since they were moved to the LostAndFound container.

Explanation D. Correct. When objects are moved to a container that is no longer present, those objects are moved to the LostAndFound container.

5. Answer: D
Explanation A. Incorrect. Installing DNS on the server would not help.

Explanation B. Incorrect. Since the administrators were able to use file and print services using the host name, the host records are already in place.

Explanation C. Incorrect. Making the server a bridgehead server would not help in this situation.

Explanation D. Correct. Restarting the Net Logon service will restore the SRV DNS record, which is what is needed here.

Chapter 3
1. Answer: B
Explanation A. Incorrect. There is no such command line utility as this.

Explanation B. Correct. This is the correct command line tool to use.

Explanation C. Incorrect. ADSI would not help in this situation.

Explanation D. Incorrect. Wbadmin is used for backing up and restoring files on Server 2008.

2. Answer: A
Explanation A. Correct. The Key Recovery Agent can decrypt private keys but cannot retrieve the keys from the Certificate Authority database.

Explanation B. Incorrect. There is no such role as the Root Recovery Agent.

Explanation C. Incorrect. The Certificate Manager can retrieve the certificates from the Certificate Authority database but cannot decrypt the keys.

Explanation D. Incorrect. The Auditor role determines what is logged and monitors the logs on the Certificate Authority.

3. Answer: D
Explanation A. Incorrect. This is not the proper option to use with the certutil command.

Explanation B. Incorrect. This is not the proper use of the certutil command.

Explanation C. Incorrect. There is no such utility as certimport.

Explanation D. Correct. This command will import the key material into her personal certificate store.

Chapter 4

1. Answer: A

Explanation A. Correct. Higher metric numbers denote higher-priority network adapters. Therefore, in this case the server will favor the LAN2 interface to the LAN1 interface.

Explanation B. Incorrect. Because in this case the LAN1 interface has a higher metric, the server will prefer the wrong interface.

Explanation C. Incorrect. We never want to use the Loopback Adapter on a production server.

Explanation D. Incorrect. We can be very certain that we don't want to use the Loopback Adapter on a production server#ever.

2. Answer: C

Explanation A. Incorrect. This should be an obvious first step; if we disable IPv6 in the network card properties, then the IPv6 protocol is completely unusable.

Explanation B. Incorrect. The scenario does not state whether DHCP or static addressing is being used on the network.

Explanation C. Correct. The Teredo protocol is what allows Windows Vista and Windows Server 2008 computers to use IPv6 in environments that consist of Network Address Translation (NAT)-enabled firewalls and routers and an IPv4 addressing infrastructure.

Explanation D. Incorrect. The set state context of the netsh int command is used to enable or disable IPv4 compatibility. In this case, since NAT is involved as well, we need to be concerned, at least principally, with Teredo settings.

3. Answer: C

Explanation A. Incorrect. The problem here is that the given IP address and the subnet mask do not match.

Explanation B. Incorrect. The problem here is in the subnet mask.

Explanation C. Correct. The given IP address is invalid with a 19-bit subnet mask. Here we need to use a /20 (255.255.240.0 in decimal) subnet mask.

Explanation D. Incorrect. This subnet mask masks only 17 bits, which continues to render the server's IP address as invalid.

4. Answers: B, C

Explanation A. Incorrect. You can ping the link-local address of the server, but not the site-local address.

Explanation B. Correct. You can ping IPv6 addresses by using the -6 flag or by specifying the link-local address of the target host.

Explanation C. Correct. The -6 flag of the ping.exe command enables you to lookup the AAAA record for the host in DNS and issue the ping.

Explanation D. Incorrect. The -426 switch is invalid.

5. Answer: D

Explanation A. Incorrect. This is a valid IPv6 address.

Explanation B. Incorrect. This is a valid IPv6 address.

Explanation C. Incorrect. This is a valid IPv6 address.

Explanation D. Correct. This IPv6 address is invalid because g is an illegal character in hexadecimal notation.

Chapter 5

1. Answer: D

Explanation A. Incorrect. We already have a system health validator in the mix. In this scenario we simply need to point the VPN server to it.

Explanation B. Incorrect. In order to link the VPN server to our Health Validation and NPS system, we need to configure VPN01 as a RADIUS client to the NPS RADIUS server.

Explanation C. Incorrect. In this case the RADIUS server is our NPS device. Remember that Network Policy Services is the Windows Server 2008 replacement for the Internet Authentication Service (IAS) that we knew and loved in Windows Server 2003.

Explanation D. Correct. In order to link our VPN server to our Health Validation server, we need to point the VPN server (as a RADIUS client) to our RADIUS server, which in this case is WINNPS.

2. Answers: A, D

Explanation A. Correct. In Windows Server 2008, you can enable one of three security layers for RDP connections with Windows Vista or other Windows Server 2008 computers: Negotiate, RDP, and SSL (TLS 1.0).

Explanation B. Incorrect. Actually, Microsoft recommends enabling SSO for Terminal Services to reduce the exposure of user credentials over the network.

Explanation C. Incorrect. Microsoft recommends that you place Terminal Server computers in their own OU to better scope policy.

Explanation D. Correct. Although this is a drastic step, it is a legitimate way to harden Terminal Services in certain high-risk situations.

3. Answer: A

Explanation A. Correct. Secure Socket Tunneling Protocol (SSTP) is Microsoft's latest innovation with regard to virtual private network (VPN) protocols. What is neat about SSTP is that it communicates over standard Web protocols (TCP 80 and TCP 443), which are ordinarily never blocked by corporate firewalls.

Explanation B. Incorrect. Layer 2 Tunneling Protocol communicates on ports other than standard Web ports.

Explanation C. Incorrect. Point to Point Tunneling Protocol (PPTP) also communicates on non-standard ports, which in this case would be blocked.

Explanation D. Incorrect. Again, Internet Protocol Security (IPSec) uses ports other than TCP 80 and TCP 443, which correspond to HTTP and HTTPS, respectively.

4. Answer: B

Explanation A. Incorrect. To configure a Windows Server 2008 computer as a remote access server, you need to install the Network Policy and Access Services role.

Explanation B. Correct. You need to install this role, and, at the least, the Routing and Remote Access role services, in order to equip the server to provide the services that are described in the question.

Explanation C. Incorrect. The Network Policy Service is a RADIUS server; nothing is stated in the scenario that leads us to conclude that the server will provide RADIUS services.

Explanation D. Incorrect. Nothing is stated in the scenario to lead us to conclude that the server will provide network health monitoring and enforcement.

5. Answer: A

Explanation A. Correct. Because FS01 is an application server, we need an application rule. The "Allow the Connection if it is Secure" option specifies IPSec communications. Finally, because the client computers are domain members, we associate the rule with the Domain profile.

Explanation B. Incorrect. This rule is all wrong for the needs as provided in the scenario.

Explanation C. Incorrect. We need this profile to be associated with the Domain profile.

Explanation D. Incorrect. None of the predefined rules gives us theflexibility we need in this scenario.

6. Answer: D

Explanation A. Incorrect. The IP allocator function of Windows Server 2008 RRAS is immaterial in this situation.

Explanation B. Incorrect. UDP port 500 is reserved for IPSec; the entire benefit of Secure Socket Tunneling Protocol (SSTP) is that it enables VPN tunnels over the standard SSL port (TCP 443).

Explanation C. Incorrect. Whereas you can obtain the NAP client with XP Service Pack 3, SSTP tunneling support is not included at all with Windows XP.

Explanation D. Correct. SSTP connections are only supported with Windows Server 2008 and Windows Vista with Service Pack 1.

7. Answer: B

Explanation A. Incorret. The Secure Socket Tunneling Protocol (SSTP), while nice inasmuch as it uses standard Web ports instead of "funky" off-ports that are often blocked, is nonetheless a VPN technology.

Explanation B. Correct. The Windows Server 2008 Terminal Services (TS) Gateway role enables an RRAS server to securely pass through Remote Desktop Protocol (RDP) connections from the Internet to internal hosts securely without the hassle and overhead of building and maintaining VPN connections.

Explanation C. Incorrect. The TS Gateway is a role service of the Terminal Services server role, not the NPS server role.

Explanation D. Incorrect. Although the server does need an SSL certificate, the scenario states that the server already has one that was purchased from Verisign.

8. Answers: A, B

Explanation A. Correct. The Open Shortest Path First (OSPF) routing protocol has been removed in Windows Server 2008 RRAS.

Explanation B. Correct. Bandwidth Allocation Protocol (BAP) is not available in Windows Server 2008 RRAS.

Explanation C. Incorrect. Routing Information Protocol version 2 (RIPv2) is alive and well in Windows Server 2008 RRAS.

Explanation D. Incorrect. The industry standard Challenge Handshake Authentication Protocol (CHAP) is very much present in Windows Server 2008 RRAS.