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 materialui de instruire: V2.0

5. Administrarea Serverelor

Introducere

Una dintre sarcinile importante ale administratorului de rețea este cea de administrare a serverelor. Pentru că de cele mai multe ori administratorul se află ceva mai departe de serverul pe care doreşte să îl controleze, trebuie cunoscute şi înțelese mecanismele şi instrumentele administrării de la distanță (*remote administration*).
Pentru administrarea unui server sunt necesare permisiuni. Una dintre metodele de oferire a permisiunilor este folosirea grupurilor prestabilite (*Builtin*), fie ele grupuri locale calculatorului sau domeniului (locale domeniului).
Într-un domeniu, grupurile preconstruite aparțin serviciului director *Active Directory*. Ele au asociate permisiuni prestabilite care asigură accesul limitat al membrilor grupurilor la componentele sistemului. Grupurile preconstruite nu pot fi şterse.
Cele mai importante grupuri preconstruite locale domeniului – şi nivelul permisiunilor asociate – sunt:
▪ ***Administrators.*** Membrii grupului *Administrators* – grup preconstruit local domeniului - pot executa toate operațiile admise de sistemul de operare. Administratorii îşi pot oferi orice drept (*„user right")* de care au nevoie şi pe care nu l-au primit implicit. Apartenența la grupul local domeniului *Administrators* ar trebui să fie restricționată: numai utilizatorii care au nevoie de acces deplin la funcțiile sistemului şi în care se poate avea deplină încredere ar putea face parte din acest grup. Deschiderea de sesiune folosind un cont de administrator se va face numai atunci când este nevoie neapărat.
Adăugarea utilizatorilor în acest grup trebuie făcută cu atenție.
De exemplu: dacă un tehnician are sarcina de a se ocupa de imprimantele organizației în care lucrează, atunci va fi inclus în grupul preconstruit *Print Operators* şi nu în *Administrators*.
▪ ***Backup Operators.*** Membrii grupului preconstruit local domeniului *Backup Operators* pot face salvarea (*backup*) şi restaurarea (*restore*) fişierelor folosind utilitarul *Backup*.
▪ ***Account Operators***. Membrii acestui grup pot gestiona conturile utilizatorilor, conturile de grup, si cele de calculator. Sunt exceptate grupurile *Administrators* şi cele de tip *Operator* pentru care operațiile de administrare pot fi efectuate numai de membrii grupului *Administrators* (grup preconstruit local domeniului).
▪ ***Server Operators***. Membrii grupului pot partaja resursele sistemului, pot deschide sesiune de la un server membru al domeniului, pot crea şi şterge partajări ale rețelei, pot lansa şi opri din execuție servicii, pot formata hard discurile serverului, pot porni şi opri calculatorul. În altă ordine de idei, pot salva şi restaura fişiere folosind utilitarul *Backup*.

▪ ***Print Operators.*** Membrii acestui grup pot construi obiecte *printer* (atât de tip local cât şi în rețea) pentru asigurarea conectării utilizatorilor la imprimantele disponibile. O dată conectați, utilizatorii vor putea folosi aceste resurse.
Folosirea grupurilor preconstruite locale domeniului şi nivelul permisiunilor asociate implicit acestora pot proteja resursele, în situația existenței unor breşe de securitate. Administratorul de sistem trebuie să facă parte din grupul cel mai restrictiv care îi oferă însă drepturile şi permisiunile necesare îndeplinirii propriilor sarcini.
Exemplu: un administrator de sistem care administrează numai imprimantele şi salvează fişiere va face parte din grupul *Print Operators* şi i se va oferi dreptul de a face *Backup*.

Comanda *Run as*

Un calculator folosit de un utilizator membru al grupului *Administrators* este un calculator vulnerabil în fața atacurilor de tip „cal troian" şi a operațiilor care folosesc breşele de securitate existente. Simpla vizitare a unor *site-uri Internet* ca şi deschiderea unor fişiere ataşate *e-mail*-urilor pot afecta funcționarea sistemului de operare: pot conține cod care o dată descărcat (*download*) se va propaga în sistem afectându-i funcționarea.

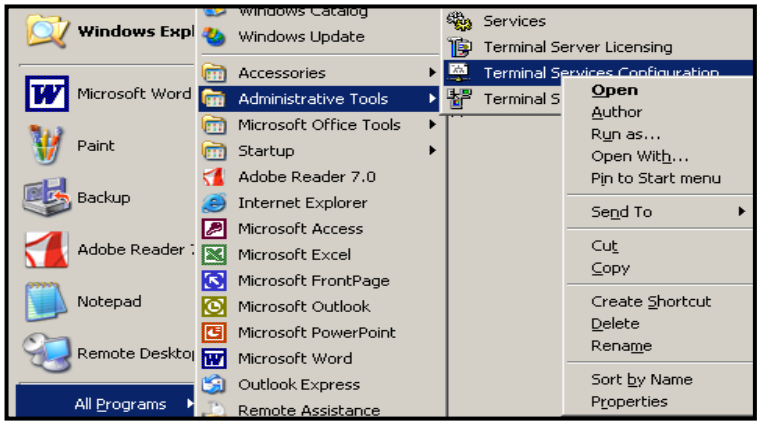
Intr-un domeniu, membrii grupului global *Domain Admins* sunt în mod automat adăugați drept membri ai grupurilor *Administrators*, atât cel local domeniului cat şi cele locale fiecărui calculator. Alte grupuri preconstruite nu au membri impliciți.

Administratorii pot folosi pentru deschiderea de sesiune conturi fără privilegii administrative şi – ori de câte ori este nevoie – pot apela la caracteristica de lucru numită ***Run as…***(*log on* secundar). Ori de câte ori va fi nevoie de lansarea în execuție a unei componente care face uz de privilegii administrative, administratorul va folosi acreditările (*credentials*) asociate unui cont cu privilegii suficiente. Acest mod de lucru asigură o mai mare securitate rețelei, limitând expunerea sistemelor pe toată durata efectuării operațiilor non-administrative.

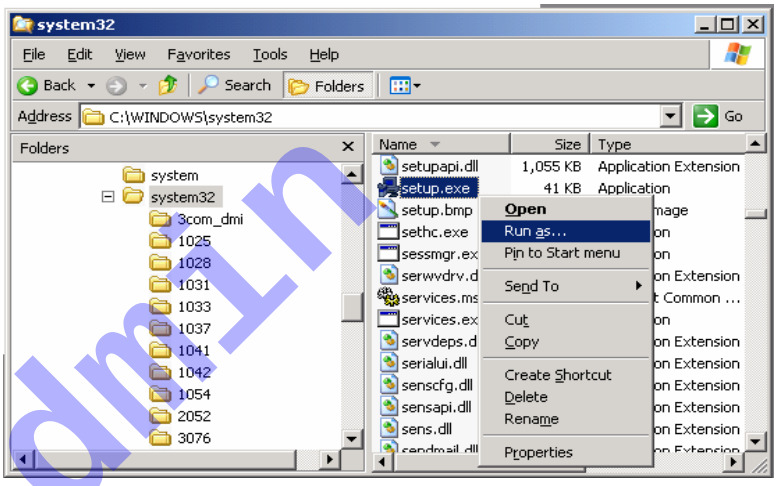
Pentru administrarea calculatorului local sau a unuia aflat la distanță se poate folosi procedura ***Run as*** pentru deschiderea consolelor *mmc* construite anterior. Comanda ***Run as*** permite accesul la serviciile şi instrumentele de administrare incluse în console, asigurând şi permisiunile necesare (aşa cum au fost ele definite pentru contul utilizator folosit la ***Run as***). Deşi comanda ***Run as*** a fost concepută pentru uzul administratorului, ea poate fi folosită de orice persoană care dispune de mai multe conturi utilizator şi care poate lansa astfel în execuție programe diferite având privilegii diferite, fără să mai fie nevoie de închiderea sesiunii curente *(log off).*

Exemple de folosire a comenzii *Run as*:

- Din meniul *Start* se ajunge la pictograma dorită (ex. *Terminal Services Configuration*) pe care se face clic dreapta.



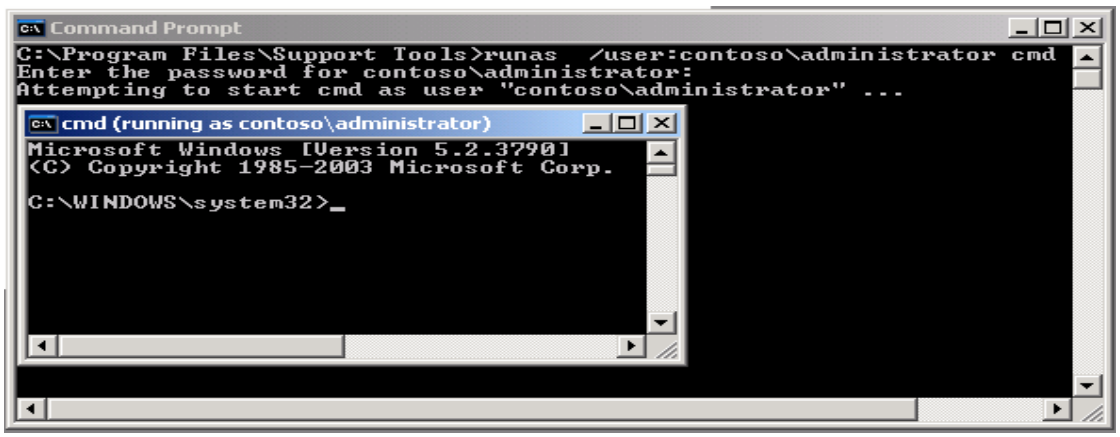
- Clic dreapta pe aplicația dorită, afişată în fereastra *Windows Explorer*



- Comanda *Run as* lansată din fereastra *Command Prompt* poate fi folosită cu una din sintaxele:

runas */user*:nume_de_domeniu\nume_utilizator nume_program

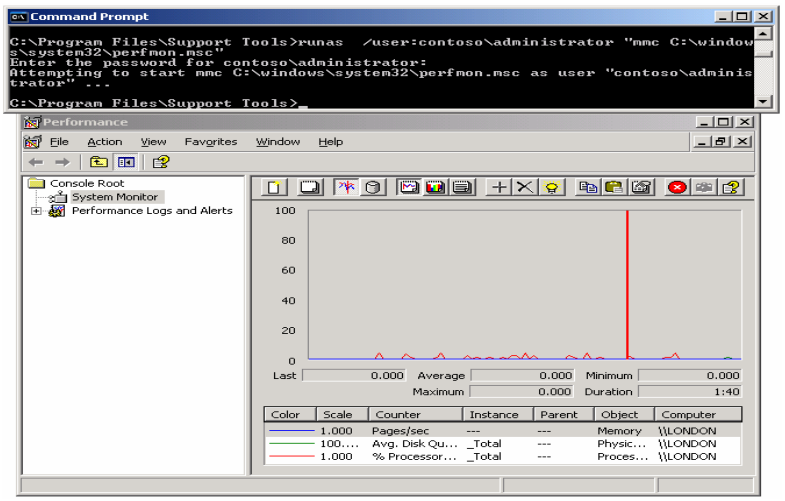
runas */user*:contoso\administrator cmd



runas /user:nume_de_domeniu\nume_utilizator ”*mmc* %windir%system32\ nume.msc”

runas /user:contoso\administrator "mmc C:\windows\system32\perform.msc"

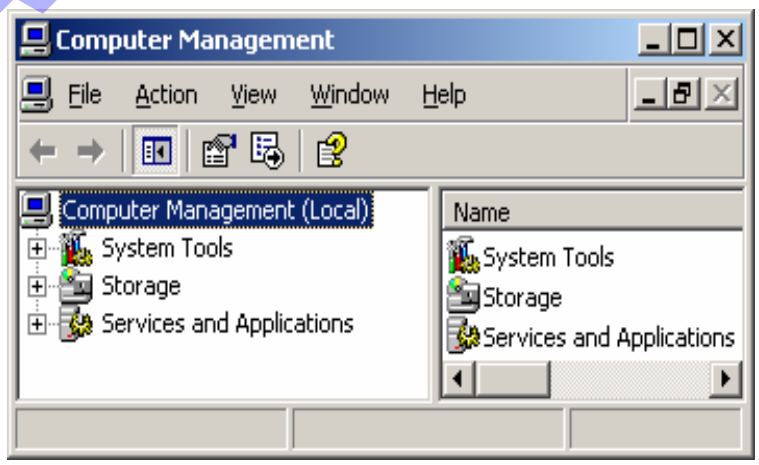
În urma lansării comenzii de mai sus, apare fereastra aplicației *Performance*.



Instrumente de administrare

Computer Management

Computer Management se compune dintr-o colecție de instrumente administrative folosite pentru administrarea calculatorului local sau a unuia aflat la distanță (*remote*).

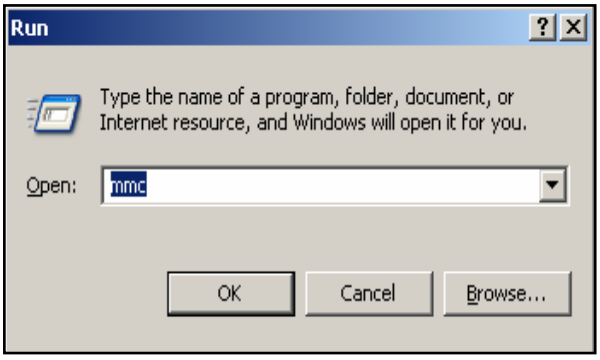


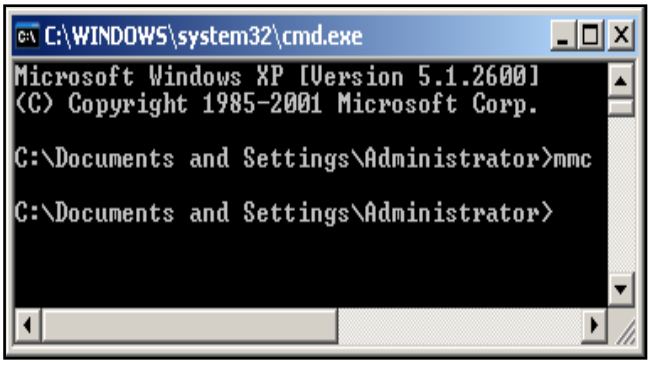
Consola ***Computer Management*** organizează instrumentele pe categorii:

- Instrumente sistem (*System Tools*)
- Depozite de date (*Storage*)
- Servicii şi Aplicații (*Services and Applications*)

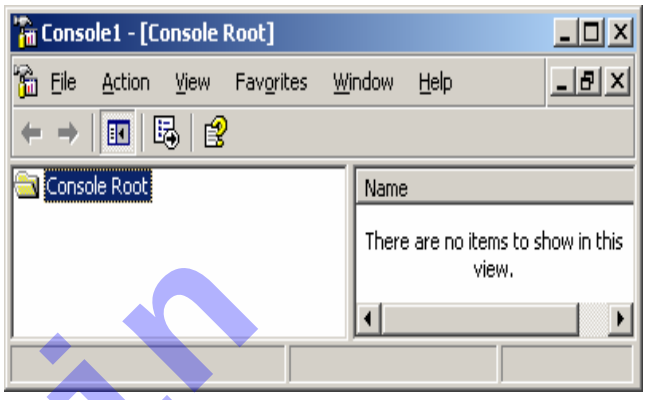
Consola *mmc*

Consola ***mmc*** (*Microsoft Management Console*) asigură interfața pentru utilizarea unitară a instrumentelor de administrare. Ea poate fi lansată prin una din variantele:

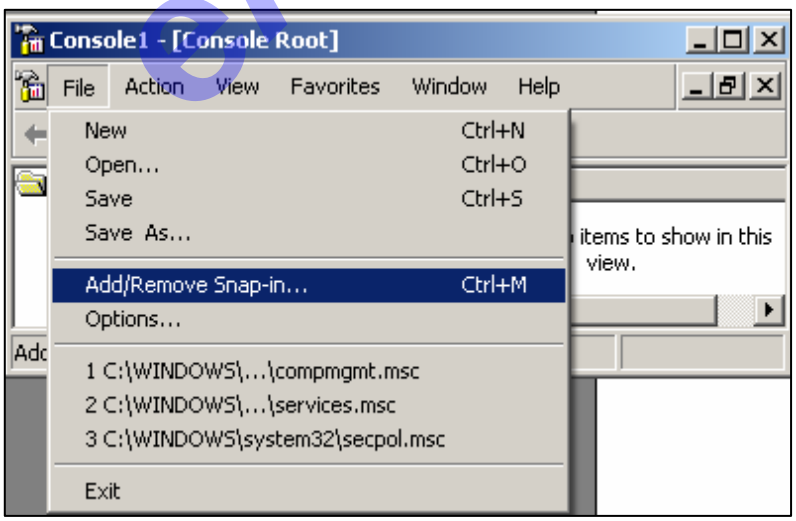




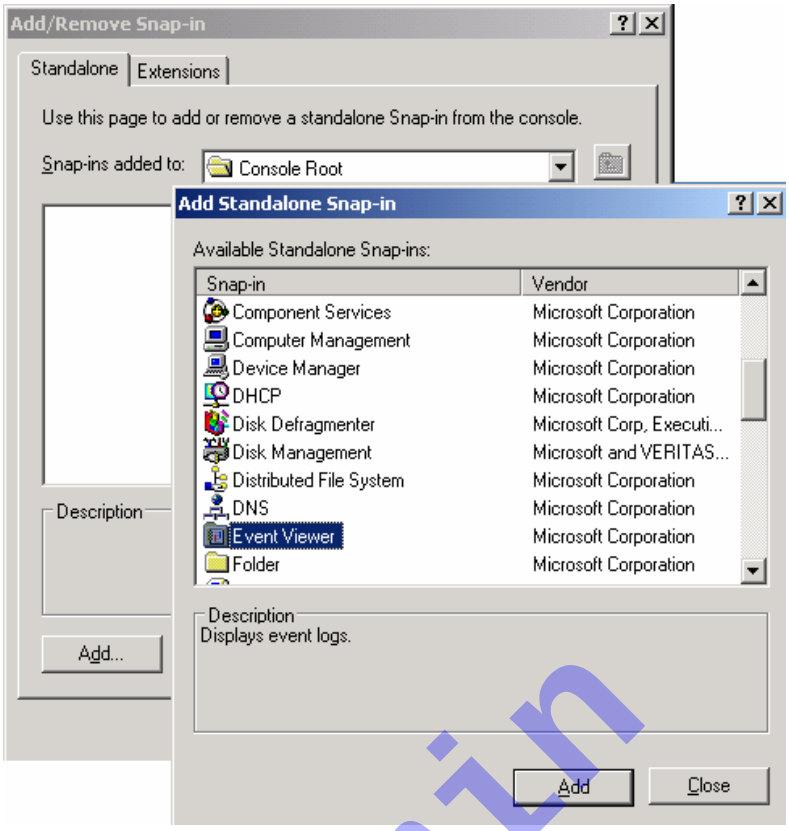
Se deschide o fereastră, numită consolă, în care urmează să fie introduse instrumente de administrare.



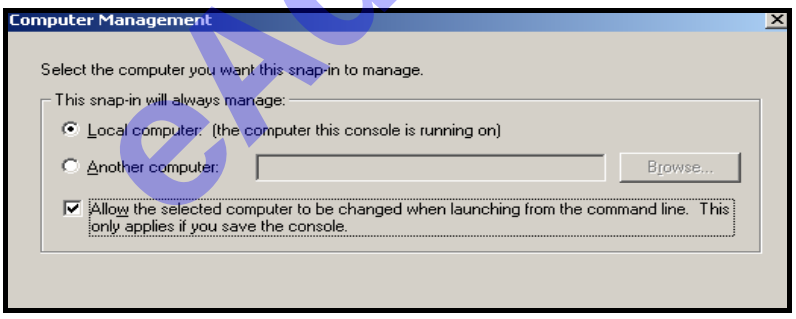
Într-o consolă de administrare se pot adăuga mai multe instrumente de administrare (*snap-ins*), prin acțiunea ***Add/Remove Snap-in.***

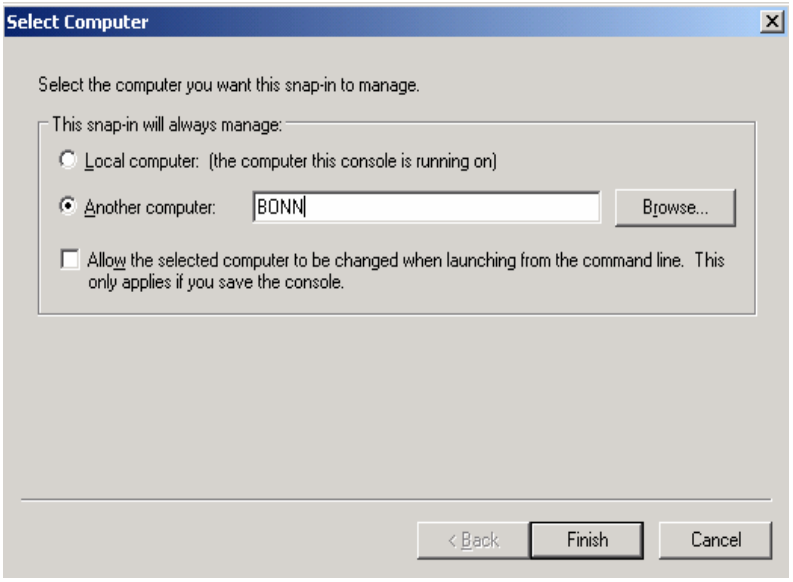


Urmează un exemplu de construire a unei console in care este adusă aplicația *Event Viewer.*

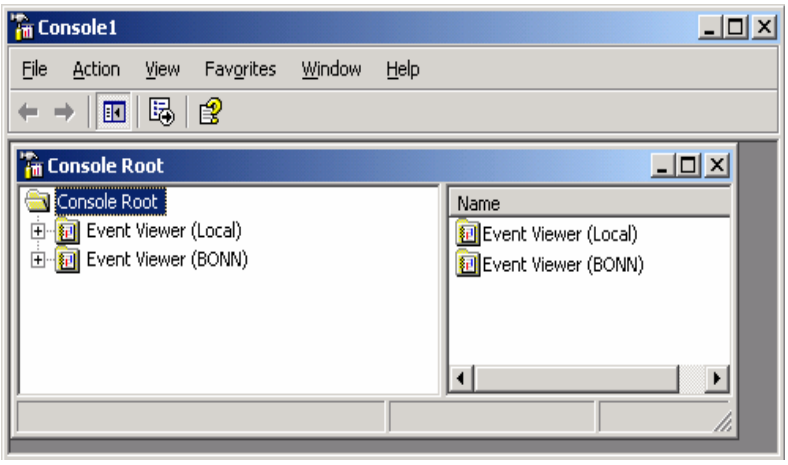


Se poate specifica dacă instrumentul de administrare ales (ex. *Event Viewer*) va administra calculatorul local sau unul aflat la distanță (ex. calculatorul numit BONN).

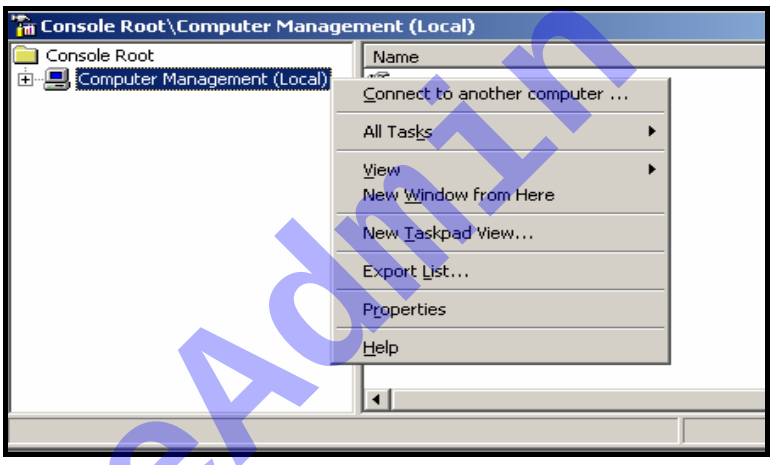




Au fost adăugate două aplicații *Event Viewer* în consola *mmc*, după care, aceasta ar putea fi salvată undeva pe discul local sau pe *Desktop* pentru a fi mai uşor de accesat.

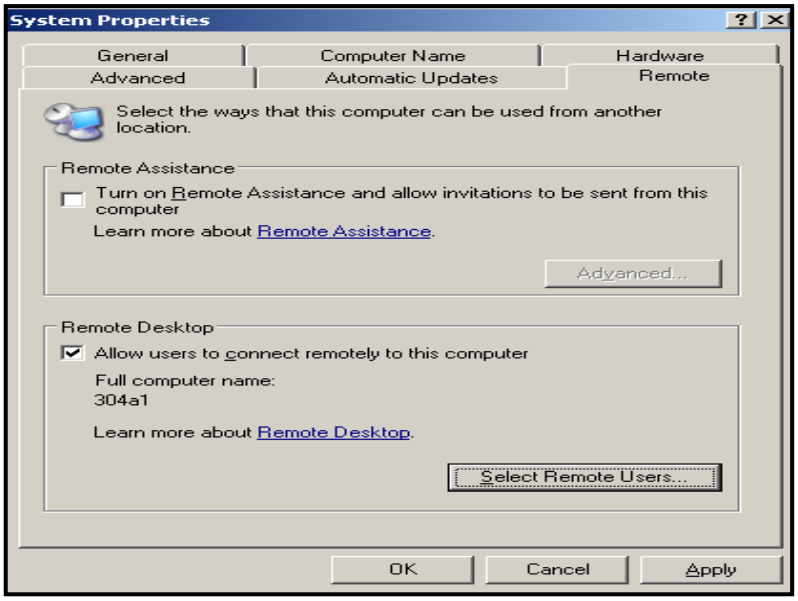


Modul de administrare, local sau a unui calculator aflat la distanță, se poate modifica şi ulterior, în consolă prin: clic dreapta pe instrumentul dorit→*Connect to another computer*.



Remote Desktop **pentru administrarea de la distanță a unui server**

Administrarea unuia sau a mai multor calculatoare de la distanță se poate face folosind modul de lucru *remote desktop* (ecranul *desktop* al calculatorului aflat la distanță). În organizațiile mari, administrarea de la distanță poate fi o soluție pentru administrarea centralizată a calculatoarelor aflate în locuri, chiar în clădiri sau oraşe diferite.



Remote Desktop for Administration asigură accesul la un server de la un alt calculator aflat la distanță, folosind protocolul *Remote Desktop Protocol* (*RDP*). RDP transferă de la client la server semnalele asociate interfeței cu utilizatorul, adică intrările de la client şi rezultatele de la server.

Pot fi create maxim două conexiuni simultane la distanță. Fiecare sesiune deschisă la distanță este independentă. *Remote Desktop for Administration* asigură conectarea de la distanță şi deschiderea de sesiune similară celei locale acelui server. Ecranul *desktop* transmis prin RDP este exact cel care ar fi fost obținut printr-o deschidere de sesiune locală la acel calculator (*server*). Pentru a asigura mai mult de două conexiuni simultane trebuie instalat serviciul *Terminal Service.*

Remote Desktop for Administration oferă două instrumente ce pot fi folosite pentru administrarea de la distanță:

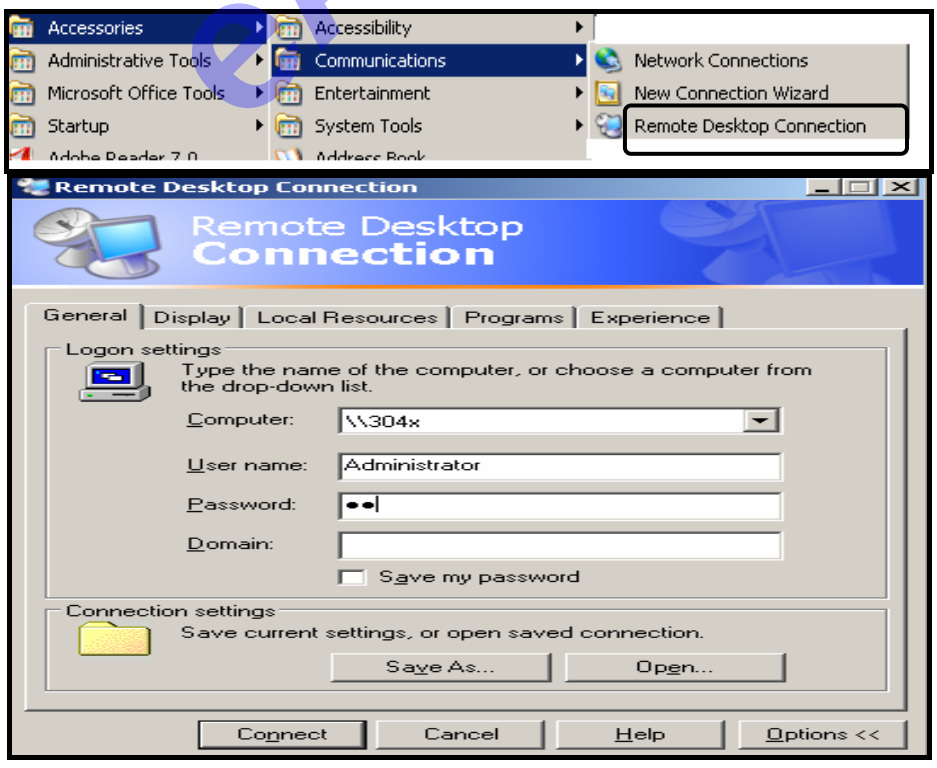
- *Remote Desktop Connection*

Fiecare exemplar de ***Remote Desktop Connection*** creează propria fereastră şi asigură administrarea unui server într-o fereastră.

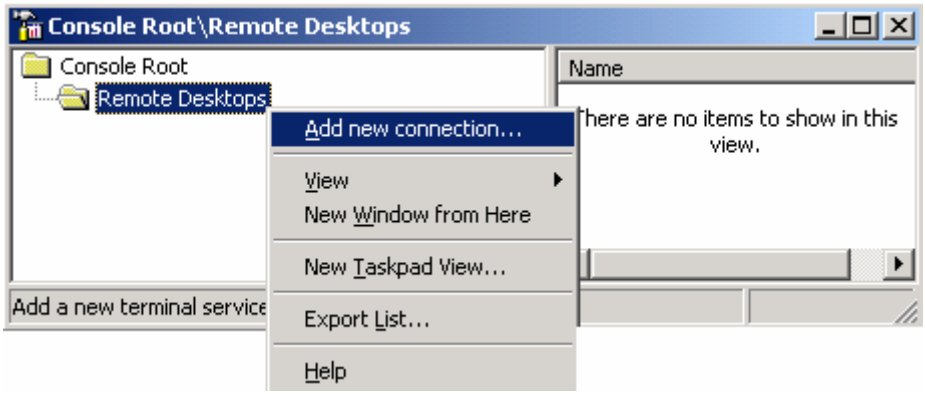
- Remote Desktops snap-in

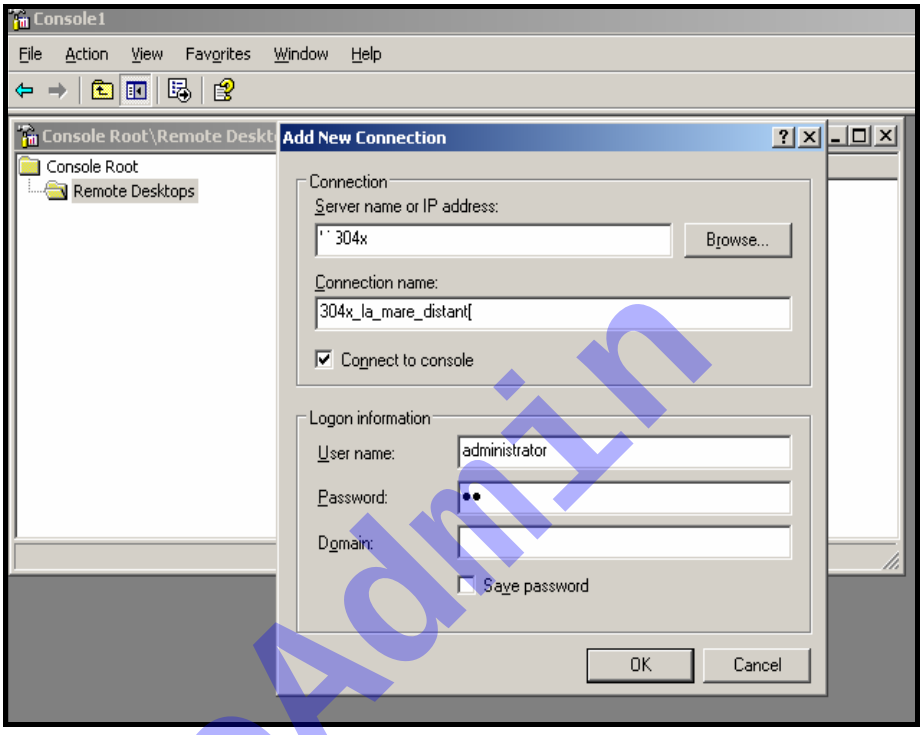
Remote Destops snap-in asigură administrarea de la distanță a mai multor servere, afişând o fereastră în care se află o structură arborescentă, în care în stânga se află conexiunile la distantă iar în dreapta detaliile ce îi sunt asociate. Accesul de la distanță la un **server** este asigurat de serviciul *Remote Desktop Service*, care este instalat şi trebuie activat (*enabled*) (*System Properties→ Remote*).

Clienții folosesc *Remote Desktop Connection* sau *Remote Desktops snap-in* şi se conectează – de la distanță – la serviciul *Remote Desktop Service* instalat la server.



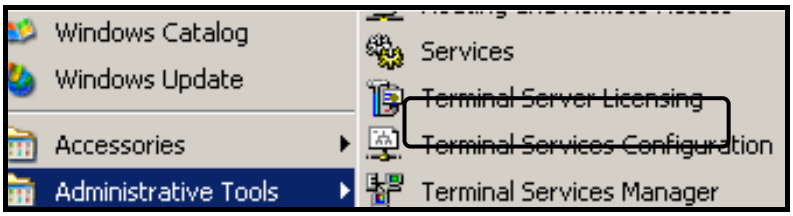
Sau

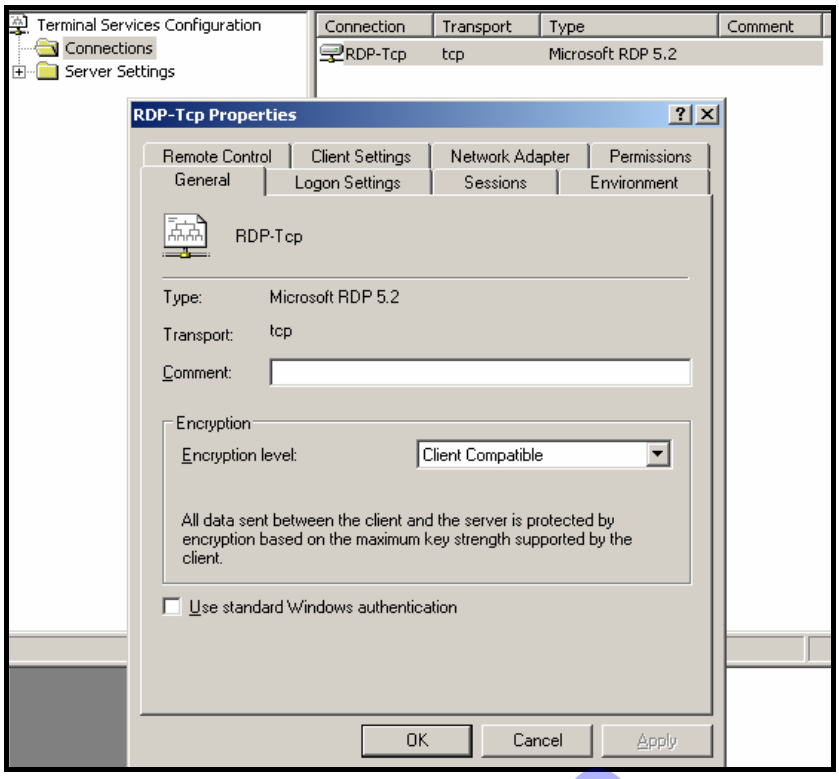




Grupul preconstruit local domeniului *Remote Desktop Users* are în mod implicit dreptul de a face *log on remote* la serverele din domeniu. Orice utilizator care nu este membru în grupul *Administrators* şi care trebuie să deschidă sesiune de tip *remote* trebuie fi inclus în acest grup.

Conexiunea cu serverul aflat la distanță (*remote* server) va rămâne deschisă până la închiderea sesiunii. O nouă conectare va însemna revenirea la sesiunea deschisă anterior. Condițiile de lucru ale unei sesiuni de tip *remote* sunt stabilite prin utilitarul *Terminal Services Configuration*.





Urmărirea şi optimizarea performanțelor serverelor

Urmărirea (supravegherea) performanțelor este o componentă esențială a operațiilor de întreținere preventivă. Urmărirea, timp îndelungat, a performanțelor serverelor asigură constituirea unui eşantion de apreciere a modului în care funcționează componentele hardware şi software. Informațiile comparative care rezultă susțin analiza şi soluționarea problemelor ce apar în funcționarea rețelei.

Datele despre performanțele sistemului pot fi folosite pentru:

- înțelegerea caracteristicilor de încărcare şi efectele corespunzătoare asupra diferitelor resurse;
- observarea modificărilor şi a tendințelor de încărcare şi folosire a resurselor, în vederea posibilelor operații de îmbunătățire a performanțelor resurselor (*upgrade*);
- urmărirea efectelor modificărilor efectuate şi ajustarea performanțelor;
- diagnosticarea problemelor;
- identificarea componentelor sau a proceselor care trebuie optimizate.

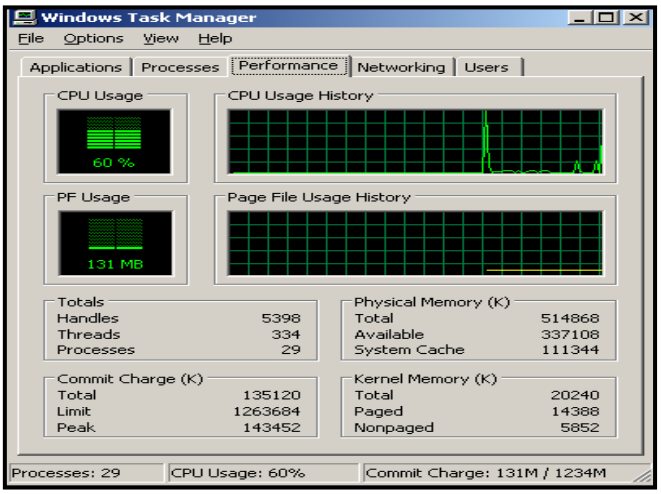
Analiza performanțelor poate evidenția existența unor probleme, cum ar fi suprasolicitarea unor resurse, ceea ce determină apariția „gâtuirilor" (*bottlenecks*). Ele sunt provocate de supraîncărcarea unor resurse, ceea ce conduce la diminuarea performanțelor de răspuns ale întregului sistem.

Monitorizarea activității curente

Cele mai simple instrumente de supraveghere pentru *Windows Server 2003* sunt: utilitarele *TaskManager*, *Performance* şi *Event Viewer.*

Task Manager

Task Manager oferă o privire de ansamblu asupra activității şi performanțelor sistemului: programe şi procese aflate în execuție, estimarea activității procesorului şi gradul de ocupare a memoriei, funcționarea adaptorului de rețea şi a conexiunii la rețea, utilizatorii conectați şi fişierele cu care lucrează.



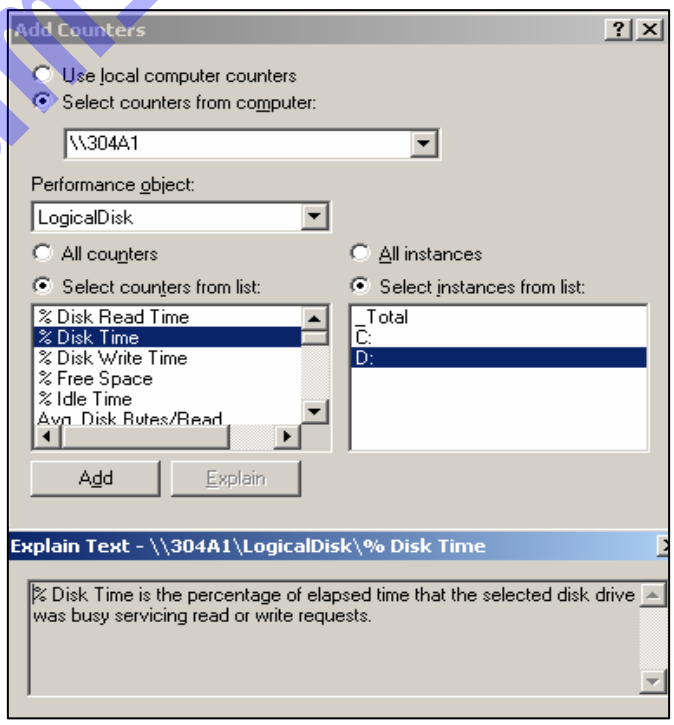
Performance

Sistemul de operare *Windows Server 2003* pune la dispoziție consola ***Performance*** care se compune din *System Monitor* şi *Performance Logs and Alerts*.

System Monitor

System Monitor colectează şi interpretează date despre activitatea curentă a calculatorului local sau a unuia aflat la distanță. În vederea colectării informațiilor trebuie specificate următoarele:

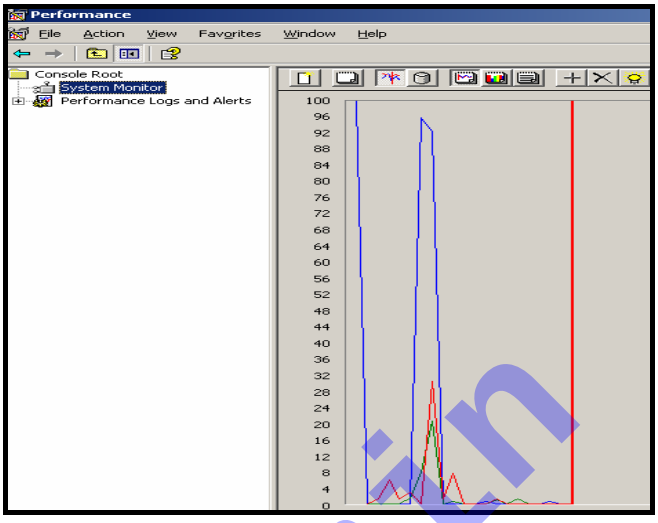
- obiectul, respectiv resursa supravegheată;
- contorul, respectiv entitatea (caracteristica) pentru care se măsoară activitatea (ocuparea sau disponibilitatea resursei);
- exemplarul (instanța) obiectului pentru care se măsoară activitatea, în situația existenței mai multor obiecte din acel tip.



Datele contoarelor păstrate în jurnale pot fi vizualizate folosind tot *System Monitor* sau pot fi exportate sub forma foilor de calcul tabelar şi a tabelelor folosite de bazele de date. Vizualizarea prin *System Monitor* prezintă informațiile într-una din următoarele forme: grafic, histogramă, raport.

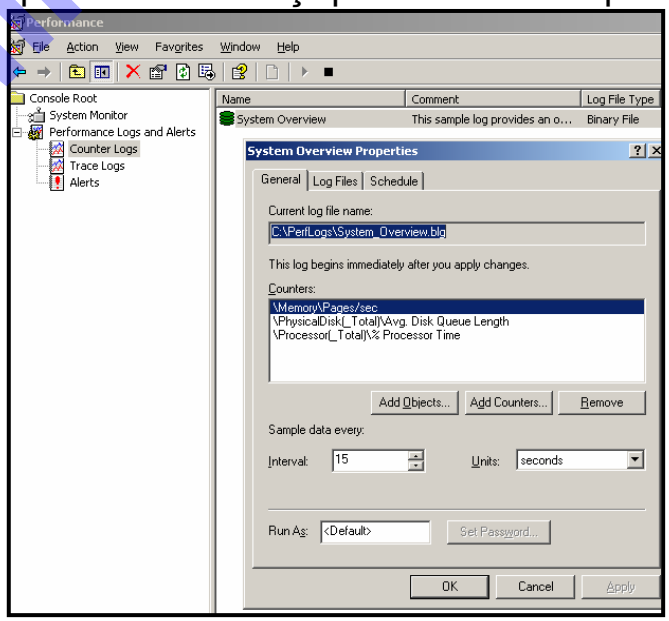
Monitorizarea (urmărirea, supravegherea) activității curente se realizează folosind utilitarul *System Monitor*, care prelucrează şi actualizează imediat valorile contoarelor cu valori primite de la sistemul de operare. Supravegherea activității curente (supraveghere în timp real) poate arăta care este starea curentă a celor patru subsisteme a căror corectă funcționare este considerată esențială, şi anume: memorie, procesor, disc, rețea.

De exemplu, dacă utilizatorii se plâng de timpul mare de răspuns pentru accesul de la client la server, atunci *System Monitor* vă poate ajuta în obținerea diagnosticului corect.



Performance Logs and Alerts

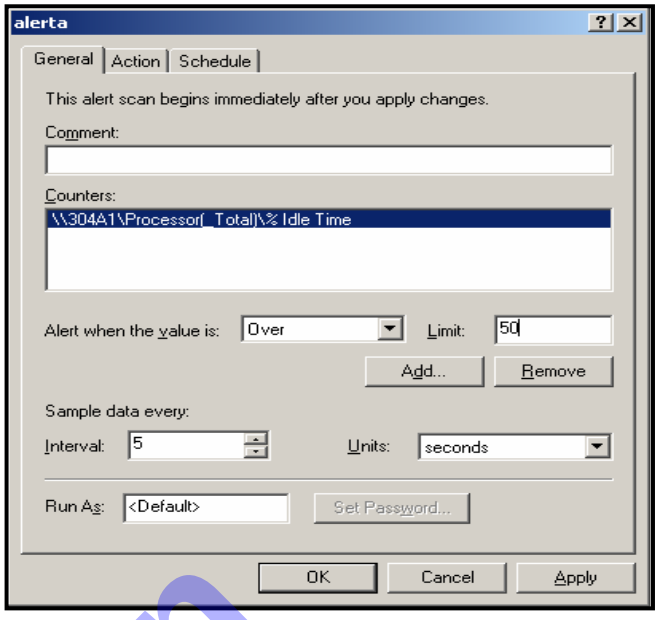
Supravegherea jurnalizată se obține prin colectarea şi păstrarea în timp a valorilor asociate contoarelor. Este modalitatea prin care se detectează „gâtuirile”, resursele critice şi se recunosc modificările apărute în timp. Pentru construirea, păstrarea şi consultarea jurnalelor se va folosi procedura *Performance Logs and Alerts*.



Jurnalul valorilor contoarelor este un fişier de tip *log*. Jurnalul se construieşte cu *Performance Logs and Alerts* (Jurnale şi Alerte). Datele din jurnal pot fi păstrate în următoarele formate:

- Fişier text – folosind virgula drept separator – fişier cu extensia .csv; poate fi folosit pentru exportarea către un program de calcul tabelar.
- Fişier text – folosind caracterul Tab drept delimitator – fişier cu extensia .tsv; poate fi folosit pentru exportarea către un program de calcul tabelar.
- Format binar – fişier cu extensia .blg; comanda *tracerpt* poate converti fişierul binar în format .csv.

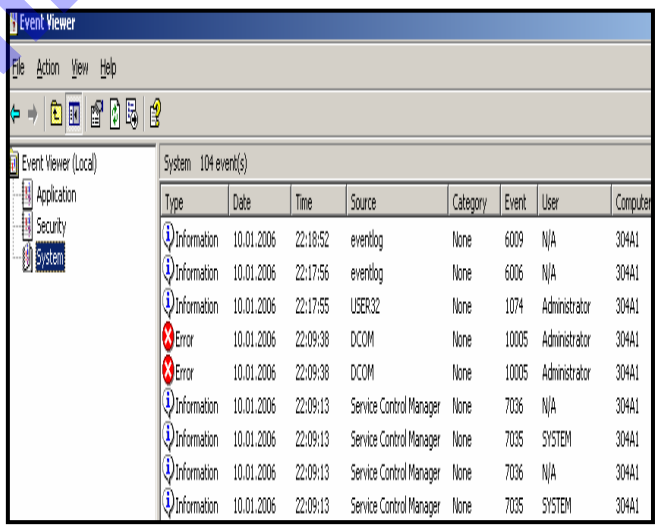
- Format binar circular: este un format binar (extensia .blg) cu mențiunea că fişierul va fi suprascris dacă datele colectate în timp fac să se depăşească lungimea prestabilită a fişierului.
- Format SQL – reprezintă o bază de date SQL existentă.



Alerta este operația prin care se detectează dacă valoarea curentă a unui contor a atins un prag considerat critic. În momentul apariției alertei va fi anunțat (notificat) administratorul şi poate fi inițiată o operație de corecție automată.

Event Viewer

Event Viewer este componenta cu care pot fi urmărite evenimentele păstrate în jurnale. Fiecare calculator păstrează o listă a propriilor evenimente în jurnale: aplicație, securitate, sistem. În afara lor, în funcție de rolul calculatorului în rețea şi de aplicațiile instalate, vor apărea şi alte jurnale. În această situație se află jurnalele diferitelor servicii.



Supravegherea performanțelor serverelor

Subsistemele care vor fi în general supravegheate sunt: memoria, procesorul (procesoarele), discul (discurile) şi rețeaua.

Memorie

Insuficiența memoriei este cauza principală a scăderii performanțelor sistemelor. Orice analiză a performanțelor trebuie să înceapă cu evaluarea performanțelor memoriei, în raport de aplicațiile instalate, de condițiile în care se execută ele, de numărul utilizatorilor care le folosesc, etc.

- memoria insuficientă conduce la o intensă activitate de paginare, ceea ce înrăutățeşte performanțele generale ale sistemului;
- capacitatea redusă a memoriei încetineşte lucrul cu aplicații şi răspunsul serviciilor, ceea ce influențează şi performanțele altor resurse;
- pierderi de memorie pot apărea în situația acelor aplicații care alocă memorie, dar nu o mai eliberează la terminarea execuției; ca urmare memoria disponibilă scade, ceea ce conduce la funcționarea defectuoasă a întregului sistem.

Obiectul *Memory* Contor	**Valoare considerată acceptabilă**	**Valoare aşteptată**	**Acțiune**
Pages/sec	Mai mic de 5	Cât mai mică	Identificarea procesului care determină activitatea mare de paginare Adăugare RAM
Available bytes	Minim 9% din memoria totală	Cât mai mare	Identificarea procesului care solicită memorie internă mai mare decât cea disponibilă Adăugare RAM
Pool non paged bytes	Constantă Nu creşte	Nu se aplică	Verificarea pierderilor de memorie datorate aplicațiilor

Procesor

După consumul de memorie, un alt parametru important în judecarea performanțelor sistemului este procesorul. Un procesor suprasolicitat înseamnă un sistem cu performanțe reduse: toată „munca" sistemului este efectuată – în fond – de procesor.

Gradul de folosire, de încărcare, a procesorului este dat de procentul de timp de funcționare. Este indicatorul principal față de care se apreciază performanțele generale ale sistemului, după cele referitoare la memorie.

Obiectul *Processor* Contor	**Valoare considerată acceptabilă**	**Valoare aşteptată**	**Acțiune**
% Procesor Time	Mai mică decât 85%	Mică	Căutarea procesului consumator excesiv *Upgrade* sau adăugare
Interrupts/sec	Depinde de procesor	Mică	Identificarea perifericului generator de un exces de întreruperi

Disc

Capacitatea discurilor şi caracteristicile legate de viteza de scriere / citire sunt informații esențiale în aprecierea posibilităților generale de lucru ale întregului sistem.

Obiectul *Physical Disk* Contor	Valoare considerată acceptabilă	Valoare aşteptată	Acțiune
% Disk Time	Sub 90% Mic	ă	Verificarea paginării *Upgrade* (subsistemul disc)
Current Disk Queue Length	0-3	Mică	*Upgrade* (subsistemul disc)

Pentru monitorizarea discurilor se folosesc obiectele: *Physical Disk* şi *Logical Disk*.

Rețea

Acolo unde există, rețeaua este o componentă importantă în menținerea unui mediu de operare eficient şi sigur. Comportamentul componentelor (hard şi soft) specifice rețelei influențează funcționarea de ansamblu a soluțiilor IT&C implementate. Se pot obține performanțe generale mai bune prin optimizarea traficului în rețea, prin distribuirea (aşezarea) resurselor şi implicit a utilizatorilor acestora.

Obiectul *Network Interface* Contor	Valoare considerată acceptabilă	Valoare aşteptată	Acțiune
Network Utilization (din *Task Manager*)	Mai mică de 30%	Mică	*Upgrade* (adaptorul de rețea sau rețeaua în ansamblu)
Server: Bytes Received/sec	Mai mică de 50% din lărgimea de bandă	Nu se aplică	*Upgrade* (adaptorul de rețea sau rețeaua în ansamblu)

Întreținerea driverelor

Pentru a funcționa, fiecare echipament (*device*) ataşat unui calculator are nevoie de un software special, cunoscut sub numele de driver (*device driver*). Rolul lui este de a asigura comunicarea cu sistemul de operare. *Driverele* folosite de sistemele de operare *Microsoft Windows* sunt cele furnizate chiar de *Microsoft* şi de fabricantul echipamentului.

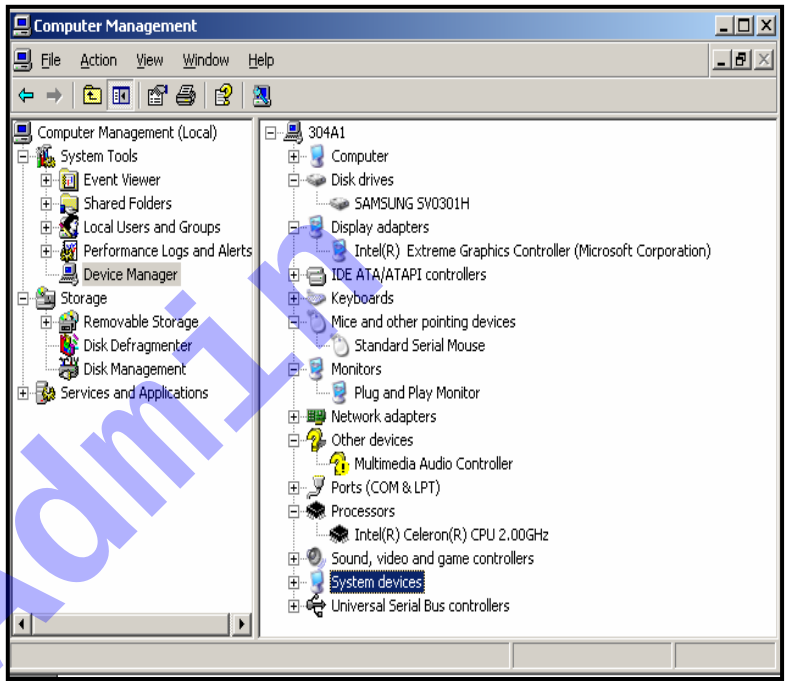
Echipamentele se pot împărți în două grupe:

- *plug and play*

Plug and Play este o combinație a suportului hardware cu cel software care face ca sistemul de operare să recunoască şi să se adapteze singur la modificările aduse în mod dinamic configurației hardware. Echipamentele care recunosc modul de lucru *Plug and Play* pot fi adăugate sau îndepărtate dinamic, fără să fie nevoie de reconfigurarea „manuală” a sistemului.

- *non-plug and play*

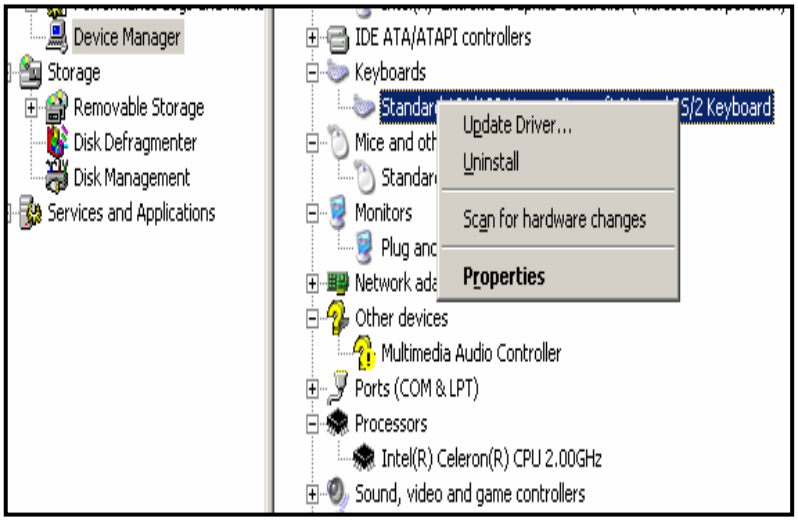
Indiferent de tipul de echipament, înainte ca el să poată fi folosit trebuie să fie instalat *driver*-ul. *Driver*-ul se va încărca la fiecare pornire a calculatorului. Dacă echipamentul este cuprins în lista *Windows Catalog* atunci sistemul de operare include şi *driver*-ul corespunzător.



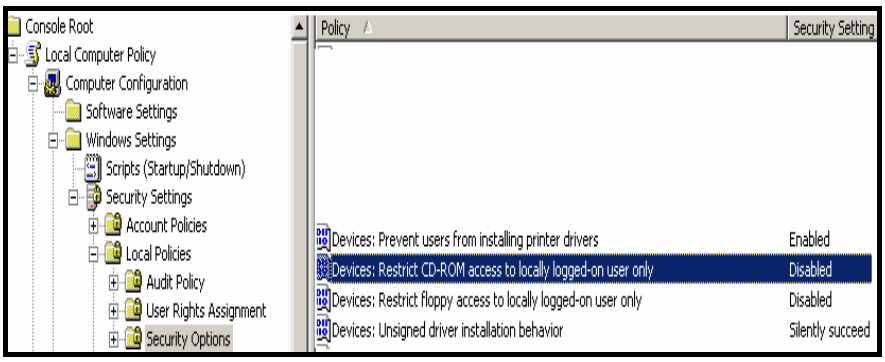
Device Manager este utilitarul cu care sunt administrate echipamentele.

Operațiile ce pot fi efectuate sunt:

- identificarea *driver*-elor încărcate şi obținerea informațiilor de configurare;
- modificarea unor caracteristici de lucru ale *driverelor*, cum ar fi cele legate de cererile de întrerupere (IRQ);
- instalarea şi *upgrade*-ul *driver*-elor;
- revenirea la o versiune mai veche a unui *driver* (*roll back*);
- verificarea corectitudinii funcționării echipamentelor instalate;
- activarea, inhibarea, dezinstalarea *driver*-elor;
- obținerea unui rezumat al informațiilor corespunzătoare echipamentelor instalate.

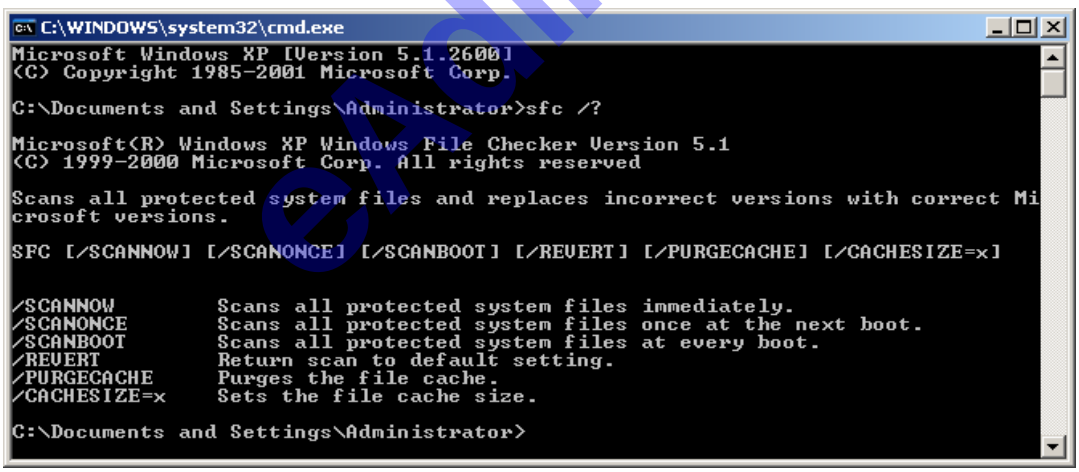


Driver-ele pot avea o semnătură digitală. Ea indică faptul că *driver*-ul (fişierul în general) a fost testat şi că nu a fost modificat sau suprascris în timpul instalării altui program. Administratorul poate configura comportamentul sistemului de operare față de componentele nesemnate identificate: ignorare, afişarea unui mesaj de avertizare, imposibilitatea instalării componentei. Comportamentul poate fi configurat manual pe fiecare calculator în parte sau prin folosirea obiectelor *Group Policy (GPO).*

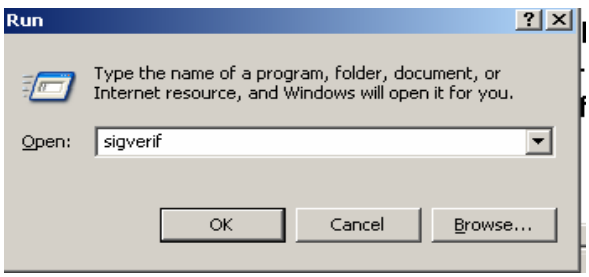


Instrumentele folosite pentru verificarea semnăturilor digitale sunt:

- **Comanda sfc** (*System File Chacker)* trece în revistă şi verifică versiunile tuturor fişierelor protejate ale sistemului de operare. *System File Chacker* poate înlocui fişierele compromise cu unele corecte oferite de *Microsoft*. Dosarul *Dllcache,* din %windir%system32\ este folosit pentru păstrarea versiunilor corecte ale fişierelor sistem. Dacă acest dosar este alterat, atunci comanda *sfc /purgecache* va încerca repararea conținutului său.



- Programul **sigverif** (*File Signature Verification*) este folosit pentru verificarea semnăturii digitale a fişierelor sistem şi a drivere-lor originale sau agreate de către *Microsoft*.

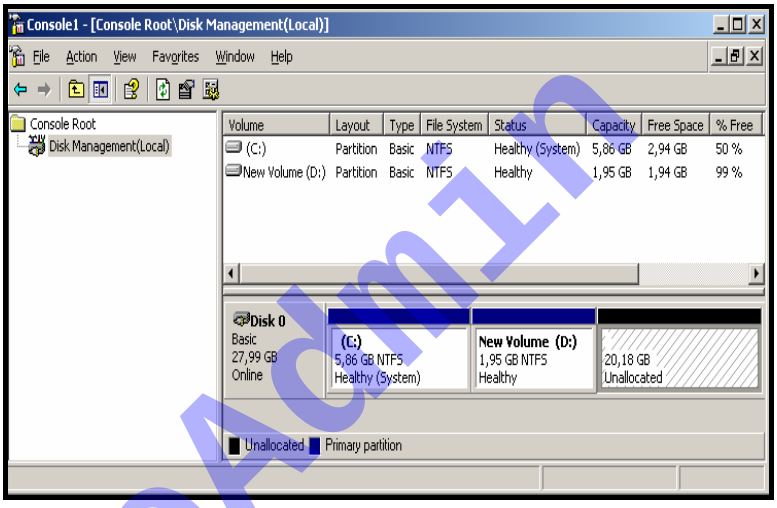


Administrarea discurilor

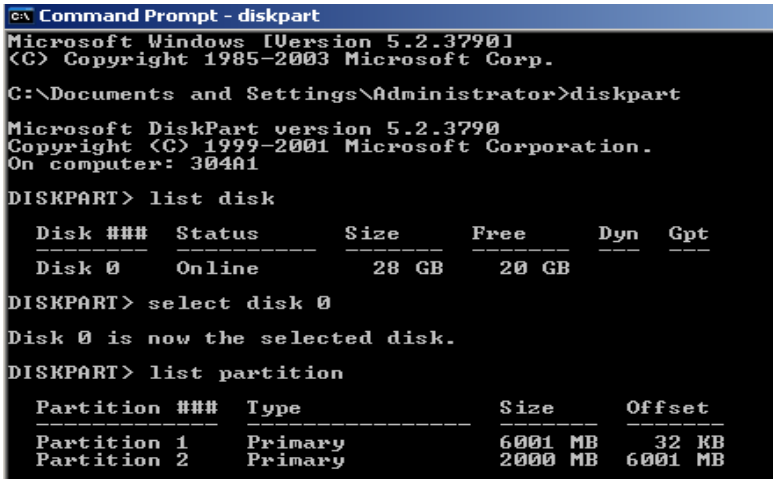
Pregătirea discurilor

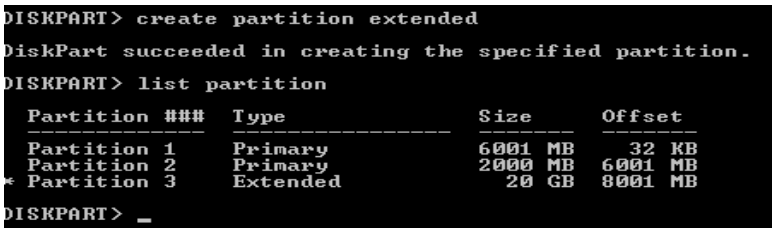
La instalarea unui nou *hard disk* sistemul de operare *Windows Server 2003* îl recunoaşte şi configurează ca disc de bază (*basic disk*). Disc de bază este formatul implicit al mediului de depozitare a datelor şi oferă posibilități limitate de configurare.

Disk Management este utilitarul folosit pentru gestiunea discurilor, atât pentru calculatoarele locale cât şi pentru cele aflate la distanță. Cele mai multe operații de gestionare a discurilor au loc fără restartarea sistemului şi fără ca utilizatorii să fie întrerupți din propriile activități. *Disk Management* este o componentă a instrumentului *Computer Management* dar şi un *snap-in* utilizabil într-o consolă *mmc*. Administrarea discurilor poate fi făcută de membrii grupului local *Administrators*.



O altă metodă folosită pentru gestionarea partițiilor şi a volumelor este utilitarul *Diskpart* obținut prin tastarea comenzii *diskpart* în linia de comandă. Pentru a vedea comenzile ce pot fi lansate sub acest utilitar tastați "?". Mai jos aveți o exemplificare a folosirii acestui instrument, respectiv lansarea unor comenzi.





Partiționarea este modalitatea de împărțire a unui disc în secțiuni (sau partiții) care funcționează ca unități separate. Fiecărei partiții i se asociază – în vederea adresării - o literă. După creare, partiția va fi formatată folosind un sistem de fişiere. În situația instalării unui nou hard disc, el trebuie mai întâi inițializat: la prima folosire a lui *Disk Management* apare lista componentelor noi identificate iar sistemul de operare va iniția liza discul scriind o semnătură a discului, marcând sectoarele şi construind înregistrarea MBR (*Master Boot Record*).

Un disc de bază conține partiții: cel mult 4 partiții primare sau cel mult trei partiții primare şi una extinsă. O partiție primară nu poate fi subîmpărțită. Partiția extinsă poate fi împărțită în unități logice. Un disc poate contine cel mult 24 de unități logice, distincte. Partițiile extinse pot fi create numai pe discurile de bază. Vor fi formatate unitățile logice construite în partiția extinsă. Formatarea configurează tabela de alocare a fişierelor şi pregăteşte operațiile de scriere şi de citire.

Ştergerea şi crearea partițiilor distruge informațiile existente pe disc. Înaintea acestor operații se recomandă salvarea (*backup*) datelor. În familia sistemelor *Windows Server 2003* sistemul de fişiere NTFS este cel care asigură protecția fişierelor prin permisiuni la dosare şi fişiere, criptarea accesului la informații, volume de dimensiuni mari, comprimarea conținutului dosarelor şi fişierelor.

Gestionarea proprietăților discurilor

Proprietățile asociate discurilor indică informații disponibile, obținute fie prin *Disk Management* fie prin *DiskPart*.

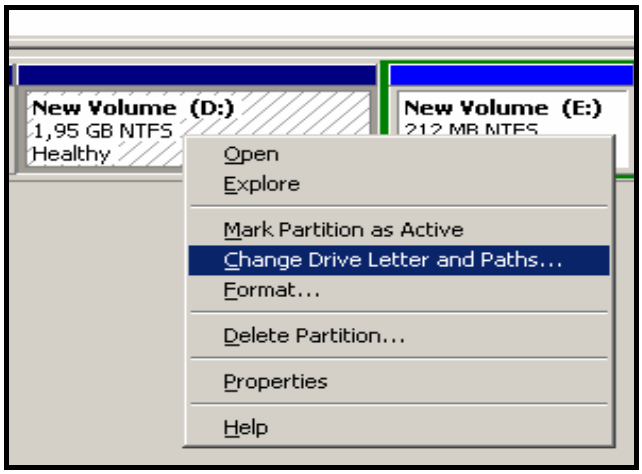
În mod normal *Disk Management* recunoaşte noile discuri imediat ce sunt instalate. Dacă se întâmplă să nu le recunoască, atunci trebuie lansată întâi o operație de scanare (*rescan*) a discurilor. Această operație trece în revistă proprietățile tuturor discurilor întâlnite şi identifică modificările de configurație. De asemenea, sunt actualizate informațiile despre mediile *movibile*, unitățile CD-ROM, volumele de tip *basic*, sistemele de fişiere, literele alocate unităților de disc în vederea adresării.

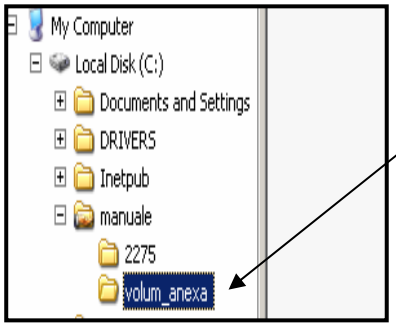
Sistemul de fişiere recomandat pentru servere este NTFS. Sistemul de fişiere NTFS oferă caracteristici îmbunătățite de securitate şi de toleranță la erori (volumele FAT şi FAT32 nu dispun de toleranță la erori).

Comanda *convert* este responsabilă de convertirea sistemelor de fişiere FAT şi FAT32 existente în volume NTFS. Toate fişierele sunt păstrate intacte după terminarea acestei operații. Ceea ce se modifică este tabela director a fişierelor.

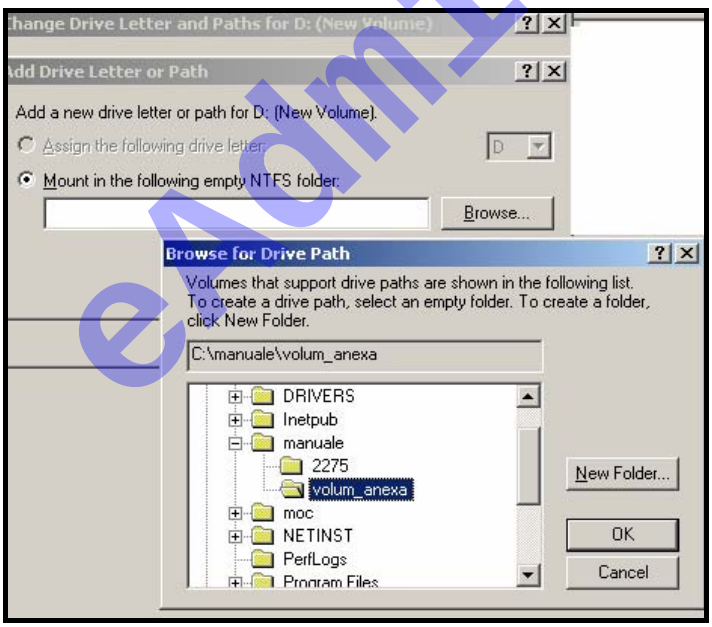
Montarea unităților de disc poate fi o soluție pentru uşurarea organizării şi gestionării discurilor. Cu ajutorul acestei operații se pot asocia şi folosi nume (nu litere) pentru desemnarea unităților de disc.

O unitate de disc montată (*mounted drive*) este un depozit de informații, administrat cu ajutorul sistemului NTFS de fişiere. Utilitarul *Disk Management* poate fi folosit pentru montarea unei unități locale în orice dosar gol al unui volum local NTFS. Metoda este similară creării unei scurtături care trimite către o partiție sau un volum de disc.





Montarea discului D: într-un folder



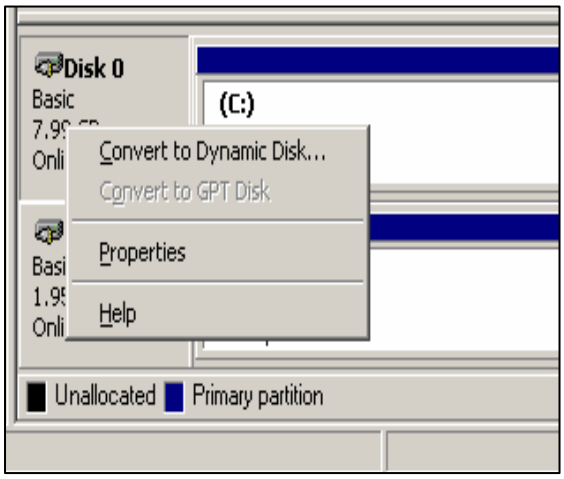
Tipul de disc de bază este implicit pentru *Windows Server 2003* şi dispune de posibilități limitate de configurare. Discurile de bază pot fi partiționate şi formatate la instalarea sistemului de operare şi prin consola *Recovery* (*Recovery Console*, cea obținută prin *winnt32 /cmdcons*).

Discurile dinamice permit mai multă flexibilitate şi implementează proceduri pentru toleranța la erori (*fault tolerance*).

În situația discurilor dinamice:

- un volum poate ocupa spațiu pe mai multe discuri (se poate extinde pe mai multe discuri);

- nu există limită pentru numărul de volume care pot fi configurate pentru un disc dinamic;
- admit toleranța la erori, adică asigură integritatea datelor prin redundanță şi proceduri de recuperare în urma erorilor hardware;



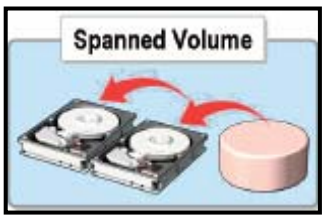
Conversia discurilor de la tipul de bază la cel dinamic poate avea loc oricând, fără pierderea datelor. Partițiile existente anterior pe discul de bază se transformă în volume. Configurația volumelor dinamice este păstrată într-o zonă de 1 MB, plasată la sfârşitul discului dinamic.

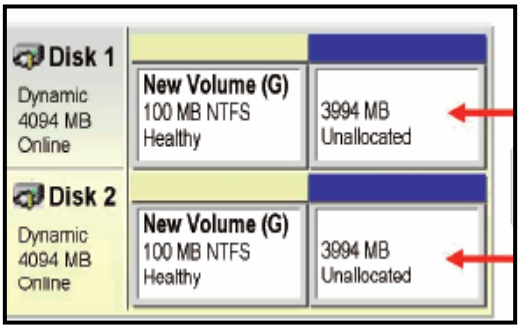
Eventuala revenire de la discul dinamic la cel de bază se poate face numai cu pierderea tuturor datelor existente pe *hard disk* prin ştergerea partițiilor: partițiile vor trebui create din nou, ca la început!

Utilitarul *Disk Management* poate fi folosit pentru conversia discurilor de la tipul de bază la cel dinamic.

Discurile dinamice permit – după cum le spune şi numele – flexibilizarea ocupării spațiului rămas liber pe un disc. Discurile dinamice operează cu volume, numite volume dinamice.

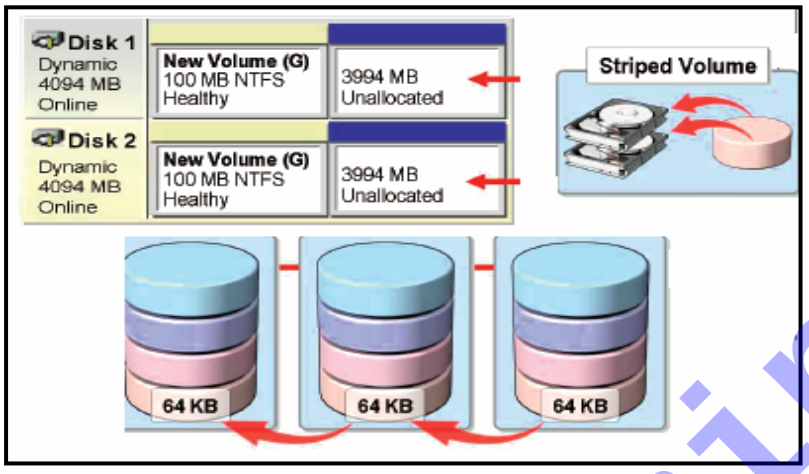
- **Volumul simplu:** Volumul simplu este o porțiune dintr-un disc fizic care funcționeaza ca unitate separată. Volumele simple sunt echivalentul dinamic al partițiilor primare. Când se foloseşte un singur disc dinamic, volumele simple sunt singurele care pot fi create. Volumul simplu poate fi formatat FAT, FAT32, NTFS, dar numai volumele simple formatate NTFS pot fi extinse.
- **Volumul extins:** se obține din extinderea volumelor simple neformatate sau formatate NTFS (versiunea de NTFS *Windows Server 2003*). Extinderea se face prin ocuparea spațiului nealocat rămas pe acelaşi disc sau pe oricare alt disc dinamic. Spațiul disponibil poate fi obținut şi prin adăugarea de hard discuri noi ce vor fi configurate ca discuri dinamice. Volumele simple obținute din partițiile de bază existente inițial nu pot fi extinse.
- **Volumul *spanned*** („împrăştiat”, care acoperă mai multe discuri): este un volum dinamic care ocupă spațiu pe două sau mai multe discuri fizice. Dimensiunea unui disc *spanned* poate creşte in mod dinamic prin extindere. Volumele *spanned* folosesc numai sistemul de fişiere NTFS şi nu implementează nici o





procedură de toleranță la erori. Dacă unul dintre discurile ce compun volumul *spanned* se defectează şi funcționează cu erori sau nu mai funcționează deloc, atunci întregul volum nu mai funcționează corect şi toate datele sunt pierdute, indiferent unde s-ar afla ele. Probabilitatea ca un volum care acoperă două discuri să se defecteze este de două ori mai mare decât probabilitatea de defectare a unui volum care ocupă spațiu pe un singur disc.

- **Volume cu fâşii** (*striped*): păstrează datele pe două sau mai multe discuri fizice, prin combinarea zonelor libere într-un singur volum logic.



Volumele cu fâşii sunt cunoscute şi sub numele de RAID-0; nu pot fi extinse şi nici oglindite (*mirrored*). În volumele RAID-0 scrierea datelor se face pe fâşii. Fâşiile sunt scrise simultan pe toate discurile care compun setul de fâşii. Cea mai mare realizare a acestui volum este viteza de citire / scriere: datele sunt accesate simultan, pe discuri diferite, prin capete de citire / scriere diferite. Nu implementează nici o soluție pentru recuperarea datelor în cazul funcționării incorecte a discurilor.

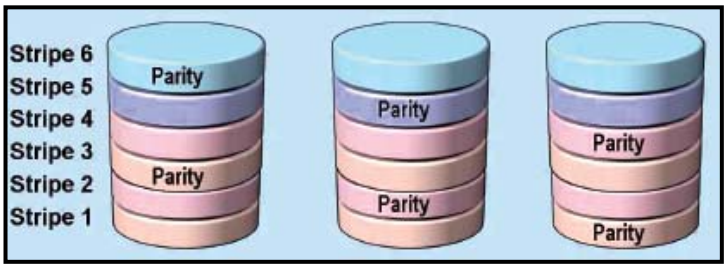
Volume tolerante la erori

Toleranța la erori este capacitatea hardware şi software a unui calculator de a asigura integritatea fizică a datelor în situația apariției defectelor hardware. Pentru sistemele Windows Server 2003 toleranța la erori este implementă prin volumele oglindite (RAID -1 , *mirrored volumes*) şi prin volumele RAID-5 (volume în fâşii cu paritate). Volumele care asigură toleranța la erori păstrează date redundante: la scriere, aceleaşi date sunt scrise în locuri diferite. Dacă un disc nu funcționează, datele sunt de găsit pe un alt disc. Volumele tolerante la erori pot fi create – la *Windows Server 2003* – numai pe discuri dinamice.

- Volume oglindite: sunt volume tolerante la erori, în care redundanța datelor se obține folosind două exemplare ale volumului (un exemplar este oglinda celuilalt). Toate datele scrise pe un exemplar al volumului sunt scrise şi pe al doilea. Cele două exemplare se află pe discuri fizice separate, distincte. Aproape toate volumele pot fi oglindite, inclusiv cele de *boot*. Dacă unul dintre discuri „cade”, celălalt continuă să funcționeze, dar nu mai este *fault tolerant*. Pentru a nu pierde datele va trebui refăcut setul *mirror* prin aducerea unui disc nou: întâi va fi „spart” setul *mirror* pentru ca sistemul să recunoască faptul că discurile lucrează independent

şi volumul rămas devine volum simplu; apoi va trebui refăcut setul *mirror*, prin crearea unui nou volum oglindit, folosind spațiul liber (neocupat) al noului disc.

- Volume RAID-5: sunt volume cu fâşii cu paritate. Paritate este metoda matematică pentru determinarea numărului par sau impar de biți al unui număr sau al unei serii de numere. Metoda este folosită pentru reconstruirea datelor dacă un număr dintr-o secvență este pierdut. Pentru volumele RAID-5, toleranța la erori se obține prin adăugarea unei fâşii cu informații de paritate la fiecare disc din volumul constituit. Dacă unul singur dintre discuri "cade", datele pot fi reconstruite folosind informația de paritate. În acest caz paritatea se referă la informația redundantă asociată unui bloc; este o valoare obținută prin calcule, astfel încât să poată fi folosită la reconstituirea datelor de pe o fâşie. Dacă un disc nu mai poate fi folosit, atunci conținutul fâşiilor aflate aici poate fi reconstituit din informația de paritate şi cea aflată pe celelalte discuri aflate încă în funcțiune.

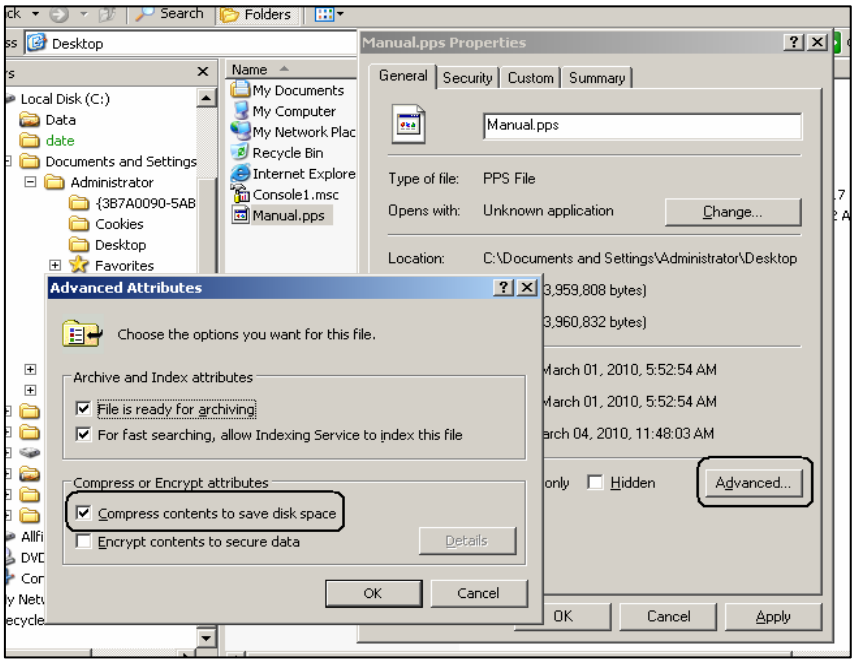


Administrarea depozitelor de date

Una dintre sarcinile cele mai importante ale administratorului de rețea este cea de gestionare a datelor păstrate pe echipamente disponibile în rețea. Gestiunea datelor se referă – în general – la comprimare, criptare, recuperarea fişierelor criptate, implementarea cotelor alocate utilizatorilor în vederea ocupării discurilor.

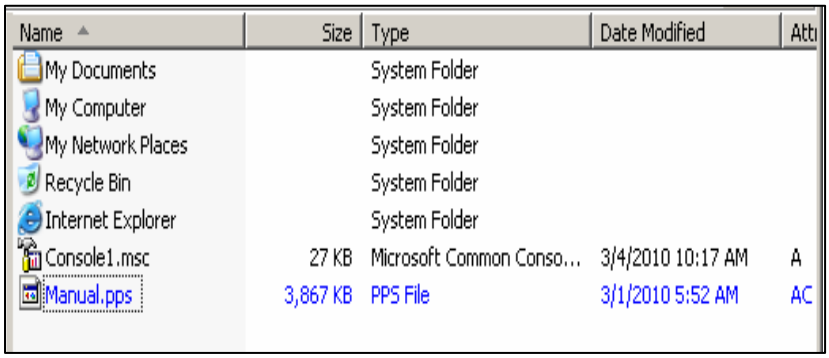
Comprimarea fişierelor

Comprimarea fişierelor şi a dosarelor conduce la scăderea dimensiunii (lungimii) acestora, adică a spațiului ocupat. *Windows Server 2003* oferă două modalități de comprimare: fie folosind caracteristica NTFS de comprimare, fie prin dosarele comprimate de tip *zip* (*Compressed – zipped – Folders*). Ambele modalități de comprimare se realizează folosind *Windows Explorer.*



Diferența de dimensiune obținută prin comprimare este cea mai spectaculoasă la fişierele de tip text, cele de tip „*bitmap*”, la foile de calcul şi la prezentările *.ppt*. Efecte mai mici se obțin pentru fişierele cu imagini grafice sau video. Se recomandă ca fişierele din dosarele sistem să nu fie comprimate: comprimarea lor afectează major performanțele serverului.

- Folosirea atributului *compress* pentru comprimarea folderelor, fişierelor, volumelor.



Într-o fereastră *Windows Explorer*, selectați obiectul de comprimat, apoi în caseta *Advanced Attributes* selectați opțiunea *Compress contents to save disk space*

Fişierele nou create într-un dosar comprimat moştenesc atributul de compresie în mod implicit.

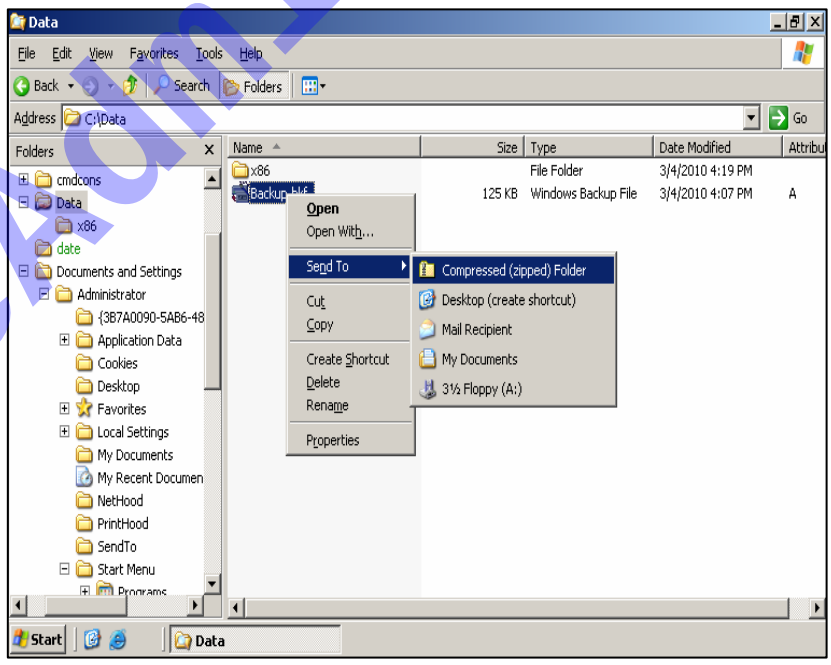
La copierea fişierelor, sistemul de operare calculează necesarul de spațiu pentru fişiere în formă necomprimată.

- Comanda *compact* lansată la *Command Prompt* este un alt instrument ce poate fi folosit pentru comprimarea fişierelor, folderelor.

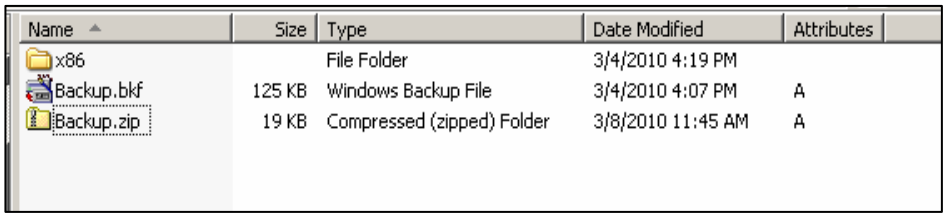
- Comprimarea fişierelor folosind dosarele *zipped* poate avea loc pentru volume FAT, FAT32, NTFS.

Într-o fereastră *Windows Explorer*, selectați obiectul de comprimat, apoi urmați calea:

clic dreapta pe obiect (folder, fişier)→*Send To→Compressed (zipped) Folder*



În fereastra de mai jos apare atât fişierul de comprimat – *Backup.bkf*, cât şi fişierul arhivat *Backup.zip*, de dimensiune semnificativ mai mică decât fişierul original.



Mutarea şi copierea fişierelor şi folderelor poate schimba starea de compresie. Astfel că putem avea următoarele situații:

- Când copiați un fişier sau folder în interiorul unei partiții NTFS, fişierul sau folderul moştenesc starea de compresie a folderului destinație. Astfel că, dacă copiați un fişier sau folder comprimate, într-un folder necomprimat, fişierul copiat va fi decomprimat.
- Când mutați un fişier sau folder în interiorul unei partiții NTFS, fişierul sau folderul păstrează starea de compresie inițială. Astfel că, dacă mutați un fişier sau folder comprimate, într-un folder necomprimat, fişierul mutat rămâne comprimat.
- Un fişier comprimat copiat în partiții FAT sau FAT32 sunt decomprimate. Aceasta deoarece compresia nu este suportată de aceste tipuri de partiții.
- Dacă fişierele sunt mutate dintr-o partiție FAT sau FAT32 într-o partiție NTFS, acestea vor primi atributul de compresie.

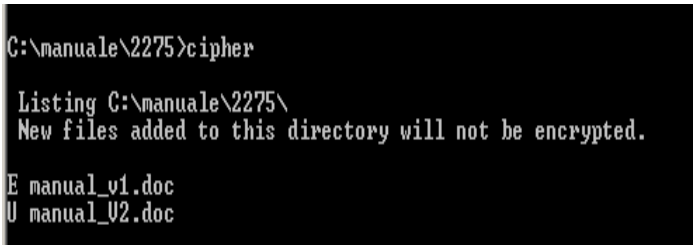
Configurarea criptării

Un utilizator intrus, care are acces fizic la un calculator, poate instala un alt sistem de operare şi poate avea acces la fişiere, trecând peste regulile de securitate impuse inițial. Un răspuns la un astfel de scenariu este folosirea Sistemului de Criptare a Fişierelor (*Encrypted File System* - EFS). Datele aflate într-un fişier criptat sunt protejate chiar şi în situația în care intrusul are permisiuni complete asupra calculatorului.

EFS funcționează numai pentru volumele NTFS. Chiar dacă se vorbeşte despre dosare criptate, trebuie reținut că – de fapt – sunt criptate numai fişierele. Un dosar marcat drept criptat conține fişiere criptate.

Criptarea / decriptarea fişierelor se face prin modificarea corespunzătoare a atributului.

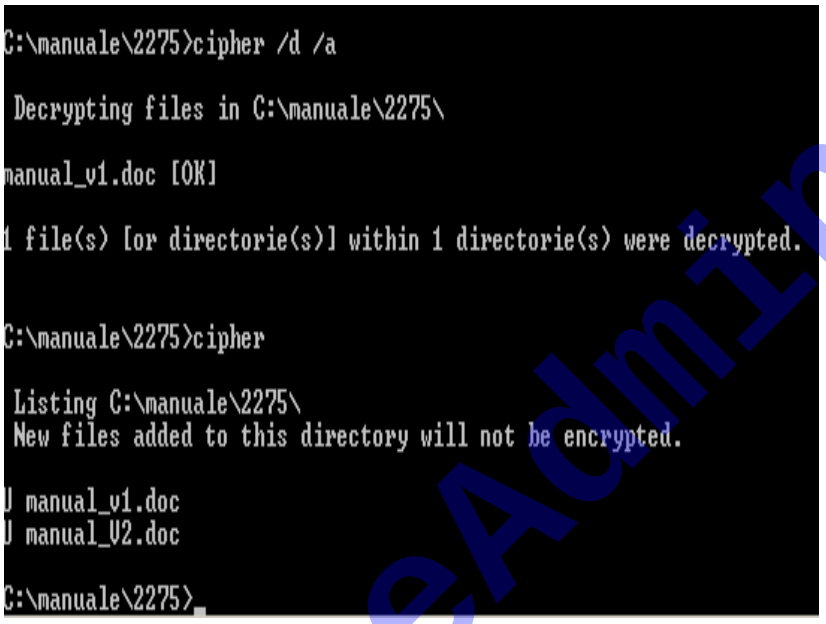
- Metoda1: aplicarea atributului de criptare se face urmând aceeaşi cale ca pentru atributul de compresie, respectiv bifați opțiunea *Encrypt contents to secure data* în fereastra *Advanced Attributes*



- Metoda 2: există şi o comandă introdusă la prompterul *Command Prompt* pentru criptarea / decriptarea fişierului, comanda se numeşte *cipher*.

În exemplul nostru a fost lansată comanda *cipher* care afişează starea curentă a atributului de criptare asociat directorului 2275 şi fişierelor din director (E – *encrypted*, U – *unencrypted*) şi informează asupra atributului de criptare pentru fişierele ce vor fi create aici.

În imaginea următoare este prezentată folosirea comenzii *cipher* cu două opțiuni, opțiuni care decriptează fişierul criptat *manual_v1.doc*.



EFS utilizează pentru criptare o combinație de chei: cheie publică – cheie privată împreună cu chei simetrice. Cheile simetrice sunt folosite pentru criptarea fişierului, iar perechea de chei publică – privată pentru protejarea celor simetrice. Criptarea de tip simetric este aceea în care, atât pentru criptare cât şi pentru decriptare, se foloseşte aceeaşi cheie.

Perechea de chei publică – privată este implementată prin certificatele utilizatorilor. Fiecare certificat conține o cheie publică folosită pentru criptarea cheii simetrice. După aceea numai utilizatorul care deține cheia privată corespunzătoare poate avea acces la cheia simetrică pentru decriptare.

Fiecare utilizator care deschide sesiune la un calculator cu sistem de operare *Windows Server 2003* poate cripta fişiere. La prima criptare de fişiere, EFS generează un certificat şi deci o pereche de chei pentru utilizator.

Toate fişierele şi dosarele create într-un dosar marcat drept criptat vor fi criptate. Fişierele criptate pot fi partajate – la nevoie – între mai mulți utilizatori locali, din domeniu, sau din alte domenii de încredere (*trusted*). Autorizarea accesului la fişierele criptate este o combinație de configurări de permisiuni ACL şi EFS. Pot fi autorizați numai utilizatori individuali, nu grupuri de utilizatori.

Agentul Recuperator

Ştergerea unui cont utilizator conduce şi la pierderea certificatului. Fără existența unui agent recuperator, utilizatorul nu mai poate folosi fişierele criptate pentru care a folosit certificatul. Mai mult chiar, modificarea parolei unui utilizator face imposibilă citirea cheii private din certificat.

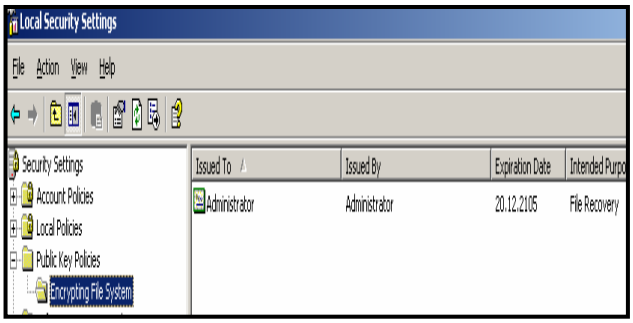
Agentul recuperator este persoana autorizată să decripteze fişiere criptate anterior de altcineva. Agentul recuperator într-un domeniu este Administratorul. Această calitate poate fi delegată însă oricui. Agentul recuperator beneficiază de un certificat special. Pentru a-l folosi în deplină siguranță, certificatul trebuie exportat şi apoi salvat într-o locație sigură. Certificatul inițial (cel instalat inițial pe calculator) va fi şters. Singurul exemplar ar trebui să rămână cel salvat. Pentru fiecare operație de recuperare certificatul va fi importat pe un calculator, folosit pentru accesul la fişier şi şters din nou.

Politica de recuperare a fişierelor criptate este implementată local, la fiecare calculator independent (*stand alone*). Pentru calculatoarele care fac parte dintr-un domeniu, politica poate fi implementată atât la nivelul domeniului, cât şi la nivelul unității organizaționale sau chiar la nivel local.

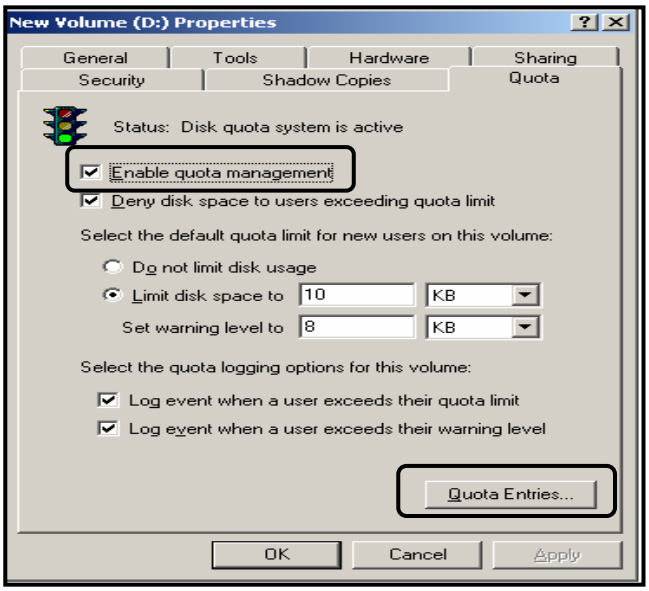
```
C:\manuale\2275>cipher /R:certificate
Please type in the password to protect your .PFX file:
Please retype the password to confirm:


Your .CER file was created successfully.
Your .PFX file was created successfully.

C:\manuale\2275>_
```

Este prezentată comanda de creare a unui certificat de recuperare (.CER) şi a unui fişier (.PFX) care conține certificatul şi cheia privată.

Administratorul este de obicei agentul recuperator:

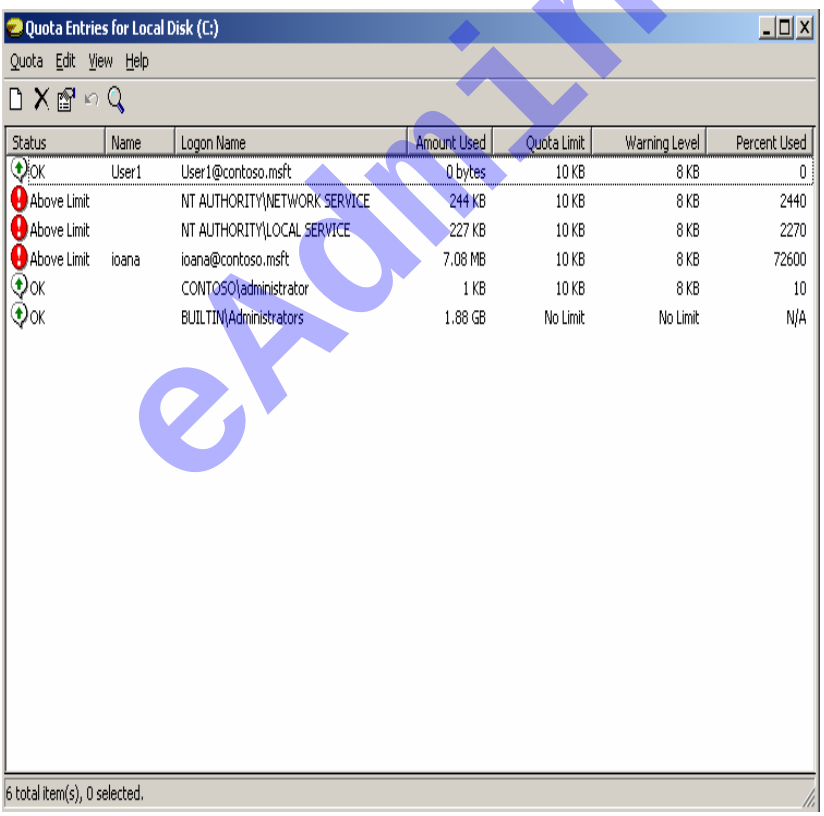


Implementarea cotelor de disc



Cotele alocate pe disc utilizatorilor sunt o metodă pentru gestionarea resurselor unui server. Cotele limitează spațiul disponibil fiecărui utilizator. Cotele asociate utilizatorilor funcționează numai pentru volume NTFS.

Opțiunea *Enable quota management* permite stabilirea unui anumit spațiu de lucru pe unitatea de disc selectată, pentru utilizatorii noi. Pentru a vizualiza starea de ocupare a spațiului alocat utilizatorilor, se deschide fereastra *Quota Entries*. Se observă avertizările de depăşire de cotă (*Above Limit*) pentru unii dintre utilizatori.



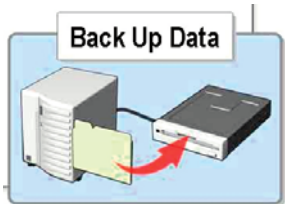
Controlul recuperării datelor în urma dezastrelor

Pierderea accidentală a datelor păstrate la un calculator poate fi asemănată cu o catastrofă. Multe activități economice, financiare sau de altă natură depind de existența şi prelucrarea unor date considerate critice. Ca urmare, trebuie acordată o mare atenție protecției datelor față de pierderea sau alterarea lor accidentală.

Recuperarea datelor „pierdute” este încercarea de revenire, de restaurare a datelor şi a serviciilor în forma existentă înaintea producerii accidentului.

Pentru fiecare aplicație, serviciu, sistem de operare folosite într-o rețea trebuie să existe în orice moment răspunsuri la următoarele întrebări:

- Care sunt scenariile posibile pentru pierderea accidentală a datelor?
- Ce date sunt critice?
- Cât de des ar trebui efectuate operațiile de salvare?
- Cât timp ar trebui păstrat un exemplar de *backup*?
- Cât de repede pot fi restaurate datele lipsă?



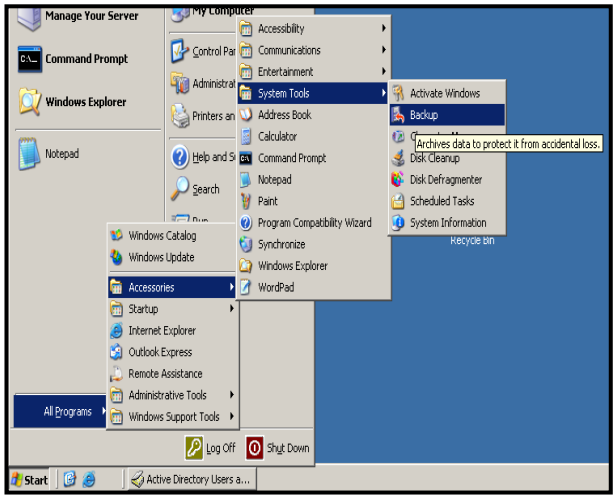
- Unde vor fi păstrate exemplare de *backup* astfel încât numai persoanele autorizate să le poată folosi rapid şi sigur?
- Dacă lipseşte administratorul de sistem există totuşi cineva care să cunoască parolele şi procedurile de *backup* şi care, la nevoie, să poată restaura / reface sistemul de operare?
- Când e bine să se efectueze operațiile de *backup* ? Atunci când lucrează şi utilizatorii sau când sistemul este *offline*?
- Cât de des se modifică datele considerate critice?
- Cum se poate verifica corectitudinea desfăşurării operației de *backup* şi integritatea datelor salvate?

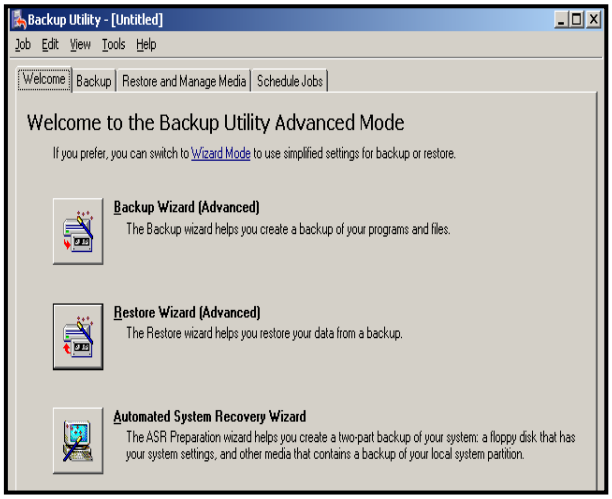
Fiecare administrator trebuie să-şi construiască un plan pentru recuperarea datelor pierdute accidental. Planul trebuie testat şi corectat, dacă este cazul. Modificările aduse planului inițial vor fi notate şi documentate cu atenție. Ar fi bine să existe în permanență două exemplare ale aceluiaşi *backup*: unul la îndemână în vederea posibilei restaurări şi celălalt păstrat în siguranță în altă parte. Nu numai datele trebuie salvate: pentru sistemul de operare trebuie să existe un *backup* al stării sistemului în vederea restaurării pe acelaşi calculator sau pe un altul.

În plus, pentru servere, se recomandă construirea unei console *Recovery Console*, inclusă ca opțiune de startare a calculatorului. CD-ul cu sistemul de operare trebuie păstrat la îndemână şi în siguranță, disponibil pentru corectarea (sau înlocuirea) la nevoie a unor componente ale sistemului de operare.

Salvarea datelor

Windows Server 2003 pune la dispoziție utilitarul *Backup* pentru salvarea datelor, inclusiv a sistemului de operare, respectiv pentru restaurarea datelor.





Folosirea acestui utilitar este permisă următorilor utilizatori:

- Utilizatorii pot face *backup* pentru fişierele şi dosarele unde sunt proprietari şi acolo unde au permisiunea *read*;
- Utilizatorii care au dreptul *Backup Files and Directories* pot salva fişiere aflate la acel server.
- Cei care au dreptul *Restore Files and Directories* pot restaura fişiere la respectivele calculatoare;
- Membrii grupurilor locale domeniului *Administrators*, *Backup Operators* şi *Server Operators* pot salva şi restaura toate fişierele indiferent de permisiunile lor NTFS.

Din raţiuni de securitate se recomandă constituirea a două grupuri noi de utilizatori: unul pentru cei care vor face salvările şi altul pentru cei care vor face restaurări. Celor două grupuri li se vor asocia, respectiv, dreptul de *Backup* sau cel de *Restore*.

Starea sistemului (*System State*) este colecția specifică de date folosită de sistemul de operare pentru încărcarea, configurarea şi execuția componentelor sale. Se cuprind aici următoarele fişiere sistem:

- *Registry*;
- Fişierele necesare încărcării sistemului de operare (fişiere de *boot*);
- Baza de date a serviciului de certificate - dacă este cazul;
- Serviciul *Active Directory* – în cazul controlerelor de domeniu;
- *SYSVOL* - în cazul controlerelor de domeniu;
- Metadirectorul IIS - dacă este cazul;
- Fişierele sistem protejate prin *Windows File Protection*;

Salvarea şi restaurarea stării sistemului sunt privite ca un întreg: nu pot fi salvate şi nici restaurate componente individuale. În schimb restaurarea stării sistemului se poate face şi pe un alt calculator decât cel originar. O astfel de restaurare nu va conduce însă la restaurarea componentelor legate de *Active Directory*, şi anume Serviciul *Active Directory* şi *SYSVOL*. Restaurarea stării sistemului pentru un controler de domeniu nu se poate face decât în modul *Directory Service Restore Mode*.

Utilitarul *Backup* admite următoarele tipuri de salvări, în funcție de modul în care este folosit atributul de arhivare asociat fişierelor salvate:

Normal	Salvează toate fişierele selectate, indiferent de valoarea atributului de arhivare. Fişierele salvate sunt marcate prin valoarea zero a atributului de arhivare.
Diferential	Dintre fişierele selectate le salvează doar pe cele modificate de la ultima salvare, adică numai pe acelea pentru care atributul de arhivare are valoarea unu. Fişierele salvate nu sunt marcate: atributul de arhivare rămâne cu valoarea unu.
Incremental	Dintre fişierele selectate vor fi salvate numai cele modificate în timpul scurs de la ultima salvare; vor fi salvate numai fişierele care au atributul de arhivare poziționat (valoare unu). Fişierele salvate sunt marcate ca atare, atributul de arhivare este poziționat la zero (atributul de arhivare este şters).
Copy	Modul de lucru este identic cu salvarea de tip normal, cu o singură excepție: atributul de arhivare rămâne nemodificat.
Daily	Nu ia în considerare atributul de arhivare şi nici nu îl modifică. Salvează fişierele care au fost modificate în ziua respectivă. Criteriul de selecție este data ultimei modificări, conform proprietăților fişierului.

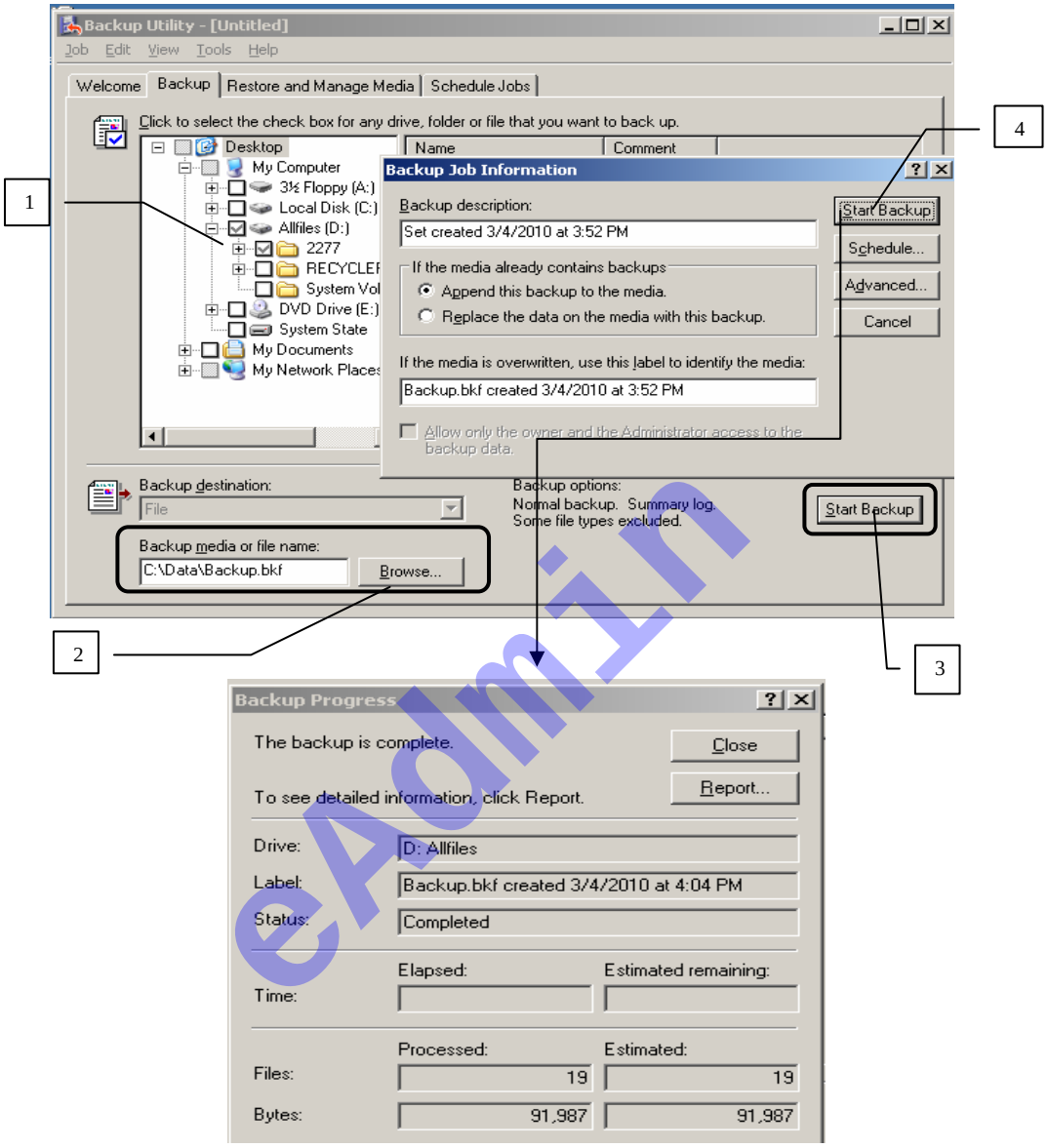
În afara utilitarului *Backup* mai poate fi folosită comanda *ntbackup*.

*Automated System Recove*y **(**ASR**)** – refacerea automată a sistemului - este componenta care ajută la recuperarea (sau refacerea) automată a unui sistem care nu mai porneşte. ASR are două componente: una de salvare – *backup* şi alta de restaurare – *recovery*. ASR salvează unele informații pe o dischetă ce va fi folosită în procedura de recuperare a sistemului.

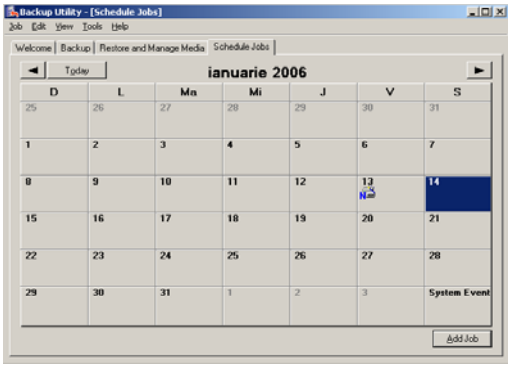
După instalarea unui nou sistem de operare *Windows Server 2003* se recomandă crearea setului ASR şi a dischetei corespunzătoare. Salvarea de tip ASR cuprinde starea sistemului, serviciile sistem, volumele *boot* şi sistem. Discheta construită de procedura ASR conține descrierea configurației discurilor, inclusiv volumele dinamice şi modalități de restaurare. ASR nu face *backup* pentru alte volume decât cele de *boot* şi sistem.

În exemplul de mai jos, folder-ul 2277 este selectat pentru lansarea *backup*-ului. Este lansată comanda *Start Backup*, după ce s-a stabilit în câmpul *Backup media or file name*, discul, locul pe disc unde se va crea copia de siguranță, precum şi numele fişierului de tip *backup*.

Numerele din figură indică ordinea acțiunilor în vederea lansării procedurii de *backup*.



Planificarea operațiilor de *backup*



Cele mai multe operații de *backup* au loc în momente de timp strict specificate. Fiind operații de rutină, execuția lor poate fi planificată (programată) din timp.

În fereastra de mai jos, este exemplificată o programare de *backup normal*.

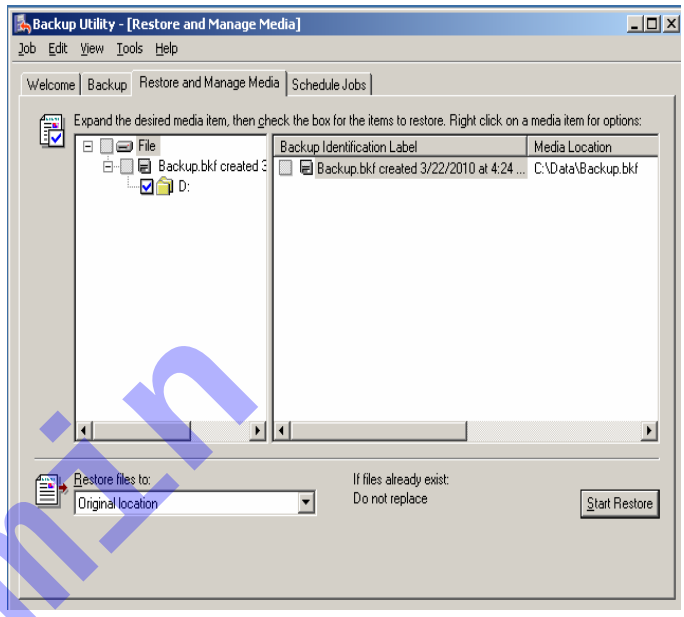
Restaurarea datelor

Procedura de *Restore*, din cadrul aplicației *Backup*, este folosită pentru restaurarea datelor, date ce au fost salvate, respectiv arhivate prin procedura de *Backup*.

Puteți folosi procedura de *Restore* pentru următoarele situații:

- Restaurarea fişierelor şi folderelor ce au fost salvate prin procedura de *Backup*

Fişierele şi folderele arhivate prin procedura de *Backup* pot fi restaurate în acelaşi loc sau în altul.



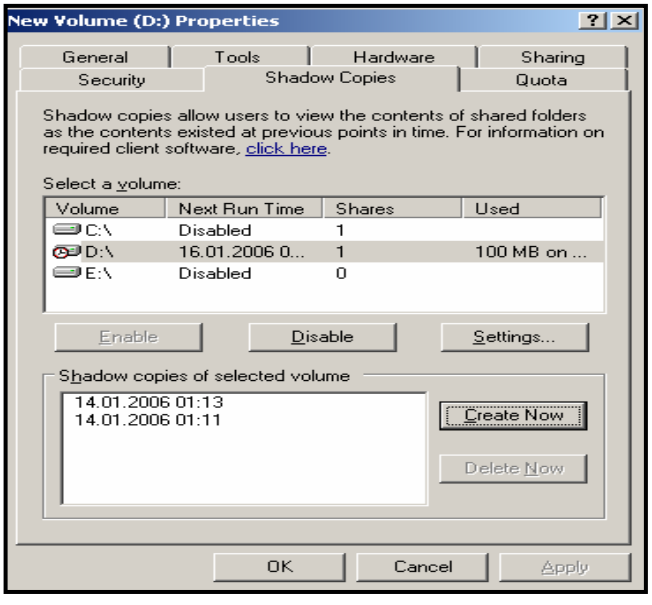
- Restaurarea datelor ce reprezintă starea sistemului - *System State*

Dacă datele ce reprezintă *System State* au fost salvate cu *Backup* şi sistemul nu mai funcționează, puteți reface calculatorul, cu ajutorul unui CD original de *Windows Server* şi folosind datele sistem salvate

- *Automated System Recovey* (ASR) – refacerea automată a sistemului

Copiile *shadow*

Exemplarele (copiile) *shadow* (din umbră) sunt exemplare *read-only* ale fişierelor din foldere partajate din rețea. Prin această tehnică pot fi văzute şi restaurate exemplare (versiuni) mai vechi ale unor dosare şi fişiere, aşa cum erau ele în decursul timpului.



Această tehnică permite:

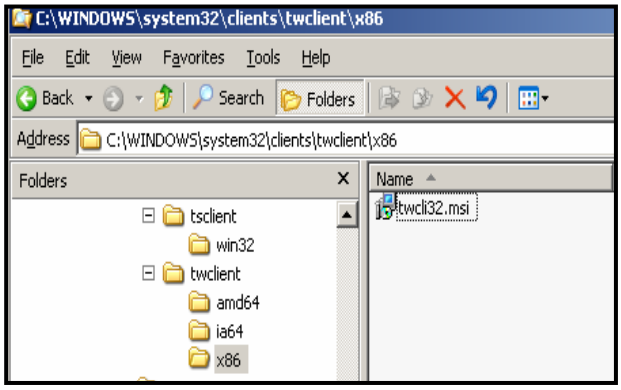
- Recuperarea fişierelor şterse din greşeală;
- Recuperarea fişierelor modificate (suprascrise) din greşeală;
- Verificarea modificărilor aduse versiunilor unor fişiere în timpul lucrului;

Caracteristica *Shadow copy* este disponibilă numai la nivelul volumului şi nu poate fi asociată numai anumitor dosare partajate.

Clienții nu au capacitatea implicită de a avea acces la exemplarele din umbră. Accesul va fi permis numai după instalarea componentei client *Previous Version*. Fişierele folosite pentru instalare sunt cele din directorul:

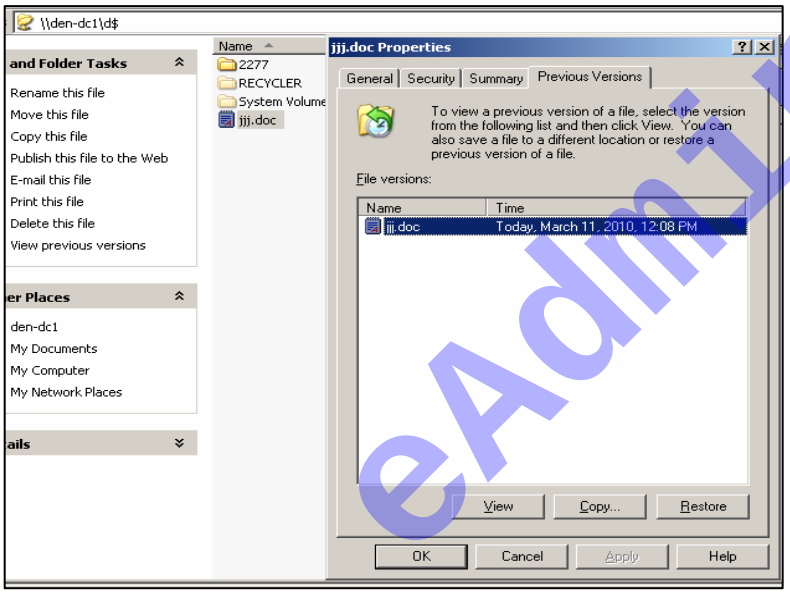
`%systemroot%\system32\clients\twclient\x86`

aflat la serverul care implementează soluția exemplarelor "din umbră".



Exemplare *Shadow* sunt instantanee ale fişierelor la un moment dat. Copiile *Shadow* nu sunt disponibile pentru fişierele stocate pe computere client, numai pe server. Acestea pot fi vizualizate de la ambele: servere şi client.

Pe server, accesul la copiile *shadow* se face astfel: discul pentru care s-a stabilit proprietatea *Shadow copies* se accesează ca un *folder shared*, apoi se intră în proprietățile fişierului – caseta *Properties*, care conține tab-ul *Previous Versions*.



Recuperarea sistemului de operare

Există mai multe metode de restaurare a informațiilor, respectiv de refacere a unui calculator, de revenire la starea anterioară considerată corectă. Dacă el nu porneşte corect ar putea fi folosit modul de lucru *safe*, cu un minim de servicii şi componente active. Este modul de lucru în care se pot diagnostica şi corecta erorile apărute.

Startarea în modul *Last Known Good Configuration* – ultima configurație considerată corectă - este opțiunea pentru revenirea la starea anterioară, dacă se consideră ca este ultima corectă, ceea ce conduce la restaurarea subcheii *registry*:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet`

Informațiile ce sunt folosite pentru startarea calculatorului în modul *Last Known Good Configuration* sunt actualizate numai în urma încărcării normale a sistemului de operare şi a deschiderii corecte a sesiunii (*log on*).

Consola de recuperare (*Recovery Console*) reprezintă lansarea în execuție a unei versiuni minimale a sistemului de operare, ce poate fi folosită pentru corectarea sistemului de operare. Consola permite execuția unui număr mare de comenzi de diagnosticare şi corecție. Consola de recuperare se instalează local, folosind comanda:

```
X:\i386\winnt32.exe /cmdcons
```

Propunere de temă practică:

1. Deschideți sesiunea ca utilizator fără privilegii de administrare. Folosind comanda *runas* lansați în execuție diverse instrumente de administrare

2. Creați o consolă *mmc* pentru aplicația *Computer Management* pentru administrarea calculatorului local şi a unui alt calculator din rețea. Salvați consola creată pe desktop cu numele CompMan

3. Monitorizați activitatea calculatorului dvs. cu ajutorul consolei *Performance* urmărind contoarele: *Pages/sec* la obiectul Memorie, *%Procesor Time* la obiectul Procesor, *%Disk Time* la obiectul Disc Fizic,*(Physical Disk)* şi *Bytes Sent/sec* la obiectul adaptor de rețea *(Network Interface).*

4. Monitorizați activitatea calculatorului dvs. cu ajutorul aplicației *Task Manager.* Deschideți consola *Performance.* Urmăriți aplicațiile (*Applications*) şi procesele (*Processes*)active. Închideți consola *Performance* şi observați efectul.

5. Folosind consola *Computer Management (Local)* identificați principalele drivere folosite. Ce resurse (*I/O Range*, *Memory Range* şi IRQ) foloseşte adaptorul de rețea?

6. Verificați dacă fişierele sistem au versiuni corecte (necesită CD !!!)

7. Verificați semnăturile digitale ale fişierelor sistem şi ale drivere-lor din calculatorul dvs.

8. Creați o consolă *mmc*, în care aduceți utilitarul Disk Management. Notați câte partiții are hard discul calculatorului dvs., ce capacitate au aceste partiții, ce tip de format de fişiere are fiecare partiție ?

9. Montați o unitate de disc într-un dosar gol, nou creat de dvs.

10. Construiți un folder cu numele dvs. în care creați unul sau mai multe fişiere de care tip doriți (.txt, .doc, .ppt) care să aibă conținut. Comprimați folderul prin metodele învățate. Notați de fiecare dată dimensiunea inițială, respectiv cea a folderului comprimat.

11. Mutați, respectiv copiați fişierele comprimate într-un folder nou creat în aceeaşi partiție şi observați starea atributului de compresie.

12. Mutați, respectiv copiați fişiere necomprimate în fodere care au atributul de compresie. Notați ce observați.

13. Aplicați atributul de criptare unuia din fişierele create de dvs.

14. Verificați dacă există un agent recuperator

15. Stabiliți un anumit spațiu de lucru (de exemplu 100 KB) pe unitatea de disc existentă.

16. Vizualizați intrările de cotă existente.

17. Pentru un utilizator nou creat, care şi-a creat un folder cu fişiere pe unitatea de disc care are limită de spațiu de lucru, vizualizați intrările de cotă (*quota entries*). Notați informațiile ce apar în fereastra *Quota entries* pentru acest utilizator.

18. Creați un *backup normal* pentru folderul creat de dvs. într-un loc pe disc.

19. Creați un fişier nou, stabiliți pentru volumul pe care ați creat fişierul proprietatea *Shadow copies*, apoi verificați copiile shadow pentru acel fişier.

Ce ați învățat în acest capitol?

- ✓ Să utilizați comanda *Run as* pentru lansarea în execuție a unei componente care cere privilegii administrative
- ✓ Să utilizați colecția de instrumente administrative ce compun *Computer Management* pentru administrarea calculatorului local sau a unuia aflat la distanță (*remote*).
- ✓ Să utilizați *Remote Desktop* pentru administrarea de la distanță a unui server
- ✓ Să urmăriți performanțelor serverelor folosind consola *Performance* şi utilitarul *Task Manager*
- ✓ Să urmăriți funcționarea sistemului prin interpretarea conținutului fişierelor de tip jurnal şi a mesajelor înregistrate cu *Event Viewer*
- ✓ Să supravegheați performanțele serverelor urmărind contoarele specifici pentru: memoria, procesorul (procesoarele), discul (discurile) şi rețeaua
- ✓ Să utilizați pentru fiecare echipament ataşat calculatorului driverul corespunzător.
- ✓ Să verificați periodic sau în cazul sesizării unei disfuncții existența unor fişiere sistem sau drivere bune, iar în caz de compromitere a unor astfel de fişiere să fie refăcute la forma corectă a lor.
- ✓ Cum să gestionați discurile calculatoarelor locale cât şi la distanță.
- ✓ Mai multe metode de gestionare a discurilor.
- ✓ Cum să montați unitățile de disc.
- ✓ Care sunt proprietățile discurilor dinamice
- ✓ Care sunt tipurile de volume dinamice.
- ✓ Ce sunt volumele tolerante la erori.
- ✓ Să comprimați fişierele, folderele.
- ✓ Să criptați fişierele
- ✓ Să creați cote alocate utilizatorilor.
- ✓ Să creați copii de siguranță datelor – *backup*.
- ✓ Ce sunt copiile *shadow* şi cum se creează.
- ✓ Moduri de lucru folosite pentru restaurarea informațiilor, refacerea unui calculator.