

Module 13: Maintaining the Active Directory Database

Contents

Overview	1
Introduction to Maintaining the Active Directory Database	2
The Process of Modifying Data in Active Directory	3
The Garbage Collection Process	5
Backing Up Active Directory	6
Restoring Active Directory	8
Lab A: Backing Up and Restoring Active Directory	16
Moving the Active Directory Database	24
Defragmenting the Active Directory Database	26
Lab B: Maintaining the Active Directory Database	31
Best Practices	35
Review	36



Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, places or events is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, BackOffice, FrontPage, IntelliMirror, PowerPoint, Visual Basic, Visual Studio, Win32, Windows, Windows Media, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Instructor Notes

Presentation:
60 Minutes

This module provides students with the knowledge and skills to manage and restore the Active Directory® directory service database.

Labs:
60 Minutes

At the end of this module, students will be able to:

- Describe the importance of maintaining the Active Directory database.
- Describe the process of modifying data in Active Directory.
- Describe the garbage collection process in Active Directory.
- Back up the system state data by using the Backup utility.
- Restore Active Directory by restoring the system state data.
- Move the Active Directory database to a new location.
- Defragment the Active Directory database.
- Apply best practices for maintaining the Active Directory database.

In the hands-on labs in this module, students will have the opportunity to maintain the Active Directory database. In the first lab, students will back up and perform a nonauthoritative and an authoritative restore of the Active Directory database. In the second lab, students will perform an offline defragmentation, run integrity and semantic database checks, move the Active Directory database to another folder, and redirect Active Directory to a new location.

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the following materials:

- Microsoft® PowerPoint® file 2154A_13.ppt

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the labs.
- Study the review questions and prepare alternative answers to discuss.
- Anticipate questions that students may ask. Write out the questions and provide the answers.
- Read chapter 2, “Active Directory Data Storage” in the Distributed Systems book in the Microsoft Windows® 2000 Server Resource Kit.
- Read chapter 9, “Active Directory Backup and Restore” in the Distributed Systems book in the Microsoft Windows 2000 Server Resource Kit.
- Read the white paper, *Windows 2000 Server Disaster Recovery Guidelines* on the Student Materials compact disc.

Module Strategy

Use the following strategy to present this module:

- Introduction to Maintaining the Active Directory Database

In this topic, you will introduce the purpose of maintaining the Active Directory database. Tell students that when referring to Active Directory in this module, it is the Active Directory information stored on a particular domain controller. The information on this domain controller may not contain all of the information in the Active Directory forest.

- The Process of Modifying Data in Active Directory

In this topic, you will introduce the process of modifying data. First, describe the different Active Directory files, and then use the illustration to explain the process of modifying data in Active Directory. Illustrate the process of modifying data in Active Directory by using the graphic provided for this topic.

- The Garbage Collection Process

In this topic, you will introduce the garbage collection process in Active Directory. Emphasize that the garbage collection process is used for deleting tombstones and for defragmentation.

- Backing Up Active Directory

In this topic, you will introduce the purpose of backing up Active Directory. Demonstrate how to back up system state data by using the Backup utility. Emphasize the guidelines that should be observed when backing up system state data.

- Restoring Active Directory

In this topic, you will introduce how to restore Active Directory by restoring the system state data. Discuss the purpose of a nonauthoritative restore. Demonstrate how to perform a nonauthoritative restore. Emphasize that a nonauthoritative restore simply restores the Active Directory data to the state in which it was backed up. Next discuss the purpose of an authoritative restore. Demonstrate how to perform an authoritative restore. Emphasize that in an authoritative restore, students can mark specific information in the database as current, thus preventing replication from overwriting that information.

- Lab A: Backing Up and Restoring Active Directory

Prepare students for the lab in which they will create a test organizational unit (OU) that will be deleted after a backup of the system state data. Next students will restore the most recent backup prior to the deletion of the test organizational units. They will also perform an authoritative restore for an OU. Finally, they will verify that the restore operation was successful by examining both authoritative and nonauthoritative data. After students have completed the lab, ask them if they have any questions concerning the lab.

- Moving the Active Directory Database

In this topic, you will introduce the purpose and the method used to move the Active Directory database to a new location whenever required. Demonstrate how to move the Active Directory database to a new location.

- Defragmenting the Active Directory Database

In this topic, you will introduce defragmentation. Explain why it is necessary to defragment the Active Directory database. Emphasize that online defragmentation occurs automatically during the garbage collection process, and the offline defragmentation must be performed manually. Tell students to perform offline defragmentation only if the disk space that will be recovered is significant enough to be used for other tasks.

- Lab B: Maintaining the Active Directory Database

Prepare students for the lab in which they will move the database on their domain controller to an alternate location and then perform an offline defragmentation to reclaim any disk space that was used by the global catalog information. Next students will perform a database integrity check and a semantic database analysis on the defragmented database. Then they will reconfigure Active Directory to use this database file without deleting the original files. After the new database is successfully online, they will delete the old database files. After students have completed the lab, ask them if they have any questions concerning the lab.

- Best Practices

Present best practices for maintaining Active Directory database. Emphasize the reason for each best practice.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

Important The labs in this module are also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for Course 2154, *Implementing and Administering Microsoft Windows 2000 Directory Services*.

Lab Setup

The following list describes the setup requirements for the labs in this module.

Setup Requirement 1

The labs in this module require student computers to be configured as domain controllers in child domains of nwtraders.msft. There are two student computers for each child domain. To prepare student computers to meet this requirement, perform one of the following actions:

- Complete the labs in Module 10, “Creating and Managing Trees and Forests,” in Course 2154, *Implementing and Administering Microsoft Windows 2000 Directory Services*.
- Run Change.vbs from the C:\Moc\Win2154A\Labfiles\Custom\Autode folder.
- Run Dcpromo.exe on the student computers by using the following parameters:
 - A domain controller for a new domain (first computer only).
 - The existing domain tree, which is nwtraders.msft (first computer only).
 - The domain controller for the existing domain (second computer only).
 - Full DNS domain name, which is *domain.nwtraders.msft* (where *domain* is the assigned domain name).
 - NetBIOS domain name, which is *DOMAIN*.
 - Default location for the database, log files, and SYSVOL.
 - Permission compatible only with Windows 2000–based servers.
 - Directory Services Restore Mode administrator password, which is **password**.

Setup Requirement 2

The labs in this module require the domain to be in native mode. To prepare student computers to meet this requirement, perform one of the following actions:

- Complete the labs in Module 10, “Creating and Managing Trees and Forests,” in Course 2154, *Implementing and Administering Microsoft Windows 2000 Directory Services*.
- Run Nativesd.vbs from the C:\Moc\Win2154a\Labfiles\Custom\Autodc folder.
- Change the domain mode to native in the *domain* (where *domain* is your assigned domain name) **Properties** dialog box in Active Directory Domains and Trusts.

Lab Results

Performing the labs in this module introduces the following configuration changes:

- The Active Directory database on each domain controller has been compacted and defragmented offline.
- A backup of the system state data is stored in C:\Backup.bkf for each student computer.
- The Backup_*restoreserver* (where *restoreserver* is the host name of the computer with the lower student number of the pair) OU is created.

Overview

Topic Objective

To provide an overview of the module topics and objectives.

Lead-in

In this module, you will learn about managing and restoring the Active Directory database.

- Introduction to Maintaining the Active Directory Database
- The Process of Modifying Data in Active Directory
- The Garbage Collection Process
- Backing Up Active Directory
- Restoring Active Directory
- Moving the Active Directory Database
- Defragmenting the Active Directory Database
- Best Practices

*****ILLEGAL FOR NON-TRAINER USE*****

Microsoft® Windows® 2000 Active Directory® directory service stores its information in a transactional database, therefore it is able to maintain the integrity of the data after a failure. The causes of a failure can range from hardware failure to a complete system loss, such as in the case of fire. The Active Directory database uses transaction log files to recover information regarding corrupted data. After recovering this information, Active Directory uses replication to recover data from other domain controllers in the domain. The interactions of Active Directory components provide the basis for how Active Directory backs up and retrieves data.

Backing up and restoring data is essential to maintaining the Active Directory database. You can back up and restore Active Directory by using the graphical user interface (GUI) and command-line tools provided in Microsoft Windows 2000 Advanced Server.

At the end of this module, you will be able to:

- Describe the importance of maintaining the Active Directory database.
- Describe the process of modifying data in Active Directory.
- Describe the garbage collection process in Active Directory.
- Back up the system state data by using the Backup utility.
- Restore Active Directory by restoring the system state data.
- Move the Active Directory database to a new location.
- Defragment the Active Directory database.
- Apply best practices for maintaining the Active Directory database.

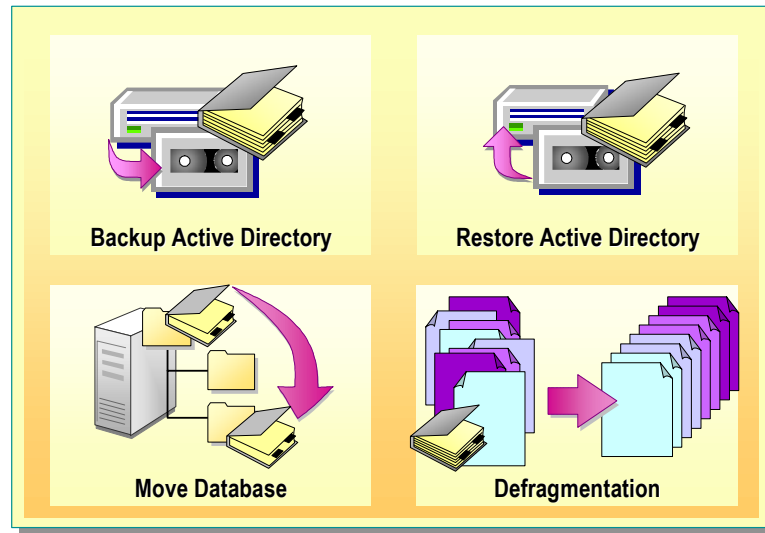
Introduction to Maintaining the Active Directory Database

Topic Objective

To introduce the importance of maintaining the Active Directory database.

Lead-in

Administrators maintain the Active Directory database by performing various tasks, which include backing up and restoring the database, moving the database to a new location, and defragmenting the database.



*****ILLEGAL FOR NON-TRAINER USE*****

This is an introduction topic. Do not go into details regarding maintaining the Active Directory database. The concepts introduced here are covered in detail in the succeeding topics.

When referring to Active Directory in this module, it is the Active Directory information stored on a particular domain controller. The information on this domain controller may not contain all of the information in the Active Directory forest.

Maintaining the Active Directory database is an important administrative task that needs to be regularly scheduled to help recover lost or corrupted data and repair the Active Directory database. When domain controllers do not function because of hardware or software problems, users may not be able to gain access to needed resources or to log on to the network. Windows 2000 Advanced Server provides the following tasks, which you can use for maintaining the Active Directory database:

- **Back up Active Directory.** You can use the Backup utility in Microsoft Windows 2000 to back up information in Active Directory. The information in Active Directory is backed up as part of the system state data.
- **Restore Active Directory.** When Active Directory is corrupted or deleted, or objects in Active Directory are changed or deleted. You can also use the Backup utility to restore Active Directory because it is part of the system state data.
- **Move the Active Directory database to a new location.** You move a database to a new location when you defragment the database. Moving the database does not delete the original database, so you can use the original database in case the defragmented database does not work or becomes corrupted. Also, if you have limited disk space, you can add another hard disk drive and move the database to the new hard disk drive.
- **Defragment the database.** Frequent updates to the database lead to an inefficient use of space in the database. Defragmenting the database can reorder the data, and in certain situations, can reduce the file size.

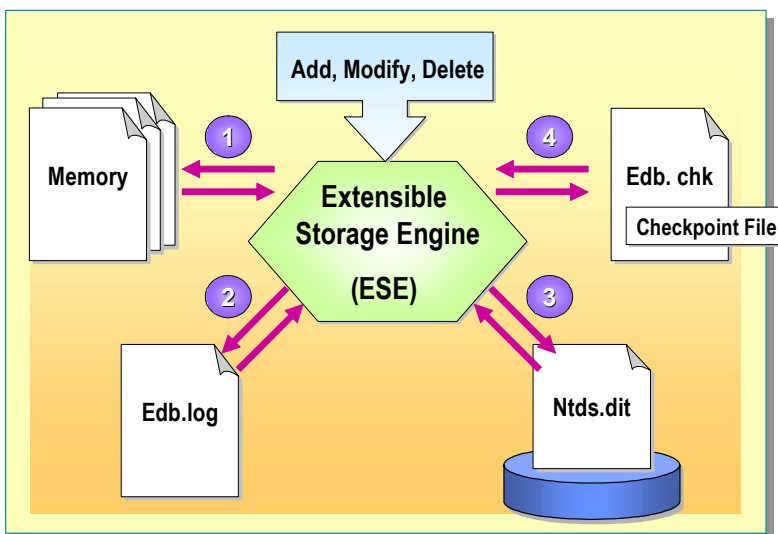
The Process of Modifying Data in Active Directory

Topic Objective

To identify the process of modifying data in Active Directory, and the process of garbage collection.

Lead-in

All updates, including adding, deleting, moving, or modifying an object in Active Directory, are accomplished by transactions.



*****ILLEGAL FOR NON-TRAINER USE*****

Use the illustration to explain the process of modifying data in Active Directory.

Key Points

Ntds.dit is the Active Directory database and stores all of the Active Directory objects on the domain controller.

Edb*.log is a transaction log file.

Edb.chk is a checkpoint file used by the database engine to track the data not yet written to the Active Directory database file.

Res1.log and Res2.log are the reserved transaction log files.

Each request to Active Directory to add, modify, or delete an object or attribute is treated as an individual *transaction*. A transaction is a set of changes, such as inserts, deletes, and updates, that act as an atomic unit.

Active Directory has its own database engine, called the Extensible Storage Engine (ESE), which stores all Active Directory objects. The ESE uses a concept of transactions and log files to ensure the integrity of the Active Directory database.

The Files in Active Directory

Active Directory includes the following files:

- Ntds.dit. This single file is the Active Directory database and stores all of the Active Directory objects on the domain controller. The .dit extension means directory information tree. The default location is the *systemroot\NTDS* folder. Each transaction in Active Directory is recorded in one or more transaction log files that are associated with the Ntds.dit file.
- Edb*.log. This is a transaction log file. The default transaction log file name is Edb.log. Each transaction log file is 10 megabytes (MB). When Edb.log is full, it is renamed to Edbnnnnn.log, where *nnnnn* is an increasing number starting from one.
- Edb.chk. This is a checkpoint file used by the database engine to track the data not yet written to the Active Directory database file. The checkpoint file is a pointer that maintains the status between memory and the database file on disk. The checkpoint file pointer indicates the starting point in the log file from which the information needs to be recovered if there has been a failure.
- Res1.log and Res2.log. These are the reserved transaction log files. The amount of disk space reserved on a drive or folder for the transaction logs is 20 MB. This reserved disk space provides the transaction log files sufficient room to shut down if all other disk space is being used.

The Database Modification Process

The following occurs when data is modified in Active Directory:

1. ESE loads the data that is to be modified into memory. ESE caches the disk in memory by swapping chunks of data, called pages, in and out of memory. ESE updates the pages in memory and writes new or updated pages back to the disk. This update enables ESE to buffer data in memory so that ESE does not need to constantly retrieve data from the hard disk. Making multiple modifications to the memory results in fewer writes to the disk. This caching speeds up performance. When users make requests, ESE starts loading the requests into memory and marks the pages. These marked pages are then written to the information store database on the disk.
2. ESE secures the transaction in the transaction log file, Edb.log, and creates a record in the log file. When ESE reaches the end of a transaction log file, it renames Edb.log to Edbnnnnn.log and creates a new log file. Old log files no longer needed are automatically deleted.
3. ESE writes the change stored in memory to the database file, Ntds.dit, on the disk.
4. The checkpoint file, Edb.chk, is updated, which indicates that the transaction in the log file has been committed to the database.

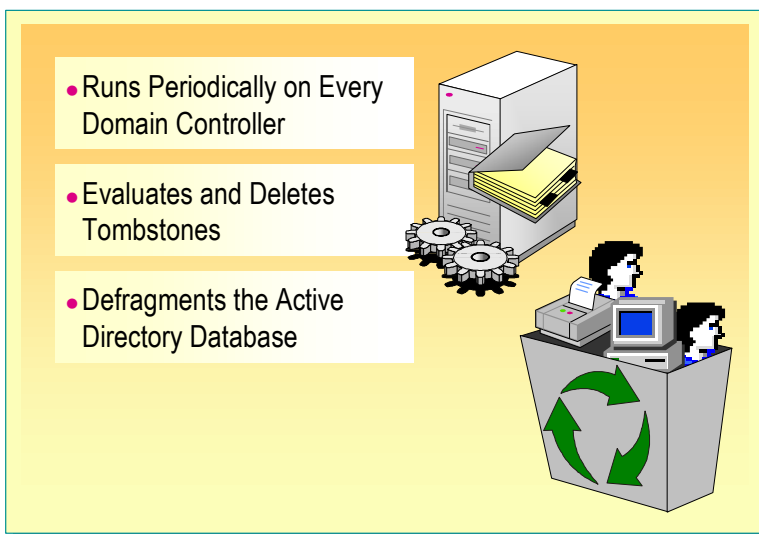
The Garbage Collection Process

Topic Objective

To describe the garbage collection process in Active Directory.

Lead-in

Garbage collection is a process that runs on every domain controller at regular intervals to delete objects that are no longer needed by Active Directory.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

Tombstones are markers that indicate that an object has been deleted.

Tombstone lifetime is a delay between the time an object is marked with the originating delete and the time it is physically removed from the database.

Defragmentation rearranges how the data is written in the database, and in some cases compacts the database.

Garbage collection is a process that runs on every domain controller after every 12 hours of continuous operation to delete objects that are expired, or tombstoned, and defragment the database. You can change the garbage collection interval. The garbage collection is used for the following tasks:

- Evaluate and delete tombstones. Tombstones are markers that indicate that an object has been deleted. Rather than immediately physically deleting a designated object, the database removes most of its attributes, moves it to the Deleted Objects folder, and then marks the object as being tombstoned. There is a delay between the time an object is marked with the originating delete and the time it is physically removed from the database. This delay period is called the *tombstone lifetime*. The delay exists to provide an interval during which the originating domain controller can replicate the deletion to other domain controllers in the forest. The database removes the tombstoned object at the completion of the tombstone lifetime. You can configure the tombstone lifetime interval or use the default of 60 days.
- Defragment the database. The defragmentation process rearranges how the data is written in the database, and in some cases compacts the database. Defragmentation can occur either automatically or manually. The garbage collection process always uses the online defragmentation process.

Note To configure the garbage collection interval and tombstone lifetime, use ADSI Edit to connect to the Configuration container of the domain controller. In the configuration partition, open the properties of Configuration/Services/Windows NT/Directory Service. In the **Select a property to view** box, click the down arrow and scroll down to the garbageCollPeriod attribute and the tombstoneLifetime attribute and edit the values. The default value appears as <not set>.

Backing Up Active Directory

Topic Objective

To identify how to back up the system state data by using the Backup utility.

Lead-in

Backup automatically backs up all of the system state data upon which Active Directory is dependent.

■ The System State Data Includes:

- Active Directory and the SYSVOL folder on a domain controller
- The registry, system startup files, and class registration database on all computers
- The Certificate Services database on certificate servers

To Back Up Active Directory

- 1** Start the Backup utility
- 2** Open the the Backup wizard
- 3** Select a method to back up the system state data

*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate how to back up Active Directory.

Key Point

The system state data includes Active Directory, the SYSVOL shared folder, the registry, the system startup files, the class registration database, and the Certificate Services database.

Backup in Windows 2000 Advanced Server has several features that make backing up Active Directory very easy. You can also integrate backing up Active Directory into your regular backup procedures without interrupting the network or the operation of the domain controller you are backing up.

The System State Data

Also, when you back up Active Directory, Backup automatically backs up all of the system components and distributed services upon which Active Directory is dependent. This dependent data is known collectively as the *system state data*.

The system state data on a domain controller includes the following:

- *Active Directory* (only on domain controllers).
- *The SYSVOL shared folder* (only on domain controllers). The SYSVOL folder is a shared folder that contains Group Policy templates and logon scripts.
- *The registry*. The registry is a database repository for information about the computer's configuration.
- *System startup files*. The system startup files are required during the initial startup phase of Windows 2000 Advanced Server.
- *Class registration database*. The class registration is a database of information about Component Services applications.
- *The Certificate Services database* (if the server is operating as a certificate server). The Certificate Services database contains certificates that Windows 2000 Advanced Server uses to authenticate users.

Backing Up the System State Data

To back up the system state data, perform the following steps:

1. On the **Start** menu, point to **Programs**, point to **Accessories**, point to **System Tools**, and then click **Backup**.
2. Click the **Backup Wizard** icon to open the Backup wizard.
3. You back up the system state data on a local computer in one of the following three ways:
 - In the Backup wizard, on the **What to Back Up** page, click **Only back up the System State data**.
 - In the Backup wizard, on the **Items to Back Up** page, expand **My Computer**, and then select the **System State** check box.
 - In the **Backup** dialog box, on the **Backup** tab, expand **My Computer**, and then select the **System State** check box.

You can use the advanced backup options in Backup to set or configure parameters, such as data verification, hardware compression, media labels, whether you want the backup job appended to a previous job, and whether you want to schedule the backup to run unattended at another time. Data verification enables Backup to check whether there are differences between the files it backed up from the domain controller and those copied to the backup media. The results of the verification are reported in Event Viewer.

Important For full disaster recovery, back up all hard disks and the system state data. To perform this backup, run Backup, and in the Backup wizard, on the **What to Back Up** page, select **Back up everything on my computer**.

Guidelines for Backing Up System State Data

Observe the following guidelines when backing up system state data:

- You must have the permission to back up files and folders. The members of the Administrators, Backup Operator, and Server Operator groups have the permission to back up files/folders by default.
- System state data does not contain Active Directory unless the server on which you are backing up the system state data is a domain controller.
- You can back up the system state data by itself, or you can back up the system state data as part of your regular backup procedures.
- You can back up the system state data while the domain controller is online.

Important Because Backup supports only local backups of Active Directory, you must perform a backup on every domain controller in the enterprise to entirely back up Active Directory. You cannot back up Active Directory on a remote computer without using third party tools, such as VERITAS.

◆ Restoring Active Directory

Topic Objective

To introduce the topics related to restoring Active Directory.

Lead-in

Because the system state data is a collection of data that defines the configuration of the operating system, you need to restore it when it is corrupted.

- What Is a Nonauthoritative Restore?
- Performing a Nonauthoritative Restore
- What Is an Authoritative Restore?
- Performing an Authoritative Restore

*****ILLEGAL FOR NON-TRAINER USE*****

Windows 2000 provides you with the ability to restore the Active Directory database if it becomes corrupted or is destroyed due to hardware or software failures. There are two methods for restoring replicated data on a domain controller. You can reinstall the domain controller, and then let the normal replication process repopulate the new domain controller with data from its replicas, or you can use Backup to restore replicated data from backup media without reinstalling the operating system or reconfiguring the domain controller. There are two methods for restoring Active Directory from backup media, which are the *nonauthoritative* method and the *authoritative* method.

When you want to restore a recently deleted object to its previous undeleted state, perform an authoritative restore of that object. However, in cases in which you need to recover Active Directory from hardware failure, you need to perform only a nonauthoritative restore from the most recent backup. After the nonauthoritative restore, Active Directory replication automatically begins propagating any changes from other domain controllers that occurred after the time of the backup.

What Is a Nonauthoritative Restore?

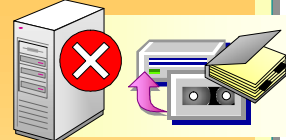
Topic Objective

To identify the purpose of a nonauthoritative restore.

Lead-in

You perform a nonauthoritative restore to reinstate the Active Directory data to the state it was in before the backup.

- **A Nonauthoritative Restore Reinstates the Active Directory Data to the State Before the Backup**



- **Distributed Services Are Restored from Backup Media and the Restored Data Is Then Updated Through Replication**
- **Backup Performs Only a Nonauthoritative Restore of Active Directory**
- **After Restoring Active Directory, Windows 2000 Automatically:**
 - Performs a consistency check, and recalculates the indexes in the the database
 - Updates Active Directory and FRS

*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

A nonauthoritative restore simply restores the Active Directory data to the state it was in when it was backed up. If any of the Active Directory objects were updated or deleted, when replication occurs, the restored data will be updated to the current state of the objects.

A nonauthoritative restore does not permanently alter the values of objects. If there are other domain controllers, they replicate the current information to this domain controller after the restore.

A nonauthoritative restore reinstates the Active Directory data to the state it was in before the backup. If any objects were updated or deleted before the backup, when replication occurs, the restored data will be updated to the current state of the objects.

During 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. One example of a situation in which you use nonauthoritative restore is a hard disk failure that requires replacing the primary hard disk on a domain controller. You format the new disk, recreate the partitions as they were before the failure, reinstall Windows 2000 Advanced Server on the primary partition, restore all data files that you had on the computer, and then restore the distributed services, including the entire Active Directory.

Backup performs only a nonauthoritative restore of Active Directory. When the domain controller is brought online after a nonauthoritative restore, it detects that the restored data has not been updated since the backup was performed. Therefore, after you have restored Active Directory, Windows 2000 automatically:

- Performs a consistency check on and recalculates the indexes in the Active Directory database.
- Updates Active Directory and File Replication service (FRS) with data from their replication partners.

Performing a Nonauthoritative Restore

Topic Objective

To identify the steps to perform a nonauthoritative restore.

Lead-in

You can restore Active Directory nonauthoritatively by using the Backup utility.

- Active Directory Can Be Restored While Replacing a Failed Domain Controller and When Repairing a Damaged Active Directory Database
- The Active Directory Database Cannot Be Running When You Restore Active Directory Files
- The Backup of the System State Data Cannot Be Older Than the Tombstone Lifetime

To Restore Active Directory Nonauthoritatively

- 1 Restart the domain controller
- 2 Select Directory Services Restore Mode
- 3 Log on to Windows 2000 using SAM account
- 4 Restore the system state
- 5 Restart the domain controller normally

*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate how to perform a nonauthoritative restore.

You can restore Active Directory nonauthoritatively during the process of replacing a failed domain controller, and when repairing a damaged Active Directory database.

If the operating system on a domain controller is functioning normally, but the Active Directory database is damaged, you must restart the computer, select the **Directory Services Restore Mode** advanced startup option, and then use Backup to restore the latest system state data. Because Active Directory is part of the system state data on a domain controller, you must restore the system state data to restore Active Directory. Backup cannot replace Active Directory files while Active Directory is running. Therefore, you must start the operating system by using the **Directory Services Restore Mode** advanced startup option.

Important You cannot restore Active Directory from a backup that is more than the tombstone lifetime, which is 60 days by default. A domain controller keeps track of deleted objects for only this period.

If you have only one domain controller, any changes that you made since the last backup are lost. If you have multiple domain controllers, and the age of the backup is less than the tombstone lifetime, restore the backup that you have and then let the replication between domain controllers make Active Directory current.

To restore Active Directory nonauthoritatively, perform the following steps:

1. Restart the domain controller, and then press F8 to display the advanced startup options.
2. Select **Directory Services Restore Mode** to start Windows 2000; however, this selection does not automatically start Active Directory.
3. Log on to Windows 2000 by using the Administrator account that resides in the local user account database on the domain controller.
4. Use Backup to restore the latest system state data.
5. Restart the domain controller as you normally would.

After the computer restarts, Windows 2000 Advanced Server performs consistency checks, initializes (re-indexes) the Active Directory database, and updates Active Directory information and FRS data from the computer's replication partners. If there are multiple domain controllers, after replication has occurred, the domain controller's Active Directory database is made current.

Warning When you restore the system state data, Backup erases the system state data that is currently on your computer and replaces it with the system state data that you are restoring. Depending on how old the system state data is, you may lose configuration changes that you have recently made to the computer. To minimize the risk of losing your configuration changes, back up this data regularly.

What Is an Authoritative Restore?

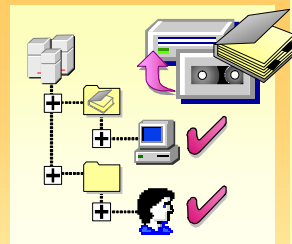
Topic Objective

To identify the purpose of an authoritative restore.

Lead-in

You can also restore individual Active Directory objects in a domain with multiple domain controllers by performing an authoritative restore.

- **An Authoritative Restore Allows You to Mark Specific Information in the Database**
- **Authoritative Restore Occurs After Nonauthoritative Restore Has Been Performed**
- **The Version Number of Each Object Marked As Authoritative Is Increased by 100,000 for Each Day**
- **The Domain Controller with the Higher Version Number for the Same Object Replicates over the Domain Controller with the Lower Version Number**



*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

An authoritative restore is simply marking specific objects, or the entire database, as the most current in Active Directory.

Replication from another domain controller does not overwrite the values of the objects marked authoritative because the version number of each attribute of the authoritative objects is increased by a large number.

An authoritative restore is the method that you use to restore individual Active Directory objects in a domain with multiple domain controllers. By using an authoritative restore, you can mark specific information in the database as current, thus preventing replication from overwriting that information. When you restore container objects, all objects in the organizational unit (OU) are also restored.

An authoritative restore occurs after a nonauthoritative restore has been performed. An authoritative restore is typically used to restore Active Directory to a previously known state; for example, before Active Directory objects were erroneously deleted.

Note You cannot mark the schema directory partition as authoritative; therefore, schema changes cannot be undone using an authoritative restore.

When you mark an object as authoritative, it has the highest *version number* in Active Directory. The version is a number, starting at one, that is incremented for each originating update to the Active Directory database. By default, the version number of each object marked as authoritative is increased by 100,000 for each day between when the backup occurred and when the restore occurred. Increasing the version number ensures that when replication of that object occurs, the authoritatively restored value replaces any update that occurred since the backup. The assumption is that the object did not change 100,000 times every day since the backup. During replication, the version number is checked before the timestamp to avoid replication conflicts. The version number is stored as a 64-bit value. You can change the default increment number for the new version number.

When two domain controllers have different version numbers for the same object, the change with the highest number replicates over the other copy of the object. By assigning the highest version number to the objects, you ensure that updates to the object since the backup do not overwrite the authoritative value during replication. Only deletions or changes that occur to the authoritatively restored object take effect.

For information about on how version numbers are used to help resolve replication conflicts, see Module 11, “Managing Active Directory Replication,” in Course 2154, *Implementing and Administering Microsoft Windows 2000 Directory Services*.

Note If you do not use an authoritative restore, the restored object has the version number that it had when it was backed up. Any change to the object after backup, such as an incorrect deletion, has a higher version number. The changed object version would replicate over the restored object version. If you have only one domain controller, this scenario does not apply.

Performing an Authoritative Restore

Topic Objective

To illustrate how to perform an authoritative restore.

Lead-in

To perform an authoritative restore, you mark Active Directory objects as authoritative.

To Restore Active Directory Authoritatively	
1	Start the domain controller, and then select Directory Services Restore Mode
2	Restore Active Directory (the system state data), but do not restart the computer
3	Run Ntdsutil.exe
4	Switch to the authoritative restore prompt
5	Provide the distinguished name of the object
6	Exit Ntdsutil
7	Restart the domain controller normally

*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate how to perform an authoritative restore.

Ntdsutil.exe is a utility that allows you to mark Active Directory objects as authoritative so that they receive a higher version number, which prevents recently changed data on other domain controllers from overwriting that information during replication.

To implement an authoritative restore, perform the following steps:

1. Start the domain controller, press F8, and then on the **Advanced Startup Options** menu, click **Directory Services Restore Mode**. You select this mode because Active Directory cannot be running during this process. Log on using the Administrator account that resides in the local user account database on the domain controller.
2. Restore Active Directory to its original location. Also, restore Active Directory to an alternate location when you need to perform an authoritative restore on SYSVOL. Use Backup to restore the system state data, but *do not restart* the computer when prompted after the restore.
3. Open a command prompt window, and run Ntdsutil.exe.
4. Switch to the **authoritative restore** prompt. At the **ntdsutil** prompt, type **authoritative restore**
5. At the **authoritative restore** prompt, type
restore subtree distinguished_name_of_object
 where *distinguished_name_of_object* is the distinguished name, or path, to the object. For example, if you want to restore an OU called Sales, which existed directly below the domain called contoso.msft, type
restore subtree OU=Sales,DC=contoso,DC=msft
 For more information about distinguished user names, see Appendix C, "LDAP Names," on the Student Materials compact disc.
6. Type **quit** and then press ENTER. Type **quit** again, and then press ENTER to exit **ntdsutil**.
7. Restart the domain controller as you normally would.

When you perform an authoritative restore of the Active Directory database, or a portion of the Active Directory database including Group Policy objects, you must perform an additional procedure involving the SYSVOL folder to ensure the proper elements are authoritatively restored.

After the SYSVOL folder is published by the File Replication service (FRS), copy the SYSVOL folder, and copy only Group Policy folders corresponding to the restored Group Policy objects from the alternate location to the existing locations. You can verify that the copy was successful by checking the contents of the SYSVOL\domain folder.

Lab A: Backing Up and Restoring Active Directory

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will backup and restore Active Directory. You will perform an authoritative restore and a nonauthoritative restore of Active Directory.



*****ILLEGAL FOR NON-TRAINER USE*****

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Perform a backup of the Active Directory database.
- Perform a nonauthoritative restore of the Active Directory database.
- Perform an authoritative restore of the Active Directory database.

Prerequisites

Before working on this lab, you must have:

- Knowledge and experience initiating Active Directory replication.
- Experience creating objects in Active Directory.

Key Points

The lab does not reflect the real-world environment. It is recommended that you always use complex passwords for any administrator accounts, and never create accounts without a password.

Outside of the classroom environment, it is strongly advised that you use the most recent software updates that are necessary. Because this is a classroom environment, we may use software that does not include the latest updates.

Important The lab does not reflect the real-world environment. It is recommended that you always use complex passwords for any administrator accounts, and never create accounts without a password.

Important Outside of the classroom environment, it is strongly advised that you use the most recent software updates that are necessary. Because this is a classroom environment, we may use software that does not include the latest updates.

Scenario

You are verifying Northwind Traders disaster recovery procedures for Active Directory. These procedures document backing up the system state data on domain controllers and then restoring it. Of particular interest to the organization is the safe restoration of accidentally deleted organizational units.

Estimated time to complete this lab: 30 minutes

Exercise 1

Backing Up Active Directory

Scenario

Northwind Traders developed disaster recovery procedures. The backup procedures need to be tested to ensure they are adequate before they are implemented in the entire organization.

Goal

In this exercise, you will create a test organizational unit that will be deleted after a backup of the computer's system state data.

Note: You will work with a partner and be grouped by domain in this exercise.

Tasks	Detailed Steps
1. Within <i>domain.nwtraders.msft</i> (where <i>domain</i> is your assigned domain name), create the following OU: Backup_<i>servername</i> (where <i>servername</i> is the host name of your computer).	a. Log on as Administrator in your domain with a password of password. b. Open Active Directory Users and Computers from the Administrative Tools menu. c. In the console tree, expand <i>domain.nwtraders.msft</i> (where <i>domain</i> is your assigned domain name), right-click <i>domain.nwtraders.msft</i>, point to New, and then click Organizational Unit. d. In the New Object – Organizational Unit dialog box, in the Name box, type Backup_<i>servername</i> (where <i>servername</i> is the name of your computer), and then click OK.
 Important: Wait until both you and your partner complete task 1 before starting task 2.	
2. Initiate replication with your partner's domain controller.	a. Open Active Directory Sites and Services from the Administrative Tools menu. b. Expand Sites, expand Default-First-Site-Name, expand Servers, expand <i>servername</i>, and then click NTDS Settings. c. Right-click the connection object from your partner's server, click Replicate Now, and then click OK to close the message indicating that replication was successful. d. In Active Directory Users and Computers, click <i>domain.nwtraders.msft</i> and press F5 to refresh the display. e. Verify that both organizational units Backup_<i>servername</i> and Backup_<i>partnerserver</i> (where <i>partnerserver</i> is the host name of your partner's computer) appear. Note: If your partner's organizational unit does not appear, perform steps c and d again. f. Close Active Directory Sites and Services.

Tasks	Detailed Steps
3. Start the backup of your domain controller's system state data to a file called C:\Backup.bkf by using detailed logging.	- Click Start, point to Programs, point to Accessories, point to System Tools, and then click Backup. - In the Backup – [Untitled] window, on the Tools menu, click Options. - In the Options dialog box, on the Backup Log tab, click Detailed to enable detailed logging, and then click OK. - In the Backup –[Untitled] window, click Backup Wizard. - On the Welcome to the Windows 2000 Backup and Recovery Tools page, click Next to continue. - On the What to Back Up page, click Only back up the System State data, and then click Next. - On the Where to Store the Backup page, in the Backup media or file name box, type C:\Backup.bkf and then click Next. - On the Completing the Backup Wizard page, click Finish. - Proceed to task 4, allowing the backup process to continue in the background.
4. While allowing the backup process to complete in the background, determine the invocation ID for the domain controller that will perform the restore.	- Open a command prompt window. - At the command prompt, type repadmin /showreps restoreserver (where <i>restoreserver</i> is the host name of the computer with the lower student number of the pair), and then press ENTER.
 What is the purpose of the invocation ID? Write down the invocation ID (or copy and paste it to a text file) of <i>restoreserver</i>. This information will be used for comparisons in a later exercise. Is this invocation ID different from the objectGUID? The invocation ID is for identifying the database and the objectGUID is for identifying the server. The invocation ID is unique for each domain controller. The invocation ID value may or may not be the same as the objectGUID.	
5. While allowing the backup process to complete in the background, determine the version number of Backup_ <i>restoreserver</i> (where <i>restoreserver</i> is the host name of the computer with the lower student number of the pair).	At the command prompt, type repadmin /showmeta "ou=Backup_restoreserver,dc=Domain,dc=nwtraders,dc=msft" and then press ENTER.

Tasks	Detailed Steps
? What is the version number for the name attribute of the Backup_<i>restoreserver</i> organizational unit? The version number for the name attribute is 1.	
5. <i>(continued)</i>	b. Close the command prompt window.
6. After the backup process completes, view the report, and then close Backup.	a. In Backup, in the Backup Progress dialog box, click Report. b. Review the backup log to see the files that are part of the system state for a domain controller, and then close the log file. c. In the Backup Progress dialog box, click Close, and then close Backup.
7. Delete both test organizational units: Backup_ <i>servername</i> and Backup_ <i>partnerserver</i> (where <i>partnerserver</i> is the host name of your partner's computer).	a. In Active Directory Users and Computers, click Backup_<i>servername</i>, press DELETE, and then click Yes to close the message confirming the deletion. b. Click Backup_<i>partnerserver</i>, press DELETE, and then click Yes to close the message confirming the deletion. c. Close Active Directory Users and Computers.

Exercise 2

Restoring Active Directory

Scenario

Northwind Traders developed disaster recovery procedures. The restore procedures, including authoritative restore, need to be tested before they are implemented in the entire organization.

Goal

In this exercise, you will restore the most recent backup prior to the deletion of the test organizational units. For one of the test organizational units, you will perform an authoritative restore.

Note: Only the domain controller with the lower student number of the pair is used in this exercise. This domain controller is designated as the restore server.

Tasks	Detailed Steps
 Important: Perform this exercise only on the domain controller designated as the restore server.	
1. Restart your domain controller in Directory Services Restore Mode, and then log on as Administrator.	- Close any open applications and restart your domain controller. - When the Boot Loader menu appears or when the message “For troubleshooting and advanced startup options for Windows 2000, press F8” appears at the bottom of the screen, press F8. - On the Windows 2000 Advanced Options menu, click Directory Services Restore Mode, and then press ENTER. - Log on as Administrator in your domain with a password of password, and then click OK to close the message indicating that Windows is running in safe mode.
2. Restore your domain controller's system state from a file named C:\Backup.bkf.	- Open Backup. - In the Backup –[Untitled] window, on the Welcome tab, click Restore Wizard to start the Restore wizard. - On the Welcome to the Restore Wizard page, click Next to continue. - On the What to Restore page, expand File, expand Media created, select the System State check box, and then click Next. - On the Completing the Restore Wizard page, click Finish. - In the Enter Backup File Name dialog box, in the Restore from backup file box, type C:\Backup.bkf and then click OK. - After the restore process completes, click Close, click No to close the message asking to restart you computer, and then close Backup.

Tasks	Detailed Steps
3. After the restore process is completed, mark the Backup_restoreserver OU to be restored authoritatively.	a. Open a command prompt window. b. At the command prompt, type ntdsutil and then press ENTER. c. At the ntdsutil prompt, type authoritative restore and then press ENTER. d. At the authoritative restore prompt, type ? and then press ENTER.  <i>Review the available options.</i> e. At the authoritative restore prompt, type restore subtree "ou=Backup_restoreserver,dc=domain,dc=nwtraders,dc=msft" press ENTER, and then click Yes to close the message confirming the authoritative restore. f. At the authoritative restore prompt, type quit and then press ENTER to change to the previous menu. g. At the ntdsutil prompt, type quit and then press ENTER to exit ntdsutil.
4. Restart the domain controller and log on as Administrator.	a. Close the command prompt window, and then restart the computer. b. Log on as Administrator in your domain with a password of password.

Exercise 3

Verifying a Restore of Active Directory

Scenario

Northwind Traders developed disaster recovery procedures. The verification procedures of an authoritative and nonauthoritative restore need to be tested before they are implemented in the entire organization.

Goal

In this exercise, you will verify that the restore operation was successful by examining both authoritative and nonauthoritative data.

Tasks	Detailed Steps
1. Initiate replication with your partner's domain controller.	a. Open Active Directory Sites and Services, expand Sites, expand Default-First-Site-Link-Name, expand Servers, expand <i>servername</i>, and then click NTDS Settings. b. Right-click the connection object from your partner's server, click Replicate Now, and then click OK to close the message indicating that replication was initiated. Note: If an error message appears stating the RPC service is unavailable, wait a moment and then repeat step c. It may take some time to get all of the necessary services running after restarting the computer. c. Close Active Directory Sites and Services. d. Open Active Directory Users and Computers, click <i>domain.nwtraders.msft</i>, and then press F5 to refresh the display.
 Which Backup_<i>servername</i> organizational units are still in Active Directory after replication with your partner's computer and why? The Backup_<i>restoreserver</i> organizational unit is there because it was restored authoritatively. The other organizational unit is not there because although it was restored, replication with the other domain controller deleted it again.	
1. (continued)	e. Close Active Directory Users and Computers.
2. Determine any changes made to the invocation ID for the domain controller that performed the restore.	▪ At a command prompt, type repadmin /showreps restoreserver and then press ENTER.

Tasks	Detailed Steps
? Is the invocation ID for the <i>restoreserver</i> the same value as it was before the restore? Is this invocation ID different from the objectGUID? The invocation ID is different than before the restore. One function of the restore is to change the invocation ID. The invocation ID is not the same as the objectGUID.	
3. Determine any changes made to the version number of Backup_<i>restoreserver</i>, and then log off.	a. At a command prompt, type repadmin /showmeta "ou=Backup_restoreserver,dc=domain,dc=nwtraders,dc=msft" and then press ENTER.
? What is the version number for the name attribute of the Backup_<i>restoreserver</i> organizational unit? The version number for the name attribute is 100,000 greater than it was before the restore.	
3. <i>(continued)</i>	b. Close the command prompt window, close all other open windows, and then log off.

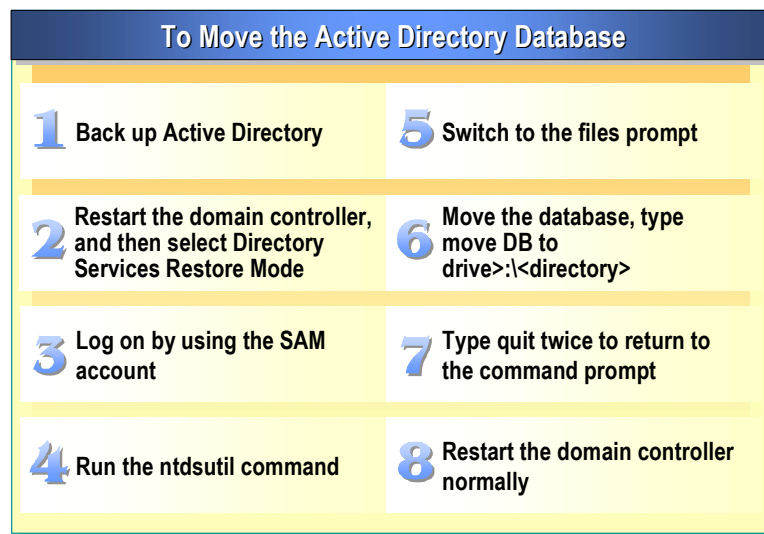
Moving the Active Directory Database

Topic Objective

To illustrate how to move the Active Directory database to a new location.

Lead-in

You can use the **ntdsutil** command in Directory Services Restore mode to move the Active Directory database from one location to another location on the disk.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate how to move the Active Directory database to a new location.

You use the **ntdsutil** command-line utility in Directory Services Restore mode to move the database from one location to another location on the disk. The **ntdsutil** command-line utility moves the database files to a new location and then updates the registry keys so that Active Directory restarts from the new location.

To move the Active Directory database, perform the following steps:

1. Back up Active Directory as a precautionary measure. You can back up Active Directory while online if in the Backup wizard, you have selected either the option to back up everything on the computer, or the option to back up the system state data.
2. Restart the domain controller, press F8 to display the **Windows 2000 Advanced Options** menu, click **Directory Services Restore Mode**, and then press ENTER.
3. Log on by using the Administrator account and the password defined for the Local Administrator account in the Security Accounts Manager (SAM).
4. At the command prompt, type **ntdsutil** and then press ENTER.
5. Type **files** and then press ENTER. This switches you to the **files** prompt, so that you can manage the Ntds.dit database file.

-
6. After you establish a location that has enough drive space for the database to be stored, type the following, and then press ENTER:

move DB to <drive>:\<directory>

where <drive> and <directory> is the path to the location where you want to place the database.

Note You must specify a directory path. If the path contains any spaces, the entire path must be surrounded by quotation marks, for example, "C:\New folder"

The database named Ntds.dit is moved to the location that you specified.

7. Type **quit** and then press ENTER. To return to the command prompt, type **quit** again.
8. Restart the domain controller as you normally would.

Note You can also move the transaction log files to another location. The **Move logs to** <drive>:\<directory> command moves the transaction log files to the new directory specified by <drive>:\<directory> and updates the registry keys so that the directory service restarts from the new location.

◆ Defragmenting the Active Directory Database

Topic Objective

To introduce the topics related to defragmenting the Active Directory database.

Lead-in

Fragmentation degrades the overall performance of the Active Directory database operations. You defragment the Active Directory database to increase the speed of access and retrieval.

- What Is Defragmentation?
- Defragmenting a Database

*****ILLEGAL FOR NON-TRAINER USE*****

Over a period of time, fragmentation occurs as records in the Active Directory database are deleted and new records are added. When the records are fragmented, the computer must search the Active Directory database each time the Active Directory database is opened to find all of the records, which slows down response time. Fragmentation also degrades the overall performance of Active Directory database operations. To overcome this problem of fragmentation, you *defragment* the Active Directory database. Defragmentation is the process of rewriting records in the Active Directory database to contiguous sectors to increase the speed of access and retrieval. When records are updated, these updates are saved on the largest contiguous space in the Active Directory database.

What Is Defragmentation?

Topic Objective

To illustrate the purpose of defragmentation.

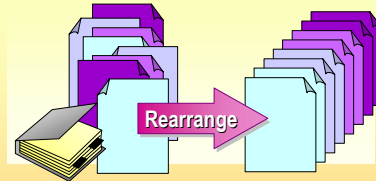
Lead-in

Active Directory database defragmentation is necessary to efficiently use the space allocated to the Active Directory database.

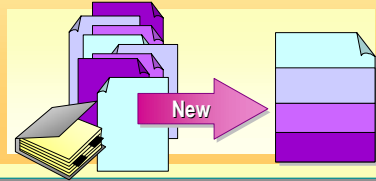
- Defragmentation Rearranges How the Data Is Stored in the Active Directory Database

- Defragmentation Can Occur Online or Offline

- Online Defragmentation Effectively Rearranges Pages Within the Database



- Offline Defragmentation Rearranges Pages Within the Database and Creates a New, Compacted Version of the Database File



*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

Defragmentation can take place online or offline. Online defragmentation rearranges pages within the database.

Offline defragmentation rearranges pages within the database, and creates a new, compacted version of the database file.

Defragmentation rearranges and compacts data storage in the Active Directory database. To update the Active Directory database file, ESE quickly updates the database; however, it does not make the most efficient use of space in the database. Therefore, Active Directory rewrites parts of the database to contiguous sectors on a hard disk, thereby increasing the speed through which users can gain access to and retrieve data. For example, data is written to pages one through 100, and then at a later time, data is deleted, freeing pages 12, 55, and 87. The next time data is written, it may get written on pages 12, 55, and 87, which would slow the response time. However, if you defragment the Active Directory database, pages 12, 55, and 87 would be grouped together, so that all of the data would be placed on pages one through 97, and pages 98 through 100 would be free to contain the new data.

Therefore, database defragmentation is necessary to efficiently use the space allocated to the database. Defragmentation can take place online while the computer is functioning as a domain controller or offline while the computer is functioning as a stand-alone server.

Online Defragmentation

Online defragmentation effectively rearranges pages within the database. Active Directory automatically performs online defragmentation of the database at certain intervals, which by default is every 12 hours, as part of the garbage collection process. Online defragmentation does not reduce the size of the database file, Ntds.dit, but instead optimizes data storage in the database and optimizes space in the directory for new objects.

Offline Defragmentation

Offline defragmentation rearranges pages within the database, and creates a new, compacted version of the database file. Depending on the fragmentation of the original database file, the new file might be considerably smaller than the original. This new file is stored in another directory that is chosen when the utility is run. The original database file remains in the same location. The only change that happens to the original database file is that it is first soft recovered. Soft recovery commits any transactions written to the log files before the compaction, so that the new compacted file is current with the log files and the checkpoint file. You manually perform offline defragmentation of the database.

Defragmenting a Database

Topic Objective

To identify how to defragment an offline and an online Active Directory database.

Lead-in

Although online defragmentation occurs automatically during the garbage collection process, you manually perform the offline defragmentation.

To Defragment an Offline Active Directory Database	
1 Back up Active Directory	6 Switch to the files prompt
2 Restart the domain controller	7 Compact the database, type <code>compact to drive>:\<directory></code>
3 Select Directory Services Restore Mode	8 Type quit twice to return to the command prompt
4 Log on by using the SAM account	9 Copy the new NTDS.DIT file over the old NTDS.DIT file
5 Run the <code>ntdsutil</code> command	10 Restart the domain controller normally

*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate how to defragment an offline Active Directory database.

Online defragmentation occurs automatically during the garbage collection process. Offline defragmentation must be performed manually and is necessary only if you want to create a new, compacted version of the original database file.

To defragment an offline Active Directory database, perform the following steps:

1. Back up Active Directory as a precautionary measure.
2. Restart the domain controller, and then press F8 to display the **Windows 2000 Advanced Options** menu.
3. Select **Directory Services Restore Mode**, and then press ENTER.
4. Log on by using the Administrator account and the password defined for the Local Administrator account in the offline SAM.
5. At the command prompt, type **ntdsutil** and then press ENTER.
6. Type **files** and then press ENTER. This switches you to the **files** prompt so that you can manage the NTDS database file.

7. Establish a location that has enough drive space for the compacted database to be stored. Type the following, and then press ENTER:

compact to <drive>:\<directory>

where <drive> and <directory> is the path to the location.

Note You must specify a directory path. If the path contains any spaces, the entire path must be surrounded by quotation marks; for example, "C:\New folder."

A new database named Ntds.dit is created in the path that you specified.

8. Type **quit** and then press ENTER. To return to the command prompt, type **quit** again.
9. Copy the new Ntds.dit file over the old Ntds.dit file in the current Active Directory database path that you noted in step 6.
10. Restart the domain controller as you normally would.

Lab B: Maintaining the Active Directory Database

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will perform an offline defragmentation of the Active Directory database, and run integrity and semantic database checks of the Active Directory database. In addition, you will move the Active Directory database to another folder and redirect Active Directory to use the database file in a different location.



*****ILLEGAL FOR NON-TRAINER USE*****

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Perform an offline defragmentation of the Active Directory database.
- Run integrity and semantic database checks of the Active Directory database.
- Move the Active Directory database to another folder.
- Redirect Active Directory to use the database file located in a different folder.

Prerequisites

Before working on this lab, you must have knowledge and experience using advanced startup options in Windows 2000.

Estimated time to complete this lab: 30 minutes

Exercise 1

Performing an Offline Defragmentation

Scenario

Northwind Traders had not initially planned which domain controllers would be global catalog servers. The result was that too many domain controllers were designated as global catalog servers. As soon as Northwind Traders realized this problem, they established an appropriate number of global catalog servers. Therefore, a large number of domain controllers that had been used as global catalog servers were now being used as domain controllers again. A maintenance schedule was defined to take domain controllers offline and perform an offline defragmentation and other database maintenance checks on these domain controllers. The primary reason for these checks is to reclaim disk space by reducing the size of the Ntds.dit database file. The domain controller's system state data was already backed up in preparation for this task.

Goal

In this exercise, you will move the database on your domain controller to an alternate location and then perform an offline defragmentation. This will reclaim any disk space that was used by the global catalog information. You will perform a database integrity check and a semantic database analysis on the defragmented database. You will reconfigure Active Directory to use this database file without deleting the original files. After the new database is successfully online, you will delete the old database files.

Tasks	Detailed Steps
1. Restart your domain controller in Directory Services Restore Mode, and then log on as Administrator.	- Log on as Administrator in your domain with a password of password. - Restart your domain controller. - When the message "For troubleshooting and advanced startup options for Windows 2000, press F8" is displayed at the bottom of the screen, press F8. - On the Windows 2000 Advanced Options menu, click Directory Services Restore Mode, and then press ENTER. - If prompted for the operating system, select Microsoft Windows 2000 Advanced Server, and then press ENTER. - Log on as Administrator with a password of password and then click OK to close the message that indicates Windows is running in safe mode.
2. Determine the current file size of the database by using the ntdsutil utility.	- Open a command prompt window. - At the command prompt, type ntdsutil and then press ENTER. - At the ntdsutil prompt, type files and then press ENTER to change to the file maintenance menu. - At the file maintenance prompt, type info and then press ENTER to display the size of the database files.

Tasks	Detailed Steps
? What is the size of the Ntds.dit file? What are the locations of the Database, Backup directory, Working directory, and Logs directory? The size of the database varies. The database is located at C:\Winnt\Ntds\Ntds.dit. The backup directory is C:\Winnt\Ntds\DSADATA.BAK. The working directory is C:\Winnt\Ntds. The Logs directory is C:\Winnt\Ntds.	
3. Move the database and log files to C:\2154_original.	a. At the file maintenance prompt, type move db to c:\2154_original and then press ENTER to move the database files to this alternate location. b. At the file maintenance prompt, type move logs to c:\2154_original and then press ENTER to move the log files to this alternate location. c. At the file maintenance prompt, type info and then press ENTER to verify the paths were also updated.
4. Perform an offline defragmentation of the database to C:\Winnt\Ntds.	▪ At the file maintenance prompt, type compact to c:\winnt\ntds and then press ENTER to defragment the database.
5. Redirect the directory services path to: - Database – C:\Winnt\Ntds\Ntds.dit - Backup dir – C:\Winnt\Ntds\Dsadata.bak - Working dir – C:\Winnt\Ntds - Log dir – C:\Winnt\Ntds	a. At the file maintenance prompt, type set path db c:\winnt\ntds\ntds.dit and then press ENTER. b. At the file maintenance prompt, type set path backup c:\winnt\ntds\dsadata.bak and then press ENTER. c. At the file maintenance prompt, type set path working dir c:\winnt\ntds and then press ENTER. d. At the file maintenance prompt, type set path logs c:\winnt\ntds and then press ENTER. e. At the file maintenance prompt, type info and then press ENTER to verify the paths have been set correctly.
? What is the size of the defragmented Ntds.dit file? Is it smaller than the original Ntds.dit file? The size of the database varies. The file size should be equal to or less than the original. How much smaller it is depends on how much free space was in the original database file.	

Tasks	Detailed Steps
6. Run an integrity check and semantic database analysis on the defragmented database file. Review the summary log created by the semantic database analysis.	a. At the file maintenance prompt, type integrity and then press ENTER to run the database integrity check. A message indicates that the operation completed successfully. b. At the file maintenance prompt, type quit and then press ENTER to return to the ntdsutil prompt. c. At the ntdsutil prompt, type semantic database analysis and then press ENTER to go to the semantic checker prompt. d. At the semantic checker prompt, type go and then press ENTER to run the semantic database analysis.  <i>A message indicates the file storing the summary results. Note the file name for use in step g.</i> e. At the semantic checker prompt, type quit and then press ENTER to return to the ntdsutil prompt. f. At the ntdsutil prompt, type quit and then press ENTER to return to the command prompt. g. At the command prompt, type notepad dsdit_file (where <i>dsdit_file</i> is the log file indicated by the semantic database analysis in step d), and then press ENTER. h. Review the summary, close Notepad, and then delete the log file.
7. Restart the domain controller, log on, verify Active Directory is working correctly, delete the original database files, and then log off.	a. Close the open command prompt window, and then restart the computer. b. Log on as Administrator in your domain with a password of password. c. Open Event Viewer, and then click Directory Service. d. Verify that no recent errors were logged since the restart, and then close Event Viewer. e. If there are no current Active Directory errors, delete the folder named C:\2154_original to free the disk space currently used by the original database files. f. Close all open windows, and then log off.

Best Practices

Topic Objective

To apply best practices for maintaining the Active Directory database.

Lead-in

Review this checklist before you maintain the Active Directory database.



The Tombstone Lifetime Interval Should Not Be Reduced



Separate the Database and Log Files



Back Up the System State Data of Domain Controllers Frequently



Perform Offline Defragmentation Only if You Can Recover a Significant Amount of Hard Disk Space

*****ILLEGAL FOR NON-TRAINER USE*****

Emphasize the reason for each best practice.

The following list provides best practices for implementing disaster recovery in Active Directory:

- The tombstone lifetime interval should not be reduced. When a domain controller is restored, backup compares the tombstone lifetime with the backup date and will not restore the system state data if the backup is older than the tombstone lifetime. The restored domain controller is not aware of deletions that have their tombstone removed, which can lead to inconsistencies between domain controllers. Therefore, it is recommended that tombstone lifetime be maintained at a value greater than either expected replication latency or backup interval, whichever is greater.
- Separate the database and log files. Move the database and log files to separate hard disks to prevent them from competing with the input output (I/O) of the operating system. Also, move the database and log files to separate hard disks to separate the I/O from each other.
- Back up the system state data of domain controllers frequently, so that you have the most current data to restore. Back up the system state data at least weekly, after you install new software, make configuration changes, or add new objects to Active Directory. Even if your domain has multiple domain controllers that can replicate Active Directory, multiple disasters can occur.
- Perform offline defragmentation only if you can recover a significant amount of disk space that you can use for other tasks. For example, if the domain controller was once a global catalog server for a multiple domain forest but was later removed, you can free a significant amount of disk space by using the offline defragmentation method.

Review

Topic Objective

To reinforce module objectives by reviewing key points.

Lead-in

The review questions cover some of the key concepts taught in the module.

- Introduction to Maintaining the Active Directory Database
- The Process of Modifying Data in Active Directory
- The Garbage Collection Process
- Backing Up Active Directory
- Restoring Active Directory
- Moving the Active Directory Database
- Defragmenting the Active Directory Database
- Best Practices

*****ILLEGAL FOR NON-TRAINER USE*****

Give students time to read and answer the review questions on their own, and then discuss the answers as a group.

1. What is the purpose of the garbage collection process?

The garbage collection process performs online defragmentation and deletes expired tombstoned objects.

2. What is the purpose of the tombstone lifetime and how does this affect the restore operation?

The tombstone lifetime is the period of time that the deleted object stays in Active Directory to ensure that all replicas are aware of its deletion. The tombstone lifetime affects the restore operation because during the restore operation backup compares the tombstone lifetime with the backup date and will not restore the system state data if the backup is older than the tombstone lifetime.

3. When you start one of the domain controllers in your domain, you receive an error message indicating that Active Directory cannot start because the Active Directory database is damaged. How do you restore the Active Directory database and make sure that it is current?

Start Windows 2000 by using the Directory Service Restore Mode, and then use Backup to restore the system state data of the domain controller. As long as you can restore a backup of the system state data, replication makes Active Directory current.

4. Someone incorrectly deleted an OU in Active Directory. What should you do?

Restore the system state data, and then mark the specific OU authoritative by using Ntdsutil.exe. Remember not to restart the domain controller until after you have marked the restored object as authoritative by using ntdsutil.

5. You are planning to defragment the Active Directory database. What is the precaution you should take so that the original database is not deleted in case there is a problem during defragmentation?

Do not copy the defragmented database over the original database until you have verified that the defragmented database works correctly. To use the defragmented database in a different location, you can copy the original database to a backup location and then copy the defragmented file to the original location.

6. What type of defragmentation would you perform to create a new, compacted version of the database file?

Offline defragmentation.

