



Torino
Technologies
Group

ICT  POWER.IT

Incontro TTG 15 febbraio 2018

Gestione del disaster recovery di Active Directory

Ermanno Goletto

MVP Cloud and Datacenter Management

@ermannog

www.devadmin.it

Roberto Massa

MVP Cloud and Datacenter Management

@robi_massa

massarobi.wordpress.com



- Troubleshooting del DNS
- Troubleshooting di AD DS e della Replica AD
- Troubleshooting della Replica SYSVOL
- Scenari di Disaster Recovery
- Backup e Restore del System State e delle GPO
- Active Directory Snapshots
- Active Directory Recycle Bin



Torino
Technologies
Group

ICT  POWER.IT

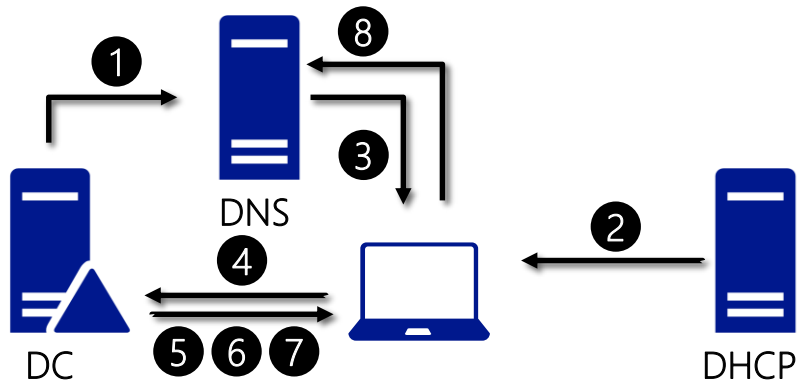
Troubleshooting del DNS

Gestione del disaster recovery di Active Directory

Active Directory e DNS

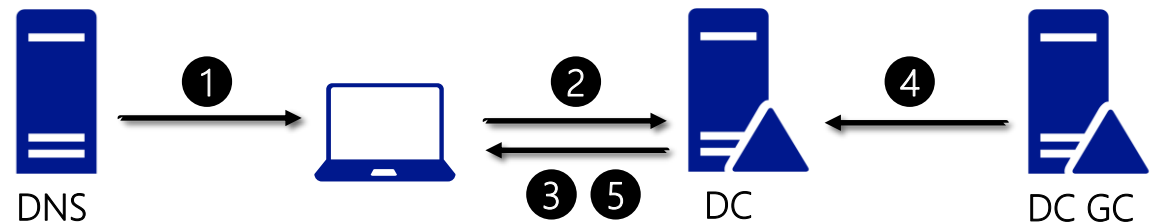
Avvio DC e avvio del computer

1. All'avvio il DC si registra nel DNS
2. Il client ottiene l'indirizzo IP
3. Il DC Locator ottiene la lista dei DC dal DNS
4. Il client instaura il secure channel col DC
5. Autenticazione Kerberos dell'Account Computer
6. Load delle GPO Computer
7. Sincronizzazione temporale
8. Il client si registra nel DNS



Logon dell'utente

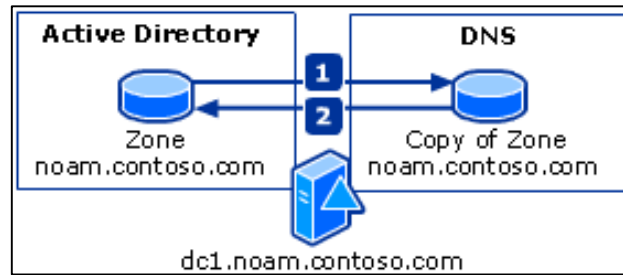
1. Il DC Locator controlla la cache e se necessario ottiene la lista dei DC dal DNS
2. Ping del DC per verifica disponibilità
3. Autenticazione Kerberos dell'Account Utente
4. Ottenimento Universal Group Membership
5. Load delle GPO Utente



Zone DNS integrate in Active Directory

Il server DNS contiene solo una copia della zona DNS

1. All'avvio il server DNS *legge la copia della zona DNS da AD*
2. Il DNS riceve le modifiche e le *scrive in AD*



Zona_MDSC

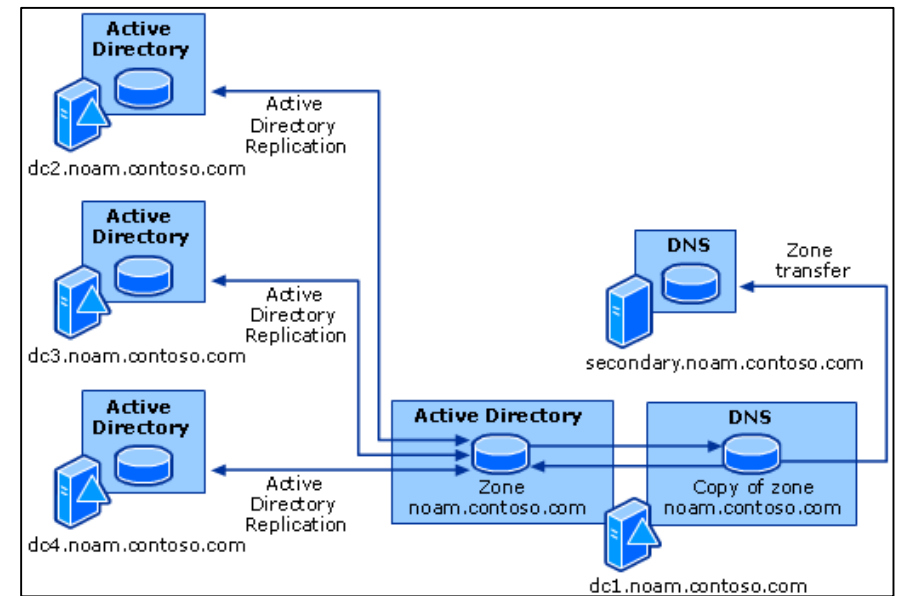
Partizione applicativa replicata a livello di foresta

Zona di dominio

Partizione applicativa replicata a livello di dominio

Replica zona DNS

- Tramite la replica di AD la *zona DNS del dominio è replicata ai DC del stesso dominio*
- Tramite il *Zone transfert* è possibile *inviare una copia della zona ad un DNS secondario*



Check della funzionalità DNS

#Verifica funzionamento servizi DNS sui DC

```
Get-ADDomainController -Filter * |  
  foreach {Get-Service DNS -ComputerName $_.hostname} |  
  select machinename, name, status
```



REM Informazioni sulla struttura DNS

```
Dnscmd /info
```



REM Test di base e verifica dynamic update per la zona AD

```
dcdiag /test:DNS /DnsDynamicUpdate /i
```

REM Test di base e verifica registrazione record A,CNAME,SRV

```
dcdiag /test:DNS /DnsRecordRegistration /i
```

REM Test registrazione nella zona DNS del dominio AD

```
dcdiag /test:RegisterInDNS /DnsDomain:%USERDNSDOMAIN% /i
```

REM Verifica funzionalità DC Locator

```
NLTEST /DSGETDC:%USERDNSDOMAIN%
```

Fixing del DNS

Riregistrazione record SRV di un DC nella zona DNS (KB556002)

- *Metodo 1: Riavvio servizio netlogon*
- *Metodo 2: Utilizzare DcDiag /Fix (o NetDiag /fix per OS pre WS2008)*
- *Metodo 3: Aggiunta manuale record SRV nel file %SystemRoot%\System32\Config\Netlogon.dns*

Rebuild delle zone DNS

- *KB 294328: How to reinstall a dynamic DNS Active Directory-integrated zone*
- *KB 817470: How to reconfigure an _msdcs subdomain to a forest-wide DNS application directory partition when you upgrade from Windows 2000 to Windows Server 2003*
- *KB 2001093: Troubleshooting DNS Event ID 4013: The DNS server was unable to load AD integrated DNS zones*

Demo



Torino
Technologies
Group

ICT  POWER.IT

Troubleshooting del DNS



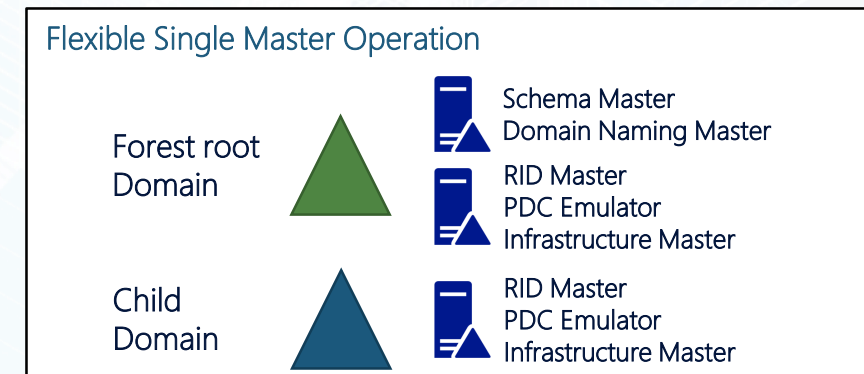
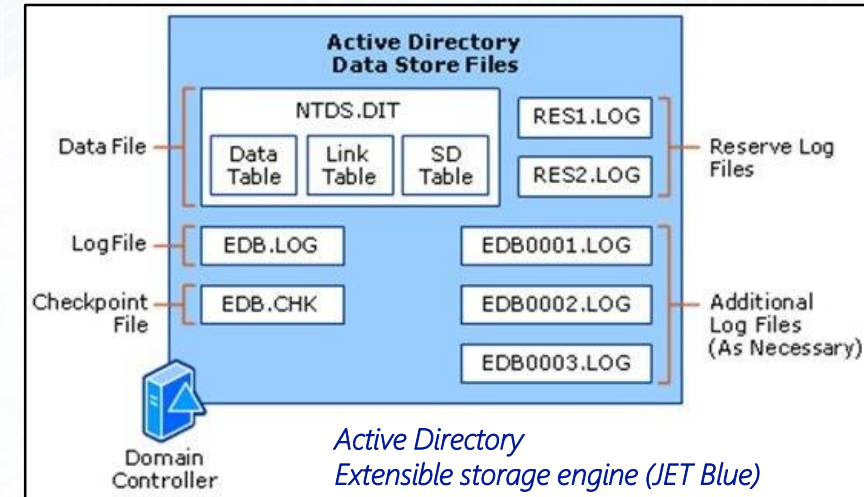
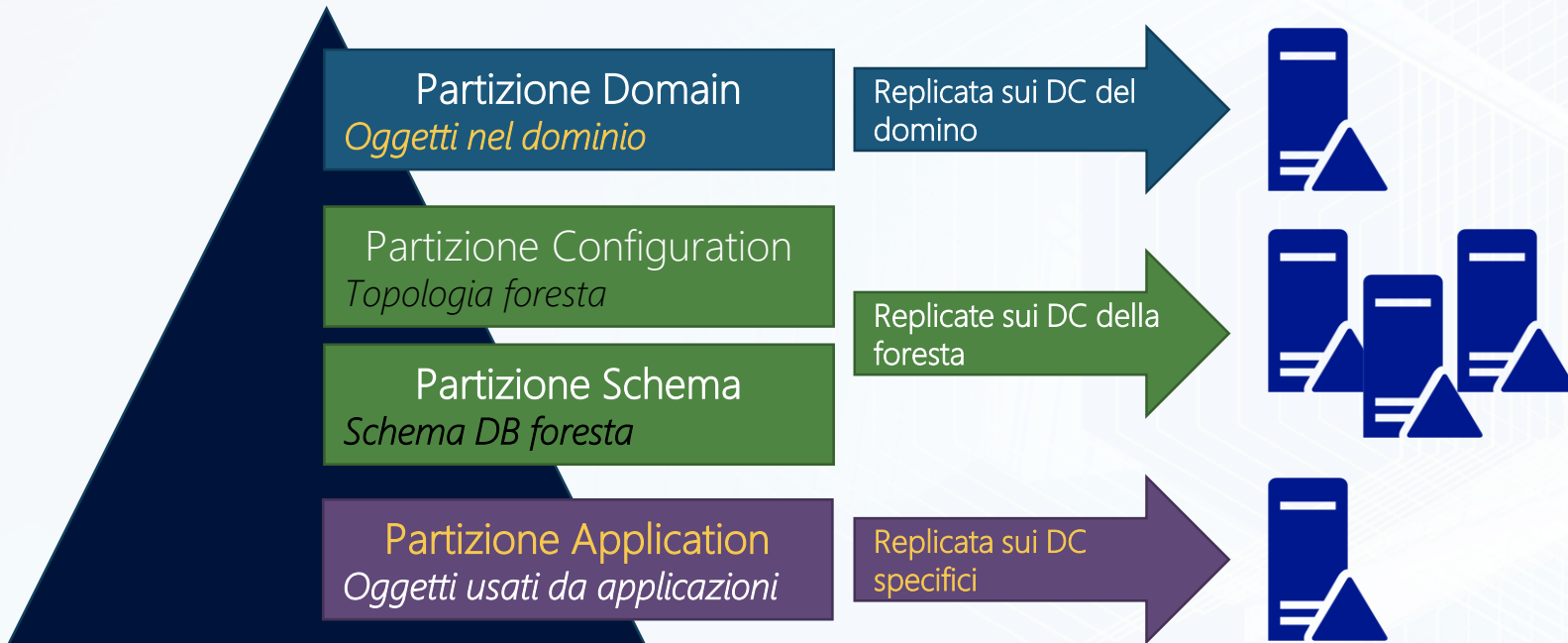
Torino
Technologies
Group

ICT  POWER.IT

Troubleshooting di AD DS e della Replica AD

Gestione del disaster recovery di Active Directory

Database di Active Directory e replica



Tools per il troubleshooting di AD

Tool	Descrizione	Tipo	Requisiti
Eventvwr.exe	Event Viewer	GUI	
Ntdsutil.exe, Esentutl.exe	Manutenzione database Active Directory	Command line	
adsiedit.msc	Active Directory Service Interfaces Editor	GUI	
Ldp.exe	Lightweight Directory Access Protocol (LDAP) client	GUI	
Repadmin.exe	Replication Diagnostics Tool	Command line	
Netdom.exe	Gestione Active Directory domains and trust relationships	Command line	
Dcdiag.exe	Domain Controller Diagnostic Tool	Command line	
BPA	Best Practices Analyzer for Active Directory Domain Services	GUI	WS2008R2 e succ.
PowerShell	Active Directory e Best Practices Analyzer Cmdlets e Active Directory provider	Command line	WS2008R2 e succ.
ADREPLSTATUS	Active Directory Replication Status Tool	GUI	Microsoft Download Center
Active Directory Utils	Active Directory Utils (RepIDiag , CheckDSAcls, TrustViewer, FindGuidInAD, SearchForDuplicateAttributeData)	Command line	CodePlex

Check della funzionalità di AD



```
REM Controllo registrazione del Machine Account  
dcdiag /test:MachineAccount /i
```

```
REM Controllo Replica
```

```
dcdiag /test:Replications /i
```

```
dcdiag /test:VerifyReplicas /i
```

```
repadmin /showreps & repadmin.exe /replsummary
```

```
REM Controllo Operations Masters
```

```
dcdiag /test:knowsofroleholders /i
```

```
dcdiag /test:fsmocheck /i
```

```
netdom /query fsmo
```

Troubleshooting Replica Active Directory

Operazione	RepAdmin	PowerShell
Metadati replicati	repadmin.exe /showobjmeta	Get-ADReplicationAttributeMetadata -object "dc=ictpower,dc=local" -server dc1.ictpower.local -showalllinkedvalues format-list
Configurazione e stato replica di un DC		Get-ADReplicationPartnerMetadata -target dc1.ictpower.local
Ultima replica fallita da un DC nella foresta		Get-ADReplicationPartnerMetadata -target * -scope server where {\$_.lastreplicationresult -ne "0"} format-table server,lastreplicationattempt,lastreplicationresult,partner -auto
Informazioni sugli errori di replica	repadmin.exe /showreplsum	Get-ADReplicationFailure dc1.ictpower.local
Informazioni sugli errori di replica dei DC in un sito		Get-ADReplicationFailure -scope site -target default-first-site-name format-table server,firstfailuretime,failurecount,lasterror,partner -auto
Forzatura della replica singolo oggetto	repadmin.exe /replsingleobject	Get-ADDomainController -filter * foreach {Sync-ADObject -object "cn=massar,cn=users,dc=ictpower,dc=local" -source dc1 -destination \$_.hostname}
Forzatura della replica	Repadmin.exe /syncall dc1 /APed	
Siti senza subnet assegnata		Get-ADReplicationSite -filter * -property subnets where-object {!\$_.subnets -eq ""} format-table name

Repadmin: [https://technet.microsoft.com/en-us/library/cc770963\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc770963(v=ws.11).aspx)

Advanced Active Directory Replication and Topology Management Using Windows PowerShell (Level 200):

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/powershell/advanced-active-directory-replication-and-topology-management-using-windows-powershell--level-200->

Free Download: CMD to PowerShell Guide for AD: <https://blogs.technet.microsoft.com/ashleymcglone/2013/01/02/free-download-cmd-to-powershell-guide-for-ad/>

Demo



Torino
Technologies
Group

ICT  POWER.IT

Troubleshooting Replica Active Directory



Torino
Technologies
Group

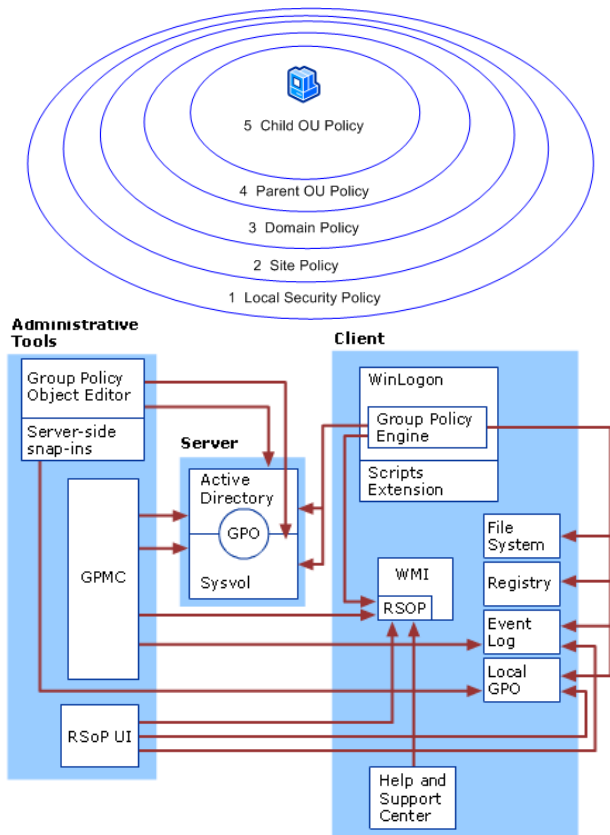
ICT  POWER.IT

Troubleshooting della Replica SYSVOL

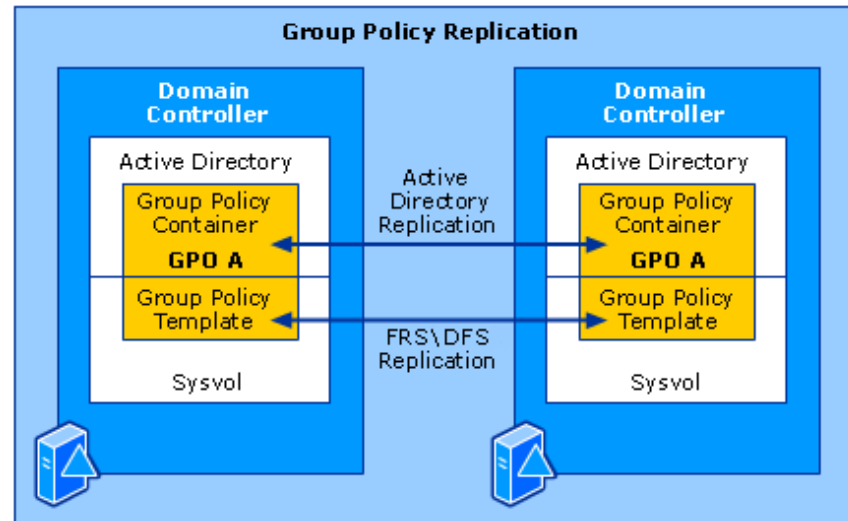
Gestione del disaster recovery di Active Directory

Replica Group Policies

Funzionamento e impostazione GPO

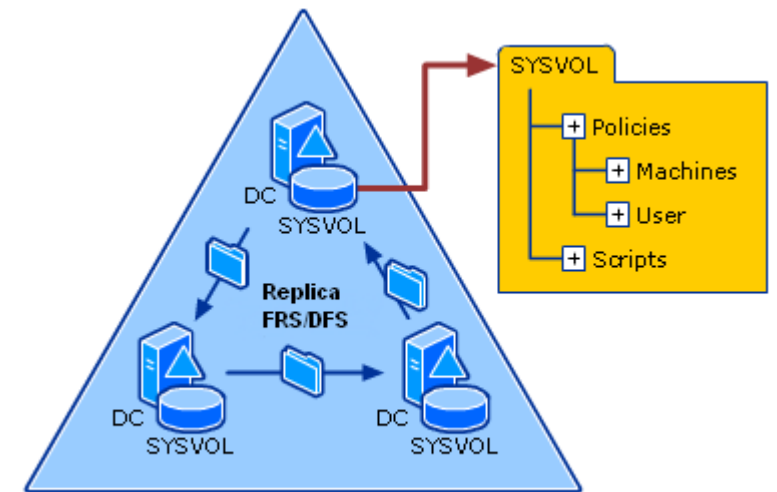


Replica GPO



Le GPO sono create nei domini e replicate solo tra i DC appartenenti al dominio di creazione

Replica directory %systemroot%\SYSVOL\domain



Tools per il troubleshooting della SYSVOL

Tool	File Replication Service Diagnostics Tool	GUI	Requisiti
FRSDiag	File Replication Service Diagnostics Tool	GUI	Microsoft Download Center
Sonar	File Replication Service (FRS) Status Viewer	GUI	Microsoft Download Center
Ultrasound	Monitoring e troubleshooting File Replication Service (FRS)	GUI	Microsoft Download Center
dfsmgmt.msc	Distributed File System (DFS) Management snap-in	GUI	Feature
Dfsrdiag.exe	Test diagnostici della replica DFS	Command line	
Dfsradmin.exe	Gestione replica DFS	Command line	
PowerShell	DFS Namespace (DFSN) Cmdlets	Command line	WS2012 e succ.

Check della funzionalità della SYSVOL

```
REM Controllo esistenza delle share  
net share
```

```
REM Verifica permission su share per Replica  
dcdiag /test:netlogons /i
```

```
REM Verifica replica FRS  
dcdiag /test:frssysvol /i  
dcdiag /test:frsevent /i
```

```
REM Verifica replica DFS  
dfsrdiag ReplicationState /all  
DfsrAdmin.exe Health New /RgName:"Domain System Volume" /RefMemName:dc01  
/RepName:c:\Reports\Sysvol.htm /FsCount:true
```



Fix SYSVOL e Default Domain Policies

Ricreazione SYSVOL

- *KB315457*: How to *rebuild the SYSVOL tree* and its content in a domain
- *KB947022*: The *NETLOGON share is not present* after you install Active Directory Domain Services on a new full or read-only Windows Server 2008-based domain controller

```
REM Restore Default Domain Policy GPO  
dcpofix /ignoreschema /target:Domain
```

```
REM Restore Default Domain Controllers Policy GPO  
dcpofix /ignoreschema /target:DC
```



Dcpofix non imposta i security settings esattamente come dopo il DCPromo (KB 833783)



Torino
Technologies
Group

ICT  POWER.IT

Scenari di Disaster Recovery

Gestione del disaster recovery di Active Directory

Issues comuni in Active Directory



Modifiche allo schema AD da parte di prodotti di terze parti



Mantenere il gruppo Schema Admins vuoto e popolarlo all'occorrenza



Cancellazione accidentale di oggetti



Abilitare la protezione da cancellazione



Mancanza di spazio sulla partizione del DB di AD



*Riservare spazio mediante un file di dummy
`fsutil file createnew %SystemDrive%\ADUtil\Space.res 1073741824`*



Attacchi di tipo DOS da malware



*Per default ogni Authenticated Users può eseguire 10 join di computer (KB251335 e KB314462)
Impostare quote sul n° oggetti instanziabile per utenti con deleghe amministrative (DsAdd, DsMod e DsQuery)*



Ripristino immagine di un DC o di uno snapshot di un virtual DC



Utilizzare Hypervisor con supporto a VM-GenerationID e DC WS2012 o succ.



Lock dei file del DB di AD (eventi 482, 414 482 & NTDS ISAM)



*Configurare correttamente l'Antivirus sul DC (KB822158, KB943556)
Eseguire correttamente il backup dei virtual DC, evitando ad esempio di utilizzare le snapshot (KB 888794)*

Domain Controller non funzionante

Soluzione 1

Demote e RePromote

Soluzione 2

Restore non autoritativo di un SystemState più recente del Tombstone lifetime

Soluzione 3

- ✓ *Eliminazione DC da AD e DNS*
- ✓ *Seize dei ruoli FSMO posseduti dal DC*
- ✓ *Demote forzato del DC*
- ✓ *Restore non autoritativo di un SystemState più recente del Tombstone lifetime o Reinstallazione o Cloning di un DC virtuale*

Rimozione forzata di un DC

Rimozione riferimenti dal DNS

- Record A e PTR relative al DC
- Tutti i record SRV relative al DC
- Record CNAME relativo al DC
- Record A nella zona gc._msdcs.<FQDN Domain> (se il DC era GC)

Rimozione riferimenti da Site and Services

- Eliminare l'oggetto DC dal sito a cui appartiene
- Eliminare le connessioni al DC sugli altri DC

Rimozione riferimenti da Active Directory Users and Computers

- Eliminare l'account computer del DC da container Domain Controllers
- Eliminare se esistono riferimenti al DC in:
 - System\DFSR-GlobalSettings\Domain System Volume\Topology
 - MOMLatencyMonitors (se si usa MOM)
 - OpsMgrLatencyMonitors (se si usa SCOM)

Mount Snapshot



```
NTDSutil
metadata cleaup
connections
connect to server <DC funzionante>
quit
select operation target
list sites
select site <id site DC da rimuovere>
list servers in sites
select server <id DC da rimuovere>
list domains
select domain <id dominio DC>
quit
remove selected server
quit
```

Seize ruoli FSMO

Tramite NTDSUtil

```
NTDSUtil
roles
  connections
  connect to server <DC funzionante>
  quit
select operation target
  list roles for connected server
seize role schema master
seize role domain naming master
seize role PDC
seize role RID master
seize role infrastructure master
quit
```



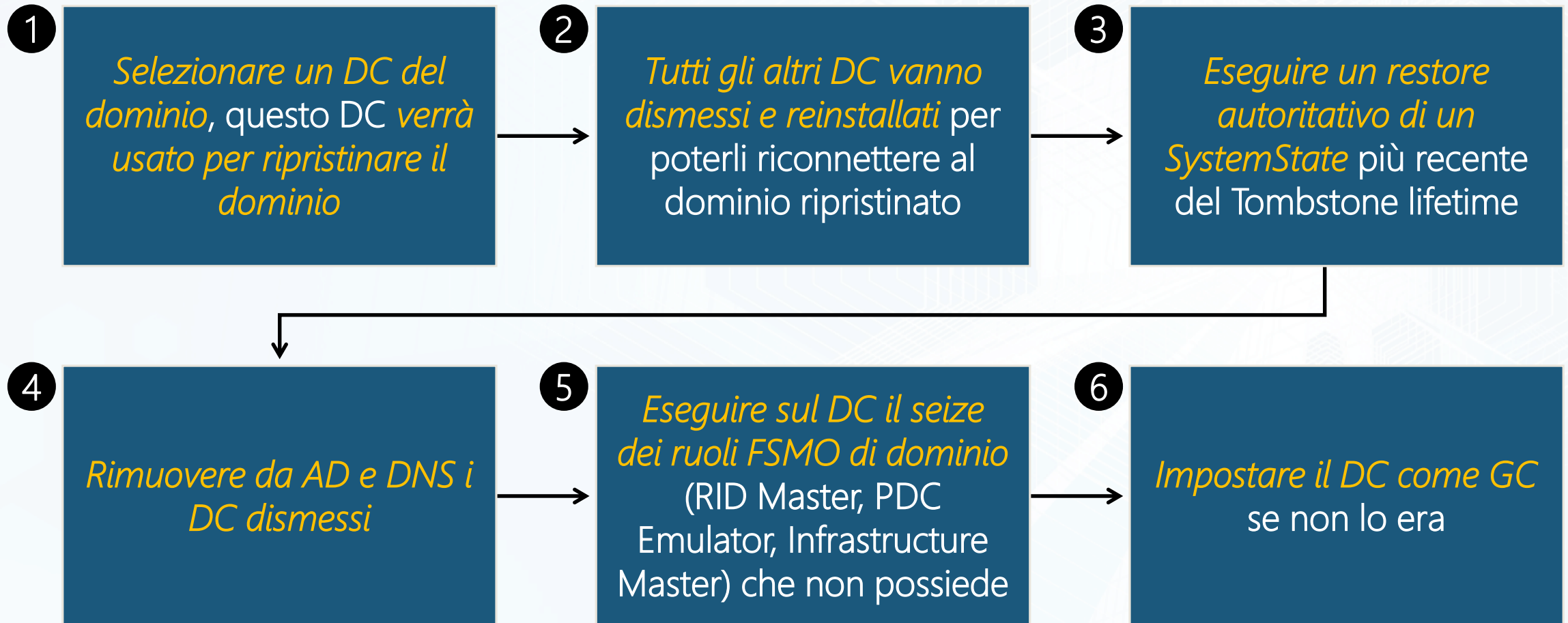
Tramite PowerShell

```
Get-ADForest | Select SchemaMaster,DomainNamingMaster
Get-ADDomain | Select PDCEmulator,RIDMaster,InfrastructureMaster

Move-ADDirectoryServerOperationMasterRole
  -Identity "<DC funzionante>"
  -OperationMasterRole SchemaMaster -Force
Move-ADDirectoryServerOperationMasterRole
  -Identity "<DC Funzionante>"
  -OperationMasterRole DomainNamingMaster -Force
Move-ADDirectoryServerOperationMasterRole
  -Identity "<DC Funzionante>"
  -OperationMasterRole PDCEmulator -Force
Move-ADDirectoryServerOperationMasterRole
  -Identity "<DC Funzionante>"
  -OperationMasterRole RIDMaster -Force
Move-ADDirectoryServerOperationMasterRole
  -Identity "<DC Funzionante>"
  -OperationMasterRole InfrastructureMaster -Force
```



Recovery di un Dominio



Recovery di una Foresta

Selezionare un DC nella foresta, questo DC verrà usato per ripristinare il Forest Root Domain (primo dominio nella foresta) e *diventerà il root DC*

1

Tutti gli altri DC nella foresta vanno disconnessi, selezionare un DC per ogni dominio figlio che verrà usato per ripristinare il dominio e *dismettere gli altri DC che verranno reinstallati* per poterli riconnettere ai domini ripristinati

2

Iniziare i recovery ripristinando il Forest Root Domain

3

Eseguire il recovery dei domini figlio

4

Recovery di oggetti o container

Oggetti o Container Modificati

- *Restore autoritativo SystemState*
- *Active Directory Snapshot*
 - Richiede DC WS2008 o successivo
 - Con WS2008 R2 e successivo è possibile eseguire il mount di un VHD e quindi il mount di un ntds.dit in esso contenuto

Oggetti o Container Eliminati

- *Restore autoritativo SystemState*
- *Tombstone Reanimation* (LDP, ADSI o ADRestore)
- *Active Directory Snapshot*
- *Recycle Bin di Active Directory* (richiede livello funzionale di foresta WS2008R2 o successivo, ovvero i DC devono essere tutti almeno WS2008R2)

Repair Database Active Directory

1. *Demote* DC
2. *Eliminazione file* del DB AD
3. *RePromote* DC

Soluzione 1

Soluzione 2

Restore non autoritativo dell'intero DB AD

Repair tramite Compattazione, Checksum e Recover del DB AD

Soluzione 3

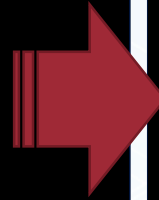
Manutenzione Database Active Directory

Info sui file del database e compattazione

```
REM Arresto servizio AD DS
Net Stop NTDS
REM Info sui file del database
NTDSUtil
Activate Instance NTDS
Files
    Info
    Quit
Quit
REM Compattazione file ntds.dit
NTDSUtil
Activate Instance NTDS
Files
    Compact to C:\NTDSTmp
    Quit
Quit
REN %SystemRoot%\NTDS\ntds.dit ntds.dit.org
Copy C:\NTDSTmp\ntds.dit %SystemRoot%\NTDS\ntds.dit
```

C:\

1



Checksum e Recover DB

```
NTDSUtil
Activate Instance NTDS
Files
    Checksum          (Controllo integrità fisica)
    Integrity         (Controllo integrità logica)
    Recover           (Soft DB Recovery)
    Quit
Quit
REM Recovery del DB
esentutl /r %SystemRoot%\NTDS\ntds.dit
REM Repair del DB
esentutl /p %SystemRoot%\NTDS\ntds.dit
REM Verifica Integrità DB
esentutl /g %SystemRoot%\NTDS\ntds.dit
REM Eliminazione logs
del %SystemRoot%\NTDS\*.log
REM Avvio servizio AD DS
Net Start NTDS
```

C:\

2



Torino
Technologies
Group

ICT  POWER.IT

Backup e Restore del System State e delle GPO

Gestione del disaster recovery di Active Directory

Backup System State Backup

Elementi del System State

- Registry
- COM+ Class Registration database
- Boot files
- Active Directory Certificate Services (AD CS) database
- Active Directory database (Ntds.dit)
- SYSVOL directory
- Cluster service information
- Microsoft Internet Information Services (IIS) metadirectory
- System files sotto Windows Resource Protection
- Active Directory Federation Services

Volumi critici di un Domain Controller

- Volume boot files Bootmgr file e Boot Configuration Data (BCD) store
- Volume sistema operativo e registry
- Volume SYSVOL directory
- Volume Active Directory database (Ntds.dit)
- Volume Active Directory database log files

Gestione Windows Backup con PowerShell

```
#Installazione Windows Backup
add-windowsfeature windows-server-backup -includeallsubfeature

#Backup System State Schedulato
wbadmin enable backup -addtarget:<target> -schedule:21:00
-systemstate -quiet

#Backup Full System + System State Schedulato (Bare Metal restore)
wbadmin enable backup -addtarget:<target> -schedule:21:00
-systemstate -quiet -allcritical -vssfull

#Backup System State manual
# -vssfull e -allcritical non sono supportati
# con start systemstatebackup
wbadmin start systemstatebackup -backuptarget:<drive> -quiet

#Elenco System State memorizzati
wbadmin get versions

#Stato backup in esecuzione
wbadmin get status
```



Restore Autoritativo e Non Autoritativo

Non Autoritativo

- *Non vengono modificati timestamp o USN* (Update Sequence Number) degli oggetti ripristinati
- *Alla replica successiva il DC riceve le modifiche* intercorse dopo il backup del System State ripristinato dagli altri DC

Autoritativo

- Ripristino di oggetti, container o dell'intero DB di AD allo stato del backup del System State
- *Il timestamp viene aggiornato* e l'USN (Update Sequence Number) *viene incrementato di 100.000*
- *Alla replica successiva il DC invia gli aggiornamenti degli oggetti ripristinati agli altri DC*
- *I back-links degli oggetti ripristinati* (es. Groups Membership) *sono ripristinati solo se sono stati creati in una foresta con livello funzionale WS2003/WS2003 Interim o successivo* (a partire da WS2003 SP1 è possibile usare LDIF per ricrearli)
- La password dell'account computer viene rinegoziata ogni 30gg, quindi un *restore autoritativo può causare il blocco della relazione di trust/join dei computer* che hanno rinegoziato dopo backup ripristinato

Restore non autoritativo System State

Avvio in AD Restore Mode (DSRM) 1

- *Se si ha accesso alla console locale*
 - Premere *F8 all'avvio*
- *Se non si ha accesso alla console locale*
 - Eseguire il comando:
Bcdedit /set safeboot dsrepair
 - Riavviare il DC

1

Restore System state con Windows Backup 2

```
REM Ricostruzione del catalogo
wbadmin restore catalog -enable backup -backuptarget:<location>
REM Elenco backup memorizzati
wbadmin get versions
REM Restore di una versione del systemstate
wbadmin start systemstatercovery -version:<version> -quiet
REM Riavviare il DC
Shutdown -r -t 0
```

2

C:\

Modifica password DSRM

```
NTDS
set dsrm password
reset password on server <nome DC>
<nuova password>
<conferma nuova password>
quit
```

Nel caso non la si conosca

C:\

Disabilitazione AD Restore Mode 3

- *Autenticarsi con le credenziali DSRM*
- *Attendere che il restore sia terminato*
- *Eseguire il comando: `Bcdedit /deletevalue safeboot`*
- *Riavviare il DC*

3

Restore autoritativo System State

1 Avvio in AD Restore Mode (DSRM)

- *Se si ha accesso alla console locale*
 - Premere *F8 all'avvio*
- *Se non si ha accesso alla console locale*
 - Eseguire il comando:
Bcdedit /set safeboot dsrepair
 - Riavviare il DC

1



2 Restore System state con Windows Backup

```
REM Ricostruzione del catalogo
wbadmin restore catalog -enable backup -backuptarget:<location>
REM Elenco backup memorizzati
wbadmin get versions
REM Restore di una versione del systemstate
wbadmin start systemstatercovery -version:<version> -quiet
REM Riavviare il DC e autenticarsi con le credenziali DSRM
Shutdown -r -t 0
```

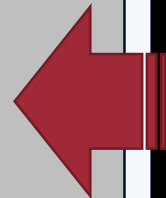
2



4 Disabilitazione AD Restore Mode

- *Autenticarsi con le credenziali DSRM*
- *Attendere che il restore sia terminato*
- *Eseguire il comando:*
Bcdedit /deletevalue safeboot
- *Riavviare il DC*

4



3 Impostazione versione

```
NTDSutil
Activate Instance NTDS
Authoritative Restore
Restore Object <DN Oggetto>
Restore Subtree <DN>
Restore Database
quit
```

3




Composizione Distinguished Name (DN)

cn=common name,ou=organizational unit, dc=domain component1, dc=domain component2

Per esempio: *ermannog, ou=Staff, dc=ictpower, dc=it*

Restore autoritativo Sysvol

Avvio in AD Restore Mode (DSRM) 1

- *Se si ha accesso alla console locale*
 - Premere *F8 all'avvio*
 - *Se non si ha accesso alla console locale*
 - Eseguire il comando:
Bcdedit /set safeboot dsrepair
 - Riavviare il DC
- 

Disabilitazione AD Restore Mode 3

- Autenticarsi con le credenziali DSRM
- Attendere che il restore sia terminato
- Eseguire il comando:
Bcdedit /deletevalue safeboot
- Riavviare il DC

Restore System state con Windows Backup 2

Ricostruzione del catalog

```
wbadmin restore catalog -enable backup -backuptarget:<location>
```

Elenco backup memorizzati

```
wbadmin get versions
```

Restore Sysvol da una versione del systemstate

```
wbadmin start systemstatercovery -version:<version> -quiet -authsysvol
```

REM Riavviare il DC e autenticarsi con le credenziali DSRM

```
Shutdown -r -t 0
```



KB utili

- *KB315457: How to rebuild the SYSVOL tree and its content in a domain*
- *KB 290762: Using the BurFlags registry key to reinitialize File Replication Service replica sets*
- *KB2218556: How to force an authoritative and non-authoritative synchronization for DFSR-replicated SYSVOL (like "D4/D2" for FRS)*
- *KB842162: How to relocate the SYSVOL tree on a domain controller that is running NT File replication service for SYSVOL*
- *KB2957985: Unexpected "AD/SYSVOL version mismatch" message in Group Policy Results in Windows 8.1 or Windows Server 2012 R2*

Backup delle GPO

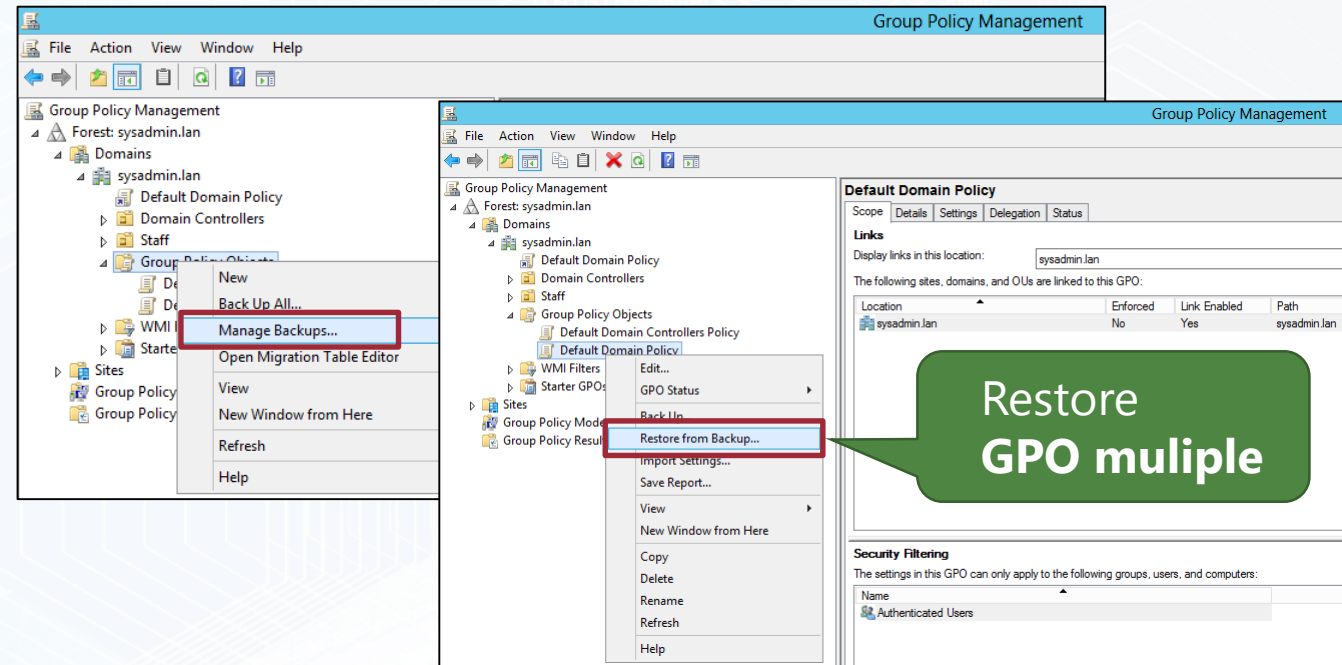
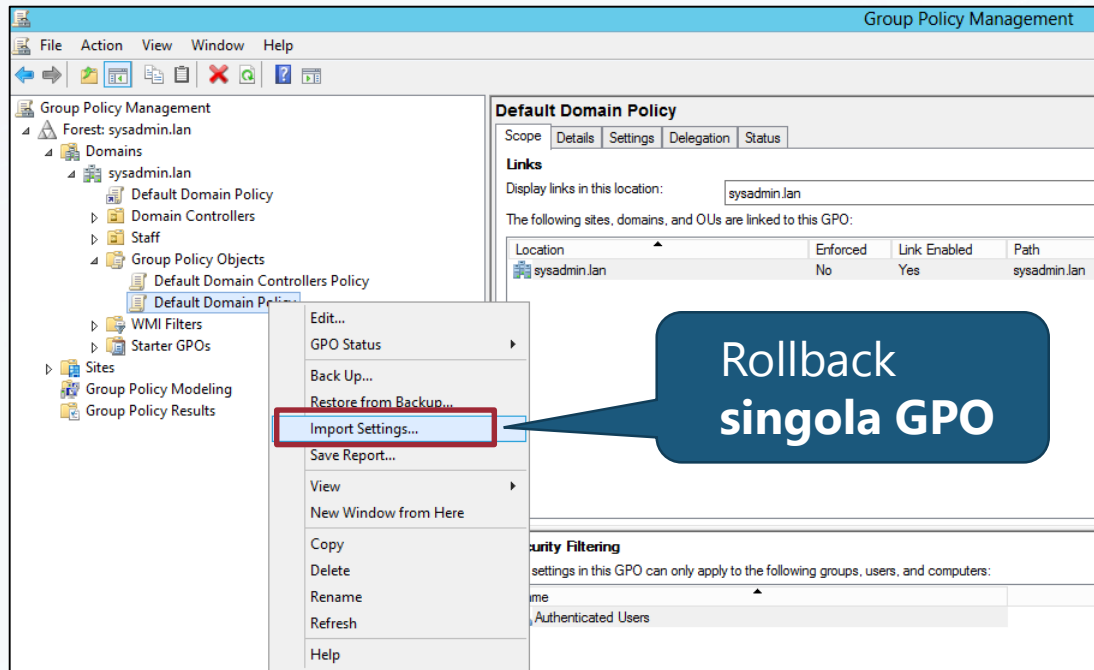
I backup eseguiti con PowerShell possono essere usati da GPMC e viceversa

The screenshot displays the Group Policy Management console with two overlapping windows. The left window shows the 'Group Policy Objects' tree with the 'Back Up All...' option highlighted in a red box, accompanied by a green callout bubble that reads 'Backup GPO multiple'. The right window shows the 'Default Domain Policy' details with the 'Back Up...' option highlighted in a red box, accompanied by a blue callout bubble that reads 'Backup singola GPO'. A third window, titled 'Back Up Group Policy Object', is open in the foreground, showing a dialog box for backing up a single GPO. The dialog box contains the following text: 'Enter the name of the folder in which you want to store backed up versions of this Group Policy Object (GPO). You can back up multiple GPOs to the same folder. Note: Settings that are external to the GPO, such as WMI filters and IPsec policies, are independent objects in Active Directory and will not be backed up. To prevent tampering of backed up GPOs, be sure to secure this folder so that only authorized administrators have write access to this location.' The 'Location' field is set to 'C:\Backup\GPO' and the 'Description' field contains 'Backup Maggio 2013'. There are 'Back Up' and 'Cancel' buttons at the bottom.

```
Backup-GPO -All -Path <string> [-Comment <string>]  
Backup-GPO [-Name] <string> -Path <string> [-Comment <string>]
```



Restore delle GPO



```
Import-GPO -BackupId <Guid> [-TargetGuid <Guid>] [-TargetName <string>]
Import-GPO [-BackupGpoName <string>] [-TargetGuid <Guid>] [-TargetName <string>]
Restore-GPO -All -Path <string>
Restore-GPO -BackupId <Guid> -Path <string>
Restore-GPO [-Name] <Name> -Path <string>
```



Demo



Torino
Technologies
Group

ICT  POWER.IT

Backup System State su VHD



Torino
Technologies
Group

ICT  POWER.IT

Active Directory Snapshots

Gestione del disaster recovery di Active Directory

Utilizzo Active Directory Snapshots

Utilizzo degli Snapshots

- Gli Snapshots *offrono un modo per avere una versione di AD con cui fare confronti senza dover eseguire un restore di un System State* su di un DC
- Gli Snapshots *non consentono di eseguire dei restore*, ma è possibile esportare gli oggetti e importarli
- Gli Snapshots sono *copie del ntds.dit montate su una porta LDAP diversa da quella di default* (389)

Creazione manuale Snapshot

```
NTDSutil  
Snapshot  
Activate instance NTDS  
REM Creazione Snapshot  
Create  
REM Elenco Snapshot  
REM compresi quelli del backup  
List all
```

C:\

1

Mount Snapshot

```
NTDSutil  
Snapshot  
List All  
Mount <snapshot GUID>  
Quit  
Quit
```

C:\

2

Connessione ad uno Snapshot

```
dsamain -dbpath <path>\ntds.dit -ldapport <portnumber>  
dsamain -dbpath c:\$SNAP_20112041648_VOLUMEC$\windows\NTDS\ntds.dit -ldapport 2222
```

3

C:\

Comando per la creazione schedulata di uno Snapshot

```
ntdsutil snapshot "activate instance ntds" create quit quit
```

C:\

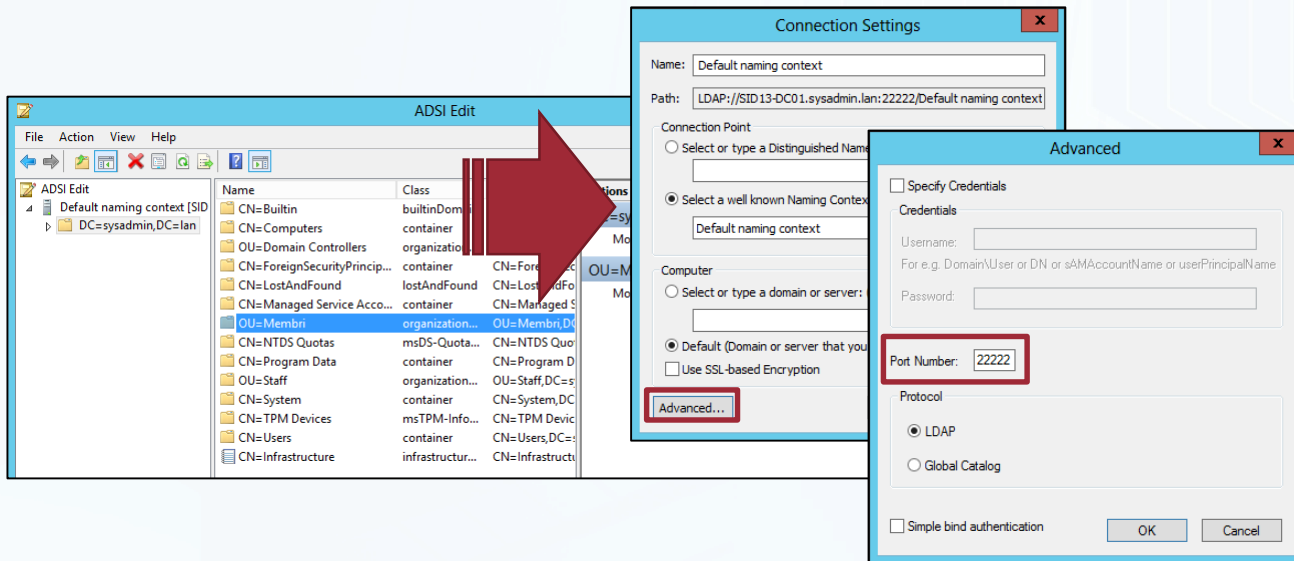
Eplorazione Active Directory Snapshots

Esplorazione e confronto

- Connessione tramite *Active Directory Users and Computers* (DSA.msc)
- Utilizzo di *LDIFE* per import ed export
- Utilizzo di *CSVDE* per import ed export con file CSV

Disconnessione Snapshot

- Dsomain cessa la connessione se:
 - Si preme CTRL+C
 - Si imposta l'attributo stopservice sull'oggetto rootDSE (per esempio nel caso di esecuzione remota)



Unmount e Delete Snapshot

NTDSutil
Snapshot

REM Unmount Snapshot

List Mounted

Unmount <snapshot number>

REM Unmount Snapshot

List All

Delete <snapshot number>

quit

Quit



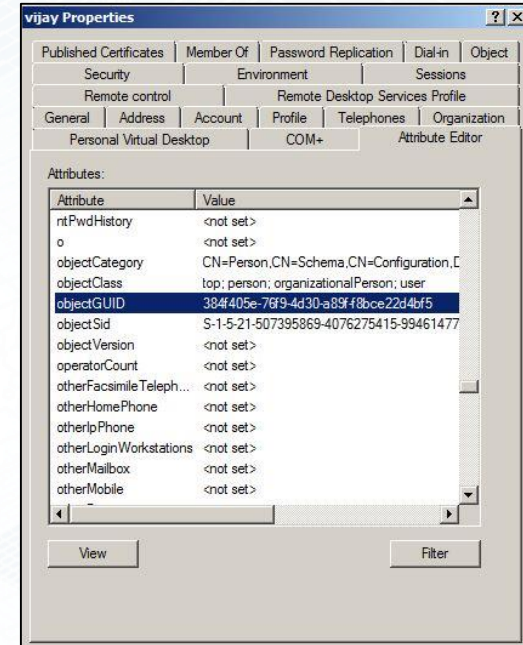
Snapshot Recovery Tools



Snapshot Recovery Tool ver.1.0.2rel (2009)



- *Tool a riga di comando* (oircmgr.exe) by Tomek Onyszko (MVP)
- *Recupero di oggetti cancellati o modificati* utilizzando come sorgente una connessione verso uno Snapshot montato
- **[Target options]**
 - o *objectGUID* GUID of object to recover. Multiple GUIDs can be specified separated with spaces
 - of *<file name>* Name of file which contains input data. Each GUID has to be specified in separated line
- **[Connection options]**
 - h *ldapHost[:port]* LDAP host in host:port format. If port will not be specified, default 389 port number will be used
 - sh *snapshot[:port]* Snapshot LDAP host in host:port format. If port will not be Specified, default 1389 port number will be used
- **[Recovery options]**
 - real Performs real recovery operation. By default this tool runs in preview mode
 - ol Recover object with recovering attributes from snapshot data. Specifying snaphsot connection option (-sh) is required



```
oircmgr.exe -o objectGUID -ol -sh snapshot[:port] -real  
oircmgr.exe -o fe6a3c0f-5e15-4022-b076-eacac4e1a23e -sh dc01.ictpower.lan -ol -real
```

Snapshot Recover Tool: <https://dirteam.com/tomek/2009/10/28/snapshot-recover-tool/>

Oh Snap! Active Directory Attribute Recovery With PowerShell: <https://blogs.technet.microsoft.com/ashleymcglone/2014/04/24/oh-snap-active-directory-attribute-recovery-with-powershell/>



StealthRECOVER

Demo



Torino
Technologies
Group

ICT  POWER.IT

Active Directory Snapshots



Torino
Technologies
Group

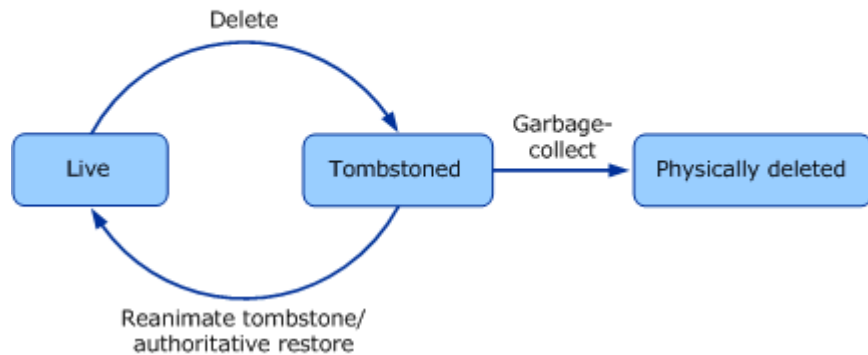
ICT  POWER.IT

Active Directory Recycle Bin

Gestione del disaster recovery di Active Directory

Ciclo di vita oggetti senza AD Recycle Bin

Active Directory Object Life Cycle in Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2 with Active Directory Recycle Bin Disabled



Oggetto in stato Tombstoned

- Oggetto *eliminato a livello logico* e spostato nel contenitore CN=Deleted Objects (modifica del DN dell'oggetto)
- L'oggetto *perde gli attributi di collegamento e la maggior parte degli attributi* (tranne quelli con searchFlags=0x8 nello schema)
- Durata del periodo pari all'attributo di foresta *tombstoneLifetime* (per default a null e pari a 180 giorni)

Protezione Oggetto

- *Opzione Proteggi oggetto da eliminazioni accidentali*
- Deny delete per Everyone
- Disponibile in WS2008 da GUI, in WS2003 abilitabile tramite DSACLs

Tombstone reanimation

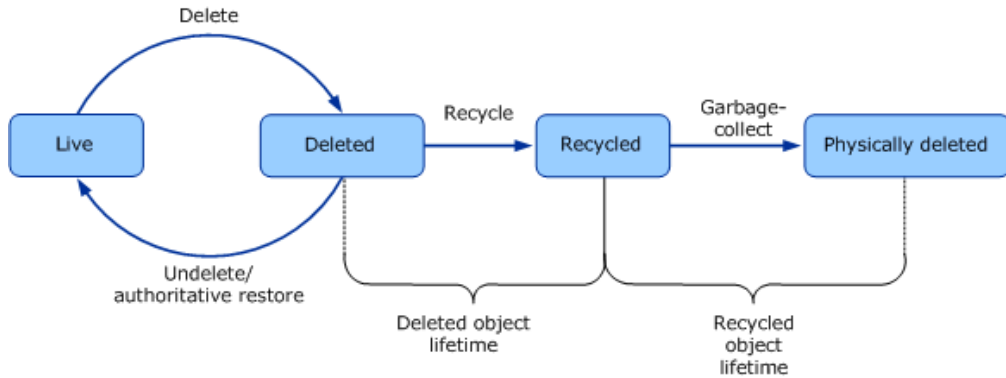
- Utilizzare *LPD* per *rimuovere il flag isDelete e modificare il DN*
- Utilizzare *ADRestore* tool a riga di comando by SysInternals (v1.1 del 2006)
- Utilizzare Veeam Explorer for Microsoft Active Directory

Restore utenti cancellati e group memberships (KB840001)

- *Metodo 1*: Restore utente cancellato e aggiunta utente ai suoi gruppi tramite Ntdsutil.exe
- *Metodo 2*: Restore utente cancellato e aggiunta utente ai suoi gruppi
- *Metodo 3*: Restore autoritativo utente cancellato e dei security groups due volte

Ciclo di vita oggetti con AD Recycle Bin

Active Directory Object Life Cycle in Windows Server 2008 R2 with Active Directory Recycle Bin Enabled



Funzionalità

- *Ripristino degli oggetti nello stesso stato logico* coerente in cui si trovavano
- *Gli account utente riottengono appartenenze ai gruppi e i diritti di accesso* all'interno del dominio e tra domini

Requisiti

- Richiede *livello funzionale foresta WS2008 R2* o superiore
- Tutti i DC nella foresta devono essere WS2008R2
- *Disattivato per default*
- *L'attivazione è irreversibile*

Oggetto in stato Deleted (Eliminato)

- *Attributo isDeleted a True* (presente su tutti gli oggetti introdotto con WS2000)
- *Eliminato a livello logico* e spostato nel contenitore CN=Deleted Objects (modifica del DN dell'oggetto)
- *Mantiene tutti attributi*, compresi quelli di collegamento
- Durata del periodo pari all'attributo di foresta *msDS-deletedObjectLifetime* (per default a null e uguale all'attributo tombstoneLifetime)

Oggetto in stato Recycled (Riciclato)

- *Attributo isRecycled a True* (presente su tutti gli oggetti introdotto con WS2008 R2)
- *Perde gli attributi di collegamento e la maggior parte degli attributi* (tranne quelli con searchFlags=0x8 nello schema)
- Durata del periodo pari all'attributo di foresta *tombstoneLifetime* (per default a null e pari a 180 giorni)

Attivazione AD Recycle Bin

Procedura di attivazione

- *Raise livello funzionale foresta a 2008R2* o superiore
- Abilitazione Recycle Bin sul *forest root domain*
- E' possibile eseguire raise e abilitazione tramite il *Centro di amministrazione di Active Directory* o *Powershell*

#Raise livello funzionale foresta

```
Set-ADForestMode -Identity ictpower.lan -ForestMode windows2008R2Forest
```

#Abilitazione AD Recycle Bin

```
Enable-ADOptionalFeature -Identity  
    'CN=Recycle Bin Feature,CN=Optional Features,  
    CN=Directory Service,CN=Windows NT,  
    CN=Services,CN=Configuration,  
    DC=ictpower,DC=lan'  
-Scope ForestOrConfigurationSet  
-Target 'ictpower.lan'
```



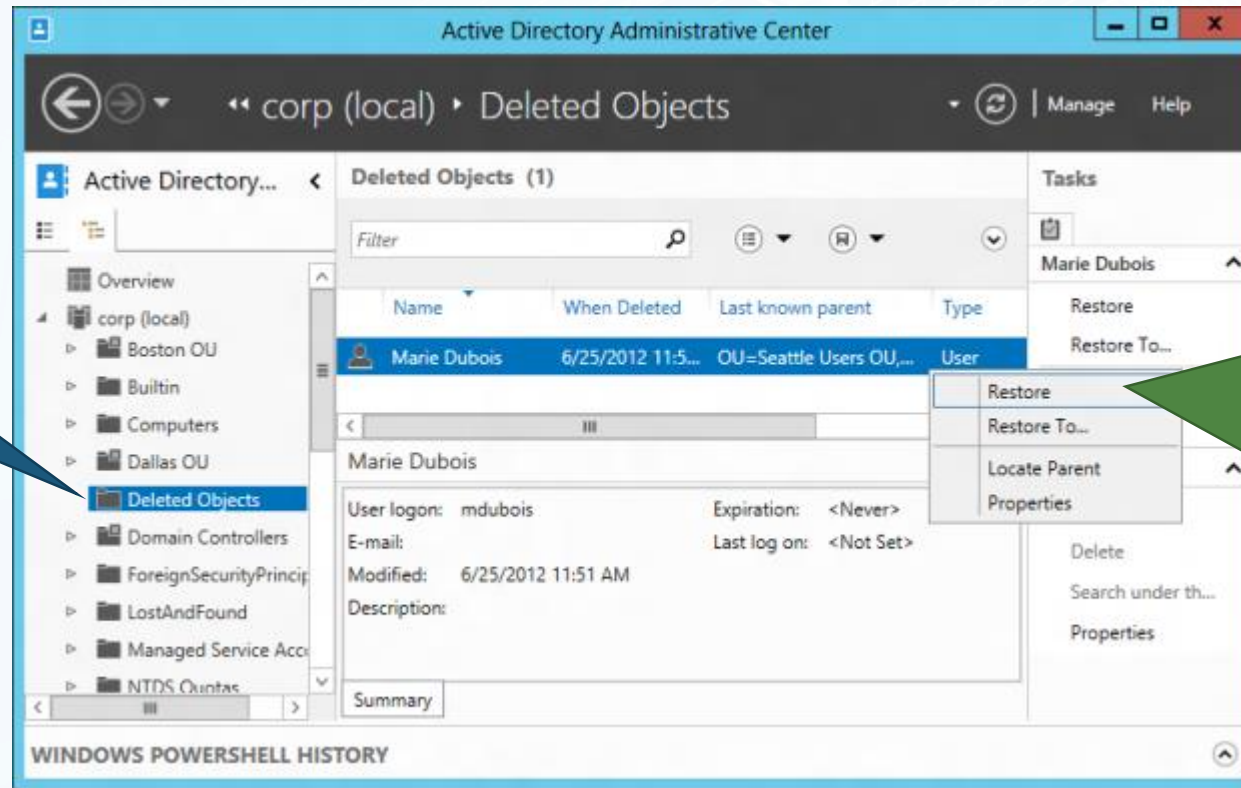
Considerazioni

- *Eliminazione fisica* dopo un periodo pari a $msDS-deletedObjectLifetime + tombstoneLifetime$ (Default 360 giorni)
- I *Recycled Object* sono *recuperabili solo con un Restore Autoritativo*
- La *validità dei backup di AD* è il *valore minore tra tombstoneLifetime e msDS-deleteObjectLifetime* (Default 180 giorni)
- *Se msDS-deletedObjectLifetime è minore del tombstoneLifetime non è possibile ripristinare un Recycled Object* con un restore autoritativo (dopo la replica gli oggetti ritornano Recycled)
- All'attivazione del recycle Bin *i Tombstoned objects diventano Recycled objects*, per recuperarli occorre un restore autoritativo da un backup precedente all'attivazione

Gestione AD Recycle Bin con ADAC

Novità
in
WS2012

Nel Centro di amministrazione di Active Directory è stato aggiunto il nodo **Deleted Objects**



E' possibile eseguire il **ripristino di un oggetto tramite Restore** o tramite **Restore To** per il **ripristino in posizione diversa dall'originale**

Gestione AD Recycle Bin con PowerShell

Impostazione attributi di foresta

#Impostazione msDS-DeletedObjectLifetime

```
Set-ADObject -Identity "CN=Directory Service,  
CN=Windows NT,CN=Services,CN=Configuration,  
DC=ictpower,DC=lan"  
-Partition "CN=Configuration,DC=ictpower,DC=lan"  
-Replace:@{ "msDS-DeletedObjectLifetime" = 365}
```



#Impostazione tombstoneLifetime

```
Set-ADObject -Identity "CN=Directory Service,  
CN=Windows NT,CN=Services,CN=Configuration,  
DC=ictpower,DC=lan"  
-Partition "CN=Configuration,DC=ictpower,DC=lan"  
-Replace:@{ "tombstoneLifetime" = 365}
```

Restore oggetti Deleted

#Restore singolo oggetto

```
Get-ADObject -Filter {sAMAccountName -eq "r.massa"}  
-IncludeDeletedObjects | Restore-ADObject
```



#Restore elenco oggetti

```
Get-ADObject -Filter 'Name -Like "*test*"'  
-IncludeDeletedObjects | Restore-ADObject
```

#Restore elenco oggetti in posizione diversa

```
Get-ADObject -Filter 'Name -Like "*test*"'  
-IncludeDeletedObjects | Restore-ADObject  
-TargetPath "OU=OU1,DC=ictpower,DC=lan"
```

Demo



Torino
Technologies
Group

ICT  POWER.IT

Active Directory Recycle Bin



Torino
Technologies
Group



Question & Answer