COMPAQ
White Paper

Active Directory Disaster Recovery

August 2000
PS-99-23

Prepared by Stephen Craike & Karl Robinson

Compaq Professional Services

Compaq Computer Corporation

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 Catalog Servers, Operations Masters (OM) servers, and simple domain controllers. The steps and considerations to recover the Active Directory database after a failure are described in this white paper, together with any of the particular requirements necessary to restore a server to a special role.

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

Contents

Notice

The information in this publication is subject to change without notice and is provided “AS IS” WITHOUT WARRANTY OF ANY KIND. THE ENTIRE RISK ARISING OUT OF THE USE OF THIS INFORMATION REMAINS WITH RECIPIENT. IN NO EVENT SHALL COMPAQ BE LIABLE FOR ANY DIRECT, CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE OR OTHER DAMAGES WHATSOEVER (INCLUDING WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION OR LOSS OF BUSINESS INFORMATION), EVEN IF COMPAQ HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The limited warranties for Compaq products are exclusively set forth in the documentation accompanying such products. Nothing herein should be construed as constituting a further or additional warranty.

This publication does not constitute an endorsement of the product or products that were tested. The configuration or configurations tested or described may or may not be the only available solution. This test is not a determination of product quality or correctness, nor does it ensure compliance with any federal, state or local requirements.

Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

Compaq, Contura, Deskpro, Fastart, Compaq Insight Manager, LTE, PageMarq, Systempro, Systempro/LT, ProLiant, TwinTray, ROMPaq, LicensePaq, QVision, SLT, ProLinea, SmartStart, NetFlex, DirectPlus, QuickFind, RemotePaq, BackPaq, TechPaq, SpeedPaq, QuickBack, PaqFax, Presario, SilentCool, CompaqCare (design), Aero, SmartStation, MiniStation, and PaqRap registered in United States Patent and Trademark Office.

Netelligent, Armada, Cruiser, Concerto, QuickChoice, ProSignia, Systempro/XL, Net1, LTE Elite, Vocalyst, PageMate, SoftPaq, FirstPaq, SolutionPaq, EasyPoint, EZ Help, MaxLight, MultiLock, QuickBlank, QuickLock, UltraView, Innovate logo, Wonder Tools logo in black/white and color, and Compaq PC Card Solution logo are trademarks and/or service marks of Compaq Computer Corporation.

Microsoft, Windows, Windows NT, Windows NT Server and Workstation, and Microsoft SQL Server for Windows NT are trademarks and/or registered trademarks of Microsoft Corporation.

NetWare and Novell are registered trademarks and intraNetWare, NDS, and Novell Directory Services are trademarks of Novell, Inc.

Pentium is a registered trademark of Intel Corporation.

NonStop registered in U.S. Patent and Trademark Office.

Document Title
White Paper prepared by Compaq Professional Services Technology Group

Second Edition (September 1999)
Document Number PS-99-23

Introduction

The Active Directory and the systems required to be running for its successful operation are 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 on the concepts of disaster recovery with respect to the Windows 2000 Active Directory.
- Provide step-by-step procedures on how to recover from the most common Active Directory disaster situations and the considerations surrounding them.

Although we encourage you to utilize this information in the formulation of your own disaster recovery plans. It is important that it be augmented with the specifics of your own internal environment and your existing disaster recovery policies.

In addition, this paper will only give a brief overview of Active Directory, and assumes that the reader is familiar with the Active Directory model and the technologies supporting it.

For further information on the base concepts discussed in this paper, you are encouraged to read the following white papers.

Active Directory – A technical overview and Understanding Active Directory Replication both of which can be obtained from:

http://www.compaq.com/activeanswers

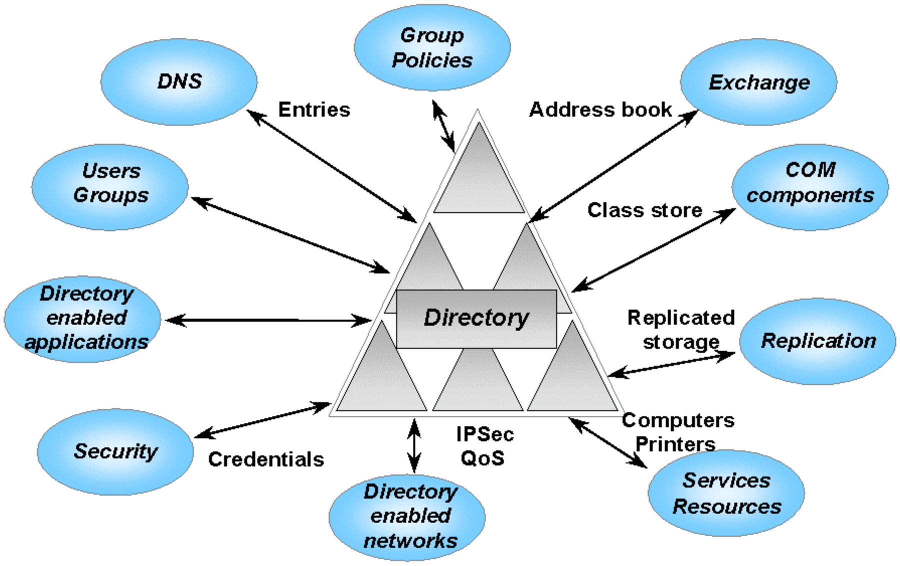
Overview Of Active Directory

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 other components within the OS.

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

Many different objects can be stored in the Active Directory, including:

- All the objects necessary for running a Windows 2000 based infrastructure such as:
- 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 that required, in previous versions of Windows NT, storing in the registry information about their location are now stored in the Class Store in the Active Directory
- Rules and policies to control the working environment



System Components of Active Directory

Although there are many components that make up Active Directory this section focus's on the system components that are relevant to us when considering the creation of a disaster recovery plan, namely:

- Domain Controllers (DC's)
- Global Catalog Servers (GC's)
- Operations Masters (OM's)

Domain Controllers (DC)

As with Windows NT 4.0, Windows 2000 requires Domain controllers (DC's) 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 just a single PDC, as with NT 4.0.

In order to keep the information on all DC's synchronized, DC's are responsible for initiating and performing replication operations to ensure that all DC's in the environment host a current and accurate version of the directory. 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 Catalog (GC) Servers

The Global Catalog's primary function is to provide fast and efficient searches that extend across the entire Active Directory forest. A GC holds a read/write full replica of all objects within the domain for which it is a member and a read-only partial 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.

In addition, the Global Catalog is also required for the enumeration of Universal Group memberships and UPN's in a native Windows 2000 domain. As a result, if a DC cannot contact a GC at the point of client logon, cached local logon credentials is all the client will receive, and access to remote resources will be denied.

Operations Masters (OM) Servers

As Active Directory supports multi-master updates (each DC hosts a writable version of their directory partition) it must allow for the possibility of conflicting changes, i.e. changes that are made simultaneously to the same object within the directory but from a different DC. This process is achieved through a well-defined conflict resolution method and eventually all DC's converge to the same value.

Even with this well-defined process however, it is sometimes better to prevent conflicts than to resolve them after the event. Operations Masters in Active Directory are used to prevent conflicting updates in cases where conflict resolution is unsuitable.

Active Directory defines five Operation Master roles:

- Schema Master
- Domain Naming Master
- Relative Identifier (RID) Master
- Primary Domain Controller emulator (PDCE)
- Infrastructure Master

Note: The Schema Master and Domain Naming Master are per-forest roles, meaning that there is only one Schema Master and one Domain Naming Master in the entire forest. The other operations master roles are per-domain roles, meaning that each domain in a forest has its own RID Master, Primary Domain Controller Emulator, and 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 can do the following:

- Add new domains to the forest.
- Remove existing domains from the forest.
- Add or remove cross-reference objects to external directories

Relative Identifier (RID) Master

This operations master manages the allocation of RID Pools to other DC's. Only one server performs this task. When a security principal (e.g., user. Group, computer) is created; it requires a RID to be combined with a domain wide identifier, to create a unique Security Identifier (SID).

Every Windows 2000 DC receives a pool of RID's (By default this is 512) it can use to create objects. The RID Master ensures that these ID's remain unique on every DC by assigning different pools. All object moves between domains of the same forest are done via the RID Master to avoid SID duplication.

Primary Domain Controller Emulator (PDCE)

The PDC Emulator provides the following major functions:

- Provides backward compatibility to down level clients and servers allowing NT4.0 BDC's to participate in the new Windows 2000 environment.
- Native Windows 2000 environments replicate password changes to the PDCE first. Each time a DC fails to authenticate a password it contacts the PDCE to see whether the password can be authenticated there, perhaps as a result of a change that has not yet been replicated down to the authenticating DC.
- Responsible for time synchronization. The PDC's of the domains within the forest will synchronise with the PDC in the root domain of the forest.

Infrastructure Master

The infrastructure master ensures consistency of objects for all inter-domain operations. When an object from another domain is referenced, this 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 SID's and DN's in cross-domain object references in that domain.

Overview Of Active Directory Replication

As Windows 2000 DC's hold a replica of all of the objects belonging to their domain and have full read/write access to these objects, administration of the domain can be done via any DC participating within that domain. These operations affect the state or the value of an object and must therefore be replicated to the other DC's.

Replication is the process of propagating object updates between DC's to maintain their copies of the Active Directory database in an accurate state.

The replication of changed objects does not occur immediately, instead, replication is triggered after a period of time, gathering all changes and providing them to other DC's in collections. As a result, in normal operation the Active Directory on any DC can be regarded as always being in a state of loose consistency. That is, the information on all DC's within a Windows 2000 environment is likely to be different as replication changes may be on the way from other DC's or waiting to be triggered. Eventually the changes arrive and DC's synchronize with each other.

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

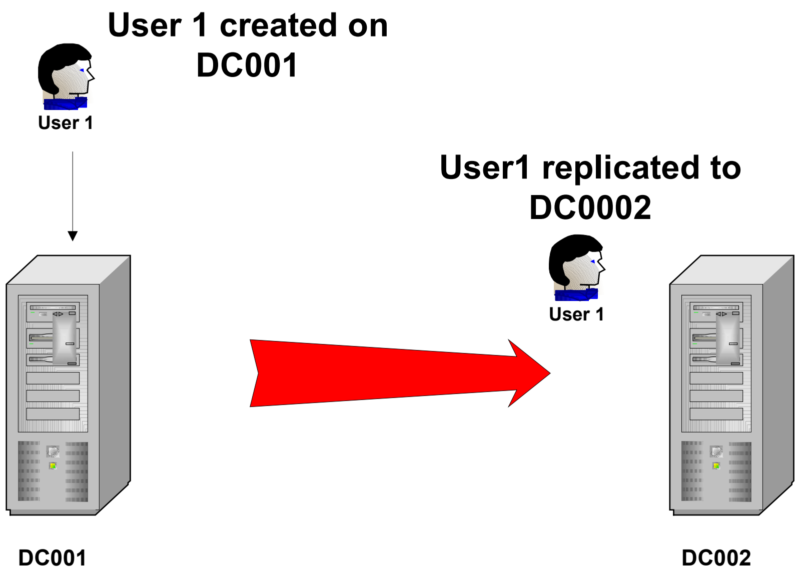


Figure 1: Replication of Information from one DC to another

Backup & the Active Directory

An important component of an Active Directory Disaster Recovery plan is understanding the implications and considerations around the backup of Active Directory.

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 a member of either the:

- Backup Operators Group
- Administrators Group

Types of Backup

Although the backup tool in Windows 2000 supports multiple types of backup e.g.

- Normal
- Copy
- Incremental
- Differential
- Daily

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 3rd party tools) will automatically backup 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 other services 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 the files that are required for Windows 2000 to boot, these 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 are 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 the following:

- 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, this 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?

In order 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 will ensure that all 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 DC's in this manner you will have Active Directory components spread out on multiple spindles, e.g. 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 will still only have to backup the system drive and system state in order to ensure a "Good Backup" even under this distributed installation.

Age

If the backup is older than the tombstone age set in Active Directory, then it 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 DC's 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 but not fully removed from the directory. The tombstone will eventually be removed 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 DC's and the object is replicated in the form of a tombstone. After 60 days all the DC's will remove the tombstone as part of the garbage collection process. This is a process routinely performed by DC's to cleanup their copy of the database.

If you attempt to restore the deleted object after 60 days the object cannot be replicated to the other DC's in the domain because it has a USN older than the current level required to trigger replication. Therefore the other DC's cannot inform the restored DC that the object was deleted resulting in an inconsistent directory.

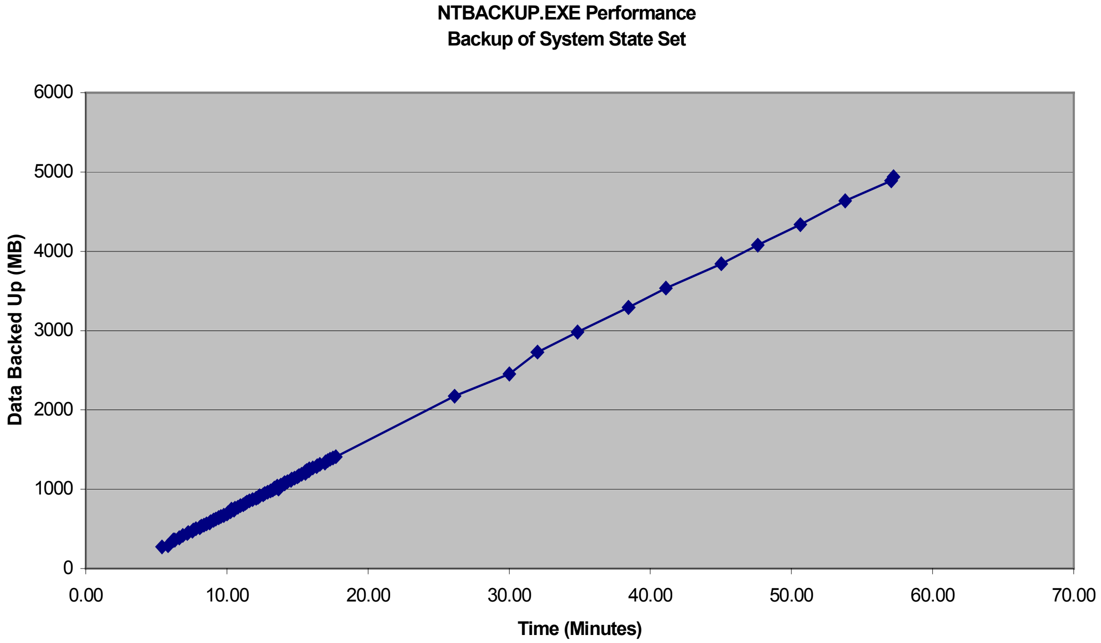
As a result, the useful life of a backup is equivalent to the "tombstone lifetime" setting for the enterprise.

Given this, the backup interval should be at least once within the tombstone lifetime. However, it is expected that administrators will backup the system state and system drive more regularly to ensure a backup that more accurately represents the current environment.

Backup Performance

Understanding the time taken to backup an active DC is an important component in determining the best backup strategy for your business. To assist with this the graph below shows some indicative times taken to backup various size Active Directory databases.

Note: The data backed up in the tests represented 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.



System Specs: Dual Pentium Pro - 200 Mhz, 128MB RAM, Adaptec AHA 2940UW SCSI controller, Seagate/Archive Python 4mm DDS-2 SCSI Tape Drive

Figure 2: Graph indicating Backup times for different size 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.

The concept of repair in this paper will deal with two aspects: -

- 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

The version of the database that Windows 2000 uses is called extensible storage engine (ESE).

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

The functionality available under NTDSUTIL for the repair of the database is extremely pervasive. As a result repairing the database using this method should *only* be used after consulting the appropriate service personnel and *only* as a last resort.

Due to the seriousness of this method of repair this paper will not discuss the steps required to carry it out, and again urges that the appropriate Microsoft and or qualified vendor support be sort before it be attempted.

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 with minimal services in safe mode and then change your computer settings or remove the newly installed software 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 the hard disk of a Windows 2000 computer, 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 will allow 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 once the initial installation sequence is complete.

To install this option, follow the steps outlined in the "To install the Recovery Console as a startup option" in the server Help file.

Emergency Repair Disk

As with NT4.0, 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, 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 be kept up to date as configuration changes on the DC are made. 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 a repair of your DC fails you have only one option left, to restore the system using one of the methods outlined in the following section.

Types Of Restore

There are two methods available to you when restoring a DC to an operational state: -

- Restore from Replication
- Restore from Backup

Restore From Replication

This method relies on Active Directory replication to restore a DC to a working state, and is only valid if another DC exists in the domain. Once Windows 2000 is installed, the system is once again promoted to a DC in the domain it existed in before the failure. During this process the replication that occurs during the normal DCPROMO operation will ensure 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 good 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 will return the DC to its state at the time of backup, the DC will then query it's replication partner(s) for any updates since that time. If there are changes they will be replicated, ensuring the DC has an accurate and up to date copy of the Active Directory database.

In addition, by restoring Active Directory from backup you have three further options available to you:

- NonAuthoritative Restore
- Authoritative Restore
- Primary Restore (SYSVOL Only)

These three methods allow you the ability 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 their differences are understood.

Nonauthoritative Restore

ACTIVE DIRECTORY

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

After a nonuthoritative restore the DC is updated using normal replication techniques. That is, if the version number of an object is less than the version number of the same object stored in it's replication partners database (indicating the object has changed since it was last backed up) the object on the restored server will be updated with the changes that were made to that object since the time of the last backup. Thus ensuring an up-to-date version of the database.

SYSVOL

By restoring the SYSVOL nonauthoritatively the local copy that is held on the restored DC will be compared with that of its replication partners (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 DC's 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 and will occur 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, in that it requires all the steps of a nonauthoritative restore before it can be initiated. The primary difference between the two is that an authoritative restore has the ability to increment the version number of an entire directory, a subtree, or individual objects (provided that they are leaf objects) to make it Authoritative in the directory.

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

Because of this, the authoritative restoration method will typically be used when human error is involved e.g. when an administrator has accidentally deleted an OU

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

Note: An Authoritative restore will NOT overwrite new objects that have been created after the backup was taken and can only be carried out 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 specifying that the copy of SYSVOL that was restored from backup is authoritative for the domain. Once the necessary configurations have been made the local SYSVOL will be marked as authoritative and be replicated out to the other DC's within the domain.

Similarly to the Active Directory Authoritative restore this method will typically be used when human error is involved and the error has propagated out to other domain controllers e.g. when an administrator has accidentally deleted an object that resides in SYSVOL for example a Group Policy object.

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.

The exact process for all these methods of restoration will be discussed further in the paper.

Required Rights for Active Directory Restore

To restore the System State data, the person performing the procedure must be a Local Administrator.

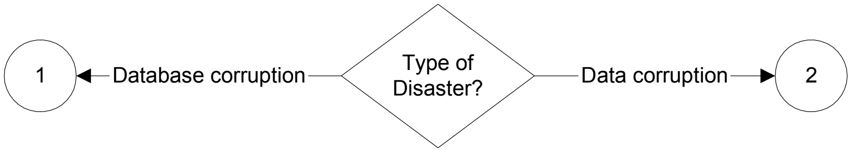
Active Directory Disaster Recovery Flowchart

To complement the information presented hitherto, the remainder of the paper will guide you through the steps and considerations required to implement the concepts discussed thus far. To assist with this, the following collection of flowcharts have been included.

Note: It is important to understand that the flowcharts included below do not depict every disaster situation. Moreover they are included as a guide to help you understand the options available to you and their appropriate use.

Type of Disaster

The first thing you must decide before progressing any further is the type of disaster that you are faced with. For the purposes of this paper the types of possible disasters are: -



Database Corruption

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

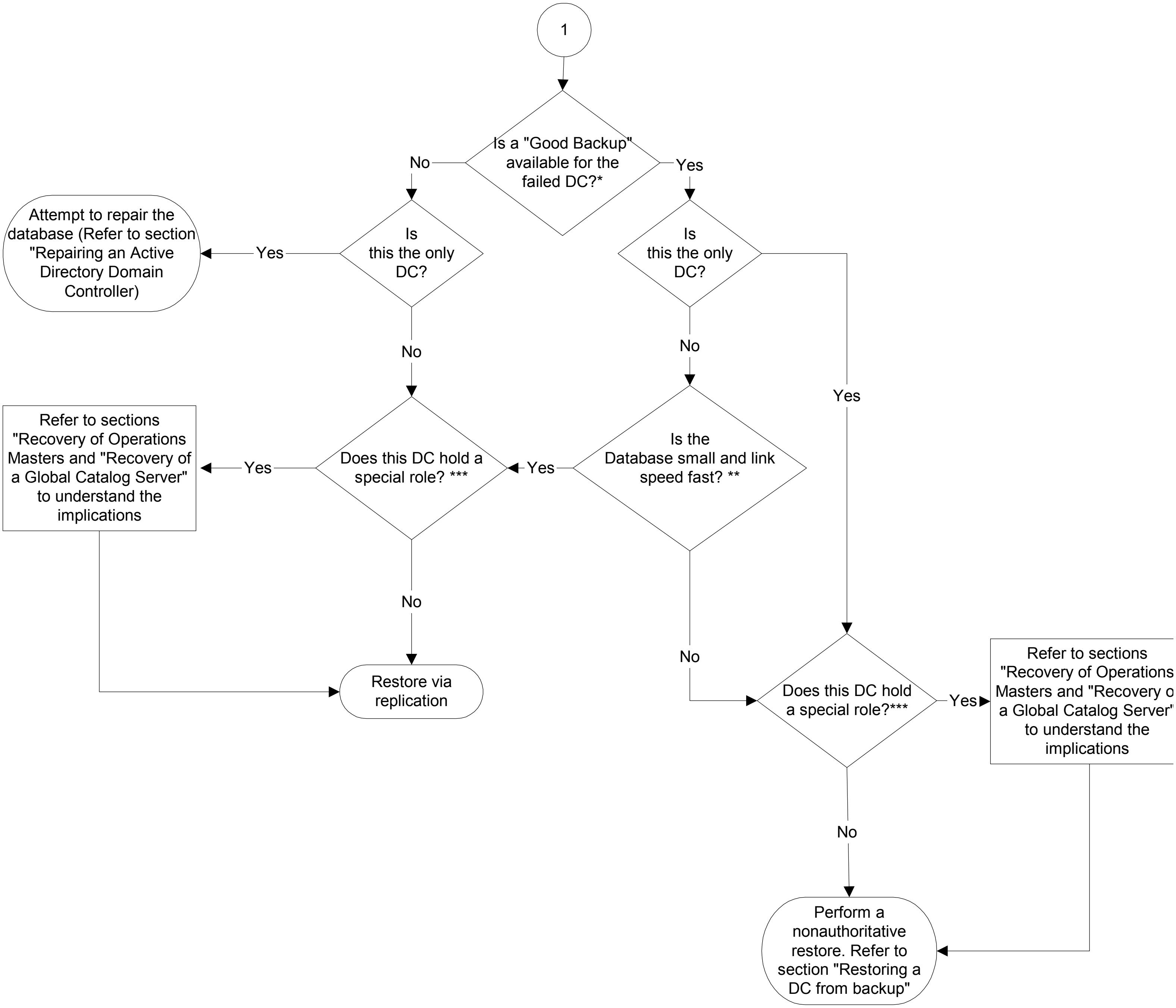
- The disk(s) has become corrupted. E.g. when the writeback cache was not saved due to a power failure and bad batteries.
- The Domain controller has suffered a severe hardware failure and needs to be replaced

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 DC's. This corrupt data needs to be replaced by a trusted backup.
- An administrator or someone with the appropriate permissions has accidentally deleted an object(s) and the deletion has replicated to other DC's within the environment.

Database Corruption

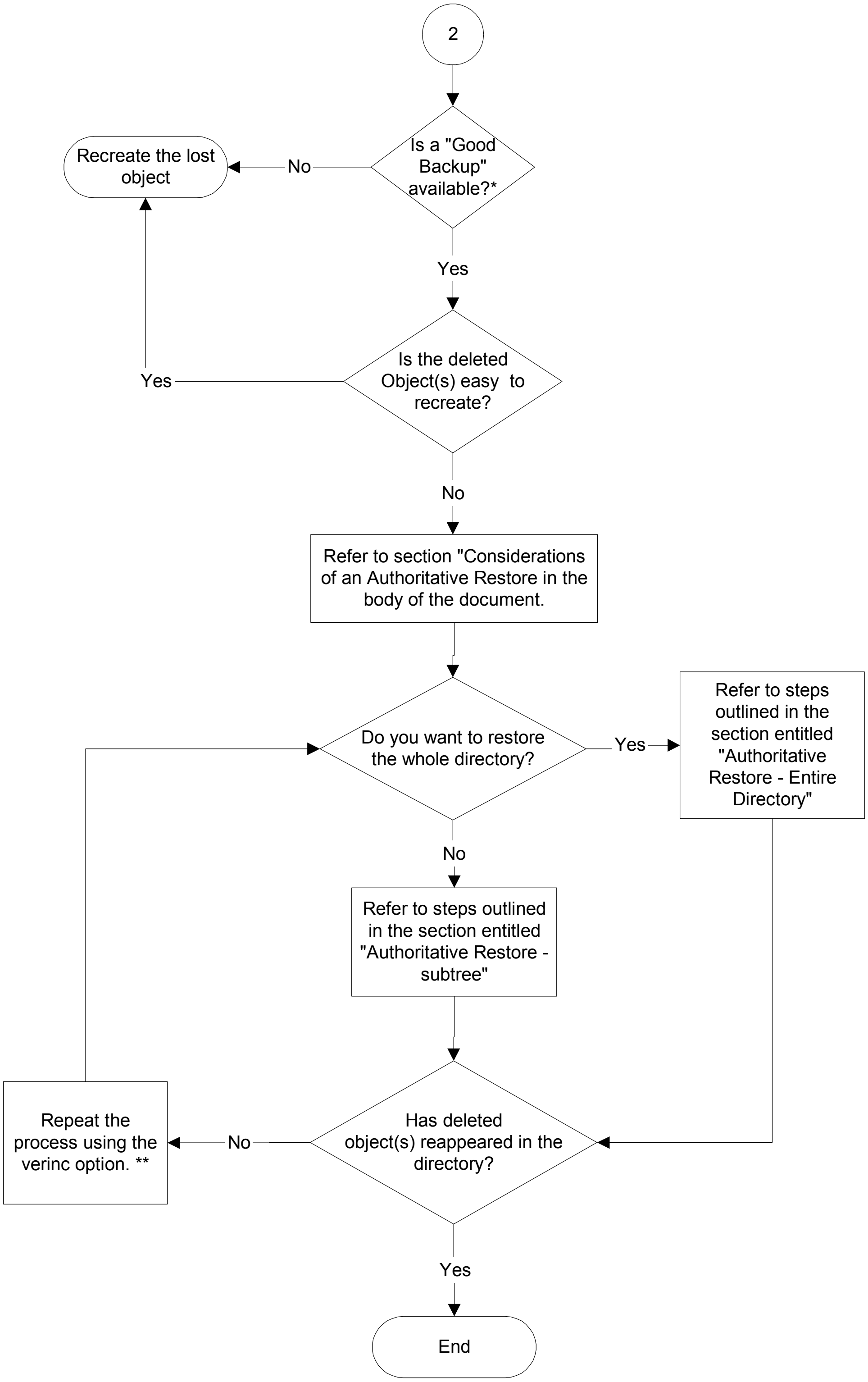

1
Is a "Good Backup" available for the failed DC?*
No
Yes
Is this the only DC?
Yes
Attempt to repair the database (Refer to section "Repairing an Active Directory Domain Controller)
No
Is this the only DC?
No
Yes
Refer to sections "Recovery of Operations Masters and "Recovery of a Global Catalog Server" to understand the implications
Yes
Does this DC hold a special role? ***
Yes
Is the Database small and link speed fast? **
No
No
Restore via replication
Does this DC hold a special role?***
Yes
Refer to sections "Recovery of Operations Masters and "Recovery o a Global Catalog Server" to understand the implications
No
Perform a nonauthoritative restore. Refer to section "Restoring a DC from backup"

* 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


2
Is a "Good Backup" available?*
No
Recreate the lost object
Yes
Is the deleted Object(s) easy to recreate?
Yes
No
Refer to section "Considerations of an Authoritative Restore in the body of the document.
Do you want to restore the whole directory?
Yes
Refer to steps outlined in the section entitled "Authoritative Restore - Entire Directory"
No
Refer to steps outlined in the section entitled "Authoritative Restore - subtree"
Has deleted object(s) reappeared in the directory?
No
Repeat the process using the verinc option. **
Yes
End

* 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

Recovery Console

Accessing the Recovery Console

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

To do this follow the steps outlined below: -

1. Place The Windows 2000 Server/Advanced Server in the CDROM, if the CD is not bootable you can achieve the same result using the Windows 2000 Boot floppies.
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 is started, 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
```

Once you have selected the appropriate installation (in the example above do this by entering 1) you will be presented with what looks like a DOS prompt and a repair can begin using the supported commands within the utility. 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, and if using floppy disks, respond to the prompts that request each floppy disk in turn.
3. When the text-based part of Setup begins, follow the prompts; choose the repair or recover option by pressing **R**.

4. When prompted, insert the Windows 2000 Setup CD in the appropriate drive.
5. When prompted, choose the emergency repair process by pressing **R**.
6. 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).
7. Follow the instructions on the screen and, when prompted, insert the Emergency Repair Disk in the appropriate drive.
8. 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.
9. Follow the instructions on the screen; it is recommended that you write down the names of files that are detected as faulty or incorrect, to help you diagnose how the system was damaged.
10. If the repair was successful, allow the process to complete; it will restart the computer.
11. The restarting of the computer 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 will detail the steps required to perform these operations and also the considerations associated with them.

Restoring a DC From Replication

Before restoring a DC using replication it is important that you understand any issues associated with its use.

Considerations for Restoring a DC from Replication

Bandwidth Considerations

The primary consideration with recovering a DC via replication is bandwidth. Obviously the bandwidth required to restore a DC via replication is directly proportional to the size of the Active Directory database and the time in which the DC is required to be at a functioning state.

The chart below represents the time needed to replicate a new DC into an existing domain over various network speeds. The Active Directory database (ntds.dit) used in the testing was 2GB in size.

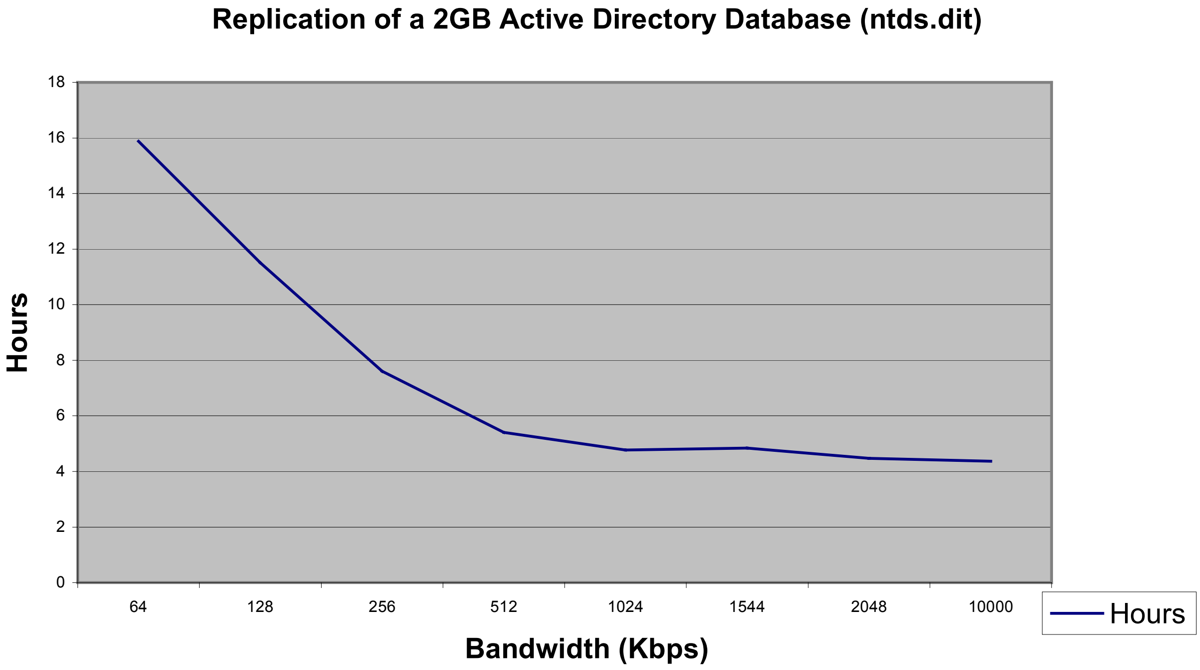


Figure 3: Graph showing the time to replicate varying sized directory databases based on available bandwidth.

Note: The Systems used to gather the data for the above chart were Proliant 1600s with Dual Pentium II 266Mhz, 256MB 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

At least one functioning DC in the target domain must exist to restore using replication. Recovering via replication is the same process as creating a new DC. Once the target server has been cleaned of any failed DC functionality, launch DCPROMO and create a DC for the target domain using appropriate parameters for the environment.

Ideally this DC should be located in the same Active Directory site as the replicating DC in an attempt to reduce the network impact and restore times associated with this method. For a more detailed look at the effect of bandwidth on this form of restoration please see figure 2 in this document.

The server that is the target for becoming the new DC must not currently be a DC for any domain, or have any components of the failed DC function installed. If the server being used to recover is the same server e.g. the same Windows 2000 installation with the same name. Then DCPROMO will clean up any old data in the Directory from the last instance of this server as a DC. If a new server is being used, either a new physical server or a new installation of Windows 2000, then the reference to the old DC must be cleaned from the Active Directory using the NTDSUTIL utility. Because this requires modifying the Configuration Naming Context, it requires Enterprise Administrator permissions.

To remove the previous instance of the DC from the Active Directory follow the steps outlined below: -

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 that will be used to clean the metadata from.
5. Type **quit** and press **Enter**. This will return you 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 a number associated with each.
8. Type **select domain <number>** and press **Enter** where <number> is the number corresponding 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> refers to the number of the site that the DC was a member.
11. Type **list servers in site** and press **Enter**. This will list all servers in that site with a corresponding number.
12. Type **select server <number>** and press **Enter** where <number> refers to the DC to be removed.

13. Type **quit** and press **Enter**. The Metadata cleanup menu is displayed.
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 error that the object could not be found, it might have already been removed from the Active Directory.

15. Type **quit** and press **Enter** successively to 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 restoring a DC from backup it is important that you understand any issues associated with its use.

Considerations for Restoring a DC From Backup

Time taken to restore a DC from Backup.

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

To illustrate this the graph below shows the time taken to restore a DC from backup with databases varying from 500Mb to 2Gb in size. The machine involved in the test was a Proliant 800, with a single 400MHz processor, 256Mb RAM and a 4/8 GB DAT Drive.

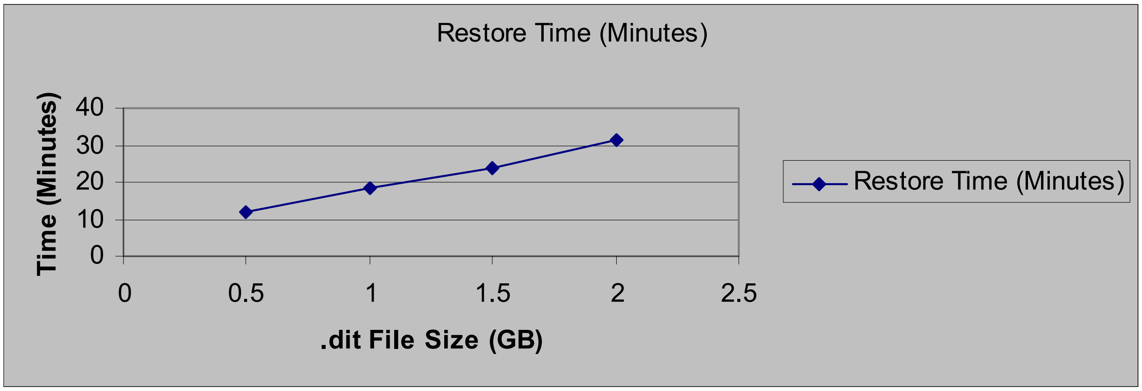


Figure 4: Graph representing times to restore varying sized DIT files from backup

Note: This graph only represents the time taken to restore System State; the restore of a "good Backup" as defined earlier, will therefore take longer depending on the size of your system drive.

Useful Life of Active Directory Backup

Ensure that the backup you are restoring from was taken within the tombstone lifecycle; by default this is set to 60 days. For more information on the useful life of an Active Directory backup please see the "What is a good backup?" section of this paper.

Restore Backup onto Different Hardware

It is possible to restore a DC onto different hardware however there are some issues you should be aware of before doing this.

- *Different HALS*

  By default the Hal.dll is not backed up as part of system state, however the Kernel32.dll is. Therefore if you are trying to restore a backup onto a machine that requires a different HAL e.g. to support a multiprocessor environment, you will run into compatibility issues with the new HAL and the original Kernel32.dll.

  The only workaround for this situation is to explicitly copy the Hal.dll from the original machine and replace it on the new machine. The limitation of this however is that the new machine will now 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 options 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

In addition to the issues of restoring a DC onto different hardware, it is also important that the partitions you have on the new machine match the ones you had on the original machine. Specifically that all the drive mappings are the same and the partition(s) size are at least the same as they were on the original machine.

Considerations of a Nonauthoritative Restore

In addition to the general considerations around restoring from backup you will also need to be aware of the specific issues related to both 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 the steps detailed below.

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

Note: The above step assumes that you are already running a DC, if this is not the case, ignore step 1 and 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 is 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* ensure you 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 containers are checked.
7. Ensure **Original Location** is selected in the "Restore Files to" drop down box.
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. Once complete click YES to restart the computer

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

Note: By executing a nonauthoritative restore on Active Directory, you automatically execute a nonauthoritative restore of SYSVOL; therefore no additional steps are required.

Considerations of an Authoritative Restore

ACTIVE DIRECTORY

Impact on Group Memberships

The most significant issue stemming from the use of this method 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 dealt with in Active Directory; the results of an authoritative restore on the representation of group membership may vary.

These variations are based upon which objects replicate first after an authoritative restore has completed.

- *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, 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 users primary group, which is always represented correctly both from the user and group reference.

Unfortunately there is no way to define which objects replicate first after an authoritative restore has been carried out. If your environment is affected by this situation the only option you have is to modify the group membership attribute of the effected 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 information held on 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 view the way their directory should look and take steps to replicate the accurate directory information out to the other DC's within the domain.

The best way to do this is to add a dummy user, 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 means any group that was either authoritatively restored itself or who had members restored, who did not have that group defined as their "Primary Group".

By doing this you will force the correct group membership information to be replicated out from the source DC (The DC that the original authoritative restore was carried out on) and update the group membership information on its replication partners. These updated objects will reflect the correct memberships and will also correct the information represented in the "Member of " Tab of the restored user objects.

Important: In order to ensure the success of the method defined above you MUST make sure that no additions are made to group membership (for the effected groups and users) on any of the other DC's within the environment.

If you do not adhere to this you risk the accurate version of the directory (held on the DC where the restore took place) being corrupted by the incorrect membership information. Once this occurs you must either update group membership manually or perform another authoritative restore of the object(s) using the /verinc switch and perform the process defined above again.

Impact on Trusts and Computer Accounts

Under Windows 2000 trust relationships and computer account passwords are negotiated at a specified interval (by default 7 days for trust relationships and 30 days for computer passwords)

When using the Authoritative Restore method, previously used passwords for the objects in the Active Directory that maintain trust relationships and computer accounts may be restored.

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 down level domains, must be removed and re-created.

In the case of a computer account password, this could impact communications between the member workstation or server and a DC of its domain. This will usually manifest itself in a user on an NT or Windows 2000 machine having issues with authentication due to an invalid machine account. If this occurs the machine account must be removed and recreated.

To help with both the recreation of trusts and the resetting of computer account passwords use the NETDOM utility included in the support tools on the Windows 2000 CD.

Note: An NT4.0 machine will change its password every 7 days.

SYSVOL

Bandwidth Considerations of SYSVOL Replication

When performing 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 DC's in the domain that the SYVOL information on the restored DC is authoritative. As a result the entire SYVOL contained on the restored DC will be replicated out to all other DC's in the domain (via replication partners)

The bandwidth associated with such replication will only ever be a consideration in a domain where there is an extensive use of large Group Policies and scripts. In addition, unlike Active Directory replication, FRS replication is not compressed between sites.

Note: Replication of SYSVOL between sites will be compressed in Whistler.

Steps Required for an Authoritative Restore

Authoritative restore of Active Directory provides the ability to restore the entire directory, a subtree, or an individual object. The examples outlined below will detail how to restore both the entire directory and 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 is a serious operation and one that should only be carried out as a last resort.

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

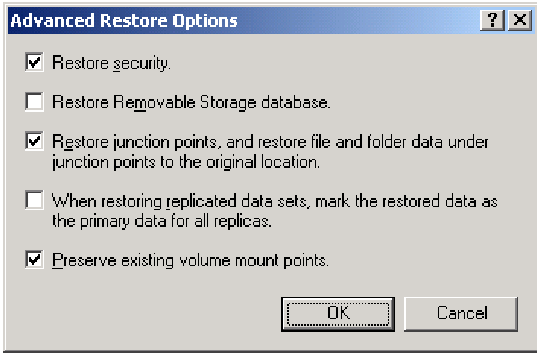
Note: Even if the system is not currently acting as a DC you are still required to reboot the system into Directory Services Restore mode to perform an authoritative restore.

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 is 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 ensure you 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 containers are checked.
7. Ensure **Original Location** is selected in the "Restore Files to" drop down box.
8. Click on 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.



Advanced Restore Options

☑ Restore security.

□ Restore Removable Storage database.

☑ Restore junction points, and restore file and folder data under junction points to the original location.

□ When restoring replicated data sets, mark the restored data as the primary data for all replicas.

☑ Preserve existing volume mount points.

12. Click **OK**
13. Click **OK** to confirm restore
14. Click **OK** to confirm restore source
15. Once 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 warning
20. Click **OK**
21. Ensure the Restore Source is the same as in step 14
22. When the restore process has finished close backup.
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 DC’s within the environment.

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

E.g. 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\…..

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 are ensuring that any new information e.g. policies or scripts that have been created after the last backup are not deleted. However, because the names of the files/folders will not change after any modifications, policies/scripts that existed at the time of the last backup will be replaced with the version that was included in that backup. This could result in a loss of data if the script/policy was changed since the last backup.

E.g. A Group Policy by the name of 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}

However shortly after the last backup was taken an administrator edited the Finance Policy, and although the properties of the policy changed the GUID of the GPO remained the same. As a result the policy was still referenced by the same directory name {31B2F340-016D-11D2-945F-00C04FB984F9}

When it came time to Authoritatively restore the directory the folder {31B2F340-016D-11D2-945F-00C04FB984F9} from the alternate sysvol location was copied to the original sysvol location replacing the old folder and thus losing the changes the administrator had made after the backup was taken. This step is necessary however to maintain the synchronization between Active Directory and SYSVOL.

Authoritative Restore – Subtree

This method of Authoritative Restore will restore specific component(s) of Active Directory and mark them as authoritative for the directory. It is expected that this will be the most common form of Authoritative Restore as there will be few occasions where the entire directory will need to be restored.

To perform the authoritative restore of a subtree follow the procedure outlined in the "authoritative restore of the entire directory" section of the paper, up to and including step 21, then follow the steps below: -

1. Type **RESTORE SUBTREE path** E.g. 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 Domain Controller for the path specified. Changes will be replicated out to the other DC's within the domain.

Because you are only restoring a portion of the Active Directory it is not necessary to do an authoritative restore of the Sysvol. However, if the subtree or object that was authoritatively restored contained elements from the SYSVOL e.g. a group policy, you should also restore that portion of the SYSVOL authoritatively.

If this is required you must complete the steps 27 and beyond outlined in the "authoritative restore of the entire directory" section of the paper.

Considerations for a Primary Restore

Before discussing the steps required to perform a Primary restore it is important to understand the considerations around doing so.

Active Directory

The Primary Restore method does not apply to the restoration of Active Directory

SYSVOL

The important thing to consider with a primary restore is that it must only be done if there are NO other DC's in the domain.

Steps required to perform a Primary restore

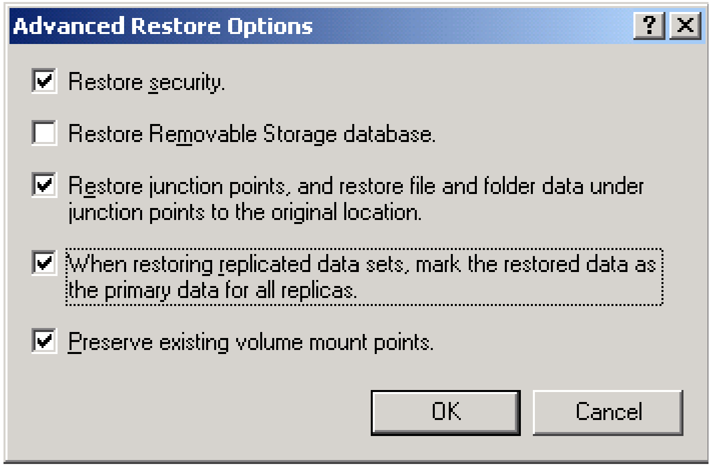
1. Reboot target system into Directory Services Restore Mode by pressing the F8 key upon system startup

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 is 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 Start Restore
8. Click OK on the warning Dialog
9. Click the Advanced button
10. Ensure that at least the following are checked



Advanced Restore Options

☑ Restore security.

□ Restore Removable Storage database.

☑ Restore junction points, and restore file and folder data under junction points to the original location.

☑ When restoring replicated data sets, mark the restored data as the primary data for all replicas.

☑ Preserve existing volume mount points.

11. Click **OK**
12. Click **OK**
13. Ensure the restore source is correct and Click **OK**
14. Click **Close** on the progress report
15. If you only need a nonauthoritative restore Click **Yes** to reboot. ***However*** if you need to perform an authoritative restore click **No** and make the necessary changes using NTDSUTIL.

Recovery of a Global Catalog Server

To recover the global Catalog server service you can either restore the effected GC from backup, or assign a new GC to compensate for the loss of the original.

Steps required for the Restore of a Global Catalog

Refer to the section “Steps Required to Restore a DC From backup” in this paper. Restoring from backup is the only way that a DC (that was functioning as a GC at the time of backup) can automatically be restored to the role of GC. Restoring a DC using the “Restore via replication” method will not automatically reinstate the GC role, as the GUID of the system will have changed and therefore be considered by the directory as a different System.

Steps Required to Assign a New GC

As there are no real detrimental effects in configuring multiple GC’s (besides the additional replication traffic) you may wish to create a new GC in your environment if you anticipate an extended downtime for the GC that has failed. This would be particularly relevant if the user community that was being serviced by the original GC no longer had access to a GC or the requirement for the GC service was significant in your environment e.g. you where running Exchange 2000.

To enable a new Global Catalog Server follow the steps outlined in the “To enable or disable a global catalog” section in the server help file.

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

Recovery of Operations Masters

Once an OM becomes unavailable the only way the service offered by that role can be reinstated is by carrying out one of the following procedures.

1. Repair the existing OM server using the repair methods discussed earlier or by restoring from Backup.
2. Seize the role to another DC within the environment.

Note: Restoring an OM server via replication will not restore it’s original role status.

Seizing an Operations Master Role

Seizing, or force transfer as it is sometimes referred to, is a process that is 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 for all 5 roles, the considerations around their seizure differ.

Note: The graceful Transfer of an OM role will not be discussed in this paper as by definition if this process can be carried out the original Role holder is active and is not involved in a disaster recovery situation.

Recovery of the Schema Master

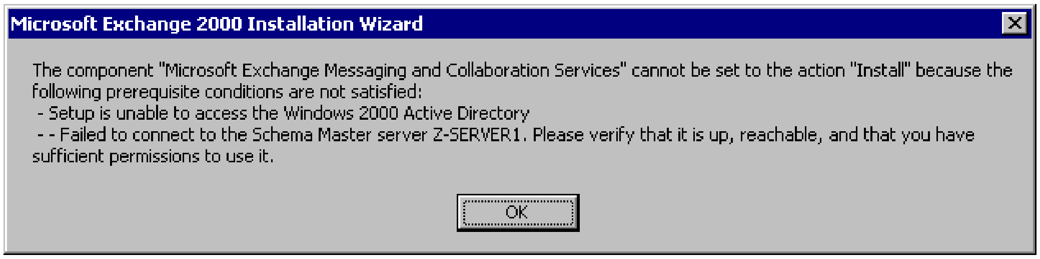
Before deciding whether to seize or repair/restore the Schema master role there are some considerations that you should be aware of before you make a decision.

Impact on Environment

The first thing you must understand before being able to decide which restoration method to use is the impact that a failed Schema Master will have on your environment. The main issues you will see are: -

Unable to make changes to the Schema

When the Schema Master is unavailable, changes to the Schema will not be possible. If changes to the Schema are attempted when the Schema Master is not available a message similar to this will be displayed:



Microsoft Exchange 2000 Installation Wizard

The component "Microsoft Exchange Messaging and Collaboration Services" cannot be set to the action "Install" because the following prerequisite conditions are not satisfied:
- Setup is unable to access the Windows 2000 Active Directory
- - Failed to connect to the Schema Master server Z-SERVER1. Please verify that it is up, reachable, and that you have sufficient permissions to use it.

Note: The exact message displayed will depend on the method you are using to make the change. The message above was experienced when 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 performing a seizure on a Schema Master

The primary consideration for deciding to seize the Schema Master role is the longevity or permanence of the outage. Because of the chance of duplicate schema alterations being propagated throughout the environment a seizure of the Schema Master role should only be carried out if the failed role holder will NEVER come back online.

In most environments, due to both the infrequent requirement for the Schema Master role and the implications of a seizure, it is likely that you will live with the outage for the period of time it takes to restore the DC holding the role. However, if for some reason you require the immediate use of the Schema Master role or 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 it is strongly recommended that the standby role holders specified in your environment be within the same site and direct replication partners with the existing role holder.

To ensure that the standby operations master that you have selected for your environment is the most appropriate, use the Repadmin tool (Included as part of 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 USN’s we are concerned with. As the USN on SYD02 (4023) is higher than the USN on MEL01 (4018) it is more up-to-date than MEL01 and is therefore the more appropriate candidate to assume the role.

Now that you have determined the best candidate to take on the Schema Master role follow the steps below to seize the Schema Master.

To seize the Schema Master role follow these steps:

1. Open a command prompt.
2. Type **NTDSUTIL**
3. At the ntdsutil prompt, type **roles**
4. Type **connections** at the fsmo maintenance prompt

5. At the server connections prompt, type **connect to server <FQDN of Server>**. For example: "connect to server syd02.whitepaper.com.au"
6. Then type **quit** at the server connections prompt
7. At the fsmo maintenance prompt type **seize schema master**

Note: FSMO (Flexible Single Master of Operations) was the previous 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. Click on **Yes** after verification
10. Type **quit** at the fsmo maintenance prompt
11. Type **quit** at the ntdsutil prompt.

Recovery of the Domain Naming Master

Before deciding whether to seize or repair/restore the Domain Naming Master role there are some considerations that you should be aware of before you make a decision.

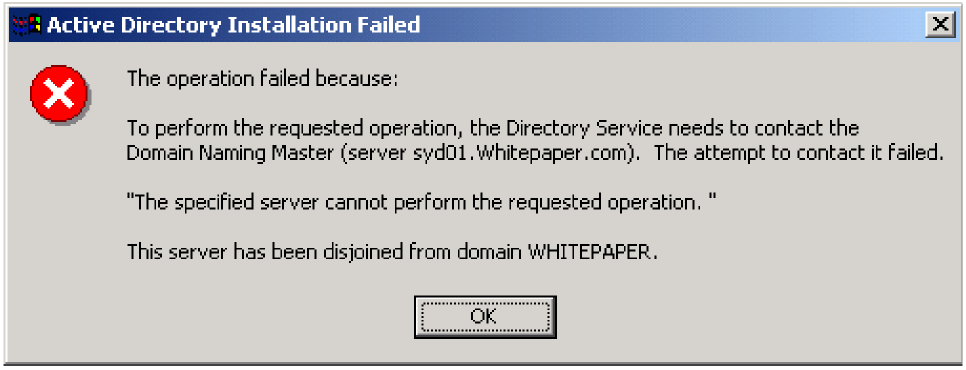
Impact on Environment

The first thing you must understand before being able to decide which restoration method to use is the impact that a failed Domain Naming Master will have on your environment. The main issues you will see are: -

Domains cannot be added to the Forest

When this master is not available domains cannot be added to the Active Directory.

Below is the message received when attempting to run DCPROMO to add a domain when the Domain Naming Master (Syd01.Whitepaper.com) is not available:



The operation failed because:

To perform the requested operation, the Directory Service needs to contact the Domain Naming Master (server syd01.Whitepaper.com). The attempt to contact it failed.

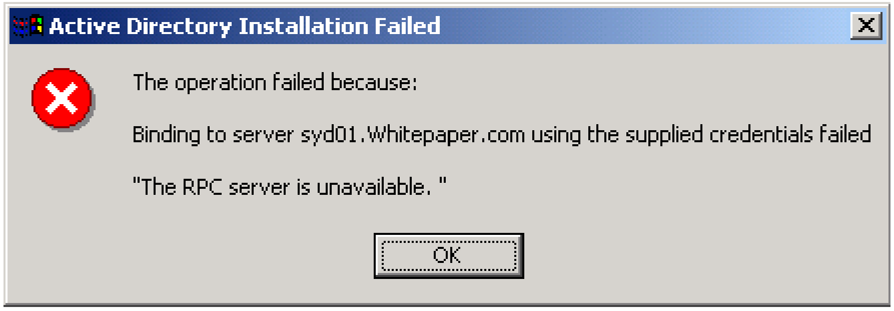
"The specified server cannot perform the requested operation. "

This server has been disjoined from domain WHITEPAPER.

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 is the message received when attempting to run DCPROMO to remove a domain when the Domain Naming Master (Syd01.Whitepaper.com) is not available:



The operation failed because:

Binding to server syd01.Whitepaper.com using the supplied credentials failed

"The RPC server is unavailable. "

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

Considerations for performing a seizure on a Domain Naming Master

The primary consideration for deciding to seize the Domain Naming Master role is the longevity or permanence of the outage. Because of the chance of duplicate domain alterations being propagated throughout the environment a seizure of the Domain Naming Master role should only be carried out if the failed role holder will NEVER come back online.

In most environments, due to both the infrequent requirement for the Domain Naming Master role and the implications of a seizure, it is likely that you will deal with the outage for the period of time it takes to restore the DC holding the role. However, if for some reason you require the immediate use of the Domain Naming Master role or 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 follow the steps outlined in the “Steps Required to Seize the Schema Master” section of this white paper. The only changes required to this process is to replace step 7 with:

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

Recovery of the RID Master

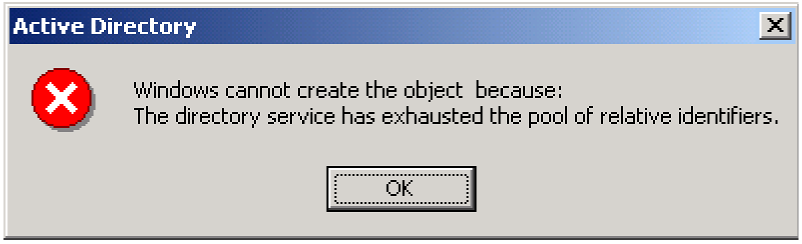
Before deciding whether to seize or repair/restore the RID master role there are some considerations that you should be aware of before you make a decision.

Impact on Environment

The first thing you must understand before being able to decide which restoration method to use is the impact that a failed RID Master will have on your environment. The main issues you will see are: -

Unable to create Security Object

The primary issue that you will face in this situation is the inability to add any new security objects, such as users, groups and computers to the domain, resulting in the following error.



Active Directory

Windows cannot create the object because:
The directory service has exhausted the pool of relative identifiers.

In addition you will also receive an Error in the event log with an event ID of 16645 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 not be able to move security principals to a new domain if the RID master in the target domain is not operational.

When considering the above issues it is important to understand that these problems will NOT emerge as soon as the RID master is off-line. These issues will only surface once the RID pool (512 individual RID's in a pool) on each of the domain controllers within the domain are depleted (as objects can be created on any DC within the domain).

Therefore if you have a domain with 5 remaining DC's you could still theoretically have 2560 (5 x 512) RID's available to you once the RID master fails. In a typical environment this would provide you with ample RID's for the creation of security principles until the RID master was 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 RID's than you have in your existing pools, a role seizure could be performed.

Considerations for performing a seizure on a RID Master

Performing a seizure on a RID master is not something you want to do without due consideration. Because of the risk of duplicate RID's on the network the sever that originally housed the RID master role should NEVER be brought back online. Instead, the original role holder should be completely rebuilt before being introduced back into the production Windows 2000 environment.

If, after understanding 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 follow the steps outlined in the "Steps Required to Seize the Schema Master" section of this white paper. The only changes required to this process is to replace step 7 with:

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

Recovery of the PDC Emulator

Before deciding whether to seize or repair/restore the PDC emulator role there are some considerations that you should be aware of before you make a decision.

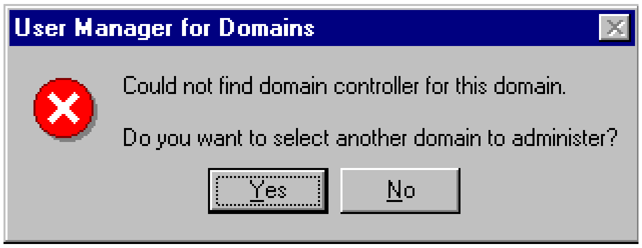
Impact on Environment

The first thing you must understand before being able to decide which restoration method to use is the impact that a failed PDC Emulator will have on your environment. The main issues you will face are: -

Mixed Mode Environment

If the PDC Emulator role suffers a disaster in a mixed mode environment where NT4.0 BDC's are active, you will witness the same issues you did in NT4.0 when the native PDC was unavailable, for example: -

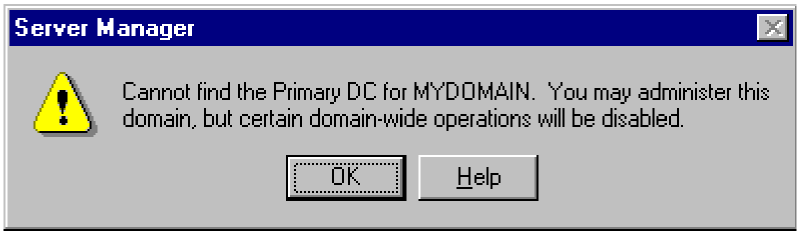
If you try and administer the NT4.0 domain using the native NT4.0 User manager for domains tool you will receive the following error.


User Manager for Domains

Could not find domain controller for this domain.

Do you want to select another domain to administer?

If you try and administer the NT4.0 domain using the native NT4.0 Server Manager tool you will receive the following error.


Server Manager

Cannot find the Primary DC for MYDOMAIN. You may administer this domain, but certain domain-wide operations will be disabled.

Native Mode Environment

The issues that occur in a native mode environment will also be present (on the Windows 2000 side) in a mixed mode environment. The primary issues you will face when the PDC Emulator suffers a failure in a Windows 2000 environment are: -

- **Possible increase in incidents of logon failure**

  If a users password is reset, e.g. he/she forgets their 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 logon.

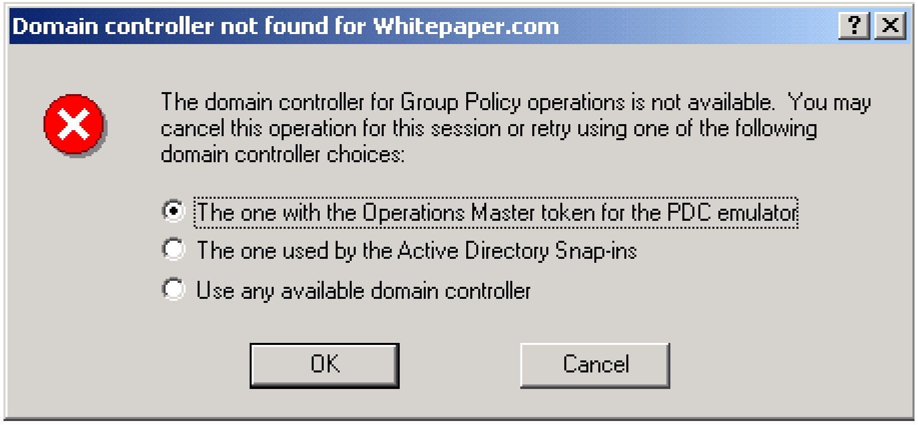
  Although the users local authentication DC will try and contact the PDC emulator to see if the password has changed since last replication, it will fail, because the PDC Emulator is offline. Therefore the authenticating DC will have no choice but to resort to it's local copy of Active Directory, which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

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

Although this can be an issue, the problem can be easily overcome by making the password alteration on the users authenticating DC.

- **Error when Attempting to edit a Group Policy Object**

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



Domain controller not found for Whitepaper.com

The domain controller for Group Policy operations is not available. You may cancel this operation for this session or retry using one of the following domain controller choices:

● The one with the Operations Master token for the PDC emulator
○ The one used by the Active Directory Snap-ins
○ Use any available domain controller

This is a very minor issue, and can be quickly rectified by selecting one of the options provided. A brief description of these 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.*

  Uses the domain controller that Active Directory management snap-ins are using. Recommended option when the PDCE 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 it is likely that a domain controller in the local site will be selected.

Note: The changes made here are only made for the single edit. In other words you will be asked this question every time you try an edit a GPO when the PDCE Master is unavailable.

Considerations for performing a seizure on a PDC Emulator Master

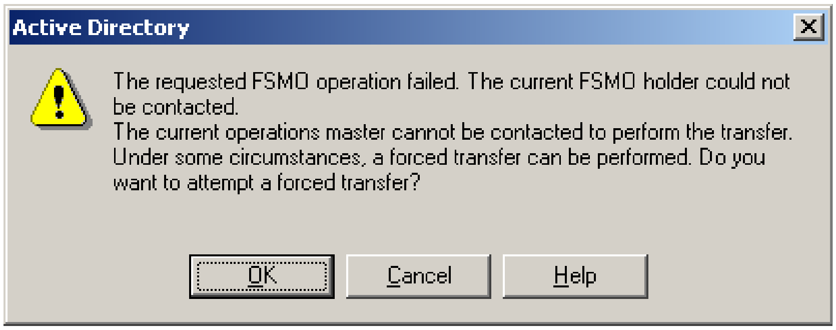
As the role of the PDC Emulator Master is not quite as critical as those previously mentioned, the act of seizing the role does not have the ramifications of the others. If you choose to seize the PDC Emulator role it is not necessary for the original role holder to be completely rebuilt before it can participate in the windows 2000 environment again.

As a result, the decision to seize the PDC Emulator role will have far less implications to your environment and would generally be considered as standard practice in the event of a PDC emulator failure, particularly in a mixed mode environment.

The only real issue to consider when seizing the PDC Emulator role is if you are functioning in a mixed mode environment with NT 4.0 BDC's. In order for the BDC's to be aware of the changes they will perform a full synchronization of the BUILTIN database with the new PDC Emulator.

Steps Required to Seize the PDC Emulator Master

As the issues associated with the seizure of the PDC Emulator role have less impact on the environment, Microsoft have allowed you to seize this role through the "Active Directory Users And Computers" Snap inn. To do this simply go through the steps you would normally go through for a Role Transfer . At the point when the DC realizes the originating PDCE is unavailable it will give you the following dialog.



Active Directory

The requested FSMO operation failed. The current FSMO holder could not be contacted.
The current operations master cannot be contacted to perform the transfer. Under some circumstances, a forced transfer can be performed. Do you want to attempt a forced transfer?

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

Note: A forced transfer is equivalent to a seizure.

In addition you can also seize the role using NTDSUTIL , to do this follow the steps outlined in the "Steps Required to Seize the Schema Master" section of this white paper. The only changes required to this process is to replace step 7 with:

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

Recovery of the Infrastructure Master

Before deciding whether to seize or repair/restore the Infrastructure Master role there are some considerations that you should be aware of before you make a decision.

Impact on Environment

The first thing you must understand before being able to decide which restoration method to use is the impact that a failed Infrastructure Master will have on your environment.

The resultant effect of an Infrastructure master failure in your environment will be limited, it will not be visible to end users and will only affect administrators if there has been considerable group manipulation. These group manipulations will typically be in the form of user additions and or user renames, and the only affect of an infrastructure master being down in this situation is a delay in these changes being referenced through the Active Directory management snap inns.

As a result their will be very few occasions where your environment could not deal without an Infrastructure Master for the period it takes to repair/recover the original, however if you foresee a very long outage a seizure of the role is recommended.

Considerations for performing a seizure on the Infrastructure Master

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

Steps Required to Seize the Infrastructure Master

As with the PDCE an Infrastructure Master can be seized through both the transfer GUI and using NTDSUTIL, to do this follow the steps outlined in the "Steps Required to Seize the PDC Emulator Master" section of this document.

APPENDIX A – Supported Recovery Console Commands

Please ensure that you understand the full impact of these commands before you use them. Some of the commands listed in the table below 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 dirty. bad. /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 might 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 might 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 a destination is not specified, it 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 only operates 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 might 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

<table>
<tr><td>diskpart</td><td>Manages the partitions on your hard disk volumes.
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.</td></tr>
<tr><td>enable</td><td>Enables a Windows system service or driver.
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 it is necessary to restore the start_type of the service. If you do not specify a new start_type, enable prints the old start_type.</td></tr>
</table>

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 this is left blank 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 command is not specified, 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 to physical device mappings that are currently active. 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 only operates 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 only operates 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 only operates 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 Enable wildcard support for some commands, such as DEL, that do not otherwise support them. AllowAllPaths Allow access to all files and folders on the computer. AllowRemovableMedia Allow files to be copied to removable media, such as floppy disks. NoCopyPrompt Do not prompt when overwriting file. To display the list of current environment variable settings, type set without parameters. NB: The set command is an optional Recovery Console command that can be enabled by using either the Group Policy snap-in or the Security Configuration and Analysis snap-in.
systemroot	Sets the current directory to %SystemRoot%.

APPENDIX B – Useful tools for Active Directory Disaster Recovery

The following applications have been compiled as a recommended set of tools that are useful in a disaster situation.

Note: All 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 DC's

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 objectClass, 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 in a domain have a consistent and accurate image of their own domain. In the case of Global Catalogs, DsaStat checks to see if the GC has a consistent image with DC's 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 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 Active Directory Service Interfaces (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.