Exam Manual

LearnSmart

Microsoft Server 2008 Active Directory

(83-640) / (70-640)

Microsoft Certified IT Professional (MCITP)

This LearnSmart exam manual familiarizes candidates with topics on the Microsoft 83-640/70-640 Exam on Windows Server 2008 Active Directory. By explaining these topics quickly and efficiently, concentrating on the most difficult portions of each domain, the manual equips IT professionals with the knowledge required to pass the exam and move closer towards earning their certification. Topics covered in this manual include:

- DNS for Active Directory
- Active Directory Infrastructure
- Active Directory Server Roles
- And more!

Sharpen your competitive edge today by purchasing this exam manual and moving one step closer towards earning your MCTS and MCITP!

Windows Server 2008 active Directory (70-640/83-640) LearnSmart Exam Manual

Product ID: 11504 & 12413
Production Date: July 6, 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@learnsmartsystems.com

International Contact Information

International: +1 (813) 769-0920

United Kingdom: (0) 20 8816 8036

Table of Contents

Abstract

This Exam Manual is designed to familiarize you with the necessary information you will need to know in order to pass the Microsoft 70-640 exam on Windows Server 2008 Active Directory. The primary purpose of this tool is to serve as a supplementary training product that you can use in conjunction with other training tools, such as LearnSmart Video Training or LearnSmart Practice Exams. It is not entirely comprehensive, but is instead designed to be quick and efficient, concentrating on the most difficult portions of the exam. After reading this Exam Manual, you should ask yourself how much you knew about the exam before you looked through it. If the answer is a lot, then you are probably prepared for the exam and can test yourself with a practice test. If not, then you need to concentrate more time studying and to reread the Exam Manual once again.

What to Know

The Microsoft 70-640 is the first exam available on the Microsoft Windows Server 2008 platform. Consequently, both the technology involved with the Microsoft exam has changed and the technology involved within the actual test differs as well. This exam is highly concentrated on specific questions involved with the Server 2008 Active Directory infrastructure, the difference between Server 2003 and Server 2008, and what you need to know to be an effective Server technology specialist. Thus, it behooves you to spend a lot of time studying the technology of the test, and not necessarily the procedure. Much of the exam is going to be concentrated on the features of the Server 2008 platform, not just what you can do with it. Be prepared!

Tips

The best thing you can do to prepare for this exam is get as much experience with Windows Server 2008 as possible. This means that you'll need to get an evaluation copy of Server 2008 and get a very fast, very reliable computer. Server 2008 is fairly demanding and if you want to know and understand the features very well, you'll need to have something that can turn them on and not stutter or struggle. Additionally, make sure that you take at least one practice test. They're available from PrepLogic and are the single best preparation tool available on the market. Good luck!

Domain 1: Configuring Domain Name System (DNS) for Active Directory

Configure zones

In Domain Name System (DNS), a DNS namespace can be divided into zones. The zones store name information about one or more DNS domains. For each DNS domain name that is included in a zone, the zone becomes the authoritative source for information about that domain.

A zone starts as a storage database for a single DNS domain name. If other domains are added below the domain that is used to create the zone, these domains can either be a part of the same zone or belong to another zone.

DNS zones can be stored in the domain or application directory partitions of Active Directory Domain Services (AD DS). A partition is a data container in AD DS that distinguishes data for different replication purposes. You can specify in which Active Directory partition to store the zone and, consequently, the set of domain controllers among which that zone's data will be replicated.

Configuring DNS Server Active Directory Integration
The DNS Server service can be configured to use AD DS to store zone data. This makes it possible for the DNS server to rely on directory replication, which enhances security, reliability and ease of administration.

Follow these steps to create a DNS application directory partition:

1. Open a command prompt
2. Type the following command, and press ENTER:
   dnscmd <ServerName> /CreateDirectoryPartition <FQDN>
3. After you create a Domain Name System (DNS) application directory partition to store a zone, you must enlist the DNS server that hosts the zone in the application directory partition. To accomplish this, type the following command, and press ENTER:

   dnscmd <ServerName> /EnlistDirectoryPartition <FQDN>

The following table details the parameters in the above commands:

Parameter	Description
dnscmd	Specifies the name of the command-line tool for managing DNS servers.
<ServerName>	Required. Specifies the DNS host name of the DNS server. You can also type the IP address of the DNS server. To specify the DNS server on the local computer, you can also type a period (.).
/CreateDirectoryPartition	Required. Creates a DNS application directory partition.
/EnlistDirectoryPartition	Required. Enlists a DNS server in a DNS application directory partition.
<FQDN>	Required. Specifies the name of the new DNS application directory partition. You must use a DNS fully qualified domain name (FQDN).

The following are some factors to consider when creating an Active Directory Integrated DNS zone:

- When you decide which replication scope to choose, consider that the broader the replication scope, the greater the network traffic caused by replication. For example, if you decide to have AD DS–integrated DNS zone data replicated to all DNS servers in the forest, this will produce greater network traffic than replicating the DNS zone data to all DNS servers in a single AD DS domain in that forest.
- AD DS-integrated DNS zone data that is stored in an application directory partition is not replicated to the global catalog for the forest. The domain controller that contains the global catalog can also host application directory partitions, but it will not replicate this data to its global catalog.
- AD DS-integrated DNS zone data that is stored in a domain partition is replicated to all domain controllers in its AD DS domain, and a portion of this data is stored in the global catalog. This setting is used to support Windows 2000.
- If an application directory partition's replication scope replicates across AD DS sites, replication will occur with the same inter-site replication schedule as is used for domain partition data.

Windows Server 2008 supports the same zone types as earlier versions of Microsoft Windows Servers along with several new features, including: background zone loading for large DNS zones, IP version 6 (IPv6) support and support for read-only domain controllers (RODCs). The following table lists the different types of zones that can be configured in Windows Server 2008:

Zone Type	Description
Primary	A primary zone is the primary source for information about this zone, and it stores the master copy of zone data in a local file or in AD DS. When the zone is stored in a file, by default, the primary zone file is named *zone_name*.dns and is located in the %windir%\System32\Dns folder on the server.
Secondary	A secondary zone is the secondary source for information about this zone. The zone at this server must be obtained from another remote DNS server computer that also hosts the zone. This DNS server must have network access to the remote DNS server that supplies it with updated information about the zone. Because a secondary zone is merely a copy of a primary zone that is hosted on another server, it cannot be stored in AD DS.
Stub	A stub zone is a copy of a zone that contains only the resource records that are necessary to identify the authoritative DNS servers for that zone. A stub zone keeps a DNS server hosting a parent zone aware of the authoritative DNS servers for its child zone. This helps maintain DNS name-resolution efficiency.
GlobalNames	The GlobalNames zone was added in Windows Server 2008 to hold single-label names and provide support for organizations still utilizing WINS. Unlike WINS, the GlobalNames zone is intended to provide single-label name resolution for a limited set of host names, typically corporate servers and Web sites that are centrally (IT) managed. The GlobalNames zone is not intended to be used for peer-to-peer name resolution, such as name resolution for workstations, and dynamic updates in the GlobalNames zone are not supported. Instead, the GlobalNames zone is most commonly used to hold CNAME resource records to map a single-label name to a fully qualified domain name (FQDN).

Table continued on next page

Forward lookup	Forward lookup zones support the primary function of Domain Name System (DNS), that is, the resolution of host names to IP addresses. Forward lookup zones provide name-to-address resolution.
Reverse lookup	A reverse lookup zone contains pointer (PTR) resource records that map IP addresses to the host name. Some applications, such as secure Web applications, rely on reverse lookups. An administrator creates a reverse lookup zone only if applications running on your network require it.

There are two ways to configure a DNS zone:

1. Use the New Zone wizard in the DNS Manager.
2. Use the ***dnscmd*** command from a command prompt. As Microsoft started with Windows Server 2003, there are more options for configuring DNS available through the command prompt than from the GUI DNS Manager.

Using the New Zone Wizard:

1. Open DNS Manager.
2. In the console tree, right-click a Domain Name System (DNS) server, and click **New Zone** to open the New Zone Wizard. At this point, the New Zone Wizard has three choices:
    a. Primary Zone
    b. Secondary Zone
    c. Stub Zone
3. Follow the wizard's instructions to create a Primary, Secondary or Stub Zone.

Using a Command Prompt:

1. Open a Command Prompt.
2. Type the following, and press ENTER:

    dnscmd *ServerName* **/ZoneResetType** *ZoneName Property* [*MasterIPaddress...*] [**/file** *FileName*] {**/OverWrite_Mem**|**/OverWrite_Ds**|**/DirectoryPartition** *FQDN*}

The following table describes the options for the ***dnscmd*** command:

Value	Description
dnscmd	Specifies the name of the command-line tool.
ServerName	Required. Specifies the DNS host name of the DNS server. You can also type the IP address of the DNS server. To specify the DNS server on the local computer, you can also type a period (.).
ZoneName	Required. Specifies the fully qualified domain name (FQDN) of the zone.
Property	Required. One of the following zone types: • **/Primary** Standard primary zone. The *FileName* must be required. • **/DsPrimary** Active Directory–integrated primary zone. • **/Secondary** Secondary zone. You must specify at least one *MasterIPaddress*. • **/Stub** Stub zone. You must specify at least one *MasterIPaddress*. • **/DsStub** Active Directory-integrated stub zone. You must specify at least one *MasterIPaddress*.
/file	Required for **/Primary**. Specifies a file for the new zone. This parameter is not valid for the **/DsPrimary** zone type.
FileName	Required for **/Primary**. Specifies the name of the zone file. This parameter is invalid for the **/DsPrimary** zone type.
MasterIPaddress...	Required for **/Secondary**, **/Stub** and **/DsStub**. Specifies one or more IP addresses for the master servers of the secondary or stub zone, from which it copies zone data.
/OverWrite_Mem |**/OverWrite_Ds** |**/Directory Partition***FQDN*	**/OverWrite_Mem** overwrites existing DNS data using the data in AD DS. **/OverWrite_Ds** overwrites Active Directory data with data in DNS. **/DirectoryPartition** stores the new zone in the application directory partition that is specified by *FQDN*, such as: DomainDnsZones.corp.example.microsoft.com.

Configuring a GlobalNames zone
While the specific steps for deploying a GlobalNames zone can vary somewhat depending on the AD DS topology of different networks, the following steps cover most situations.

1. Create the GlobalNames zone
    - Create the zone on a DNS server that is a domain controller running Windows Server 2008. The GlobalNames zone is not a special zone type; rather, it is simply an AD DS-integrated forward lookup zone that is called GlobalNames.
2. Enable GlobalNames zone support
    - The GlobalNames zone is not available to provide name resolution until GlobalNames zone support is explicitly enabled by using the following command on every authoritative DNS server in the forest:

      dnscmd <ServerName> /config /enableglobalnamessupport 1

      where *ServerName* is the DNS name or IP address of the DNS server that hosts the GlobalNames zone. To specify the local computer, replace *ServerName* with a period (.), for example: **dnscmd . /config /enableglobalnamessupport 1**.
3. Replicate the GlobalNames zone
    a. To make the GlobalNames zone available to all DNS servers and clients in a forest, replicate the zone to all domain controllers in the forest; that is, add the GlobalNames zone to the forest-wide DNS application partition.
    b. To limit the servers that will be authoritative for the GlobalNames zone, create a custom DNS application partition for replicating the GlobalNames zone.
4. Populate the GlobalNames zone
    - For each server that will be able to provide single-label name resolution, add an alias (CNAME) resource record to the GlobalNames zone.
5. Publish the location of the GlobalNames zone in other forests
    a. If you want DNS clients in other forests to use the GlobalNames zone for resolving names, add service location (SRV) resource records to the forest-wide DNS application partition, using the service name _globalnames._msdcs and specifying the FQDN of the DNS server that hosts the GlobalNames zone.
    b. In addition, run the **dnscmd***ServerName***/config /enableglobalnamessupport 1** command on every authoritative DNS server in the forests that do not host the GlobalNames zone.

Updating DNS Servers
Once DNS has been installed and configured, the next step is to configure which type of update to allow from client and server computers to the DNS Server. There are three choices:

1. Dynamic DNS (DDNS)
2. Non-dynamic DNS (NDDNS)
3. Secure Dynamic DNS (SDDNS)

Dynamic update enables DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur. This reduces the need for manual administration of zone records, especially for clients that frequently move or change locations and use Dynamic Host Configuration Protocol (DHCP) to obtain an IP address.

Dynamic updates can be secure or non-secure. DNS update security is available only for zones that are integrated into AD DS. After you directory-integrate a zone, access control list (ACL) editing features are available in the DNS Manager console so that you can add or remove users or groups from the ACL for a specified zone or resource record.

NOTE: As a best practice, Microsoft recommends that client computers have Dynamic DNS updates turned on by default and that DHCP Servers be used to configure the DNSServer list. Similarly for branch office sites, clients should be configured to use Dynamic DNS updates, and you should set the Primary DNSServer, or use DHCP to set the DNS Server list to direct clients to the DNS Server running on the RODC.

Configuring Secure Dynamic Updates
Using the Windows interface:

1. Open DNS Manager.
2. In the console tree, right-click the applicable zone, and click **Properties**.
3. On the **General** tab, verify that the zone type is **Active Directory-integrated**.
4. In **Dynamic Updates**, click **secure only**.
   Secure dynamic update is supported only for AD DS-integrated zones. If the zone type is configured differently, you must change the zone type and directory-integrate the zone before securing it for DNS dynamic updates.

Using a command line:

1. Open a Command Prompt.
2. Type the following, and press ENTER:
   dnscmd *ServerName* **/Config** {*ZoneName*|**..AllZones**} **/AllowUpdate 2.**

The following table describes the options for the ***dnscmd*** command:

Value	Description
dnscmd	Specifies the name of the command-line program.
ServerName	Required. Specifies the DNS host name of the DNS server. You can also type the IP address of the DNS server. To specify the DNS server on the local computer, you can also type a period (.).
/Config	Required. Specifies the configuration command.
ZoneName|**.. AllZones**	Required. Specifies the fully qualified domain name (FQDN) of the zone. To configure all zones that are hosted on the specified DNS server to allow dynamic updates, type: **..AllZones**.
/AllowUpdate	Required. Specifies the allow update command.
2	Required. Configures the server to allow secure update. If you exclude the **2**, the zone will be set to perform standard dynamic updates only.

DNS Manager Zone Properties Dialog Box
You can use the controls in the zone properties sheet to administer the properties of a single zone. The following table lists the tabs that can appear in the zone properties sheet, depending on the zone type.

Item	Details
General	Use this tab to view the zone's status and to configure the following zone properties: • Default aging and scavenging settings • Dynamic updates • Zone type (including whether the zone data is stored in Active Directory Domain Services, AD DS, or in a file) • Replication scope (Active Directory-integrated zones only) • Master servers (secondary and stub zones only)
Start of Authority (SOA)	Use this tab to configure the zone's SOA record. The SOA record specifies the following for the zone: • Primary server • Zone administrator's e-mail address • Secondary zone expiration values • Minimum default Time-to-Live (TTL) for zone resource records
Name Servers	Use this tab to manage the list of authoritative name servers (NS) for the zone.
WINS	Use this tab to enable and manage WINS name resolution for the zone. This tab is not available for stub zones.
Zone Transfers	Use this tab to enable replication of zone data to other servers and to specify which servers can receive zone data. This tab is not available for stub zones.
Security	Use this tab to specify the user accounts that can be used to access the zone and the type of access to be allowed to each account. This tab is available for Active Directory-integrated zones only.

Configure Zone Scavenging
Follow the steps below to configure zone scavenging.
Using the Windows interface:

1. Open the DNS Manager.
2. In the console tree, right-click the applicable DNS server, and click **Set Aging/Scavenging for all zones**.
3. Select the **Scavenge stale resource records** check box.
4. Modify other aging and scavenging properties as needed.

Using a command line:

1. Open a Command Prompt.
2. Type the following, and press ENTER:
   dnscmd *ServerName* **/Config** {**/ScavengingInterval** *Value*|**/DefaultAgingState** *Value*|**/DefaultNoRefreshInterval** *Value*|**/DefaultRefreshInterval** *Value*}

The following table describes the options for the ***dnscmd*** command:

Value	Description
dnscmd	Specifies the name of the command-line program.
ServerName	Required. Specifies the DNS host name of the DNS server. You can also type the IP address of the DNS server. To specify the DNS server on the local computer, you can also type a period (.).
/Config	Required. Specifies the configuration command.
/ScavengingInterval	Required. Sets the frequency by which the server will perform scavenging for all scavenging-enabled zones.
/DefaultAgingState	Required. Sets the default aging configuration for all zones on the server.
/DefaultNoRefreshInterval	Required. Sets the default No-refresh interval for scavenging-enabled zones.
/DefaultRefreshInterval	Sets the default Refresh interval for scavenging-enabled zones.
Value	For **/ScavengingInterval**, type a value in hours. The default is 168 (one week). For **/DefaultAgingState**, type 1 to enable aging for new zones when they are created. Type 0 to disable aging for new zones. For **/DefaultNoRefreshInterval**, type a value in hours. The default is 168 (one week). For **/DefaultRefreshInterval**, type a value in hours. The default is 168 (one week).

NOTE:

- Aging and scavenging properties that are configured by this procedure act as server defaults that apply only to Active Directory Domain Services (AD DS)–integrated zones. For standard primary zones, you must set the appropriate properties at the applicable zone.
- When you apply changes for server aging/scavenging settings, the DNS console prompts you to confirm the changes. You then have the option to apply your changes to new AD DS-integrated zones only. If necessary, you can also apply your changes to existing AD DS-integrated zones.
- Regardless of whether the **Scavenge stale resource records** check box is selected, as described in step 3, this feature is disabled for standard primary zones, unless it is manually enabled at the applicable zone.

Configure DNS server settings

Configuring DNS to use forwarders

Using the Windows interface

1. Open the DNS Manager.
2. In the console tree, click the applicable DNS server.
3. On the **Action** menu, click **Properties**.
4. On the **Forwarders** tab, under **DNS domain**, click a domain name.
5. Under **Selected domain's forwarder IP address list**, type the IP address of a forwarder, and click **Add**.

NOTE:

- When specifying a conditional forwarder, select a DNS domain name before entering an IP address.
- By default, the DNS server will wait five seconds for a response from one forwarder IP address before trying another forwarder IP address. In **Number of seconds before forward queries time out**, you can change the number of seconds the DNS server will wait. When the server has exhausted all forwarders, it will attempt standard recursion.
- If you want the DNS server to only use forwarders and not attempt any further recursion if the forwarders fail, select the **Do not use recursion for this domain** check box.
- You can disable recursion for the DNS server so that it will not perform recursion on any query. If you disable recursion on the DNS server, you will not be able to use forwarders on the same server.
- Do not enter a forwarder's IP address more than once in a DNS server's forwarders list because it is a more reliable or a geographically-closer server. If one of the forwarders is preferred, that forwarder should be ordered first in the series of forwarder IP addresses.
- Problems associated with forwarders often result from inefficient configurations and overuse.

Using a command line

1. Open a Command Prompt.
2. Type the following, and press ENTER:

   dnscmd *ServerName* **/ZoneAdd** *ZoneName* **/Forwarder** *MasterIPaddress* **...** [**/TimeOut** *Time*] [**/Slave**]

The following table describes the options for the ***dnscmd*** command:

Value	Description
dnscmd	Specifies the name of the command-line tool.
ServerName	Required. Specifies the DNS host name of the DNS server. You can also type the IP address of the DNS server. To specify the DNS server on the local computer, you can also type a period (.).
/ZoneAdd	Required. Adds a zone.
ZoneName	Required. Specifies the fully qualified domain name (FQDN) of the zone.
/Forwarder	Required. Specifies the command to configure a forwarder. When configuring forwarders on DNS servers running on Active Directory domain controllers, you must use **/DsForwarder** in place of **/Forwarder**. **/DsForwarder** will replicate the forwarder setting to all DNS servers running on domain controllers in an Active Directory domain.
MasterIPaddress...	Required. Specifies a space-separated list of one or more IP addresses of the DNS servers where queries for *ZoneName* are forwarded. You may specify a list of space-separated IP addresses.
/TimeOut	Specifies the timeout setting. The timeout setting is the number of seconds before unsuccessful forward queries time out.
Time	Specifies the value for the **/TimeOut** parameter. The value is in seconds. The default timeout is five seconds.
/Slave	Determines whether or not the DNS server uses recursion when querying for the domain name that is specified by *ZoneName*.

NOTE:

- To view a zone added for use as only a conditional forwarder, use the following command:
  dnscmd *ServerName* **/ZoneInfo** *ZoneName*.
- To reset the forwarder IP addresses for a conditional forwarder domain name, type:
  dnscmd *ServerName* **/ZoneResetMasters** *ZoneName* [**/Local**] [*ServerIPs*].
- The **/Local** parameter sets the local master list for Active Directory-integrated forwarders, and the *ServerIPs* parameter is the list of one or more IP addresses of master servers for the zone. Master servers may include DNS servers that host primary or secondary copies of the zone, but they should not include DNS server IP addresses in such a way that two DNS servers hosting copies of a zone use each other as master servers. Such a configuration would make the forwarding path cyclical.
- To reset the standard, non-conditional forwarder for a DNS server, type:
  dnscmd *ServerName* **/ResetForwarders** [*IPAddress ...*] [**/**[**No**]**Slave**] [**/TimeOut** *Time*].

- The parameter *IPAddress* is the IP address where the DNS server will forward unsolvable DNS queries. The **/Slave** parameter sets the DNS server as a subordinate server. The **/NoSlave** parameter (default setting) sets the DNS server as a non-subordinate server, meaning that it will perform recursion. The **/Timeout** and *Time* parameters are described in the table above.

Configuring DNS Root Hints
To configure root hints, use the following steps:

1. Open the DNS Manager.
2. In the console tree, click the applicable DNS server.
3. On the **Action** menu, click **Properties**.
4. Select the **Root Hints** tab.
5. Modify the Root Hints properties as needed.

The following table lists the tabs that appear on the DNS Server Properties Sheet:

Item	Details
Interfaces	Use this tab to select the IP addresses that the Domain Name System (DNS) server will use to listen for DNS queries.
Forwarders	Use this tab to specify the DNS servers to which this server will refer queries when it cannot resolve them itself. Using forwarders prevents this server from using recursion to resolve DNS queries.
Advanced	Use this tab to perform the following actions: • View the server version number • Set advanced server options • Select the type of name checking to be performed for all zones • Select where the server obtains zone data when starting • Enable and configure default scavenging settings
Root Hints	Use this tab to specify the servers to be used for root hints when forwarders are not configured or do not respond.
Debug Logging	Use this tab to configure packet-level logging for debugging purposes.
Event Logging	Use this tab to specify the types of events that will be recorded in the DNS event log.
Monitoring	Use this tab to perform tests to verify the correct server configuration.

Configuring Zone Delegation
Using the Windows interface

1. Open the DNS Manager.
2. In the console tree, right-click the applicable subdomain, and click **New Delegation**.
3. Follow the instructions in the New Delegation Wizard to finish creating the newly delegated domain.
    - All domains (or subdomains) that appear as part of the applicable zone delegation must be created in the current zone before performing delegation.

Using a command line

1. Open a Command Prompt.
2. Type the following, and press ENTER:

   dnscmd *ServerName* **/RecordAdd** *ZoneName NodeName* [**/Aging**] [**/OpenAcl**] [*Ttl*] **NS** {*HostName*|*FQDN*}

The following table describes the options for the ***dnscmd*** command:

Value	Description
dnscmd	Specifies the name of the command-line tool.
ServerName	Required. Specifies the DNS host name of the DNS server. You can also type the IP address of the DNS server. To specify the DNS server on the local computer, you can also type a period (.).
/RecordAdd	Required. Specifies the command to add a resource record.
ZoneName	Required. Specifies the fully qualified domain name (FQDN) of the zone.
NodeName	Required. Specifies the FQDN of the node in the DNS namespace for which the SOA record is added. You can also type the node name relative to the *ZoneName* or @, which specifies the zone's root node.
/Aging	If this command is used, this resource record is able to be aged and scavenged. If this command is not used, the resource record remains in the DNS database, unless it is manually updated or removed.
/OpenAcl	Specifies that new records are open to modification by any user. Without this parameter, only administrators may modify the new record.
Ttl	Specifies the Time-To-Live (TTL) setting for the resource record. (The default TTL is defined in start-of-authority, SOA, resource record.)
NS	Required. Specifies that you are adding a name server (NS) resource record to the zone that is specified in *ZoneName*.
HostName| *FQDN*	Required. Specifies the host name or FQDN of the new authoritative server.

NOTE: When zone delegations are correctly configured, normal zone referral behavior can sometimes be circumvented if you are using forwarders in your DNS server configuration.

Configuring Round Robin
Round robin is configured in the following registry subkey:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\DNS\Parameters

The default setting for round-robin rotation is contained in the registry entry **RoundRobin** (REG_DWORD). By default, this entry's value is 1, rotating all RR types except those listed in the **DoNotRoundRobinTypes** registry entry. If the value of **RoundRobin** is set to 0, then no RR types will be round-robin rotated.

By default, DNS will perform round-robin rotation for all RR types. You can specify that certain RR types are not to be round-robin rotated in the registry. There is a registry entry called **DoNotRoundRobinTypes** (REG_SZ) with a string value containing a list of RR types. By modifying this entry, you turn off round-robin rotation for specific RR types. For example, to prevent round-robin rotation for A, PTR, SRV and NS record types, you would enter the following value for the registry entry:

a ptr srv ns

Disabling DNS Recursion
Using the Windows interface:

1. Open DNS Manager.
2. In the console tree, right-click the applicable DNS server, then click **Properties**.
3. Click the **Advanced** tab.
4. In **Server options**, select the **Disable recursion** check box, and click **OK**.

NOTE: If you disable recursion on the DNS server, you will not be able to use forwarders on the same server.

Using a command line:

1. Open a Command Prompt.
2. Type the following, and press ENTER:
   dnscmd*ServerName***/Config/NoRecursion** {**1**|**0**}

The following table describes the options for the ***dnscmd*** command:

Value	Description
dnscmd	Specifies the name of the command-line tool.
ServerName	Required. Specifies the DNS host name of the DNS server. You can also type the IP address of the DNS server. To specify the DNS server on the local computer, you can also type a period (.).
/Config	Required. Specifies the configuration command.
/NoRecursion	Required. Specifies the command to disable recursion.
{**1**|**0**}	Required. To disable recursion, type **1** (off). To enable recursion, type **0** (on). By default, recursion is enabled.

Configure Debug Logging
Using the Windows interface:

1. Open DNS Manager.
2. In the console tree, right-click the applicable DNS server, then click **Properties**.
3. Click the **Debug Logging** tab.
4. Select **Log packets for debugging**, and then select the events that you want the DNS server to record for debug logging.

NOTES:

- To get useful debug logging output you need to select a **Packet direction**, a **Transport protocol** and at least one more option.
- In addition to selecting events for the DNS debug log file, you can specify the file name, location and maximum file size for the file.
- Using debug logging options slows DNS server performance. For this reason, all debug logging options are disabled by default.

Configure DNS Server Scavenging
Use the following procedure to provide for automatic scavenging of resource records in the zones that are hosted by the Domain Name System (DNS) server:

1. Open the DNS Manager.
2. In the console tree, right-click the applicable DNS server, and then click **Properties**.
3. Click the **Advanced** tab.
4. Select the **Enable automatic scavenging of stale records** check box.

To adjust the **Scavenging period**, right-click the applicable DNS server, and in the drop-down list, select an interval in either hours or days, and then type a number in the text box.

Server Aging/Scavenging Properties Dialog Box
When you configure the following settings for server properties, the settings apply as the default value for all zones. When they are configured at a specific zone, the settings apply only to that zone. The following table details the options in the DNS Server Aging/Scavenging Properties dialog box:

Item	Details
Scavenge stale resource records	Specifies whether stale resource records should be removed from the Domain Name System (DNS) database.
No-refresh interval	Specifies an interval of time in either days or hours. When a resource record is refreshed, it is not refreshed again until this interval of time has elapsed.
Refresh	Specifies the minimum amount of time that resource records are expected to remain in the DNS database after the no-refresh interval expires. This interval should not be smaller than the maximum refresh period for any resource records. In most networks, this interval corresponds to the Dynamic Host Configuration Protocol (DHCP) lease renew interval. For DHCP servers running Windows, the default renew interval is four days.

Configure zone transfers and replication

Configure Zone Replication Scope
Using the Windows interface:

1. Open the DNS Manager.
2. In the console tree, right-click the applicable zone, and click **Properties**.
3. On the **General** tab, note the current zone replication type, and click **Change**.
4. Select a replication scope for the zone.

Using a command line:

1. Open a Command Prompt.
2. At a command prompt, type the following command, and press ENTER:
   dnscmd *ServerName* **/ZoneChangeDirectoryPartition** *ZoneName NewPartitionName*

The following table describes the options for the ***dnscmd*** command:

Value	Description
ServerName	Required. Specifies the Domain Name System (DNS) host name of the DNS server. You can also type the IP address of the DNS server. To specify the DNS server on the local computer, you can also type a period (.).
/ZoneChange Directory Partition	Required. Changes a zone's replication scope.
ZoneName	Required. Specifies the fully qualified domain name (FQDN) of the zone.
NewPartition Name	Required. The FQDN of the DNS application directory partition where the zone will be stored.

Incremental zone transfers
Incremental zone transfers (IXFR) are described in Request for Comments (RFC) 1995 as an additional DNS standard for replicating DNS zones. When incremental transfers are supported by both a DNS server acting as the source for a zone and any servers that copy the zone from it, it provides a more efficient method of propagating zone changes and updates. Incremental zone transfers replicate only the changed portions of a zone, which conserves network bandwidth.

For this process to work, a version history must be kept so that all name servers will know what changes have already been applied. The primary server maintains a version history, tracking all changes that have been made since the last version update was transferred to a secondary server. When an IXFR request is received from a secondary server, the primary server sends the updates, starting with the oldest and progressing to the newest updates.

When the secondary server begins receiving the updates, it creates a new version of the zone and applies the updates to that copy. When all the updates are committed to the copy of the zone database, the original database is replaced with the copy.

NOTE: If the primary server does not support incremental transfers, it simply ignores the incremental request of the secondary server and performs a full zone transfer.

Configuring DNS Notify
Follow the steps below to configure DNS Notify.

1. Open DNS.
2. In the console tree, click the applicable zone.
3. On the **Action** menu, click **Properties**.
4. Click the **Zone Transfers** tab.
5. Click **Notify**.
6. Verify that the **Automatically notify** check box is checked.

7. Select the method to be used for creating a list for notifying other DNS servers when changes to the zone occur. Your options are:
    a. Use the default, **Servers listed on the Name Servers tab**, to permit only those servers that appear by IP address on the **Name Servers** tab to be included in the notify list.
    b. Select **The following servers** if you want to specify a different notify list to be used instead.
8. If you selected **The following servers** in the previous step, add or remove server IP addresses to form the notify list as needed:
    a. To add a server to the notify list, type its IP address in the **IP address** field, and click **Add**.
    b. To remove a server from the notify list, click the server IP address in the list box, and click **Remove**.

NOTE: Changes to the notify list properties are only available on primary zones. For secondary zones, these properties are read-only.

The following table defines the items in the DNS Notify dialog box:

Item	Details
Automatically notify	When this option is selected, it specifies that the indicated secondary servers are to be notified of zone updates.
Servers listed on the Name Servers tab	When this option is selected, it specifies that all secondary servers are to be notified of zone updates.
The following servers	When this option is selected, it lists the secondary servers that are notified of zone updates. To add a server to the list, click the list, type the IP address or Domain Name System (DNS) name of the server, and click the list again to resolve and verify the server.

Configuring Secondary Name Servers
Using the Windows interface:

1. Open the DNS Manager.
2. In the console tree, right-click the applicable zone, and click **Properties**.
3. Click the **Name Servers** tab.
4. Click **Add**.
5. Specify additional DNS servers by their names and IP addresses, and click **Add** to add them to the list.

Using a command line:

1. Open a Command Prompt.
2. Type the following, and press ENTER:

    dnscmd *ServerName* **/RecordAdd** *ZoneNameNodeName* [**/Aging**] [**/OpenAcl**] [*Ttl*] **NS** {*HostName*|*DomainName*}

The following table describes the options for the ***dnscmd*** command:

Value	Description
dnscmd	Specifies the name of the command-line tool.
ServerName	Required. Specifies the DNS host name of the DNS server. You can also type the IP address of the DNS server. To specify the DNS server on the local computer, you can also type a period (.).
/RecordAdd	Required. Specifies the command to add a resource record.
ZoneName	Required. Specifies the fully qualified domain name (FQDN) of the zone.
NodeName	Required. Specifies the FQDN of the node in the DNS namespace for which the start-of-authority (SOA) record is added. You can also type the node name relative to the *ZoneName* or @, which specifies the zone's root node.
/Aging	If this command is used, this resource record is able to be aged and scavenged. If this command is not used, the resource record remains in the DNS database, unless it is manually updated or removed.
/OpenAcl	Specifies that new records are open to modification by any user. Without this parameter, only administrators may modify the new record.
Ttl	Specifies the Time-To-Live (TTL) setting for the resource record. (The default TTL is defined in SOA resource record.)
NS	Required. Specifies that you are adding a name server (NS) resource record to the zone that is specified in *ZoneName*.
HostName|FQDN	Required. Specifies the host name or FQDN of the new authoritative server.

Configure DNS Application Directory Partitions
Using the Windows interface

1. Open the DNS Manager.
2. In the console tree, right-click the applicable DNS server.
3. Click **Create Default Application Directory Partitions**.
4. Follow the instructions to create the DNS application directory partitions.

The following table describes the options available when creating the DNS default application directory partitions:

Option	Partition name	Description
Create a single application directory partition that stores DNS zone data and replicates that data to all DNS servers in the domain	DomainDnsZones.*DnsDomainName*	DNS application directory partition for each domain in the forest. DNS zones stored in this application directory partition are replicated to all DNS servers running on domain controllers in the domain.
Create a single application directory partition that stores DNS zone data and replicates that data to all DNS servers in the forest	ForestDnsZones.*DnsForestName*	DNS application directory partition for the entire forest. It contains all the DNS servers running on the domain controllers in the forest. DNS zones stored in this application directory partition are replicated to all DNS servers running on domain controllers in the forest.

Using a command line:

1. Open a Command Prompt.
2. Type the following, and press ENTER:
   dnscmd ServerName **/CreateBuiltinDirectoryPartitions** {**/Domain**|**/Forest**|**/AllDomains**}

The following table describes the options for the ***dnscmd*** command:

Value	Description
dnscmd	Specifies the name of the command-line tool.
ServerName	Required. Specifies the DNS host name of the DNS server. You can also type the IP address of the DNS server. To specify the DNS server on the local computer, you can also type a period (.).
/CreateBuiltin DirectoryPartitions	Required. Creates a default application directory partition.
{**/Domain**|**/Forest**|**/AllDomains**}	Required. Specifies which default application directory partition to create. Do one of the following: To create a default domain-wide DNS application directory partition for the AD DS domain where the specified DNS server is located, type **/Domain**. To create a default forest-wide DNS application directory partition for the AD DS forest where the specified DNS server is located, type **/Forest**. To create a default domain-wide DNS application directory partitions on a DNS server in each domain in the AD DS forest where the user running this command is logged on, type **/AllDomains**. The *ServerName* parameter is ignored for **/AllDomains**. The computer on which this command is run must be joined to a domain in the forest where you want to create all of the default domain-wide application directory partitions.

NOTES:

- By default, the DNS Server service will attempt to locate and create the default DNS application directory partitions in AD DS. If the DNS Server service is unable to do this, the administrator can manually create the application directory partitions using this procedure.
- If the default DNS application directory partitions are currently available in AD DS, the option to create the default application directory partitions in the DNS console will not be available.
- By default, the Net Logon service registers domain controller locator (Locator) DNS resource records for any application directory partitions hosted on a domain controller in the same manner as it registers domain controller locator (Locator) DNS resource records for any domain hosted on a domain controller. After the default DNS application directory partitions are created, Net Logon will register domain controller locator (Locator) DNS resource records on behalf of the domain controller hosting the default DNS application directory partitions.

Domain 2: Configuring the Active Directory Infrastructure

Windows Server 2008 has simplified the process of setting up a domain or forest. The basic steps are:

1. Design the domain or forest.
2. Configure DNS.
3. Deploy the first domain controller.
4. Adjust domain function levels, as needed.
5. Configure operations master roles, as needed.

Configure a forest or a domain

Performing an Unattended Installation

When you have to set up Active Directory on multiple computers, the easiest way to accomplish it is by running an unattended installation. This is done by running *Dcpromo.exe* along with an answer file; there are no requirements for the answer file name.

The syntax for the *Dcpromo.exe* command is:

> **dcpromo [/answer[:<filename>] | /unattend[:<filename>] | /unattend | /adv] /uninstal Binaries [/CreateDCAccount | /UseExistingAccount:Attach] /? /?[:{Promotion | CreateDC Account | UseExistingAccount | Demotion}]**

The following table defines the parameters for the *Dcpromo* command:

Parameter	Description
/answer[:<filename>]	Specifies an answer file that contains installation parameters and values.
/unattend[:<filename>]	Specifies an answer file that contains installation parameters and values. This provides the same function as /answer[:<filename>].
/unattend	Specifies an unattended installation in which you provide installation parameters and values at the command line.
/adv	Performs an install from media (IFM) operation.
/UninstallBinaries	Uninstalls AD DS binaries.
/CreateDCAccount	Creates a read-only domain controller (RODC) account. You must be a member of the Domain Admins group or the Enterprise Admins group to run this command.
/UseExistingAccount:Attach	Attaches a server to an existing RODC account. A member of the Domain Admins group or a delegated user can run this command.

The answer file can be created in any text editor, like Notepad. The essential configuration values needed in this file are:

- On the first line type [DCINSTALL] and press enter.
- The following entries must be on their own line:
    - InstallDNS=yes
    - NewDomain=forest
    - NewDomainDNSNae=<fully qualified DNS name>
    - DomainNetBiosName=<first label of the fully qualified DNS name, by default>
    - ReplicaOrNewDomain=domain
    - ForestLevel=<forest functional level number>
    - DomainLevel=<domain functional level number>
    - DatabasePath=<path to a folder on a local volume, surrounded by double
    - quotation marks>
    - RebootOnCompletion=yes
    - SYSVOLPath=<path to a folder on a local volume, surrounded by double quotation marks>
    - SafeModeAdminPassword=<password>

The ForestLevel function level numbers are:

- 0 = Windows 2000 Server
- 2 = Windows Server 2003
- 3 = Windows Server 2008

The DomainLevel function level numbers are:

- 0 = Windows 2000 Server native mode
- 2 = Windows Server 2003
- 3 = Windows Server 2008

Raising Forest and Domain Functional Levels

Functional levels determine the available Active Directory Domain Services (AD DS) domain or forest capabilities. They also determine which Windows Server operating systems you can run on domain controllers in the domain or forest. However, functional levels do not affect which operating systems you can run on workstations and member servers that are joined to the domain or forest.

When you deploy AD DS, set the domain and forest functional levels to the highest value that your environment can support. This way, you can use as many AD DS features as possible. For example, if you are sure that you will never add domain controllers that run Windows Server 2003 to the domain or forest, select the Windows Server 2008 functional level during the deployment process. However, if you might retain or add domain controllers that run Windows Server 2003, select the Windows Server 2003 functional level.

NOTE: After you raise the domain or forest functional level, you cannot go back to a lower functional level.

The following table explains the features that are available at each domain functional level.

Domain Function Level	Available Features	Supported Domain Controller Operating Systems
Windows 2000 Native	All of the default AD DS features and the following directory features are available: • Universal groups for distribution and security. • Group nesting. • Group conversion between security and distribution groups. • Security identifier (SID) history.	• Windows 2000 • Windows Server 2003 • Windows Server 2008
Windows Server 2003	All the default AD DS features, all the features that are available at the Windows 2000 native domain functional level, and the following features are available: • *Netdom.exe* • Logon time-stamp updates. • Able to set the *userPassword* attribute as the effective password on *inetOrgPerson* and user objects. • Able to redirect Users and Computers containers. • Authorization Manager is able to store its authorization policies in AD DS. • Constrained delegation. • Selective authentication.	• Windows Server 2003 • Windows Server 2008
Windows Server 2008	All of the default AD DS features, all of the features from the Windows Server 2003 domain functional level, and the following features are available: • Distributed File System (DFS) replication support for the Windows Server 2003 System Volume (SYSVOL). • Advanced Encryption Standard (AES 128 and AES 256) support Kerberos. • Last Interactive Logon Information. • Fine-grained password policies.	• Windows Server 2008

Important guidelines when raising domain or forest function levels:

- You can raise the domain functional level on the primary domain controller (PDC) emulator operations master only. The AD DS administrative tools that you use to raise the domain functional level (the Active Directory Domains and Trusts snap-in and the Active Directory Users and Computers snap-in) automatically target the PDC emulator when you raise the domain functional level.
- You can raise the forest functional level on the schema operations master only. Active Directory Domains and Trusts automatically target the schema operations master when you raise the forest functional level.
- You can raise the functional level of a domain only if all domain controllers in the domain run the version or versions of Windows that the new functional level supports.
- You can raise the functional level of a forest only if all domain controllers in the forest run the version or versions of Windows Server operating system that the new functional level supports.
- You cannot set the domain functional level to a value that is lower than the forest functional level.
- You cannot reverse the operation of raising the domain and forest functional levels. If you have to revert to a lower functional level, you must rebuild the domain or forest, or you must restore it from a backup copy.
- The first Windows Server 2008 domain controller that you deploy in your forest root domain sets the functional levels by default, unless otherwise specified in *Dcpromo*, to:
    - Windows 2000 forest functional level.
    - Windows 2000 native domain functional level.

Follow the following steps to raise the forest functional level:

1. To open the Active Directory Domains and Trusts snap-in, click **Start**, click **Administrative Tools**, and then click **Active Directory Domains and Trusts**.
2. In the console tree, right-click **Active Directory Domains and Trusts**, and click **Raise Forest Functional Level**.
3. In **Select an available forest functional level**, do one of the following:
    a. To raise the forest functional level to Windows Server 2003, click Windows Server 2003, and then click **Raise**.
    b. To raise the forest functional level to Windows Server 2008, click Windows Server 2008, and then click **Raise**.

NOTE: Do not raise the forest functional level to Windows Server 2008 if you have, or will have, any domain controllers running Windows Server 2003 or earlier.

Follow the steps below to raise the domain functional level:

1. To open the Active Directory Domains and Trusts snap-in, click **Start**, click **Administrative Tools**, and then click **Active Directory Domains and Trusts**.
2. In the console tree, right-click the domain for which you want to raise functional level, and click **Raise Domain Functional Level**.

3. In **Select an available domain functional level**, do one of the following:
   a. To raise the domain functional level to Windows Server 2003, click Windows Server 2003, and then click **Raise**.
   b. To raise the domain functional level to Windows Server 2008, click Windows Server 2008, and then click **Raise**.

NOTE: Do not raise the domain functional level to Windows Server 2003 or Windows Server 2008 if you have, or will have, any domain controllers running earlier versions of Windows Server.

Configuring Alternate User Principal Name (UPN) Suffix

Follow the steps below to configure additional UPN suffixes:

1. Open the **Active Directory Domains and Trusts** snap-in.
2. In the left pane, right-click **Active Directory Domains and Trusts** and select **Properties**.
3. Under **Alternate UPN suffixes**, type the name of the suffix you want to add.
4. Click **Add** and **OK**.
5. Repeat steps three and four to add additional UPN suffixes.

Preparing Windows 2000 and Server 2003 Servers for Windows Server 2008 AD DS

To prepare exiting domains running earlier versions of Windows, you will need to extend the existing Active Directory schema and update permissions before adding a domain controller running Windows Server 2008. This is done by running the *Adprep.exe* command-line tool found on the Windows Server 2008 installation disk in the *\sources\adprep* folder. *Adprep* can only be run from an elevated command prompt.

The syntax for Adprep is:

adprep {/forestprep | /domainprep | /domainprep /gpprep | /rodcprep | /wssg | /silent }

The following table defines the parameters for the Adprep command:

Parameter	Description
/forestprep	Prepares a forest for the introduction of a domain controller that runs Windows Server 2008. You run this command only once in the forest. You must run this command on the domain controller that holds the schema operations master role (also known as flexible single master operations or FSMO) for the forest.
/domainprep	Prepares a domain for the introduction of a domain controller that runs Windows Server 2008. You run this command after the **forestprep** command finishes and after the changes replicate to all the domain controllers in the forest. Run this command in each domain where you plan to add a domain controller that runs Windows Server 2008. You must run this command on the domain controller that holds the infrastructure operations master role for the domain.

Table continued on next page

/domainprep /gpprep	Performs similar updates as **domainprep**. However, this command also provides updates that are necessary to enable Resultant Set of Policy (RSOP) Planning Mode functionality. In Active Directory environments that run Microsoft Windows 2000, this command performs updates during off-peak hours. This minimizes replication traffic that is created in those environments by updates to file system permissions and Active Directory permissions on existing Group Policy objects (GPOs). This command is also available on Microsoft Windows Server 2003 with Service Pack 1 (SP1) or later. Run this command after the **forestprep** command finishes and after the changes replicate to all domain controllers in the forest. You must run this command on the infrastructure master for the domain.
/rodcprep	Updates permissions on application directory partitions to enable replication of the partitions to read-only domain controllers (RODCs). This operation runs remotely; it contacts the infrastructure master in each domain to update the permissions. You need to run this command only once in the forest. However, you can rerun this command any time if it fails to complete successfully because an infrastructure master is not available. This command can be run on any computer in the forest.
/wssg	Returns an expanded set of exit codes, instead of just 0 (success) and 1 (failure).
/silent	Specifies that no standard output is returned from an operation. This parameter can be used only if **/wssg** is also used.
quit	Returns to the prior menu.

NOTE: If you run *Adprep* on a domain controller running Windows 2000 Server, the domain controller must be running Windows 2000 Server Service Pack 4 (SP4) or later.

The following table lists exit codes that *Adprep* can return after an operation completes.

Return Code	Description
0	Success
1	Failure
2	Schema conflict error
3	FSMO role error
4	Connection error
5	Schema upgrade error
6	Unable to modify error
7	Server busy error

Table continued on next page

8	Permission error
9	Unable to initialize log file error
10	Not a domain controller
11	In nonnative mode
12	Need to run forest update first
13	Forest update already done
14	Domain update already done
15	GPO update already done
16	Forest update wait replication

Removing a Windows Server 2008 Domain Controller

The process for removing an instance of AD DS is relatively simple. You can select from three different methods: the Windows interface, unattended with an answer file, and the command line. However, if you are running an instance of Server Core you must use the unattended method.

Follow the steps below to remove a domain controller by using the Windows interface:

1. Click **Start**; click **Run**; type **dcpromo**, and press ENTER.
2. In the **Welcome to the Active Directory Domain Services Installation Wizard** page, click **Next**.
3. If the domain controller is a global catalog server, a message appears to warn you about the effect of removing a global catalog server from the environment. Click **OK** to continue.
4. On the **Delete the Domain** page, make no selection, and click **Next**.
5. If the domain controller has application directory partitions, on the **Application Directory Partitions** page, view the application directory partitions in the list, and remove or retain application directory partitions, as follows:
    a. If you do not want to retain any application directory partitions that are stored on the domain controller, click **Next**.
    b. If you want to retain an application directory partition that an application has created on the domain controller, use the application that created the partition to remove it, and then click **Refresh** to update the list.
6. If the **Confirm Deletion** page appears, select the option to delete all application directory partitions on the domain controller, and click **Next**.
7. On the **Remove DNS Delegation** page, verify that the **Delete the DNS delegations pointing to this server** check box is selected, and click **Next**.
8. If necessary, enter administrative credentials for the server that hosts the DNS zones that contain the DNS delegation for this server, and click **OK**.
9. On the **Administrator Password** page, type and confirm a secure password for the local Administrator account, and click **Next**.

10. On the **Summary** page, to save the settings that you selected to an answer file that you can use to automate subsequent Active Directory Domain Services (AD DS) operations, click **Export settings**. Type a name for your answer file, and click **Save**. Review your selections, and click **Next** to remove AD DS.
11. On the **Completing the Active Directory Domain Services Installation Wizard** page, click **Finish**.
12. You can either select the **Reboot on completion** check box to have the server restart automatically, or you can restart the server to complete the AD DS removal when you are prompted to do so.

Follow the steps below to remove a domain controller by using the unattended method:

1. Open Notepad or any text editor.
2. On the first line, type [DCINSTALL], and press ENTER.
3. Create the following entries, one entry on each line:
    a. username=<administrative account in the domain>
    b. userdomain=<domain name of administrative account>
    c. password=<password for the account in UserName>
    d. administratorpassword=<local administrator password for server>
    e. removeapplicationpartitions=yes
    f. removeDNSDelegation=yes
    g. DNSDelegationUserName=<DNS server administrative account for the DNS zone that contains the DNS delegation>
    h. DNSDelegationPassword=<Password for the DNS server administrative account>
4. Save the answer file to the location on the installation server from which it is to be called by **dcpromo**, or save the file to a network shared folder or removable media for distribution.
5. The **dcpromo** command to use an answer file is the same for both removing and installing a domain controller.

Follow the process below to remove a domain controller by using the command prompt:

- At a command prompt, the *dcpromo* command uses the same parameters that you would use in an unattended operation. The following table details the new options for removing AD DS from a server:

Parameter	Possible Values	Default Value	Description
/Administrator-Password	n/a	n/a	Sets the local administrator password for the computer during removal of a domain controller.
/DemoteFSMO	Yes | No	No	Indicates that a forced removal should continue, even if an operations master role is held by the domain controller.
/DNSDelegation-Password	*password* | *	n/a	Specifies the password for the user name (the account credentials) that is used to create or remove the DNS delegation. Specify * to prompt the user to enter credentials.
/DNSDelegation-UserName	n/a	n/a	Specifies the user name to be used when the DNS delegation is created or removed. If you do not specify a value, then the account credentials that you specify for the AD DS installation or removal are used for the DNS delegation.
/IgnoreIsLastDcIn-DomainMismatch	Yes | No	No	Specifies whether to continue the demotion of the domain controller when either the switch /IsLastDCInDomain:Yes is specified and Dcpromo detects that there is actually another active domain controller in the domain, or when the switch /IsLastDCInDomain:No is specified and Dcpromo cannot contact any other domain controller in the domain.
/IgnoreIsLast-DNSServerForZone	Yes | No	No	Specifies whether to continue the demotion even when the domain controller is the last DNS server for one or more Active Directory-integrated DNS zones that it hosts.
/IsLastDCInDomain	Yes | No	No	Specifies whether the computer that is being demoted is the last domain controller in the domain.
/Password	*Password* | *	n/a	Specifies the password corresponding to the user name (account credentials) that is used to promote the domain controller. Specify * to prompt the user to enter credentials.

Table continued on next page

/RebootOn-Completion	Yes | No	Yes	Specifies whether to restart the computer upon completion, regardless of success.
/RebootOnSuccess	Yes | No | NoAndNo-PromptEither	Yes	Specifies whether to restart the computer upon successful completion of an operation.
/Remove-ApplicationPartitions	Yes | No	No	Specifies whether to remove application directory partitions during removal of a domain controller.
/RemoveDNS-Delegation	Yes | No	Yes	Specifies whether to remove DNS delegations that point to this DNS server from the parent DNS zone.
/RetainDCMetadata	Yes | No	No	Retains domain controller metadata in the domain, after AD DS removal, to allow a delegated administrator to remove AD DS from an RODC.
/UserDomain	*domain_ name*	n/a	Specifies the domain name for the user name (account credentials) used for promoting a domain controller.
/UserName	*Domain\ user_name*	n/a	Specifies the user name (account credentials) used for promoting a domain controller. We recommend that you specify the account credentials in the domain\ user_name format.

Configure trusts

Understanding Trusts

In Windows Server 2008 you can use either the New Trust Wizard or the Netdom command-line tool to create four trust types: forest, external, shortcut and realm trusts. These trust types are described in the following table:

Trust Type	Transitivity	Direction	Description
Forest	Transitive	One-way or two-way	Use forest trusts to share resources between forests. If a forest trust is a two-way trust, authentication requests that are made in either forest can reach the other forest.
External	Nontransitive	One-way or two-way	Use external trusts to provide access to resources that are located on a Windows NT 4.0 domain or a domain that is located in a separate forest that is not joined by a forest trust.
Shortcut	Transitive	One-way or two-way	Use shortcut trusts to improve user logon times between two domains within a Windows Server 2008 forest. This is useful when two domains are separated by two domain trees.
Realm	Transitive or nontransitive	One-way or two-way	Use realm trusts to form a trust relationship between a non-Windows Kerberos realm and a Windows Server 2008 domain.

Forest Trusts

Follow the steps below to create a forest trust:

1. Open Active Directory Domains and Trusts. To open Active Directory Domains and Trusts, click **Start**; click **Administrative Tools**, and then click **Active Directory Domains and Trusts**.
2. In the console tree, right-click the domain that you want to administer, and then click **Properties**.
3. On the **Trusts** tab, click **New trust**, and then click **Next**.
4. On the **Trust Name** page, type the Domain Name System (DNS) name (or NetBIOS name) of the domain, and click **Next**.
5. On the **Trust Type** page, click **Forest trust**, and then click **Next**.
6. On the **Direction of Trust** page, do one of the following:
    a. To create a two-way forest trust, click **Two-way**.
        - Users in this forest and users in the specified forest will be able to access resources in either forest.
    b. To create a one-way incoming forest trust, click **One-way:incoming**.
        - Users in the specified forest will not be able to access any resources in this forest.

c. To create a one-way outgoing forest trust, click **One-way:outgoing**.
   - Users in this forest will not be able to access any resources in the specified forest.

7. Continue to follow the instructions in the wizard.

NOTES:

- If you have the appropriate administrative credentials for each forest, you can create both sides of a forest trust at the same time by clicking **Both this domain and the specified domain** on the **Sides of Trust** page.
- If you want users from the specified forest to have access to all computers in the local forest, on the **Outgoing Trust Properties** page, click **Forest-wide authentication**. This option is preferred when both forests belong to the same organization.
- If you want to selectively limit authentication to particular users and groups from the specified forest, on the **Outgoing Trust Properties** page, click **Selective authentication**. This option is preferred if the specified forest belongs to a separate organization.

External Trusts

Follow the steps below to create an external trust using the Windows interface:

1. Open Active Directory Domains and Trusts. To open Active Directory Domains and Trusts, click **Start**; click **Administrative Tools**, and then click **Active Directory Domains and Trusts**.
2. In the console tree, right-click the domain node for the domain that you want to establish a trust with, and then click **Properties**.
3. On the **Trusts** tab, click the **New Trust**, and then click **Next**.
4. On the **Trust Name** page, type the Domain Name System (DNS) name (or NetBIOS name) of the domain, and click **Next**.
5. On the **Trust Type** page, click **External trust**, and then click **Next**.
6. On the **Direction of trust** page, do one of the following:
   a. To create a two-way external trust, click **Two-way**.
      - Users in this domain and users in the specified domain will be able to access resources in either domain.
   b. To create a one-way incoming external trust, click **One-way:incoming**.
      - Users in the specified domain will not be able to access any resources in this domain.
   c. To create a one-way outgoing external trust, click **One-way:outgoing**.
      - Users in this domain will not be able to access any resources in the specified domain.
7. Continue to follow the instructions in the wizard.

Follow the steps below to create an external trust using a command prompt:

1. Open a command prompt. To open a command prompt, click **Start**; click **Run**; type **cmd**, and then click **OK**.
2. Type the following command, and press **ENTER**:
    a. **netdom trust <TrustingDomainName> /d:<TrustedDomainName> /add**

The following table describes the *Netdom* command parameters:

Parameter	Description
netdom trust	Manages or verifies the trust relationship between domains.
<TrustingDomainName>	Specifies the DNS name (or NetBIOS name) of the trusting domain in the trust that is being created.
/d:	Specifies that the DNS domain name that follows is a trusted domain.
<TrustedDomainName>	Specifies the DNS name (or NetBIOS name) of the domain that will be trusted in the trust that is being created.
/add	Specifies that a trust be created.

Shortcut Trusts

Follow the steps below to create a shortcut trust using the Windows interface:

1. Open Active Directory Domains and Trusts. To open Active Directory Domains and Trusts, click **Start**; click **Administrative Tools**, and then click **Active Directory Domains and Trusts**.
2. In the console tree, right-click the domain node for the domain with which you want to establish a shortcut trust, and then click **Properties**.
3. On the **Trusts** tab, click **New Trust**, and then click **Next**.
4. On the **Trust Name** page, type the Domain Name System (DNS) name (or NetBIOS name) of the domain, and click **Next**.
5. On the **Direction of Trust** page, do one of the following:
    a. To create a two-way shortcut trust, click **Two-way**.
        - Users in this domain and users in the specified domain will be able to use this trust path.
    b. To create a one-way incoming shortcut trust, click **One-way:incoming**.
        - Users in the specified domain will not be able to use this trust path.
    c. To create a one-way outgoing shortcut trust, click **One-way:outgoing**.
        - Users in this domain will not be able to use this trust path.
6. Continue to follow the instructions in the wizard.

NOTE: The process for creating a shortcut trust using the *Netdom* command is the same one that you would use when creating an external trust.

Realm Trusts

Follow the steps below to create a realm trust using the Windows interface:

1. Open Active Directory Domains and Trusts. To open Active Directory Domains and Trusts, click **Start**; click **Administrative Tools**, and then click **Active Directory Domains and Trusts**.
2. In the console tree, right-click the domain that you want to administer, and then click **Properties**.
3. On the **Trusts** tab, click **New trust**, and then click **Next**.
4. On the **Trust Name** page, type the realm name for the target realm, and click **Next**.
5. On the **Trust Type** page, select the **Realm trust** option, and click **Next**.
6. On the **Transitivity of Trust** page, do one of the following:
    a. To form a trust relationship with the domain and the specified realm, click **Nontransitive**, and then click **Next**.
    b. To form a trust relationship with the domain and the specified realm and all trusted realms, click **Transitive**, and then click **Next**.
7. On the **Direction of Trust** page, do one of the following:
    a. To create a two-way realm trust, click **Two-way**.
        - Users in this domain and users in the specified realm will be able to access resources in either domain or realm.
    b. To create a one-way incoming realm trust, click **One-way:incoming**.
        - Users in the specified realm will not be able to access any resources in this domain.
    c. To create a one-way outgoing realm trust, click **One-way:outgoing**.
        - Users in this domain will not be able to access any resources in the specified realm.
8. Continue to follow the instructions in the wizard.

Follow the steps below to create a realm trust from the command line:

1. Open a command prompt. To open a command prompt, click **Start**; click **Run**; type **cmd**, and click **OK**.
2. Type the following command, and press ENTER:

    netdom trust <TrustingDomainName> /d:<TrustedDomainName> /add /realm /PasswordT :<NewRealmTrustPassword>.

The following table describes the additional parameters in the *Netdom* command:

Parameter	Description
/realm	Indicates that the trust is to be created to a non-Windows Kerberos realm.
/PasswordT:	Specifies the new trust password. This parameter is valid only if one of the domains specified is a non-Windows Kerberos realm.
<NewRealm-TrustPassword>	Specifies the trust password for the new realm trust. This password must match the password that is used in the Kerberos realm.

Configure sites

Follow the steps below to create a site:

1. Open Active Directory Sites and Services. To open Active Directory Sites and Services, click **Start**; click **Administrative Tools**, and then click **Active Directory Sites and Services**.
2. In the console tree, right-click **Sites**, and then click **New Site**.
3. In **Name**, type the name of the new site.
4. In **Link Name**, click a site link object, and then click **OK**.

NOTE: Microsoft recommends that you use valid DNS names when you create new site names. Otherwise, your site will be accessible only where there is a Microsoft DNS server.

Follow the steps below to create a subnet:

1. Open Active Directory Sites and Services. To open Active Directory Sites and Services, click **Start**; click **Administrative Tools**, and then click **Active Directory Sites and Services**.
2. In the console tree, double-click **Sites**; right-click **Subnets**, and then click **New Subnet**.
3. In **Prefix**, type the IP version 4 (IPv4) or IP version 6 (IPv6) subnet prefix.
4. In **Select a site object for this prefix**, click the site to associate with this subnet, and click **OK**.

Follow the steps below to create a site link:

1. Open Active Directory Sites and Services. To open Active Directory Sites and Services, click **Start**; click **Administrative Tools**, and then click **Active Directory Sites and Services**.
2. In the console tree, right-click the intersite transport protocol, IP or SMTP that you want the site link to use.
3. Click **New Site Link**.
4. In **Name**, type the name for the site link.
5. In **Sites not in this site link**, click a site to add to the site link, and then click **Add**. Repeat to add more sites to the site link. To remove a site from the site link, in **Sites in this link**, click the site, and then click **Remove**.
6. When you have added the sites that you want to be connected by this site link, click **OK**.

NOTE: Microsoft recommends the use of the IP intersite transport unless your network has remote sites where network connectivity is intermittent or end-to-end IP connectivity is not available. Simple Mail Transfer Protocol (SMTP) replication has restrictions that do not apply to IP replication.

Follow the steps below to configure the site link costs:

1. Open Active Directory Sites and Services.
2. Expand the **Sites** container and the **Inter-Site Transports** container, and click the **IP** container.
3. In the details pane, right-click the Site Link object you want to configure, and then click **Properties**.
4. In the **Cost** box, specify the number for the comparative cost of using the site link, and click **OK**.

Configure Active Directory Replication

Distributed File System

DFS is installed as part of the file server role. Follow the steps below to configure DFS:

1. Click **Start**; point to **All Programs**; point to **Administrative Tools**, and click **Server Manager**.
2. In the console tree of Server Manager, right-click the **Roles** node, and then click **Add Roles**.
3. Select the **File Services** check box, and click **Next**.
4. Select the **Distributed File System** check box to install both DFS Namespaces and DFS Replication. To install DFS Namespaces or DFS Replication individually, select the check box that corresponds to the part of DFS that you want to install.
5. Select the **Create a namespace later using the DFS Management snap-in in Server Manager** check box.
6. Click **Install** to install the file server role and DFS.

A new DFS feature, supported only on Windows Server 2008, is access-based enumeration which allows users to see only files and folders on a file server to which they have access permission. To enable this feature you must type the following command at a command prompt:

dfsutil property able enable \\<namespace_root>

The following table details some of the *dsfutil* command parameters:

Parameter	Description
/map *DFSname**DFSshare*\ *path* *server**share**path*-[*comment*] [/restore]	Creates a DFS folder and assigns the specified shared folder as the folder target. When used with the **/restore** parameter, does not verify the existence of the shared folder.
/unmap \\DFSname\ DFSshare\path	Deletes a DFS folder and removes all of its folder targets.
/add \\DFSname\DFSshare\ path \\server\share-\path [/restore]	Adds a folder target to a DFS folder. When used with the **/restore** parameter, does not verify the existence of the shared folder.
/view \\DFSname\DFSshare [/partial | /full | /batch || / batchrestore]	Views all the DFS folders in the DFS namespace. Without arguments, views just the volume names. Additional parameters: • **/partial** - views comment also. • **/full** - displays a list of all the servers for a volume. • **/batch** - outputs a batch file to recreate the DFS. • **/batchrestore** - outputs a batch file to recreate the DFS using the /restore switch.
/move \\DFSname\DFSshare\ path1 \\DFSname\DFSshare\ path2 [/force]	Moves a folder that is in the DFS to a different logical path. With **/force**, replaces links that exist if necessary.

Bridgehead Servers

Use the Active Directory Sites and Services dialog box to configure bridgehead servers, as well as the replication protocol used for replication between the sites. By right-clicking on the selected server and selecting **Properties**, you can configure these options. The following table describes the options in the server properties dialog box:

Item	Details
Transports available for inter-site data transfer	Lists the replication transports that this server can use for replication. • **IP**: The IP transport is the default replication transport for intrasite and intersite replication. • **SMTP**: The Simple Mail Transfer Protocol (SMTP) transport uses e-mail messages to transfer replication data. Using this transport requires additional configuration in your network properties and has significant limitations.
This server is a preferred bridgehead server for the following transports	Contains the transports that you have added to designate this server as a preferred bridgehead server. By adding a transport to the list, you designate the server as a preferred bridgehead server for replications that use that transport. By removing a transport, you return the server to non–bridgehead-server status.

NOTES:

- Use the IP intersite transport unless your network has remote sites where network connectivity is intermittent or end-to-end IP connectivity is not available. Simple Mail Transfer Protocol (SMTP) replication has restrictions that do not apply to IP replication.
- You cannot configure a Windows Server 2008 RODC to be a bridgehead server for a site because RODC servers only perform inbound replication.

Replication Scheduling

Follow the steps below to configure the replication schedule:

1. Open Active Directory Sites and Services.
2. In the console tree, click the intersite transport folder, IP or SMTP that contains the site link for which you are configuring intersite replication availability.
3. In the details pane, right-click the site link whose schedule you want to configure, and click **Properties**.
4. In **Replicate every**, type or select the number of minutes between replications.
5. The **Replicate every** value will be processed as the nearest multiple of 15 minutes, ranging from a minimum of 15 minutes to a maximum of 10,080 minutes (1 week).

In Windows Server 2008, the *Repadmin* command-line tool can be used to view the replication metadata, view and manually create the replication topology, and force replication events between domain controllers. The format of the command is:

repadmin <cmd> <args> [/u:{domain\\user}] [/pw:{password|*}]
[/rpc] [/ldap] [/retry[:<retries>][:<delay>]]
[/csv] - see /csvhelp

Configure the global catalog

Universal Group Membership Caching

Follow the steps below to configure UGMC:

1. Open Active Directory Sites and Services.
2. Click to select a site object.
3. The NTDS Site Settings object for the site is visible in the details pane. Right-click the **NTDS Site Settings** object, and click **Properties**.
4. In the **NTDS Site Settings Properties** dialog box, click **Enable Universal Group Membership Caching**.

Create a Global Catalog Server

Follow the steps below to promote a server as a Global Catalog server:

1. Open Active Directory Sites and Services.
2. Expand the **Sites** until you locate the server that will become a **Global Catalog**.
3. Right-click the **NTDS Settings** icon under the server, and press **Properties**.
4. On the **General** tab, check the **Global Catalog** box, and click **OK**.

Configure operations masters

You must configure the operations master roles, or Flexible Single Master Operations (FSMOs), to ensure the availability and performance of the organization's domain controllers. Use the following guidelines when configuring operations master roles:

- Leave the operations master roles on the first domain controller in the regional domain.
- Monitor the regional domain controller closely to ensure that it is not a global catalog server.
- Deploy an additional domain controller to the domain to which you deployed the first domain controller. The additional domain controller acts as the standby operations master.
- Host the primary domain controller (PDC) emulator operations master role on a powerful and reliable domain controller to ensure that it is available and capable of handling the workload.

- The PDC emulator operations master role has the highest impact on the performance of the domain controller that hosts that role. In domains with more than 10,000 users, it might be necessary to reduce the number of authentication requests that are performed by the PDC emulator to decrease its workload and allow it to perform other tasks. If CPU utilization is higher than 50 percent or disk queues remain higher than 2 for several hours or days, reduce the number of client authentication requests that the PDC emulator receives.
- To reduce the number of client authentication requests that the PDC emulator receives, adjust the weight or priority of the PDC emulator in the DNS environment. To proportionately reduce the number of client authentication requests that the PDC emulator receives, you adjust its weight. To ensure that the PDC emulator does not receive any client authentication requests, you adjust its priority.
- AD DS assigns a default value of 100 for the weight. If you create a new registry entry for the weight and assign it a decreased value of 50, you proportionately reduce the number of client authentication requests that AD DS sends to the PDC emulator. This ensures that the PDC emulator authenticates half of the number of clients that it would if the weight value remained at 100.
- AD DS assigns a default value of zero for the priority. If you create a new registry entry for the priority and assign it an increased value of 200, you ensure that the PDC emulator receives client authentication requests only if it is the only accessible domain controller.
- Repeat these procedures if you transfer or seize the PDC emulator operations master role to another domain controller in the regional domain.

Extending the Schema

Follow the steps below to prepare the forest schema for Windows Server 2008:

1. Log on to the schema master as a member of the Enterprise Admins, Schema Admins, and Domain Admins groups.
2. Insert the Windows Server 2008 DVD into the CD or DVD drive. Copy the contents of the \sources\adprep folder to an Adprep folder on the schema master.
3. Open a command prompt, and change directories to the Adprep folder.
4. At the command prompt, type the following, and press ENTER: **adprep /forestprep**
5. If you plan to install an RODC in any domain in the forest, type the following, and press ENTER: **adprep /rodcprep.**
6. Allow the operation to complete, and then allow the changes to replicate throughout the forest before you prepare any domains for a domain controller that runs Windows Server 2008.

Transfer and Seize Operations Master Roles

Use the *Roles* subset of the *Ntdsutil* command to transfer and seize Operations Master roles. You must be at an elevated command prompt in order to run this command. The syntax of this command is:

connections
[select operation target] [{seize naming master | seize infrastructure master | seize PDC | seize RID master | seize schema master}] [{transfer naming master | transfer infrastructure master | transfer PDC | transfer RID master | transfer schema master}]

The following table describes the *Roles* parameters in the *Ntdsutil* command:

Parameter	Description
connections	Invokes the **Server connections** submenu.
seize naming master	Forces the domain controller to which you are connected to claim ownership of the naming master operations master role without regard to the data associated with the role. Use only for recovery purposes.
seize infrastructure master	Forces the domain controller to which you are connected to claim ownership of the infrastructure operations master role without regard to the data associated with the role. Use only for recovery purposes.
seize PDC	Forces the domain controller to which you are connected to claim ownership of the PDC operations master role without regard to the data associated with the role. Use only for recovery purposes.
seize RID master	Forces the domain controller to which you are connected to claim ownership of the relative ID master role without regard to the data associated with the role. Use only for recovery purposes.
seize schema master	Forces the domain controller to which you are connected to claim ownership of the schema operations master role without regard to the data associated with the role. Use only for recovery purposes.
select operation target	Invokes the **Select operation target** submenu.
transfer naming master	Instructs the domain controller to which you are connected to obtain the naming master role by means of controlled transfer.
transfer infrastructure master	Instructs the domain controller to which you are connected to obtain the infrastructure operations master role by means of controlled transfer.
transfer PDC	Instructs the domain controller to which you are connected to obtain the PDC operations master by means of controlled transfer.
transfer RID master	Instructs the domain controller to which you are connected to obtain the relative ID master role by means of controlled transfer.
transfer schema master	Instructs the domain controller to which you are connected to obtain the schema operations master role by means of controlled transfer.
quit	Takes you back to the previous menu or exits the utility.

Domain 3: 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.

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.

11. 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.
12. 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.
    - **NOTE**: 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))**

Table continued on next page

-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.

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.

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.

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 4: Creating and Maintaining Active Directory Objects

Automate creation of Active Directory accounts

Bulk Import

The quickest way to get a lot of account information into Active Directory is to use a bulk import tool. Windows Server 2008 utilizes the command-line tool, *csvde*, to accomplish this task. The syntax of csvde is:

Csvde [-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 used in csvde:

Parameter	Description
-i	Specifies import mode. If not specified, 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.
-c <String1> <String2>	Replaces all occurrences of *String1* with *String2*. Use this parameter to import data from one domain to another and to 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 is the current path.
-t <PortNumber>	Specifies an LDAP port. The default LDAP port is 389. The global catalog port is 3268.
-u	Specifies Unicode format.
-d <BaseDN>	Sets the distinguished name of the search base for data export.
-r <LDAPFilter>	Creates an LDAP search filter for data export.
-p <Scope>	Sets the search scope. Search scope options are Base, OneLevel, or SubTree.

Table continued on next page

-l <LDAPAttributeList>	Sets the list of attributes to return in the results of an export query. LDAP can return attributes in any order, and **csvde** does not attempt to impose any order on the columns. If you omit this parameter, AD DS returns all attributes.
-o <LDAPAttributeList>	Specifies the list of attributes to omit from the results of an export query. Use this parameter if you need to export objects from AD DS and then import them into another LDAP-compliant directory. If the other directory does not support certain attributes, you can use this parameter to omit those attributes from the result set.
-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. The following is a complete list of ignored errors: • Object already exists • Constraint violation • Attribute or value already exists
-a [<UserDistinguishedName> {<Password> | *}]	Performs a simple LDAP bind with the user name and password. Sets the command to run using the supplied *UserDistinguishedName* and *Password*. By default, the command runs using the credentials of the user who is currently logged on to the network.
-b [<UserName> <Domain> { <Password> | *}]	Performs a secure LDAP bind with the NEGOTIATE authentication method. Sets the command to run using the supplied *Username*, *Domain*, and *Password*. By default, the command will run using the credentials of the user who is currently logged on to the network.

Here is an example using csvde to import data to a current, logged domain from a file named input.csv:

```
csvde -i -f input.csv
```

Create Accounts
The process for creating new computer, user, or group accounts is very similar. You have two methods to choose from:

1. Use Active Directory Users and Computers.
2. Use the command-line tool dsadd.

The basic process for creating new accounts using the Windows interface is as follows:

1. To open Active Directory Users and Computers, click **Start**; click **Control Panel**; double-click **Administrative Tools**, and then double-click **Active Directory Users and Computers**.
2. In the console tree, right-click **Computers**. Or, right-click the folder in which you want to add the computer.
3. Point to **New**, and click **Computer**, **User**, or **Group**.
4. Type the computer, user, or group name.

NOTE: You can easily create template user accounts to simplify adding new users:

- Create several typical users reflecting various groups within your organization.
- Copy the user account most like the new account you want to create.
- Modify the attributes: name, e-mail address, logon name, etc.

Here is an example of creating a new user account from the command-line:

1. To open a command prompt, click **Start**; click **Run**; type **cmd**, and then click **OK**.
2. Type the following command, and press **Enter**:
   dsadd user <UserDN> [-samid<SAMName>] -pwd {<Password>|*}

The following table details the parameters of the dsadd command:

Parameter	Description
<UserDN>	Specifies the distinguished name of the user object to be added.
-samid	Sets <SAMName> value.
<SAMName>	Specifies the Security Accounts Manager (SAM) name as the unique SAM account name for this user (for example, Linda). If the SAM name is not specified, **dsadd** attempts to create the SAM account name using up to the first 20 characters from the common name (CN) value of *UserDN*. When creating a group, it specifies the Security Accounts Manager (SAM) name as the unique SAM account name for the group (for example, Operators).
-pwd	Sets <Password> value.
<Password>	Specifies the password to be used for the user account. If this parameter is set to *, you are prompted for a user password.
<ComputerDN>	Specifies the distinguished name of the computer that you want to add. The distinguished name specifies the directory location.
<GroupDN>	Specifies the distinguished name of the group object to be added.
-secgrp	Sets the value for the group type.

Table continued on next page

{yes|no}	Specifies whether the group that you want to add is a security group (yes) or a distribution group (no).
-scope	Sets the value for the group scope.
{l|g|u}	Specifies whether the scope of the group that you want to add is domain local (l), global (g), or universal (u).

The following is an example of using the dsadd command to create a computer account:

dsadd computer <ComputerDN>

The following is an example of using the dsadd command to create a security group account:

dsadd group "cn=Marketing,ou=Vancouver,dc=VancouverDC,dc=com" –samid Marketing –secgrp yes –scope g

The following is an example of using the dsadd command to create a distribution group:

dsadd group "cn=Managers,ou=Vancouver,dc=VancouverDC,dc=com" -samid Updates -secgrp no

UPN
The user principal name (UPN) is configured when creating or editing a user account in Active Directories Users and Computers under User Properties – Account Tab. Under the User logon name control, there is a drop-down list box on the right which lists the available UPN suffixes that may be used with the user logon name. The list contains the full Domain Name System (DNS) name of the current domain, the full DNS name of the root domain of the current forest, and any alternative UPN suffixes that are created through Active Directory Domains and Trusts.

Maintain Active Directory accounts

Configure Group Membership
Follow the steps below to configure a user's group membership:

1. Open **Active Directory Users and Computers**.
2. In the console tree, click **Users**.
3. In the details pane, right-click the user that you want to change, and then click **Properties**.
4. On the **Member Of** tab, click the group that you want to set as the user's primary group, and then click **Set Primary Group**.

When working with groups, Microsoft recommends using the AGDLP or the AGGUDLP method. AGDLP states that you place the account into a global group which is then added to a domain local group where permissions are assigned. AGGUDLP states that you place the account into a global group which is then added to a universal group that is placed into a domain local group where permissions are assigned.

Account Resets
The most common account reset involves resetting a users' password. Follow the steps below to reset a password from the Windows interface:

1. Open Active Directory Users and Computers.
2. In the console tree, click **Users**.
3. In the details pane, right-click the user whose password you want to reset, and then click **Reset Password**.
4. Type and then confirm the password.
5. If you want to require the user to change this password at the next logon process, select the **User must change password at next logon** check box.

You can also reset a password from the command line using the dsmod command:

dsmod user <UserDN> -pwd <NewPassword> -mustchpwd {yes|no}

The following table describes the parameters of the dsmod password reset command:

Parameter	Description
<UserDN>	Specifies the distinguished name of the user for which the password will be reset.
-pwd	Sets the <NewPassword>.
<NewPassword>	Specifies the password that will replace the current user password.
-mustchpwd	Sets the pwdExpired flag.
{yes|no}	Specifies the value of the pwdExpired flag.

Local Groups
A local group is a collection of user accounts or domain groups created on a member server of an AD DS domain or stand-alone server. You can create local groups to grant permissions for resources residing on the local computer. Local groups can contain local or domain user accounts, computers, global groups, and universal groups.

You cannot create local groups on AD DS domain controllers. Domain controllers do not have local users and groups, as the only security database located on a domain controller is the AD DS database.

Disabling Accounts
It is always preferable to disable an account as opposed to deleting the account. When an object is created, a unique security identifier (SID) is assigned to it. There is no way to re-create that SID once the object has been deleted, even if you give the object the same name. Therefore, unless you are absolutely certain that you will never need that SID again you should always disable accounts.

Follow the steps below to disable a user account using the Windows interface:

1. Open **Active Directory Users and Computers**.
2. In the console tree, click **Users**.
3. In the details pane, right-click the user.
4. Click **Disable Account.**

You can also disable an account from the command line using the dsmodd command:

dsmod user <UserDN> -disabled {yes|no}

The following table describes the parameters of the dsmod account disable command:

Parameter	Description
<UserDN>	Specifies the distinguished name of the user object to be added.
-disabled	Sets the value of UF_ACCTDISABLED in userAccountControl.
{yes|no}	Specifies whether the user account is disabled for logon (**yes**) or not (**no**).

Creating Organizational Units (OUs)
The following is an example of using the dsadd command to create an organizational unit:

dsadd ou "ou=Sales,dc=VancouverDC,dc=com" –desc "Sales Department" –d VancouverDC.com –u Administrator –p Pa$$w0rd

Delegation of Control
Follow the steps below to run the Delegation of Control Wizard:

1. Select the desired OU, and click the **Delegation** tab.
2. Click **Add**.
3. In the Select Users dialog box, type the user's name in the Object name field, and click **OK**.
4. In the Add Group or User dialog box, select **This container only**, and click **OK**.

Create and Apply Group Policy Objects (GPOs)

Enforce
Follow the steps below to enforce a GPO link:

1. In the **Group Policy Management Console** (GPMC) tree, double-click the forest containing the domain, site, or organizational unit (OU) having the link you want to enforce, and then do one of the following:
    a. To enforce a GPO link at the domain level, double-click **Domains**, and then double-click the domain containing the GPO link.
    b. To enforce a GPO link at the OU level, double-click **Domains**, double-click the domain containing the OU, and then double-click the OU containing the GPO link.
    c. To enforce a GPO link at the site level, double-click **Sites**, and double-click the site containing the GPO link.
2. Right-click the GPO link, and then click **Enforced** to enable or disable enforcing the link. A check mark next to **Enforced** indicates that the link is enforced.

OU Hierarchy
As with earlier Windows operating systems, Windows Server 2008 utilizes an OU hierarchy that affects Group Policy inheritance. By default, options set in GPOs linked to higher levels of Active Directory sites, domains, and OUs are inherited by all OUs at lower levels. However, inherited policy can be overridden by a GPO that is linked at a lower level.

An example of this would be when an administrator utilizes this process to control desktops at different OU levels. The process would work this way: utilize a GPO linked at a high level OU to establish the standard desktop features. Then link a second GPO to a lower-level OU with different desktop features. Because lower-level GPOs are applied last, the second GPO will override the domain-level GPO and provide that specific lower-level OU with a different set of Group Policy settings. However, you can modify this default inheritance behavior by using Block Inheritance and Enforced.

Block Inheritance
You can block inheritance for a domain or organizational unit. Blocking inheritance prevents Group Policy objects (GPOs) that are linked to higher sites, domains, or organizational units from being automatically inherited by the child-level.

Follow the steps below to block inheritance:

1. In the **Group Policy Management Console** (GPMC) tree, double-click the forest containing the domain or organizational unit (OU) for which you want to block inheritance for GPO links, and then do one of the following:
    a. To block inheritance of the GPO links of an entire domain, double-click **Domains**, and then right-click the domain.
    b. To block inheritance for an OU, double-click **Domains**; double-click the domain containing the OU, and then right-click the OU.
2. Click **Block Inheritance**.

Group Policy Processing Priority
In Windows Server 2008, like earlier Windows operating systems, it is important to remember that by default GPOs are inherited, cumulative, and affect all computers and users in an Active Directory container and its children. GPOs are processed in the following order: Local Group Policy, site, domain, and then OU, with the last GPO processed overriding the earlier GPOs. The default inheritance method is to evaluate Group Policy starting with the Active Directory container farthest from the computer or user object. The Active Directory container closest to the computer or user overrides Group Policy set in a higher-level Active Directory container unless you set the *Enforced (No Override)* option for that GPO link or if the *Block Policy Inheritance* policy setting has been applied to the domain or OU. The local group policy object is processed first, so policy settings from GPOs linked to Active Directory containers override the local policy settings.

For this exam, you should also remember that although you can link more than one GPO to an Active Directory container, you need to be aware of the processing priority. The GPO link with the lowest link order in the Group Policy Object Links list (displayed in the *Linked Group Policy Objects* tab in the GPMC) has precedence by default. However, if one or more GPO links have the *Enforced* option set, the highest GPO link set to *Enforced* takes precedence.

Remember, *Enforced* is a link property, and *Block Policy Inheritance* is a container property. Enforced takes precedence over Block Policy Inheritance. In addition, you can disable policy settings on the GPO itself in four other ways: a GPO can be disabled, have its computer settings disabled, have its user settings disabled, or have all of its settings disabled.

Windows Management Instrumentation (WMI)
Windows Management Instrumentation (WMI) filters allow you to dynamically determine the scope of Group Policy Objects (GPOs), based on attributes of the target computer.

When a GPO that is linked to a WMI filter is applied on the target computer, the filter is evaluated on the target computer. If the WMI filter evaluates to false, the GPO is not applied (unless the client computer is running Windows 2000, in which case the filter is ignored and the GPO is always applied). If the WMI filter evaluates to true, the GPO is applied.

Follow the steps below to link a WMI filter to a GPO:

1. In the Group Policy Management Console (GPMC) tree, double-click **Group Policy Objects** in the forest and domain containing the Group Policy Object (GPO) to which you want to link a WMI filter.
2. Click the GPO.
3. In the results pane on the **Scope** tab, under **WMI Filtering**, select a WMI filter from the drop-down list.
4. When prompted to confirm the selection, click **Yes**.

Group Policy Filtering
Follow the steps below to filter GPOs using security groups:

1. In the Group Policy Management Console (GPMC) tree, expand **Group Policy Objects** and click the Group Policy Object (GPO) to which you want to apply security filtering.
2. In the results pane on the **Scope** tab, click **Add**.
3. In the **Enter the object name to select** box, type the name of the group, user, or computer that you want to add to the security filter. Click **OK**.

Group Policy Loopback
In Windows Server 2008, administrators can use the Group Policy loopback feature to apply GPOs that depend only on which computer the user logs on to. Loopback operates using the following two modes:

- Merge mode
- Replace mode

Follow the steps below to set user configuration per computer:

1. In the Group Policy Microsoft Management Console (MMC), click **Computer Configuration**.
2. Locate **Administrative Templates**; click **System**; click **Group Policy**, and enable the **Loopback Policy** option.

Configure GPO templates

ADMX Central Store
The central store is a folder structure created in the Sysvol directory on the domain controllers in each domain in an organization. The central store only needs to be created once on a single domain controller for each domain in the organization. The File Replication service replicates the central store to all domain controllers in a domain. Microsoft recommends that you create the central store on the primary domain controller. Group Policy Management Console and Group Policy Object Editor can use ADMX files more quickly because Group Policy tools connect to the primary domain controller by default.

Follow the steps below to create the central store:

1. Create the root folder for the central store on the domain controller:

   *%systemroot%***sysvol\domain\policies\PolicyDefinitions**
2. Create a subfolder of *%systemroot%***sysvol\domain\policies\PolicyDefinitions** for each language the Group Policy administrators will use. Each subfolder is named after the appropriate ISO-style Language/Culture Name. For example, to create a subfolder for United States English, create the subfolder:

   *%systemroot%***sysvol\domain\policies\PolicyDefinitions\EN-US**.

Follow the steps below to populate the central store with ADMX files:

1. At a command prompt, type the following to copy all language-neutral ADMX files (.admx) from an administrative workstation to the central store on the domain controller:

   copy *%systemroot%***PolicyDefinitions*** *%logonserver%***sysvol***%userdnsdomain%***policies\PolicyDefinitions**
2. At a command prompt, type the following to copy all ADMX language-specific resource files (.adml) from an administrative workstation to the central store on the domain controller:

   copy *%systemroot%***PolicyDefinitions***[MUIculture]****** *%logonserver%***sysvol***%userdnsdomain%***policies\PolicyDefinitions***[MUIculture]***
3. For example, to copy all United States English .adml files, type the following:

   copy *%systemroot%***PolicyDefinitions\EN-US*** *%logonserver%***sysvol***%userdnsdomain%***policies\PolicyDefinitions\EN-US**

Administrative Templates
Follow the steps below to edit Administrative Templates policy settings:

1. Open the Group Policy Management Console. Right-click the Group Policy object you want to edit, and click **Edit**.
2. In the console tree, click the folder under **Administrative Templates** that contains the policy settings you want to set.
3. In the **Setting** column, click the name for a policy setting to read a description of the policy setting.
4. To change that policy setting from its default (not configured) state, double-click the name of the policy setting.
5. On the **Setting** tab, click one of the following:
    a. **Not Configured**: The registry is not modified.
    b. **Enabled**: The registry reflects that the policy setting is selected.
    c. **Disabled**: The registry reflects that the policy setting is not selected.
6. Select any other available options that you want on the **Setting** tab, and click **OK**.

Security Templates
Follow the steps below to create a security template for the file and print servers:

1. Click **Start**; click **Run**, and type **MMC**.
2. Add the snap-in for **Security Templates**.
3. Expand **Security Templates**; right-click **C:\Users\Administrators\Documents\Security\Templates**, and then click **New Template**.
4. Give the new template an appropriate name.
5. Navigate to **Local Policies, Security Options**. Define the **Accounts: Rename administrator account** with the value **FPAdmin**.
6. Define the **Interactive Logon: Do not display last user name** to either **Enabled** or **Disabled**.
7. In the folder pane, right-click the name of the template that you created, and then click **Save**.
8. Close the MMC console.

Restricted Groups
Configure restricted groups for the local administrators group:

1. Open the **Group Policy Management Console**.
2. Open the **Group Policy Objects** folder, and edit the **Default Domain Policy**.
3. Navigate to **Windows Settings, Security Settings**; right-click **Restricted Groups**, and then click **Add Group**.
4. Add the **Administrators** group, and click **OK**.
5. In the **Administrators Properties** dialog box, add the desired groups.
6. Close the Group Policy Management Editor.

Starter GPOs
Windows Server 2008 introduces the new Group Policy Management Console version 2. Included in this is a new container called Starter GPOs. Starter GPOs enable administrators to save baseline templates for use when creating new GPOs. These templates can also be exported to other domains.

Follow the steps below to create a Starter GPO:

1. Open the **Group Policy Management Console**.
2. Right-click **Starter GPOs**, and then click **New**.
3. In the **New Starter GPO** dialog box, type the name of the Starter GPO in the **Name** box. Optionally, you can type comments in the **Comments** box.
4. Click **OK**.

NOTE: Do not confuse Starter GPOs with System Starter GPOs. Both derive from a GPO and provide the ability to store a collection of Administrative Template policy settings in a single object. However, System Starter Group Policy objects are read-only Starter GPOs that provide a baseline of settings for a specific scenario.

Configure software deployment GPOs

Windows Server 2008 includes a feature called Software Installation and Maintenance that uses AD DS and Group Policy and the Microsoft Windows Installer service to install, maintain, and remove software on your organization's computers.

To enable Group Policy to deploy and manage software, Windows Server 2008 uses the Windows Installer service. This component automates the installation and removal of applications by applying a set of centrally defined setup rules during the installation process.

- Software can be categorized in the Add Program applet.
- File extensions can be associated with particular applications.
- Software deployment can be customized using MST files.

Publishing to Users
Follow the steps below to publish an application:

1. Open Group Policy Software Installation.
2. Right-click in the details pane; point to **New**, and click **Package**.
3. In the **Open** dialog box, use the search boxes to find the package you want to publish; click the Windows Installer package to be published, and then click **Open**.
4. In the **Deploy Software** dialog box, click **Published**.

Assigning Software to Users
Follow the steps below to assign an application:

1. Open Group Policy Software Installation.
2. In the console tree, right-click **Software installation**; point to **New**, and click **Package**.
3. In the **Open** dialog box, use the search boxes to find the application you want to deploy; click the Windows Installer package, and then click **Open**.
4. In the **Deploy Software** dialog box, click **Assigned**, and then click **OK**.

Software Removal
Follow the steps below to remove a managed application:

1. Open Group Policy Software Installation.
2. In the details pane, right-click the application that you want to remove; point to **All Tasks**, and click **Remove**.
3. In the **Remove Software** dialog box, click one of the following removal methods:
    a. To specify that the application should be removed the next time a user logs on or restarts the computer, click **Immediately uninstall the software from users and computers**.
    b. To specify that users can continue to use the application if they have already installed it, click **Allow users to continue to use the software, but prevent new installations**. If users have removed the application or if they have never installed it, they will not be able to install it.

Configure account policies

Domain Password and Account Lockout Policy
Within Active Directory, Group Policy establishes and controls the Account Policies for the entire domain. The following table outlines the password, account lockout, and Kerberos settings:

Policies	Description
Password	• Enforce password history: 24 passwords • Max password age: 42 days • Min password age: 1 day • Min password length: 7 characters • Complex Password: enabled • Store password using reversible encryption: disabled
Account lockout	• Lockout duration: not defined • Lockout threshold: 0 invalid logon attempts • Reset account lockout after: not defined
Kerberos	• Can only be applied at the domain level

Fine-Grain Password Policies
In previous Windows operating systems you could apply only one password and account lockout policy to all users in the domain. Fine-grained password policies allow you to have different password requirements and account lockout policies for different Active Directory users or groups. This is desirable when you want different sets of users to have different password requirements but do not want separate domains. If you do not implement fine-grained passwords, then the normal, default domain account policies apply to all users.

There are three major steps involved in implementing fine-grained passwords:

1. Create necessary groups, and add the appropriate users.
2. Create PSOs for all defined password policies.
3. Apply PSOs to the appropriate users or global security groups.

Follow the steps below to create a PSO using ADSI Edit:

1. In the Run menu, type **adsiedit.msc**, and press **Enter**.
2. Right-click **ADSI Edit**; click **Connect to**, and then click **OK** to accept the defaults.
3. Navigate to the desired location. For example: *DC=VancouverDC, DC=com, CN=System, CN=Password Settings Container*. Right-click **CN=Password Settings Container**, and then create a new object.
4. In the Create Object dialog box click msDS-PasswordSettings, and then click Next.
5. In **Value**, type the group name.
6. In the **msDS-PasswordSettingsPrecedence**, type the desired value.
7. In the **msDS-PasswordReversibleEncryptionEnabled** value, type either **True** or **False**.
8. In the **msDS-PasswordHistoryLength**, type the desired value.
9. In the **msDS-PasswordComplexityEnabled**, type either **True** or **False**.
10. In the **msDS-MinimumPasswordLength**, type the desired value.
11. In the **msDS-MinimumPasswordAge**, type the desired value.
12. In the **msDS-MaximumPasswordAge**, type the desired value.
13. In the **msDS-LockoutThreshold**, type the desired value.
14. In the **msDS-LockoutObservationWindows**, type the desired value.
15. In the **msDS-LockoutDuration**, type the desired value.
16. Click **Finish**.

Follow the steps below to assign a PSO to a global group:

1. Open **Active Directory Users and Computers**.
2. Click **View**, and then click **Advanced Features**.
3. Expand the domain; expand **System**, and click **Password Settings Container**. In the details pane, right-click the desired PSO, and then click **Properties**.
4. Click the **Attribute Editor** tab. Scroll down; select the **msDS-PSOAppliesTo** attribute, and click **Edit**.
5. Add the desired global group.
6. Close **Active Directory Users and Computers**.

Configure audit policy by using GPOs

Audit Logon Events
Follow the steps below to configure auditing for logon events:

1. Open the **Group Policy Management Editor**.
2. Expand **Computer Configuration** | **Policies** | **Windows Settings** | **Security Settings** | **Local Policies**.
3. Click on **Audit Policy**.
4. Double-click on **Audit logon events** in the right-hand window to define the desired policy setting.

Audit Account Logon Events
Follow the steps below to configure auditing for account logon events:

1. Open the **Group Policy Management Editor**.
2. Expand **Computer Configuration** | **Policies** | **Windows Settings** | **Security Settings** | **Local Policies**.
3. Click on **Audit Policy**.
4. Double-click on **Audit account logon events** in the right-hand window to define the desired policy setting.
5. Click on **Define these policy settings**.
6. Under **Audit these attempts**, select one or both of the following:
    a. Success
    b. Failure

Audit Policy Change
Follow the steps below to configure auditing for policy change events:

1. Open the **Group Policy Management Editor**.
2. Expand **Computer Configuration** | **Policies** | **Windows Settings** | **Security Settings** | **Local Policies**.
3. Click on **Audit Policy**.
4. Double-click on **Audit policy change** in the right-hand window to define the desired policy setting.
5. Click on **Define these policy settings**.
6. Under **Audit these attempts**, select one or both of the following:
    a. Success
    b. Failure

Audit Access Privilege Use
Follow the steps below to configure auditing for privilege use events:

1. Open the **Group Policy Management Editor**.
2. Expand **Computer Configuration** | **Policies** | **Windows Settings** | **Security Settings** | **Local Policies**.
3. Click on **Audit Policy**.
4. Double-click on **Audit privilege use** in the right-hand window to define the desired policy setting.
5. Click on **Define these policy settings**.
6. Under **Audit these attempts**, select one or both of the following:
    a. Success
    b. Failure

Audit Directory Service Access
Enabling the global audit policy, Audit directory service access, enables all directory service policy subcategories. The global audit policy can be set in the Default Domain Controllers Group Policy (under Security Settings\Local Policies\Audit Policy). In Windows Server 2008, this global audit policy is enabled by default; therefore, the subcategory, Directory Service Changes, is also enabled by default. This subcategory is turned on only for success events.

Follow the steps below to configure directory service access auditing:

1. Open the **Group Policy Management Console**.
2. In the console tree, expand the forest to see the selected domain.
3. Right-click **Default Domain Policy**, and then click **Edit**.
4. In the console tree, expand **Computer Configuration | Windows Settings | Security Settings | Local Policies**, and click **Audit Policy**.
5. Set the **Audit directory services access Properties** to desired setting.
6. Set the **Audit object access Properties** to the desired setting.
7. Type the following at a command prompt to enable subcategories:

    auditpol /set /subcategory:"directory service changes" /success:enable

Audit Object Access
Follow the steps below to configure auditing for object access events:

1. Open the **Group Policy Management Editor**.
2. Expand **Computer Configuration** | **Policies** | **Windows Settings** | **Security Settings** | **Local Policies**.
3. Click on **Audit Policy**.
4. Double-click on **Audit object access** in the right-hand window to define the desired policy setting.
5. Click on **Define these policy settings**.
6. Under **Audit these attempts**, select one or both of the following:
    a. Success
    b. Failure

Domain 5: 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.

Table continued on next page

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.

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.

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.

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.

Table continued on next page

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.

Table continued on next page

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.

Table continued on next page

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.

Table continued on next page

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-Active-Directory_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.

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.)

Table continued on next page

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.

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.

Domain 6: 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

Table continued on next page

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

Table continued on next page

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

Table continued on next page

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

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.

8. Select one certificate and click **OK**. You may view the highlighted certificate to ensure that you have selected the intended certificate.
9. 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:
    1. Open the Certificate Services snap-in. Select an issued certificate.
    2. Double-click the certificate, and then click the **Details** tab.
    3. Scroll down and select the **CRL Distribution Points** field.
    4. Select and copy the URL for the CRL distribution point that you want to use.
    5. 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**.
11. 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**.

Practice Questions

Chapter 1

1. William is the network administrator for his company, an avionics research company based in Oklahoma City. The business' network consists of one Active Directory domain which is comprised of 5 servers running Windows Server 2008 and 65 workstations running Windows Vista. Of the 5 servers William manages, three of them are domain controllers all running DNS. William is on vacation when one of his junior systems administrators tells him that the domain controllers are taking very long to restart. He also tells William that some of the users are having issues logging into the network when the domain controllers are restarting. When William gets back into the office, he opens DNS on all the servers and sees the following screen. William needs to ensure that all the domain controllers can reboot without taking so long and that all users can log in without having issues. William also needs to make sure that updates to the avionics.com zone are as secure as possible. What can William do to accomplish this? Select two:

   - ❍ A. William needs to change the zones to secondary zones so that users can log in without having issues.
   - ❍ B. William needs to change the avionics.com zone to an Active Directory-integrated zone.
   - ❍ C. William needs to change the dynamic updates option from none to secure-only for the avionics.com zone.
   - ❍ D. William needs to edit the Hosts files for all workstations and add the IP addresses of the DNS servers.

2. You are the network administrator for your company. You are responsible for the entire network, which consists of one Windows Server 2008 Active Directory forest with one domain. The forest is at the Windows Server 2008 functional level. You have configured a DNS server, named NS1, for the domain. After recently moving to a new ISP, many users have said they cannot access websites on the Internet. What steps can you take to ensure that users can access websites as well as resources in the internal domain? Select two:

   - ❍ A. You should manually configure all client computers on your network to use the ISP's DNS server as their default name resolution server.
   - ❍ B. You should make NS1 the Infrastructure Master to aid in internal and external name resolution.
   - ❍ C. You should configure NS1 to use the default root hints.
   - ❍ D. You should configure a forwarder on NS1 to the ISP's DNS server.

3. You are the network administrator for your company. The network consists of one 2008 Active Directory domain named svenson.com. Users browse the internal network as well as the Internet from their computers. All web and email hosting for a separate DNS domain called svenson.au is outsourced to an ISP. All name resolution for the svenson.au domain is resolved by the ISP. You have no control or access to the ISP's DNS servers, and you cannot list the contents of svenson.au by using nslookup against the ISP's DNS servers. You have configured a Windows Server 2008 server named NS1 to host the primary zone for svenson.com. You have removed all the root hints from this DNS server. All client computers refer to this DNS server for name resolution. You need to configure DNS resolution so that all client computers can access resources in svenson.net, svenson.au, and the Internet. How can you accomplish this?

   - ❍ A. You should configure a stub zone on NS1 for svenson.au.
   - ❍ B. You should configure a secondary zone on NS1 for svenson.net.
   - ❍ C. You should set up a primary zone on NS1 for svenson.* and enable the default root hints.
   - ❍ D. You should configure simple forwarding with the default settings with the IP address of the DNS server at the ISP.

4. You are the network administrator for your company. The network is comprised of four 2008 Active Directory domains. Each domain has two domain controllers, each configured as a DNS server. The forest root domain is called company.com. The three other domains are called marketing.company.com, geology.company.com, and eastern.geology.company.com. You want to ensure that the DNS zone for the geology.company.com domain remains available in case of a single server failure. You also want to ensure that the zone only supports secure dynamic updates. How can you accomplish this with the least amount of administrative effort?

   - ❍ A. You should create an Active Directory-integrated zone on the domain controllers in the geology.company.com domain. Then, you should configure the zone to replicate to all domain controllers in the domain.
   - ❍ B. You should configure a secondary zone in the company.com domain with the information for the geology.company.com domain.
   - ❍ C. You should create DNS forwarders on the DNS servers in the geology.company.com domain to all the other DNS servers in the forest.
   - ❍ D. You should create a stub zone on the DNS servers in the geology.company.com domain that refers to the primary zone in the company.com domain.

5. You are the network administrator for your company. You are in charge of the office in London. The company has a branch office in Sydney. DNS servers in both offices are running Windows Server 2008. Your office hosts the company.com DNS namespace, and the Sydney office hosts the australia.company.com namespace. Your office has some servers that are registered in the company.com zone and others that are registered in the australia.company.com zone. All client computers use the local DNS server as their preferred server. The two offices are connected over an unreliable WAN link. Firewall configurations prevent the DNS servers from receiving queries from the Internet. You need to configure the DNS server in your office to resolve queries from your office for host names in the australia.company.com namespace, even when the WAN link is down. How can you accomplish this?

- ❍ A. On your server, you should create a secondary zone named australia.company.com and specify the DNS server in the Australia office as a master server.
- ❍ B. You should create a stub zone on your DNS server for the australia.company.com zone.
- ❍ C. You should create a host record for the DNS server in the Australia office on your DNS server.
- ❍ D. You should create a delegated subdomain called australia and specify the DNS server in the Australia office as a name server.

Chapter 2

1. You are the systems administrator for your company. The network you administer has over 20 servers running Windows Server 2008 Enterprise and 250 workstations running a mixture of Windows XP and Windows Vista. The network is comprised of one root domain and two child domains all under one forest. The root domain is called sentec.com, and the child domains are called marketing.sentec.com and accounting.sentec.com. The forest and domain functional levels are all at Windows 2008. All domains are contained in one Active Directory Site. You want users from one domain to be able to log onto any other domain, but you have noticed that there are many users that share the same username in different domains. An example of this would be Sharon Smith in the sentec.com domain and Sharon Smith in the marketing.sentec.com domain. You decide to add alternative UPN suffixes to the forest so that users can log on with those different UPN suffixes. Where do you need to add the UPN suffixes for the domains?

- ❍ A. You need to first open up Active Directory Domains and Trusts. You then need to right-click the Active Directory Domains and Trusts and choose Properties. From here, you can add additional UPN suffixes.
- ❍ B. You need to open Active Directory Users and Computers first. You then need to right-click the root domain and choose Properties. Click on the Advanced tab, and you will be able to add the UPN suffixes from here.
- ❍ C. You need to open Active Directory Sites and Services first. You then need to right-click on the site, and choose Properties. Here, you will be able to add additional UPN suffixes.
- ❍ D. You need to first open up the Active Directory Schema snap-in. Right-click on the root, and choose properties. Here, you will be able to add UPN suffixes.

2. Simpson is the systems administrator for his company. Simpson oversees the entire company network which consists of one 2008 Active Directory domain. Simpson is leaving for vacation and he is putting one of the junior systems administrators in charge. While he is gone, one of the domain controllers will need to be demoted on the network. To help his junior systems administrator, Simpson has created the following answer file to automate the procedure. Simpson has set the file to run the demotion with the permissions of the junior systems administrator, who is a local administrator on the other servers that are member servers. When this junior systems administrator runs dcpromo with the answer file, it says that he does not have the necessary permissions. Why is the junior systems administrator not able to run the demotion properly?

   - ❍ A. Since the "administratorpassword=" setting is not defined, it will not be able to run the demotion properly.
   - ❍ B. The junior systems administrator is not a Domain Admin and, therefore, cannot run the demotion of the domain controller.
   - ❍ C. Since the junior systems administrator is not a local admin on the current domain controller, he will not be able to run the demotion process.
   - ❍ D. The removeapplicationpartion setting is set to yes, which requires a Schema Admin to run.

3. You are the network administrator for your company. The company's network is made up of one Windows Server 2008 forest with ten domains. The company has ten regional offices, each with their own domain. The company also has over two hundred branch offices that are connected to the nearest regional office over a slow WAN link. Every branch office has one domain controller that is configured as an additional domain controller in the regional office's domain. All site links that link the branch offices to their regional office domain are set to replicate every 15 minutes. You have received reports from users in the branch offices that say they are getting slow response times when accessing resources in the regional office domains. You monitor some of the branch office WAN connections and can see that bandwidth utilization is spiking quite often. You want to improve response time when branch office users access resources in the regional office domain, as well as ensure users can log on without having to use cached credentials if their WAN link goes down. How can you accomplish this?

   - ❍ A. You should decrease the replication interval for the site link between each branch office and its regional office.
   - ❍ B. You should increase the replication interval for the site links between the branch offices and the regional offices.
   - ❍ C. You should make the domain controllers in each branch office a global catalog server.
   - ❍ D. You should make all the domain controllers in every branch office a DNS server.

4. You are the network administrator for your company. Your company's network is comprised of one Active Directory forest with two domains, one domain for the Chicago office and one do main for the Miami office. The Chicago office has one DNS server with an IP address of 10.10.2.11, and the Miami office has one DNS server with an IP address 10.10.3.11. Both domains are connected over a WAN link. Both offices use the same ISP. The ISP's DNS server has an IP address of 204.99.5.121. The DNS server in the Chicago office has the primary DNS zone as the Chicago domain and the secondary zone as the Miami domain. You need to configure the primary and secondary DNS address referrals on all client computers in the Chicago office by using the least amount of effort. You also need to ensure that users access the Internet with the least amount of hops possible. You need to ensure that clients in the Chicago office can access resources as quickly as possible and that DNS lookup traffic does not occur over the WAN if the local DNS server is online. How can you accomplish this?

   - ❍ A. You need to configure 204.99.5.121 as the primary server and 10.10.3.11 as the secondary server.
   - ❍ B. You need to configure 10.10.2.11 as the primary DNS server and 204.99.5.121 as the secondary DNS server.
   - ❍ C. You need to configure 10.10.2.11 as the primary DNS server and 10.10.3.11 as the secondary server.
   - ❍ D. You need to set up DNS forwarding on 10.10.2.11 to the ISP's DNS server at 204.99.5.121.

5. You are the network administrator for your company. The company's network is comprised of one Active Directory Forest with two domains, called victories.com and southwest.victories.com. Both domains are at the Windows Server 2008 functional level. The Dallas office comprises the southwest.victories.com domain and is its own Active Directory site. The Chicago office comprises the victories.com domain and is its own Active Directory site as well. The Dallas office has around 100 users, and the Chicago office has around 5000 users. The two offices are connected to each other over a slow WAN link. A server named SVR1 in the Chicago office is a global catalog server and is running DNS. The Dallas office only has one server, named SVR2, which is a domain controller. Users in the Dallas office are reporting that it takes a very long time to log onto the network. How can you alleviate this issue of long logon times?

   - ❍ A. You can make SVR2 a global catalog server.
   - ❍ B. You can install DNS on SVR2.
   - ❍ C. You can create a Domain Local group in the victories.com domain and add all the users in the Dallas office to that group.
   - ❍ D. You can enable universal group membership caching for SVR2 in Active Directory Sites and Services.

Chapter 3

1. Johnson is the systems administrator for Taggert & Sons, a large law firm in Miami. Johnson is in the process of upgrading his company's servers from Windows Server 2003 to Windows Server 2008. Johnson wants to deploy RODC's in the law firm's branch offices since they do not have any IT personnel at those remote offices. All the branch offices are currently in the same do main as the home office.Johnson upgrades his first server, a Windows Server 2003 DC, at the home office to Windows Server 2008 Enterprise. Johnson logs onto his workstation computer as an Enterprise Admin and tries to run the adprep /rodcprep command from the infrastructure master through a command prompt, but he receives an error. What must Johnson do before he can successfully run this command?

   - ❍ A. He must raise the forest functional level to Windows Server 2003.
   - ❍ B. He must log on to a computer in the domain as a schema admin.
   - ❍ C. He must log onto the domain controller that holds the schema master operations role.
   - ❍ D. He must enable the Bridge all site links option in the Sites and Services snap-in for the links between the branch and home offices.

2. 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?

   - ❍ 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.

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?

   - ❍ 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

Chapter 4

1. Jayson is the systems administrator for his company. The company's network consists of 100 Windows Vista workstations, 50 Windows XP workstations, and 15 Windows Server 2008 Enterprise servers.Jayson has three helpdesk technicians who work under him and perform day-to-day IT tasks. One of the main functions they work on is adding and removing computers to and from the domain. Previously, these technicians had Domain Admin permissions, but Jayson has decided to take them out of that group for security reasons. Jayson still needs them to be able to add and remove computers to and from the domain, so he creates a GPO linked to the technicians' OU in Active Directory. This GPO gives them the permissions they need.Jayson has one of the technicians log on to a new computer that needs to be removed from the domain. When the technician tries to remove the computer, it states that he does not have enough permission to do so. Jayson checks the GPOs that are applied to this computer and can see that the new GPO has not been applied. What can Jayson do to make the GPO settings immediately apply to the computer?

   - ❍ A. Jayson should run the command gpresult /force.
   - ❍ B. If Jayson runs the gpupdate /force command, the new GPO settings will be applied immediately.
   - ❍ C. Jayson should have the technician log off and log back onto the computer.
   - ❍ D. Jayson should open the Active Directory Users and Computers snap-in. From here, Jayson should remove the technician from the OU where the GPO is applied and then re-add the technician back to that OU, thus forcing the GPO to be applied.

2. You are the senior Windows systems administrator for your company. The company consists of one forest and three domains all running under Windows 2008 Active Directory. All servers are running Windows server 2008, and the forest functional level is Windows Server 2008. Under each domain, you have implemented fine-grained password policies to allow for different users to have different policies. Company policy states that all user accounts must have an account lockout policy associated with them for security reasons. Many of the executives have com plained about this since they often lockout their accounts after the current limit of 5 is passed. You decide to change the password policies for just the executives so that their accounts still have a lockout policy, but it is at the maximum allowed by 2008. What is the maximum number of attempts allowed in 2008 before an account is locked out?

   - ❍ A. The maximum number of attempts allowed is 999.
   - ❍ B. The maximum number of attempts allowed is 99.
   - ❍ C. The maximum number of attempts allowed is 199.
   - ❍ D. The maximum number of attempts allowed is 99999.

3. Tyler is the systems administrator for Kelvin Unlimited, a custom car manufacturing company in Oklahoma City. The company's network consists of one2008 Active Directory Domain. All company servers are running Windows Server2008 and all workstations are running Windows Vista. Tyler has created numerousgroup policies to apply corporate standards as well as send out softwareapplications. One group policy that applies to the Sales team installs a customapplication whenever a Sales user logs onto any computer in the network. All Salesusers are in the Sales OU. The company also has publicly available computers inthe office lobby where Sales members show potential customers the productsoffered by the company. These computers in the lobby have their computeraccounts in an OU called Public Tyler does not want the custom Sales applicationinstalled on these public computers in the lobby whenever they log in. What canTyler do to prevent the application from installing on the computers in the lobbywhen the Sales members log in?

   - ❍ A. Tyler can set the application installation GPO to uninstall when it falls out of the scope of management.
   - ❍ B. Tyler can make the Sales users local administrators on the public computers which would prevent the application from being installed.
   - ❍ C. Tyler can create a group policy linked to the Public OU. In this policy he should set the computer policy settings to be applied before the user policy settings.
   - ❍ D. Tyler can create a new group policy linked to the Public OU. In this group policy, he should enable the user group policy loopback processing mode of replace.

4. Roger is the network administrator for his company. Roger manages a team of 10IT personnel which includes two software developers. The company networkconsists of one Windows Server 2008 Active Directory domain. These developershave recently created a custom inventory application that will run on one of thecompany's servers and all the workstations. Roger has created a domain account onthe network which will serve as the service account used by the new customapplication. The developers have informed Roger that this service account willneed to run as a process on client computers and will need to be able to use theidentity of any user and access the resources authorized to that user. Roger wantsto make one centralized setting change on the network to make sure the serviceaccount will work properly when running the application. What Group Policysetting can Roger edit to affect this change on the network?

   - ❍ A. He should add the new service account to the users list in the "Act as SYSTEM account on domain computers" Default Domain Group Policy.
   - ❍ B. If he adds the new service account to the list of users in the "Impersonate a client after authentication" setting in the Default Domain Group Policy, the application will work properly.
   - ❍ C. He should add this service account to the users list in the "Replace a process level token" Default Domain Group Policy.
   - ❍ D. He should add the new service account to the list of users in the "Act as part of the operating system" Default Domain Group Policy.

5. You are the network administrator for your company. The network is comprised ofa single Active Directory forest and a single domain, called Robertson. com. AllServers are running Windows Server 2008, and all clients are running WindowsVista. You have developed a new Group Policy object (GPO) in a test lab that youwant to implement on the production domain. How can you implement this GPO inthe production domain using the least amount of administrative effort?

   - ❍ A. You should copy the Group Policy Template (GPT) files in theSYSVOL folder from the test to the production domain.
   - ❍ B. You should link a new GPO to the production domain and includeall the settings of the GPO in the test environment.
   - ❍ C. You should use the Group Policy Management Console (GPMC) toback up the GPO in the test lab and import it into the productiondomain.
   - ❍ D. You should copy the System folder from the domain controller inthe test lab to any domain controller in the production environment.

Chapter 5

1. Katy is the systems administrator for Goodness Manufacturing, a candy-makingcompany in Pennsylvania. The company's network is currently running a WindowsServer 2003 Active Directory environment. All workstations are running WindowsXP. Katy is the sole person responsible for updating and maintaining theservers. Katy normally has to wait till after normal working hours to perform anyapplication or Windows updates, since they require a reboot. She also performsoffline defragmentation of the Active Directory database after hours, since itrequires a reboot as well. Katy is trying to convince her boss that migrating toWindows Server 2008 would be very beneficial and would save him from payingher so much overtime from working after hours. What feature in Windows Server2008 would allow Katy to perform updates and offline defragmentation withoutrebooting?

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

2. Levi is the systems administrator for his company. Levi has been told by his bossthat he needs to change the password policy on the network. Users are apparentlyreusing passwords over and over and changing them immediately whenever ITresets their passwords for them. Levi's boss doesn't want users to be able to changetheir passwords so often or be able to change their password right after IT resetstheir passwords. The company's network consists of one 2008 Active Directorydomain. What password policy settings does Levi need to adjust to accomplish what his boss has asked him to do? (Select 2)

   - ❍ A. Levi should adjust the "Maximum Password Age" Group Policysetting.
   - ❍ B. To accomplish what his boss has asked, Levi should adjust the"Enforce User Change at Next Logon" policy.
   - ❍ C. Levi should change the "Enforce Password History" setting in theGroup Policy settings module.
   - ❍ D. Levi should adjust the "Minimum Password Age" setting.

3. You are the network administrator for your company. Your network is comprisedof one 2008 Active Directory domain. You have 20 servers running WindowsServer 2008 and 300 workstations running a mixture of Windows XP andWindows Vista. You have configured the domain to use only Kerberosauthentication. You have received a report that a user is receiving an access deniederror when trying to connect to a member server. You want to test the functionalityof Kerberos authentication on the user's computer. What command should you runon the user's computer?

   - ❍ A. You should run the netdiag tool.
   - ❍ B. You should run the finger command.
   - ❍ C. You should run the netsh command.
   - ❍ D. You should run the netstat -an command.

4. You are the network administrator for your company. The network is made up ofone 2008 Active Directory domain. All servers are running Windows Server 2008,and all workstations are running Windows Vista. All HR users frequently accessconfidential files stored on the file server. To make sure that the confidential datais not compromised in data transmissions, you want to secure all communicationbetween the HR users and the file server. You want to ensure that all other userswill continue to have access to the file server as well. What two actions should youtake? Select two:

   - ❍ A. You will need to assign the Secure (Require Security) IPSec policyon the file server.
   - ❍ B. You will need to assign the Server (Request Security) IPSec policyon the file server.
   - ❍ C. You will need to assign the Client (Respond Only) IPSec policy onthe file server.
   - ❍ D. You will need to assign the Client (Respond Only) IPSec policy onall the HR client computers.

Chapter 6

1. Justin is the systems administrator for the University of Southwest Oklahoma. Theuniversity's network is a Windows Server 2008 Active Directory network. Allnetwork users are using Microsoft Exchange 2007. Because of the sensitiveinformation that users send back and forth in email, many Exchange users areutilizing S/MIME to encrypt their email. To accommodate S/MIME, Justin hasinstalled an Active Directory Certificate Server. The only problem is that there aremany satellite schools associated with the university that need to use S/MIME aswell. Instead of installing Certificate Authorities at all the satellite schools, Justinhas decided to deploy online responders so clients can check certificate statusthrough HTTP. Periodically, Justin checks the IIS servers that are working asOnline Responders to ensure that they are working properly. From the servers' logfiles, Justin can see that most of them are responding with cached answers sincethey are receiving so many requests. He can also see that requests are answeredvery quickly within a 120 second interval; then requests take longer to answer. Justin knows that the online responders use ISAPI extension caching, but not inthis manner. What mechanism is caching responses for 120 seconds in order toanswer requests quicker?

   - ❍ A. Network Load Balancing is being used by the online responders to route requests and cache responses to provide answers quicker.
   - ❍ B. The IIS HTTP.SYS library is what is being used to cache responsesfor 120 seconds. The library file helps to cache responses inaddition to the OCSP ISAPI extension caching.
   - ❍ C. The CACHING.SYS library file built into IIS is being used tocache responses for 120 seconds to respond to requests.
   - ❍ D. The CACHING.XML file, which is installed by default with IIS,handles client requests quickly by caching responses for up to 120seconds at a time.

2. You are the systems administrator for your company. You have just installedCertificate Services on a domain controller running Windows Server 2008 on yournetwork, choosing the option to install the Online Certificate Status Protocol(OCSP). You need to un-register the Web proxy on this server. How can youaccomplish this?

   - ❍ A. You should delete the OCSP virtual directory.
   - ❍ B. You should run the certsrv -unregsiter command to accomplish this.
   - ❍ C. You should stop the OCSP service, delete the Proxy virtualdirectory in IIS, and restart the OCSP service.
   - ❍ D. You should run the certutil -vocsproot delete command.

3. You are the network administrator for your company. All the servers in yournetwork are running Windows Server 2008. You need to change the hashalgorithm for some certificate templates used for user authentication on yourcertificate authority server. How can you accomplish this?

- ❍ A. You should right-click the template that needs to be changed andchoose properties. Then, you can click on the Cryptography tab andmake the change.
- ❍ B. You should right-click the template that needs to be changed andchoose change cryptography.
- ❍ C. You should right-click the template that needs to be changed andchoose properties. You should then click on the Hash tab andchange to the desired setting.
- ❍ D. You should run the certtemplate /hash command.

Answers & Explanations

Chapter 1

1. Answers: B, C

Explanation A. Incorrect. Making the zones secondary will not allow for users to log inwithout issues. There must also always be at least one primary zone.

Explanation B. Correct. Active Directory-integrated zones store their zone data inActive Directory and allow for fast data retrieval by DNS servers. A zone must also beActive Directory-integrated to allow for secure dynamic updates.

Explanation C. Correct. This will ensure that all dynamic updates use secure channels.

Explanation D. Incorrect. This will help if there are name resolution issues but wouldnot help in this situation.

2. Answers: C, D

Explanation A. Incorrect. This will hinder internal name resolution.

Explanation B. Incorrect. Making a server the Infrastructure Master does nothing for name resolution.

Explanation C. Correct. This will help users resolve Internet addresses.

Explanation D. Correct. This will help with name resolution without affecting internal resolution.

3. Answer: D

Explanation A. Incorrect. This will not allow clients to resolve names in all the necessary domains and the Internet.

Explanation B. Incorrect. This will not allow clients to resolve names in all the necessary domains and the Internet.

Explanation C. Incorrect. You cannot create a zone with a wildcard character like this.

Explanation D. Correct. This will allow resolution to the required domains and the Internet.

4. Answer: A

Explanation A. Correct. This will accomplish all that is needed.

Explanation B. Incorrect. This will not accomplish all that is needed in this situation.

Explanation C. Incorrect. This will not accomplish all that is needed in this situation.

Explanation D. Incorrect. This will not accomplish what is needed in this situation.

5. Answer: A

Explanation A. Correct. This will allow queries from the company.com zone to resolve host names in the australia.company.com zone, even if the WAN link is down.

Explanation B. Incorrect. A stub zone would not help in this situation.

Explanation C. Incorrect. Creating a host record on your DNS server would not allow queries to be resolved for the australia.company.com zone.

Explanation D. Incorrect. A subdomain would not help in this situation.

Chapter 2

1. Answer: A

Explanation A. Correct. This is the appropriate place to add UPN suffixes.

Explanation B. Incorrect. There is no such tab as this.

Explanation C. Incorrect. This is not the proper place to add UPN suffixes.

Explanation D. Incorrect. This is not where you can add UPN suffixes. There is not a Properties option when you right-click the schema root either.

2. Answer: B

Explanation A. Incorrect. This password determines the new local administrator password of the server once it becomes a member server, which can be left blank.

Explanation B. Correct. The minimum permissions needed to run a domain controller demotion is a Domain Admin.

Explanation C. Incorrect. Domain controllers do not have local users or local administrators.

Explanation D. Incorrect. The whole demotion process only needs a Domain Admin, not a Schema Admin, to run correctly.

3. Answer: A

Explanation A. Correct. Decreasing the time interval for replication traffic will decrease the size of the traffic each time it must be replicated.

Explanation B. Incorrect. Increasing the replication interval will make the size of the traffic larger each time it must be replicated.

Explanation C. Incorrect. Global catalog servers hold objects; they do not help with replication.

Explanation D. Incorrect. This will not help with slow response times when users try to access resources in the regional offices.

4. Answer: C

Explanation A. Incorrect. That will not accomplish what is needed in this scenario.

Explanation B. Incorrect. That will not accomplish what is need in this scenario.

Explanation C. Correct. That will allow users to access local resources and the Internet as quickly as possible.

Explanation D. Incorrect. That will not accomplish what is needed in this scenario.

5. Answer: D

Explanation A. Incorrect. While this would allow users to log on quicker, it would create a great deal of replication traffic over the slow WAN link, which is not advised.

Explanation B. Incorrect. This will not help users in the Dallas office log on any quicker.

Explanation C. Incorrect. This will not help the Dallas users to log on any quicker.

Explanation D. Correct. This will allow users in the Dallas office to log on quicker.

Chapter 3

1. Answer: A

Explanation A. Correct. The forest functional level must be Windows Server 2003, so that linked-value replication is available. This provides a higher level of replication consistency.

Explanation B. Incorrect. You must be logged on as an Enterprise Admin to run adprep /rodcprep.

Explanation C. Incorrect. This command can be run on any computer in a domain that has a connection to the domain controller with the infrastructure master operations role.

Explanation D. Incorrect. This option is not necessary to enable the adprep /rodcprep command to function properly.

2. 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.

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.

Chapter 4

1. Answer: B

Explanation A. Incorrect. The gpresult command is used to display the GPOs that have been applied to that computer and the user that is logged on. This command does not force a GPO to be applied.

Explanation B. Correct. The gpupdate /force command forces any GPOs that apply to that computer or logged-on user to be applied immediately.

Explanation C. Incorrect. While this action might help the new GPO to be applied, it will not happen immediately as would the gpupdate command.

Explanation D. Incorrect. Removing and re-adding a user to an OU that has an applied GPO will not force the GPO to be applied.

2. Answer: A

Explanation A. Correct. This is the maximum number of attempts allowed before an account is locked out.

Explanation B. Incorrect. This is not the correct number of maximum attempts allowed.

Explanation C. Incorrect. This is not the maximum number of attempts allowed.

Explanation D. Incorrect. The number of attempts allowed is 999.

3. Answer: D

Explanation A. Incorrect. This will only uninstall the application when the Sales users are moved out of the Sales OU.

Explanation B. Incorrect. This would not affect the application group policy in any way.

Explanation C. Incorrect. This would not accomplish anything since he has not modified anything for the computer policy settings for the Public OU.

Explanation D. Correct. This would, in effect, not apply any user applied group policies, which would not install the custom Sales application.

4. Answer: D

Explanation A. Incorrect. There is no such group policy setting.

Explanation B. Incorrect. This will not allow the application to run properly.

Explanation C. Incorrect. This will not allow the application to run properly.

Explanation D. Correct. This will allow the service to run as part of the operating system, giving it the permissions it needs.

5. Answer: C

Explanation A. Incorrect. This will not implement the new GPO.

Explanation B. Incorrect. While this would work, it would take too much administrative effort.

Explanation C. Correct. This will implement the GPO into the production environment.

Explanation D. Incorrect. This will not copy over the new GPO.

Chapter 5

1. 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.

2. Answers: C, D

Explanation A. Incorrect. This will not accomplish what his boss has asked.

Explanation B. Incorrect. This is not a group policy setting. This is a setting in the properties for the individual user account.

Explanation C. Correct. This will prevent users from utilizing the same passwords over and over again.

Explanation D. Correct. This will prevent users from immediately changing their passwords after being reset by IT.

3. Answer: A

Explanation A. Correct. The netdiag tool would be able to test the network connectivity of the client computer.

Explanation B. Incorrect. The finger command would not help in this situation.

Explanation C. Incorrect. The netsh command would not help in testing the network connectivity of the client computer.

Explanation D. Incorrect. The netstat -an command will show all the active and listening ports on the client computer.

4. Answers: B, D

Explanation A. Incorrect. This would only be needed if all transmissions to the file server needed to be encrypted.

Explanation B. Correct. This will help to encrypt the transmission between the HR users and the file server.

Explanation C. Incorrect. This would not help encrypt the traffic needed.

Explanation D. Correct. This will help encrypt the data between the HR computers and the file server.

Chapter 6

1. Answer: B

Explanation A. Incorrect. Network Load Balancing is used to route IP traffic to the appropriate computer, based on its availability. It is not used to cache Online Responder responses.

Explanation B. Correct. This library file, built into IIS, is used to cache responses for 120 seconds to answer requests to the online responder quicker.

Explanation C. Incorrect. There is no such file built into IIS.

Explanation D. Incorrect. There is no such file installed with IIS.

2. Answer: D

Explanation A. Incorrect. This will not un-register the Web proxy.

Explanation B. Incorrect. This command will not un-register the Web proxy.

Explanation C. Incorrect. This will not un-register the Web proxy.

Explanation D. Correct. This will un-register the Web proxy on the server.

3. Answer: A

Explanation A. Correct. This is the appropriate place to change the hash algorithm for an certificate template.

Explanation B. Incorrect. There is no such option when right-clicking a certificate template.

Explanation C. Incorrect. There is no hash tab in the certificate template properties.

Explanation D. Incorrect. There is no such command.