

ATENŢIONARE!

Conținutul acestei platforme de instruire a fost elaborat în cadrul proiectului "Dezvoltarea resurselor umane în educație pentru administrarea rețelelor de calculatoare din școlile românești prin dezvoltarea și susținerea de programe care să sprijine noi profesii în educație, în contextul procesului de reconversie a profesorilor și atingerea masei critice de stabilizare a acestora în școli, precum și orientarea lor către domenii cerute pe piața muncii". Conținutul platformei este destinat în exclusivitate pentru activități de instruire a membrilor grupului țintă eligibil în proiect.

Utilizarea conținutului în scopuri comerciale sau de către persoane neautorizate nu este permisă.

Copierea, totală sau parțială, a conținutului de instruire al acestei platforme de către utilizatori autorizați este permisă numai cu indicarea sursei de preluare (platforma de instruire eadmin.cpi.ro).

Pentru orice probleme, nelămuriri, sugestii, informații legate de aspectele de mai sus vă rugăm să utilizați adresa de email: proiect.eadmin@cpi.ro

Acest material a fost elaborat de o echipă de experți 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 luga
- Lidia Băjenaru
- Rodica Majaru

Versiunea materialui de instruire: V2.0

4. Administrarea domeniilor

Serviciul director Active Directory

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

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

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

Domeniul

Conform terminologiei *Microsoft*, domeniul este reprezentat dintr-un grup de calculatoare care fac parte dintr-o rețea și care folosesc în comun aceeași bază de date în care sunt reprezentate resursele rețelei. Domeniul este administrat ca entitate distinctă, cu reguli și proceduri comune pentru toate calculatoarele care îl compun. Domeniile sunt recunoscute prin nume. Calculatoarele membre ale domeniului respectă politica de securitate a domeniului. În plus, domeniul oferă și soluția administrării centralizate a tuturor resurselor rețelei, indiferent unde ar fi ele distribuite: administrarea tuturor



resurselor reprezentate prin obiecte înscrise în această bază de date. O singură operație de *logon* în domeniu (deschidere de sesiune) este suficientă pentru ca un utilizator să fie recunoscut în domeniu și să aibă acces la resursele domeniului, în limita permisiunilor și a privilegiilor de care dispune.

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

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



Fiecare domeniu are un nume propriu.

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

Numele subdomeniului se formează prin concatenarea unui sufix la numele părintelui, ca de exemplu *uk.microsoft.com*, care este un

subdomeniu al domeniului *microsoft.com.* Liniile care unesc domeniile definesc relațiile dintre ele: în acest caz sunt relații de genul "părinte-copil" (*parent-child*) sau domeniu-subdomeniu.

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



În această figură este reprezentat un *forest* cu cu două arborescențe. Fiecare dintre ele are un spațiu de nume independent. Numele *forest*-ului este dat de numele primului domeniu creat în *forest* numit și domeniul rădăcină pentru forest (*forest root domain*). În cazul nostru este *microsoft.com*.

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

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

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

Caracteristicile domeniilor Windows Server 2003 sunt următoarele:

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

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



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

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



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

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

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

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



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

Utilizatorii care folosesc calculatoarele membre ale domeniului pot deschide sesiune local – folosind un cont utilizator local calculatorului – sau în

domeniu. In vederea deschiderii de sesiune în domeniu, clientul Active Directory care este și client DNS, interoghează mai întâi serverul DNS în căutarea unui controler de domeniu. Controlerul de domeniu este cel căruia i se va adresa și va rezolva cererea de autentificare.

Instalarea Active Directory

Serviciul director Active Directory (Active Directory Service) poate fi instalat pe calculatoare unde funcționează sisteme de operare Microsoft Windows Server 2003, ediții Standard, Enterprise și Data Center. Serviciul Active Directory are nevoie de o partiție NTFS cu minim 1 GB de spațiu liber, pentru început. În partiția NTFS se va afla baza de date a domeniului care va crește pe măsură ce vor fi adăugate obiecte în domeniu. În urma instalării serviciului Active Directory serverul devine controler de domeniu. Serverul care va deveni controler de domeniu trebuie să aibă de la început o adresa IP statică și să fie client la serverul DNS responsabil cu rezolvarea numelor în domeniu. Microsoft recomandă ca serverul controler de domeniu să îndeplinească și rolul de server DNS. Mai mult decât atât, Microsoft recomandă ca instalarea serviciului DNS să aibă loc o dată cu instalarea Active Directory.

Promovarea unui server la rolul de controler de domeniu

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



 Start -> Run şi introducem dcpromo în caseta de dialog Run.

2. Vrăjitorul (*Wizard*) **Active Directory Installation Wizard** a fost lansat în execuție și continuăm (*Next*).

3. În caseta de dialog **Domain Controller Type**, va fi ales tipul noului controler de domeniu: va fi el un controler pentru un domeniu nou (încă necreat) sau un controler de domeniu suplimentar într-un domeniu existent, creat cândva înainte. **Domain Controller for a new domain** este opțiunea pentru crearea unui domeniu nou, implicit a unui controler de domeniu într-un nou domeniu.

ctive Directo	ry Installation Wizard				
Domain Co Specify	the role you want this server to have.				
Do you addition	want this server to become a domain controller for a new domain or an al domain controller for an existing domain?				
• Don	nain controller for a new domain				
Sele This	ect this option to create a new child domain, new domain tree, or new forest. s server will become the first domain controller in the new domain.				
O <u>A</u> dd	itional domain controller for an existing domain				
	Proceeding with this option will delete all local accounts on this server.				
All cryptographic keys will be deleted and should be exported before continuing.					
All encrypted data, such as EFS-encrypted files or e-mail, should be decrypted before continuing or it will be permanently inaccessible.					
	< <u>B</u> ack <u>N</u> ext > Cancel				

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

Active Directory Installation Wizard
Create New Domain Select which type of domain to create.
Create a new:
Domain in a new forest
Select this option if this is the first domain in your organization or if you want the new domain to be completely independent of your current forest.
Child domain in an existing domain tree
If you want the new domain to be a child of an existing domain, select this option. For example, you could create a new domain named headquarters.example.microsoft.com as a child domain of the domain example.microsoft.com.
O Domain tree in an existing forest
If you don't want the new domain to be a child of an existing domain, select this option. This will create a new domain tree that is separate from any existing trees.
<u> </u>

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

Active Directory Installation Wizard	×
New Domain Name Specify a name for the new domain.	X
Type the full DNS name for the new domain (for example: headquarters.example.microsoft.com).	
Eull DNS name for new domain:	
sinca.ad	
< <u>B</u> ack <u>N</u> ext>	Cancel

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

Active Directory Installation Wizard	×
NetBIOS Domain Name Specify a NetBIOS name for the new domain.	
This is the name that users of earlier versions of Windows will use to identify the new domain. Click Next to accept the name shown, or type a new name.	
Domain NetBIOS name: SINCA	-

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

Active Directory Installation Wizard	×
Database and Log Folders Specify the folders to contain the Active Directory database and log file	es.
For best performance and recoverability, store the database and the log hard disks.	g on separate
Where do you want to store the Active Directory database?	
Database folder:	
C:\WINDOWS\NTDS	B <u>r</u> owse
Where do you want to store the Active Directory log?	
Log folder:	
C:\WINDOWS\NTDS	Br <u>o</u> wse
< <u>B</u> ack <u>N</u> ext	> Cancel

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

Active Directory Installation Wizard	×
Shared System Volume Specify the folder to be shared as the system volume.	X
The SYSVOL folder stores the server's copy of the domain's public files. The contents of the SYSVOL folder are replicated to all domain controllers in the domain.	
The SYSVOL folder must be located on an NTFS volume.	
Enter a location for the SYSVOL folder.	
Eolder location:	
C:\WINDOWS\SYSVOL Browse	
< <u>B</u> ack <u>N</u> ext > Ca	ancel

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

Active Directory Installation Wizard			×
DNS Registration Diagnostics Verify DNS support, or install DNS on this c	omputer.		A
Diagnostic Failed			▲
The registration diagnostic has been run 1	time.		
Warning: Domain Controller functions like jo and Active Directory replication will not be a Active Directory is correctly configured.	pining a domain, available until the	logging onto a dor e DNS infrastructur	nain, re for
None of the DNS servers used by this com interval.	puter responded	within the timeout	
For more information, including steps to corr	rect this problem	. see Help.	-
I have corrected the problem. Perform the problem.	he DNS diagnos	tic test again.	
 Install and configure the DNS server on this DNS server as its preferred DNS se 	this computer, a rver.	and set this comput	ter to use
O I will correct the problem later by configured in the problem later by configured	uring DNS manu	ally. (Advanced)	
	< <u>B</u> ack	<u>N</u> ext >	Cancel

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

Active Directory Installation Wizard
Permissions Select default permissions for user and group objects.
Some server programs, such as Windows NT Remote Access Service, read information stored on domain controllers.
C Permissions compatible with pre-Windows 2000 server operating systems
Select this option if you run server programs on pre-Windows 2000 server operating systems or on Windows 2000 or Windows Server 2003 operating systems that are members of pre-Windows 2000 domains.
Anonymous users can read information on this domain.
 Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems
Select this option if you run server programs only on Windows 2000 or Windows Server 2003 operating systems that are members of Active Directory domains. Only authenticated users can read information on this domain.
< <u>B</u> ack <u>N</u> ext > Cancel

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

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

Verificarea instalării Active Directory

😽 Event Viewer						_	П×
<u>File Action View H</u> elp							
← → 🗈 💽 😭 💀 🛱	?						
💼 Event Viewer (Local)	Directo	ry Service 1,23	5 event(s)				
		Date	Time	Source	Category	Event	ι.
Security	nation	10/5/2004	7:08:24 PM	NTDS General	Internal	2065	F
System	nation	10/5/2004	7:05:55 PM	NTDS KCC	Knowled	1404	Æ
Directory Service	nation	10/5/2004	7:05:52 PM	NTDS General	Service C	1394	F
Bile Deplication Service	nation	10/5/2004	7:05:46 PM	NTDS Inter-site Messa	Intersite	1570	- N
The Replication Service	nation	10/5/2004	7:05:22 PM	NTDS General	Service C	1000	Æ
	nation	10/5/2004	7:05:00 PM	NTDS Database	Internal	2064	D.
	nation	10/ Event Pro	nerties		·	2	
	nation	10/	percies				
	nation	10/ Event					
	nation	10/	N O 15 1000 (_	
	nation	10/ D <u>a</u> te:	10/5/2004	<u>Source:</u> NTDS Genera	3l	+	
	nation	10/ li <u>m</u> e:	7:05:22 PM	1 Category: Service Contri	ol	L	
	nation	10/ Тур <u>е</u> :	Information	Event ID: 1000			
	nation	10/ <u>U</u> ser:	NT AUTHO)RITYVANONYMOUS LOGO	DN .	Ē	
	nation	iation 9/2 Computer: SERVER1					
	nation	9/2 Davai					
	ng	ng 9/2 Description:					
	100	9/2 Micros	oft Active Direct	tory startup complete, versio	n 5.2.3790.183	30	
For more information, see Help and Support Center at							
http://go.microsoft.com/fwlink/events.asp.							

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

🚊 dnsmgmt - [DNS\L304A5\Forward Lookup Zones\sinca.ad_tcp]							
虎 Eile Action View Window Help							
	_ tcp 4 record(5)					
	Name	Туре	Data				
 □- □ Forward Lookup Zones □- □ _msdcs □- □ _sites □- □ _udp □- □ _udp □- □ ForestDnsZones □- □ ForestDnsZones □- □ Reverse Lookup Zones □- □ Event Viewer 	Updap	Service Location (SRV) Service Location (SRV) Service Location (SRV) Service Location (SRV)	[0][100][3268] 304a5.sinca.ad. [0][100][88] 304a5.sinca.ad. [0][100][464] 304a5.sinca.ad. [0][100][389] 304a5.sinca.ad.				

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

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

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

- Active Directory Domains and Trusts: pentru vizualizarea şi modificarea relațiilor de încredere dintre domeniile Active Directory.
- Active Directory Sites and Services: pentru crearea şi coordonarea siteurilor şi a serviciilor Active Directory.

Includerea unui computer în domeniu

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

Courseluine		
Connect using:	General Alternate Configuration	
🖷 Realtek RTL8168/8		and an and a
This connection uses the fi	this capability. Otherwise, you need to ask your network at the appropriate IP settings.	Jork supports Iministrator for
🗹 🔜 Client for Microsof		
🗹 🚚 File and Printer Sk	Obtain an IP address automatically	
🗹 🛃 QoS Packet Sche	O Use the following IP address:	
Internet Protocol (IP address:	-
Install	Subnet mask:	10
Description	Default gateway:	-
Transmission Control Pro wide area network proto across diverse interconr	Obtain DNS server address automatically	
	Use the following DNS server addresses:	
Show icon in notification	Preferred DNS server: 172 . 20 . 1	. 13
Notify me when this cor	Alternate DNS server:	
C	(Advanced

Introducerea calculatorului în domeniu, se obține prin System Properties.

system Properties			<u>?</u> ×		
Advanced General Windows uses	Automatic Updat Computer Name s the following informatic	es Rem Hardwa on to identify your comp	ote are uter		
on the network Computer description: Full computer name: Workgroup: To rename this computer	k. For example: "IIS Pro "Accounting Server" 1304b3. L304 r or join a domain, click	Computer Name Cl You can change the computer. Changes Computer name: [1304b3 Full computer name: 1304b3.	Computer Name of Computer Name of Computer Name of Computer Name of Computer Enter the name ar to join the domain User name: Eassword:	Changes Ind password of an accou	2 ×
	<u></u> DK	Member of Domain: sinca.ad Workgroup: L304	OK	OK	Cancel

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

Log On to Wi	ndows
	Windows Server 2003 Enterprise Edition
Copyright © 1985-	2003 Microsoft Corporation Microsoft
<u>U</u> ser name: <u>P</u> assword:	administrator
Log on to:	L304B3 (this computer) L304B3 (this computer) SINCA Cancer Options <<

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

Objecte Active Directory

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

nterial Comparison of the Active Directory Users and Comp	uters							
Generation View Window Help								
	😫 🦉 👸 🕷	n 🖓 🍕 🗽 👘						
Active Directory Users and Computer	Computers 1 obje	cts						
🗄 💼 Saved Queries	Name	Туре	Description					
🖻 🔂 sinca.ad	COMPUTER1	Computer						
E								
ForeignSecurityPrincipals								
NTDS Quotas								
E System								

Unitate organizațională

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

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

4	Sective Directory Users and Computers											
Ø	Eile	<u>A</u> ctior	n <u>V</u> iew	<u>W</u> ind	ow	Hel	þ					
Ŷ	\Rightarrow	£	🖸 🛍	8	¢	B	🕄		1 0 1 0	i 🐌 🖓 🍕 ն	1	
9	Activ	e Direc	tory Users	and C	ompu	ter	sinca	a.ad S	5 object	s		
	· 🛄 🗅 .esti 👼	aved Q	ueries				Name	;		Туре	Description	
.		Buil Cor Dor For Use	D <u>e</u> lega Find Conne <u>C</u> onne R <u>a</u> ise [Operat	te Con :t to <u>D</u> (:t to D()omain ions <u>M</u>	trol omain omain Func aster:	I Cor tiona	ntroller al Leve	 I	s ont cur	builtinDomain Container Organizational Container Container	Default container for upgr Default container for dom Default container for secu Default container for upgr	
	New					Þ	Con	nputer				
			All Tas	<u>s</u>			•		Cor	itact		
View New <u>W</u> indow from Here Refresh Export List P <u>r</u> operties			Here	e	•	Gro Inel MSN	up tOrgPerson 40 Queue Alias					
					Org Prin	anizational Unit Iter						
			User Shared Folder		r red Folder							
			<u>H</u> elp								-	
		-							_			



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

Active Directory Users and Comp	uters	
🥪 Eile Action <u>V</u> iew <u>W</u> indow <u>H</u> e	lp	
🌤 🗕 🗈 🖪 🖬 🖻 🗟	- 1 🖸 🐮 🖉 ն 🤉	7 🍕 🙍
Active Directory Users and Computer	OU1 0 objects	
E Saved Queries	Name Type	Description
	•	There are no items to show in tl
Computers Computers Operation Controllers ForeignSecurityPrincipals ForeignSecurityPrincipals	D <u>e</u> legate Control Mo <u>v</u> e Find	
	<u>N</u> ew All Tasks	Computer
	Refresh	Group
	⊻iew	MSMQ Queue Alias
	Arrange <u>I</u> cons Lin <u>e</u> up Icons P <u>r</u> operties	Organizational Unit Printer User Shared Folder
	Help	

3111.7

Conturi pentru utilizatori

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

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

Active Directory Users and Computers							
🎸 Eile <u>A</u> ction <u>V</u> iew <u>W</u> indow <u>H</u> e	þ						
	😢 💵 🦉 🖉 🏙 🖓 🍕)	Ð					
Active Directory Users and Computer:	Users 21 objects						
terment Saved Queries	Name	Type ⊽	Description				
	🙎 Administrator	User	Built-in account for adm				
	🜆 Guest	User	Built-in account for gue				
Domain Controllers	🔮 IUSR_L304A5	User	Built-in account for ano				
E ForeignSecurityPrincipals	🕵 IWAM_L304A5	User	Built-in account for Inte				
	5UPPORT_388945a0	User	This is a vendor's accou				
🛛 🕜 OU1	🕵 DnsUpdateProxy	Security Group	DNS clients who are per				
	🕵 Domain Admins	Security Group	Designated administrati				
	🕵 Domain Computers	Security Group	All workstations and ser				
	🕵 Domain Controllers	Security Group	All domain controllers in				
	🕵 Domain Guests	Security Group	All domain guests				

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

🌍 Eile Action <u>V</u> iew <u>W</u> indow Help	〕 蔺 │ 海 閷 浩 ▽	2.0
		🍕 🔟
Active Directory Users and Computer: OUT	1 0 objects ne Delegate Control Moye Find Find New All Tasks Refresh View Arrange Icons Ling up Icons Properties Help	Type ▼ D There are no items to sho Computer Contact Group InetOrgPerson MSMQ Queue Alias Organizational Unit Printer User Shared Folder

New Object - User		×
Create in: sinca.ad/D	001	
Eirst name: user1	Initials:	
Last name:		
Full n <u>a</u> me: user1		
User logon name:		
user1	@sinca.ad	
User logon name (pre- <u>W</u> indows 20	00):	
SINCAL	user1	
	< Back Next > Cancel	

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

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

	Resetare Parola (Reset	File Action Yiew Window Help			
	Password) – îi oferă		a na Lao		A2 Cm
			2 🖻 🗟	🛄 🕂 🕅 🕅 🕅 🕅	≪ 🧏
	administratorului posibilitatea	Astino Directory Heave and Computers [
	stabilirii unei noi parole pentru	Active Directory Users and Computers [UU1 100)	ects	
	acel utilizator		Name		Tuna 🗸
		🖻 🖓 sinca.ad			Tyhe
		Builtin	🗶 user1	Cody	User
•	Dezactivare cont <i>Disable</i>			Add to a group	
	Account) - contul devine	Compacers		Aud to a group	
	demostivet perfolosibili pu ee			Di <u>s</u> able Account	
	dezactivat, neroiosibii, nu se			Reset Password	
	poate face deschidere de	📴 Users		Move	
	sesiune folosind un cont	🙆 OU1		Anna Hana Basa	
		<u> </u>		Open Home Page	
	dezactivat. Operația inversa			Send M <u>a</u> il	
	este Activare cont (Enable				
	Accout)			All Tas <u>k</u> s 🔹 🕨	
	, 1000at)				
				Cu <u>t</u>	
•	Adaugare in grup (Add to a			<u>D</u> elete	
	aroup)			Rename	
	9.000			Kond <u>m</u> o	
_				Properties	
	Copiere (Copy)				
				Help	
	Mutare (Move)		·		1
			1		

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

Active Directory Users and Computers [Saved Queries Saved Queries	OU1 1 objects				
 inca.ad Builtin Computers Domain Controllers ForeignSecurityPrincipals Users OU1 	Name	Copy Add to a group Digable Account Reset Password Moye Open Home Page Send Mail All Tasks Cut Delete Rename Properties Help	licer		

Să examinăm câteva dintre proprietățile sau atributele conturilor utilizator:

	user1 Properties
dintre	Member Of Dial-in Environment Sessions Remote control Terminal Services Profile COM+ General Address Account Profile Telephones Organization
ridutele	User logon name: User1 @sinca.ad ▼ User logon name (pre- <u>W</u> indows 2000):
	SINCA\ user1
	Account gotions:
	User must change password at next logon User cannot change password Password never expires Store password using reversible encryption
	Account expires Never End of: Wednesday, March 10, 2010
	OK Cancel Apply

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



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

Conturi pentru computere

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



(Controlere de domeniu). Includerea unui calculator în domeniu determină crearea automată a unui cont calculator în containerul **Computers** (Computere).

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

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

Identificarea obiectelor Active Directory

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

Din structura unui specificator complet calificat fac parte:

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



Specificatorul LDAP al contului utilizator user1 este:

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

Notă: Numele CN al unui cont utilizator va fi

First name Initials. Last name.

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

user1 Properties				?)				
Member Of	Dial-in	Enviro	nment	Sessions				
Remote control	Termi	inal Services	Profile	COM+				
General Address	Account	Profile	Telephones	Organization				
User logon name: user1 @sinca.ad								
User logon name (pre- <u>W</u> indows 2000): SINCA\ user1								

Obiectele utilizator pot fi identificate prin aşa-numitul *User Principal Name* (UPN). Formatul general al acestui specificator este **sufix@domeniu**, sau în cazul nostru *user1@sinca.ad*. Toate obiectele Active Directory pot fi identificate prin GUID – *Globally Unique Identifier* – identificatorul unic global. Identificatorul este creat odată cu obiectul și nu se va modifica niciodată pe toată durata existenței obiectului, indiferent dacă obiectul se mută dintr-un loc în altul sau dacă i se schimbă numele.

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

🍕 Find Users, Contacts, and Groups	×
<u>File Edit View H</u> elp	
Find: Users, Contacts, and Groups Use Computers Printers Printers Na Shared Folders Organizational Units Gueranne Common Queries Queries	
A 4 Y	

Grupuri

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

File Action View Window He		New Object - Group	×
 Pile Action Yiew Window H → L En L	elp	New Object - Group Image: Create in: sinca.ad/OU1 Group name: gl1 Group name (pre-Windows 2000): gl1 Group scope © Dogmain local Image: Gobal Image: Global Image: Global Image: Global Image: Global Image: Global	×
	Ling up Icons Properties Help	OK Car	ncel

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

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

- Globale
- Locale domeniului
- Universale

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

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

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

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

🐗 Active Directory Users and Comput	ers		
🌍 Eile Action <u>V</u> iew <u>W</u> indow <u>H</u> elp			
	😫 💵 🦉 📆	🎽 🖓 🍕 🗑	
Active Directory Users and Computers [Builtin 17 objects	;	
i in the saved Queries	Name	Туре	Description
	🕵 Account Ope	Security Group	Members can administer d
	🕵 Administrators	Security Group	Administrators have compl
Onion Controllers	🕵 Backup Oper	Security Group	Backup Operators can ov
	Distributed C	Security Group	Members are allowed to la
🛄 Users	Guests	Security Group	Guests have the same acc
	Manager Incoming For	Security Group	Members of this group ca
	Metwork Con	Security Group	Members in this group can
	Performance	Security Group	Members of this group ha
	Performance	Security Group	Members of this group ha
	Pre-Windows	Security Group - Do	main Local rd compatibility
	Print Operators	Security Group	Members can administer d
	Remote Desk	Security Group	Members in this group are
	Replicator	Security Group	Supports file replication in
	Server Oper	Security Group	Members can administer d
	Terminal Ser	Security Group	Terminal Server License S
	🕵 Users 💎	Security Group	Users are prevented from
	Windows Aut	Security Group	Members of this group ha

Drepturile implicite pentru principalele grupuri predefinite din domeniu sunt următoarele:

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

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

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

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

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

Cele mai cunoscute grupuri sistem sunt :

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

Nivelul funcțional al unui domeniu

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

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

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

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

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

Active Direct	ory Users and Computers	A File Action Vi	ew Window Heln
🌀 File 🛛 <u>A</u> ction	Raise Domain Functional Level		
		主 🔣	X ■ X ☎ ฿ ฿ ๗ ฅ ₩ ₩ ₩ ∀ ฬ ฅ
	Domain name:	7	Raise Domain Functional Level 🛛 🛛 🗙
ő Active Directo	sinca.ad	Active Directory L	
🗄 📄 Saved Qu		E 📃 Saved Querie:	Domain name:
🗄 🗊 sinca.ad	Current domain functional level:	inca.ad	vince ad
🕂 🖳 Builtin	Windows 2000 mixed	🗄 📋 Builtin	anodidu
🗄 💼 Compi		🗄 📋 Computer	Current description of local
- 🧭 Domai	Select an available domain functional level:	- 🔕 Domain Co	Current domain functional revel
🕂 📄 Foreig		🕀 🦲 ForeignSe	Windows Server 2003
🖻 🙆 OU1	Windows 2000 native	in an	
Ci	Windows 2000 native		The second second second second second second second
	on domain functional levels, click Help	📼 🖾 u 🗠	I his domain is operating at the highest possible functional level. For more information on
	on domain renotional lovelo, click help.	H- Users	domain runctional levels, click Help.
			Close Help
	<u>R</u> aise		

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

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

New Object - Group	×
Create in: sinca.ad/OU1	
Group name:	
Group name (pre- <u>W</u> indows 2000):	
Group scope	
O Domain local O Security	
O Global O Distribution	
• Universal	-
OK. Ca	ancel

Strategia A G DL P

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

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

Publicarea resurselor partajate

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

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

\\NumeComputer\NumeResursăPartajată

Pentru publicarea dosarelor partajate se folosește Active Directory Users and Computers:



New Object - Shared Folder	x
Create in: sinca.ad/0U1	
N <u>a</u> me:	_
partajatu	
Natural nath (Nserver) share):	
\\l304a5\folderx	
	_
OK Cancel	

Active Directory Users and	OU1 3 objects		
Saved Queries	Name	Туре	Desc
File Builtin	Cursuri	Organizational Unit	
	🛒 partajatu	Shared Folder	
🗄 🧭 Domain Controllers	🕵 user1	User	
🗄 🧰 ForeignSecurityPrin			

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

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

Find Shared Folders		
Elle Edit Alem Helb		
Fing: Shared Folders 🗾 In: 🗊	sinca 💌	Browse
Shared Folders Advanced		
Named:		Find Now
Kaumandar		Stop
Keywords:		<u>C</u> lear All
		- S
Search results:		
Name Share Name	Keywords	
partajatu \\ 304a5\folderx	Rena <u>m</u> e	
	Delete	
	Mo <u>v</u> e Open	
	Explore	
	Find Man Network Drive	
•	Properties	
Connect to the published Network Share		



💕 Imprim Proper	ties				? ×		
Color Management Security Device Settings General Sharing Ports Advanced Image: Start Star							
C Do not she C Share this Share name: ✓ List in the Drivers If this printe Windows. y users do not the shared	this printer to be shared with other computers on the network. Do got share this printer Share name: Institut List in the directory Drivers If this printer is shared with users running different versions of Windows, you may want to install additional drivers, so that the users do not have to find the print driver when they connect to the shared printer. Additional Drivers						
		ОК	Cance		oly		

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



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

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

🍜 Active Directory Users and Computers							
G Eile <u>A</u> ction <u>V</u> iew <u>W</u> indow	v <u>H</u> elp						
← → 🗈 💽 🖀 😭 🖸) 🗈 😫 💷 🦉 👸	l 💩 💎 🍕 🙍					
Active Directory Users and Cor Saved Queries Saved Queries Sinca.ad Computers Domain Controllers L304A5 ForeignSecurityPrincips Cursuri H-20 Cursuri H-20 Cursuri H-20 Users	OU1 3 objects Name Image: Cursuri Image: Partajatu Image: Cursuri Image: Partajatu <th>Type Descriptio Organizational Unit Shared Folder User User Computer Contact Group InetOrgPerson MSMQ Queue Alias Organizational Unit Printer User Shared Folder Inatore Folder </th>	Type Descriptio Organizational Unit Shared Folder User User Computer Contact Group InetOrgPerson MSMQ Queue Alias Organizational Unit Printer User Shared Folder Inatore Folder 					

Imprimanta va fi apoi identificată prin specificatorul UNC, de tipul

\\servername\printername

Permisiuni la obiectele din Active Directory

Fiecare obiect din *Active Directory* are asociat un descriptor de securitate care definește cine are permisiunea de a accesa obiectul și ce tip de acces

ile Action View Window Help Add/Remove Columns Add/Remove Columns Iar Add/Remove Columns Saved Que Smaal Lons Jist Detail Detail Detail Detail Iar Adyanced Features Eiter Options Customize Customize Customize Window Enterprise Administ (SINCAVAccount Operators) Advinenticated Users Domain Administ (SINCAVAccount Operators) Authenticated Users Add Bernove emissions for Account Operators Allow Denvy Full Control Read Write Craned Add Bernove Bern		ory Use	rs and Co	omputers			
Properties Properties <td><u>File</u> <u>A</u>ction</td> <td><u>V</u>iew</td> <td><u>W</u>indow</td> <td>Help</td> <td></td> <td></td> <td></td>	<u>File</u> <u>A</u> ction	<u>V</u> iew	<u>W</u> indow	Help			
ctive Director Large Icons Saved Que Small Icons sinca.ad List Builtin Detail	→ 🗈 📧	<u>A</u> dd	/Remove (Iolumns			i 👸 🗸
Saved Que Small Icons List Detail Detail Domair Users, Groups, and Computers as containers Advanced Features Either Options Customize Custo	Active Director	Larg	įe Icons				
Sinca.ad List Detail Omain Visers, Groups, and Computers as containers Advanced Features Foreign Eiter Options Customize Add Bernove Customize Add Bernove Customize Add Bernove Customize Add Bernove Customize Customize Add Bernove Customize Add Bernove Customize Add Bernove Customize Add Bernove Customize Customize	📄 Saved Que	S <u>m</u> a	ll Icons				_
Properties Properties Image: Comparing the second sectings.	🗊 sinca.ad	List					ational Unit
	🗄 🖳 📴 Builtin	• <u>D</u> eta	ail				acional onic Folder
Wollindi Adyanced Features Image: State of the state of	E Compu	🗸 User	rs. Groups	. and Compu	iters as contain	ers	
Foreign Eilter Options Customize Add Customistrators		Adv	anced Fea	tures			
Properties Properties <td>E Foreigr</td> <td>Eilte</td> <td>r Options.</td> <td></td> <td></td> <td></td> <td></td>	E Foreigr	Eilte	r Options.				
Properties Properties neral Managed By Object Security COM+ Group Policy roup or user names: Account Operators Administrators (SINCA\Account Operators) Administrators (SINCA\Account Operators) Administrators (SINCA\Count Operators) Administrators (SINCA\Count Operators) Authenticated Users Domain Admins (SINCA\Count Operators) Add Bemove ermissions for Account Operators Add Bemove Full Control Read Write Create All Child Objects Delete All Child Objects Generate Resultant Set of Policy(Logging) or special permissions or for advanced settings, ick Advanced.	🖻 🙆 OU1	Cuel	tomize				
Properties ? × neral Managed By Object Security COM+ Group Policy roup or user names: * Account Operators (SINCA\Account Operators) * * Account Operators (SINCA\Account Operators) * * * * Account Operators (SINCA\Administrators) * * * * Addministrators (SINCA\Administrators) * * * * Addministrators (SINCA\Administrators) * * * * Pomain Adminis (SINCA\Domain Adminis) * * * * Puttopopulation Decisions for Account Operators Allow Deny * Full Control * * * * Read * * * * Write * * * * * Create All Child Objects * * * * * Delte All Child Objects * * * * * * Generate Resultant Set of Policy(Logging) * * * *	🕀 🙆 Cu						1
Properties		er1					
Properties ? × neral Managed By Object Security COM+ Group Policy roup or user names: Account Operators (SINCA\Account Operators) Administrators (SINCA\Administrators) Administrators (SINCA\Administrators) Authenticated Users Domain Admins (SINCA\Enterprise Admins) Enterprise Admins (SINCA\Enterprise Admins) Full Control Read Write Create All Child Objects Delete All Child Objects Delete All Child Objects Generate Resultant Set of Policy(Logging) or special permissions or for advanced settings, ick Advanced.	±… <u> </u> Users						
Properties ? × meral Managed By Object Security COM+ Group Policy roup or user names: Account Operators (SINCA\Account Operators) Administrators (SINCA\Administrators) Administrators (SINCA\Administrators) Administrators (SINCA\Administrators) Authenticated Users Domain Admins (SINCA\Domain Admins) Enterprise Admins (SINCA\Domain Admins) Image: Complex Control							
Properties ? × Ineral Managed By Object Security COM+ Group Policy Group or user names: Account Operators (SINCA\Account Operators) Administrators) Administrators (SINCA\Administrators) Administrators (SINCA\Administrators) Authenticated Users Domain Admins (SINCA\Enterprise Admins) Enterprise Admins (SINCA\Enterprise Admins) Image: Add Enterprise Admins (SINCA\Enterprise Admins) Image: Add Full Control Image: Adlow Deny Full Control Image: Adlow Deny Full Control Image: Adlow Deny Greate All Child Objects Image: Advanced Image: Advanced or special permissions or for advanced settings, lick Advanced. Advanced Image: Advanced							
Properties ? × meral Managed By Object Security COM+ Group Policy iroup or user names: Account Operators (SINCA\Account Operators) Administrators (SINCA\Administrators) Administrators (SINCA\Administrators) Administrators (SINCA\Administrators) Authenticated Users Administrators (SINCA\Count Operators) Image: Count Operators (SINCA\Count Operators) Authenticated Users Domain Admins (SINCA\Enterprise Admins) Image: Count Operators (SINCA\Enterprise Admins) Enterprise Admins (SINCA\Enterprise Admins) Image: Count Operators (SINCA\Enterprise Admins) Image: Count Operators (SINCA\Enterprise Admins) Full Control Image: Count Operators (SINCA\Enterprise Admins) Image: Count Operators (SINCA\Enterprise Admins) Full Control Image: Count Operators (SINCA\Enterprise Admins) Image: Count Operators (SINCA\Enterprise Admins) Full Control Image: Count Operators (SINCA\Enterprise Admins) Image: Count Operators (SINCA\Enterprise Admins) Full Control Image: Count Operators (SINCA\Enterprise Admins) Image: Count Operators (SINCA\Enterprise Admins) Full Control Image: Count Operators (SINCA\Enterprise Admins) Image: Count Operators (SINCA\Enterprise Admins) Generate All Child Objects Image: Count Operators (SINCA\Enterprise Admins) <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>							
Ineral Managed By Object Security CDM+ Group Policy inoup or user names: Account Operators (SINCA\Account Operators) Administrators (SINCA\Administrators) Administrators (SINCA\Administrators) Authenticated Users Domain Admins (SINCA\Domain Admins) Enterprise Admins (SINCA\Enterprise Admins) Enterprise Admins (SINCA\Enterprise Admins) Full Control Read Write Create All Child Objects Delete All Child Objects Delete All Child Objects Generate Resultant Set of Policy(Logging) or special permissions or for advanced settings, ick Advanced.							•
Account Operators (SINCA\Account Operators) Administrators (SINCA\Administrators) Administrators (SINCA\Administrators) Authenticated Users Domain Admins (SINCA\Domain Admins) Enterprise Admins (SINCA\Enterprise Admins) Enterprise Admins (SINCA\Enterprise Admins) Full control Read Write Create All Child Objects Delete All Child Objects Generate Resultant Set of Policy(Logging) or special permissions or for advanced settings, lick Advanced.	1 Properties						2
	1 Properties ieneral Mana	aged By	Object	Security	COM+ Grou	ıp Policy	<u>י</u>
Authenticated Users Domain Admins (SINCA\Domain Admins) Enterprise Admins (SINCA\Enterprise Admins) Enterprise Admins (SINCA\Enterprise Admins) Enterprise	1 Properties ieneral Mana Group or user	nged By) Object	Security	COM+ Grou	ıp Policy	2
	1 Properties ieneral Mana Group or user	aged By names: Operato ators (S	Dbject	Security	COM+ Grou	ıp Policy	? , ,
Add Remove Add Remove ermissions for Account Operators Allow Deny Full Control Image: Control Contrel Contrecontrol Control Contrecontrol Control Contre	1 Properties General Mana Group or user Account Administr Administr	aged By names: Operato cators (S cated U	Dbject	Security \\Account (ninistrators)	COM+ Grou Operators)	p Policy	? ,
Aga emiove remissions for Account Operators Allow Deny Full Control	1 Properties aeneral Mana Group or user Account Administr Administr Authentic Domain A Enterpris	aged By names: Operato ators (S cated U Admins e Admins	Dbject	Security	COM+ Grou	p Policy	?
Full Control Image: Control Control Read Fead Image: Control Control Control Read Write Image: Control Contrecontrol Control Control Control Control Control Control C	1 Properties General Mana Group or user Account Administr Authentic Domain A Enterpris	aged By names: Operato ators (S cated U Admins (Admins (Admins (Dbject Drs (SINCA INCA\Adr sers (SINCA\D IS (SINCA)	Security MAccount (ministrators) omain Admi Enterprise	COM+ Grou Operators) ns) Admins)	ip Policy	
Read Image: Constraint of Policy (Logging) Image: Constraint of Policy (Logging) Or special permissions or for advanced settings, lick Advanced. Advanced	1 Properties aeneral Mana Group or user Account Administr Administr Authentic Domain A Enterpris	aged By names: Operato ators (S cated U Admins (e Admins (Object INCA\Adr sers (SINCA\D is (SINCA\D	Security	COM+ Grou Operators) ns) Admins) - ac Add		?
Write Create All Child Objects Delete All Child Objects Generate Resultant Set of Policy(Logging) or special permissions or for advanced settings, Lick Advanced.	1 Properties General Mana Group or user Account Administr Authentio Domain A Enterpris Enterpris Permissions fo Full Control	aged By names: Operators ators (S cated U Admins (e Admins (e Admins (r Accou	Dis (SINCA INCA\Adr sers (SINCA\D is (SINCA\D is (SINCA)	Security MAccount (ministrators) omain Admi Enterprise	COM+ Grou Operators) ns) Admins) -oc Add Allow	p Policy	? , emove eny
Delete All Child Objects Generate Resultant Set of Policy(Logging) or special permissions or for advanced settings, Ick Advanced OK Cancel Apply	1 Properties General Mana Group or user Account Administr Authentic Domain A Enterpris Enterpris Permissions fo Full Control Read	names: Operato ators (S cated U Admins (e Admins (r Accou	Dbject Drs (SINCA INCA\Adr sers (SINCA\D IS (SINCA\D IS (SINCA\D IS (SINCA\D IS (SINCA\D) IS (SINCA\D)	Security Ninistrators) omain Admi Enterprise ors	COM+ Grou Dperators) ns) Admins) -Dc Add Allow		emove
or special permissions or for advanced settings, Advanced	1 Properties General Mana Group or user Account Administr Authentic Domain A Enterpris Enterpris Permissions fo Full Control Read Write Create All C	aged By names: Operators (S cated U Admins (e Admins (e Admins (r Accou	Dbject Drs (SINCA INCA\Adr sers (SINCA\D is (SINCA) is (SINCA) is (SINCA)	Security	COM+ Grou Operators) ns) Admins) -oc Add Allow		eny
lick Advanced.	1 Properties General Mana Group or user Account Administr Authentic Domain A Enterpris Permissions fo Full Control Read Write Create All C Delete All C Delete All C	aged By names: operato ators (S cated U Admins I e Admins I e Admins I r Accou	Object INCA\Adr sers (SINCA\D is (SINCA\D is (SINCA\D is (SINCA\D is (SINCA\D is (SINCA\D) is (SINCA\D) is (SINCA\D)	Security Ninistrators) omain Admi Enterprise	COM+ Grou		emove
	1 Properties General Mana Group or user Account Administr Authentic Domain A Enterpris Enterpris Permissions fo Full Control Read Write Create All C Delete All C Generate R	aged By names: Operato ators (S cated U Admins (e Admins (e Admins (r Accou r Accou child Obj child Obj esultant	Dbject INCA\Adr sers (SINCA\D is (SINCA\D is (SINCA\D)) (SINCA\D is (SINCA\D)) (SINCA\D is (SINCA\D)) (SINCA\D) (SIN	Security	COM+ Grou		
	Properties ieneral Mana Group or user Account Administr Authentic Domain A Enterpris Enterp	aged By names: Operato ators (S cated U Admins I e Admins I e Admin r Accou r Accou shild Obj child Obj esultant mission rd.	Object INCA\Adr sers (SINCA\D is (SINCA\D is (SINCA\D)) is (SINCA\D is (SINCA\D)) is (SINCA\D is (SINCA\D)) is (SINCA\D) is (SINCA\D) i	Security NAccount (ministrators) omain Admi VEnterprise ors ors ors	COM+ Grou		emove eny

te permis. La fel са ntru foldere, fişiere sau primante. lista rmisiunilor este definită n Discretionary Access ontrol Lists (DACLs). Lista CL nu este afişată prin tive DirectoryUsers and decât mputers dacă bdul de vizualizare eniul View) este lvanced Features aracteristici avansate).

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

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

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

Permisiunile standard sunt următoarele:

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

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

Reguli:

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

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

Duran a Mara	
Properties	
meral Managed By Object Security COM+ Group Policy	
iroup or user names:	Advanced Security Settings for OU1
ENTERPRISE DOMAIN CONTROLLERS	Permissions Auditing Owner Effective Permissions
Pre-Windows 2000 Compatible Access (SINCA\Pre-Windows 2 Print Operators (SINCA\Print Operators) SYSTEM	To view more information about special permissions, select a permission entry, and then click Permission entries:
🖸 user1 (user1@sinca.ad)	Tupe Name Permission Inherited From Applu To
Add Bemove termissions for user1 Allow Deny Full Control Image: Control Contrecontro Contrel Control Control Control Control Contrec	Dery user1 (user1@sinca Write (not inherited) This object and the sobject on the sobject o
OK Cancel App	To replace all permission entries with the default settings, click Default.

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

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

Cursuri Properties General Managed By Object Security Group or user names: ENTERPRISE DOMAIN CONTROL Pre-Windows 2000 Compatible Acce Print Operators (SINCA\Print Operators) SYSTEM User1 (user1@sinca.ad)	CDM+ Group F LERS sss (SINCA\Pre-Wi ors)	? 'olicy ndows 2	Advanced Security Settings for Cursuri Permissions Auditing Owner Effective Permissions The following list displays the permissions that would be granted to the selected group or user, based sole on the permissions granted directly through group membership.	?] :
Permissions for user1 Full Control Read Write Create All Child Objects Delete All Child Objects Generate Resultant Set of Policy(Loggi For special permissions or for advanced sec click Advanced. OK	Agd	<u>H</u> emove Deny □ ▲ □ ↓ Advanced	Group or user name: user1 Effective permissions: Full Control List Contents Read All Properties Write All Properties Delete Delete Subtree Read Permissions Modify Demissions Modify Demissions All Validated Writes All Extended Rights Learn more about how effective permissions are determined.	

Moştenirea permisiunilor

Există două tipuri de permisiuni: explicite și moștenite. Permisiunile explicite sunt asignate direct la obiect, iar permisiunile moștenite sunt propagate de la obiectul părinte. În mod implicit, orice obiect moștenește permisiunile de la

ursuri Properties	71
General Managed By Object Security C	OM+ Group Policy
<u>G</u> roup or user names:	
🗾 🕵 ENTERPRISE DOMAIN CONTROLLER	RS 🔺
🖉 🕵 Pre-Windows 2000 Compatible Access ((SINCA\Pre-Windows 2
Print Operators (SINCA\Print Operators)	
SYSTEM	
🚺 🙍 user1 (user1@sinca.ad)	-
	Add <u>R</u> emove
Permissions for user1	Allow Deny
Full Control	
Read	
Write	
Create All Child Objects	
Delete All Child Objects	
Generate Resultant Set of Policy(Logging)	
For special permissions or for advanced settin click Advanced.	igs, Ad <u>v</u> anced

containerul din care face parte, adică de la containerul părinte.

Permisiunile moștenite nu pot fi modificate. Dacă se dorește ca un obiect să aibă alte permisiuni față de cele moștenite, trebuie mai întâi dezactivată moștenirea.

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

Properties	<u>? ×</u>			
neral Managed By Object Security COM+	Group Policy			
Cursuri Properties	? ×			
General Managed By Object Security C	DM+ Group Policy			
Group or user names:	dvanced Security Settings for Cursuri			? ×
ENTERPRISE DOMAIN CONTROLL Pre-Windows 2000 Compatible Acces	Permissions Auditing Owner Effective	Permissions		1
Print Operators (SINCA\Print Operator SYSTEM	To view more information about special pe	rmissions, select a p	permission entry, and then click	Edit.
😰 user1 (user1@sinca.ad)	Permission entries:			
J <u>P</u> ermissions for user1	Type Name Allow Pre-Windows 2000 Compa Allow Pre-Windows 2000 Compa Allow Pre-Windows 2000 Compa Allow Pre-Windows 2000 Compa	Permission Special Special Special	Inherited From DC=sinca,DC=ad DC=sinca,DC=ad DC=sinca,DC=ad	Apply Tr User ob InetOrgf Group o
Full Control	Allow Print Operators (SINCANPri Allow SYSTEM	Ereate/Delete Full Control	<not inherited=""></not>	This obj
Read	Allow user1 (user1@sinca.ad)	Read	<not inherited=""></not>	This obj
Write	Deny user1 (user1@sinca.ad)	Write	OU=OU1,DC=sinca,DC=ad	This obj
Create All Child Objects	<u> </u>			
Delete All Child Objects Generate Resultant Set of Policy(Loggin	<u>Add</u> <u>E</u> dit	<u>R</u> emove		
 For special permissions or for advanced set click Advanced 	Allow inheritable permissions from the permission these with entries explicitly defined here	parent to propagate e.	to this object and all child objec	cts. Include

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

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

Advanced Secur <u>ity Settings for Cursuri</u>
Security
To view more ii 2 Selecting this option means that the parent permission entries that apply to child objects will no longer be applied to this object.
Permission/entr -To copy the permission entries that were previously applied from the parent to this object, click Copy. Type Na Allow Pre Allow Pri Prior Prove Cancel Prior
Deny userI (userI @sinca.ad) Write UU=UUT,DL=sinca,DL=ad This obj ↓
Add Edit <u>R</u> emove Allow inheritable permissions from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here.

Vor apărea trei variante de lucru:

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

Advanced Security Settings for	' Cursuri			? ×	Intestitut (
Permissions Auditing Quinor	Effective Permission				
r childesiene [Additing] owner [i	Effective Femilission	-1	Permission Entry for	r Cursuri	
To view more information about s	special permissions,	select a permission			
			Object Properties		
Permission en <u>t</u> ries:					
Name	Permission	Inherited From	<u>N</u> ame: user1 (use	er1@sinca.ad)	<u>C</u> hange
Pre-Windows 2000 Compa	Special	DC=sinca,DC=ad			
Pre-Windows 2000 Compa	Special	DC=sinca,DC=ad	Apply <u>o</u> nto: This o	bject only	
Pre-Windows 2000 Compa	Special	DC=sinca.DC=ad	Den This o	bject only	
Print Uperators (SINLA\Pri	Eull Control	<not inherited=""></not>	Eennissions. This o	bject and all child objects	
user1 (user1@sinca ad)	Bead	<not inherited=""></not>	Full Contre accou	objects only int objects	
user1 (user1@sinca.ad)	Write	OU=OU1,DC=sinc	List Conte aCSR	esourceLimits objects	
	/		Read All Fapplic	ationVersion objects	
			Write All F Comp	cationAuthority objects	
A <u>d</u> d <u>E</u> dft.	<u>R</u> em	iove	Delete Conne	ection objects	
			Delete Su Conta	ct objects	
Allow inheritable permissions	from the parent to p	ropagate to this obj	Bead Peri docun	nent objects	
these with entries explicitly de	ennea nere.		Modifu Re domai	nentsenes objects nBelatedObject objects	
			Modily Federical	hicObject objects	
			moairy ov friendl	yCountry objects	
To replace all permission entries	with the default sett	ings, click Default.	All Validat Group	i objects Dil Inigual I amas abiasta	
			All Extend group	PolicyContainer objects	
Learn more about access control	ļ.		Create All InetOr	gPerson objects	
			Intellik untellik	firror Group objects	
			Apply the Intellin	Airror Service objects	
			containe msCO	M-PartitionSet objects	
			msDS	App-Configuration objects	
			msDS	-AppData objects	
			msDS msDS	-AzAdminmanager objects AzApplication objects	
			msDS	AzOperation objects	
			msDS	AzBole objects	

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

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

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

Auditing Owner	Effective Permission	ns	Permission Entry for Cursuri		2	x
view more information about	special permissions,	select a permission	Object Properties			
mission en <u>t</u> ries:						
ame	Permission	Inherited From	<u>N</u> ame: user1 (user1@sinca.ad)		<u>C</u> hange	
re-Windows 2000 Compa	Special Special	DC=sinca,DC=ad	Apply opto: This object and all child o	biects		
re-Windows 2000 Compa	Special	DC=sinca,DC=ad		blooks		
rint Operators (SINCA\Pri	Create/Delete	<not inherited=""></not>	Permissions:	Allow	Deny	
YSTEM	Full Control	<not inherited=""></not>	Full Control			
seri (useri@sinca.ad) seri (useri@sinca.ad)	Head Write	<pre><not inherited=""> OU=OU1 DC=sind</not></pre>	List Contents			
serr (userre-sinea.aa)	WING	00-001,50-311	Read All Properties			
			Write All Properties			
A <u>d</u> d <u>E</u> dit	t <u>R</u> en	nove	Delete			
All	()		Delete Subtree			
Allow inheritable permissions these with entries explicitly d	: from the parent to p lefined here.	propagate to this obj	Read Permissions			
			Modify Permissions			
			Modify Owner			
and an all a surfactory of the	with the defendence	in an allah Data k	All Validated Writes			
replace all permission entries	with the default sett	ings, click Default.	All Extended Rights			
arn more about access control.		Create All Child Objects				
	_		Dalata All Child Objects	_		
			Apply these permissions to objects	and/or	Clear All	
		OK	containers within this container only			

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

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

Regulile aplicate obiectelor mutate sunt următoarele:

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

Delegarea controlului administrativ



Structurarea ierarhică a domeniului se construieste prin unitătile organizationale. Ele sunt containere care conțin obiecte. Administratorul domeniului poate delega către un alt utilizator competente administrative unităti asupra unei organizationale evident. Şİ asupra obiectelor din unitatea organizatională. Utilizatorul primește astfel capacitatea de a gestiona, de a controla obiectele aflate în acea unitate organizatională.

Delegarea controlului administrativ se referă la atribuirea responsabilităților legate

de gestionarea unor obiecte dintr-o unitate de organizare. Unele dintre sarcinile administrative vor fi preluate astfel de un utilizator sau, eventual, de un grup de utilizatori.

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

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

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

Delegation of Control Wizard	Delegation of Control Wizard
Users or Groups Select one or more users or groups to whom you want to delegate control.	Tasks to Delegate You can select common tasks or customize your own.
Selected users and groups: gelected users and groups: gelected users and gelected us	Delegate the following common tasks: Create, delete, and manage user accounts Reset user passwords and force password change at next logon Read all user information Create, delete and manage groups Modify the membership of a group Manage Group Policy links Generate Resultant Set of Policy (Planning) Generate Resultant Set of Policy (Logging) Create a custom task to delegate
< <u>B</u> ack Next> Cancel	<u> < ₿</u> ack <u>N</u> ext > Cancel

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

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

anced S	security Settings for OU	1	<u>?</u> ×		
ermission: Fo view r Permissio	Auditing Owner Effect more information about speci n entries:	stive Permissions al permissions, select a perm	Permission Entry for OU1 is Object Properties		?
Туре	Name	Permission	<u>N</u> ame: <u>Useri (useri @sinca.ad)</u>		nange
Allow Allow Allow	user1 (user1@sinca.ad) user1 (user1@sinca.ad) Authenticated Users	Read/Write Property Reset Password Special	Apply onto: User objects Permissions:	Allow	💌 Denv
Allow Allow Allow Allow Allow Allow Allow Allow these	Account Operators (SINC SYSTEM Account Operators (SI Id <u>Edit</u> inheritable permissions from with entries explicitly defined the all permission entries with re about <u>access control</u> .	the default settings, click De	Write Post Office Box Read postalAddress Write postalAddress Read preferredLanguage Write preferredLanguage Read profilePath Write profilePath Read pwdLastSet Write pwdLastSet Head roomNumber Write roomNumber Read scriptPath Write roomNumber Read scriptPath Write roomNumber Read scriptPath Write roomNumber Read scriptPath		
				ок	Cancel

Politica de grup

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

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

Politicile de grup pot configura printre altele:

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

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

• Opțiuni de redirectare a folderelor

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

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

Politica de grup conține următoarele două ramuri majore:



Computer Configuration

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

User Configuration

Administratorii pot utiliza *User Configuration* pentru configurarea

politicilor care se aplică utilizatorilor, indiferent de computerul pe care aceștia îl folosesc. *User Configuration* conție subelemente pentru set ări *software*, setări *Windows* și șabloane administrative.

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

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

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

Run	<u>? ×</u>
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	mmc
	OK Cancel <u>B</u> rowse

1.*Group Policy* pentru calculatorul local

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

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

•	<u> </u>		
🚡 Console 1	Add/Remove Snap-in		?× _ □ ×
<u>File A</u> ction <u>V</u> iew	Standalone Extensions		
	the this search and a Sec		
		Add Standalone Snap-in	? ×
Console Root	Snap-ins added to: 🚗	Available standalone snap-ins:	
		Snap-in	Vendor 🔺
		Component Services	Microsoft Corporation
		📃 Computer Management	Microsoft Corporation
		Bovice Manager	Microsoft Corporation
		🛛 👺 Disk Defragmenter	Microsoft Corp, Execut
		👹 Disk Management	Microsoft and VERITAS —
		🔒 🕹 Distributed File System	Microsoft Corporation
		, 🚉 DNS	Microsoft Corporation
		🔃 🔃 Event Viewer	Microsoft Corporation
·		Folder	Microsoft Corporation
		Group Policy Object Editor	Microsoft Corporation 📃 🚽
	Description		_
		Description This snap-in allows you to edit Group Po to a Site, Domain, or Organizational Unit stored on a computer.	licy Objects which can be linked t in the Active Directory or
	A <u>d</u> d <u>R</u> em		/

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

Vizard	
	rowse for a Group Policy Object
	Domains/OUs Sites Computers All
Group Relieu Obieste een he stered in Ves Asting Directory	Look in: Sinca.ad
or on a local computer.	Domains, OUs and linked Group Policy Obje
Use the Browse button to select a Group Policy Object.	Name
	OU1.sinca.ad
	📑 Default Domain Policy
Group Policy Object:	
Local Computer	
<u>B</u> rowse	
Allow the focus of the Group Policy Snap-in to be changed when launching from the command line. This	

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

2. Obiectele Group Policy din Active Directory

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

Containerul Group Policy Object (GPO) este obiect în Active un Directory. Atributele acestui obiect includ numele GPO, permisiuni, respectiv modifica cine poate conținutul obiectului GPO și informații de versiune.



 Macheta GPO (*template*), este un set de fişiere care se găsesc în folderul partajat Sysvol. Folderul partajat Sysvol există pe fiecare controler de domeniu, conținutul său fiind replicat între toate controlerele de domeniu din domeniu, prin intermediul serviciului *File Replication Service* (FRS).

Un obiect GPO conține informații de configurare pentru calculator și pentru utilizator.

Active Directory Us	ers and Computers			
ile <u>A</u> ction <u>V</u> iew	Window <u>H</u> elp		_	_₽×
🖕 🔿 🚡 Group Poli	cy Object Editor			
Activ Eile Action	⊻iew <u>H</u> elp			
	🖬 🖹 🔮 🖬			
🗎 🖻 💱 🗍 😴 Goot [304'	4b3 sinca.ad] Policy	Satting	State	
Compu	Iter Configuration	Permove user's folders from the Start Menu	Not configured	
Sof	ftware Settings	Demove links and access to Windows Undate	Not configured	1/
📗 🚆 🗓 💼 Wir	ndows Settings	Remove common program groups from Start Menu	Not configured	1/
📕 🕌 📶 🖻 🖮 🧰 Adr	ministrative Templates 📗	Persove My Doruments icon from Start Menu	Not configured	1/
	Windows Components	Remove Documents menu from Start Menu	Not configured	
▋ 글…】 ● … 🚞	System	Perove programs on Settings menu	Not configured	
	/ Network	Remove Network Connections from Start Menu	Not configured	
	Printers	Remove Favorites menu from Start Menu	Not configured	
	onfiguration	Remove Search menu from Start Menu	Not configured	
	tware Settings	Remove Heln menu from Start Menu	Not configured	
	ndows Settings	Remove Run menu from Start Menu	Not configured	
	Ministrative Templates	Remove My Pictures icon from Start Menu	Not configured	
	Start Menu and Taskh	Remove My Music icon from Start Menu	Not configured	
	l Deskton	Remove My Network Places icon from Start Menu	Not configured	
	Control Panel	Add I nooff to the Start Menu	Not configured	
	I Shared Folders	Remove Logoff on the Start Menu	Not configured	
📕 🕴 📩 👘 🧰	Network	Remove and prevent access to the Shut Down command	Not configured	
📕 🛉 👘 🧰	System	Remove Drag-and-drop context menus on the Start Menu	Not configured	
		Prevent changes to Taskbar and Start Menu Settings	Not configured	
		Remove ascess to the context menus for the taskbar	Not configured	
		Do not keep history of recently opened documents	Not configured	
		Gear history of recently opened documents on exit	Not configured	
		Turn off personalized menus	Not configured	
		Turn off user tracking	Not configured	
		Add "Run in Separate Memory Space" check box to Run dialog box	Not configured	
		Do not use the search-based method when resolving shell shortsute	Not configured	<u> </u>
		Extended λ Standard /		

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

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

Obiectele GPO sunt evaluate în ordinea următoare:

Local Policy \rightarrow Site GPO \rightarrow Domain GPO \rightarrow OU GPO \rightarrow Child OU GPO etc.

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

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

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

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

OU1 Properties		<u>? ×</u>					
General Managed By Object Security COM	+ Group Poli	cy					
To improve Group Policy management, upgrade to the Group Policy Management Console (GPMC).							
Group Policy Object Links No Override Disabled							
Group Policy Objects higher in the list have the h This list obtained from: I304a5.sinca.ad	ighest priority.						
New Add Edit Options Delete Properties		<u>∐p</u> Do <u>w</u> n					
□ <u>B</u> lock Policy inheritance							
ОК	Cancel	Apply					

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

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

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

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

Internet Explorer Outlook Express Remote Assistance Active Directory Domains and Tru Active Directory Sites and Service Active Directory Users and Comp All Programs Administrative Tools Log Off Domain Controller Security Policy Start Start Start Outlook Express Coup Policy Management	În urma instalării, se creează o intrare în <i>Administrative Tools</i> numită <i>Group Policy</i> <i>Management.</i>
Image: File Action View Window Help Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File Image: File<	Group Policy Objects in sinca.ad
Domains Sinca.ad Default Domain Policy Domain Controllers OU1 Group Policy Objects Default Domain Controllers Policy Default Domain Policy Default Domain Policy WMI Filters Sites Group Policy Modeling Group Policy Results	Contents Delegation Name GPO Status Default Domain Controllers Policy Enabled Default Domain Policy Enabled

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

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

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

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







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



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



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



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

🚡 Group Policy Object Editor		
<u>File Action View H</u> elp	<u> </u>	
← → 🗈 💽 🖆 🗟 🔮 🖸		
🗊 Gpo1 [l304a5.sinca.ad] Policy 🗠	Setting	State
🗟 🛃 Computer Configuration	Active Desktop	
E Software Settings	Active Directory	
Windows Settings	🔞 Hide and disable all items on the desktop	Enabled
Administrative Templates	🙀 Remove My Documents icon on the desktop	Enabled
English Configuration	👔 Remove My Computer icon on the desktop	Enabled
Software bettings	🙀 Remove Recycle Bin icon from desktop	Enabled
Windows Settings	😭 Remove Properties from the My Documents context menu	Not configured
Administrative Templates	🙀 Remove Properties from the My Computer context menu	Not configured
	🙀 Remove Properties from the Recycle Bin context menu	Not configured
Start Menu and Taskba	🙀 Hide My Network Places icon on desktop	Enabled
🗗 🔄 Desktop	Hide Internet Explorer icon on desktop	Disabled
E Control Panel	😰 Do not add shares of recently opened documents to My Network Plac	<mark>ces</mark> lot configured
Shared Folders	💱 Prohibit user from changing My Documents path	Not configured
🗄 📲 Network	💱 Prevent adding, dragging, dropping and closing the Taskbar's too	Not configured
🗄 📲 System	😰 Prohibit adjusting desktop toolbars	Not configured
	😰 Don't save settings at exit	Not configured
	😤 Remove the Desktop Cleanup Wizard	Not configured

Să examinăm fereastra de mai sus. Numele ferestrei este *Group Policy Object Editor,* ceea ce înseamnă că în această fereastră se pot stabili configurările pentru componentele *computer configuration* și *user configuration.* Obiectul GPO supus examinării se numește *Gpo1* și ceea ce examinăm acum este conținutul obiectului așa cum se găsește în exemplarul de la controlerul de domeniu *I304a5.sinca.ad,* numele domeniului fiind *sinca.ad.* Componenta *User configuration* este cea în care por fi stabilite condițiile deosebite ale mediului de operare al utilizatorilor. Pentru moment se face referire la ecranul *desktop.* Conform acestora, utilizatorul căruia i se va aplica politica *Gpo1* va avea – după deschiderea de sesiune – o imagine *desktop* pe care nu mai apare nicio pictogramă.

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



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

Utilitarul GPMC conține și o

componentă prin care pot fi vizualizate configurările (setările) existente întrun obiect GPO. *Tab*-ul folosit este *Settings* după ce a fost ales obiectul pentru care se dorește vizualizarea conținutului.

🗈 📧 🔗 😫 💵							
p Policy Management	Defau	ult Dome	ain Poli	су			
orest: sinca.ad	Scope Details Settings Delegation						
gi Domains				1 3 1			
Default Domain Polic	Default Domain Policy						
	Dat	Data collected on: 2/15/2010 2:30:24 PM					
	Cor	nputer Co	onfigurati	on (Enabled)		<u>hide</u>	
Gpo1	v	/indows 9	ettings			<u>hide</u>	
ि जि़्ही Gpo2 स-@ि Cursuri		Security	Settings			<u>hide</u>	
E G Testx		Accou	Account Policies/Password Policy			<u>hide</u>	
🕞 🔂 Gpo3		Po	olicy		Setting		
		Er	force pass	word history	24 passwords remembered		
		Ma	aximum pa:	ssword age	42 days		
- Gpo1		Mi	nimum pas	sword age	1 days		
Gpo2		Mi	nimum pas	sword length	7 characters		
Gpo3		Pa rec	issword mu quirements	ist meet complexity	Enabled		
j Sites		Sti	ore passwo	ords using reversible	Disabled		
Group Policy Modeling		en	cryption				
Group Policy Results		Accou	nt Policie	s/Account Lockout	Policy	<u>hide</u>	
		Po	olicy		Setting		
		Ac	count lock	out threshold	0 invalid logon attempts		
		Accou	nt Policie	es/Kerberos Policy		<u>hide</u>	
		Po	olicy		Setting		

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

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



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

roup Policy Modeling V	Yizard	
User and Computer You can view simu information) and co	Selection lated policy settings for a selected user (or a container wi mputer (or a container with computer information).	th user
Example container na Example user or com	ame: CN=Users,DC=sinca,DC=ad puter: SINCA\administrator	
Simulate policy settings	for the following:	
User information		
Container:	OU=Testx,OU=OU1,DC=sinca,DC=ad	B <u>r</u> owse
O <u>U</u> ser:		Br <u>o</u> wse
Computer information		
 Container: 	OU=Domain Controllers,DC=sinca,DC=ad	Bro <u>w</u> se
C Computer:		Brows <u>e</u>
Skip to the final pag	e of this wizard without collecting additional data	
	< Back (<u>Next</u> >	Cancel

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

Croup Policy Management					
5월 Eile Action <u>V</u> iew <u>W</u> indow <u>H</u> e	lp				_ 뭔 🏼
Group Policy Management		Domain Controlloro			
A Forest: sinca.ad	rest on L				
Domains	Summary 5	ettings Query			1
🖻 🖓 sinca.ad		Grou	p Policy Mode	eling	
Derault Domain Policy	sinca a	d/0111/Testy on sin	ca ad/Domair	n Controllers	
	Data colle	cted on: 2/16/2010 11:21:3	2 AM	Conditioners	hide all
- \iint Gpo1	Compute	r Configuration			show
Gpo2		figuration			bide
	User con	Lide			
Gpo3	Adminis	nide			
🗈 🕎 Group Policy Objects	Sta	art Menu and Taskbar			hide
🕀 🖅 WMI Filters		Policy	Setting	Winning GPO	
Group Policy Modeling		Remove Run menu from	Enabled	Gpo3	
Testx on Domain Controllers		Start Menu			
Group Policy Results					
					-
J				1	



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

sisteme de operare Windows XP sau Windows Server 2003.

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

Scoup Policy Managemer	ıt 💦		
පිළි <u>Fi</u> le <u>A</u> ction <u>V</u> iew <u>W</u> in	dow <u>H</u> elp		_8×
← → 🗈 📧 🙆 😫			
Group Policy Management Forest: sinca.ad Grow Domains Grow Sinca.ad Grow Domain Controll Grow Domain Controll Grow OU1	Gpo3 Scope Details Settings Delegation These groups and users have the spec Groups and users: Name A	ified permission for this GPO Allowed Permissions	Inherited
Gool Good Cursuri Good Fostx Group Policy Ob WMI Filters Group Policy Modeling Testx on Domain Cc Group Policy Results	Autmenticated Users Domain Admins (SINCA\Domain Enterprise Admins (SINCA\Enter ENTERPRISE DOMAIN CONT SYSTEM	Read (from Security Fintering) Edit settings, delete, modify security Edit settings, delete, modify security Read Edit settings, delete, modify security	No No No
	Add <u>R</u> emov	e <u>P</u> roperties	Advanced

În mod implicit, toate setările din obiectele GPO legate la un container se aplică tuturor utilizatorilor şi computerelor din container. acel Dacă intentia administratorului de domeniu este са politicile să se aplice numai anumitor utilizatori sau anumitor calculatoare, atunci vor intra în operă

procedurile de filtrare, prin care vor fi selectate numai acele calculatoare şi, respectiv, acei utilizatori cărora trebuie să li se aplice politica. Filtrele sunt construite folosind *tab*-ul *Delegation* pentru fiecare obiect GPO în parte.

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

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



Replicarea Active Directory

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

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

Partițiile Active Directory sunt:

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

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

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



Replicarea Active Directory poate avea loc, de la caz la caz, între controlere de domeniu care aparțin aceluiași site – situație în care vorbim despre replicarea în interiorul site-ului (intrasite) – sau între controlere care aparțin de site-uri diferite – situație în care are loc replicare între site-uri (intersite). Replicarea în interiorul aceluiași *site* pornește de la presupunerea că legăturile dintre controlere sunt sigure, de viteză mare și permanent disponibile. Traficul de replicare nu este comprimat și se realizează prin *"change notification*", partenerii de replicare fiind anunțați imediat sau aproape imediat de producerea replicării.

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

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

Instalarea unui controler de domeniu suplimentar

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

omai Sp	n Controller Type ecify the role you want this server to have.
Do ad	you want this server to become a domain controller for a new domain or an ditional domain controller for an existing domain?
С	Domain controller for a new domain
	Select this option to create a new child domain, new domain tree, or new forest. This server will become the first domain controller in the new domain.
œ	Additional domain controller for an existing domain
	A Proceeding with this option will delete all local accounts on this server.
	 All cryptographic keys will be deleted and should be exported before continuing.
	All encrypted data, such as EFS-encrypted files or e-mail, should be decrypted before continuing or it will be permanently inaccessible.
	Canad

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

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

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

ctive Directory Insta	llation Wizard
Network Credentia Provide a networ	Is k user name and password.
Type the user na to install Active D	me, password, and user domain of an account with sufficient privileges irectory on this computer.
<u>U</u> ser name:	administrator
Password:	••
<u>D</u> omain:	sinca.ad
	< <u>B</u> ack <u>N</u> ext > Cancel

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

👷 Active Di	rectory Sites and Service	es				
📓 Eile 🛛 Ad	tion <u>V</u> iew <u>W</u> indow <u>H</u> e	łp				
⇔ ⇒ €	J 📧 🗙 😭 🖻 🗟					
Active Di	rectory Sites and Services [l:	NTDS Settings 1 objects				
Eries	efault-First-Site-Name	Name	From Server	From Site	Туре	Desc
	Servers	🖳 <automatically generat<="" th=""><th>L304B3</th><th>Default-First-Sit</th><th>Connection</th><th></th></automatically>	L304B3	Default-First-Sit	Connection	
	- E L304A5					
	WIDS Settings					
6						
÷ 🦲 I	nter-Site Transports					
÷ 🧰 S	ubnets					

În fereastra de mai sus remarcăm:

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

Conexiunile pot fi însă construite și manual.





Serverul Catalog Global

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

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

Find Users, Contacts, and Groups File Edit View Help Find: Users, Contacts, and Groups In: In: Entire Directory Users, Contacts, and Groups Advanced Sinca Name: Description: In: In:	Browse Find Now Stop Qlear All	Image: Site services Image: Site services <td< th=""></td<>
		depending on your replication topology.

Salvarea și restaurarea Active Directory

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

-			
Address 🛅 C:\WINDOWS\NTDS			
Name 🔺	Size	Туре	Date
Drop		File Folder	2/5/2
👏 edb.chk	8 KB	Recovered File Fragments	2/18/
🗒 edb.log	10,240 KB	Text Document	2/18/
國 ntds.dit	10,256 KB	DIT File	2/18/
🗒 res1.log	10,240 KB	Text Document	2/5/2
🗒 res2.log	10,240 KB	Text Document	2/ 5/2
🖬 temp.edb	2,064 KB	EDB File	2/18/

 Ntds.dit - baza de date care stochează toate obiectele Active Directory.. Extensia .dit înseamnă "directory information tree".

 Edb.log - fişierul jurnal de tranzacţii (transaction log) folosit de această bază de date.
 Dimensiunea maximă a acestui fişier este de 10M.

• *Edb*.log* – când fișierul Edb.log atinge dimensiunea maximă, el va fi redenumit **Edbnnnnn.log**, unde nnnnn este un număr care va fi succesiv incrementat.

 Edb.chk – fişierul de tip checkpoint, folosit pentru a identifica până unde au fost efectuate tranzacțiile în baza de date.

 Res1.log, Res2.log – fişiere rezervate pentru transaction log; fiecare are câte 10M; spațiul ocupat de ele va fi alocat fişierului transaction log în cazul în care nu mai există spațiu pe disc.

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

Componentele System State pentru controlerele de domeniu sunt următoarele:

- Active Directory
- folder-ul partajat SYSVOL

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

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

Alegem pentru salvare System State și locația unde va fi salvat fișierul.



Pentru restaurarea bazei de date *Active Directory* în urma unei salvări (*backup*) controlerul de domeniu trebuie pornit în modul *Active Directory Restore Mode* (mod restaurare *Active Directory*). Acest mod de lucru se obține prin apăsarea tastei F8 la startarea serverului și alegând din meniu intrarea cu același nume.



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

Backup or Restore Wizard		×
What to Restore You can restore any combination o	of drives, folders, or files.	
Double click an item on the left check box next to any drive, fo Ite <u>m</u> s to restore:	to see its contents. Then select the Ider, or file that you want to restore.	Browse
E Backup_AD.bkf creat	Backup Identification Label	Мес 7/2010 at С:\{
		Þ
	< <u>B</u> ack <u>N</u> ext >	Cancel

În final suntem întrebați dacă dorim să restartăm sau nu computerul. În cazul în care alegem **Yes** se va realiza un **restore normal**, adică se va restaura totul exact ca în momentul salvării. Eventualele modificări în *Active Directory* efectuate după momentul salvării și existente pe un alt controler de domeniu vor fi actualizate prin replicare. Răspunsul *NO* (nu) la restartarea sistemului poate continua cu cererea pentru un **restore authoritativ.** Este vorba de restaurarea unei porțiuni din *Active Directory* care nu va mai fi modificată prin propagarea replicării. Pentru o restaurare de acest fel se continuă prin lansarea utilitarului **Ntdsutil.** Procedura de lucru este următoarea: folosind interfața **Command Prompt** (linie de comandă) se lansează utilitarul **ntdsutil** și după prompterul **ntdsulit** se introduce de la tastatură **authoritative restore.**

🖎 Command Prompt - ntdsutil	
Semantic database analysis Set DSRM Password tor account password	- Semantic Checker - Reset directory service restore mode administra
ntdsutil: authoritative restor authoritative restore: ?	e
? Create ldif file(s) from %s	 Show this help information Creates ldif file(s) using specified authoritatively restored objects list to recreate back-links of those objects.
Help List NC CRs	 Show this help information Lists Partitions and cross-refs. You need the cross-ref of a Application Directory Partition to restore it.
Quit	- Return to the prior menu
Restore database	- Authoritatively restore entire database
Restore object Zs	- Authoritatively restore an object
Restore object %s verinc %d	and override version increase
Restore subtree %s	- Authoritatively restore a subtree
Restore subtree %s verinc %d	and override version increase
authoritative restore: 🛓	

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

Restore object nume_obiect_ldap



Propunere de temă practică

Notați modul în care rezolvați temele propuse.

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

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

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

1. Includeți un calculator în domeniul creat.

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

3. Instalați Administrative Tools folosind comanda adminpak.msi.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2. Creați in containerul dumneavoastră o subunitate organizațională.

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

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

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

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



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

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

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

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

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

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

Ce ați învățat în acest modul?

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