ATENŢIONARE!

Acest material a fost elaborat de o echipă de experţi din S.C. Centrul de Pregătire în Informatică S.A., partener de implementare a proiectului POSDRU /3/1.3/S/5, compusă din:

- Mihaela Tudose
- Veronica Iuga
- Lidia Băjenaru
- Rodica Majaru

Versiunea materialului de instruire: V2.0

3. Administrarea grupurilor de lucru

Caracteristici generale ale sistemelor de operare Microsoft Windows

Numim sistem de operare un ansamblu de programe care gestionează resursele calculatorului. Sistemul de operare este cel care permite şi controlează accesul la resursele (componentele) hardware. Prin componentele sale specializate, sistemul de operare controlează echipamentele periferice, oferă mijlocul (instrumentul) de comunicare cu utilizatorul şi lansează în execuție alte programe. Într-un sens larg se spune că sistemul de operare este "interfața" dintre utilizator şi hardware-ul calculatorului.

Caracteristici generale ale sistemelor de operare din familia Microsoft Windows includ:

1. *multitasking*
2. memorie virtuală
3. multiprocesare simetrică
4. "*plug" & "play*"
5. lucrul "*offline*" cu fişiere (sincronizare)
6. tipărirea în rețea
7. sistem de fişiere FAT16, FAT32, NTFS – inclusiv cote de ocupare a discului, securitatea accesului, compresia fişierelor
8. sistem de criptare a fişierelor
9. criptarea datelor transmise între calculatoare (IPSec)
10. tentificare Kerberos (inclusiv "*smart card*")
11. *logon* secundar ("*run as…*")

Rețele de calculatoare Microsoft Windows

Numim **rețea de calculatoare** un grup de calculatoare conectate între ele şi care comunică în aşa fel încât un utilizator poate avea acces atât la resursele locale cât şi la resurse partajate aflate la distanță. Resursele rețelei pot fi partajate ("*share*") între mai mulți utilizatori.

În funcție de rolul pe care îl îndeplinesc sistemele *Microsoft Windows*, rețelele respectă fie modelul egal la egal, fie pe cel cu domenii.

Într-o rețea de calculatoare există relații de tip client – server: clientul cere acces, iar server-ul … serveşte, adică oferă serviciul solicitat. Serviciul solicitat este oferit dacă cel care l-a cerut era în drept să-l ceară şi dacă are suficiente privilegii pentru a folosi ceea ce i se pune la dispoziție.

Calculatoarele client (în general calculatoarele pe care le folosesc utilizatorii) formulează cereri pentru obținerea de date sau pentru accesul la un serviciu. Cererile lor sunt trimise calculatoarelor care îndeplinesc rol de server.

Exemple de servere:

- servere de fişiere şi imprimare
- server de baze de date
- server de poştă electronică
- server de fax
- server pentru servicii director de resurse

Rolurile de client şi server ale calculatoarelor stau la baza stabilirii modelului logic al rețelei:

I. ***Rețele "Egal la egal (peer to peer-P2P)"*** se compun din calculatoare care se consideră toate egale ca rang[1]. Fiecare calculator îndeplineşte atât rol de server cât şi de client: atunci când cere acces la un fişier aflat în altă parte îndeplineşte rolul de client; dacă oferă acces la unul din fişierele lui, atunci acționează ca un server. Aceste rețele se numesc grupuri de lucru ("*workgroup*"). Marele dezavantaj al acestui model este imposibilitatea stabilirii unor reguli stricte şi sigure de acces la resurse. Securitatea rețelei nu este punctul forte al acestui model. Rețelele P2P se construiesc prin adăugarea ad-hoc de noduri în rețea. În rețelele ad-hoc eliminarea unui nod nu are un impact deosebit asupra rețelei în întregul ei. Calculatoarele componente ale unui grup de lucru sunt considerate autonome (*standalone*).

II. ***Domeniile Windows Server*** sunt grupuri de calculatoare pe care rulează sisteme de operare *Microsoft Windows* şi care folosesc în comun o bază de date centrală, comună, numită director. Această bază de date conține conturile utilizatorilor şi informații legate de securitatea resurselor rețelei. Fiecare persoană care foloseşte calculatoare incluse în domeniu, primeşte un cont unic de utilizator. Acest cont are acces la resursele domeniului. Directorul unui domeniu se află pe controlerul de domeniu. Controlerul de domeniu este un server care controlează toate aspectele legate de securitatea accesului la resurse şi de administrarea domeniului.

Activitatea de administrare a unei rețele cuprinde în general următoarele operații (activități):

- Gestiunea conturilor utilizatorilor
- Gestiunea resurselor
- Salvarea / restaurarea datelor
- Supravegherea (monitorizare) activităților din rețea

[1] În limba engleză "peer" înseamnă semen, egal, dar şi nobil, aristocrat, *pair*.

Windows Help este instrumentul de învățare cel mai rapid şi mai comod. La baza sistemului de <ajutor> se află o bază de date care poate localiza uşor informația de care are nevoie un utilizator (eventual administratorul rețelei) aflat în impas.

Pentru buna administrare a rețelei, trebuie cunoscut mai întâi mediul de operare. Iată câteva instrumente:

- *Scheduled Tasks* (sarcini programate, planificate)
- *Administrative tools* (instrumente de administrare)
- *Control panel* (panoul de control)
- *Registry* (regiştrii)
- *System properties* (proprietățile sistemului)
- *Computer management* (gestionarea calculatorului), *System information* (informații despre sistem) şi *Local users and groups* (conturi locale pentru utilizatori şi grupuri).
- *Active Directory Users and Computers* (utilizatori şi calculatoare din *Active Directory)*
- *Event viewer* (vizualizarea evenimentelor)
- *Task manager* (gestionarul de taskuri)
- *Performance* (performanțe)
- *Printers* (Imprimante)
- *Shared foders* (dosare, foldere partajate)
- *Disk management* (gestiunea discului)
- *Backup* (salvare)
- *Network and Dial-up connections* (conexiuni în rețea şi prin *dial-up*)
- *Network monitor* (supravegherea rețelei)
- *Configure your server* (configurați-vă serverul)
- *Add/remove programs* (adăugare / eliminare de programe)
- *Microsoft Management Console - mmc* (Consola Microsoft)

Modelul “egal la egal” sau grupurile de lucru

Un grup de lucru se compune din mai multe calculatoare egale ca rang. Administrarea unei astfel de rețele se realizează distribuit, separat la fiecare calculator în parte.

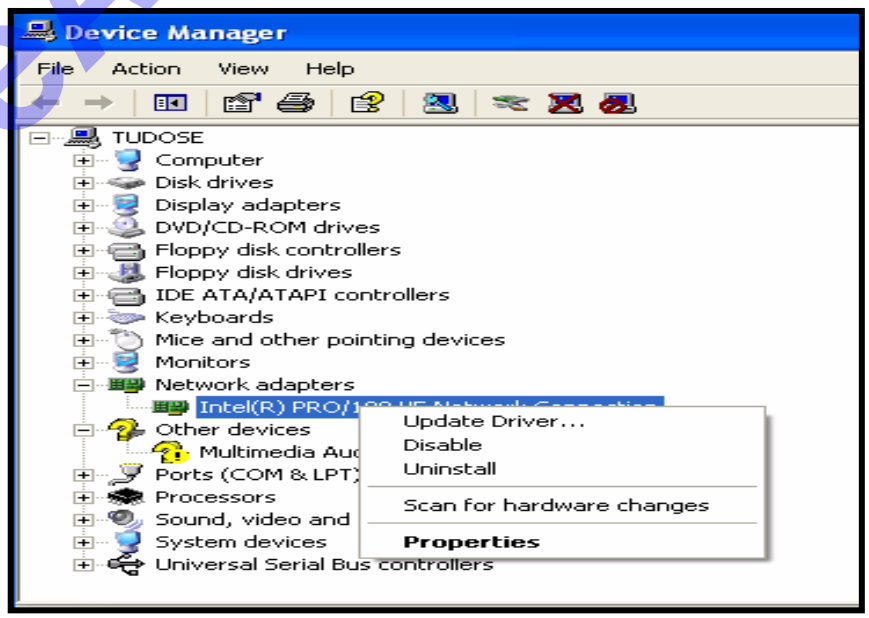
În rețelele care respectă modelul grupurilor de lucru (*workgroup*) utilizatorii sunt autentificați local: baza de date *Registry* – locală calculatorului – conține o structură de informații care reprezintă numele de utilizatori locali şi grupurile locale din care fac parte aceştia. Când un utilizator (autentificat local) doreşte acces la o resursă aflată la distanță, el trebuie reautentificat la calculatorul care deține resursa.

Caracteristicile modelului *workgroup* sunt următoarele:

- Pentru a avea acces la un calculator (local) utilizatorul trebuie să fie autentificat local (să treacă prin procedura de deschidere de sesiune – *logon*).
- Resursele sunt distribuite în rețea, dar sunt considerate ca fiind locale fiecărui calculator.
- Accesul la o resursă aflata la distanță se face în urma unei reautentificări, ce are loc la calculatorul care deține resursa.
- Administrarea rețelei nu se face centralizat: fiecare calculator este administrat separat.
- Fiecare calculator deține o bază de informații SAM[2] – *Security Account Manager* unde se află toate conturile locale. Pentru ca un utilizator să poată avea acces la resurse distribuite în rețea, el trebuie să aibă câte un cont de utilizator local pe fiecare calculator care deține resursele folosite în rețea.
- Se recomandă ca într-un grup de lucru să existe cel mult 10 calculatoare Grupurile de lucru devin greu de administrat dacă conțin mai mult de 10 calculatoare. Mai mult chiar, numărul de conexiuni simultane la un calculator cu sistem de operare de tipul client, cum este *Windows XP,* este de maxim 10.

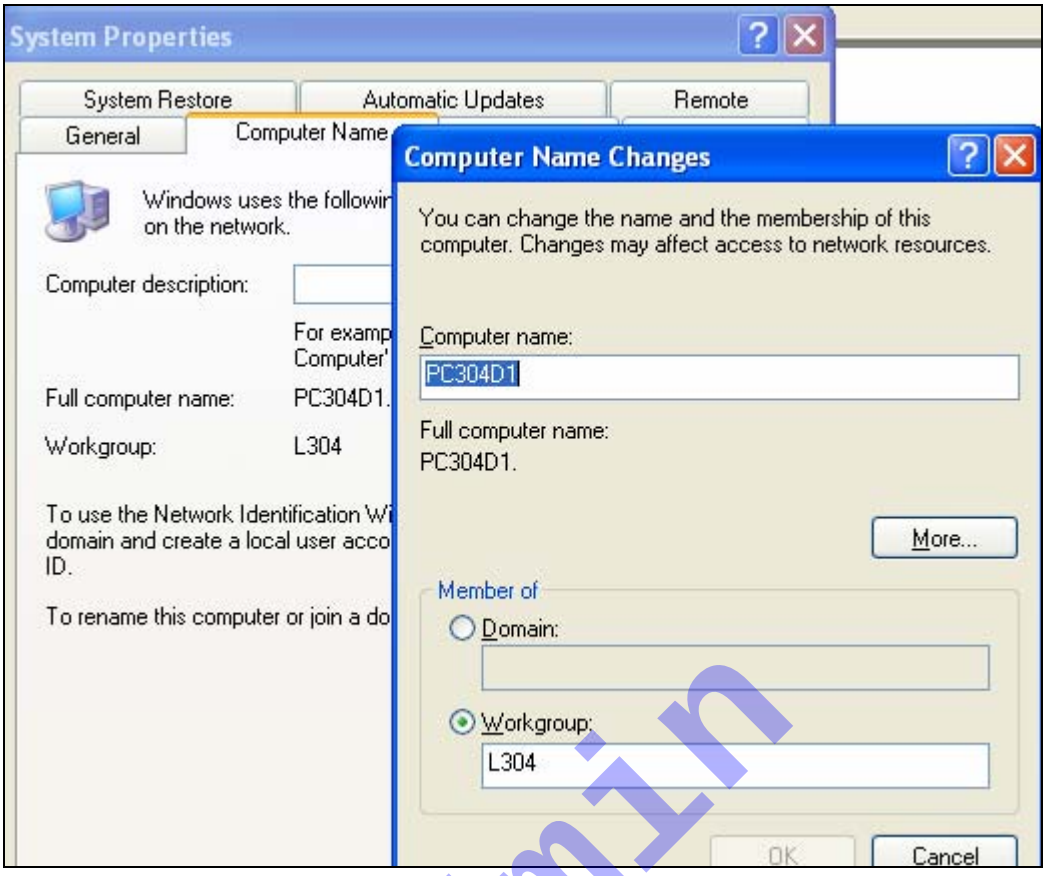
Proprietățile sistemului

De la prima întâlnire cu calculatoarele, administratorul trebuie să încerce să le cunoască cât mai bine. Primul pas este căutarea proprietăților calculatorului.

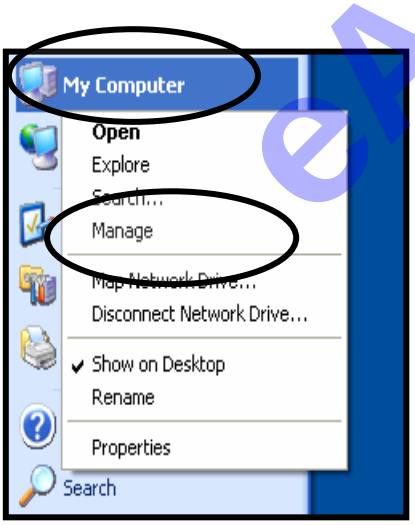


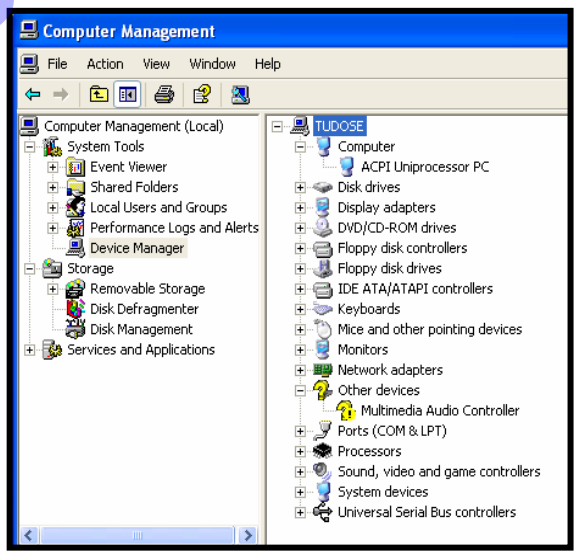
[2] Baza de informații SAM se află în Registry (se va folosi utilitarul regedt32.exe)

Primele informații cu care ne întâlnim sunt legate de numele calculatorului, apartenența la un grup de lucru (*workgroup*) sau la un domeniu.



Computer Management.





Fereastra de lucru oferă multe informații!

Conturile utilizatorilor şi grupurile de utilizatori

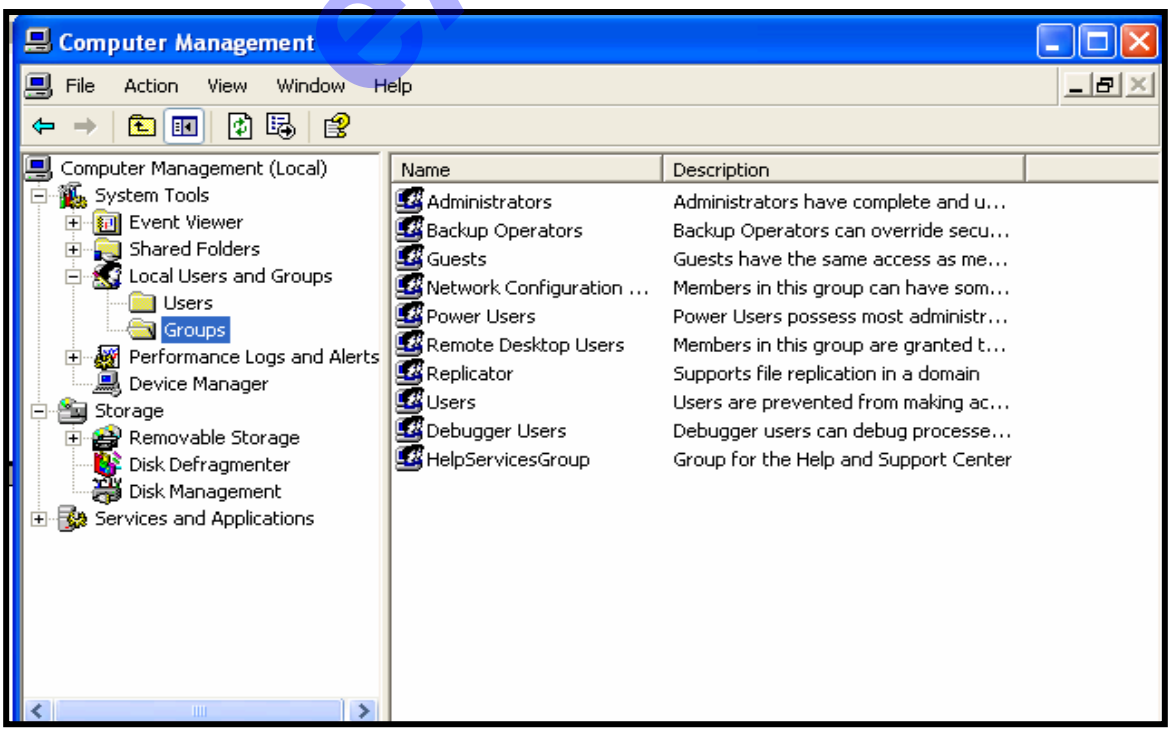
Un cont utilizator este o structură de informații care descrie şi identifică un utilizator. Informațiile sunt folosite la deschiderea de sesiune (*logon*). Fiecare persoană care foloseşte resursele unei rețele trebuie să aibă un cont utilizator. Imediat ce dispune de un cont, un utilizator îl poate folosi pentru a fi autentificat local sau în domeniu. Cu acest cont el va putea avea acces la resursele locale (ale calculatorului respectiv) şi la resursele rețelei (resurse aflate la distanță şi partajate). Există la unele sisteme de operare din familia *Windows* utilizatori aşa-zişi preconstruiți (deja construiți), ca de exemplu *Administrator*, *Guest*.

Calculatorul local poate fi gestionat prin utilitarul *Computer Management.*

Printre alte informații, aici există şi lista utilizatorilor cunoscuți local, respectiv *Local Users and Groups*.

Un grup este o colecție (listă) de nume de conturi utilizator. Dacă un grup are asociat un set de privilegii în raport cu resursele rețelei, atunci fiecare membru al grupului se bucură de acest set de privilegii. Un cont utilizator poate face parte din mai multe grupuri. În acest caz privilegiile asociate contului sunt cele care se obțin din însumarea celor atribuite fiecăruia din grupurile din care face parte.

Sistemele de operare *Microsoft Windows* folosesc grupuri preconstruite (ca de exemplu *Administrators, Backup Operators, Users*, etc.), grupuri cu identități speciale (exemplu: *Everyone, System*, etc.) şi grupuri construite de utilizatori. Grupurilor li se asociază privilegii. Apartenența unui cont utilizator la un grup îi conferă contului respectiv toate privilegiile care sunt asociate grupului.



Drepturile utilizatorilor şi apartenența la grupuri

Pentru sistemele de operare *Microsoft Windows* privilegiile se compun din drepturile utilizatorilor şi permisiunile la resurse.

Drepturile sunt operații (acțiuni) pe care un utilizator le poate efectua asupra sistemului în ansamblu (să facă "*shut down",* să schimbe data şi ora sistemului, să salveze şi să restaureze fişiere, să instaleze drivere, etc.).

Iată câteva din drepturile utilizatorilor ("*User Rights*"):

- *Logon locally* – dreptul de a face *logon* (de a deschide sesiune) folosind calculatorul local
- *Change system time* – dreptul de a modifica data şi ora sistemului
- *Shut down* – dreptul de a opri funcționarea calculatorului
- *Access this computer from the network* – dreptul de a avea acces din rețea (folosind orice calculator) la calculatorul local.

Unele dintre drepturi sunt asociate grupurilor preconstruite.

Grupul *Administrators* (Administratori). Membrii acestui grup au control deplin asupra calculatorului sau domeniului.

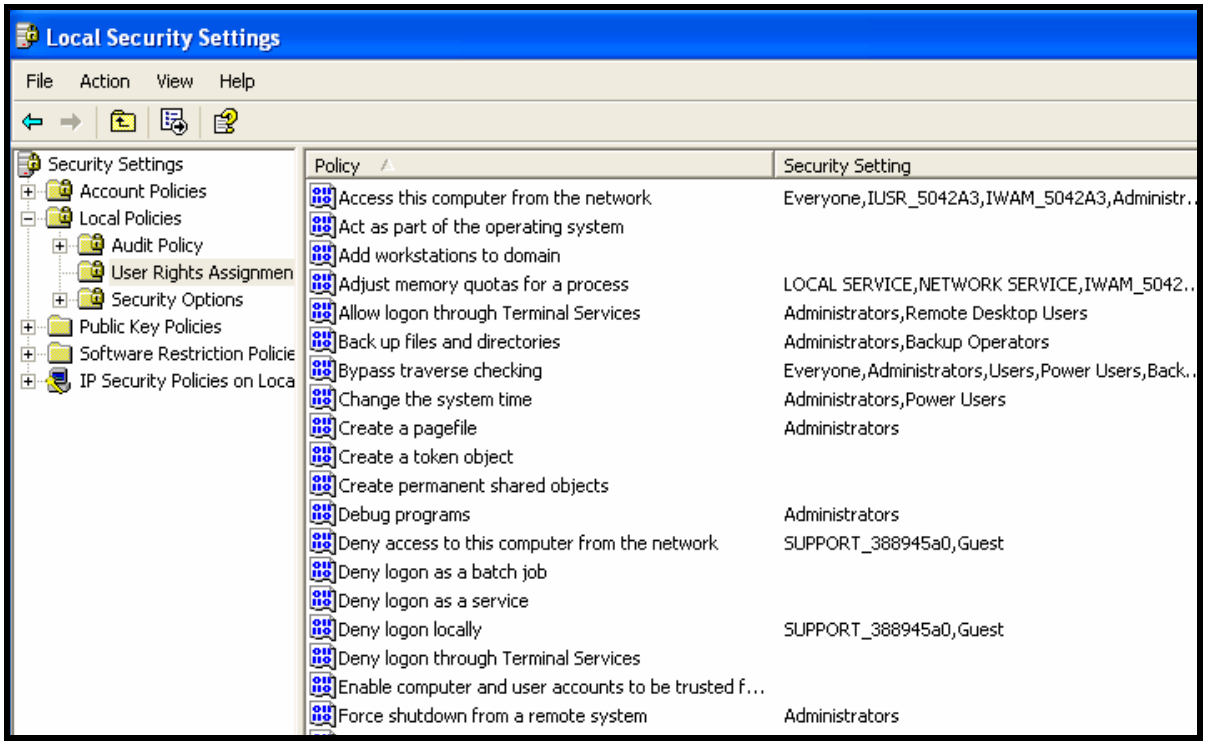
Grupul *Users* (Utilizatori) - Membrii acestui grup pot executa numai acele sarcini pentru care au primit drepturi, ca de exemplu: lansarea în execuție a aplicațiilor, acces la imprimantele din rețea, oprirea funcționării calculatorului. Membrii acestui grup nu pot crea grupuri locale şi nici utilizatori locali, nu pot partaja dosare (foldere).

Grupul *Power Users* (Utilizatori privilegiați) – este un grup preconstruit aflat pe calculatoare non-controlere de domeniu. Membrii acestui grup pot executa unele sarcini administrative, dar nu dețin controlul deplin asupra sistemului.

Ei pot să:

- creeze conturi pentru utilizatori şi grupuri (la calculatorul local)
- modifice şi să şteargă conturile pe care le-au creat
- partajeze resurse

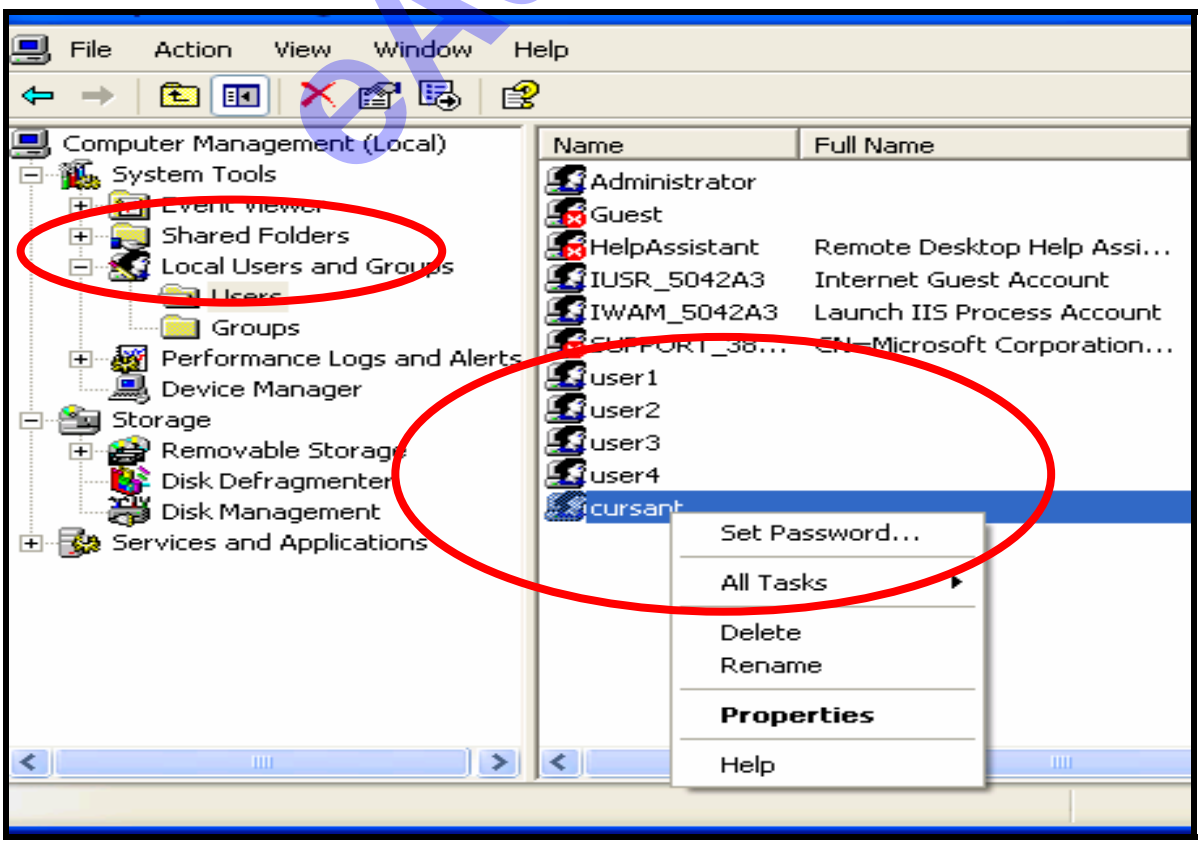
Grupul *Backup Operators* (Operatori de *Backup* <"salvare">) - Membrii acestui grup pot să salveze şi să restaureze fişiere aflate la acel calculator, indiferent de permisiunile pe care le au la fişierele respective. Ei mai pot să deschidă sesiune folosind calculatorul acela şi pot opri funcționarea lui.



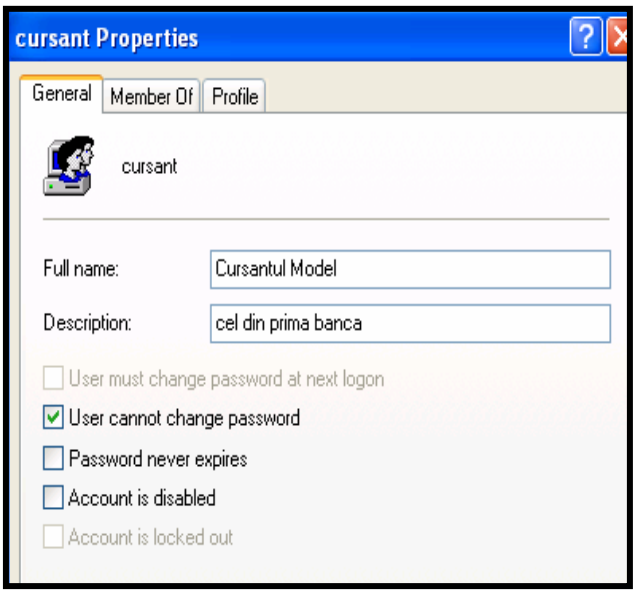
Utilizatori locali şi grupuri locale

În modelul egal - la - egal utilizatorii deschid sesiune folosind conturile locale. Prin deschiderea de sesiune utilizatorii sunt autentificați şi vor avea acces la resurse locale, în limita privilegiilor. Conturile locale ale utilizatorilor se află în baza de date "*registry*".

Computer management este utilitarul pe care îl folosim pentru crearea şi gestionarea conturilor utilizator.



Contul unui utilizator poate fi şters, redenumit şi i se poate schimba parola asociată.



Un cont utilizator are următoarele proprietăți:

1.utilizatorul trebuie să-şi modifice parola la următoarea deschidere de sesiune

2.utilizatorul nu poate schimba parola

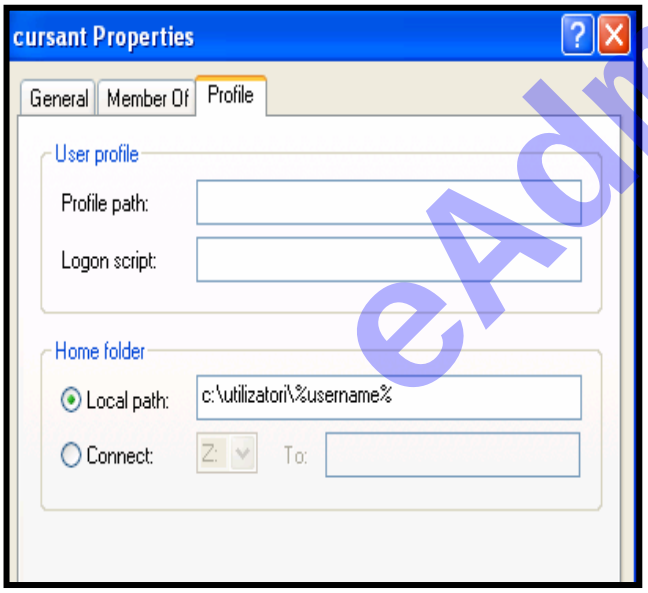
3.parola nu expiră niciodată

4.contul este indisponibil

5.cont blocat (în urma încercărilor repetate, nereuşite de deschidere de sesiune)

Utilizatorii fac parte din grupuri. Dacă un grup de utilizatori are asociate privilegii atunci fiecare membru al grupului beneficiază de acele privilegii.

Informația asociată cu profilul utilizatorului se compune din:

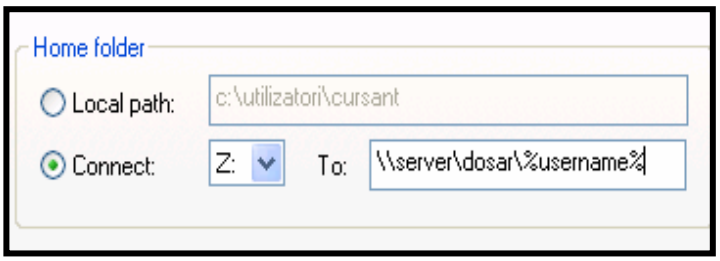


1. Calea până la folderul care indică profilul utilizatorului. Profilul descrie imaginea *desktop,* care se afişează în urma autentificării utilizatorului, împreună cu constante de lucru ale utilizatorului, ca de exemplu: mărimea pictogramelor, mărimea şi culoarea ferestrelor, informații despre formatul de afişare a datei, etc. Calea implicită a acestui folder este:

%systemroot%\Documents and Settings\%username%

2. *Logon script* se referă la fişierul cu comenzi care va fi executat la fiecare deschidere de sesiune. Acest fişier ar putea, de exemplu, configura mediul de operare al utilizatorului, astfel încât el să lucreze numai cu anumite aplicații şi în anumite condiții.

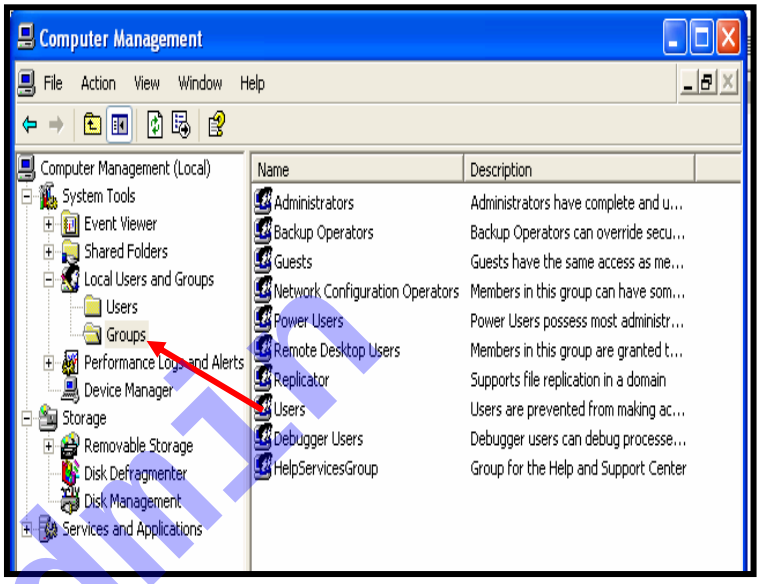
3. Utilizatorul ar putea avea şi un dosar (director, folder) personal – numit generic “acasă”, acolo unde îşi salvează lucrările şi unde îşi plasează informațiile de lucru de care are nevoie. Acest dosar personal se poate afla pe un hard disc local sau se poate afla undeva la distanță, la un alt calculator. În acest din urma caz, utilizatorul se va conecta la resursa aflată la distanță folosind o unitate logică:



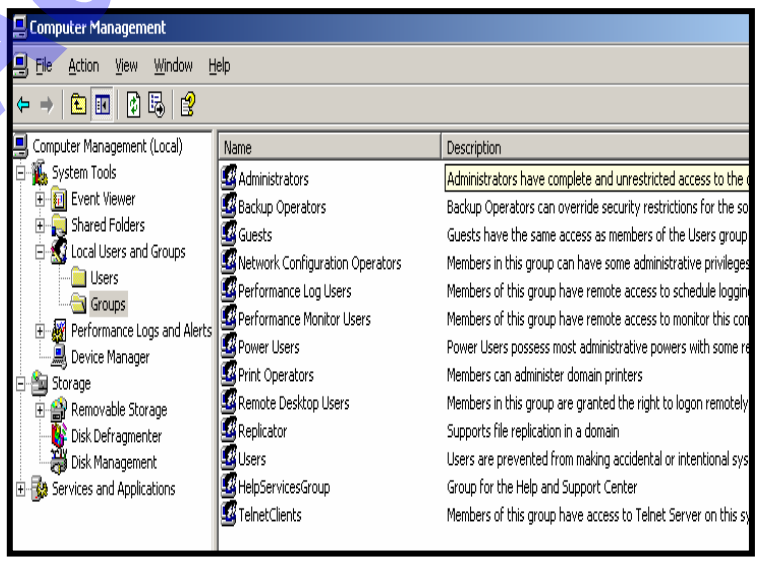
În acest exemplu va fi folosită unitatea logică Z: pentru conectarea la dosarul personal al utilizatorului.Utilizatorii au, în general, toate permisiunile la dosarul lor personal (“acasă”).

Utilizatorii pot fi grupați în … grupuri de utilizatori. Dacă un utilizator face parte dintr-un grup, atunci el are aceleaşi privilegii cu cele ale grupului din care face parte.

Iată un exemplu de grupuri preconstruite pentru sistemul de operare *Windows XP Professional:*



Pentru sistemele de operare *Windows Server 2003* grupurile preconstruite sunt:



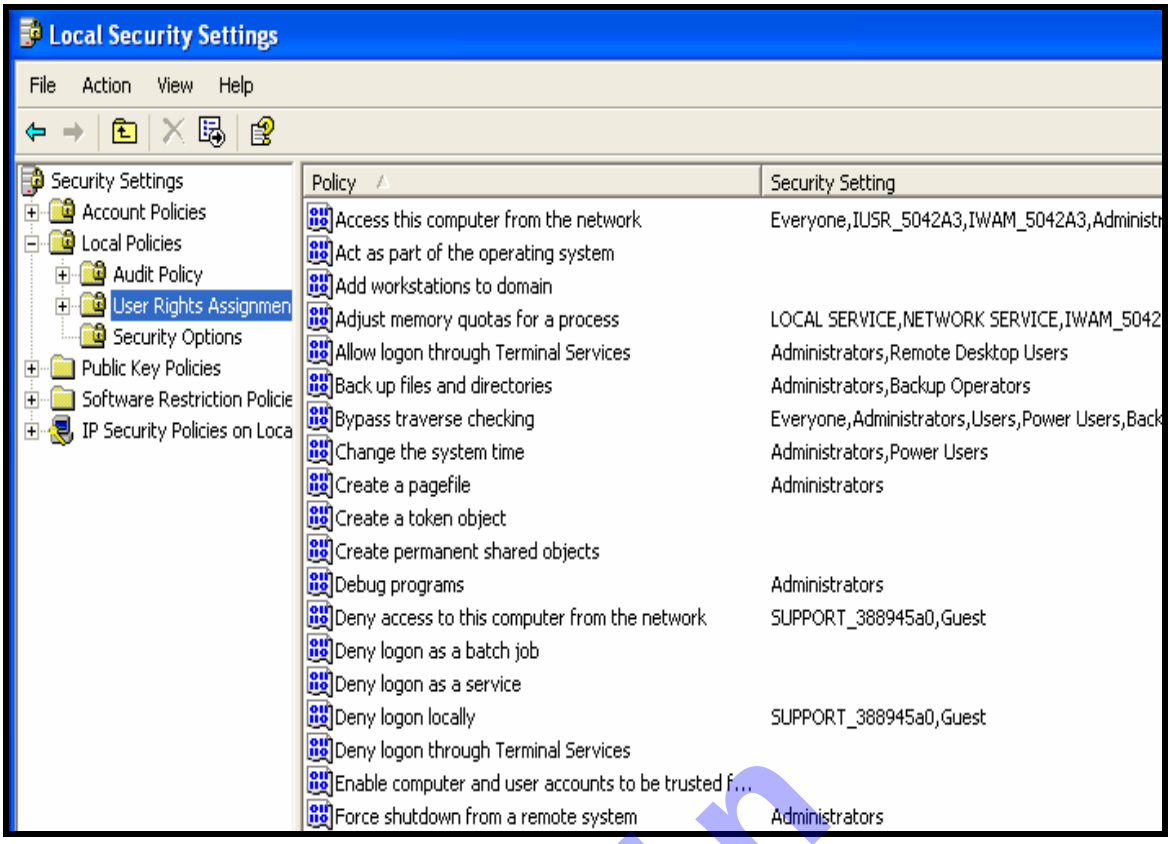
La instalarea sistemului de operare sunt create – implicit – grupurile locale numite preconstruite. Grupul local *Administrators* îi cuprinde pe administratorii sistemului: sunt cei care au privilegii complete asupra sistemului; pot instala / dezinstala orice componenta hard şi / sau soft, pot face orice fel de operație de configurare, pot crea, şterge, modifica orice cont utilizator şi / sau de grup. Utilizatorii locali fac în mod implicit parte din grupul *Users*.

Includerea unui cont utilizator într-un grup preconstruit îi oferă acelui utilizator privilegiile asociate grupului. De exemplu, incluzând un cont utilizator în grupul *Administrators*, utilizatorul primeşte privilegii de administrator.

Administrators	Au privilegii complete, inclusiv acelea de a-şi modifica drepturile şi permisiunile
Backup operators	Pot să facă salvări şi restaurări de fişiere ("*backup*" şi "*restore*") indiferent de permisiunile pe care le au la nivelul fişierelor. Pot face *log on* (deschidere de sesiune) şi *shut down* (oprirea calculatorului)
Power users	Pot crea conturi de utilizator, le pot modifica şi şterge pe cele create; pot crea grupuri locale şi pot modifica lista membrilor pentru aceste grupuri. Nu pot modifica grupurile *Administrators* şi *Backup operators*. Nu pot prelua posesia asupra fişierelor şi nu pot face salvarea/restaurarea fişierelor şi nici nu pot instala/dezinstala drivere. Pot partaja (share) resurse.
Users	Pot efectua sarcini obişnuite: lansarea în execuție a unor aplicații, pot folosi imprimantele locale şi de rețea, pot opri calculatoarele cu rol de stații de lucru.
Guests	Sunt utilizatori ocazionali care deschid sesiunea folosind contul *Guest*
Replicator	Asigură funcțiile de replicare; conturile utilizator obişnuite nu trebuie incluse sub nici un motiv în acest grup.

Accesul la resursele locale. Permisiuni

Pentru sistemele de operare *Microsoft Windows* privilegiile utilizatorilor se compun din drepturi şi din permisiuni la resurse. Drepturile ("*user rights*") sunt operații (verbe, acțiuni) pe care le pot executa utilizatorii asupra sistemelor văzute în ansamblu. Politica locală de securitate (*local security policy*) conține componenta "*user rights*" (drepturile utilizatorilor).



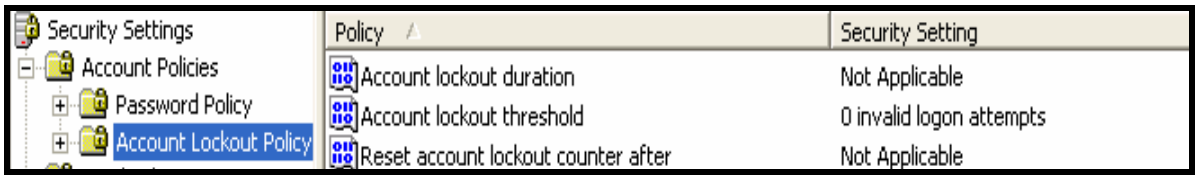
Aceste drepturi se referă la operații de tipul:

- Accesul din rețea la acest calculator
- Salvarea fişierelor şi a directoarelor (dosare)
- Restaurarea fişierelor şi a directoarelor (dosarelor)
- Modificarea datei sistemului
- Deschiderea de sesiune folosind echipamentele acestui calculator
- Închiderea calculatorului
- Etc. …

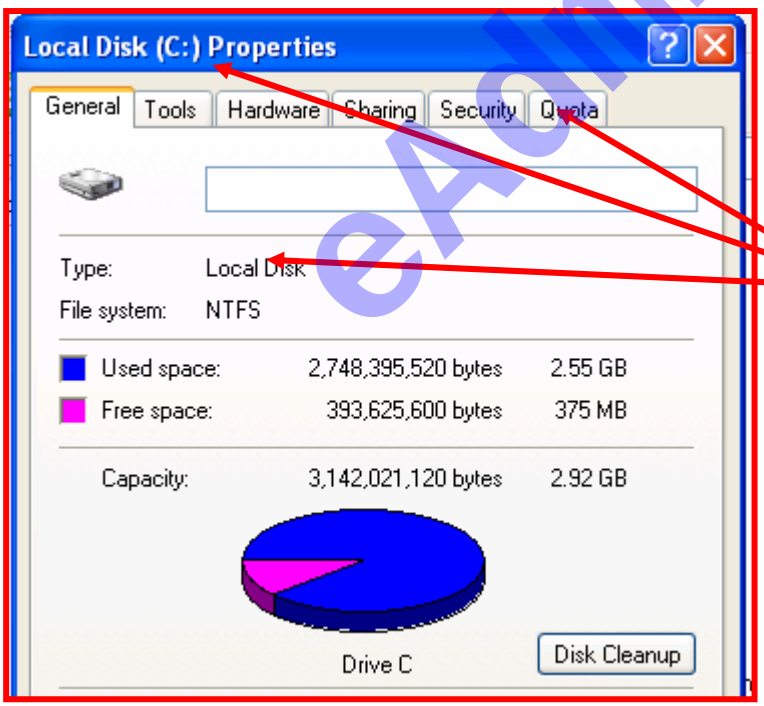
La întrebarea “cine poate face <<*shut down*>> la sistem?” Răspunsul este :

Controlul modului în care utilizatorii pot face *logon* este realizat prin politica asociată conturilor.

şi



Accesul la dosare şi fişiere aflate pe hard discul calculatorului local poate fi controlat (restricționat) numai în situația în care unitatea logică respectivă (de exemplu C:) adresează o partiție formatată NTFS (*New Technology File System*).



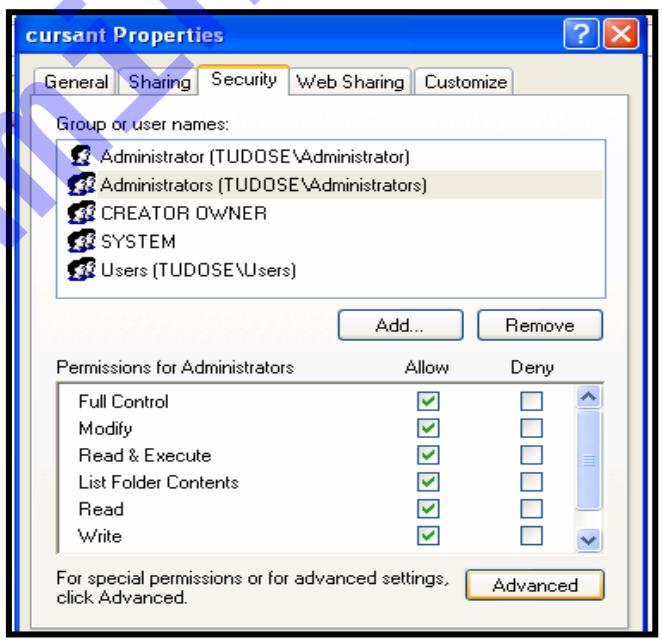
Unitățile de disc formatate NTFS au o proprietate numită „*security*” unde se pot asocia reguli de securitate a accesului la dosare şi fişiere

Permisiuni NTFS

Sistemul de fişiere NTFS[3] este singurul care poate asigura protecția şi securitatea accesului local la fişiere şi dosare. Pentru volumele NTFS se poate controla strict accesul local al utilizatorilor la dosare şi fişiere. Acest lucru nu este asigurat de celelalte sisteme de fişiere acceptate de *Windows*, adică FAT16 şi FAT32. Pentru acestea din urmă, accesul local al unui utilizator nu poate fi restricționat în nici un fel.

Sistemele de operare *Microsoft Windows* asociază permisiuni dosarelor şi fişierelor aflate în partiții formatate NTFS. Permisiunile sunt acordate utilizatorilor individuali sau grupurilor. Dacă un utilizator nu are nici o permisiune asupra unui fişier sau dosar, atunci el nu poate efectua nicio operație asupra acelui obiect. Fiecare dosar şi fişier dintr-o partiție NTFS are asociată câte o listă ACL (*Access Control List* – listă care controlează accesul). În lista ACL se află înscrise perechi de informații de tipul: ce utilizator (sau grupuri, sau eventual calculatoare) au acces şi ce tip de acces le este permis. Pentru ca un utilizator să aibă acces la un dosar sau fişier el trebuie sa fie cuprins în lista ACL (direct sau indirect, prin apartenența la un grup). Dacă utilizatorul nu apare în lista ACL atunci el nu are acces la acel obiect!

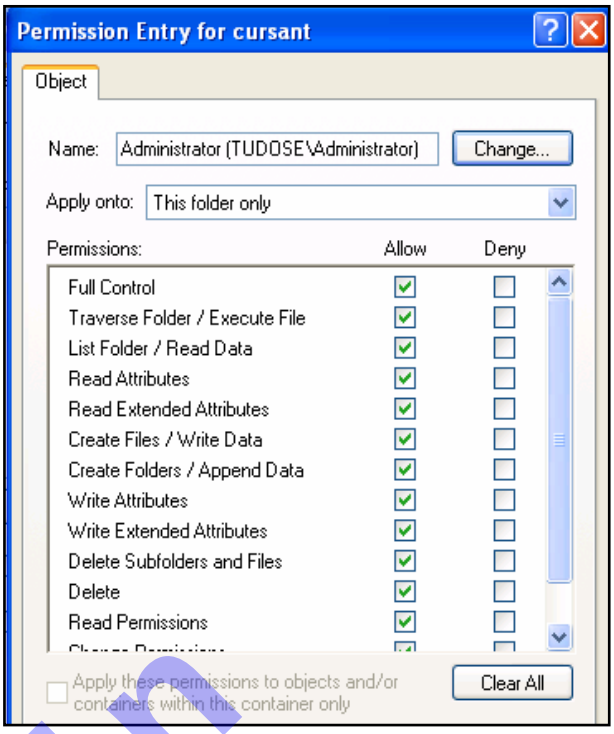
În dreptul permisiunilor asociate unui cont utilizator sau unui grup de utilizatori apar aşa numitele permisiuni speciale, de exemplu: Full Control (control deplin, complet), Modify (modifică), Read & Execute (citeşte şi execută), ş.a.m.d.



Acestor permisiuni de ordin mai general le corespund permisiuni specifice strict delimitate, după cum urmează (vizibile după folosirea butonului <*Advanced*>):

[3] NTFS=New Technology File System

Verbele *Allow* (permite) şi *Deny* (nu permite, neagă) indică semnificația permisiunii. De exemplu, asocierea *Delete* - *Allow* arată că este permisă operația de ştergere.



Permisiuni NTFS pentru fişiere	**Utilizatorul:**
Full control (control deplin)	Schimbă permisiuni, ia în posesiune (devine proprietar) şi execută toate operațiile permise prin toate celelalte permisiuni NTFS
Modify (modifică)	Modifică şi şterge fişierul şi execută operațiile permise prin *Write* şi *Read & Execute*
Read & Execute (citeşte şi execută)	Lansează în execuție aplicația şi execută operațiile permise prin *Read*
Write (scrie)	Suprascrie fişierul, schimbă atributele fişierului, citeşte proprietarul şi permisiunile
Read (citeşte)	Citeşte fişierul, citeşte atribute, proprietar şi permisiuni

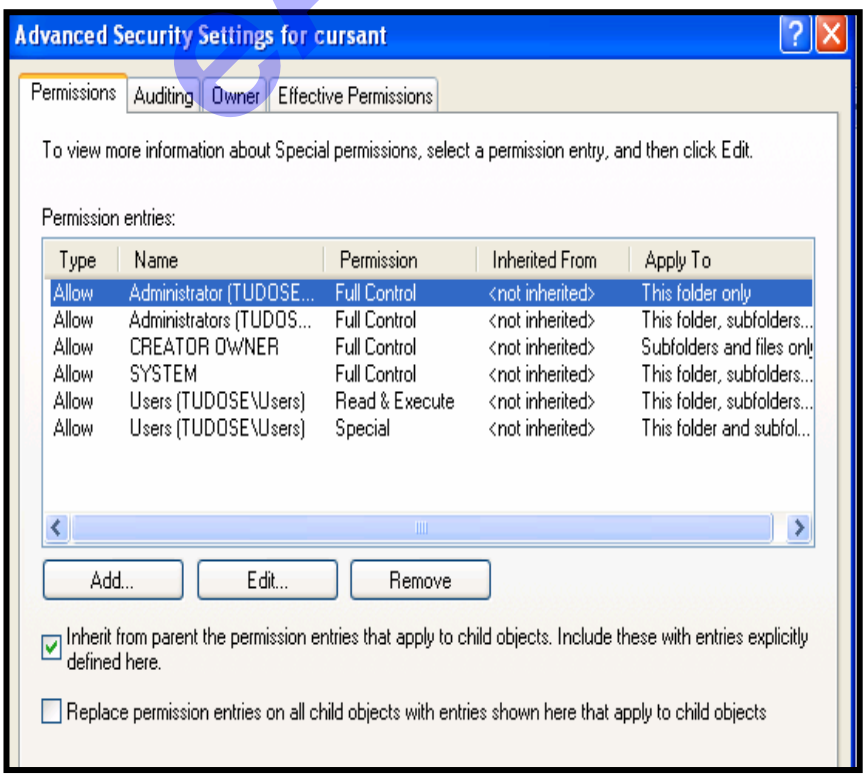
Permisiuni NTFS pentru foldere	**Utilizatorul:**
Full control (control deplin)	Schimbă permisiuni, ia în posesiune, şterge subfoldere şi fişiere, execută toate acțiunile permise prin celelalte permisiuni NTFS
Modify (modifică)	Şterge folderul şi execută operațiile permise prin *Write* şi *Read & Execute*
Read & Execute (citeşte şi execută)	Traversează foldere şi execută operațiile permise prin *Read* şi *List folder contents.*
Write (scrie)	Creează fişiere şi subfoldere noi în folder, schimbă atributele folderului, citeşte proprietarul şi permisiunile
Read (citeşte)	Citeşte fişiere şi subfoldere, atribute, proprietar şi permisiuni
List folder contents (listează conținut folder)	Citeşte numele fişierelor şi ale subfolderelor

	Full Control	***Modify***	***Read & Execute***	***List Folder Contents (numai pentru dosare)***	***Read***	***Write***
	Control deplin	**Modifică**	**Citeşte & Execută**	**Listează conținut folder (numai pentru foldere)**	**Citeşte**	**Scrie**
Traverse Folder/Execute File (traversează folder / execută fişier)	**x**	**x**	**x**	**x**		
List Folder/Read Data	**x**	**x**	**x**	**x**	**x**	

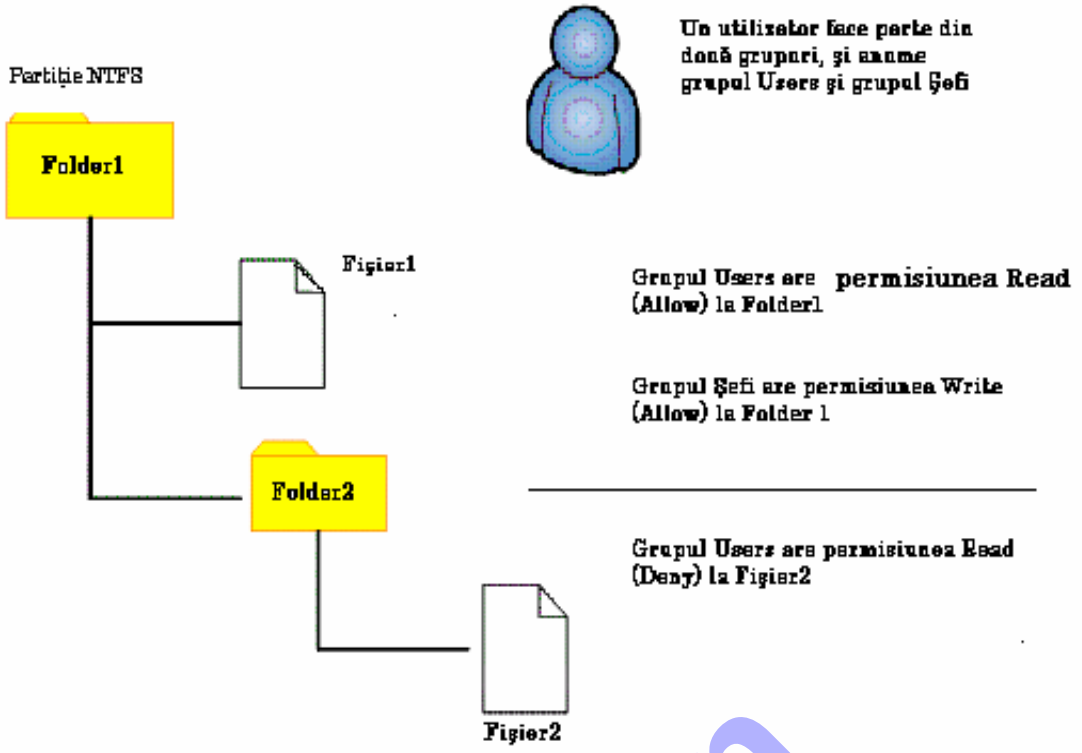
(listează folder / citeşte date)						
Read Attributes (citeşte atribute)	**x**	**x**	**x**	**x**	**x**	
Read Extended Attributes (citeşte atribute extinse)	**x**	**x**	**x**	**x**	**x**	
Create Files/Write Data (crează fişiere/scrie date)	**x**	**x**				**x**
Create Folders/App end Data (crează foldere/adaugă date)	**x**	**x**				**x**
Write Attributes (scrie atribute)	**x**	**x**				**x**
Write Extended Attributes (scrie atribute extinse)	**x**	**x**				**x**
Delete Subfolders and Files (şterge subfoldere şi fişiere)	**x**					

Delete (şterge)	x	x				
Read Permissions (citeşte permisiuni)	x	x	x	x	x	x
Change Permissions (schimbă permisiuni)	x					
Take Ownership (ia în posesie)	x					

Permisiunile sunt asociate atât conturilor de utilizator cât şi grupurilor. Permisiunile efective ale unui utilizator se obțin prin însumarea tuturor permisiunilor care îi revin individual şi prin apartenența la grupuri (un utilizator poate face parte din mai multe grupuri simultan). Permisiunea „*deny*" suprascrie permisiunile corespunzătoare „*allow*" (permis). De exemplu, dacă un utilizator are, asupra aceluiaşi fişier, permisiunea *Read Allow* şi *Read Deny*, atunci permisiunea efectivă, cumulată este *Read Deny.* Permisiunile NTFS asociate unui dosar se propagă (se moştenesc) în ierarhia de subdosare şi fişiere, dacă nu cumva moştenirea este inhibată.



Exercițiu practic:



1. Ce permisiuni are utilizatorul la Folder1? Dar la Fişier1?
2. Ce permisiuni are utilizatorul la Fişier2 ?

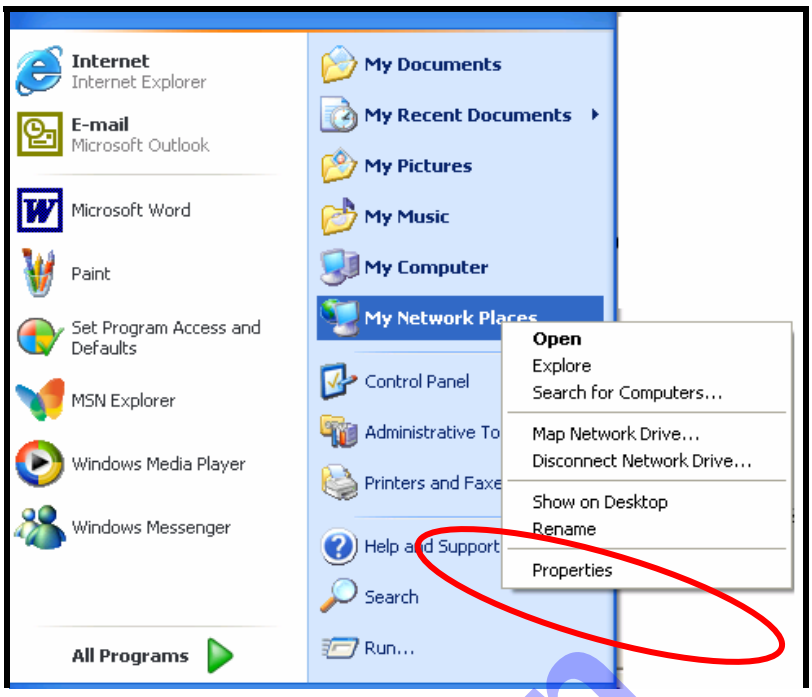
Conectarea la rețea

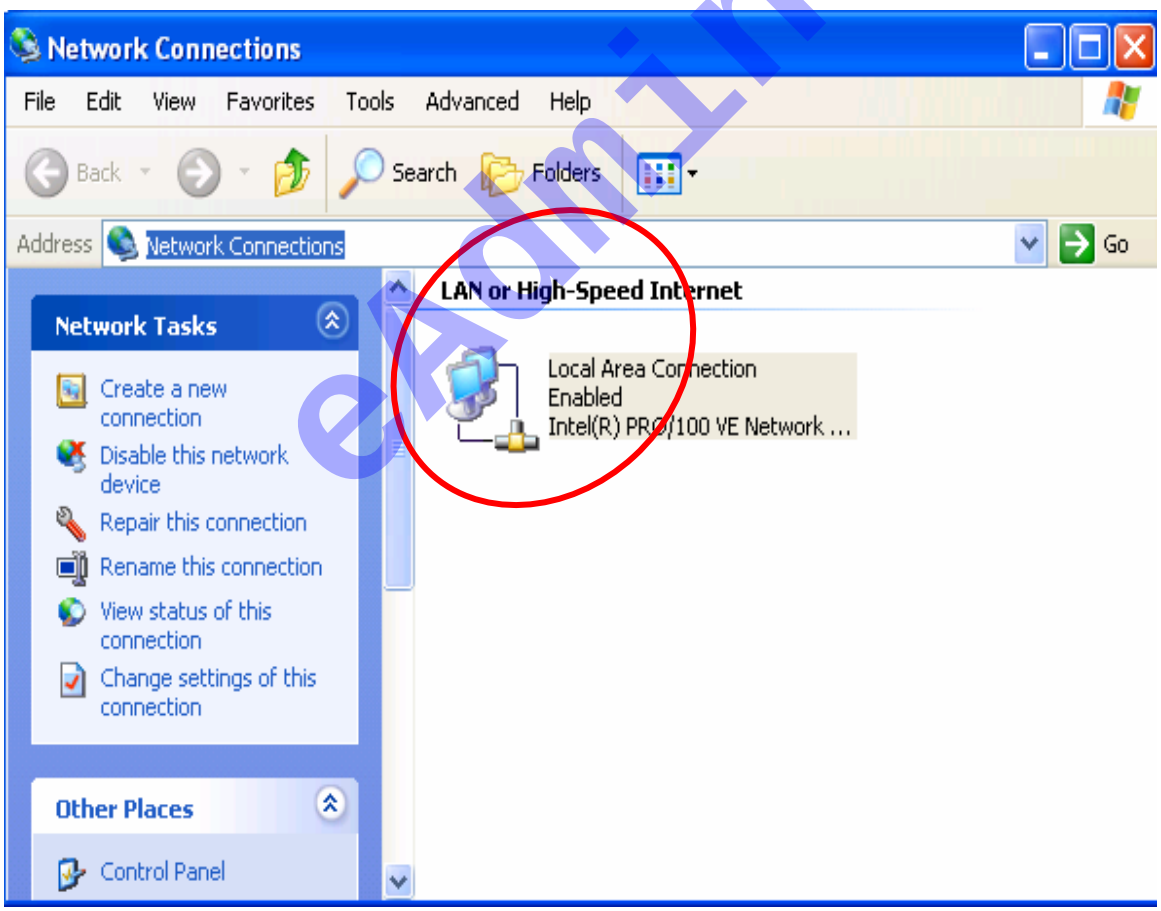
Conexiune activă, corectă

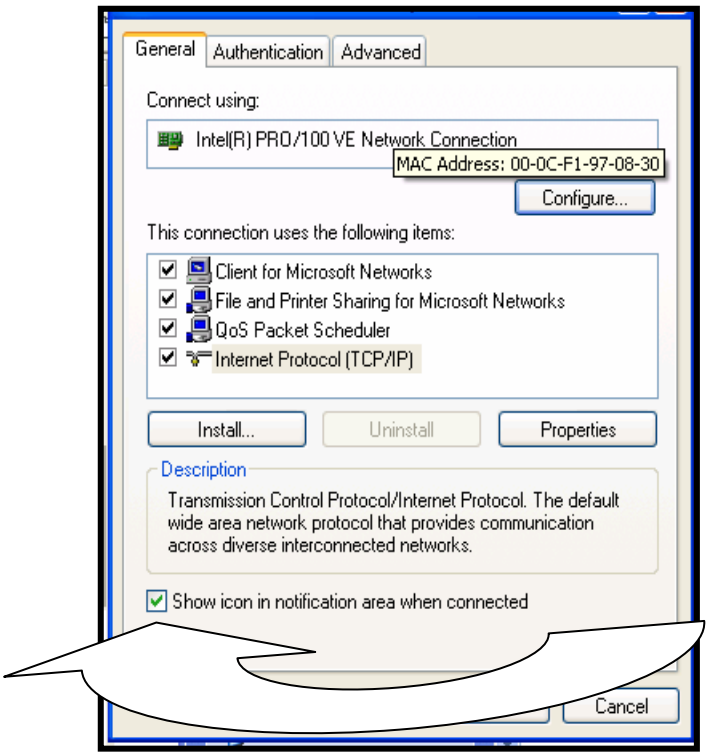
Mediul de transmisie deconectat

Driver dezafectat (nu funcționează)

Starea conexiunii în rețea este indicată de una dintre aceste pictograme.



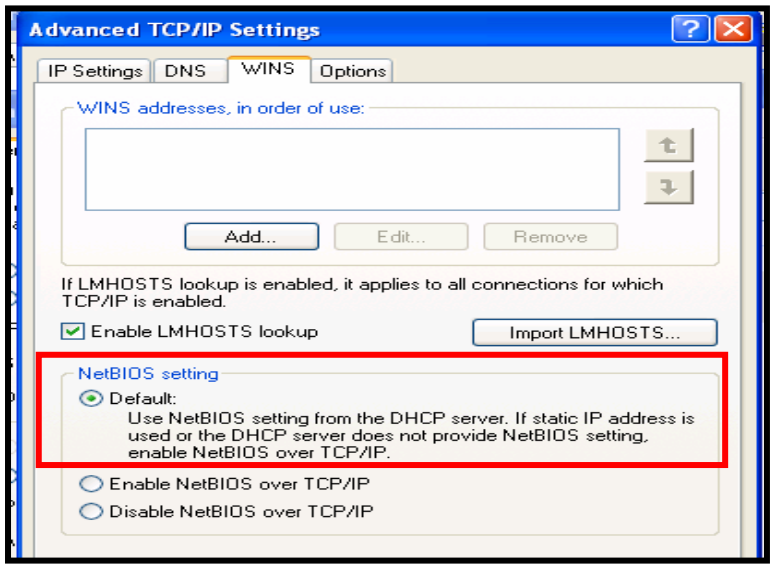




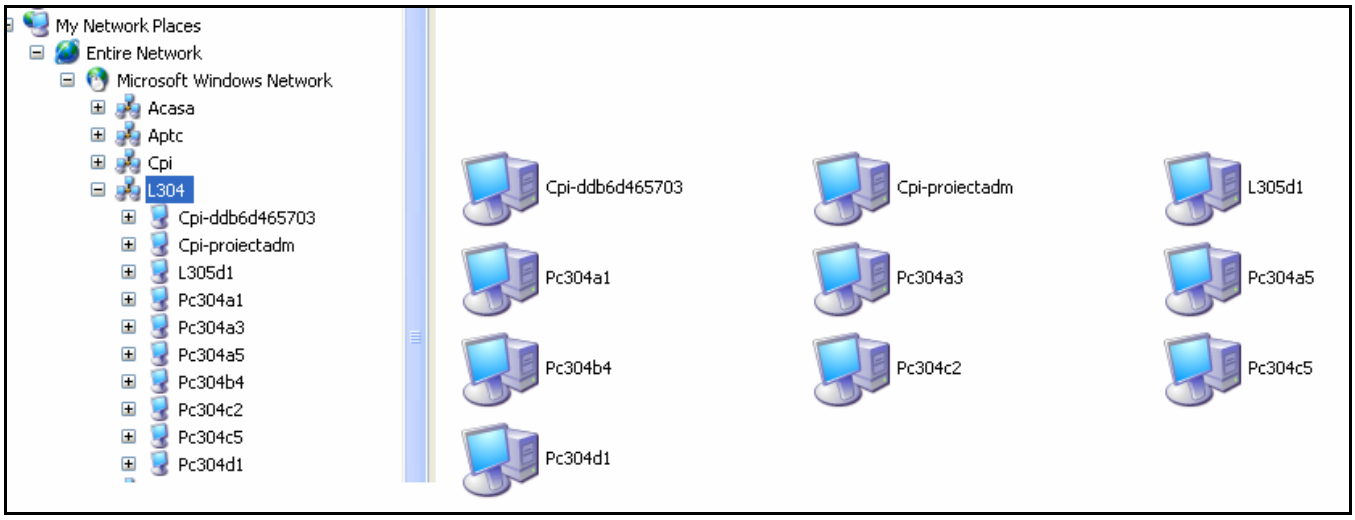
componenta client / server: ▪ client for Microsoft Networks sau ▪ file and printer Sharing for Microsoft Networks	
Transport: ▪ TCP	protocol
Rețea: ▪ IP	
Driver: ▪ Intel® PRO/100 VE	
Placa de rețea: ▪ Adresa MAC ▪ Mediul de transmitere a datelor	

În situația configurării corecte a tuturor componentelor necesare conectării, putem spune că avem un calculator conectat la rețea. Reamintim definiția unei rețele de calculatoare: mai multe calculatoare **interconectate** şi care **comunică** între ele, astfel încât **utilizatorul** să poată folosi – în limita privilegiilor (permisiuni şi drepturi) - **resursele locale** ale calculatorului dar şi **resurse** aflate **la distanță**.

Pentru sistemele de operare din familia *Windows* care folosesc protocolul TCP/IP, calculatoarele pot fi identificate prin numele NetBIOS dacă este activ protocolul „NetBIOS peste TCP/IP”.



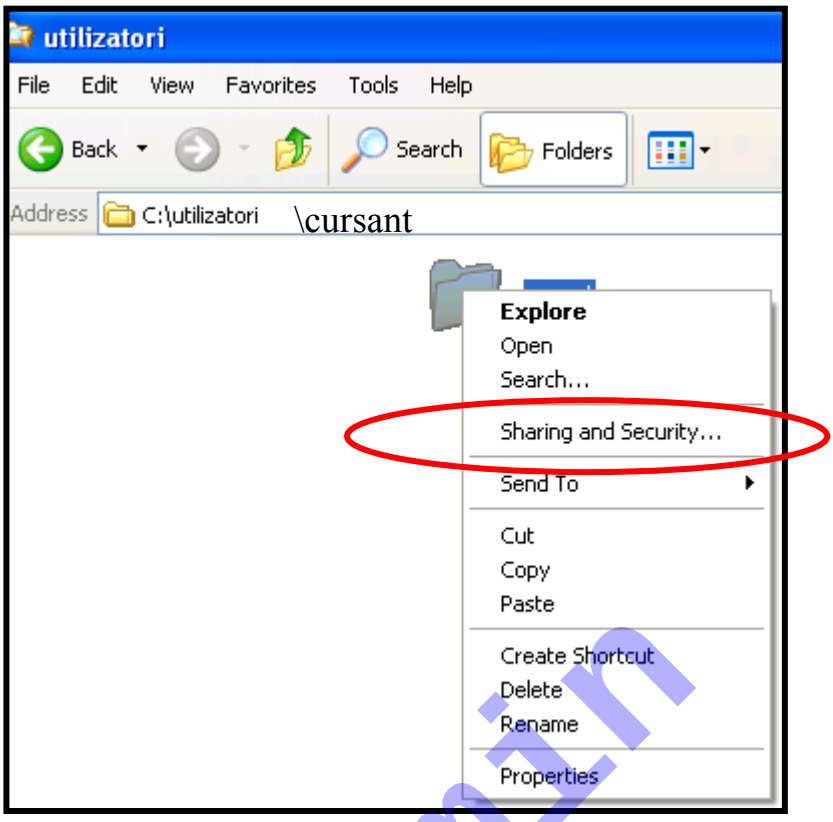
Protocolul „NetBIOS peste TCP/IP” este cel care rezolvă numele NetBIOS al calculatorului, deci calculatorul poate fi identificat prin nume. Este suficient – în aceste condiții – să cunoaştem numele calculatorului din rețea pentru a ajunge la resursele aflate acolo.
Ajungând aici este momentul să verificăm dacă într-adevăr rețeaua funcționează. Vom încerca întâi să folosim aplicația *My Network Places,* în traducere „locurile din rețea care îmi sunt accesibile”

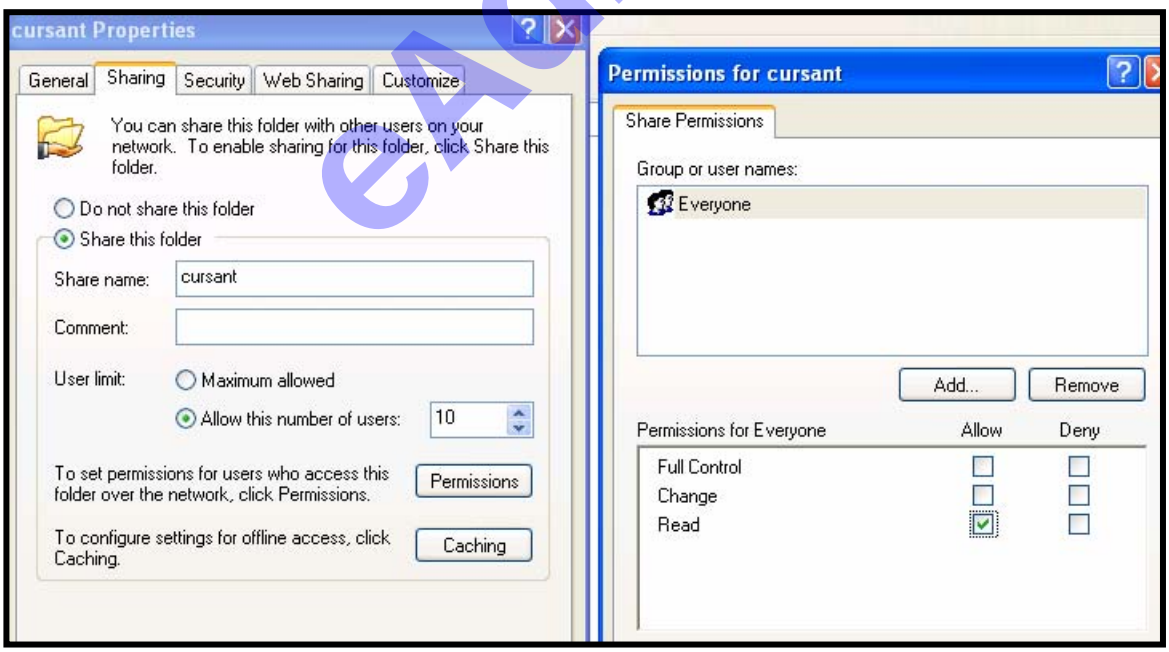


Partajarea resurselor

Resursele partajate sunt cele care pot fi accesate din rețea, adică de utilizatori care folosesc alte calculatoare decât cel care deține resursa. Resursele partajabile sunt dosarele şi imprimantele. Prin partajare se stabilesc – pe de o parte - numele prin care resursa va fi recunoscută în rețea, iar pe de altă parte utilizatorii care o pot folosi precum şi tipul de acces permis. Permisiunile de partajare pot fi asociate individual fiecărui utilizator sau pot fi asociate grupurilor din care fac parte utilizatorii. Pentru aceeaşi resursă partajată se vor specifica permisiuni diferite pentru grupuri sau utilizatori diferiți. Atunci când un utilizator încearcă să se conecteze şi să folosească o resursă aflată la distanță se cunoaşte deja lista grupurilor din care face parte (autentificarea utilizatorilor înseamnă şi stabilirea listei de grupuri din care fac parte). Se construiesc astfel permisiunile de acces pentru resursele aflate la distanță. Dacă un utilizator face parte din mai multe grupuri, atunci permisiunile lui de acces – pentru o resursă aflată la distanță - se obțin prin însumarea celor asociate grupurilor din care face parte şi a celor asociate individual, dacă este cazul. Specificatorul „*deny*” (interzis) este mai puternic decât corespunzătorul „*allow*” (permis).

Pentru a fi disponibile de la distanță resursele trebuie partajate (*share*):





Permisiunile de partajare (*share*) indică tipul de acces permis prin partajare:

Read – asigură:

vizualizarea numelor fişierelor şi subfolderelor
trecerea dintr-un subfolder (subdosar) în altul
vizualizarea (citirea) datelor din fişiere
lansarea în execuție a programelor

Change – asigură permisiunea *Read* plus:

adăugarea de fişiere şi subdosare
modificarea datelor din fişiere
ştergerea subfolderelor şi a fişierelor

Full Control asigură *Read* şi *Change* plus:

Modificarea permisiunilor pentru fişiere şi foldere (în format NTFS)
Luarea în posesie a fişierelor şi dosarelor (în format NTFS)

Atenție: permisiunile de partajare (*share*) au efect numai în situația accesului de la distanță. Pentru accesul la resursele locale nu funcționează aceste restricții!

Imprimantele, la rândul lor, sunt disponibile ca resurse din rețea numai după ce au fost partajate.

Permisiunile de partajare şi efectele lor sunt următoarele:

Print – utilizatorii se pot conecta la imprimantă şi pot transmite documente spre tipărire.

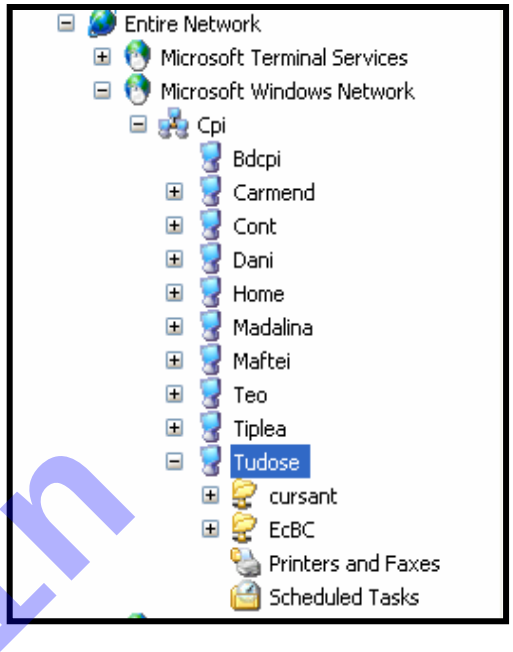
Manage printers – utilizatorii pot executa operațiile permise prin „*print*” şi au în plus controlul complet asupra „obiectului *printer*”. Ei pot modifica valorile asociate caracteristicilor de lucru din „obiectul *printer*”, pot partaja imprimanta, pot modifica permisiunile de partajare existente.

Manage documents – utilizatorii pot rearanja documentele în coada de aşteptare, pot opri sau relua servirea cererilor de tipărire afişate în coada de aşteptare.

Accesul la resursele aflate la distanță

Accesul la resursele aflate la distanță se face în limita permisiunilor de partajare. Pentru accesul la dosare partajate care sunt însoțite şi de permisiuni NTFS cele două seturi de permisiuni se combină. Rezultatul se obține prin intersectarea permisiunilor de partajare cu cele NTFS.

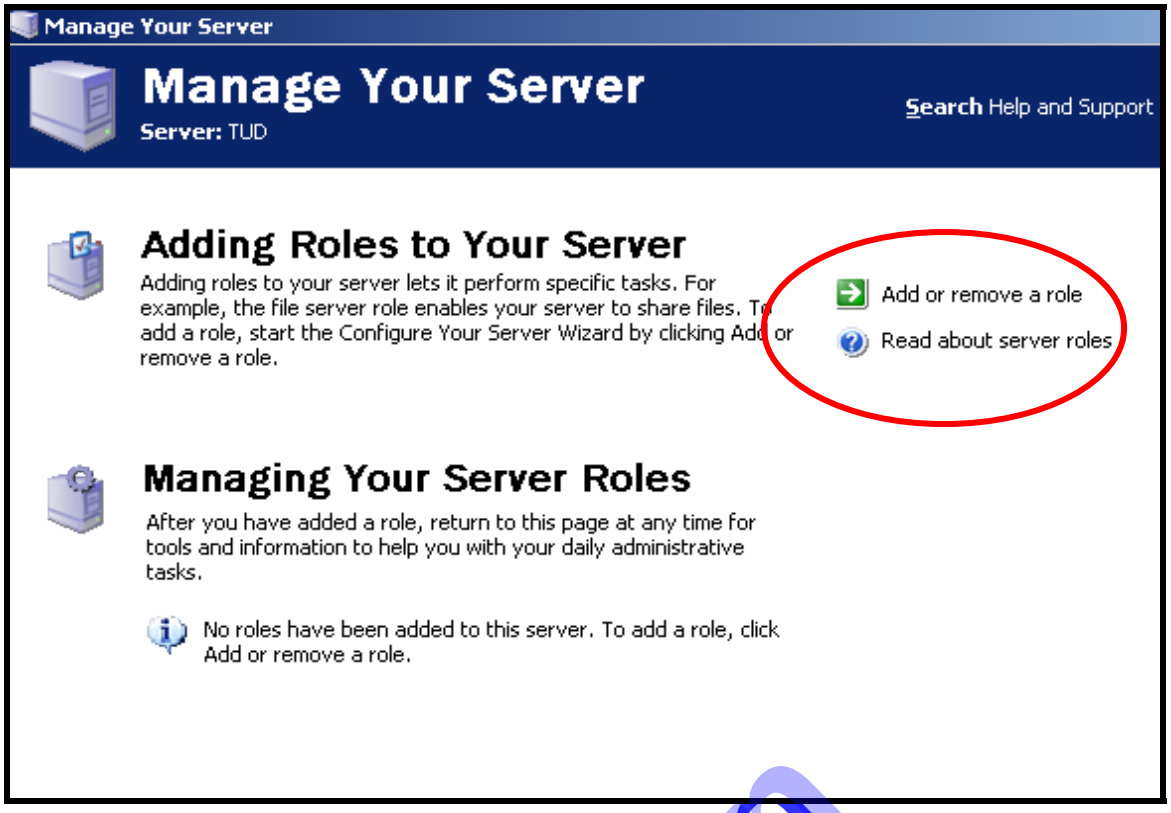
Pentru a ajunge la o resursă aflată la distanță un utilizator trebuie să cunoască numele calculatorului (sau alt identificator al calculatorului) la care doreşte să se conecteze şi numele de partajare al resursei pe care o va folosi. În exemplu care urmează \\duo2 este numele calculatorului, iar \doc este numele de partajare al unei resurse. La fel se întâmplă şi dacă se foloseşte aplicația *My Network Places.*



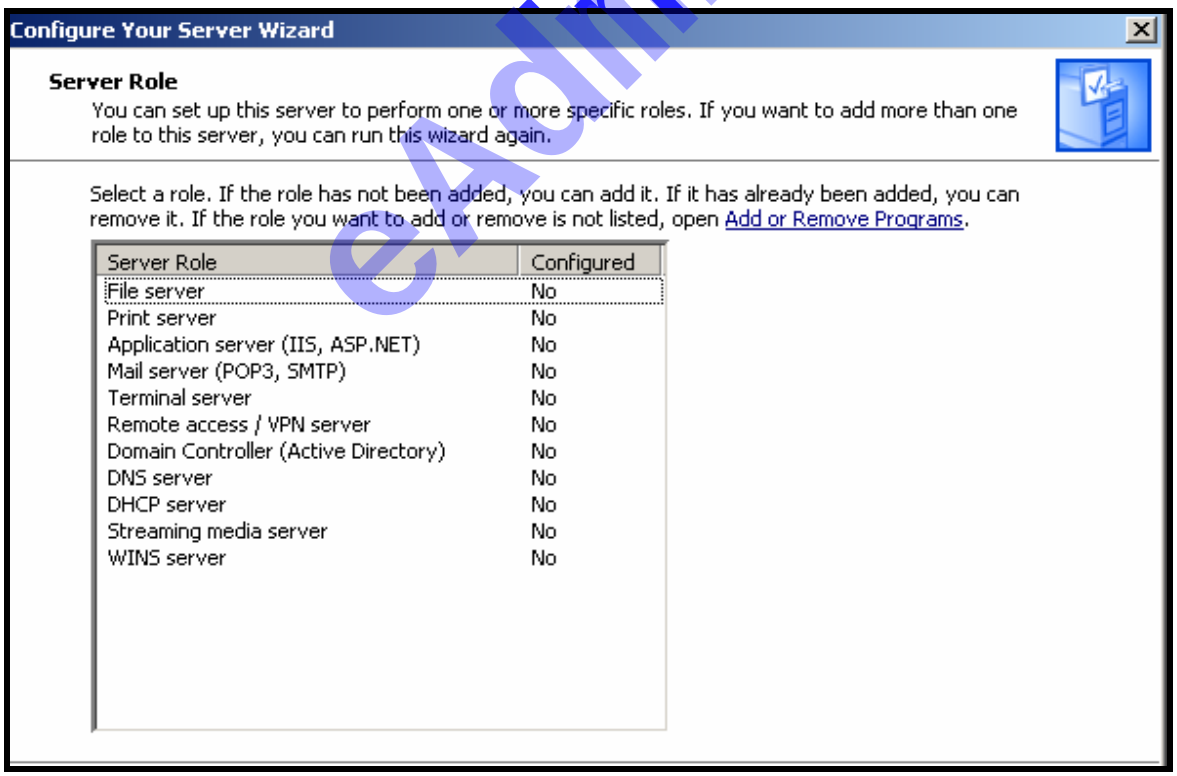
Configurarea serverelor

În sens larg, serverele sunt calculatoarele care pot pune la dispoziție … servicii. Microsoft pune la dispoziție sisteme de operare *Windows Server 2003*, disponibile în ediții diferite, ca de exemplu: *Web Edition, Standard, Enterprise, Datacenter*. Sunt sisteme de operare care pot deține servicii. Serviciile sunt cele care oferă funcționalitate rețelei; rolurile pe care le îndeplineşte un server sunt date de serviciile instalate şi configurate.

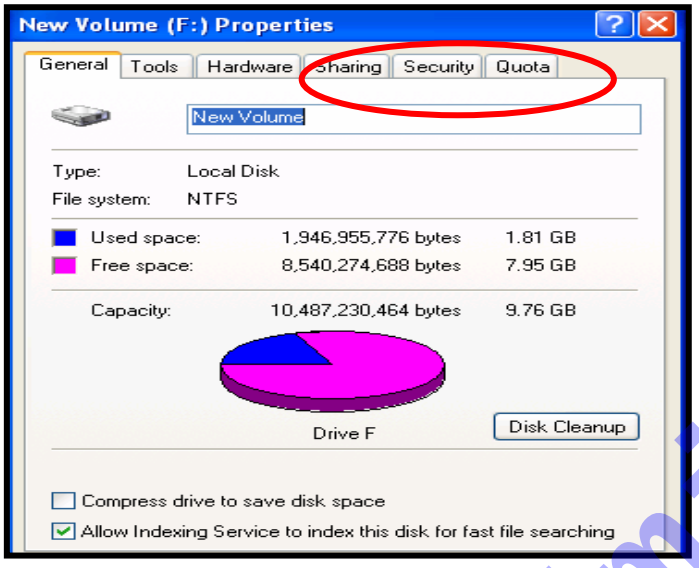
La prima întâlnire cu un sistem de operare server facem cunoştință şi cu aplicația *„Manage your server*”. Este un „vrăjitor” (*wizard*) care îl conduce şi îndrumă pe administrator în activitățile legate de administrarea curentă a rețelei.



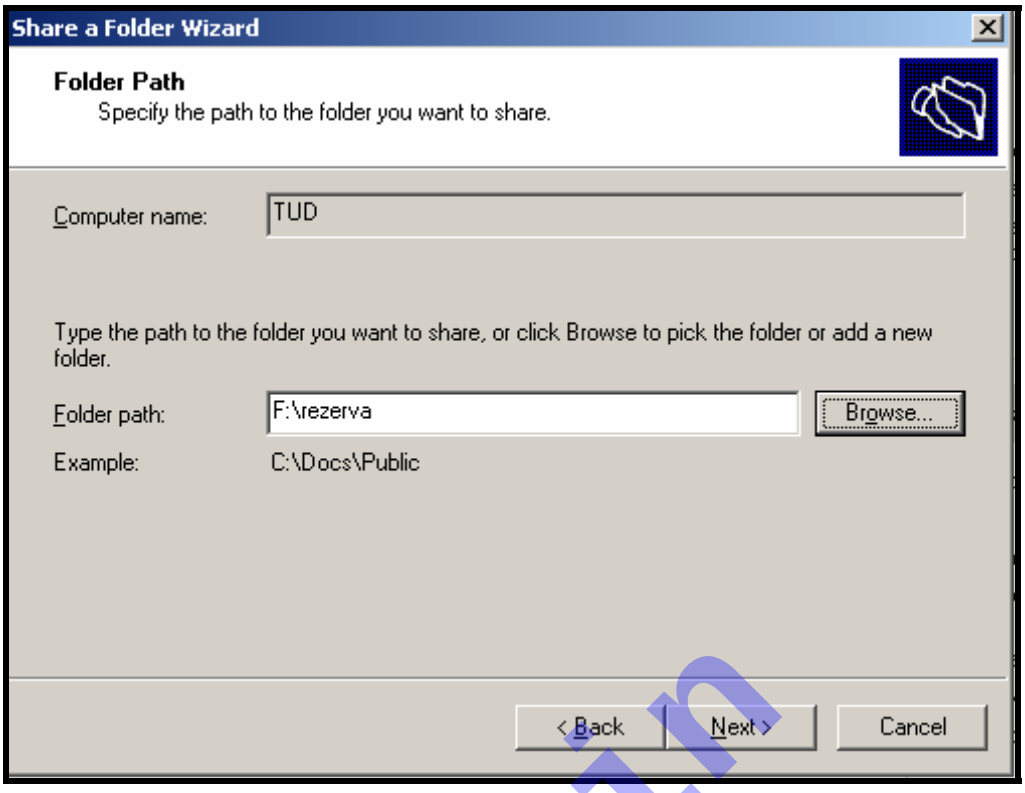
Ceea ce urmează sunt rolurile pe care le poate îndeplini un server *Microsoft Windows Server 2003*:

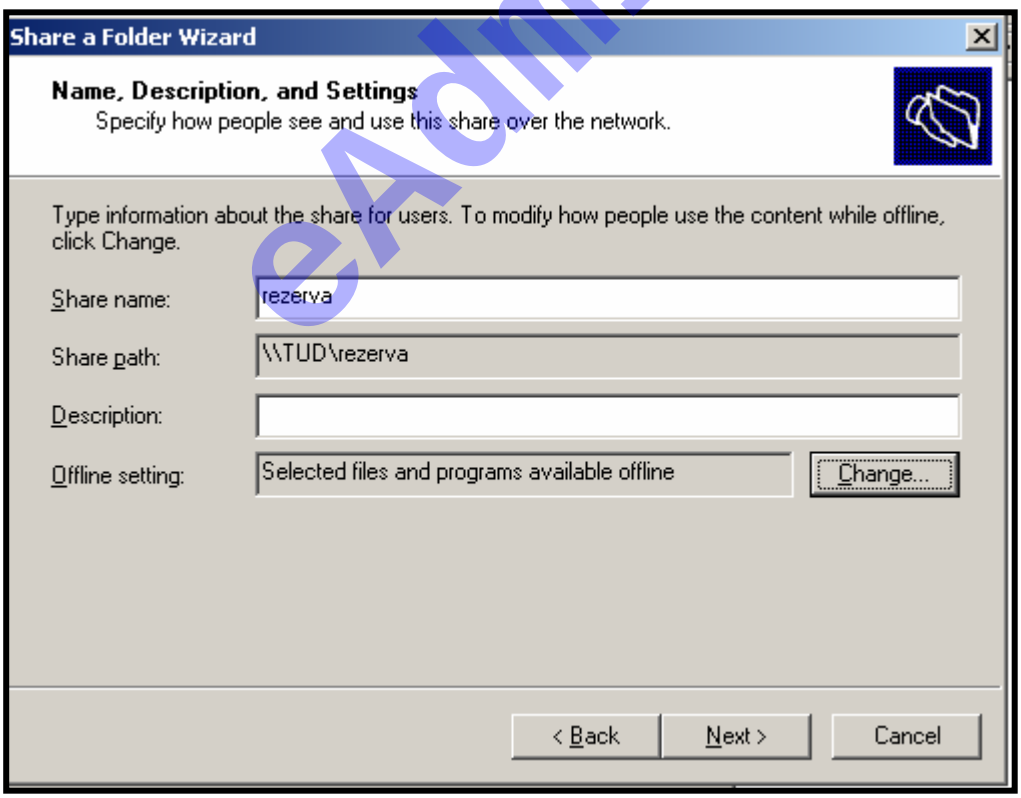


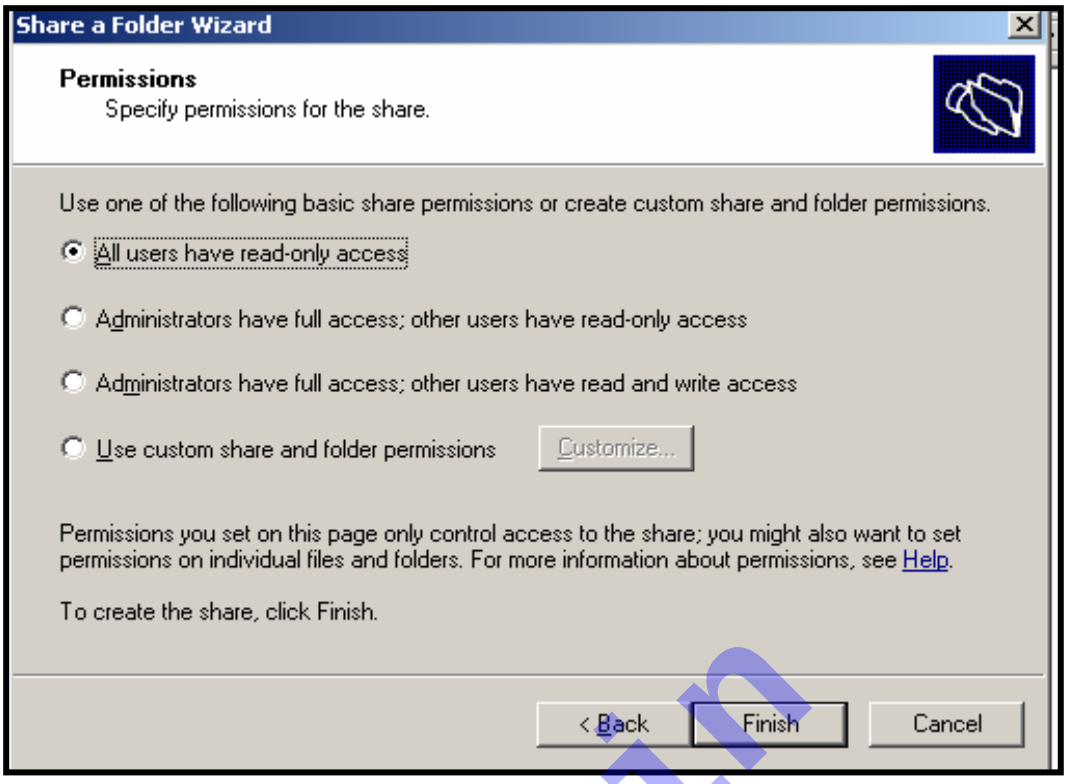
Cel mai simplu rol este cel de server de fişiere. Pentru a fi server de fişiere calculatorul trebuie să fie conectat la rețea, să comunice corect cu celelalte calculatoare din rețea şi să aibă resurse partajate puse la dispoziția utilizatorilor din rețea. Fiind vorba de sistemul de operare *Windows* trebuie să fie activă procedura „*File and Print Server for Microsoft Networks*.” În măsura în care dosarele partajate (*share*) se află pe discuri cu sistem de fişiere NTFS putem vorbi de caracteristici deosebite ale discului şi deci ale serverului de fişiere:



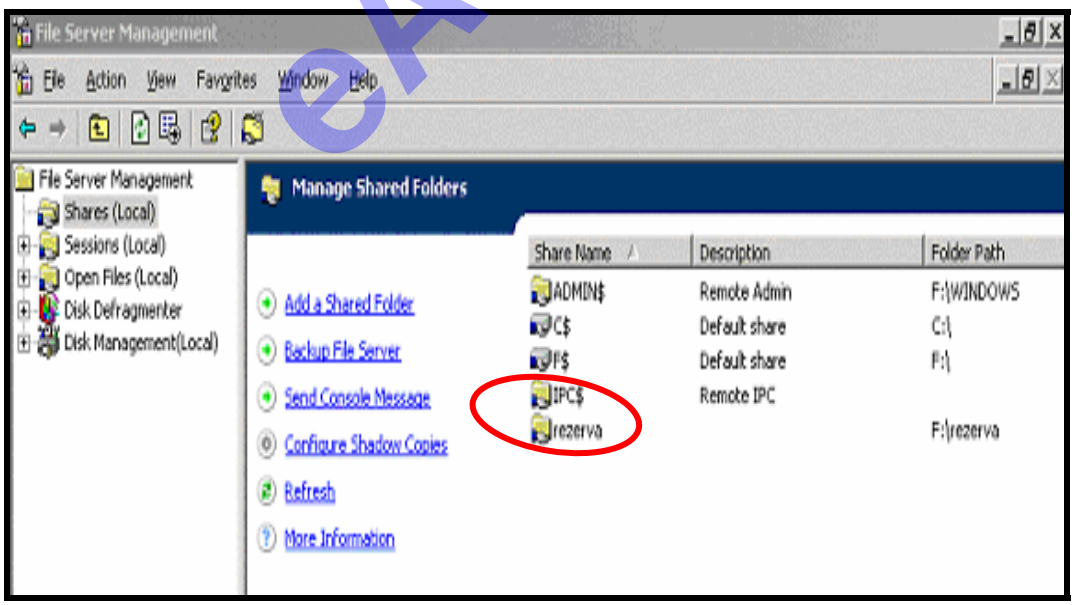
Volumul F: a fost ales drept resursă disponibilă în rețea. Aici se vor afla dosare partajate disponibile utilizatorilor. Fiind vorba de formatul NTFS, caracteristicile hard discului includ: cote alocate pe disc, permisiuni NTFS, posibilitatea de lucru *offline* cu fişierele, alături de permisiunile de partajare.

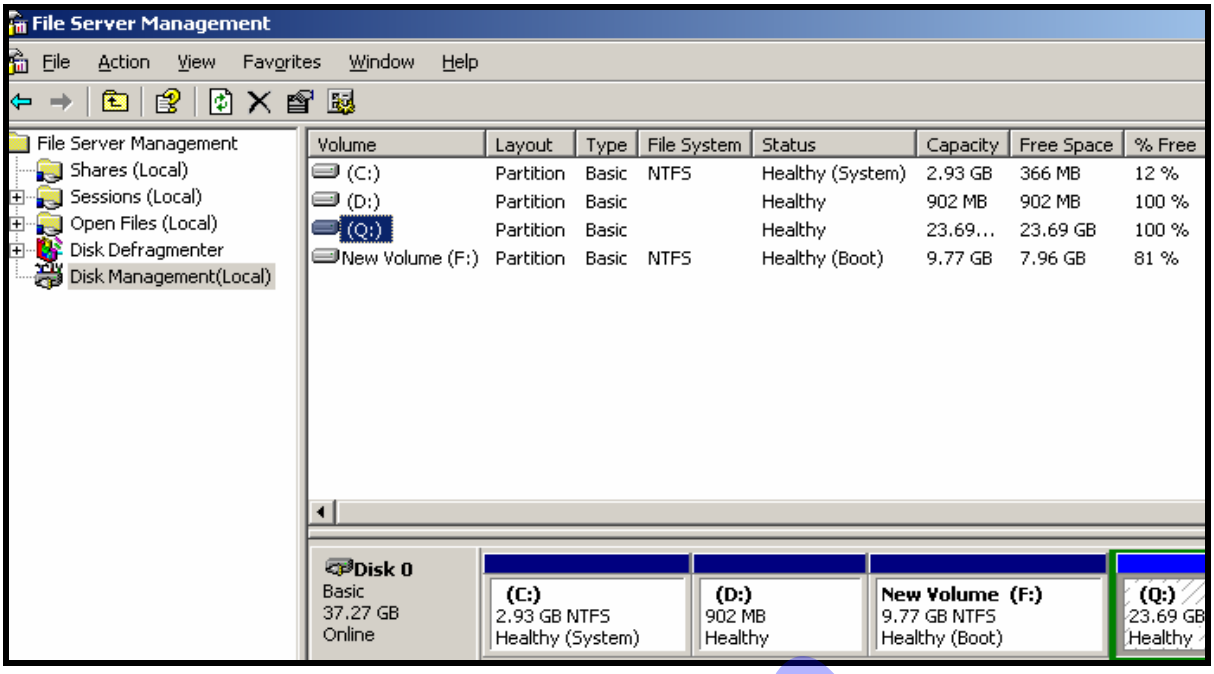

Share a Folder Wizard
Folder Path
Specify the path to the folder you want to share.
Computer name:
TUD
Type the path to the folder you want to share, or click Browse to pick the folder or add a new folder.
Folder path:
F:\rezerva
Browse...
Example:
C:\Docs\Public
< Back
Next >
Cancel


Share a Folder Wizard
Name, Description, and Settings
Specify how people see and use this share over the network.
Type information about the share for users. To modify how people use the content while offline, click Change.
Share name:
rezerva
Share path:
\\TUD\rezerva
Description:
Offline setting:
Selected files and programs available offline
Change...
< Back
Next >
Cancel

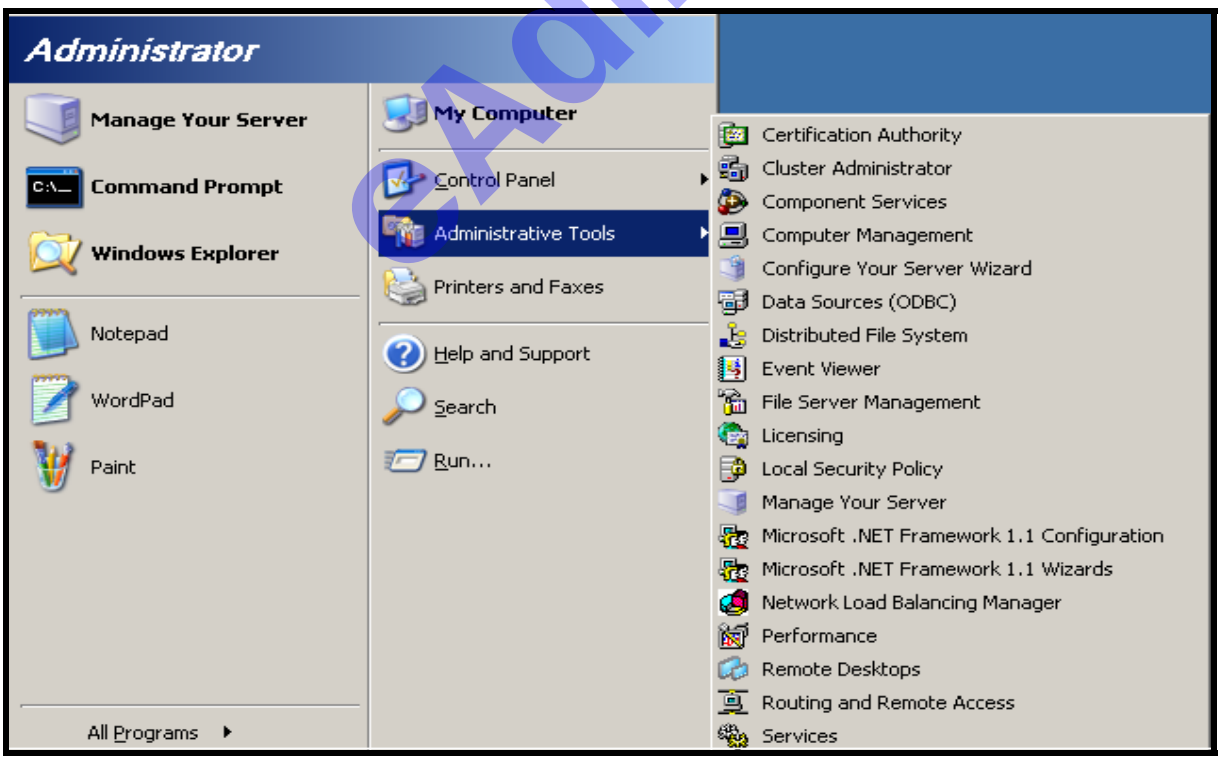


Spre final facem cunoştință cu un format nou al aplicației „*Computer Management*”:



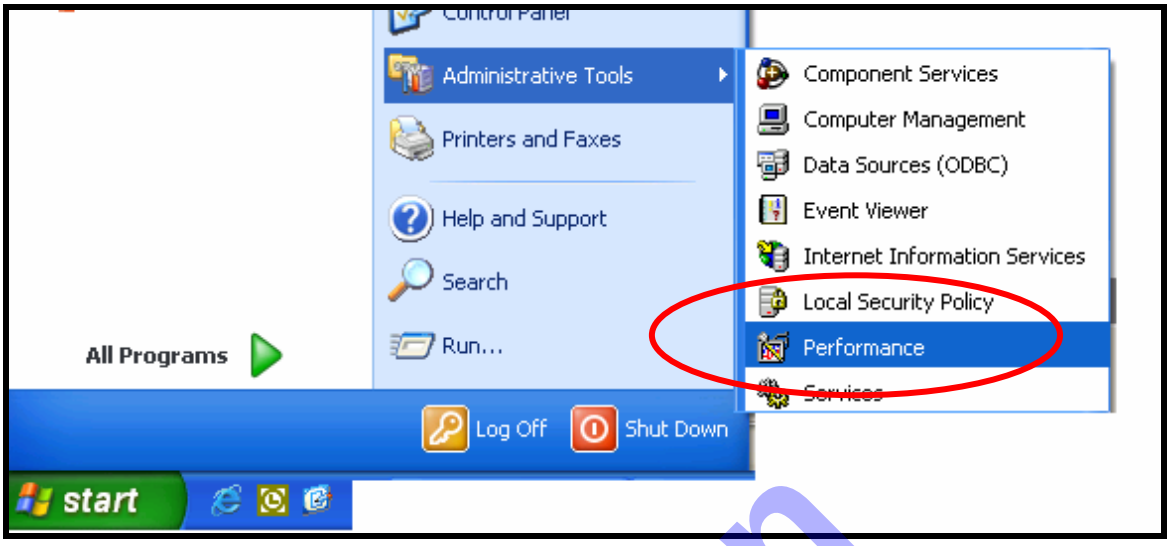


Manage Your Server nu este decât unul dintre utilitarele care stau de la început la îndemâna administratorului. Pentru administratorul local al calculatorului sunt disponibile implicit următoarele utilitare, grupate sub numele „*Administrative Toos*” (Instrumente de administrare).



Strategii locale de securitate. Drepturile utilizatorilor. Strategia de audit.

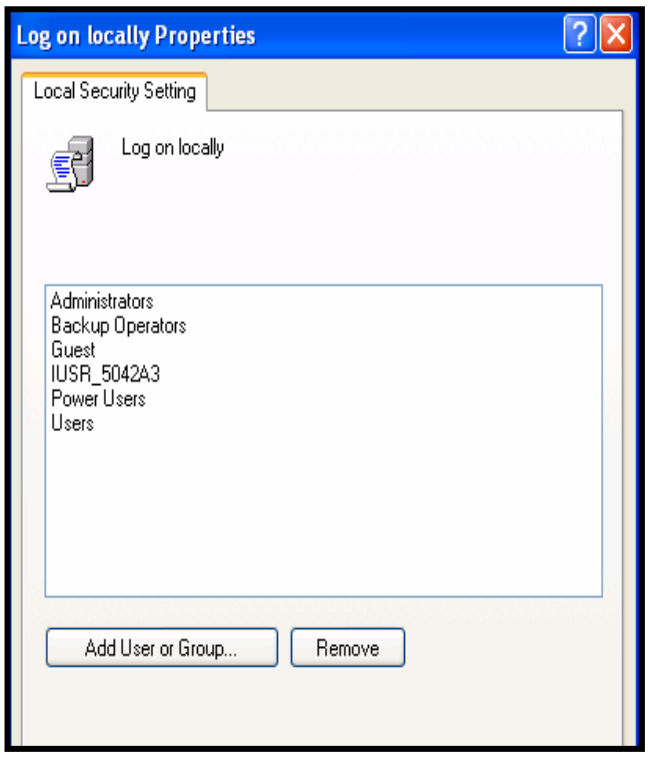
Politicile (numite şi strategii) de securitate sunt implementate prin ceea ce se numeşte „*Local Security Policy*” (Politica Locală de Securitate).



Aici identificăm pentru moment politici (strategii) care se referă la:

- politica conturilor locale
  - parole
  - blocarea conturilor
- politici locale
  - audit
  - drepturile utilizatorilor
  - opțiuni de securitate

Pentru deschiderea de sesiune – în afară de politicile asociate conturilor mai trebuie avute în vedere şi drepturile utilizatorilor. Pot face „*logon* ” acei utilizatori care au dreptul „*Logon locally*”.



Remarcăm aici grupul „*Users*”, acoperitor pentru toți utilizatorii locali. În plus e vorba despre utilizatori care nu au alte **restricții, legate de parolă** sau de **blocarea conturilor.**

Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	0
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store password using reversible encryption for all users in the domain	Disabled

Policy	Security Setting
Account lockout duration	Not Applicable
Account lockout threshold	0 invalid logon attempts
Reset account lockout counter after	Not Applicable

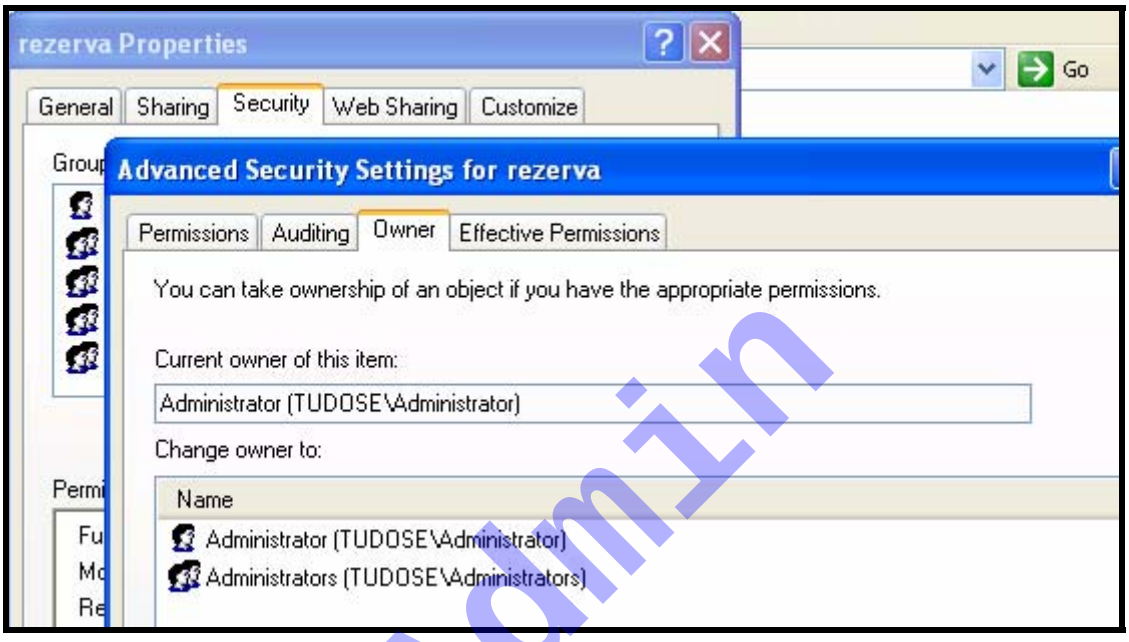
În mod implicit regulile de securitate implementate nu specifică nimic la aceste capitole; sarcina Administratorului este însă şi aceea de a nu lăsa pe oricine să folosească orice calculator!

Din categoria drepturilor utilizatorilor vom remarca în cele ce urmează „preluarea posesiei asupra fişierelor şi a dosarelor”, adică:

Take ownership of files or other objects	Administrators

Administratorii (grupul local de Administratori) sunt singurii în măsură să devină proprietarii fişierelor şi ai dosarelor. Proprietarul are – sau îşi arogă – toate permisiunile asupra obiectelor. Cu alte cuvinte, o dată deveniți proprietari, Administratorii pot modifica permisiunile asociate dosarelor şi fişierelor.

Obiectele (foldere / dosare şi fişiere) din volume NTFS sunt însoțite de câteva caracteristici importante: proprietar (*owner*) şi procedura de *audit* (sau procedura de supraveghere):

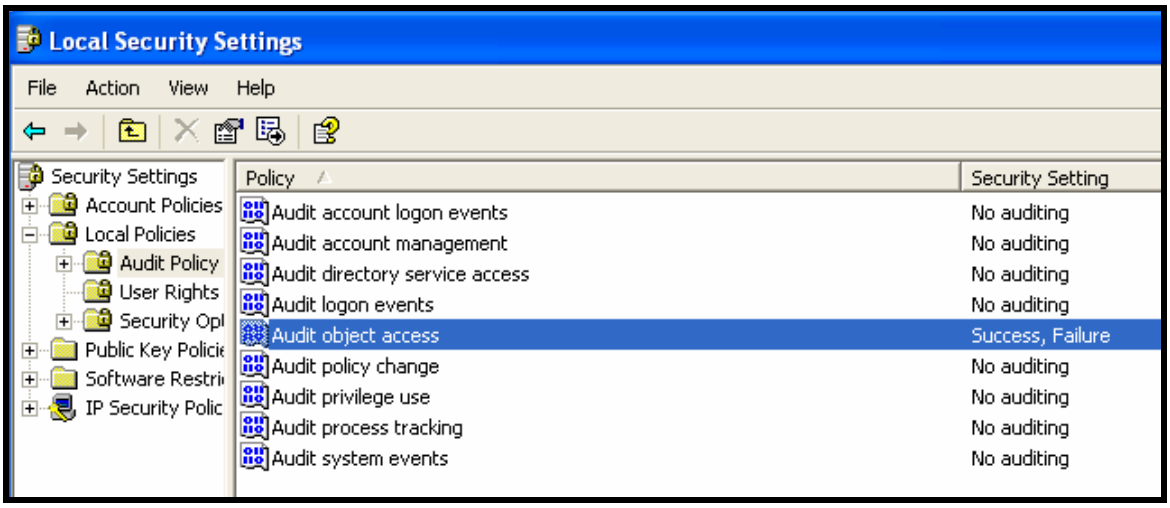


De multe ori administratorul este interesat să ştie care au fost acțiunile utilizatorilor, dacă ele au fost în concordanță sau nu cu limitările – restricțiile – dorite de administrator. Într-o astfel de situație, administratorul porneşte o activitate de supraveghere a accesului la diferite obiecte recunoscute de sistemul de operare.

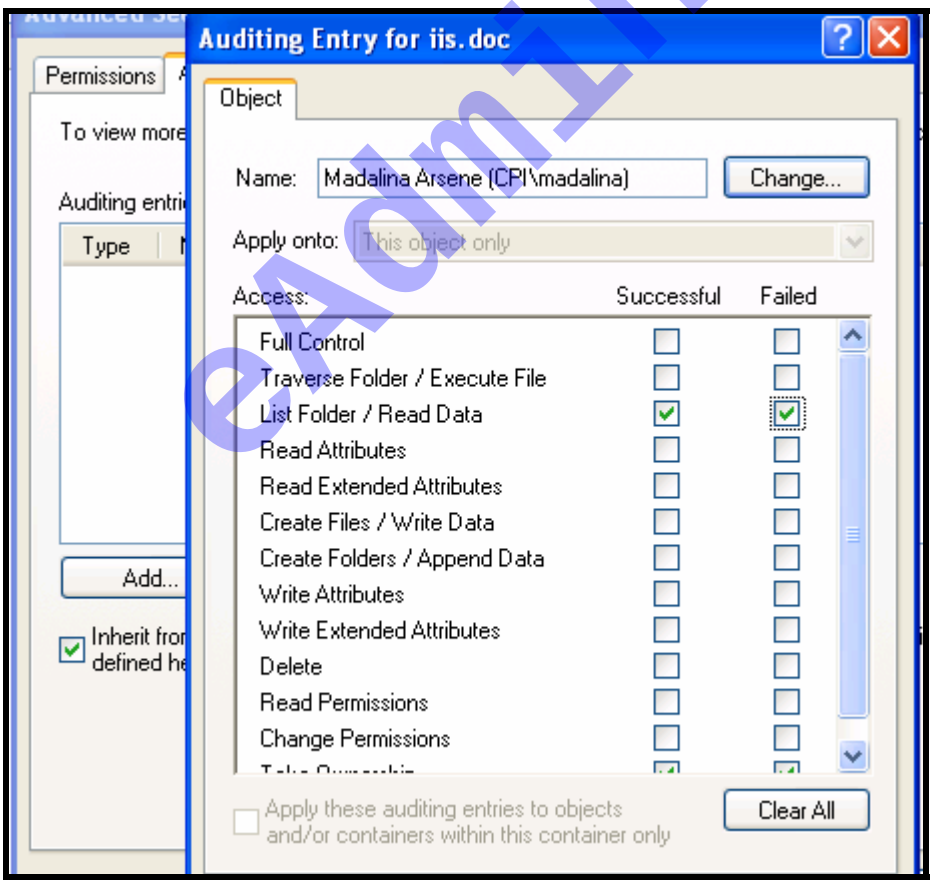
Operația de audit va funcționa după parcurgerea următoarei succesiuni de paşi:

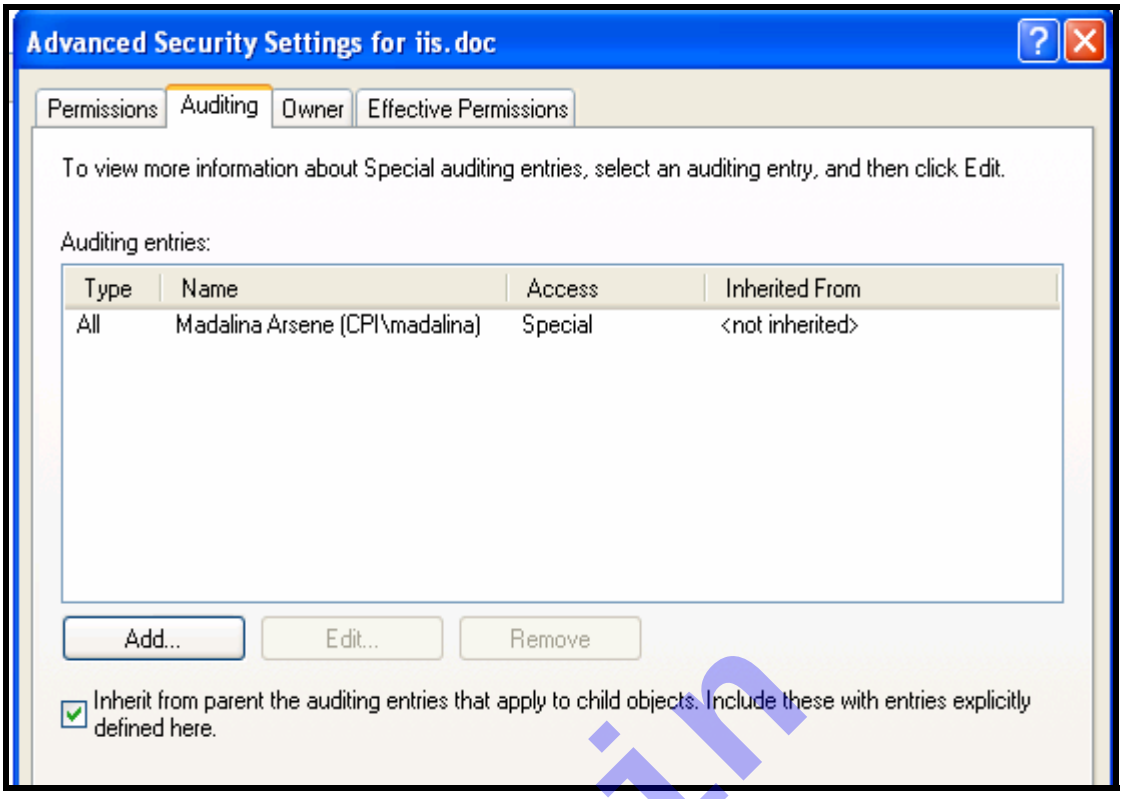
1. Activarea operației de audit pentru dosare şi fişiere.

Este vorba despre activarea procedurii de audit din „*Local Security Policy*”. Auditul (supraveghere) se va referi la accesul la obiecte (dosare şi fişiere). Vor fi supravegheate toate încercările de acces, atât cele reuşite cât şi cele nereuşite („*success*” şi „*failure*”).



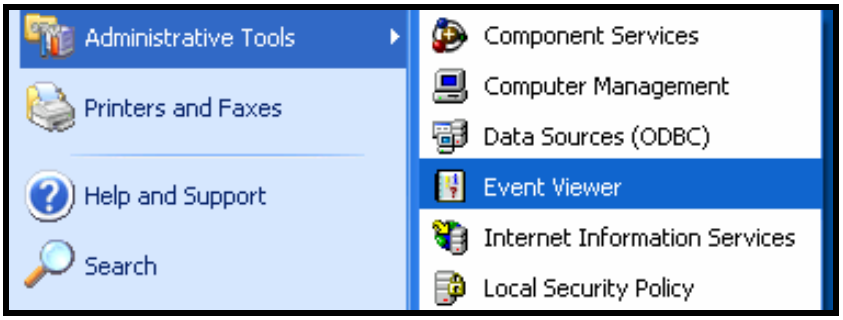
2. Alegerea obiectelor supuse supravegherii şi persoanele supravegheate (utilizatori şi / sau grupuri).

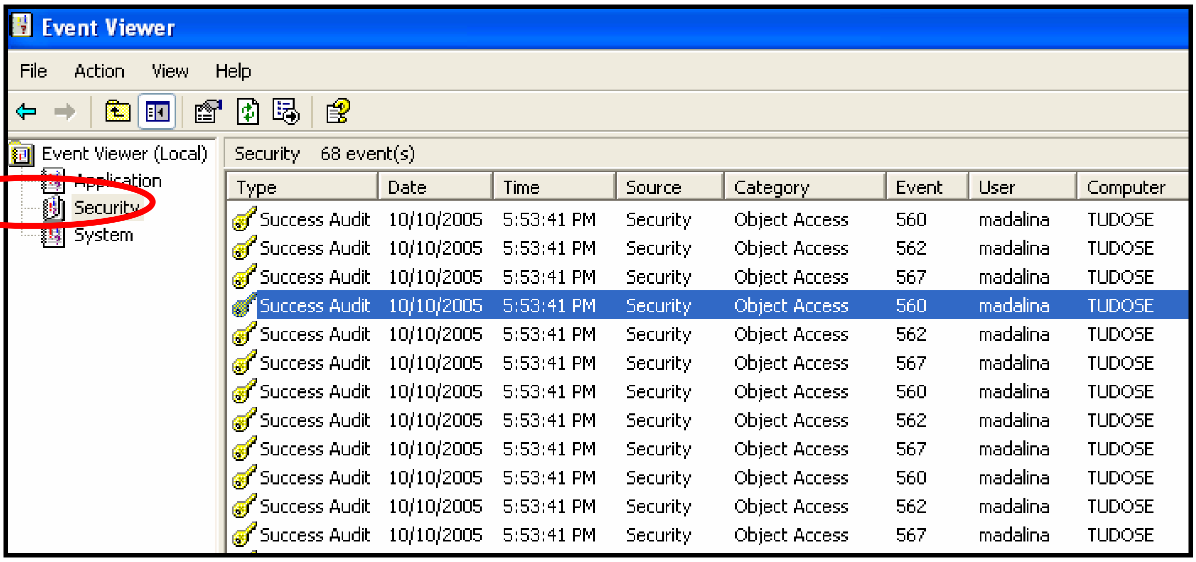




După cum au fost configurate condițiile de audit, va fi supravegheat utilizatorul CPI\madalina şi îi vor fi evidențiate încercările de citire a fişierului şi cele de preluare a posesiunii!

3. În măsura în care utilizatorul va lucra cu fişierul şi va efectua – sau măcar va încerca să efectueze – operațiile marcate, în aceeaşi măsură operațiile vor fi înregistrate în **jurnalul evenimentelor** legate de **regulile de securitate** a accesului la resurse.




Event Viewer
File Action View Help
Event Viewer (Local)
Application
Security
System
Security 68 event(s)
Type Date Time Source Category Event User Computer
Success Audit 10/10/2005 5:53:41 PM Security Object Access 560 madalina TUDOSE
Success Audit 10/10/2005 5:53:41 PM Security Object Access 562 madalina TUDOSE
Success Audit 10/10/2005 5:53:41 PM Security Object Access 567 madalina TUDOSE
Success Audit 10/10/2005 5:53:41 PM Security Object Access 560 madalina TUDOSE
Success Audit 10/10/2005 5:53:41 PM Security Object Access 562 madalina TUDOSE
Success Audit 10/10/2005 5:53:41 PM Security Object Access 567 madalina TUDOSE
Success Audit 10/10/2005 5:53:41 PM Security Object Access 560 madalina TUDOSE
Success Audit 10/10/2005 5:53:41 PM Security Object Access 562 madalina TUDOSE
Success Audit 10/10/2005 5:53:41 PM Security Object Access 567 madalina TUDOSE
Success Audit 10/10/2005 5:53:41 PM Security Object Access 560 madalina TUDOSE
Success Audit 10/10/2005 5:53:41 PM Security Object Access 562 madalina TUDOSE
Success Audit 10/10/2005 5:53:41 PM Security Object Access 567 madalina TUDOSE

Propunere de temă practică

1. Identificați numele calculatorului dumneavoastră (inclusiv apartenența la un grup de lucru sau la un domeniu). Identificați adresa IP a conexiunii de rețea. Identificați şi notați principalele caracteristici ale calculatorului pe care îl folosiți:

Tip procesor
Dimensiune memorie
Tip de hard disc, capacitate
Periferice ataşate
Sistemul de operare instalat
Caracteristicile conexiunii la rețea

Notați răspunsurile – inclusiv metoda de rezolvare.

2. Ce aplicații sunt instalate pe calculatorul dumneavoastră? Dar servicii? Ce aplicații sunt active în acest moment? Notați orice fel de observații, inclusiv metoda de rezolvare!

3. Construiți un cont utilizator local. Verificați dacă poate face „*Shut down”* şi în caz contrar faceți cuvenitele modificări. Deschideți sesiunea folosind contul creat. Configurați ecranul *desktop* plasând câteva scurtături (*shortcut*). Terminați cu „*Shut down”.* Deschideți o noua sesiune de lucru folosind acelaşi nume de utilizator. Observați dacă modificările aduse imaginii *desktop* au rămas aceleaşi. Cum explicați? Notați orice fel de observații, inclusiv metoda de rezolvare!

4. Continuați exercițiul 3. Pentru acelaşi utilizator creați un folder personal de lucru, unde îşi poate păstra în siguranță lucrările, fişierele. Partajați acest dosar pentru a putea fi folosit în rețea. Verificați, testați ce utilizatori pot avea acces la folder şi la conținutul lui.

5. Continuați exercițiul 4. De la mai multe calculatoare mai mulți utilizatori se conectează la resursa partajată şi citesc fişierele aflate acolo. Care sunt utilizatorii conectați acum, de la ce calculator s-au conectat, ce fişiere citesc?

6. Notați-vă caracteristicile aplicațiilor: *Computer Management, Event Viewer* şi *Performance Monitor*. Folosiți orice posibilitate de *help on line* pentru a învăța cum se utilizează ele. Nu uitați: notați orice fel de observații, inclusiv metoda de rezolvare!

Ce ați învățat în acest modul?

- ✓ să identificați deosebirile dintre grupurile de lucru şi domenii
- ✓ să folosiți conturile utilizatorilor pentru accesul la resursele locale şi la resurse aflate la distanță
- ✓ să folosiți grupurile de utilizatori
- ✓ să identificați şi să folosiți drepturile şi permisiunile utilizatorilor
- ✓ să partajați resurse şi să asigurați utilizatorilor accesul la resursele partajate în rețea
- ✓ să supravegheați (*audit*) accesul utilizatorilor la resurse