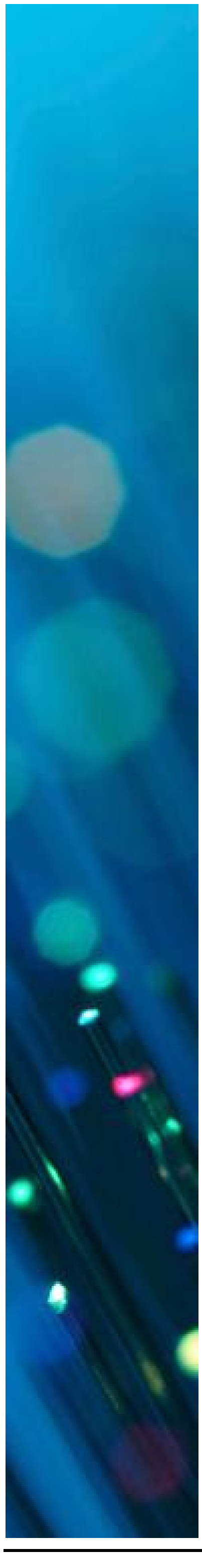


Active Directory Recovery Planning for Small and Large Organizations

By Alan Klietz
Algin Technology LLC

Algin
Technology

Algin Technology LLC
3055 Old Highway 8, Suite 35
Minneapolis, MN 55418
E-mail: sales@algintech.com
Telephone: +1 866 488 6657   +1 612 235 2100
Fax: +1 612 235 2108

Table of Contents

Introduction

Active Directory® (AD) is a distributed directory system developed by Microsoft® Corporation to serve a wide variety of organizations from small offices to large multinational corporations. In addition to traditional directory information such as phone numbers and job titles, Active Directory contains the Identification and Authentication (I&A) credentials for the users of a Microsoft Windows® network. AD determines the security boundaries (“domains”), access rights, and usage policies for your network.

Because Active Directory is a central component of Windows I&A, developing a recovery plan is essential for reliability and availability of your network. The requirements of your AD recovery plan will be influenced by several factors, including your organizational size, your security and reliability requirements, and your budget and resource availability.

Small Organizations

A small organization usually has a limited budget and staff. Often the most significant requirement is the need to limit Total Cost of Ownership (TCO) while serving the mission of the organization.

Scenario: Grace Community Church

Mary is a volunteer who runs the computer system for the church staff at Grace Community Church. Because it is a small organization with a limited budget, Mary needs to be frugal in budgeting expenses.

In planning church’s Windows network, Mary decides on Microsoft Small Business Server with Active Directory as the most economical choice. Mary now needs to develop an AD maintenance and recovery plan.

Mary’s AD recovery plan includes the following considerations:

- Running a small domain with a single server.
- Recovering AD if the single server fails.
- Minimizing capital and maintenance costs.

Running a domain with a single server: Microsoft generally allows only one Small Business Server (SBS) domain controller in an Active Directory forest (Q884453). Intended for small organizations, the SBS computer is often the only domain controller for the entire organization.

Recovering AD if the single server fails: With one server there are three basic methods for recovering AD: 1) Restore the entire System State and the Windows files from the system disk. 2) Move only the AD database and related data files. 3) Rebuild the AD forest.

Method 1: Restore the System State and Windows disk. This method copies the entire Windows operating system and all related files from the system disk (typically C:).

The advantage of this method is that all settings and installed applications are copied with complete fidelity, and it can be accomplished without any external tools.

The disadvantage is that the replacement computer must be hardware compatible. In addition, any bugs, viruses, bad drivers, or other causes of system instability will also be copied to the new computer.

Microsoft does not support restoring a system state backup from one computer to a second computer of a different make, model, or hardware configuration (Q249694). Even if the source and destination computers appear to be identical makes and models, there may be driver, hardware, or firmware differences that can prevent successful transfer between the source and destination computers.

Method 2: Move only the AD database. This method copies only the Active Directory database and related data files. These include NTDS.DIT, EDB*.LOG), the System Volume (SYSVOL), DNS settings, and security credential files.

The advantage is that you can move AD to a computer running on different hardware. The new computer can be any make or model. And you can install AD on a “clean” computer, eliminating any instability issues.

The disadvantage is that you need to re-install applications and re-apply settings.

Method 3: Rebuild a new AD forest. This is the default fallback option. It requires unjoining and rejoining all member computers, creating all new user accounts, and issuing new passwords. All user desktop settings will be lost, including icons and desktop application settings. Private user files and folders, such as My Documents, saved e-mail messages, and Web Favorites will need to be manually copied on each desktop computer from the old dead accounts to the new accounts. Because of the amount of work required this should be considered the method of last resort.

Minimizing capital and maintenance costs: Running AD on a single server instead of two can cut in half the initial hardware and software capital expenses as well as ongoing maintenance and Software Assurance fees. However you need to take into account the organizational cost of having your AD server down during the time it takes to replace it. A plan should take this into account and consider options to limit downtime. For example, you can select in advance a designated non-server PC that you can press into service on short notice.

A single server environment can work to your advantage in controlling costs if you understand the tradeoffs when developing your AD recovery plan.

Large Organizations

Large organizations have diverse and complex IT requirements. These often dictate the need for sophisticated AD recovery management techniques.

Scenario: General Products Corporation

General Products Corporation is a large corporation with several divisions and branch offices. It recently acquired another corporation and is in the process of consolidating domains and servers.

Robert has been tasked with creation of an AD recovery and management plan for General Products. The AD forest contains several domains, some of which were independently managed prior to consolidation.

Robert's AD recovery management plan includes the following considerations:

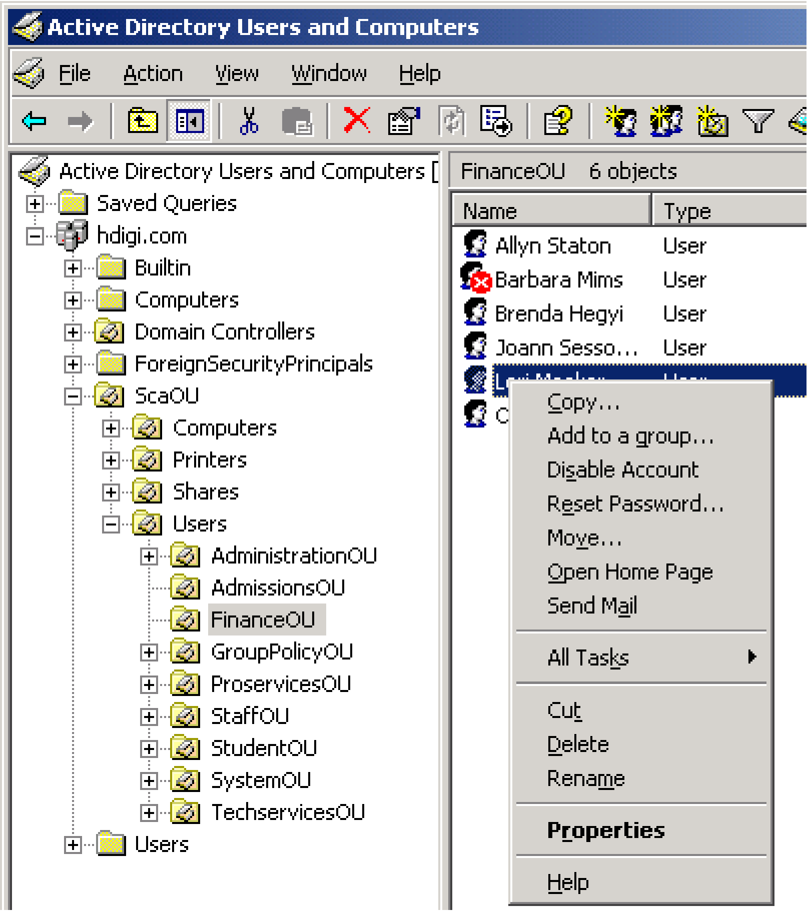
- OU-level and object-level recovery
- Branch-office recovery
- Disaster recovery
- Testing major or irreversible changes
- Staff training
- Domain consolidation and restructuring

OU-level and object-level recovery

Active Directory is a distributed database system. Within a domain AD uses multi-master replication between domain controllers (DCs) such that each DC contains the same copy of the domain's objects. Queries for objects in other domains are delegated via referral to a domain controller for the target domain.

Computer and user objects in a domain can be grouped into an Organizational Units (OUs). The number and grouping of OUs usually reflects the business structure of the organization. AD allows delegation of management at the OU level.

The objects in AD are managed using the Microsoft Management Console (MMC). MMC provides a tree-like structure for managing OUs, computers, and users (see figure).



OU-level or object-level recovery is needed when an administrative user inadvertently deletes or modifies an OU or an individual object.

AD does not provide a way to recover from administrative errors. (In other words, there is no "undo" capability.)

> Recovery of OU or individual objects is possible using an object-level database recovery utility such as NetPro™ RestoreADmin™. These utilities create a shadow database to track changes to AD in order to provide an "undo" capability.

Object recovery is important for domains that require high availability, or that have many domain controllers hosting the domain, or that have other requirements where a domain-level restore would be inconvenient or impractical. Object recovery does not undo global or irreversible changes (page 5) or system errors (page 8).

Deleted user accounts or group memberships can be restored manually using an authoritative restore with NTDSUTIL. However the procedure is complex and error prone and is not recommended. For details see the Microsoft Knowledge Base article "How to restore deleted user accounts and their group memberships in Active Directory" (Q840001).

Branch Office Recovery

General Products has several branch offices, with a small number of employees at each site. As a general rule your Active Directory topology should match your organizational topology. At General Products each branch office has its own domain. Since a domain is also a security boundary, having separate domains helps to limit the propagation of a security breech in a branch office from compromising the main computer center. (OU-level delegation is mainly functional and does not provide strong protection.)

Depending on reliability and budget requirements, a branch office can be assigned one domain controller. The case of a single domain controller at a branch office can be handled similarly to the Small Organization scenario. Your plan will need to judge the tradeoff between reliability and cost.

Disaster Recovery

Floods, fires, and earthquakes can cause damage or loss of your entire computer center. Offsite backups are essential, and backup tapes/discs should be rotated to a secure remote location on a regular basis. The root domain of the AD forest and other important domains should have offsite replication, with remote accessibility via VPN or dedicated links.

Two or more geographically separated computer centers should house DCs for important domains to provide distributed redundancy to mitigate against power failures or network disconnections. The consolidation of WAN network providers means that you need to carefully consider the physical routes of the alternate connections between your sites. Otherwise, a backhoe digging a trench in Chicago may cut all your backup connections between your west-coast and east-coast operations. A VPN connection using the public Internet (using a high hop-count in the routing table) can take advantage of the Internet's dynamic routing capability to temporarily replace broken dedicated links.

Your recovery plan should include a contingency for moving operations to a replacement data center in case of a long-term outage. For example, you can establish a reciprocity agreement with another organization or contract with a commercial data recovery center to host your servers.

Forest-wide recovery

Some changes to the AD configuration are permanent and irreversible. These include adding new types of objects to the database schema or elevating the Forest Functional Level. Global changes will propagate throughout the entire forest and affect all domain controllers in your organization. Once made, these changes generally cannot be rolled back. The only supported recovery method is to restore the entire AD forest.

For more information on AD forest recovery procedures see the Microsoft technical paper, "Best Practices: Active Directory Forest Recovery", http://www.microsoft.com/downloads/details.aspx?familyid=3eda5a79-c99b-4df9-823c-933feba08cfe

While forest recovery might be an option for a small site, it is clearly a disastrous situation in a large organization. Your AD recovery plan should focus on preventative steps. The best preventative method is to carefully test major or irreversible changes on an offline copy of the AD forest (see below).

Testing Major or Irreversible Changes

Microsoft recommends that you validate the compatibility of all security-related configuration changes in a test forest before you introduce them in a production environment (Q823659). This is especially important before making major or irreversible changes to your AD configuration, such as elevating the Domain Functional Level or the Forest Functional Level.

You can use either a physical computer or a virtual machine (VM) for your testing. A VM is the recommended choice, as it is easier to "reset" and can guarantee network isolation because it does not run on real network hardware.

> UMove works with VMware® and with Microsoft® Virtual Server™.
>
> VMware Server is a free product that allows you to run Windows Server as a virtual machine. It can be installed on any host computer that is already running Windows Server.
> http://www.vmware.com/products/server/

Offline testing is also important before attempting domain consolidation or types of major restructuring (see below).

When conducting your testing it is generally not necessary to clone AD from every domain controller. Usually cloning one domain controller from each affected domain is sufficient. (Exception: if you are testing changes to replication settings you should clone all of the affected DCs.)

Staff Training

In addition to offline testing, offline training is important as a preventative measure to avoid administrative errors. Staff responsible for managing Active Directory should have access to an offline copy at least one domain controller for training purposes. Ideally it should be a VM with a snapshot capability for quick reset.

Domain Consolidation and Restructuring

Corporate mergers or reorganizations often require the consolidation or restructuring of a number of domains. Domain consolidation can be accomplished offline, with new replication and DNS settings established in a virtual environment. When tested and approved, the restructured forest can copied *en masse* to the live environment.

Recovery Best Practices

The following guidelines are recommended when writing the recovery procedures in your AD recovery plan:

Backup Schedule

Establish a procedure to make periodic backups of Active Directory. For a small organization where AD is relatively static a weekly backup may be sufficient. A large organization where AD is changed frequently should be backed up daily.

Backups can be incorporated into your standard backup procedure for the System State. Also be sure to back up the system disk (usually C:). This is because the System State does **not** include all information required to move AD to a replacement computer.

> For a list of all files required to move AD to a replacement or test computer see http://utools.com/help/StagingFolder.asp.
>
> UMove can be used to create a minimal-sized .BKF file so that you do not need to back up the entire C: disk daily.

An object-level recovery utility should also be considered where changes are frequent or high availability is important (page 3). Establish a snapshot schedule for the shadow database, at minimum daily and more often if needed.

Restore Order

When restoring multiple domain controllers,

- Restore the forest root domain before other domains.
- Restore the parent domain before the child domain(s).
- In each domain, restore the domain controller with the PDC emulator role before non-PDCs.
- Restore DCs offering DNS before other DCs.

SYSVOL

Best Practices for Restoring SYSVOL

The System Volume (SYSVOL) contains a shared copy of the domain's public files. It includes the files that define the domain's Group Policy settings and the domain's user logon scripts.

Using the File Replication Service (FRS), the files in SYSVOL are kept identical on every domain controller in the domain.

When restoring SYSVOL,

- If the domain has only one domain controller select authoritative restore of SYSVOL.
- When restoring a non-PDC select non-authoritative restore of SYSVOL.

- When restoring all the domain controllers, first restore the PDC and select authoritative restore of SYSVOL. For the remaining domain controllers select non-authoritative restore of SYSVOL.

For more information on SYSVOL recovery see page 9.

Recovery Technical Issues

The following technical issues need to be considered in the operational section of your AD recovery plan.

AD Database Size

The file \Windows\NTDS\NTDS.DIT contains the bulk of the Active Directory database. The size is roughly proportional to the number of objects stored therein. It is typically 200 MB for a small organization and 1-10 gigabytes for a large organization. It rarely exceeds 10 gigabytes except when a single domain contains a very large number of users/computers (100,000 or more).

If you have a very large number of users or computers, you should consider splitting up your organization into multiple domains to reduce the size of the NTDS.DIT file. This will make it easier to create daily/weekly snapshots without running out of disk space. It will also improve your security by allowing you to subdivide your organization into smaller security domains. (Remember, a domain is a security boundary.) Smaller security domains help to compartmentalize and reduce the impact of security breeches.

The NTDS.DIT file can become fragmented due to many additions and deletions of objects. If the file is excessively large, you can defragment it offline (Q232122).

Minimizing the size of the NTDS.DIT reduces the risk of exposure to ESE page corruption (see below).

ESE page corruption

Due to the demand for disk manufacturers to produce disks at lower prices and higher data densities, hard disk drives (HDDs) are not as reliable as those manufactured several years ago. In particular, bad disk sectors are more common.

Bad disk sectors can be ignored in many cases (e.g., in media files). However, a bad disk sector in the NTDS.DIT file is catastrophic.

NTDS.DIT is an Indexed Sequential Access Method (ISAM) file. The software component that accesses the file is called the Extensible Storage Engine (ESE). ESE stores ISAM data in pages. The size of each page is 4096 bytes (the same as the size of a disk block in the NTDS file system).

Each page contains a checksum. The checksum is used to detect corruption of the data page, typically due to a bad physical disk block or a bad bit in a memory DIMM.

When backing up Active Directory with NTBACKUP, ESE copies the data out of NTDS.DIT and feeds it to NTBACKUP. During the backup ESE recomputes the checksum of each data page and compares it to the value stored on the disk. **If the ESE checksum does not match, the entire backup is aborted.**

NTBACKUP will terminate prematurely and the backup will be unusable. The Event Log for Directory Services will report “a read verification error occurred” (0xC80003FA) or “a disk I/O error occurred” (0xC80003FE). The error message will include the page number of the ESE page that contained the bad checksum.

There is no documented way to fix a page with a bad ESE page checksum. The only recovery option is to restore the entire Active Directory database from a clean backup.

The best way to prevent ESE page corruption is to use a high reliability disk system with RAID (Reliable Array of Independent Disks) and a high-reliability memory system with ECC (Error Correction Codes) in a server-class computer system.

It is important that you detect ESE page corruption early so that errors do not compromise the integrity of Active Directory. The best way to detect ESE page errors is to make daily backups of the AD database.

> UMove can create daily scheduled backups of the AD database. During the backup it will report ESE page corruption via e-mail notification. You can then restore a clean AD database from the previous day’s backup. Replication from other DCs will bring the restored DC up to date.

Running AD on a desktop-class computer system that does not have RAID or ECC protection increases the risk of ESE page corruption.

SYSVOL Recovery

SYSVOL and the Active Directory database are closely coupled. They contain cross-reference links between them. When you restore the AD database you must also restore SYSVOL.

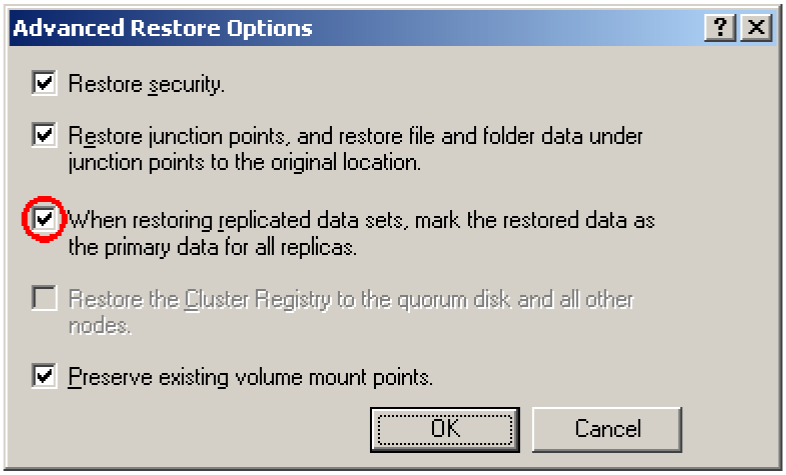
The File Replication Service (FRS) replicates the contents of SYSVOL to all of the domain controllers in the domain. Its purpose is to ensure that the files in SYSVOL are always identical.

SYSVOL Restore Types

There are three types of methods for restoring SYSVOL: authoritative, non-authoritative, and normal.

An **authoritative** restore causes other domain controllers to replace their copies of SYSVOL with the copy on the restored computer. Conversely, a **non-authoritative** restore causes the restored computer to replace SYSVOL with a copy from an authoritative domain controller.

You can select an authoritative versus non-authoritative restore of SYSVOL by checking the box in NTBACKUP, “When restoring replicated data sets, mark the restored data as the primary for all replicas.” (See figure)



☑ Restore security.

☑ 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.

☐ Restore the Cluster Registry to the quorum disk and all other nodes.

☑ Preserve existing volume mount points.

Group Policy Containers and Version Synchronization

The Active Directory database is tightly coupled to SYSVOL and they must be restored together as a unit. This is because the AD database contains Group Policy Container (GPC) objects, which are connected to the Group Policy files in SYSVOL.

GPC objects are stored in AD under a Distinguished Name (DN). The DN is CN={GUID}, CN=Policies, CN=System, DC=*your-domain*, DC=com, where {GUID} is a globally-unique identifier for the Group Policy object. The GPC object contains the attribute **versionNumber**. It must match the **Version** attribute in the corresponding file at \Windows\SYSVOL\domain\Policies\{GUID}\gpt.ini.

If the version numbers go out of sync the system will refuse to apply the Group Policy objects. The result is that your policies may not be enforced (Q814609)

If you do an authoritative restore of AD using NTDSTIL and include the GPC branch, you need to also restore SYSVOL authoritatively as shown above. Otherwise the version numbers may go out of sync.

> UMove automatically synchronizes the GPCs in AD with the GPOs in SYSVOL.

EFS Key Recovery

The Encrypting File System (EFS) encrypts folders and files on the NTFS file system.

EFS provides for a *recovery agent* to protect against the accidental loss of your encrypted files. A recovery agent is a privileged user who can recover data from an encrypted file if the original user forgets his/her password (or if the original user's account is deleted).

When the Administrator account logs on to the first domain controller in a domain, Windows Server will automatically generate an EFS Recovery Agent certificate and store it in Active Directory. This allows the Administrator account to recover encrypted files.

However, the private key for the EFS Recovery Agent certificate is stored outside of Active Directory, in an undisclosed location. It is stored only on the first domain controller in the domain. This means the Administrator must directly log on to the first domain controller in order to recover encrypted files. (This is presumably for security reasons.)

If you shuffle domain controllers, for example by adding a second domain controller and then deleting the first domain controller, you will lose the private key for your EFS Recovery Agent certificate. You will not be able to recover any previously encrypted EFS files. Once the private key is lost it can never be recovered.

Guidelines for EFS Key Recovery

If your organization uses EFS, you should take into account the recovery of the EFS Recovery Agent private key in your AD recovery plan

- The EFS Recovery Agent private key is stored on the first domain controller promoted in the domain.

- If you lose the first domain controller you will lose the EFS private key.

> UMove will copy the Administrator EFS private key when moving AD to a new domain controller.

USN Rollback

What is USN Rollback?

A domain controller tracks objects in AD based on their Update Serial Numbers (USN). Every object in AD has a USN. As objects are modified, the USN increases monotonically, like an odometer on a car. The latest USN on each DC is called the “high water mark”. During replication each DC compares its USN high water mark with the USN high water mark of its neighbors.

USN rollback happens when an older copy of Active Directory is restored but the computer fails to notify the other domain controllers that it was rolled back to an out-of-date copy of AD (and therefore that its high water mark has rolled back).

If you restore AD from a .BKF file, the restored computer recognizes that its high water mark has rolled back, so it notifies the other DCs (by changing its invocationID). The other DCs respond by “playing back” all changes made to AD since then, bringing the restored computer up to date.

However, if you restore AD from the image of a dead computer's disk that is out-of-date (for example, if you restore an old disk image created with Norton Ghost), the computer will be unaware that it has been rolled back. If the restored disk is older than the most recent actual disk that successfully replicated with the other domain controllers, any more recent changes made to AD on other domain controllers will not be "played back" to the out-of-date DC. This is because the restored DC is unaware that it has been rolled back.

How to Avoid USN Rollback

To avoid USN rollback, use one of the following procedures:

- Restore AD from a .BKF file instead of a disk image.
- Restore AD from an image of the most **recent** disk that had replicated with the other domain controllers.

You can create a disk image using Norton Ghost.

How to Fix USN Rollback

To correct USN rollback use one of the following procedures:

- Restore AD again, this time using a .BKF file instead of a disk image.
- Restore AD again, this time using the image of the most **recent** disk that had replicated with the other domain controllers.
- Last-ditch recovery method: Run DCPROMO.EXE to demote the domain controller, then re-promote it again. You may need to erase the metadata for the demoted DC before promoting it again. (See the Knowledge Base articles below.)

For more information about USN rollback see the Microsoft Knowledge Base articles "How to detect and recover from a USN rollback in Windows 2000 Server" and "How to detect and recover from a USN rollback in Windows Server 2003".

http://support.microsoft.com/kb/885875
http://support.microsoft.com/kb/875495

Backup Expiration

When restoring a backup file, Active Directory generally requires that the backup file be no more than 60 days old. The limit is 180 days if the AD forest was originally created using Windows Server 2003.

> Your AD recovery plan should require that backups of AD be made at regular intervals, at least monthly (and preferably weekly or daily).
>
> In an emergency situation, UMove can restore an expired backup. However you may encounter problems due to lingering objects (see below).

Lingering Objects

What are Lingering Objects?

If attempt to you restore an backup that is expired, you may encounter problems due to “lingering objects”.

When a DC deletes an object it replaces the object with a **tombstone** object. The tombstone object is a placeholder that represents the deleted object. When replication occurs, the tombstone object is transmitted to the other DCs, which causes them to delete the AD object as well.

Tombstone objects are kept for 60 (or 180) days, after which they are garbage-collected and removed.

If a DC is restored from a backup that contains an object deleted elsewhere, the object will re-appear on the restored DC. Because the tombstone object on the other DCs has been removed, the restored DC will not receive the tombstone object (via replication), and so it will never be notified of the deletion. The deleted object will “linger” in the restored local copy of Active Directory.

How to Remove Lingering Objects

Windows Server 2003 has the ability to manually remove lingering objects using the **repadmin** console utility from the Windows Server 2003 Support Tools, located on the Windows Server CD. Use the option **/removelingeringobjects**. See below for more information.

For more information on lingering objects and how to remove them, see “Outdated Active Directory objects generate event ID 1988 in Windows Server 2003” and the topic “Lingering Object Removal” in the TechNet white paper *How the Active Directory Replication Model Works*.

http://support.microsoft.com/kb/870695
http://technet2.microsoft.com/windowsserver/en/library/1465D773-B763-45EC-B971-C23CDC27400E1033.mspx

Administrator Password Recovery

Good security practices dictate that you change passwords regularly, especially passwords for privileged accounts. You can use Group Policy to enforce a password-change policy, requiring passwords to be changed at a regular interval. (When enabled the default is 42 days.)

If you restore AD from a backup made prior to the last password change, it is possible that you may no longer remember the old Domain Administrator password in the restored database.

To avoid being “locked out” your AD recovery plan should arrange to record the prior passwords for the Domain Administrator account, going at least as far back as your AD backups.

> If you forget the old Domain Admin password UMove can overwrite it during the restore process. The account will be re-enabled if necessary.

Conclusion

Active Directory is a critical component for implementing your organization's computer security policy in a Microsoft Windows environment. Every organization, large and small, should have a plan in place for recovering Active Directory.

Your recovery plan should consider and explore possible types of failure (hardware, administrative error, network disconnection) and analyze the necessary tradeoffs between reliability versus cost in recovering from each type of failure. Preventative steps (for example, offline testing) should be included in your plan where practical. This is especially important to avoid the need for forest-level recovery.