Windows Server 2003 AD Backup and Disaster Recovery Procedures

Peter Van Keymeulen, 2011
EDE Consulting

ICT Infrastructure Architect

Version: 2.1

1. Contents

2. Contact Information

"IT" doesn't matter

Even in our fast growing world of technology, IT became a commodity the same way as electricity did. It's not the software, hardware or technologies that will make the difference, but the way how you design, implement, maintain and use it. Speaking personally, as an architect, software, hardware and technology "as such" are not that important. They are only a way to create a stable, reliable and secure IT infrastructure to meet all your business and technical needs. Cost reductions, flexibility and future scalability are key words in every project I'm involved with.

EDE Consulting

EDE Consulting was formed in 2006. Though a young company, all our IT professionals are senior consultants with 10 to 20 years of experience in IT business. EDE Consulting has extensive experience with everything related to enterprise system management, network management, system migration and integration, and this at consultancy, architectural and implementation level.
While you take care of your core business, EDE Consulting looks after your IT infrastructure.
We think beyond the technical aspects of IT. If, for example, we design a disaster recovery procedure, this procedure includes all documentation, personal procedures, access lists, and so on.
Among our current customers you will find: Fortis, Dexia, ING, Oleon, AGF, KUL, ...

EDE Consulting bvba
Beverstraat 19
9500 Geraardsbergen
BE-0881.137.013
www.edeconsulting.be

Peter Van Keymeulen
ICT Infrastructure Architect
peter.vankeymeulen@edeconsulting.be
+32 (0)473 98 62 99

http://www.linkedin.com/pub/peter-van-keymeulen/3/531/783

3. Version Control

Version	Status	Date	Authors	Changes
V2.0	Final	15.03.2011	Van Keymeulen Peter	
V2.1	Update	28.04.2011	Van Keymeulen Peter	

4. Terms and Abbreviations

Term	Explanation
RTO	Recovery Time Objective
RPO	Recovery Point Objective
BIA	Business Impact Analysis
ADDS	Active Directory Domain Services
VSS	Volume Shadow Copy
MOSS	Microsoft Office SharePoint Server
SCCM	System Center Configuration Manager
SCOM	System Center Operations Manager
EPO	ePolicy Orchestrator
DNS	Domain Name System
NTP	Network Time Protocol
IPV6	IP version 6
RPC	Remote Procedure Call
WINS	Windows Name Service
NTDS	NT Directory Service - Active Directory database
DFSR	Distributed File System Replication
UNC	Universal Naming Convention (path)
SRV	DNS server record
CNAME	DNS canonical name record
FSMO	Flexible Single Master Operation
PDC	Primary Domain Controller Master
RID	Relative ID Master
INFR	Infrastructure master
GC	Global Catalog
SCHEM	Schema Master
DOM	Domain Naming Master
NT5DS	Windows Time Protocol

5. Introduction

Recovering a Windows 2003 Domain Controller requires more care and attention to detail than the equivalent operation in Windows NT 4.0.

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

5.1 System State Backup and Restore Content

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 2003 backup utility (and other supported third party tools) will automatically back up all of the system components and all of the distributed services upon which Active Directory is dependent. This dependent data, which includes Active Directory, is known collectively as the system state.

The Active Directory backup makes part of the System State backup. It's not possible to backup or restore only the Active Directory; you always get the entire system state.

The System state backup / recovery contain:

- **Active Directory data**: Contains the Active Directory data and configuration and includes:
  - NTDS.DIT the AD database
  - EDB.CHK the checkpoint file
  - EDB*.LOG the transaction logs, each 10 MB in size
  - RES*.LOG reserved transaction logs
- **The Registry**: The contents of the registry are backed up when you backup system state data. In addition, a copy of your registry files is also saved in the folder %systemroot%\repair\RegBack, allowing you to restore the registry without doing a complete system state restore.
- **COM+ Class Registration Database**: 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 backup.

- **SYSVOL data**: The SYSVOL data provides a default Active Directory location for files that must be shared for common access throughout the domain. The SYSVOL folder on a domain controller contains:
    - The Netlogon share
    - GPOs
    - File Replication Service (NTFRS) staging directories and files that are required to be available and synchronized between domain controllers
- **System files that are under Windows File protection**

5.2 Backing up GPOs

There are two procedures to backup the group policies:

The first backup procedure is a part of the "create and update" process of the group policies. Each time a GPO is created or updated, a backup is taken by using the Group Policy Management console. The backup is stored in a folder with the same name as the GPO and all successive backups have the same target folder. Since GPMC does not overwrite the previous backup, we have after each update an additional backup of the GPO. This allows us to restore a GPO to any previous version when needed. These backups are also used to import the settings in the corresponding GPO's that exist is other domains.

The second procedure is a monthly backup of all GPO's in all domains. This procedure is built around the BackupAllGPOs.wsf and GetReportsForAllGPOs.wsf scripts. It stores the backup for each domain in a folder with the same name as the domain name.

5.3 When to Restore

When an object is deleted in Windows 2003, the DC from which the object was deleted informs the other DCs in the environment about the deletion by replicating what is known as a tombstone.
A tombstone is a representation of an object that has been deleted from the directory. The tombstone is removed, eventually, based on the tombstone lifetime setting, which by default is set to 60 days.

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

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

If you attempt to restore the deleted object after 60 days, the object cannot be replicated to the other DCs in the domain because it has a USN that is older than the level required to trigger

replication. And the other DCs cannot inform the restored DC that the object was deleted, so the result is an inconsistent directory.

5.4 Where to Restore

Never restore a system state from ServerA on another hardware (ServerB) while ServerA is still up and running. The system state restore will restore the registry from the original server which causes duplicate names on the network. Moreover, you'll end-up with a domain with two identical domain controllers, same names, and same connection objects. This causes the NTDS service to exclude both, the original and the restored server, from AD replication.

Since the system state contains drivers for network and Raid controller hardware, never restore a system state backup on servers with other hardware than the original server.

5.5 Restoring Back-Links

Restoring back-links is not needed when both are true:

- Your DC's are running "Windows Server 2003 SP1" and the forest operates at the "Windows Server 2003 Forest Functional Level".
- Only users are deleted, or only groups are deleted, never both at the same time

In variations of this scenario, user accounts, computer accounts, or security groups may have been deleted individually or in some combination. In all these cases, the same initial steps apply--you authoritatively restore those objects that were inadvertently deleted.

Some deleted objects require more work to be restored. These objects include objects such as user accounts that contain attributes that are back links of the attributes of other objects. Two of these attributes are managedBy and memberOf.

If your DC's are running "Windows Server 2003 SP1" and the forest operates at the "Windows Server 2003 Forest Functional Level".

There are two methods:

1. Restore the deleted user accounts, and then add the restored users back to their groups by using Ntdsutil.exe
2. Authoritatively restore the deleted user accounts and the deleted users' security groups two times.

5.5.1 *Restore group memberships through NTDSUTIL and LDIFF*

For each user that you restore, at least two files are generated. These files have the following format:

ar_*YYYYMMDD-HHMMSS*_objects.txt
This file contains a list of the authoritatively restored objects. Use this file with the ntdsutil authoritatative restore "create ldif file from" command in any other domain in the forest where the user was a member of Domain Local groups.

ar_*YYYYMMDD-HHMMSS*_links_usn.loc.ldf

If you perform the authoritative restore on a global catalog, one of these files is generated for every domain in the forest. This file contains a script that you can use with the Ldifde.exe utility. The script restores the backlinks for the restored objects. In the user's home domain, the script restores all the group memberships for the restored users. In all other domains in the forest where the user has group membership, the script restores only universal and global group memberships. The script does not restore any Domain Local group memberships. These memberships are not tracked by a global catalog.

To restore the back-links:

- Disconnect the computer from the network.
- Reboot the DC in normal “Active Directory Mode”
- Disable all inbound replication by launching the following command:

  repadmin /options *<recovery dc name>* +DISABLE_INBOUND_REPL

- Type the following command to push the auth-restored objects to all the cross-site replica domain controllers in the domain and to all the global catalogs in the forest:

  epadmin /syncall /d /e /P *<recovery dc>* *<Naming Context>*

- Type the following command to restore the users’ group memberships using LDIFF:

  ldifde -i -f ar_*YYYYMMDD-HHMMSS*_links_usn.loc.ldf

- Enable inbound replication:

  repadmin /options *<recovery dc name>* -DISABLE_INBOUND_REPL

5.5.2 *Restore security principals two times*

To restore all security principals twice:

- Authoritatively restore all deleted user accounts and all security groups, for more information please refer to: 7.2.2 Authoritative Restore.
- Reboot the system in normal Active Directory operation mode
- Wait for the end-to-end replication of the restored users and of the security groups to all the domain controllers in the deleted user's domain and to the forest's global catalog domain controllers.
- Repeat step 1,2 and 3 once again.
- If the deleted users were members of security groups in other domains, authoritatively restore all the security groups that the deleted users were members of in those domains. Or, if system state backups are current, authoritatively restore all the security groups in those domains.

6. Common Tasks

This part of the document contains tasks which are used in almost every type of restore. References to these tasks are made throughout the document.

6.1 Remove Domain Controller from DNS

Ask your local DNS team to remove the domain controller from DNS. Remind them that they have to:

- Delete the A and PTR record form the DNS zone for which this server was a Domain Controller.
- Delete the A record for the domain for which this server was a Domain controller.
- Remove all ACL's on all _zones of the domain for which the server was a Domain Controller.
- Remove all ACL's on all _zones of the root domain of the forest from which this Domain Controller was a member.
- Perform a full regeneration of the DNS zones
- Perform a full replication of the DNS zones to all secondary DNS Servers

6.2 Remove Domain Controller from Active Directory

During this process, you have to know the name of two servers, the server you want to remove, and the Domain Controller on which you want to remove this server.

To remove a Domain Controller from Active Directory.

- Start, on the command prompt on a remaining domain controller, **ntdsutil.**
- Type, without the quotes: "**m c**" and press return to enter the meta cleanup part of ntdsutil.
- Type: "**c"** and press return to enter the connection part.
- Type: "**Connect to server <servername>"** where the server name is the name of the remaining domain controller, not the name of the server you have to remove from the directory.
- Type: "**Q"** (and return) to leave the connection part.
- Type: "**s o t"** to enter the "Select Operation Target" part of ntdsutil
- Type: "**list sites"** to get all existing sites for the forest
- Type: **"select site <number>"** Where the number should be the number of the site on which the "to be removed" server is located.
- Type: **"list domains in site"** to get the list of all domains on that site.
- Type: **"select domain<number>"** where the number should be the number of the domain for which the "to be removed" server was a domain controller.
- Type: **"list servers for domain in site"** to get all domain controllers for the selected domain on the selected site.

- Type: **"select server <number>"** where the number should be the number of the "to be removed" server
- Type: **"Q"** to leave the "select operation target" part of ntdsutil.
- Type: **"remove selected server"**.
- Confirm the deletion of the server from Active Directory
- Close **ntdsutil**
- Open the MMC "**Active Directory Site and Services Settings**" snap-in and select the site from which you deleted the domain controller.
- Select the "**to be removed**" server and delete this object from AD.
- On each server, remove all connection objects coming from the removed server.
- Open the MMC "**Active Directory Users and Computers**" snap-in and select the domain from which you removed the server.
- From the View menu, select "**Advanced Features**".
- Select the "**System**" container
- Select the "**File Replication Service**" container
- Select the "**Domain System Volume** (SYSVOL Share) container and be sure that the removed server doesn't have an object in this container. If it does, remove it.
- Remove the domain controller's computer account from the "Domain Controller" container (if it still exists).

6.3 Change the Active Directory Restore Mode Administrator Password

Change Directory Services Restore Mode Administrator password if you don't know it. Every domain administrator can change the DSRM Administrator Password. This account and password can only be used on a Domain Controller booted in the "Active Directory Restore mode".

As from Windows Server 2003 SP1, both, the DSRM Administrator password and the Domain Administrator password should be exactly the same, otherwise, it's not possible to logon into DSRM.

To change the password:

- Start, on the command prompt, **ntdsutil**
- Type, without the quotes: "**set dsrm password**" and press return to enter the DSRM part of ntdsutil.
- Type: **"Reset Password on server <servername>**", where servername is the name of the Domain Controller on which we have to perform an AD recovery operation.
- Enter the new administrator password.
- Confirm the new administrator password.
- Close **ntdsutil**.

- Using "**Active Directory Users and Computers**", connect to the domain for which you want to do a restore.
- Be sure your MMC has been connected to the Domain Controller on which you want to restore the AD
- Change the local domain administrator password in such a way it is exactly the same as the DSMR password.
- Reboot the system as soon as possible into the DSRM, otherwise the Domain policies are re-enabling the service and the administrator password will be changed.

6.4 Verification of a Successful Restore

To verify the success of a restore, use the following basic tests:

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

- Check if both, the NETLOGON and SYSVOL share are created. If so, the SYSVOL was successfully published to the other domain controllers.
- Check the Directory Service Event log for any messages.
- Check if the domain controller is able to replicate with its neighbors.
- Check if the domain controller is able to authenticate with its neighbors.

6.5 Non-authoritative restore through RDP

The vast majority of servers do have a Rilo board making it possible to access the server in Active Directory Restore mode. RDP can be used for those without Rilo. This part outlines the procedure to access the domain controller in "Active Directory Restore Mode".

Remark: This procedure can only be used to perform a non-authoritative restore since some authoritative restores needs a - from the network - disconnected domain controller.

To access the DC in "AD Restore" mode through RDP:

- Change the boot.ini file on the domain controller by adding the following line to it:

  ```
  multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows Server 2003" /safeboot:dsrepair /sos
  ```

  Keep in mind that the /SAFEBOOT parameter doesn't work in combination with some other parameters. The /SAFEBOOT will be ignored when, for example, the /fastdetect option is used too.
- Make sure you put this new line on the first place in the list, either manual or through the "System Properties / Advanced / Startup and Recovery options".
- Before you reboot the system, be sure you know the DSRM password. For more information, please refer to: 6.3 Change the Active Directory Restore Mode Administrator Password.
- Reboot the system and connect to it through RDP

7. Active Directory Content Recovery

7.1 Overview

The only circumstances in which you should have to recover the content of the directory is when someone, accidentally or on purpose, deleted parts from the directory or when a failing procedure made incorrect changes.

When restoring AD, two possible types of restore exist:

- Authoritative restore
- Non-Authoritative

7.1.1 *Authoritative Restore*

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

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

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

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

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

7.1.2 *Non-Authoritative Restore*

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

After a non-authoritative restore, the DC is updated using normal replication techniques. That is, if the version number of an object is less than the same object's version number stored by its replication partner(s) (indicating the object has changed since it was last backed up), the object on the restored server is updated. This ensures an up-to-date version of the database.

7.2 Domain Naming Context Recovery

The domain naming context contains all users, groups, computers and other objects.

7.2.1 *Non-Authoritative Restore*

To restore the Domain Naming Context or parts of it non-authoritatively:

- Change the DSRM password if you don't know it. For more information, please refer to: *6.3. Change the Active Directory Restore Mode Administrator Password.*
- Restore, the necessary NTBACKUP file you backed-up to another location. Be sure you restore the correct file. Never use a file from another Domain Controller.
- Reboot the server in the "Directory Services Restore mode" by pressing the F8 button during the boot phase.
- Log on to the system using the Administrator account and DSRM password.
- Start ntbackup.exe. Do not use the wizard mode.
- Select the "Restore and Manage Media" tab.
- Select, from the existing list, the file you need. If you restored the file to another location, right click on "File", select "Catalog file" and select the file you restored through your backup system.
- Mark the "System State" box for restoration.
- Select "Restore Files To:" "Original Location"
- Start Restore
- Select "OK"
- Select "OK", do not change the "Advanced" options
- At the end of the restore, select "yes" to reboot.
- The system will reboot and automatically start replicating, from another domain controller, all changes made between now and the time of the backup.
- Validate the successful restore, please refer to: *6.4.Verification of a Successful Restore*

7.2.2 *Authoritative Restore*

Remark: When users and groups have to be restored together, some kind of special order has to be followed. For more information, please refer to: 5.5 Restoring Back-Links.

To restore the Domain Naming Context or parts of it authoritatively:

- Change the DSRM password if you don't know it. For more information, please refer to: *6.3. Change the Active Directory Restore Mode Administrator Password.*
- Restore, the necessary NTBACKUP file you backed-up to another location. Be sure you restore the correct file. Never use a file from another Domain Controller
- Reboot the server in the "Directory Services Restore mode" by pressing the F8 button during the boot phase.
- Log on to the system using the Administrator account and DSRM password.

- Start ntbackup.exe. Do not use the wizard mode.
- Select the "Restore and Manage Media" tab.
- Select, from the existing list, the file you need. If you restored the file to another location, right click on "File", select "Catalog file" and select the file you restored from backup system.
- Mark the "System State" box for restoration.
- Select "Restore Files To:" "Original Location"
- Start Restore
- Select "OK"
- Select "OK", do not change the "Advanced" options
- At the end of the restore, select "NO" to reboot. Do not reboot the system.
- On the command prompt, start ntdsutil
- Type: **"Authoritative Restore"**
    - To restore one user object, type: **"Restore Object "<distinguished name of the user object>""** and select "Yes". Don't forget the quotes around the distinguished name!

      Important: You have to use the "Display Name" of the user account to construct the DN. This means that, if you want to restore the user: G71628, you have to use the following DN:

      cn=peter van keymeulen,ou=pers usr,ou=usr,dc=be,dc=ede,dc=local
    - To restore one computer object, type: **"Restore Object "<distinguished name of the computer object>""** and select "yes". Don't forget the quotes around the distinguished name!
    - To restore an OU container without his child objects, type **"Restore Object "<distinguished name of the OU>""** and select "yes". Don't forget the quotes around the distinguished name!
    - To restore an entire OU container and all his child objects, type **"Restore Subtree "<distinguished name of the OU>""** and select "yes". Don't forget the quotes around the distinguished name!
    - To restore an entire Active Directory, that is; the entire content of one domain, type "**Restore Database"** and select "yes"
- Close ntdsutil
- Reboot the system. This domain controller becomes the master for the domain and all restored data will be replicated to all other domain controllers in the domain.
- Validate the successful restore, please refer to: *6.4.Verification of a Successful Restore*

7.3 Configuration Naming Context Recovery

The configuration naming context contains all Active Directory configuration settings such as the sites and subnets settings, DFS settings and configuration.

7.3.1 *Non-authoritative Restore*

During a non-authoritative restore, only the entire database can be restored. Therefore, follow the same procedure as explained in: 7.2.1.Non-Authoritative Restore.

7.3.2 *Authoritative Restore*

The Configuration Naming Context is a forest wide part of AD. This part has the same structure and content on each domain controller, regardless the domain he serves, through the forest. This means you can restore the Configuration Naming Context authoritatively on every domain controller within the forest.

Follow the same procedure as explained in: *7.3.2.Authoritative Restore.*

7.4 Schema Naming Context Recovery

Schema Naming Context can't be recovered.

8. Domain Controller Recovery

8.1 Recovery from Replication

This is the easiest domain controller recovery method. Just restage the domain controller and let the NTDS service replicate all Active Directory data.

Before restarting the staging, whether or not the original server name and IP address will be used, be sure you remove the server from the Active Directory. For more information please refer to: 6.2, Remove Domain Controller from Active Directory.

When the original server doesn't come back, also remove all his DNS entries from the DNS. For more information please refer to: 6.1, Remove Domain Controller from DNS.

8.2 Recovery from Backup

Recovering an entire domain controller form backup is only useful when you want to save time and network bandwidth by restoring the Active Directory data rather then replicating them across a (slow) link. It's useless to say that you need the NTBACKUP file on a CDROM or tape if you want to safe network bandwidth. This procedure is only useful when restoring a Domain Controller on a site on which you don't have another Domain Controller from the same domain.

To restore a Domain Controller from backup:

- Remove the server from Active Directory. For more information please refer to: *6.2, Remove Domain Controller from Active Directory.*
- Remove all old server DNS entries from the DNS. For more information please refer to: *6.1, Remove Domain Controller from DNS.*
- Restage a computer using the domain controller bootstrap profile.You have to use another hostname.
- Reboot the server in the "Directory Services Restore mode" by pressing the F8 button during the boot phase.
- Log on to the system using the Administrator account.
- Start ntbackup.exe. Do not use the wizard mode.
- Select the "Restore and Manage Media" tab.
- Select, from the existing list, the file you need. If you restored the file to another location, right click on "File", select "Catalog file" and select the file you restored from backup system.
- Mark the "System State" box for restoration.
- Select "Restore Files To:" "Original Location"
- Start Restore
- Select "OK"
- Select "OK", do not change the "Advanced" options
- At the end of the restore, select "yes" to reboot.
- Validate the successful restore, please refer to: 6.4.Verification of a Successful Restore

9. Entire Domain Recovery

This procedure is only valid if the domain doesn't exist anymore, that is, there are no domain controllers anymore. This procedure is not intended to be followed blindly. By this I mean, exceptions within the steps to take can occur as this is a very complex process. It depends on the FSMO role distribution, SYSVOL content, …..

To recover an entire domain:

9.1 Recover System State

- Power down all existing domain controllers for the domain to recover, if any
- Restage a computer using the domain controller bootstrap profile as member of another remaining domain. You have to use another hostname.
- Restore, the necessary NTBACKUP file you backed-up to another location
- Reboot the server in the "Directory Services Restore mode" by pressing the F8 button during the boot phase.
- Log on to the system using the Administrator account.
- Start ntbackup.exe. Do not use the wizard mode.
- Select the "Restore and Manage Media" Tab.
- Select, from the existing list, the file you need. If you restored the file to another location, right click on "File", select "Catalog file" and select the file you restored from your backup system.
- Mark the "System State" box for restoration.
- Select "Restore Files To:" "Original Location"
- Start Restore
- Select "OK"
- Select "OK", do not change the "Advanced" options
- At the end of the restore, select "yes" to reboot.
- Validate the successful restore, please refer to: *6.4.Verification of a Successful Restore*

9.2 Clean up Active Directory and Forest

- Using ntdsutil, remove all but the restored domain controller for the restored domain from the domain. The goal is to end up with a forest in which only the recovered domain controller remains for the recovered domain. When using ntdsutil, connect to the recovered domain controller.
- Keep in mind that the domain is not reachable. This means that the MMC snap in "Active Directory Users and Computers" would not work. So use ADSI editor to remove objects from the AD.
- To remove a DC from Active Directory, please refer to: 6.2.Remove Domain Controller from Active Directory

- Unless you plan to use the same names as the original servers, start cleaning out DNS for each domain controller removed from the domain. For more information, please refer to: 6.1.Remove Domain Controller from DNS.
- Be sure that all domain wide FSMO roles are now maintained on the recovered domain controller. To seize the FSMO roles, refer to: 11.2.Recovering or Seizing an FSMO Role.
- Reboot the system
- Start a command prompt and check if the NETLOGON and SYSVOL exist. The domain controller and therefore the domain will be up and running only when these two shares exist.
- If these shares do not exist:
    - Copy the entire content of the D:\SYSVOL to another location
    - Stop the NTFRS service
    - In the registry, locate the BurFlags value in the following location:

      HKLM\SYSTEM\CurrentControlSet\Services\NtFrs\Parameters\Backup/Restore\Process at Startup
    - Change his value to D4 (HEX)
    - Restart the NTFRS service
    - This domain controller will now be the SYSVOL master
    - Wait until the SYSVOL and NETLOGON Share are present
    - Copy the SYSVOL share content from the backup to the share
    - Validate the successful restore, please refer to: *6.4.Verification of a Successful Restore*
- Add additional domain controllers through normal staging procedures using the most recent domain controller profile.
- Reshuffle the recovered server with the latest domain controller profile.
- Validate the successful restore, please refer to: *6.4.Verification of a Successful Restore.*

10. Entire Forest Recovery

Restoring an entire forest is much easier than it looks like. You only have to respect the order of all steps to take to get the forest up and running again.

10.1 Active Directory Schema

Although the AD schema can't be restores as such, when restoring a root domain controller, the schema will be restored in the state it was at the last backup, meaning that all schema extensions made are restored to.

10.2 Rules to follow

These are the most important rules to follow:

- Always start from the root domain down to the child domains following the domain hierarchy
- Restore only one domain controller from each domain
- Clean out all other domain controllers in the restored domain, before starting the restore of the next domain
- To speed up the recovery, and to avoid all manual DNS changes, use the same IP address and hostname as the original DC.

10.3 Restore Procedure

To restore an entire forest:

- For each domain, stage one member server in another existing forest of the same environment using the same IP address and hostname as the original DC's.
- Starting at the root domain, restore the necessary NTBACKUP file you backed-up to another location.
- Starting at the root domain, restore the entire Active Directory Database. For more information, refer to: 8.2. Recovery from Backup.
- For the restored domain, remove all other remaining domain controllers from the AD. For more information, please refer to: 6.2. Remove Domain Controller from Active Directory.
- Move all domain based FSMO roles to the recovered domain controller. For more information, please refer to: 11.2. Recovering or Seizing an FSMO Role
- Using normal staging procedures, stage all other additional domain controllers for the restored domain.
- Repeat all previous steps for each domain within the forest with respect for the domain hierarchy.

11. FSMO Roles Recovery

11.1 Overview

In a Windows NT4 domain, only the PDC holds an updatable copy of the User Account Database. All other domain controllers have only read-only replicas of the PDC.

In Windows 2003, all domain controllers are maintaining an updatable copy of the Active Directory. However, not all attributes or objects are updatable on every domain controller. Some are things; such as the Schema can only be updated on one single DC in the entire forest, other things are done on one single DC in each domain, whatever the number of domains there are.

To avoid some unsolvable replication conflicts if the same object was modified on two different domain controllers at the same time, 5 different roles are maintained throughout the infrastructure:

Role	Scope	Goals
Schema Master	Forest	Modifies the Schema
Domain Naming Master	Forest	Makes changes to the forest-wide domain name space of the directory
RID Master	Domain	Processes RID Pool requests from all DC's within a given domain
PDC Emulator	Domain	Synchronize time in an enterprise. Account lockout is processed on the PDC emulator. Password changes performed by other DC's in the domain are replicated preferentially to the PDC emulator.
Infrastructure Master	Domain	The infrastructure FSMO role holder is the DC responsible for updating an object's SID and distinguished name in a cross-domain object reference.

11.2 Recovering or Seizing an FSMO Role

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

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

11.2.1 Recovering the Schema Master

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

Because of the infrequent requirement for a schema master role and the implications of a seizure, you can usually live with the outage during the period of time it takes to restore the DC holding the role. However, if you require the immediate use of the schema master role or if the original role holder will never be brought back into the Windows 2003 environment, a seizure can be carried out.

11.2.2 Recovering the Domain Naming Master

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

Because of the infrequent requirement for a domain naming master role and the implications of a seizure, you can usually live with the outage during the period of time it takes to restore the DC holding the role. However, if you require the immediate use of the domain naming master role or if the original role holder will never be brought back into the Windows 2003 environment, a seizure can be carried out.

11.2.3 Recovering the RID Master

Consider carefully before you decide to perform a seizure on an RID master. Because of the risk of duplicate RIDs on the network, the sever that originally housed the RID master role should never come back online.

11.2.4 Recovering the PDC Emulator

Because the role of the PDC emulator is not quite as critical as those previously mentioned, the act of seizing the role does not have the ramifications of the others. If you choose to seize the PDC emulator role, you do not need to completely rebuild the original role holder before it can participate in the Windows 2003 environment again.

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

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

11.2.5 Recovering a Global Catalog

This will never happen since all domain controllers through the forest are Global Catalog.

11.2.6 *Recovering the Infrastructure Master*

This will never happen since all domain controllers through the forest are Global Catalog.

11.3 How to find the existing FSMO role holders

- Start, on the command prompt on a remaining domain controller, **ntdsutil**
- Type, without the quotes: "**roles**" and press return to enter the "FSMO Maintenance" part of ntdsutil
- Select "Meta Cleanup"
- Select "Select Operations Target"
- Select "Connections"
- Select "Connect to server <local dc name>"
- Select "Q"
- Select "List roles for connected server"

11.4 How to Seize a Role

To seize a role:

- Start, on the command prompt on a remaining domain controller, **ntdsutil**
- Type, without the quotes: "**roles**" and press return to enter the "FSMO Maintenance" part of ntdsutil
- Type: "**Select Operation Target"** and press return to enter the connection part
- Type: **"Connections"**
- Type: "**Connect to server <servername>"** where the server name is the name of the remaining domain controller on which you have to install the role
- Type: **"Q"** to leave
- Type: **"Q"** to leave
- Type: **"seize <role>"** , where the role could be one of the following:
    - PDC
    - Domain naming master
    - Infrastructure master
    - RID Master
    - Schema master
- Type: **"Select Operation Target"**
- Type: **"List roles for connected server"** to be sure all seized roles are now on your domain controller
- Close ntdsutil
- Restart the netlogon service

11.5 How to Move a Role

To seize a role:

- Start, on the command prompt on a remaining domain controller, **ntdsutil**
- Type, without the quotes: "**roles**" and press return to enter the "FSMO Maintenance" part of ntdsutil
- Type: "**Select Operation Target"** and press return to enter the connection part
- Type: **"Connections"**
- Type: "**Connect to server <servername>"** where the server name is the name of the remaining domain controller on which you have to install the role
- Type: **"Q"** to leave
- Type: **"Q"** to leave
- Type: **"transfer <role>"** , where the role could be one of the following:
    - PDC
    - Domain naming master
    - Infrastructure master
    - RID Master
    - Schema master
- Type: **"Select Operation Target"**
- Type: **"List roles for connected server"** to be sure all seized roles are now on your domain controller
- Close ntdsutil
- Restart the netlogon service

12. SYSVOL Recovery

12.1 Overview

Although you should only authoritatively restore the SYSVOL together with the authoritative restore of Active Directory, it's possible (not recommended) to restore the SYSVOL authoritatively, but independently from the AD restore. Keep in mind that GPO settings are stored on both, Active directory database and the SYSVOL, and that these two have to be in sync with each other at any moment in time.

It's only possible to restore the content of the SYSVOL share and the NETLOGON share. If someone deleted the entire SYSVOL directory, restore from tape will be successful, but SYSVOL and NETLOGON replication won't work.

It's better to recreate the entire structure in case you have to restore the entire SYSVOL folder. Please refer to the following Microsoft Technet Article: Q315457

12.2 Authoritative SYSVOL Restore during AD Restore

When the AD restore has completed, DO NOT REBOOT the system but:

- Start ntbackup.exe. Do not use the wizard mode.
- Select the "Restore and Manage Media" tab.
- Select, from the existing list, the file you need. If you restored the file to another location, right click on "File", select "Catalog file" and select the file you restored from your backup system.
- Mark the "System State" box for restoration.
- Choose alternate location to restore the system state on it
- Start the restore by clicking on the "Start Restore" button
- Be sure that "Restore junction points" is NOT selected. Leave all the other options on their default setting.
- Start restore
- If finished, close the utility
- Reboot the server
- Logon to the server
- Wait until SYSVOL is published to other domain controllers. This can take a while. SYSVOL is published from the moment that the following shares are created:
  - NETLOGON
  - SYSVOL
- Copy the contents of the SYSVOL on the alternative location to the operational SYSVOL
- From this point on, SYSVOL will be replicated to all other domain controllers

12.3 Authoritative Restore of SYSVOL Only

- Change the DSRM password if you don't know it. For more information, please refer to: *6.3. Change the Active Directory Restore Mode Administrator Password.*
- Restore, the necessary NTBACKUP file you backed-up to another location. Be sure you restore the correct file. Never use a file from another Domain Controller.
- Reboot the server in the "Directory Services Restore mode" by pressing the F8 button during the boot phase.
- Log on to the system using the Administrator account and DSRM password.
- Start ntbackup.exe. Do not use the wizard mode.
- Select the "Restore and Manage Media" tab.
- Select, from the existing list, the file you need. If you restored the file to another location, right click on "File", select "Catalog file" and select the file you restored from your backup system.
- Mark the "System State" box for restoration.
- Choose alternate location to restore the system state on it
- Start the restore by clicking on the "Start Restore" button
- Be sure that "Restore junction points" is NOT selected. Leave all the other options on their default setting.
- Start restore
- If finished, close the utility
- Reboot the server
- Logon to the server
- Wait until SYSVOL is published to other domain controllers. This can take a while. SYSVOL is published from the moment that the following shares are created:
    - NETLOGON
    - SYSVOL
- Copy the contents of the SYSVOL on the alternative location to the operational SYSVOL
- From this point on, SYSVOL will be replicated to all other domain controllers

13. Recovering Group Policy Objects

13.1 Rollback GPO update

To rollback a GPO update or to restore some settings in a GPO:

- Select the GPO in the Group Policy Management console
- Right-click and choose 'Import Settings…'
- Choose the latest backup from the individual GPO backup folder
- Complete the import settings wizard

13.2 Restore one or more GPOs

To restore one or more deleted GPOs:

- Select the 'Group Policy Objects' container within the Group Policy Management console
- Right-click and choose 'Manage Backups…'
- Browse to the folder that contains all GPO backups for that domain
- Select one or more GPOs to restore
- Click on 'Restore' within the Manage Backups dialog box.
- For each restored GPO, open the report file (.html) from the backup folder and recreate the reported links when needed.

14. Fast Disaster Recovery from Delayed Replicated Site

14.1 Introduction

Today, between sites, replication happens every 15 minutes. This means that changes to AD are replicated to each Domain Controller in the domain within a max of 105 minutes. But, errors, corruptions and accidentally object deletions are replicated within 105 minutes too. If we change the replication schedule to 24 hours, that is; one replication every 24 hour, we do have 24 hours to detect corruptions, procedural or human errors causing the Active Directory to become unavailable. Should this happen, the Delayed Replicated site can than be used to recover very fast from a totally lost domain on another site.

14.2 Recover a domain on another site

To recover a domain on from another "Delayed Replicated site":

- On a domain controller on the "Delayed Replicated Site", logon using Enterprise Admin Rights.
- Change the DSRM password if you don't know it. For more information, please refer to: *6.3. Change the Active Directory Restore Mode Administrator Password.*
- Reboot the server in the "Directory Services Restore mode" by pressing the F8 button during the boot phase.
- Log on to the system using the Administrator account and DSRM password.
- On the command prompt, start ntdsutil
- Type: **"Authoritative Restore"**
- To restore the entire Active Directory, that is; the entire content of one domain, type "**Restore Database"** and select "yes"
- Close ntdsutil
- Reboot the system. This domain controller becomes the master for the domain and all restored data will be replicated to all other domain controllers in the domain.
- Force a replication across all site links to replicate the restored objects to the other sites immediately.
- Validate the successful restore, please refer to: *6.4.Verification of a Successful Restore*

15. Active Directory Disaster Recovery Procedures

15.1 Introduction

By design, Active Directory Services are build to be always available even should we encounter the outage of en entire site.

The KCC service running on each domain controller recalculates and rebuilds if necessary the entire replication topology every 15 minutes. The replication topology will be dynamically changed should one or more domain controllers, site links or entire sites become unavailable. This makes ADS less vulnerable to network issues or Domain Controller hardware issues.

15.2 When to go into DRP mode

Putting ADS into DRP mode has a huge impact on the way to return back to normal operational level.
ADS have 5 different FSMO roles which are unique through the domain or even through the forest. The original domain controller providing one or more of these roles may never be put back on line once the roles, he maintained before the disaster, are moved to a DC on another site. Moving a FSMO role to the DRP site causes the original role holder to be reinstalled afterwards. ADS, on the other hand, can life for a short time without having the FSMO roles available. So deciding when to go into DRP mode is a crucial choice between a time consuming DRP or facing some issues caused by missing FSMO roles.

ADS should go into DRP mode only:

- When one more sites are down. A “site”, from and Active Directory point of view is not the same a physical building our site. A site in ADS is a collection of networks in which all servers are fully connected to each other through fast network links. Therefore, the AB and the Haren site in Belgium are in ADS only one single site. From an ADS DRP point of view, AB and Haren need to be considered as two different sites.
- When the site outage will be longer than 8 hours.

15.3 Putting ADS into Disaster Recovery Mode

We’re facing the following issues should we loose a site:

- The remaining domain controllers will be much more called by clients and users for authentication and authorisation operations. This will slow down the reaction time of these domain controllers.
- ADS have 5 different FSMO roles, which are unique through the domain or the forest. It would be possible that some of these roles become unavailable since they are on the failing site.

To address one or both above issues:

- Some manual interventions in both cases.
- Install additional domain controllers on the remaining sites
- Move all failed roles to domain controllers on the remaining sites

15.3.1 *Common tasks when going into DR mode*

Once the DRP has been started all of the following manual interventions have to be initiated:

- Shutdown all domain controllers on the remaining site (if she still exists)
- The DNS team should, for each domain controller on the failing site:
    - Remove the A and PTR record for the server name from the DNS
    - Remove the A record for the domain for the server from the DNS
    - Remove all SRV records for the server from the DNS
- The DNS team should, once the DNS cleanup has been done, launch a full regeneration of the DNS zones and forces a full replication to all secondary DNS servers.

15.3.2 *Installing additional domain controllers*

Please refer to the documentation regarding the XBOW server staging procedures for the server.

Remark: Keep in mind that new domain controller should have write access to all _zones of his own domain and some _zones of the forest root domain. So please inform the DNS people to grant the new server all necessary rights. They know exactly what rights.

15.3.3 *Move all FSMO roles*

To know which roles are missing or which role exists on which server, please refer to: 11.3 How to find the existing FSMO role holders

15.4 To Seize a role, please refer to: 11.4 How to find the existing FSMO role holders

- Start, on the command prompt on a remaining domain controller, **ntdsutil**
- Type, without the quotes: "**roles**" and press return to enter the "FSMO Maintenance" part of ntdsutil
- Select "Meta Cleanup"
- Select "Select Operations Target"
- Select "Connections"
- Select "Connect to server <local dc name>"
- Select "Q"
- Select "List roles for connected server"

- How to Seize a Role

15.5 How to move back to the original operation level

This part describes how we can switch over from DRP mode back to normal operations mode, meaning that the site failed site is back online.

- Be sure all domain controllers have the necessary rights to update and or create their SRV records in the DNS. Be sure the A and the PTR record for the servers exists and that their A record also exist on the domain record.
- Power on all domain controllers which did not have any FSMO role before the DRP started.
- Verify if, after the boot, all necessary SRV records for each server exists. To do, log onto the server and launch the “CheckDNS.exe” tool.
- Ask the DNS people to force a full regeneration of all zones and force a full replication to each secondary DNS server.
- Reinstall all domain controllers which maintained a FSMO role before the DRP started.
- Verify if, after the boot, all necessary SRV records for the reinstalled server exists. To do, log onto the server and launch the “CheckDNS.exe” tool.
- Ask the DNS people to force a full regeneration of all zones and force a full replication to each secondary DNS server.
- Move all FSMO roles to their original server. For more information, please refer to: 7.5 How to move a Role

16. References

16.1 Microsoft TechNet and Knowledge Base Articles

Q316790 The SYSVOL and NETLOGON Share are missing after you Restore a Domain Controller from Backup.

Q257338 Troubleshooting Missing SYSVOL and NETLOGON Shares on 2000 Domain Controllers.

Q315457 How to rebuild the SYSVOL tree and its content in a domain?

http://support.microsoft.com/kb/840001 How to restore deleted user accounts and their group memberships in Active Directory