



Operating System

Backup and Recovery of the Distributed Services: Active Directory, Certificate Server, and File Replication

Beta 3 Technical Walkthrough

Abstract

This paper introduces you to disaster recovery and the distributed services for the Microsoft® Windows® 2000 operating system using the Windows 2000 backup utility, Windows NT Backup. The Windows 2000 distributed services discussed in this paper include the Microsoft Active Directory™ directory service, Certificate Server, and File Replication Service.

In this walkthrough, you perform a full system backup to any of the media types supported by Windows NT Backup, fault the server by reformatting the system, reinstall Windows 2000, and then recover the server's functionality by restoring from the backup device.

© 1999 Microsoft Corporation. All rights reserved.

THIS IS PRELIMINARY DOCUMENTATION. The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This BETA document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Microsoft, Active Directory, Windows, the Windows logo, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other product or company names mentioned herein may be the trademarks of their respective owners.

*Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA
0599*

CONTENTS

INTRODUCTION	1
Prerequisites	1
Walkthrough Scenarios	1
BACKING UP THE SERVER	2
System Requirements	2
RECOVERING FROM SERVER FAILURE	6
Simulating Server Failure	6
Reinstalling the Operating System	6
Restoring the Server	6
Verify Active Directory Restoration	9
AUTHORITATIVE RESTORE	11
Authoritative Restore of the Active Directory	11
Authoritative Restore of File Replication Service	12
FOR MORE INFORMATION	14
Before You Call for Support	14
Reporting Problems	14

INTRODUCTION

This paper introduces you to disaster recovery and the distributed services for the Microsoft® Windows® 2000 operating system using the Windows 2000 backup utility, Windows NT Backup. The Windows 2000 distributed services discussed in this paper include the Microsoft Active Directory™ directory service, Certificate Server, and File Replication Service.

In this walkthrough, you perform a full system backup to any of the media types supported by Windows NT Backup, fault the server by reformatting the system, reinstall Windows 2000, and then recover the server's functionality by restoring from the backup device.

Prerequisites

Prior to attempting this walkthrough, you must have installed the Beta 3 release of Windows 2000 Server (including the Active Directory) on a server in your network.

You must then populate the Active Directory with users and groups. Refer to the Configure Your Server wizard for information about adding objects such as users, groups, computers, volumes and printers to the Active Directory.

Walkthrough Scenarios

This document walks you through the following tasks:

Backing up the server	Use the Windows NT Backup utility to create a media set and back up the Distributed Services (Active Directory, Certificate Server, and File Replication Service).
Recovering from server failure	Remove the Active Directory service from the domain controller by reformatting the system. Then reinstall the Windows 2000 Server operating system. The disaster recovery scenario supports replacement of the failed domain controller with a standalone or member server with the same hardware configuration (network, video, disk volumes) and name as the failed domain controller. Restore the server from backup media, and restart the server in normal operational mode.
Advanced Options – repairing the server	Start the server in Directory Services Repair Mode to verify that the Active Directory was restored. Perform Authoritative Restore of the Active Directory and File Replication Service.

BACKING UP THE SERVER

Windows NT Backup offers three wizards to simplify backup and restore operations:

- The Backup wizard takes you through the steps to perform a system backup.
- The Disaster Recovery Preparation wizard allows you to prepare a set of Disaster Recovery disks that can be used to fully recover a failed system.
- The Recovery wizard takes you through the steps to recover a system.

In this walkthrough, the Backup wizard is used to back up the entire server. You then manually restore the system without using the Restore wizard.

This version of Windows NT Backup supports backup and recovery operations from the local computer only. You cannot perform backup and recovery of the Active Directory on a remote computer.

System Requirements

In this procedure, Windows NT Backup is used to perform recovery between computers with the same hardware configuration (disk volumes, graphics adapter, network adapter) as the failed system.

To back up the system

1. Log on to the Windows NT Server Domain Controller using an account that has Administrator or Backup Operator privileges. If you log on using an account that does not have these privileges, you cannot back up the Active Directory.
2. Start the Windows NT Backup wizard. From the **Start** menu, point to **Programs**, then point to **Accessories**, and then click **Backup**.

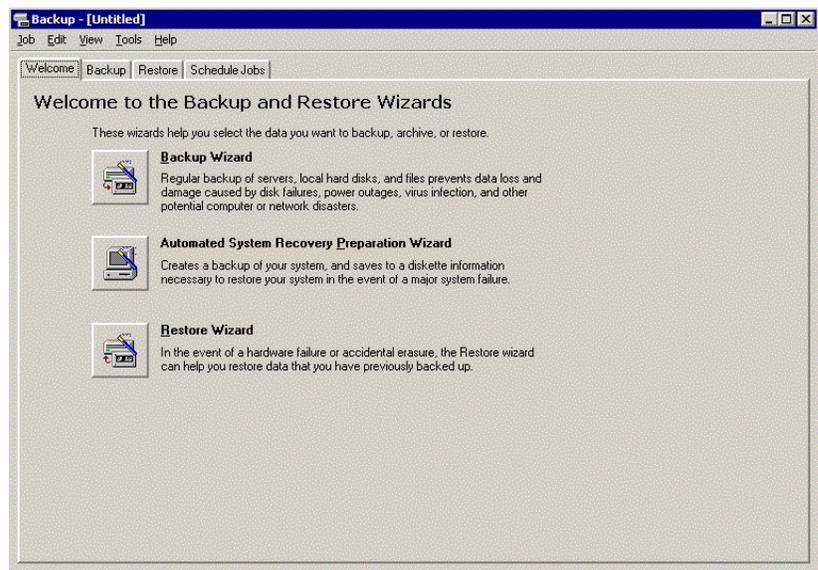


Figure 1. Backup Wizard

3. Click the **Backup Wizard** button to start the backup process.

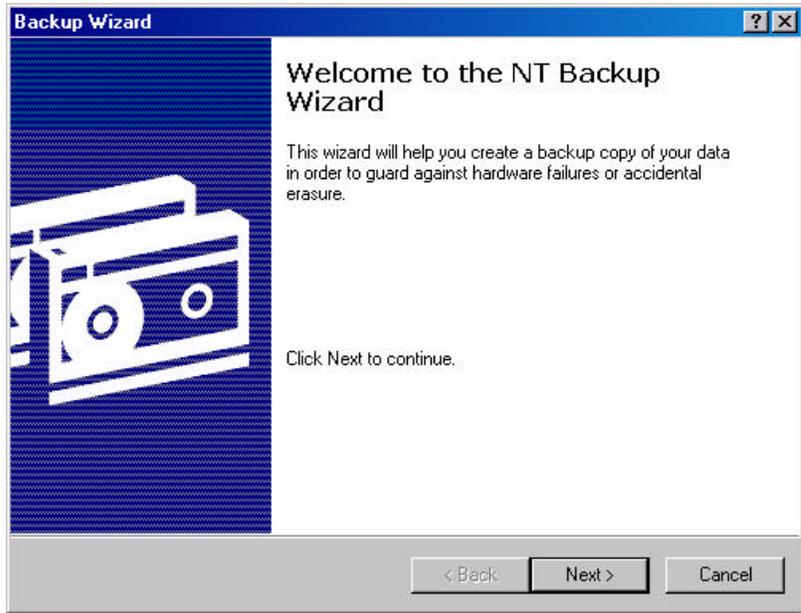


Figure 2. The Backup Wizard

4. Click **Next**.
5. Select **Back up everything on my computer**
6. Select the destination media. If you have a tape backup unit installed, you can select that. This example uses a backup file on the disk system.

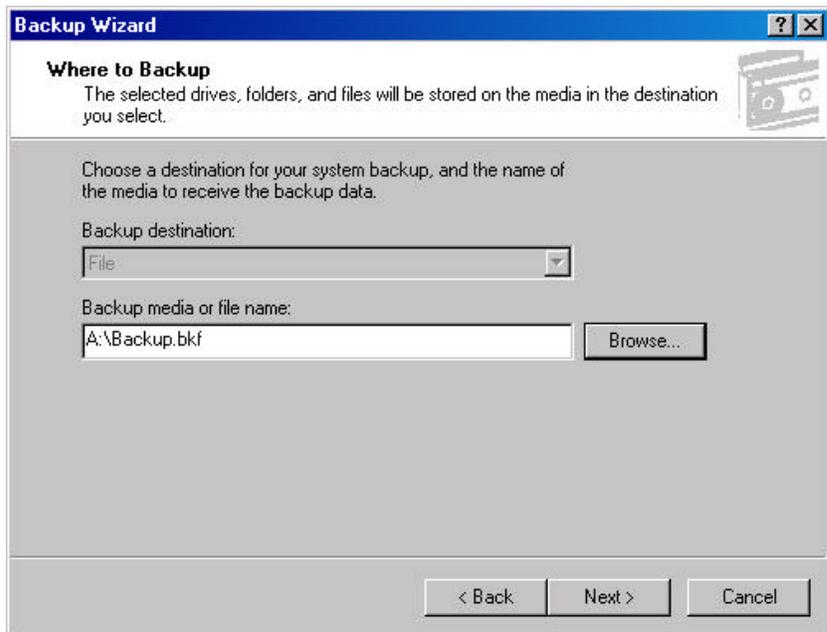


Figure 3. Specify Where to Backup

7. Create a backup file. In this example the file name is *isbackup.bkf*.

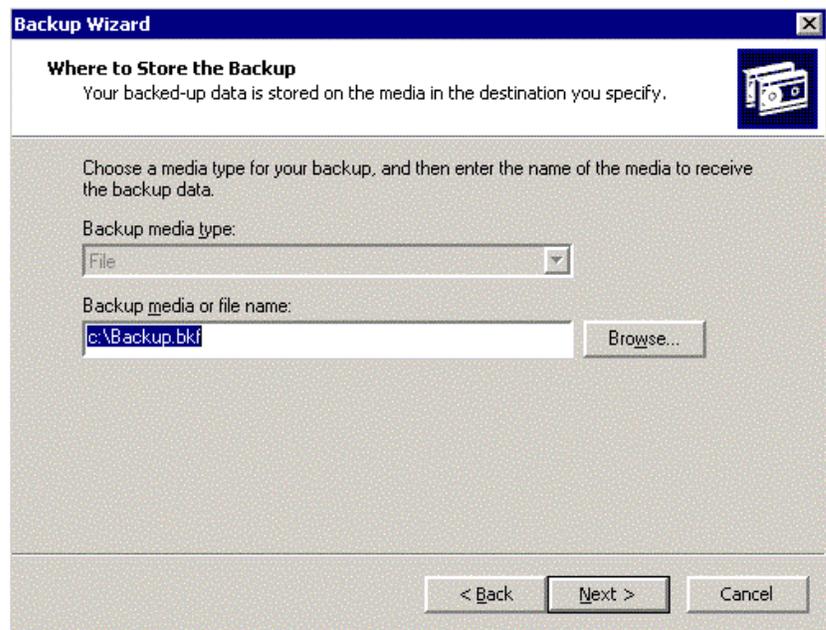


Figure 4. Name the backup file

8. Specify your media options. This example creates a new backup and overwrites any data that is present on the backup media.

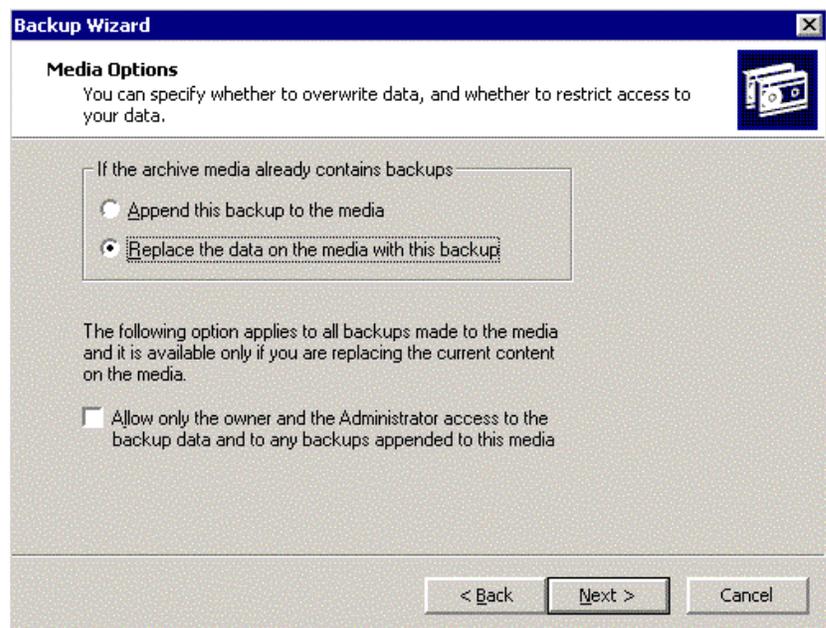


Figure 5. Media options

9. Complete the remaining wizard screens, and begin the backup operation. A progress indicator shows the status of the backup operation.

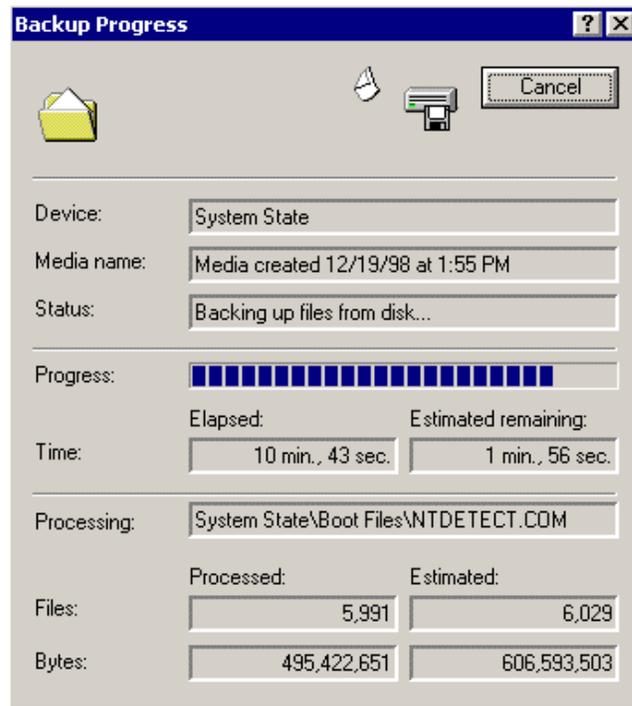


Figure 6. Status indicator

You have now successfully backed up the system, including the Active Directory, File Replication Service, and Certificate Server.

RECOVERING FROM SERVER FAILURE

This procedure simulates a failed domain controller and walks you through the recovery process. First, you reinstall the Windows 2000 Server operating system. Once you have reinstalled the operating system, you can use the backup set to restore the system to its state prior to the failure.

Simulating Server Failure

To simulate server failure, reformat your hard drive.

Reinstalling the Operating System

Refer to the instructions contained in the beta release to reinstall the Windows 2000 Server operating system. Ensure that you reinstall the Windows 2000 Server operating system on the same drive and volume that were used previously.

Once you have reinstalled the operating system, continue with the next steps to fully recover the failed server.

Restoring the Server

Use your system backup media to restore the server. The restore process recovers the Windows 2000 Server operating system configuration, the Active Directory including database and registry settings, the Certificate Server database files, and the File Replication Service.

Once the restoration is completed, an optional step is to restart in Directory Service Repair Mode and verify that the Active Directory database has been restored. This process is covered later in this document.

You can then restart the server in normal operational mode. The system automatically performs a series of steps to ensure data integrity. The Active Directory database files undergo an automatic consistency check, and are re-indexed. Both the Active Directory and File Replication Service are brought up to date from their replication partners using the standard replication protocols for each of those services.

You can verify the success of the restore process by checking that the Active Directory, Certificate Server, and File Replication Services are operational.

To use WindowsNT Backup to restore the server

1. Start Windows NT Backup: from the **Start** menu, point to **Programs**, then point to **Accessories**, and then click **Backup**.
2. Click the **Restore Wizard** button on the Welcome page.
3. Create a catalog. To build the catalog, rightclick the **File** icon, and then select **Catalog File**.

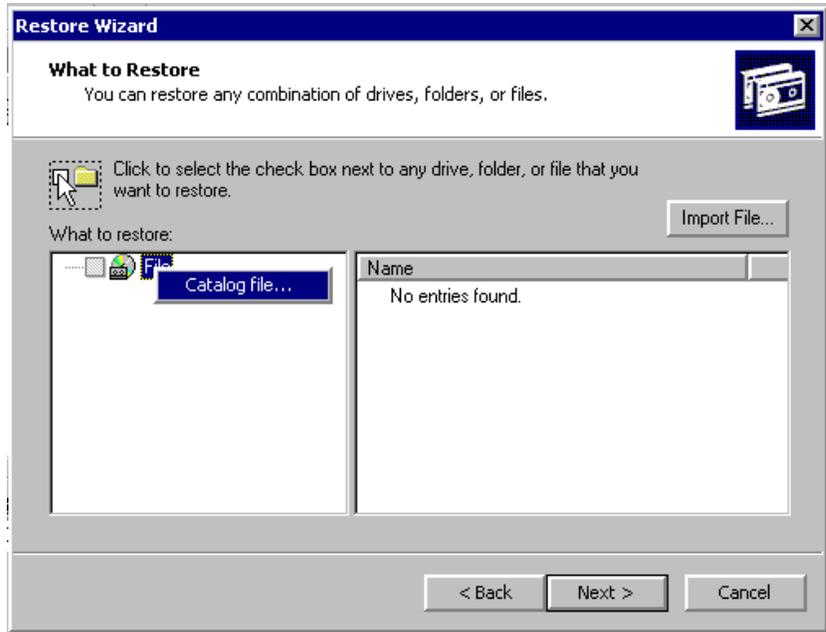


Figure 7. The Restore Wizard

4. Use the browse dialog to locate the backup set that you created previously. In this example, the file is called *backup.bkf*.

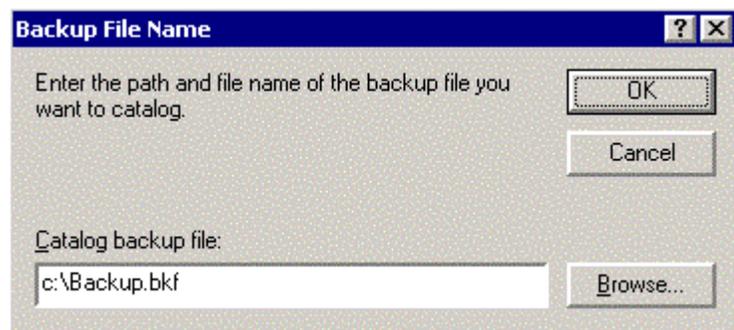


Figure 8. Locate the backup file

5. Ensure that all of the volumes and System State options are selected. The System State refers to the distributed services components—the Active Directory, Certificate Server, and File Replication Service.

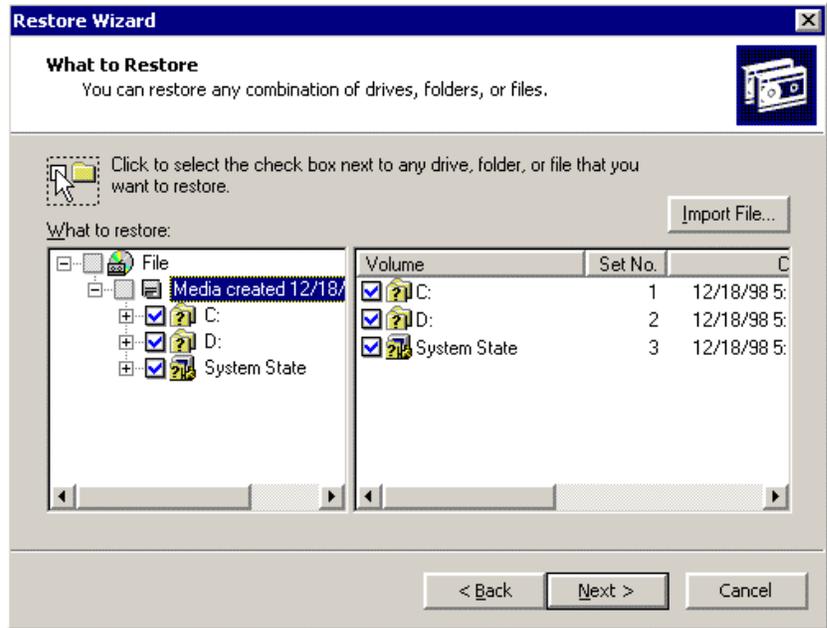


Figure 9. Select the volumes and System State

6. Select the backup media name for the restore operation. In this example, were the backup media was a disk file, the backup file called `backup.bkf` which was created during the previous backup operation is selected.

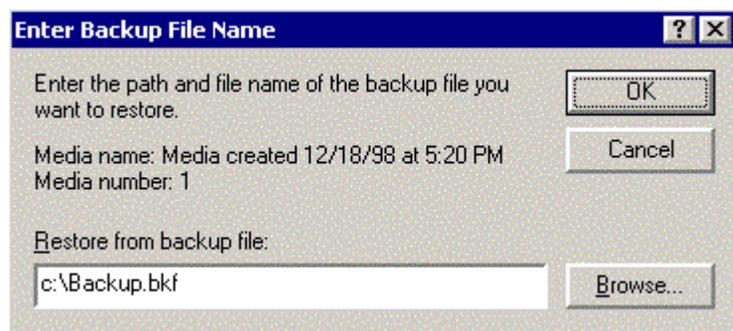


Figure 10. Enter the backup file name

7. Click OK and continue through the restore process. A visual progress indicator is displayed.

Verify Active Directory Restoration

After the restore is completed, you can either restart the server in normal operation mode and perform basic verification or continue with the advanced verification. Both processes are explained below.

To perform basic verification

1. Once the restore operation has completed, restart the computer in normal operational mode. The Active Directory and Certificate Server automatically detect that they have been recovered from a backup. They perform an integrity check and re-index the database.
2. After you can logon to the system, browse the directory. All of the user and group objects that were present in the directory prior to backup should be restored. Similarly, files that were members of a File Replication Service replica set and certificates that were issued by the Certificate Server should be present.

To perform advanced verification

Note The following procedure introduces an advanced option, which is not normally required for normal recovery operations. Incorrect usage of the utility described in this section can corrupt the Active Directory database, requiring you to restore the database from backup to ensure reliable operation.

1. Immediately after performing the restore operation, restart the server and select **Directory Service Repair Mode** from the boot menu.
2. Once the system has started, log on using the standalone server administrator account.
3. Verify that the Active Directory is in a state consistent with having been recovered from a backup. To do this, check for a specific registry key. Start Registry Editor: from the **Start** menu, click **Run**, and then type
Regedit
4. Click **OK**.
5. Select the registry key
**HKEY_LOCAL_MACHINE\
SYSTEM\
CurrentControlSet\
Services\
NTDS**
6. Check that there is a subkey called **Restore In Progress**. This key is automatically generated by Windows NT Backup, and indicates to the Active Directory Service that the database files have been restored and that Active Directory Service should perform a consistency check and re-index the next time the directory is started. This key is automatically removed upon completion

of this check. **DO NOT ADD or DELETE** this key.

7. Use the NTDSutil.exe utility to check for the recovered Active Directory database files. From the **Start** menu, point to **Programs**, and click **Command Prompt**. At the command prompt, type

```
NTDSUTIL
```

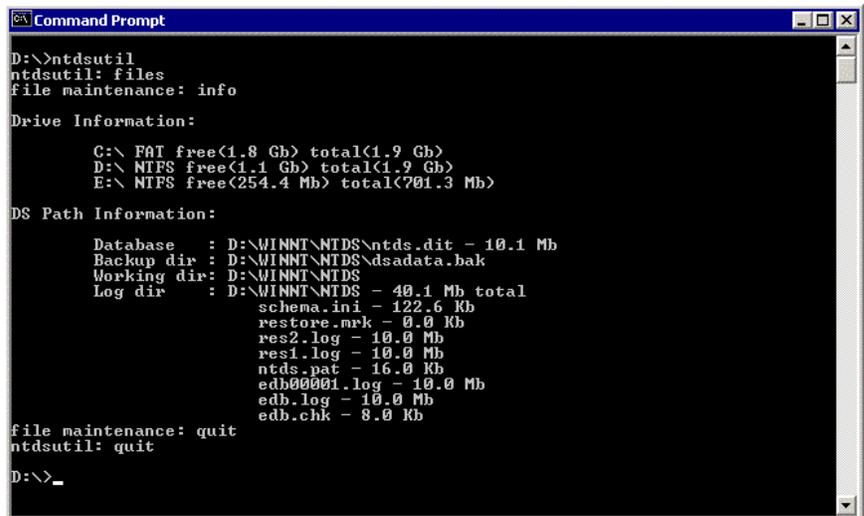
8. At the NTDSUTIL prompt, type

```
Files
```

9. At the file maintenance prompt type

```
Info
```

If the Active Directory files have been recovered successfully, you should see list information similar to that shown below. **DO NOT SELECT ANY OTHER OPTIONS.**



```
Command Prompt
D:\>ntdsutil
ntdsutil: files
file maintenance: info
Drive Information:
    C:\ FAT free(1.8 Gb) total(1.9 Gb)
    D:\ NTFS free(1.1 Gb) total(1.9 Gb)
    E:\ NTFS free(254.4 Mb) total(701.3 Mb)
DS Path Information:
    Database : D:\WINNT\NTDS\ntds.dit - 10.1 Mb
    Backup dir : D:\WINNT\NTDS\dsadata.bak
    Working dir: D:\WINNT\NTDS
    Log dir : D:\WINNT\NTDS - 40.1 Mb total
              schema.ini - 122.6 Kb
              restore.mrk - 0.0 Kb
              res2.log - 10.0 Mb
              res1.log - 10.0 Mb
              ntds.pat - 16.0 Kb
              edb00001.log - 10.0 Mb
              edb.log - 10.0 Mb
              edb.chk - 8.0 Kb
file maintenance: quit
ntdsutil: quit
D:\>_
```

Figure 11. Verification of Active Directory recovery

10. Once you have confirmed that the Active Directory has been restored from the backup and that the registry keys are present, restart the server in normal mode.

When the computer is restarted in normal mode the Active Directory automatically detects that it has been recovered from a backup and performs an integrity check and re-indexes the database. Once you can log on to the system, you should be able to browse the directory. All user and group objects that were present in the directory prior to backup should be restored.

AUTHORITATIVE RESTORE

When there are replica domain controllers, the Active Directory replicates directory objects (such as users, groups, organizational units, and computers) among all domain controllers in that domain. Similarly, the File Replication Service replicates files present in replica sets with other servers that are hosting the same replica sets. For example, Group Policy files and logon and logoff scripts are replicated between all domain controllers that use the SYSVOL replica set.

The default mode for data recovery as performed in the previous sections is *non-authoritative*. That means that the restored server is brought up to date with its replicas through the normal replication mechanism. For example if a domain controller was restored from a backup tape that was two weeks old, once it was restarted, it would be brought up to date with respect to its partners using the normal replication mechanism.

There may be a requirement to perform an *authoritative* restore. For example, if an administrator inadvertently deleted an organizational unit containing a large number of users and the server was restored from tape, it would be brought up-to-date—including the inadvertent deletion of the organizational unit—if the default non-authoritative restore was used. Again, if a file that was replicated with the File Replication Service was inadvertently modified or deleted, a normal (non-authoritative) restore would not recover the file to its original state, as replication would bring it to the current modified or deleted state.

Authoritative restore allows the administrator to recover a domain controller, restore it to a specific point in time, and mark objects in the Active Directory and files in the File Replication Service as being authoritative with respect to their replication partners. This prevents accidental deletions or modifications from recurring when the data is restored.

Authoritative Restore of the Active Directory

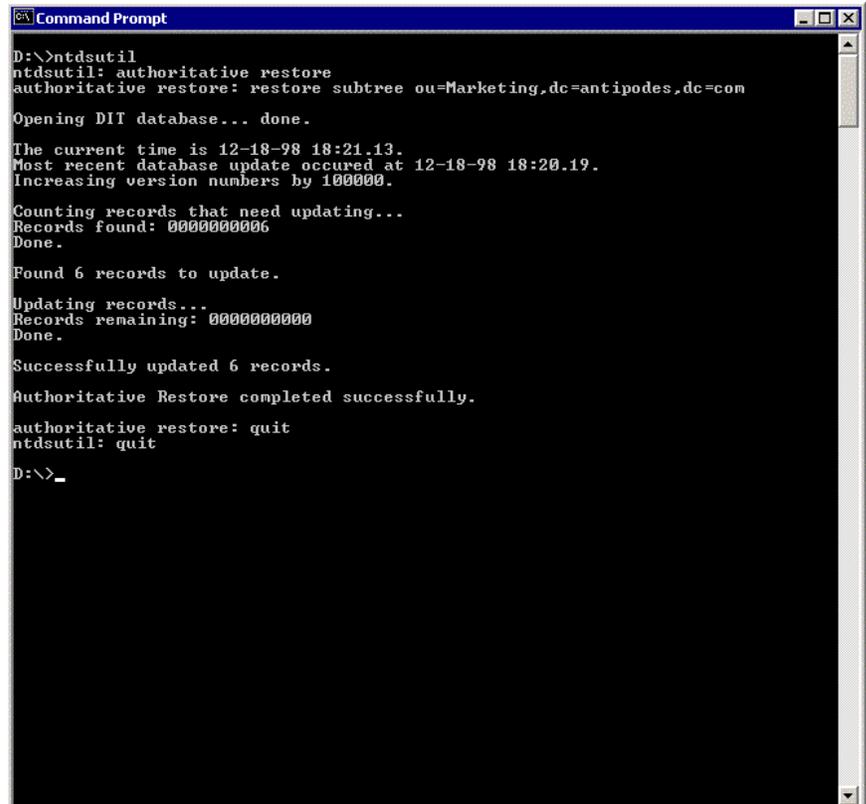
In this procedure, you should assume that the administrator has inadvertently deleted the Marketing organizational unit in the domain called Antipodes.com. (Note that this procedure assumes that you have configured your directory following the examples described in the walkthrough document titled *Advanced Management of the Active Directory*.)

After restoring the domain controller as described in the previous section, perform the following steps.

To perform authoritative restore

1. Start Windows NT Backup: from the **Start** menu, point to **Programs**, then point to **Accessories**, and click **Backup**.
2. Select the **Restore Wizard**, from the Welcome page.
3. Select the drive, directory, and files that you want to authoritatively restore. In this example, the system directory is D:\WINNT. The group policy files are located in the directory SYSVOL.

4. Select **Advanced Options**
5. At the NTDSUTIL Authoritative Restore prompt, type
Restore Subtree OU=Marketing, DC=Antipodes, DC=COM
6. Exit from NTDSUTIL.



```
Command Prompt
D:\>ntdsutil
ntdsutil: authoritative restore
authoritative restore: restore subtree ou=Marketing,dc=antipodes,dc=com
Opening DIT database... done.
The current time is 12-18-98 18:21.13.
Most recent database update occurred at 12-18-98 18:20.19.
Increasing version numbers by 100000.
Counting records that need updating...
Records found: 0000000006
Done.
Found 6 records to update.
Updating records...
Records remaining: 0000000000
Done.
Successfully updated 6 records.
Authoritative Restore completed successfully.
authoritative restore: quit
ntdsutil: quit
D:\>_
```

Figure 12. Authoritative Restore

Authoritative Restore of File Replication Service

In this example, the administrator has inadvertently deleted the logon scripts for the marketing organizational unit in the domain called *Antipodes.com*. The logon script is called *mktglogon.vbs*.

All that is required is that you restore the correct version of the logon script while the File Replication Service is operational.

To perform an authoritative restore of the File Replication Service

1. Start Windows NT Backup: from the **Start** menu, point to **Programs**, then point to **Accessories**, and click **Backup**.
2. Select the **Restore Page**, and navigate through the directories and files to locate *mktglogon.vbs* file

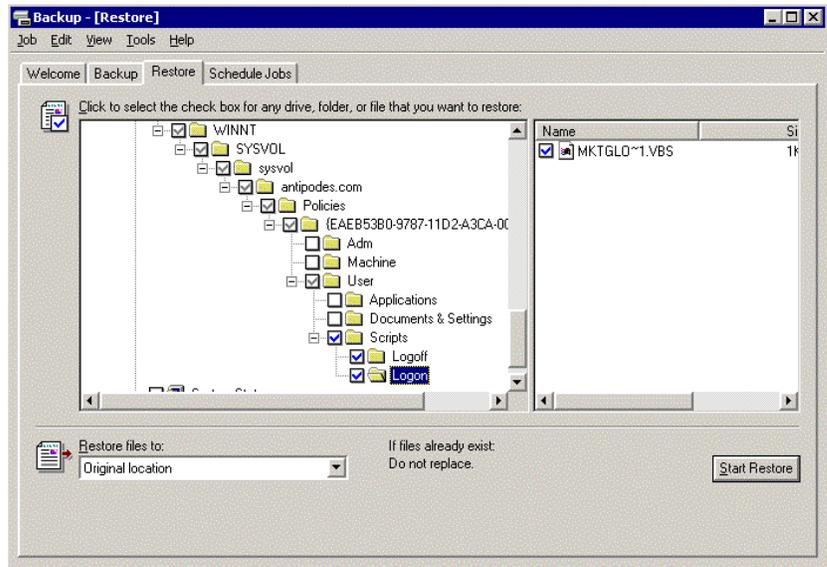


Figure 13. Authoritative Restore of the File Replication Service

3. Start the restore, and select the **Advanced Restore Options**
4. Check the option to mark the data from restored replica sets as the primary (or authoritative) data.



Figure 14. Select primary data

Once the restore has completed, the restored mktglogon.vb\$file is replicated to the other replicas using the normal File Replication Service protocol.

FOR MORE INFORMATION

For the latest information on Microsoft Windows2000 network operating system, visit our World Wide Web site at <http://www.microsoft.com/windows/server/> and the Windows NT Server Forum on the Microsoft Network (GO WORD: MSNTS).

For the latest information on the Windows2000 Beta 3, visit the World Wide Web site at <http://ntbeta.microsoft.com/>.

Before You Call for Support

Please keep in mind that Microsoft does not support these walkthroughs. The purpose of the walkthroughs is to facilitate your initial evaluation of the Microsoft Windows 2000 features. For this reason, Microsoft cannot respond to questions you might have regarding specific steps and instructions.

Reporting Problems

Problems with Microsoft Windows 2000 should be reported via the appropriate bug reporting channel and alias. Please make sure to adequately describe the problem so that the testers and developers can reproduce it and fix it. Refer to the Release Notes included on the Windows2000 Beta distribution media for some of the known issues.