3 Administering Active Directory

Exam Objectives in this Chapter:
- Set an Active Directory forest and domain functional level based upon requirements.
- Manage schema modifications.
- Add or remove a UPN suffix.
- Restore Active Directory directory service.
- Perform an authoritative restore operation.
- Perform a nonauthoritative restore operation.
- Diagnose and resolve issues related to the Active Directory database.

Why This Chapter Matters
The information in this chapter shows you how to use various tools to administer Active Directory. Both graphical and command-line tools are available. The graphical tools are typically easier to use, especially for simple and unique tasks. Many of the command line tools are quite useful when troubleshooting or automating processes. No matter how you decide to administer Active Directory, you should be sure to back up your Active Directory database routinely. Despite many technological advances, people still make mistakes and equipment sometimes fails. If someone accidentally deletes an Active Directory container object, or if a server crashes, you might need to restore from backup.

Microsoft Windows Server 2003 with Service Pack 1 (SP1) includes new functionality that provides notification of the backup status of the directory service partitions. Windows Server 2003 with SP1 also increases the duration of the tombstone lifetime, the time after which deleted objects in Active Directory are permanently removed from the directory service.

The Active Directory Domains And Trusts console, the Active Directory Sites And Services Console, and the Active Directory Users And Computers console are the main tools for handling Active Directory—it's important to know what function each console serves. Windows Support Tools are also available; you must know how to install them to be able to administer the fine points of Active Directory. Microsoft Management Consoles (MMCs) allow you to administer Active Directory from remote locations or to allow other administrators to manage Active Directory.
Chapter 3 Administering Active Directory

This chapter shows you how to create and work with MMCs. Finally, you use the Backup Or Restore Wizard to create backups of Active Directory and perform a restore. Being able to maintain effective backups and having the ability to restore Active Directory from backup is vital for effective system administration.

Lessons in this Chapter:

- Lesson 1: Using Active Directory Administration Tools .................................................. 3-3
- Lesson 2: Customizing MMCs ......................................................................................... 3-18
- Lesson 3: Backing Up Active Directory ............................................................................ 3-30
- Lesson 4: Restoring Active Directory ............................................................................... 3-44

Before You Begin

To complete the lessons in this chapter, you must

- Prepare your test environment according to the descriptions given in the “Getting Started” section of “About This Book”
- Complete the practices for installing and configuring Active Directory as discussed in Chapter 2, “Installing and Configuring Active Directory”
Lesson 1: Using Active Directory Administration Tools

The powerful and flexible Active Directory administration tools that are included with Windows Server 2003 simplify directory service administration. The Active Directory administrative consoles enable you to administer Active Directory directory service. A number of additional Active Directory administration tools are available in the Windows Support Tools. This lesson introduces the Active Directory administrative consoles and Windows Support Tools that are used to configure, manage, and debug Active Directory.

After this lesson, you will be able to

- Describe the functions of the Active Directory Users And Computers administrative console
- Describe the functions of the Active Directory Sites And Services administrative console
- Describe the functions of the Active Directory Domains And Trusts administrative console
- Describe the functions of the Active Directory Schema snap-in
- Change the domain functional level
- Change the forest functional level
- Add or remove a UPN suffix
- Explain the purpose of each of the Windows Support Tools that pertain to Active Directory

Estimated lesson time: 20 minutes

Active Directory Administration Tools

Two main tools are used to administer Active Directory:

- Active Directory administrative consoles
- Active Directory-specific tools in Windows Support Tools

Active Directory Administrative Consoles

The Active Directory administrative consoles are installed automatically on computers configured as Windows Server 2003 domain controllers when Active Directory is installed. The administrative consoles can also be installed on other servers running Windows Server 2003 using the optional Administrative Tools package. This enables you to administer Active Directory from a computer that is not a domain controller. The following administrative consoles are available on the Administrative Tools menu of all Windows Server 2003 domain controllers:

- Active Directory Domains And Trusts console
- Active Directory Sites And Services console
Active Directory Users And Computers console

The Active Directory Schema snap-in is also available on a computer configured as a domain controller, but must be installed manually.

Active Directory Domains And Trusts Console

The Active Directory Domains And Trusts console provides the interface to manage domains and manage trust relationships between forests and domains. Using Active Directory Domains And Trusts, you can:

- Provide interoperability with other domains (such as pre–Microsoft Windows 2000 domains or domains in other Windows Server 2003 forests) by managing explicit domain trusts. Trusts are discussed in detail in Chapter 4, “Installing and Managing Domains, Trees, and Forests.”
- Change the domain functional level (formerly known as a domain mode) of a Windows Server 2003 domain from Windows 2000 mixed to the Windows 2000 native or Windows Server 2003 functional level.
- Change the forest functional level from Windows 2000 to Windows Server 2003 functional level.
- Add and remove alternate user principal name (UPN) suffixes used to create user logon names.
- Transfer the domain naming operations master role from one domain controller to another. Operations master roles are discussed in detail in Chapter 4, “Installing and Managing Domains, Trees, and Forests.”

Domain Functional Levels

As you learned in Chapter 1, domain functional levels (formerly known as domain modes) provide a way to enable domain-wide Active Directory features within your network environment. Four domain functional levels are available: Windows 2000 mixed (default), Windows 2000 native, Windows Server 2003 interim, and Windows Server 2003.

- **Windows 2000 native** The Windows 2000 native functional level allows a domain controller running the Windows Server 2003 operating system to interact with domain controllers in the domain running Windows 2000 or Windows Server 2003. You can raise the functional level of a domain to Windows 2000 native if the domain controllers in the domain are all running Windows 2000 Server or later.
Windows Server 2003 interim The Windows Server 2003 interim functional level allows a domain controller running the Windows Server 2003 operating system to interact with domain controllers in the domain running Windows NT 4 or Windows Server 2003. The Windows Server 2003 interim functional level is an option only when upgrading the first Windows NT domain to a new forest and can be manually configured after the upgrade. This functional level does not support domain controllers running Windows 2000.


Real World Integrating Windows Server 2003 into Existing Domains

If you plan to install Windows Server 2003 servers configured as domain controllers into an existing Windows 2000 domain, you’ll have to run the Adprep.exe command line utility. This utility is located in the I386 directory of the Windows 2003 Server installation CD-ROM. You’ll have to run the command `adprep /forestprep` on your existing Windows 2000 Server domain controller holding the schema operations master role. You’ll have to run `adprep /domainprep` on the Windows 2000 Server domain controller holding Infrastructure Operations Master role. Be sure to search for articles concerning ADPREP at `http://support.microsoft.com` before you actually run these commands.

Note that the Adprep.exe tool in Windows Server 2003 with SP1 has been improved to reduce the impact of File Replication service (FRS) synchronization that results from updating SYSVOL files during the upgrade. The tool allows you to perform SYSVOL operations in a separate step when preparing the domain for upgrade. The `adprep /domainprep` command, which formerly performed both directory and SYSVOL updates, now updates only the directory. A new switch, `/gpprep`, has been added to accommodate the SYSVOL updates, which can be performed at a convenient time following the upgrade. Adprep.exe also now detects third-party schema extensions that can block an upgrade, identifies the blocking extensions, and recommends fixes. Adprep.exe also detects Microsoft Exchange Server schema objects so that the Exchange Server schema can be prepared appropriately to accommodate InetOrgPerson naming.
When you convert from Windows 2000 mixed or Windows Server 2003 interim functional level to the Windows 2000 native or Windows Server 2003 functional level, keep in mind the following:

- Support for pre–Windows 2000 replication ceases. Because pre–Windows 2000 replication is gone, you can no longer have any domain controllers in your domain that are not running Windows 2000 Server or later.
- You can no longer add new pre–Windows 2000 domain controllers to the domain.
- The server that served as the primary domain controller during migration is no longer the domain master; all domain controllers begin acting as peers.

**Note** The change in domain functional level is one-way only; you cannot change from the Windows 2000 native or Windows Server 2003 functional level to the Windows 2000 mixed or Windows Server 2003 interim functional level.

Table 3-1 describes the domain-wide features that are enabled for their corresponding domain functional level.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain controller rename tool</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Update logon timestamp</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>User password on InetOrgPerson object</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Group Nesting</td>
<td>Enabled for distribution groups. Disabled for security groups, except for domain local security groups that can have global groups as members.</td>
<td>Enabled. Allows full group nesting.</td>
<td>Enabled. Allows full group nesting.</td>
</tr>
</tbody>
</table>
Lesson 1 Using Active Directory Administration Tools

Table 3-1 Features Enabled by Domain Functional Level

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SID History</td>
<td>Disabled</td>
<td>Enabled. Allows migration of security principals from one domain to another.</td>
<td>Enabled. Allows migration of security principals from one domain to another.</td>
</tr>
</tbody>
</table>

Exam Tip Be able to distinguish between the domain functional levels.

To change the domain functional level to Windows 2000 native or Windows Server 2003, complete the following steps:

1. Click Start, select Administrative Tools, and then click Active Directory Domains And Trusts.
2. Right-click the domain and then click Raise Domain Functional Level.
3. On the Raise Domain Functional Level dialog box, in the Select An Available Domain Functional Level list, select the domain functionality you want. Click Raise.
4. In the Raise Domain Functional Level message box, click OK.


- **Windows Server 2003 interim** The Windows Server 2003 interim functional level allows a domain controller running the Windows Server 2003 operating system to interact with domain controllers in the domain running Windows NT 4 or Windows Server 2003. The Windows Server 2003 interim functional level is an option only when upgrading the first Windows NT domain to a new forest and can be manually configured after the upgrade. This functional level does not support domain controllers running Windows 2000.
Windows Server 2003 The Windows Server 2003 functional level allows a domain controller running the Windows Server 2003 operating system to interact only with domain controllers in the domain running Windows Server 2003. You can raise the functional level of a forest to Windows Server 2003 only if all domain controllers in the forest are running Windows Server 2003 and all domain functional levels in the forest have been raised to Windows Server 2003.

Once the forest functional level has been raised, domain controllers running earlier operating systems cannot be introduced into the forest. Table 3-2 describes the forest-wide features that are enabled for their corresponding functional levels.

Table 3-2 Features Enabled by Forest Functional Levels

<table>
<thead>
<tr>
<th>Forest Feature</th>
<th>Windows 2000</th>
<th>Windows Server 2003</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global catalog replication improvements</td>
<td>Enabled if both replication partners are running Windows Server 2003. Otherwise, disabled.</td>
<td>Enabled</td>
</tr>
<tr>
<td>Defunct schema objects</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Forest trusts</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Linked value replication</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Domain rename</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Improved Active Directory replication algorithms</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Dynamic auxiliary classes</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>InetOrgPerson objectClass change</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Exam Tip Be able to distinguish between the forest functional levels.

To change the forest functional level to Windows Server 2003, complete the following steps:

1. Click Start, select Administrative Tools, and then click Active Directory Domains And Trusts.
2. Right click the Active Directory Domains And Trusts node and then click Raise Forest Functional Level.
3. On the Raise Forest Functional Level dialog box, click Raise.
4. In the Raise Forest Functional Level message box, click OK.
UPN Suffixes  A UPN suffix is the part of a UPN to the right of the @ character. The default UPN suffix for a user account is the Domain Name System (DNS) domain name of the domain that contains the user account. You can add alternative UPN suffixes to simplify administration and user logon processes by providing a single UPN suffix for all users. The UPN suffix is only used within the Active Directory forest and is not required to be a valid DNS domain name.

Using alternative domain names as the UPN suffix can provide additional logon security and simplify the names used to log on to another domain in the forest. For example, if your organization uses a deep domain tree, such as one organized by department and region, the domain name can be long. The default user UPN for a user in such a domain might be sales.cbi.contoso.com. Creating a UPN suffix of “contoso” would allow the user to log on using the much simpler logon name of user@contoso. If you create an alternative UPN, the UPN is then available when you create users by using Active Directory Users And Computers.

To add or remove UPN suffixes, complete the following steps:

1. Click Start, select Administrative Tools, and then click Active Directory Domains And Trusts.
2. Right click the Active Directory Domains And Trusts node and then click Properties.
3. On the Active Directory Domains And Trusts dialog box, in the UPN Suffixes tab, shown in Figure 3-1, do one of the following:
   - To add a UPN suffix, type an alternative UPN suffix in the Alternative UPN Suffixes box, and then click Add.
   - To remove a UPN suffix, select the suffix from the Alternative UPN Suffixes box, and then click Remove. On the Active Directory Domains and Trusts message box, click Yes.
4. Click OK.

Active Directory Sites And Services Console  You provide information about the physical structure of your network by publishing sites to Active Directory using the Active Directory Sites And Services console. Active Directory uses this information to determine how to replicate directory information and handle service requests. Sites are discussed in more detail in Chapter 5, “Configuring Sites and Managing Replication.”

Active Directory Users And Computers Console  The Active Directory Users And Computers console allows you to add, modify, delete, and organize Windows Server 2003 user accounts, computer accounts, security and distribution groups, and published resources in your organization’s directory. It also allows you to manage domain controllers and organizational units (OUs).

Note  Windows Server 2003 with SP1 extends the default period that Active Directory retains a deleted object, called the tombstone lifetime, from 60 days to 180 days. The longer tombstone lifetime increases the shelf life of system state backups and decreases the chance that a deleted object will reappear in the directory service. This reappearance can occur if a domain controller is reconnected to the network after a directory service object has been permanently deleted from the online domain controllers.

The tombstone lifetime does not change automatically when you upgrade to Windows Server 2003 with SP1, but you can change the tombstone lifetime manually after the upgrade.

New forests created with domain controllers running Windows Server 2003 with SP1 have a default tombstone lifetime of 180 days.
Active Directory Schema Snap-In  The Active Directory Schema snap-in is available so you can view and modify Active Directory schema. By default, the snap-in is not available on the Administrative Tools menu. You must install it using the command line and by creating an MMC for it. This action is required to ensure that the schema cannot be modified by accident.

To install the Active Directory Schema snap-in, complete the following steps:

1. Log on as an Administrator.
2. Click Start, and then click Command Prompt.
3. Type `regsvr32 schmmgmt.dll`.
4. Click Start, and then click Run.
5. In the Run box, type `mmc` and then click OK.
6. On the File menu, click Add/Remove Snap-In.
7. In the Add/Remove Snap-In dialog box, click Add.
8. In the Add Standalone Snap-In dialog box, in the Snap-In column, double-click Active Directory Schema, and then click Close.
9. In the Add/Remove Snap-In dialog box, click OK.
10. To save this console, on the File menu, click Save. In the Save As dialog box, ensure that Administrative Tools is shown in the Save In box. Then type **Active Directory Schema** in the File Name box and click Save. The Active Directory Schema snap-in is now available from the Administrative Tools menu.

See Also  Modifying the Active Directory schema is an advanced operation that is best performed by experienced programmers or system administrators. For detailed information about modifying the Active Directory schema, see the Microsoft Windows Server 2003 Resource Kit, located on the Microsoft Web site at [http://www.microsoft.com/windows/reskits/default.asp](http://www.microsoft.com/windows/reskits/default.asp).

For further information about using MMCs, refer to Lesson 2.

Active Directory-Specific Windows Support Tools

In Chapter 2, you installed the Windows Support Tools to assist you in troubleshooting Active Directory installation. In addition, several tools that can be used to configure, manage, and debug Active Directory are available in the Windows Support Tools. The Windows Support Tools are included on the Windows Server 2003 CD in the
Chapter 3  Administering Active Directory

Support\Tools folder. These tools are intended for use by Microsoft support personnel and experienced users.

Table 3-3 describes the Windows Support Tools that pertain to Active Directory.

**Table 3-3  Active Directory-Specific Windows Support Tools**

<table>
<thead>
<tr>
<th>Tool</th>
<th>Used to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acldiag.exe: ACL Diagnostics</td>
<td>Determine whether a user has been granted or denied access to an Active Directory object. It can also be used to reset access control lists (ACLs) to their default state.</td>
</tr>
<tr>
<td>Adsiedit.msc: ADSI Edit†</td>
<td>Add, delete, and move objects in the directory (including schema and configuration naming contexts). Object attributes can be viewed, modified, and deleted.</td>
</tr>
<tr>
<td>Dcdiag.exe: Domain Controller Diagnostic Tool*</td>
<td>Analyze the state of domain controllers in a forest or enterprise and report any problems. Note that Dcdiag.exe in Windows Server 2003 with SP1 includes a new DNS health check, and a new security check that can detect security configurations that can cause replication to fail.</td>
</tr>
<tr>
<td>Dfscmd.exe: Distributed File System Command Tool*</td>
<td>Manage a distributed file system from the command line. Note that Dfscmd.exe in Windows Server 2003 with SP1 includes new commands to move or rename links.</td>
</tr>
<tr>
<td>Dfsutil.exe: Distributed File System Utility*</td>
<td>Manage all aspects of Distributed File System (DFS), check the configuration concurrency of DFS servers, and display the DFS topology. Note that Dfsutil.exe in Windows Server 2003 with SP1 includes the ability to implement failback settings for roots and links.</td>
</tr>
<tr>
<td>Dsacls.exe*</td>
<td>View or modify the ACLs of objects in Active Directory.</td>
</tr>
<tr>
<td>Dsastat.exe: Directory Services Utility*</td>
<td>Compare naming contexts on domain controllers and detect differences.</td>
</tr>
<tr>
<td>Ldp.exe: LDP Tool‡</td>
<td>Allow Lightweight Directory Access Protocol (LDAP) operations, such as connect, bind, search, modify, add, and delete, to be performed against Active Directory.</td>
</tr>
<tr>
<td>Movetree.exe: Active Directory Object Manager*</td>
<td>Move Active Directory objects such as OUs and users between domains in a single forest to support domain consolidation or organizational restructuring operations.</td>
</tr>
<tr>
<td>Netdom.exe: Windows Domain Manager*</td>
<td>Manage Windows Server 2003 domains and trust relationships from the command line.</td>
</tr>
<tr>
<td>Nltest.exe*</td>
<td>Provide a list of primary domain controllers, force a remote shutdown, provide information about trusts and replication.</td>
</tr>
</tbody>
</table>
See Windows Support Tools help for more information about using the Windows Support Tools that pertain to Active Directory.

Active Directory Service Interfaces (ADSI) provides a simple, powerful, object-oriented interface to Active Directory. ADSI makes it easy for programmers and administrators to create programs utilizing directory services by using high-level tools such as Microsoft Visual Basic, Java, C, C#, or Visual C++ as well as scripted languages such as VBScript, JScript, or PerlScript without having to worry about the underlying differences between the different namespaces. ADSI is a fully programmable Automation object for use by administrators.
ADSI enables you to build or buy programs that give you a single point of access to multiple directories in your network environment, whether those directories are based on LDAP or another protocol.


**Practice: Viewing Active Directory Administration Tools**

In this practice, you view the Active Directory administrative consoles and some of the Active Directory support tools.

**Exercise 1: Viewing Active Directory Administrative Consoles**

In this exercise, you view the Active Directory administrative consoles.

**To view Active Directory administrative consoles**

1. Log on to Server01 as Administrator.

2. Click Start, point to Administrative Tools, and then click Active Directory Domains And Trusts.

3. In the console tree, right-click the contoso.com domain and then select Properties. In the Properties dialog box for the contoso.com domain, click the Trusts tab. Notice the trust information boxes that would contain information about trusts if there were other domains in the forest. Click Cancel.

4. In the console tree, right-click the contoso.com domain and then select Raise Domain Functional Level. On the Raise Domain Functional Level dialog box, notice the list in which you can raise domain functionality. Click Cancel. In the console tree, right-click the Active Directory Domains And Trusts node and then select Raise Forest Functional Level. On the Raise Forest Functional Level dialog box, notice that you cannot raise forest functionality until you have raised the domain functional level to Windows Server 2003. Click OK.

5. In the console tree, right-click the Active Directory Domains And Trusts node and then select Properties. On the UPN Suffixes tab, notice where you can enter alternate UPN suffixes. Click OK and then close the Active Directory Domains And Trusts console.

6. Click Start, point to Administrative Tools, and then click Active Directory Sites And Services. In the console tree, double-click the Sites folder. Notice that a site called Default-First-Site is present. This site is created automatically when Active Directory is installed. Close the Active Directory Sites And Services console.
Lesson 1 Using Active Directory Administration Tools

7. Click Start, point to Administrative Tools, and then click Active Directory Users And Computers. In the console tree, double-click the Builtin folder and examine all the default groups. Double-click the Users folder and examine all the default users. Close the Active Directory Users And Computers console.

Exercise 2: Installing and Viewing the Active Directory Schema Snap-In

In this exercise, you install the Active Directory Schema snap-in and view its contents.

► To install and view the Active Directory Schema snap-in

1. Use the procedure provided earlier in this lesson to install the Active Directory Schema snap-in.


3. In the console tree, double-click any class. Notice the list of attributes for that class provided in the Details pane. Close the Active Directory Schema snap-in.

4. On the Microsoft Management Console message box, click No.

Exercise 3: Installing and Viewing the Active Directory-Specific Windows Support Tools

In this exercise, you install Windows Support Tools and view some of the Active Directory-specific support tools.

► To install and view the Active Directory-specific Windows Support Tools

1. If you haven’t already installed the Windows Support Tools, use the procedure provided in Chapter 2 to install them.

2. Click Start, point to All Programs, point to Windows Support Tools, then click Support Tools Help.

3. Access the Dsacls.exe tool in the alphabetical list of tools by file name. View Help for this tool.

4. In help, click Open Command Prompt. At the command prompt, type `dsacls \server1\DC=contoso,DC=com` and press ENTER. The output shows the access control list for Active Directory on Server01.


Lesson Review

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review the lesson and then try the question
Chapter 3 Administering Active Directory

again. Answers to the questions can be found in the “Questions and Answers” section at the end of this chapter.

1. What is the purpose of the Active Directory Domains And Trusts console?

2. What is the purpose of the Active Directory Sites And Services console?

3. What is the purpose of the Active Directory Users And Computers console?

4. Why isn’t the Active Directory Schema snap-in provided automatically on the Administrative Tools menu after you install Active Directory?

5. Which Active Directory-specific Windows Support Tool enables you to manage Windows Server 2003 domains and trust relationships?
   a. Ntdsutil.exe
   b. Netdom.exe
   c. Active Directory Domains And Trusts console
   d. Nltest.exe

Lesson Summary

■ Three Active Directory administrative consoles are available on the Administrative Tools menu of all Windows Server 2003 domain controllers. The Active Directory Schema snap-in is also available on a domain controller, but must be installed manually to ensure the schema is not modified by accident.

■ Domain functional level (formerly known as the domain mode) provides a way to enable domain-wide Active Directory features within your network environment. Four domain functional levels are available: Windows 2000 mixed (default), Windows 2000 native, Windows Server 2003 interim, and Windows Server 2003. The change in domain functional level is one-way only.
Lesson 1   Using Active Directory Administration Tools   3-17


- You can add alternative UPN suffixes to simplify administration and user logon processes by providing a single UPN suffix for all users. Using alternative domain names as the UPN suffix can provide additional logon security and simplify the names used to log on to another domain in the forest.

- Several additional tools that can be used to configure, manage, and debug Active Directory are available in the Windows Support Tools. To use these tools you must first install the Windows Support Tools on your computer.
Lesson 2: Customizing MMCs

In the previous lesson, you learned how to use the standard administrative consoles provided when you install Active Directory. You can also create custom consoles that focus on management tasks you specify by using the MMC. This lesson explains how you can create, use, and modify custom consoles.

After this lesson, you will be able to
■ Create customized MMCs
■ Modify customized MMCs

Estimated lesson time: 25 minutes

The MMC

The MMC is a tool used to create, save, and open collections of administrative tools, which are called consoles. When you access the Active Directory administrative consoles discussed in Lesson 1, you are accessing the MMC for that tool. The Active Directory Domains And Trusts, Active Directory Sites And Services, and Active Directory Users And Computers administrative tools are each a console. The console does not provide management functions itself, but is the program that hosts management applications called snap-ins. Snap-ins are programs used by administrators to manage network services.

There are two types of MMCs: preconfigured and custom. Preconfigured MMCs contain commonly used snap-ins, and they appear on the Administrative Tools menu. You create custom MMCs to perform a unique set of administrative tasks, such as the MMC for the Active Directory schema discussed in the previous lesson. You can use both preconfigured and custom MMCs for remote administration.

Preconfigured MMCs

Preconfigured MMCs contain snap-ins that you use to perform the most common administrative tasks. The Windows Server 2003 family installs a number of preconfigured MMCs during installation. The following are characteristics of preconfigured MMCs:

■ They contain a stand-alone snap-in that provides the functionality to perform a related set of administrative tasks.

■ They function in user mode. Because preconfigured MMCs are in user mode, you cannot modify them, save them, or add additional snap-ins. However, when you create custom consoles, you can add as many preconfigured consoles as you want as snap-ins to your custom console.
■ They might be added by Windows Server 2003 when you install additional components. Optional Windows Server 2003 components might include additional preconfigured MMCs that Windows Server 2003 adds when you install a component. For example, when you install the DNS service, Windows Server 2003 also installs the DNS Management console.

Custom MMCs

You can use many of the preconfigured MMCs for administrative tasks. However, there will be times when you need to create your own custom MMCs. Although you can’t modify preconfigured consoles, you can combine multiple preconfigured snap-ins with third-party snap-ins provided by independent software vendors that perform related tasks to create custom MMCs. You can then do the following:

■ Save the custom MMCs to use again.
■ Distribute the custom MMCs to other administrators.
■ Use the custom MMCs from any computer to centralize and unify administrative tasks.

Creating custom MMCs allows you to meet your administrative requirements by combining snap-ins that you use to perform common administrative tasks. By creating a custom MMC, you do not have to switch between different programs or different preconfigured MMCs because all of the snap-ins that you need to perform your job are located in the custom MMC.

Consoles are saved as files and have an .msc extension. All the settings for the snap-ins contained in the console are saved and restored when the file is opened, even if the console file is opened on a different computer or network.

Console Tree and Details Pane

Every MMC has a console tree, which displays the hierarchical organization of its associated snap-ins. The MMC in Figure 3-2, for example, contains Device Manager on the local computer and the Disk Defragmenter snap-ins.
The console tree organizes snap-ins that are part of an MMC. This allows you to easily locate a specific snap-in. Items that you add to the console tree appear under the console root. The details pane lists the contents of the active snap-in.

Every MMC contains an Action menu and a View menu. The choices on these menus vary, depending on the current selection in the console tree.

**Snap-Ins**

Snap-ins are applications that are designed to work in an MMC. Use snap-ins to perform administrative tasks. There are two types of snap-ins: stand-alone snap-ins and extension snap-ins.


Extension snap-ins are usually referred to simply as *extensions*. They are snap-ins that provide additional administrative functionality to another snap-in. The following are characteristics of extensions.

- Extensions are designed to work with one or more stand-alone snap-ins, based on the function of the stand-alone snap-in. For example, the Group Policy extension is available in the Active Directory Users And Computers console; however, it is not available in the Disk Defragmenter snap-in, because Group Policy does not relate to the administrative task of disk defragmentation.
When you add an extension, Windows Server 2003 displays only extensions that are compatible with the stand-alone snap-in. Windows Server 2003 places the extensions into the appropriate location within the stand-alone snap-in.

When you add a snap-in to a console, MMC adds all available extensions by default. You can remove any extension from the snap-in.

You can add an extension to multiple snap-ins.

Figure 3-3 demonstrates the concept of snap-ins and extensions. A toolbox (an MMC) holds a drill (a snap-in). You can use a drill with its standard drill bit, and you can perform additional functions with different drill bits (extensions). Extensions are pre-assigned to snap-ins, and multiple snap-ins can use the same extension.

Some stand-alone snap-ins can use extensions that provide additional functionality, for example, Computer Management. However, some snap-ins, like Event Viewer, can act as either a snap-in or an extension.

**Console Options**

Use console options to determine how each MMC operates by selecting the appropriate console mode. The console mode determines the MMC functionality for the person who is using a saved MMC. The two available console modes are author mode and user mode.

**Note** Additional console options can be set using Group Policy. For information on setting group policies, see Chapter 11, “Administering Group Policy.”

When you save an MMC in author mode, you enable full access to all MMC functionality, which includes modifying the MMC. Save the MMC using author mode to allow those using it to do the following:

- Add or remove snap-ins.
- Create new windows.
Chapter 3 Administering Active Directory

- View all portions of the console tree.
- Save MMCs.

**Note**  By default, all new MMCs are saved in author mode.

Usually, if you plan to distribute an MMC to other administrators, you save the MMC in user mode. When you set an MMC to user mode, users cannot add snap-ins to, remove snap-ins from, or save the MMC.

There are three types of user modes that allow different levels of access and functionality. Table 3-4 describes when to use each type of user mode.

**Table 3-4  MMC User Mode Types**

<table>
<thead>
<tr>
<th>User mode</th>
<th>Use when</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full access</td>
<td>You want to allow users to navigate between snap-ins, open new windows, and gain access to all portions of the console tree.</td>
</tr>
<tr>
<td>Limited access, multiple</td>
<td>You do not want to allow users to open new windows or gain access to a portion of the console tree. You want to allow users to view multiple windows in the console.</td>
</tr>
<tr>
<td>Limited access, single</td>
<td>You do not want to allow users to open new windows or gain access to a portion of the console tree. You want to allow users to view only one window in the console.</td>
</tr>
</tbody>
</table>

**Using MMCs for Remote Administration**

When you create custom MMCs, you can set up a snap-in for remote administration. Remote administration allows you to perform administrative tasks from any location. For example, you can use a computer running Windows XP Professional with Service Pack 1 or the 329357 hotfix applied to perform administrative tasks on a computer running Windows Server 2003. You cannot use all snap-ins for remote administration; the design of each snap-in dictates whether or not you can use it for remote administration.

To perform remote administration:

- You can use snap-ins from computers running different editions of the Windows Server 2003 family.

- You must use specific snap-ins designed for remote administration. If the snap-in is available for remote administration, Windows Server 2003 prompts you to choose the target computer to administer.

Suppose you need to administer Windows Server 2003 from a Windows XP Professional desktop. Because Windows XP Professional does not provide the same level of...
administrative tools as Windows Server 2003, you will need to install a more complete set of tools on the Professional desktop. By accessing the server and executing the Adminpak.msi file located at %Systemroot%\System32, you can copy the administrative tools onto the Professional desktop. Then configure each tool for use with the server. One benefit of installing the entire package is that it includes the Active Directory Management MMC, which contains the three major Active Directory MMCs and the DNS MMC. Note that some tools may be installed that are not actually running on the server; the Windows Server 2003 Administration Tools Setup Wizard is simply a means for loading administrative tools to a remote machine.

### Off the Record

The Adminpak.msi can be used to repair console issues related to file corruption. For example, if you find that you can no longer open a console, such as the DNS console, you should try reinstalling Adminpak.msi.

### Creating Custom MMCs

To create a custom MMC, you must open an empty console and then add the snap-ins needed to perform the desired administrative tasks.

To create a custom MMC, complete the following steps:

1. Click Start and point to Run.
2. Type `mmc` in the Run box, and then click OK. An MMC window opens, titled Console1 and containing a window titled Console Root. This is an empty MMC.
3. Maximize the Console1 and Console Root windows.
4. On the File menu, click Add/Remove Snap-In.
5. In the Standalone tab in the Add/Remove Snap-In dialog box, click Add.
6. In the Add Standalone Snap-In dialog box, shown in Figure 3-4, select the snap-in you want to add and click Add. In some instances, the snap-in is simply added to the MMC. In other cases, MMC requires you to specify additional details for the snap-in in a dialog box or through a wizard.
7. Enter additional details for the snap-in as needed.

8. If the snap-in supports remote administration, a dialog box for the snap-in appears, as shown in Figure 3-5. Do one of the following:
   - Select Local Computer to manage the computer on which the console is running.
   - Select Another Computer to manage a remote computer. Then click Browse. In the Select Computer dialog box, type the name of the remote computer, then click OK.

9. Click Finish.
10. When you are finished adding snap-ins, click Close in the Add Standalone Snap-In dialog box. The snap-ins you have added appear in the list in the Add/Remove Snap-In dialog box.

11. In the Add/Remove Snap-In dialog box, click OK. MMC displays the snap-ins you have added in the console tree below Console Root.

12. Select the Console Root.

13. On the File menu, click Options. MMC displays the Options dialog box with the Console tab active, as shown in Figure 3-6.

![Figure 3-6 Options dialog box](image)

14. Select the console mode in the Console Mode box, and then click OK.

15. On the File menu, click Save As.

16. In the File Name box in the Save As dialog box, type the name for your customized MMC and then click Save. The name of your console appears in the MMC title bar.

17. On the File menu, click Exit. The customized console has been created and saved and can now be accessed on the Administrative Tools menu.

**Modifying Custom MMCs**

You can modify a custom MMC by adding or removing snap-ins or extensions. Not all snap-ins have extensions. You can add or remove extensions from a console when you need to expand or limit administrative tasks. This allows you to include only those extensions that are relevant to the computer being administered.
Chapter 3 Administering Active Directory

To add a snap-in to an existing MMC, complete the following steps:

1. Click Start, point to All Programs, point to Administrative Tools, and then click the name of the custom MMC.
2. On the File menu, click Add/Remove Snap-In.
3. In the Standalone tab in the Add/Remove Snap-In dialog box, click Add.
4. In the Add Standalone Snap-In dialog box, select the snap-in you want to add to the existing MMC and click Add.
5. Enter additional details for the snap-in as described in the previous procedure.
6. When you are finished adding snap-ins, click Close in the Add Standalone Snap-In dialog box. The snap-ins you have added appear in the list in the Add/Remove Snap-In dialog box.
7. In the Add/Remove Snap-In dialog box, click OK. MMC displays the snap-ins you have added in the console tree below Console Root.

To remove a snap-in from an existing MMC, complete the following steps:

1. Click Start, point to All Programs, point to Administrative Tools, then click the name of the custom MMC.
2. On the File menu, click Add/Remove Snap-In.
3. In the Standalone tab in the Add/Remove Snap-In dialog box, select the snap-in you want to delete and click Remove. Then click OK. The snap-in is removed from the console.

To add or remove an extension to a snap-in on an existing MMC, complete the following steps:

1. Click Start, point to All Programs, point to Administrative Tools, and then click the name of the custom MMC.
2. On the File menu, click Add/Remove Snap-In.
3. In the Standalone tab in the Add/Remove Snap-In dialog box, click the Extensions tab. Then select the snap-in for which you want to add or remove an extension.
4. In the Extensions tab, shown in Figure 3-7, indicate the extension(s) you want to add or delete, as follows:
   - To add an extension, click the desired extension.
   - To remove an extension, clear the Add All Extensions check box and then in the Available Extensions box, clear the check box for the desired extension.
5. Click OK.
6. Expand the snap-in to confirm that the desired extension has been added or removed.

Practice: Customizing an MMC

In this practice, you customize an MMC.

Exercise 1: Creating a Custom MMC

In this exercise, you create a custom MMC.

To create a custom MMC

1. Log on to Server1 as Administrator.
2. Use the procedure provided earlier in this lesson to create a custom MMC. Add the Computer Management snap-in to the MMC. Although the Computer Management snap-in supports remote administration, set up the snap-in to manage the local computer. Set the console mode to author mode. Save the MMC with the name Administrator A.

Do not use any of the tools at this point.

Exercise 2: Adding a Snap-In to an Existing MMC

In this exercise, you add a snap-in to an existing MMC.

To add a snap-in to an existing MMC

1. Use the procedure provided earlier in this lesson to add the Event Viewer snap-in to the Administrator A MMC.
Chapter 3 Administering Active Directory

2. Set this snap-in to manage the local computer.
3. Confirm that the Event Viewer snap-in has been added to the Administrator A MMC.

Exercise 3: Removing an Extension to a Snap-In on an Existing MMC

In this exercise, you remove an extension to a snap-in on an existing MMC.

To remove an extension to a snap-in on an existing MMC

1. Use the procedure provided earlier in this lesson to remove the Disk Management extension from the Computer Management snap-in on the Administrator A MMC.
2. Confirm that the Disk Management extension has been removed from the Computer Management snap-in.

Lesson Review

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review the lesson and then try the question again. Answers to the questions can be found in the “Questions and Answers” section at the end of this chapter.

1. What is the function of an MMC? Why is it necessary to create customized MMCs?

2. What is a snap-in?

3. What is the function of a console tree?

4. What are extensions?

5. Which of the following console mode types allows users to create new windows in the console?
   a. Author mode
   b. User mode—full access
Lesson 2 Customizing MMCs

c. User mode—limited access, multiple window
d. User mode—limited access, single window

Lesson Summary

- There are two types of MMCs: preconfigured and custom. Preconfigured MMCs contain commonly used snap-ins and appear on the Administrative Tools menu. You create custom MMCs to perform a unique set of administrative tasks.

- Snap-ins are applications that work within an MMC and are used to perform administrative tasks. There are two types of snap-ins: stand-alone and extension. Stand-alone snap-ins are referred to simply as snap-ins, and provide one function or a related set of functions. Extension snap-ins are referred to as extensions, and provide additional administrative functionality to another snap-in.

- The console mode determines how an MMC is used. There are two console modes: author and user. Author mode provides full access to all MMC functionality, which includes modifying the MMC. In user mode, users cannot add snap-ins to, remove snap-ins from, or save the MMC.

- For custom MMCs, you can set up a snap-in for remote administration, allowing you to perform administrative tasks from any location. Not all snap-ins are available for remote administration.
Lesson 3: Backing Up Active Directory

This lesson guides you through the steps required to back up Active Directory data. When you create a backup, you need to conduct several preliminary tasks, and then perform a number of tasks using the Backup Or Restore Wizard. In this lesson you will learn how to back up Active Directory data, how to schedule and run an unattended backup, and how to delete an unattended backup.

After this lesson, you will be able to
■ Back up Active Directory data at a local computer
■ Schedule and run an unattended backup of Active Directory data
■ Delete an unattended backup of Active Directory data

Estimated lesson time: 25 minutes

Preliminary Backup Tasks

An important part of backing up Active Directory data is performing the preliminary tasks. You must prepare the files that you want to back up, and, if you are using a removable media device, you must prepare the device. If you use a removable media device, you must ensure that:

■ The backup device is attached to a computer on the network and is turned on. If you are backing up to tape, you must attach the tape device to the computer on which you run Windows Backup.
■ The media device is listed on the Windows Server 2003 Hardware Compatibility List (HCL).
■ The medium is loaded in the media device. For example, if you are using a tape drive, ensure that a tape is loaded in the tape drive.

You must be a member of the Administrators or the Backup Operators groups to perform a backup.

Creating an Active Directory Backup

After you have completed the preliminary tasks, you can perform the Active Directory backup using the Backup Or Restore Wizard. When you back up Active Directory, the Backup Or Restore Wizard automatically backs up all the system components and all the distributed services that Active Directory requires. Collectively, these components and services are known as system state data.

For Windows Server 2003, the system state data comprises the registry, COM+ Class Registration database, system boot files, files under Windows File Protection, and the
Certificate Services database (if the server is a certificate server). If the server is a domain controller, Active Directory and the Sysvol directory are also contained in the system state data. When you choose to back up system state data, all of the system state data that is relevant to your computer is backed up; you cannot choose to back up individual components of the system state data. This is due to dependencies among the system state components. You can back up only the system state data on a local computer. You cannot back up the system state data on a remote computer.

To assist with your backup strategy, Windows Server 2003 with SP1 includes event ID 2089 in the Directory Service event log. Event ID 2089 provides the backup status of each directory partition that a domain controller stores. This event appears in the Directory Service event log if a directory partition has not been backed up for a period greater than half the backup latency interval (tombstone lifetime). The event is logged daily until the partition is backed up.

To create an Active Directory backup, complete the following steps:

1. Log on to your domain as Administrator, point to Start, point to All Programs, point to Accessories, point to System Tools, and select Backup.

2. On the Welcome To The Backup Or Restore Wizard page, click Next.

3. On the Backup Or Restore page, shown in Figure 3-8, select Backup Files And Settings, and then click Next.

4. On the What To Back Up page, shown in Figure 3-9, select Let Me Choose What To Back Up, and then click Next.
5. On the Items To Back Up page, shown in Figure 3-10, expand the My Computer item, and then select System State. Click Next.

6. On the Backup Type, Destination, And Name page, shown in Figure 3-11, complete the following steps:
   - Select Tape in the Select The Backup Type list if you are using tape; otherwise this option defaults to File.
   - In the Choose A Place To Save Your Backup list, choose the location where Windows Backup will store the data. If you are saving to a tape, select the tape name. If you are saving to a file, browse to the path for the backup file location.
In the Type A Name For This Backup box, enter a name for the backup you are going to do.

Click Next.

---

On the Completing The Backup Or Restore Wizard page, click Advanced.

On the Type Of Backup page, shown in Figure 3-12, select Normal as the backup type used for this backup job. Normal is the only backup type supported by Active Directory. If the Hierarchical Storage Manager (HSM) has moved data to remote storage and you want to back it up, select the Backup Migrated Remote Storage Data check box. Click Next.
9. On the How To Back Up page, shown in Figure 3-13, select the Verify Data After Backup check box. This option causes the backup process to take longer but it confirms that files are correctly backed up. If you are using a tape device and it supports hardware compression, select the Use Hardware Compression, If Available check box to enable hardware compression. It’s recommended that you do not select the Disable Volume Shadow Copy check box. By default, Backup creates a volume shadow copy of your data to create an accurate copy of the contents of the hard drive, including open files or files in use by the system. Click Next.

![Figure 3-13  How To Back Up page](image)

10. On the Backup Options page, shown in Figure 3-14, select the Replace The Existing Backups option, then select the Allow Only The Owner And The Administrator Access To The Backup Data And To Any Backups Appended To This Medium check box. This action saves only the most recent copy of Active Directory and allows you to restrict who can gain access to the completed backup file or tape. Click Next.
11. On the When To Back Up page, shown in Figure 3-15, select Now. Click Next.

12. On the Completing The Backup Or Restore Wizard page, click Finish to start the backup operation.

13. The Backup Progress window shows the progress of the backup.

14. When the backup operation is complete, the Backup Progress window, shown in Figure 3-16, shows that the backup is complete. You can click the Report button to see a report about the backup operation, as shown in Figure 3-17. The report is stored on the hard disk of the computer on which you are running the backup.
Chapter 3  Administering Active Directory

Scheduling Active Directory Backup Operations

Scheduling an Active Directory backup operation means that you can have an unattended backup job occur later when users are not at work and files are closed. You can also schedule Active Directory backup operations to occur at regular intervals. To enable this, Windows Server 2003 integrates the backup operation with the Task Scheduler service. To schedule a backup operation, you must access the advanced backup settings as described in the following procedure.

To schedule an Active Directory backup operation, complete the following steps:

1. Follow steps 1–10 in the previous section, “Creating an Active Directory Backup.”

2. On the When To Back Up page, shown in Figure 3-18, select Later. Then type the job name in the Job Name box and click Set Schedule.
3. In the Schedule tab in the Schedule Job dialog box, shown in Figure 3-19, select the frequency of the backup operation: Daily, Weekly, Monthly, Once, At System Startup, At Logon, or When Idle from the Schedule Task list. Indicate the time the backup operation will begin in the Start Time list. Indicate when the task will occur in the Schedule Task box for the selected frequency. Click Advanced.

4. In the Advanced Schedule Options dialog box, shown in Figure 3-20, you can specify when the backup operations should begin, end, or how often they should be repeated in the Start Date, End Date, and Repeat Task boxes, respectively. Enter information as necessary and click OK.
In the Schedule tab in the Schedule Job dialog box, select the Show Multiple Schedules check box if you wish to set up more than one schedule for the backup operation. Repeat steps 1–4 for each schedule. Click the Settings tab when you are finished setting up schedules.

6. In the Settings tab in the Schedule Job dialog box, shown in Figure 3-21, specify whether to delete the task file from your computer’s hard disk after the backup operation has finished running and is not scheduled to run again in the Scheduled Task Completed box. Specify whether to start or stop the backup operation based on the computer’s idle time in the Idle Time box. Specify whether to start or stop the backup operation based on the computer’s power status in the Power Management box. Click OK.

7. On the When To Back Up page, click Next.
8. In the Set Account Information dialog box, shown in Figure 3-22, type the password for the account shown in the Password box and confirm the password in the Confirm Password box. Click OK.

![Set Account Information dialog box](image)

Figure 3-22  Set Account Information dialog box

9. Confirm your selections on the Completing The Backup Or Restore Wizard page, then click Finish to schedule the backup.

**Deleting Scheduled Active Directory Backup Operations**

To delete a scheduled Active Directory backup operation, you must access the advanced backup settings as described in the following procedure.

To delete a scheduled Active Directory backup operation, complete the following steps:

1. Log on to your domain as Administrator, point to Start, point to All Programs, point to Accessories, point to System Tools, and select Backup.

2. On the Welcome To The Backup Or Restore Wizard page click the Advanced Mode link.

3. On the Welcome To The Backup Utility Advanced Mode page, shown in Figure 3-23, click the Schedule Jobs tab.

![Welcome To The Backup Utility Advanced Mode page](image)

Figure 3-23  Welcome To The Backup Utility Advanced Mode page
4. In the Schedule Jobs tab, shown in Figure 3-24, icons for the scheduled backup operation(s) appear on the schedule for the date(s) the operation is specified to be performed. In this example, a backup operation is scheduled daily. Click the backup operation you want to delete.

![Schedule Jobs tab]

**Figure 3-24** Schedule Jobs tab

5. In the Scheduled Job Options dialog box that appears, shown in Figure 3-25, ensure that the job you want to delete appears in the Job Name box. Click Delete.

![Scheduled Job Options dialog box]

**Figure 3-25** Scheduled Job Options dialog box

6. In the Removing a Scheduled Job message box that appears, click Yes. The backup operation has been deleted from the schedule.
Practice: Backing Up Active Directory

In this practice, you back up Active Directory and perform tasks related to backup scheduling.

Exercise 1: Creating an Active Directory Backup

In this exercise, you create an Active Directory backup.

To create an Active Directory backup

1. Log on to Server1 as Administrator.
2. Open the Active Directory Users And Computers console. Create a new, empty OU by right-clicking the domain in the console tree, pointing to New, and then clicking Organizational Unit. In the New Object-Organizational Unit dialog box, type TEST1 in the Name box, then click OK. Verify that the TEST1 OU appears in the console tree.
3. Use the procedure provided earlier in this lesson to create an Active Directory backup. Name this backup Active Directory Backup1. Check with your administrator to ensure the availability of disks or tapes for backup storage.
4. When you have finished the backup operation for Active Directory Backup1, return to Active Directory Users And Computers and delete the TEST1 OU you created in step 2.

Note In this exercise, you backed up Active Directory when it contained the TEST1 OU and then deleted the TEST1 OU. In the next lesson you will restore Active Directory to contain the TEST1 OU.

Exercise 2: Scheduling an Active Directory Backup Operation

In this exercise, you schedule an Active Directory backup operation.

To schedule an Active Directory backup operation

1. Use the procedure provided earlier in this lesson to schedule an Active Directory backup operation. Name this backup Active Directory Backup2.
2. Schedule this backup to occur daily at 12:00 A.M.
3. Check with your administrator to ensure the availability of disks or tapes for backup storage at the specified time.

Exercise 3: Deleting a Scheduled Active Directory Backup Operation

In this exercise, you delete a scheduled Active Directory backup operation.
To delete a scheduled Active Directory backup operation

Use the procedure provided earlier in this lesson to delete Active Directory Backup2 after you have completed the exercise and the backup operation runs.

Lesson Review

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review the lesson and then try the question again. Answers to the questions can be found in the “Questions and Answers” section at the end of this chapter.

1. What tasks should you complete before attempting to back up Active Directory data?

2. What is system state data and why is it significant to backing up Active Directory?

3. Can you restrict who can gain access to a completed backup file or tape? If so, how?

4. When you specify the items you want to back up in the Backup Or Restore Wizard, which of the following should you select to successfully back up Active Directory data?
   a. System state data
   b. Shared system volume folder
   c. Database and log files
   d. Registry

Lesson Summary

- Before you can back up Active Directory data, you must prepare the files that you want to back up, and, if you are using a removable media device, you must prepare the device.
- Active Directory and the Sysvol directory are also contained in the system state data. Therefore, when you back up Active Directory data, you must specify that you want to back up only system state data.
You can perform a backup of Active Directory data on demand, or you can schedule the backup operation to occur daily, weekly, monthly, once, at system startup, at logon, or when idle.
Lesson 4: Restoring Active Directory

There are two ways to restore Active Directory: nonauthoritatively and authoritatively. This lesson shows you how to perform both methods of restoring Active Directory.

After this lesson, you will be able to
- Explain the difference between nonauthoritative and authoritative restore
- Restore Active Directory

Estimated lesson time: 35 minutes

Restoring Active Directory

Like the backup process, when you choose to restore Active Directory, you can only restore all of the system state data that was backed up, including the registry, the COM+ Class Registration database, system boot files, files under Windows File Protection; the Sysvol directory and Active Directory (if the server is a domain controller); and the Certificate Services database (if the server is a certificate server). You cannot choose to restore individual components (for example, only the Active Directory) of the system state data.

If you are restoring the system state data to a domain controller, you must choose whether you want to perform a nonauthoritative restore or an authoritative restore. The default method of restoring the system state data to a domain controller is nonauthoritative. You must be a member of the Administrators or the Backup Operators groups to perform a restore.

Nonauthoritative Restore

In nonauthoritative restore, the distributed services on a domain controller are restored from backup media and the restored data is then updated through normal replication. Each restored directory partition is updated with that of its replication partners by replication after you restore the data. For example, if the last backup was performed a week ago, and the system state is restored nonauthoritatively, any changes made subsequent to the backup operation will be replicated from the other domain controllers. The Active Directory replication system will update the restored data with newer data from your other servers. Nonauthoritative restore is typically performed when a domain controller has completely failed due to hardware or software problems.

Authoritative Restore

An authoritative restore brings a domain or a container back to the state it was in at the time of backup and overwrites all changes made since the backup. If you do not want to replicate the changes that have been made subsequent to the last backup operation, you must perform an authoritative restore. For example, you must perform an authoritative
restore if you inadvertently delete users, groups, or OUs from Active Directory and you want to restore the system so that the deleted objects are recovered and replicated. Authoritative restore is typically used to restore a system to a previously known state, for example, before Active Directory objects were erroneously deleted.

To authoritatively restore Active Directory data, you must run the Ntdsutil utility after you have performed a nonauthoritative restore of the system state data but before you restart the server. The Ntdsutil utility allows you to mark objects as authoritative. Marking objects as authoritative changes the update sequence number of an object so it is higher than any other update sequence number in the Active Directory replication system. This ensures that any replicated or distributed data that you have restored is properly replicated or distributed throughout your organization. The Ntdsutil utility can be found in the %Systemroot%\System32 directory and accompanying documentation within the Windows Server 2003 Help files (available from the Start menu).

### Using Windows Server 2003 SP1 to Remove Domain Controller Metadata

Ntdsutil in Windows Server 2003 with SP1 has two commands that make it easier to remove domain controller metadata. Preliminary steps, such as connecting to a server, domain, and site, are no longer required. You simply specify the server to remove. These two commands have the following syntax:

- **Ntdsutil “metadata cleanup” “remove selected server”**`ServerObject`

  - When using this command, specify the distinguished name (DN) path of the server object (`ServerObject`) of the domain controller whose metadata you want to remove. The server object is the parent of the NTDS settings object in the configuration container. For example, for the domain controller named DC1 located in the Default-First-Site-Name of the contoso.com forest, the DN path of the server object would be `cn=DC1,cn=servers,cn=default-first-site-name,cn=configuration,dc=contoso,dc=com`. If the DN path contains any spaces, enclose the entire DN path in quotes.

- **Ntdsutil “metadata cleanup” “remove selected server”**`ServerObject on TargetDC`

  - This command is identical to the preceding one, except it allows the administrator to specify the domain controller (`TargetDC`) on which the removal is performed. `TargetDC` must be entered as the DNS or NetBIOS name of the domain controller.

For example, suppose you back up the system on Monday, and then create a new user called Ben Smith on Tuesday, which replicates to other domain controllers in the domain, but on Wednesday, another user, Nancy Anderson, is accidentally deleted. To authoritatively restore Nancy Anderson without reentering information, you can non-authoritatively restore the domain controller with the backup created on Monday. Then, using Ntdsutil you can mark the Nancy Anderson object as authoritative. The result is that Nancy Anderson is restored without any effect on Ben Smith.
Exam Tip Know when to use authoritative or nonauthoritative restore.

Preliminary Restore Tasks

Like the backup process, an important part of restoring Active Directory data is performing the preliminary tasks. Before you can restore Active Directory, you must perform the following tasks:

- Ensure that you can access all locations that require the restoration of files.
- Ensure that the appropriate device for the storage medium containing the data to be restored is attached to a computer on the network and is turned on.
- Ensure that the medium containing the data to be restored is loaded in the device.

Performing a Nonauthoritative Restore

To restore the system state data on a domain controller, you must first start your computer in a special safe mode called directory services restore mode. This allows you to restore the Sysvol directory and Active Directory directory services database. You can only restore system state data on a local computer. You cannot restore the system state data on a remote computer.

However, you can restore backed up system state data to an alternate location—a folder you designate. By restoring to an alternate location, you preserve the file and folder structure of the backed up data—all folders and subfolders appear in the alternate folder you specify.

Note If you restore the system state data and you do not designate an alternate location for the restored data, Backup will erase the system state data that is currently on your computer and replace it with the system state data you are restoring. Also, if you restore the system state data to an alternate location, only the registry files, Sysvol directory files, Cluster database information files (if applicable), and system boot files are restored to the alternate location. The Active Directory database, Certificate Services database (if applicable), and COM+ Class Registration database are not restored if you designate an alternate location.

To nonauthoritatively restore Active Directory, complete the following steps:

1. Restart the computer.
2. During the phase of startup where the operating system is normally selected, press F8.
3. On the Windows Advanced Options Menu, select Directory Services Restore Mode and press ENTER. This ensures that the domain controller is offline and is not connected to the network.
4. At the Please Select The Operating System To Start prompt, select the appropriate Microsoft Windows Server 2003 operating system and press ENTER.

5. Log on to your domain as Administrator.

**Note** When you restart the computer in directory services restore mode, you must log on as an Administrator by using a valid Security Accounts Manager (SAM) account name and password, *not* the Active Directory Administrator’s name and password. This is because Active Directory is offline, and account verification cannot occur. Rather, the SAM accounts database is used to control access to Active Directory while it is offline. You specified this password when you set up Active Directory.

6. In the Desktop message box that warns you that Windows is running in safe mode, click OK.

7. Point to Start, point to All Programs, point to Accessories, point to System Tools, and then select Backup.

8. On the Welcome To The Backup Or Restore Wizard page, click Next.

9. On the Backup Or Restore page, shown previously in Figure 3-8, select Restore Files And Settings. Click Next.

10. On the What To Restore page, shown in Figure 3-26, expand the media type that contains the data that you want to restore in the Items To Restore box or click Browse. The media can be either tape or file. Expand the appropriate media set until the data that you want to restore is visible. Select the data you want to restore, such as system state, then click Next.

![Backup or Restore Wizard](image-url)

**Figure 3-26** Backup Or Restore Wizard, What To Restore page with system state data selected for restore
11. Ensure that media containing the backup file is in the correct location.

12. On the Completing The Backup Or Restore Wizard page, do one of the following:
   - Click Finish to start the restore process. The Backup Or Restore Wizard requests verification for the source of the restore data and then performs the restore. During the restore, the Backup Or Restore Wizard displays status information about the restore.
   - Click Advanced to specify advanced restore options. Refer to the next section, “Specifying Advanced Restore Settings for a Nonauthoritative Restore” for details.

13. In the Warning message box that warns you that restoring system state will always overwrite current system state, click OK.

14. The Restore Progress dialog box displays status information about the restore process. As with the backup process, when the restore is complete, you can choose to view the report of the restore. The report contains information about the restore, such as the number of files that have been restored and the duration of the restore process.

15. Close the report when you have finished viewing it and then click Close to close the restore operation.

16. When prompted to restart the computer, click Yes.

---

Real World  Shutdown Event Tracker

You’ve probably noticed that Windows Server 2003 has a new feature that requests a shutdown reason each time you restart the server. This feature is called the Shutdown Event Tracker. If you are working in a test environment, you might choose to disable this feature to avoid the hassle of typing in a reason each time you restart. To disable this feature, you can perform the following steps:

1. Click Start, click Run, and type `gpedit.msc` and press ENTER.

2. Expand the Computer Configuration and then Administrative Templates objects. Click on the System object. In the right-hand pane you’ll see several settings appear.

3. Locate and double-click that Display Shutdown Event Tracker setting. The Display Shutdown Event Tracker Properties dialog box opens.

4. Click the Disabled radio button to disable the Shutdown Event Tracker. Click OK. Close the Group Policy Editor console.

Now when you shut down this server, you won’t be asked to enter a reason.
Specifying Advanced Restore Settings for a Nonauthoritative Restore

The Advanced settings in the Backup Or Restore Wizard vary, depending on the type of backup media from which you are restoring.

To specify advanced restore settings for a nonauthoritative Active Directory restore, complete the following steps:

1. On the Where to Restore page, in the Restore Files To list, select the target location for the data that you are restoring. The choices in the list are the following:
   - **Original Location**—Replaces corrupted or lost data. This is the default and must be selected to restore Active Directory.
   - **Alternate Location**—Restores an older version of a file to a folder you designate.
   - **Single Folder**—Consolidates the files from a tree structure into a single folder. For example, use this option if you want copies of specific files but do not want to restore the hierarchical structure of the files.

   **Note** If you select either an alternate location or a single folder, you must also provide the path to the location or folder.

2. Click Next.

3. On the How to Restore page, select how you want to restore the system state data from the following:
   - **Leave Existing Files (Recommended)**—Prevents accidental overwriting of existing data. This is the default.
   - **Replace Existing Files If They Are Older Than The Backup Files**—Verifies that the most recent copy exists on the computer.
   - **Replace Existing Files**—Windows Backup does not provide a confirmation message if it encounters a duplicate file name during the restore operation.

4. Click Next.

5. On the Advanced Restore Options page, select whether or not to restore security or special system files from the following:
   - **Restore Security Settings**—Applies the original permissions to files that you are restoring to a Windows NTFS file service volume. Security settings include access permissions, audit entries, and ownership. This option is available only if you have backed up data from an NFTS volume and are restoring to an NTFS volume.
   - **Restore Junction Points, But Not The Folders And File Data They Reference**—Restores junction points on your hard disk but not the data to which the junction
points refer. If you have any mounted drives and you want to restore the data that mounted drives point to, you should not select this check box.

- **Preserve Existing Volume Mount Points**—Prevents the restore operation from writing over any volume mount points on the destination volume. If you are restoring data to a replacement drive, and you have partitioned and formatted the drive and restored volume mount points, you should select this option so your volume mount points are not restored. If you are restoring data to a partition or drive that you have just reformatted, and you want to restore the old volume mount points, you should not select this option.

- **Restore The Cluster Registry To The Quorum Disk And All Other Nodes**—Makes certain that the cluster quorum database is restored and replicated on all nodes in a server cluster. If selected, the Backup Or Restore Wizard will stop the Cluster service on all other nodes of the server cluster after the node that was restored reboots.

- **When Restoring Replicated Data Sets, Mark The Restored Data As The Primary Data For All Replicas**—Ensures that restored File Replication service (FRS) data is replicated to your other servers. If you are restoring FRS data, you should choose this option. If you do not choose this option, the FRS data that you are restoring may not be replicated to other servers because the restored data will appear to be older than the data already on the servers. This will cause the other servers to overwrite the restored data, preventing you from restoring the FRS data.

6. Click Next.

7. On the Completing The Backup Or Restore Wizard page, click Finish to start the restore process. The Backup Or Restore Wizard requests verification for the source of the restore data and then performs the restore. During the restore, the Backup Or Restore Wizard displays status information about the restore.

### Performing an Authoritative Restore

An authoritative restore occurs after a nonauthoritative restore and designates the entire directory, a subtree, or individual objects to be recognized as authoritative with respect to replica domain controllers in the forest. The Ntdsutil utility allows you to mark objects as authoritative so that they are propagated through replication, thereby updating existing copies of those objects throughout the forest.

To authoritatively restore Active Directory, complete the following steps:

1. Perform a nonauthoritative restore as described previously.

2. Restart the computer.

3. During the phase of startup where the operating system is normally selected, press F8.
4. On the Windows Advanced Startup Options Menu, select Directory Services Restore Mode and press ENTER. This ensures that the domain controller is offline and is not connected to the network.

5. At the Please Select The Operating System To Start prompt, select the appropriate Microsoft Windows Server 2003 operating system and press ENTER.

6. Log on as Administrator.

**Note** When you restart the computer in directory services restore mode, you must log on as an Administrator by using a valid SAM account name and password, not the Active Directory Administrator's name and password. This is because Active Directory is offline and account verification cannot occur. Rather, the SAM accounts database is used to control access to Active Directory while it is offline.

7. In the Desktop message box that warns you that Windows is running in safe mode, click OK.

8. Point to Start, then select Command Prompt.

9. At the command prompt, type `ntdsutil` and press ENTER.

10. At the Ntdsutil prompt, type `authoritative restore` and press ENTER.

11. At the authoritative restore prompt, do the following:

    - To authoritatively restore the entire directory, type `restore database` and press ENTER.
    - To authoritatively restore a portion or subtree of the directory, such as an OU, use the OU's distinguished name, type `restore subtree subtree_distinguished_name` and press ENTER.

For example, to restore the Security1 OU in the `microsoft.com` domain, the commands would be:

```
ntdsutil
authoritative restore
restore subtree OU=Security1,DC=Microsoft,DC=COM
```

    - To authoritatively restore the entire directory *and* override the version increase, type `restore database verinc version_increase` and press ENTER.
    - To authoritatively restore a subtree of the directory *and* override the version increase, type `restore subtree subtree_distinguished_name verinc version_increase` and press ENTER.

The authoritative restore opens the Ntds.dit file, increases version numbers, counts the records that need updating, verifies the number of records updated, and
reports completion. If a version number increase is not specified, one is automatically calculated.

12. Type **quit** and press **ENTER** to exit the Ntdsutil utility and close the Command Prompt window.

13. Restart the domain controller in normal mode and connect the restored domain controller to the network. When the restored domain controller is online and connected to the network, normal replication brings the restored domain controller up to date with any changes from the additional domain controllers that were not overridden by the authoritative restore. Replication also propagates the authoritatively restored object(s) to other domain controllers in the forest. The deleted objects that were marked as authoritative are replicated from the restored domain controller to the additional domain controllers. Because the objects that are restored have the same object globally unique identifier (GUID) and object SID, security remains intact, and object dependencies are maintained.

14. Ensure the integrity of the computer’s Group Policy by performing one of the following:

- If you authoritatively restored the entire Active Directory database, copy the Sysvol directory on the alternate location over the existing one **after** the Sysvol share is published.

- If you authoritatively restored specific Active Directory objects, copy only the policy folders (identified by the GUID) corresponding to the restored policy objects from the alternate location **after** the Sysvol share is published. Then, copy them over the existing ones.

When authoritatively restoring either the entire Active Directory database or selected objects, it is important that you copy the Sysvol and policy data from the alternate location **after** the Sysvol share is published. If the computer is in a replicated domain, it may take several minutes before the Sysvol share is published because it needs to synchronize with its replication partners. If all computers in the domain are authoritatively restored and restarted at the same time, then each will be waiting (indefinitely) to synchronize with each other. In this case, restore one of the domain controllers first so that its Sysvol share can be published; then restore the other computers nonauthoritatively.

**Impact of Authoritative Restore on Trust Relationships and Network Connections**

Both parent and child trust relationships in Windows domains and Kerberos and NTLM trust relationships to other Windows domains reside in the domain directory partition. Because trust relationship and computer account passwords are renegotiated at a specified interval, if you authoritatively restore an entire domain directory partition, computer passwords and trust relationship passwords are restored to the values at the time of the backup. If the password values are different from the current values, trust relationships and computer accounts might be invalidated. For trust relationships, domain
controllers may no longer be able to communicate with domain controllers from other domains. If an older computer account password is restored, the member's workstation may no longer be able to communicate with the server and the domain controller. If you authoritatively restore objects that affect trust relationships or computer account passwords, you must reset the passwords. Therefore, you should restore only those portions of the domain directory partition that are absolutely necessary. The more of the domain hierarchy included in the restore, the greater chance that trust relationships are affected.

Note  By default, passwords are reset every seven days; except for computer accounts. The previous password is also maintained. Therefore, performing authoritative restore with a backup that is older than 14 days can affect the trust relationships.

To minimize the effort involved with resetting trusts and rejoining computers, you must perform regular backups.

Practice: Restoring Active Directory

In this practice, you restore Active Directory from the backup you made in Lesson 3.

Note  To complete this practice, you must have successfully completed the practice in Lesson 3.

Exercise 1: Restoring Active Directory

In this exercise, you perform an authoritative restore to restore Active Directory.

To restore Active Directory

1. Use the procedure provided earlier in this lesson to authoritatively restore Active Directory using Active Directory Backup1. Hint: Use the restore subtree command parameter with OU=TEST1,DC=contoso,DC=com as the subtree distinguished name.

2. Verify that the TEST1 OU you created, backed up, and deleted in Lesson 3 has been restored in the Active Directory Users And Computers console.

Lesson Review

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review the lesson and then try the question again. Answers to the questions can be found in the “Questions and Answers” section at the end of this chapter.
Chapter 3 Administering Active Directory

1. Describe what happens in a nonauthoritative restore.

2. Describe what happens in an authoritative restore.

3. Which method of restore should you use if you accidentally delete an OU?

4. Which method of restore should you use if a domain controller has completely failed due to hardware or software problems?

5. Which of the following Ntdsutil command parameters should you use if you want to restore the entire directory?
   a. Restore database
   b. Restore subtree
   c. Database restore
   d. Subtree restore

Lesson Summary

- You restore Active Directory data by performing a nonauthoritative restore (default) or an authoritative restore.
- In nonauthoritative restore, the distributed services on a domain controller are restored from backup media and the restored data is then updated through normal replication. Each restored directory partition is updated with that of its replication partners.
- An authoritative restore brings a domain or a container back to the state it was in at the time of backup and overwrites all changes made since the backup.
- Before you can restore Active Directory, you must ensure that you can access all locations that require the restoration of files, the appropriate device for the storage medium containing the data to be restored is attached to a computer on the network and is turned on, and the medium containing the data to be restored is loaded in the device.
To restore the system state data on a domain controller, you must start your computer in directory services restore mode. To perform a nonauthoritative restore, use the Backup Or Restore Wizard. To perform an authoritative restore, use the Backup Or Restore Wizard and the Ntdsutil command.

Case Scenario Exercise

You are a network consultant. You are consulting for an educational institution called Graphic Design Institute as described in Chapter 2. You’ve just finished installing the Research department’s forest root domain controller. The Research department is using a server running Windows Server 2003 configured as a domain controller. You’ve installed a primary DNS server and configured those records to be stored in Active Directory.

As you are working, Laura Steele, the director of the institute, asks you to discuss potential upgrades for the Administrative and Marketing departments. The following list describes significant details about the departments and network environment of the Graphic Design Institute:

- **Information Technology Services (ITS)** This department utilizes UNIX client and server operating systems. The ITS department maintains DNS servers and Internet access for the entire institute. There are 10 users and 25 computers in this department. The ITS department also maintains the institute’s physical network infrastructure which includes 100 Mbps and gigabit Ethernet capable cables, hubs, switches, and routers.

- **Administration department** This department has a Windows 2000 Active Directory domain structure. The operating systems in use include Windows 2000 Advanced Server, Windows 2000 Professional, and Windows XP Professional. There are 12 domain controllers, eight file servers, and 5,000 users in this department. Ten of those domain controllers are also hosting the domain’s Active Directory-integrated DNS zone. The ITS department delegated the admin.graphicdesigninstitute.com namespace to the Administration department.

- **Marketing department** This department has a Windows NT 4 domain that includes one primary domain controller (PDC) and one backup domain controller (BDC). The operating systems in use are Windows NT 4 Server, Windows NT 4 Workstation, and Windows 2000 Professional. The department has 15 users and 20 computers.

- **Research department** At this time the Research department has 25 employees and 30 computers. You’ve installed a forest root domain controller and DNS server on one computer. Most of the employees haven’t yet been issued computers. They are still putting together their office furniture. However, you’ve suggested installing
a Remote Installation Services (RIS) server to deploy Windows XP Professional. Steve Masters, the newly hired network manager for Research, plans to install the client computers once you are finished configuring the directory structure.

Given this information, answer the following questions:

1. Before you move on to upgrading the other departments, what should you do to ensure the Research department’s Active Directory data is protected? What should you ensure that Steve will continue to do in order to protect the Research department’s data?

2. What similarities exist between the implementation of Active Directory in the Research and Marketing departments?

3. If you must install an additional Windows Server 2003 domain controller in the existing Administration domain, what must you first do to the Administration domain?

4. If you’re asked to upgrade the PDC of the Marketing domain, but hold off on the upgrade of the BDC, what functional level should you use on the new Windows 2003 Server domain?

5. The network administrators of the Marketing domain want to know what the equivalent of the User Manager for Domains and the Server Manager applications are on Windows Server 2003 domain controller. What would you tell them?

### Troubleshooting Lab

You are a network administrator for Contoso Pharmaceuticals. You recently lost one of your domain controllers, named Server2, due to a hardware failure. This domain controller cannot be repaired and there was no recent backup. You notice many replication errors start to appear in the Directory Service log of the Event Viewer on your other domain controller. You need to install a new server to replace Server2. You attempt to install a new domain controller named Server2, but the installation fails, reporting Server2 already exists. You must resolve this issue.

You’ll begin this lab by installing Server2 as a domain controller. Then, you’ll pretend that Server2 has experienced an unrecoverable error by reinstalling the entire operating system without first demoting Server2.

1. Install Active Directory on Server2. You can do this manually or by using the Server2dc.txt answer file on the Supplemental CD-ROM. Place the companion CD-ROM in your CD-ROM drive. To use the answer file, run the command `dcpromo /answer:d:\70-294\labs\chapter03\Server2dc.txt` (this command makes the assumption that your CD-ROM drive is D; if not, substitute the drive letter of your CD-ROM drive). If you’d prefer to install Active Directory manually, use the written steps in Chapter 2 to install an additional domain controller for the contoso.com domain.
Caution What you are about to do is not the recommended method for removing a domain controller from your Active Directory infrastructure. The recommended method is to run DCPROMO to uninstall the domain controller first. You are performing these steps to simulate an unexpected failure of your domain controller.

2. Ensure that you allow Server2 to fully complete the installation of Active Directory. You are now about to reinstall Server2 using the Windows 2003 Enterprise Server installation CD-ROM. You can use an unattended setup file to install Server2. For directions on using the unattended installation, see the Setup.txt file in the D:\70-394\Labs\Unattend\ folder.

3. Then, place the Windows Server 2003 CD-ROM in the CD-ROM drive. When you see the Press Any Key To Boot From The CD-ROM message, press the Space bar. If you want to use the unattended installation method, insert the floppy disk with the Winnt.sif immediately following this prompt. Otherwise, install manually, choosing options that are appropriate for your network.

Note Whether you are using the unattended or manual method, you should not fully complete the Server2 reinstallation at this point. Just begin the installation, but don’t go past the point of entering the Product Key code until you finish your work on Server1 (in the steps that follow). You need to be sure that you’ve removed all references of Server2 from Active Directory before you rejoin the domain.

4. Log on to Server1 using the domain administrator name and password.

Important If you are completing this exercise on a domain controller running Windows Server 2003 SP1, replace the following steps (5–18) with this new step 5:

Open a command prompt. Type `ntdsutil “metadata cleanup” “remove selected server” cn=Server2,cn=servers,cn=default-first-site-name ,cn=configuration,dc=contoso,dc=com`.

5. Open a command prompt. Type `ntdsutil` and press ENTER. The Ntdsutil prompt is displayed.

6. Type `metadata cleanup` and press ENTER. The metadata cleanup prompt is displayed.

7. Type `connections` and press ENTER. The server connections prompt is displayed.

8. Type `connect to server server1` and press ENTER.

9. Type `quit` and press ENTER. The metadata cleanup prompt appears again.

10. Type `select operation target`.
11. Type **list domains**. You should see only one domain and it should be numbered zero (0). If this is not the case, take note of which object and number represents `contoso.com` and use that number in the next step.

12. Type **select domain 0** and press ENTER.

13. Type **list sites** and press ENTER. You should see only one site and it should be numbered zero (0). If this is not the case, take note of which object and number represents your site and use that number in the next step.

14. Type **select site 0** and press ENTER.

15. Type **list servers in site** and press ENTER. You should see two servers. Take note of which number represents Server2, probably the number one (1). If that is not the case, then substitute the actual number of Server2 in the following step (instead of typing 1).

16. Type **select server 1** and press ENTER.

17. Type **quit** and press ENTER. The metadata cleanup prompt is displayed.

18. Type **remove selected server** and press ENTER. A prompt appears asking you to confirm the removal of Server2. Read this prompt carefully and then click Yes to remove the object.

19. Type **quit** and press ENTER twice. This closes the metadata cleanup and Ntdsutil prompts. Then type **exit** to close the command prompt.

20. You've now successfully removed the NTDS Setting object. However, there are still remnants of Server2 in the database. Therefore, you'll have to delete additional items using the DNS console and ADSIEdit.

21. Open the DNS console. Expand the structure as necessary to locate the `contoso.com` domain object and click on it.

22. In the right-hand pane, locate the (same as parent folder) Host (A) record that has the same IP address as Server2. Right-click that record and select Delete. Click Yes to confirm deletion.

23. Also in the right-hand pane, right-click the Server2 host record and select Delete. Click Yes to confirm deletion. You've now removed the DNS record for Server2. Close the DNS console.

24. Click Start, click Run, and then type **ADSIEdit.msc** and press ENTER. The ADSIEdit console opens.

25. Expand the following structure: Domain\DC=contoso,DC=com\OU=Domain Controllers. Click on the CN=Server2 object, and then press DELETE. Click Yes to confirm this deletion. You've now removed the Server object from the Active Directory Domain Name Context.
26. Expand the following structure: Configuration\CN=Configuration,DC=contoso, DC=com\CN=Sites\CN=Default-First-Site-Name\CN=Servers. Click on the CN=Server2 object, and then press DELETE. Click Yes to confirm this deletion.

You've now removed the Server object from the Configuration Name Context. Close the ADSIEdit console.

You've now successfully removed the references to Server2 in the Active Directory domain hosted by Server1. This is how you would clean up Active Directory after the loss of a domain controller. Now you should finish the installation of Server2. Then, join Server2 to the contoso.com domain as a member server. Directions on how to do that are covered in Chapter 2.

Chapter Summary

- The Active Directory administration tools include the Active Directory Domains And Trusts console, the Active Directory Sites And Services console, the Active Directory Users And Computers console, the Active Directory Schema snap-in, and the Active Directory-specific Windows Support Tools.


- Alternative UPN suffixes simplify administration and user logon processes by providing a single UPN suffix for all users. Using alternative domain names as the UPN suffix can provide additional logon security and simplify the names used to log on to another domain in the forest.

- Several additional tools that can be used to configure, manage, and debug Active Directory are available in the Windows Support Tools. To use these tools you must first install the Windows Support Tools on your computer.

- The MMC is a tool used to create, save, and open collections of administrative tools, called consoles. There are two types of MMCs: preconfigured and custom. Preconfigured MMCs contain commonly used snap-ins and appear on the Administrative Tools menu. You create custom MMCs to perform a unique set of administrative tasks.

- You use the Backup Or Restore Wizard to back up Active Directory.
When you back up Active Directory data, you must specify that you want to back up only system state data. You can only back up the system state data on a local computer. You cannot back up the system state data on a remote computer.

You restore Active Directory data by performing a nonauthoritative restore (default) or an authoritative restore. To restore the system state data on a domain controller, you must start your computer in directory services restore mode.

In a nonauthoritative restore, the distributed services on a domain controller are restored from backup media and the restored data is then updated through normal replication. Each restored directory partition is updated with that of its replication partners. An authoritative restore brings a domain or a container back to the state it was in at the time of backup and overwrites all changes made since the backup.

Exam Highlights

Before taking the exam, review the key points and terms that are presented in this chapter. You need to know this information.

Key Points

The Active Directory Domains And Trusts console provides the interface for setting the domain and forest functional levels and for specifying alternative UPN suffixes.


Alternative UPN suffixes simplify administration and user logon processes by providing a single UPN suffix for all users. Using alternative domain names as the UPN suffix can provide additional logon security and simplify the names used to log on to another domain in the forest.

You use the Backup Or Restore Wizard to back up Active Directory. To back up Active Directory data, you must specify that you want to back up only system state data. You cannot back up the system state data on a local computer. You cannot back up the system state data on a remote computer.

You restore Active Directory data by performing a nonauthoritative restore (default) or an authoritative restore. You must start your computer in directory services restore mode to initiate a restore.
Key Terms

**authoritative restore**  In Backup, a type of restore operation performed on an Active Directory domain controller in which the objects in the restored directory are treated as authoritative, replacing (through replication) all existing copies of those objects.

**domain functional level**  The level on which a domain running Windows Server 2003 is running. The functional level of a domain can be raised to enable new Active Directory features that will apply to that domain only.

**forest functional level**  The level on which a forest running Windows Server 2003 is running. The functional level of a forest can be raised to enable new Active Directory features that will apply to every domain in the forest.

**nonauthoritative restore**  A restore operation performed on an Active Directory domain controller in which the objects in the restored directory are not treated as authoritative. The restored objects are updated with changes held on other domain controllers in the domain.

**UPN suffix**  The part of the UPN to the right of the @ character. The default UPN suffix for a user account is the DNS domain name of the domain that contains the user account. The UPN suffix is only used within the Active Directory forest, and it is not required to be a valid DNS name.
Lesson 1 Review

1. What is the purpose of the Active Directory Domains And Trusts console?

The Active Directory Domains And Trusts console provides the interface to manage domains and manage trust relationships between forests and domains.

2. What is the purpose of the Active Directory Sites And Services console?

The Active Directory Sites And Services console contains information about the physical structure of your network.

3. What is the purpose of the Active Directory Users And Computers console?

The Active Directory Users And Computers console allows you to add, modify, delete, and organize Windows Server 2003 user accounts, computer accounts, security and distribution groups, and published resources in your organization’s directory. It also allows you to manage domain controllers and OUs.

4. Why isn’t the Active Directory Schema snap-in provided automatically on the Administrative Tools menu after you install Active Directory?

By default, the Active Directory Schema snap-in is not available on the Administrative Tools menu and must be installed. This action is required to ensure that the schema cannot be modified by accident.

5. Which Active Directory-specific Windows Support Tool enables you to manage Windows Server 2003 domains and trust relationships?

a. Ntdsutil.exe

b. Netdom.exe
c. Active Directory Domains And Trusts console
d. Nltest.exe

The correct answer is b. The Netdom.exe tool enables you to manage Windows Server 2003 domains and trust relationships. While the Active Directory Domains And Trusts console also provides this capability, this tool is not an Active Directory-specific Windows Support Tool.

Lesson 2 Review

1. What is the function of an MMC? Why is it necessary to create customized MMCs?

The MMC is a tool used to create, save, and open collections of administrative tools, which are called consoles. The console does not provide management functions itself, but is the program that hosts management applications called snap-ins. You create custom MMCs to perform a unique set of administrative tasks.
2. What is a snap-in?
Snap-ins are programs used by administrators to manage network services.

3. What is the function of a console tree?
A console tree displays the hierarchical organization of the snap-ins contained within an MMC.

4. What are extensions?
Extensions are snap-ins that provide additional administrative functionality to another snap-in.

5. Which of the following console mode types allows users to create new windows in the console?
   a. Author mode
   b. User mode—full access
   c. User mode—limited access, multiple window
   d. User mode—limited access, single window

The correct answer is a. Author mode allows users to add or remove snap-ins, create new windows in the console, view all portions of the console tree, and save MMCs.

Lesson 3 Review

1. What tasks should you complete before attempting to back up Active Directory data?
Before attempting to back up Active Directory data, you must prepare the files that you want to back up, and, if you are using a removable media device, you must prepare the device.

2. What is system state data and why is it significant to backing up Active Directory?
For the Windows Server 2003 operating system, the system state data comprises the registry, COM+ Class Registration database, system boot files, files under Windows File Protection, and the Certificate Services database (if the server is a certificate server). If the server is a domain controller, Active Directory and the Sysvol directory are also contained in the system state data. To back up Active Directory, you must back up the system state data.

3. Can you restrict who can gain access to a completed backup file or tape? If so, how?
You can restrict who can gain access to a completed backup file or tape by selecting the Replace The Data On The Media With This Backup option and the Allow Only The Owner And The Administrator Access To The Backup Data And To Any Backups Appended To This Medium option on the Backup Options page in the Backup Or Restore Wizard.

4. When you specify the items you want to back up in the Backup Or Restore Wizard, which of the following should you select to successfully back up Active Directory data?
   a. System state data
   b. Shared system volume folder
Chapter 3 Administering Active Directory

c. Database and log files
d. Registry

The correct answer is a. When you specify the items you want to back up in the Backup Or Restore Wizard, you must specify system state data to successfully back up Active Directory data.

Lesson 4 Review

1. Describe what happens in a nonauthoritative restore.

In a nonauthoritative restore, the distributed services on a domain controller are restored from backup media and the restored data is then updated through normal replication. Each restored directory partition is updated with that of its replication partners.

2. Describe what happens in an authoritative restore.

An authoritative restore brings a domain or a container back to the state it was in at the time of backup and overwrites all changes made since the backup.

3. Which method of restore should you use if you accidentally delete an OU?

Authoritative.

4. Which method of restore should you use if a domain controller has completely failed due to hardware or software problems?

Nonauthoritative.

5. Which of the following Ntdsutil command parameters should you use if you want to restore the entire directory?

a. Restore database
b. Restore subtree
c. Database restore
d. Subtree restore

The correct answer is a. Database restore and subtree restore are not Ntdsutil command parameters. Restore subtree is used to restore a portion or a subtree of the directory.

Case Scenario Exercise

1. Before you move on to upgrading the other departments, what should you do to ensure the Research department’s Active Directory data is protected? What should you ensure that Steve will continue to do in order to protect the Research department’s data?

First, the Research department should have a minimum of two domain controllers, so they have an online redundant copy of the Active Directory database. Second, they should be sure to back up the system state of the domain controllers routinely. Backing up system state data monthly
Chapter 3 Administering Active Directory

is probably the bare minimum. Remember, the default lifespan of an Active Directory backup is 60 days due to the tombstone lifetime.

Note Remember that Windows Server 2003 with SP1 extends the tombstone lifetime from 60 days to 180 days.

Performing system state backups on a weekly basis is common. They should also perform a backup anytime major changes are made to the Active Directory database, such as when large numbers of accounts are added, modified, or deleted. Also, they would be wise to run a system state backup if sites or domains are added, modified, or removed.

Note Also remember that Windows Server 2003 with SP1 includes event ID 2089, which provides the backup status of each directory partition that a domain controller stores, including application directory partitions. Monitoring for this event ID would indicate whether a directory service partition had not been backed up for a period of at least half the tombstone lifetime.

2. What similarities exist between the implementation of Active Directory in the Research and Marketing departments?

The need to determine which department will manage the DNS namespace. Also, what will that namespace be? (The answer is marketing.graphicdesigninstitute.com.) You should also install at least two Active Directory domain controllers and tell the network administration team for Research to make regular backups of Active Directory.

3. If you must install an additional Windows Server 2003 domain controller in the existing Administration domain, what must you do first to the Administration domain?

You must run Adprep.exe on the Windows 2000 domain so that it can support servers running Windows Server 2003 configured as domain controllers.

4. If you’re asked to upgrade the PDC of the Marketing domain, but hold off on the upgrade of the BDC, what functional level should you use on the new Windows 2003 Server domain?

The best option is Windows Server 2003 interim, since this domain is meant to interact only with Windows NT 4 domain controllers. That is all that is required in the Marketing department. Another option is the Windows 2000 mixed functional level because this option allows a Windows Server 2003 to interact with Windows 2000, Windows NT 4, and Windows Server 2003 products.
5. The network administrators of the Marketing domain want to know what the equivalent of the User Manager for Domains and the Server Manager applications are on Windows Server 2003 domain controller. What would you tell them?

User Manager for Domains and Server Manager allow you to add computer and user accounts. In Active Directory there is a single interface for doing this called Active Directory Users And Computers. The snap-in is Dsa.msc. Server Manager allows you to also control some items like shared directories. You can do that by accessing the Computer Management console. The fastest way to do so is to click Start, click Run, type `compmgmt.msc`, and then press ENTER.
4 Installing and Managing Domains, Trees, and Forests

Exam Objectives in this Chapter:

■ Plan flexible operations master role placement.
■ Plan for business continuity of operations master roles.
■ Identify operations master role dependencies.
■ Implement an Active Directory directory service forest and domain structure.
■ Create a child domain.
■ Establish trust relationships. Types of trust relationships might include external trusts, shortcut trusts, and cross-forest trusts.
■ Manage an Active Directory forest and domain structure.
■ Manage trust relationships.
■ Troubleshoot Active Directory.
■ Diagnose and resolve issues related to operations master role failure.

Why This Chapter Matters

This chapter shows you how to create the domains, trees, and forests that make up your Active Directory structure. Large organizations or those that have multiple autonomous departments often require Active Directory structures that include multiple domains. Other organizations may have the need to share data between previously autonomous business units or companies that have separate Active Directory forests. The Microsoft Windows Server 2003 Active Directory implementation has the ability to better conform to these situations than did the Microsoft Windows 2000 Active Directory implementation. As network administrator, you may be faced with situations in which you must be able to create multiple domains, rename domains, or restructure existing domains. You must also know how to protect your Active Directory structure from potential disasters and mistakes, so that you can restore data if necessary.
Lessons in this Chapter:

- Lesson 1: Creating Multiple Domains, Trees, and Forests ................. 4-3
- Lesson 2: Renaming and Restructuring Domains and Renaming Domain Controllers ......................................................... 4-18
- Lesson 3: Managing Operations Master Roles ................................. 4-23
- Lesson 4: Managing Trust Relationships ....................................... 4-39

Before You Begin

To complete the lessons in this chapter, you must

- Prepare your test environment according to the descriptions given in the “Getting Started” section of “About This Book”
- Complete the practices for installing and configuring Active Directory as discussed in Chapter 2, “Installing and Configuring Active Directory”
- Learn to use Active Directory administration tools as discussed in Chapter 3, “Administering Active Directory”
- Install the Windows Support Tools on Server2 as explained in Chapter 2