COMPAQ
White Paper

Active Directory Disaster Recovery

August 2000
PS-99-23

Prepared by Stephen Craike & Karl Robinson

Compaq Professional Services

Compaq Computer Corporation

Contents

Abstract: Recovering a Windows 2000 Domain Controller requires more care and attention to detail than the equivalent operation in Windows NT 4.0.

Domain Controllers can assume numerous roles within an Active Directory infrastructure: global catalogs, operations masters, and simple domain controllers. This paper describes the steps you use to recover the Active Directory database after a failure, the associated considerations, and the issues you need to keep in mind when restoring a server to a special role.

The steps outlined in this paper have been verified through recovery operations staged in the Compaq QTEST Windows 2000 organization. QTEST is a worldwide deployment of Windows 2000 servers that is used by Compaq consultants to verify and test deployment scenarios.

Special Acknowledgments:

Special thanks to.

Compaq	*Micky Balladelli*
	Dung Hoang Khac
	Tony Redmond
Microsoft:	*Khushru Irani*
	Ulric Dihle
	Stuart Kwan
	Ulric, Stuart
	Jeff Parham
	Murli Satagopan
	Don Hacherl
	Sudarshan Chitre

Notice

Document Title
White Paper prepared by Compaq Professional Services Technology Group

Second Edition (August 2000)
Document Number PS-99-23

Introduction

The Active Directory and its supporting systems are at the core of Microsoft's Windows 2000 operating system. Keeping these systems functional and understanding what to do in the event of a failure is imperative to a successful and robust Windows 2000 infrastructure.

In support of this, the following white paper has been written to:

- Inform readers about disaster recovery concepts with respect to the Windows 2000 Active Directory.
- Provide step-by-step recovery procedures for the most common Active Directory disaster situations and related considerations.

We encourage you to use this information to form your own disaster recovery plans. However, it is important that you augment it with the specifics of your own internal environment and your existing disaster recovery policies.

This paper provides only a brief overview of Active Directory. It assumes the reader is familiar with the Active Directory model and the technologies supporting it.

For further information on the basic concepts discussed in this paper, we encourage you to read the following white papers:

- ≅ Active Directory – A Technical Overview
- ≅ Understanding Active Directory Replication

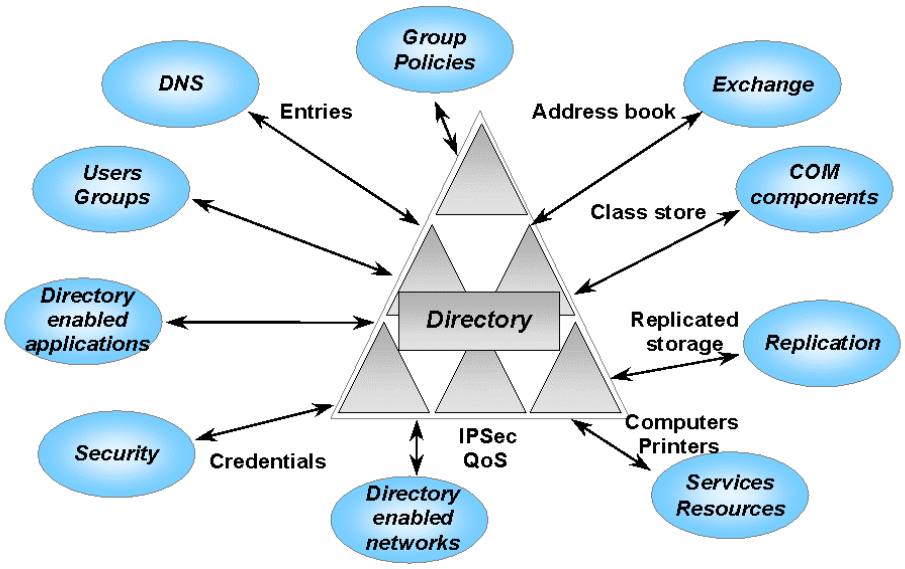
Both can be obtained from: http://www.compaq.com/activeanswers

Overview of Active Directory

The Active Directory is the directory service used by Microsoft Windows 2000 servers. It is a core component of the operating system and provides essential data to both the enterprise and to other components within the operating system.

Active Directory provides a central service for administrators to organize network resources, manage users, computers and applications.

- The Active Directory stores many different objects, including all the objects necessary for running a Windows 2000 based infrastructure:Users, groups
- Security credentials, such as certificates
- System resources, such as computers (or servers) and resources
- Replication components (Settings are themselves objects in the Active Directory.)
- COM components (In previous versions of Windows NT, information about COM component locations had to be stored in the registry. With Active Directory, this information is stored in the Class Store.)
- Rules and policies to control the working environment



System Components of Active Directory

- Although many components make up the Active Directory, this section focuses on the system components that are relevant when considering the creation of a disaster recovery plan, namely:Domain Controllers (DCs)
- Global Catalogs (GCs)
- Operations Masters (OMs)

Domain Controllers (DCs)

As with Windows NT 4.0, Windows 2000 requires domain controllers (DCs) to host a domain database and perform authentication services. However, under Windows 2000, object changes can be made on any DC within the environment instead of on a single PDC, as with NT 4.0.

To ensure that all DCs in the environment host a current, synchronized and accurate version of the directory, DCs are responsible for initiating and performing replication operations. In addition to this domain information, all of the domain controllers in a particular forest host a copy of the forest configuration and schema containers.

Global Catalogs (GCs)

The global catalog's (GC's) primary function is to provide fast and efficient searches that extend across the entire Active Directory forest. A GC holds a full read/write replica of all objects within the domain for which it is a member, and a partial read-only replica (all objects but only a partial attribute set) of every other domain within the forest. The global catalog, therefore, makes directory structures within a forest transparent to end users, creating a search mechanism that makes finding objects in the directory uncomplicated and efficient.

The global catalog is also required for the enumeration of universal group memberships and UPNs in a native Windows 2000 domain. As a result, if a DC cannot contact a GC at the time of client logon, cached local logon credentials are all that the client receives, and access to remote resources is denied.

Operations Masters (OMs)

Because Active Directory supports multi-master updates (each DC hosts a writeable version of its directory partition), it must allow for the possibility of conflicting changes, that is, changes that are made simultaneously to the same object within the directory but from different DCs. The conflicts are resolved eventually and all DCs update to the same value.

However, in some cases it is better to prevent conflicts than to resolve them after the event. Operations masters (OMs) in Active Directory prevent conflicts in cases where conflict resolution is inappropriate.

Active Directory defines five Operations Master (OM) roles:

- ≅ Per-Forest Roles
  - Schema master
  - Domain naming master

- ≅ Per-Domain Roles
  - Relative IDentifier (RID) master
  - Primary Domain Controller (PDC) emulator
  - Infrastructure master

Schema Master

The DC that holds the schema master role is the only DC that can perform write operations to the directory schema. Those schema updates are replicated from the schema master to all other domain controllers in the forest.

Domain Naming Master

The DC that houses the domain naming master role is the only DC that:

- Adds new domains to the forest
- Removes existing domains from the forest
- Adds or removes cross-reference objects in external directories

Relative IDentifier (RID) Master

This operations master manages the allocation of RID pools to other DCs. Only one server performs this task. When a security principle (for example, user, group, or computer) is created, it requires that a RID be combined with a domain-wide identifier to create a unique Security IDentifier (SID).

Every Windows 2000 DC receives a pool of RIDs (512 by default) it can use to create objects. The RID master ensures unique IDs on every DC by assigning different pools. All object moves between domains of the same forest are accomplished using the RID master to avoid SID duplication.

Primary Domain Controller (PDC) Emulator

The PDC emulator provides the following major functions:

- Backward compatibility for clients and servers, allowing NT 4.0 BDCs to participate in the new Windows 2000 environment.
- Password management. Native Windows 2000 environments replicate password changes to the PDC emulator first. When a DC fails to authenticate a password (perhaps as a result of a change that has not yet been replicated to the authenticating DC), it contacts the PDC emulator to see whether the password can be authenticated there.
- Time synchronization. The PDCs of the domains within the forest synchronize with the PDC in the root domain of the forest to ensure accurate time synchronization.

Infrastructure Master

The infrastructure master ensures the consistency of objects for all inter-domain operations. When an object from another domain is referenced, the reference contains the Globally Unique IDentifier (GUID), the Security IDentifier (SID) and the Distinguished Name (DN) of that object. If the referenced object moves, the DC holding the infrastructure master role in a domain is responsible for updating the SIDs and DNs in cross-domain object references.

Overview of Active Directory Replication Replication is the process of propagating object updates between DCs to maintain accurate copies of the Active Directory database.

Because Windows 2000 DCs hold a replica of all of the objects belonging to their domain, and they have full read/write access to those objects, administration of the domain can be done using any DC belonging to that domain. These operations affect the state or the value of an object and must therefore be replicated to the other DCs.

The replication of changed objects does not occur immediately. After a period of time, replication is triggered, collecting all changes and providing them to other DCs. So the normal operational state of the Active Directory on any DC is always one of loose consistency. That is, at any one time, the information across DCs within a Windows 2000 environment is likely to differ as replication changes are underway or are waiting to be triggered. Eventually, the changes arrive and the DCs are synchronized.

Replication and "loose consistency" are important concepts that must be understood when considering the recovery techniques of Active Directory.

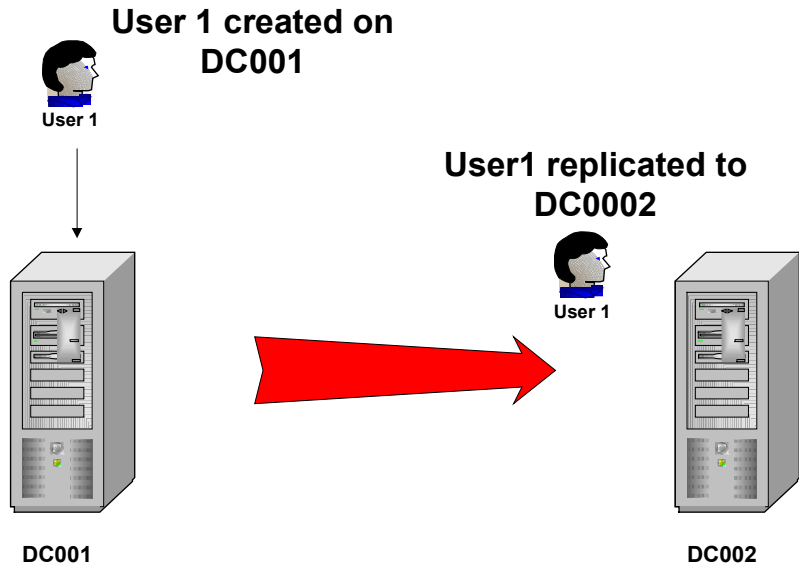


Figure 1: Replication of information from one DC to another

Backup & the Active Directory

It is important to understand and consider the implications of Active Directory backup as part of an Active Directory disaster recovery plan.

Required Rights for Active Directory Backup

Under Windows 2000, backup and restore rights are independent of each other. To back up Active Directory, you must be a member of either the:

- Backup operators group
- Administrators group

Types of Backup

The backup tool in Windows 2000 supports multiple types of backup:

- Normal
- Copy
- Incremental
- Differential
- Daily

However, the only type of backup supported by Active Directory is normal. A normal backup creates a backup of the entire system while the domain controller is online. In addition, it marks each file as having been backed up, which clears the archive attribute of the file. A normal backup also truncates the log files.

When backing up Active Directory using normal backup, the Windows 2000 backup utility (and other supported third party tools) will automatically back up all of the system components and all of the distributed services upon which Active Directory is dependent. This dependent data, which includes Active Directory, is known collectively as the system state.

System State

On a Windows 2000 system acting **only** as a DC (running no services other than those required for DC operation), system state data encompasses the:

- System start-up files
- System registry
- Class registration database of COM+
- SYSVOL
- Active Directory

System Start-Up Files

System start-up files are those required for Windows 2000 to boot. They are automatically backed up as part of the system state.

System Registry

The contents of the registry are automatically backed up when you back up system state data. In addition, a copy of your registry files is also saved in the folder %SystemRoot%\Repair\Regback allowing you to restore the registry without doing a complete restore of the system state.

Class Registration Database of COM+

The Component Object Model (COM) is a binary standard for writing component software in a distributed systems environment. The Component Services Class Registration Database is backed up and restored with the system state data.

SYSVOL

The system volume provides a default Active Directory location for files that must be shared for common access throughout a domain. The SYSVOL folder on a domain controller contains:

- Net logon shares -- these usually host logon scripts and policy objects for non-Windows 2000 based network clients
- File system junctions
- User logon scripts for Windows 2000 based clients and clients that are running Windows 95, Windows 98, or Windows NT 4.0
- Windows 2000 group policy
- File Replication Service (FRS) staging directories and files that are required to be available and synchronized between domain controllers

Active Directory

Important Active Directory information is backed up as part of system state. It includes:

- Ntds.dit -- the Active Directory database
- Edb.chk -- the checkpoint file
- Edb*.log -- the transaction logs, each 10 megabytes (MB) in size
- Res1.log and Res2.log -- reserved transaction logs

What Is a Good Backup?

To ensure a successful restore from backup, it is important to know what defines a good backup. For Active Directory, two things must be considered:

- Contents
- Age

Contents

The first important aspect of a backup is its contents. A good backup will include, at least, the system state, the contents of the system drive, and the SYSVOL folder (if not located on the system drive). As described above, the system state includes many key files and settings to restore a domain controller. Backing up the system drive and SYSVOL folder structure ensures that all of the required system files and folders are in place to initiate a successful restoration.

Note: Best practice states that the Active Directory's log and database files should be separated to provide better performance and redundancy. If you have configured your DCs in this manner, you have Active Directory components spread out on multiple spindles, for example, D:\Winnt\NTDS for your logs and E:\Winnt\NTDS for your database.

Because the Active Directory log files and database are backed up as part of system state, you only have to backup the system drive and the system state to ensure a good backup under this distributed installation.

Age

A backup older than the tombstone lifetime set in Active Directory is not considered to be a good backup.

When an object is deleted in Windows 2000, the DC from which the object was deleted informs the other DCs in the environment about the deletion by replicating what is known as a tombstone.

A tombstone is a representation of an object that has been deleted from the directory. The tombstone is removed, eventually, based on the tombstone lifetime setting, which by default is set to 60 days.

The Active Directory protects itself from restoring data older than the tombstone lifetime. For example, let's assume that we have a user object that is backed up. If after the backup the object is deleted, a replication operation is performed to the other DCs and the object is replicated in the form of a tombstone. After 60 days, all the DCs remove the tombstone as part of the garbage collection process. This is a process routinely performed by DCs to clean up their copy of the database.

If you attempt to restore the deleted object after 60 days, the object cannot be replicated to the other DCs in the domain because it has a USN that is older than the level required to trigger replication. And the other DCs cannot inform the restored DC that the object was deleted, so the result is an inconsistent directory.

Therefore, the useful life of a backup is equivalent to the tombstone lifetime setting for the enterprise.

Given this, Active Directory backup should occur at least once within the tombstone lifetime. However, administrators are generally expected to back up the system state and system drive more regularly to ensure a backup that accurately represents the current environment.

Backup Performance

Understanding the time needed to back up an active DC is important when you are determining the best backup strategy for your business. The graph below shows the time taken to backup Active Directory databases of various sizes.

Note: The data backed up in the tests shown below is for the system state only. As the definition of a good backup also includes the backup of the system drive and SYSVOL, a good backup will take slightly longer, depending on the size of the additional files.

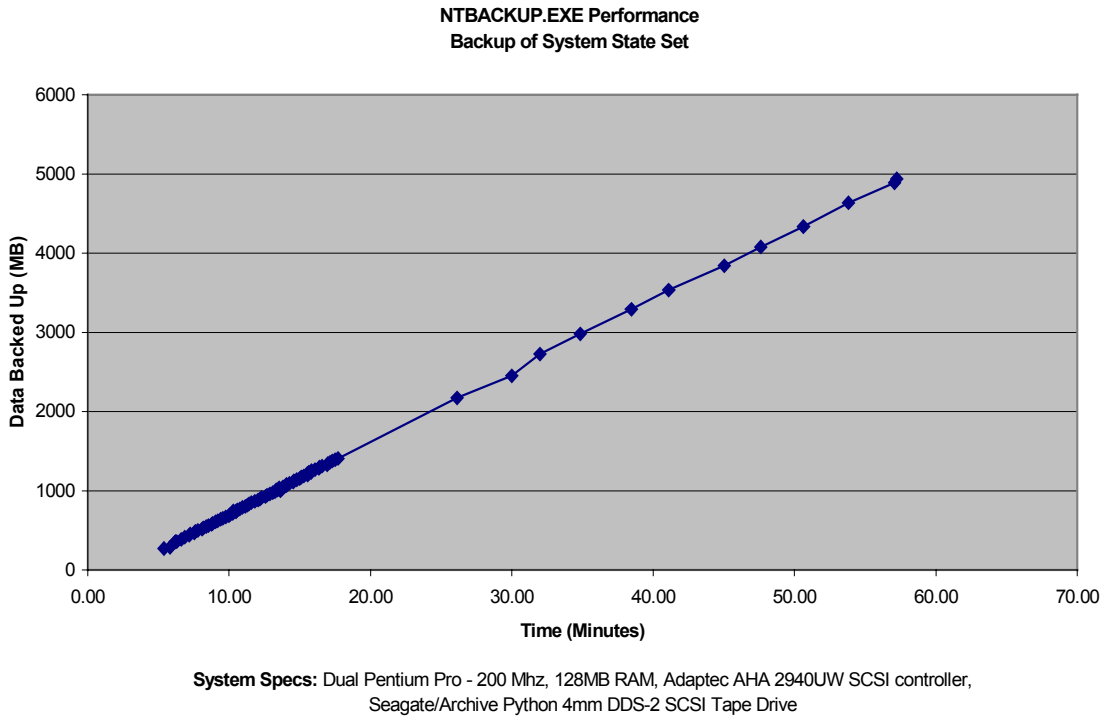


Figure 2: Graph showing backup times for different sizes of Active Directory databases

Repair & The Active Directory

Before discussing the types of restore available under Windows 2000, it is important to understand what options are available to you for the repair of a DC.

In this paper, we list two options:

- Repair of the Active Directory database using NTDSUTIL
- Repair of the DC using various Windows 2000 repair options

Repair of the Active Directory Database Using NTDSUTIL

Windows 2000 uses the version of the database that is called Extensible Storage Engine (ESE).

ESE is a transacted database system that uses log files to support rollback semantics. This ensures that transactions are committed to the database. NTDSUTIL provides a mechanism to access the database for certain database file management functions.

The database repair functionality available under NTDSUTIL is extremely pervasive. Therefore, this method should be used **only** after consulting with the appropriate service personnel and, then, **only** as a last resort.

Due to the potential for damage [error] related to this method of repair, this paper will not discuss the steps required to carry it out. You are urged to seek out the appropriate Microsoft and/or qualified vendor support before attempting it.

Repair of the DC Using Various Windows 2000 Repair Options

Windows 2000 provides three major tools for repairing problems with a Windows 2000 DC (available for all Windows 2000 installations):

- Safe mode startup
- Recovery console
- Emergency repair disk

Safe Mode Startup

If your computer will not start, you may be able to start it in safe mode by pressing F8 when the DC is booting. In safe mode, Windows 2000 uses default settings (VGA monitor, Microsoft mouse driver, no network connections, and the minimum device drivers required) to start Windows.

For example, if your computer will not start after you install new software, you may be able to start it in safe mode with minimal services, and then change your computer settings or remove the newly installed software that is causing the problem. You can reinstall the service pack or the entire operating system, if necessary.

Recovery Console

The recovery console is a text-mode command interpreter (separate from the Windows 2000 command prompt) that allows the system administrator to gain access to a Windows 2000 computer's hard disk, regardless of the file format used. The purpose of this tool is to facilitate basic troubleshooting and system maintenance.

The recovery console allows limited access to NTFS, FAT16 and FAT32 volumes without starting the graphical interface. The recovery console allows administrators to start and stop services, and repair the system in a very granular way. It can also be used to repair the Master Boot Record (MBR), boot sector, and to format volumes.

The recovery console prevents unauthorized access to volumes by requiring the user to enter the system administrator password. This password is defined during the DCPROMO process.

Although the recovery console is not installed on a Windows 2000 DC by default, it is **strongly** recommended you do so after the initial installation sequence is complete.

To install this option, follow the steps outlined in "To Install the Recovery Console as a Startup Option" in the server help file.

Emergency Repair Disk

As with NT 4.0, Windows 2000 has maintained the concept of an Emergency Repair Disk (ERD). The ERD helps you repair problems with system files, your startup environment, and the partition boot sector on your boot volume. If a system failure occurs, you can start the system using the Windows 2000 Setup CD or the Windows 2000 Setup floppy disks, and then use the Emergency Repair Process to restore core system files.

It is strongly recommended that an ERD be created for every DC in your environment, and that it be kept up to date as configuration changes are made on the DC. To create an ERD, follow the steps outlined in the "To Create an Emergency Repair Disk" section of the server help file.

Restore & The Active Directory

If your DC repair fails, you must restore the system using one of the methods outlined in the following section. A brief description is provided here. The exact process is discussed later in this paper.Types of Restore

There are two methods available for restoring a DC to an operational state:

- Restore from replication
- Restore from backup

Restore From Replication

This method relies on Active Directory replication, and is available only if another DC exists in the domain. Once Windows 2000 is installed, the system is once again promoted to a DC in the domain in which it existed before the failure. During this process, the replication that occurs during the normal DCPROMO operation ensures that the DC has an accurate and up-to-date copy of the Active Directory database.

Restore From Backup

This method relies primarily on the last backup taken of the DC before the failure. Once Windows 2000 is installed, a restore process is initiated using either the Windows 2000 backup utility or a supported third-party utility selected by your organization. The restore process returns the DC to its state at the time of backup, and the DC then queries its replication partner(s) for any updates since that time. If there are changes, they will be replicated, ensuring that the DC has an accurate and up-to-date copy of the Active Directory database.

In addition, when you restore Active Directory from backup, you have three further options:

- Non authoritative restore
- Authoritative restore
- Primary restore (SYSVOL only)

These three methods allow you to manipulate two important components of the system state during the restore process: the Active Directory and SYSVOL. Although these components are restored together, they are discussed separately here to ensure that their differences are understood.

Nonauthoritative Restore

ACTIVE DIRECTORY

Nonauthoritative restore is the default method for the restoration of Active Directory, and is used for the majority of restore operations. Using this method, the settings and entries that existed in the Domain, Schema, Configuration, and (optionally) Global Catalog naming contexts maintain the version number they had at the time of backup.

After a nonauthoritative restore, the DC is updated using normal replication techniques. That is, if the version number of an object is less than the same object's version number stored by its

replication partner(s) (indicating the object has changed since it was last backed up), the object on the restored server is updated. This ensures an up-to-date version of the database.

SYSVOL

By restoring the SYSVOL nonauthoritatively, the local copy that is held on the restored DC is compared with that of its replication partner(s) (using MD5 checksums). Once the DC reboots, it will contact its replication partner(s), compare SYVOL information, and replicate the necessary changes, bringing it up to date with the other DCs within the domain.

This method should be used when there is at least one other functioning DC in the domain. This is the default SYSVOL restoration method that occurs automatically if a nonauthoritative restore of the Active Directory is carried out.

Authoritative Restore

ACTIVE DIRECTORY

An authoritative restore is, in essence, an extension of the nonauthoritative restore process. That is, it requires all the steps of a nonauthoritative restore before it can be initiated. The authoritative restore's distinguishing characteristic is that it increments the version number of an entire directory, a subtree, or individual objects (provided that they are leaf objects) to mark them as authoritative in the directory.

As with a nonauthoritative restore, once a DC is back online, it contacts its replication partner(s) to see what has changed since the last backup. But because the version number of the object(s) restored is higher than the existing instances of those objects held on replication partner(s), the objects on the restored DC appear to be more recent and, therefore, must be replicated out to the rest of the DCs within the environment. (By default, version numbers are incremented by 100,000 under the authoritative restore process.)

Because of this, the authoritative restoration method is typically used when human error is involved, such as when an administrator has accidentally deleted an OU.

Unlike a nonauthoritative restore, an authoritative restore requires the use of a separate application: NTDSUTIL. No backup utilities (at the time of this writing), including the native Windows 2000 utility, can perform an authoritative restore.

Note: An authoritative restore does **not** overwrite new objects created after the backup occurred. An authoritative restore can be carried out only on objects from the configuration and domain contexts. The authoritative restore of schema components is **not** supported.

SYSVOL

By restoring the SYSVOL authoritatively, you are authorizing the copy of SYSVOL that was restored from backup for the domain. Once the necessary configurations have been made, the local SYSVOL is marked as authoritative and replicated out to the other DCs within the domain.

Similar to an Active Directory authoritative restore, this method is typically used when human error is involved and the error has propagated out to other domain controllers, for example when an administrator has accidentally deleted an object that resides in SYSVOL such as Group Policy.

Note: The authoritative restore of SYSVOL does not occur automatically after an authoritative restore of Active Directory, additional steps are required.

Primary Restore

Unique to SYSVOL (and other distributed services) is the concept of a primary restore. A primary restore builds a new ntfrs database by loading the data present under SYSVOL on the local DC. This method should be used when you are trying to restore a domain where no other valid domain controllers exist.

Required Rights for Active Directory Restore

To restore the system state data you must be a Local Administrator.

Active Directory Disaster Recovery Flowchart

The remainder of this paper guides you through the steps required to implement the concepts discussed thus far.

Note: It is important to understand that the flowcharts do not depict every disaster situation. They are included as a guide to help you understand your options.

Type of Disaster

Your first step is to identify the type of disaster you have. For the purposes of this paper, the types of possible disasters are:

≅□□□ Database Corruption

≅□□□ Data Corruption

Database Corruption

Database corruption is defined as a situation where one of the following occurs:

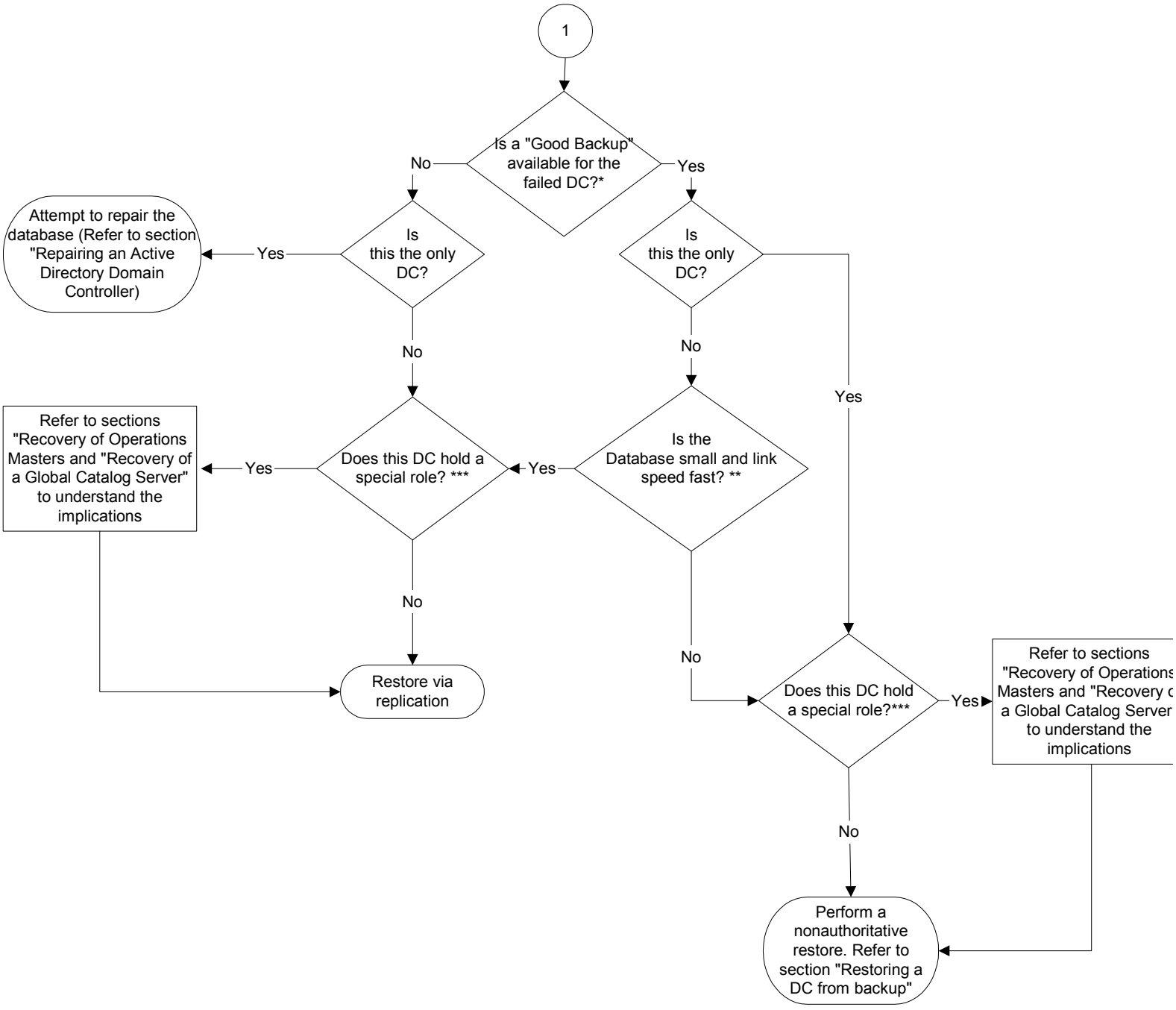
- The disk(s) has (have) become corrupted. For example, when the writeback cache was not saved due to simultaneous power failure and bad batteries.
- The domain controller has suffered a severe hardware failure and needs to be replaced.

Data Corruption

Data corruption is defined as a situation where one of the following occurs:

- The directory contains corrupt data that has replicated to all DCs. This corrupt data needs to be replaced by a trusted backup.
- An administrator (or someone with the necessary permissions) has accidentally deleted an object(s) and the deletion has replicated to other DCs within the environment.

Database Corruption

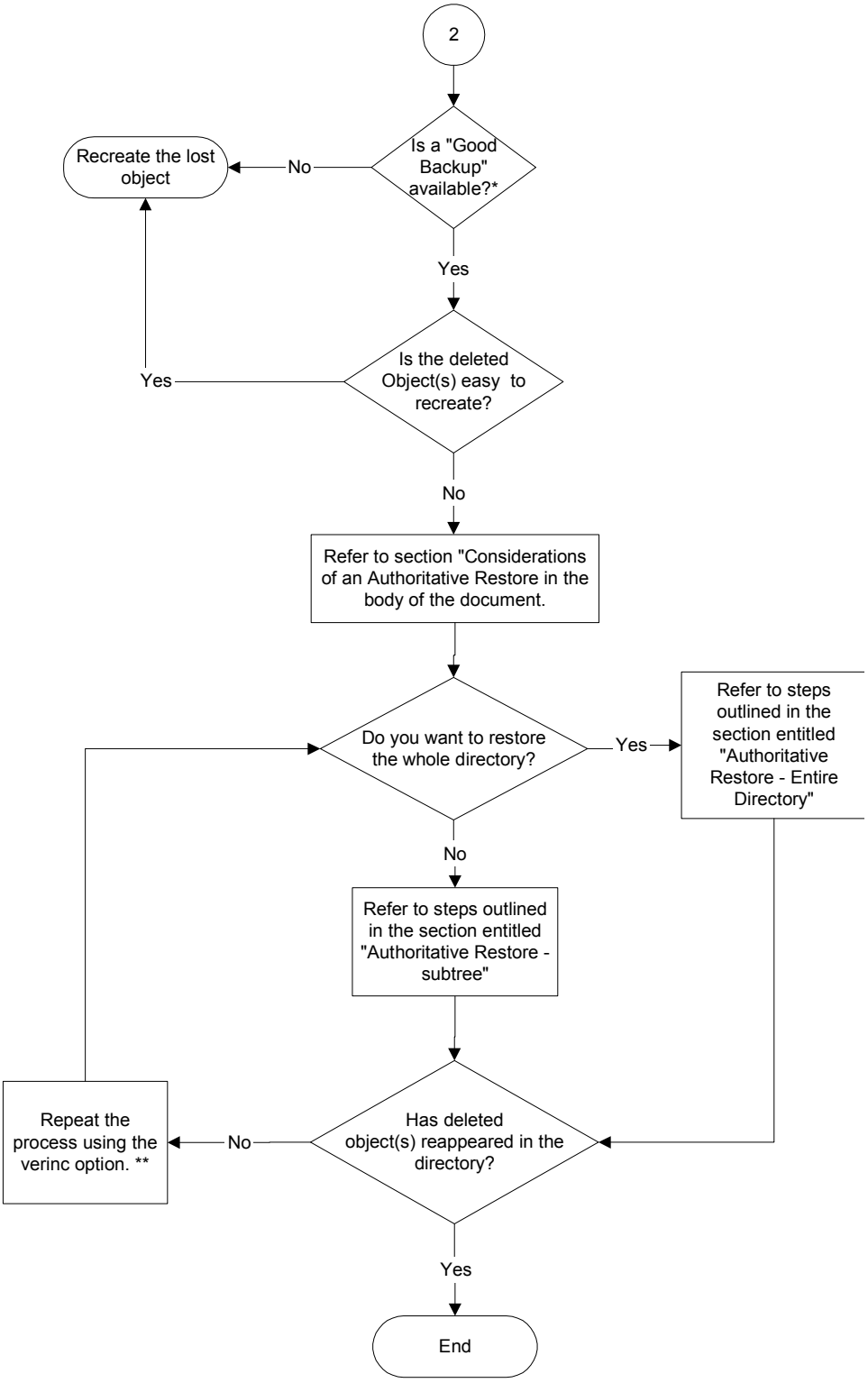


* For the definition of a "good backup" please refer to pg 12 in the paper.

** Decision needs to be made as to the method of restore either via replication or backup. To assist in the decision see section "Recovery of a Windows 2000 Domain Controller.

*** A special role refers to either an OM Role or a GC.

Data Corruption



* Refer to section "What is a good Backup?" in the paper
** For information on the /verinc switch type help at the Authoritative Restore prompt when in NTDSUTIL.

Repairing an Active Directory Domain Controller

This section will discuss to distinct areas of Active Directory Repair:

- Repairing the Active directory
- Repairing the domain Controller

Repairing the Active Directory

Repairing the Active Directory should be the *last resort*. If a valid backup is available, you should always restore that backup. There is no guarantee that repairing Active Directory will work, and in fact there is a risk that this process will result in further loss of data. In addition this could be a very time consuming process.

After doing a repair, a semantic integrity check of the database must be done as outlined in the next section.

To do a repair of the Active Directory, use the repair option in the ntdsutil tool –

```
C:¥>ntdsutil
ntdsutil: files
ntdsutil: repair
```

Ensuring Database Entegrity – Post Repair

The 'Ntdsutil' tool includes a semantics checker that can be invoked by selecting the Semantic database analysis option. The role of the semantic checker is to check the integrity of the contents of the Active Directory database.

The tool is run during Directory Service Restore mode. Errors are written into dsdit.dmp .xx log files. A progress indicator indicates the status of the check.

To perform Semantic database analysis

1. Back up Active Directory. Windows 2000 Backup natively supports backing up Active Directory while online. This occurs automatically when you select the option to back up everything on the computer in the Backup wizard, or independently by selecting to back up the "System State" in the wizard.

2. Restart the domain controller, select the appropriate installation from the startup menu, and press **F8** to display the **Windows 2000 Advanced Option Menu**.

3. Select **Directory Services Restore Mode**, and then press **ENTER**. To start the boot process again, press **ENTER**.

4. Log on by using the Administrator account with the password defined for the Local Administrator account in the offline SAM.

5. From the **Start** menu, point to **Programs and Accessories**, and then click **Command Prompt.**

6. At the command prompt, type **ntdsutil** and then press **ENTER**.

7. Type **Semantic database analysis**, and then press **ENTER**.
8. Type **Verbose on**, and then press ENTER. This displays the Semantic Checker.
9. Type **go**, and then press **ENTER**. The Semantic Checker is started without repairing any errors it encounters. To repair the errors encountered, select the **Go Fixup** option.
10. Type **quit**, and then press **ENTER**. To return to the command prompt, type **quit** again.

Repairing the Domain Controller

Recovery Console

Accessing the Recovery Console

Because the recovery console is installed on the local hard disk, it is typically accessed using the Windows 2000 startup menu. However, if the MBR or the system volume boot sector has been damaged, you will need to start the computer using either the Windows 2000 Setup floppy disks or the Windows 2000 Setup CD.

To do this, follow these steps:

1. Place the Windows 2000 Server/Advanced Server CD in the CDROM drive. If the CD is not bootable, you can use the Windows 2000 Boot floppy disks.
2. Start the computer and enter Windows 2000 Setup.
3. Press **ENTER** at the "Setup Notification" screen.
4. Press **R** to repair a Windows 2000 installation.
5. Press **C** to use the recovery console.

When the recovery console starts, the following information is displayed:

```
Microsoft Windows 2000(TM) Recovery Console.

The Recovery Console provides system repair and recovery functionality.

Type EXIT to quit the Recovery Console and restart the computer.

1: C:\WINNT
```

After you select an installation (In the example above, do this by entering 1.), you will see what looks like a DOS prompt. Then you can begin the repair using the utility-supported commands. For a detailed listing of supported commands, please see Appendix A.

Emergency Repair Disk (ERD)

The process outlined below assumes that you have already created an ERD prior to the failure.

1. Insert the Windows 2000 Setup CD, or the first floppy disk you created from the CD, in the appropriate drive.
2. Restart the computer.

   Floppy Disk users:

   a. Respond to the prompts that request each floppy disk.

   b. When the text-based part of Setup begins, follow the prompts; choose the repair or recover option by pressing **R**.

   Windows 2000 Setup CD users:

   a. When prompted, choose the Emergency Repair Process by pressing **R**.
3. When prompted, choose between the following:
   - Manual Repair (press M): This should be used only by advanced users or administrators. Use this option to choose whether you want to repair system files, partition-boot sector problems, or startup environment problems.
   - Fast Repair (press F): This is the easiest option, and does not require input. This option will attempt to repair problems related to system files, the partition-boot sector on your system disk, and your startup environment (if you have a dual-boot or multiple-boot system).
4. Follow the instructions on the screen and, when prompted, insert the Emergency Repair Disk (ERD) in the appropriate drive.
5. During the repair process, missing or corrupted files are replaced with files from the Windows 2000 CD or from the %SystemRoot%\Repair folder on the system partition. Replacement files from either of these sources will not reflect any configuration changes made after setup.
6. Follow the instructions on the screen. To help diagnose the system damage, we recommend that you write down the names of files that are detected as bad.
7. If the repair was successful, allow the process to complete; the computer will restart. Restart indicates that replacement files were successfully copied to the hard disk.

Recovery of a Windows 2000 Domain Controller

As stated earlier, there are two primary methods for the restoration of a Windows 2000 DC:

- Restore from replication
- Restore from backup

This section outlines the steps required and the considerations associated with these operations.

Restoring a DC From Replication

Before you restore a DC using replication, it is important for you to understand the associated issues.

Considerations for Restoring a DC From Replication

Bandwidth

The primary consideration when restoring a DC from replication is bandwidth. Obviously, the bandwidth required to restore a DC from replication depends on the size of the Active Directory database and the time you have to restore the DC to a functioning state.

The chart below shows the time needed to replicate a DC to an existing domain at various network speeds. The size of the Active Directory database (ntds.dit) we used in the testing was 2 GB.

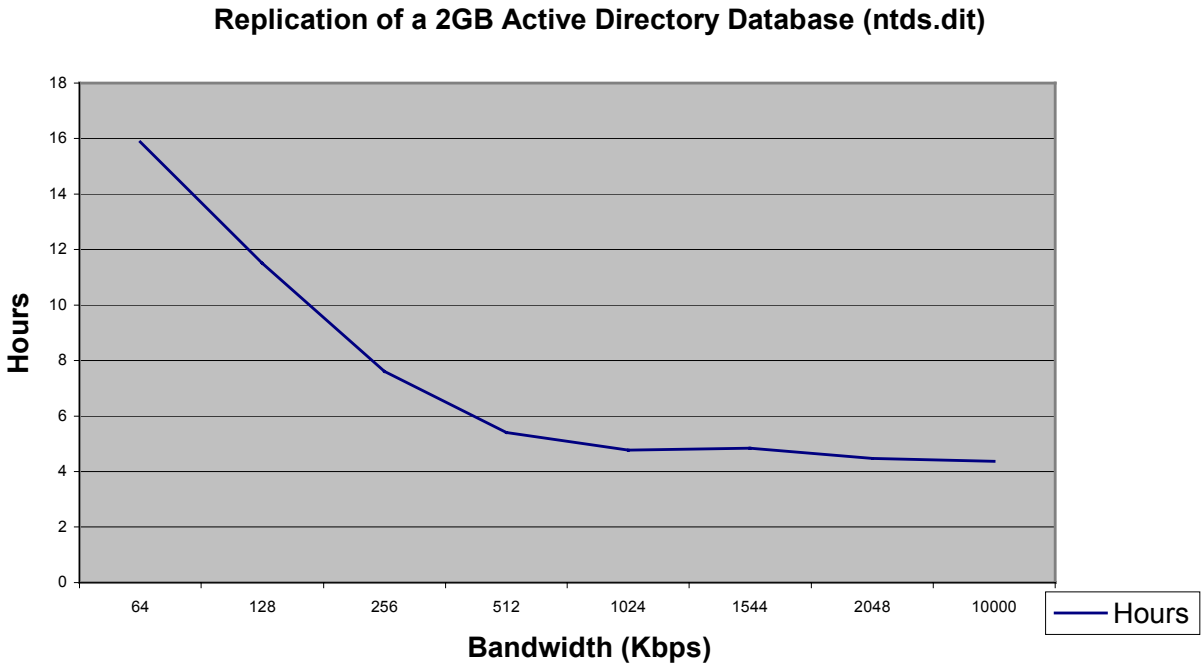


Figure 3: Graph showing time to replicate 2GB NTDS.dit file over varying network speeds.

Note: The systems used to gather the data for the above chart were Proliant 1600s with dual Pentium II 266 MHz, 256 MB RAM, and a single hard drive. Using different systems may affect the results, but the overall trend will remain consistent.

Steps Required to Restore a DC From Replication

The target domain must contain at least one DC that is functioning. To restore from replication, you follow the same steps you use to create a new DC. After you clean any failed DC functionality from the target server, launch DCPROMO and then create a DC for the target domain using appropriate parameters for the environment.

Ideally, the new DC should be located in the same Active Directory site as the replicated DC. This reduces the network impact and the restore time associated with replication. For a look at the effect of bandwidth on replication, see Figure 3 in this document.

If the server you use to restore is the same server, that is, the same Windows 2000 installation with the same name, then the target server cannot be the DC for any domain, nor can it have any components of the failed DC function installed in it. DCPROMO removes any metadata in the Active Directory from the last instance of this server as a DC.

If a new server is being used (a new physical server or a new installation of Windows 2000), then any reference to the old DC must be cleaned from the Active Directory using NTDSUTIL. Because this involves modification of the configuration naming context, it requires Enterprise Administrator permissions.

To remove the previous instance of the DC from the Active Directory, follow these steps:

1. Type **NTDSUTIL** from the command line.
2. Type **metadata cleanup** and press **Enter**.
3. Type **connections** and press **Enter**.
4. Type **connect to server** <servername> and press **Enter,** where <servername> is the DC name.
5. Type **quit** and press **Enter** to return to the metadata cleanup menu.
6. Type **select operation target** and press **Enter**.
7. Type **list domains** and press **Enter**. This lists all domains in the forest with their corresponding numbers.
8. Type **select domain <number>** and press **Enter,** where <number> is the number that corresponds to the domain in which the failed server was located.
9. Type **list sites** and press **Enter**.
10. Type **select site <number>** and press **Enter,** where <number> is the number of the site in which the DC was a member.
11. Type **list servers in site** and press **Enter**. This lists all servers in that site with their corresponding numbers.
12. Type **select server <number>** and press **Enter,** where <number> is the DC to be removed.
13. Type **quit** and press **Enter** to return to the metadata cleanup menu.
14. Type **remove selected server** and press **Enter**.

At this point, you should receive confirmation that the DC was removed successfully. If you receive an "object could not be found" error, the DC may have already been removed from the Active Directory.

15. Type **quit** and press **Enter.** Repeat this step until you return to the command prompt.
16. Delete the DC using the Active Directory Users and Computers tool.
17. Delete the DC using the Active Directory Sites and Services tool.

Restoring a DC From Backup

Before you restore a DC using backup, it is important for you to understand the associated issues.

Considerations for Restoring a DC From Backup

Time

The obvious advantage when restoring a DC from backup as opposed to replication is the faster restore times available to you.

The chart below shows the time needed to restore a DC from backup with databases from 500 MB to 2 GB in size. The machine used in the test was a Proliant 800 with a single 400 MHz processor, 256 MB RAM, and a 4/8 GB DAT drive.

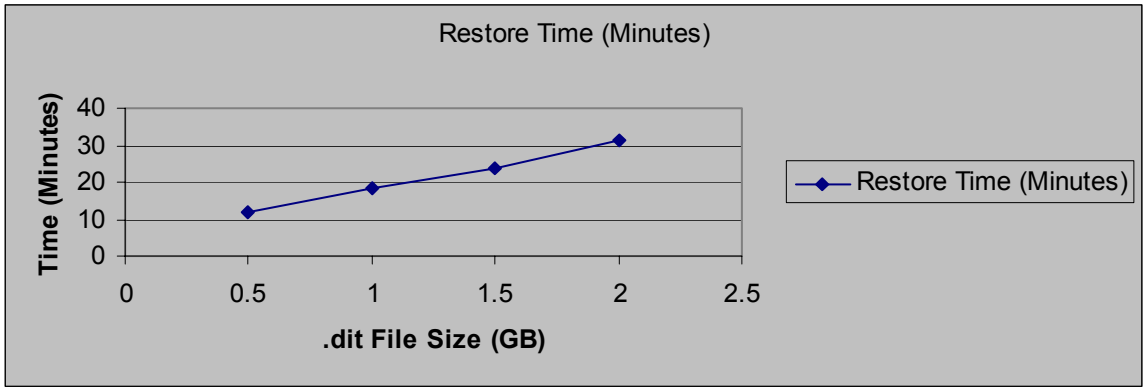


Figure 4: Graph showing time to restore different sizes of DIT files from backup

Note: This chart shows the time to restore system state only. A "good backup," as defined earlier, will take longer, depending on the size of your system drive.

Useful Life of Active Directory Backup

You must ensure that the backup you use for the restore was taken within the tombstone lifetime. By default, this is set to 60 days. For more information on the useful life of an Active Directory backup, see the "What Is a Good Backup?" section of this paper.

Different Hardware

You can restore a DC to different hardware, however, you should be aware of some issues:

- *Different hal.dll Files*

  By default, the hal.dll is not backed up as part of the system state; however the kernel32.dll is. Therefore, if you are trying to restore a backup to a machine that requires a different hal.dll (for example, to support a multiprocessor environment), you will run into compatibility issues with the new hal.dll and the original kernel32.dll.

  The only workaround for this situation is to explicitly copy the hal.dll from the original machine to the new machine. The limitation associated with this workaround is that the new machine will be bound to using only a single processor.

- *Incompatible boot.ini File*

  If you backup and restore the boot.ini file, you may have some incompatibility issues with your new hardware configuration, resulting in a failure to boot. Before restore, ensure that the boot.ini file is correct for your new hardware environment.

- *Different Cards*

  If your new hardware has a different video adapter or multiple network adapters, uninstall them before you restore data. When you restart the computer; the normal plug-and-play functionality will make the necessary changes.

Disk Space and Partition Configuration for Different Hardware

In addition to the above issues, you must ensure that the partitions you have on the new machine match the ones you had on the original machine. Specifically, all the drive mappings must be the same and the partition size(s) must be at least the same as they were on the original machine.

Considerations for a Nonauthoritative Restore

You also need to be aware of issues related to the authoritative and nonauthoritative methods of restoration.

ACTIVE DIRECTORY

There are no real issues with this method of restoration.

SYSVOL

There are no real issues with this method of restoration.

Steps Required for a Nonauthoritative Restore

To perform a nonauthoritative restore using the Windows 2000 native backup utility, follow these steps:

1. Reboot the target system into Directory Services Restore Mode by pressing the **F8** key upon system startup.

Note: Step 1 assumes that you are already running a DC. If this is not the case, begin the process from step 4.

2. Select **Directory Services Restore Mode** (Windows 2000 domain controllers only).
3. Select the operating system that you wish to start in restore mode.
4. Log in as Administrator (local system account, no domain selection available).

5. Run the Windows 2000 Backup utility and select the Restore tab.

Note: If you use the Restore Wizard for step 5, you **must** also click the Advanced button and make sure you are restoring junction points. If you do not follow the Advanced menu, the restore process will fail.

6. Select the appropriate backup location and ensure that at least the System Drive and System State check boxes are selected and checked.
7. Ensure **Original Location** is selected in the "Restore Files to" drop-down list.
8. Click on the **Start Restore** button.
9. Click **OK** to accept the warning.
10. Click **OK**.
11. Click **OK** to confirm restore.
12. Click **OK** to confirm restore source.
13. When the restore is complete, click **YES** to Restart Computer.

The system will reboot and replicate any new information since the last backup with its replication partner(s).

Note: A nonauthoritative restore of Active Directory automatically executes a nonauthoritative restore of SYSVOL; therefore, no additional steps are required.

Considerations for an Authoritative Restore

ACTIVE DIRECTORY

Group Memberships

The most significant issue is the possible loss of group membership information. Due to the multi-attribute nature of security groups and the way links, back links, and deletions are handled in Active Directory; the results of an authoritative restore may vary. The variations depend on which objects replicate first after the authoritative restore is complete.

- *User object replicates first*

  If the un-deletion of the user replicates first, then the group membership information of both the group (the members it contains) and the user (the groups he/she belongs to) will be represented correctly.

- *Group object replicates first*

  If the un-deletion of the group replicates first, then the replicator on the replication partner(s) will drop the addition of the (locally) deleted user from the group. The only exception to this is the user's primary group, which is always represented correctly both from the user and group reference.

Unfortunately, you cannot define which objects replicate first after an authoritative restore. The only workaround is to modify the group membership attributes of the affected groups on the DC where the authoritative restore was carried out.

Because this issue stems **not** from the integrity of the restored data, but from the way in which the data is replicated, the DC where the authoritative restore was carried out holds the only accurate copy of the directory within the domain.

By looking at this DC, administrators can see the way their directory should look and take steps to replicate the accurate directory information to the other DCs within the domain. The best way to do this is to add a dummy user to, and then delete that same dummy user to/from, each group that was involved in the authoritative restore.

Note: The definition of "involved" in this context is any group that was authoritatively restored, any group whose members were restored, or any group that was not defined as the Primary Group.

By doing this, you force the replication of the correct group membership information from the source DC (the DC where the authoritative restore was carried out) to its replication partner(s). The updated objects will correct the information shown in the "Member of " tab of the restored user objects.

Important: To ensure the success of the method defined above, you **must** make sure that no additions are made to group memberships (for the affected groups and users) on any of the other DCs within the environment.

Otherwise, you risk corruption of the accurate version of the directory (held on the DC where the restore took place) by the new membership information. If additions are made to group memberships, you must either update group membership manually, or you must perform another authoritative restore of the object(s) using the /verinc switch and then perform the process defined above again.

Trusts and Computer Accounts

Under Windows 2000, trust relationships and computer account passwords are negotiated at specified intervals (by default, 7 days for trust relationships and 30 days for computer accounts).

The Authoritative Restore method allows you to restore previously used passwords for the objects in the Active Directory that maintain trust relationships and for computer accounts.

In the case of trust relationships, this may impact communication with other domain controllers from other domains, manifesting in permissions errors when trying to access resources across domain boundaries. To rectify this, NTLM trust relationships to Windows 2000 or earlier domains must be removed and recreated.

In the case of computer accounts, this could impact communication between the member workstation or server and a DC in its domain. This usually manifests itself in NT or Windows 2000 user authentication issues (invalid account). If this occurs, the account must be removed and recreated.

To restore trust relationships and to reset computer account passwords, you can use the NETDOM utility included in the support tools on the Windows 2000 CD.

Note: NT 4.0 machines change passwords every 7 days.

SYSVOL

Bandwidth

When you perform an authoritative restore of the Active Directory, you should also perform an authoritative restore of the SYSVOL. By doing this, you are telling the other DCs in the domain that the SYSVOL information on the restored DC is authoritative. As a result, the SYSVOL information on the restored DC is replicated to all other DCs in the domain through replication partner(s).

The bandwidth associated with such replication is a consideration only in a domain where there is extensive use of large Group Policies and scripts. Unlike Active Directory replication, FRS replication is not compressed between sites.

Note: SYSVOL replication between sites is expected to be compressed in future versions of the Windows 2000 operating system.

Steps Required for an Authoritative Restore

You can restore the entire directory, a subtree, or an individual object. The sections below provide steps for restoring the entire directory and for restoring a subtree of a directory.

Note: The following process is based on NTBACKUP.exe.

Authoritative Restore – Entire Directory

Note: The authoritative restore of the entire directory should be carried out **only** as a last resort.

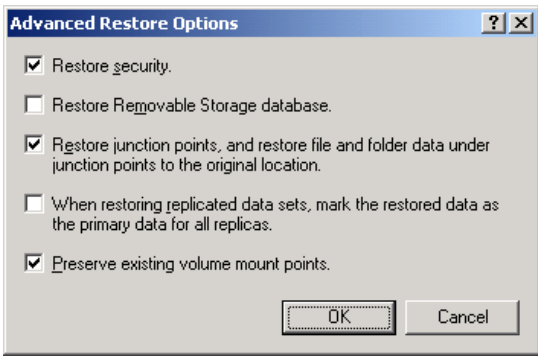
1. Reboot the target system into Directory Services Restore Mode by pressing the **F8** key upon system startup.

   Note: Even if the system is not currently acting as a DC, you are still required to reboot the system into Directory Services Restore Mode to perform an authoritative restore.

2. Select **Directory Services Restore Mode** (Windows 2000 domain controllers only).
3. Select the operating system that you wish to start in restore mode.
4. Log in as Administrator (local system account, no domain selection available).
5. Run the Windows 2000 Backup utility and select the Restore tab.

   Note: If you use the Restore Wizard for step 5, you **must** also click the Advanced button and make sure you are restoring junction points. If you do not go through the Advanced menu, the restore process will fail.

6. Select the appropriate backup location and ensure that at least the System Drive and System State check boxes are selected.
7. Ensure **Original Location** is selected in the "Restore Files to" drop-down box.
8. Click the **Start Restore** button.
9. Click **OK** to accept the warning.
10. Click **Advanced** in the "Confirm Restore" dialog box.
11. Ensure that at least the following are checked:



12. Click **OK**.
13. Click **OK** to confirm restore.
14. Click **OK** to confirm restore source.
15. When the restore is complete, click **NO** to Restart Computer.
16. Click on the Restore tab again.
17. Ensure **Alternate Location** is selected in the "Restore Files to" drop-down list.
18. Click **Start Restore**.
19. Click **OK** to accept the warning.
20. Click **OK**.
21. Ensure the restore source is the same as in step 14.
22. When the restore is complete, close NTBACKUP Application
23. Open a command prompt and type **ntdsutil**.
24. Type **authoritative restore**.
25. Type **restore database**.
26. At the "Authoritative Restore Confirmation" dialog box, click **OK**.
27. Type **quit**.
28. Type **quit**.
29. Type **exit**.
30. Restart the server.

    The server is now the authoritative DC for the domain. Changes will be replicated to the other DCs within the environment.

31. When the system has rebooted, and **AFTER** the SYSVOL share is published (this may take a few minutes), copy the required files/folders from the alternate SYSVOL directory location to the original location.

For example:

Copy the contents of the Scripts directory from

c:\<Alternate Sysvol Location>\sysvol\c_\winnt\Sysvol\Domain\scripts\ …. to

c:\Winnt\SYSVOL\Sysvol\domain\scripts\…..

Copy the contents of the Policies directory from

c:\<Alternate Sysvol Location>\sysvol\c_\winnt\Sysvol\Domain\policies\ …. to

c:\Winnt\SYSVOL\Sysvol\domain\policies\…..

By restoring the SYSVOL this way, you ensure that new or edited files/folders, such as policies or scripts created after the last backup, are not deleted. Because the names of the new or edited files/folders did not change after they were modified, the files/folders that existed at the time of

the last backup are replaced with the version that was included in that backup. This could result in a loss of data, if the files/folders were changed since the last backup.For example, a Group Policy called Finance Policy existed at the time of the last backup, and was referenced by a folder in the SYSVOL directory as:

C:\WINNT\SYSVOL\Sysvol\Domain.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}

Shortly after the last backup, an administrator edited the Finance Policy, and although the properties of the policy changed, the GUID of the Group Policy object remained the same. So the policy continues to be referenced by the same directory name {31B2F340-016D-11D2-945F-00C04FB984F9}.

During the authoritative restore of the directory, the folder {31B2F340-016D-11D2-945F-00C04FB984F9} in the alternate SYSVOL location was copied to the original SYSVOL location, replacing the old folder and thus losing the changes the administrator made after the backup. This step is necessary, however, to maintain the synchronization between the Active Directory and SYSVOL.

Authoritative Restore – Subtree

This method restores specific component(s) of Active Directory and marks them as authoritative for the directory. This method is the most commonly used because there are few occasions when the entire directory needs to be restored.

To perform the authoritative restore of a subtree, follow the steps in the "Authoritative Restore – Entire Directory" section of this paper, up to and including step 21. Then follow these steps:

1. Type **restore subtree <path>**. For example: restore subtree OU=Sales,OU=Sydney,DC=Whitepaper,DC=com
2. At the "Authoritative Restore Confirmation" dialog box, click **Yes**.
3. Type **quit**.
4. Type **quit**.
5. Type **exit**.
6. Restart the server.

This server is now the authoritative Active Directory DC for the path you specified. Changes will be replicated to the other DCs within the domain.

Because you are restoring only a portion of the Active Directory, you do not need to do an authoritative restore of the SYSVOL. However, if the subtree or object that was authoritatively restored contained elements from the SYSVOL (for example, a group policy), you should also restore that portion of the SYSVOL authoritatively.

If this is required, follow steps 27 and beyond from the "Authoritative Restore – Entire Directory" section of this paper.

Considerations for a Primary Restore

Before you perform a primary restore, it is important for you to understand the associated issues.

Active Directory

The primary restore method cannot be used to restore Active Directory.

SYSVOL

You can perform a primary restore only if there are **no** other DCs in the domain.

To perform a primary restore, follow these steps:

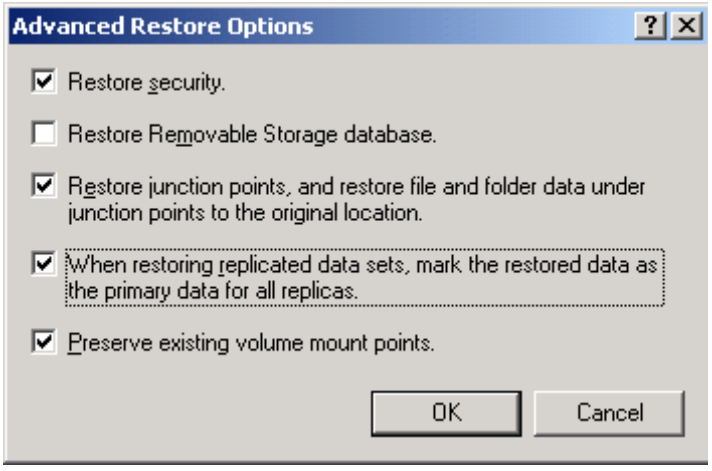
1. Reboot the target system into Directory Services Restore Mode by pressing the **F8** key upon system startup.

Note: Even if the system is not currently acting as a DC, you are still required to reboot the system into Directory Services Restore Mode to perform a primary restore.

2. Select **Directory Services Restore Mode** (Windows 2000 domain controllers only).
3. Select the operating system that you wish to start in restore mode.
4. Log in as Administrator (local system account, no domain selection available).
5. Run the Windows 2000 Backup utility and select the Restore tab.

Note: You cannot perform a primary restore of the SYSVOL using the Restore Wizard. You must go directly to the Restore tab.

6. Select the System Drive (typically C:) and System State for recovery.
7. Click the **Start Restore** button.
8. Click **OK** to accept the warning.
9. Click **Advanced** in the "Confirm Restore" dialog box.
10. Ensure that at least the following are checked:



11. Click **OK**.
12. Click **OK** to confirm restore.
13. Click **OK** to confirm restore source.
14. Click **Close** on the progress report.

15. If you only need a nonauthoritative restore, click **Yes** to reboot. If you need to perform an authoritative restore, click **No** and make the necessary changes using NTDSUTIL.

Verification of a successful Restore

Although there could be a number of tests to see if a domain controller is functioning correctly after a restore, the following are two of the basic tests one should perform to verify the success of a restore.

Reboot in normal mode

If the domain controller is able to successfully boot into normal mode, means the directory is able to successfully initialize. Especially if it wasn't able to do so before it was restored.

Check if domain controller is able to authenticate with its neighbors

Use the 'repadmin' tool to verify this. This is primarily used to check if the restored domain controller can authenticate with another domain controller and replicate in changes, so as to update its copy of the directory. Being able to do so is critical for it to be able to carry out its task of being a domain controller.

The first check is to obtain the inbound partners for the 'restored' domain controller. The options used are –

```
D:\>repadmin /showreps
testlab\test-machine3
DSA Options : (none)
objectGuid  : a07b44e6-76ba-4f03-80c9-5a4a256347bb
invocationID: 6037d0c3-2194-4f27-95ed-578b38861414

==== INBOUND NEIGHBORS ======================================

CN=Schema,CN=Configuration,DC=testdom,DC=nttest,DC=microsoft,DC=com
   testlab\test-machine1 via RPC
      objectGuid: 465848f9-5446-4176-a504-59629c7a8fd8
      Last attempt @ 2000-09-08 14:10.16 was successful.

CN=Configuration,DC=testdom,DC=nttest,DC=microsoft,DC=com
   testlab\test-machine1 via RPC
      objectGuid: 465848f9-5446-4176-a504-59629c7a8fd8
      Last attempt @ 2000-09-08 14:10.16 was successful.

DC=testdom,DC=nttest,DC=microsoft,DC=com
   testlab\test-machine1 via RPC
      objectGuid: 465848f9-5446-4176-a504-59629c7a8fd8
      Last attempt @ 2000-09-08 14:10.16 was successful.
```

In the above case, the restored DC is 'test-machine 3'. The test has been run on the restored machine, but the tool is remote able and hence can be used on any domain controller. 'Test-machine 1' is its inbound partner.

The next command would attempt to sync the ‘schema’ naming context on the ‘restored’ domain controller with changes from its ‘inbound’ neighbor.

```
D:\>repadmin /sync <naming context> <destination DSA> <source DSA GUID>

D:\>repadmin /sync "CN=Schema,CN=Configuration,DC=testdom,DC=nttest,DC=microso
ft,DC=com" test-machine3 465848f9-5446-4176-a504-59629c7a8fd8
Sync from 465848f9-5446-4176-a504-59629c7a8fd8 to test-machine3 completed.
```

You could then try the same command to sync the ‘inbound’ neighbor with the restored domain controller to check if outbound replication is working –

```
D:\>repadmin /sync "CN=Schema,CN=Configuration,DC=testdom,DC=nttest,DC=microso
ft,DC=com" test-machine1 a07b44e6-76ba-4f03-80c9-5a4a256347bb
Sync from a07b44e6-76ba-4f03-80c9-5a4a256347bb to test-machine1 completed succ
essfully.
```

If the sync is successful, then the domain controller is able to authenticate with a neighboring domain controller and receive changes from it. If not, then it could mean that the machine account password on the restored domain controller is old, such that the inbound partner cannot authenticate the ‘restored’ domain controller. You should use the netdom tool to set the password on the replica domain controller and restored domain controller to be the same. For more information on the ‘netdom’ tool, see the ‘Support tools help’.

Check the Directory Service Event log for any ‘error’ messages

You could also check the Directory and System event logs for any error messages pertaining to the restore process.

To verify an authoritative restore

In addition to the above steps for ‘non-authoritative’ restore, you should verify that the objects you authoritatively restored appear in the directory.

You can also use the Repadmin command-line tool to verify that the authoritative restore was successful by checking the version number increase on the directory or subtree. Do this by carrying out the /showmeta command followed by the exact distinguished name of the directory or subtree that you authoritatively restored.

Recovery of a Global Catalog Server

To recover the Global Catalog (GC) service, you can either restore the affected GC from backup, or you can assign a new GC to compensate for the loss of the original.

Steps Required for the Restore of a Global Catalog

Refer to the "Restoring a DC From Backup" section in this paper. Restoring from backup is the only way you can automatically restore a DC (that was functioning as a GC at the time of backup) to the role of GC. Restoring from replication does not automatically reinstate the GC role, because the GUID of the system has changed and the directory therefore considers it to be a different system.

Steps Required to Assign a New GC

You may wish to create a new GC in your environment if you anticipate an extended downtime for the GC that failed. This would be particularly relevant if the user community that was being served by the original GC no longer had access to a GC, or if the requirement for the GC is significant in your environment (for example, you are running Exchange 2000). To enable a new Global Catalog, follow the steps in the "To Enable or Disable a Global Catalog" section in the server help file.

Note: Having multiple GCs in a forest increases replication traffic and adds to the overall complexity of the environment. If you reinstall the failed DC and maintain its role as a GC, you should remove any additional GCs you may have configured during its absence if the services are no longer required.

Recovery of Operations Masters

When an OM becomes unavailable, the only way the service can be reinstated is to:

- Repair the existing OM by using the repair methods discussed earlier or by restoring it from backup.
- Seize the role to another DC within the environment.

Note: Restoring an OM from replication will not restore its original role status.

Seizing an Operations Master Role

Seizing, or forcing transfer, as it is sometimes called, is a process carried out without the cooperation of the original role holder. In other words, when the original role holder has suffered a disaster, you can seize the role, forcing it to be moved to another DC within the domain/forest.

Although the process required to seize an OM role is similar to the process used for all five roles, the issues associated with OM seizure differ.

Note: The graceful transfer of an OM role will not be discussed in this paper. Logically, if a transfer is still possible, then the original role holder is active and a recovery is not required.

Recovering the Schema Master

Before you decide whether to seize or to repair/restore the schema master role, it is important for you to understand the associated issues.

Impact on Environment

Unable to Make Changes to the Schema

When the schema master is unavailable, changes to the schema are not possible. If you attempt to make changes to the schema when the schema master is unavailable, you will see a message similar to this:

Note: The message displayed depends on the method of change you are attempting. Above, we were attempting to install Exchange 2000 while the schema master was unavailable.

In most production environments, changes to the schema should be infrequent and planned well in advance, so a schema master outage should not pose any immediate problems.

Considerations for Seizing a Schema Master

The primary consideration is the permanence of the outage. Because of the chance of duplicate schema changes being propagated throughout the environment, a seizure of the schema master role should be carried out only if the failed role holder will **never** come back online.

Because of the infrequent requirement for a schema master role and the implications of a seizure, you can usually live with the outage during the period of time it takes to restore the DC holding the role. However, if you require the immediate use of the schema master role or if the original role holder will never be brought back into the Windows 2000 environment, a seizure can be carried out.

Steps Required to Seize the Schema Master

The DC that will be seizing the role must be fully synchronized with respect to updates performed on the previous role holder. This is why we strongly recommend that you specify standby role holders that (1) are located within the same site and that (2) are direct replication partners with the existing role holder.

To ensure that the standby operations master that you selected for your environment is the most appropriate, use RepAdmin.exe (included in the support tools on the Windows 2000 CD) to check its status.

To demonstrate this, suppose that server SYD01 is the schema master of domain Whitepaper.com.au, SYD02 is the specified standby OM, and MEL01 is the only other DC of domain Whitepaper.com.au.

Type the following two commands:

C:\>**repadmin /showvector dc=whitepaper,dc=com,dc=au SYD02.whitepaper.com.au**
Sydney\SYD01 @ USN 4023
Melbourne\MEL01 @ USN 4087

C:\>**repadmin /showvector dc= whitepaper,dc=com,dc=au MEL01.whitepaper.com.au**
Sydney\ SYD01 @ USN 4018
Sydney\SYD02 @ USN 5017

Because SYD01 was the originating schema master, these are the only USNs we are concerned with. Because the USN on SYD02 (4023) is higher than the USN on MEL01 (4018), we know that it is more up to date than MEL01 and, therefore, it is the more appropriate candidate to assume the role.

Now that you have determined the best candidate to take on the schema master role, follow these steps:

1. Open a command prompt.
2. Type **ntdsutil**.
3. At the ntdsutil prompt, type **roles**.
4. At the fsmo maintenance prompt, type **connections**.
5. At the server connections prompt, type **connect to server <FQDN of server>**. For example: connect to server syd02.whitepaper.com.au
6. At the server connections prompt, type **quit**.

7. At the fsmo maintenance prompt, type **seize schema master**.

Note: FSMO (Flexible Single Master of Operations) was the name for operations masters in beta releases of Windows 2000. The name change has yet to be reflected in the tool.

8. At the popup window, verify the role seizure information.
9. After verification, click **Yes**.
10. At the fsmo maintenance prompt, type **quit**.
11. At the ntdsutil prompt, type **quit**.

Recovering the Domain Naming Master

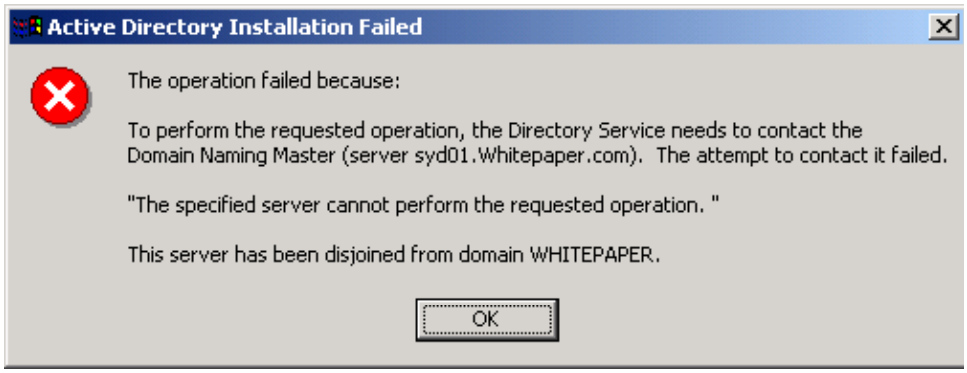
Before you decide whether to seize or to repair/restore the domain naming master role, it is important for you to understand the associated issues.

Impact on Environment

Domains Cannot Be Added to the Forest

When the domain naming master is unavailable, domains cannot be added to the Active Directory.

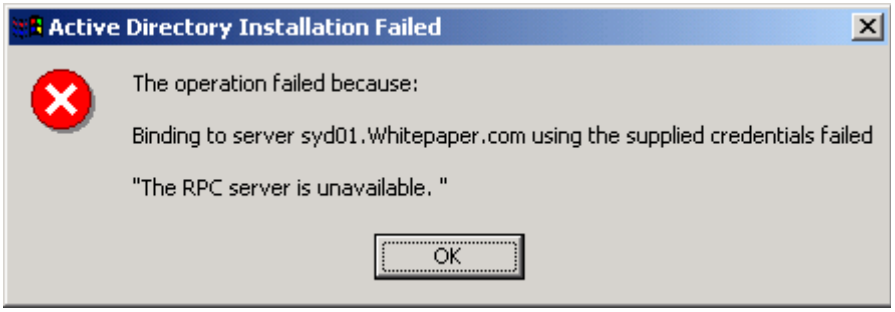
Below, we were attempting to run DCPROMO to add a domain when the domain naming master (Syd01.Whitepaper.com) was unavailable:



In a stable production environment this should not be a significant issue, but in a development, testing or growing production environment, the failure of this master can halt growth until it is restored or seized.

Domains Cannot Be Removed From the Forest

Below, we were attempting to run DCPROMO to remove a domain when the domain naming master (Syd01.Whitepaper.com) was unavailable:



Again, this should be of limited concern in the vast majority of environments.

Considerations for Seizing a Domain Naming Master

The primary consideration is the permanence of the outage. Because of the chance of duplicate domain naming changes being propagated throughout the environment, a seizure of the domain naming master role should be carried out only if the failed role holder will **never** come back online.

Because of the infrequent requirement for a domain naming master role and the implications of a seizure, you can usually live with the outage during the period of time it takes to restore the DC holding the role. However, if you require the immediate use of the domain naming master role or if the original role holder will never be brought back into the Windows 2000 environment, a seizure can be carried out.

Steps Required to Seize the Domain Naming Master

To seize the domain naming master, you follow the steps in the "Steps Required to Seize the Schema Master" section of this white paper, except you replace step 7 with:

At the fsmo maintenance prompt, type **seize domain naming master**.

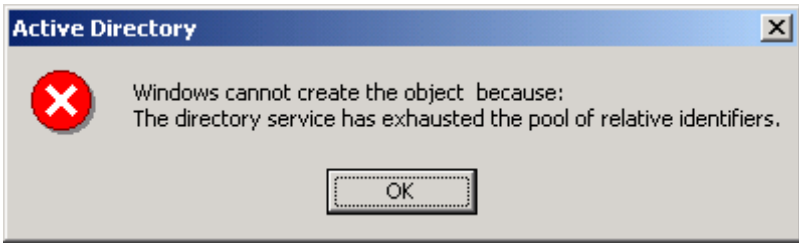
Recovering the RID Master

Before you decide whether to seize or to repair/restore the RID master role, it is important for you to understand the associated issues.

Impact on Environment

Unable to Create Security Object

When the RID master is unavailable, you cannot add any new security objects, such as users, groups and computers to the domain. You will receive the following error:



You will also receive an error (event ID 16645) in the event log on the DC in which you attempted to create the object. The error will explain that the maximum account identifier allocated to this domain controller has been assigned.

Failure to Move Security Principles Between Domains

You will be unable to move security principles to a new domain when the RID master in the target domain is not operational.

When considering the above issues, it is important for you to understand that these problems will **not** emerge as soon as the RID master is offline. These issues will surface **after** the RID pool (512 individual RIDs in a pool) for each domain controller within the domain has been depleted.

So, if you have a domain with five remaining DCs, you could still theoretically have 2560 (5 x 512) RIDs available to you after the RID master fails. In a typical environment, this would provide you with ample RIDs for the creation of security principles until the RID master is repaired/restored using the methods discussed earlier. If, however, you were in the middle of a mass creation of security objects or inter-domain object moves that required more RIDs than you have in your existing pools, a role seizure could be performed.

Considerations for Seizing a RID Master

Consider carefully before you decide to perform a seizure on a RID master. Because of the risk of duplicate RIDs on the network, the sever that originally housed the RID master role should **never** come back online. Instead, you should completely rebuild the original role holder before you reintroduce it to the production Windows 2000 environment.If, after you understand all the implications of a RID master seizure, your situation still requires you to have an active RID master immediately, follow the steps below to seize the RID master role.

Steps Required to Seize the RID Master

To seize the RID master, you follow the steps in the “Steps Required to Seize the Schema Master” section of this white paper, except you replace step 7 with:

At the fsmo maintenance prompt, type **seize RID master**.

Recovering the PDC Emulator

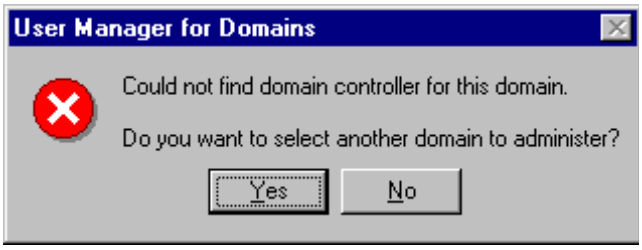
Before you decide whether to seize or to repair/restore the PDC emulator role, it is important for you to understand the associated issues.

Impact on Environment

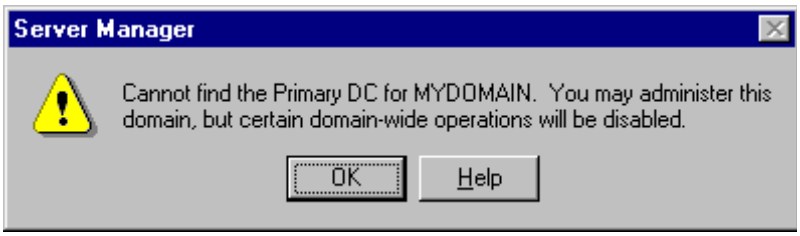
Mixed Mode Environment

When the PDC emulator role suffers a disaster in a mixed mode environment where NT 4.0 BDCs are active, you will witness the same issues you did in NT 4.0 when the native PDC was unavailable.

For example, below we were attempting to administer the NT 4.0 domain using the native NT 4.0 user manager for domains tool.



Here, we were attempting to administer the NT 4.0 domain using the native NT 4.0 server manager tool.



Native Mode Environment

The issues that occur in a native mode environment are also present (on the Windows 2000 side) in a mixed mode environment. When the PDC emulator suffers a failure in a Windows 2000 environment, you face these issues:

- **Possible Increase in Incidents of Logon Failure**

  If a user's password is reset (for example, when he/she forgets the password and an administrator resets that password on a DC that is **not** the authentication DC), that user must wait until the password is replicated to their authentication DC before he/she is able to log on.

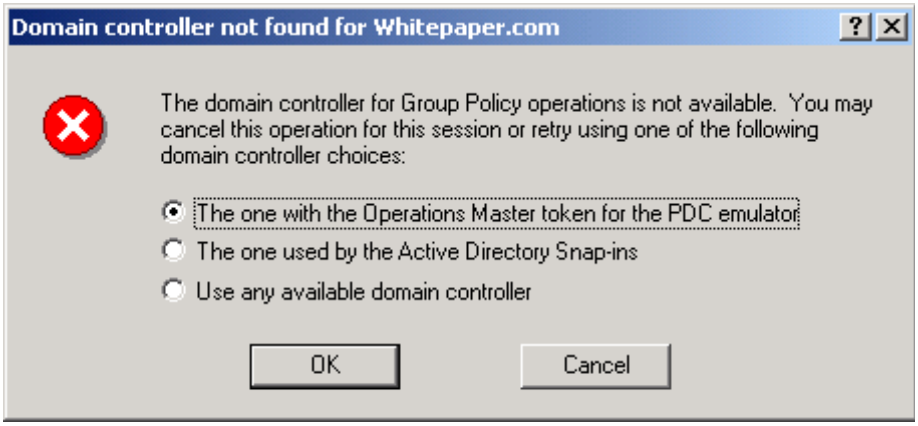
  Although the user's local authentication DC will try to contact the PDC emulator to see if the password has changed since last replication, it will fail because the PDC emulator is offline. Therefore, the authenticating DC has no choice but to resort to its local copy of Active Directory, which still reflects the original (forgotten) password.

  In this situation, you will see no obvious errors from the client side or from the authenticating DC. The only errors you will see (in addition to a failed login message on the client) are replication errors to the PDC emulator DC. These will occur as other DCs try to replicate the normal naming contexts required for Active Directory functionality.

You can easily overcome the problem by resetting the password on the user's authenticating DC.

- **Error When Attempting to Edit Group Policy Objects**

  To help ensure that no data loss occurs during the editing of a Group Policy object, the default DC for changes to a Group Policy object is the one holding the PDC emulator role. Therefore, if the PDC emulator is unavailable, you will receive the following message when you attempt to edit a Group Policy object within the domain.



This is a very minor issue that you can correct by selecting one of the options provided. A brief description of the options is listed below.

- *The one with the Operations Master token for the PDC emulator*.

  This option is, obviously, not possible when the role is unavailable.

- *The one used by Active Directory Snap-ins*.

  This option uses the domain controller that Active Directory management snap-ins are using. This option is recommended when the PDC emulator is unavailable.

- *Use any available domain controller*.

  The third, and least desirable option, allows the Group Policy snap-in to choose any available domain controller. When this option is selected, a domain controller in the local site is usually selected.

Note: The change you make here applies only to this individual edit. In other words, you will be asked this question every time you try to edit a Group Policy object when the PDC emulator is unavailable.

Considerations for Seizing a PDC Emulator

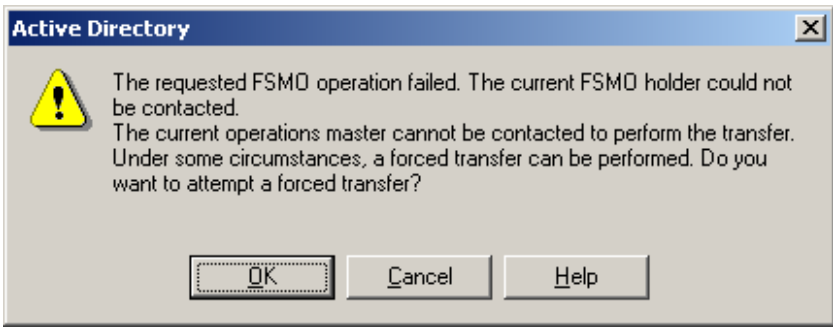
Because the role of the PDC emulator is not quite as critical as those previously mentioned, the act of seizing the role does not have the ramifications of the others. If you choose to seize the PDC emulator role, you do not need to completely rebuild the original role holder before it can participate in the Windows 2000 environment again.

As a result, the decision to seize the PDC emulator role has fewer implications to your environment and is generally considered a standard practice in the event of a PDC emulator failure, particularly in a mixed mode environment.

The only real issue to consider is whether you are functioning in a mixed mode environment with NT 4.0 BDCs. For the BDCs to be aware of the changes, a full synchronization of the BUILTIN database with the new PDC emulator will occur.

Steps Required to Seize the PDC Emulator

Because the issues associated with the seizure of the PDC emulator role have a minor impact on the environment, Microsoft allows you to seize this role through the Active Directory Users and Computers snap-in. To do this, you follow the steps you would use for a role transfer. When the DC recognizes that the PDC emulator is unavailable, you will see the following:



Simply click **OK** and the role will be seized.

Note: A forced transfer is equivalent to a seizure.

You can also seize the role using NTDSUTIL. To do this, you follow the steps in the "Steps Required to Seize the Schema Master" section of this white paper, except you replace step 7 with:

At the fsmo maintenance prompt, type **seize pdc**.

Recovering the Infrastructure Master

Before you decide whether to seize or to repair/restore the infrastructure master role, it is important for you to understand the associated issues.

Impact on Environment

The effects resulting from an infrastructure master failure in your environment are limited. They will not be visible to end users, and they will affect administrators only if there has been considerable group manipulation. These group manipulations are typically in the form of user additions and/or user renames. In this situation, the only result of an infrastructure master being down is a delay in these changes being referenced through the Active Directory management snap-ins.

There are very few occasions when your environment cannot be without an infrastructure master during the period of time it takes to repair/recover the original. However, if you foresee a very long outage, a seizure of the role is recommended.

Considerations for Seizing the Infrastructure Master

The primary consideration is to ensure that the new DC is not a GC server, but that it has good connection to a GC — ideally it is a direct replication partner within the same site.

Steps Required to Seize the Infrastructure Master

As with the PDC emulator, the infrastructure master can be seized by transferring the GUI or by using NTDSUTIL. To do this, follow the steps in the "Steps Required to Seize the PDC Emulator" section of this document.

APPENDIX A – Supported Recovery Console Commands

Please be sure that you understand the full impact of these commands before you use them. Some of the commands can be harmful in certain circumstances.

Command	Explanation
attrib	Changes attributes on one file or directory. ATTRIB -R | +R | -S | +S | -H | +H | -C | +C filename + Sets an attribute. - Clears an attribute. R Read-only file attribute. S System file attribute. H Hidden file attribute. C Compressed file attribute. More than one attribute can be set or cleared at a time. To view attributes, use the dir command.
batch	Executes commands specified in a text file. BATCH Inputfile [Outputfile] Inputfile Specifies the text file that contains the list of commands to be executed. Outputfile If specified, contains the output of the specified commands. If not specified, the output is displayed on the screen. Batch cannot be one of the commands included in the Inputfile.

cd/chdir	Displays the name of the current directory, or switches to a new directory. CHDIR [path] CHDIR [..] CHDIR [drive:] CD [path] CD [..] CD [drive:] CD .. Specifies that you want to change to the parent directory. Type cd [drive:] to display the current directory in the specified drive. Type cd without parameters to display the current drive and directory. The chdir command treats spaces as delimiters. Use quotation marks around a directory name containing spaces. For example: cd "\winnt\profiles\username\programs\start menu" Chdir operates only within the system directories of the current Windows installation, removable media, the root directory of any hard disk partition, or the local installation sources.
chkdsk	Checks a disk and displays a status report. chkdsk [drive:] [/p] | [/r] [drive:] Specifies the drive to check. /p Check even if the drive is not flagged /r Locates bad sectors and recovers readable information (implies /p). Chkdsk may be used without any parameters, in which case the current drive is checked with no switches. You can specify the listed switches. Chkdsk requires the autochk.exe file. Chkdsk automatically locates Autochk.exe in the startup (boot) directory. If it cannot be found in the startup directory, chkdsk attempts to locate the Windows 2000 Setup CD. If the installation CD cannot be found, chkdsk prompts for the location of autochk.exe.
cls	Clears the screen.

copy	Copies a single file to another location. copy source [destination] source Specifies the file to be copied. destination Specifies the directory and/or file name for the new file. The source may be removable media, any directory within the system directories of the current Windows installation, the root of any drive, the local installation sources, or the cmdcons directory. The destination may be any directory within the system directories of the current Windows installation, the root of any drive, the local installation sources, or the cdirectory. The destination cannot be removable media. If you do not specify a destination, the command defaults to the current directory. Copy does not support replaceable parameters (wild cards). Copy prompts if the destination file already exists. A compressed file from the Windows 2000 Setup CD is automatically decompressed as it is copied.
del/delete	Deletes one file. del [drive:][path]filename delete [drive:][path]filename [drive:] [path]filename Specifies the file to delete. Delete operates only within the system directories of the current Windows installation, removable media, the root directory of any hard disk partition, or the local installation sources. Del and delete do not support replaceable parameters (wild cards).

dir	Displays a list of files and subdirectories in a directory. dir [drive:][path][filename] [drive:] [path][filename] Specifies drive, directory, and/or files to list. Dir lists all files, including hidden and system files. Files may have the following attributes: a Files ready for archiving h Hidden c Compressed p Reparse point d Directory r Read-only e Encrypted s System file
disable	Disables a Windows system service or driver. disable servicename servicename The name of the service or driver to be disabled. Disable prints the old start_type of the service before resetting it to service_disabled. You should make a note of the old start_type, in case you need to enable the service again. The start_type values that the disable command displays are: service_disabled service_boot_start service_system_start service_auto_start service_demand_start

	Manages the partitions on your hard disk volumes.
diskpart	diskpart[/add | /delete] [device-name | drive-name | partition-name] [size] /add Create a new partition. /delete Delete an existing partition. device-name Device name for creating a new partition (such as \Device\HardDisk0). drive-name Drive-letter based name for deleting an existing partition (such as D:). partition-name Partition-based name for deleting an existing partition and can be used in place of the drive-name argument (such as \Device\HardDisk0\Partition1). size Size of the new partition, in megabytes. If no arguments are used, a user interface for managing your partitions appears.
	Enables a Windows system service or driver.
enable	enable servicename [start_type] servicename Name of the service or driver to be enabled. start_type How the service or driver is scheduled to be started. Valid start-type values are: SERVICE_BOOT_START SERVICE_SYSTEM_START SERVICE_AUTO_START SERVICE_DEMAND_START Enable prints the old start_type of the service before resetting it to the new value. Note the old value, in case you need to restore the start_type of the service. If you do not specify a new start_type, enable prints the old start_type.

exit	Quits the recovery console and restarts your computer.
expand	Expands a compressed file. EXPAND source [/F:filespec] [destination] [/Y] EXPAND source [/F:filespec] /D source Specifies the file to be expanded. May not include wildcard (* and ?) characters. Destination Specifies the directory for the new file. Default is the current directory. /y Do not prompt before overwriting an existing file. /f:filespec If the source contains more than one file, this parameter is required to identify the specific file(s) to be expanded. May include wildcards. /d Do not expand; only display a directory of the files which are contained in the source. The destination might be any directory within the system directories of the current Windows installation, the root of any drive, the local installation sources, or the Cmdcons directory. The destination cannot be removable media. The destination file cannot be read-only. Use the attrib command to remove the read-only attribute. Expand prompts if the destination file already exists unless /Y is used.
fixboot	Writes a new boot sector onto the system partition. fixboot [drive:] drive: Specifies the drive to which a boot sector will be written, overriding the default choice of the system boot partition.

fixmbr	Repairs the master boot code of the boot partition. fixmbr [device-name] device-name Optional name that specifies the device that needs a new MBR. If you do not specify a device, then the boot device is used. If fixmbr detects an invalid or nonstandard partition table signature, it prompts you before rewriting the MBR.
format	Formats a disk for use with Windows 2000. format [drive:] [/q] [/fs:file-system] [drive:] Specifies the drive to format. /q Performs a quick format. /fs:file-system Specifies the file system to use (FAT, FAT32, or NTFS).
help	Displays information about commands supported by the recovery Console. help [command] command Any Recovery Console command. If you do not specify a command, all of the commands supported by the recovery console are listed. The command parameter is used to see the help for a specific command.
listsvc	Lists all available services and drivers on the computer.
logon	Lists the detected installations of Windows 2000, and requests the local administrator password for those installations.
map	Lists the drive letter associated with the current physical device mappings. map [arc] arc Tells map to use arc paths instead of Windows 2000 device paths.

md/mkdir	Creates a directory. md [drive:]path mkdir [drive:]path Mkdir operates only within the system directories of the current Windows installation, removable media, the root directory of any hard disk partition, or the local installation sources.
more/type	Displays a text file to the screen. more [filename] type [filename] More or type displays a text file.
rd/rmdir	Removes (deletes) a directory. rd [drive:]path rmdir [drive:]path Rmdir operates only within the system directories of the current Windows installation, removable media, the root directory of any hard disk partition, or the local installation sources.
ren/rename	Renames a single file. ren [drive:][path]filename1 filename2 rename [drive:][path]filename1 filename2 You cannot specify a new drive or path for your destination file. Rename operates only within the system directories of the current Windows installation, removable media, the root directory of any hard disk partition, or the local installation sources.

Set	Displays and sets recovery console environment variables. set variable = parameter set AllowWildCards = TRUE The following environment variables are supported: AllowWildCards Enables wildcard support for some commands, such as DEL, which do not otherwise support them. AllowAllPaths Allows access to all files and folders on the computer. AllowRemovableMedia Allows files to be copied to removable media, such as floppy disks. NoCopyPrompt Does not prompt when overwriting files. To display the list of current environment variable settings, type set without parameters. Note: The set command is an optional recovery console command that can be enabled using either the Group Policy snap-in or the Security Configuration and Analysis snap-in.
systemroot	Sets the current directory to %SystemRoot%.

APPENDIX B –Tools for Active Directory Disaster Recovery

The following tools are useful in a disaster situation.

Note: All of these tools are included in the support tools on the Windows 2000 CD.

DsaStat

This diagnostic tool compares and detects differences between naming contexts on DCs.

DsaStat can be used to compare two directory trees across replicas within the same domain or, in the case of a Global Catalog, across different domains. The tool retrieves capacity statistics such as megabytes per server, objects per server, and megabytes per object class, and performs comparisons of attributes of replicated objects.

The user specifies the targeted domain controllers and additional operational parameters from the command line or from an initialization file. DsaStat determines if Domain Controllers within a domain have consistent and accurate images of their own domain. In the case of Global Catalogs, DsaStat checks to see if the GC has a consistent image with DCs in other domains.

Active Directory Replication Monitor (ReplMon.exe)

This utility graphically displays the replication topology of connections between servers on the same site. ReplMon enables administrators to view low-level status and performance of replication between Active Directory domain controllers and, optionally, the status of Group Policy objects.

Windows 2000 Domain Manager (NetDom.exe)

This tool enables administrators to manage Windows 2000 domains and trust relationships from the command line.

Replication Diagnostics Tool (RepAdmin.exe)

This tool allows the administrator to view the replication topology as seen from the perspective of each domain controller. In addition, RepAdmin.exe can be used to manually create the replication topology (although, in normal practice, this should not be necessary), to force replication events between domain controllers, and to view both the replication metadata and up-to-datedness vectors.

ADSI Edit

ADSI Edit is a Microsoft Management Console (MMC) snap-in that acts as a low-level editor for Active Directory. Using the Active Directory Service Interface (ADSI), it provides a means to add, delete, and move objects within the directory services. The attributes of each object can be viewed, changed, and deleted.