Capitolo 16: Troubleshooting, Disaster Protection & Recovery Active Directory

Introduzione

Lo scopo di questo capitolo è di fornire alcune informazioni utili in fase di identificazione e analisi dei problemi (i.e.: troubleshooting) quotidiani che si possono presentare in una infrastruttura Active Directory (AD) nonché di quelle azioni che bisogna intraprendere per prevenire e risolvere situazioni più complesse (i.e.: *Disaster Protection & Recovery*).

Troubleshooting

Con il termine *troubleshooting* s'intende il processo di identificazione, analisi e risoluzione di problemi e malfunzionamenti (o guasti) in qualsiasi contesto operativo. Per affrontare con sicurezza, determinazione e profitto il *troubleshooting* dei problemi in ambiente AD, è necessario avere acquisito e maturato tutti gli argomenti trattati in questo libro, oltre ad avere una profonda conoscenza della "strumentazione" ovvero degli attrezzi del mestiere o "*tools*".

Nel capitolo 6 "La soluzione Microsoft Active Directory Services" sono state fornite le informazioni sui tre kit standard a disposizione di un amministratore (i.e.: *AdminPak.msi*, *Support Tools*, *Resource Kit*) e le istruzioni su come installarli.

Oltre a questi, esistono spesso altre *utility* rilasciate successivamente da Microsoft e disponibili sul sito (e.g.: portqry.exe, dcgpofix.exe, *Group Policy Managemente Console*, ecc.).

Naturalmente, oltre ad avere una ottima conoscenza degli strumenti, è fondamentale acquisire nel tempo, e con l'esperienza maturata sul campo, delle vere e proprie strategie di *troubleshooting* che consentano di ottimizzare i tempi necessari a identificare e isolare le fonti di informazione primarie per la identificazione e la risoluzione dei problemi (e.g.: se esistono dei problemi di autenticazione in un contesto AD uno degli indiziati principali è quasi sempre il DNS (lato client o lato server oppure da entrambe le parti). Pertanto è

necessario iniziare ad effettuare dei test (e.g.: utilizzando nslookup) per verificare il buon funzionamento della risoluzione dei nomi DNS da parte dei client coinvolti).

Alcuni assiomi del Troubleshooting

- *Le persone brave sono brave perchè sono diventate sagge sbagliando (Anonimo).*
- *Dopo averle provate tutte, leggete le istruzioni (Assioma di Cahn).*
- *Qualsiasi programma non banale contiene almeno un bug. Non esistono programmi banali (Settima Legge della programmazione).*

Troubleshooting di problemi correlati al servizio DNS

Una errata configurazione del DNS (sia lato client che lato server) o un malfunzionamento di un server DNS può avere ripercussioni sulle seguenti attività:

- Risoluzione nomi.
- Autenticazione utenti.
- Registrazione dinamica sia dei resource record A e PTR (workstation/server/DC) che dei resource record DNS SRV relativamente ai soli DC.
- Promozione di server a DC (DCPROMO).
- Integrazione DNS/DHCP per la registrazione di computer client pre-Win2K.
- Applicazione di GPO.

Prevedere una configurazione DNS sicura e ridondata (i.e.: fault-tolerant)

Come si è visto nel capitolo 7 "DNS e Active Directory" il servizio DNS è assolutamente fondamentale per il buon funzionamento di tutta l'infrastruttura AD. Pertanto è importante garantire la sua disponibilità e integrità. Per questo è consigliato utilizzare, laddove possibile, come server DNS dei DC Win2K3 con le zone integrate in AD e configurate con la modalità di aggiornamento dinamica sicura (Secure Only).

In questo modo oltre a garantire la sicurezza nei riguardi della registrazione delle zone DNS si realizza una struttura multi-master e ad elevata disponibilità. Ciò in quanto:

1. *la registrazione in una zona DNS integrata in AD e "marcata" come "Secure Only" è possibile solamente agli Authenticated Users (i.e.: computer ed utenti autenticati da un qualsiasi DC di un dominio di una foresta).*

2. *ogni server DNS/DC abilitato alla replica riceve una copia della zona.*
3. *ogni zona integrata in AD ospitata da un DNS/DC è per definizione primaria. Pertanto configurando opportunamente i client dislocati nelle varie sedi, questi possono registrarsi nelle zone ospitate dai DNS/DC locali.*

Troubleshooting di problemi correlati alla replica AD e del servizio File Replication Service (FRS)

Un malfunzionamento della replica AD e del servizio *File Replication Service* (FRS) può avere conseguenze sulle seguenti attività:

- Disallineamento dei dati all'interno di AD (e.g.: utenti creati su un DC nella sede centrale non vengono replicati sul DC di una filiale remota).
- Autenticazione utenti.
- Disallinenamento GPO ed eventuale non applicazione delle GPO coinvolte. In alcuni casi è possibile che i problemi di replicazione siano localizzati solamente a livello di servizio FRS e non di AD (i.e.: la replicazione degli oggetti consultabili nel DIT (e.g.: tramite Active Directory Users and Computers) di AD avviene perfettamente). Pertanto può accadere che la componente AD di una GPO (i.e.: la GPC) viene replicata correttamente da un DC ai suoi partner di replica, ma non la componente SysVol (i.e.:GPT).

  Questi problemi possono verificarsi o a causa di un errore nel servizio FRS (cf. articoli Microsoft Knowledge Base 290762 "*FRS: Using the BurFlags Registry Key to Reinitialize File Replication Service Replica Sets*"e 292438 "*Troubleshooting journal_wrap errors on Sysvol and DFS replica sets*") oppure per difetti legati alla scelta dei protocolli di replica associati ai site link (e.g.: utilizzo del protocollo SMTP per interconnettere due site all'interno dei quali esiste almeno un DC appartenente a un dominio che è "rappresentato" in entrambi i site da uno o più DC). In quest'ultimo caso la replicazione della componente Sysvol delle GPO non può avvenire in quanto il servizio FRS utilizza il protocollo RPC/IP e non SMTP.

Alcuni problemi riscontrati con il service FRS di Win2K3 sono stati risolti con una *hotfix* pre-SP1 di Win2K3 (cf. Articolo Microsoft Knowledge Base: http://support.microsoft.com/?scid=kb;en-us;823230, "Issues that are resolved in the pre-Service Pack 1 release of Ntfrs.exe"). Come specificato all'interno del sopra citato articolo è consigliato installare la hotfix solamente se sono presenti i problemi ad essa connessi. Altrimenti si consiglia di attendere l'uscita del Service Pack 1 di Win2K3.

Implementare una infrastruttura AD ridondata

Per avere una garanzia di fault-tolerant sulla sopravvivenza dei dati AD (database, SysVol e Global Catalog) è necessario predisporre almeno due DC per ciascun

dominio opportunamente configurati. In presenza di una infrastruttura distribuita geograficamente, è necessario tenere conto anche della struttura fisica AD e della tipologia di connessioni WAN utilizzate per interconnettere le sedi, per dislocare opportunamente i DC, Global Catalog e DNS all'interno dei vari site. In generale assumendo un numero di utenti superiori a 100 per ogni sede remota ed in presenza di connessioni di rete abbastanza performanti è consigliato disporre in ogni site almeno di un server DNS, DC e GC.

Laddove vengano utilizzate delle GPO collegate ad alcuni site, è consigliato dislocare anche un DC del dominio root della foresta nel relativo site, in quanto gli oggetti GPC e GPT in tal caso appartengono sempre alla partizione corrispondente al dominio root.

Effettuare dei test su un DC per verificare se la replicazione AD e FRS avviene correttamente

Creare delle GPO di prova e verificare se sia la parte AD (GPC) che la parte Sysvol (GPT) si replicano correttamenet tra i DC di uno stesso dominio localizzati su uno stesso site (per semplicità e per non sovrapporre eventuali problemi dovuti alla topologia di replica inter-site).

Per testare il buon funzionamento della replica FRS è possibile anche (molto più semplicemente) creare un file di testo nella condivisone NETLOGON di un DC e verificare se viene replicato sugli altri DC del dominio.

Troubleshooting di problemi correlati ai domain controller

Alcuni problemi tipici legati alla gestione dei DC sono indicati nella tabella 1:

Table 1: Alcuni problemi tipici con i DC

Problema	Probabile messaggio di errore	Possibile Causa
Impossibile promuovere un server a DC	▪ DNS name does not exist ▪ DNS Lookup Failure. ▪ An Active Directory domain controller for the domain learning-solutions.local could not be contacted. ▪ Errore in fase di creazione di un oggetto	▪ L'indirizzo IP del server DNS di riferimento (*Preferred DNS Server*) è sbagliato. Verifica: eseguire da una sessione *Command Prompt* il comando nslookup. ▪ Verificare la corretta associazione della

	nella partizione Configuration nel site di riferimento corrispondente alla subnet IP di cui fa parte l'indirizzo IP del server.	subnet corrispondente al nuovo server/DC con il site indicato nell'errore.
Impossibile declassare un DC a server	▪ Pur non essendo stato inserito il flag "Questo server è l'ultimo DC del dominio" nessun altro DC per questo dominio può essere contattato. ▪ Il dominio indicato è inesistente.	▪ L'indirizzo IP del server DNS di riferimento (*Preferred DNS Server*) è sbagliato. Verifica: eseguire da una sessione *Command Prompt* il comando nslookup.

Forzare il declassamento di un DC a server anche in "condizioni off-line"

In alcuni casi è necessario forzare il declassamento di un DC a server anche in condizioni nelle quali il dominio di appartenenza non è raggiungibile. In questi casi, non volendo reinstallare il sistema operativo e desiderando trasformare il DC in server stand-alone è possibile utilizzare il seguente comando: dcpromo /ForceRemoval.

Prima di effettuare la suddetta procedura (tranne che il DC non sia l'ultimo della foresta) è necessario verificare se il DC è detentore di ruoli FSMO o svolge funzioni di Global Catalog. In tal caso ricordarsi di assegnare i suddetti ruoli ad altri DC.

Da notare che questa procedura non aggiorna i meta-data Active Directory relativi al DC declassato. Ciò rende necessario (tranne che il DC sia l'ultimo della foresta) effettuare la pulizia manuale secondo quanto indicato nella sezione "Rimuovere dal database AD i meta-data degli oggetti domain controller e domini".

A tal proposito si consiglia la consultazione dei seguenti articoli Microsoft Knowledge Base:

- *KB 332199: Domain controllers do not demote gracefully when you use the Active Directory Installation Wizard to force demotion in Windows Server 2003 and in Windows 2000 Server.*
- *KB 216498: How to remove data in Active Directory after an unsuccessful domain controller demotion.*

Install From Media (IFM): effettuare la promozione di un server a DC tramite la nuova opzione /ADV del wizard DCPROMO

Grazie all'opzione /ADV dell'utility DCPROMO di Win2K3 è possibile effettuare la promozione di un "additional domain controller" senza necessità di far replicare tutto il database AD e la SysVol via rete da un altro DC dello stesso dominio. In tal caso l'installazione viene eseguita "prelevando" le informazioni da un restore locale effettuato in "alternate location" di un System State (i.e.: da un supporto magnetico o media: da cui il termine IFM) valido effettuato su un altro DC dello stesso dominio e dotato di sistema operativo Win2K3 (la procedura non funziona se il backup del System State è originato da un DC Win2K). A tal proposito è consigliato che il System State utilizzato come sorgente (dal quale eseguire la restore locale in modalità "alternate location") sia prelevato da un DC abilitato come Global Catalog (GC). In questo modo, esiste la possibilità di far diventare il nuovo DC immediatamente GC con tempi di rigenerazione estremamente rapidi (che possono variare da circa 10' a poco più di un ora, a seconda delle dimensioni della foresta AD). Con l'installazione del Service Pack 1 di Win2K3 esiste la possibile di installare e configurare contestualmente anche il servizio DNS se il DC originario del backup del System State è un DNS server con la zona integrata in AD (DomainDNSZones e ForestDnsZones).

Da notare che la suddetta strategia richiede la presenza di una connessione di rete con un altro DC dello stesso dominio. Inoltre essa è utilizzabile solamente in caso di installazione di un "additional domain controller" e si dimostra assolutamente inutile per la reinstallazione di un eventuale primo e unico domain controller di un dominio AD Win2K3.

Per ulteriori informazioni sulla modalità di installazione IFM consultare l'articolo Microsoft Knowledge Base 311078:
http://support.microsoft.com/default.aspx?scid=kb;EN-US;311078.

Troubleshooting di problemi correlati al servizio DHCP

Alcuni problemi che si possono presentare nella gestione dei server DHCP in un contesto AD possono essere i seguenti:

- Problemi di autorizzazione a rilasciare indirizzi IP: ogni server DHCP Win2K/2K3 che si trova ad operare in un contesto AD deve essere autorizzato da un membro del gruppo Enterprise Admins (o utente/gruppo opportunamente appositamente delegato) per poter rilasciare indirizzi ai client DHCP. Eventuali server DHCP Win2K/2K3 configurati in modalità workgroup (pertanto non autorizzati e non autorizzabili in AD) che si trovano ad operare sulla stessa rete dove sono presenti dei server DHCP Win2K/2K3 autorizzati, verranno da questi ultimi automaticamente "disattivati" e sarà impedito loro di rilasciare indirizzi.
- Problemi di autorizzazione a registrare e/o aggiornare resource record in una zona DNS per conto dei client DHCP (*DHCP Proxy*) oppure presi in carico da un altro server DHCP: in caso di più server DHCP in configurazione fault-tolerant (regola

70/30, ecc.) è necessario inserire i relativi computer account dei server DHCP (ed in casi particolari anche dei client; soprattutto nel caso di aggiornamento di client Win9x a Win2K/XP con il server DHCP configurato per registrare solo i resource record PTR (default)) nel gruppo speciale *DnsUpdateProxy* in modo da autorizzare la presa in carico del record registrato (i.e.: in effetti permette di eseguire una *take ownership* sull'oggetto computer account) o da un client oppure da un diverso DHCP server che nel frattempo si è guastato o è stato dismesso.

Prevedere una procedura di backup/restore della configurazione di un server DHCP

Per facilitare la reinstallazione e relativa configurazione di un server DHCP Win2K3 è possibile sfruttare le nuove funzionalità di backup/restore dello snap-in DHCP di Win2K3 oppure utilizzare l'utility netsh nel modo seguente:

- *Backup: netsh dhcp server export <path-file-export> all*
- *Import: netsh dhcp server import <path-file-export> all*

Altrimenti, non avendo effettuato un precedente salvataggio della configurazione è possible automatizzare la creazione degli scope (e relative configurazione) con il comando netsh come di seguito indicato:

- *Creare un file con la definizione dei parametri dello scope:*

Ad esempio:
add scope 10.1.1.0 255.255.255.0 "Scope Milano, Piano 1, Subnet 1" "Sede Centrale Milano"
Scope 10.1.1.0 Add iprange 10.1.1.150 10.1.1.254
Scope 10.1.1.0 set state 1
Scope 10.1.1.0 set optionvalue 44 IPADDRESS "10.1.1.10" "10.1.1.11"
Scope 10.1.1.0 set optionvalue 51 DWORD "86400"
Scope 10.1.1.0 set optionvalue 3 IPADDRESS "10.1.1.1"
Scope 10.1.1.0 set optionvalue 15 STRING "learning-solutions.local"
Scope 10.1.1.0 set optionvalue 6 IPADDRESS "10.1.1.10" "10.1.1.11"
Scope 10.1.1.0 set optionvalue 46 BYTE "8"

- *Importare le configurazioni tramite il comando:*

  netsh -c "dhcp server" -r <NomeServerDhcp> -f <PathFileDefScope>

Esempio: netsh –c "dhcp server" –r 10.1.1.10 –f c:\temp\scope.txt

Troubleshooting di problemi correlati al database AD

Alcuni problemi correlati alle funzionalità del database AD possono essere i seguenti:

- Problemi legati allo spazio a disposizione sui volumi che ospitano il database e/o i file di log. Ciò può compromettere la generazione dei file di log per la gestione delle transazioni AD.
- Corruzione del database AD.
- Necessità di forzare una *deframmentazione off-line* (e.g.: per ridurre le dimensioni del DB dopo avere cancellato centinaia o migliaia di oggetti).
- Rimozione di *meta-data* di oggetti domain contoller e domini rimasti "orfani" in AD.

Per le operazioni di manutenzione del database AD e dei file di log consultare la sezione "La gestione del database AD" seguente.

Troubleshooting di problemi correlati ai ruoli FSMO

Un malfunzionamento ad un DC detentore di uno dei ruoli FSMO (*Flexible Single Master Operation*) può causare diversi problemi in una infrastruttura AD:

- Creazione di GPO e istanziazione di oggetti Security Principal (SP) (i.e.: utenti, computer e gruppi security): tipicamente determinata dal non disponibilità del DC che svolge il ruolo di PDC Emulator nel dominio. Da notare che problemi in fase di creazione di SP possono essere riscontrati anche a causa della indisponibiltà del DC RID Master, in caso di esaurimento del "blocco" di RID a disposizione di ciascun DC.
- Estensione allo Schema AD: dovuta alla indisponibilità del DC che detiene il ruolo di Schema Master oppure al fatto che sullo Schema Master la modifica allo Schema è stata disabilitata.
- Creazione e/o cancellazione di domini da una foresta: dovuta alla indisponibilità del DC Domain Naming Master.
- Riferimenti errati ad oggetti Security Principal di altri domini della stessa foresta (e.g.: in un gruppo Universale di un dominio A viene elencato un utente appartenente ad un dominio B, anche se l'utente è stato trasferito in un dominio C): ciò in genere è dovuto a problemi con il DC Infrastructure Master locale il quale non è in grado di aggiornare i riferimenti ad oggetti esterni al dominio (chiamati *phantom record*) tramite l'utilizzo del Global Catalog (GC) oppure in quanto il DC Infrastructure Master è esso stesso GC. In tal caso esso non sarà in grado di aggiornare i puntamenti ai "*phantom record*" in conseguenza di una cancellazione, spostamento o rinomina dell'oggetto remoto.

Per le operazioni di trasferimento e *seizing* dei ruoli FSMO si rimanda il lettore al cap. 11 "I ruoli Flexible Single Master Operation ed il Global Catalog in una infrastruttura Active Directory".

Troubleshooting di problemi correlati al Global Catalog

Il Global Catalog (GC) è uno degli oggetti più importanti in una infrastruttura AD sia mono-dominio che multi-dominio. Dalla sua disponibilità possono dipendere le seguenti attività:

- Creazione utenti.
- Autenticazione di utenti (escluso l'utente administrator) che per la prima volta eseguono un logon al dominio.
- Buon funzionamento di applicazioni integrate in AD (e.g.: Exchange 2K/2K3 o altre appplicazioni terze parti).

Effettuare dei test su un DC per verificare se è stato eletto come Global Catalog

Un modo molto semplice per verificare se un DC è stato configurato come Global Catalog, e soprattutto se, una volta inserito il relativo flag "Global Catalog", sia già in grado di accettare le richieste sulla porta TCP/3268 (in genere a seconda della struttura di rete l'operazione può anche non essere immediata) è il seguente:

portqry –n <IP o Nome DC> -e 3268 –p tcp

Esempio: portqry -n 10.1.1.10 -e 3268 -p tcp.

Alcuni malfunzionamenti in ambiente AD Win2K pre-SP3: "Lingering Objects"

In un contesto AD Win2K (Domain Controller, Server e workstation) esiste un problema noto (cf. articolo KB 293421" Domain Controllers Continue to Use Global Catalog Server After It Has Been Demoted") per il quale anche dopo il declassamento di un DC/GC Win2K a server, altri DC continuano ad inviare query LDAP/GC sulla porta 3268 provocando delle risposte errate e inutile traffico sulla rete. Per risolvere il problema è necessario applicare almeno il SP3. Naturalmente è consigliato installare sempre l'ultimo.

Un altro malfunzionamento noto (cf. articoli 314282 "Lingering objects may remain after you bring an out-of-date global catalog server back online" e 317097 "Lingering objects prevent Active Directory replication from occurring") è quello causato dal ritorno on-line di un DC/GC rimasto off-line (i.e.: spento, fuori rete o che non ha potuto replicare a causa di problemi di configurazione) per un numero di giorni superiore al valore del tombstoneLifetime (di default 60 gg), causando la rimessa in circolazione di oggetti cosiddetti "lingering objects" (i.e.: oggetti esistenti in partizioni read-only (i.e.: nel GC) che contengono alcuni attributi (e.g.: sAMAccountName) appartenenti ad altri oggetti "ancora in vita"). Essi possono presentare dei seri problemi di inconsistenza delle informazioni, di corretta replicazione AD e, non ultimo, di sicurezza. In Win2K pre-SP3 la cancellazione di tali

oggetti si presentava difficoltosa se non impossibile. In Win2K SP3 e Win2K3 questo problema è stato risolto inserendo la nuova voce "Strict Replication Consistency" nella chiave seguente dei registry HKLM\System\CurrentControlSet\Services\NTDS\Parameters. Il suo valore di default è 1 (1 = Strict Replication Consistency) in modo da rinforzare la consistenza delle informazioni: nessun oggetto viene accettato da un DC Win2K-SP3 o Win2K3, in conseguenza di un aggiornamento se esso non esiste nella sua replica locale. Viceversa forzando a 0 questa variabile su tutti i DC, si disattiva questo controllo permettendo la riesumazione dei "lingering objects" per tutto il dominio. Questo effetto viene identificato come "Loose Replication Consistency". Per eliminare i "lingering objects" è necessario utilizzare il seguente comando:

repadmin /RemoveLingeringObjects < Nome-DC> <GUID-DC-Sorgente> <NC>

dove <GUID-DC-Sorgente> è il GUID del DC che detiene una copia "scrivibile" della partizione o naming context (NC). Per ottenere il GUID eseguire il comando repadmin /shorepl <Nome-DC>.

Esempio:
repadmin /RemoveLingeringObjects ls-mi-dc-01 04c43d01-44ff-4d90-973e-0a68500c1a9b learning-solutions,dc=local /ADVISORY_MODE

Prima di eliminare fisicamente gli oggetti è consigliato utilizzare l'opzione /ADVISORY_MODE. Eessa equivale ad una modalità di tipo "trial" o di prova nella quale vengono solamente visualizzate le azioni che verrebbero portate a termine in caso di esecuzione normale.

Infine un altro problema noto era quello causato dalla "pubblicazione" di un Global Catalog non ancora completamente replicato che poteva causare malfunzionamenti in ambiente Exchange 2000/2003 (cf. Articolo KB 304403 "Exchange Considerations for Promoting a DomainController to A Global Catalog Server"). In Win2K SP3 e Win2K3 questo problema è stato risolto inserendo la nuova value "Global Catalog Promotion Complete" nella chiave seguente dei registry HKLM\System\CurrentControlSet\Services\NTDS\Parameters. Essa per default vale 1 ed impone al nuovo GC di "pubblicarsi" in AD solamente quando tutte le partizioni read-only del GC sono state completamente replicate.

Per ulteriori informazioni sul Global Catalog e sulla sua gestione si rimanda il lettore al cap. 11 "I ruoli Flexible Single Master Operation ed il Global Catalog in una infrastruttura Active Directory".

Documentazione

Il tema della documentazione degli oggetti che popolano un sistema informatico (i.e.: server (domain controller, file/print/application/database server), workstation, stampanti, router, firewall, proxy, switch, ecc.), in particolare basato su una infrastruttura AD, è spesso trascurato, adducendo varie motivazioni: mancanza di tempo, complessità e

dinamicità delle strutture, ecc. La mancanza di una documentazione dettagliata ed aggiornata si nota nel momento in cui è necessario effettuare delle operazioni di *disaster recovery* ovvero di ripristino di dati AD, server, domain controller, successivamente al verificarsi di eventi più o meno "catastrofici" (e.g: cancellazione di informazioni da AD, crash di DC, danneggiamento al database di AD, ecc.).

Quali informazioni devono essere previste nella documentazione del "sistema AD" ?

Alcune informazioni che certamente non possono mancare e che sono di vitale importanza in una operazione di ripristino di AD sono le seguenti:

- Struttura logica:
    - Layout della foresta.
    - Identificazione del *Forest Root Domain* (FRD).
    - Eventuali relazioni di fiducia o *trust* esistenti con altre foreste o domini WinNT o anche intra-foresta (e.g.: *shortcut trust*).
    - Domain Controller:
        - Nome host e FQDN.
        - Configurazione TCP/IP: indirizzo(i) IP, subnet mask, default gateway, DNS server, ecc.
        - Dominio di appartenenza.
        - Ruoli FSMO.
        - Se è abilitato come Global Catalog (GC).
        - Site di collocazione (struttura fisica).
        - Se svolge il ruolo di server DNS (se ospita zone integrate in AD (DNS o ADP (*Application Directory Partition*) o standard primaria/secondaria).
        - Password per *Directory Service Restore Mode* e/o *Recovery Console*.
        - Stato dei backup del System State (ed eventuali floppy disk di repair (*Emergengy Repair Disk* (ERD)) per DC pre-Win2K).
        - Presenza di un set di backup ASR (*Automated System Recovery*) nel caso di DC Win2K3.
        - Configurazione hardware:
            - Dischi e controller (IDE/EIDE/SATA/SCSI)
            - Partizioni/Volumi:
                - lettere di unità.
                - tipo di file system,
                - dimensione dei volumi.
                - Utilizzo: System Partition, Boot Partition, SysVol, Database AD, Log File AD, ecc.
            - Scheda Video
- Struttura Fisica:
    - Layout della topologia dei site:
        - Site Link:

        - Costi associtai ai connettori di replica.
        - Protocolli.
        - Schedulazione.
    - Site Link Bridge.
  - Dislocazione dei DC dei vari domini della foresta all'interno dei site.
  - Quali sono i GC per ogni site e per l'intera foresta.
  - Se in un site è stata abilitata la funzionalità di "*Universal Group Membership Caching* (UGMC)".
  - DC che agiscono da *Intersite Topology Generator* (ISTG) e *BridgeHead Server* (BS).

Uno strumento dalle mille risorse: Replication Monitor

L'utility Replication Monitor (compresa nei Support Tools di Win2K/2K3) costituisce un vero e proprio "coltellino svizzero" (o "swiss knife") dell'amministratore AD. Oltre a gestire tutte le attività legate alla replicazione AD (da cui il nome), tramite Replication Monitor è possibile effettuare le seguenti attività:

- *Generare un report completo sullo stato attuale della replica di un DC che comprende:*
  - *Informazioni generali sullo stato delle repliche.*
  - *Site, Site-Link (con i relativi costi), Site-Link Bridge e Subnet.*
  - *Ruoli FSMO.*
  - *Path dei file di log e del database NTDS.DIT*
- *Forzare una replica a cascata di tutti i DC della foresta (Synchronizing Each Directory Partition with All Servers" anche in modalità "push" (di default la replica AD avviene sempre in modalità pull: ovvero il DC origine della modifica avvisa i propri partner di replicazione, i quali si connettono per prelevare gli aggiornamenti).*
- *Visualizzarelo stato di allineamento delle GPO (GPC e GPT) (Show Group Policy Object Status).*
- *Consultare la lista di tutti i Global Catalog nella foresta (Show Global Catalog Servers in Enterprise).*
- *Visualizzare graficamente le connessioni di replica (connection-object) tra i DC in un site (Show Replication Topologies).*

Avvio di un server in modalità provvisoria

Per effettuare operazioni di "manutenzione straordinaria" su un server, e soprattutto su un DC, è necessario riavviare il computer premendo il tasto F8 in fase di startup. Ciò provoca la comparsa del menu "Advanced Startup Options" indicato in tabella 2.

Table 2: Menu opzioni di startup avanzate per un computer Win2K/XP/2K3

F8 Menu delle opzioni avanzate modalità provvisoria (*safe-mode*) ***F8***	
Safe Mode	Carica i dispositivi e driver di base senza i servizi di rete
Safe Mode with Networking	Safe Mode con i servizi di rete
Safe Mode with Command Prompt	Safe Mode senza interfaccia grafica (GUI) e senza servizi di rete
Enable Boot Logging	Effettua il log del caricamento di driver e servizi
Enable VGA Mode	Carica un driver universale per la scheda di rete
Last Known Good Configuration	Utilizza l'ultima configurazione "buona" conosciuta e che ha permesso di effettuare una procedura di logon con successo fino ad arrivare sulla shell del sistema operativo (Explorer)
Directory Service Restore Mode (DSRM): : solo per i domain controller	Permette di effettuare manutenzione sul database AD di un domain controller
Debugging Mode	Abilita la modalità di debug

Per operazioni di manutenzione su un DC è necessario selezionare la voce *Directory Service Restore Mode* (DSRM). Questa scelta determina l'avvio del sistema operativo in una modalità particolare, nella quale tutte le funzionalità Active Directory sono disabilitate (e.g.: servizi Netlogon, Kerberos KDC, File Replication Service (FRS), Intersite Messaging, ecc.). In questa modalità, il DC si comporta come un server *stand-alone* caratterizzato da una "*SAM* (*Security Account Manager*) *Off-Line*" valida solo per gestire l'accesso in DSRM, nella quale esiste, di default, solamente l'account administrator (oltre a guest disabilitato) a cui corrisponde la password specificata al momento della promozione del server a DC tramite l'utility DCPROMO. Infatti, effettuando la procedura di logon (*sequenza di tasti Control+Alt+Del* o *Secure Attention Sequence* (SAS), il terzo campo "*Log on to:*" non è disponibile.

Come effettuare il reset della password DSRM in ambiente Win2K3

Per forzare il reset della password di DSRM è necessario utilizzare l'utility NTDSUTIL nel seguente modo:

- *Aprire una sessione Command Prompt:*
- *Lanciare il comando NTDSUTIL.EXE:*
- *Dal prompt di NTDSUTIL inserire il comando Set DSRM Password (o le iniziali Set d p).*
  - *Dal prompt "Reset DSRM Administrator Password" inserire il comando*

seguente per reinserire la password per il DC locale (null):

reset password on server null

oppure:

reset password on server <AltroDC>

per forzare il cambio della password DSRM per un DC remoto.

- *Inserire e confermare la nuova password e digitare QUIT per uscire dal contesto "Reset DSRM Administrator Password".*

- *Digitare QUIT per uscire da NTDSUTIL*

*Attenzione: non è possibile modificare la password di DSRM mediante l'utility NTDSUTIL nel mentre si opera in DSRM (Errore: "Setting password failed. Win32 Error Code: 0x32. Error Message: The request is not supported."). Viceversa è possibile farlo da DSRM mediante la sequenza di tasti Control+Alt+Del e cliccando sul bottone "Change Password..." oppure inserendo il comando seguente: "net user Administrator *".*

Come effettuare il reset della password DSRM in ambiente Win2K

Dal SP4 in poi di Win2K è disponibile l'utility setpwd che permette di forzare il cambio password per la modalità DSRM.

Aggiungere utenti "amministrativi" al gruppo locale Administrators utilizzato in modalità DSRM

Di default l'utente administrator è l'unico (oltre guest) ad essere presente nella "SAM-Off-Line" utilizzata in modalità DSRM (per consultare la lista degli utenti è sufficiente eseguire il comando "net user" dal prompt dei comandi una volta che si è effettuata l'autenticazione in DSRM come utente administrator).

Per aggiungere ulteriori utenti amministratori per la gestione della modalità DSRM è necessario procedere nel seguente modo:

- *Riavviare il DC in modalità DSRM.*
- *Aprire una sessione Command Prompt ed eseguire i comandi seguenti:*
  - *Net user <NomeUtente> /add <Password>*

    Esempio: net user simoneR /add P@ssw0rd

    ***NB**: anche se non è richiesta nessuna password per la creazione di un nuovo account ciò non è un buon motivo per non inserirla !!!*
  - *Net localgroup Administrators /add <NomeUtente>*

    Esempio: net localgroup Administrators /add simoneR

Creazione di un floppy disk di ripristino della password (Password

Reset Disk) di un utente administrator per l'accesso in modalità DSRM

Oltre alla possibilità vista in precedenza di reset della password dell'utente administrator della SAM-Off-line è possibile generare un floppy disk di ripristino password, dalla finestra Windows Security dopo avere inserito la sequenza di tasti Control+Alt+Del, nel seguente modo:

- *cliccare sul bottone "Change Password...".*
- *Cliccare sul bottone Backup...*
- *Inserire un FD*
- *Il FD può essere utilizzato all'atto del logon nel caso in cui venga smarrita la password. In questo caso al primo tentativo di logon fallito per l'utente per il quale è stato generato il FD di reset della password, verrà visualizzata una finestra nella quale sio chiede di inserire il FD e di cliccare sul bottone Reset...*
- *Successivamente verrà presentata la finestra Reset the User Account Password nella quale occorre inserire la nuova password ed una "frase da utilizzare come hint".*

La gestione del Database AD

Operazioni di scrittura sul database AD e gestione dei file di log

Come si è visto nel capitolo 8, "La struttura logica di Active Directory", ogni domain controller (DC) o *Directory System Agent* (DSA) di un qualsiasi dominio di una foresta AD ospita una replica del database AD o *Directory Information Base* (DIB). Il contenuto di questo database dipende dalla sua posizione logica e fisica all'interno della infrastruttura AD, oltre che dal fatto di essere o meno un server DNS e di ospitare una zona integrata in AD ed eventuali altre partizioni applicative o *Application Directory Partition* (ADP). Il DIB di AD è basato su un database di tipo ISAM (*Indexed and Sequential Access Method*) gestito da un DBMS (*DataBase Management System*) chiamato ESE (*Extensible Storage Engine*) o *Jet-Engine*.

NTDS ISAM

NTDS ISAM è il database engine che gestisce le attività di registrazione e recovery del database NTDS.DIT (i.e.: il DIB di Active Directory).

Da notare che l'Event Viewer identifica come source delle suddette attività proprio il "servizio" NTDS ISAM.

Esso rappresentata una versione potenziata del *Jet-Engine* utilizzato da Microsoft anche per altre applicazioni (e.g.: WINS, Access, Exchange, ADAM, ecc.). ESE offre delle

buone performance e garanzie di scalabilità per gestire fino a decine di milioni di oggetti, ed è implementato mediante uno strato software o *database layer* che si interpone tra il DSA/DC ed il DIB, e può essere utilizzato anche da altre applicazioni grazie alle API (*Application Program Interface*) che ne espongonole funzioni di accesso (e.g.: MAPI, ecc.).

Nota sulle Dimensioni del database NTDS.DIT in un contesto di dominio Win2K/2K3 in modalità mista (mixed-mode o Domain Functional Level Win2K Mixed)

Anche se potenzialmente il DB NTDS.DIT può raggiungere dimensioni fino a decine di GB (alcuni test Microsoft sono stati eseguiti per DB di 62 GB), in uno scenario di migrazione di un dominio WinNT a Win2K/2K3 nel quale il dominio deve operare in modalità mista è raccomandato attenersi ai limiti "fisiologici" della SAM di un dominio WinNT (circa 40 MB).

Il cuore del database AD è costituito dal file NTDS.DIT che di default viene creato nella directory %SystemRoot%\NTDS secondo il modello di base contenuto nella directory %SystemRoot%\System32 ed utilizzato dal comando DCPROMO all'atto della promozione del server a DC. Oltre a NTDS.DIT esistono nella directory %SystemRoot%\NTDS altri file utilizzati dal DBMS ESE per la gestione dei log (e.g.: edb.log, edb*.log, res1.log e res2.log) e per il meccanismo dei *checkpoint* (edb.chk). Di default la dimensione di questi file è 10 MB.

Struttura del database NTDS.DIT

Ogni oggetto all'interno del DB NTDS.DIT è rappresentato da un record o riga. Ogni riga è costituita da un insieme di attributi o colonne (eccezione per alcuni attributi (e.g.: linked attributes o back link/forward link, che contengono riferimenti ad altri attributi (e.g.: memberOf, manager, directReports, ecc.) che sono implementati in tabelle separate per motivi di efficienza nelle ricerche).

Il DB ESE NTDS.DIT contiene le seguenti tabelle:

- *Schema table: contiene i tipi di oggetti che possono essere istanziati, le relazioni di dipendenza (genealogy constraints), attributi mandatori e opzionali, sintassi, ecc. Questa tabella presenta delle dimensioni limitate rispetto alle altre ed il suo contenuto ha una variabilità molto limitata nel tempo.*
- *Link table: contiene gli attributi di tipo linked attribute intercollegati da una relazione back link/forward link (cf. Capitolo 15 "Lo Schema di un SDS").*
- *Data table: contiene fisicamente gli oggetti che servono ad implementare utenti, gruppi, computer, OU, ecc.*

Come localizzare la posizione esatta del database e dei file di log di AD

Per localizzare con esattezza la posizione del database (NTDS.DIT) e dei log file di AD è possibile procedere in uno dei seguenti modi:

- *Identificare la seguente chiave dei registry e le variabili sotto indicate:*

  HKLM\System\CurrentControlSet\Services\NTDS\Parameters

  - *Database log files path*
  - *DSA Database file*
- *Aprire una session Command Prompt:*
  - *Settare la seguente variabile:*

    set SAFEBOOT_OPTION=DSREPAIR
  - *Lanciare il comando NTDSUTIL.EXE:*
    - *Dal prompt di NTDSUTIL inserire il comando Files.*
    - *Dal prompt "File maintenance" inserire il comando "Info".*
    - *Digitare QUIT per uscire dal contesto "File maintenance".*
  - *Digitare QUIT per uscire da NTDSUTIL.*

Ogni volta che viene eseguita una operazione su un DC che scatena una scrittura nel database o "*Write Request"* (i.e.: creazione/cancellazione di un nuovo oggetto, modifica di un attributo di un oggetto già presente o replica di oggetti e attributi da altri DC partner di replica), viene generata una transazione che contiene i *dati* coinvolti nella modifica (e.g.: displayName = Leone Randazzo) e i *meta-dati* associati (e.g.: numero di versione (USN), timestamp, GUID del server sul quale si è generata la modifica).

Che cos'è una transazione AD

Una transazione è una unità indipendente di esecuzione di operazioni su un database. Le operazioni che costituiscono una transazione formano un'unità atomica ovvero esse devono essere portate a termine tutte con successo oppure deve essere ripristinata la situazione precedente alla esecuzione della transazione. Un esempio di transazione è costituito dal trasferimento di soldi da un conto corrente ad un altro.

In AD una transazione è una operazione di scrittura attinente un singolo oggetto o attributo di un oggetto.

Scopo dei file di Log

AD utilizza i file di log per garantire l'integrità e la consistenza dei dati in caso di crash al sistema. Per tale motivo vengono gestiti i seguenti processi:

- *Logging: identifica il processo di registrazione in un file di log delle operazioni da effettuare nel database AD e nel file dei checkpoint delle operazioni già portate a termine con successo (committed).*
- *Recovery: identifica il processo che permette di ripristinare lo stato di consistenza di un database a seguito di un crash di sistema, riportando la situazione ad uno stato consistente precedente utilizzando le informazioni contenute nei file di log e di check-point.*

Le transazioni AD vengono immediatamente registrate in maniera sequenziale nel file di log corrente (edb.log) e contestualmente viene eseguita la modifica nella copia del database in memoria (*in-memory copy*). Ciò assicura che le modifiche vengano in ogni caso eseguite anche a seguito di uno shutdown o crash immediatamente successivo. E' compito del DBMS ESE aggiornare continuamente il database NTDS.DIT con le transazioni riscontrate nei file di log, aggiornando il contenuto del file di *checkpoint* (edb.chk) attraverso un meccanismo identificato come "*advancing the checkpoint*". Il *checkpoint* indica la posizione (transazione) fino alla quale tutte le operazioni di scrittura nel database sono state effettuate con successo (*stato di committed* della transazione). Eventi asincroni che possono forzare il trattamento dei file di log sono: backup/restore del System State, shutdown del DC.

Quando il file di log corrente raggiunge la dimensione massima di 10 MB (10.240 KB), il file corrente viene rinominato come edbHHHHH.log (dove H è una cifra esadecimale che può assumere valori da 0 a F (e.g.: edb00001.log, edb0000F.log, edb0001A.log, ecc.)) e viene creato un nuovo edb.log della stessa dimensione. Per una gestione più efficiente dello spazio disco, la gestione dei file di log avviene secondo una modalità chiamata *circular logging*. Essa consiste nel sovrascrivere i log più vecchi in maniera circolare, cancellando i file di log non più necessari una volta effettuate le scritture sul database NTDS.DIT ed aggiornato il file di *checkpoint*.

Per garantire la disponibilità di spazio anche in situazioni di emergenza o per le normali operazioni di deframmentazione on-line, il sistema predispone altri due file di riserva (res1.log e res2.log) delle dimensioni standard dei file di log. Essi vengono utilizzati nel momento in cui il sistema dovesse esaurire lo spazio a disposizione nel volume contenente il database e i file di log. Altri due fili di log temporanei per attività "di servizio" (e.g.: deframmentazione on-line, recover, situazioni di emergenza derivanti da sovraccarico, ecc.) del DBMS ESE sono: edbtmp.log e temp.edb.

In casi di chiusura non corretta del sistema (e.g.: mancanza di corrente, crash improvviso (*Blue Screen Of The Dead* (BSOD), ecc.) il DBMS ESE rileva una situazione anomala

controllando l'ultimo log scritto nel file. Se l'ultimo record non corrisponde ad uno "shutdown normale" ESE riapplica i log segnalati nel file di *checkpoint* (edb.chk) come segnalato nell'Event Viewer negli eventi elencati in tabella .

Table 3: Eventi tipici del processo di recovery del database Active Directory da parte del database engine NTDS ISAM

Source	EventI D	Descrizione
NTDS ISAM	300	NTDS (520) NTDSA: The database engine initiating recovery steps.
NTDS ISAM	301	NTDS (520) NTDSA: The database engine has begun replaying logfile C:\WINDOWS\NTDS\edb0000A.log.
NTDS ISAM	301	NTDS (520) NTDSA: The database engine has begun replaying logfile C:\WINDOWS\NTDS\edb.log.
NTDS ISAM	302	NTDS (520) NTDSA: The database engine has successfully completed recovery steps.

In assenza del file di *checkpoint* vengono rieseguite tutte le transazioni presenti nei file di log.

Da quanto finora affermato si può intuire come sia fondamentale in fase di acquisto dell'hardware per i DC pianificare l'utilizzo di controller e dischi performanti (nonchè di una adeguata cache di seconda livello che per i DC dovrebbe essere sempre di almeno 1 MB) e riservare uno spazio adeguato per i volumi che devono ospitare il database AD e i file di log (oltre che alla directory Sysvol).

Le dimensioni dei file NTDS.DIT dei vari DC devono essere uguali ?

Le dimensioni dei file NTDS.DIT localizzati sui vari DC non necessariamente devono avere le stesse dimensioni.

A tal proposito è bene ricordare che:

- *AD è un SDS replicato, distribuito e partizionato.*
- *Ogni DC possiede una replica locale del database NTDS.DIT che contiene almeno le partizioni Schema, Configuration e quella del dominio a cui appartiene il DC (oltre ad eventuali altre partizioni applicatine (e.g.: DNS o ADP personalizzate).*
- *Per ciò che riguarda la partizione di dominio il modello utilizzato da AD è di tipo multi-master. Ciò vuol dire che le richieste di scrittura (write request) possono avere origine in qualsiasi DC.*

Inoltre è importante osservare che la replicazione tra i DC si riferisce alle sole modifiche AD e non all'intero database NTDS.DIT.

Load Balancing e ottimizzazione delle performance di scrittura AD

Di default tutti i file utilizzati da AD per implementare il DIB (file di database, log e check point) vengono posizionati nella stessa directory %SystemRoot%\NTDS.

Per la maggioranza delle installazioni ciò non costituisce un problema. Viceversa, per installazioni di una certa dimensione (nelle quali le dimensioni del file NTDS.DIT possono essere anche diverse centinaia di MB o anche qualche GB) e nelle quali esistono delle notevoli richieste di accesso al database, Microsoft consiglia di dislocare i file nel seguente modo per migliorare le performance di I/O e rendere più agevole le eventuali operazioni di ripristino:

- *Sistema Operativo: utilizzare due dischi in mirroring.*
- *Database AD (NTDS.DIT): utilizzare un set di dischi in RAID5.*
- *Log File: utilizzare due dischi in mirroring.*

Come verificare la gestione dei file di log AD in un ambiente di test

Per verificare la generazione dei file di log in un ambiente di test è possibile effettuare le seguenti prove, suppondendo di operare all'interno di un dominio Win2K3 con i livelli funzionali Win2K3:

- *Creare una OU Utenti-Lab.*
- *Redirigere la posizione di default per la creazione degli utenti nella suddetta OU tramite il comando: redirusr ou=utenti-lab,<DN-Dominio>*
  - *Esempio: redirusr ou=utenti-lab,dc=learning-solutions,dc=local*
- *Aprire Windows Explore e posizionarsi nella directory %SystemRoot%\NTDS del DC sul quale si sta operando. Posizionando un'altra istanza di Windows Explorer su un altro DC partner di replica si possono osservare gli effetti sui file di log dovuti alla replica delle modifiche scatenate dalle operazioni eseguite sul precedente DC.*
- *Creare un numero elevato di utenti mediante il seguente comando:*

For /L %a in (1,1,10000) do net user Utente%a /add "P@ssw0rd" /Comment:"Descriszione Utente di Prova %a" /FullName:"Utente%a" /Domain

- *Da notare che è possible eseguire il comando di redirezione della posizione di default per la creazione degli utenti anche anche durante l'esecuzione del comando di creazione degli utenti.*

Attenzione: per visualizzare tutti gli utenti creati in un'unica finestra tramite lo snap-in Active Directory Users and Computers è necessario modifica le impostazioni del filtro: dal menu View, selezionare Filter Options e nel campo "Maximum number of items displayed per folder" inserire 10000.

Il processo di deframmentazione del database AD e la garbage collection

La deframmentazione è una operazione che consiste nella riorganizzazione degli spazi all'interno del database AD per consetire il riutilizzo delle aree liberate dalla cancellazione di oggetti. Questo tipo di deframmentazione viene chiamata *deframmentazione on-line* e viene eseguita di routine da ogni DC (è segnalata nell'Event Viewer dagli eventi 300 e 301 generati dal *database engine* NTDS ISAM). Essa produce degli oggetti chiamati *tombstoned*, che corrispondono agli stessi oggetti cancellati (eliminando molti degli attributi non essenziali) che vengono "parcheggiati" temporaneamente nel container nascosto *Deleted Objects* (il cui DN è: CN=Deleted Objects,<DN-Partizione>) della partizione di appartenenza dell'oggetto assegnando.

La partizione Schema non possiede un container Deleted Objects

La sola eccezione a questa regola è rappresentata dalla partizione Schema nella quale non essendo possibile cancellare oggetti non esiste questo container.

L'oggetto cancellato/*tombstoned* viene marcato tale imponendo l'attributo isDeleted = True. Ogni oggetto *tombstoned* è identificato da un DN con un formato particolare per garantirne l'univocità. Ad esempio, per l'utente "LudovicoR" appena cancellato esso è:

CN=Ludovico Randazzo\0ADEL:8953835b-05b8-4c12-a8a8-ca82f23b7efb,CN=Deleted Objects,DC=learning-solutions,DC=local.

Come consultare il container Deleted Objects e riesumare un oggetto cancellato

Per consultare gli oggetti tombstoned è necessario utilizzare l'utility LDP.EXE di presente nei Support Tools di Win2K3, nel modo seguente:

- *Eseguire il comando LDP.EXE.*
- *Connettersi ad uno dei DC del dominio ed effettuare il binding con un*

account con diritti amministrativi.

- *Selezionare dal menu view la voce Tree ed inserire il DN del proprio dominio AD (e.g.: dc=learning-solutions,dc=local).*
- *Abilitare il controllo LDAP "Return Deleted Objects Lightweight Directory" (cf. figura 1) nel modo seguente:*
    - *selezionare dal menu Options, la voce Controls.*
    - *Selezionare le voci Critical e Server Control Type (cf. figura 1).*
    - *Selezionare dalla lista Load Predefined la voce "Return Deleted Objects".*
    - *Cliccare prima su Check-out e poi su Check-in.*
    - *Confermare su OK.*
- *Forzare il refresh degli oggetti nell'arborescenza LDAP cliccando due volte sulla root dell'albero LDAP (cf. figura 2).*
- *Identificato l'oggetto tombstoned da riesumare cliccare con il tasto e selezionare Modify*
- *Eliminare l'attributo isDeleted inserendo all'interno della finestra Modify i seguenti valori:*
    - *Campo Attribute: isDeleted*
    - *Campo Values: lasciare in bianco*
    - *Nella sezione Operation selezionare la voce Delete e quindi cliccare sul bottone Enter*
- *Ripetere la precedente operazione inserendo all'interno della finestra Modify i seguenti valori:*
    - *Campo Attribute: distinguishedName*
    - *Campo Values: il DN nel quale riesumare l'oggetto*
    - *Nella sezione Operation selezionare la voce Replace e quindi cliccare sul bottone Enter*
- *Ripetere ancora l'operazione per inserire/modificare tutti gli attributi obbligatori per l'oggetto da riesumare secondo il tipo di classe.*
- *Alla fine cliccare sul bottone Run.*

Di default solamente i membri del gruppo Domain Admins possono eseguire le operazioni di "rianimazione" degli oggetti tombstoned. E' possibile, comunque, delegare questa operazione assegnando il permesso "Reanimate Tombstones" anche ad altri utenti e/o gruppi agendo tramite ADSI Edit sulla scheda Security, direttamente sulle proprietà della partizione.

Per eseguire una ricerca degli oggetti tombstoned è possibile impostare i seguenti filtri LDAP:

- *Ricerca di tutti gli oggetti tombstoned: (isDeleted=True).*
- *Ricerca solamente di tutti gli oggetti di classe User cancellati: (&(isDeleted=True) (objectClass=User)).*

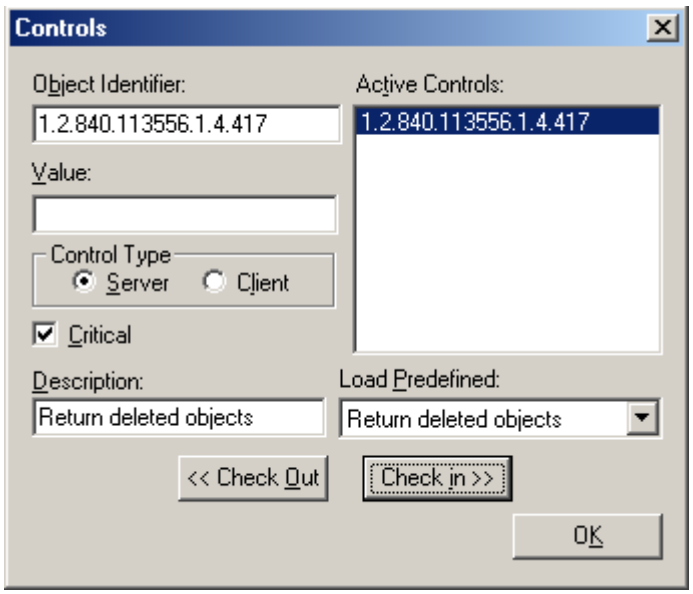

Figure 1: Abilitazione del controllo LDAP Return Deleted Objects

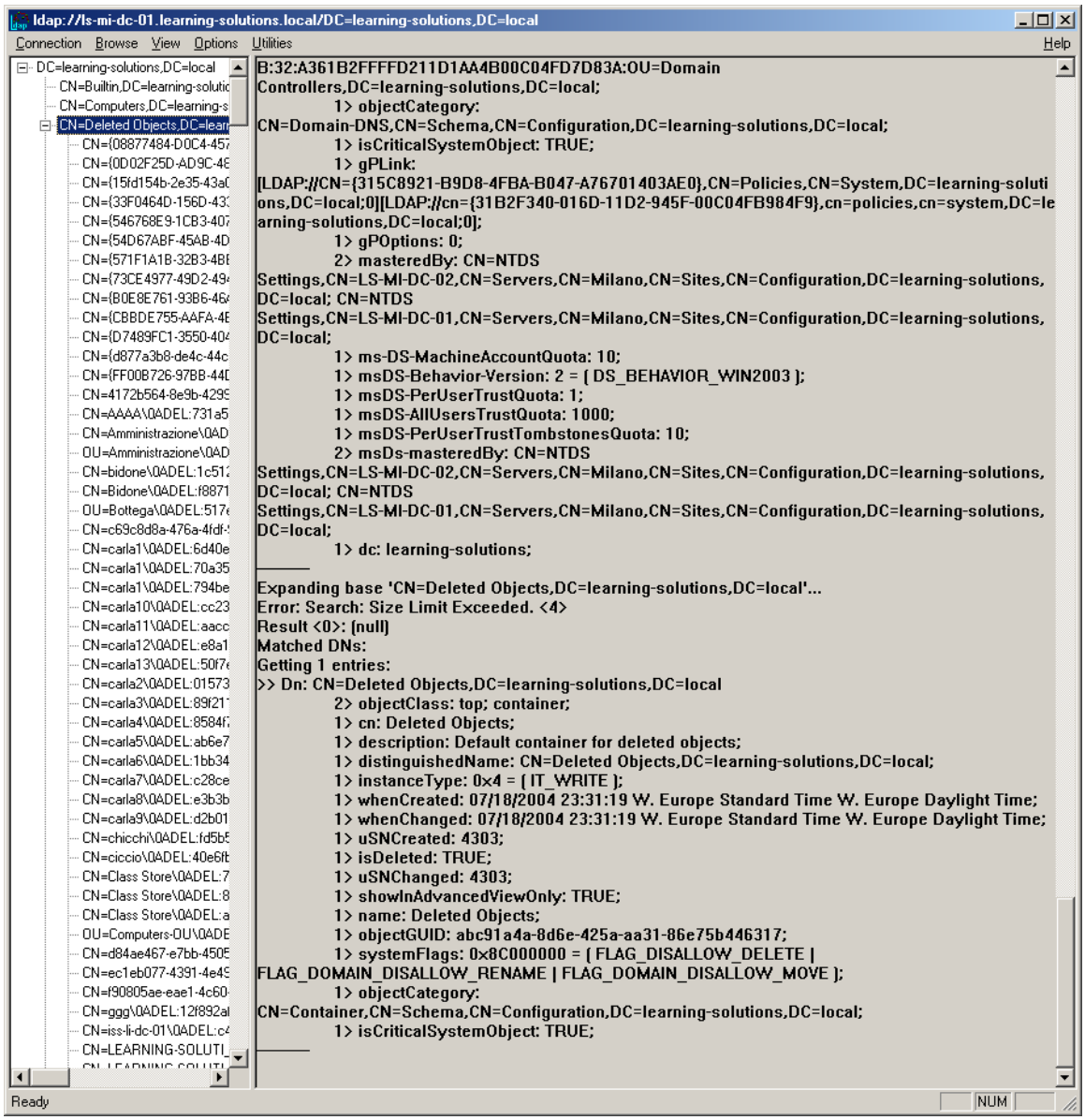

Figure 2: Browse degli oggetti *tombstoned* (container *Deleted Objects*) tramite LDP

Per default la permanenza degli oggetti *tombstoned* nel contenitore *Deleted Objects* è di 60 gg (con l'installazione del Service Pack 1 di Win2K3 questa soglia verrà portata a 180 gg per le nuove foreste, mentre in caso di aggiornamento è necessario modificare manualmente tale limite come di seguito indicato). Dopodichè ogni 12 h viene eseguita in *background* la procedura di *garbage collection* che consiste nella eliminazione fisica degli oggetti *tombstoned* dal contenitore *Deleted Objects*. Il ritardo nella "eliminazione fisica" degli oggetti *tombstoned* dal contenitore *Deleted Objects* è necessario, in un contesto di SDS replicato e distribuito geograficamente, per consentire a tutti i DC della foresta di essere messi al corrente della avvenuta cancellazione di un oggetto, tenendo conto dei ritardi "fisilogici" o latenze di propagazione della rete.

Modifica della tempistica di default della Garbage Collection

Anche se non consigliato, è possibile modificare la tempistica di default della Garbage Collection, la quale è valida per l'intera foresta AD.Pertanto la modifica richiede i diritti di Enterprise Admins.

A tal proposito è necessario

- *Eseguire il logon con un account avente i diritti di Enterprise Admins.*
- *Aprire lo snap-in ADSI Edit (adsiedit.msc).*
- *Identificare la partizione Configuration, e posizionarsi nel container: identificato dal DN:*

CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,<DN-Forest Root Domain>

Esempio:
CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=learning-solutions,DC=local

- *Cliccare con il tasto destro del mouse sul contenitore Directory Service e selezionare Properties.*
- *Identificare gli attributi:*
    - *"garbageCollPeriod": indica l'intervallo di tempo che scatena il processo di Garbage Collection per la eliminazione fisica degli oggetti tombstoned per ciascun DC della foresta.*
        - *Valore di default: 12 h.*
        - *Valore minimo: 1 h (viene applicato nel caso in cui viene impostato un valore inferiore a quello minimo consentito (e.g.: 0)).*
        - *Valore massimo consentito = 1/3 * tombstoneLifeTime*
        - *Esempio:*
            - *Se tombstoneLifeTime = 30 gg*
            - *Allora garbageCollPeriod Max = (30*24)/3= 240 h = 10 gg.*
    - *"tombstoneLifetime": indica l'intervallo di "sopravvivenza" di un oggetto tombstoned nel container Deleted Objects, dopo il quale esso viene eliminato definitivamente. Questo valore vale per l'intera foresta ed influisce sulla scadenza o validità dei backup del System State e sulla reintegrazione in rete di DC che sono rimasti off-line per un tempo superiore al tombstoneLifeTime. In tal caso nè i backup possono essere utilizzati nè i DC possono essere riconnessi alla rete.*
        - *Valore di default: 60 gg.*
        - *Valore minimo: 2 gg h (viene applicato nel caso in cui*

viene impostato un valore inferiore a quello minimo consentito (e.g.: 0)).

- *Attenzione: scegliere un valore che tenga conto del diametro della rete in modo tale da garantire la replica degli oggetti cancellati tra i DC posti "alle due estremità più lontane" della foresta. In altre parole, il tombstoneLifeTime deve essere maggiore del più elevato ritardo di replica (latenza) riscontrabile tra due qualsiasi DC in una foresta.*

Esiste una relazione tra gli oggetti tombstoned (Deleted Objects) e gli oggetti contenuti nel container LostAndFound ?

Non esiste nessuna relazione tra gli oggetti contenuti nei due contenitori Deleted Objects e LostAndFound, in quanto la prima contiene gli oggetti tombstoned definitivamente cancellati da AD, mentre la seconda contiene gli oggetti che sono rimasti "orfani" del loro contenitore, mentre venivano creati da un utente A su un DC A, quando nel frattempo un utente B operando sulla partizione di un DC B per errore lo cancellava.

Inoltre, esiste un altro tipo di deframmentazione identificata come *deframmentazione off-line* che forza la riorganizzazione delle aree libere in modo contiguo allo scopo di ottimizzare l'allocazione degli spazi (*compact*) e ottimizzare le operazioni di I/O e di ricerca.

Contrariamente alla *deframmentazione on-line* che viene eseguita in *background* dai DC, la *deframmentazione off-line* deve essere eseguita con il DC avviato in modalità provvisoria (*safe-mode*) tramite l'utilizzo del comando NTDSUTIL. Essa si ritiene necessaria o obbligatoria a seguito della cancellazione di migliaia di oggetti per ridurre le dimensioni fisiche del database NTDS.DIT. Ad esempio: dopo avere creato circa 10.000 (utilizzando lo script/batch precedentemente indicato) utenti il database ha raggiunto le dimensioni di circa 61,5 MB partendo da una dimensione iniziale di circa 14 MB (dominio appena creato). Dopo averli ricancellati, le dimensioni del file sono rimaste inalterate, in quanto AD ha eseguito solamente una *deframmentazione on-line*.

Deframmentazione Off-Line

La deframmentazione off-line è una operazione da eseguire DC-per-DC e consiste di due fasi:

- *Compattare il file del database in una nuova posizione, generando un nuovo file.*
- *Sovrascrivere il file originale con la nuova versione compattata.*

Per eseguire la deframmentazione off-line proseguire come sotto-indicato:

- *Eseguire un backup del System State del DC.*
- *Riavviare in modalità "Directory Service Restore Mode (DSRM)".*
- *Eseguire il logon con l'account administrator e la password della "SAM Off-Line".*
- *Eseguire una copia di backup del contenuto della directory NTDS.*
- *Aprire una sessione Command Prompt ed eseguire il comando NTDSUTIL.*
- *Al prompt di NTDSUTIL, inserire i seguenti comandi:*
    - *Inserire il comando Files.*
        - *Dal prompt "File maintenance" inserire il comando "Info": questo commando permette di visualizzare le informazioni sulla situazione attuale del database e dei file di log (i.e.: path, dimensioni, ecc.).*
        - *Identificare un volume contenente spazio a sufficienza per ospitare il nuovo file compresso ed inserire il comando seguente:*

          compact to unita:\directory

Esempio:

****

file maintenance: ***compact to c:\backup***

Opening database [Current].

Executing Command:

C:\WINDOWS\system32\esentutl.exe /d"C:\WINDOWS\NTDS\ntd

/t"c:\backup\ntds.dit" /p /o

Initiating DEFRAGMENTATION mode...

Database: C:\WINDOWS\NTDS\ntds.dit

Temp. Database: c:\backup\ntds.dit

Defragmentation Status (% complete)

0 10 20 30 40 50 60 70 80 90 100

|----|----|----|----|----|----|----|----|----|----|

.....

Note:

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.

Operation completed successfully in 90.891 seconds.

Spawned Process Exit code 0x0(0)

If compaction was successful you need to:

copy "c:\backup\ntds.dit" "C:\WINDOWS\NTDS\ntds.dit"

and delete the old log files:

del C:\WINDOWS\NTDS.log*

file maintenance:

****

- *Digitare QUIT per uscire dal contesto "File maintenance".*
- *Digitare QUIT per uscire da NTDSUTIL.*

- *A questo punto, come indicato dall'output del compact precedente, è necessario copiare il nuovo file compresso nella posizione di default e cancellare i file di log presenti (del *.log).*
- *Riavviare il DC.*

NB: come si può notare il comando di basso livello utilizzato da NTDSUTIL per effettuare le operazioni di manutenzione dul DB NTDS.DIT è ***esentutl.exe****. Questo comando può essere utilizzato in casi eccezionali anche per operazioni di recover del DB, come indicato nella sezione "Effettuare il ripristino di un database AD inconsistente".*

Esempio di utilizzo: esentutl.exe /?:
DESCRIPTION: Maintenance utilities for Microsoft(R) Windows(R) databases.

MODES OF OPERATION:
Defragmentation: ESENTUTL /d <database name> [options]
Recovery: ESENTUTL /r <logfile base name> [options]
Integrity: ESENTUTL /g <database name> [options]
Checksum: ESENTUTL /k <database name> [options]
Repair: ESENTUTL /p <database name> [options]
File Dump: ESENTUTL /m[mode-modifier] <filename>

<<<<< Press a key for more help >>>>>
D=Defragmentation, R=Recovery, G=inteGrity, K=checKsum, P=rePair, M=file duMp
=>

Prevenire attacchi di tipo Denial Of Service tendenti ad esaurire lo spazio disco a disposizione sul volume che ospita il database e i log file AD

Alcuni tipici attacchi a DC mirano ad esaurire lo spazio disco a disposizione sul volume dedicato al database e ai file log di AD, tenendo conto che anche cancellando gli oggetti in eccesso creati, AD impone la loro permanenza nel container Deleted Objects ancora per 60 gg (tempo di default stabilito dal parametro tombstoneLifeTime).

Nel capitolo 9 "Creazione e Gestione di Account Utenti, Grupppi e Computer in un contesto AD" si è visto come misura cautelativa l'imposizione di quote sul numero di oggetti istanziabili da un utente.

Un altra azione che si può intraprendere a tal proposito consiste nella creazione di un cosiddetto "file di riserva spazio" mediante l'utility fsutil.exe nativa di WinXP/2K3. Il file di riserva deve essere creato all'interno dello stesso volume contenente il database AD e i file di log e deve avere una dimensione pari ad almeno l'1% della dimensione del volume o comunque non inferiore a 250 MB. Dopo avere creato il file assegnare Full Control solamente al gruppo Administrators.

Per la creazione utilizzare il comando seguente:

fsutil file createnew <PathFileRiserva> <DimensioniInBytes>

Esempio: fsutil file createnew file-riserva.txt 262144000

In caso di necessità è sufficiente cancellare il file riserva per ripristinare la normale operatività del DC.

Spostare il file del database AD e/o i file di log

In caso particolari (e.g.: esaurimento dello spazio a disposizione sul disco che ospita i dati AD oppure per motivi di ridondanza ed ottimizzazione delle performance di I/O del DBMS ESE) può essere necessario spostare il file del database AD e/o i file di log da un volume/disco ad un altro.

Per effettuare le operazioni di spostamento seguire le seguenti istruzioni:

- Riavviare il DC in modalità "Directory Service Restore Mode (DSRM)".
- Eseguire il logon con l'account administrator e la password della "SAM Off-Line".
- Aprire una sessione Command Prompt ed eseguire il comando NTDSUTIL.
- Al prompt di NTDSUTIL, inserire i seguenti comandi:
    - Inserire il comando *Files*.
        - Dal prompt "*File maintenance*" inserire il comando "*Info*": questo commando permette di visualizzare le informazioni sulla situazione attuale del database e dei file di log (i.e.: path, dimensioni, ecc.).
        - Per spostare il file del database inserire il comando seguente:

Move db to %s

Dove %s corrisponde alla directory nella quale si desidera spostare il database.

- Per spostare i file di log inserire il comando seguente:

  Move logs to %s

  Dove %s corrisponde alla directory nella quale si desiderano spostare i file di log.

- Digitare *quit* per uscire dal contesto "*File maintenance*".

- Digitare *quit* per uscire dal comando NTDSUTIL.
- Riavviare il DC in modalità normale.

Effettuare il ripristino di un database AD inconsistente

Il ripristino o *recover* del database AD si ritiene necessario in casi eccezionali laddove all'avvio del DC viene presentato un errore di inconsistenza che impedisce il normale funzionamento.

A tal proposito esistono due possibili strade come indicato di seguito:

- Procedura standard di recover:
  - Riavviare il DC in modalità provvisoria e selezionare la voce "Directory Service Restore Mode (DSRM)".
  - Eseguire il logon con l'account administrator e la password della "SAM Off-Line"
  - Aprire una sessione Command Prompt ed eseguire il comando NTDSUTIL.
  - Al prompt di NTDSUTIL, inserire i seguenti comandi:
  - Inserire il comando *Files*.
    - Dal prompt "File maintenance" inserire il comando "Recover".
  - Digitare *quit* per uscire dal contesto "*File maintenance*".
  - Digitare *quit* per uscire dal comando NTDSUTIL.
  - Riavviare il DC in modalità normale.
- Procedura per casi eccezionali:
  - Riavviare il DC in modalità provvisoria e selezionare la voce "Directory Service Restore Mode (DSRM)".
  - Eseguire il logon con l'account administrator e la password della "SAM Off-Line"
  - Aprire una sessione Command Prompt ed eseguire il comando seguente:

    esentutl /r <path-db-ntds.dit>

    Esempio: esentutl /r c:\windows\ntds\ntds.dit

- Cancellare i file di log (*.log).
- Riavviare il DC in modalità normale.

Rimuovere dal database AD i meta-data degli oggetti domain controller e domini

Alcune delle situazioni che richiedono la pulizia dei meta-data AD sono le seguenti:

- Declassamento (DCPROMO) dell'ultimo domain controller di un dominio figlio senza avere selezioanto la voce "*This is the last domain controller in the domain*".
- Interruzione anomala della DCPROMO in fase di declassamento di un DC a server.
- Interruzione anomala della DCPROMO in fase di promozione di un server a DC (ciò può causare in futura l'impossibilità di aggiungere un altro DC con lo stesso nome del precedente server in quanto viene trovato nel database AD).
- *Crash* improvviso di un DC.

Per rimuovere i meta-data di un DC e tutte le informazioni interconnesse (i.e.: computer account del dominio, server object e relativi connection-object nella partizione Configuration e resource record DNS) seguire la seguente procedura:

- Autenticarsi con un account avente diritti Enterprise Admins.
- Aprire una sessione Command Prompt ed eseguire il comando NTDSUTIL.
- Al prompt di NTDSUTIL, inserire il comando *Metadata cleanup (o le iniziali m c)*.
    - Dal prompt "*Metadata cleanup*" inserire il comando "*connections*".
        - Dal prompt "*Connections*" inserire il comando "*connect to server <nomeDC>*" (e.g.: connect to server ls-mi-dc-01).
        - Digitare *quit* per uscire dal contesto "*Connections*".
    - Dal prompt "*Metadata cleanup*" inserire il comando "*Select operation target*".
        - Dal prompt "*Select operation target*" inserire il comando "*List domains*".
        - Identificare il numero del dominio di cui faceva parte il DC da rimuovere ed inserire il comando: *select domain* <NumeroDominio> (e.g.: *select domain* 0).
        - Dal prompt "*Select operation target*" inserire il comando "*List sites*".
        - Identificare il numero del site di cui faceva parte il DC da rimuovere ed inserire il comando: *select site* <NumeroSite> (e.g.: *select site* 0).
        - Dal prompt "*Select operation target*" inserire il comando "*List servers in site*".
        - Identificare il numero del server/DC da rimuovere ed inserire il comando: *select server* <NumeroServer> (e.g.: *select server* 1).

        - Uscire dal contesto "*Select operation target*" inserendo il comando quit.
    - Dal prompt "*Metadata cleanup*" inserire il comando "Remove *selected server*" e confermare l'operazione cliccando sul bottone Yes all'interno della finestra "*Server Remove Confirmation Dialog*".
    - Uscire dal contesto "*Metadata cleanup*" inserendo il comando *quit*.
- Digitare *quit* per uscire dal comando NTDSUTIL.
- Mediante lo snap-in ADSI Edit rimuovere tutte le entry relative al DC in questione dai seguenti container (corrispondenti al dominio ed al site di appartenenza del DC che sono stati utilizzati nella procedura NTDSUTIL)
    - OU=Domain Controllers,<*DominioCheContenevaDC*>.
    - CN=Servers,CN=<*SiteCheContenevaDC*>,CN=Sites,CN=Configuration,<*DN-ForestRootDomain*>
- Mediante lo snap-in DNS eliminare da tutte le zone (compreso la zona _msdcs.<FQDN-Dominio>) gli eventuali resource record DNS SRV, A e PTR riferiti al DC eliminato da AD.

Riassegnazione di eventuali ruoli FSMO e servizi svolti dal DC rimosso ad altri DC

E' bene verificare se il DC rimosso da AD possedeva dei ruoli FSMO o ospitava dei servizi strategici per AD e/o per l'infrastruttura di rete aziendale (e.g.: Global Catalog, DNS, DHCP, WINS, ecc.). Nel caso premurarsi a riassegnare ad altri DC i suddetti ruoli e servizi ed eventualemente aggiornare la configurazione delle workstation/server che puntavano staticamente al vecchio DC (e.g.: come server DNS e/o WINS).

Per rimuovere i meta-data di un dominio AD per il quale sono stati rimossi tutti i meta-data dei relativi DC (e.g.: è il caso della esecuzione della DCPROMO su un DC senza specificare di essere l'ultimo DC del dominio), seguire la seguente procedura:

- Autenticarsi con un account avente diritti Enterprise Admins.
- Aprire una sessione Command Prompt ed eseguire il comando NTDSUTIL.
- Al prompt di NTDSUTIL, inserire il comando *Metadata cleanup (o le iniziali m c).*
    - Dal prompt "*Metadata cleanup*" inserire il comando "*connections*".
        - Dal prompt "*Connections*" inserire il comando "*connect to server <nomeDC>*" (e.g.: connect to server ls-mi-dc-01).
        - Digitare *quit* per uscire dal contesto "*Connections*".
    - Dal prompt "*Metadata cleanup*" inserire il comando "*Select operation target*".
        - Dal prompt "*Select operation target*" inserire il comando "*List domains*".

        - Identificare il numero il dominio da rimuovere ed inserire il comando: *select domain* <NumeroDominio> (e.g.: *select domain* 1).
        - Uscire dal contesto "*Select operation target*" inserendo il comando *quit*.
    - Dal prompt "*Metadata cleanup*" inserire il comando "Remove *selected domain*" e confermare l'operazione cliccando sul bottone Yes all'interno della finestra "*Domain Remove Confirmation Dialog*".
    - Uscire dal contesto "*Metadata cleanup*" inserendo il comando *quit*.
- Digitare *quit* per uscire dal comando NTDSUTIL.

La successiva procedura permette di eliminare delle partizioni applicative e di dominio (essa richiede che siano stati rimossi tutti i meta-data dei relativi DC) che sono interdipendenti a causa di una relazione padre-figlio (e.g.: non è possibile eliminare un dominio Win2K3 se esiste ancora la relativa partizione applicativa DNS).

- Autenticarsi con un account avente diritti Enterprise Admins.
- Aprire una sessione Command Prompt ed eseguire il comando NTDSUTIL.
- Al prompt di NTDSUTIL, inserire il comando *Domain management (o le iniziali d m).*
    - Dal prompt "*Domain management*" inserire il comando "*connections*".
        - Dal prompt "*Connections*" inserire il comando "*connect to server <nomeDC>*" (e.g.: *connect to server* ls-mi-dc-01).
        - Digitare *quit* per uscire dal contesto "*Connections*".
    - Dal prompt "*Domain management*" inserire il comando "*list*".
        - Dal prompt "*Domain management*" inserire il comando "*Delete nc <DN-PartizioneDaEliminare>*" per la partizione ADP "figlia" da eliminare..

          Esempio:

          Delete nc DC=DomainDnsZones,DC=conferenze,DC=learning-solutions,DC=local.

        - Dal prompt "*Domain management*" inserire il comando "*Delete nc <DN-PartizioneDaEliminare>*" del dominio AD da eliminare.

          Esempio:

          Delete nc DC=conferenze,DC=learning-solutions,DC=local.

Segnalazione di errore in caso di esistenza di DC nel dominio AD da rimuovere

Se esistono ancora dei DC nel dominio AD che si sta cercando di eliminare viene segnalato il seguente errore:

"ldap_delete_ext_sW error 0x35(53 (Unwilling To Perform).
Ldap extended error message is 00002162: SvcErr: DSID-03100BB8, problem 5003 (WILL_NOT_PERFORM), data 0

Win32 error returned is 0x2162(The requested domain could not be deleted because there exist domain controllers that still host this domain.)."

Non è possibile ricreare un dominio con lo stesso nome fino a quando la modifica non è stata replicata a tutti i DC che detenevano un copia della partizione

E' importante notare l'avviso seguente, che segnala di non creare una partizione con lo stesso nome prima di aver dato il tempo a tutti i DC partner nella replica della partizione eliminata, di rimuoverla:

"The operation was successful. The partition has been marked for removal from the enterprise. It will be removed over time in the background.

Note: Please do not create another partition with the same name until the servers which hold this partition have had an opportunity to remove it. This will occur when knowledge of the deletion of this partition has replicated throughout the forest, and the servers which held the partition have removed all the objects within that partition. Complete removal of the partition can be verified by consulting the Directory event log on each server."

Segnalazione di errore nel tentativo di rimozione di un dominio/partizione che possiede delle partizioni "figlie"

Tentando di cancellare una partizione (e.g.: quella relativa al dominio DC=conferenze,DC=learning-solutions,DC=local) viene segnalato l'errore seguente:

"ldap_delete_ext_sW error 0x42(66 (Not allowed on Non-leaf).
Ldap extended error message is 00002015: UpdErr: DSID-03100B87, problem 6003 (CANT_ON_NON_LEAF), data 0

Win32 error returned is 0x2015(The directory service can perform the requested operation only on a leaf object.)
)"

Dovuto al fatto che il dominio possiede ancora una partizione figlia (e.g.: DC=DomainDnsZones,DC=conferenze,DC=learning-solutions,DC=local).

- Uscire dal contesto "*Domain management*" inserendo il comando quit.

- Digitare *quit* per uscire dal comando NTDSUTIL.

Utilizzare ADSI Edit in caso di necessità

In caso di necessità è possibile procedere tramite ADSI Edit per eliminare eventuali informazioni residue inerenti partizioni DNS applicative, domain controller, ecc..

Per ulteriori informazioni riguardo all'argomento trattato si consiglia di consultare i seguenti articoli Microsoft Knowkedge Base: 332199 "*Domain controllers do not demote gracefully when you use the Active Directory Installation Wizard to force demotion in Windows Server 2003 and in Windows 2000 Server*" *e* 216498 "*How to remove data in Active Directory after an unsuccessful domain controller demotion"*.

Pianificazione delle operazioni di backup in un contesto AD: backup del System State

Il *System State* identifica un insieme di informazioni intercorrelate che definiscono lo stato di un sistema/computer Win2K/XP/2K3 e che deve essere salvato tramite operazione di backup come una unità atomica (cf. figura 3). Ciò vuol dire che a causa delle relazioni di dipendenza esistenti tra i singoli componenti, il backup del *System State* è indivisibile. Il contenuto del *System State* può variare a seconda del tipo di sistema operativo e dei servizi installati su un computer, a partire da una base comune costituita dai seguenti elementi:

- Registry.
- File di boot (e.g.: ntldr, boot.ini, ntdetect.com) e file di sistema (contenuti nella directory %SystemRoot%\System32 e necessary per il caricamento del sistema operativo (e.g.: hal.dll, ntoskrnl.exe, smss.exe, ecc.).
- File di sistema sotto la protezione del meccanismo *Windows File Protection*.
- Database delle classi di registrazione COM+.

Attenzione: i registry del sistema sono contenuti nel System State e non più nel floppy Emergency Repair Disk (ERD) come per WinNT

E' da osservare che rispetto a WinNT i registry non si trovano più nel cosiddetto dischetto di emergenza o Emergency Repair Disk (ERD) ma sono parte integrante del System State. Inoltre, sempre rispetto a WinNT non esiste più il comando rdisk per la generazione del floppy ERD.

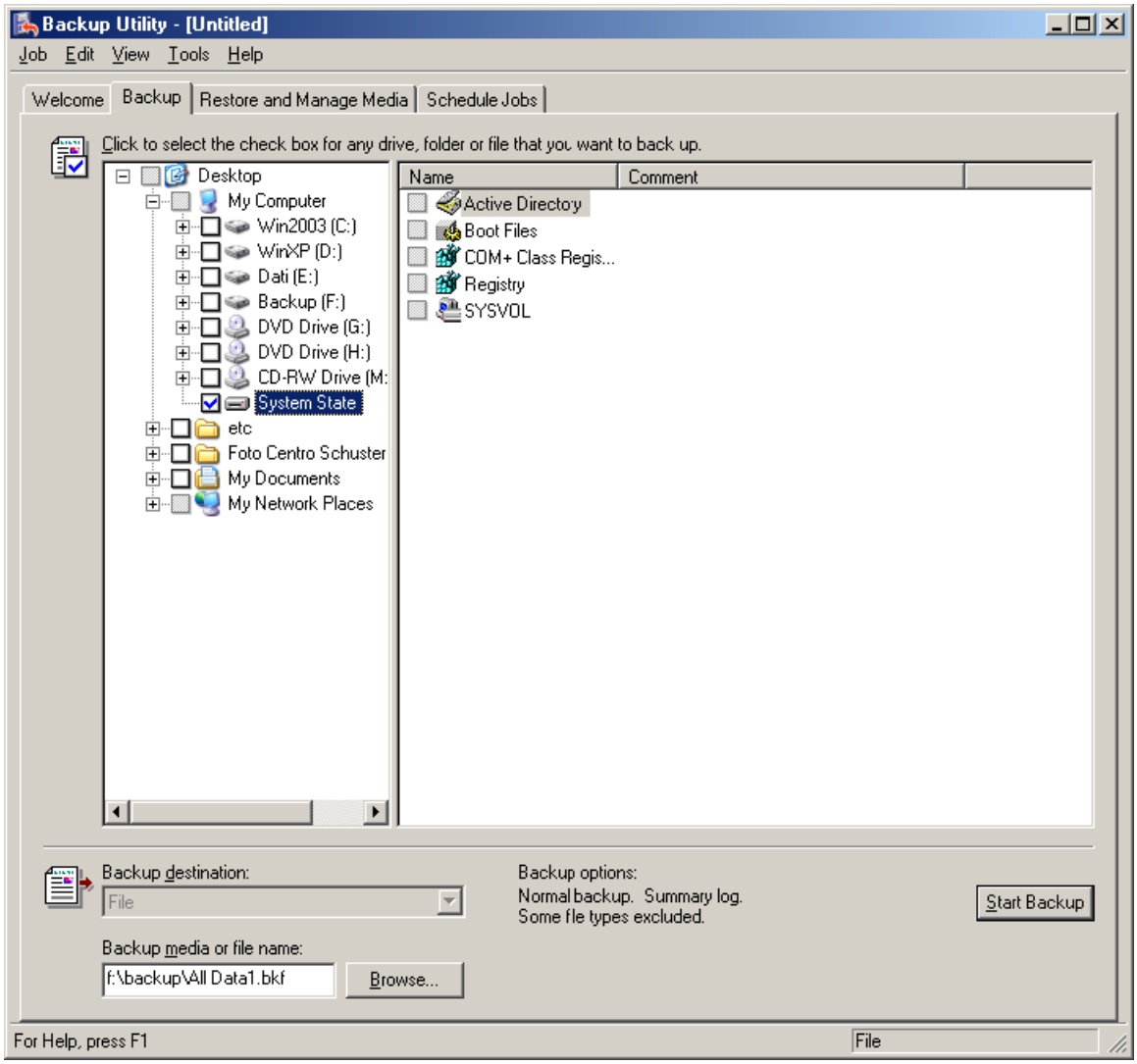

Figure 3: Contenuto del backup del System State

Altri possibili componenti del *System State* dipendono dal tipo di servizi installati e dalla configurazione di un computer. Essi possono essere:

- Active Directory + Sysvol: nel caso di un server Win2K/2K3 che promosso a DC.
- Certificate Services Database: nel caso di un server con il servizio Certificate Service installato.
- Configurazione del servizio cluster: nel caso di un server Win2K Advanced Server o Win2K3 Enterprise Edition configurato come nodo di un sistema cluster.
- IIS Metadirectory: solo se installato IIS.

Data l'importanza del *System State* in un contesto AD è necessario pianificarne il backup e, soprattutto, effettuare delle verifiche periodiche di restore.

Data di scadenza del System State e frequenza dei backup

Il backup del System State è soggetto a scadenza secondo le tempistiche impostate per la gestione del processo di garbage collection (di default 60 gg).

Ciò vuol dire che non è possibile ripristinare il backup di un System State effettuato in data antecedente i 60 gg. Ciò causerebbe il seguente errore:

"The operation failed because:

The attempt to restore Active Directory failed because the restored copy of Active Directory is too old.

Restored Active Directory age (days): XX
Maximum restored age (days): 60 (by default)"

Inoltre, è consigliato eseguire almeno un doppio backup degli oggetti di ogni partizione AD per avere la possibilità di poter ripristinare un qualsiasi oggetto cancellato erroneamente.

Per ottimizzare una eventuale fase di restore degli oggetti si consiglia di effettuare i backup del System State in modalità Full/Normal (i.e.: non incrementale nè differenziale).

A partire dal Service Pack di Win2K3 verrà registrato un nuovo evento nella sezione Directory Service dell'Event Viewer (event ID 2089) di un DC per comunicare lo stato dei backup delle partizioni da esso ospitate, in caso di superamento della metà dei giorni indicati dal tombstoneLifetime senza aver effettuato nessun backup del System State.

Alcune limitazioni del comando NTBACKUP nativo di Win2K/2K3

Alcune limitazioni del comando ntbackup nativo di Win2K/2K3 sono le seguenti:

- *Non è possibile effettuare il backup/restore del System State di un sistema remoto.*
- *Non è possibile eseguire il restore dal prompt dei comandi (i.e.: non esiste l'opzione restore del comando ntbackup).*

E' sufficiente il backup del System State di un DC per essere sicuri di avere a disposizione tutte le informazioni necessari per un ripristino in caso di crash ?

Per avere un salvataggio completo di tutta l'infrastruttura AD è necessario tenere in considerazione la configurazione del servizio DNS. Se le zone DNS sono integrate in AD allora nel System State sono contenuti i dati del DNS. Viceversa, è necessario

procedere con il backup della directory di sistema del DNS (%SystemRoot%\System32\DNS se si tratta di un DNS Microsoft).

Quali e di quanti server occorre eseguire il backup del System State ?

Per rispondere a questa domanda bisogna ricordare, come ripetuto tante altre volte, che:

- *AD è un SDS replicato, distribuito e partizionato.*
- *Ogni DC possiede una replica locale del database NTDS.DIT che contiene almeno le partizioni Schema, Configuration e quella del dominio a cui appartiene il DC (oltre ad eventuali altre partizioni applicatine (e.g.: DNS o ADP personalizzate).*

Pertanto, per avere la certezza di poter ripristinare degli oggetti erroneamente cancellati in un qualsiasi dominio di una foresta è necessario disporre del backup del System State di almeno un DC rappresentante per ciascun dominio. Dovendo scegliere tra tanti DC è consigliato selezionare sempre i DC che detengono i ruoli FSMO o che sono anche Global Catalog.

Per motivi di ottimizzazione delle eventuali operazioni di ripristino, è consigliato effettuare il backup del System State di un DC di ogni dominio rappresentato in un site.

Oltre ai DC è necessario ricordarsi di effettuare i backup dei server che forniscono servizi "infrastrutturali" per AD: DNS, DHCP ed eventualmente WINS.

Pianificazione delle operazioni di restore del System State in un contesto AD

Il restore del *System State* in un contesto AD è un'operazione delicata e importante in quanto tutti i DC sono impegnati continuamente a replicare le informazioni inerenti le partizioni tra loro condivise. Tutti i DC potenzialmente possono replicare oggetti delle partizioni Schema e Configuration, mentre solamente i DC appartenenti ad uno stesso dominio possono, e devono, replicarsi le informazioni in esso contenute.

In generale esistono quattro possibilità di restore del *System State* in un contesto AD:

- *Alternate* location o restore in una posizione alternativa.
- *Primary restore* o restore primario.
- *Normal restore* o restore non-autoritativo.

- *Authoritative restore* o restore non-autoritativo.

Nella scelta di una metodologia per il restore occorre tenere in considerazione i seguenti fattori:

- Il backup del *System State* effettuato su un DC contiene tutte le informazioni relative alla replica di AD (e.g.: database NTDS.DIT, file di log e SysVol) da esso ospitata (oltre a informazioni sui Registry, file di boot, ecc.). Tutti gli oggetti AD contenuti in un set di backup del *System State*, sono caratterizzati dal *timestamp* e dal *version number* (o *Update Sequence Number* (USN)) relativi alla data e ora di effettuazione del backup.
- Una operazione di backup o restore del *System State* coinvolge complessivamente tutto il blocco di informazioni relativo ad un computer, e non è possibile selezionare solamente alcuni componenti (se non operando un *restore in alternate location*, come di seguito indicato).
- Infrastruttura logica AD: quanti altri DC esistono all'interno dello stesso dominio o di altri domini.
- Infrastruttura fisica AD: quanti altri DC esistono nello stesso site dello stesso dominio o di altri domini.
- Se alcuni o tutti gli oggetti AD (e.g.: l'intero database AD o solo una OU (con il relativo contenuto) o solamente un utente) ripristinati con il restore del System State devono essere "imposti" agli altri DC oppure se essi saranno soggetti alla replica degli altri DC partner dello stesso dominio o di altri domini della stessa foresta ?

Restore "FRS-aware" e "non-FRS-aware"

Il restore eseguito su server non DC è sempre di tipo non-FRS-aware, nel senso che il server assume di far parte di un ambiente "non replicato" (tranne che non faccia parte di un set di replica DFS) e che non esistano altre repliche su altri server. Esso pertanto è da considerarsi un restore autoritativo. Viceversa nel caso di un DC il restore è inteso sempre di tipo FRS-aware, nel senso che il DC assume di default di trovarsi in un ambiente "replicato" nel quale possono esistere altri DC ciascuno dotato di una propria replica. In tal caso il restore è di default non-autoritativo (i.e. il flag "*When restoring replicated data sets, mark the restored data as the primary data for all replicas*" *non è inserito).*

Attenzione !

1. *Quando si effettua il restore del System State senza specificare l'opzione "Alternate Location", vengono sovrascritte tutte le informazioni inerenti il set di informazioni del System State sul computer sul quale avviene l'operazione di restore (compreso i registry).*
2. *Il restore del System State su un DC richiede il riavvio del computer in modalità DSRM.*

Restore del System State in una posizione alternativa

Il restore in "*Alternate location*" del *System State* si effettua selezionando l'opzione "*Restore file to: Alternate Location*" nella scheda "*Restore and Manage Media*", come indicato in figura 4. Nel caso di un domain controller Win2K3 le componenti ripristinate nella directory indicata come locazione alternativa (e.g.: C:\NtdsRestore) sono i seguenti:

- Active Directory
- Boot Files.
- COM+ Class Registration Database
- Registry.
- SysVol.

Questo tipo di restore viene effettuato nei casi in cui è necessario recuperare, su un computer diverso da quello sul quale è stato generato il *System State*, solamente alcune parti (e.g.: singole GPO o parte dei registry) senza rischiare di sovrascrivere completamente i dati del *System State* del computer sul quale si opera, oppure in preparazione della promozione di un domain controller addizionale (i.e.: additional domain controller) in un dominio tramite il comando DCPROMO /ADV (i.e.: *modalità Installa From Media* (IFM)).

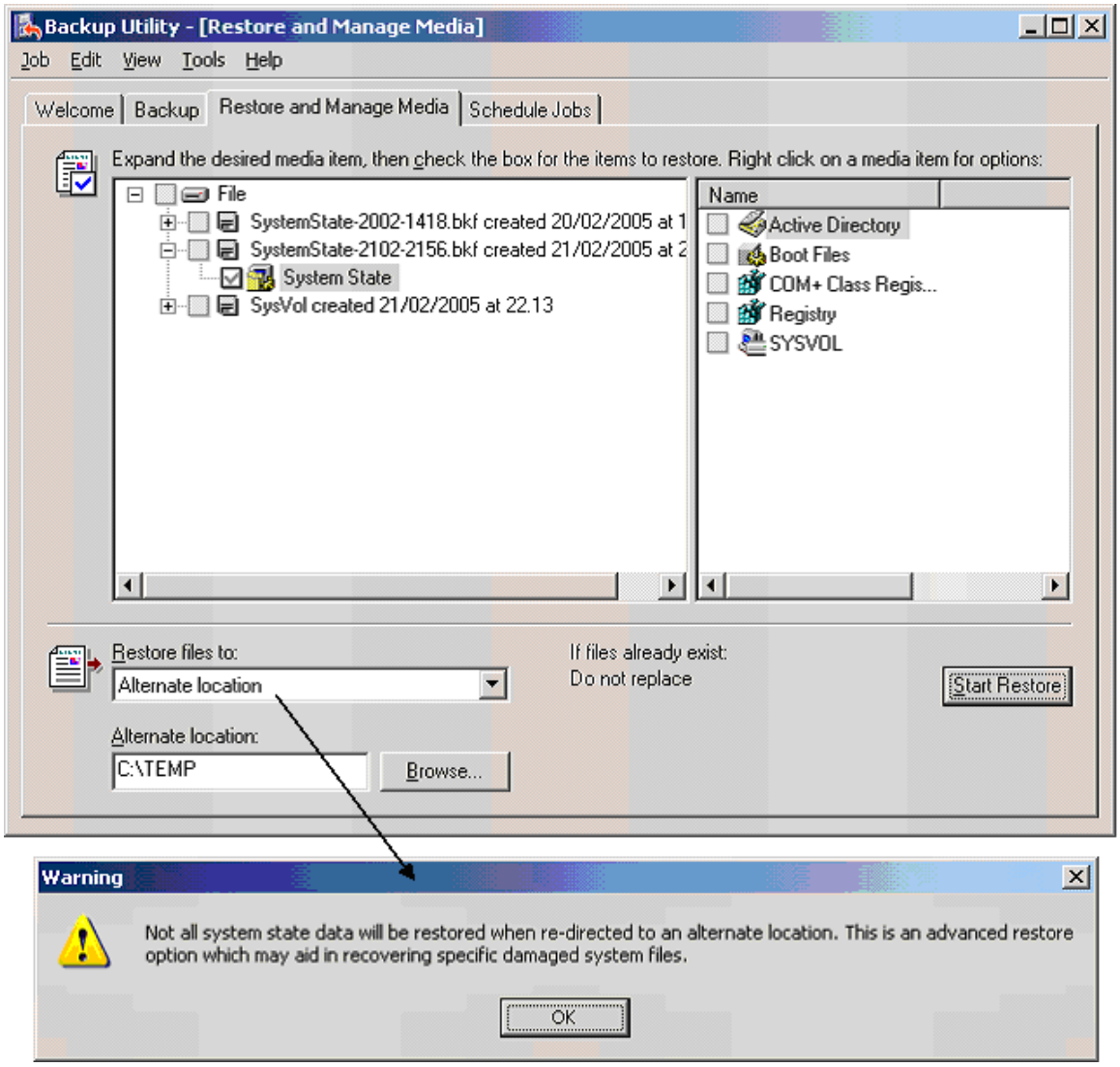

Figure 4: Restore del System State in una posizione alternativa (Alternate Location)

Restore primario

Il restore primario viene effettuato nel caso in cui un server o DC è l'unico all'interno di un set di replica (FRS, SysVol) oppure se intenzionalmente si vuole forzare il contenuto a tutti gli altri server dello stesso set di replica. Viene utilizzato solamente in caso di ricostruzione di una infrastruttura AD o FRS (e.g.: DFS) nella quale tutti i DC di uno stesso dominio hanno avuto dei problemi e devono essere reinstallati. Un'altra "situazione problematica" nella quale è richiesto di effettuare un restore primario è quella citata nei due seguenti articoli: Microsoft Knowledge Base 290762 "*FRS: Using the BurFlags Registry Key to Reinitialize File Replication Service Replica Sets*"e 292438 "*Troubleshooting journal_wrap errors on Sysvol and DFS replica sets*".

Per effettuare un restore primario è necessario seguire la seguente procedura:

- Avviare l'utility NTBACKUP.
- Selezionare la scheda *Restore and Manage Media* e selezionare i file da ripristinare (e.g.: System State).
- Cliccare sul bottone *Start Restore*.
- Cliccare sul bottone *Advanced* e selezionare la voce "*When restoring replicated data sets, mark the restored data as the primary data for all replicas*".

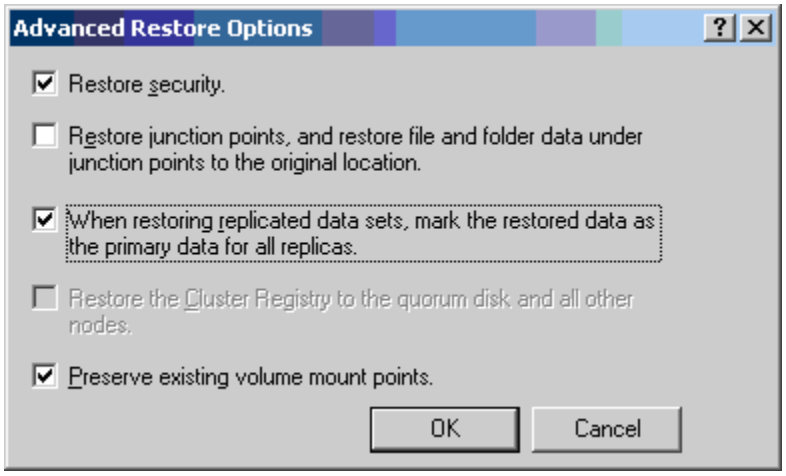

Figure 5: Restore Primario

Attenzione !

Eseguire un restore primario solamente in caso di "disastro" e quando nessun altro membro dello stesso set di replica (o domain controller di dominio) è stato precedentemente ripristinato.

Restore normale o non-autoritativo

Il restore normale o non-autoritativo (modalità di default) del *System State* di un DC viene effettuato per ripristinare un DC nello stato corrispondente alla "fotografia" del suo *System State*, rispetto alla data e ora della sua esecuzione. Ciò vuol dire che tutti gli oggetti AD verranno ripristinati dal set di backup nel loro stato originale. Successivamente, al primo evento di replica del DC con gli eventuali partner di replica, gli oggetti e/o attributi, che nel frattempo sono stati modificati o aggiunti nelle repliche AD degli altri DC partner, verranno sovrascritti o aggiunti alla copia del database precedentemente ripristinato.

Per effettuare un restore non-autoritativo è necessario seguire la seguente procedura:

- Riavviare il DC in modalità provvisoria e selezionare la voce "Directory Service Restore Mode (DSRM)".

- Eseguire il logon con l'account administrator e la password della "*SAM Off-Line*"
- Avviare l'utility NTBACKUP.
- Selezionare la scheda *Restore and Manage Media* e selezionare il set di backup del *System State* da ripristinare.
- Cliccare sul bottone *Start Restore*.

Attenzione !

Non modificare l'opzione "Restore files to: Original Location.

- Confermare cliccando sul bottone OK all'interno della finestra del messaggio di sovrascrittura del System State corrente riportato in figura 6.

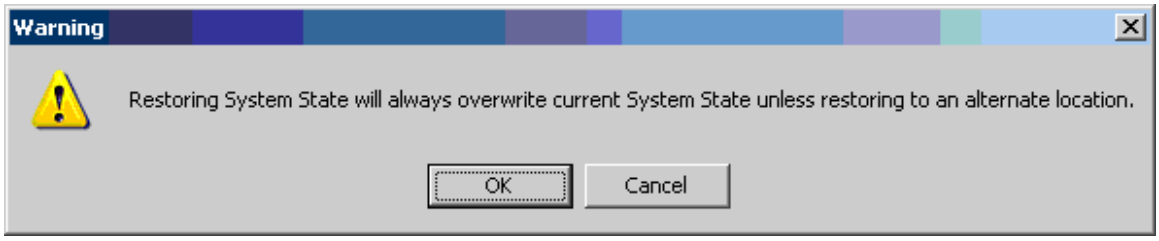

Figure 6: Avviso che il restore del System State sovrascriverà l'attuale System State presente sul computer

- Confermare cliccando sul bottone OK all'interno della finestra *Confirm Restore*.
- Verificare che il restore sia andato a buon fine e cliccare sul bottone *Close* all'interno della finestra *Restore Progress*.
- Riavviare il DC (questa volta in modalità normale) cliccando sul bottone Yes all'interno della finestra *Backup Utility* indicata in figura 7.

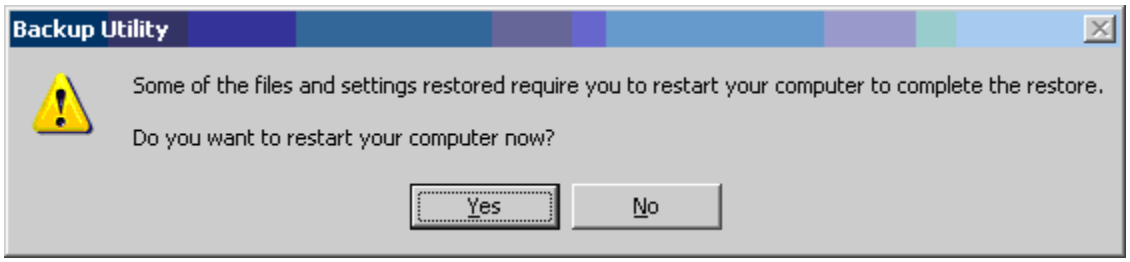

Figure 7: Riavviare il DC per completare il restore non-autoritativo

Successivamente alla esecuzione di un restore non-autoritativo, al riavvio del DC, vengono effettuate le seguenti verifiche:

- Controllo di consistenza del database.
- Ricostruzione indici.

- Allinenamento con lo stato del SDS AD (database AD e SysVol) corrispondente agli altri DC partner di replica.

Il restore non-autoritativo può essere utile in uno dei seguenti casi:

- Il DC danneggiato (e.g.: corruzione del database o guasto al computer) è l'unico di un dominio/foresta: in tal caso non esiste la possibilità di replicare con nessun altro DC e quindi il *System State* ripristinato sarà definitivo (*i.e.: in tal caso è come se fosse autoritativo*).
- Il DC danneggiato (e.g.: corruzione del database o guasto al computer) non è l'unico di un dominio/foresta: in tal caso il *System State* ripristinato sarà in parte (i.e.: relativamente a tutti gli oggetti modificati e/o aggiunti successivamente alla data e ora di esecuzione del backup del *System State*) sovrascritti dagli altri DC partner di replica.

Restore non-autoritativo in un contesto Win2K

Il restore non-autoritativo era molto utilizzato in ambiente AD Win2K in caso di reinstallazione di DC (conseguente a crash) in sedi remote ed in presenza di linee di collegamento non molto performanti. In queste condizioni per evitare la replicazione dell'intero database AD e della SysVol attraverso la rete geografica (WAN) a partire da un DC di un altro site (e.g.: sede centrale) si potevano adottare due metodi:

- *Effettuare la reinstallazione del nuovo DC direttamente in sede come un qualsiasi DC del site centrale. Successivamente, dopo aver modificato opportunamente i parametri relativi alla configurazione TCP/IP e spostato l'oggetto server dal site centrale al site della sede remota di appartenenza, rispedire il DC.*
- *Effettuare un restore non-autoritativo su un nuovo server nel seguente modo:*
    - *Reinstallazione del computer con la stessa configurazione del precedente (i.e.: nome computer, coordinate IP,controller dischi, partizioni (tipo di file system e dimensione almeno uguale a quella del precedente sistema), ecc.).*
    - *Senza rieseguire la DCPROMO effettuare il restore non-autoritativo a partire da un backup valido del System State dello stesso DC.*

In ambiente Win2K3 la stessa procedura presenta qualche problema per la risoluzione dei quali è necessario installare il SP1. Esiste comunque la possibilità, nel caso il DC da ripristinare non sia il primo e unico all'interno di un dominio AD Win2K3, di sfruttare la nuova opzione /ADV dell'utility DCPROMO per eseguire la promozione a DC a partire da una restore (eseguita in modalità alternate location) del System State di un altro DC (Install From Media (IFM)).

Restore-autoritativo

Il restore autoritativo di un DC viene effettuato nel caso in cui è necessario "riesumare" degli oggetti erroneamente cancellati a partire da un backup del *System State* avendo la

garanzia che essi vengano considerati "come se fossero stati appena ricreati" ed essere forzatamente replicati verso gli altri DC replication partner.

Il restore autoritativo può essere eseguito di un singolo oggetto, di un contenitore (e.g.: una OU con il relativo contenuto) o dell'intero database AD. In quest'ultimo caso occorre prestare attenzione ai potenziali problemi che si possono determinare relativamente alla gestione delle password dei computer e delle trust tra eventuali altri domini Win2K/2K3 o WinNT. Infatti di default queste password vengono automaticamente ri-negoziate con una certa cadenza (i.e.: per i computer account ogni 5 gg) ed effettuando un restore autoritativo di tutto il contesto di dominio si rischia di ripristinarle ad un valore non più congruente con lo stato attuale. Pertanto, in caso di restore autoritativo dell'intero database AD o di porzioni del *naming context* (i.e.: partizione) relativo al dominio che include oggetti interessati alle suddette password è necessario procedere con il reset dei computer account e/o la ricreazione delle trust manualmente o attraverso l'utility NETDOM contenuta nei Support Tools di Win2K3.

Per effettuare un restore autoritativo è necessario seguire la seguente procedura:

- Effettuare un restore non-autoritativo senza riavviare il DC.
- Aprire una sessione Command Prompt ed eseguire il comando NTDSUTIL.
- Al prompt di NTDSUTIL, inserire i seguenti comandi:
    - Inserire il comando *Authoritative restore* (o semplicemente le iniziali a r).
        - Dal prompt "*Authoritative restore*" inserire i seguenti comandi per marcare autoritativo l'oggetto AD da "riesumare":

          restore subtree <DN-Oggetto>

          alla comparsa della finestra di dialogo mostrata in figura 8, confermare cliccando sul bottone Yes.

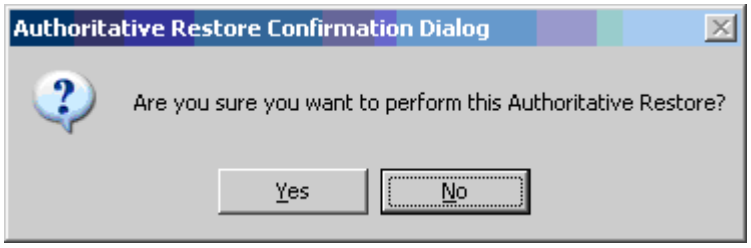

Figure 8: Restore autoritativo del System State

- Esempio 1: restore di un oggetto utente

authoritative restore: restore subtree "CN=Leone Randazzo,OU=sistemisti, DC=learning-solutions,DC=local"

Opening DIT database... Done.

```
The current time is 02-22-05 12:35.10.
Most recent database update occured at 02-22-05 11:08.46.
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.

Authoritative Restore completed successfully.
```

- Esempio 2: restore di una OU (e del relativo contenuto)

```
authoritative restore: restore subtree "OU=servers,dc= DC=learning-solutions,DC=local"

Opening DIT database... Done.

The current time is 02-22-05 12:43.59.
Most recent database update occured at 02-22-05 12:35.10.
Increasing attribute version numbers by 100000.

Counting records that need updating...
Records found: 0000000003
Done.

Found 3 records to update.

Updating records...
Records remaining: 0000000000
Done.

Successfully updated 3 records.

Authoritative Restore completed successfully.
```

- Esempio 3: restore dell'intero database AD (da eseguire solo in casi eccezionali e con molta cautela):

restore database

- Ripetere l'operazione di *restore subtree* per tutti gli oggetti da ripristinare.
- Inserire il comando *quit* per uscire dal contesto *Authoritative restore*.

- Inserire il comando *quit* per uscire da NTDSUTIL.
- Riavviare in modalità normale il DC.

L'effetto del comando di restore autoritativo (come si può notare dagli esempi precedenti) è di rimarcare l'oggetto indicato con un *timestamp* aggiornato ed avanzare il contatore USN (*Update Sequence Number*) ad un valore che risulti sicuramente superiore a quello di qualsiasi altro oggetto all'interno dell'infrastruttura AD (di solito viene sommato 100.000 moltiplicato per il numero dei giorni intercorsi dal backup del *System State*).

Al riavvio del DC in modalità normale e successivamente alla replica con eventuali altri DC partner di replica, si verifica un "authoritative merge", nel senso che tutti gli oggetti ripristinati autoritativamente (i.e.: quelli precedentemente cancellati o modificati) verranno replicati agli altri DC, mentre eventuali nuovi oggetti creati o modificati successivamente al backup del System State ripristinato verranno replicati dagli altri DC al DC "ripristinato autoritativamente".

E' da notare che esistono alcune parti di AD che non possono essere ripristinate autoritativamente, tra questi:

- Gli oggetti della partizione Schema AD non possono essere ripristinati autoritativamente.
- Gli oggetti della partizione Configuration devono essere trattati con molta cautela in quanto il loro impattto è esteso a tutta la foresta. In ogni caso per alcuni tipi di oggetti (e.g.: connection object per la replica tra DC) non ha senso ripristinarli in quanto essi vengono ricreati automaticamente dal *Knowledge Consistency Checker* (KCC) come indicato nel capitolo 10 "La struttura fisica AD".
- Oggetti che interessano il servizio FRS solitamente contenuti in CN=File Replication Service,CN=System,DC=<DN-Dominio> e CN=NTFRS Subscriptions,CN=<Domain Controller> non devono essere ripristinati per non causare effetti collaterali con la replica gestita dal servizio FRS.
- Gli oggetti che interessano il ruolo FSMO RID Master (e.g.: l'oggetto "RID Set" del DC RID Master e l'oggetto "RID Manager$" del contenitore System) non devono essere ripristinati per non causare effetti collaterali con la gestione dei SID degli oggetti Security Principal.
- In ogni caso è consigliato ripristinare solo parti limitati di un qualsiasi Naming Context o Partizione.

La Recovery Console come strumento di disaster recovery

La *Recovery Console* (RC) è un mini-sistema operativo Win2K/XP/2K3 che opera in modalità console o *command-prompt* che può essere pre-installata su un computer WinNT/2K/XP/2K3 (attraverso il comando <unità-CD>\I386\Winnt32 /CmdCons) oppure può essere utilizzata nell'ambito della procedura di restore di un sistema operativo (selezionando la voce R (Repair Console) dopo avere confermato con Invio sulla prima schermata blu "*Setup Notification*"; in questo caso la RC viene emulata in RAM):

```
Microsoft Windows (TM) Recovery Console.

The Recovery Console provides system repair and recovery functionality.
Type EXIT to quit the Recovery Console and restart the computer.

1: C:\WINDOWS

Which Windows  installation would you like to log onto
(To cancel, press ENTER)?: 1
Type the Administrator password:******
C:\WINDOWS>set

AllowWildCards = FALSE
AllowAllPaths = FALSE
AllowRemovableMedia = FALSE
NoCopyPrompt = FALSE

C:\WINDOWS>
```

Essa utilizza la stessa *SAM-Off-line* della modalità DSRM (*Directory Service Restore Mode*) e mette a disposizione un insieme di comandi limitati (digitare HELP dal promp per avere la lista) e permette di svolgere operazioni di:

- Ripristino file di boot e di sistema danneggiati ricopiandoli dal CD originale tramite il comando copy (di default non è possibile utilizzare i caratteri *Wild Card* (i.e.: *, .).
- Elencare i servizi avviabili (listsvc).
- Stoppare/Avviare dei servizi (disable/enable).
- Ripristinare MBR (fixmbr) e Settore di Boot (fixboot) danneggiati da virus.
- Partizionamento dei dischi (diskpart).
- Formattazione volumi (format).
- Ecc.

Normalmente la Recovery Console permette l'accesso solamente all'utente Administrator e limitatamente alla directory di sistema (i.e.: %SystemRoot%). Inoltre, non è consentito l'uso delle *Wild Card* e delle unità floppy.

Per visualizzare le opzioni disponibili è sufficiente inserire il comando set dal prompt della RC come indicato nel precedente box informativo. Da notare che non è possibile modificare direttamente dalla RC queste opzioni, ma è necessario prevedere le seguenti policy nella GPO locale del computer oppure (preferibile) in una GPO di una OU nella quale risiedono i computer per i quali si vuole modificare il comportamento di default della RC:

- Computer Configuration\Windows Settings\Local Policies\Security Options\Recovery Console:
    - Allow automatic administrative logon (default disabled).
    - Allow floppy copy and access all drivers and folders (default disabled).

Creazione di un floppy disk di startup per un server WinNT/2K/2K3

Una buona abitudine è quella di "corredare" ogni server di un floppy disk di startup (FDS) o quanto meno crearne uno e poi, tenendo conto della configurazione riportata nella documentazione dei server (cf. Sezione Documentazione), adattarlo alle varie situazioni. Un FDS deve essere creato nel modo seguente:

- Formattare un floppy disk su un computer dotato di sistema operativo WinNT/2K/XP/2K3.

Il FDS non funziona se la formattazione viene eseguita su un sistema operativo pre-WinNT

E' bene prestare attenzione al fatto che, eseguendo la formattazione del floppy disk su un computer con sistema operativo precedente a WinNT il comando format scrive sul boot sector del floppy disk che il boot loader da invocare è IO.SYS (e poi MSDOS.SYS). Non essendo questi tra i file da copiare sul FDS, allo startup del computer viene presentato il classico errore "Disco non di sistema/Non System Disk".

- Copiare i file di boot necessari per il sistema operativo:
    - Ntldr
    - Boot.ini
    - Ntdetect.com
    - Ed eventualmente il file Ntbootdd.sys nel caso si disponga di controller SCSI.

Il FDS può essere utile per risolvere situazione del genere:

- Danneggiamenti al boot sector e/o MBR del disco che ne compromettono l'avvio.
- Infezioni da virus.

- Mancanza o danneggiamento di uno dei file di boot del sistema operativo (i.e.: ntldr, boot.ini o ntdetect.com).
- Effettuare il boot da un membro di un set di dischi in mirroring software in seguito al danneggiamento del disco master.

Emergency Management Services (EMS)

La famiglia dei sistemi operativi Windows Server 2003 mette a disposizione un nuovo tipo di tecnologia chiamata *Emergency Management Services* (EMS) la quale consente di effettuare la gestione dei server in condizioni precarie di funzionamento e senza disporre di tastiera, mouse, scheda grafica (naturalmente ciò richiede che il BIOS del server Win2K3 permetta l'avvio anche in assenza di questi componenti hardware), monitor e anche in assenza di connessione di rete (i.e.: in modalità *out-of-band*), semplicemente attraverso una connessione in modo testo (i.e.: senza interfaccia grafica (o GUI)) con emulazione terminale VT-UTF8, VT100 o VT100+. A tal proposito, è possibile utilizzare l'emulatore di terminale *Hyper-Terminal* attraverso una connessione seriale null-modem oppure disporre di concentratori di terminali per connessioni multiple da remoto.

Per poter usufruire di questa possibilità per un qualsiasi server Win2K3 è necessario preventivamente abilitare la redirezione dell'output verso una predefinita porta seriale mediante il comando bootcfg, come indicato nell'esempio seguente:

bootcfg /ems on /port com1 /baud 115200 /id 1

dove /id 1 si riferisce alla entry del file boot.ini (per visualizzare le entry è sufficiente inserire il comando bootcfg) sulla quale si vuole abilitare il servizio EMS. Nel caso utilizzato come esempio, viene abilitata la funzione di redirezione EMS verso la porta seriale COM1 con velocità di 115.200 baud.

Da notare che il suddetto comando produce la seguente modifica nel file boot.ini:

[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
redirect=COM1
redirectbaudrate=115200
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows Server 2003, Enterprise" /fastdetect **/redirect**
multi(0)disk(0)rdisk(0)partition(2)\WINXP="Microsoft Windows XP Professional" /fastdetect /NoExecute=OptIn
C:\CMDCONS\BOOTSECT.DAT="Microsoft Windows 2000 Recovery Console" /cmdcons

Riavviando il server Win2K3, e predisponendo un collegamento da un altro computer attraverso la porta seriale utilizzando un cavo null-modem e l'utility *Hyper-Terminal* come emulatore di terminale (con i parametri di connessione seguenti: COM1; Terminal Type VT100; 115.200 baud; 8N1; flow control hardware), si ottiene la redirezione della schermata di boot visualizzata dal loader NTLDR del sistema operativo Win2K3:

```
Please select the operating system to start:

Microsoft Windows Server 2003, Enterprise [EMS enabled]
Microsoft Windows XP Professional
Microsoft Windows Recovery Console

Use the up and down arrow keys to move the highlight to your choice.
Press Enter to choose.
Seconds until highlighted choice will be started automatically: 29

For troubleshooting and advanced startup options for Windows, press F8.
```

A questo punto selezionando il sistema operativo Win2K3 abilitato per la gestione EMS viene immediatamente avviata la console primaria nativa di EMS, chiamata SAC (*Special Administration Console*):

```
Computer is booting, SAC started and initialized.

Use the "ch -?" command for information about using channels.
Use the "?" command for general help.

SAC>
```

Nel caso in cui il server Win2K3 sia già operativo e predisposto per la gestione via EMS, in seguito alla connessione via emulatore di terminale sulla relativa porta seriale con un cavo null-modem, viene presentata immediatamente la console SAC.

Da notare che la console SAC opera in maniera completamente indipendente dal prompt dei comandi del sistema operativo ed offre un insieme limitato di funzioni. Inoltre, essa è disponibile anche nelle prime fasi del processo di boot del sistema operativo (consentendo di effettuare un dump del log di caricamento del kernel, driver e servizi) e rimane attiva fino a quando il kernel è in funzione. Alcuni comandi a disposizione nella SAC sono i seguenti (ottenibili tramite il comando help o ?):

```
SAC>?

ch              Channel management commands.  Use ch -? for more help.
cmd               Create a Command Prompt channel.
d               Dump the current kernel log.
```

```
f                 Toggle detailed or abbreviated tlist info.
? or help         Display this list.
i                 List all IP network numbers and their IP addresses.
i <#> <ip> <subnet> <gateway> Set IP addr., subnet and gateway.
id                Display the computer identification information.
k <pid>           Kill the given process.
l <pid>           Lower the priority of a process to the lowest possible.
lock              Lock access to Command Prompt channels.
m <pid> <MB-allow>   Limit the memory usage of a process to <MB-allow>.
p                 Toggle paging the display.
r <pid>           Raise the priority of a process by one.
s                 Display the current time and date (24 hour clock used).
s mm/dd/yyyy hh:mm   Set the current time and date (24 hour clock used).
t                 Tlist.
restart           Restart the system immediately.
shutdown          Shutdown the system immediately.
crashdump         Crash the system. You must have crash dump enabled.
SAC>id
        Computer Name: LS-MI-DC-01
        Computer GUID: 4c4c4544-0039-4810-8051-b2c04f39304a
  Processor Architecture: x86
       Version Number: 5.2
        Build Number: 3790
            Product: Windows Server 2003 Enterprise Edition
   Applied Service Pack: None
  Time since last reboot: 0:45:05

SAC>i
Net: 6, Ip=172.26.1.254  Subnet=255.255.255.0  Gateway=172.26.1.254
Net: 4, Ip=10.1.1.10  Subnet=255.255.255.0  Gateway=10.1.1.10
Net: 2, Ip=192.168.171.1  Subnet=255.255.255.0  Gateway=192.168.171.1
Net: 3, Ip=192.168.137.1  Subnet=255.255.255.0  Gateway=192.168.137.1

EVENT: The CMD command is now available.
SAC>ch
Channel List

(Use "ch -?" for information on using channels)

# Status  Channel Name
0 (AV)    SAC
SAC>cmd
The Command Prompt session was successfully launched.
SAC>
EVENT:   A new channel has been created.  Use "ch -?" for channel help.
Channel: Cmd0001
```

```
SAC>ch
Channel List

(Use "ch -?" for information on using channels)

# Status  Channel Name
0 (AV)    SAC
1 (AV)    Cmd0001
```

All'avvio del servizio *SacSvr* (SAC *Helper Service*), comunicato nella console SAC tramite l'evento "EVENT: The CMD command is now available" viene reso disponibile il comando cmd che consente di aprire un nuovo canale (oltre al canale 0 che corrisponde alla console SAC) per avviare la console command prompt di Windows. Una volta inserito il comando cmd è possibile commutare sul canale cmd con il commando "ch –si 1". Prima di entrare nella console dei comandi Windows è obbligatorio effettuare l'autenticazione:

```
SAC>ch –si 1

Please enter login credentials.
Username: leoner
Domain  : learning-soluti
Password: **************

Welcome, leoner@LEARNING-SOLUTIONS.LOCAL.
I'm ready !

C:\>
```

Diritti per la connessione alla console SAC e per l'apertura del canale "cmd"

L'accesso alla console SAC non richiede nessuna forma di autenticazione. Pertanto è importante garantire la sicurezza fisica dei server Win2K3 gestiti via EMS.

Viceversa, per aprire la console cmd è necessario essere membri del gruppo Administrators locale (nel caso di server Win2K3 stand-alone) oppure del gruppo Domain Admins al quale appartiene il server. Inoltre, nel caso in cui l'utente (anche Administrator) non ha password, l'accesso non viene comunque autorizzato.

La commutazione da un canale all'altro avviene tramite la sequenza di tasti ESC+TAB+0 per la SAC e ESC+TAB+1 per la console cmd. Dal prompt della console cmd, sono

disponibili tutti i comandi ad interfaccia non-grafica normalmente utilizzabili da una sessione Windows command prompt.

In caso di fallimento della console primaria viene automaticamente avviata una console ausiliaria chiamata !SAC, la quale fornisce un sottoinsieme dei comandi della SAC per consentire il ripristino delle funzionalità del sistema in caso di crash, per redirigere eventuali messaggi di stop oppure per riavviare il sistema.

Aprire una console Command-Prompt in fase di installazione di un server Windows Server 2003

In fase di installazione di un server Win2K3 nella modalità GUI (*Graphical User Interface*) è possibile aprire una console command prompt mediante la sequenza di tasti SHIFT+F10. Ciò si rivela estremamente utile per effettuare controlli sulla rete, come ad esempio: duplicazione IP, test ping, stop di servizi, lanciare Task Manager, copiare driver, ecc..