ATENŢIONARE!

Conţinutul acestei platforme de instruire a fost elaborat în cadrul proiectului „**Dezvoltarea resurselor umane în educaţie pentru administrarea reţelelor de calculatoare din şcolile româneşti prin dezvoltarea şi susţinerea de programe care să sprijine noi profesii în educaţie, în contextul procesului de reconversie a profesorilor şi atingerea masei critice de stabilizare a acestora în şcoli, precum şi orientarea lor către domenii cerute pe piaţa muncii**”. Conţinutul platformei este destinat în exclusivitate pentru activităţi de instruire a membrilor grupului ţintă eligibil în proiect. Utilizarea conţinutului în scopuri comerciale sau de către persoane neautorizate nu este permisă. Copierea, totală sau parţială, a conţinutului de instruire al acestei platforme de către utilizatori autorizaţi este permisă numai cu indicarea sursei de preluare (platforma de instruire eadmin.cpi.ro). Pentru orice probleme, nelămuriri, sugestii, informaţii legate de aspectele de mai sus vă rugăm să utilizaţi adresa de email: proiect.eadmin@cpi.ro

Acest material a fost elaborat de Veronica Iuga, expert la S.C. Centrul de Pregătire în Informatică S.A., partener de implementare a proiectului POSDRU /3/1.3/S/5.

Versiunea materialului de instruire: V2.0

Active Directory 2008

Instalarea Active Directory

Instalarea *Active Directory 2008* se realizează instalând inițial rolul *AD DS (Active Directory Domain Services)* după care urmează instalarea efectivă a domeniului folosind comanda **dcpromo,** care realizează promovarea la *domain controller*. *AD DS (Active Directory Domain Services)* poate fi instalat pe calculatoare unde există sisteme de operare *Microsoft Windows Server 2008* sau *2008 R2*, edițiile *Standard, Enterprise* şi *Data Center*. Necesită o partiţie NTFS cu minim 250 GB de spaţiu liber, pentru început.

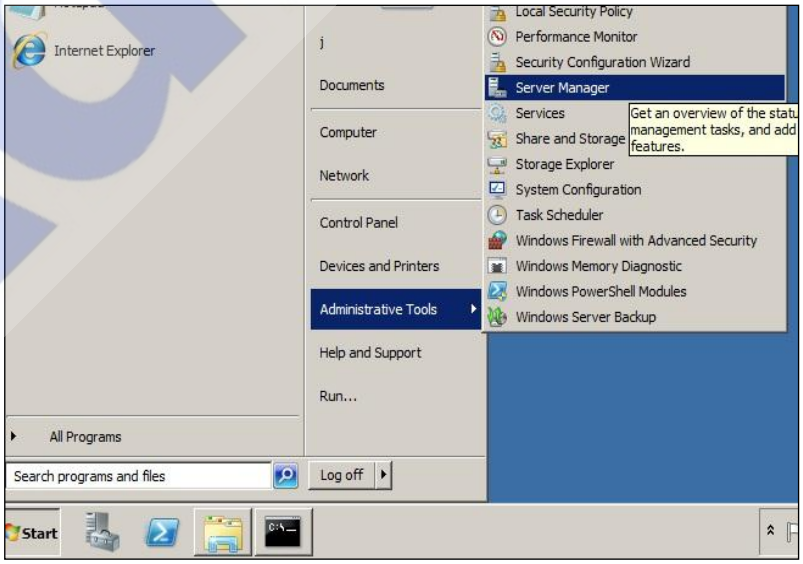
Dacă se lansează direct comanda **dcpromo**, înainte ca acest rol să fi fost instalat, aceasta va începe iniţial instalarea rolului AD DS şi va continua cu promovarea la *domain controller*.

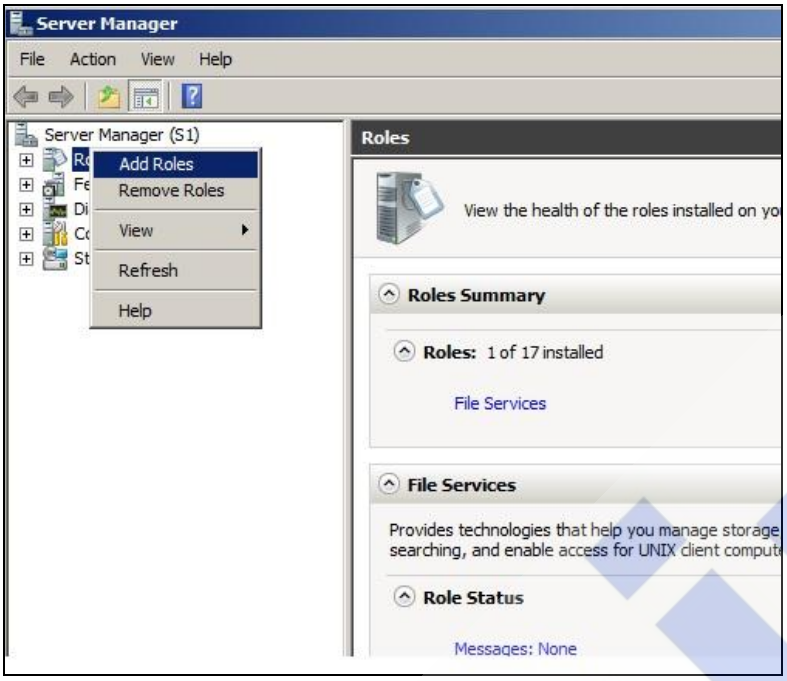
Este posibil să se realizeze numai instalarea rolului AD DS, fără instalarea de controler de domeniu, pentru anumite situaţii, de exemplu atunci când pe acel server sunt instalate anumite servicii relaţionate cu *Active Directory*, de exemplu *Exchange Server*, fără însă a fi nevoie ca acel server să fie promovat la controler de domeniu.

La fel ca și la *Windows 2000/2003*, serverul care va deveni controler de domeniu trebuie să aibă de la început o adresă IP statică şi să fie client la serverul DNS responsabil cu rezolvarea numelor în domeniu. Microsoft recomandă ca serverul controler de domeniu să îndeplinească şi rolul de server DNS. Mai mult decât atât, Microsoft recomandă ca instalarea serviciului DNS să aibă loc o dată cu instalarea *Active Directory*.

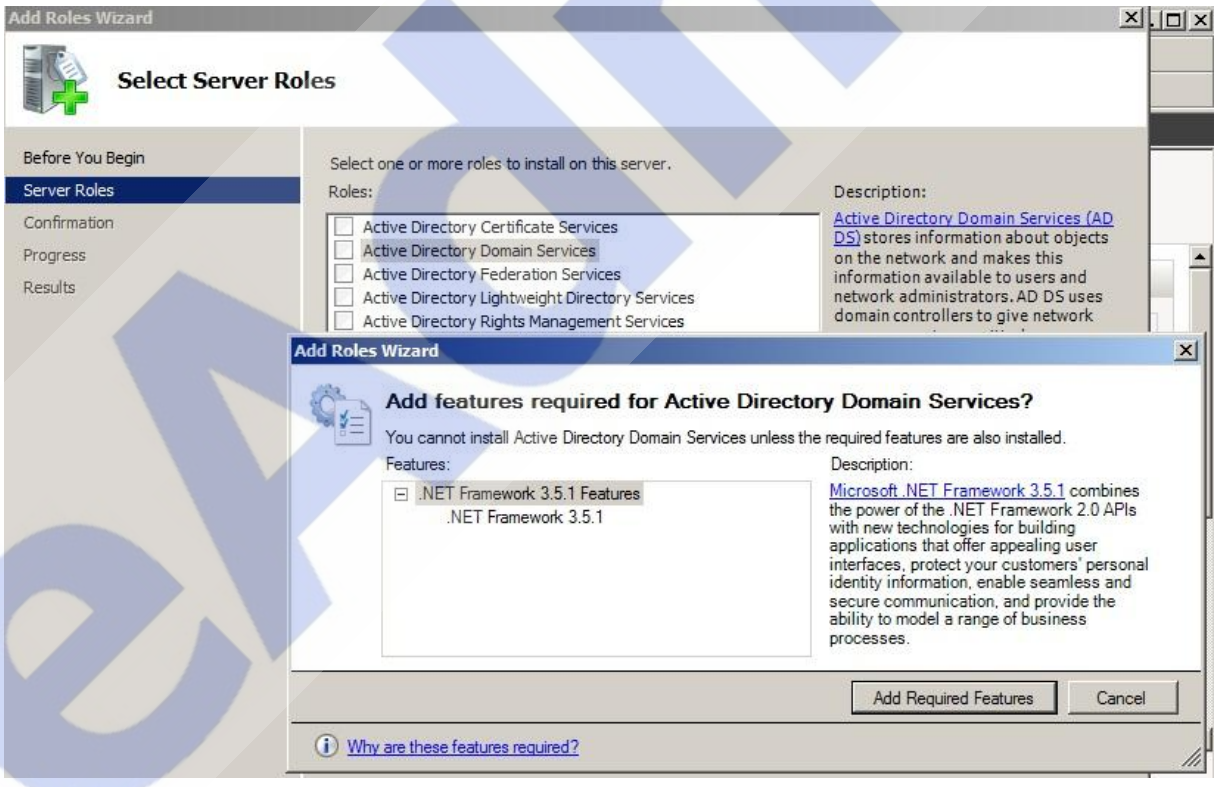
Adăugarea rolului AD DS se realizează folosind utilitarul **Server Manager**, din **Administrative Tools**.

Cu acest utilitar putem adăuga/elimira roluri sau *features* (caracteristici) din sistem.

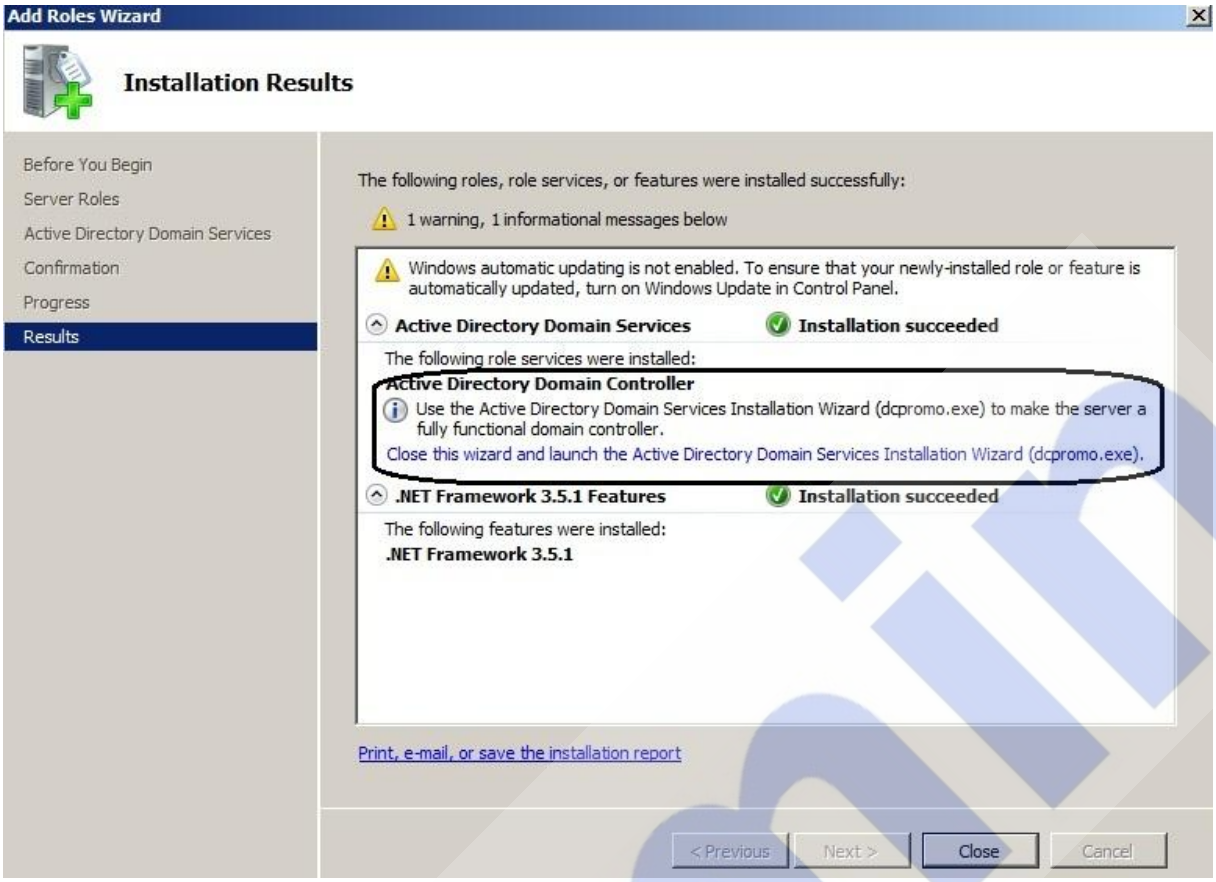




Specificăm rolul care trebuie adăugat, în cazul nostru AD DS. Uneori adăugarea unui rol implică necesitatea adăugării de *feature* suplimentare, care trebuie instalate dacă nu au fost instalate anterior. De exemplu în acest caz este nevoie de instalarea **Microsoft .NET framework 3.5.1features.**

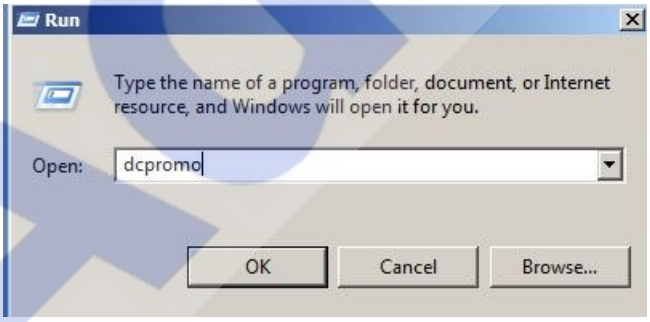


După realizarea acestei instalări, trebuie rulat **dcpromo** pentru a realiza promovarea la domain controller. Acest lucru este specificat și în **Server Manager.**

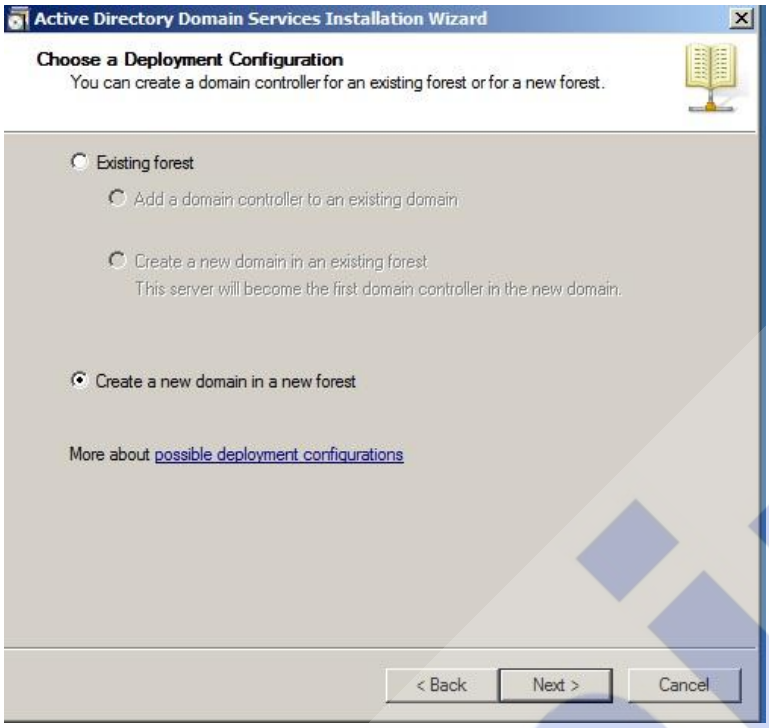


Pașii sunt asemanatori cu cei necesari pentru instalarea *Active Directory* pentru *Windows 2003*.

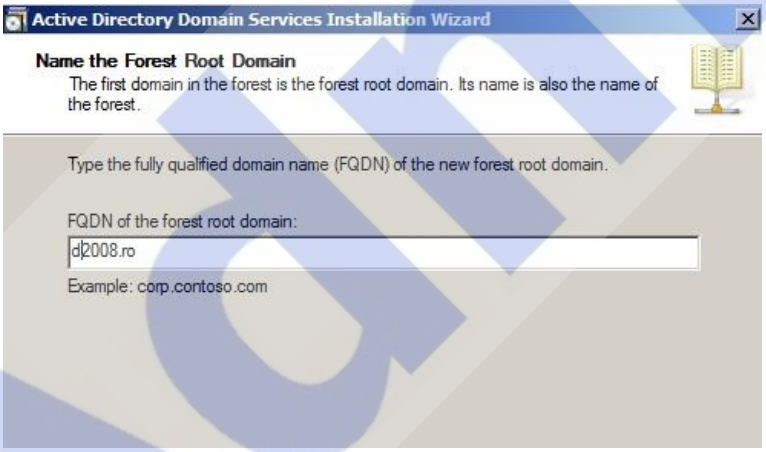
1. Se lansează **dcpromo**



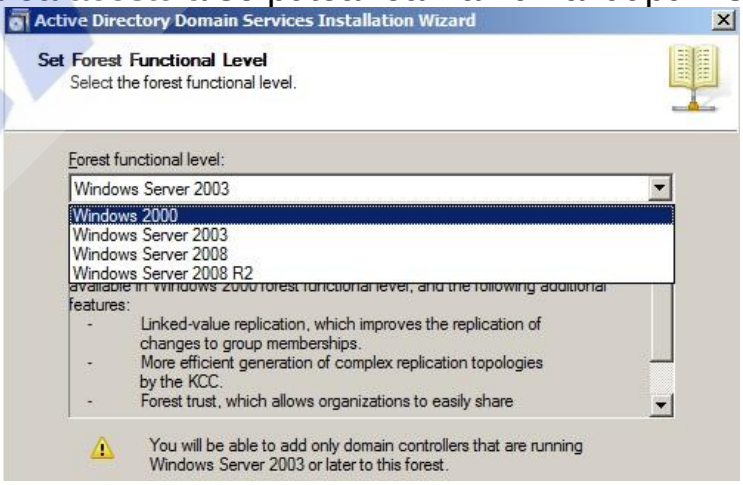
2. Se specifică dacă se va crea un *forest* nou sau se va folosi un *forest* deja existent şi în acest caz specificăm dacă se realizează crearea unui domeniu nou sau se adaugă acest controler de domeniu la un domeniu deja existent.



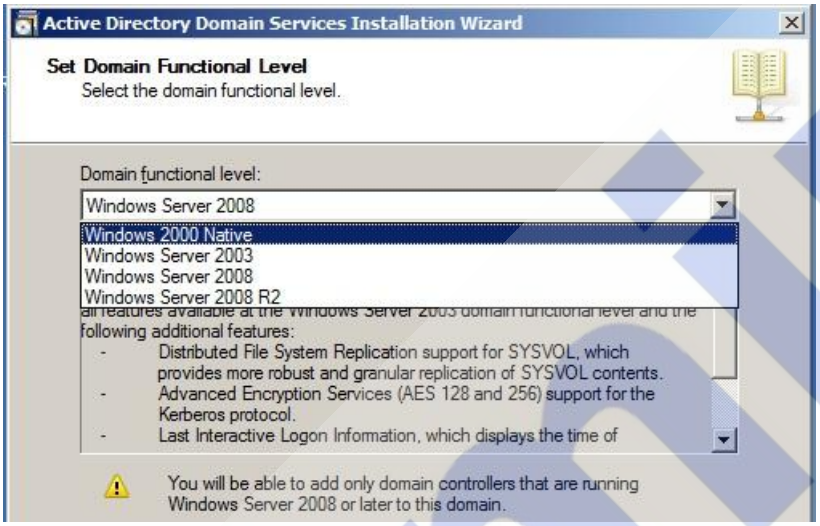
3. În cazul în care se crează un domeniu nou se specifică numele acestui domeniu, în format FQDN.



4. Se specifică *forest functional level (*nivelul funcțional al pădurii).
La *Windows 2003* nu se putea specifica acest lucru la crearea *forestului*, *forest functional level* era în urma instalării întotdeauna la valoarea **Windows 2000** și modificarea acestuia se putea realiza numai după instalare.



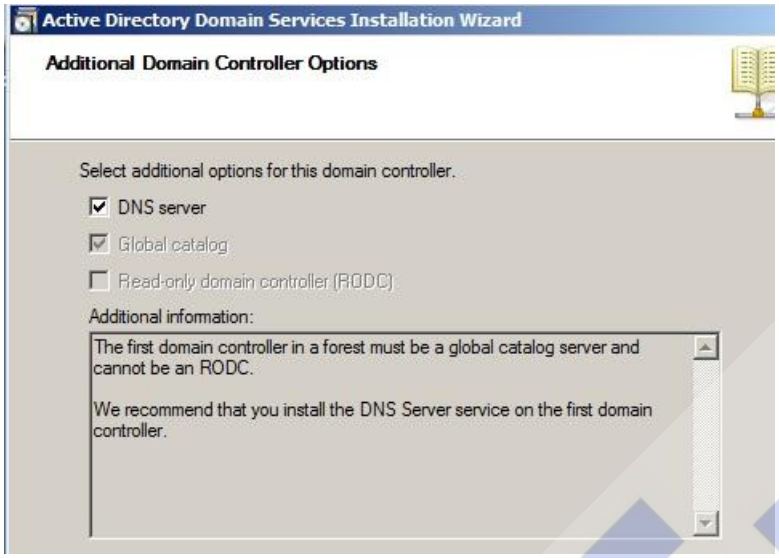
5. Se setează *domain functional level* (nivelul funcțional al domeniului). Valorile permise sunt în funcţie de *forest functional level* ales, adică valoarea de la *domain functional level* nu poate fi mai mică decât cea care a fost aleasă pentru *forest functional level*. La *Windows 2003* nu se putea specifica acest lucru la crearea domeniului, *domain functional level* era în urma instalării întotdeauna *Windows 2000 mixt* și modificarea acestuia se putea realiza numai după instalarea domeniului. Nivelul *Windows 2000 mixt* nu mai există, nemaifiind suportate domain controlere de tip NT4.0.



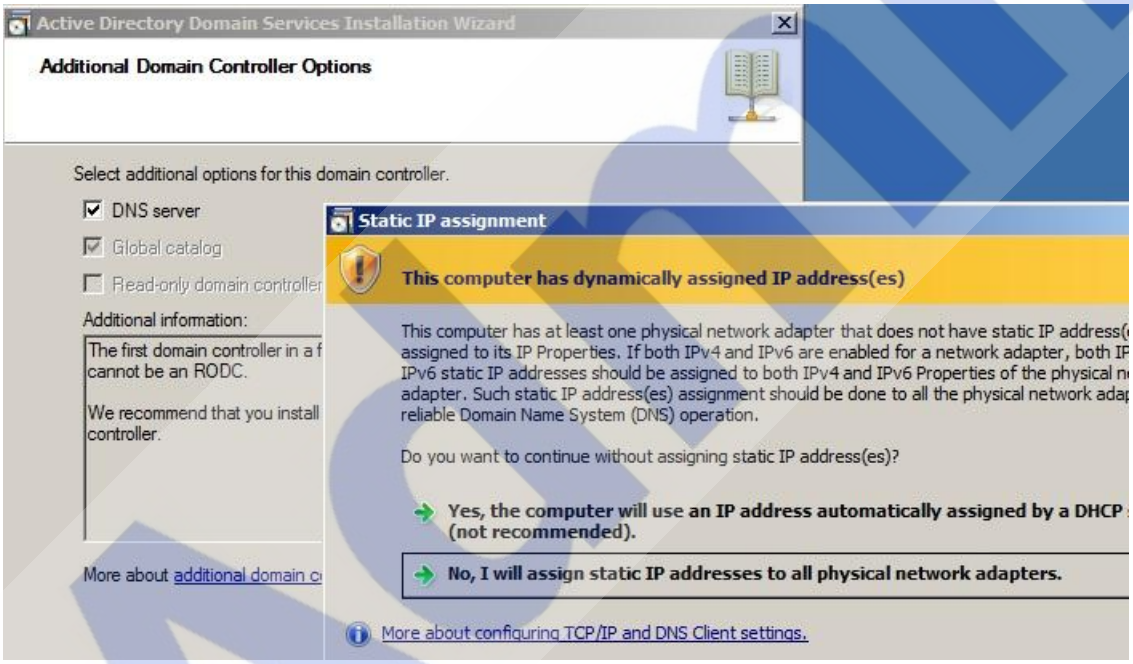
În tabelul de mai jos sunt prezentate *domain functional level* –urile posibile și pentru fiecare în parte ce sisteme de operare sunt permise pentru controlerele de domeniu.

Domain Functional Level	**Sisteme de operare permise pe controlerele de domeniu**
Windows 2000 Native	Windows Server 2008 R2 Windows Server 2008 Windows Server 2003 Windows 2000
Windows Server 2003	Windows Server 2008 R2 Windows Server 2008 Windows Server 2003
Windows Server 2008	Windows Server 2008 R2 Windows Server 2008
Windows Server 2008 R2	Windows Server 2008 R2

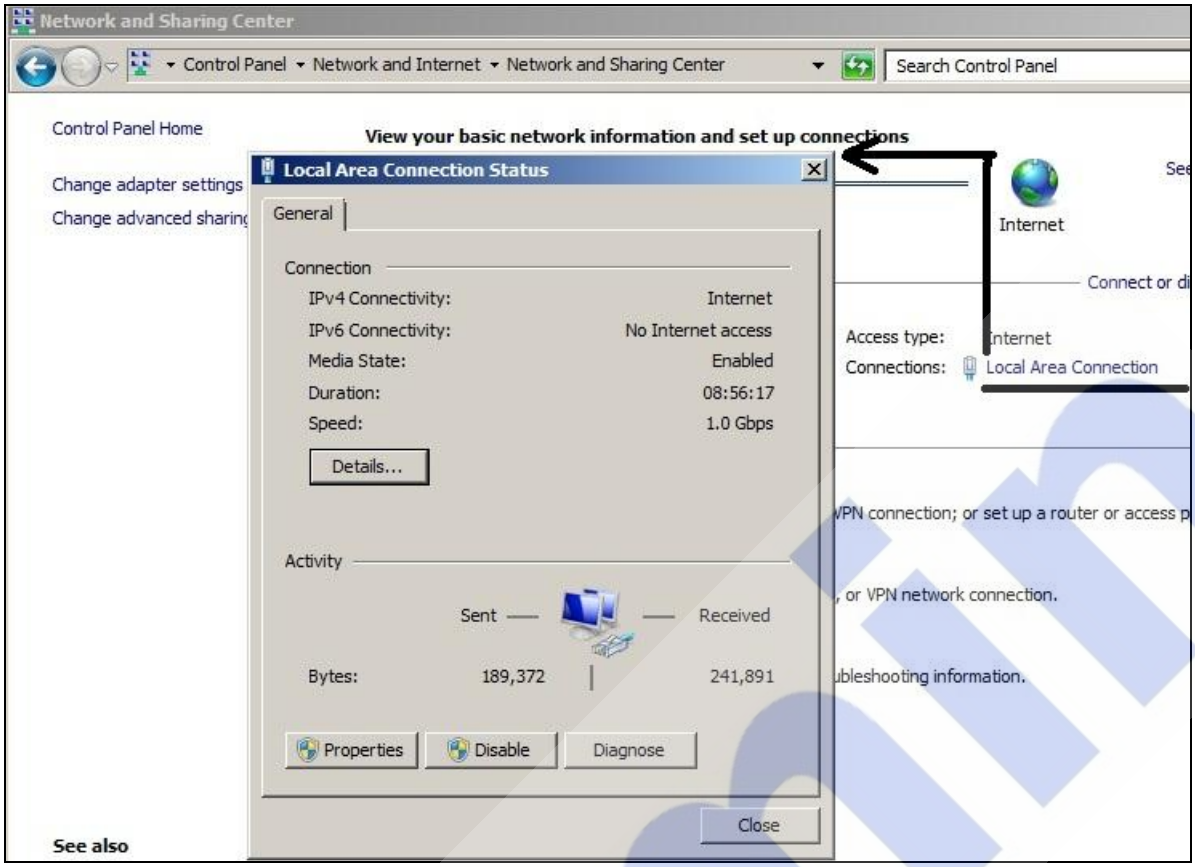
6. În continuare se setează diverse alte opţiuni pentru *domain controller*, de exemplu poate fi instalat şi rolul de DNS, poate fi *Global Catalog* server (pentru primul domeniu din *forest* această setare este obligatorie şi nu poate fi debifată) sau poate fi *RODC (Read Only Domain Controller* - Controler de domeniu care permite numai citire*),* dar numai dacă nu este primul controler de domeniu, altfel trebuind să fie în mod obligatoriu de tip *RWDC (Read Write Domain Controller* - Controler de domeniu care permite citire și scriere).



7. Se recomandă setatarea adresei IP statică.

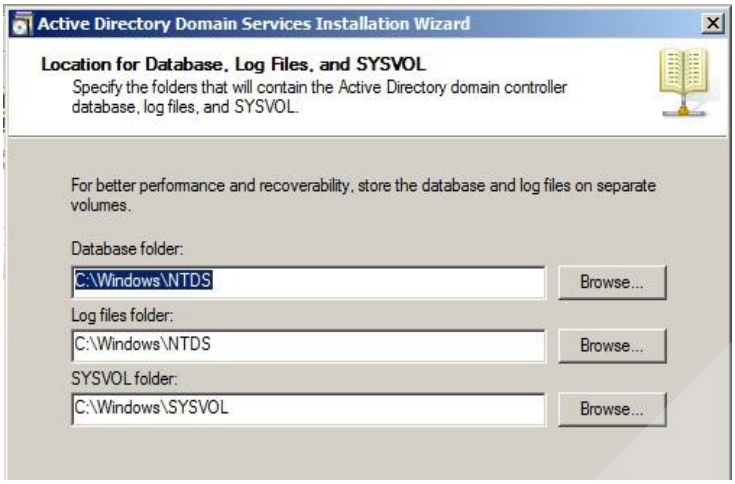


Setarea adresei IP se realizează din **Control Panel –> Network and Internet –> Network and Sharing Center –> Local Area Connection –> Properties**

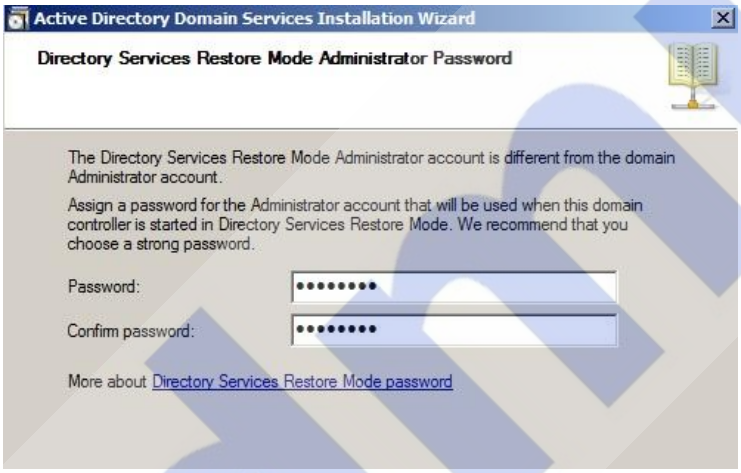


8. În cazul în care nu se poate realiza în mod automat delegarea la serverul DNS care deține domeniul părinte, trebuie să permitem continuarea procesului de instalare fară a se realiza în mod automat această delegare. Aceasta se poate realiza manual ulterior, dacă este necesară.

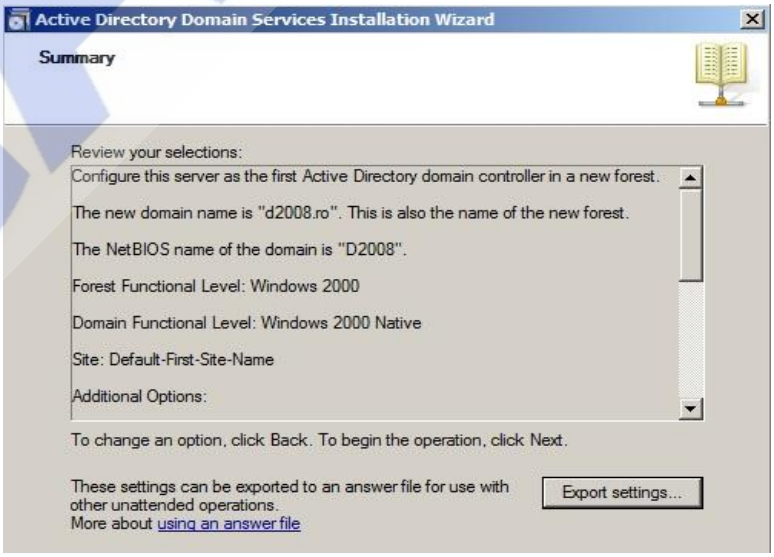
9. Se specifică locațiile pentru baza de date *Active Directory*, *log files* și folderul SYSVOL.
În mod implicit, este vorba despre folderele **C:\Windows\NTDS,** respectiv **C:\Windows\SYSVOL.**



10. Urmează stabilirea parolei administratorului pentru modul de lucru *Directory Services Restore Mode* (Restaurarea Serviciilor Director).



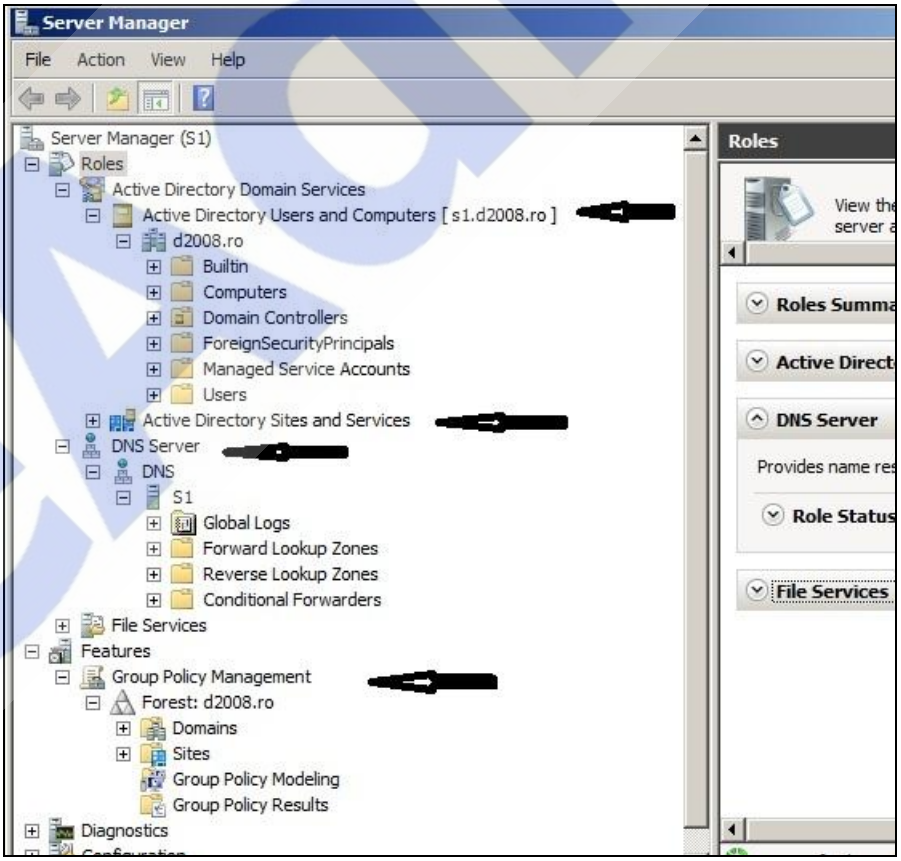
11. În baza opţiunilor de instalare pe care le-am selectat, ***Active Directory Domain Services Installation Wizard*** (vrăjitorul pentru instalarea *Active Directory Domain Services*) afişează un sumar al alegerilor făcute şi construieşte apoi baza de date a serviciului.
Acest sumar poate fi exportat, folosind butonul **Export Settings** într-un fişier text care poate fi folosit (eventual cu anumite modificări de rigoare) pentru o altă instalare de tip *unatteded* (neasistată).



Instalarea nu este completă decât după restartarea sistemului.
În urma instalării, în grupul de programe *Administrative Tools* sunt adăugate o serie de utilitare pentru gestionarea *Active Directory*, printre care:

- **Active Directory Users and Computers:** permite crearea conturilor de utilizator, a grupurilor, conturilor de calculator, a unităţilor organizaţionale. Este utilitarul folosit pentru administrarea obiectelor *Active Directory*.
- **Active Directory Domains and Trusts:** pentru vizualizarea şi modificarea relaţiilor de încredere dintre domeniile *Active Directory*.
- **Active Directory Sites and Services:** pentru crearea şi coordonarea *site-urilor* şi a serviciilor *Active Directory*.
- **Group Policy Management:** utilitarul specializat pentru managementul obiectelor *Group Policy*. La *Windows Server 2003* nu este inclus în *kit-ul* de instalare, trebuind să fie descărcat pe *site-ul* Microsoft, însă la *Windows 2008* este instalat ca și *feature* în mod implicit, odată cu instalarea *Active Directory*. Dacă se dorește gestionarea de la distanță a *Group Policy Object*-urilor din domeniu, se poate adăuga acest *feature*, folosind **Server Manager**, pe calculatoarele corespunzătoare.

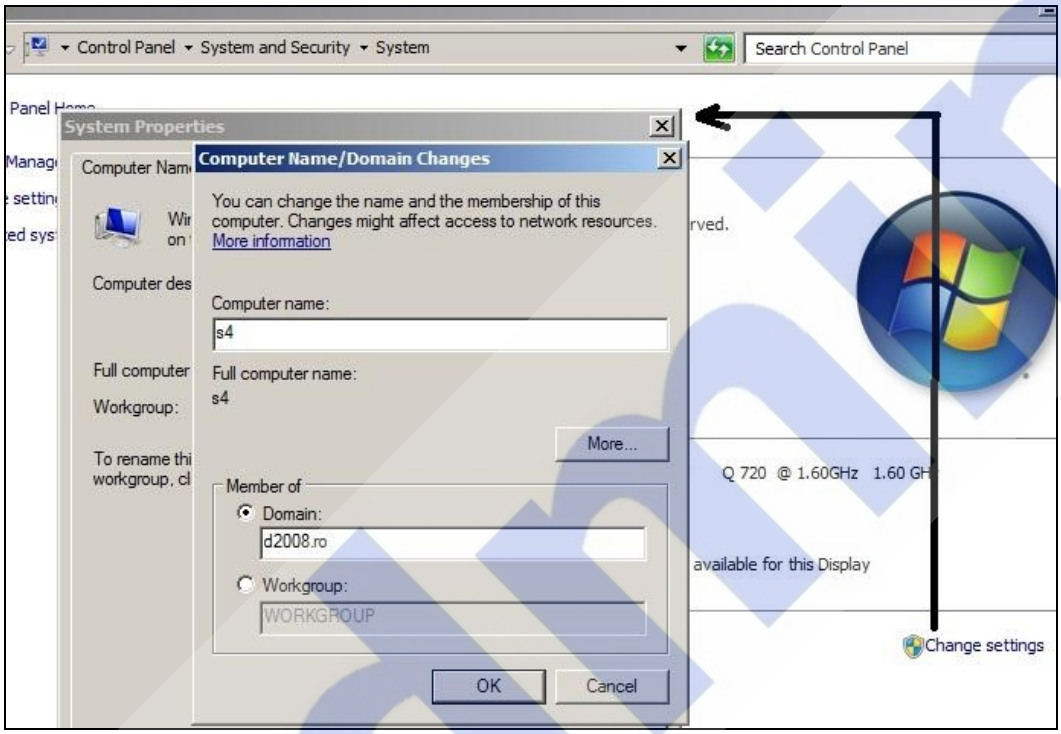
Folosind utilitarul **Server Manager** putem vizualiza rolurile și *featur-ile* care au fost instalate și putem avea acces la cele mai uzuale instrumente de administrare a acestora.



Includerea unui computer în domeniu

Apartenenţa unui calculator (staţie de lucru sau server) la un domeniu este o proprietate a sistemului. În acelaşi timp, calculatorul membru al domeniului trebuie să fie client la serverul DNS care controlează domeniul DNS cu acelaşi nume ca şi domeniul Active Directory.

Introducerea calculatorului în domeniu se obţine prin *ControlPanel->System and Security ->System -> Change settings -> Change*



De la calculatoarele incluse în domeniu, utilizatorii pot deschide sesiune folosind fie un cont din domeniu, fie un cont din baza de date locală SAM. Spre deosebire de *Windows 2003*, nu mai există posibilitatea alegerii uneia dintre cele două opţiuni în fereastra de *logon*, ci trebuie specificat (scris) manual numele domeniului (pentru logarea pe acel domeniu) sau al calculatorului (pentru logare locala), în formatul:

nume_domeniu_sau_calculator\nume_utilizator

În exemplul de mai sus dom2008 este numele domeniului și s4 este numele stației membre în domeniu.

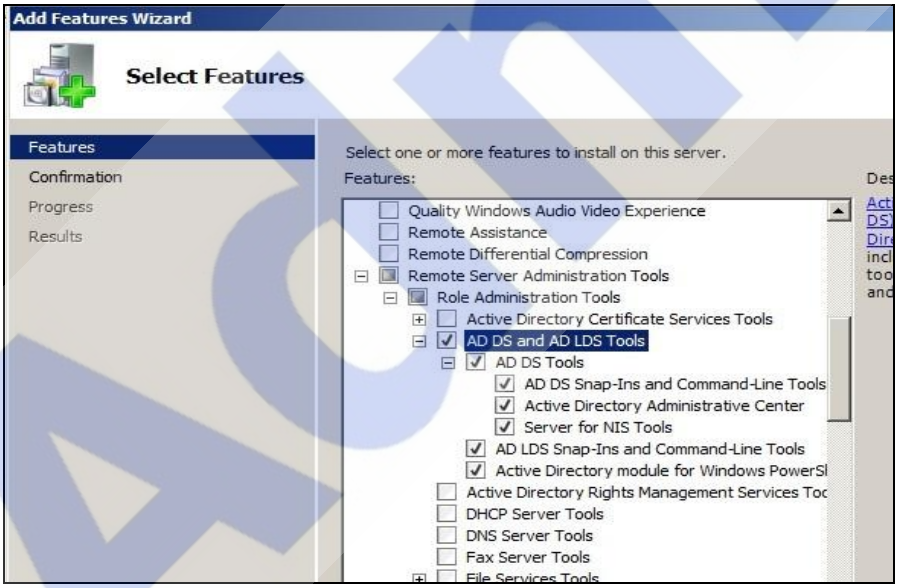
Remote Server Administration Tools (RSAT) – Instrumente pentru gestionare distantă a serverului

Administrarea unui domeniu se poate realiza, în calitate de administrator al domeniului, de la orice calculator membru al domeniului.

Instrumentele de administrare pot fi instalate ca *feature*, numit **Remote Server Administration Tools (RSAT)**. Acesta inlocuiește **adminpak.msi**, existent la versiunile anterioare.

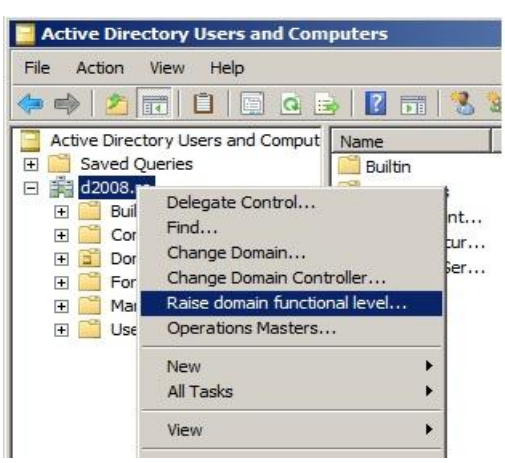
Spre deosebire de situația când se folosea **adminpak.msi,** când erau instalate toate instrumentele de administrare, *RSAT* permite să alegem ceea ce dorim să fie instalat, astfel încât să instalăm numai instrumentele necesare, de exemplu ne putem alege numai utilitarele administrative relaționate cu *Active Directory*.

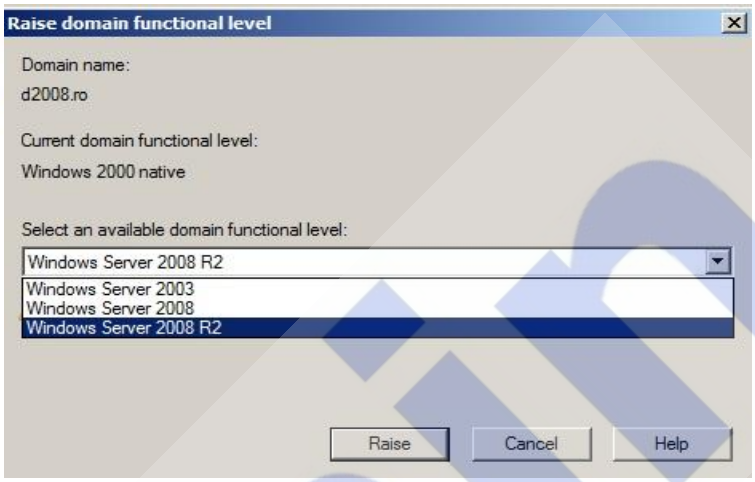
RSAT se poate instala și pe calculatoare care rulează *Windows Vista* cu *Service Pack 1 (SP1)* sau superior sau *Windows 7*, fișierele necesare trebuind însă descărcate de pe internet de la site-ul Microsoft.



Modificare domain functional level

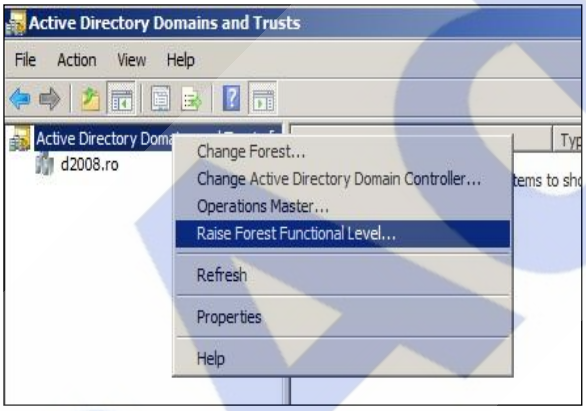
Se realizează folosind **Active Directory Users and Computers**.
Odată stabilit un anumit nivel, nu se mai poate reveni la un nivel inferior.

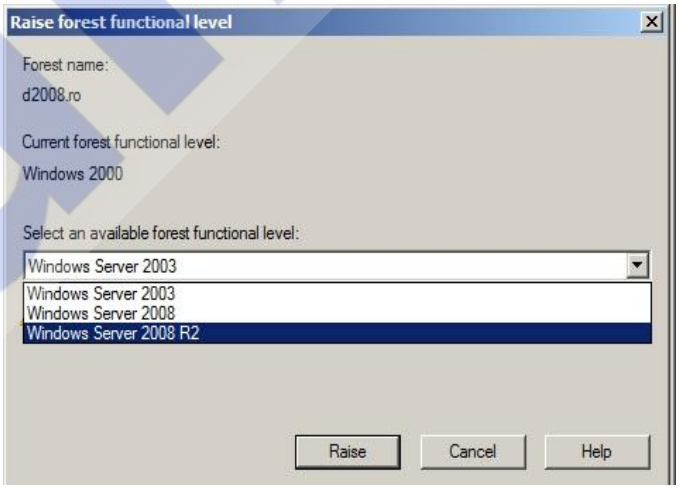




Modificare forest functional level

Se realizează folosind **Active Directory Domains and Trusts**.
Odată stabilit un anumit nivel , nu se mai poate reveni la un nivel inferior.





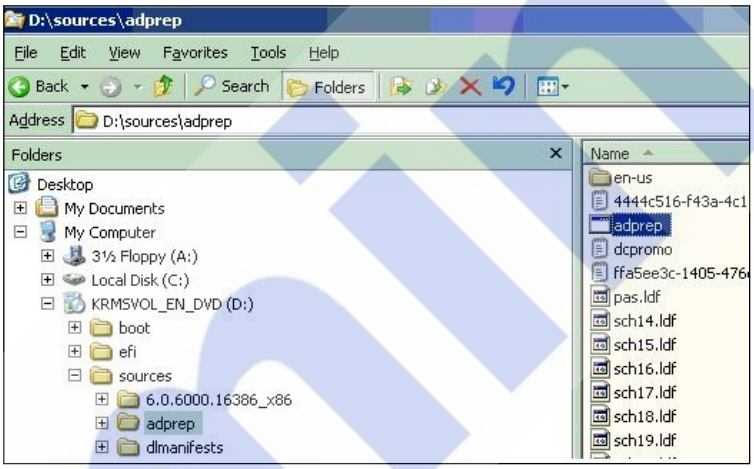
Se recomandă ca nivelul funcțional (atât pentru *forest* cât și pentru domeniu) să fie cel maxim posibil, pentru a putea beneficia de toate facilitățile suportate.

Instalarea unui *domain controller* adițional Windows 2008/R2 într-un *forest* care conține *domain controllere Windows 2000* sau *Windows 2003*

Trebuie realizată o pregătire atât a forestului cât și a domeniului pentru a putea primi astfel de domain controllere.

Nivelul pentru *domain functional level* și *forest functional level* trebuie să fie minim *Windows 2000 native* (nivelul *Windows 2000 mixt* nu mai este suportat de domeniile *Windows 2008/R2*).

Se utilizează comanda **adprep,** care există pe *kit-ul* de instalare, în folderul **sources\adprep** pentru *Windows 2008* respectiv **support\adprep** pentru *Windows 2008 R2*.



Se rulează comanda **adprep /forestprep** pe *domain controllerul* cu rol de *Schema Master* (implicit este primul *domain controller* din *forest*), de către un membru al grupurilor *Enterprise Admins , Schema Admins* și *Domain Admins* pentru domeniul care conține *domain controllerul* cu rol de *Schema Master*.

Se rulează comanda **adprep /domainprep /gpprep** pe *domain controllerul* cu rol de *Infrastructure Master* (implicit este primul *domain controller* din domeniu) pentru fiecare domeniu în care va fi introdus un *domain controller Windows 2008/R2*, de către un membru al grupului *Domain Admins* pentru domeniul respectiv.

Upgradarea unui *domain controller Windows 2003* la *Windows 2008/R2*

Necesită pregătirea domeniului, pentru a putea primi un *domain controller* de acest tip. Ca și în cazul anterior, nivelul pentru *domain functional level* și *forest functional level* trebuie să fie minim *Windows 2000 native.*

Se rulează comenzile **adprep /forestprep** și **adprep /domainprep /gpprep** ca în condițiile de mai sus.

Dacă se dorește upgradarea de la *Windows 2000* la *Windows 2008/R2*, acest lucru nu este posibil direct, ci trebuie realizată mai întâi o upgradare de la *Windows 2000* la *Windows 2003*.

Read Only Domain Controller (RODC)

Este un tip nou de *domain controller* introdus la *Windows 2008*, pentru care toate partițiile *Active Directory* deținute sunt *read-only*.

Condiții care trebuie indeplinite pentru instalarea unui *RODC:*

- se poate instala numai pe *domain controllere* de tip *Windows 2008* sau *Windows 2008 R2*

- nu poate fi primul *domain controller writable* (pe care se pot efectua modificări) de tip *Windows 2008* sau *Windows 2008 R2* din domeniu

- *domain functional level* și *forest functional level* trebuie să fie minim *Windows Server 2003*

- dacă acest *domain controller* se instalează într-un *forest* care conține *domain controllere Windows 2003*, trebuie rulată comanda **adprep /rodcprep**, pentru a permite replicarea partițiilor DNS. Dacă în *forest* există numai *domain controllere* cel puțin *Windows 2008*, nu mai este necesară rularea acestei comenzi

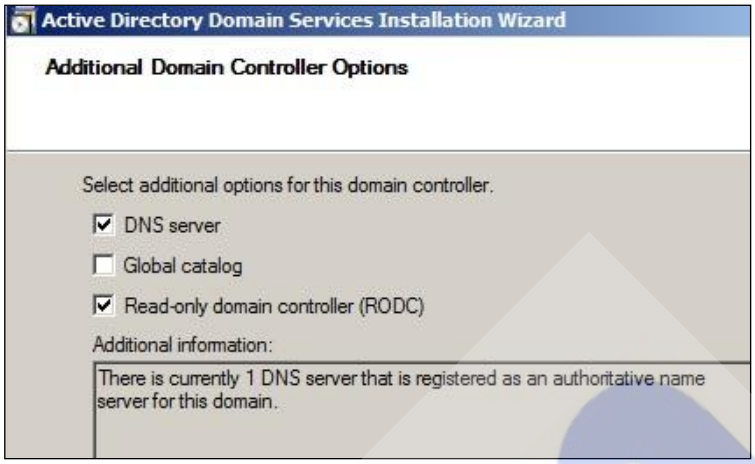
- dacă *domain controllerul* RODC va funcționa ca *Global Catalog Server*, atunci trebuie rulată comanda **adprep /domainprep** pe toate domeniile din *forest*, chiar dacă în domeniu există numai *domain controllere* cel puțin *Windows 2008*

- serverul nu trebuie să fie membru în acel domeniu

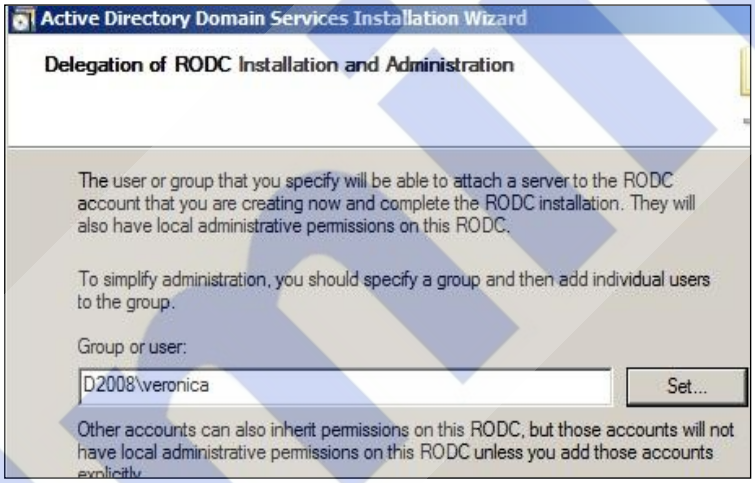
Instalarea RODC

Instalarea RODC urmează pașii uzuali pentru instalarea unui *domain controller*.
Nefiind primul *domain controller* din domeniu, se alege opțiunea **Add a domain controller to an existing forest**, trebuind de asemenea specificat numele utilizatorului care realizează adăugarea acestui *domain controller* în domeniu (de obicei administratorul domeniului).

În fereastra **Additional Domain Controller Options** se alege opțiunea **Read-Only Domain Controller**, eventual se pot alege și alte opțiuni, și anume DNS sau *Global Catalog*.



De asemenea se poate specifica și numele unui utilizator sau grup de utilizatori care vor avea drepturi administrative locale pe acel *domain controller*.



În urma instalării se crează un cont pentru acesta în containerul *Domain Controllers* , vizibil din **Active Directory Users and Computers**.

Un RODC trebuie să aibă un *RWDC (Read Write Domain Controller*) ca partener de replicare, nu poate să preia datele de la un alt RODC.

Password Replication Policy (Politica de replicare parole)

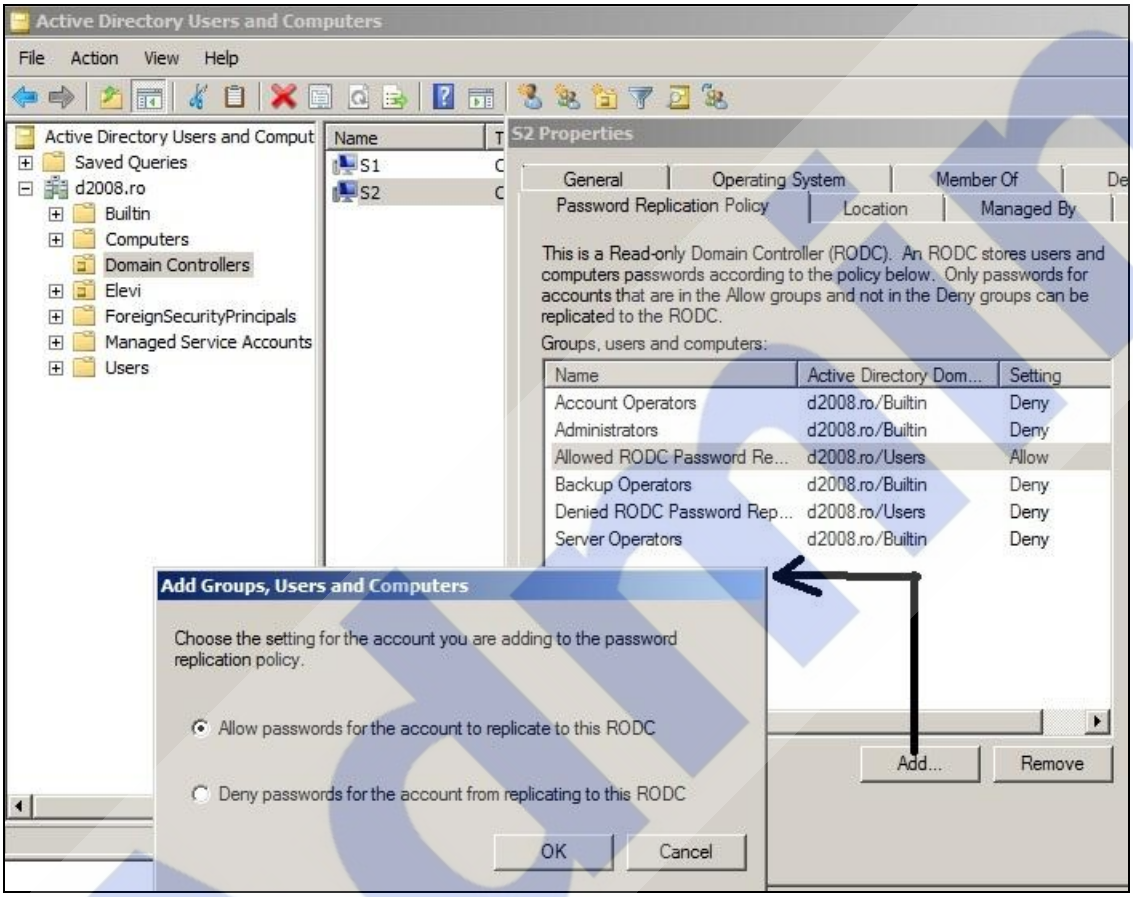
În mod implicit, pe RODC nu sunt salvate parolele pentru conturi, deci nu poate fi folosit pentru autentificare.

Conform politicii specificate, de tip *Password Replication Policy,* anumite credențiale pot fi stocate pe RODC și pentru acei utilizatori acesta poate fi folosit pentru autentificare. Stocarea se realizează după ce s-a realizat o

autentificare a acelui utilizator folosind un RWDC sau se poate realiza o prepopulare a RODC cu credențialele necesare.

Din proprietățile contului pentru RODC, tab-ul *Password Replication Policy,* putem specifica pentru un utilizator, computer sau grup dacă se salvează sau nu parola pe RODC.

Specificarea este în formatul *Allow* sau *Deny*, iar *Deny* are precedență.



Există două grupuri predefinite, *Allowed RODC Password Replication Group*, care au dreptul de Allow pentru salvarea parolelor pentru orice RODC din domeniu, respectiv *Denied RODC Password Replication Group,* care au dreptul de Deny pentru salvarea parolelor pentru orice RODC din domeniu.

De asemenea, grupurile *Account Operators, Server Operators, Backup Operators* și *Administrators* au dreptul de *Deny* pentru salvarea parolelor pentru orice RODC din domeniu.

Implicit, grupul *Allowed RODC Password Replication Group* nu are niciun membru iar grupul *Denied RODC Password Replication Group* conține urmatorii membri: *Enterprise Domain Controllers, Enterprise Read-Only Domain Controllers, Group Policy Creator Owners, Domain Admins, Cert Publishers, Enterprise Admins, Schema Admins, krbtgt*.

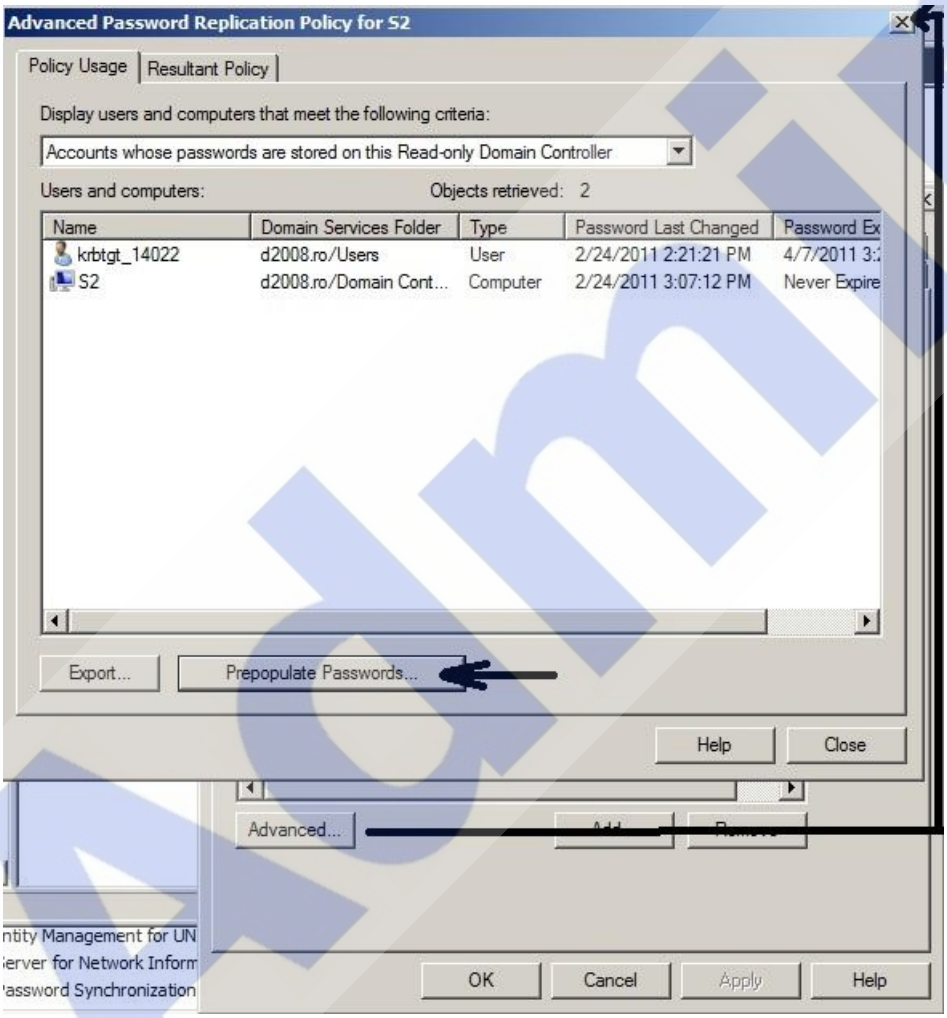
Folosind butonul **Add** putem adăuga în listă utilizatori, computere sau grupuri de utilizatori.

Pentru a putea fi folosit integral pentru logare, RODC trebuie să dețină credențiale atât pentru contul de utilizator cât și pentru cel de computer.

Folosind butonul **Advanced** putem vizualiza conturile pentru care este sunt stocate credentialele pe acel RODC .

Folosind butonul **Prepopulate**, putem prepopula cache-ul RODC cu credențiale pentru anumite conturi, dar acestea trebuie să fie dintre cele care au permisiunea de a salva parola pe RODC.

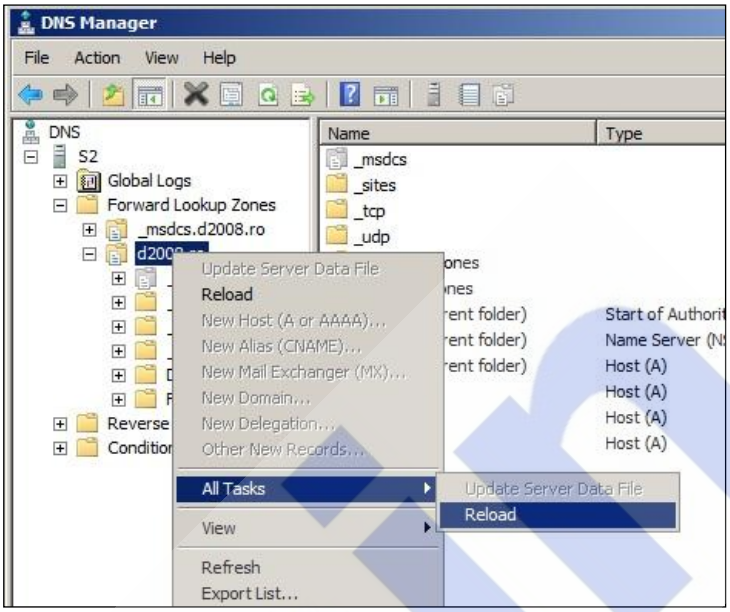
Nu există nicio modalitate de a șterge aceste credentiale din cache.



Read Only DNS (RODNS)

Dacă RODC este și server DNS, atunci va deveni *RODNS (Read Only DNS)* pentru zonele DNS integrate în *Active Directory* și replicate pe acesta. Înregistrările din aceste zone nu pot fi modificate pe acest server.

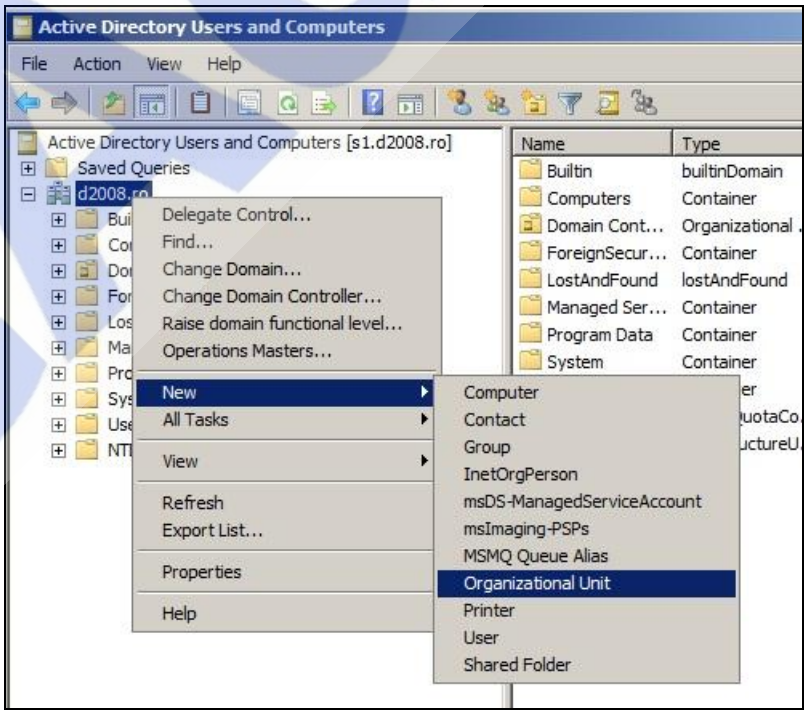
Se pot crea însă zone neintegrate *Active Directory* pe acest server DNS, care să fie de tip *writable*.



Active Directory Users and Computers

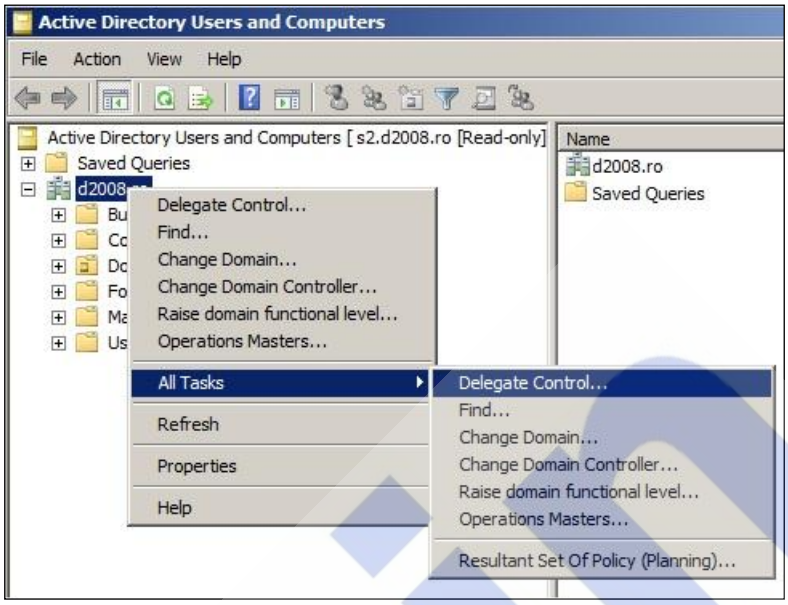
Active Directory Users and Computers este utilitarul care afişează structura logică, arborescentă a unui domeniu. El asigură interfaţa pentru crearea şi administrarea obiectelor din *Active Directory*. Pentru creare folosim întotdeauna comanda **New**. Obiectele, oricare ar fi ele, sunt recunoscute prin nume.

Exemple de obiecte: unitate organizațională, useri, computere, grupuri.

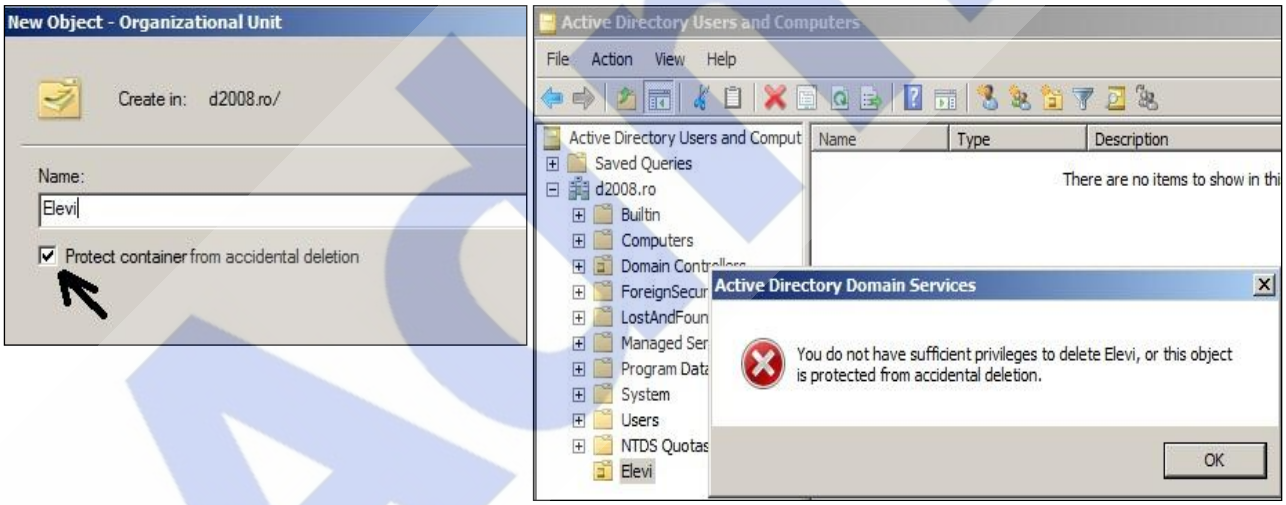


Pentru a crea obiecte noi trebuie accesat un RWDC.

În figura alaturată este prezetat un RODC, pentru care nu avem opțiunea de creare noi obiecte (nu există comanda **New**).

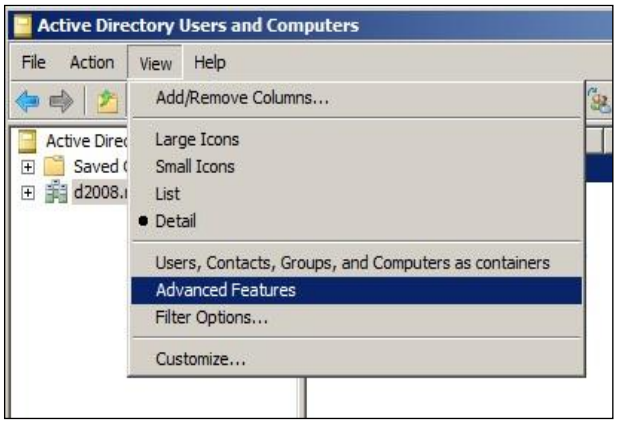


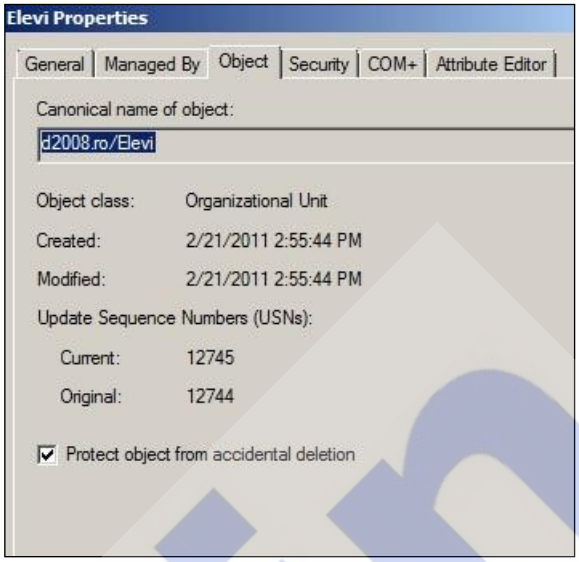
Când se crează o unitate organizațională nouă, aceasta este protejată la ștergere, niciun utilizator neputând efectua acest lucru. Implicit bifa **Protect Container from Accidental Deletion** este selectată și obiectul nu poate fi șters.



Pentru ca obiectul să poată fi şters, se poate anula efectul acestei bife accesând tab-ul **Object** din proprietăţile obiectului.

Toate obiectele au acest tab, chiar dacă la creare nu este vizibilă bifa pentru protecţie. Implicit acest tab nu este vizibil, el poate fi accesat numai dacă se selectează opţiunea **Advanced Features** din meniul **View**. În acest caz putem deproteja sau proteja la ştergere acel obiect.





Group Policy

Există aproximativ 700 de setări noi disponibile în *Windows Server 2008*. Exemple de astfel de setări:

Categoria	Descriere	Locația setării
Antivirus	Gestiune atașamente	User Configuration\Administrative Templates\Windows Components\Attachment Manager
Client Help	Gestionare asistență Online	Computer Configuration\Administrative Templates\Online Assistance User Configuration\Administrative Templates\Online Assistance
Deployed Printer Connections	Conectare automată imprimante	Computer Configuration\Windows Settings\Deployed Printers User Configuration\Windows Settings\Deployed Printers
Internet Explorer 7	Setări Internet Explorer 7	Computer Configuration\Administrative Templates\Windows Components\Internet Explorer User Configuration\Administrative Templates\Windows Components\Internet Explorer

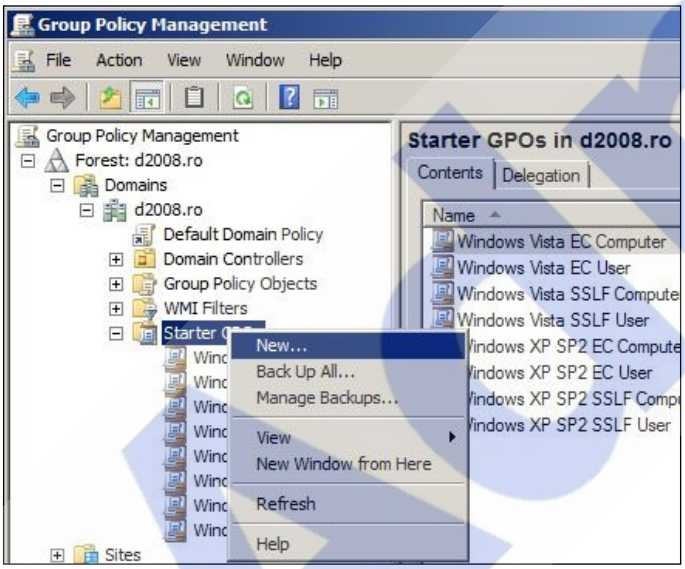
Networking: Wired Wireless	Configurare politici retele cu sau fără fir	Computer Configuration\Windows Settings\Security Settings\Wired Network (IEEE 802.11) Policies Computer Configuration\Windows Settings\Security Settings\Wireless Network (IEEE 802.11) Policies
Power Options	Configurare opțiuni Power Options din Control Panel	Computer Configuration\Administrative Templates\System\Power Management
Security Protection	Combină gestionarea Windows Firewall și IPsec	Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security
Windows Error Reporting	Gestionare Windows Feedback	Computer Configuration\Administrative Templates\Windows Components\Windows Error Reporting User Configuration\Administrative Templates\Windows Components\Administrative Templates\Windows Error Reporting
Removable Storage	Permite controlarea instalării de dispozitive hardware de tip Removable Storage, citirea și scrierea pe acestea	Computer Configuration\Administrative Templates\System\Removable Storage Access User Configuration\Administrative Templates\System\Removable Storage Access

eAdmin

Starter GPO

Este un şablon pe baza căruia se pot crea GPO-uri.

Când se crează un GPO nou, se poate alege ca acesta să aibă la bază un *Starter GPO*, deci va porni cu setările existente în acesta şi nu va fi un GPO gol. Crearea *Starer GPO* se realizează folosind **Group Policy Management.**

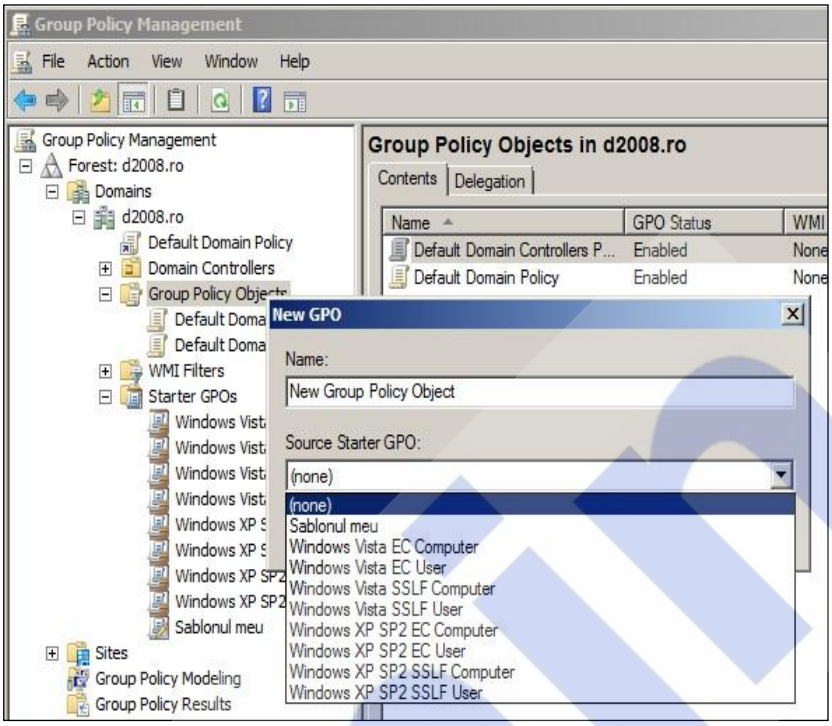


În urma creării *Starter GPO folder* sunt create anumite astfel de șabloane care vor putea fi folosite ulterior și de asemenea ne putem crea propriile noastre șabloane.

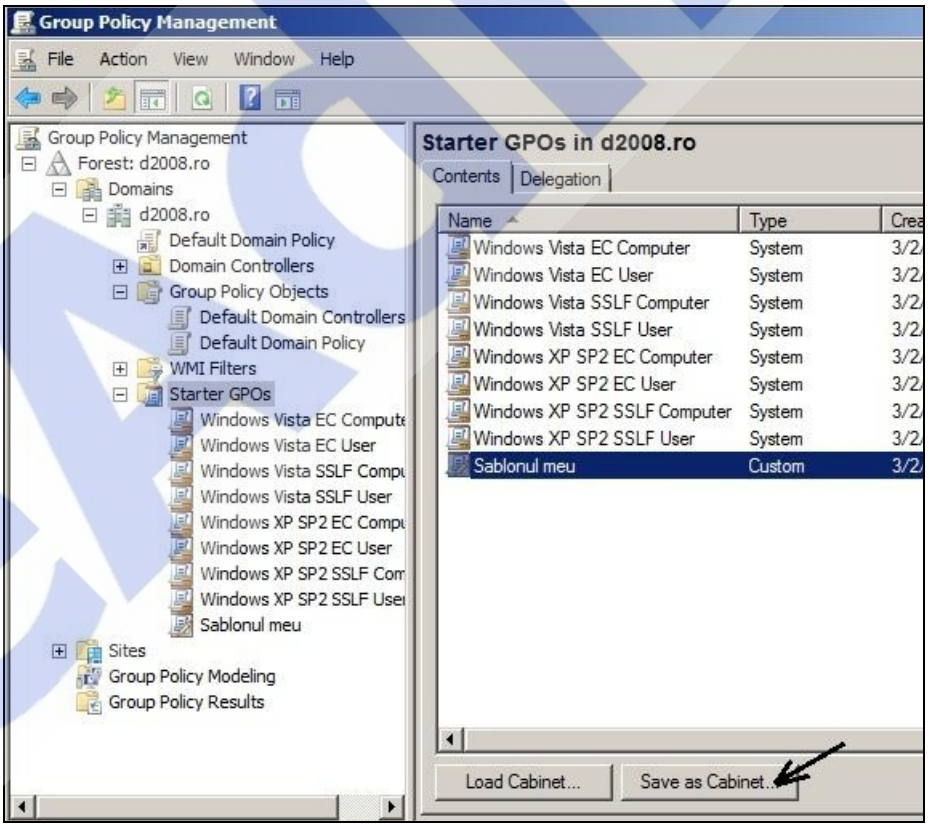
Editarea acestuia se realizează folosind același utilitar cu care se realizează editarea GPO-urilor, și anume **GPO Editor**.

Spre deosebire de un GPO obișnuit, acesta nu conține decât nodul **Administrative Templates**, atât pentru *User Configuration* cât și pentru *Computer Configuration*.

În momentul când se crează un GPO nou putem alege ca acesta să aibă ca sursă un *GPO Starter* dintre cele existente sau nici unul, dacă dorim ca GPO-ul nou creat să fie gol.



Putem salva un *GPO Starter* ca și fișier .cab (de tip cabinet), care poate fi încărcat ulterior, chiar și pe un alt *forest*. Pentru aceasta se folosesc butoanele **Save as Cabinet** (pentru salvare) respectiv **Load Cabinet** pentru încărcarea unui *GPO Starter* dintr-un fișier cabinet salvat anterior.



Fișierele .adm și .admx

În template-uri sunt definite setări de politică de grup. În *Windows Server 2008* există sute de setări noi şi un nou format de fişier pentru a defini aceste setări.

În mod tradiţional au fost folosite fișierele de tip .adm pentru a defini setările care se pot configura prin politica de grup. Șabloanele .adm sunt amplasate în folderul ***%SystemRoot%\Inf***.

Windows Vista şi *Windows Server 2008* introduc un nou format pentru setările de tip registry din politicile de grup, și anume un format de fişier XML cunoscut sub numele de fişiere ADMX, înlocuind fişierele ADM.

Fişierele ADMX conţin două componente: template-uri ADMX şi fişiere ADML.

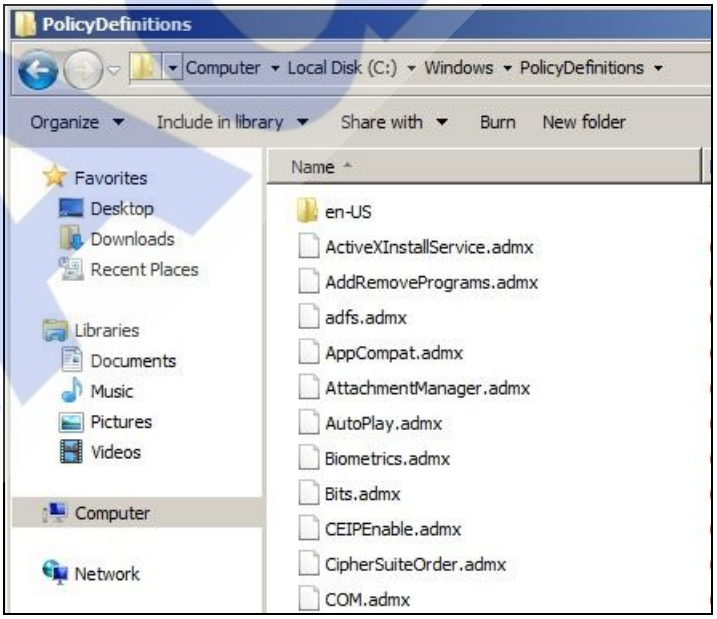
Fișierele ADMX sunt independente de limbă.

Fișierele ADML furniezază textul de pe ecran şi fiecare limbă are un fişier ADML separat. În acest fel, administratorii din diferite ţări pot vizualiza acelaşi GPO , dar în limba lor maternă.

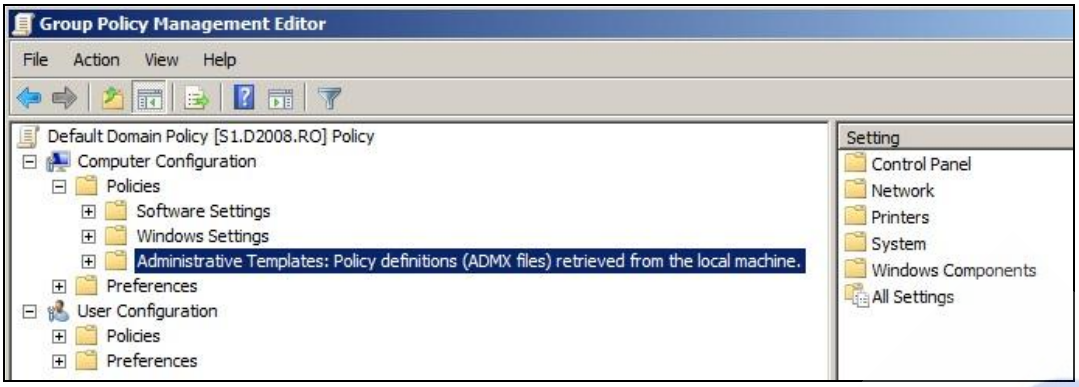
Fişierele ADMX şi ADML nu sunt copiate în SYSVOL, așa cum sunt fișierele ADM, ci ele se află pe computerul local. În SYSVOL există numai setările efective, în acest mod se minimizează dimensiunea acestui folder.

Fișierele ADMX sunt stocate în folderul ***%SystemRoot%\PolicyDefinitions***.

Fişierele ADML sunt stocate într-un subfolder al lui *PolicyDefinitions*, specific limbii, de exemplu pentru engleză ***%systemroot%\policyDefinitions\en-us*.**



În momentul în care editățm un GPO, este specificat faptul că fișierele ADMX sunt încărcăte de pe mașina locală.



Central Store (Locație centrală)

Pentru cazul când se lucrează cu domenii, administratorii pot crea o locaţie centrală, numită *central store*, care conține fişierele ADMX și ADML pentru întregul domeniu.

Group Policy Management Editor (GPME) din *Windows Server 2008* , va citi și afişa în mod automat în **Administrative Template** setările din fişierele ADMX din central store şi le va ignora pe cele stocate local.

În cazul în care controlerul de domeniu nu este disponibil, vor fi utilizate fişierele ADMX și ADML locale.

Crearea *central store* se efectuează manual, pe domain controller în locatia ***%systemroot%*\sysvol\domain\policies,** folderul **PolicyDefinitions,** prin copierea fișierelor ADMX corespunzatoare.

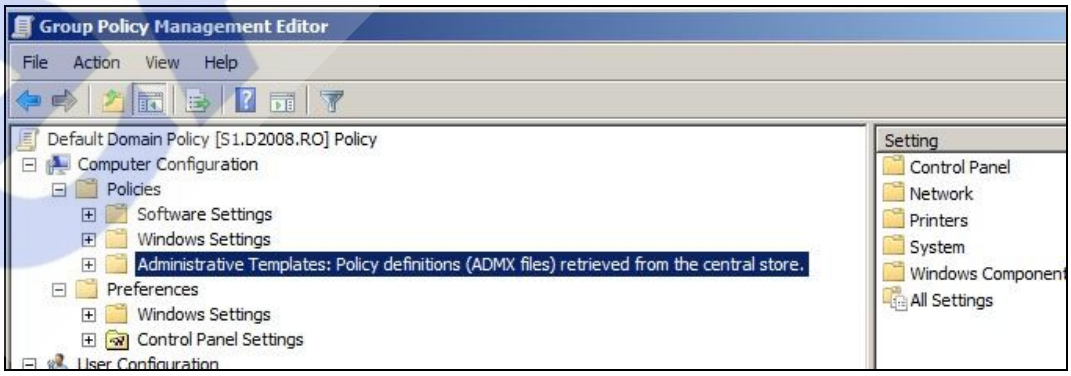
De asemenea se crează în folderul
***%systemroot%*\sysvol\domain\policies\PolicyDefinitions**

câte un subfolder pentru fiecare limbă folosită, unde se vor copia fișierele ADML corespunzatoare.

De exemplu pe *domain controller* putem copia
C:\Windows\Policydefinitions

în **C:\Windows\SYSVOL\domain\policies\PolicyDefinitions.**

În urma creerii *central store*, GPME afișează această informație.

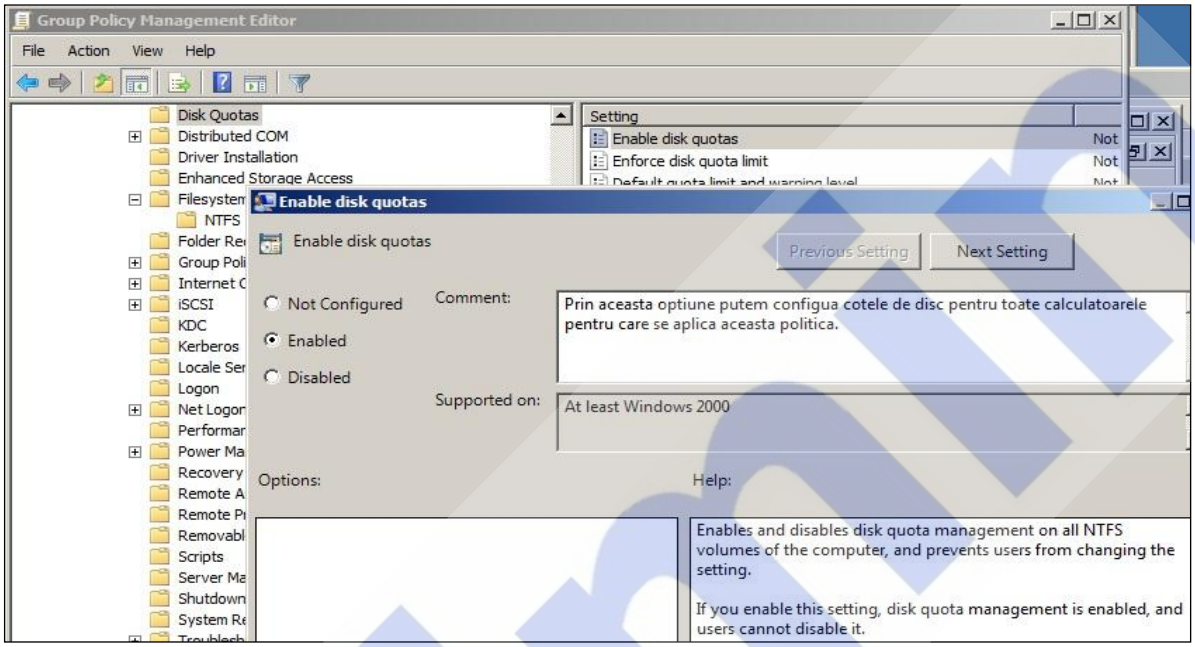


Pentru compatibilitate cu clienți mai vechi se poate lucra în continuare cu fișiere de tip ADM, deoarece aceștia nu vor înțelege decât astfel de fișiere.

Imbunătățiri aduse în Group Policy Management Editor

Comentarea setărilor

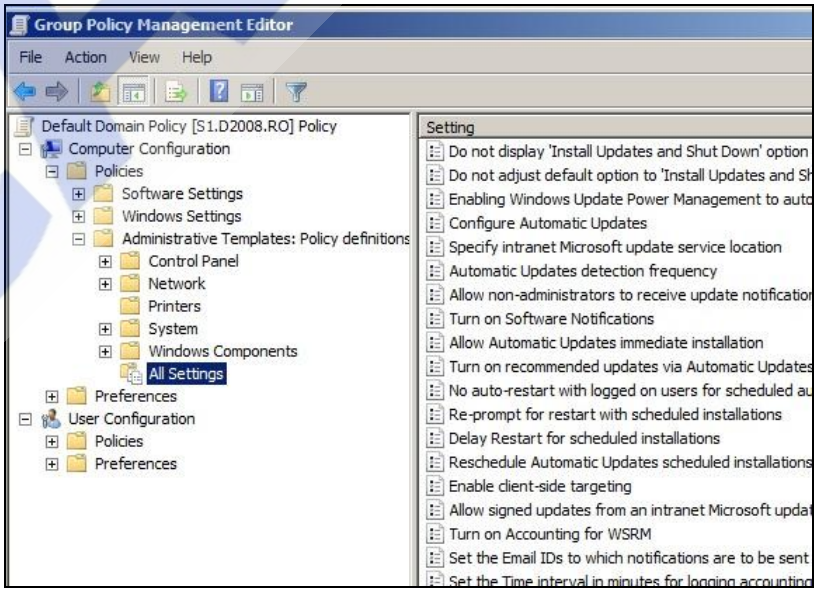
Fiecare setare de tip **Administrative Templates** are un tab nou, numit comentariu, în proprietăţile acesteia. Adăugarea de comentarii este facultativă, dar ea oferă posibilitatea de a documenta scopul utilizării setării respective.



All Settings

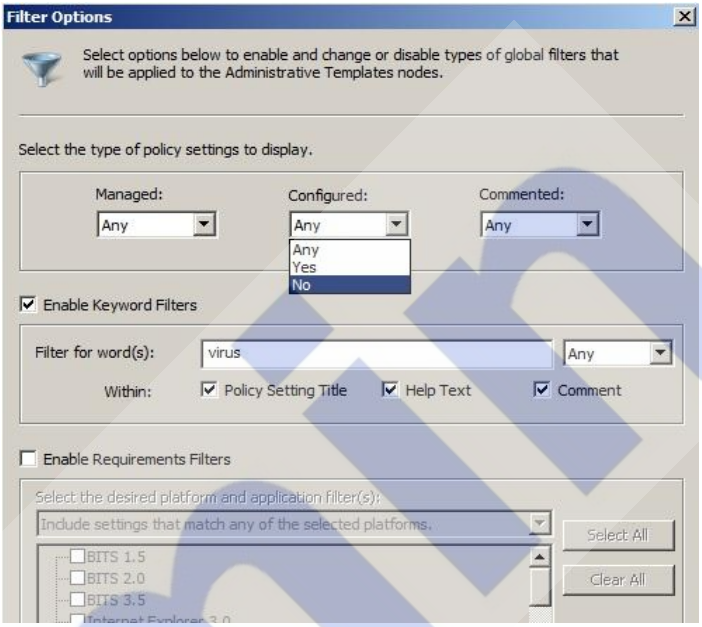
Nodul **All Settings** există atât în **Computer** cât și în **User Administrative Templates** din GPME. Furnizează următoarele informații:

- Listarea alfabetică a tuturor setărilor
- Starea lor (*configured* sau *not configured*)
- Dacă sunt sau nu comentate
- Calea în ierarhia **Administrative Templates**



Filtrarea

Există posibilitatea de a filtra setările care satisfac anumite condiții, de exemplu putem căuta dupa anumite cuvinte cheie sau putea vizualiza numai setările care sunt configurate.



Group Policy Preferences

Group Policy Preferences (GPP) , facilitate nou introdusă în *Windows Server 2008*, adaugă o serie de setări de configurare a clientului, atât pentru partea de **Computer Configuration** cât și pentru cea de **User Configuration**. Ambele conțin două subfoldere, **Windows Settings** și **Control Panel Settings**.

Sunt disponibile numai pentru politicile din domeniu, nu și pentru cele locale.

Numele *Preferences* subliniază faptul că toate aceste facilități noi adăugate de GPP sunt doar niște preferinţe, în contrast cu politicile, care nu pot fi anulate de către un utilizator final. Astfel, ele permit o mare varietate de configurări suplimentare, care anterior necesitau logon script-uri complexe pentru automatizare.

Pentru a fi suporate de clienții mai vechi, trebuie instalat pe aceștia **Group Policy preferences client-side extension (CSE)**, descărcabil de pe site-ul Microsoft. Acesta există pentru următoarele versiuni de sistem de operare:

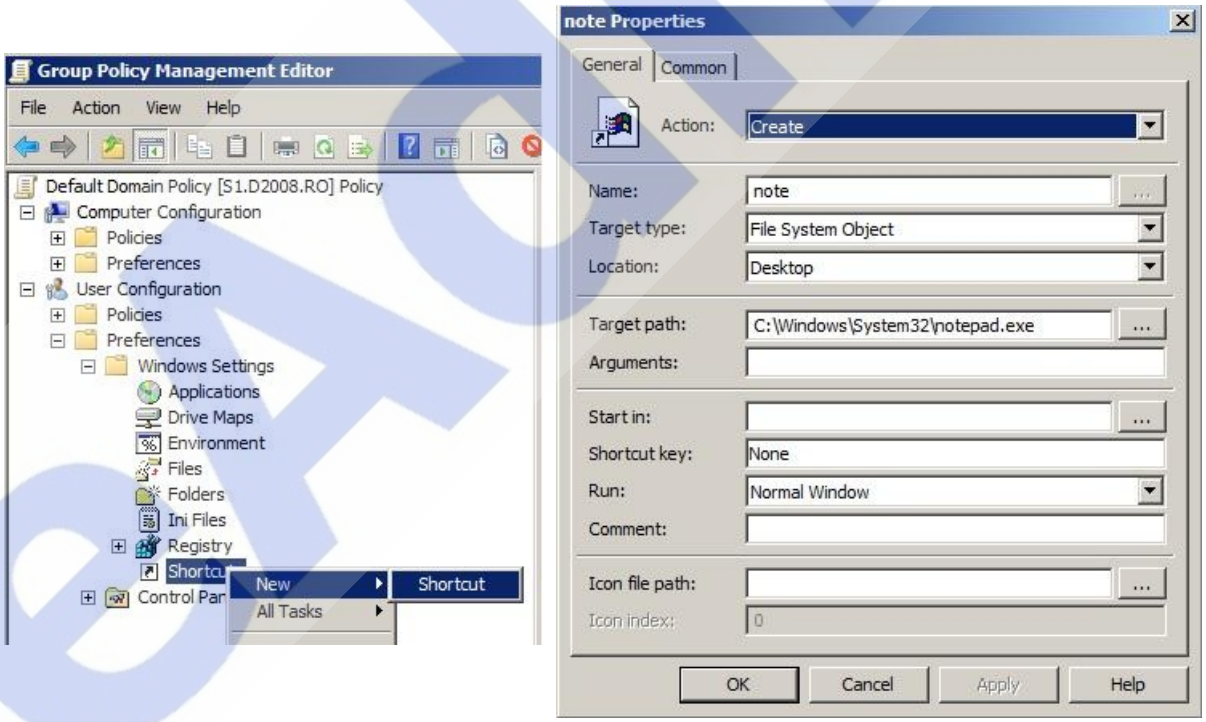
- *Windows XP SP2* sau superior
- *Windows Vista* sau superior
- *Windows Server 2003 SP1* sau superior

Majoritatea *Group Policy Preference* suportă următoarele acţiuni pentru fiecare element preferinţă:

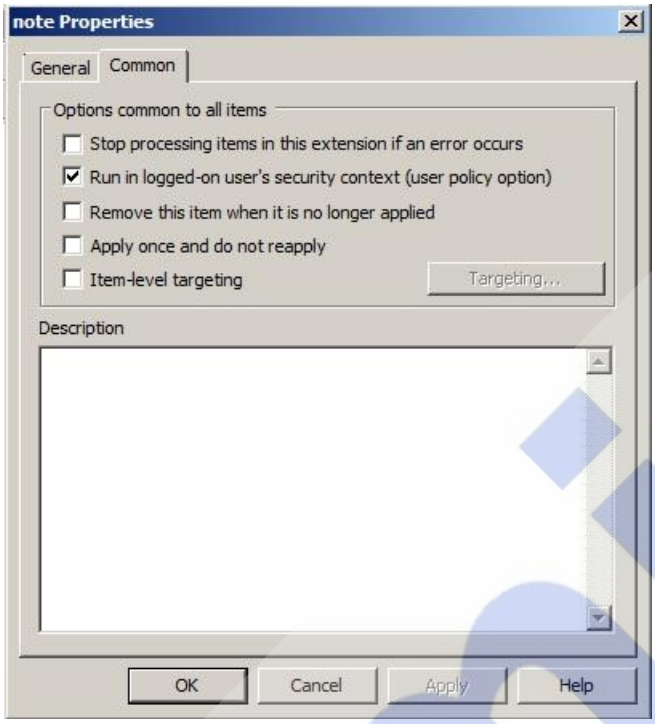
Create - pentru a crea un element nou pe computerul ţintă
Delete - pentru a șterge un element de pe computerul ţintă
Replace - pentru a șterge și recrea un element pe computerul ţintă
Update - pentru a actualiza un element de pe computerul ţintă

Printre setările care pot fi efectuate folosind GPP se numară posibilitatea de a crea/șterge/actualiza/înlocui variabile de mediu, fișiere, foldere, chei registry, imprimante, foldere partajate, utilizatori și grupuri de utilizatori locali, de a configura meniul de start, Internet Options, *Folder Options*, de a crea *Scheduled Tasks*.

Crearea unui GPP se realizează folosind opțiunea New.



Fiecare GPP conține tabul **Common** care permite configurarea de opţiuni suplimentare ce controlează comportamentul elementului.



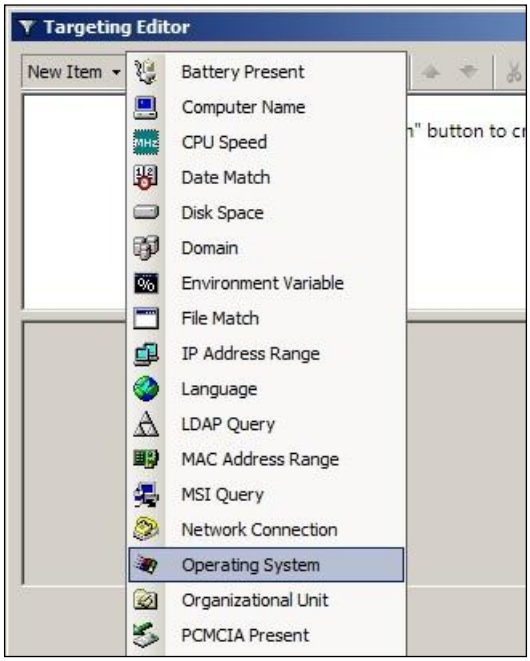
Stop processing items in this extension if an error occurs - pentru a nu mai fi procesate celelalte preferințe, în cazul în care a apărut o eroare.

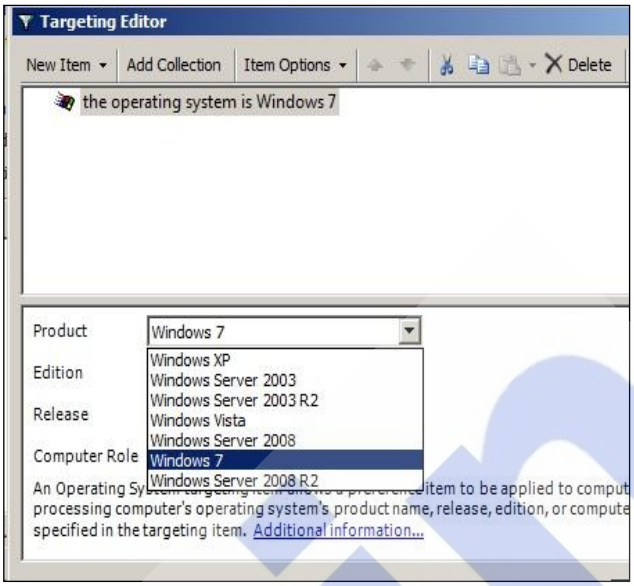
Run in logged-on user's security context – pentru a rula ca userul logat și nu ca și *local System account*, asa cum se întâmplă implicit.

Remove this item when it is no longer applied – pentru a stabili ce se întimplă cu setarea respectivă atunci când preferința nu se mai aplică . Se poate stabili, dacă opțiunea nu e bifată, ca setarea să ramană validă în continuare.

Apply once and do not reapply – pentru a stabili dacă preferința se reaplică în timpul reaplicării normale şi periodice a GPO-urilor. Dacă opţiunea nu e bifată, utilizatorul poate face modificări asupra acelei preferinţe şi ele rămân în continuare valide, nu vor fi suprascrise la următoarea reaplicare GPO. Aceasta este o facilitate care nu există la setările GPO anterioare, la acestea chiar dacă utilizatorul ar fi putut modifica opţiunea respectivă, nu exista nici un fel de modalitate de a împiedica ca reaplicarea politicii să efectueze la loc modificările, conform cu cele existente în GPO.

Item-level targeting – pentru a determina pe ce calculatoare sau pentru ce utilizatori se aplică politica. Se pot stabili criterii complexe, de exemplu putem stabili ca acele calculatoare să aibă un anumit sistem de operare sau să aibă adresa IP într-un anumit rang de adrese.

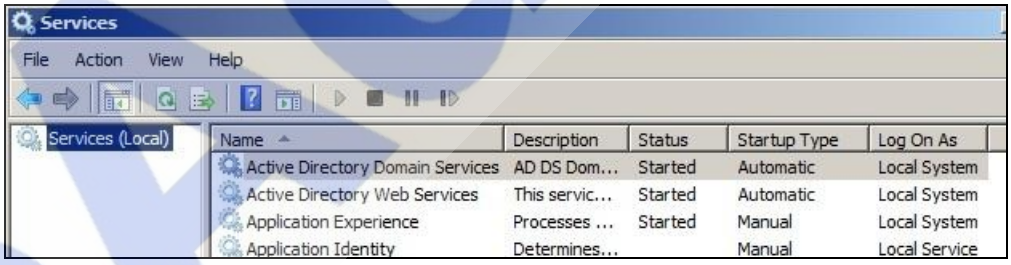




Gestionarea AD DS

Serviciul AD DS în *Windows Server 2008* poate fi oprit şi repornit, ca orice alt serviciu, în timp ce maşina este pornită. În versiunile anterioare, în cazul în care un administratorul dorea să pornească un domain controler fără încărcare lui *Active Directory*, serverul trebuia repornit în *Active Directory Restore Mode*, deci necesita o restartare a sistemului.

În *Windows Server 2008*, serviciul de director pot fi oprit în timp ce maşina este în stare de funcţionare, existând astfel întreruperi minime pentru alte servicii.

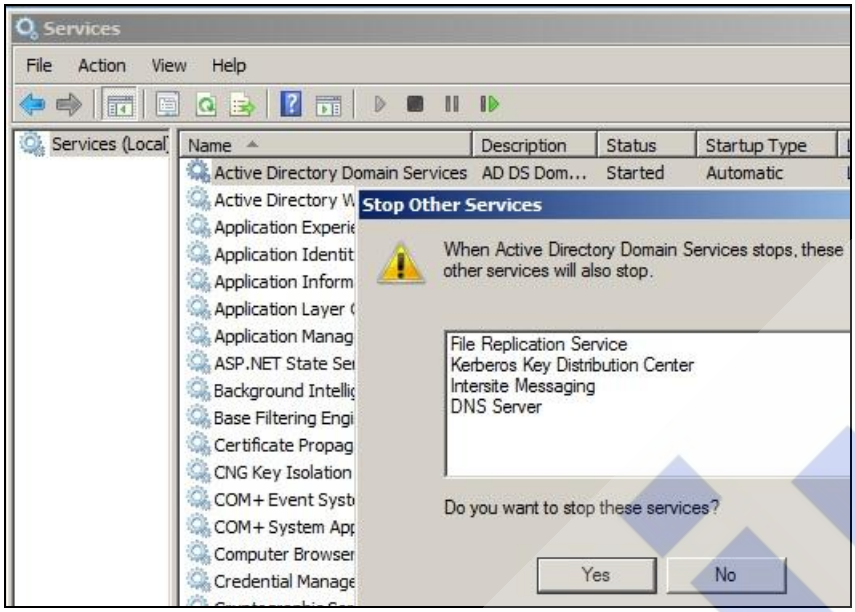


Exemple de operații care pot fi efectuate cu serviciul AD DS offline:

- defragmentare offline
- mutarea fişierelor bazei de date *Active Directory* sau a fișierelor de log

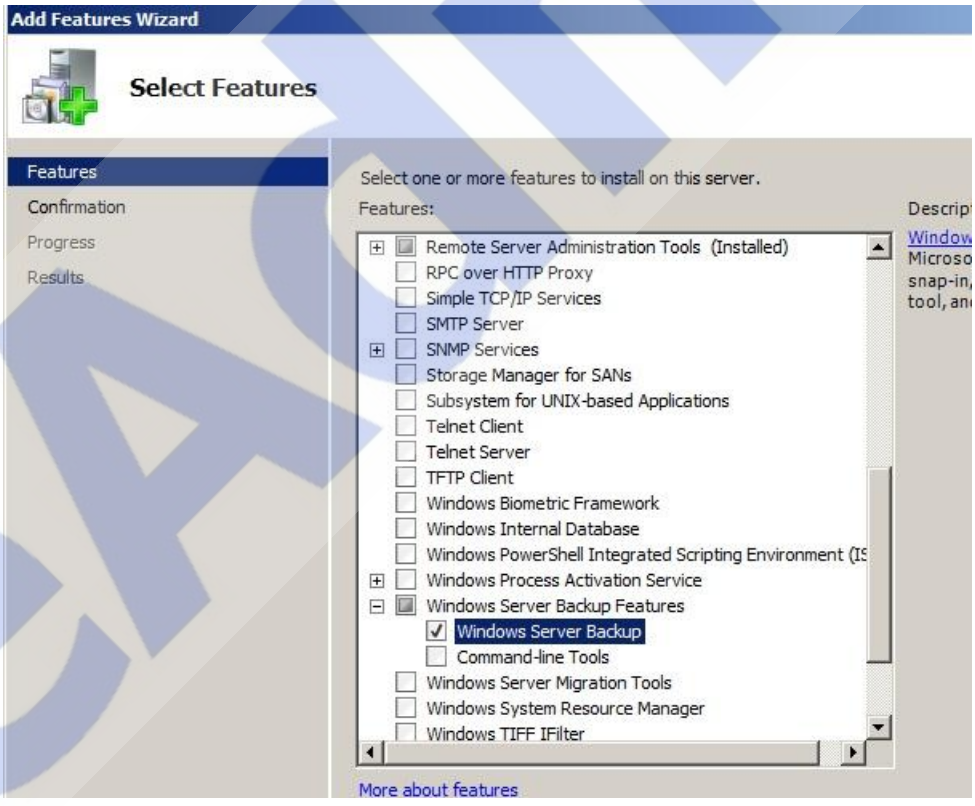
Oprirea serviciului AD DS determină oprirea și a următoarelor servicii:

- *Kerberos Key Distribution Center (KDC)*
- *Intersite Messaging*
- *File Replication Service (FRS)*
- *Domain Name System (DNS)*, dacă serviciul este instalat



Salvarea şi restaurarea AD DS

Se realizează folosind **Windows Server Backup**. Acesta nu este instalat implicit, ci trebuie adăugat ca și *feature* folosind **Add Features** din **Server Manager**.

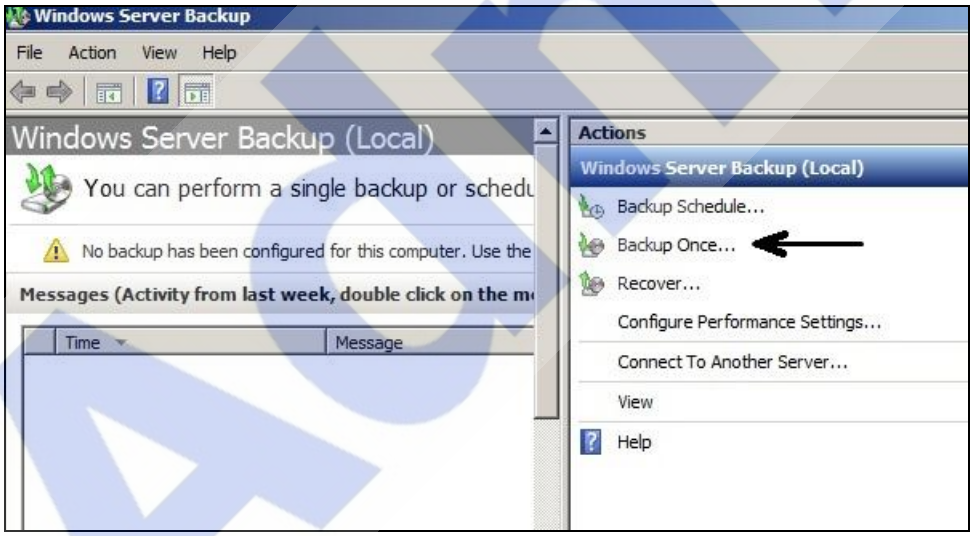


Salvarea bazei de date *Active Directory* se realizează prin salvarea la controlerul de domeniu, folosind utilitarul **Windows Server Backup**, a lui *System State* (starea sistemului).

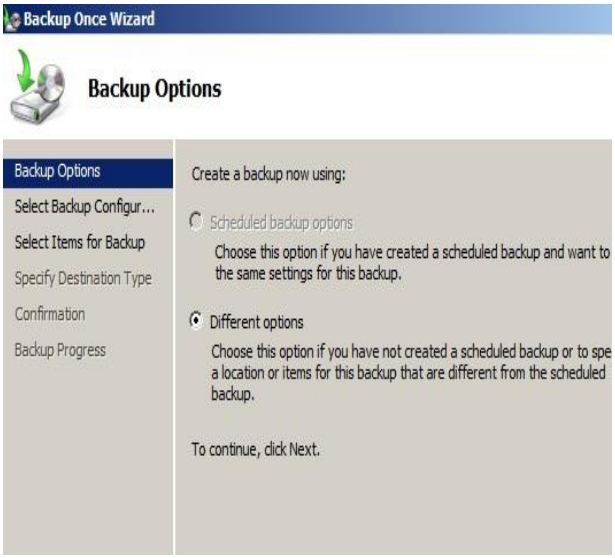
Componentele *System State* pentru controlerele de domeniu sunt următoarele:

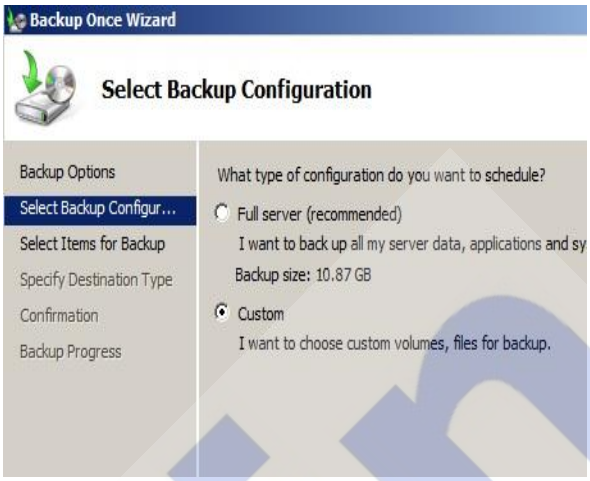
- Baza de date *AD DS*
- *folder*-ul partajat *SYSVOL*
- *Registry*
- *System startup files*
- *COM + Class Registration database*
- *Baza* de date pentru *Certificate Services* **–** numai în cazul în care este instalat serviciul *Certificate Services* pe controlerul de domeniu
- *Cluster service information* **-** numai în cazul în care controlerul de domeniu face parte dintr-un *cluster*.
- *Microsoft Internet Information Services (IIS) metadirectory* - numai în cazul în care este instalat serviciul *Internet Information Services* pe controlerul de domeniu.
- Fișierele sistem protejate de *Windows Resource Protection.*

Salvarea se realizează folosind utilitarul **Windows Server Backup**, accesibil după instalare *feature* din **Administrative Tools**.

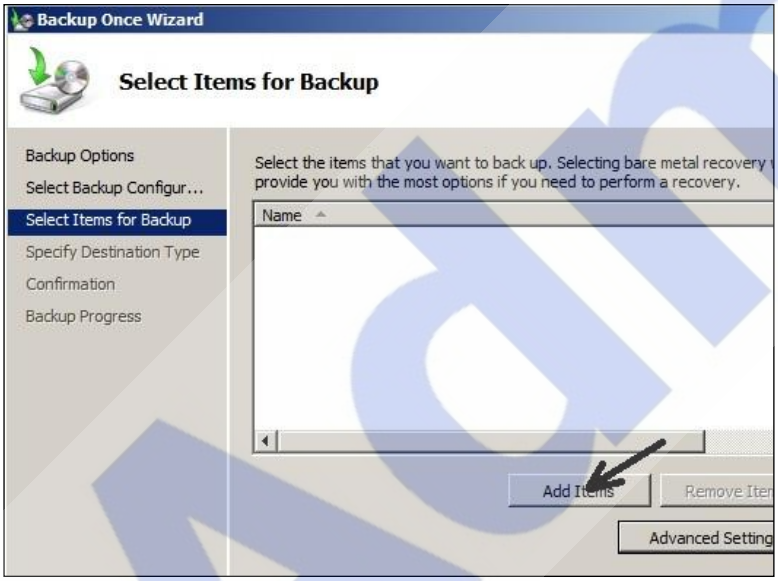


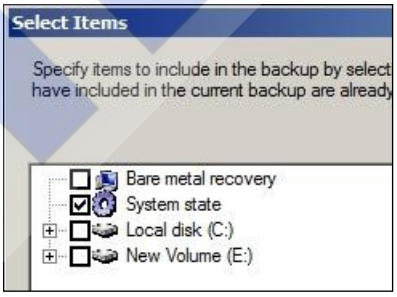
Vor trebui specificate opțiunile de *Backup* și configurația necesară.



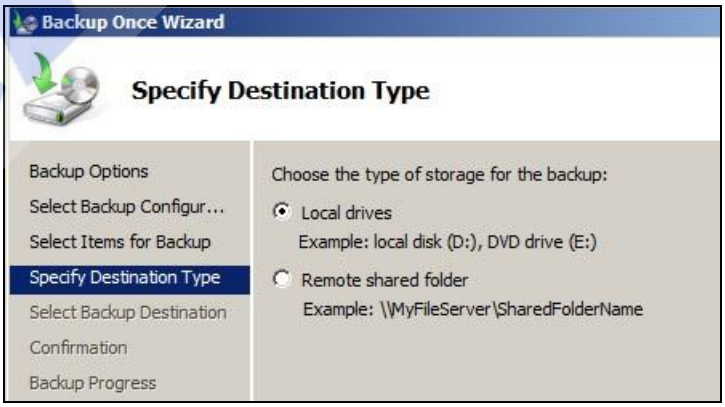


Vor trebui alese componentele care vor fi salvate, în cazul nostru *System State*.

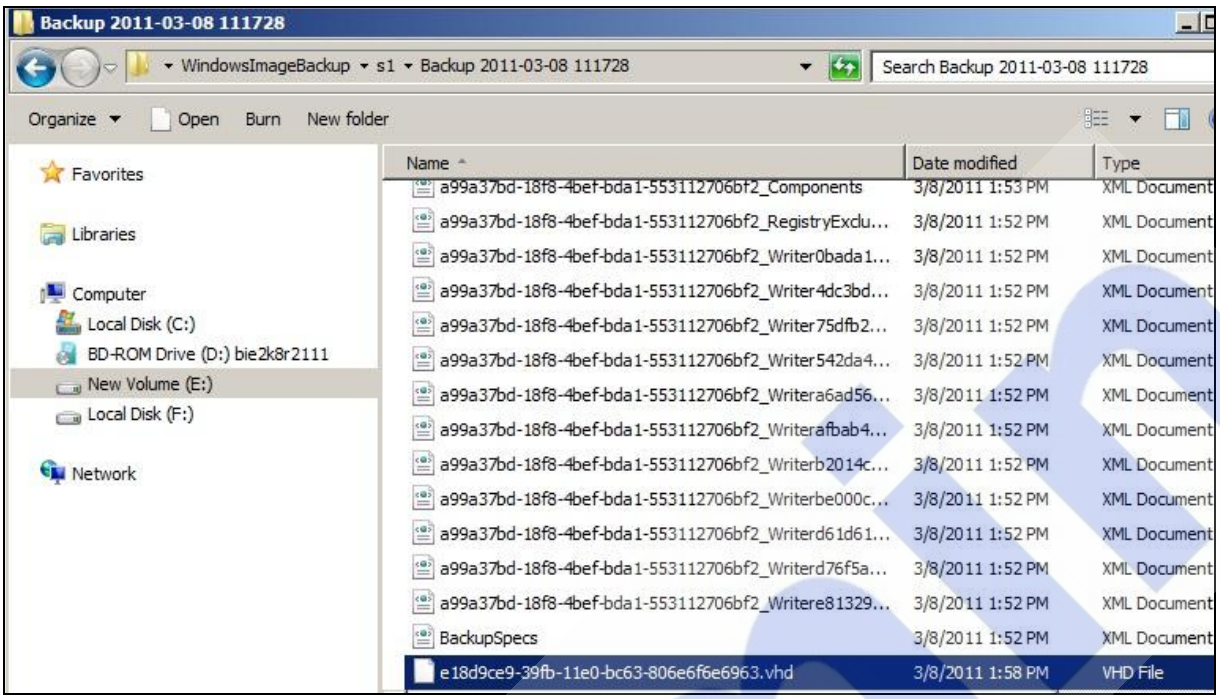




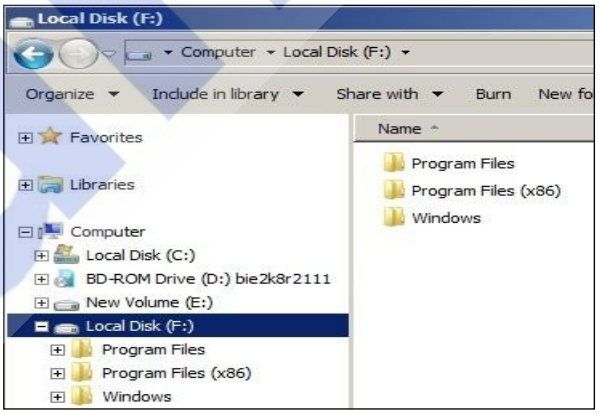
În continuare trebuie specificată locația unde va fi salvat fișierul de *backup*, poate fi local sau pe un folder partajat de pe un alt server.



Fișierul de *backup* are extensia .vhd. În afară de acesta mai există și fișiere .xml care conțin informații adiționale.



Fișierele .vhd pot fi atașate în **Disk Management** și pot fi vizualizate ca o partiție în sistem, de pe care putem accesa fișiere sau chiar face modificări (dacă nu este atașată *Read Only*).



Pentru restaurarea bazei de date *Active Directory* în urma unei salvări (*backup*) controlerul de domeniu trebuie pornit în modul **Active Directory Restore Mode** (mod restaurare *Active Directory*). Acest mod de lucru se obţine fie prin apăsarea tastei **F8** la startarea serverului şi alegând din meniu intrarea cu acelaşi nume, fie rulând comanda:

bcdedit /set safeboot dsrepair

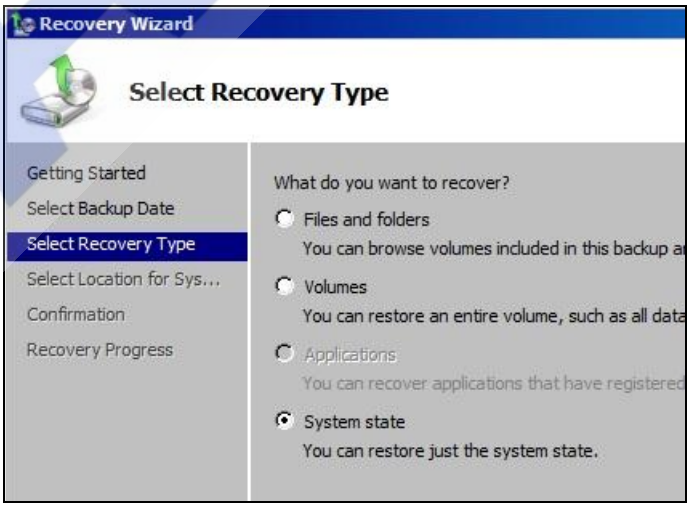
În urma rulării acestei comenzi sistemul va intra în **Active Directory Restore Mode** și la urmatoarea restartare. Pentru a porni în mod normal după efectuarea restaurării trebuie anulat efectul acestei comenzi, rulând comanda:

bcdedit /deletevalue safeboot

După intrarea în **Active Directory Restore Mode** se utilizează utilizarul **Windows Server Backup**, accesibil din **Administrative Tools** și se alege acțiunea **Recover.**

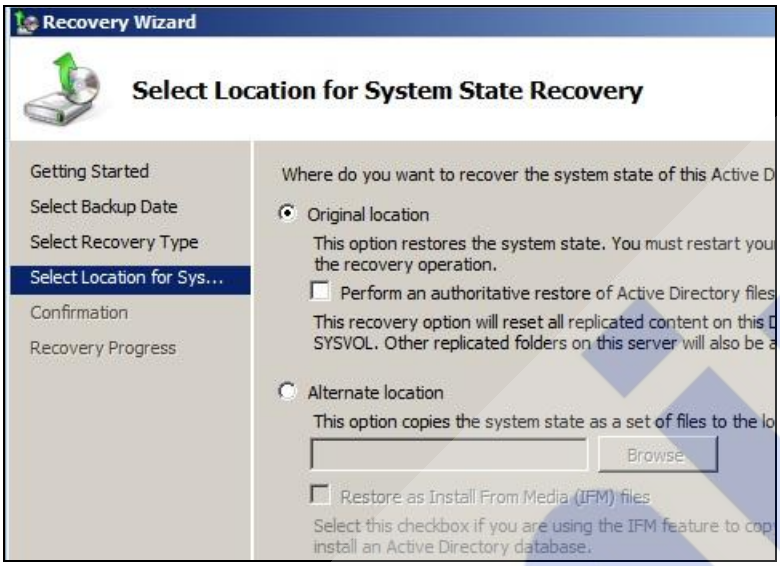
Se specifică locația unde se află fișierul de *backup* și data la care acesta a fost creat.

Se alege ce dorim să restaurăm, în cazul nostru *System State*.



Se alege locația unde vor fi restaurate, poate fi cea originală sau o locație alternativă.

Pentru cazul în care se alege restaurarea în locația originală se poate opta și pentru efectuarea unui *restore autoritativ*.



La fel ca la *Windows 2003*, înainte de a restarta sistemul se poate folosi comanda **ntdsutil** pentru a efectua o restaurare autoritativă pentru întregul *Active Directory* sau numai pentru o ramură din acesta.

Database Mounting Tool (Instrumentul de montare a bazei de date)

Database Mounting Tool (Dsamain.exe) permite administratorilor să vizualizeze şi să compare datele din baza de date de tip *snapshot* fără a fi nevoie să efectueze restaurări ale acestora.

Dsamain.exe se comportă ca un server LDAP, expunând date de tip *snapshot* AD DS. **Dsamain.exe** nu poate fi folosit pentru a restaura datele. **Dsamain.exe** nu conţine în sine un *viewer* pentru date, astfel încât trebuie utilizat un instrument de tip *LDAP viewer*, cum ar fi **LDP.exe**, pentru a vizualiza obiectele, în timp ce **Dsamain.exe** rulează.

Dacă se montează simultan mai multe *snapshoturi* pe un singur server, fiecare *snapshot* trebuie să utilizeze un port diferit pentru serviciile LDAP, SSL, Global Catalog, şi Global Catalog SSL.

Creare snapshot (instantaneu)

Procedura de lucru este următoarea: folosind interfaţa **Command Prompt** se lansează utilitarul **ntdsutil** şi după prompterul **ntdsutil** se introduce de la tastatură:

```
snapshot
activate instance ntds
create
```

Comanda va returna un număr, numit *Snapshot set {GUID},* care va fi folosit ulterior pentru montare.

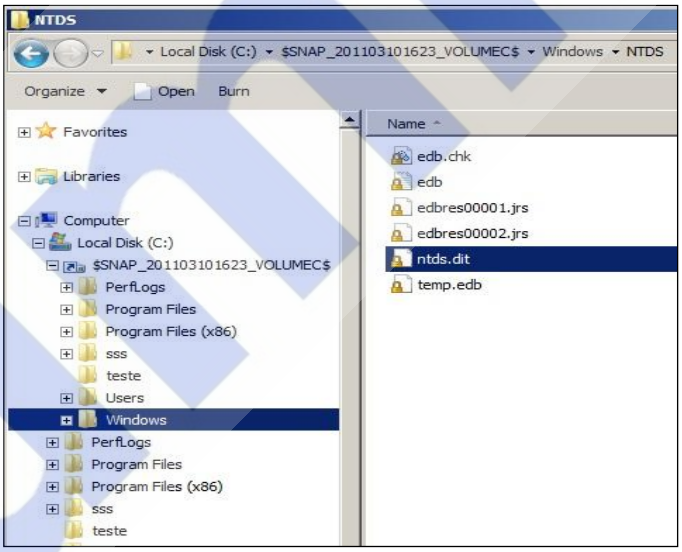
```
C:\Users\Administrator.S1>ntdsutil
ntdsutil: snapshot
snapshot: activate instance ntds
Active instance set to "ntds".
snapshot: create
Creating snapshot...
Snapshot set {b910dab3-3d13-440d-a529-eebd18f00690} generated successf
```

După creare trebuie montat acest *snapshot* pentru a fi accesibil din sistemul de operare, folosind comanda **mount *{GUID},*** din cadrul comenzii **ntdsutil,** unde *{GUID}* este numărul obținut la pasul anterior.

După montare putem părăsi comanda **ntdsutil** lansând de 2 ori **quit**.

```
snapshot: mount {b910dab3-3d13-440d-a529-eebd18f00690}
Snapshot {0f12d3cc-ff7d-46b3-aa3f-d82ce8fad0d5} mounted as C:\$SNAP_201103101623
_VOLUMEC$\
snapshot: quit
ntdsutil: quit
```

În acest moment putem vedea *snapshot-ul* din sistemul de fișiere.



Expunere snapshot ca server LDAP

Se lansează comanda:
Dsamain -dbpath <*calea către ntds.dit din snapshot* > **-ldapport** <*port*>
unde :
<*calea către ntds.dit din snapshot* > este locația fișierului **ntds.dit** din *snapshot* Cum se vede și din imaginea de mai sus, implicit este **windows\ntds\ntds.dit** din locul în care s-a efectuat montarea.

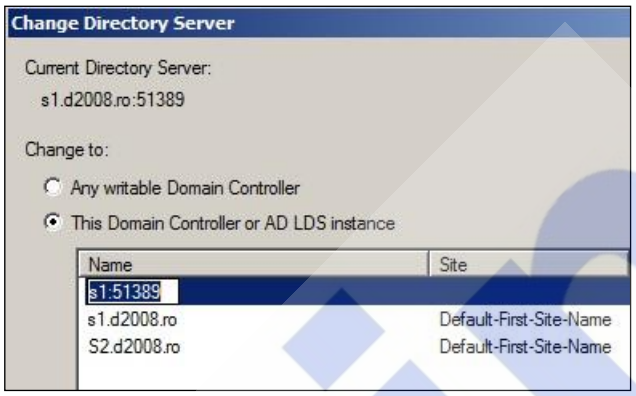
<*port*> este portul LDAP pe care va rula serverul. Trebuie ales un port liber.

Comanda nu se va închide, trebuie să ruleze, pentru a avea acces la datele din snapshot.

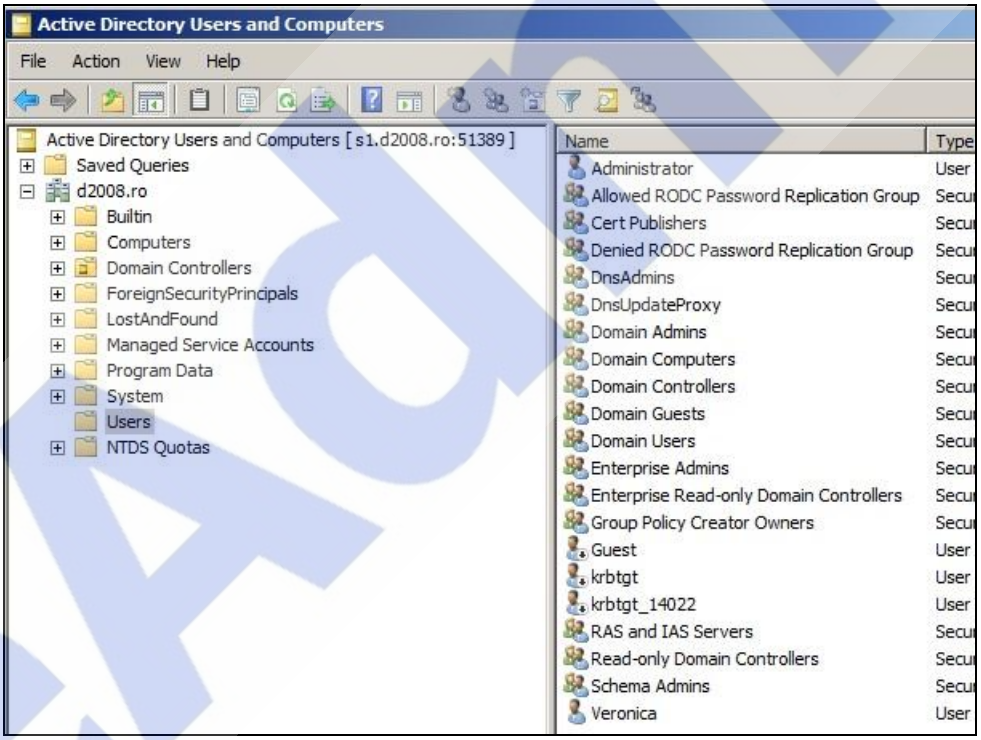
```
C:\Users\Administrator.S1>dsamain -dbpath C:\$SNAP_201103101623_VOLUMEC$\Windows
\NTDS\ntds.dit -ldapport 51389
EVENTLOG (Informational): NTDS General / Service Control : 1000
Microsoft Active Directory Domain Services startup complete, version 6.1.7600.16
385
```

Conectarea la baza de date snapshot

Se realizează folosind **Active Directory Users and Computers**, va trebui să ne conectăm specificând numele serverului și portul pe care acesta rulează.



Obiectele care au fost şterse după crearea *snapshot-ului* vor fi vizibile în acesta cu toate atributele. După reanimarea obiectelor, putem vizualiza valorile acestora şi eventual recrea manual. Nu există nicio modalitate de a copia obiecte sau valori ale atributelor din *snapshot* în instanţa AD DS reală.



Reanimarea obiectelor tombstoned (piatră de mormânt)

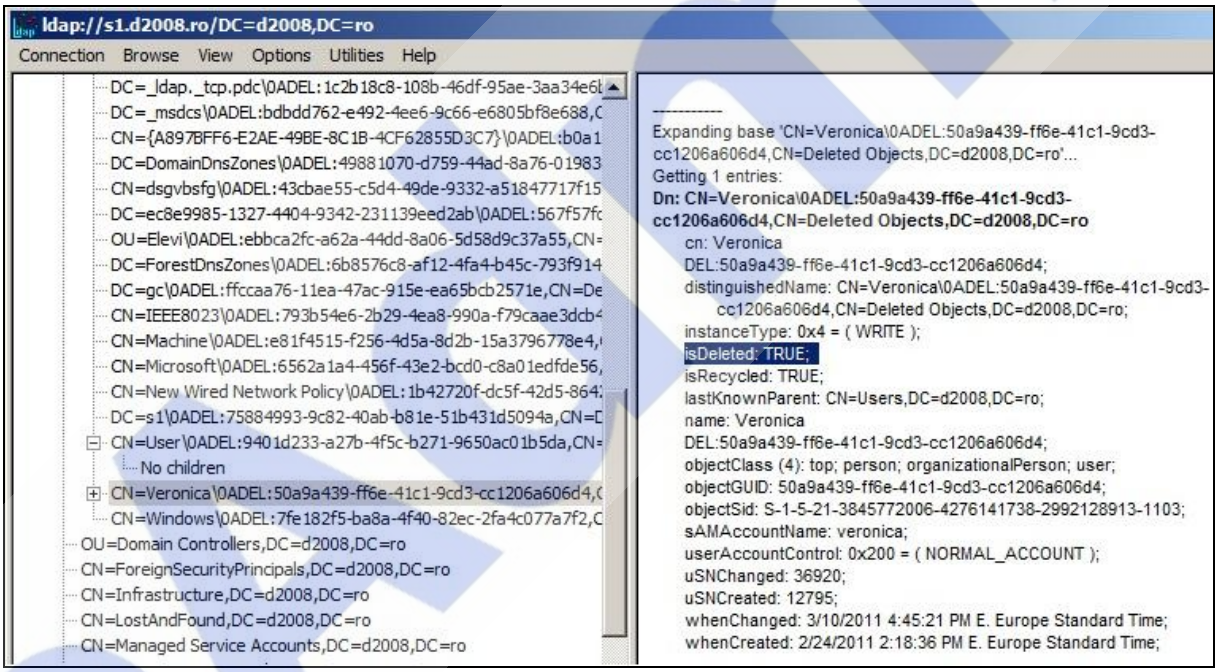
Un obiect *tombstoned* este un obiect care este marcat ca fiind şters în AD DS. Atunci când se şterge un obiect, aceasta este convertit la *tombstone* și va rămâne în baza de date AD DS într-o stare dezactivată pentru un interval de timp specificat de *Tombstone Lifetime*, care este 180 de zile implicit. El este replicat în întregul domeniu şi apoi eliminat de pe fiecare controler de domeniu când durata de viaţă expiră.

Când un obiect este marcat ca fiind *tombstoned*, atributul **isDeleted** este setat la **True** iar de cele mai multe dintre celelalte atribute se elimină. Sunt reţinute doar câteva atribute critice, printre care **SID, ObjectGUID, LastKnownParent, SAMAccountName**. Astfel, chiar dacă administratorul reanimă obiectul, aceasta nu mai are toate informaţiile pe care le-a avut înainte de a fi fost șters. Valorile atributelor lipsă trebuie recreate manual.

Pentru reanimare se folosește comanda :

ldp
meniul **Connection**, **Connect**, **OK**.
meniul **Connection** , **Bind**, **OK**
meniul **Options , Controls**
în lista **Load Predefined** , se alege **Return Deleted Objects**, **OK**
meniul **View, Tree**, alegem DC=d2008,DC=ro, **OK**
expandăm CN=Deleted Objects**,** DC=d2008,DC=ro

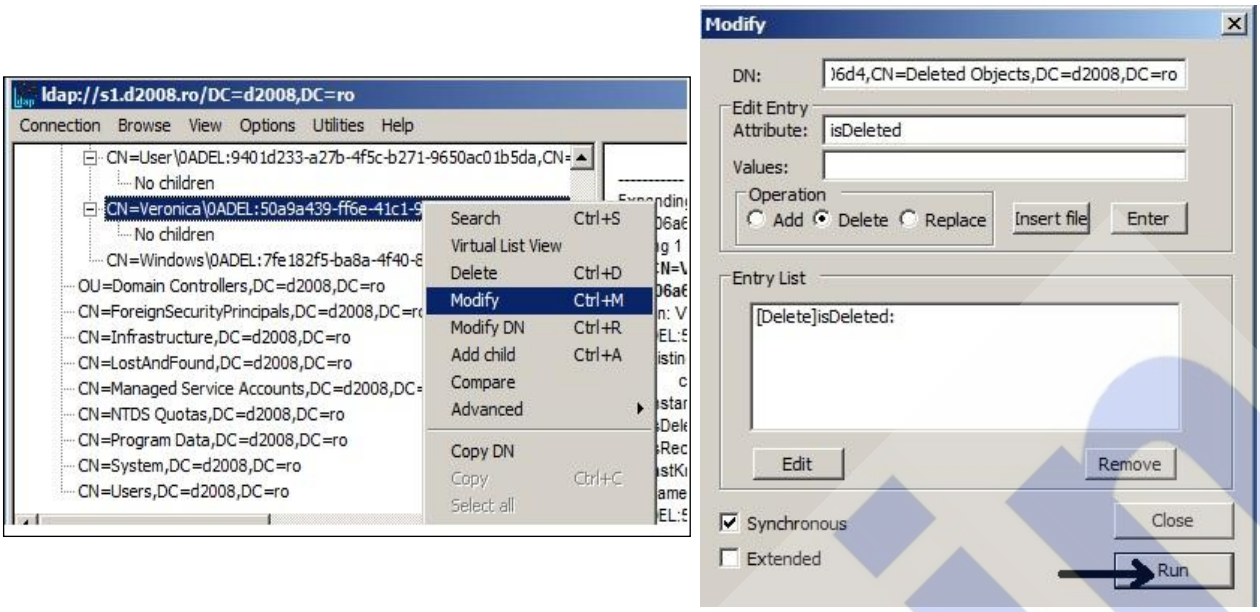
Aici există obiectele șterse, de tip *tombstone* și putem să vizualizăm atributele acestora.



Trebuie efectuate următoarele operații pentru atributele specificate:
isDeleted trebuie șters
distinguishedName va fi setat la valoarea dorită, conform cu locația unde va fi restaurat obiectul, întrucât acesta nu va mai exista în *Deleted Objects*.

Modificarea se realizează folosind opțiunea **Modify**.

Atributele care nu au putut fi restaurate (întrucât fuseseră șterse atunci când obiectul a devenit *tombstoned*) trebuie reeditate manual.



Gestionarea evenimentelor

Event Viewer este aplicația care permite vizualizarea, gestionarea şi monitorizarea evenimentelor înregistrate în jurnalele de evenimente (*event logs*).

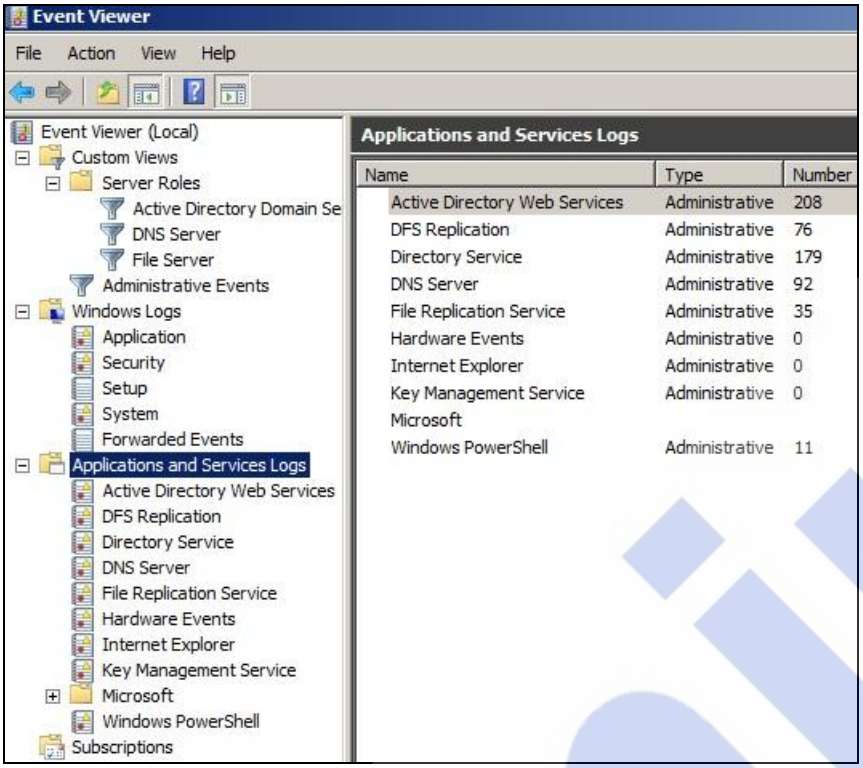
În *Windows 2008* această aplicație este rescrisă complet, având o interfaţă de utilizator nouă, care permite filtrarea, sortarea și controlarea mai ușoară a evenimentelor care sunt înregistrate.

Event Viewer oferă, de asemenea, multe fişiere noi de tip jurnal (log).

În afară de logurile standard *Application, Security* și *System*, există câte un log pentru fiecare rol instalat în sistem.

Event Viewer oferă, de asemenea, două noi **Windows Logs**:
•**Setup**: care înregistrează evenimente referitoare la instalarea fiecarei noi aplicații
•**Forwarded Events**: care înregistrează evenimente care sunt transmise de către alte computere.

Există, de asemenea, o nouă categorie de fişiere log, numită **Application and Services Logs**, care include jurnale separate pentre programele care rulează pe calculator şi jurnale mai detaliate relative la anumite servicii *Windows*.



Evenimente relaționate cu *Active Directory* există și în următoarele *log-uri* din **Application and Service Logs** :

Distributed File System (DFS) Replication
Directory Service
Domain Name System (DNS) Server
Microsoft\Windows\Group Policy\Operational

Configurare AD DS auditing

Audit log înregistrează o intrare ori de câte ori utilizatorii efectuează anumite acţiuni specificate. Se pot înregistra atât încercările reuşite cât şi cele nereuşite pentre diverse acțiuni. Înainte de a pune în aplicare politica de audit, trebuie decis care categorii de evenimente să fie înregistrate.

O setare de audit poate avea următoarele stări:

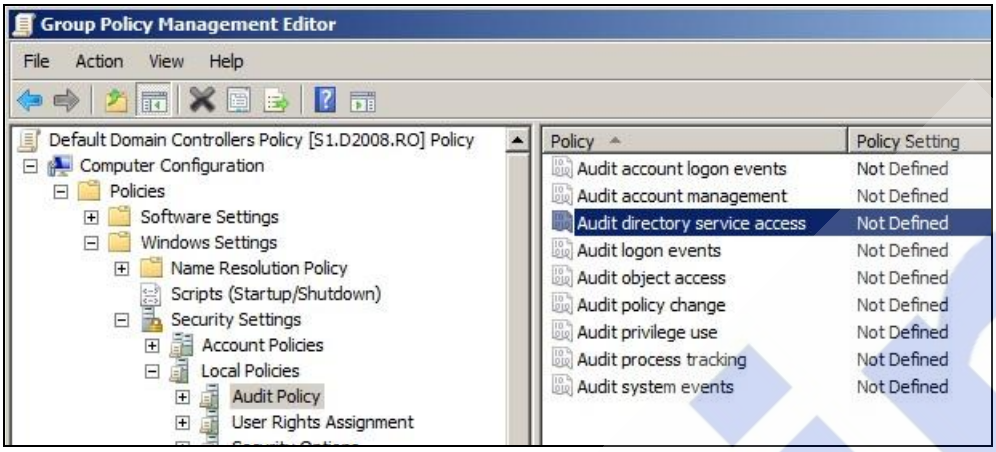
Sucess – se înregistrează eveniment atunci când operația respectivă s-a efectuat cu succes.

Failure - se înregistrează eveniment atunci când operația respectivă s-a efectuat cu eșec.

No audit - nu se înregistrează eveniment atunci când operația respectivă s-a efectuat, indiferent de rezultatul operației.

Există o setare globală de audit, numită **Audit directory service access**, care, atunci când este setată, definește setări pentru toate subcategoriile existente. Locația acestuia în Group Policy este:

Computer Configuration \ Windows Settings \ Security Settings \ Local Policies \ Audit Policy \ Audit Directory Service Access



În versiunile anterioare de *Windows*, această politică de audit era singura existentă. În *Windows Server 2008*, această politică se împarte în patru subcategorii:

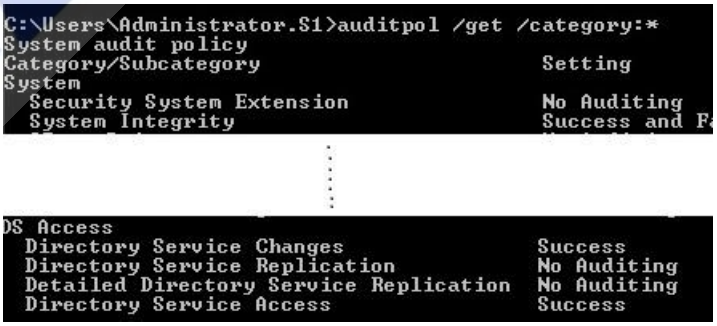
- **Directory service access** (activă implicit)
- **Directory service changes** (inactivă implicit)
- **Directory service replication** (inactivă implicit)
- **Detailed Directory service replication** (inactivă implicit)

Dacă nu specificăm nicio valoare pentru setarea globala de audit, **Audit directory service access**, atunci implicit va fi activă subcategoria **Directory service access**.

Dacă specificăm o valoare pentru setarea globala de audit, **Audit directory service access**, atunci toate cele patru categorii specificate mai sus vor avea valoarea respectivă.

Cele patru categorii nu se pot seta din interfața grafică, ci numai cu comanda **auditpol.exe**. Cu aceasta comandă putem vizualiza sau modifica setările legate de **Audit Policy**.

Comanda pentru vizualizare:
auditpol.exe /get /category:*



Subcategoria **Directory Service Access** oferă informaţii despre toate evenimentele care au loc în director şi este activată în mod implicit.

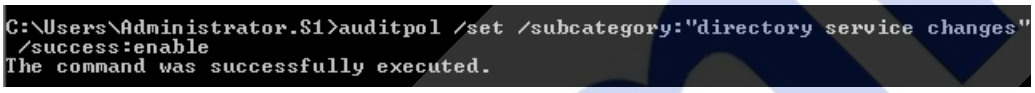
Subcategoriile sunt folosite pentru a afișa informaţii mai detaliate. Subcategoria **Directory Services Changes** permite înregistrarea valorilor vechi și a celor noi, atunci când se fac modificări la obiecte şi atributele lor.

De exemplu când redenumim un obiect, se va înregistra un eveniment în care suntem informați despre valoarea veche și cea noua a acestuia .

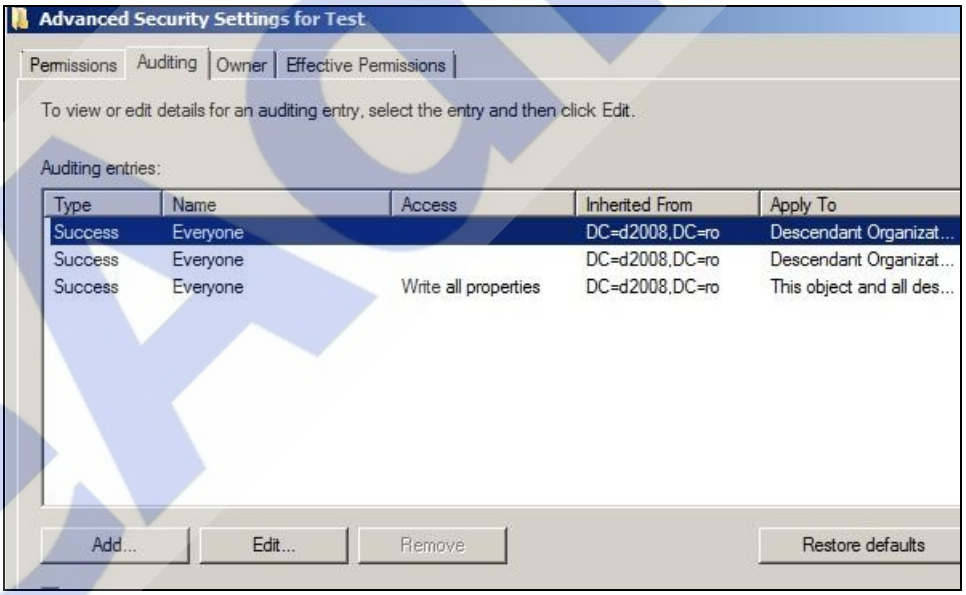
Subcategoriile **Directory Service Replication** și **Detailed Directory Service Replication** furnizează informații despre replicare.

Modificarea valorii unei subcategorii se realizează cu comanda **auditpol**, de exemplu dacă dorim setarea pe Succes pentru subcategoria **Directory Service Changes** avem comanda:

```
auditpol /set /subcategory:"Directory Service Changes" /success:enable
```



În afară de aceste setări, trebuie specificate ce obiecte vor fi urmărite, iar pentru fiecare obiect în parte ce activitați și pentru ce utilizatori. Acest lucru se realizează folosind **Active Directory Users and Computers**, în proprietățile obiectului respectiv, tab-ul **Security** / **Advanced** /**Auditing/ Add**



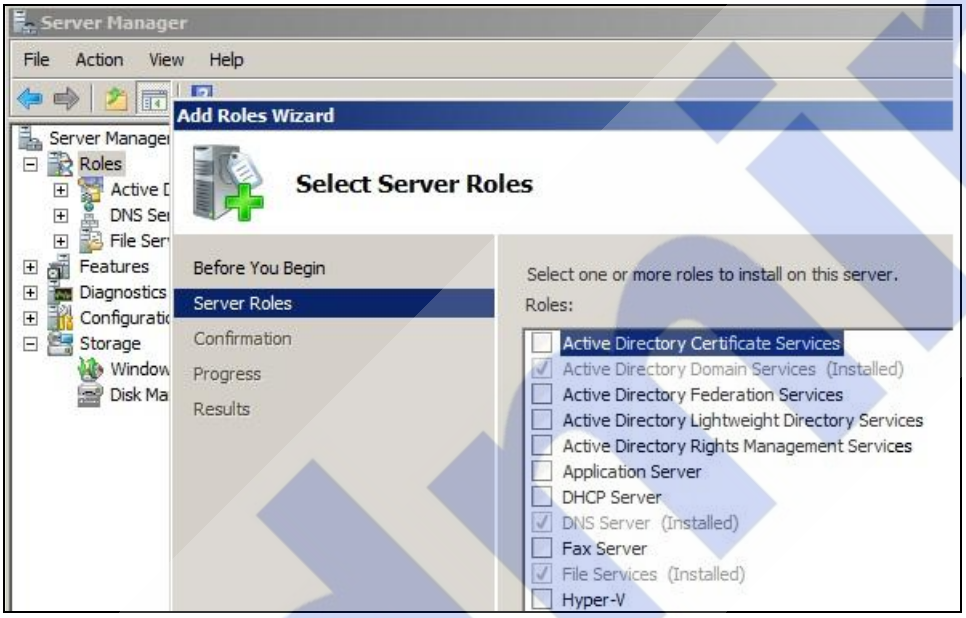
Vizualizarea evenimentelor înregistrate se realizează folosind **Event Viewer**, **Windows Log/Security**.

Noi roluri introduse în Windows 2008

În *Windows 2008* există urmatoarele roluri relaționate cu *Active Directory*:

Active Directory Lightweight Directory Services (AD LDS)
Active Directory Certificate Services (AD CS)
Active Directory Rights Management Services (AD RMS)
Active Directory Federation Services (AD FS)

Instalarea acestora se realizează folosind **Server Manager**.



Active Directory Lightweight Directory Services (AD LDS)

Active Directory Lightweight Directory Services (AD LDS) este un rol de tip *Active Directory* care oferă servicii de director conforme protocolului **Lightweight Directory Access Protocol (LDAP).**

Acesta poate furniza servicii de de autentificare şi de director pentru aplicații personalizate, *Microsoft* sau *third-party*.

LDAP este un protocol standardizat, de tip client/server, bazat pe TCP/IP, care definește modalităţi consistente pentru a numi şi stoca obiecte în director. LDAP prevede, de asemenea, metode pentru accesarea, căutarea şi modificarea informaţiilor stocate în director.

AD LDS este utilizat pentru aplicaţii care nu pot sau nu ar trebui să folosească AD DS sau pentru a rezolva scenarii , în cazul în care accesul la AD DS nu este recomandat datorită problemelor de securitate.

AD LDS poate stoca informații despre utilizatori sau setări de configurare pentru aplicații.

Active Directory Certificate Services (AD CS)

Certificatele digitale sunt utilizate pentru a cripta informațiile sau pentru a autentifica utilizatorii şi calculatoarele. **PKI (Public Key Infrastructure)** permite unei organizaţii să distribuie certificate digitale pentru utilizatori şi computere.

Active Directory Certificate Services (AD CS) este implementarea *Microsoft* a PKI. AD CS oferă un PKI complet funcţional pentru o reţea *Windows*, putându-se extinde aceste servicii și la dispozitive *non-Windows*.

AD CS oferă toate serviciile de bază PKI, cum ar fi instrumente de management şi de revocare.

Un PKI constă din mai multe obiecte, aplicaţii şi servicii corelate:

Certification authorities (CA) - generează și gestionează certificate pentru utilizatori, computere şi servicii. Fiecare certificat emis de CA este semnat cu certificat-ul digital al acelui CA.

Certificate revocation lists - O listă de certificate care au fost revocate sau eliminate din CA înainte de expirare.

Certificate and CA management tools – instrumente pentru gestionare certficate.

Certificatele digitale - sunt acreditările electronice asociate cu o cheie publică şi o cheie privată, utilizate pentru autentificarea utilizatorilor.

Integrarea AD DS și AD CS

Integrarea AD DS și AD CS se realizează prin următoarele:

Generare automată de certificate - obiectele de tip Computer şi User pot avea certificate generate de AD CS în mod automat dacă utilizatorii şi computerele au permisiuni corespunzătoare şi politica de certificat este configurată pentru a permite *auto-enrollment*.

Stocare certificate în AD DS

Active Directory Rights Management Services (AD RMS)

Windows Rights Management Services este un serviciu folosit pentru restricţionarea accesului la documente cu conţinut protejat, accesul fiind permis numai pentru utilizatorii autorizaţi.

Acesta foloseşte o arhitectură de tip *client-server*, utilizând *Windows Server 2008* pentru a găzdui **Active Directory Rights Management Server**, care emite licenţe de tip RMS. Acestea definesc nivelul de acces disponibil pentru

un fișier, care nu se poate deschide fără o licență de utilizare. Documentele protejate RMS pot fi create utilizând aplicaţii *RMS-enabled*.

Serverul AD RMS criptează conţinutul şi aplică conţinutului permisiunile alocate de creator, astfel încat numai utilizatorii autorizați pot efectua operațiile care le-au fost permise.

Active Directory Federation Services (AD FS)

Active Directory Federation Services (AD FS) permite extinderea autentificării de tip AD DS, prin crearea de relații de trust de tip *federated* între două organizaţii, astfel încât utilizatorii autentificați într-o organizaţie vor putea accesa aplicaţii din alte organizaţii (de exemplu de tip Web).

Ce ați învățat în acest modul

- ✓ Cum se instalează *Active Directory*
- ✓ Upgradarea unui domain controller *Windows 2003* la *Windows 2008/R2*
- ✓ Instalarea unui *Read Only Domain Controller(RODC)*
- ✓ Îmbunatățiri relative la Group Policy aduse de *Windwos 2008*
- ✓ Realizarea salvării/restaurării bazei de date *Active Directory*
- ✓ Reanimarea obiectelor *tombstoned*
- ✓ Configurare AD DS auditing
- ✓ Descriere roluri noi relaționate cu *Active Directory*, introduse în *Windows 2008*

eAdmin