Active Directory

Databáze
Obnova smazaných objektů
Disaster Recovery (zotavení z havárie)

Jan Žák

Microsoft CERTIFIED Trainer

Systems Administration
Systems Engineering

Co je „Disaster Recovery“?

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

- 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?

Před obnovou

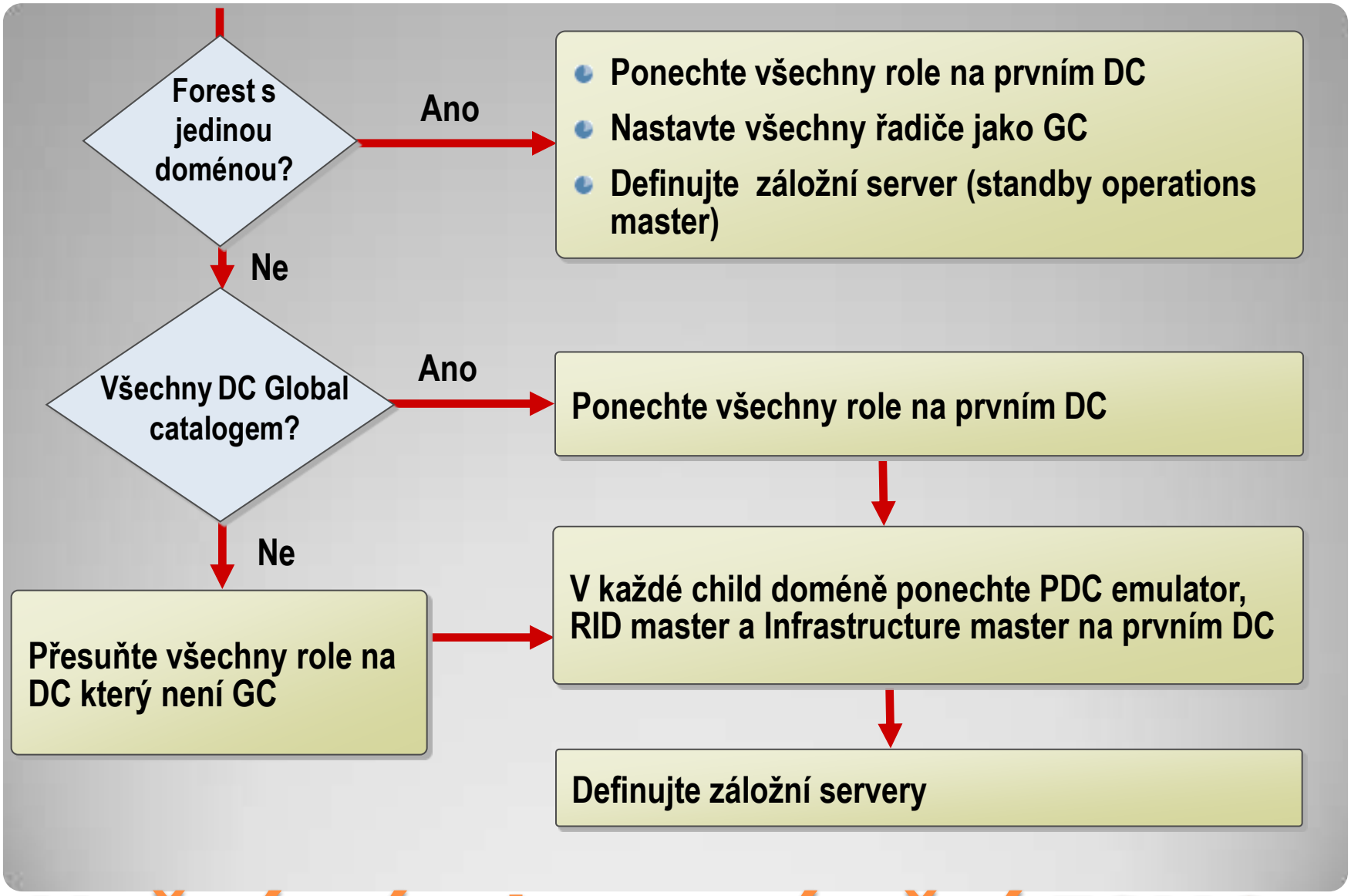
- Používejte kvalitní hardware, provádějte pravidelně testy.
- Všechny změny testujte na testovacím prostředí.
- Připravte, otestujte a nacvičte scénáře obnovy.
- Provádějte Risk assesment (najděte např. „single points of failure“).
- Používejte dodatečné DC.
- Zálohujte před každou změnou.
- Zálohujte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

FSMO

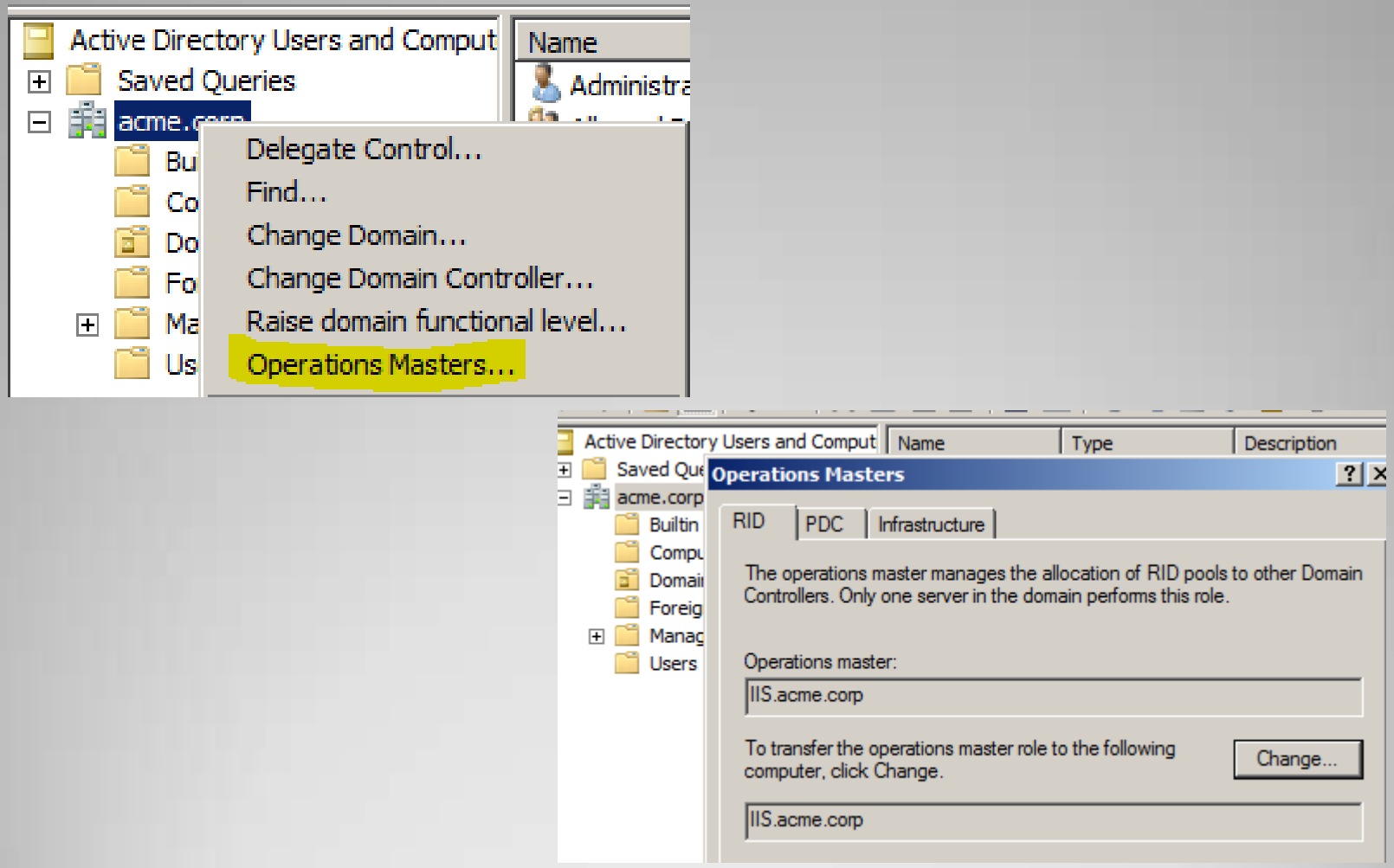
Active Directory Distaster Recovery

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

FSMO



Možný návrh rozmístění FSMO



Seizing/transfer role: GUI

c:\WINDOWS>ntdsutil
activate instance ntds
ntdsutil:roles
fsmo maintanance:connections
server connections:connect to server <server>
server connections: q
fsmo maintanance:

- Seize domain naming master
- Seize infrastructure master
- Seize PDC
- Seize RID master
- Seize schema master

Seizing/transfer role: NTDSUTIL

Pokud není k dispozici FSMO

FSMO	Možné dopady
Schema	Schéma není možné rozšířit. Krátkodobě obvykle nebývá problém, všechny DC mají repliku.
Domain Naming	Nelze přidat nebo odebrat doménu. Krátkodobě není problém.
RID	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.
PDC Emulator	Je třeba řešit rychle. NT 4.0 BDCs nelze replikovat, přestává fungovat synchronizace času, mohou se vyskytnou problémy s GPO a změnami hesel uživatelů a počítačů.
Infrastructure	Členství ve skupinách nemusí být aktuální. Není problém v prostředí s jedinou doménou.

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 Distaster Recovery

Možnosti oprav

- **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 (ESENTUTL) pro obnovu databáze, kontrola integrity
  - ☹ Obvykle poslední možnost, neznáme dobu obnovy ani výsledek

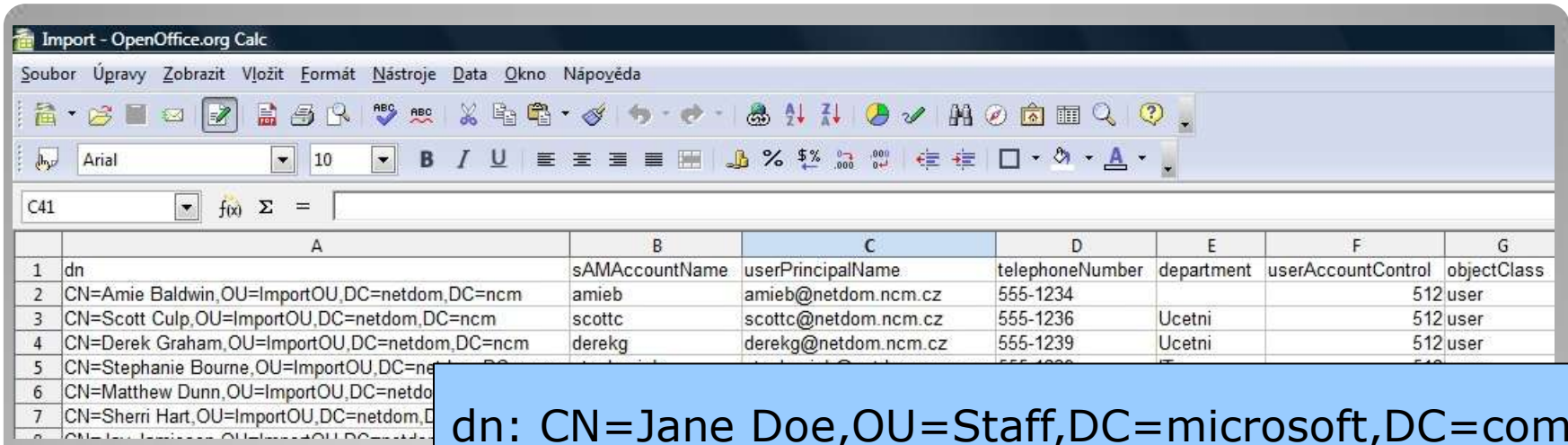
Možnosti obnovy ze zálohy

- **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 přepíší verze na ostatních řadičích, neoznačené objekty jsou naopak aktualizovány z kopií replikačních partnerů.

```
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“



	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=ne						
6	CN=Matthew Dunn,OU=ImportOU,DC=netdo						
7	CN=Sherri Hart,OU=ImportOU,DC=netdom,D						

```
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"
```

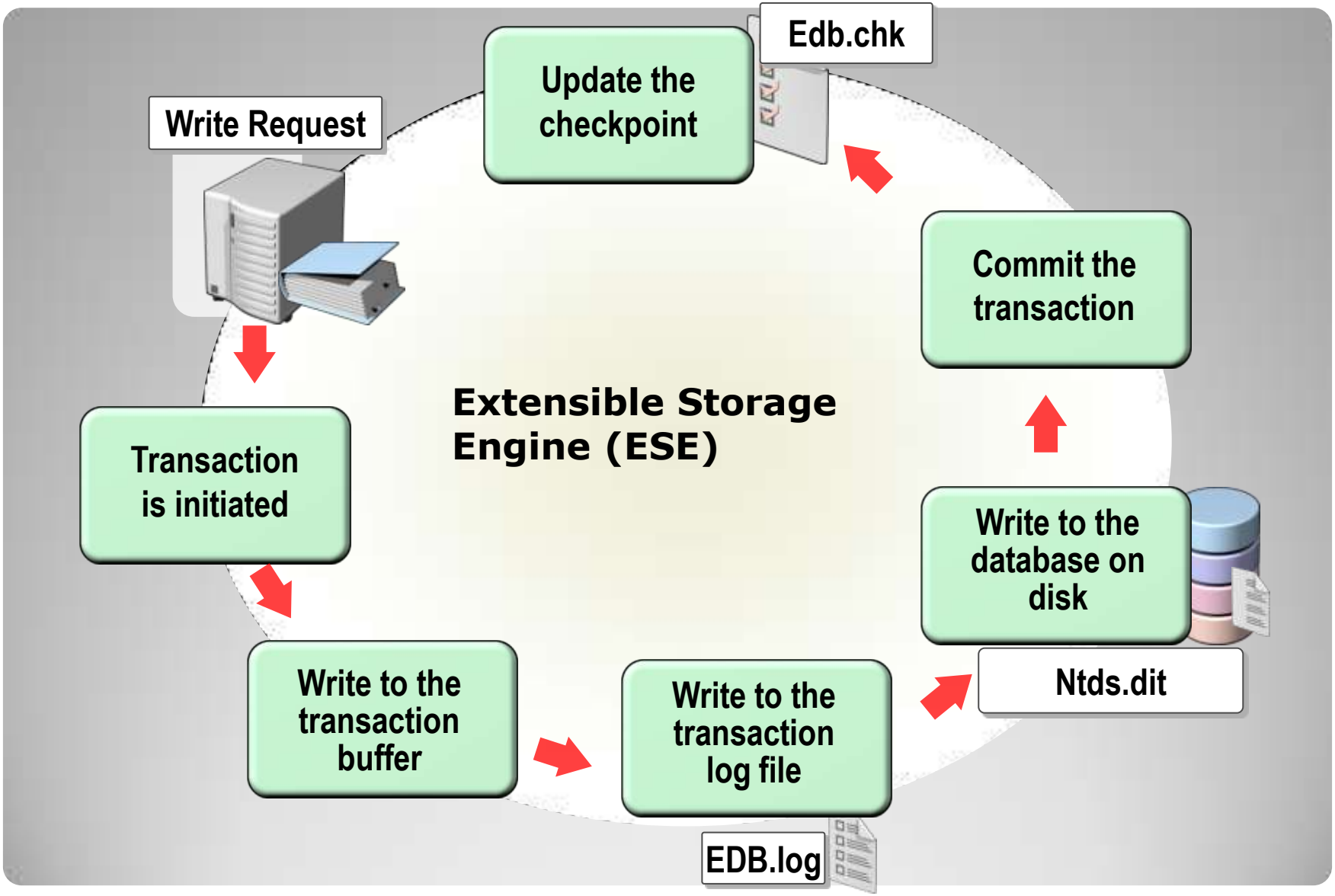
Export informací o objektech

Zákaz replikace

- **repadmin /options** *ServerName* **+DISABLE_INBOUND_REPL**
- **repadmin /options** *ServerName* **+DISABLE_OUTBOUND_REPL**

Databáze AD

Active Directory Distaster Recovery



Modifikace dat v databázi AD

Defragmentace databáze (ntds.dit)

- 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.

```
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

Umístění a přesun databáze

- 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>

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 (fffffbf8) 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 úrovní (nízko úrovňové). **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 vektoru" 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

Recover/repair databáze

- DSRM, NTDSUTIL – files - recover (nebo repair)

nebo

- esentutl /f <path>\ntds.dit (nebo esentutl /p)
- smazání (záloha) *.log souborů

- Import chybějících objektů z .ldf soborů

Odstraňování objektů

Active Directory Distaster 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 smazání objektu

- 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.

- 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)

Nástroje pro obnovení smazaných objektů

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

Ochrana objektu před odstraněním

- 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"

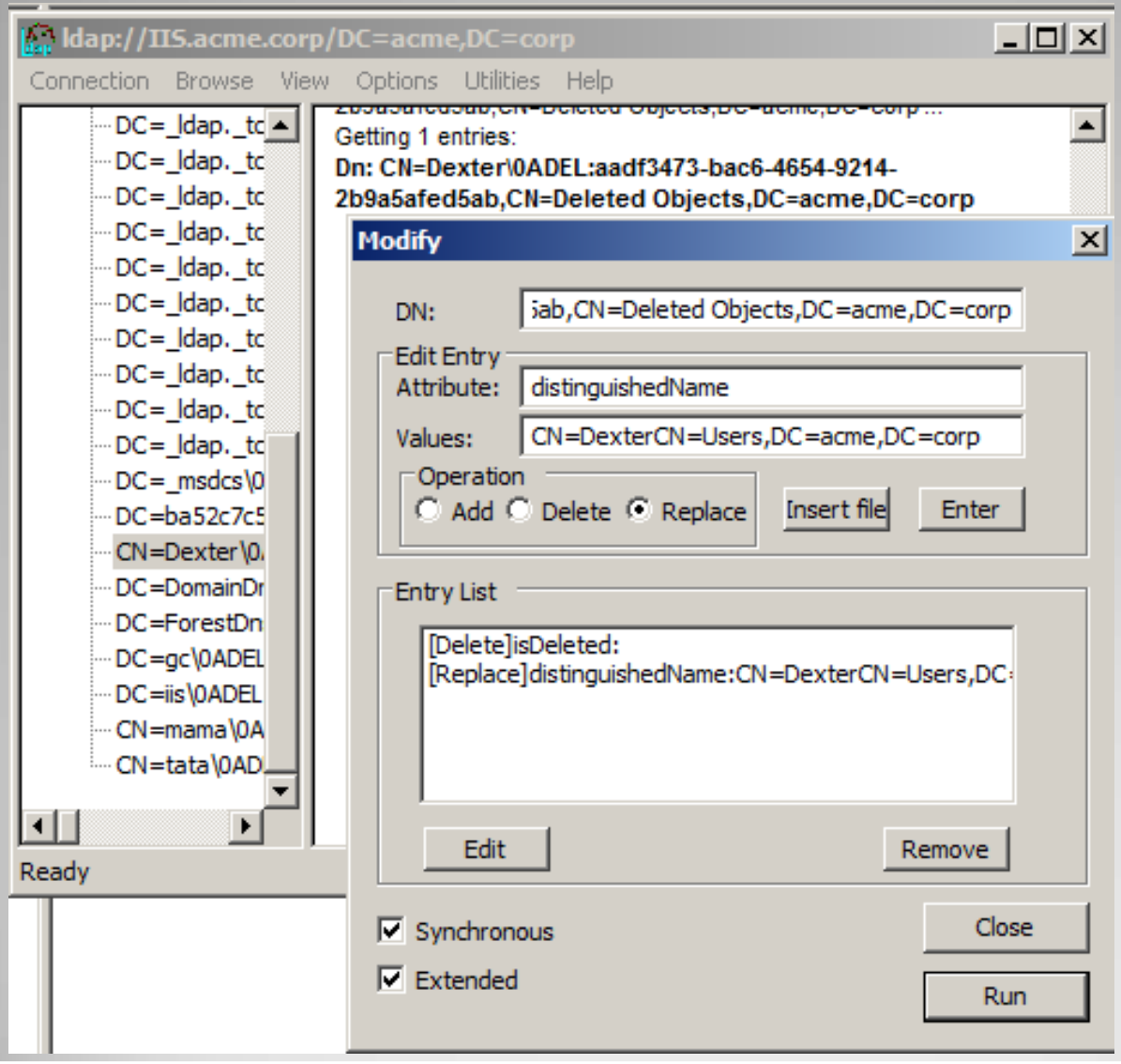
Pro OU=Users: DENY ACE pro Everyon s „DELETE“ a „DELETE TRE“ – s „This object only“:

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

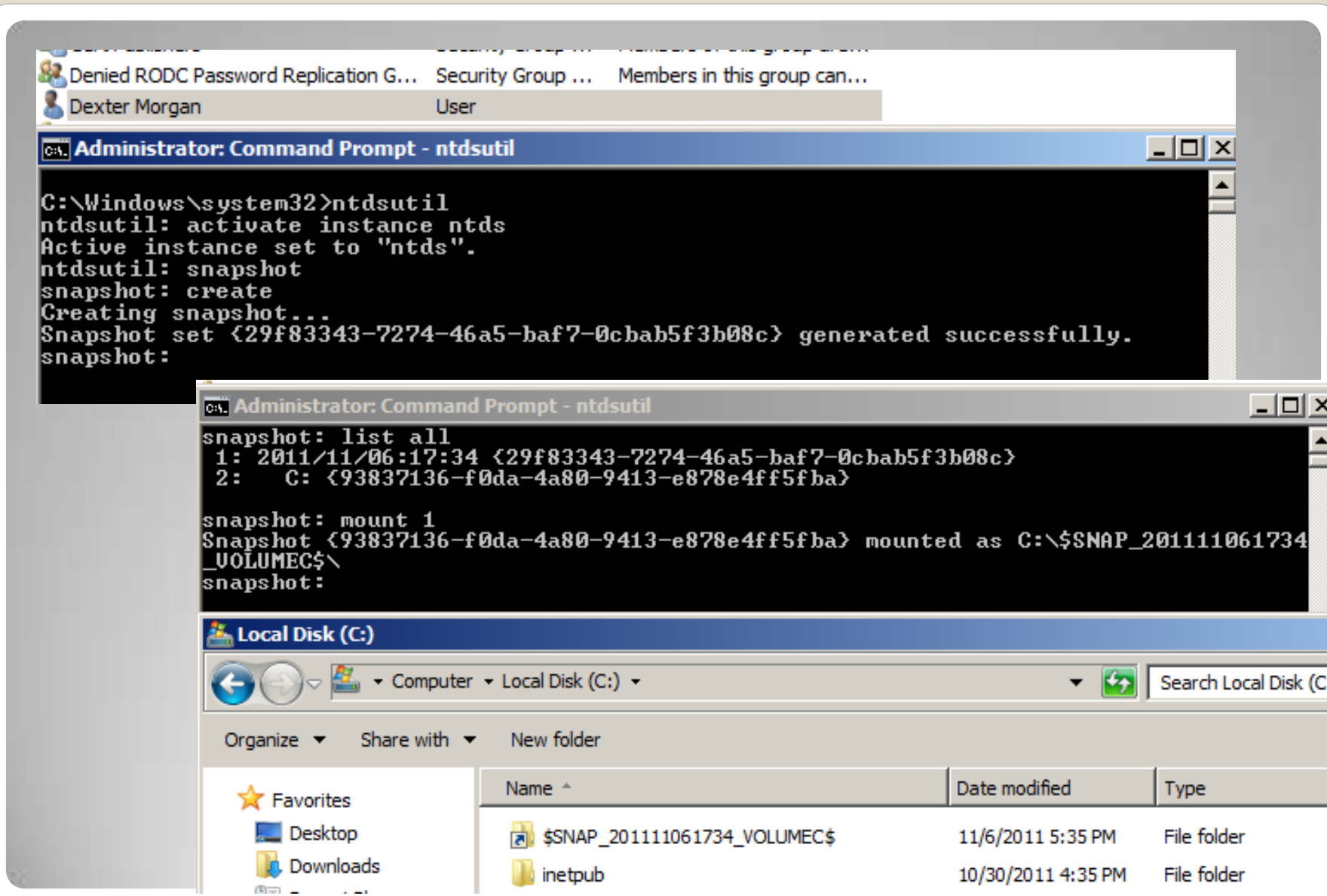
POZN. totéž jako „**Protect object from accidental deletion“** ve Win 2008

- 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 !!!

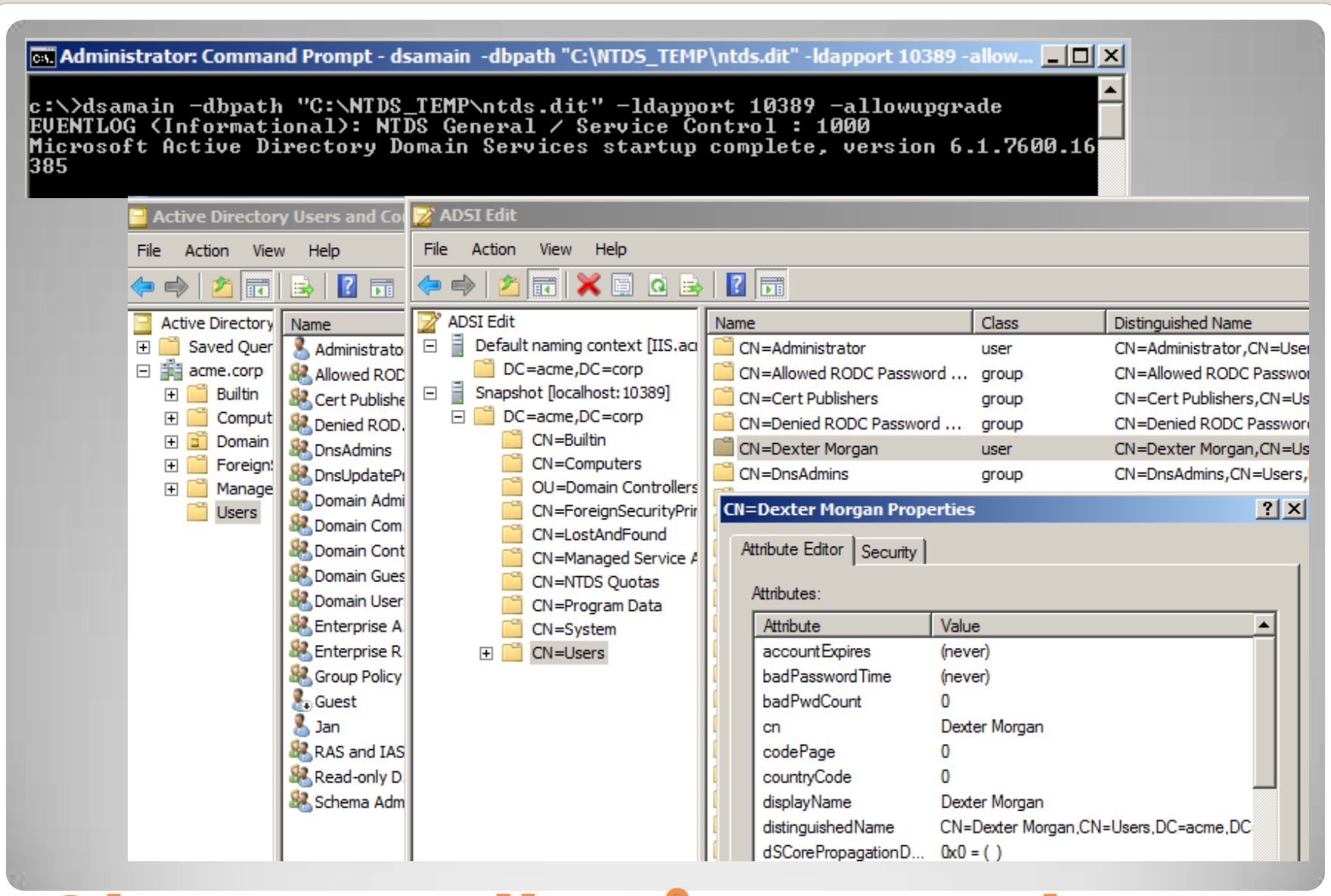
Windows Server Backup



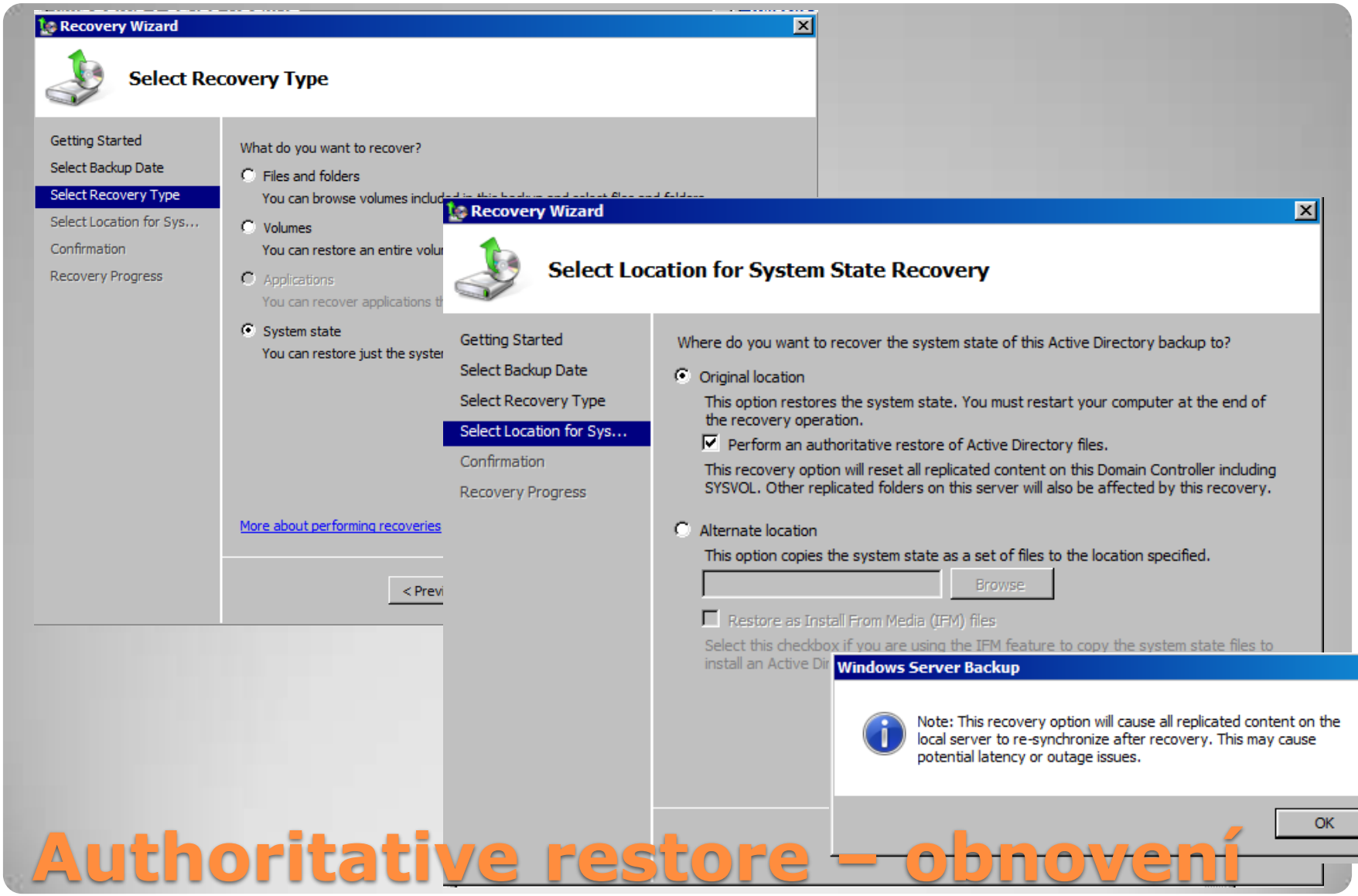
Rychlá obnova smazaného objektu



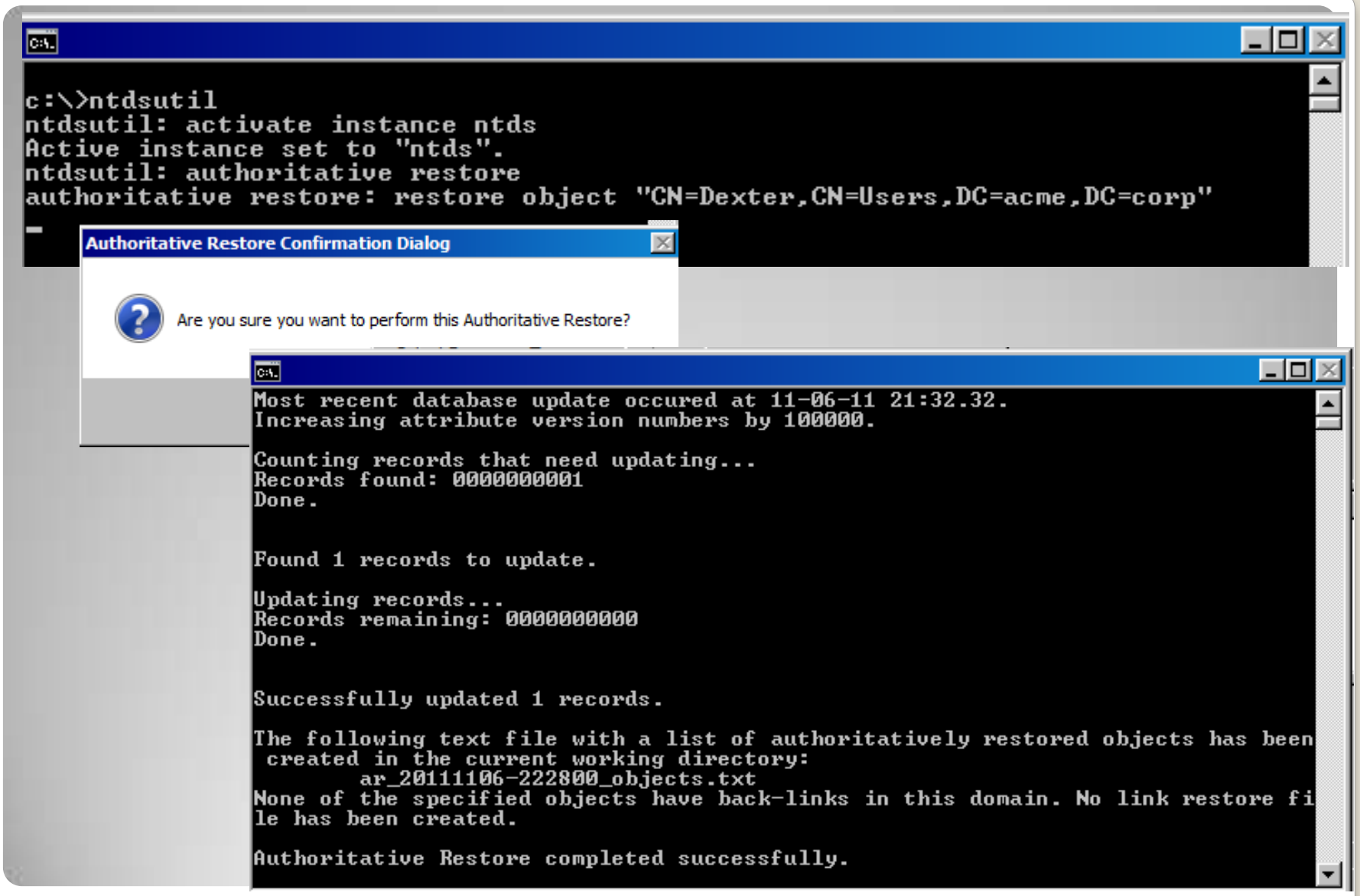
Snapshot AD - vytvoření



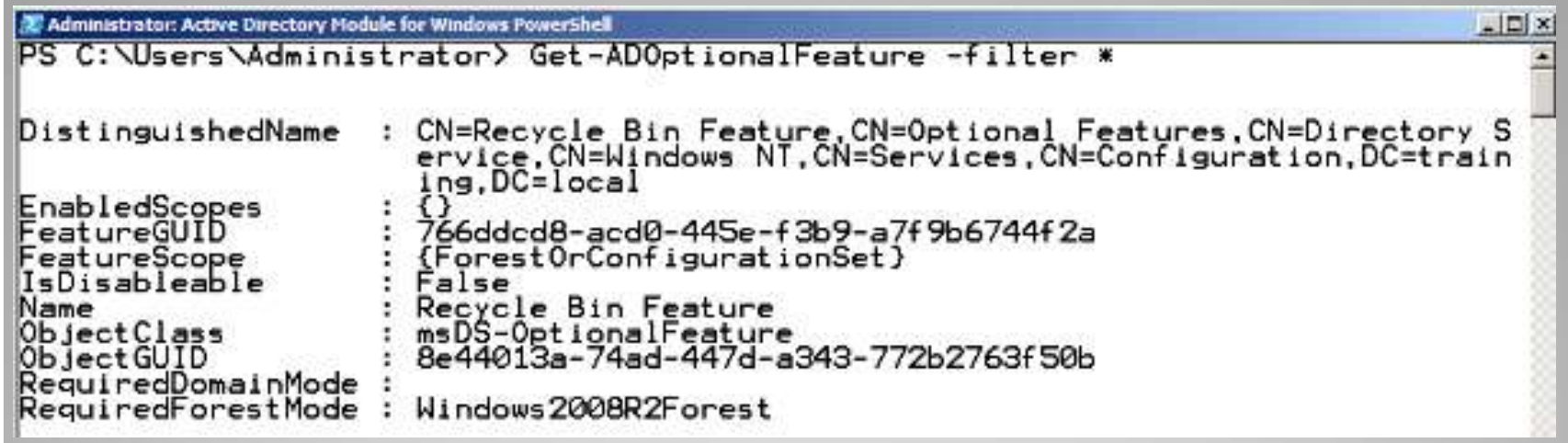
Obnova atributů ze snapshotu

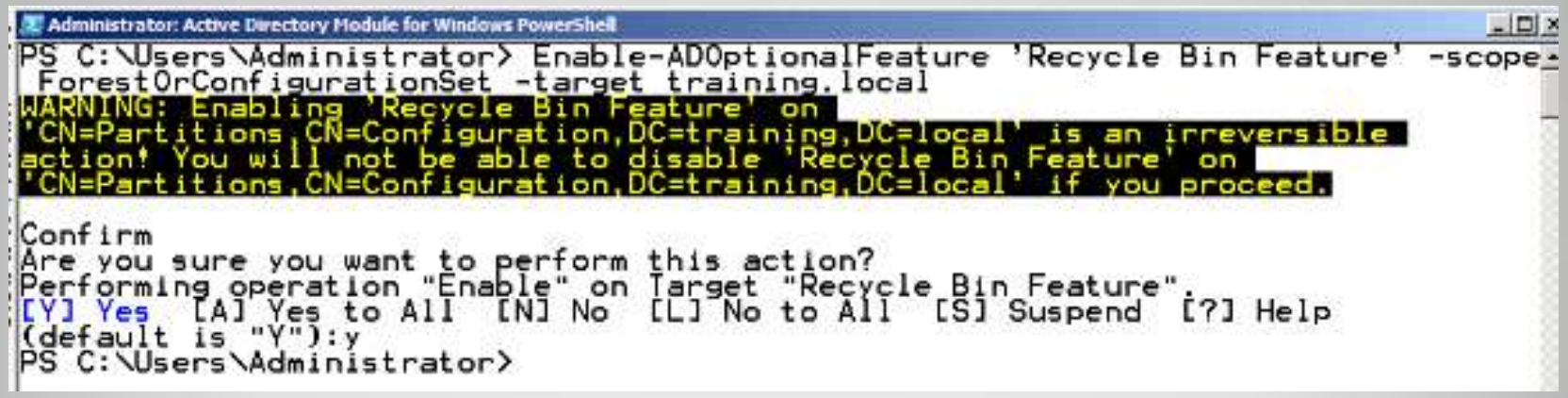


Authoritative restore – obnovení stavu systému

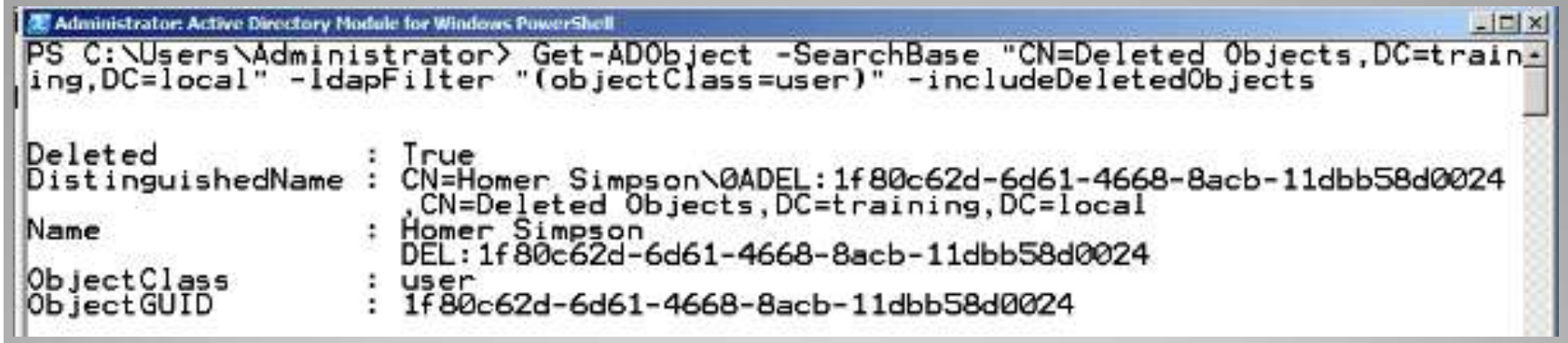


Authoritative restore – obnovení objektu

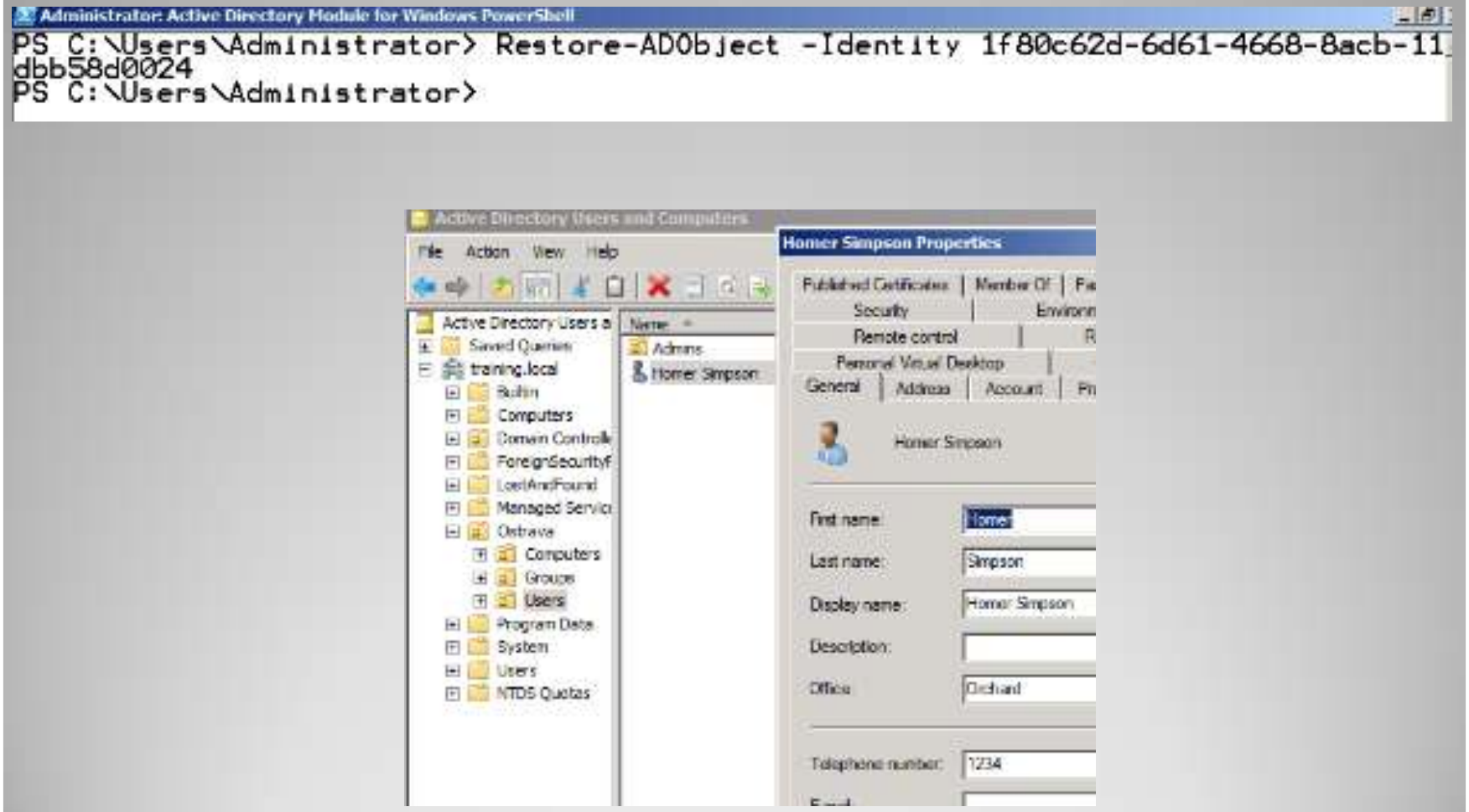




Recycle Bin (Windows 2008 R2) – aktivace



Recycle Bin – vyhledání objektu



Recycle Bin – obnovení objektu

Lingering objects

Active Directory Distaster Recovery

Lingering objects

- When you restore AD from expired backup, deleted objects re-appers (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 – STRICT REPLICATION

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.

- **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)

Indications that DC has lingering objects (2)

- 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.

- 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

repadmin /regkey <servername> +strict
repadmin /regkey * +strict

Note:
This apply on Windows Server 2003 SP1 only!

Configuring strict replication with repadmin

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 replicatioin consistency on newly promoted DC's

Removing Lingering Objects

- REPADMIN (W2003 version only) can be used with **/removelingeringobjects**
  - Repadmin compares databse objects on reference DC with objects on target DC (which is suspected to contan) 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

```
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_APDC02 "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 DCPROMO an install new temporary domain
- Run DCPROMO 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)

Zdroje a odkazy

- 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
- 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://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
- 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
- Lingering 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