4. Administrarea domeniilor

Serviciul director *Active Directory*

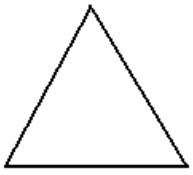
Creşterea numărului de calculatoare existente la un moment dat într-o rețea a impus necesitatea folosirii unui serviciu centralizat care să asigure efectuarea diverselor operații de rețea, modelul *workgroup* fiind greu de implementat şi gestionat în astfel de situații.

Un serviciu director (*directory service*) cuprinde o colecție de informații despre obiecte care sunt în legătură unele cu altele într-o anumită privință. Serviciul director furnizează un mod consistent de a identifica, localiza, organiza, securiza şi simplifica accesul la resursele unei rețele de calculatoare.

Active directory este tehnologia creată de *Microsoft* pentru serviciul director *Windows Server 2003*. *Active Directory* păstrează şi pune la dispoziție informații despre resursele unei rețele, organizate în obiecte. Fiecare obiect are un set de atribute asociate, informații care identifică şi descriu obiectul. Baza structurii logice în *Active Directory* este domeniul. Domeniul este în general o colecție de obiecte, unele dintre ele create de administratorul domeniului. Folosind o singură bază de date, *Active Directory* oferă posibilitatea administrării centralizate a tuturor resurselor unei rețele. Structura *Active Directory* este reprezentată printr-o ierarhie de obiecte, în care fiecare obiect reprezintă o singură entitate: un computer, un utilizator, un grup, o imprimantă. Obiectele au proprietăți, numite şi atribute. Unele obiecte sunt containere, deci conțin alte obiecte, inclusiv alte containere. De aici structura ierarhică *Active Directory*. La nivelul cel mai înalt al ierarhiei *Active Directory* se află *forest* (pădure). Un *forest* se compune din arbori (*tree*). La rândul lui un arbore este compus din domenii.

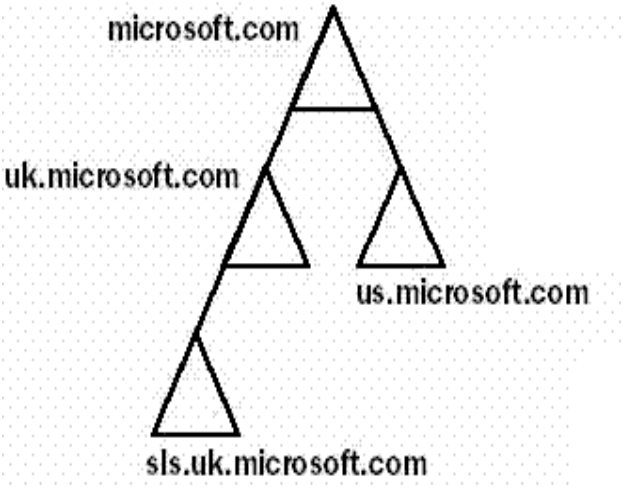
Domeniul

Conform terminologiei *Microsoft*, domeniul este reprezentat dintr-un grup de calculatoare care fac parte dintr-o rețea şi care folosesc în comun aceeaşi bază de date în care sunt reprezentate resursele rețelei. Domeniul este administrat ca entitate distinctă, cu reguli şi proceduri comune pentru toate calculatoarele care îl compun. Domeniile sunt recunoscute prin nume. Calculatoarele membre ale domeniului respectă politica de securitate a domeniului. În plus, domeniul oferă şi soluția administrării centralizate a tuturor resurselor rețelei, indiferent unde ar fi ele distribuite: administrarea bazei de date a domeniului este în fond soluția pentru administrarea tuturor resurselor reprezentate prin obiecte înscrise în această bază de date. O singură operație de *logon* în domeniu (deschidere de sesiune) este suficientă pentru ca un utilizator să fie recunoscut în domeniu şi să aibă acces la resursele domeniului, în limita permisiunilor şi a privilegiilor de care dispune.



Reprezentarea grafică a domeniului este triunghiul care sugerează frontiera de administrare, frontiera de securitate şi aşezarea ierarhică a componentelor sale. Domeniul este construit în jurul unui controler de domeniu (*domain controller*). Într-un domeniu trebuie să existe cel puțin un controler de domeniu. El deține toate informațiile despre domeniu, despre resursele rețelei şi este serverul folosit pentru autentificarea în domeniu (*logon* în domeniu). Crearea unui domeniu se obține prin crearea controlerului de domeniu. Instalarea serviciului *Active Directory* pe un server îl transformă în controler de domeniu. *Active Directory* se poate instala pe sistemele de operare *Windows Server 2003*, mai puțin ediția *Web Edition.* Mai multe domenii pot fi organizate ierarhic şi pot constitui structuri arborescente, numite *tree*.

Un arbore (*tree*) este o grupare de domenii din acelaşi spațiu de nume, deci o convenție relativă la modul în care sunt denumite acestea. Între domenii există relații de tip părinte - copil: un subdomeniu este fiul domeniului părinte.

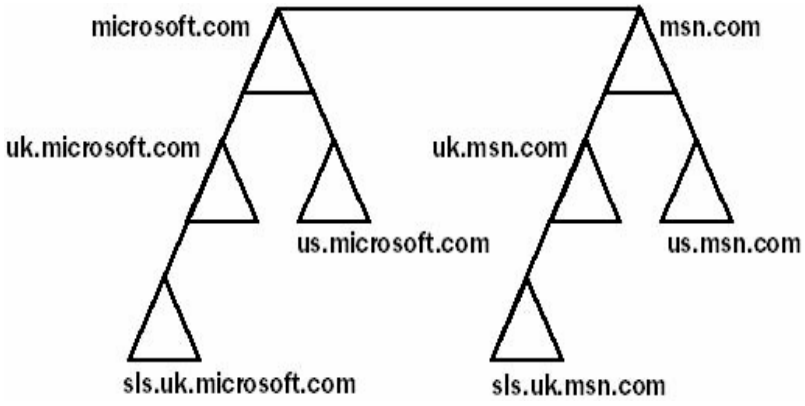


Fiecare domeniu are un nume propriu.

În figura alăturată este reprezentată o structură de domenii, în care avem un singur *tree* (arbore). Numele domeniului rădăcină este *microsoft.com*, nume în formatul *Domain Name System* (DNS).

Numele subdomeniului se formează prin concatenarea unui sufix la numele părintelui, ca de exemplu *uk.microsoft.com*, care este un subdomeniu al domeniului *microsoft.com.* Liniile care unesc domeniile definesc relațiile dintre ele: în acest caz sunt relații de genul „părinte-copil” (*parent-child*) sau domeniu-subdomeniu.

O pădure (*forest*) este o grupare de arbori (*tree*) care au spații de nume distincte.



În această figură este reprezentat un *forest* cu cu două arborescențe. Fiecare dintre ele are un spațiu de nume independent.

Numele *forest*-ului este dat de numele primului domeniu creat în *forest* numit şi domeniul rădăcină pentru forest (*forest root domain*). În cazul nostru este *microsoft.com.*

În situația în care structura unui *Active Directory* conține un singur domeniu atunci el este şi domeniul rădăcină. Cu alte cuvinte există şi în acest caz particular un arbore şi un *forest*.

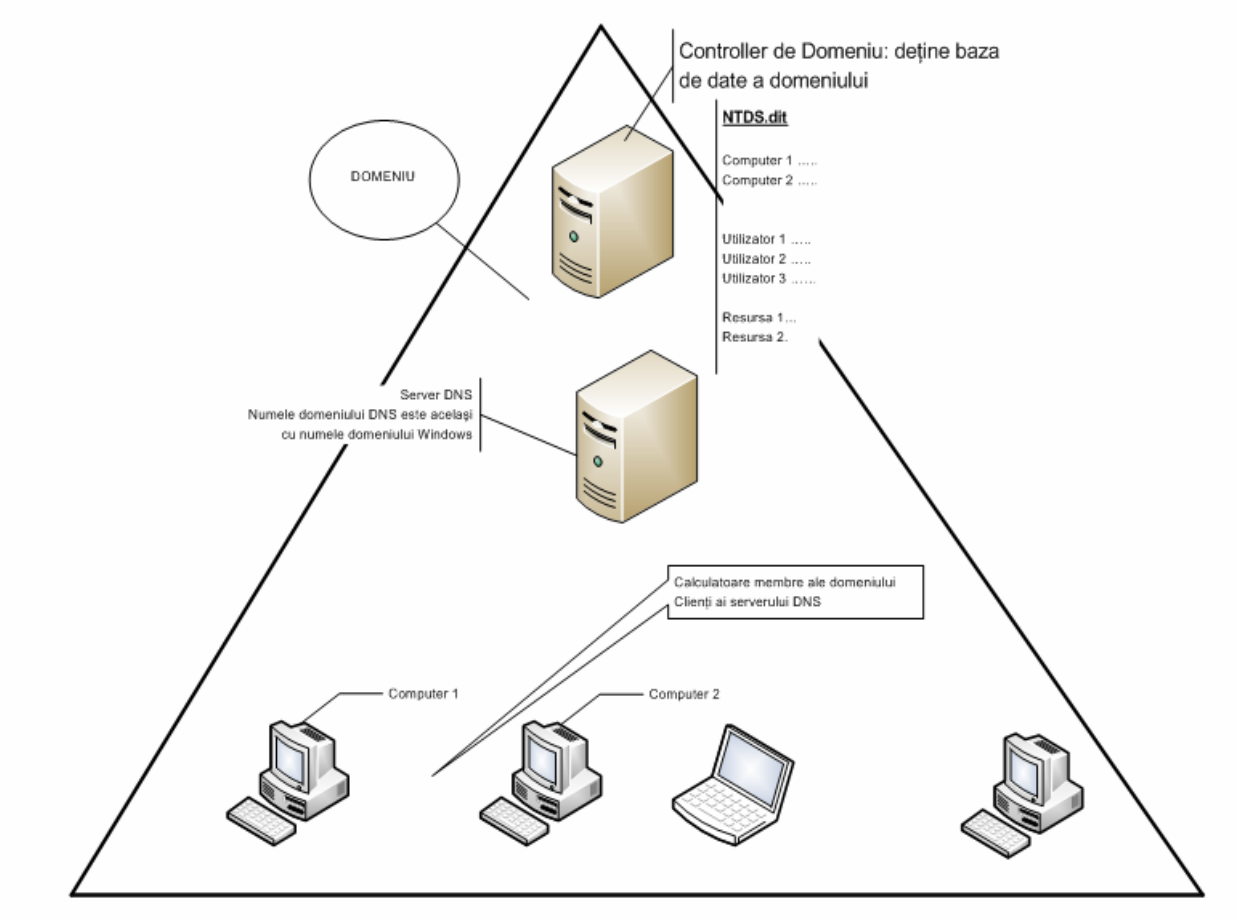
Între domenii există relații de încredere (*trust*). Este cunoscut faptul că un utilizator autentificat în domeniu, deci cunoscut la nivelul acelui domeniu, are acces la resursele domeniului, în limita permisiunilor. Relația de încredere (*trust*) între domenii se referă la faptul că un utilizator autentificat într-un domeniu poate folosi o resursă ce aparține altui domeniu; fiind un utilizator cunoscut, „domeniul" are suficientă încredere în el şi îi pune la dispoziție resursele, presupunând că utilizatorul are permisiunile necesare.

Relațiile părinte-copil sunt relații de încredere (*trust*) bidirecționale şi tranzitive. Între domeniile rădăcină ale arborilor care formează pădurea există o relație de încredere (*trust*) bidirecțională.

Caracteristicile domeniilor *Windows Server 2003* sunt următoarele:

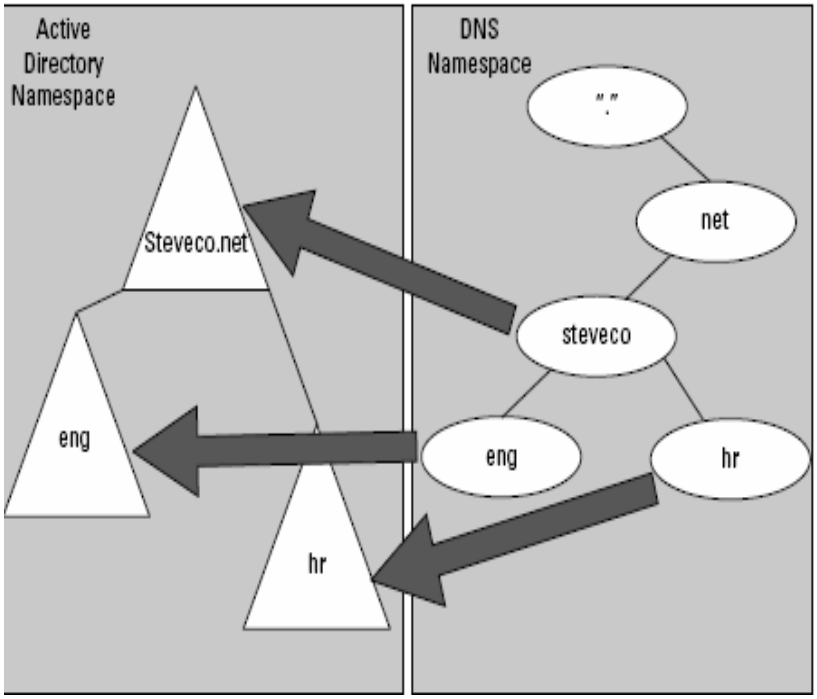
- Există o singură bază de date care păstrează toate conturile utilizatorilor din domeniu. Baza de date face parte din serviciul *Active Directory*. Pentru a avea acces la oricare resursă din domeniu, utilizatorul are nevoie de un singur cont de utilizator în domeniu. Este suficientă o singură operație de autentificare în domeniu pentru ca utilizatorul să fie recunoscut de fiecare resursă a domeniului.
- Administrarea resurselor şi autentificarea utilizatorilor sunt centralizate.
- Domeniile sunt scalabile: pot conține un număr mic de calculatoare, dar pot găzdui la fel de bine mai multe mii de calculatoare.
- Un domeniu este gestionat prin cel puțin un *domain controller*.
- Un controler de domeniu (*domain controller*) controlează numai un singur domeniu.
- Într-un domeniu pot să funcționeze mai multe controlere de domeniu.
- Toate exemplarele bazei de date a domeniului, aflate pe controlerele acelui domeniu, sunt modificabile. Modificările realizate pe un exemplar sunt transmise către celelalte printr-un proces numit replicare. Întrucât sunt acceptate modificări pe orice *domain controller*, replicarea este de tipul *multi-master*. În afară de transmiterea modificărilor, cu această ocazie se realizează şi gestionarea eventualelor conflicte care ar putea să apară în urma efectuării simultane a unor modificări. Instalarea mai multor controlere de domeniu pentru acelaşi domeniu se justifică prin asigurarea toleranței la erori sau pentru echilibrarea cererilor provenite de la clienți.

- Un *domain controller* conține integral baza de date a domeniului. Nu există posibilitatea menținerii unor exemplare parțiale ale bazei de date asociate cu domeniul în cauză.



La proiectarea *Active Directory* trebuie avut în vedere, ca principiu de design, minimizarea numărului de domenii. Fiind arii de securitate distincte, un număr cât mai mic de domenii, preferabil unul singur, permite gestionarea mai uşoară a domeniului. Unul din motivele pentru care am dori mai multe controlere de domeniu este legat de echilibrarea cererilor de autentificare a utilizatorilor. În situația în care, pentru acel domeniu funcționează două controlere în aceeaşi rețea, e de aşteptat ca fiecare dintre ele să fie egal încărcate (*load balance*) cu cereri de autentificare. Redundanța informațiilor este alt motiv pentru care funcționează mai multe controlere în acelaşi domeniu. În cazul în care unul dintre ele nu mai funcționează toate rolurile şi funcțiile îi vor putea fi preluate de cele rămase în funcțiune, iar utilizatorii nu vor avea de suferit.

Active Directory foloseşte serviciul *Domain Name System* (DNS): pentru fiecare domeniu *Active Directory* trebuie să existe un domeniu DNS cu acelaşi nume.

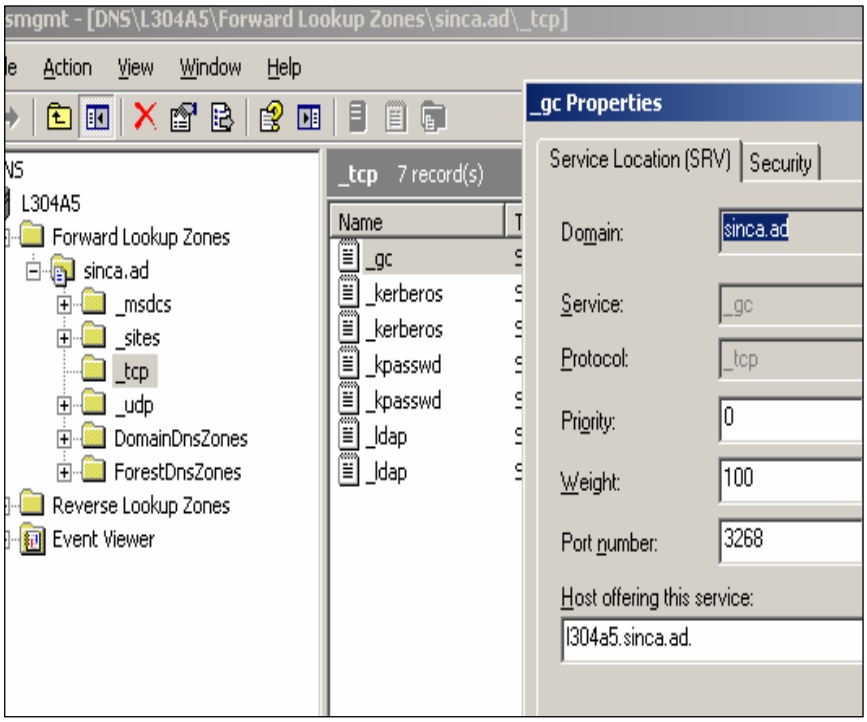


În figura alăturată este prezentată corespondența dintre domeniile DNS şi cele de tip *Active Directory.*

Domeniul DNS poate să existe înainte de instalarea lui *Active Directory* sau poate fi instalat pe *domain controller* în timpul procesului de instalare a serviciului *Active Directory.*

Cerința minimală a domeniului DNS este aceea de a permite înregistrări de tip SRV. Este recomandabil ca domeniul DNS să asigure şi actualizarea dinamică a înregistrărilor (*dynamic update*).

Înregistrările DNS de tip SRV sunt folosite pentru identificarea serviciilor. De



exemplu, în figura alăturată este prezentat serviciul de catalog global care rulează pe portul 3268. Înregistrarea SRV (*service*) indică numele *host*-ului care oferă acest serviciu.

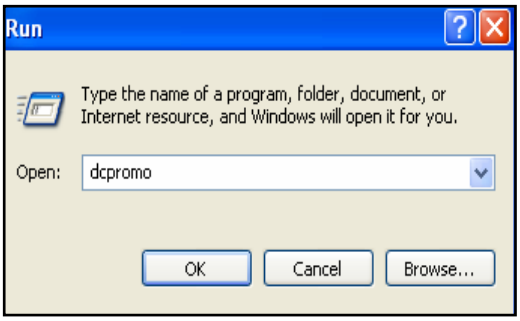
Utilizatorii care folosesc calculatoarele membre ale domeniului pot deschide sesiune local – folosind un cont utilizator local calculatorului – sau în domeniu. In vederea deschiderii de sesiune în domeniu, clientul *Active Directory* care este şi client DNS, interoghează mai întâi serverul DNS în căutarea unui controler de domeniu. Controlerul de domeniu este cel căruia i se va adresa şi va rezolva cererea de autentificare.

Instalarea *Active Directory*

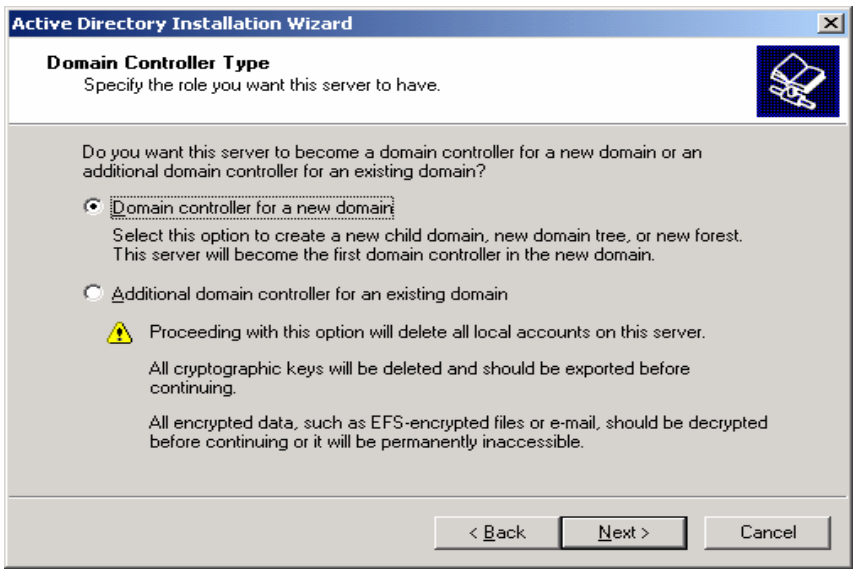
Serviciul director *Active Directory* (*Active Directory Service)* poate fi instalat pe calculatoare unde funcționează sisteme de operare *Microsoft Windows Server 2003*, ediții *Standard, Enterprise* şi *Data Center*. Serviciul *Active Directory* are nevoie de o partiție NTFS cu minim 1 GB de spațiu liber, pentru început. În partiția NTFS se va afla baza de date a domeniului care va creşte pe măsură ce vor fi adăugate obiecte în domeniu. În urma instalării serviciului *Active Directory* serverul devine controler de domeniu. Serverul care va deveni controler de domeniu trebuie să aibă de la început o adresa 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.

Promovarea unui server la rolul de controler de domeniu

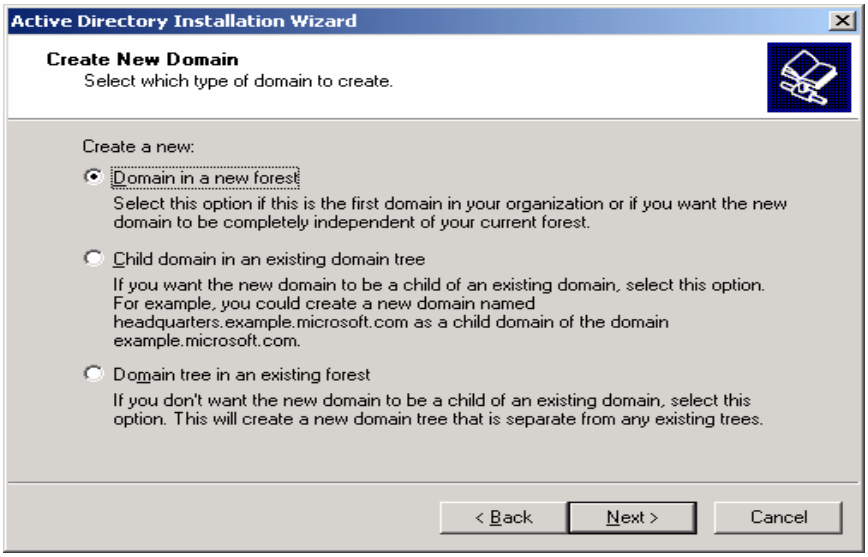
Comanda de promovare este ***dcpromo***. Aceeaşi comandă poate fi folosită şi pentru retrogradarea controlerului de domeniu: dacă serverul este deja controler de domeniu comanda *dcpromo* dezinstalează serviciul *Active Directory*.



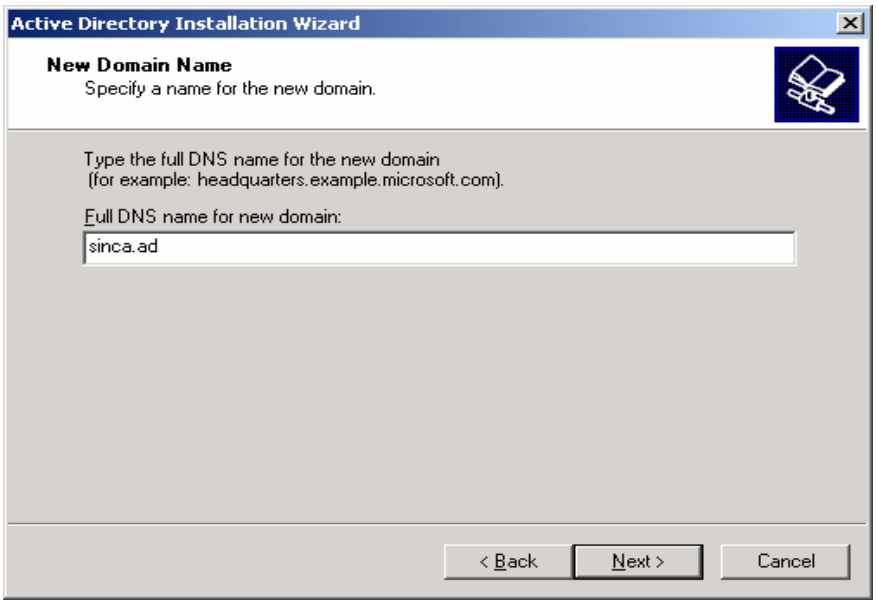
1. **Start -> Run** şi introducem ***dcpromo*** în caseta de dialog Run.
2. Vrăjitorul (*Wizard*) ***Active Directory Installation Wizard*** a fost lansat în execuție şi continuăm (*Next*).
3. În caseta de dialog ***Domain Controller Type***, va fi ales tipul noului controler de domeniu: va fi el un controler pentru un domeniu nou (încă necreat) sau un controler de domeniu suplimentar într-un domeniu existent, creat cândva înainte. ***Domain Controller for a new domain*** este opțiunea pentru crearea unui domeniu nou, implicit a unui controler de domeniu într-un nou domeniu.



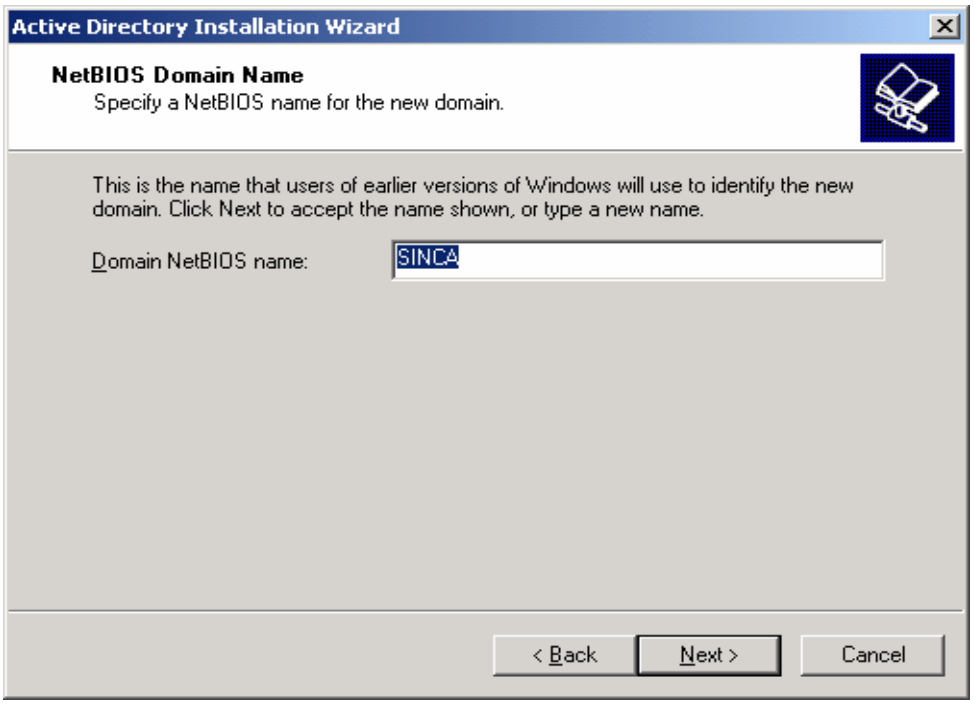
4. Noul domeniu trebuie plasat într-o ierarhie: este începutul unei ierarhii noi (adică un *forest* nou), sau doar un arbore nou într-un *forest* existent, sau este un subdomeniu (domeniu copil – *child*) al unui domeniu existent. Întrucât acesta va fi primul domeniu *Active Directory*, selectăm opțiunea ***Create a New Domain in a new forest*** (crearea unui domeniu nou într-un *forest* nou).



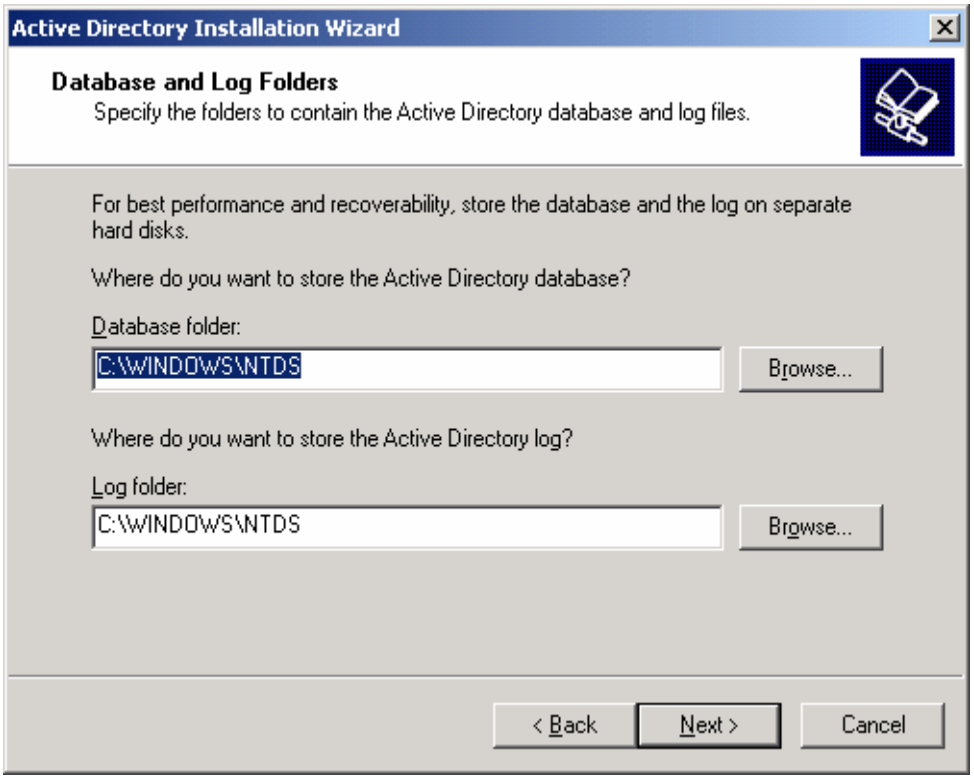
5. ***New Domain Name*** (numele noului domeniu) este locul unde va fi specificat numele în format DNS al noului domeniu. De aici în acolo, domeniul va purta două nume: numele în format DNS şi cel în format NetBIOS.



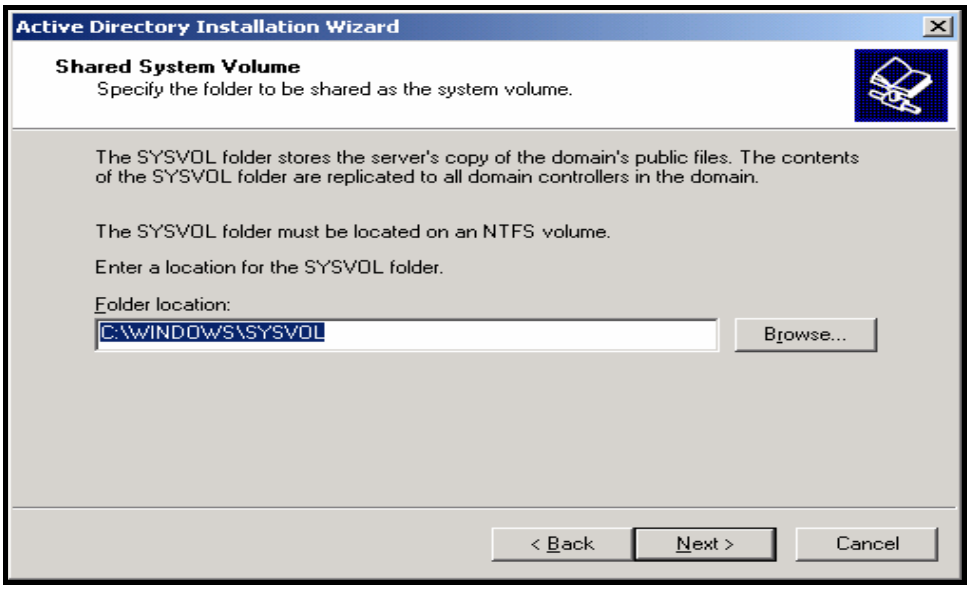
6. Numele NetBIOS ale domeniilor sunt utilizate pentru compatibilitatea cu alte sisteme de operare. Implicit, numele NetBIOS al domeniului va fi prima parte a numelui în specificator DNS (până la primul punct).



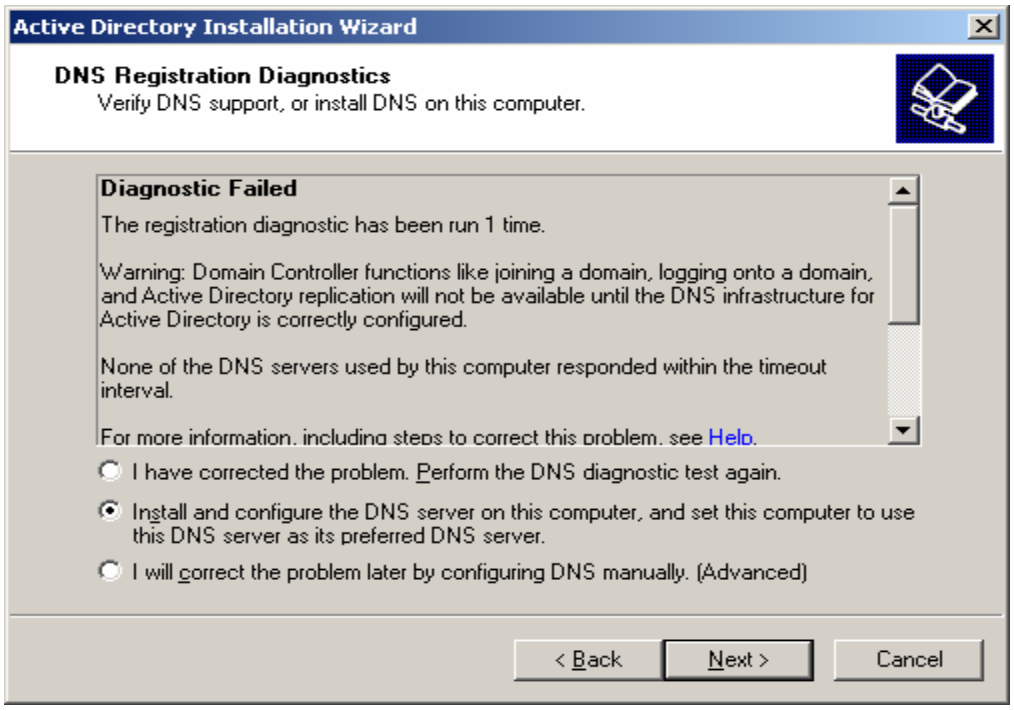
7. În caseta de dialog ***Database and Log Folders*** (baza de date şi fişiere *log* - jurnal) va fi specificat locul unde vor fi create baza de date a serviciului şi fişierele jurnal. În mod implicit, este vorba despre calea C:\Windows**NTDS.**



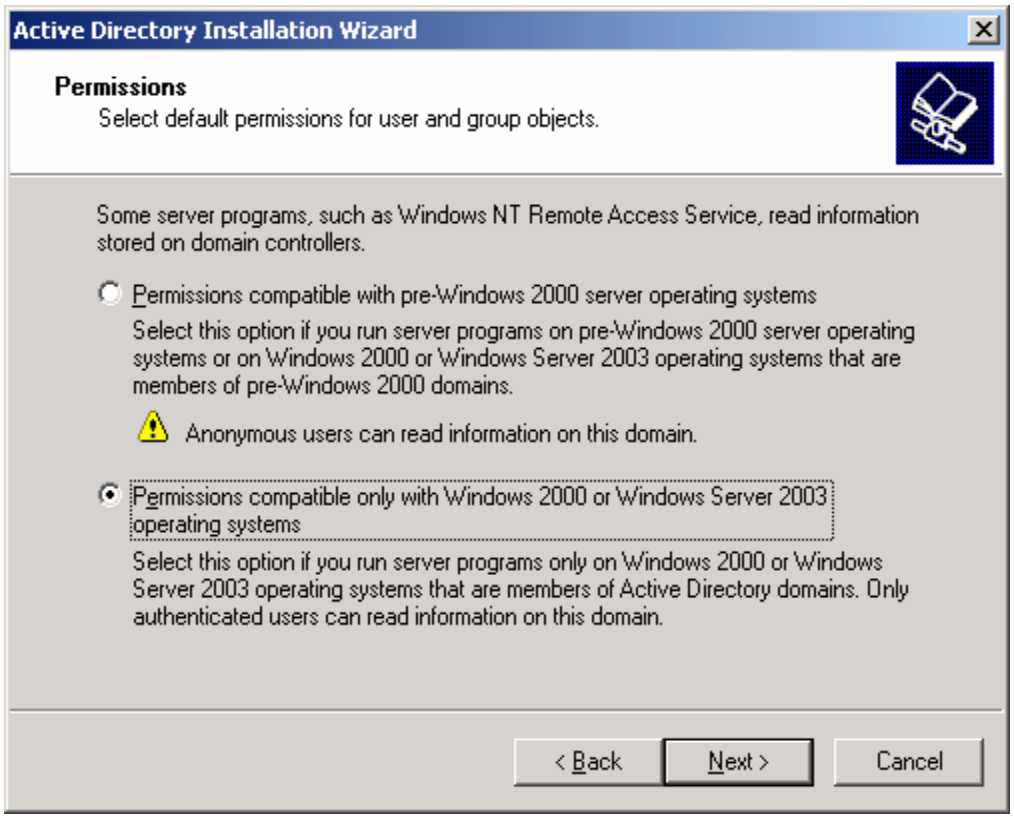
8. Volumul S***hared System Volume*** (volum sistem partajat) păstrează politicile de securitate *Active Directory*. O replică a conținutului va fi transmisă către toate celelalte controlere de domeniu. Acest folder se va afla într-o partiție NTFS şi se numeşte **SYSVOL.** Calea implicită este C:\Windows.



9. Serviciul *Active Directory* are nevoie de suportul DNS. Controlerul de domeniu trebuie să fie client al unui server DNS, unde există un domeniu DNS cu acelaşi nume ca şi numele domeniului *Active Directory*. În cazul în care nu există deja un server DNS care să îndeplinească aceste condiții, promovarea serverului la rolul de controler de domeniu poate conține şi secvența de instalare şi configurare a serviciului *Domain Name System* (DNS) – ***Install and configure the DNS Server.***



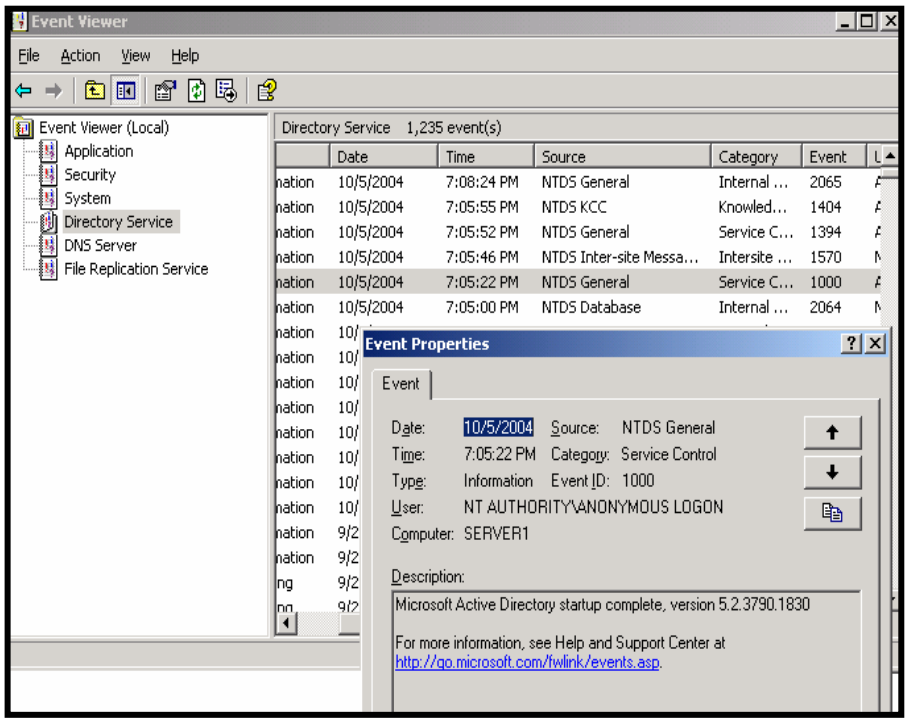
10. Caseta de dialog ***Permissions*** **(permisiuni):** ca parte a procesului de promovare, sistemul de operare are nevoie de stabilirea permisiunilor pentru utilizatori şi grupuri.



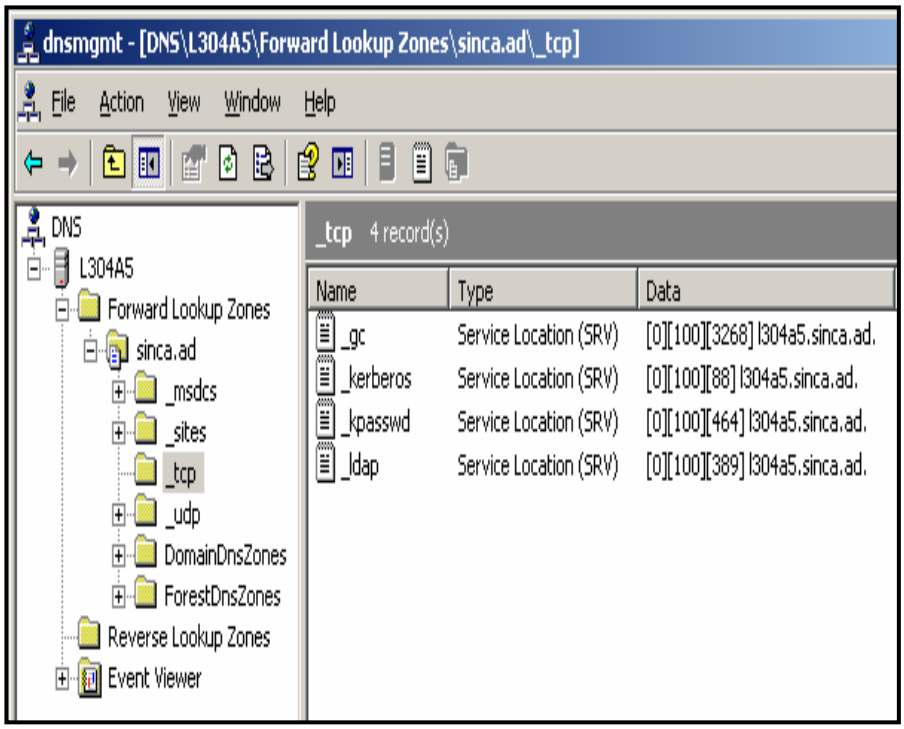
11. Urmează stabilirea parolei administratorului pentru modul de lucru ***Directory Services Restore Mode*** **(**restaurarea serviciilor director**)**. Este situația când administratorul va încerca să restaureze serviciul *Active Diretory* folosind pentru autentificare un cont special. Pentru restaurare administratorul va folosi o copie de siguranță (*backup*) în timp de serviciul Active Directory nu va fi pornit.

12. În baza opțiunilor de instalare pe care le-am selectat, ***Active Directory Installation Wizard*** **(**vrăjitorul pentru instalarea *Active Directory***)** afişează un sumar al alegerilor făcute şi construieşte apoi baza de date a serviciului.

Verificarea instalării *Active Directory*



I. Cea mai bună cale de verificare a operațiile legate de instalarea *Active Directory* este consultarea jurnalului *Directory Service* cu ajutorul utilitarului ***Event Viewer***.



II. Consola serviciului DNS arată înregistrările specifice serviciului *Active Directory*, respectiv înregistrările de tip SRV.

III. În grupul de programe *Administrative Tools* sunt adăugate o serie de programe pentru gestionarea *Active Directory*:

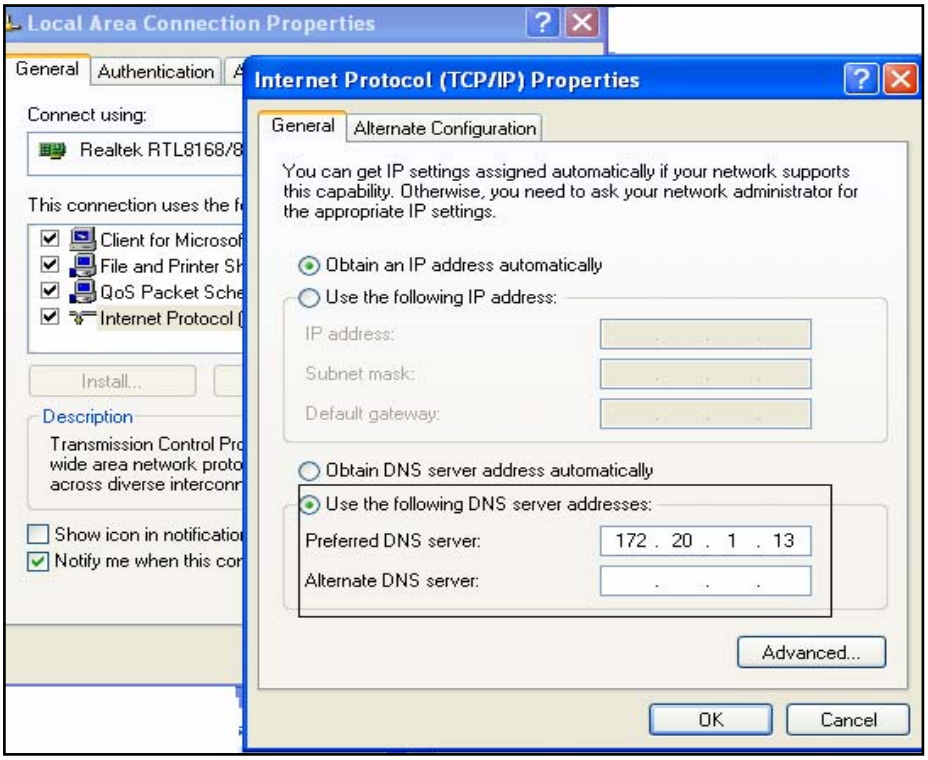
- ***Active Directory Users and Computers*:** permite crearea conturilor de utilizator, a grupurilor, conturilor de calculator, a unităților organizaționale, a politicilor de securitate aferente domeniului şi unităților organizaționale. Este utilitarul folosit pentru administrarea tuturor obiectelor *Active Directory*.

- ***Active Directory Domains and Trusts*:** pentru vizualizarea şi modificarea relațiilor de încredere dintre domeniile *Active Directory*.

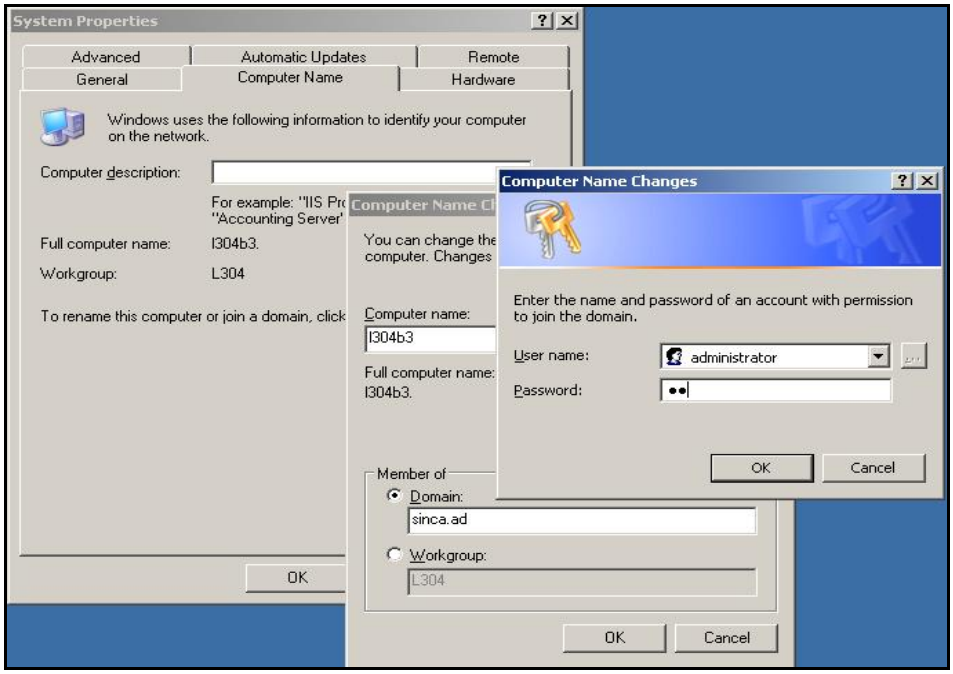
- ***Active Directory Sites and Services*:** pentru crearea şi coordonarea site-urilor şi a serviciilor *Active Directory*.

Includerea unui computer în domeniu

Apartenența unui calculator (stație 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 obține prin *System Properties*.

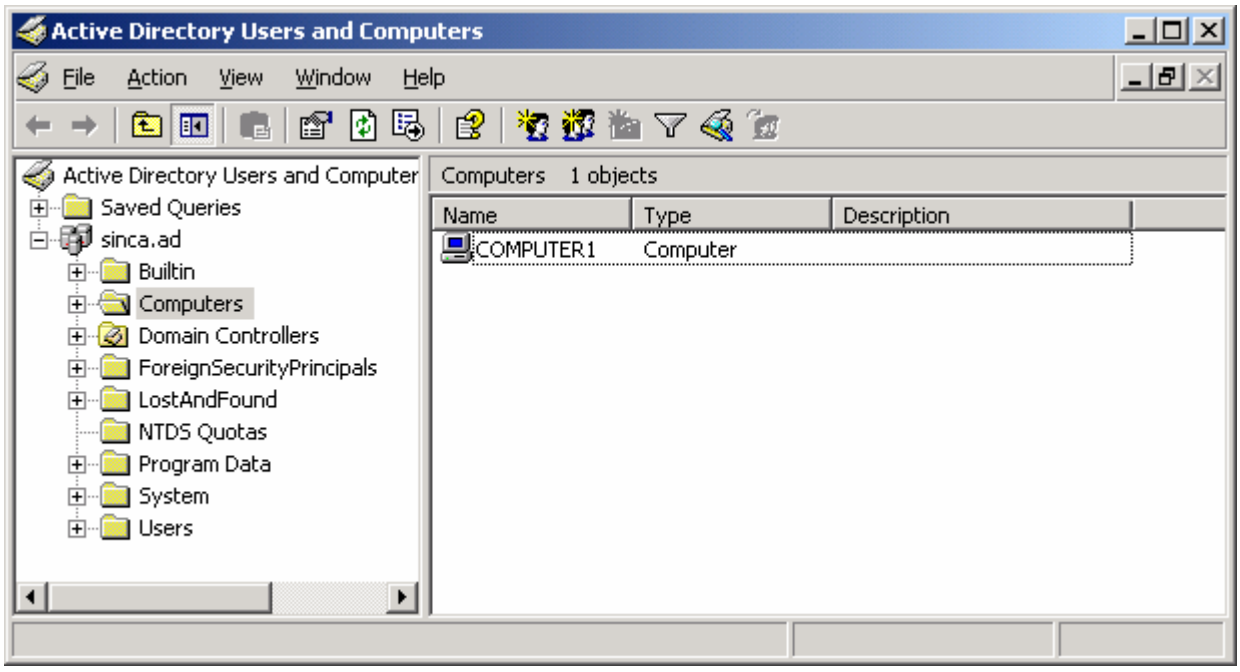


De la calculatoarele incluse în domeniu, utilizatorii pot deschide sesiune folosind fie un cont din domeniu, fie un cont din baza de date locală SAM. Există posibilitatea alegerii uneia dintre cele două opțiuni în fereastra de *logon*:

Administrarea unui domeniu se poate face, în calitate de administrator al domeniului, de la orice calculator membru al domeniului. Instrumentele de administrare sunt utilitare care pot fi instalate de pe *kit*-ul de instalare al sistemului de operare *Windows Server 2003*. Pachetul de instalare se numeşte ***adminpak.msi***. Lansarea în execuție a acestui pachet instalează instrumentele de administrare. Pentru calculatoarele care au instalat *Windows Server 2003* ***adminpak.msi*** poate fi găsit şi în C:\Windows\System32.

Obiecte *Active Directory*

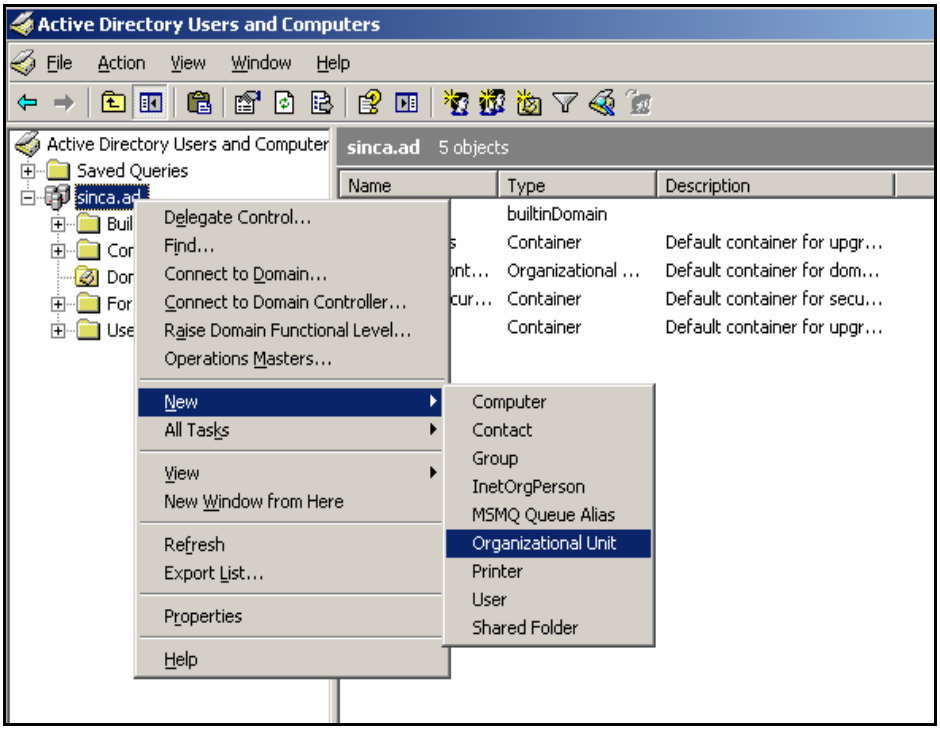
Active Directory Users and Computers este utilitarul care afişează structura logică, arborescentă a unui domeniu. El asigură interfața pentru crearea şi administrarea obiectelor din *Active Directory*.

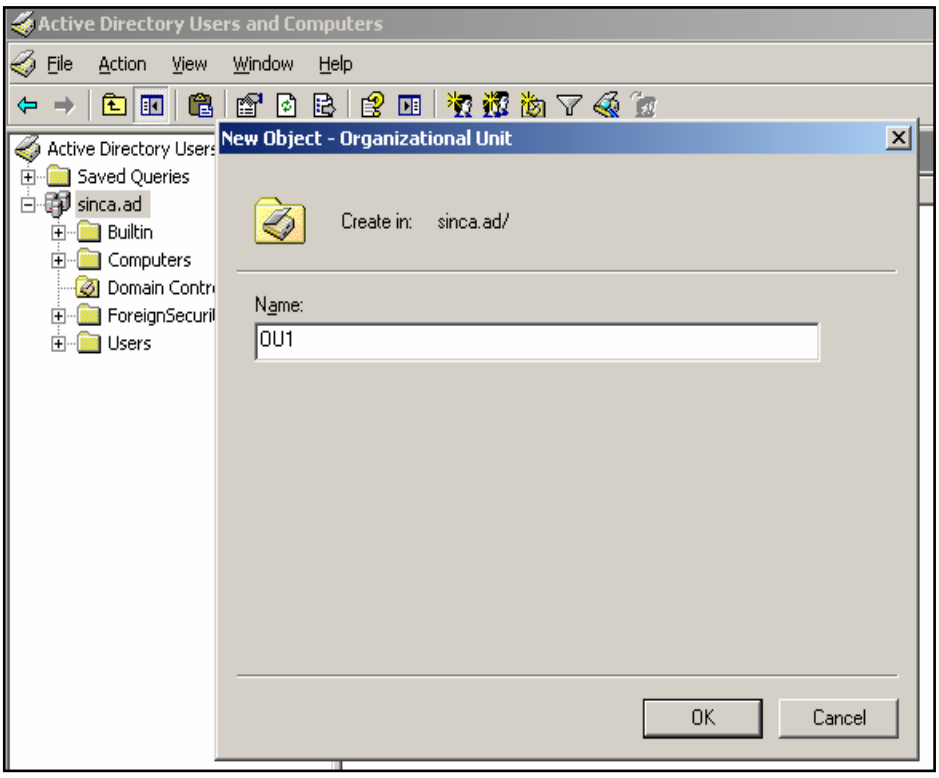


Unitate organizațională

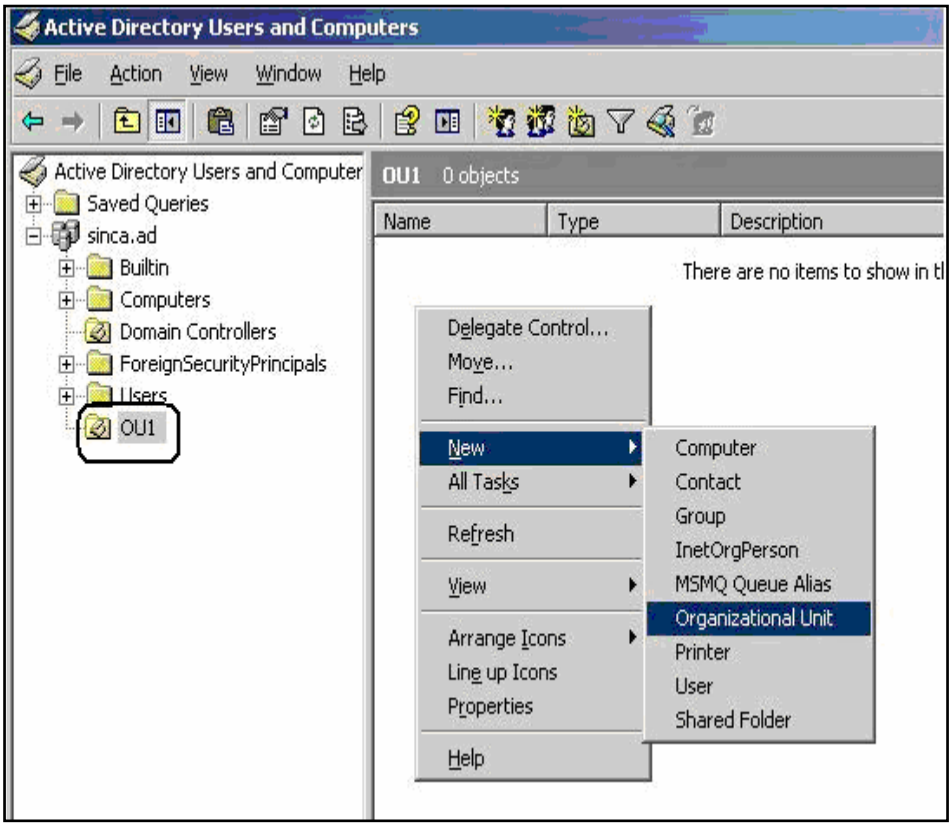
O unitate organizațională (OU) este un container din domeniu folosit pentru a stoca şi organiza obiecte. Unitățile organizaționale pot fi folosite în vederea delegării sarcinilor administrative distincte unor utilizatori care nu sunt administratorii domeniului. Ei vor primi numai sarcina administrării unora dintre obiectele din acea unitate organizațională. Unitățile organizaționale pot fi incluse unele în altele, ceea ce asigură o structură ierarhică a obiectelor.

O unitate organizațională poate fi creată folosind utilitarul ***Active Directory Users and Computers*** (utilizatori şi computere din *Active Directory*). Pentru creare folosim întotdeauna comanda ***New*** (Nou). Obiectele, oricare ar fi ele, sunt recunoscute prin nume.





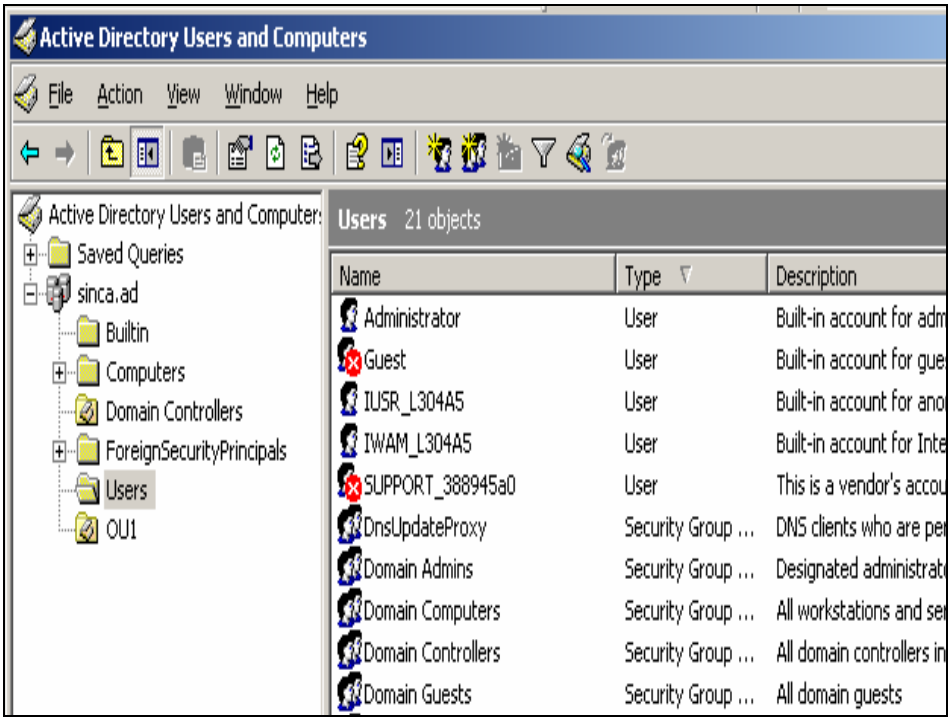
Nou creata unitate de organizare este un container, aşa cum indică şi pictograma care îi este asociată. Se observă că pot fi crete aici obiecte noi.



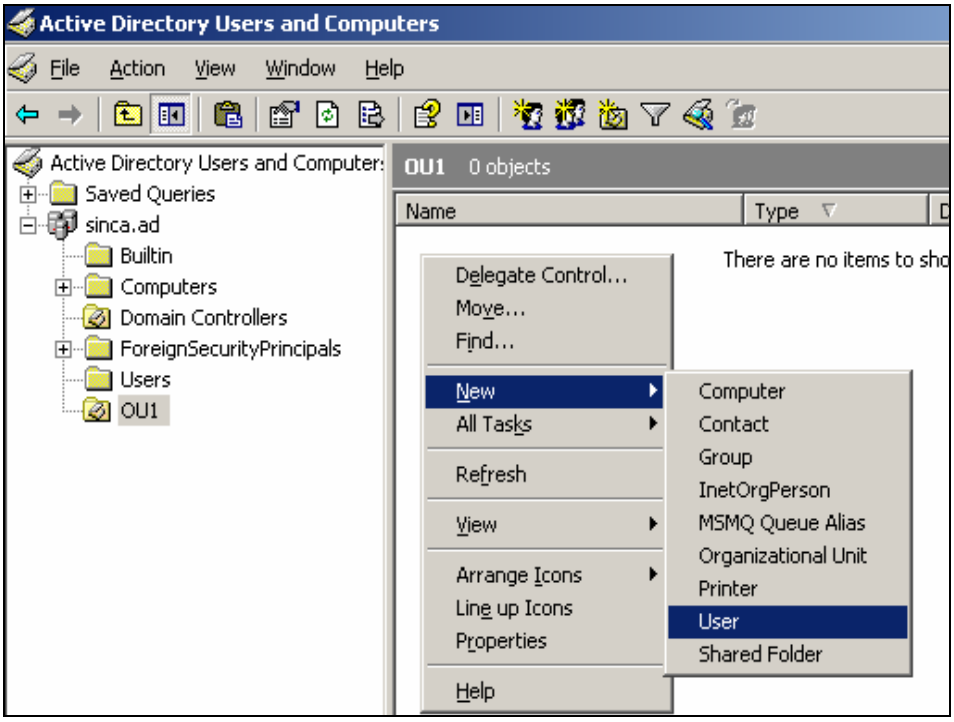
Conturi pentru utilizatori

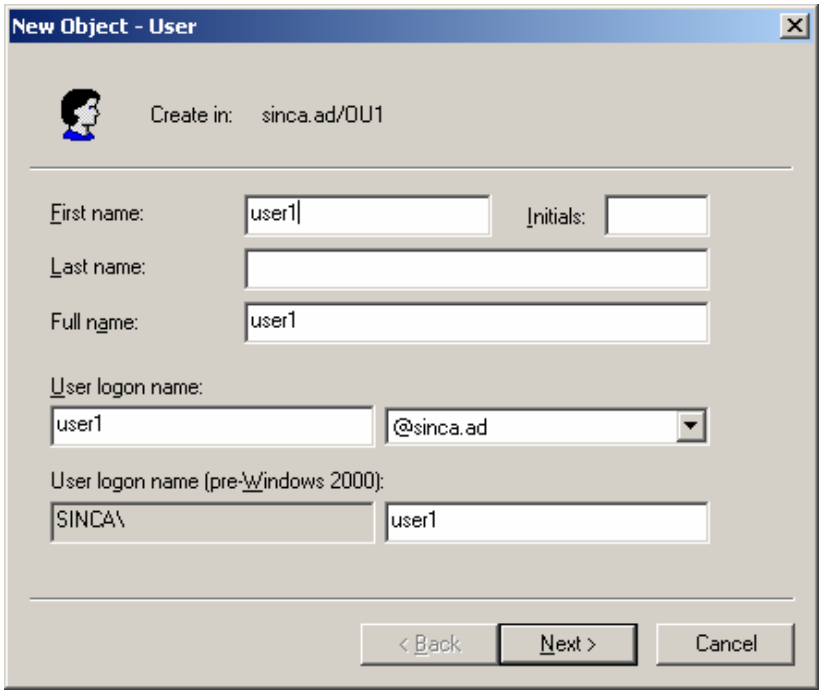
Contul pentru utilizatori este un obiect *Active Directory* care conține toate informațiile necesare pentru definirea şi identificarea unui utilizator în domeniu. Administratorul domeniului va crea câte un cont pentru fiecare utilizator din domeniu. Unele conturi sunt create automat, la instalarea serviciului *Active Directory*.

În domeniu există, de la bun început, contul *Administrator* pentru administratorul domeniului şi respectiv contul *Guest* (oaspete, musafir), care este implicit dezactivat şi care are drepturi limitate în sistem. Ambele conturi sunt plasate în containerul *Users,* care – atenție – nu este unitate organizațională.



Pentru crearea unui cont utilizator avem la îndemână comanda ***New -> User***

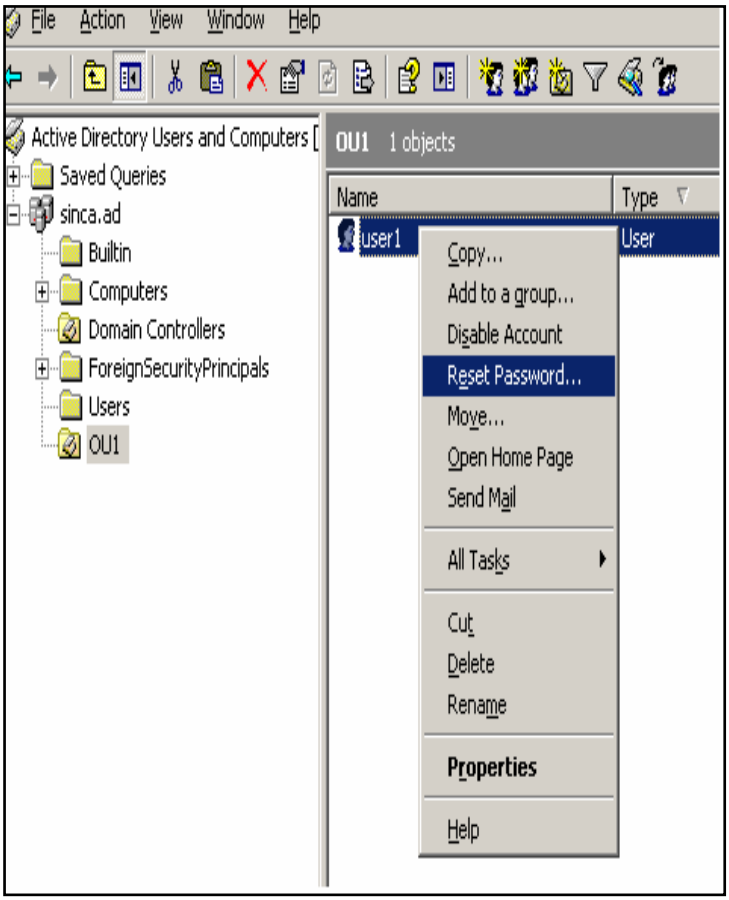




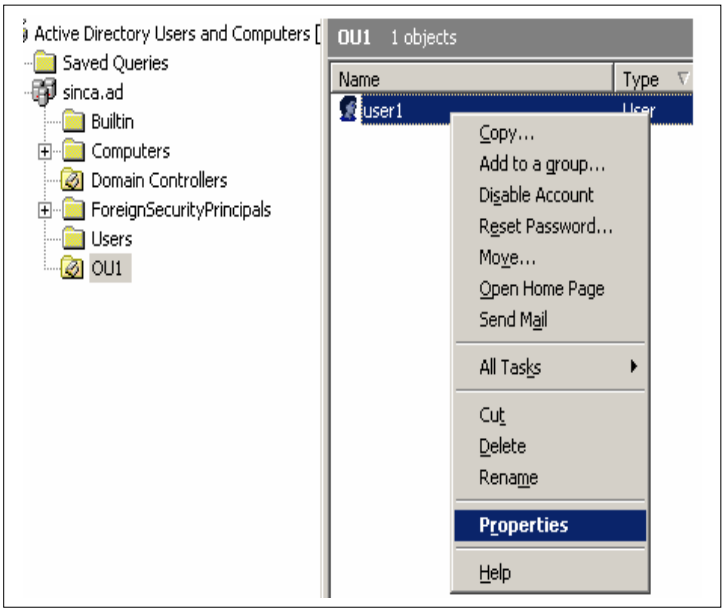
Primele informații despre noul utilizator sunt cele legate de identitatea lui şi de numele folosit pentru deschiderea de sesiune. Urmează apoi parola şi celelalte informații.

Odată contul de utilizator creat putem efectua diverse operații asupra acestuia, ca de exemplu cele care apar după un clic dreapta pe obiectul respectiv:

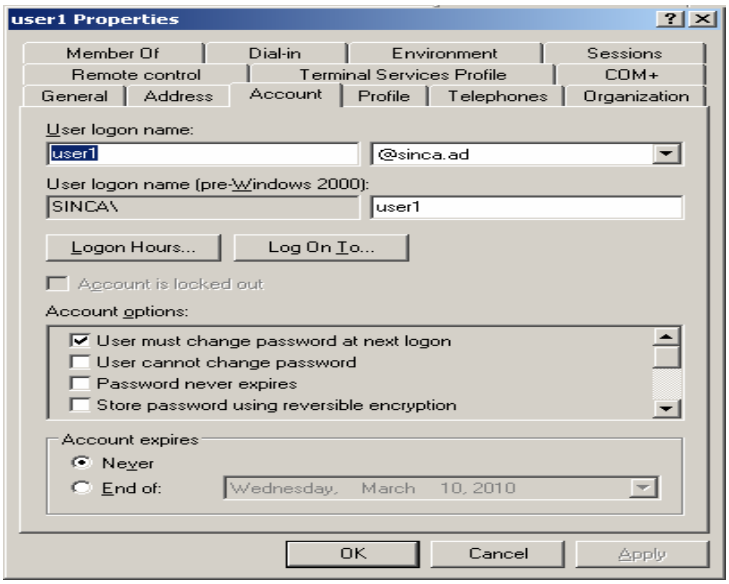
- **Resetare Parolă** (*Reset Password*) – îi oferă administratorului posibilitatea stabilirii unei noi parole pentru acel utilizator.
- **Dezactivare cont** (*Disable Account*) - contul devine dezactivat, nefolosibil; nu se poate face deschidere de sesiune folosind un cont dezactivat. Operația inversă este **Activare cont** (*Enable Accout*)
- **Adăugare în grup** (*Add to a group*)
- **Copiere** (*Copy*)
- **Mutare** (*Move*)



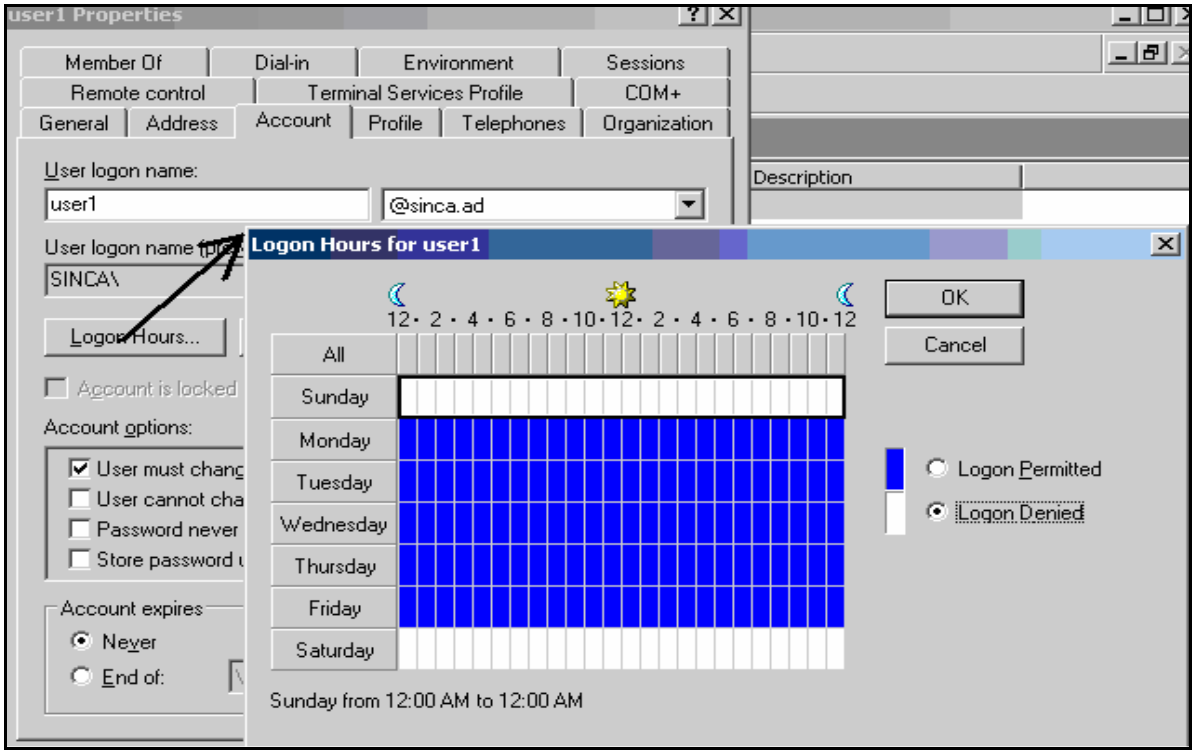
Obiectele *Active Directory* au proprietăți, numite în alte situații atribute. Valorile asociate proprietăților asigură identificarea unică a obiectelor.



Să examinăm câteva dintre proprietățile sau atributele conturilor utilizator:



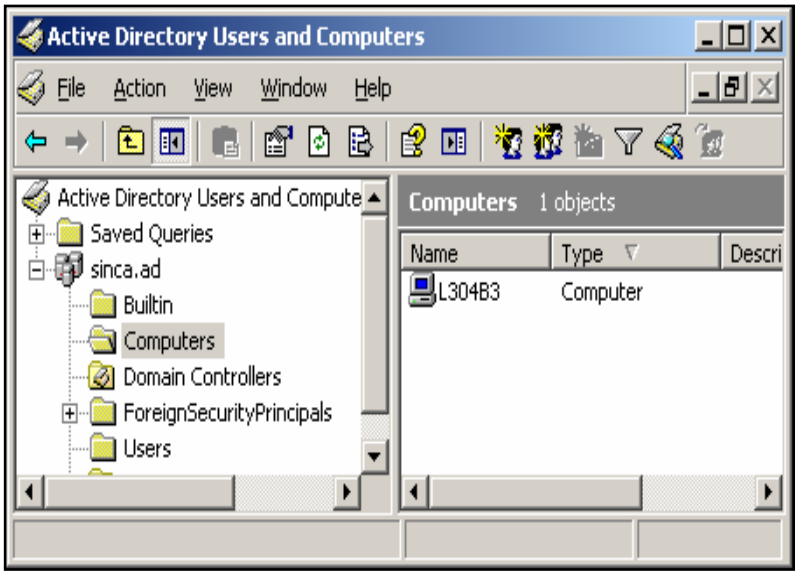
Pentru început remarcăm categoria de proprietăți de tipul ***Account*** (cont) unde apare data de expirare a contului sau, altfel spus durata de valabilitate a contului creat. Tot aici sunt şi posibilele restricții legate de deschiderea de sesiune, şi anume ***Logon hours*** (intervalul de timp în care este permisă deschiderea de sesiune) şi ***Log On To*** (calculatoarele care pot fi folosite pentru deschiderea de sesiune).



De exemplu în figura de mai sus, utilizatorul *user1* nu poate deschide sesiune în zilele de sâmbătă şi duminică.

Conturi pentru computere

Fiecare calculator din domeniu este reprezentat printr-un cont de calculator. Conturile pentru calculatoare pot fi create manual sau automat. Promovarea unui server la rangul (rolul) de controler de domeniu se materializează prin crearea automată a unui cont calculator în containerul ***Domain Controllers*** (Controlere de domeniu). Includerea unui calculator în domeniu determină crearea automată a unui cont calculator în containerul ***Computers*** (Computere).



- ***Domain Controllers*** este un container de tip unitate organizațională pentru conturile controlerelor de domeniu.

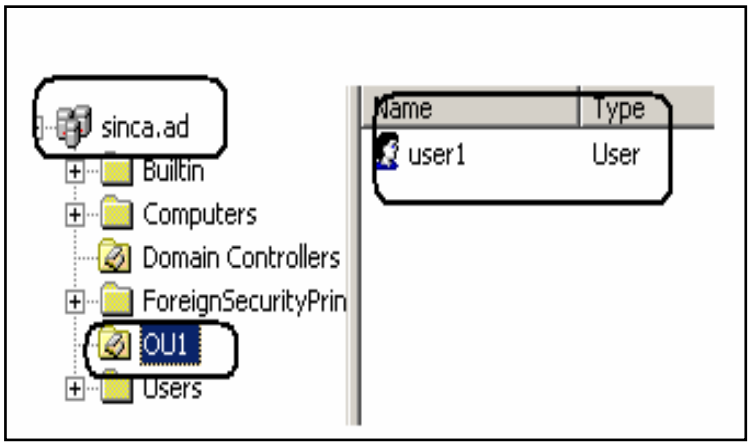
▪ Containerul *Computers* conține calculatoarele membre în domeniu (Containerul *Computers* nu este unitate organizațională).

Identificarea obiectelor *Active Directory*

Obiectele *Active Directory* pot fi identificate prin specificatorii lor LDAP. ***Lightweight Directory Access Protocol*** (**LDAP**) este un protocol standard, stabilit de *Internet Engineering Task Force* (IETF). Specificatorul LDAP complet calificat (numit conform protocolului *distinguished name*) asigură identificarea unică a unui obiect *în Active Directory*.

Din structura unui specificator complet calificat fac parte:

- DC - ***Domain Component*** pentru componentele de nume ale domeniului
- OU - ***Organizational Unit*** pentru unitățile organizaționale care compun calea până la obiect
- CN - ***Common Name*** numele obiectului



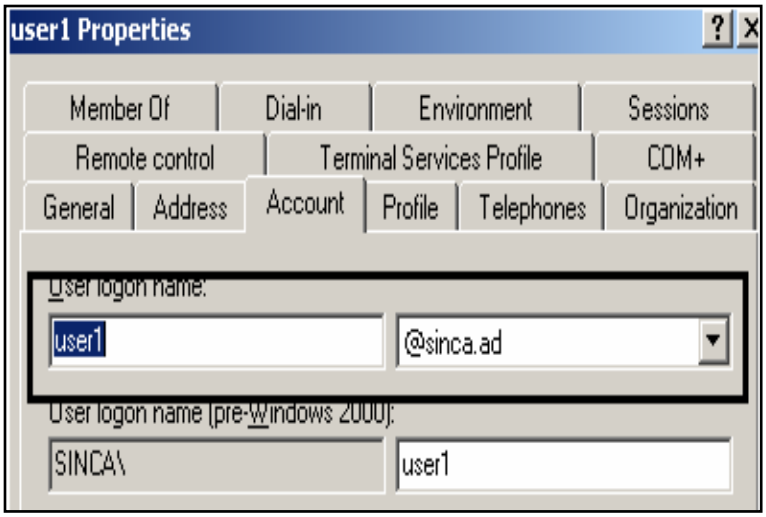
Specificatorul LDAP al contului utilizator user1 este:

CN=user1, OU=OU1, DC=sinca, DC=ad

Notă: Numele CN al unui cont utilizator va fi

First name Initials. Last name.

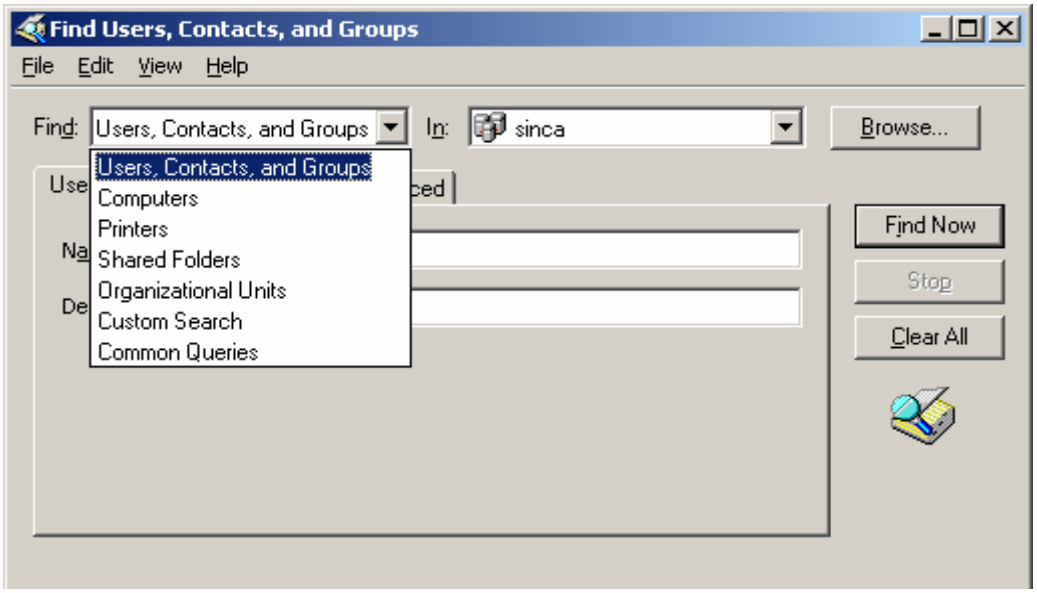
Specificatorul LDAP OU=Cursuri, OU=OU1, DC=sinca, DC=ad se referă la obiectul unitate organizațională numit *Cursuri* aflat în *OU1* care la rândul lui se află în domeniul *sinca.ad*.



Obiectele utilizator pot fi identificate prin aşa-numitul *User Principal Name* (UPN). Formatul general al acestui specificator este **sufix@domeniu**, sau în cazul nostru *user1@sinca.ad*.

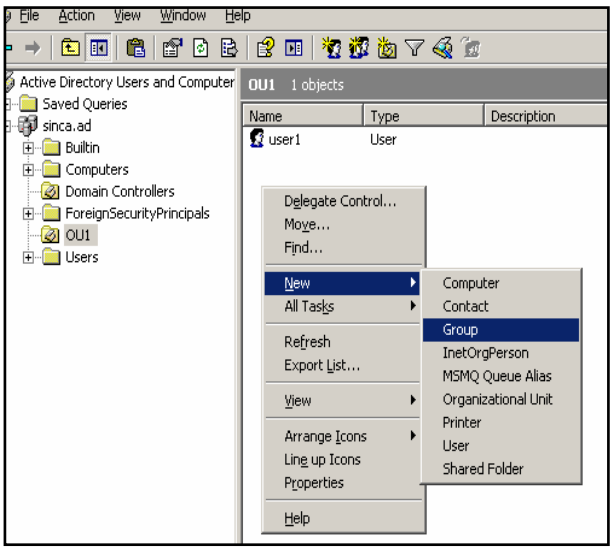
Toate obiectele Active Directory pot fi identificate prin GUID – ***Globally Unique Identifier*** – identificatorul unic global. Identificatorul este creat odată cu obiectul şi nu se va modifica niciodată pe toată durata existenței obiectului, indiferent dacă obiectul se mută dintr-un loc în altul sau dacă i se schimbă numele.

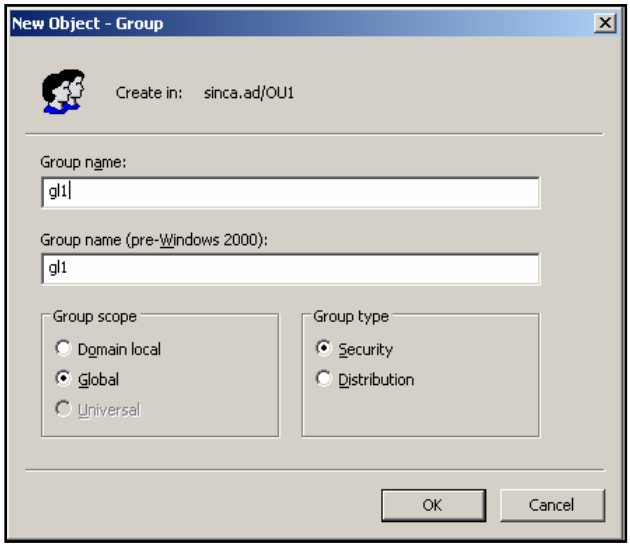
Utilitarul *Active Directory Users and Computers* permite căutarea şi găsirea, localizarea obiectelor din *Active Directory*. Comanda este *Find* (caută). Vor trebui indicate criteriile de căutare.



Grupuri

Grupurile sunt colecții de utilizatori şi calculatoare care pot fi tratate unitar. Grupurile au membrii şi pot fi incluse în alte grupuri. Grupurilor le sunt de obicei asociate drepturi sau permisiuni, ceea ce face ca fiecare membru al grupului să beneficieze de acelaşi set de drepturi sau permisiuni. Crearea conturilor de grup se face printr-o comandă ***New → Group***





Grupurile sunt caracterizate prin tip şi arie de cuprindere sau arie de vizibilitate (*scope*). În funcție de tip, grupurile pot fi de distribuție, adică membrii grupului vor fi destinatarii mesajelor e-mail trimise către grup, sau de tip securitate (*security*). În acest ultim caz, grupului i se pot asocia drepturi, permisiuni, restricții, ceea ce va face ca fiecare membru al grupului să aibă exact acelaşi set de drepturi, permisiuni şi restricții.

După aria de cuprindere sau aria de vizibilitate grupurile pot fi:

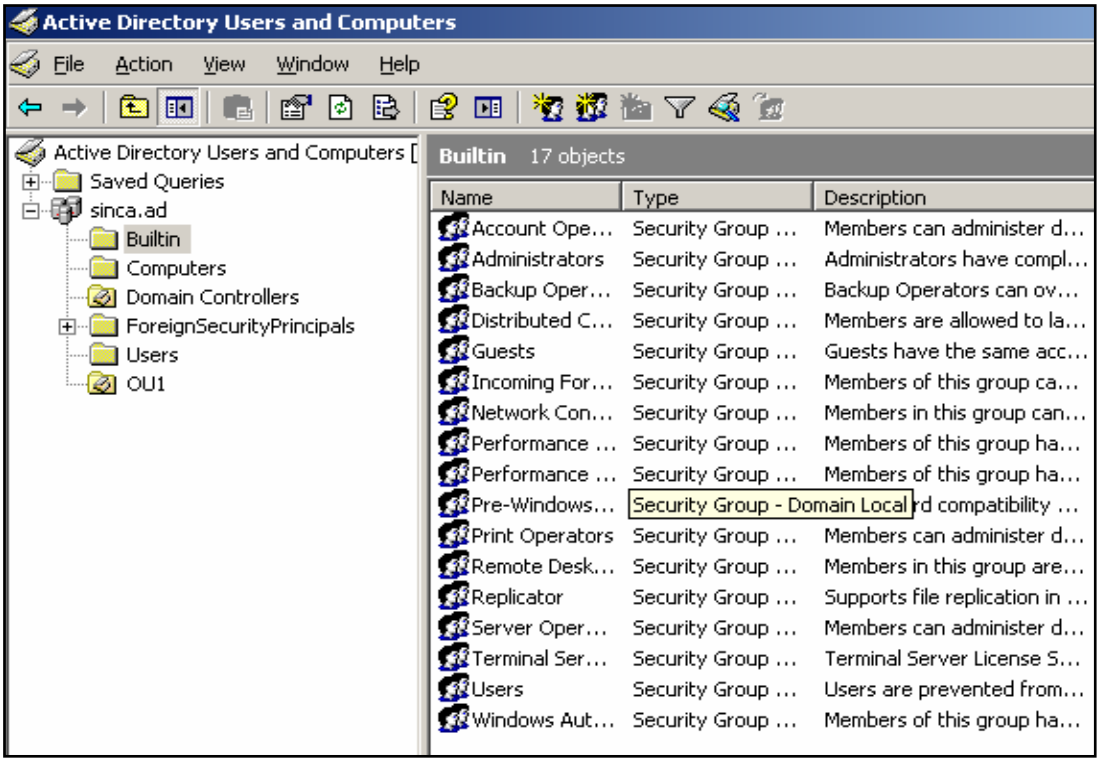
- Globale
- Locale domeniului
- Universale

Diferențierea în funcție de *scope* apare când se analizează relația dintre membrii grupului şi resursele disponibile. În general, grupurile au membri care pot fi conturi de utilizator şi/sau alte grupuri. Resursele disponibile, respectiv resursele pe care le pot folosi membrii grupului, sunt foldere, fişiere, imprimante distribuite pe calculatoarele din rețea. În analiza ce urmează considerăm o structură *Active Directory* cu cel puțin două domenii.

Grup Global	**Membrii**	Conturi (de utilizator sau de computer) şi grupuri globale din acelaşi domeniu cu cel în care se află grupul
	Resursele disponibile	Oriunde, în orice domeniu al pădurii
Grup Universal	**Membrii**	Conturi (de utilizator sau de computer), grupuri globale şi universale din orice domeniu al pădurii
	Resursele disponibile	Oriunde, în orice domeniu al pădurii
Grup local domeniului Domain Local)	**Membrii**	Conturi (de utilizator sau de computer), grupuri globale şi universale din orice domeniu al pădurii şi grupuri locale domeniului din acelaşi domeniu cu cel în care se află grupul
	Resursele disponibile	Locale domeniului, din domeniul în care se află grupul

În domeniu există câteva grupuri preconstruite. Apartenența la aceste grupuri oferă membrilor drepturile asociate.

Grupurile preconstruite există în containerele *Users* şi *Builtin* şi pot fi vizualizate folosind ***Active Directory Users and Computers*.**



Drepturile implicite pentru principalele grupuri predefinite din domeniu sunt următoarele:

Grup	Descriere	Drepturi implicite
Account Operators	Membrii acestui grup pot crea, modifica, şterge conturi pentru utilizatori în containere, altele decât *Domain controllers*	*Allow log on locally;* *Shut down the system.*
Administrators	Membrii acestui grup au control deplin asupra tuturor controlerelor de domeniu	*Access this computer from the network;* *Back up files and directories;* *Change the system time;* *Debug programs;* *Enable computer and user accounts to be trusted for delegation;* *Force a shutdown from a remote system;*

Grup	Descriere	Drepturi implicite
		Increase scheduling priority; Load and unload device drivers; Allow log on locally; Manage auditing and security log; Modify firmware environment values; Profile system performance; Remove computer from docking station; Restore files and directories; Shut down the system; Take ownership of files or other objects.
Backup Operators	Membrii acestui grup pot salva şi restaura toate fişierele de pe controlere de domeniu, indiferent de permisiunile lor la fişiere	*Back up files and directories; Allow log on locally; Restore files and directories; Shut down the system.*
Print Operators	Membrii pot controla imprimarea: creează, partajează, şterg obiectele printer, gestionează obiectele printer din *Active Directory*	*Allow log on locally; Shut down the system.*
Server Operators	Membrii pot crea pe controlerele de domeniu resurse partajate, le pot şterge, pot starta şi opri anumite servicii, pot salva şi restaura fişiere	*Back up files and directories; Change the system time; Force shutdown from a remote system; Allow log on locally; Restore files and directories; Shut down the system.*
Users	Membrii pot executa sarcini obişnuite, care includ lansarea în execuție a aplicațiilor. *Domain Users* este membru aici	

Grup	Descriere	Drepturi implicite
Domain Admins	Membrii acestui grup au control deplin asupra domeniului. Implicit este inclus în *Administrators* local domeniului	*Access this computer from the network; Back up files and directories; Change the system time; Debug programs; Enable computer and user accounts to be trusted for delegation; Force a shutdown from a remote system; Increase scheduling priority; Load and unload device drivers; Allow log on locally; Manage auditing and security log; Modify firmware environment values; Restore files and directories; Shut down the system; Take ownership of files or other objects.*
Domain Users	Conține toți utilizatorii din domeniu. Orice cont utilizator creat este implicit membru în acest grup.	
Enterprise Admins (exista numai în domeniul rădăcină)	Dețin controlul asupra întregii păduri (*forest*) Implicit este inclus în grupul *Administrators* local domeniului	Idem ca *Domain Admins*, dar pentru toate domeniile din *forest*.

Frecvent, un cont utilizator este referit prin grupul de utilizatori căruia îi aparține. De exemplu, un cont din grupul *Domain Admins* este denumit administrator de domeniu. Un cont poate fi membrul mai multor grupuri. În această situație drepturile, permisiunile şi restricțiile contului sunt cele obținute prin însumarea drepturilor, permisiunilor şi restricțiilor asociate grupurilor din care face parte contul.

Grupurile sistem sunt create de sistemul de operare iar lista membrilor grupului este implicită, deci nu poate fi modificată explicit.

Cele mai cunoscute grupuri sistem sunt :

Nume	Descriere
Everyone	toți utilizatorii din rețea.
Anonymous Logon	utilizatorii şi serviciile care accesează prin rețea computerul şi resursele sale, fără a utiliza un nume de cont şi parolă.
Interactive	utilizatorii care au sesiune deschisă în acel moment
Network	utilizatorii care accesează resursele de la acel calculator, prin rețea
Authenticated Users	utilizatorii din *Active Directory*. Utilizatorii de tip *guest* nu fac parte din acest grup
Creator Owner	contul utilizator care a creat sau a luat în proprietate resursa (obiectul). Membrii acestui grup au în mod implicit permisiunea de a modifica permisiunile la obiectul pe care îl dețin în proprietate

Nivelul funcțional al unui domeniu

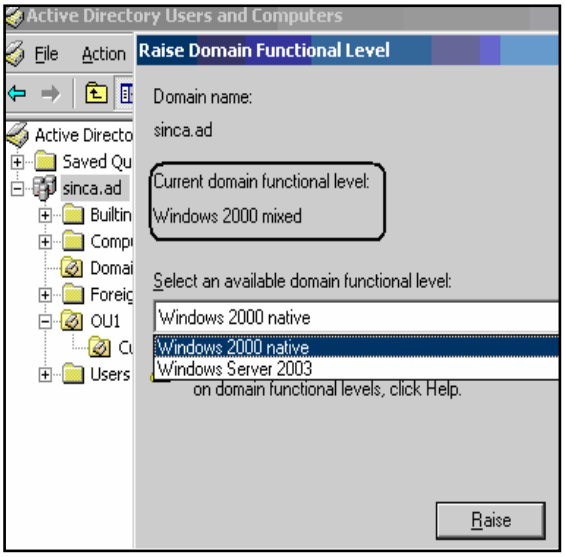
În domeniile *Windows 2003 Active Directory*, controlerele de domeniu pot rula versiuni diferite de sisteme de operare *Windows Server*.

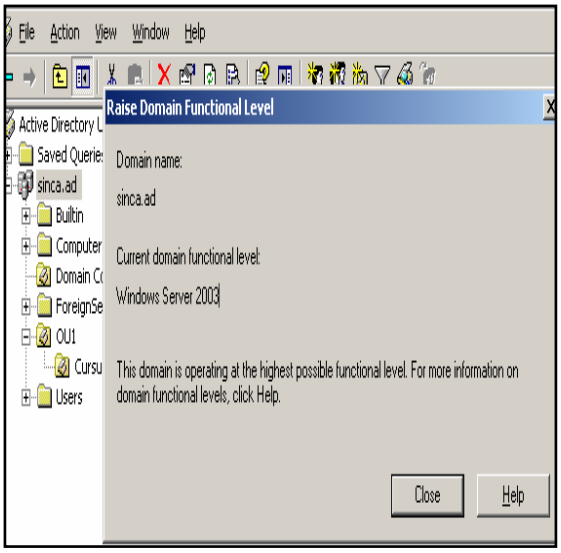
În acest context, există patru niveluri de funcționare a unui domeniu.

- *Windows 2000* mixt (implicit)
- *Windows 2000* nativ
- *Windows Server 2003* interim (obținut numai în urma *upgrade*-ului direct de la *Windows NT4.0* la *Windows 2003 Server*)
- *Windows Server 2003*

Domain Functional Level	**Controlere de domeniu**
Windows 2000 mixt	Windows Server 2003 Windows 2000 Windows NT 4.0
Windows 2000 nativ	Windows Server 2003 Windows 2000
Windows Server 2003 interim	Windows NT 4.0 Windows Server 2003
Windows Server 2003	Windows Server 2003

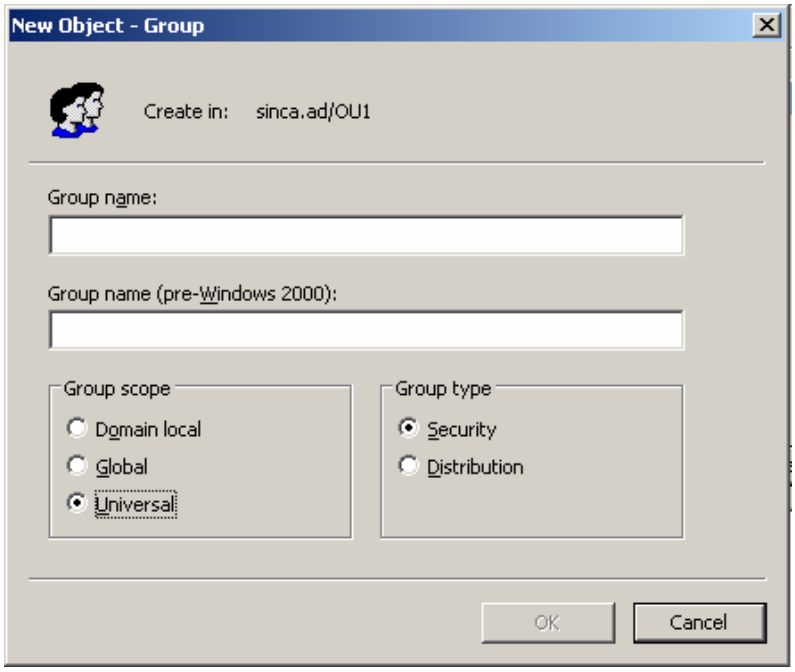
Pentru crearea grupurilor universale este nevoie ca nivelul funcțional al domeniului să fie *Windows 2000 nativ* sau *Windows Server 2003.* După promovarea unui server la rolul de controler de domeniu, în mod implicit nivelul funcțional este *Windows 2000 mixt*. Ar fi nevoie deci de ridicarea nivelului funcțional (*raise functional level*).





Odată stabilit, ridicat nivelul funcțional nu se mai poate reveni la un nivel inferior.

În acest moment se pot crea grupuri de tip *security* universal.



Strategia A G DL P

AGDLP (*Account→Global groups→Domain Local group→Permission*) este strategia recomandată de către *Microsoft* pentru acordarea de permisiuni pentru utilizatorii din rețea.

- Conturile(A) sunt incluse în grupuri globale (G) din acelaşi domeniu.
- Resursele din domeniu vor fi protejate prin permisiuni/restricții acordate grupurilor locale domeniului (DL)
- Grupurile globale (G) sunt incluse în grupurile locale domeniului (DL) în conformitate cu permisiunile pe care trebuie să le aibă utilizatorii.

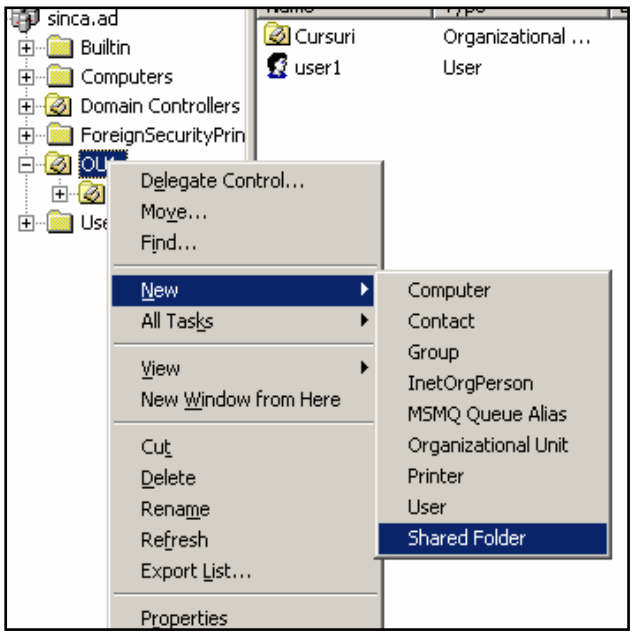
Publicarea resurselor partajate

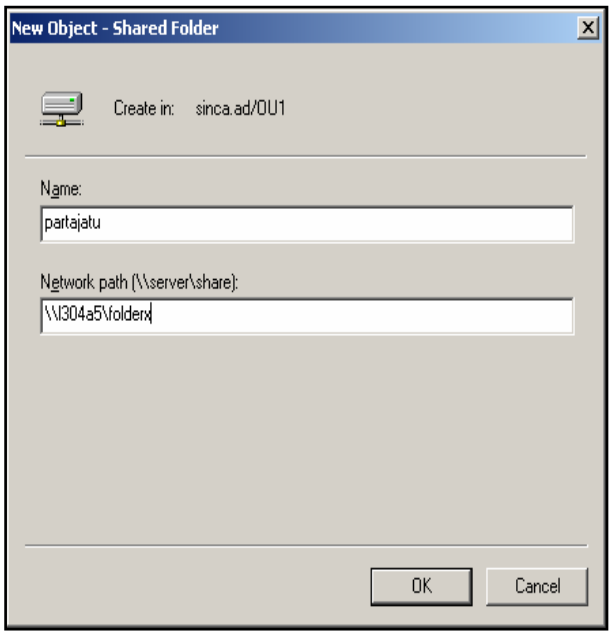
Resursele partajate ale unei rețele – directoare (foldere) sau imprimante partajate – pot fi publicate în *Active Directory*. Prin publicare se creează în *Active Directory* un obiect nou de tipul *shared folder* (folder partajat), respectiv *shared printer* (imprimantă partajată), corespunzător resursei existente şi deja partajate. Obiectele din *Active Directory* sunt uşor de localizat şi de folosit de către utilizatorii din domeniu, la fel şi resursele partajate reprezentate prin obiecte publicate (plasate) în *Active Directory*.

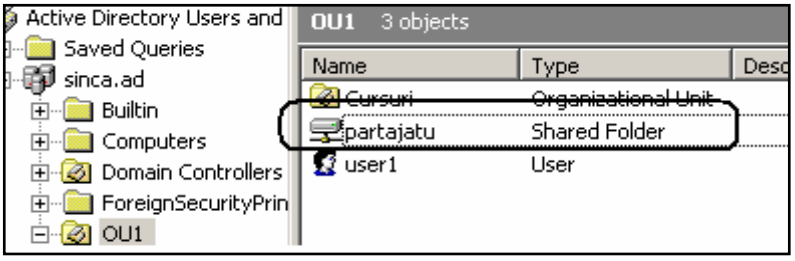
Resursele partajate publicate în *Active Directory* sunt specificate prin numele UNC (*Universal Naming Convention).* Sintaxa generală UNC este:

\\NumeComputer\NumeResursăPartajată

Pentru publicarea dosarelor partajate se foloseşte *Active Directory Users and Computers:*

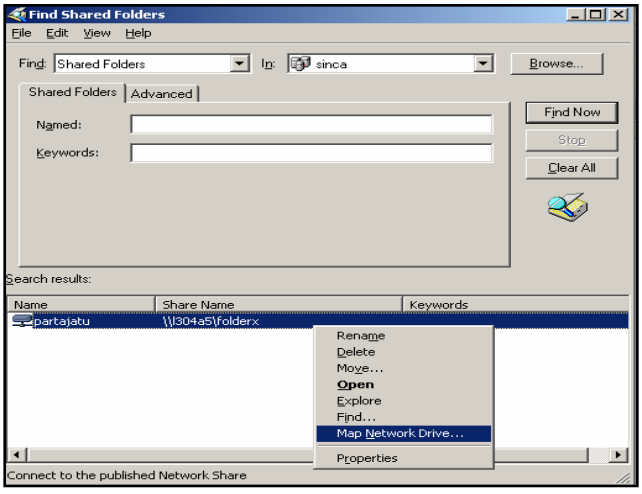


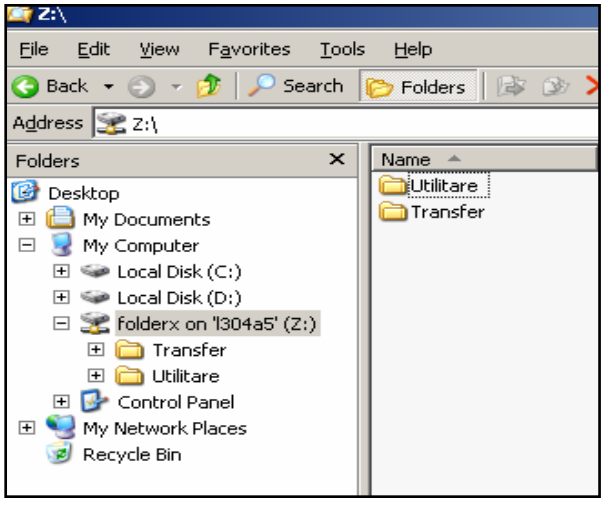


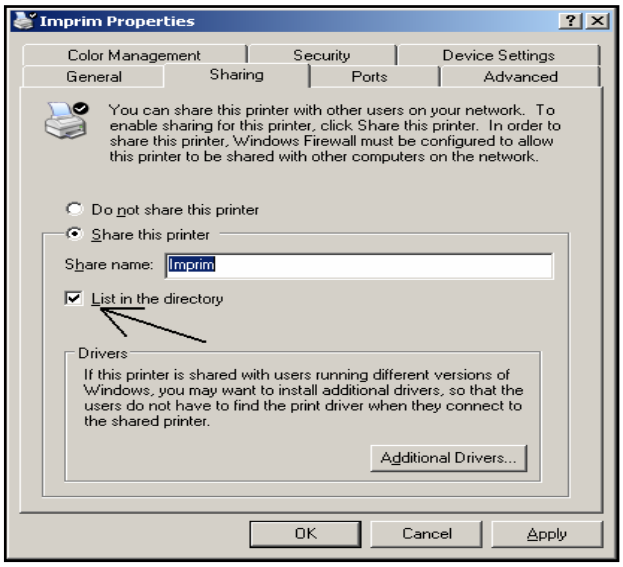


Obiectul din *Active Directory* care corespunde resursei partajate a fost creat în unitatea organizațională *OU1* şi se numeşte *partajatu*.

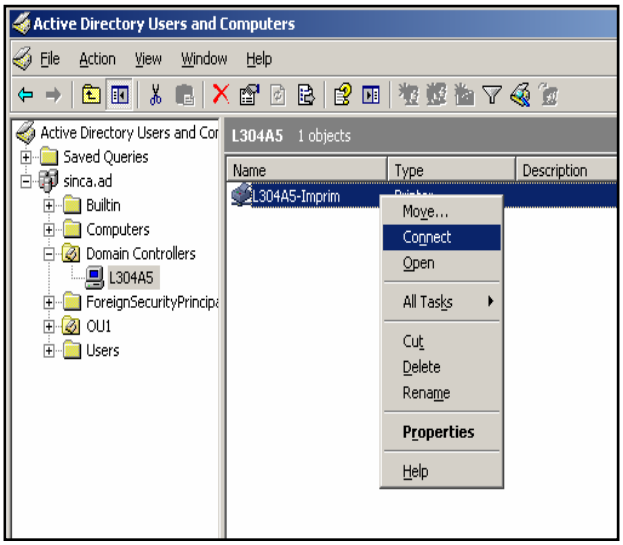
Acest obiect va fi folosit la fel ca toate obiectele *Active Directory*. De la calculatoare membre ale domeniului şi cu sesiune deschisă în domeniu, utilizatorii se pot conecta la folderul partajat şi vor avea acces în limita permisiunilor acordate. Utilizatorul îşi poate construi propriile proiecții de tip *Map Network Drive* prin care asociază un nume de unitate logică (*drive*:) cu obiectul din *Active Directory* care corespunde resursei partajate.





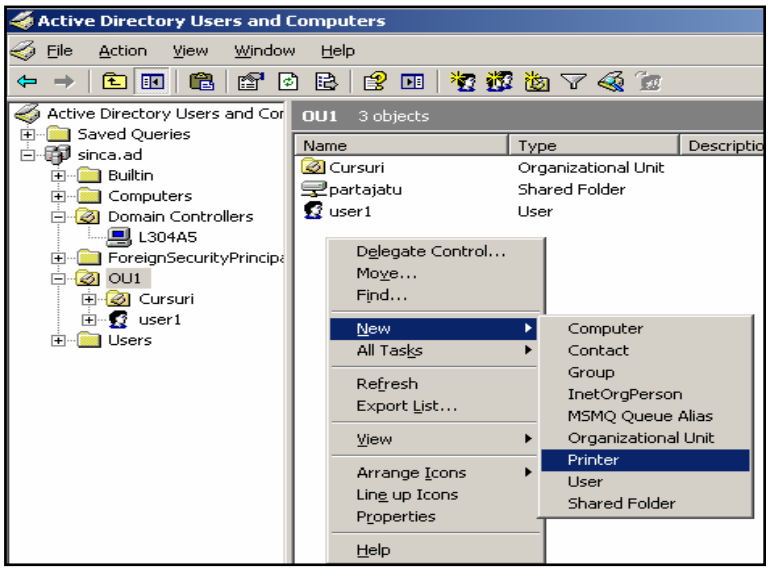


Publicarea în *Active Directory* a unei imprimante partajate are loc chiar la partajarea ei. În mod implicit, imprimantele partajate sunt listate în *Active Directory* (***List in the Directory).***



Containerul în care apare obiectul imprimantă partajată este chiar calculatorul la care este conectată imprimanta. Pentru ca acest obiect să fie vizibil în ierarhia oferită de *Active Directory Users and Computers* va trebui activată opțiunea ***Users, Groups, and Computers as containers*** din meniul ***View***.

În eventualitatea că publicarea în *Active Directory* nu se face automat poate fi folosit mecanismul tradițional, şi anume *New→Printer*

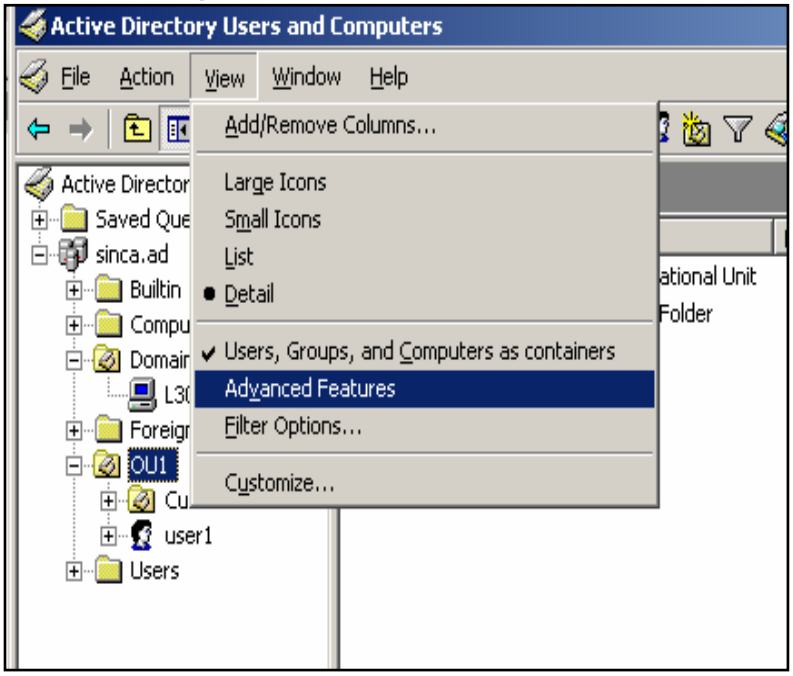


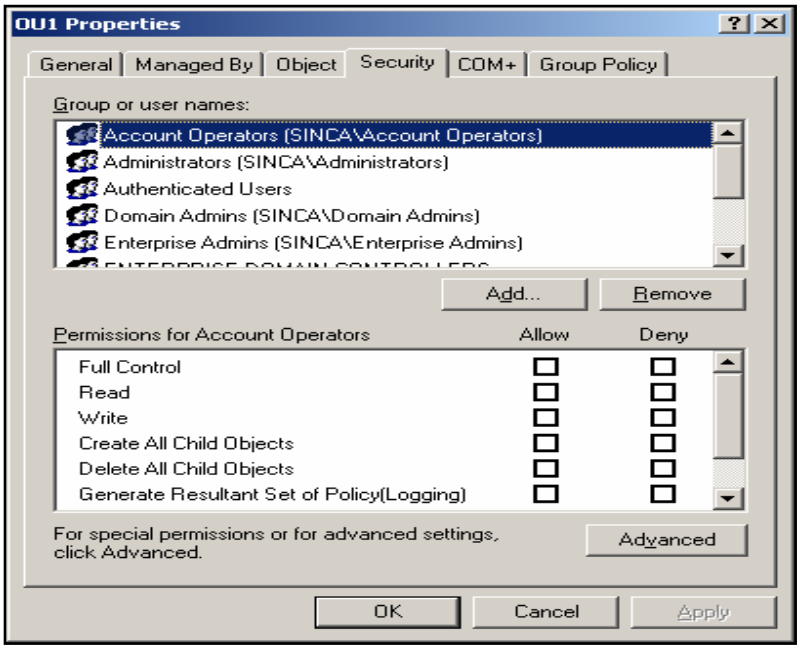
Imprimanta va fi apoi identificată prin specificatorul UNC, de tipul

\\servername\printername

Permisiuni la obiectele din *Active Directory*

Fiecare obiect din *Active Directory* are asociat un descriptor de securitate care defineşte cine are permisiunea de a accesa obiectul şi ce tip de acces este permis. La fel ca pentru foldere, fişiere sau imprimante, lista permisiunilor este definită prin *Discretionary Access Control Lists (DACLs)*. Lista DACL nu este afişată prin *Active DirectoryUsers and Computers* decât dacă modul de vizualizare (meniul ***View***) este ***Advanced Features*** (caracteristici avansate).





Lista permisiunilor este afişată în *tab*-ul *Security* din proprietățile fiecărui obiect.

Active Directory este o structură ierarhică de obiecte. Structura ierarhică este dată de obiectele de tip container. Domeniul este cel mai cuprinzător container. Urmează apoi unitățile organizaționale sau alte obiecte cu rol de container; de exemplu, obiectul de tip computer este implicit container pentru imprimantele locale publicate.

Permisiunile acordate unui utilizator sau unui grup la nivelul unui container se propagă, se moştenesc la obiectele conținute de acel container. *Tab*-ul *Security* (securitate) din fereastra de proprietăți ale unui obiect prezintă setul de permisiuni standard la acel obiect. Permisiunile standard sunt seturi sau combinații de permisiuni acordate unor grupuri şi utilizatori.

Permisiunile standard sunt următoarele:

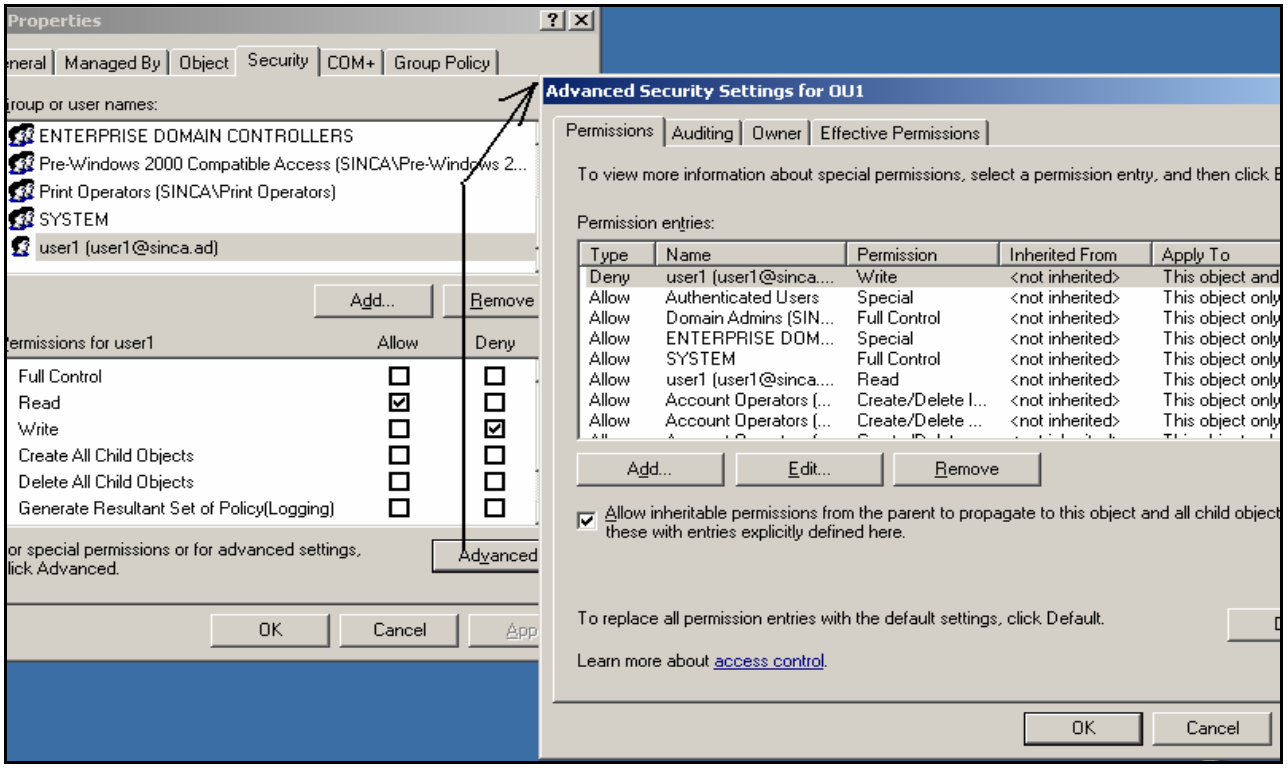
- ***Full Control*** – Control deplin, complet. Utilizatorul care are această permisiune poate avea acces deplin la obiect. În cazul în care este vorba despre un container, atunci utilizatorul care are această permisiune are ***acces*** deplin la toate obiectele din container.
- ***Read*** – Citire. Cine are această permisiune poate citi, poate afişa conținutul şi proprietățile obiectului.
- ***Write*** – Scriere. Este permisiunea necesară în vederea modificării conținutului şi a proprietăților obiectului.
- ***Create All Child Objects*** – Creare obiecte copil. Este o permisiune asociată containerelor şi permite crearea obiectelor copil în acel container.
- ***Delete All Child Objects*** – Ştergere obiecte copil. Este o permisiune asociată containerelor şi permite ştergerea din container a oricărui obiect copil.

Permisiunile pot lua două valori : ***Allow*** (permite) sau ***Deny*** (interzice).

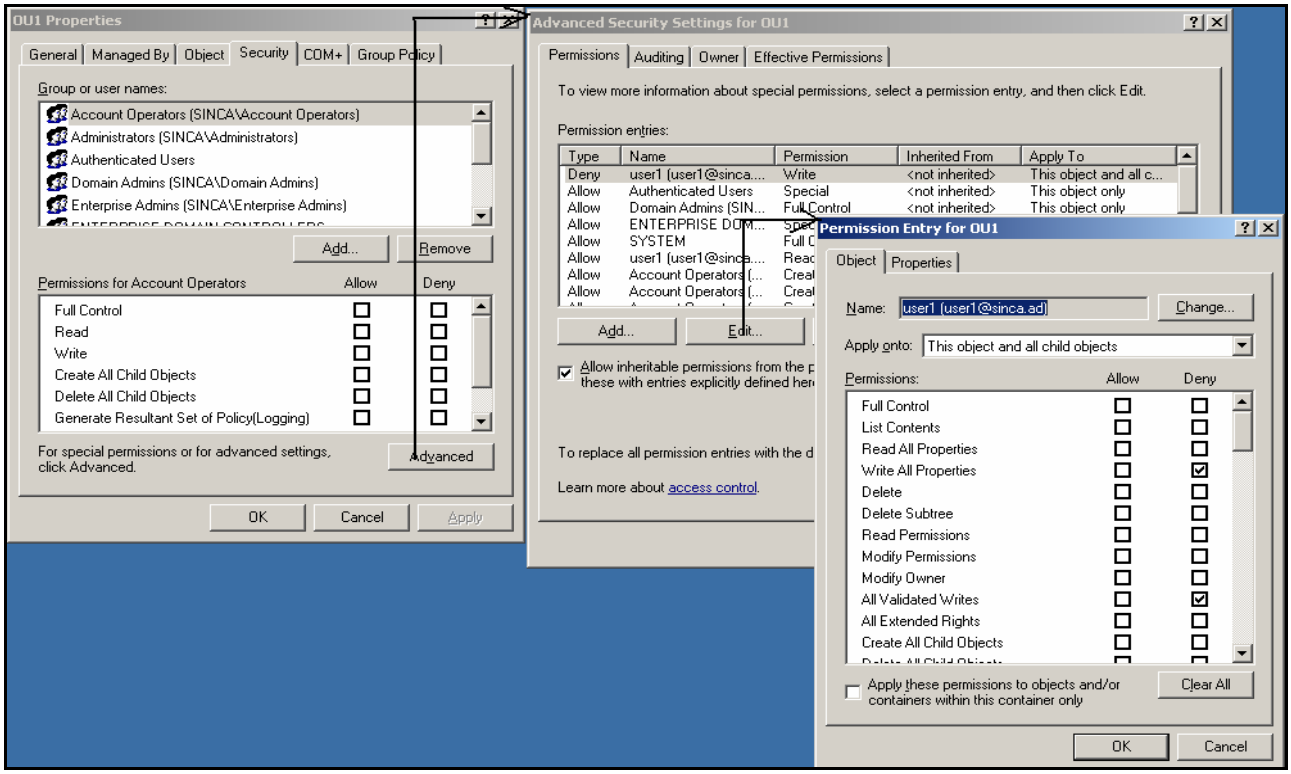
Reguli:

- Permisiunile sunt cumulative, în sensul ca se iau în considerație toate permisiunile acordate utilizatorului şi tuturor grupurilor de utilizatori din care acesta face parte, în mod explicit sau implicit.
- Permisiunea de tip *Deny* (interzis) are prioritate față de orice permisiune de tip *Allow* (permite) acordată contului de utilizator sau grupurilor din care face parte acesta. Permisiunile *Deny* sunt primele evaluate şi nu pot fi anulate prin alte permisiuni de tip *Allow*.
- Permisiune acordată în mod explicit la un anumit nivel are precedență față de o permisiune moştenită.
- Dacă o permisiune nu este acordată nici direct nici prin moştenire, deci dacă nu se spune nimic despre valoare – nici *Allow* nici *Deny*, atunci se consideră implicit *Deny.*

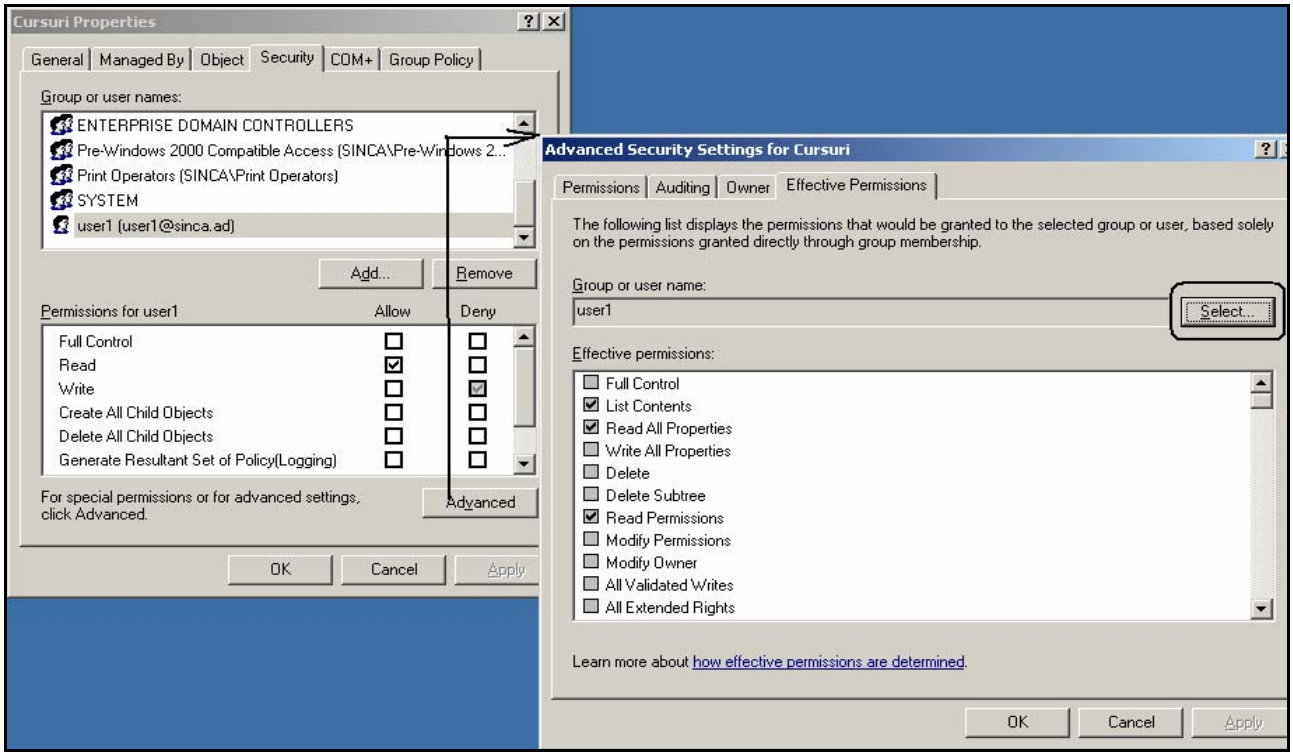
În figura de mai jos este prezentat *tab*-ul *Security* pentru un obiect şi lista de permisiuni detaliate care poate fi vizualizată realizând clic pe butonul *Advanced* (Avansat).



O detaliere suplimentară se poate obține mai departe prin clic pe butonul *Edit*; aici se vor vedea explicit permisiunile acordate.

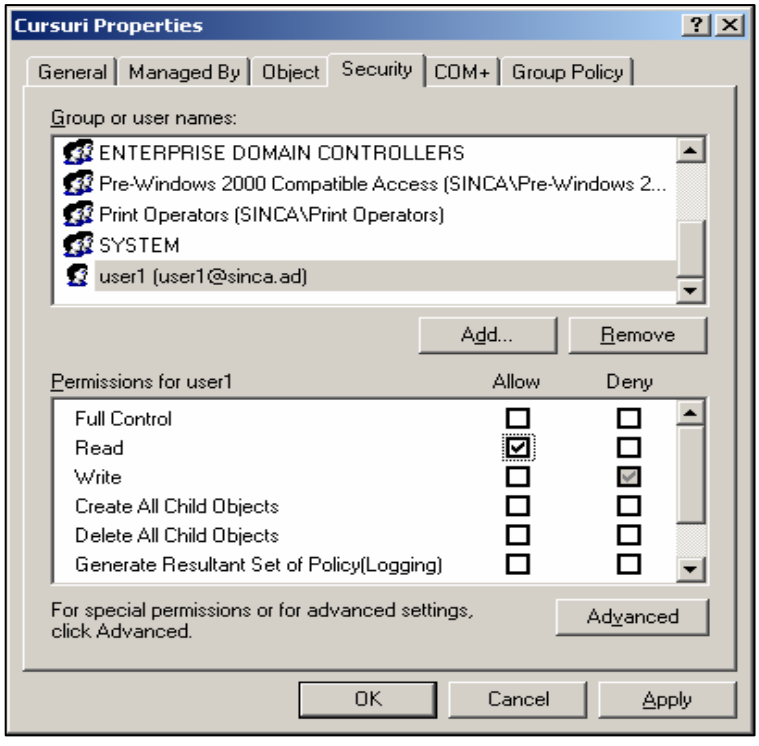


Permisiunile efective (*Effective Permissions*) sunt permisiuni calculate. În lista permisiunilor efective, acolo unde nu există bifă, nu există nici permisiune.



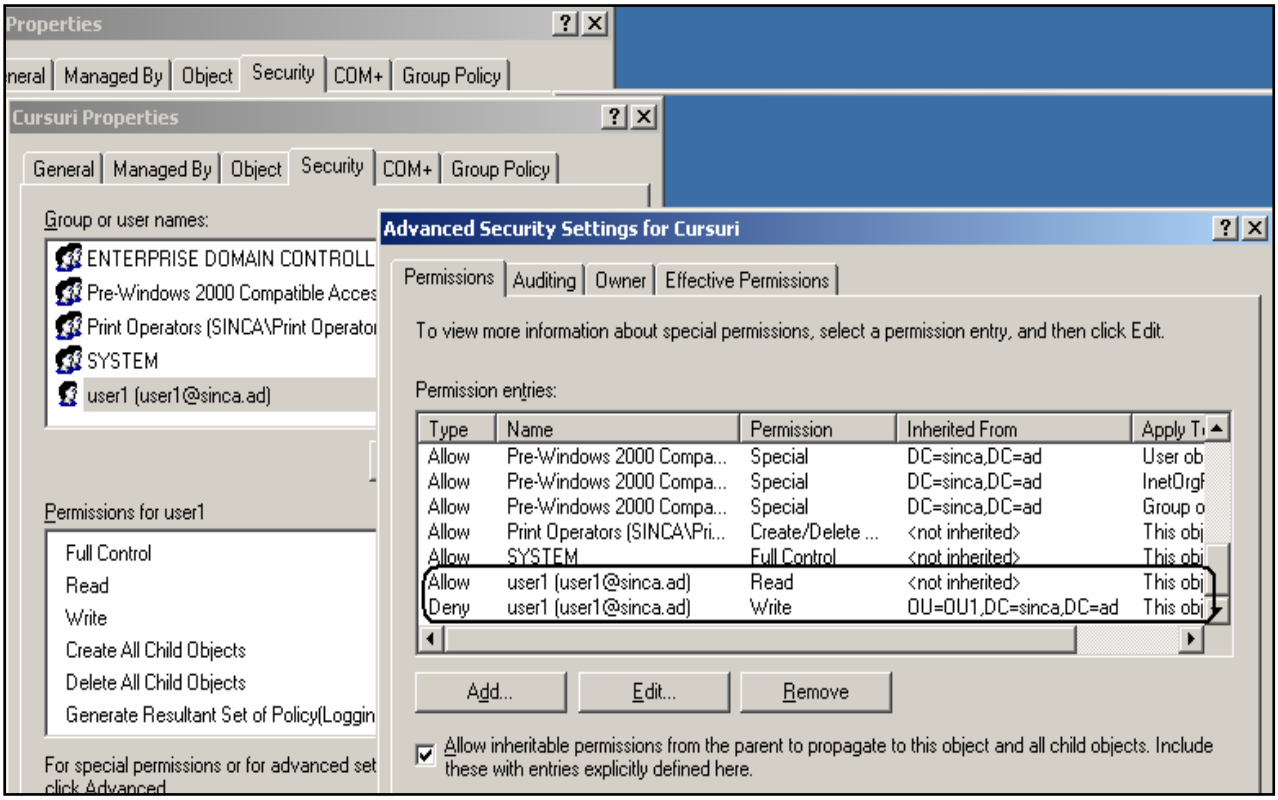
Moştenirea permisiunilor

Există două tipuri de permisiuni: explicite şi moştenite. Permisiunile explicite sunt asignate direct la obiect, iar permisiunile moştenite sunt propagate de la obiectul părinte. În mod implicit, orice obiect moşteneşte permisiunile de la containerul din care face parte, adică de la containerul părinte.



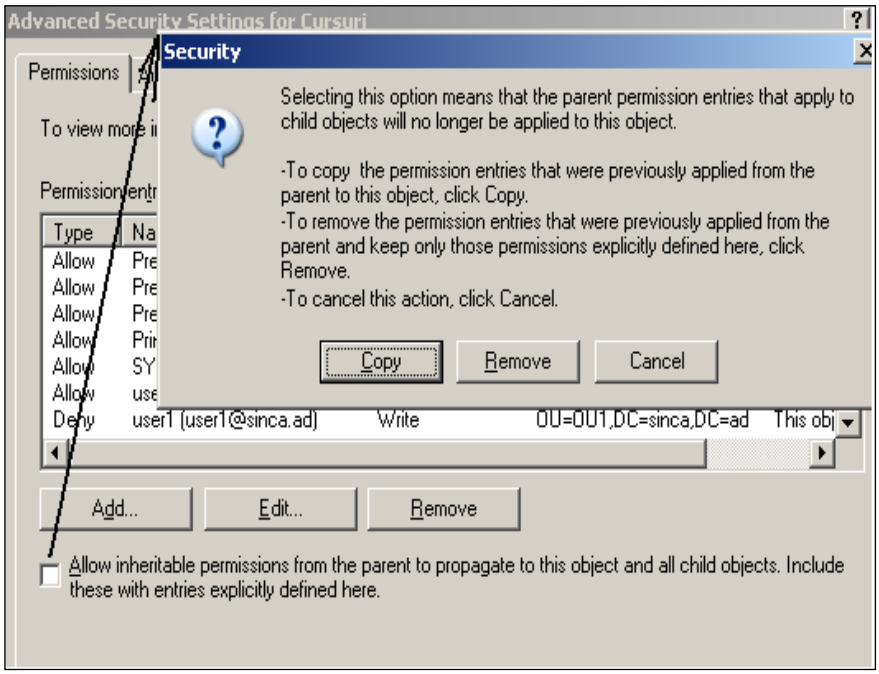
Permisiunile moştenite nu pot fi modificate. Dacă se doreşte ca un obiect să aibă alte permisiuni faţă de cele moştenite, trebuie mai întâi dezactivată moştenirea.

În figura alăturată, utilizatorul *user1* are permisiunea *Read* acordată explicit, în timp de *Deny* pentru *Write* este o valoare moştenită. Permisiunea moştenită este afişată printr-o bifă de culoare gri.



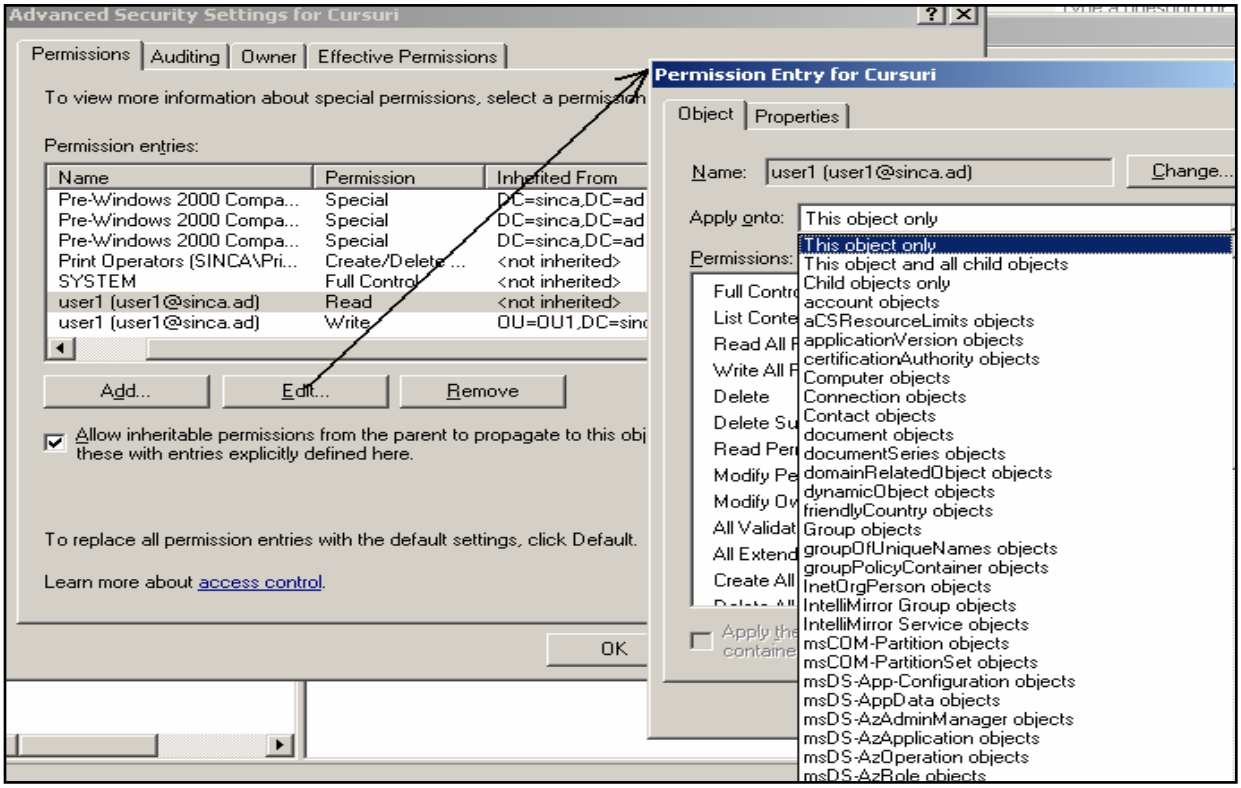
Mai departe, la *Advanced Security,* putem vedea explicit informații despre permisiuni: *Read* nu este moştenită (*not inherited*) iar *Deny Write* este moştenită de la unitatea organizațională OU1. Unitatea organizațională părinte este precizată prin specificatorul LDAP: OU=OU1, DC=sinca, DC=ad.

Dezactivarea moştenirii, adică renunțarea la moştenire, se poate face anulând opțiunea ***Allow Inheritable Permissions from Parent to Propagate to This Object and All Child Objects*** (Este permisă propagarea de la părinte la acest obiect şi la toate obiectele copil a permisiunilor care pot fi moştenite).



Vor apărea trei variante de lucru:

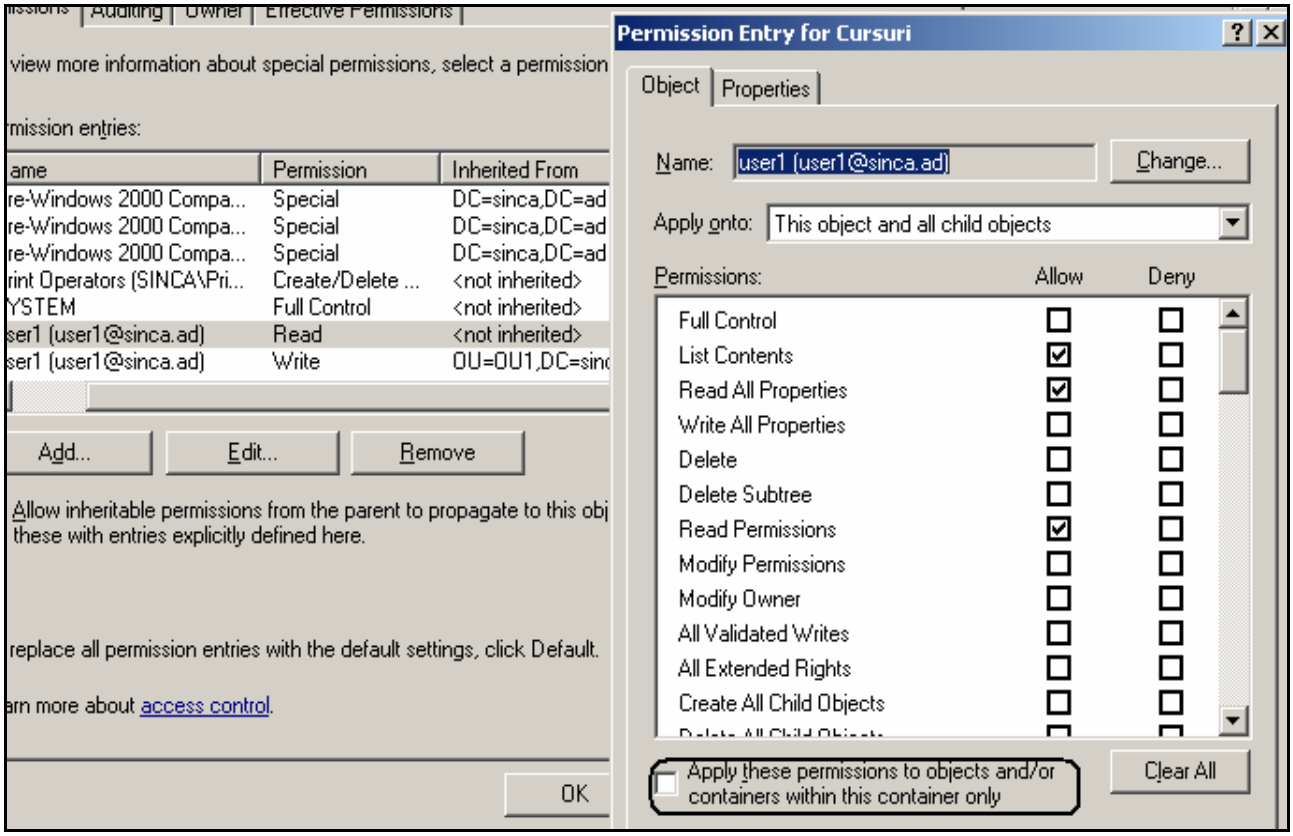
- ***Copy*** – pentru copierea, acordarea explicită, în clar a permisiunilor. Permisiunile existente la obiectul părinte se vor copia la nivelul acestui obiect.
- ***Remove*** – elimină, şterge permisiunile moştenite.
- ***Cancel*** – închide fereastra.



Acordarea unei permisiuni la nivelul unui container este însoțită de opțiunea ***Apply Onto,*** prin care se va indica modul în care permisiunea va fi propagată, sau nu, la nivelul obiectelor din container.

- ***This object only –*** Numai pentru acest obiect - , caz în care permisiunea nu va fi transmisă mai departe; permisiunea este acordata numai obiectului curent.
- ***This object and all child Objects -*** Acest obiect şi toate obiectele copil - , este situația în care permisiunea se aplică obiectului container curent şi tuturor obiectelor pe care le conține.
- ***Child Objects Only -*** Numai pentru obiecte copil - , se referă la permisiuni care se aplică numai obiectelor din container, nu şi containerului însuşi.
- Un anumit tip de obiect, caz în care permisiunea se acordă numai obiectelor de tipul respectiv din acel container.

Transmiterea permisiunilor în jos în arborescență este controlată prin opțiunea ***Allow these permissions to objects and/or containers within this container only*** (Aceste permisiuni sunt acordate numai obiectelor şi / sau containerelor din acest container)***.*** Dacă opțiunea este bifată atunci permisiunile se transmit numai la obiectele aflate în acel container nu şi la obiectele aflate în subcontainerele pe care le conține containerul respectiv.



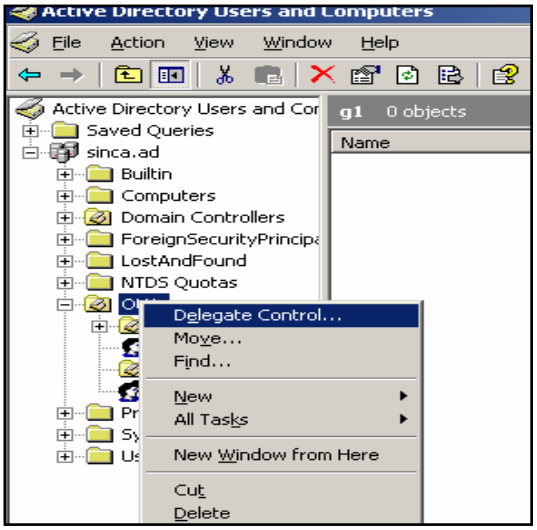
Mutarea obiectelor dintr-un container în altul poate afecta lista DACL asociată obiectului. Cu alte cuvinte, mutarea poate modifica permisiunile la obiectul respectiv. Următoarele tipuri de obiecte pot fi mutate în cadrul structurii *Active Directory*:

- Cont utilizator (*User account*)
- Cont contact (*Contact account*)
- Imprimantă (*Printer*)
- Grup (*Group*)
- Folder partajat (*Shared folder*)
- Computer
- Controler de domeniu (*Domain controller*)
- Unitate organizațională (*Organizational unit*)

Regulile aplicate obiectelor mutate sunt următoarele:

- Permisiunile stabilite în mod explicit rămân neschimbate.
- Obiectul moşteneşte permisiunile de la unitatea organizațională în care este mutat.
- Obiectul nu mai moşteneşte (pierde) permisiunile de la unitatea organizațională din care a fost mutat.

Delegarea controlului administrativ



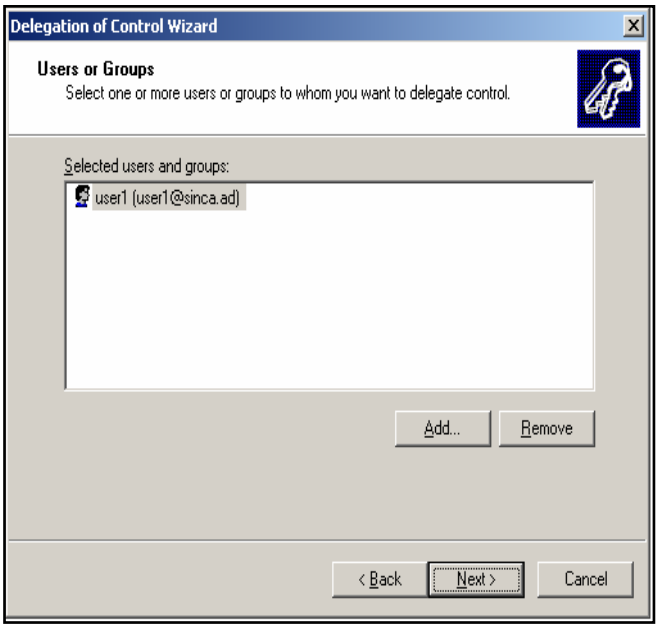
Structurarea ierarhică a domeniului se construieşte prin unitățile organizaționale. Ele sunt containere care conțin obiecte. Administratorul domeniului poate delega către un alt utilizator competențe administrative asupra unei unități organizaționale şi evident, asupra obiectelor din unitatea organizațională. Utilizatorul primeşte astfel capacitatea de a gestiona, de a controla obiectele aflate în acea unitate organizațională.

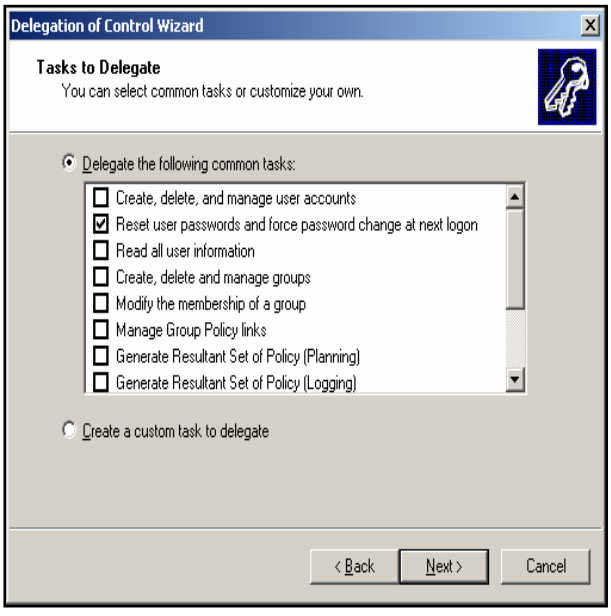
Delegarea controlului administrativ se referă la atribuirea responsabilităților legate de gestionarea unor obiecte dintr-o unitate de organizare. Unele dintre sarcinile administrative vor fi preluate astfel de un utilizator sau, eventual, de un grup de utilizatori.

Vrăjitorul ***Delegation of Control Wizard*** (Delegarea controlului) este modalitatea rapidă prin care vor fi acordate permisiunile necesare efectuării sarcinilor uzuale de administrare la nivelul unității organizaționale. Se vor construi în acest fel listele de permisiuni la nivelul unității de organizare (liste DACL). Altfel spus, obiectului unitate de organizare i se asociază perechi de informații de tipul „cine poate avea acces şi ce acces este permis”.

Un efect similar cu cel obținut prin folosirea vrăjitorului ***Delegation of Control Wizard*** obținem şi prin acordarea manuală de permisiuni pentru anumiți utilizatori sau grupuri asupra obiectului unitate organizațională.

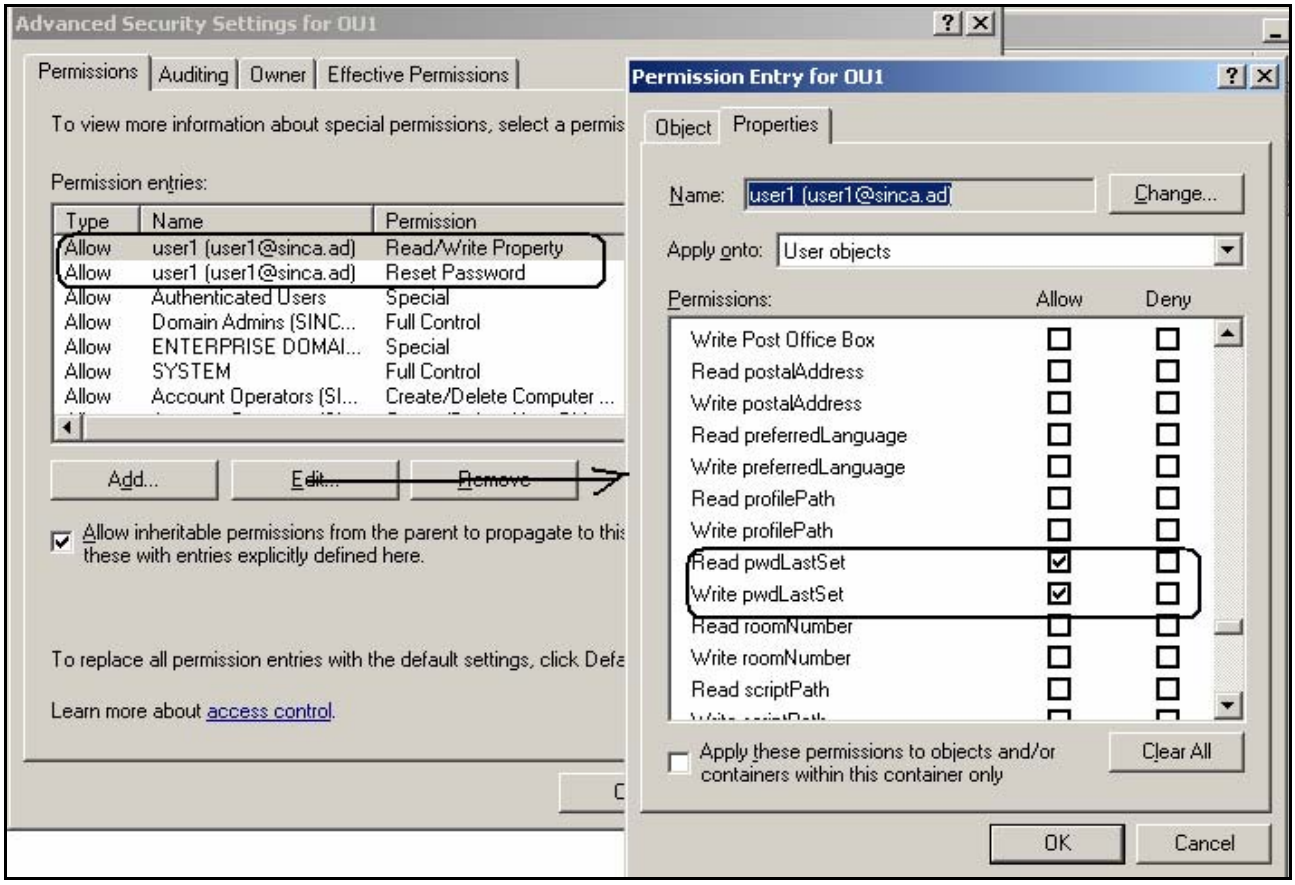
În exemplul nostru utilizatorul *user1* va primi competențe administrative la nivelul unității organizaționale *OU1*.





Sarcinile administrative care i-au fost delegate lui *user1* sunt legate de modificarea parolelor pentru utilizatorii ale căror conturi se găsesc în unitatea organizațională *OU1*: *user1* va putea folosi *Active Directory Users and Computers* pentru a schimba parolele utilizatorilor ale căror conturi sunt în unitatea de organizare *OU1*.

Efectul delegării sarcinilor administrative este acordarea permisiunilor. Lui *user1* i s-au acordat permisiuni la unitatea organizațională *OU1*, ceea ce va apărea în *tab*-ul *Security* .



Politica de grup

Politica de grup (*Group policy*) oferă administratorilor posibilitatea de a controla mediul de lucru pentru fiecare utilizator şi calculator din domeniu. Aceste politici pot conține setări care să modifice aspectul *desktop*-ului utilizatorului, să reconfigureze opțiunile legate de securitate, să instaleze automat anumite pachete *software* pe un calculator şi încă multe altele.

Politicile de grup se pot aplica obiectelor computer şi utilizator din întreg domeniul sau numai dintr-o anumită unitate organizațională.

Politicile de grup pot configura printre altele:

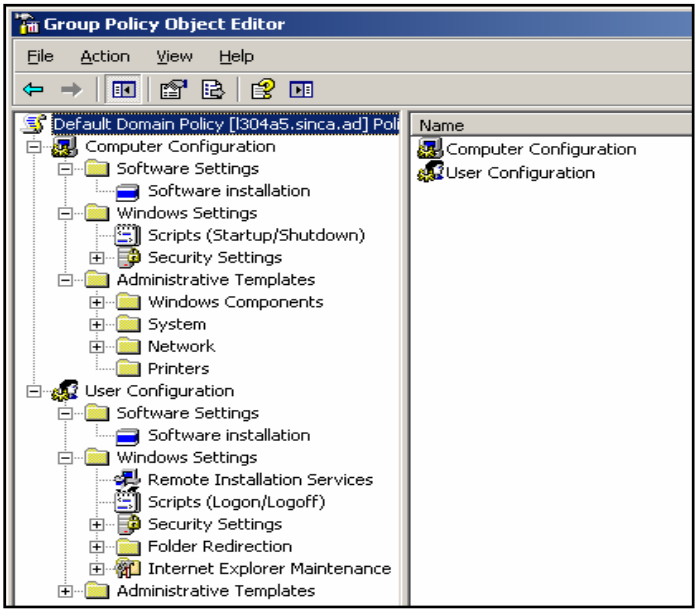
- Configurări din *Registry*
- Opțiuni de securitate
- Opțiuni de instalare şi de întreținere *software*

- Opțiuni pentru fişierele cu comenzi folosite în anumite situații, cum ar fi la startarea sau oprirea funcționării calculatoarelor, la deschiderea sau închiderea sesiunii utilizatorilor
- Opțiuni de redirectare a folderelor

Notă: Politicile de grup nu au efect asupra computerelor care au sisteme de operare mai vechi, cum ar fi *Windows NT 4.0* sau *Windows 98*. Politicile de grup se aplică pentru calculatoare membre ale domeniului şi care rulează sisteme de operare server sau stație de lucru începând cu *Microsoft Windows 2000*.

Politica de grup se poate defini atât la nivelul calculatorului local cât şi în domeniul *Active Directory.*

Politica de grup conține următoarele două ramuri majore:



- ***Computer Configuration***

Administratorii pot utiliza *Computer Configuration* pentru stabilirea politicilor care se aplică pentru computer, indiferent cine deschide sesiune (*logon*) folosind calculatorul. *Computer Configuration* conține subelemente pentru setări *software*, setări *Windows* şi şabloane administrative.

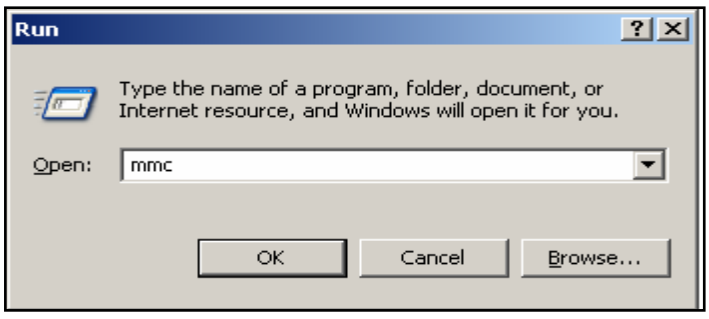
- ***User Configuration***

Administratorii pot utiliza *User Configuration* pentru configurarea politicilor care se aplică utilizatorilor, indiferent de computerul pe care aceştia îl folosesc. *User Configuration* conține subelemente pentru setări *software*, setări *Windows* şi şabloane administrative.

Pe fiecare calculator există *Local Group Policy* care conține setări locale pentru acel computer. Pentru calculatoarele care nu fac parte din domeniu acesta este singura politică aplicată. Pentru cele care fac parte din domeniu, aceasta se combină cu eventualele politici din domeniu.

Group Policy Editor este utilitarul de editare pentru politicile de grup (*Group Policy*).

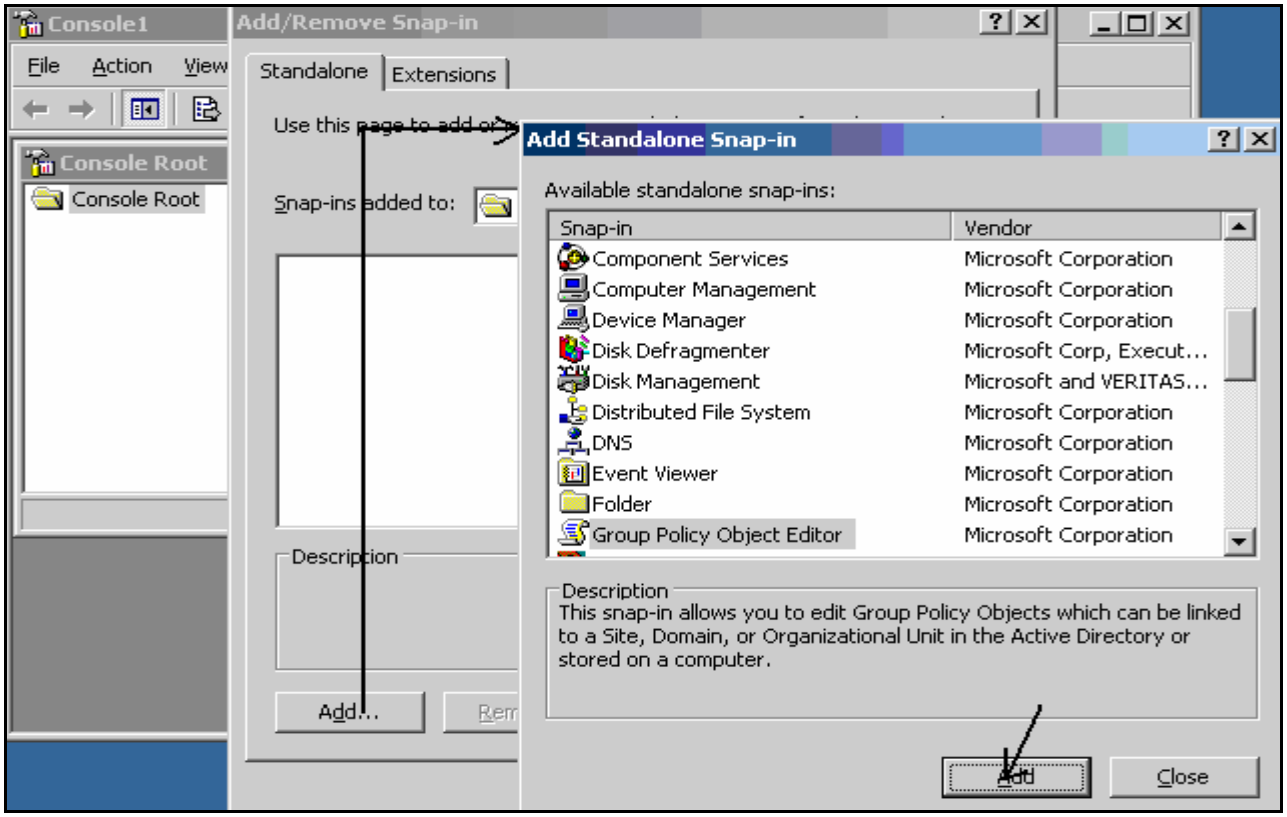
Editorul pentru obiectele *Group Policy* poate fi invocat (apelat) în mai multe moduri:



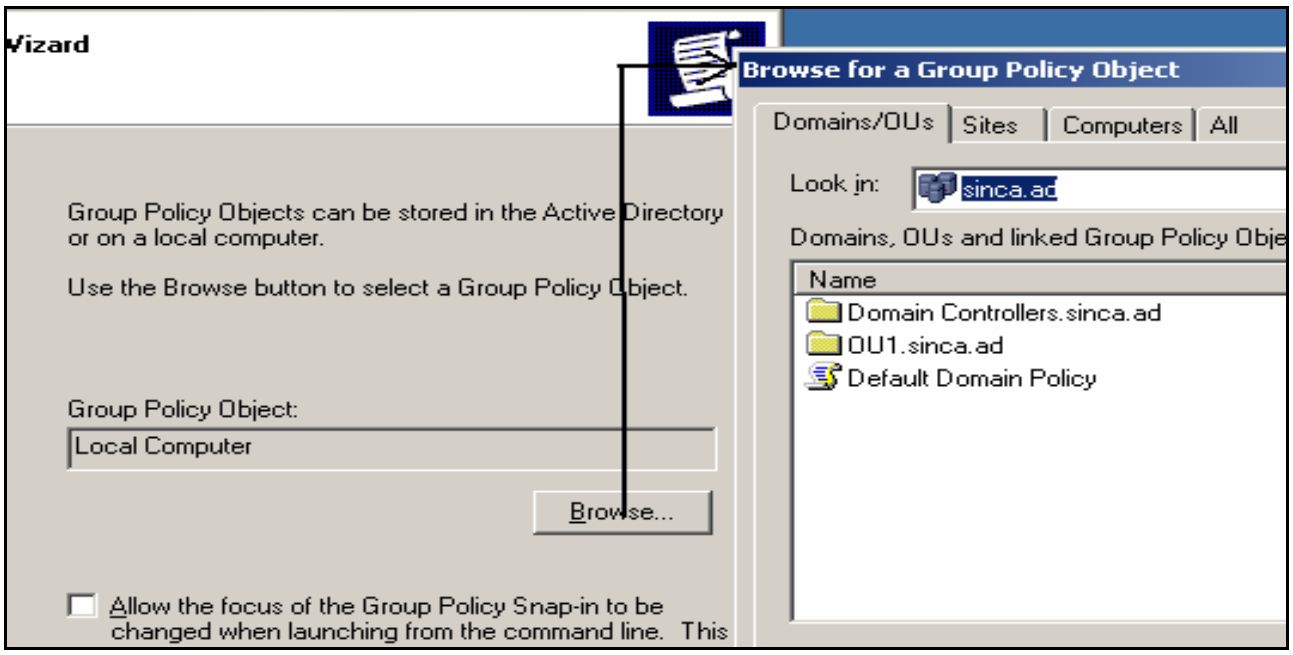
1.*Group Policy* pentru calculatorul local

În consola mmc (*Microsoft Management Console*) poate fi adus utilitarul ***Group Policy Object Editor.***

File→ Add/Remove Snap-in→Add şi din fereastra *Available Stand-alone Snap-ins* se alege *Group Policy Editor.*



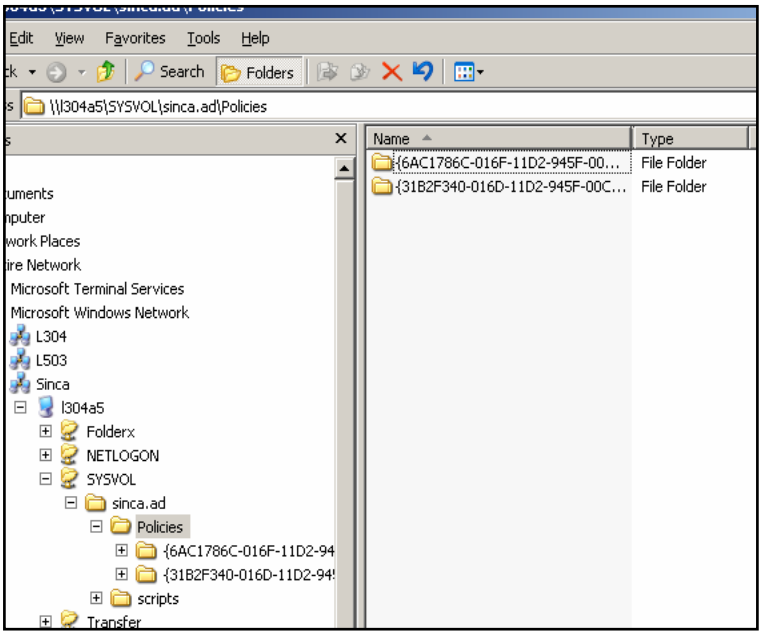
Dacă doriți să editați politica computerului local, alegeți opțiunea implicită ***Local Computer***. Altfel, pentru a modifica o politică de domeniu, faceți clic pe *Browse* pentru a identifica obiectul politică de grup (***Group Policy Object***) pe care îl doriți. Furnizați numele de utilizator şi parola dacă vi se solicită, apoi, când reveniți la caseta de dialog ***Select Group Policy Object***, faceți clic pe *Finish*.



Gpedit.msc este numele utilitarului pe care îl puteți folosi pentru editarea politicii locale, ***Local Group Policy.***

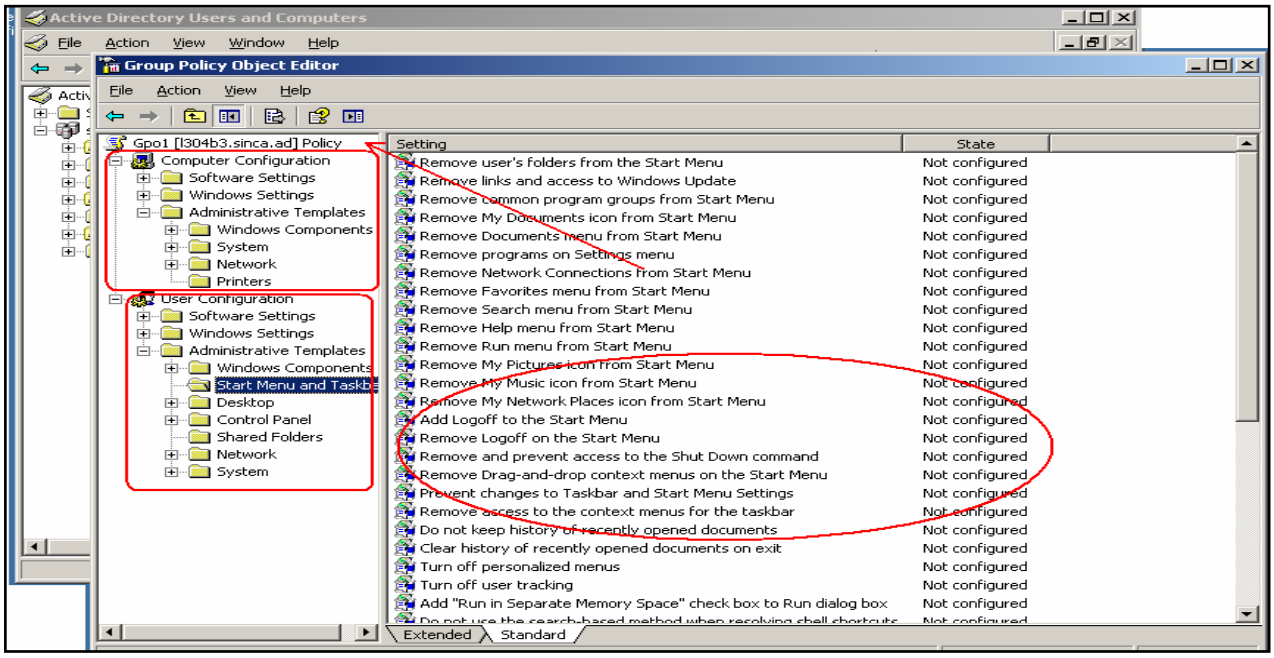
2. Obiectele *Group Policy* din *Active Directory*

Obiectele *Group Policy* din *Active Directory* sunt obiecte de un tip deosebit. Ele se prezintă sub forma a două componente separate, după cum urmează:



- Containerul *Group Policy Object* (GPO) este un obiect în *Active Directory.* Atributele acestui obiect includ numele GPO, permisiuni, respectiv cine poate modifica conținutul obiectului GPO şi informații de versiune.
- Macheta GPO (*template*), este un set de fişiere care se găsesc în folderul partajat *Sysvol*. Folderul partajat *Sysvol* există pe fiecare controler de domeniu, conținutul său fiind replicat între toate controlerele de domeniu din domeniu, prin intermediul serviciului *File Replication Service* (FRS).

Un obiect GPO conține informații de configurare pentru **calculator** şi pentru **utilizator**.



Un GPO poate fi asociat la nivel de site, domeniu şi unitate organizațională. Despre obiectele *group policy* se spune că sunt legate la nivelul *site*-ului, domeniului şi al unităților organizaționale.

Aplicarea unui obiect GPO la nivelul domeniului se traduce prin aceea că: (1) toate calculatoarele din domeniu vor fi afectate de configurările asociate în partea de *computer configuration* şi (2) toți utilizatorii care deschid sesiune în domeniu vor fi afectați de partea de configurare din *user configuration*. În situația în care un obiect GPO este legat la nivelul unei unități organizaționale vor fi afectate de configurările specifice: (1) calculatoarele din unitatea organizațională şi (2) utilizatorii care au conturi în unitatea organizațională.

Obiectele GPO sunt evaluate în ordinea următoare:

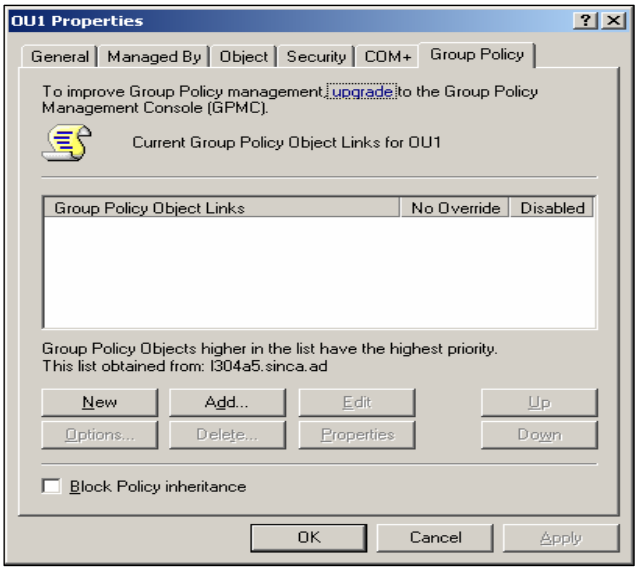
Local Policy → Site GPO → Domain GPO → OU GPO → Child OU GPO etc.

Există două căi de evaluare. Prima este cea în care se află obiectul de tip ***computer***. A doua este cea în care se află obiectul de tip ***user*** care va deschide sesiune pe acel computer. Ca parte a procedurii de autentificare, vor fi localizate în *Active Directory* mai întâi obiectul computer şi apoi contul utilizator al celui care deschide sesiunea. Cu alte cuvinte, la pornirea calculatorului se aplica întâi setările din politica locală (*local policy*) şi apoi componenta *computer configuration* din obiectele GPO legate, în ordine, de domeniu şi de unitățile organizaționale care reprezintă calea până la contul computer din *Active Directory*. La deschiderea de sesiune se vor aplica componentele *user configuration,* în ordine, din politica locală (*local policy*) şi din obiectele GPO legate la nivelul domeniului şi al unităților organizaționale care fac parte din calea până la contul de utilizator folosit la deschiderea de sesiune.

Aplicarea în succesiune a politicilor GPO poate conduce la suprascrierea (modificarea) configurărilor anterioare. In această situație ultima valoare va fi cea care se va aplica.

Valorile folosite pentru configurarea opțiunilor din obiectele GPO sunt *Enable* (permis), *Disable* (nepermis, dezactivat) şi *Not Defined* (nedefinit, nici permis, nici nepermis).

Valoarea finală a unei opțiuni este calculată în modul următor: pentru valori de tipul *single value.* de genul *enable* sau *disable* se realizează suprascrierea. Pentru valori de tipul *multiple value,* cum sunt *logon script* sau instalare de software, se iau in considerare toate valorile care se cumulează.

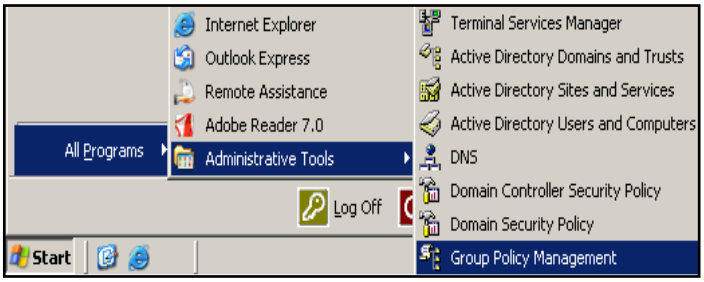


Crearea, gestionarea şi controlul asupra aplicării obiectelor GPO în domeniu se face cu ajutorul utilitarului ***Active Directory Users and Computers.*** Printre proprietățile unei unități organizaționale se află şi ***Group Policy***.

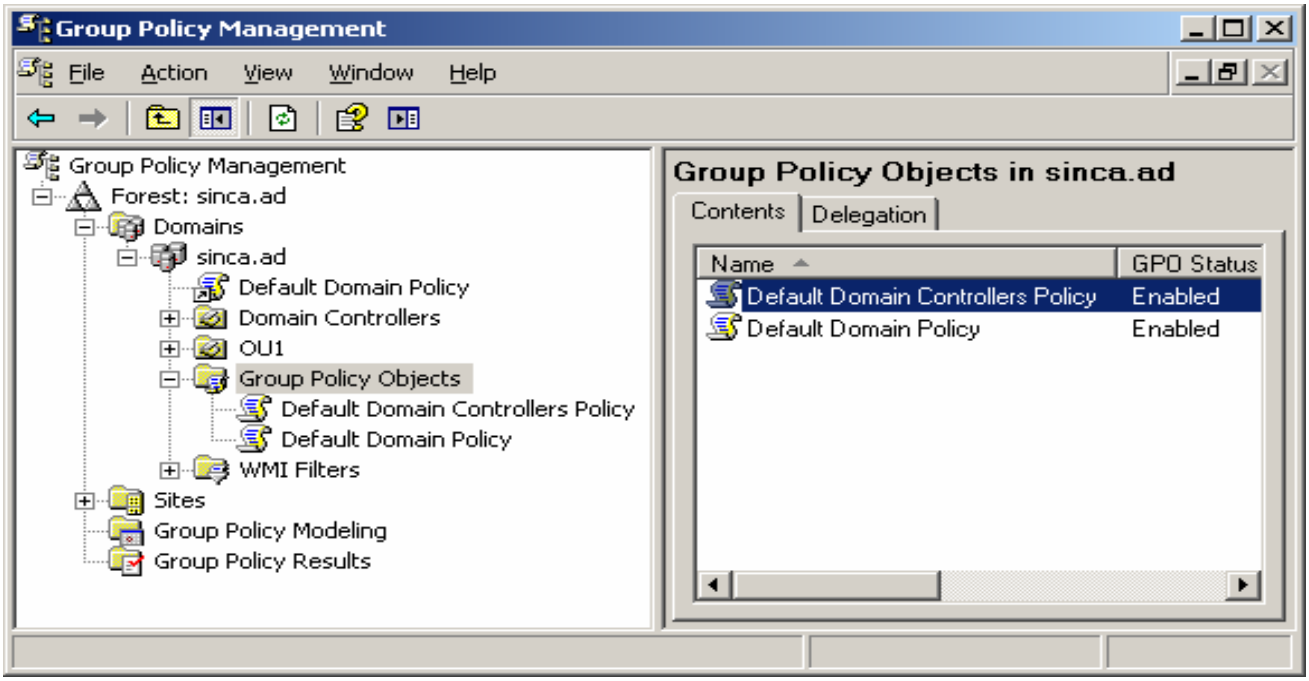
Obiectele GPO legate la nivelul *site*-ului sunt create, gestionate, controlate folosind utilitarul ***Active Directory Sites and Services.***

Utilitarul specializat pentru managementul obiectelor *Group Policy* se numeşte ***Group Policy Management Console*** **(GPMC).** Deşi nu este inclus în *kit*-ul de instalare *Windows Server 2003,* este utilitarul recomandat pentru crearea, gestionarea şi controlul aplicării politicilor construite prin obiecte GPO. Poate fi descărcat de pe *site*-ul *Microsoft,* eventual de la următoarea adresă:

http://www.microsoft.com/downloads/details.aspx?familyid=0A6D4C24-8CBD-4B35-9272-DD3CBFC81887&displaylang=en



În urma instalării, se creează o intrare în *Administrative Tools* numită ***Group Policy Management.***

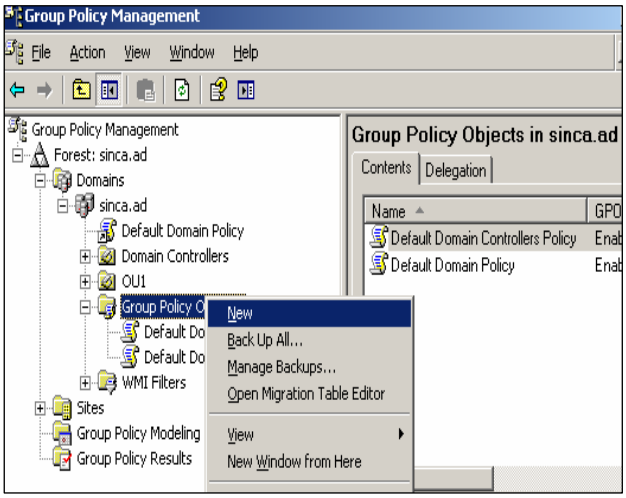


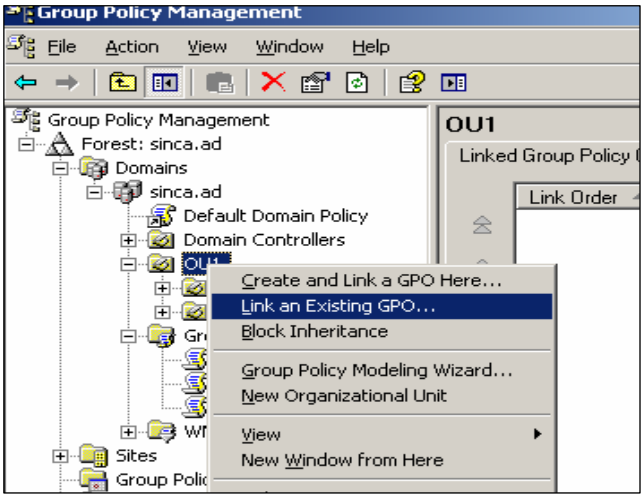
Fereastra *Group Policy Management Console* (GPMC - consola pentru managementul *grup policy*) prezintă structura *Active Directory* şi obiectele *group policy* existente.

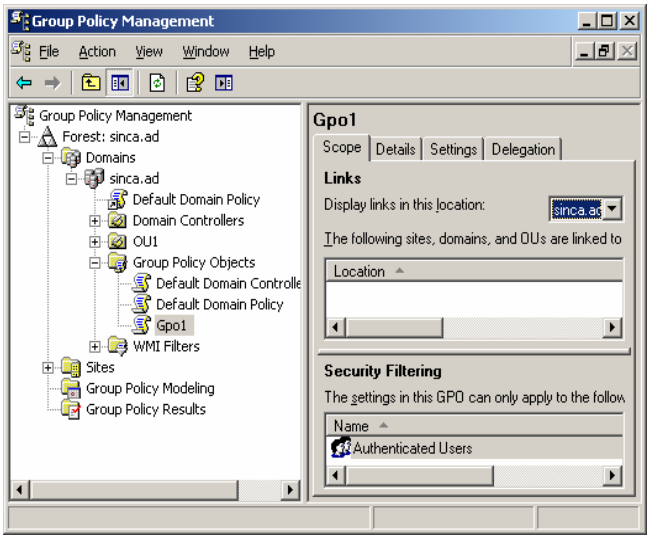
În mod implicit, în urma creării unui domeniu, sunt construite două politici

speciale: o politică aplicată domeniului şi una aplicată containerului – de tip OU – *Domain Controllers*, containerul în care se găsesc controlerele de domeniu. Constatăm deci, că există o politică implicită aplicată tuturor calculatoarelor şi tuturor utilizatorilor din domeniu. În plus, numai asupra controlerelor de domeniu este aplicată şi o politică suplimentară.

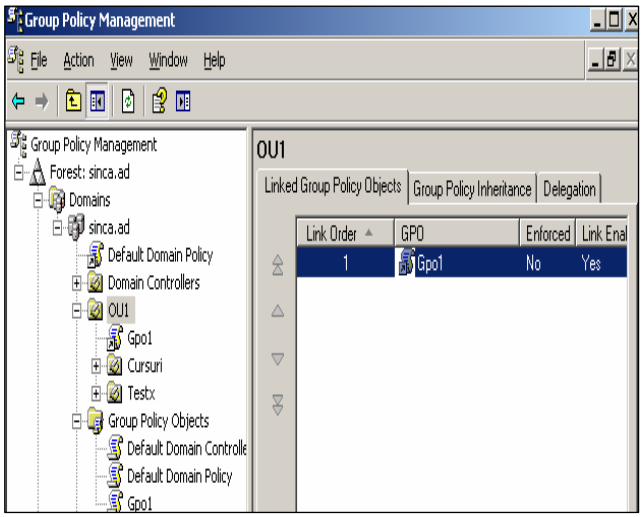
Crearea (construirea) unui obiect GPO şi legarea unuia existent sunt operații distincte. Aşa cum se poate observa din ferestrele următoare:



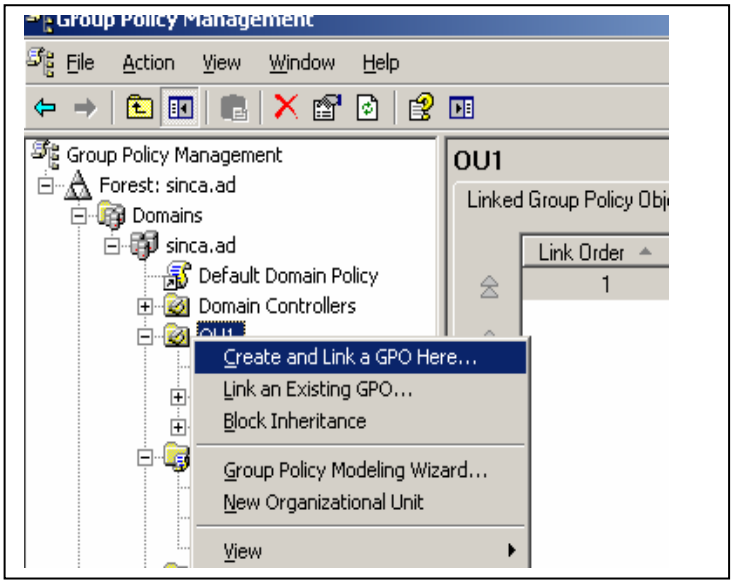




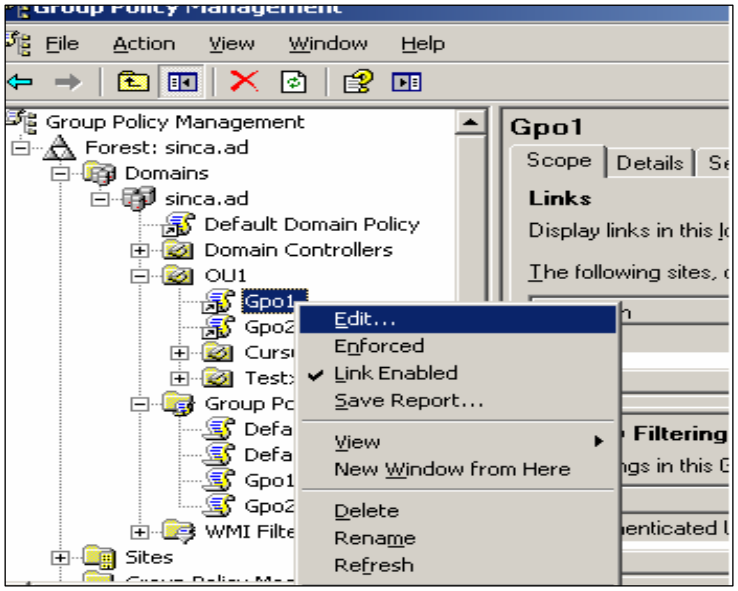
Gpo1 este, în exemplul nostru, numele noului obiect creat. Pentru a fi aplicat el va trebui legat (*link*). Un obiect GPO se poate afla în una dintre următoarele stări: legat sau nelegat. Acelaşi obiect GPO poate fi legat la mai multe unități organizaționale.



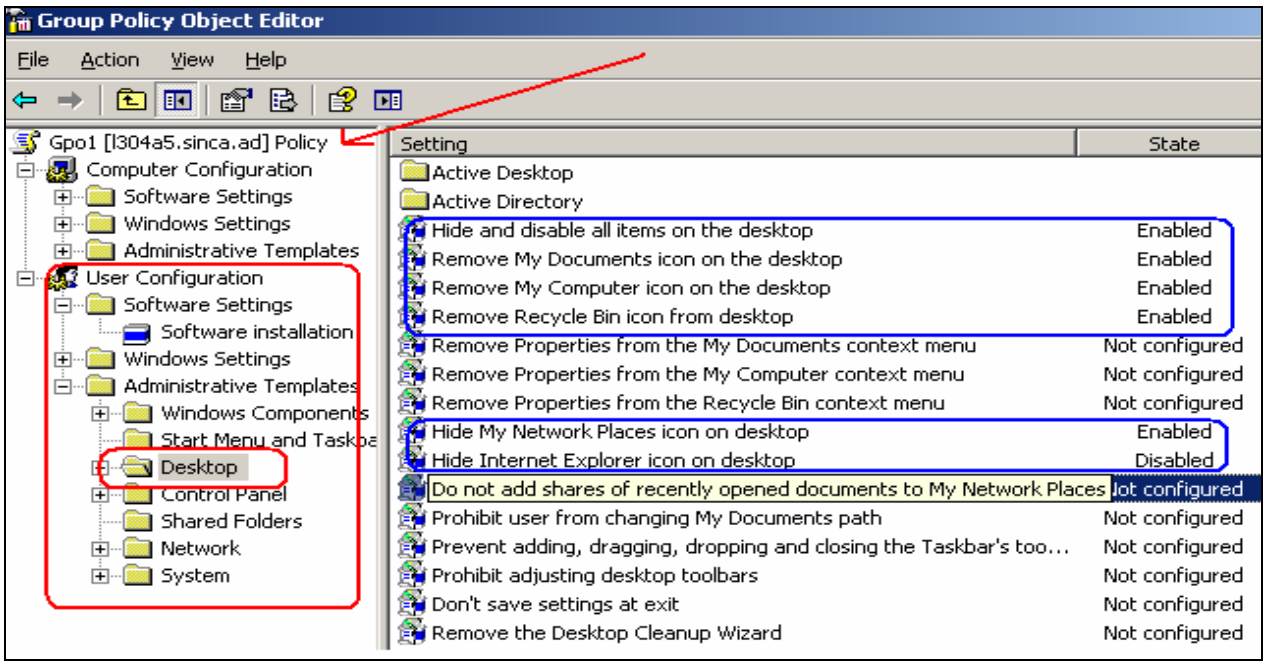
În exemplul nostru, obiectul *Gpo1* a fost legat de unitatea organizațională OU1.



Utilitarul GPMC permite însă, concomitent, crearea şi legarea obiectului GPO, dacă se începe prin alegerea unității organizaționale unde va fi legat, deci unde va fi aplicat noul obiect creat

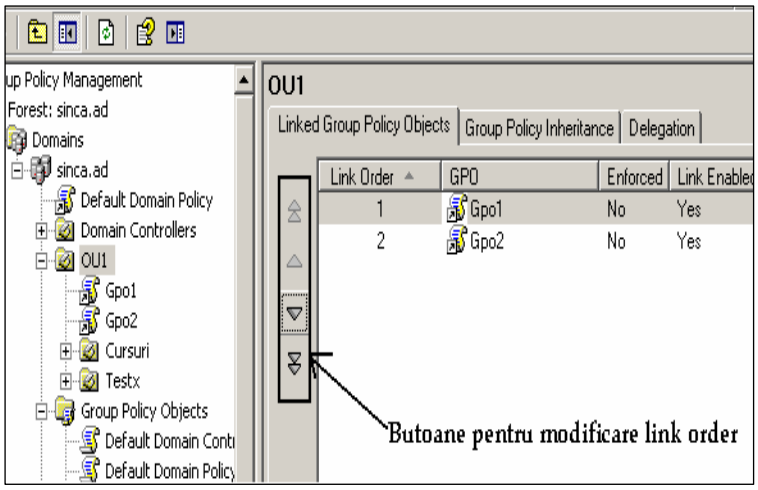


Imediat ce au fost create obiecte GPO, ele se constituie din machete de informații în care însă nu este nimic configurat. Configurarea conținutului obiectului, respectiv configurările pentru componentele *Computer configuration* şi *User configuration* vor fi efectuate prin comanda *Edit* (editare, modificare).



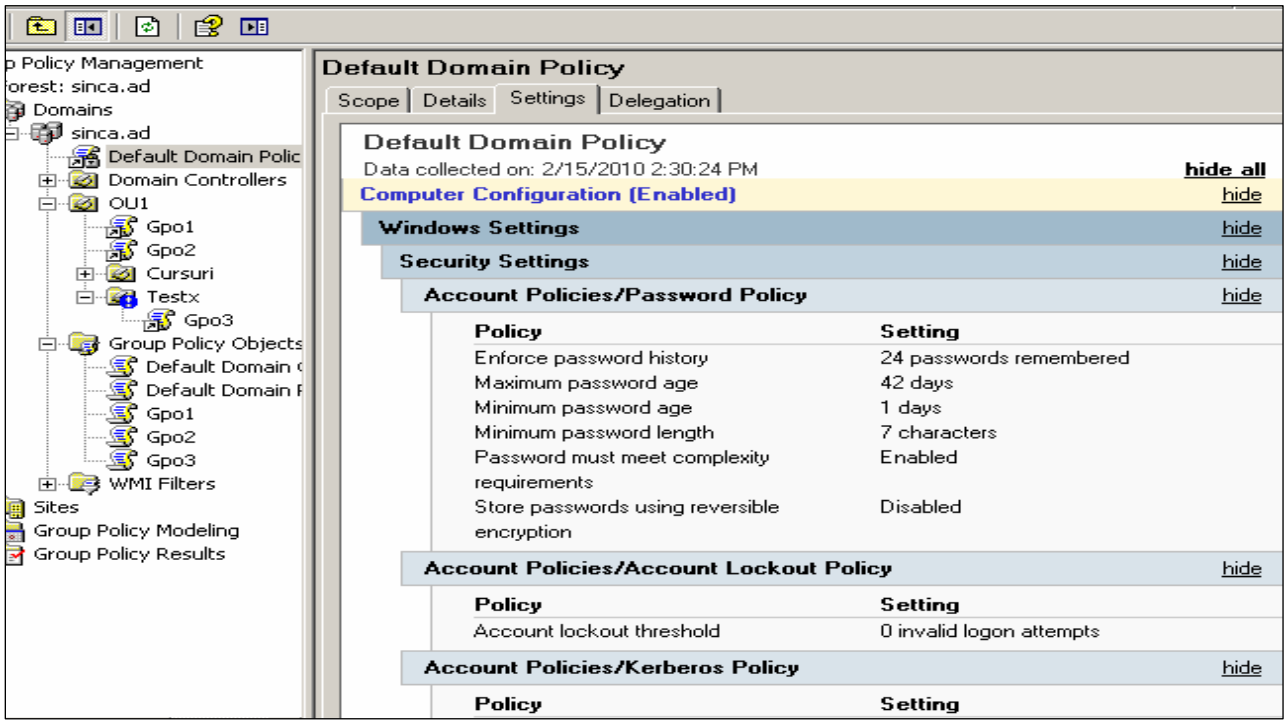
Să examinăm fereastra de mai sus. Numele ferestrei este *Group Policy Object Editor,* ceea ce înseamnă că în această fereastră se pot stabili configurările pentru componentele *computer configuration* şi *user configuration*. Obiectul GPO supus examinării se numeşte *Gpo1* şi ceea ce examinăm acum este conținutul obiectului aşa cum se găseşte în exemplarul de la controlerul de domeniu *l304a5.sinca.ad*, numele domeniului fiind *sinca.ad*. Componenta *User configuration* este cea în care por fi stabilite condițiile deosebite ale mediului de operare al utilizatorilor. Pentru moment se face referire la ecranul *desktop*. Conform acestora, utilizatorul căruia i se va aplica politica *Gpo1* va avea – după deschiderea de sesiune – o imagine *desktop* pe care nu mai apare nicio pictogramă.

Există situații în care la aceeaşi unitate organizațională sunt legate două sau mai multe obiecte GPO. Ordinea în care vor fi aplicate aceste obiecte este foarte importantă.



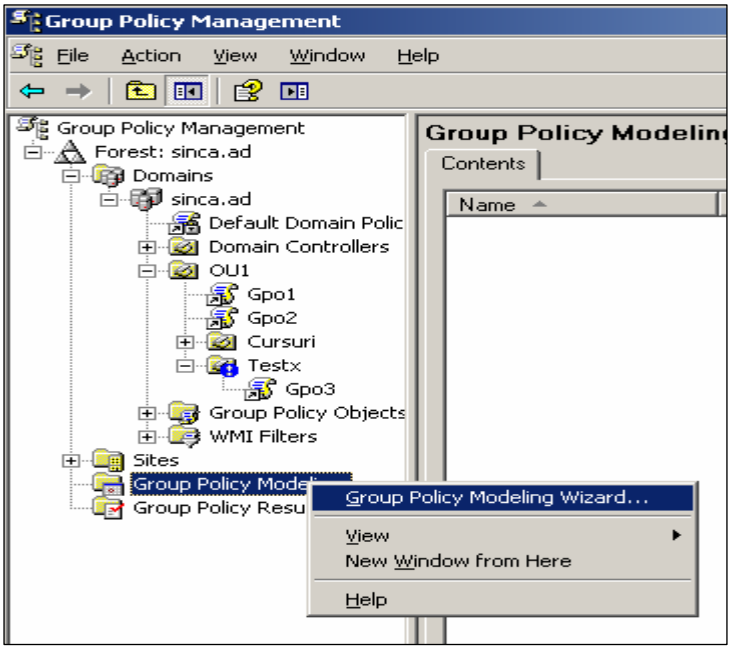
Imaginea alăturată indică două obiecte **GPO** legate la unitatea organizațională *OU1***.** Ordinea aplicării este de jos în sus: întâi se va aplica *Gpo2* şi apoi *Gpo1*. Obiectul *Gpo1* este mai prioritar decât celălalt şi se aplică ultimul.

Utilitarul GPMC conține şi o componentă prin care pot fi vizualizate configurările (setările) existente într-un obiect GPO. *Tab*-ul folosit este *Settings* după ce a fost ales obiectul pentru care se doreşte vizualizarea conținutului.

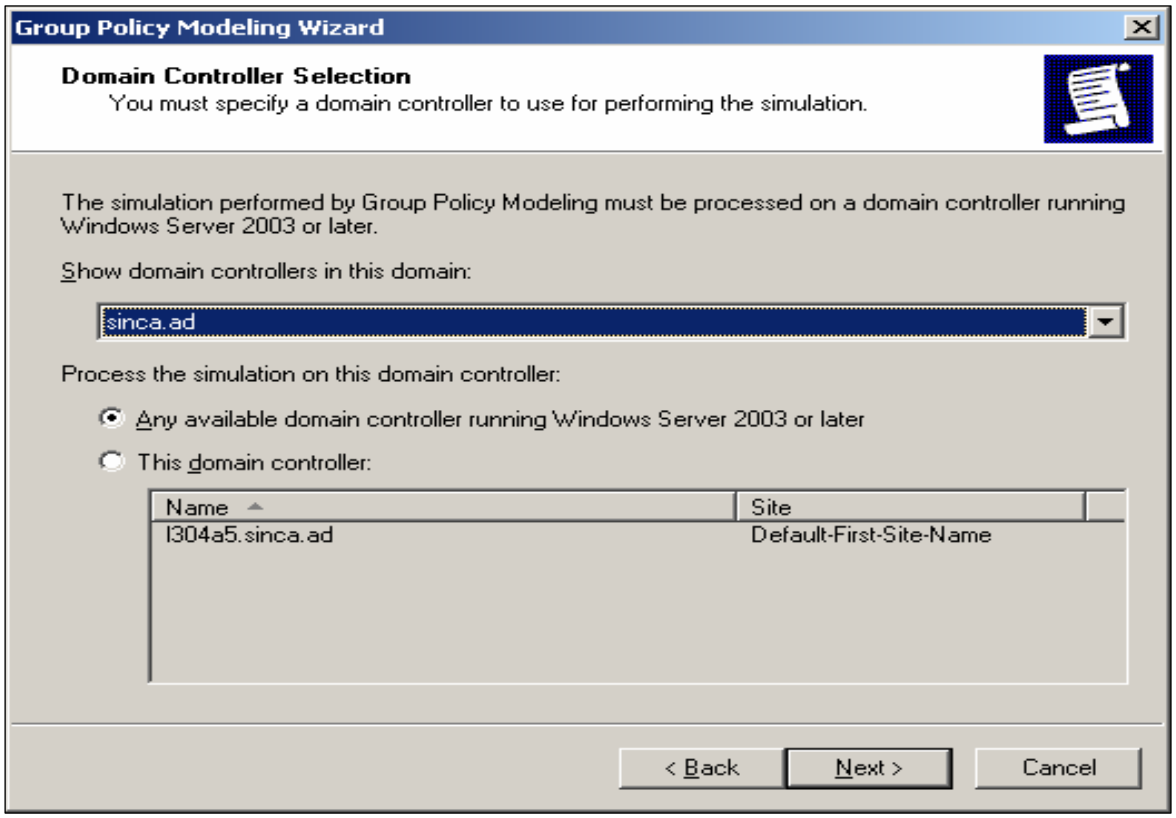


Group Policy Modeling este componenta care permite simularea aplicării setărilor GPO pentru utilizatori şi computere, înainte de implementarea efectivă a politicii conținute de obiectul respectiv.

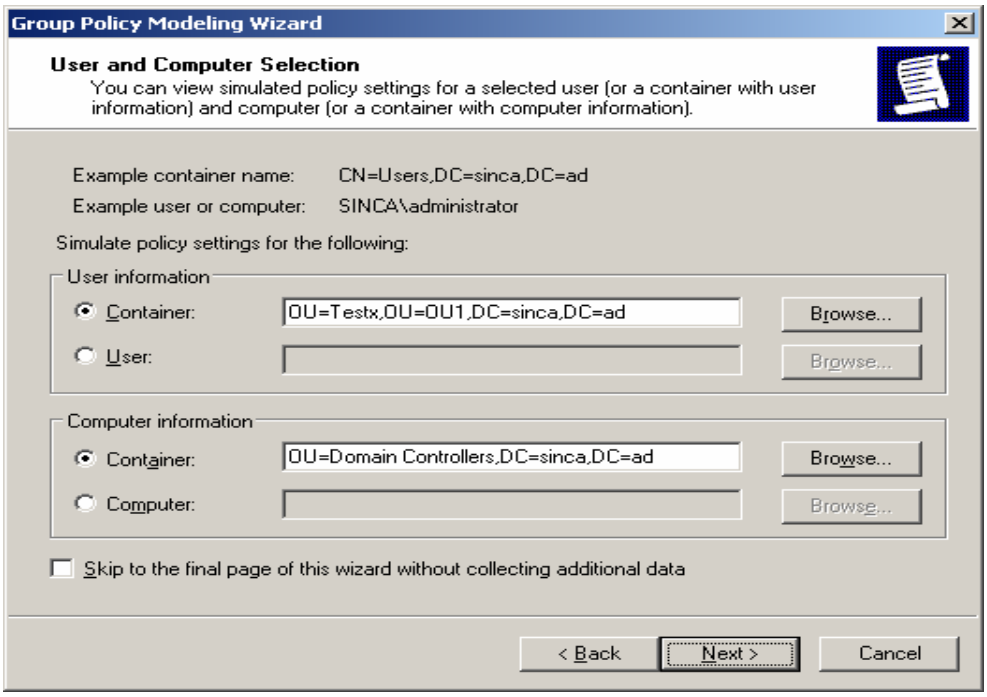
Group Policy Management→Group Policy Modeling→click dreapta→Group Policy Modeling Wizard→Next



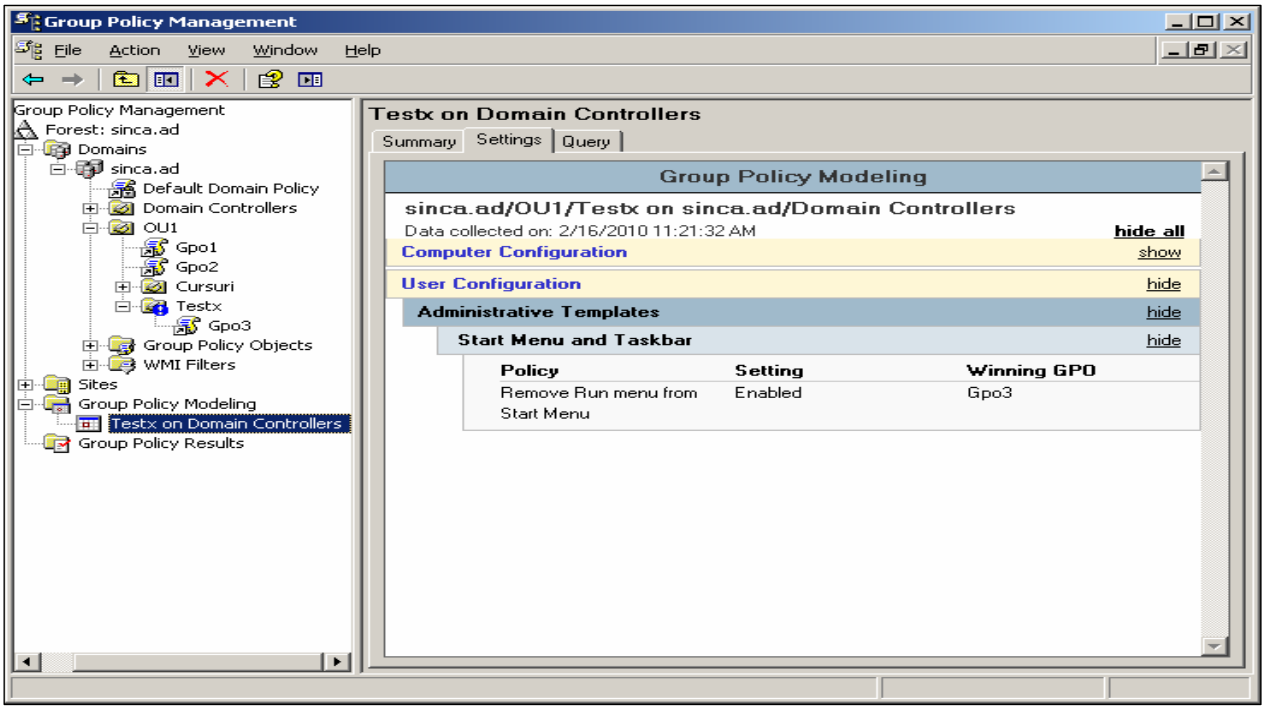
Va fi ales în continuare controlerul de domeniu pe care se va executa procedura de simulare. Trebuie să fie un controler de domeniu unde este instalat un sistem de operare *Windows Server 2003*.

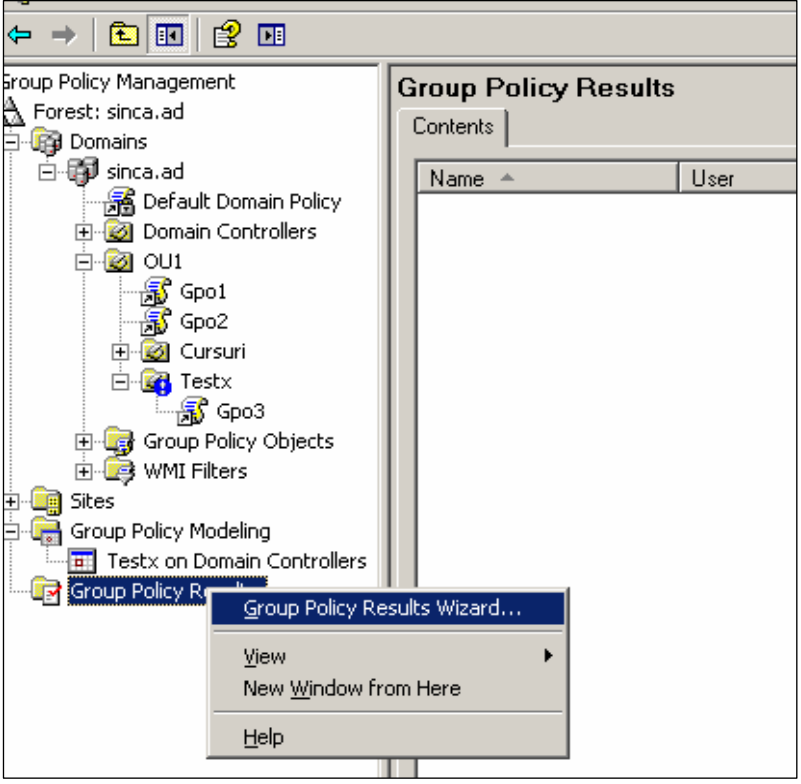


Urmează alegerea contextului în care va avea loc simularea: pentru ce utilizator din domeniu şi pentru ce calculator. Se poate specifica în clar atât utilizatorul cât şi calculatorul sau, pentru oricare dintre aceste obiecte se poate specifica containerul unde se află obiectele pentru care se simulează efectele aplicării configurărilor.



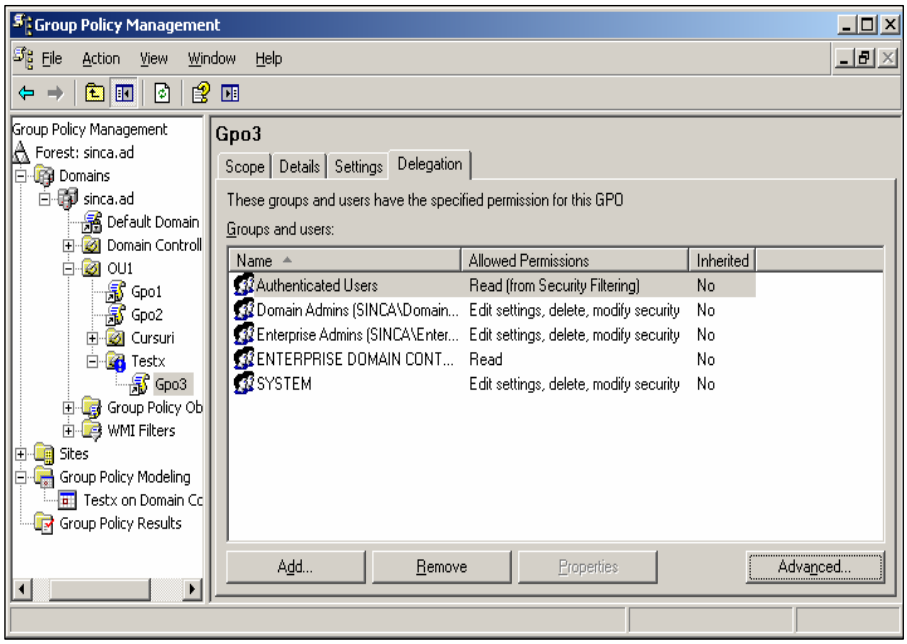
Urmează câteva referiri la *site* şi în final vor fi specificate grupurile din care fac parte conturile utilizator şi computer pentru care se face simularea. *Tab*-ul *Settings* oferă rezultatele simulării.





Group Policy Results este componenta folosită pentru vizualizarea rezultatelor. Formatul de prezentare este similar ce cel de la *Group Policy Modeling.* De data aceasta însă rezultatele sunt cele reale nu simulate. Sunt prezentate deci, efectele, rezultatele aplicării obiectelor GPO construite şi legate anterior. Pe calculatoarele pentru care se vor afişa rezultatele trebuie să fie instalate sisteme de operare *Windows XP* sau *Windows Server 2003*.

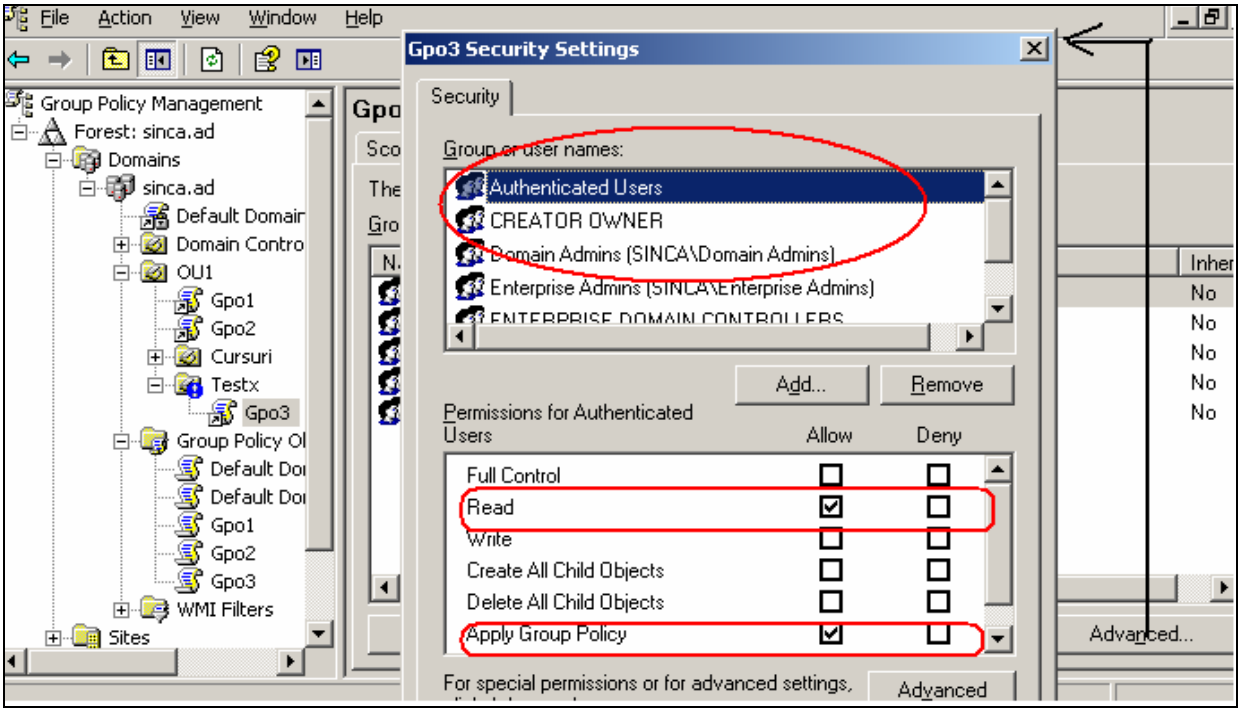
Când un utilizator porneşte un calculator şi deschide sesiune în domeniu, vor fi procesate pe rând, setările GPO asociate computerului şi apoi cele pentru utilizator. Din timp în timp însă, aceste setări vor fi reîmprospătate, reaplicate. Pentru calculatoarele membre ale domeniului reîmprospătarea are loc la intervale prestabilite. Intervalul implicit este de 90 de minute cu abateri (plus sau minus) de maxim 30 de minute. Controlerele de domeniu au un regim diferit: reîmprospătarea are loc din 5 în 5 minute. Administratorii de domeniu pot forța aplicarea (împrospătarea) politicilor prin comanda ***gpupdate*.**



În mod implicit, toate setările din obiectele GPO legate la un container se aplică tuturor utilizatorilor şi computerelor din acel container. Dacă intenția administratorului de domeniu este ca politicile să se aplice numai anumitor utilizatori sau anumitor calculatoare, atunci vor intra în operă procedurile de filtrare, prin care vor fi selectate numai acele calculatoare şi, respectiv, acei utilizatori cărora trebuie să li se aplice politica. Filtrele sunt construite folosind *tab*-ul *Delegation* pentru fiecare obiect GPO în parte.

Filtrele sunt de fapt permisiuni acordate calculatoarelor şi utilizatorilor pentru acel GPO. Pentru ca setările dintr-un obiect GPO să se aplice unui cont utilizator sau unui cont de calculator, conturile trebuie să aibă permisiunile ***Read*** **(**citire**)** şi ***Apply Group Policy*** (aplică politica de grup) pentru acel GPO. În mod implicit grupul ***Authenticated Users*** dispune de permisiunile ***Read*** şi ***Apply Group Policy*** pentru orice GPO din domeniu.

Butonul ***Advanced*** rafinează informațiile despre permisiunile necesare conturilor, în vederea aplicării conținutului configurărilor din obiectul GPO.



Replicarea *Active Directory*

Serviciul *Active Directory Service* funcționează pe baza informațiile stocate pe controlerele de domeniu. Pentru existența unui domeniu este nevoie de un controler de domeniu. Într-un domeniu pot funcționa unul sau mai multe controlere de domeniu. Fiecare controler de domeniu deține un exemplar al bazei de date *Active Directory*. Modificările efectuate într-un exemplar vor fi sincronizate cu celelalte exemplare *Active Directory*, în aşa fel încât toate exemplarele de pe toate controlerele din domeniu să fie identice. Operația de sincronizare a exemplarelor *Active Directory* este o replicare multi-master. Fiecare controler de domeniu deține un exemplar master al domeniului, adică fiecare exemplar poate fi modificat, prin crearea şi ştergerea de obiecte, prin modificarea valorilor asociate proprietăților (atributelor) unui obiect. Din timp în timp modificările survenite într-un exemplar vor fi transmise celorlalte controlere de domeniu.

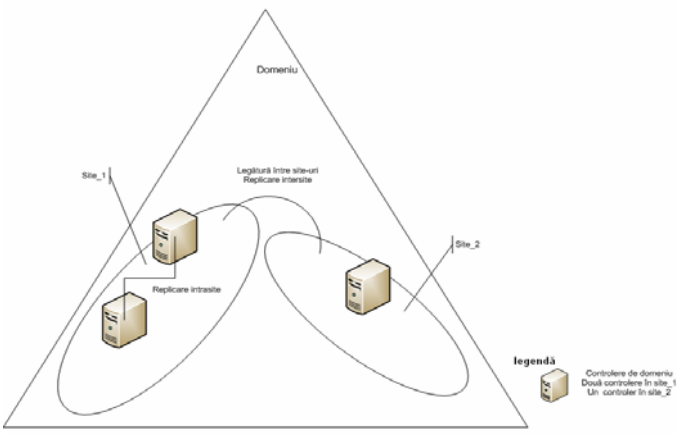
Baza de date *Active Directory* este împărțită, separată din punct de vedere logic în partiții. Fiecare partiție este o unitate de replicare şi poate avea propria topologie de replicare.

Partițiile *Active Directory* sunt:

- *schema partition* (partiția schemă) - conține definițiile tuturor obiectelor şi atributele acestora precum şi regulile pentru crearea şi manevrarea obiectelor. Într-un *forest* există o singură schemă şi ea este stocată pe toate controlerele de domeniu din *forest.* În acest fel, toate obiectele din *forest* vor respecta aceleaşi reguli de creare, modificare şi manevrare.
- *configuration partition* (configurare) - conține informații despre structura fizică la nivel de *forest*. Sunt indicate domeniile din *forest*, unde se află şi cum pot fi localizate controlerele de domeniu din *forest*, serviciile pe care le pot oferi controlerele de domeniu. Fiecare controler de domeniu deține un exemplar al partiției configurare.
- *domain partition* (partiția domeniului) - conține toate obiectele acelui domeniu: utilizatori, grupuri, computere, unități organizaționale şi încă multe altele. Fiecare domeniu are propria partiție de tip domeniu. Fiecare controler deține un exemplar al propriei partiții domeniu.
- *application partition* (partiția aplicație) – sunt stocate aici informații despre aplicații. Unele aplicații pot stoca informații în *Active Directory*. Un exemplu este serviciul DNS care îşi poate păstra informații în *Active Directory*.

Partițiile schemă şi configurarea sunt replicate pe toate controlerele de domeniu din *forest*. Partițiile de domeniu sunt replicare numai între controlerele din acelaşi domeniu.

Legătura dintre structura logică *Active Directory* şi structura fizică a rețelei se obține prin folosirea conceptului şi a obiectului *site*. Obiectul *site* din *Active Directory* descrie aşezarea fizică, geografică a rețelelor care găzduiesc resursele descrise prin obiecte din *Active Directory*. *Site*-urile conțin obiecte numite subrețele (*subnets*). Obiectele *site* sunt folosite în legătură cu obiectele *Group Policy*, uşurează descoperirea resurselor, controlează replicarea *Active Directory* şi gestionează traficul în rețea. *Site*-urile pot fi legate unele de altele prin aşa-numitele legături între *site*-uri (*site link*). Din punct de vedere fizic un *site* constă în general din una sau, eventual, mai multe subrețele interconectate la viteză mare în care funcționează servere controlere de domeniu.



Replicarea *Active Directory* poate avea loc, de la caz la caz, între controlere de domeniu care aparțin aceluiaşi *site* – situație în care vorbim despre replicarea în interiorul *site*-ului *(intrasite)* – sau între controlere care aparțin de *site*-uri diferite – situație în care are loc replicare între *site*-uri *(intersite)*.

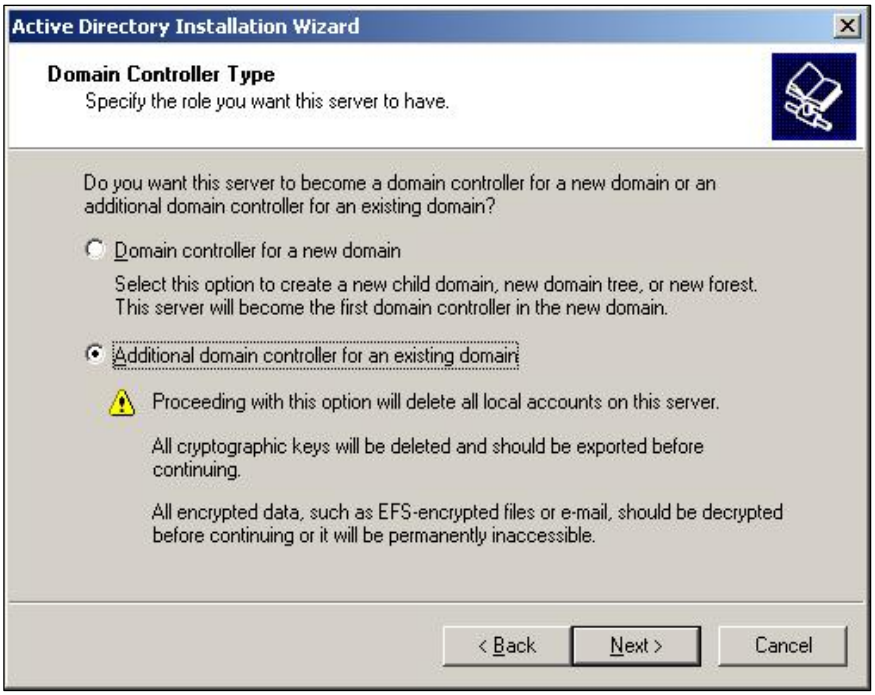
Replicarea în interiorul aceluiaşi *site* porneşte de la presupunerea că legăturile dintre controlere sunt sigure, de viteză mare şi permanent disponibile. Traficul de replicare nu este comprimat şi se realizează prin „*change notification*”, partenerii de replicare fiind anunțați imediat sau aproape imediat de producerea replicării.

Replicarea între *site*-uri presupune că legăturile dintre *site*-uri nu sunt sigure, sunt de viteză mică şi nu sunt disponibile permanent. Traficul de replicare este comprimat, nu este transmis pe măsura apariției modificărilor ci în conformitate cu un orar stabilit de către administratori.

Topologia de replicare (*replication topology*) este calea prin care se desfăşoară traficul de replicare în rețea. Topologia de replicare se referă la controlerele care comunică direct între ele, două câte două. Fiecare partiție *Active Directory* are propria topologie de replicare.

Instalarea unui controler de domeniu suplimentar

Întrucât funcționarea *Active Directory* se bazează în mod esențial pe serviciul DNS, pentru instalarea unui controler de domeniu adițional, serverul care va deține acest rol trebuie să fie client al serverului DNS care deține domeniul DNS asociat domeniului *Active Directory* sau care poate rezolva numele în specificator DNS al domeniului *Active Directory*.

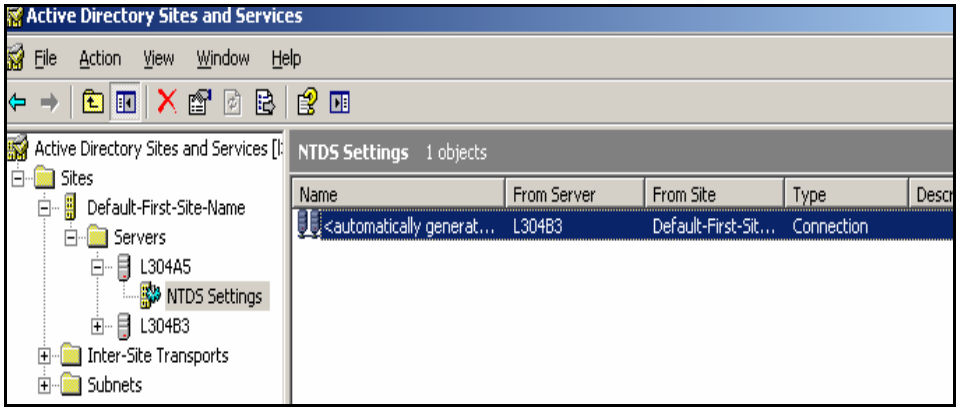


Comanda folosită pentru instalarea controlerului adițional de domeniu este ***dcpromo***.

Vor fi specificate în continuare numele şi parola pentru contul de utilizator care poate instala serviciul *Active Directory Service*.

Pentru că este vorba despre instalarea unui controler de domeniu într-un domeniu existent, se alege opțiunea ***Additional domain controller for an existing domain*** (controler de domeniu suplimentar pentru un domeniu existent). Opțiunile şi ferestrele sunt similare cu cele de la instalarea primului controler de domeniu.

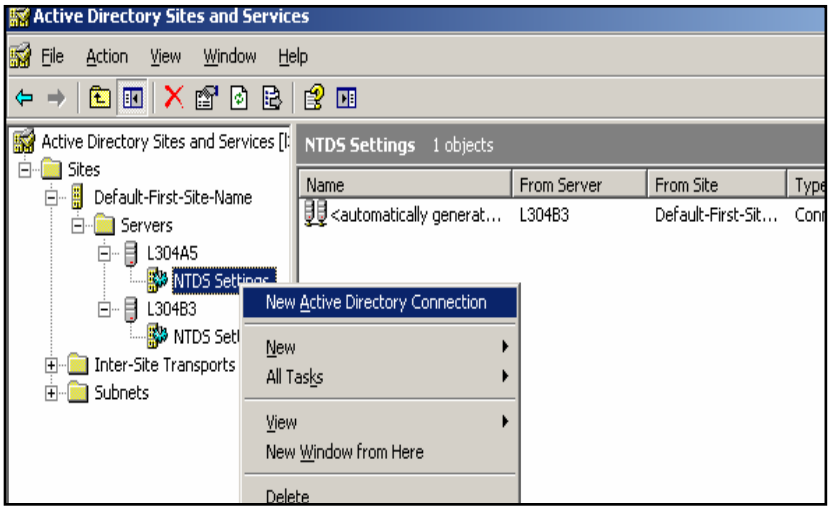
Utilitarul ***Active Directory Sites and Services*** *(Site*-uri şi servicii *Active Directory),* aflat în *Administrative Tools,* poate fi folosit pentru identificarea controlerelor de domeniu, a *site*-urilor şi pentru verificarea efectuării replicării între controlerele de domeniu.

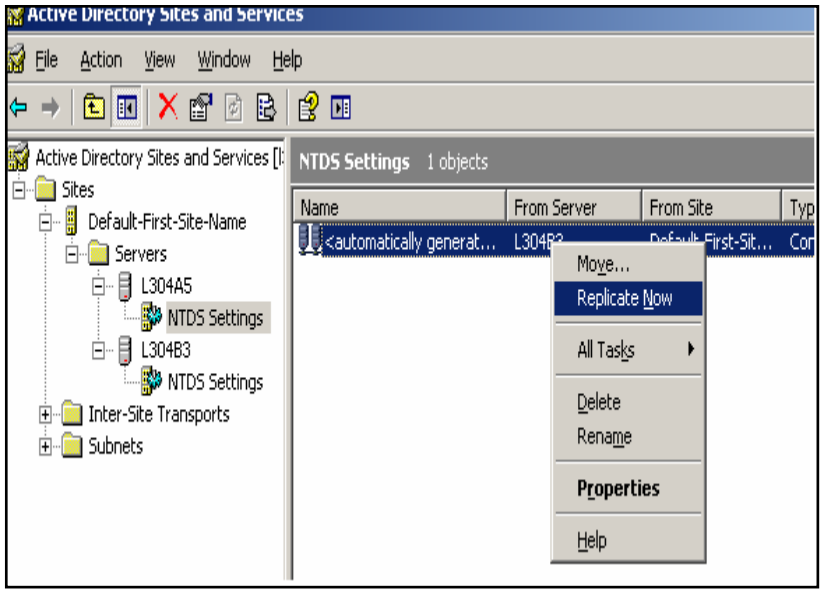


În fereastra de mai sus remarcăm:

- Site-ul implicit – *Default-First-Site-Name.*
- Containerul *Servers* unde sunt plasate servere NTDS (controlerele de domeniu).
- Obiectele de tip conexiune (*connection*) fac legătura între controlerele între care există activitate de replicare. Cele două controlere de domeniu deţin fiecare câte un exemplar master al domeniului. Oricare dintre aceste exemplare poate fi modificat. Modificările efectuate pe un exemplar vor fi transmise către partenerul de replicare prin această conexiune. În interiorul aceluiaşi *site* obiectele de tip conexiune sunt generate automat, în conformitate cu topologia de replicare construită automat de componentele sistemului de operare. Replicarea *intrasite* va fi la rândul ei automată.

Conexiunile pot fi însă construite şi manual.



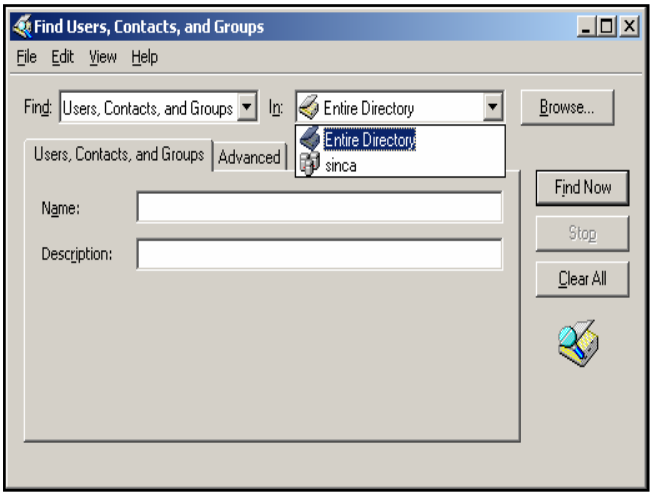


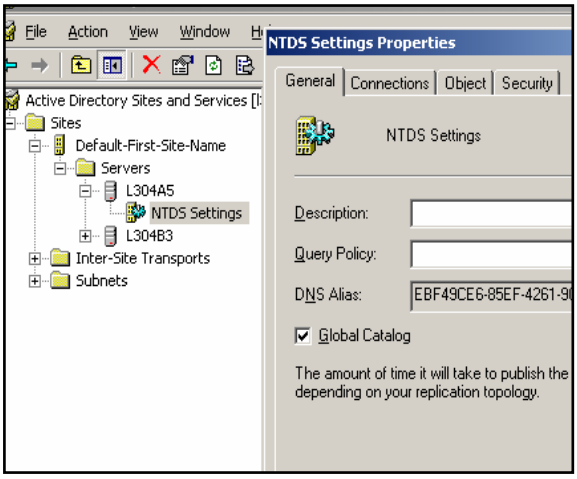
Replicarea automată poate fi înlocuită cu replicarea la cerere, folosind comanda ***Replicate Now*** (Replicare acum)***.***

Serverul Catalog Global

Serverul Catalog Global este un controler de domeniu care, pe lângă partițiile obişnuite, mai deține şi exemplare de tip *read-only* (numai citire) ale tuturor partițiilor de tipul *domain* din *forest*. Exemplarul propriului domeniu este integral, în schimb pentru celelalte domenii exemplarele sunt *read-only* şi sunt parțiale. Exemplarele parțiale conțin toate obiectele din domeniu, însă nu cu toate atributele.

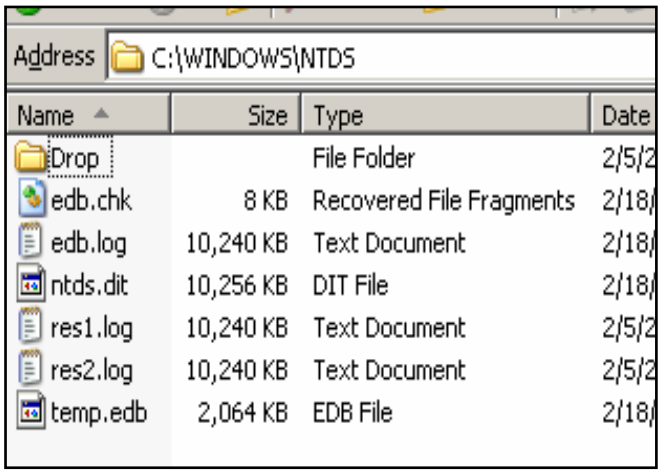
Serverele catalog global sunt folosite pentru căutarea şi găsirea obiectelor în ierarhia de domenii din *forest*. Căutările efectuate în întregul *Active Directory* (*Entire Directory)* au loc în catalogul global. Primul controler de domeniu din *forest* devine implicit şi server catalog global. Rolul de server catalog global poate fi modificat prin ***Active Directory Sites and Services.***





Salvarea şi restaurarea *Active Directory*

Active Directory conține următoarele fişiere, a căror locație este stabilită la instalare (implicit folderul %systemroot%\NTDS).



- ***Ntds.dit*** - baza de date care stochează toate obiectele *Active Directory*.. Extensia **.dit** înseamnă "*directory information tree*".
- ***Edb.log*** - fişierul jurnal de tranzacții (*transaction log*) folosit de această bază de date. Dimensiunea maximă a acestui fişier este de 10M.
- ***Edb*.log*** – când fişierul Edb.log atinge dimensiunea maximă, el va fi redenumit **Edbnnnnn.log,** unde nnnnn este un număr care va fi succesiv incrementat.
- ***Edb.chk –*** fişierul de tip *checkpoint*, folosit pentru a identifica până unde au fost efectuate tranzacțiile în baza de date.
- ***Res1.log , Res2.log –*** fişiere rezervate pentru *transaction log*; fiecare are câte 10M; spațiul ocupat de ele va fi alocat fişierului *transaction log* în cazul în care nu mai există spațiu pe disc.

Salvarea bazei de date *Active Directory* se realizează prin lansarea la controlerul de domeniu a utilitarului *Backup* procedura *System State* (starea sistemului).

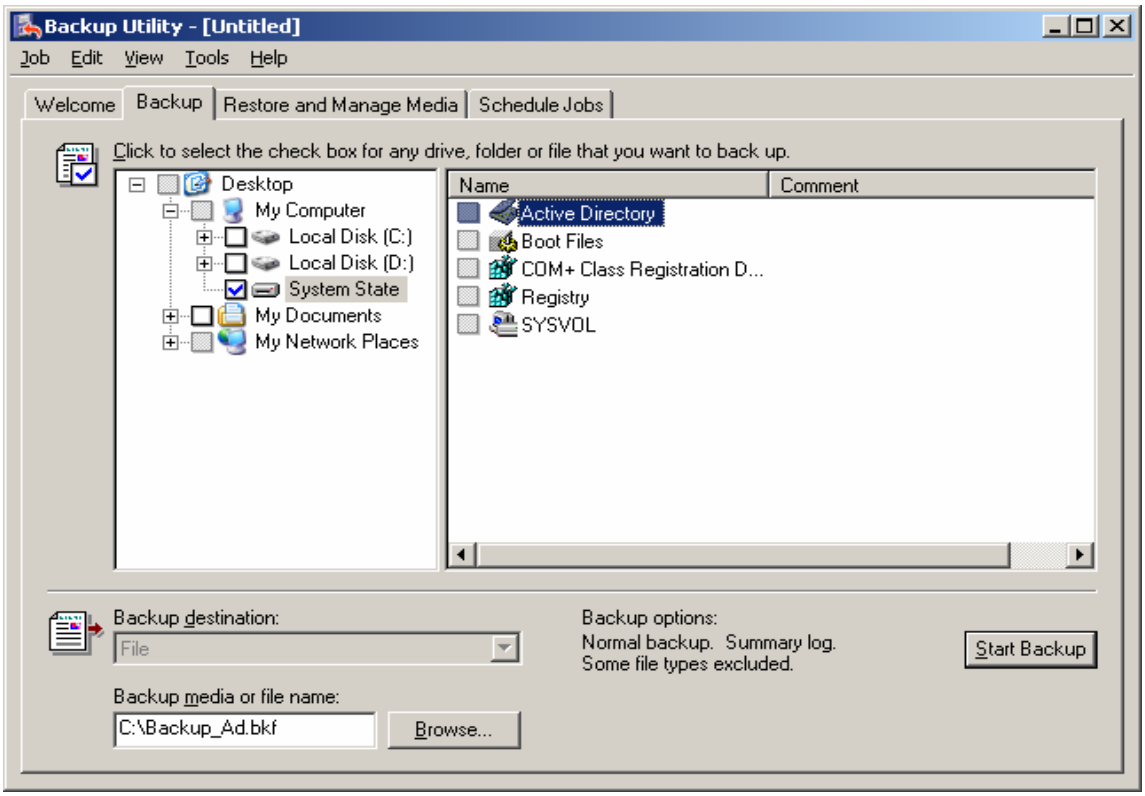
Componentele *System State* pentru controlerele de domeniu sunt următoarele:

- ***Active Directory***
- ***folder*-ul partajat *SYSVOL***

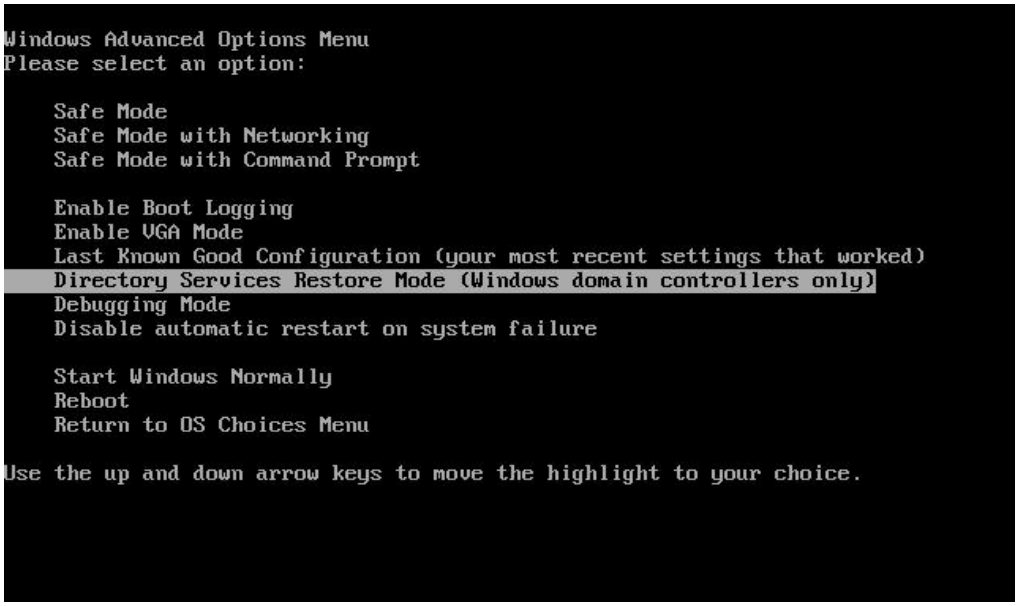
- ***Registry***
- ***System startup files***
- ***COM + Class Registration database***
- ***Baza* de date pentru *Certificate Services* –** numai în cazul în care este instalat serviciul *Certificate Services* pe controlerul de domeniu

Start→All Programs→Accessories→System Tools→Backup, modul Advanced Mode tab-ul Backup

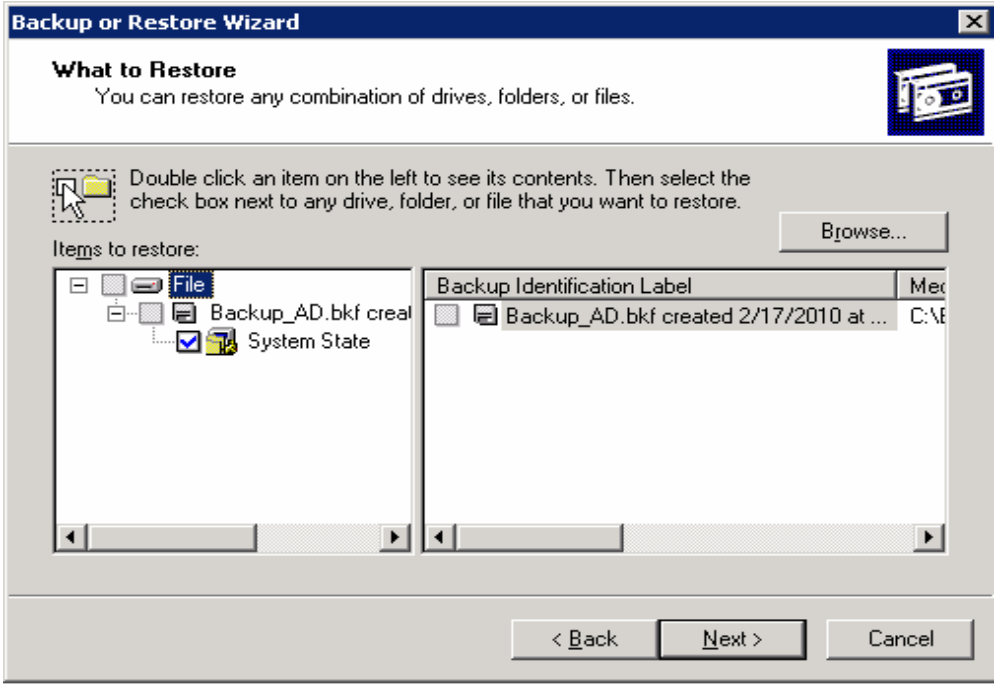
Alegem pentru salvare ***System State*** şi locația unde va fi salvat fişierul.



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 obține prin apăsarea tastei F8 la startarea serverului şi alegând din meniu intrarea cu acelaşi nume.

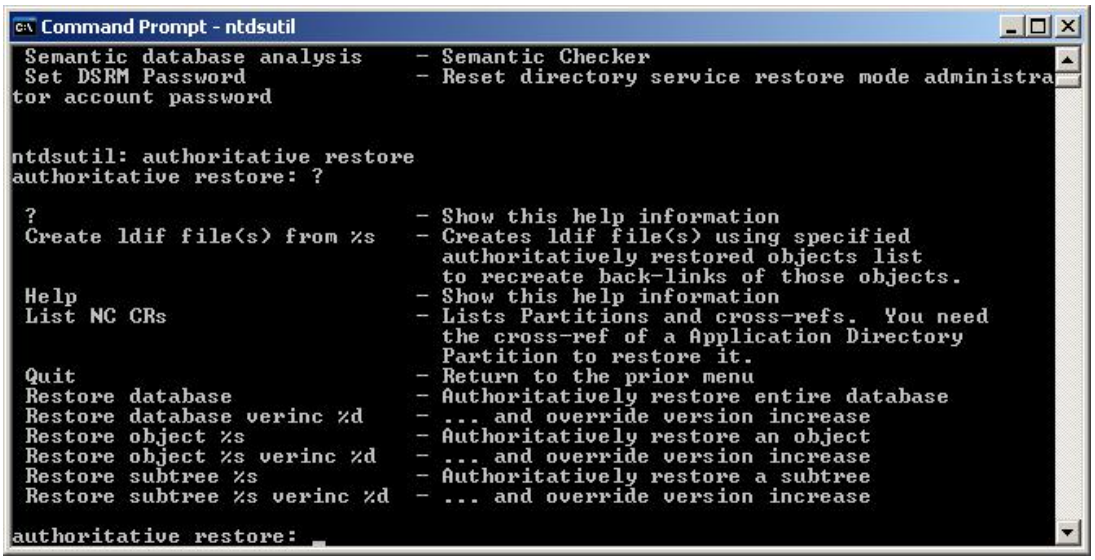


În acest caz serviciul *Active Directory Service* nu este pornit. Restaurarea se poate face folosind parola special stabilită pentru modul restaurare, la momentul instalării *Active Directory*. Restaurarea se face folosind acelaşi utilitar *Backup*, componenta *Restore* (restaurare).



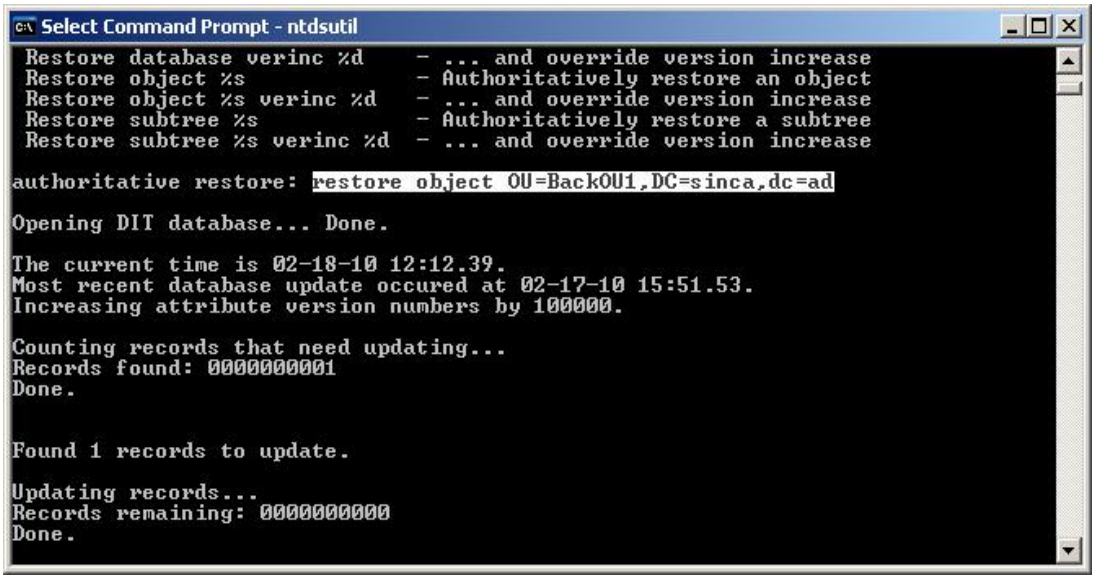
În final suntem întrebați dacă dorim să restartăm sau nu computerul. În cazul în care alegem ***Yes*** se va realiza un ***restore normal***, adică se va restaura totul exact ca în momentul salvării. Eventualele modificări în *Active Directory* efectuate după momentul salvării şi existente pe un alt controler de domeniu vor fi actualizate prin replicare. Răspunsul *NO* (nu) la restartarea sistemului poate continua cu cererea pentru un ***restore authoritativ.*** Este vorba de restaurarea unei porțiuni din *Active Directory* care nu va mai fi modificată prin propagarea replicării. Pentru o restaurare de acest fel se continuă prin lansarea utilitarului ***Ntdsutil.***

Procedura de lucru este următoarea: folosind interfața ***Command Prompt*** (linie de comandă) se lansează utilitarul ***ntdsutil*** şi după prompterul *ntdsulit* se introduce de la tastatură ***authoritative restore.***



Dintre opțiunile prezentate putem alege ***restore database*** pentru restaurarea întregii baze de date sau ***restore object*** pentru restaurarea unei singure ramuri.

Restore object *nume_obiect_ldap*



Propunere de temă practică

Notați modul în care rezolvați temele propuse.

1. Construiți un domeniu *Active Directory* nou care se va numi **curs.ro**. Serverul DNS care va deține domeniul DNS cu acelaşi nume va fi instalat pe acelaşi server, în timpul instalării *Active Directory*.

2. Verificați realizarea corectă a instalării folosind *Windows Server 2003* ***Event Viewer*** şi verificați existența domeniului DNS cu acelaşi nume. Identificați înregistrările SRV.

3. Lansați în execuție cele trei utilitare din ***Administrative Tools*** specifice pentru lucrul cu *Active Directory*, şi anume: ***Active Directory Users and Computers, Active Directory Sites and Services*** şi ***Active Directory Domains and Trusts***

---

1. Includeți un calculator în domeniul creat.

2. Deschideți sesiune de la calculatorul membru din domeniu, ca administrator al domeniului.

3. Instalați *Administrative Tools* folosind comanda ***adminpak.msi*.**

4. Verificați existența utilitarelor administrative nou instalate în ***Administrative Tools*** şi lansați în execuție cele trei utilitare specifice pentru lucrul cu *Active Directory*, şi anume : ***Active Directory Users and Computers, Active Directory Sites and Services*** şi ***Active Directory Domains and Trusts.*** Identificați obiectele existente.

---

1. Construiți (creați) în domeniu o unitate organizațională şi identificați proprietățile noului obiect. Ce fel de obiecte noi pot fi create în unitatea organizațională pe care tocmai ați creat-o?

---

1. În calitate de administrator al domeniului creați în unitatea organizațională un cont utilizator cu parola Pa$$w0rd. Utilizatorul (*user*) va avea dezactivată opțiunea *User must change password at next logon* (utilizatorul trebuie să schimbe parola la următoarea deschidere de sesiune).

2. Modificați (reset) parola utilizatorului creată anterior, noua parola fiind Pa$$w0rd1. Încercați să deschideți sesiune de la controlerul de domeniu folosind numele şi parola cea nouă a utilizatorului.

Notă: pentru deschiderea de sesiune de la controlerul de domeniu sunt necesare drepturi deosebite.

3. Deschideți sesiunea folosind acelaşi cont de utilizator dar de această dată de la calculatorul membru al domeniului. Creați un nou cont utilizator în unitatea de organizare pe care ați creat-o. Dacă nu reuşiți explicați de ce!

4. Deschideți sesiune ca administrator al domeniului de la calculatorul membru al domeniului. Încercați din nou să construiți un nou cont utilizator în unitatea dumneavoastră de organizare. Dacă puteți să duceți până la capăt operația, explicați de ce ați reuşit de această dată.

5. Căutați şi găsiți conturile utilizatorilor din domeniu al căror nume începe cu „a”. Identificați un criteriu prin care să puteți căuta conturile de utilizator pe care le-ați creat. Căutați şi găsiți conturile de utilizator pe care le-ați creat anterior şi identificați proprietățile conturilor.

---

1. Creați în containerul propriu (unitatea organizațională) un grup *security* de tip local domeniului şi unul de tip global. Pentru identificarea uşoară a tipului, numele fiecărui grup va începe cu dl_ în cazul grupului local domeniului şi cu gl_ în cazul grupului global.

2. Ridicați nivelul funcțional al domeniului la Windows Server 2003.

3. Creați un grup universal şi aveți grijă să respectați regula stabilită pentru numele grupurilor.

4. Includeți utilizatorii creați de dumneavoastră în grupurile global şi local domeniului. Fiecare utilizator va fi inclus în alt grup.

5. Creați un folder nou în rădăcina discului C: pe controlerul de domeniu. Oferiți permisiunea *full control* grupului local domeniului şi verificați permisiunile efective ale celor doi utilizatori creați anterior pentru accesul la acest folder.

---

1. Partajați folderul pe care l-ați creat şi publicați-l în *Active Directory* în containerul propriu. Păstrați permisiunile de partajare implicite. Verificați dacă utilizatorul membru al grupului local domeniului poate avea acces de la distanță la acest folder. Pentru verificare va trebui să deschideți sesiune cu acel utilizator folosind computerul membru al domeniului. Construiți o proiecție *map* prin care asociați o unitate logică (*drive* - eventual *Z*:) la obiectul partajat. Identificați şi comentați alte modalități prin care utilizatorul se poate conecta de la distanță la acest folder.

---

1. Instalați şi partajați o imprimantă. Publicați-o în *Active Directory*. Căutați în *Active Directory* imprimanta publicată. Configurați tot ceea ce credeți că ar mai trebui pentru ca unul dintre utilizatorii pe care i-ați creat să se poată conecta la această imprimantă. Verificați că acel utilizator se poate conecta la imprimantă.

---

1. Deschideți sesiune ca administrator al domeniului şi includeți grupul global domeniului, creat anterior, în grupul local domeniului.

2. Creați in containerul dumneavoastră o subunitate organizațională.

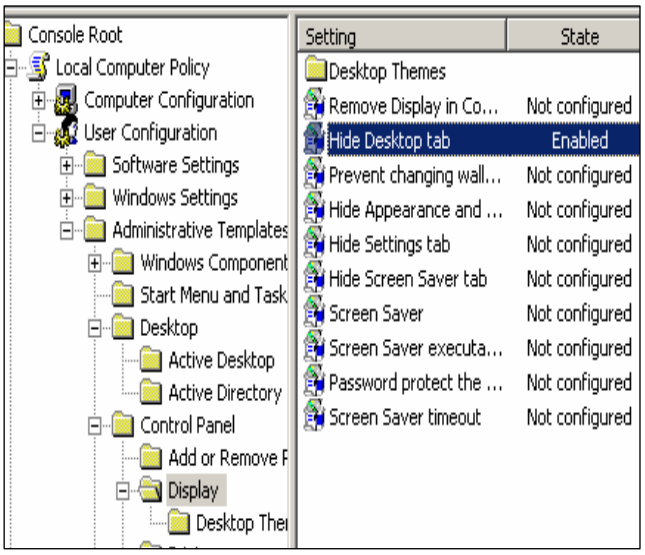
3. Analizați permisiunile la cele două unități organizaționale pe care le dețineți. Identificați permisiunile implicite. Identificați permisiunile la aceste obiecte ale celor doi utilizatori creați anterior.

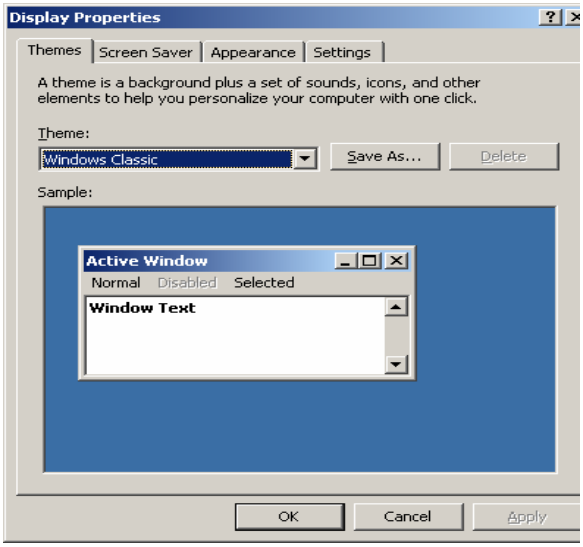
4. Oferiți permisiunea *full control* la subunitatea de organizare pentru membrii grupului local domeniului. Identificați permisiunile moştenite şi pe cele explicite. Amendați permisiunea *full control* stabilită anterior cu permisiunea *deny write*. Identificați din nou permisiunile efective pentru cei doi utilizatori.

---

1. Deschideți sesiune ca administrator al domeniului folosind chiar controlerul de domeniu. Instalați utilitarul GPMC (*Group Policy Management Console*) dacă nu ați făcut-o cumva înainte. Identificați configurările implicite ale politicilor de grup existente, respectiv *Default Domain Policy* şi *Default Domain Controllers Policy*. Identificați configurările legate de conturile şi parolele utilizatorilor din domeniu şi pe cele legate de drepturile utilizatorilor (*user rights*) asupra controlerelor de domeniu.

2. Deschideți sesiune ca administrator al domeniului folosind calculatorul membru din domeniu. Modificați condițiile de lucru locale acestui computer, astfel încât niciun utilizator care va folosi acest computer să nu mai poată avea acces la *tab*-ul *Desktop* din proprietățile *Display* (*Display* este aplicația din *Control Panel*). Să se verifice efectul aplicării acestor noi condiții de lucru.





3. Lansați în execuție utilitarul GPMC şi creați un nou obiect GPO (nelegat). Stabiliți configurările necesare pentru ca utilizatorii cărora li se va aplica politica, să nu mai găsească pe meniul *Start*, nici *Run* şi nici *Control Panel*. Legați obiectul GPO de una dintre unitățile organizaționale pe care le-ați creat. Verificați ca în acea unitate organizațională să existe conturi pentru utilizatori. Forțați aplicarea politicii prin *gpupdate*. Verificați aplicarea politicii pentru utilizatori (deschideți sesiune ca un utilizator din unitatea organizațională şi verificați aplicarea politicii).

---

1. Pe computerul membru al domeniului instalați al doilea controler de domeniu pentru domeniul **curs.ro**. Verificați informațiile legate de cele două controlere de domeniu folosind *Active Directory Sites and Services* (*Site*-uri şi servicii în *Active Directory*), inclusiv activitatea de replicare a *Active Directory*. Porniți o replicare la cerere (*Replicate now*).

2. Folosind utilitarul *Active Directory Users and Computers* şi exemplarul *Active Directory* de pe un controler de domeniu, creați o unitate organizațională nouă în domeniu. Verificați crearea ei şi pe exemplarul de pe celălalt controler.

3. Salvați baza de date a domeniului (*backup System state*).

4. Ştergeți unitatea organizațională pe care tocmai ați creat-o. Aşteptați ca operația să fie propagată pe ambele controlere.

5. Restaurați imaginea *Active Directory* salvată şi încercați o restaurare de tip autoritativ pe unul dintre controlerele de domeniu. Succes!

Ce ați învățat în acest modul?

- ✓ Ce este *Active Directory*
- ✓ Cum se instalează *Active Directory*
- ✓ Cum se creează obiecte în *Active Directory*
- ✓ Acordarea de permisiuni pentru obiectele din *Active Directory*
- ✓ Utilizarea *Group Policy Objects* (GPO) în vederea controlării mediului de lucru
- ✓ Realizarea replicării *Active Directory*
- ✓ Realizarea salvării/restaurării bazei de date *Active Directory*