

# Active Directory

**Databáze**

**Obnova smazaných objektů**

**Disaster Recovery (zotavení z havárie)**

Jan Žák

**Microsoft**  
**CERTIFIED**  
*Trainer*

Systems Administration  
Systems Engineering

- Disaster Recovery je sada procesů a postupů spojených s obnovením provozu služeb, které jsou pro organizaci klíčové.
- Risk Assessment – vyhodnocení rizik.

**Co je „Disaster Recovery“?**

- Výpadek služeb (DNS, AD DS...)
- Selhání trustů mezi doménami
- Nedostupnost FSMO
- Smazání nebo poškození objektů
- Selhání řadiče domény
- Ztráta celého forestu
- Selhání replikace (data, SYSVOL)
- Poškození GPO
- USN rollback
- Lingering objects
- Napadení a kompromitace řadiče domény
- Duplicitní SIDy
- Virová nákaza klientů nebo serverů
- ...

**Mám repliky na různých řadičích,  
co se může stát?**

- Používejte kvalitní hardware, provádějte pravidelně testy.
- Všechny změny testujte na testovacím prostředí.
- Připravte, otestujte a nacvičte scénáře obnovy.
- Provádějte Risk assesment (najděte např. „single points of failure“).
- Používejte dodatečné DC.
- Zálohujte před každou změnou.
- Zálohujte po každé změně.
- Plánujte exporty objektů např. do .ldf nebo csv. souborů.
- Nespolehejte jen na jeden způsob obnovy.

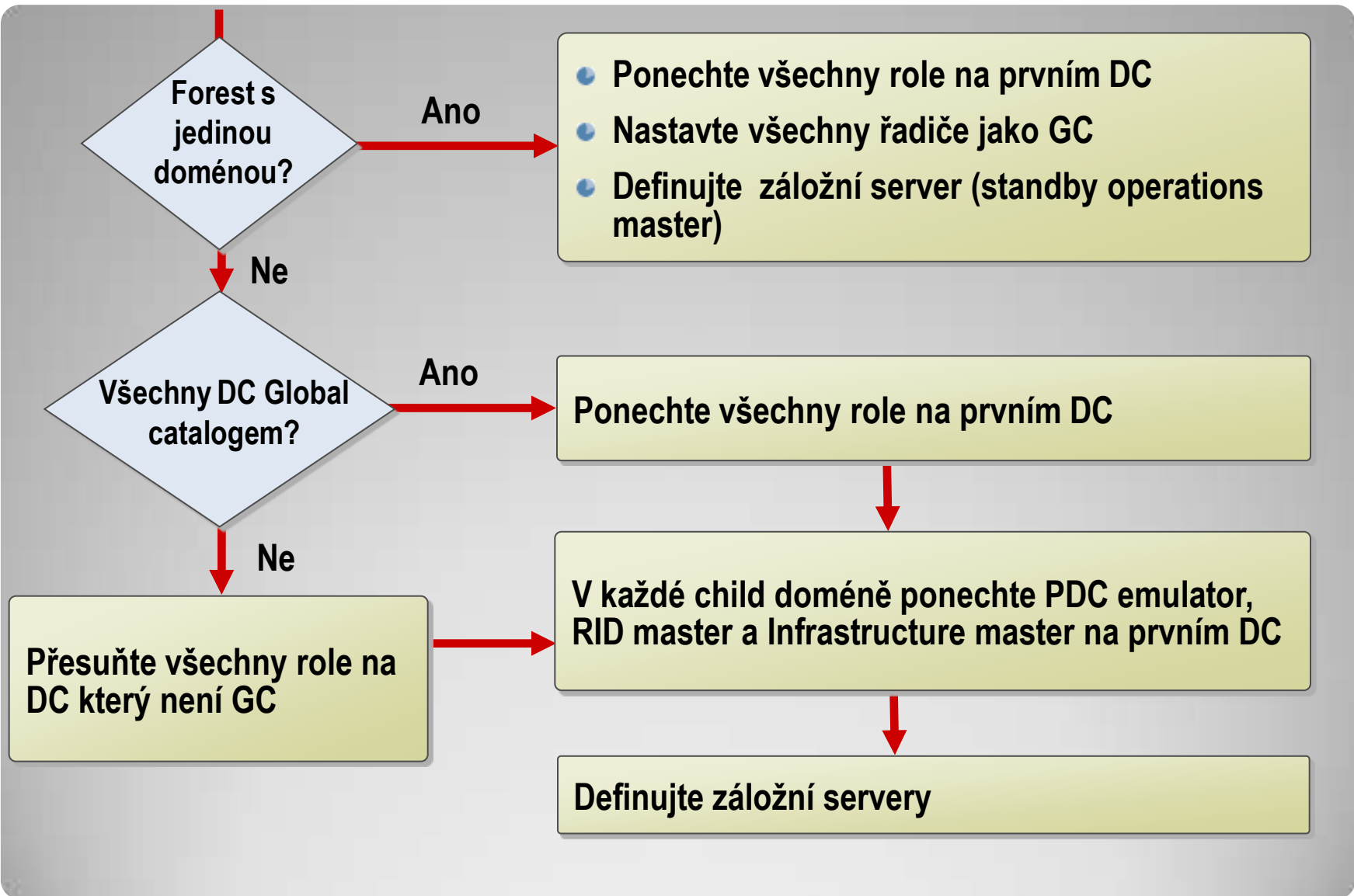
## Před obnovou



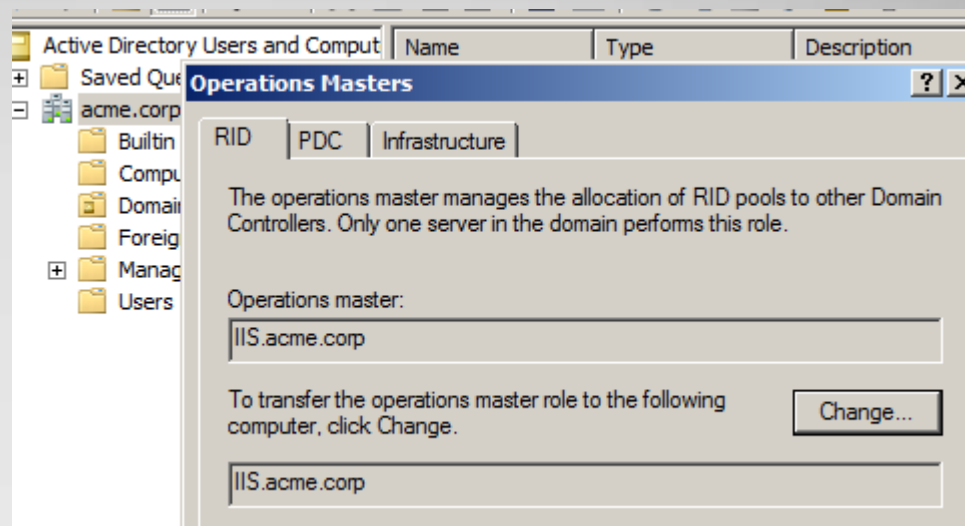
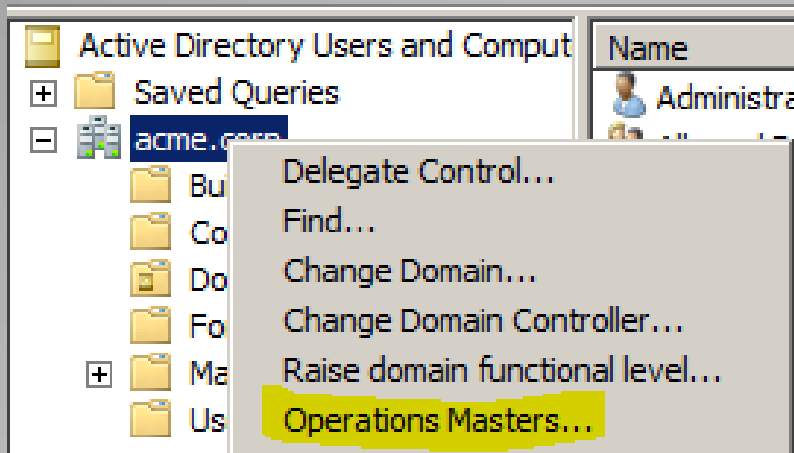
# FSMO

Active Directory Disaster Recovery

- Schema Master
- Domain Naming Master
- PDC Emulator
- RID Master
- Infrastructure Master



# Možný návrh rozmístění FSMO



## Seizing/transfer role: GUI



```
c:\WINDOWS>ntdsutil
activate instance ntds
ntdsutil:roles
fsmo maintenance:connections
server connections:connect to server <server>
server connections: q
fsmo maintenance:
  ◦ Seize domain naming master
  ◦ Seize infrastructure master
  ◦ Seize PDC
  ◦ Seize RID master
  ◦ Seize schema master
```

**Seizing/transfer role: NTDSUTIL**

| <b>FSMO</b>           | <b>Možné dopady</b>  |
|-----------------------|--|
| <b>Schema</b>         | Schéma není možné rozšířit. Krátkodobě obvykle nebývá problém, všechny DC mají repliku.  |
| <b>Domain Naming</b>  | Nelze přidat nebo odebrat doménu. Krátkodobě není problém.   |
| <b>RID</b>            | Řadiče mohou vytvářet nové objekty, dokud mají k dispozici nepřidělené RIDy. Nové objekty je možné přidávat i na jiných řadičích, doba akceptovatelného výpadku závisí na počtu přidávaných objektů. |
| <b>PDC Emulator</b>   | Je třeba řešit rychle. NT 4.0 BDCs nelze replikovat, přestává fungovat synchronizace času, mohou se vyskytnout problémy s GPO a změnami hesel uživatelů a počítačů.                                  |
| <b>Infrastructure</b> | Členství ve skupinách nemusí být aktuální. Není problém v prostředí s jedinou doménou.   |

**Pokud není k dispozici FSMO**

| FSMO Role      | Restrictions                  |
|----------------|-------------------------------|
| Schema         | Original must be reinstalled  |
| Domain Naming  |                               |
| RID            |                               |
| PDC Emulator   | Can transfer back to original |
| Infrastructure |                               |

| FSMO Role      | Administrator must be a member of |
|----------------|-----------------------------------|
| Schema         | Schema Admins                     |
| Domain Naming  | Enterprise Admins                 |
| RID            | Domain Admins                     |
| PDC Emulator   |                                   |
| Infrastructure |                                   |

- Při výpadku musí být k dispozici účet s dostatečnými oprávněními.
- Je vhodné předem znát nejvhodnější server (návrh replikace...).

## Oprávnění pro přesun rolí

```
C:\>repadmin /showvector
dc=whitepaper,dc=corp,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
```

- Protože SYD01 byl původní operation master, zajímají nás pouze USN (Update Sequence Number) pro tento server.
- USN na SYD02 (4023) je vyšší než USN na MEL01 (4018), proto má SYD02 novější verzi dat než MEL01 a je proto vhodnějším kandidátem na přesun role.

**Nejlepší server pro seizing je...**



# Zálohování a obnovování

Active Directory Disaster Recovery

- **Rebuild (reinstalace)**
  - reinstalace OS, povýšení serveru na DC, replikace
  - 😊 Přibližná doba obnova i výsledek jsou známy
- **Restore (obnovení)**
  - Použití zálohy pro obnovu použitelného stavu systému, ruční oprava konfigurace, replikace
- **Repair (oprava)**
  - Použití NTDSUTIL (ESENTUTIL) pro obnovu databáze, kontrola integrity
  - 😞 Obvykle poslední možnost, neznáme dobu obnovy ani výsledek

## Možnosti oprav

- **Primary restore**

Prostředí s jediným DC, nebo ztráta všech DC. Změny provedené po poslední záloze jsou ztraceny.

- **Normal restore**

Prostředí s existujícími replikami, obnovujeme systém, ne smazané objekty. Obnovené objekty jsou při první replikaci aktualizovány.

- **Authoritative restore**

Všechny objekty AD jsou obnoveny ze zálohy. Vybrané objekty jsou označeny pro autoritativní obnovení – zvýší se jejich USN. Při první replikaci tyto objekty přepíše verze na ostatních řadičích, neoznačené objekty jsou naopak aktualizovány z kopií replikačních partnerů.

## Možnosti obnovy ze zálohy

```
C:\Windows\system32>ntdsutil
ntdsutil: activate instance ntds
Active instance set to "ntds".
ntdsutil: set dsrm password
Reset DSRM Administrator Password: reset
password on server null
Please type password for DS Restore Mode
Administrator Account: ****
Please confirm new password: ****
Password has been set successfully.

Reset DSRM Administrator Password:quit
```

**Resetování hesla pro nouzové  
obnovení – „DSRM password“**



Import - OpenOffice.org Calc

Šoubor Úpravy Zobrazit Vložit Formát Nástroje Data Okno Nápověda

Arial 10 B / U

C41 f(x) Σ =

|   | A  | B              | C                       | D               | E          | F                  | G           |
|---|--|----------------|-------------------------|-----------------|------------|--------------------|-------------|
| 1 | dn   | sAMAccountName | userPrincipalName       | telephoneNumber | department | userAccountControl | objectClass |
| 2 | CN=Amie Baldwin,OU=ImportOU,DC=netdom,DC=ncm     | amieb          | amieb@netdom.ncm.cz     | 555-1234        |            | 512                | user        |
| 3 | CN=Scott Culp,OU=ImportOU,DC=netdom,DC=ncm       | scottc         | scottc@netdom.ncm.cz    | 555-1236        | Ucetni     | 512                | user        |
| 4 | CN=Derek Graham,OU=ImportOU,DC=netdom,DC=ncm     | derekg         | derekg@netdom.ncm.cz    | 555-1239        | Ucetni     | 512                | user        |
| 5 | CN=Stephanie Bourne,OU=ImportOU,DC=netdom,DC=ncm | stephanie      | stephanie@netdom.ncm.cz | 555-1238        | Ucetni     | 512                | user        |
| 6 | CN=Matthew Dunn,OU=ImportOU,DC=netdom,DC=ncm     | mattdunn       | mattdunn@netdom.ncm.cz  | 555-1237        | Ucetni     | 512                | user        |
| 7 | CN=Sherri Hart,OU=ImportOU,DC=netdom,DC=ncm      | sherrih        | sherrih@netdom.ncm.cz   | 555-1235        | Ucetni     | 512                | user        |

dn: CN=Jane Doe,OU=Staff,DC=microsoft,DC=com  
 changetype: modify  
 replace: extensionAttribute1  
 extensionAttribute1: Staff  
 -

dn: CN=John Doe,OU=Staff,DC=microsoft,DC=com  
 changetype: modify  
 replace: extensionAttribute1  
 extensionAttribute1: Staff

```
ldifde -f exportOu.ldf -s Server1 -d "dc=Export,dc=com" -
p subtree
-r "(objectCategory=organizationalUnit)" -l
"cn,objectclass,ou"
```

# Export informací o objektech

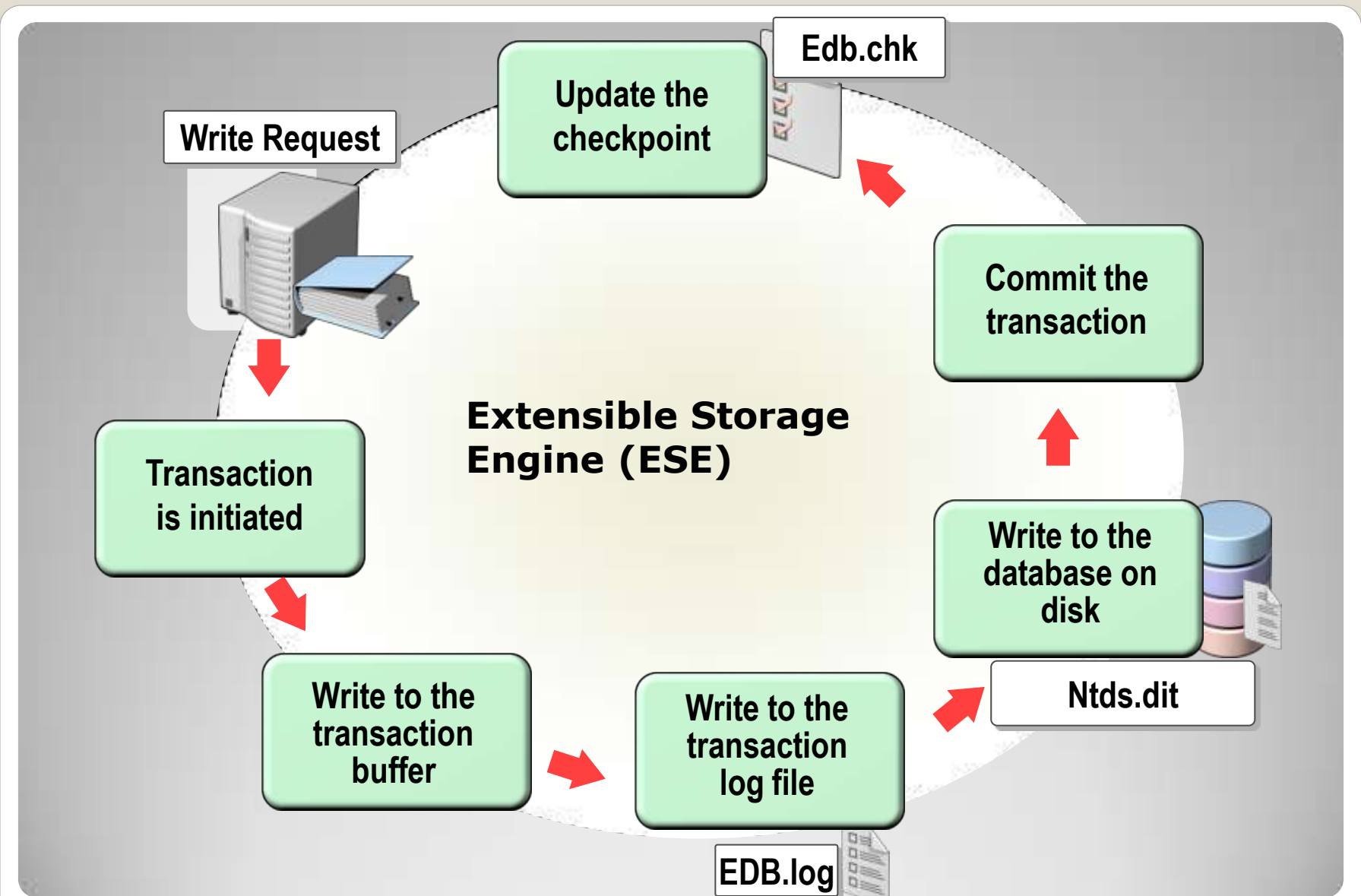
- **repladmin /options *ServerName*  
+DISABLE\_INBOUND\_REPL**
- **repladmin /options *ServerName*  
+DISABLE\_OUTBOUND\_REPL**

**Zákaz replikace**



# Databáze AD

Active Directory Disaster Recovery



## Modifikace dat v databázi AD

- Online defragmentace se spouští na každém DC každých 12 hodin jako součást procesu „garbage-collection“.
- Online defragmentace pouze optimalizuje, nezmenšuje velikost databáze.
- Offline defragmentace obvykle nebývá zapotřebí, vytvoří novou, kompaktní databázi.

**Defragmentace databáze  
(ntds.dit)**

```
C:\Windows\system32>net stop ntds
C:\Windows\system32>ntdsutil
ntdsutil: activate instance ntds
Active instance set to "ntds".
ntdsutil: files
file maintenance: compact to C:\NTDS_TEMP
Initiating DEFRAGMENTATION mode...
Source Database: C:\Windows\NTDS\ntds.dit
Target Database: C:\NTDS_TEMP\ntds.dit
```

**Defragmentation Status (% complete)**

```
0 10 20 30 40 50 60 70 80 90 100
|----|----|----|----|----|----|----|----|----|----|
.....
```

**It is recommended that you immediately perform a full backup of this database. If you restore a backup made before the defragmentation, the database will be rolled back to the state it was in at the time of that backup.**

**Compaction is successful. You need to:**  
copy "C:\NTDS\_TEMP\ntds.dit" "C:\Windows\NTDS\ntds.dit"  
and delete the old log files:  
del C:\Windows\NTDS\\*.log

## **Offline defragmentace ntds.dit**

- set path <object> <location/folder>
  - backup
  - database
  - logs
  - working directory

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters

- move db to <path>
- move logs to <path>

## Umístění a přesun databáze

**LSASS.EXE - System Error, security accounts manager initialization failed because of the following error: Directory Services cannot start. Error status 0xc00002e1.**

**Please click OK to shutdown this system and reboot into directory services restore mode, check the event log for more detailed information.**

- **Event ID: 700**  
**Description: "NTDS (260) Online defragmentation is beginning a pass on database NTDS.DIT."**
- **Event ID: 701**  
**Description: "NTDS (268) Online defragmentation has completed a full pass on database 'C:\WINNT\NTDS\ntds.dit'."**
- **Event ID: 101**  
**Description: "NTDS (260) the database engine stopped."**
- **Event ID: 1004**  
**Description: "The directory was shut down successfully."**
- **Event ID: 1168**  
**Description: "Error: 1032 (ffffbf8) has occurred. (internal ID 4042b). Please contact Microsoft product support services for assistance."**
- **Event ID: 1103**  
**Description: "The windows directory services database could not be initialized and returned error 1032. Unrecoverable error, the directory can't continue."**

**Poškození databáze ☹**



- NTFS práva? (root, ntds)
- Změna písmen disků?
- NTDS.DIT je opravdu poškozena?
- NTDS složka je zkomprimována?

TIP: NTDSUTIL – files – info

**Před opravou db**

- Příkazem **integrity** lze detekovat poškození databáze na binární úrovni (nízko úrovně).  
**Integrity** čte jednotlivé bajty datového souboru  
→ časově náročná operace.
- **Integrity** také kontroluje správnost hlaviček, konzistenci a funkčnost jednotlivých tabulek.  
Kontrola se provádí offline a výstup je zapsán do logu.

**Integrity check (ntdsutil)**

- **Kontrola počtu odkazů (Reference count check).** Počítá všechny odkazy z datové tabulky a porovnává s uvedeným počtem záznamů (viz Active Directory Data Storage in the Distributed Systems Guide of the [Windows 2000 Resource Kit](#).) Toto také zajistí, že každý objekt má GUID, DN a nenulový počet odkazů.
- **Kontrola smazaných objektů (Deleted object check).** Kontrola přítomnosti data a času smazání, kontrola přítomnosti speciálního DN.
- **Kontrola předchůdců (Ancestor check).** Kontrola aktuálního počtu „distinguished name tag (DNT)” – musí odpovídat počty v seznamech aktuálního objektu a jeho předchůdců.
- **Kontrola popisovačů zabezpečení (Security descriptor check).** Kontrola platného popisovače a jeho polí, přítomnost ACE.
- **Kontrola replikací (Replication check).** Kontrola „UpToDate vektorů” pro hlavičky directory partition – musí odpovídat počet kurzorů. Každý objekt také musí obsahovat vektor metadat.

## Semantic check (ntdsutil)

- DSRM, run NTDSUTIL – files – integrity
- semantic database analysis - go
- semantic database analysis - go fixup
- Offline defragmentace
- Pokud je k dispozici další DC, odinstalace AD DS, nové povýšení na DC
- Pokud není k dispozici další DC, obnova z poslední zálohy
- Znovuvytvoření domény, ... ☹️

**Check/fix ntds.dit**

- DSRM, NTDSUTIL – files - recover (nebo repair)  
nebo
- esentutl /f <path> \ntds.dit (nebo esentutl /p)
- smazání (záloha) \*.log souborů
- Import chybějících objektů z .ldf souborů

**Recover/repair databáze**



# Odstraňování objektů

Active Directory Disaster Recovery

- Když je objekt smazán, není odstraněn z databáze.
- Objekt je po smazání označen pro pozdější odstranění.
- Tento příznak je replikován na ostatní řadiče. Teprve později je proces garbage collection fyzicky odstraní z databáze.
- Tyto objekty jsou nazývány „*tombstones*“.
- Garbage collection také maže nepotřebné logy.
- Následně proces spustí vlákno defragmentace.

**Jak jsou mazány objekty z AD**

- Po změně objektu na „tombstone“ jsou téměř všechny atributy odebrány.
- Zůstávají pouze objectGUID, objectSid, nTSecurityDescriptor, uSNChanged, sIDHistory.
- Další atributy mohou být také ponechány, je ale potřeba hrubší zásah do konfigurace schématu.

**Po smazání objektu**



- tombstonelifetime  
(cn=DirectoryServices,cn=WindowsNT,cn=Services,cn=Configuration,dc=)

Pozn.:( <not set> znamená 60 dnů), W2003 SP1 zvýšil TLS z výchozích 60ti na 180 dnů

```
C:\>dsquery * "CN=Directory Service,CN=Windows NT,  
CN=Services,CN=Configuration,DC=acme,DC=corp" -  
scope base -attr tombstonelifetime
```

```
tombstonelifetime  
180
```

# Tombstone lifetime (TLS)

- Obnova poslední zálohy stavu systému obsahující objekt, označení objektu pro „authoritative restore“.
- Nalezení řadiče, na který ještě nebylo smazání replikováno, označení objektu jako autoritativní verze.
- Odstranění atributu „isDeleted“, změna DN objektu, obnovení atributů např. z exportního souboru CSV.
- Integrace nástroje od jiného dodavatele.

## **Postup při obnovení objektu (bez Recycle Bin)**

- Authoritative restore
- LDF
- LDP.EXE
- ADRESTORE.EXE
- „Lag DC“
- AD snapshot
- „Recycle Bin“ (pouze W 2008 R2)
- Další nástroje třetích stran

**Nástroje pro obnovení smazaných objektů**

- Ochrana „OU=MyCompany“ přidáním DENY ACE (DELETE CHILD) pro skupinu Everyone – s „This object only“:

### **DSACLS**

```
"OU=MyCompany,DC=CONTOSO,DC=COM" /D  
"EVERYONE:DC"
```

Pro OU=Users: DENY ACE pro Everyone s „DELETE“ a „DELETE TREE“ – s „This object only“:

### **DSACLS**

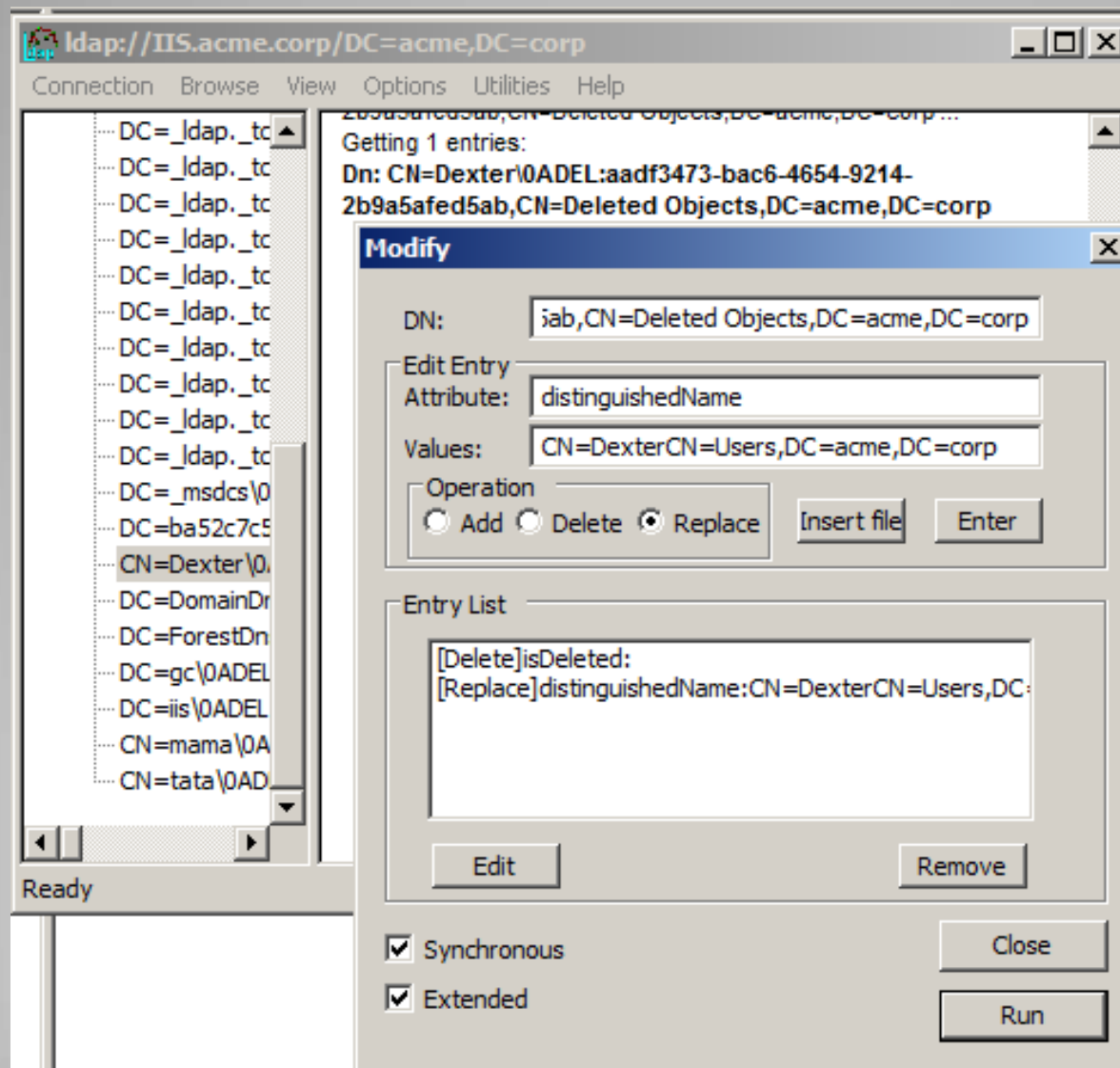
```
"OU=Users,OU=MyCompany,DC=CONTOSO,DC=COM" /D "EVERYONE:SDDT"
```

POZN. totéž jako „**Protect object from accidental deletion**“ ve Win 2008

# Ochrana objektu před odstraněním

- Funkce
  - Provádí online zálohu AD
  - Plán automatických záloh
- Backup life = hodnota tombstonelifetime
  - Default = 180 dnů
  - Změna hesla počítače = 30 dnů
  - Password history = 2 (aktuální a předcházející)
  - Použitelnost zálohy = TLS nebo 2\*změna hesla počítače
  - Aplikování staré zálohy může obnovit již smazané objekty
- Schema rollback není podporován !!!

## Windows Server Backup



**Rychlá obnova smazaného objektu**

Denied RODC Password Replication G... Security Group ... Members in this group can...  
Dexter Morgan User

Administrator: Command Prompt - ntdsutil

```
C:\Windows\system32>ntdsutil
ntdsutil: activate instance ntds
Active instance set to "ntds".
ntdsutil: snapshot
snapshot: create
Creating snapshot...
Snapshot set <29f83343-7274-46a5-baf7-0cbab5f3b08c> generated successfully.
snapshot:
```

Administrator: Command Prompt - ntdsutil

```
snapshot: list all
1: 2011/11/06:17:34 <29f83343-7274-46a5-baf7-0cbab5f3b08c>
2: C: <93837136-f0da-4a80-9413-e878e4ff5fba>

snapshot: mount 1
Snapshot <93837136-f0da-4a80-9413-e878e4ff5fba> mounted as C:\$SNAP_201111061734_
_VOLUMEC$\
snapshot:
```

Local Disk (C:)

Computer > Local Disk (C:) Search Local Disk (C:)

Organize > Share with > New folder

★ Favorites

Desktop

Downloads

Name ^

Date modified

Type

\$SNAP\_201111061734\_VOLUMEC\$

11/6/2011 5:35 PM

File folder

inetpub

10/30/2011 4:35 PM

File folder

# Snapshot AD - vytvoření

```
Administrator: Command Prompt - dsamain -dbpath "C:\NTDS_TEMP\ntds.dit" -ldapport 10389 -allow...
c:\>dsamain -dbpath "C:\NTDS_TEMP\ntds.dit" -ldapport 10389 -allowupgrade
EUEVENTLOG (Informational): NTDS General / Service Control : 1000
Microsoft Active Directory Domain Services startup complete, version 6.1.7600.16385
```

The screenshot shows two windows: 'Active Directory Users and Computers' and 'ADSI Edit'. The 'ADSI Edit' window is open to a snapshot of the 'acme.corp' domain. The 'CN=Users' container is selected, showing a list of users. The 'CN=Dexter Morgan' user is highlighted. A 'CN=Dexter Morgan Properties' dialog box is open, showing the 'Security' tab with a table of attributes.

| Name                         | Class | Distinguished Name          |
|------------------------------|-------|-----------------------------|
| CN=Administrator             | user  | CN=Administrator,CN=Users   |
| CN=Allowed RODC Password ... | group | CN=Allowed RODC Passwor...  |
| CN=Cert Publishers           | group | CN=Cert Publishers,CN=Us... |
| CN=Denied RODC Password ...  | group | CN=Denied RODC Passwor...   |
| CN=Dexter Morgan             | user  | CN=Dexter Morgan,CN=Us...   |
| CN=DnsAdmins                 | group | CN=DnsAdmins,CN=Users,      |

| Attribute             | Value                                    |
|-----------------------|--|
| accountExpires        | (never)                                  |
| badPasswordTime       | (never)                                  |
| badPwdCount           | 0  |
| cn                    | Dexter Morgan                            |
| codePage              | 0  |
| countryCode           | 0  |
| displayName           | Dexter Morgan                            |
| distinguishedName     | CN=Dexter Morgan,CN=Users,DC=acme,DC=... |
| dSCorePropagationD... | 0x0 = ( )                                |

# Obnova atributů ze snaphsotu



Recovery Wizard

## Select Recovery Type

Getting Started  
Select Backup Date  
**Select Recovery Type**  
Select Location for Sys...  
Confirmation  
Recovery Progress

What do you want to recover?

- Files and folders  
You can browse volumes included in this backup and select files and folders.
- Volumes  
You can restore an entire volume.
- Applications  
You can recover applications that were installed on the system.
- System state  
You can restore just the system state.

Getting Started  
Select Backup Date  
Select Recovery Type  
**Select Location for Sys...**  
Confirmation  
Recovery Progress

[More about performing recoveries](#)

< Prev


Recovery Wizard

## Select Location for System State Recovery

Where do you want to recover the system state of this Active Directory backup to?

- Original location  
This option restores the system state. You must restart your computer at the end of the recovery operation.  
 Perform an authoritative restore of Active Directory files.  
This recovery option will reset all replicated content on this Domain Controller including SYSVOL. Other replicated folders on this server will also be affected by this recovery.
- Alternate location  
This option copies the system state as a set of files to the location specified.
- Restore as Install From Media (IFM) files  
Select this checkbox if you are using the IFM feature to copy the system state files to install an Active Directory.

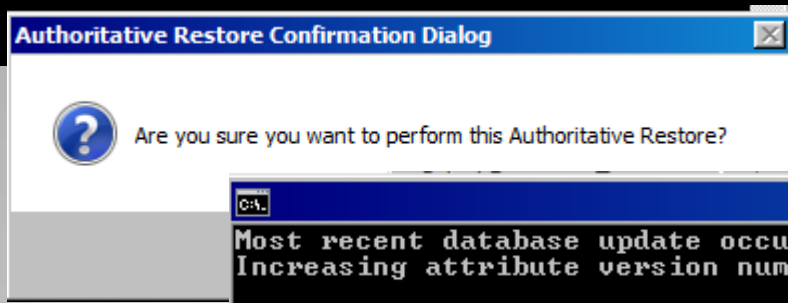
Windows Server Backup

 Note: This recovery option will cause all replicated content on the local server to re-synchronize after recovery. This may cause potential latency or outage issues.

OK

# Authoritative restore – obnovení stavu systému

```
c:\>ntdsutil
ntdsutil: activate instance ntds
Active instance set to "ntds".
ntdsutil: authoritative restore
authoritative restore: restore object "CN=Dexter,CN=Users,DC=acme,DC=corp"
```



```
Most recent database update occurred at 11-06-11 21:32.32.
Increasing attribute version numbers by 100000.

Counting records that need updating...
Records found: 0000000001
Done.

Found 1 records to update.

Updating records...
Records remaining: 0000000000
Done.

Successfully updated 1 records.

The following text file with a list of authoritatively restored objects has been
created in the current working directory:
    ar_20111106-222800_objects.txt
None of the specified objects have back-links in this domain. No link restore fi
le has been created.

Authoritative Restore completed successfully.
```

## Authoritative restore – obnovení objektu

```
Administrator: Active Directory Module for Windows PowerShell
PS C:\Users\Administrator> Get-ADOptionalFeature -filter *

DistinguishedName      : CN=Recycle Bin Feature,CN=Optional Features,CN=Directory S
                        ervice,CN=Windows NT,CN=Services,CN=Configuration,DC=train
                        ing,DC=local
EnabledScopes           : {}
FeatureGUID            : 766ddcd8-acd0-445e-f3b9-a7f9b6744f2a
FeatureScope           : {ForestOrConfigurationSet}
IsDisableable          : False
Name                   : Recycle Bin Feature
ObjectClass             : msDS-OptionalFeature
ObjectGUID             : 8e44013a-74ad-447d-a343-772b2763f50b
RequiredDomainMode     :
RequiredForestMode     : Windows2008R2Forest
```

```
Administrator: Active Directory Module for Windows PowerShell
PS C:\Users\Administrator> Enable-ADOptionalFeature 'Recycle Bin Feature' -scope-
ForestOrConfigurationSet -target training.local
WARNING: Enabling 'Recycle Bin Feature' on
'CN=Partitions,CN=Configuration,DC=training,DC=local' is an irreversible
action! You will not be able to disable 'Recycle Bin Feature' on
'CN=Partitions,CN=Configuration,DC=training,DC=local' if you proceed.

Confirm
Are you sure you want to perform this action?
Performing operation "Enable" on Target "Recycle Bin Feature".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help
(default is "Y"):y
PS C:\Users\Administrator>
```

## Recycle Bin (Windows 2008 R2) – aktivace

```
Administrator: Active Directory Module for Windows PowerShell
PS C:\Users\Administrator> Get-ADObject -SearchBase "CN=Deleted Objects,DC=training,DC=local" -ldapFilter "(objectClass=user)" -includeDeletedObjects

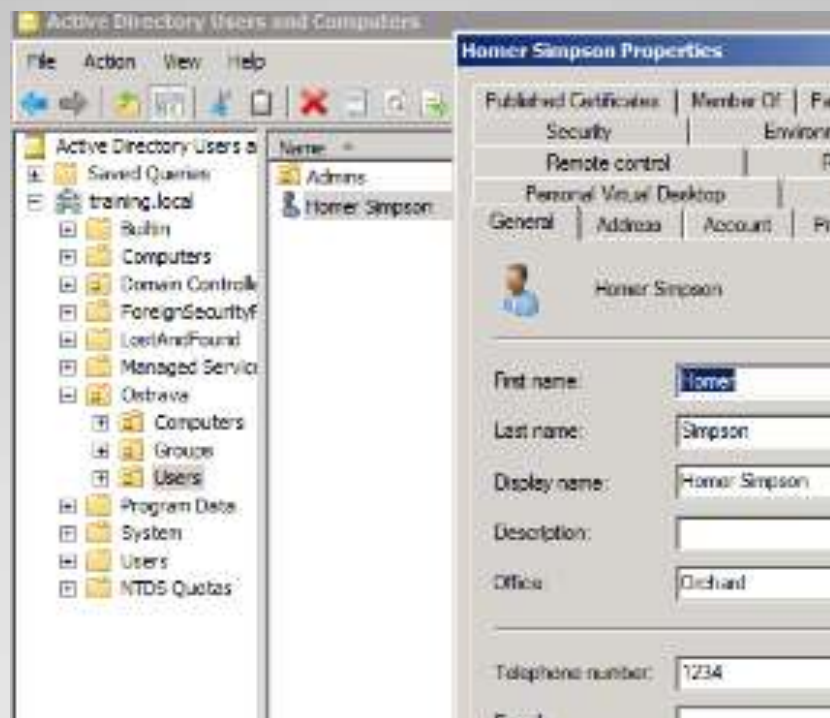
Deleted                : True
DistinguishedName      : CN=Homer Simpson\0ADEL:1f80c62d-6d61-4668-8acb-11dbb58d0024
                        ,CN=Deleted Objects,DC=training,DC=local
Name                   : Homer Simpson
                        DEL:1f80c62d-6d61-4668-8acb-11dbb58d0024
ObjectClass            : user
ObjectGUID             : 1f80c62d-6d61-4668-8acb-11dbb58d0024
```

```
Administrator: Active Directory Module for Windows PowerShell
PS C:\Users\Administrator> Get-ADObject -filter (Name -like "*Homer Simpson*") -
SearchScope Subtree -includeDeletedObjects

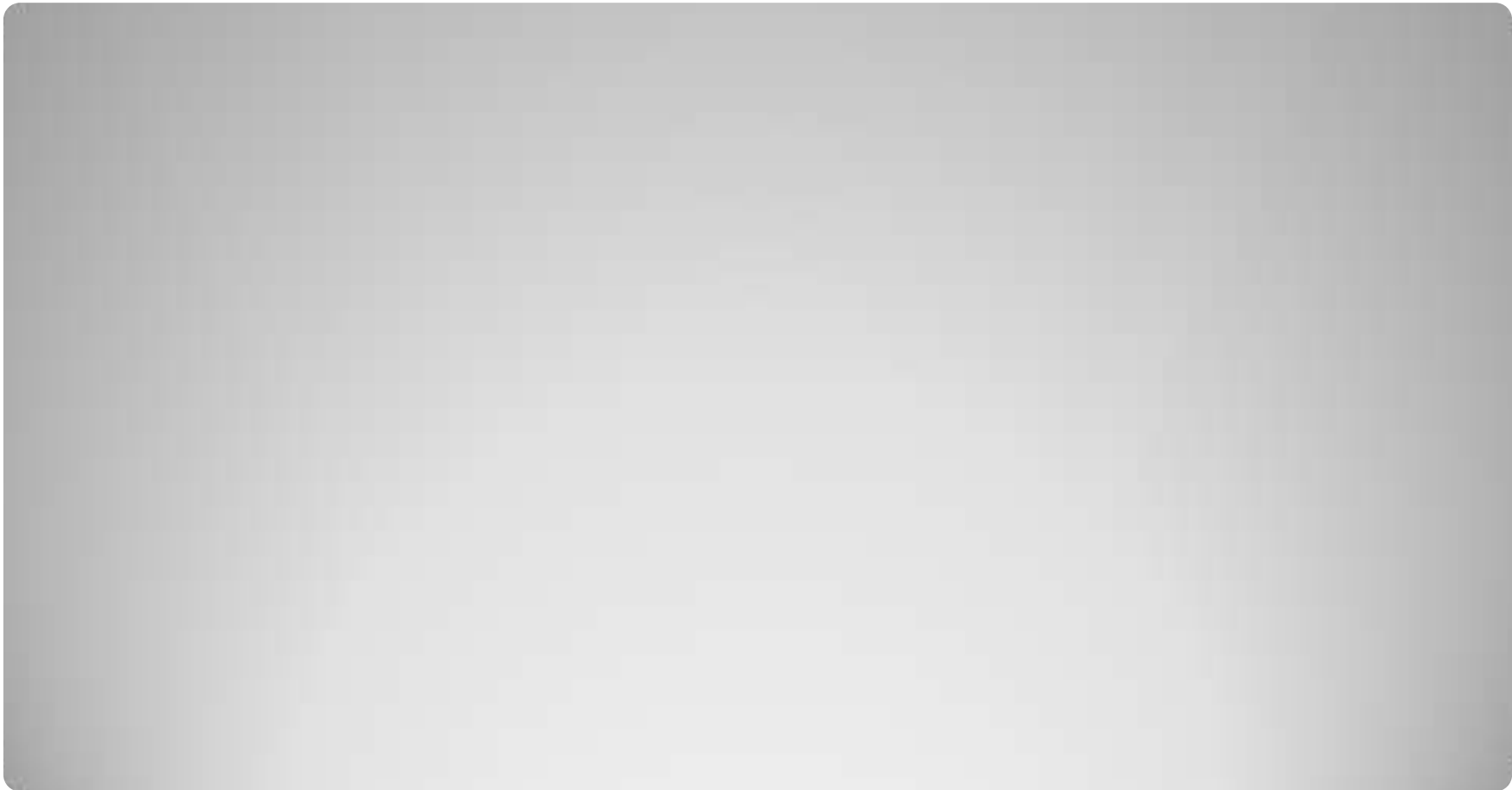
Deleted                : True
DistinguishedName      : CN=Homer Simpson\0ADEL:1f80c62d-6d61-4668-8acb-11dbb58d0024
                        ,CN=Deleted Objects,DC=training,DC=local
Name                   : Homer Simpson
                        DEL:1f80c62d-6d61-4668-8acb-11dbb58d0024
ObjectClass            : user
ObjectGUID             : 1f80c62d-6d61-4668-8acb-11dbb58d0024
```

## Recycle Bin – vyhledání objektu

```
Administrator: Active Directory Module for Windows PowerShell
PS C:\Users\Administrator> Restore-ADObject -Identity 1f80c62d-6d61-4668-8acb-11dbb58d0024
PS C:\Users\Administrator>
```



**Recycle Bin – obnovení objektu**



# Lingering objects

Active Directory Disaster Recovery

- When you restore AD from expired backup, deleted objects re-appears (lingers) on restored DC.
- When your DC is offline for longer time (more than TSL period), same thing can happen.
- NOTE: GC replicate read-only replicas with lower priority. GC is often bridgehead → high replication load. When replication interval is too short and many repl. partners, read-only replicas can remain in the queue indefinitely. These conditions can result in lingering objects on global catalog server.

## Lingering objects

Replication problems occur when the object on the source domain controller is updated. In this case, when the destination attempts to inbound-replicate the update, the destination domain controller responds in one of two ways:

- If the destination domain controller has **strict replication consistency enabled**, it recognizes that it cannot update the object and locally halts inbound replication of the directory partition from that source domain controller.
- If the destination domain controller has **strict replication consistency disabled**, it requests the full replica of the updated object. In this case, the object is reintroduced into the directory.

## Lingering objects – STRICT REPLICATION



- **Event ID 1388 or 1988**

Event Type:Error

Event Source:NTDS Replication

Event Category:Replication

Event ID:1388

Date:2/21/2005

Time:9:19:48 AM

User:NT AUTHORITY\ANONYMOUS LOGON

Computer:DC3

Description:

Another domain controller (DC) has attempted to replicate into this DC an object which is not present in the local Active Directory database. The object may have been deleted and already garbage collected (a tombstone lifetime or more has past since the object was deleted) on this DC. The attribute set included in the update request is not sufficient to create the object. The object will be re-requested with a full attribute set and re-created on this DC.

Source DC (Transport-specific network address):

4a8717eb-8e58-456c-995a-c92e4add7e8e.\_msdcs.contoso.com

Object:

CN=InternalApps,CN=Users,DC=contoso,DC=com

Object GUID:

a21aa6d9-7e8a-4a8f-bebf-c3e38d0b733a

Directory partition:

DC=contoso,DC=com

Destination highest property USN:

20510

User Action:

Verify the continued desire for the existence of this object. To discontinue re-creation of future similar objects, the following registry key should be created.

Registry Key:

HKLM\System\CurrentControlSet\Services\NTDS\Parameters\Strict Replication Consistency

# Indications that DC has lingering objects (1a)

- **Event ID 1388 or 1988**

Event Type:Error  
Event Source:NTDS Replication  
Event Category:Replication  
Event ID:1988  
Date:2/21/2005  
Time:9:13:44 AM  
User:NT AUTHORITY\ANONYMOUS LOGON  
Computer:DC3

Description:

Active Directory Replication encountered the existence of objects in the following partition that have been deleted from the local domain controllers (DCs) Active Directory database. Not all direct or transitive replication partners replicated in the deletion before the tombstone lifetime number of days passed. Objects that have been deleted and garbage collected from an Active Directory partition but still exist in the writable partitions of other DCs in the same domain, or read-only partitions of global catalog servers in other domains in the forest are known as "lingering objects".

This event is being logged because the source DC contains a lingering object which does not exist on the local DCs Active Directory database. This replication attempt has been blocked.

The best solution to this problem is to identify and remove all lingering objects in the forest.

Source DC (Transport-specific network address):  
4a8717eb-8e58-456c-995a-c92e4add7e8e.\_msdcs.contoso.com  
Object:  
CN=InternalApps,CN=Users,DC=contoso,DC=com  
Object GUID:  
a21aa6d9-7e8a-4a8f-bebf-c3e38d0b733a

# Indications that DC has lingering objects (1b)

- A deleted user or group account remains in the global address list (GAL) on Exchange servers. Therefore, although the account name appears in the GAL, attempts to send e-mail messages result in errors.
- Multiple copies of an object appear in the object picker or GAL for an object that should be unique in the forest. Duplicate objects sometimes appear with altered names, causing confusion on directory searches. For example, if the relative distinguished name of two objects cannot be resolved, conflict resolution appends "\*CNF:GUID" to the name, where \* represents a reserved character, CNF is a constant that indicates a conflict resolution, and GUID represents the **objectGUID** attribute value.
- E-mail messages are not delivered to a user whose Active Directory account appears to be current. After an outdated domain controller or global catalog server becomes reconnected, both instances of the user object appear in the global catalog. Because both objects have the same e-mail address, e-mail messages cannot be delivered.
- A universal group that no longer exists continues to appear in a user's access token. Although the group no longer exists, if a user account still has the group in its security token, the user might have access to a resource that you intended to be unavailable to that user.
- A new object or Exchange mailbox cannot be created, but you do not see the object in Active Directory. An error message reports that the object already exists.
- Searches that use attributes of an existing object incorrectly find multiple copies of an object of the same name. One object has been deleted from the domain, but it remains in an isolated global catalog server.

## Indications that DC has lingering objects (2)

- If a writable lingering object exists in your environment and an attempt is made to update the object, the value in the **strict replication consistency** registry entry (type REG\_DWORD) in **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters** determines whether replication proceeds or is stopped, as follows:
  - **1** (enabled): Inbound replication of the specified directory partition from the source is stopped on the destination.
  - **0** (disabled): The destination requests the full object from the source domain controller, and the lingering object is revived in the directory as a new object.

**Determine whether lingering objects are replicated**

```
reppadmin /regkey <servername> +strict  
reppadmin /regkey * +strict
```

Note:

This apply on Windows Server 2003 SP1  
only!

**Configuring strict replication with reppadmin**

The object that you create is an operational GUID with the following name:

**CN=94fdebc6-8eeb-4640-80de-ec52b9ca17fa,CN=Operations,CN=ForestUpdates,CN=Configuration,DC=<ForestRootDomain>**

Perform the following procedure on any domain controller in the forest to add this object to the configuration directory partition.

You can use .ldf file:

dn:

CN=94fdebc6-8eeb-4640-80de-ec52b9ca17fa,CN=Operations,CN=ForestUpdates,CN=Configuration,DC=<ForestRootDomain>

changetype: add

objectClass: container

showInAdvancedViewOnly: TRUE

name: 94fdebc6-8eeb-4640-80de-ec52b9ca17fa

objectCategory: CN=Container,CN=Schema,CN=Configuration,DC=<ForestRootDomain>

**Enable strict replication consistency on newly promoted DC's**

- REPADMIN (W2003 version only) can be used with  
**/removelingerobjects**
  - Repadmin compares database objects on reference DC with objects on target DC (which is suspected to contain) lingering objects
  - **/advisory\_mode** only reports (to event log) existing lingering objects

**Example (Event ID 1946):**

Active Directory has identified the following lingering object on the local domain controller in advisory mode. The object had been deleted and garbage collected on the following source domain controller yet still exists on the local domain controller.

Object:

CN=SORCMM1250-HP DeskJet 692C\0ADEL:c809ed02-d78f-4938-9f51-9335ba0776e7,CN=Deleted Objects,DC=am1,DC=mnet

Object GUID:

c809ed02-d78f-4938-9f51-9335ba0776e7

Source domain controller:

12034b03-56a9-47bc-b33d-6ae6a95d1ae7.\_msdcs.mnet

## Removing Lingering Objects

- SET G\_EUDC01=608E585F-4F95-4032-951D-EFB5CE4B4297
  - SET G\_EUDC02=2C100092-82E7-43AE-9739-7E52D4B86054
  - SET G\_EUDC03=74110BF1-03A8-4812-9324-6921BCC8AB1C
  - SET G\_MCCOY=7BA54BCE-B7AA-407F-A463-19F6DF2F442D
  - SET G\_MONROE=5F3376F6-05C2-4C15-9BD6-72455EF5CB4A
  - SET G\_NADC01=748B0EF7-F605-4ADE-A2DC-EF2D4AFC5D36
  - SET G\_NADC02=D33F4A12-099E-4F8F-BC89-1FB422E2B0F3
  - SET G\_APCD02=2D309905-8731-4FAE-8804-6B8A0340DAA0
- 
- rem Naming Context: DC=DomainDnsZones,DC=eu,DC=tieto,DC=com from EUDC01
  - repadmin /removelingeringobjects %computername% G\_EUDC01 "DC=eu,DC=tieto,DC=com" /advisory\_mode pause
- 
- rem Naming Context: DC=tieto,DC=com from MONROE
  - repadmin /removelingeringobjects %computername% G\_MONROE "DC=tieto,DC=com" /advisory\_mode pause
- 
- rem Naming Context: DC=ap,DC=tieto,DC=com from APDC02
  - repadmin /removelingeringobjects %computername% G\_APCD02 "DC=ap,DC=tieto,DC=com" /advisory\_mode pause
- 
- rem Naming Context: DC=NA,DC=tieto,DC=com from NADC02
  - repadmin /removelingeringobjects %computername% G\_NADC02 "DC=NA,DC=tieto,DC=com" /advisory\_mode pause
- 
- rem Naming Context: CN=Configuration,DC=tieto,DC=com from MONROE
  - repadmin /removelingeringobjects %computername% G\_MONROE "CN=Configuration,DC=tieto,DC=com" /advisory\_mode pause
- 
- rem Naming Context: DC=ForestDnsZones,DC=tieto,DC=com from MONROE
  - repadmin /removelingeringobjects %computername% G\_MONROE "DC=ForestDnsZones,DC=tieto,DC=com" /advisory\_mode pause
- 
- rem Naming Context: DC=eu,DC=tieto,DC=com from EUDC01
  - repadmin /removelingeringobjects %computername% G\_EUDC01 "DC=eu,DC=tieto,DC=com" /advisory\_mode pause

To get DC's GUID:  
 repadmin /showrepl <servername>

## Example – lingering objects



- In DSRM, start REGEDIT
- Go to  
„HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\ProductOptions“
- In „**ProductType**“, set „**ServerNT**“ in to Value data
- Restart server and logon with DSRM password
- Computer should behave as member server now
- In  
„HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters“  
delete „**Src Root Domain Srv**“
- Run DCPRMO an install new temporary domain
- Run DCPRMO again and remove temporary domain
- Remove metadata in production domain

**If DC cannot start in normal mode  
(really last option 😊)**

- Odebrání DC
- Odebrání DC z konfigurace po neúspěšném odebrání role AD DS
- Odebrání domény z konfigurace, pokud doména již není dostupná
- Přejmenování DC, domény

**Další postupy (viz odkazy)**



# Recovery Manager for Active Directory Forest Edition (Quest Software)

- Recovery manager for AD Forest Edition (Quest Software)  
<http://www.quest.com/recovery-manager-for-active-directory-forest-edition/>
- Overall Solutions – RecycleBin  
[http://www.overall.ca/index.php?option=com\\_content&view=article&id=40:adrecyclebin&catid=15:adrecyclebinexe&Itemid=64](http://www.overall.ca/index.php?option=com_content&view=article&id=40:adrecyclebin&catid=15:adrecyclebinexe&Itemid=64)
- 4SYSOPS – Recycle Bin PowerPack for PowerGUI  
<http://4sysops.com/archives/free-powergui-active-directory-recycle-bin-powerpack/>
- Removing orphaned domain  
<http://support.microsoft.com/default.aspx?scid=kb;en-us;q230306>
- Renaming domain  
<http://technet.microsoft.com/en-us/windowsserver/bb405948.aspx>  
[http://www.petri.co.il/windows\\_2003\\_domain\\_rename.htm](http://www.petri.co.il/windows_2003_domain_rename.htm)  
[http://dsg.port.ac.uk/~hx/rename\\_domain/index.php](http://dsg.port.ac.uk/~hx/rename_domain/index.php)
- Renaming DC  
<http://technet.microsoft.com/en-us/library/cc782761.aspx>  
[http://www.petri.co.il/windows\\_2003\\_domain\\_controller\\_rename.htm](http://www.petri.co.il/windows_2003_domain_controller_rename.htm)
- DCPROMO – FORCEREMOVAL  
<http://support.microsoft.com/kb/332199>
- Remove FRS a DFS objects if exists after forceremoval  
<http://support.microsoft.com/kb/296183/>
- How to remove data in Active Directory after an unsuccessful domain controller demotion  
<http://support.microsoft.com/kb/216498/en-us>
- How to rebuild the SYSVOL tree and its content in a domain  
<http://support.microsoft.com/kb/315457/en-us>
- Linging objects  
<http://support.microsoft.com/kb/314282>
- <http://technet.microsoft.com/en-us/library/cc738018.aspx>
- <http://technet.microsoft.com/en-us/library/cc785298.aspx>

# Zdroje a odkazy