# SISTEME DE OPERARE ÎN REȚEA

## Material de predare I

## Familia Microsoft Windows Server

**Domeniul: Informatică**

**Calificarea: Tehnician infrastructură rețele de telecomunicații**

**Nivel 3 avansat**

**2009**

**AUTOR:**

**IORDACHE FLORIN**

**COORDONATOR:**

**LADISLAU SEICA**

**CONSULTANȚĂ:**

**IOANA CÎRSTEA** – expert CNDIPT

**ZOICA VLĂDUȚ** – expert CNDIPT

**ANGELA POPESCU** – expert CNDIPT

**DANA STROIE** – expert CNDIPT

# Cuprins

# I. Introducere

Materialele de predare reprezintă o resursă – suport pentru activitatea de predare, instrumente auxiliare care includ un mesaj sau o informație didactică.

Prezentul material de predare, se adresează cadrelor didactice care predau în cadrul şcolilor postliceale, domeniul **Informatică**, calificarea **Tehnician infrastructură rețele de telecomunicații**

El a fost elaborat pentru modulul **Sisteme de operare în rețea**, ce se desfăşoară în 93 ore, din care laborator tehnologic 31

| **Teme** | **Fise suport** | **Competențe/Rezultate ale învățării** |
|---|---|---|
| Tema 1. Familia Microsoft Windows Server | Fisa 1.1. Familia Microsoft Windows Server | • C2, C3, C4 |
| Tema 2 Protocoale de rețea | Fisa 2.1. Protocoale de rețea | • C2, C3, C4 |
| Tema 3: Servicii de rețea | Fișa 3.1 Servicii de rețea<br>Fișa 3.2. Active directory - Serviciul de catalog<br>Fișa 3.3. Instalarea serverului DHCP<br>Fișa 3.4 Instalarea serverului DNS<br>Fișa 3.5 Instalarea serviciului file server | • C1, C2, C3, C4 |
| Tema 4: Instalarea WIN2003/ WIN2008 server | Fișa 4.1. Operațiuni pregătitoare<br>Fișa 4.2 Instalarea sistemului de operare | • C1, C2, C3 |
| Tema 5: Configurarea sistemelor de operare in retea | Fisa 5.1. Configurarea Active Directory | • C3, C4 |
| Tema 6: Securitatea NOS | Fisa 6.1. Securizarea sistemului | • C2, C3, C4 |

C1. Pregateste sistemul de calcul pentru instalare

C2. Analizează sistemele de operare de rețea.

C3. Utilizează  sistemele de operare în rețea

C4. Administrează sistemele de operare în rețea

# I. Documente necesare pentru activitatea de predare

Pentru predarea conținuturilor abordate în cadrul materialului de predare cadrul didactic are obligația de a studia următoarele documente:

- *Standardul de Pregătire Profesională* pentru calificarea Tehnician echipamente de calcul, nivelul 3 avansat – www.tvet.ro, secțiunea SPP sau www.edu.ro , secțiunea învățământ preuniversitar
- *Curriculum* pentru calificarea Tehnician echipamente de calcul, nivelul 3 avansat – www.tvet.ro, secțiunea Curriculum sau www.edu.ro , secțiunea învățământ preuniversitar

# Tema 1. Familia Microsoft Windows Server

## Fisa 1.1. Familia Microsoft Windows Server


Familia de sisteme de operare Windows 2003/2008 server oferă o gamă variată de servicii care poate acoperi majoritatea cerințelor în materie de servere de pe piața IT. Are în componență următoarele sisteme de operare:

1. **Standard edition** - sistem de operare de rețea, care oferă soluții simple şi rapide pentru firme. Windows Standard Server 2003/2008 oferă servicii pentru partajarea fişierelor şi imprimantelor, conectarea securizată la Internet, desfăşurarea centralizată a aplicațiilor din spațiul de lucru Windows Standard Server 2003/2008 permite multiprocesare simetrică pe 2 căi şi până la 4 GB de memorie.

2. **Enterprise edition** – sistem de operare de rețea destinat rețelelor mari de calculatoare. Oferă funcționalitatea necesară pentru infrastructura întreprinderii, aplicațiile tip linie de afaceri şi tranzacțiile de comerț electronic. Windows Enterprise Server 2003/2008 este un sistem de operare complet, care acceptă până la 8 procesoare, cluster cu 4 noduri şi până la 32 GB de memorie. Este disponibil şi pentru platformele de calcul pe 64 de biți.

3. **Datacenter edition** - Conceput pentru activitățile care necesită un nivel ridicat de scalabilitate şi disponibilitate, Windows Datacenter Server 2003/2008 oferă o bază solidă pentru construirea soluțiilor critice de baze de date, software de planificare a resurselor întreprinderii (ERP), prelucrarea în timp real a volumelor mari de tranzacții şi consolidarea serverelor. Este cel mai puternic şi mai funcțional sistem de operare pentru server din familia windows 2003/2008 server, permițând multiprocesare simetrică cu până la 32 de căi (SMP), având drept caracteristică standard atât clusterul cu 8 noduri cât şi serviciile de load-balancing. Windows Datacenter Server 2003 este disponibil şi pentru platforme de calcul pe 64 de biți.

4. **Web edition** - Este un server Web orientat pe funcții, optimizat astfel încât să furnizeze firmelor o platformă cuprinzătoare şi stabilă pentru servire şi găzduire pe Web. Uşor de instalat şi de administrat.

5. **For Itanium based systems -** Windows Server 2008 pentru sistemele Itanium-Based este optimizat pentru baze de date mari, linie de afaceri și aplicații specifice oferind disponibilitate mare precum și scalabilitate până la 64 de procesoare.

6. **HPC server -** Windows HPC Server 2008, reprezintă următoarea generație de high-performance computing (HPC), oferind unelte enterprise pentru un mediu HPC extrem de productiv. Construit pe platforma Windows Server 2008, cu tehnologie 64-bit, Windows HPC Server2008, poate scala eficient până la mii de nuclee de procesare incluzând console de administrare care vă ajuta să monitorizați proactiv starea generală a sistemului. Programarea operațiunilor, interoperabilitatea și flexibilitatea vă permit integrarea între platforme HPC Windows și Linux, suportând aplicații SOA. Productivitate sporită, performanțe scalabile, ușurință în utilizare, sunt doar câteva din capacitățile care fac din Windows HPC Server 2008 unul din cele mai reușite sisteme de operare server.

   O analiză comparativă a sistemelor de operare din familia Windows 2003/2008 Server este dată în tabelul de mai jos:

| Caracteristică | Web Server | Standard Server | Enterprise Server | Data Center |
|---|---|---|---|---|
| **Tehnologii de clustere** | | | | |
| Echilibrarea încărcării rețelei (NLB) | da | da | da | da |
| Protecție la defecțiuni în cluster | nu | nu | da | da |
| **Communicații şi servicii de rețea** | | | | |
| Suport pentru Rețea privată virtuală (VPN) | parțial | da | da | da |
| Serviciul Protocol de inițiere a sesiunii (SIP) | nu | da | da | da |
| Serviciul de autorizare Internet (IAS) | nu | da | da | da |
| Network Bridge | nu | da | da | nu |
| Partajare conexiune la Internet (ICS) | nu | da | da | nu |
| **Directory Services** | | | | |
| Active Directory | nu | da | da | da |
| Suport pentru servicii Metadirector (MMS) | nu | nu | da | da |
| **Servicii de fişiere şi imprimare** | | | | |
| Sistem de fişiere distribuite (DFS) | da | da | da | da |
| Sistem de criptare fişiere (EFS) | da | da | da | da |

| | | | | |
|---|---|---|---|---|
| Shadow Copy Restore | nu | da | da | da |
| SharePoint Team Services | nu | da | da | da |
| Suport stocare la distanță | nu | da | da | da |
| Serviciul de fax | nu | da | da | da |
| Servicii pentru Macintosh | nu | nu | da | da |
| **Servicii de management** | | | | |
| IntelliMirror | nu | da | da | da |
| Resultant Set of Policy (RSoP) | nu | da | da | da |
| Windows Management Instrumentation (WMI) Command Line | nu | da | da | da |
| Servicii de instalare la distanță (RIS) | nu | da | da | da |
| **Servicii de securitate** | | | | |
| Internet Conection Firewall | nu | da | da | nu |
| Certificate Services | nu | parțial | da | da |
| **Servicii de terminal** | | | | |
| Spațiu de lucru la distanță pentru administrare | da | da | da | da |
| Terminal Server | nu | da | da | da |
| Sesiuni Terminal Server | nu | nu | da | da |
| **Servicii multimedia** | | | | |
| Servicii Windows MediaT | nu | da | da | nu |
| **Scalabilitate** | | | | |
| Suport de 64 biți pentru computere bazate pe IntelR ItaniumT | nu | nu | da | da |
| Hot add memory.[1] | nu | nu | da | da |
| Acces neuniform la memorie (NUMA)[1] | nu | nu | da | da |
| Control procese | nu | nu | da | da |
| Suport | nu | nu | nu | da |
| **Servicii pentru Web şi aplicații** | | | | |
| .NET Framework | da | da | da | da |
| Internet Information Services (IIS) 6.0 | da | da | da | da |
| ASP.NET | da | da | da | da |

[1] Poate să fie limitat datorită lipsei de suport hardware OEM.

Familia windows 2008 server aduce facilități suplimentare:

| Facilități noi / îmbunătățite | Enterprise Server | Datacenter Server | Standard Server | Web Server | Itanium Server | HPC Server |
|---|---|---|---|---|---|---|
| AD Rights Management Services (RMS) | da | da | da | nu | nu | nu |
| Criptare a datelor (CNG) | da | da | da | da | da | da |
| Opțiuni suplimentare pentru politica de grup (Group Policy) | da | da | da | da | da | da |
| Virtualizare - Hyper-V | da | da | da | nu | nu | da |
| Internet Information Services (IIS) 7.0 | da | da | da | da | da | da |
| NEW: Protecția accesului la rețea (NAP) | da | da | da | nu | nu | nu |
| Controllere de domeniu read only (RODC) | da | da | da | da | nu | da |
| Server Core | da | da | da | da | nu | nu |
| Server Manager | da | da | da | da | da | da |
| Servicii de terminal și aplicații la distanță | da | da | da | nu | nu | nu |
| Servicii de instalare în rețea - (WDS) | da | da | da | nu | nu | da |

# Tema 2 Protocoale de rețea

## Fisa 2.1. Protocoale de rețea

În Internet se folosesc protocoale care fie se bazează pe TCP/IP, fie utilizează protocolul TCP/IP. Vom prezenta în continuare cele mai folosite protocoale utilizate în mediul Internet.

**Protocolul ARP** – protocol de rezoluție a adresei

Pentru ca două sisteme de calcul să poată comunica într-o rețea este necesară cunoașterea atât a adresei MAC, cât şi a adresei IP. În cazul în care numai una dintre adrese este disponibilă se apelează la un protocol dedicat care pe baza acesteia va determina cealaltă adresă.

Stiva de protocoale TCP/IP conține două protocoale de nivel rețea pentru a servi acest scop: ARP (Address Resolution Protocol) şi RARP (Reverse Address Resolution Protocol). ARP este protocolul ce va oferi adresa MAC a unui dispozitiv de rețea, dată fiind adresa sa IP. ARP se bazează pe construirea şi menținerea unei tabele ARP. O tabela ARP are rolul de a oferi o corespondență între adresele IP şi cele MAC. Acestea sunt construite dinamic şi sunt stocate în memoria RAM. Deși există mecanisme pentru adăugarea sau eliminarea unei intrări într-o tabelă ARP acestea sunt rareori folosite. Fiecare computer sau dispozitiv de rețea își păstrează propria sa tabelă ARP.

**Protocolul ICMP** – protocolul mesajelor de control

Arhitectura internetului implică o serie de probleme atunci când o maşină anume nu funcționează. Dacă funcționează, totul e bine. Dacă nu, intervine ICMP: Internet Control Message Protocol.

ICMP este protocolul responsabil cu determinarea eventualelor probleme datorate "căderii" unei maşini. Nu-i aşa că ați folosit comanda ping? Aşa trimiteți un pachet. Ținta va răspunde - în cazul în care va primi pachetul. Dacă totul e în ordine, rezultatul este

un pachet identic. Dacă nu, veți primi un pachet ICMP. Acesta conține, în header-ul său, informațiile de care are nevoie pentru a determina o eventuală problemă.

Protocolul ICMP este unul de mare importanță, în primul rând pentru administratori. Ei îşi pot da seama dacă cineva a scos din uz o maşină în mod intenționat - spre exemplu dacă o maşină funcționează perfect, dar portul 80 (HTTPD) nu este accesibil, avem un indiciu al unui eventual atac.

**DHCP** – protocol pentru alocarea dinamică a adreselor IP

În primele zile ale rețelelor TCP/IP, administratorii defineau adresa fiecărui dispozitiv într-un fişier text sau într-o casetă de dialog. Din acel moment, adresa rămânea fixată până când cineva o modifica. Problema era că administratorii, ocazional, atribuiau din greșală adrese contradictorii altor dispozitive din rețea, provocând multe și mari neplăceri. Pentru a rezolva această problemă şi pentru a facilita atribuirea adreselor TCP/IP a inventat un serviciu numit Dynamic Host Configuration Protocol (DHCP).

Serviciile DHCP rulează pe un server DHCP, unde controlează un domeniu de IP, denumite domeniu de acoperire. Când dispozitivele se conectează la o rețea contactează serverul DHCP pentru a obține o adresă atribuită pe care să o poată folosi. Se spune că adresele de la un server DHCP sunt închiriate clientului care le folosește, cea ce înseamnă că rămân atribuite unui anumit dispozitiv pentru un interval de timp înainte de a expira şi devin disponibile pentru utilizare de către un alt dispozitiv. Perioadele de închiriere sunt de numai câteva zile, dar administratorii de rețea pot folosi orice perioadă de timp doresc.

**HTTP** - Hypertext Transfer Protocol

World Wide Web este alcătuit din documente care folosesc un limbaj de formatare denumit HTML, abreviere de la Hypertext Markup Language (limbaj de marcare prin hipertext). Aceste documente sunt compuse din text de afişat, imagini grafice, comenzi de formatare şi hiperlegături spre alte documente situate altundeva în Web. Documentele HTML sunt afişate cel mai frecvent folosind browsere Web, precum Internet Explorer, Safari sau Mozilla Firefox.

Un protocol denumit Hypertext Transfer Protocol (protocol de transfer prin hipertext) controlează tranzacțiile dintre un client Web şi un server Web. HTTP este un protocol destinat stratului aplicație. Protocolul HTTP face uz în mod transparent de DNS şi de alte protocoale Internet pentru a forma conexiuni între clientul și serverul Web astfel încât utilizatorul cunoaşte numai numele domeniului şi numele documentului însuşi.

HTTP este, în esență, un protocol nesigur. Informațiile pe suport text sunt transmise „în clar", între client şi server. Pentru a satisface necesitatea unor rețele Web sigure există alternative precum Secure HTTP (S-HTTP) sau Secure Sockets Layer (SSL).

Cererile unui client Web către un server Web sunt orientate spre conexiune, deci sunt persistente. Odată ce clientul a primit conținutul unei pagini HTML, conexiunea nu mai este activă. Executarea unui clic în documentul HTML reactivează legătura fie către serverul original (dacă într-acolo indică hiperlegătura), fie către un alt server, situat altundeva.

**FTP** – protocol pentru transferul fișierelor

Abrevierea FTP simbolizează două lucruri: File Transfer Protocol (protocol de transfer al fişierelor) şi File Transfer Program (program de transfer al fişierelor).

FTP este un protocol de nivel aplicație folosit pentru trimiterea şi recepționarea fişierelor între un client FTP şi un server FTP. De regulă, aceasta se realizează cu programul FTP sau cu un alt program care poate de asemenea folosi protocolul. Transferurile FTP pot fi bazate pe text sau sunt binare și pot manipula fişiere de orice dimensiune. Când vă conectați la un server FTP pentru a transfera un fişier, vă conectați la serverul FTP folosind un nume de utilizator şi o parolă valabile. Totuşi, multe site-uri sunt configurate să permită ceea ce se numeşte FTP anonim, când se introduce numele de utilizator *anonymous* şi apoi introduceți și adresa dumneavoastră de e-mail ca parolă.

**Telnet** – protocol pentru stabilirea de conexiuni la distanță

Telnet defineşte un protocol care permite stabilirea unei sesiuni terminal de la distanță la o gazdă din Internet, astfel ca utilizatorii de la distanță să aibă acces ca şi cum ar sta la un terminal conectat direct la calculatorul gazdă. Folosind Telnet, utilizatorii pot controla sistemul gazdă aflat la distanță, executând operații precum gestiunea fișierelor,

rularea aplicațiilor sau chiar (cu permisiuni corespunzătoare) administrarea sistemui aflat la distanță.

**SMTP –** protocol simplu de transfer de poștă

Poşta electronică a avut un început cam nesigur pe Internet; primele programe de e-mail partajau puține standarde cu alte programe de e-mail, mai ales în ceea ce priveşte manipularea datelor binare ataşate. În ziua de azi, toate programele curente de e-mail recunosc toate standardele acceptate pe scară largă.

Simple Mail Transfer Protocol (SMTP) este folosit pentru trimiterea şi recepționarea mesajelor de e-mail de la un server e-mail la celălalt. Detalii despre SMTP se pot găsi în RFC 821. Protocolul SMTP defineşte un dialog între un sistem emițător şi unul receptor. Un dialog SMTP începe când un sistem emițător se conectează la portul 25 al unui sistem receptor. După stabilirea conexiunii, sistemul emițător trimite o comandă HELO, urmată de adresa sa. Sistemul receptor confirmă comanda HELO, alături de adresa sa proprie. Apoi, dialogul continuă; sistemul emițător trimite o comandă prin care se arată că sistemul doreşte să trimită un mesaj şi se indică destinatarul căruia îi este destinat mesajul. Dacă sistemul receptor cunoaşte destinatarul, confirmă cererea şi apoi sistemul emițător transmite corpul mesajului, alături de eventualele fişiere ataşate. În final, conexiunea dintre cele două sisteme este încheiată odată ce sistemul receptor confirmă recepționarea întregului mesaj.

**POP3 –** protocol de poștă electronică

Post Office Protocol, pe scurt, POP, este primul protocol de poștă electronică şi încă este folosit în zilele noastre. Pentru utilizatorii ce folosesc sisteme care fie nu sunt capabile să ruleze un server complet de tipul Simple Mail Transfer Protocol (SMTP) fie nu sunt conectate permanent, este utilizată o maşină de tip „Post Office". Această maşină Post Office este conectată permanent la Internet şi primeşte e-mail-urile destinate utilizatorului prin SMTP. Mesajele sunt trimise într-o căsuță electronică de pe maşina Post Office ca şi cum ar fi fost maşina folosită de utilizator din modelul vechi. Cândva, mai târziu, utilizatorul se conectează de pe stația de pe care operează cu ajutorul unui client de e-mail la serverul POP existent pe maşina Post Office şi face transferul mesajelor care

aşteaptă pe stație. Din acest moment, utilizatorul îşi poate citi sau procesa după cum doreşte mesajele în stația locală. Acest sistem foarte simplu a servit şi serveşte foarte bine utilizatorii de ceva timp încoace.

**IMAP –** protocol interactiv de poștă electronică

Internet Message Access Protocol, pe scurt, IMAP, a fost proiectat pentru a depăşi câteva dintre limitările protocolului POP. În loc să transfere toate mesajele pe stația clientului, IMAP reține aceste mesaje pe server. Metoda folosită de POP este denumită câteodată „offline" deoarece, după ce v-ați transferat mesajele, teoretic, puteți să vă deconectați în timp ce vă citiți e-mail-ul. Metoda principală folosită de către IMAP este considerată a fi „online" deoarece presupune conectarea pe toată perioada cât vă citiți mesajele. Atunci când vă conectați la un server IMAP, inițial doar anteturile noilor mesaje sunt descărcate în clientul de e-mail pentru vizualizare şi în momentul selectării unui mesaj este descărcat şi conținutul acestuia. La final, sunt trimise înapoi la server mesaje pentru setarea unor flaguri ce determină starea mesajelor (citit / necitit).

# Tema 3. Servicii de rețea

## Fișa 3.1 Servicii de rețea

Un sistem de operare de rețea trebuie să constituie o platformă puternică, o bază pentru serviciile care pot rula într-o rețea de calculatoare. Principalele servicii de care este nevoie într-o rețea sunt:

- Servicii de catalog (autentificare a utilizatorilor) - active directory
- Servicii de suport pentru utilizatorii mobili – remote access
- Servicii de mesagerie - mail server
- Servicii de tipărire - print server,
- Servicii de fișiere - file server:
- Servicii de infrastructură - DNS, DHCP

## Fișa 3.2. Active directory - Serviciul de catalog

Utilizarea unei rețele include și utilizarea resurselor unei rețele. Deoarece resursele unei rețele pot fi extrem de variate (autentificare, redirecționare cereri, securitate, partajare resurse) s-a simțit nevoia unei centralizări a acestor resurse. Aici apar așa numitele servicii de catalog.

Catalogul este de fapt o bază de date ce conține:

- Lista cu utilizatorii ce au permisiunea de a se conecta în sistem
- Lista cu permisiuni pentru fiecare utilizator / resursă
- Lista cu dispozitivele din rețea care au acces la resursele rețelei

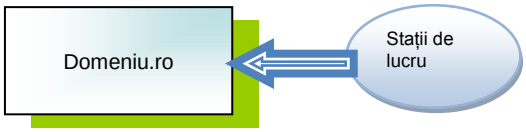



Fig. 1

Deoarece o asemenea bază de date poate ajunge la milioane de înregistrări s-a simțit nevoia unei ierarhizări. Această ierarhizare presupune existența unui domeniu și a unui controller de domeniu (fig 1).

De asemenea dacă baza de date este mare sau foarte mare, respectiv dacă cerințele de proiectare ale domeniului o cer putem avea situații în care vom avea arbori (fig. 2) sau păduri de domenii (fig. 3).

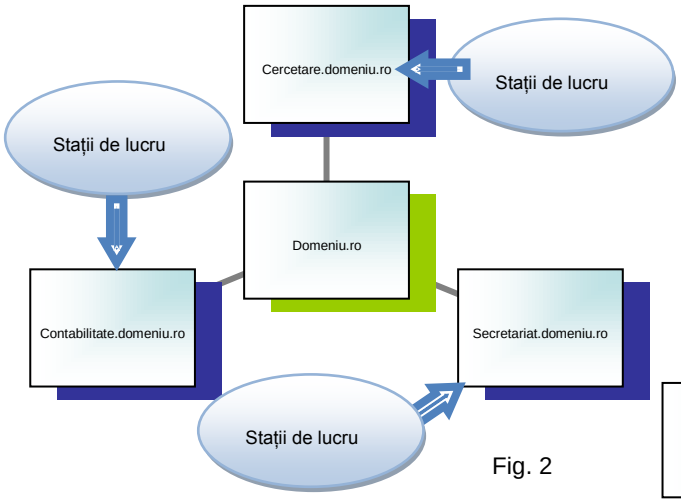



Fig. 2

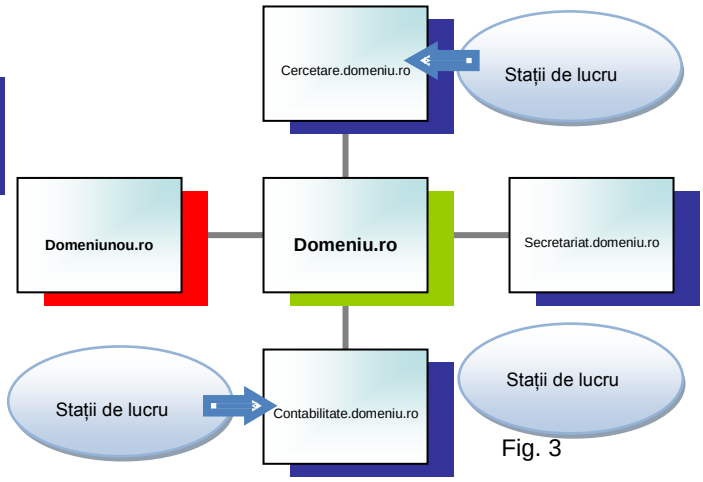
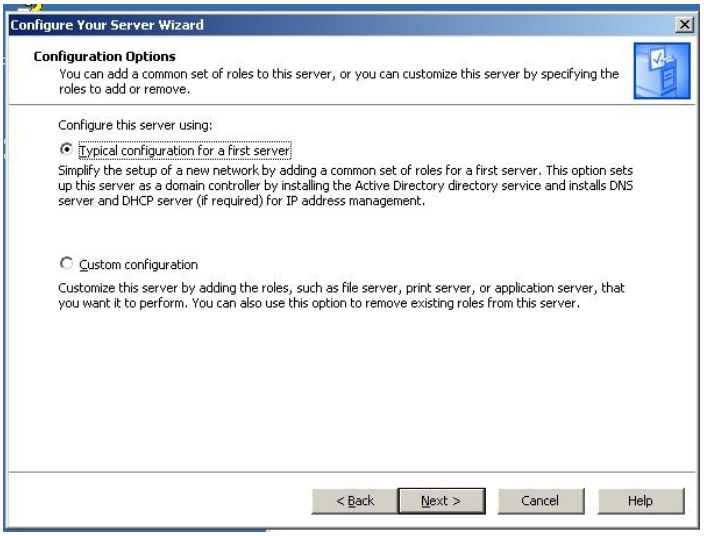



Fig. 3

Instalarea Active Directory în sistemul de operare Winows 2003 server se realizează uşor şi intuitiv cu ajutorul vrăjitorului existent în fereastra Manage Your Server alegând opțiunea

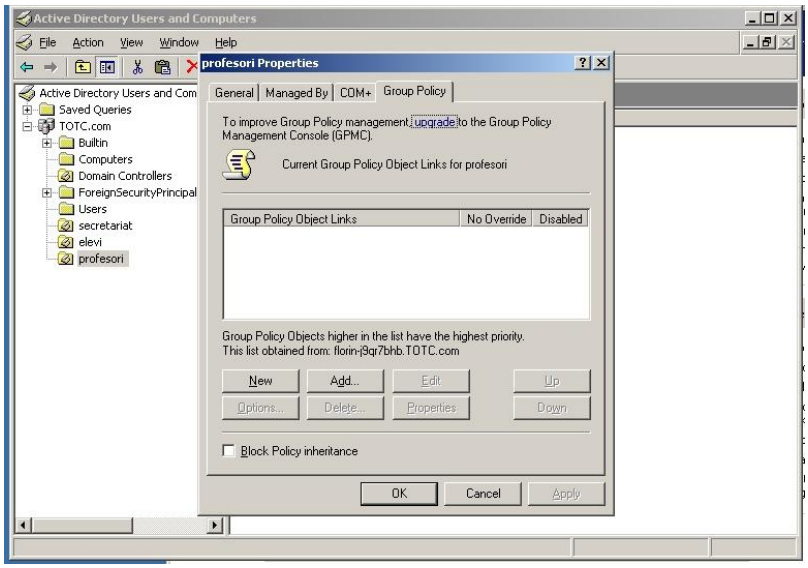



Add a role, apoi Active Directory. Dacă este prima dată când instalați un controller de domeniu cel mai bine e să lăsați vrăjitorul să vă îndrume în instalare şi să instalați atât Active Directory, cât şi serverul DNS şi serverul DHCP.

Pe măsură ce instalarea avansează vor fi cerute informații vitale pentru organizarea şi buna funcționare a controllerului de domeniu:

- Numele de domeniu: poate fi .local dacă dorim ca domeniul creat să fie „local” (să fie separat de domeniul de internet)
- Numele din DNS al domeniului şi numele din Netbios pentru clienții non windows

În continuare vom face prezentarea celei mai importante componente din **Active Directory** şi anume **Active Directory Users and Computers**




**Active Directory Users and Computers** pentru domeniul curent conține, în mod implicit, 5 categorii:

• Builtin - care conține un set de utilizatori predefiniți cu diferite roluri în cadrul domeniului d-voastră.

• Computers - conține toate stațiile incluse în domeniul curent.

• Domain Controllers - include toate serverele din domeniul curent care au instalat şi configurat serviciul Active Directory.

• ForeignSecurityPrincipals - conține identificatorii de securitate (security identifiers - SIDs) asociați obiectelor Active Directory din alte domenii decât cel curent.

• Users - conține informații despre toți utilizatorii şi grupurile de utilizatori implicite.

**Active Directory Users and Computers** poate gestiona informații despre calculatoare, grupuri de utilizatori, grupuri organizaționale, imprimante, utilizatori şi directoare puse la dispoziție în rețea (shared folder).

Recomandabil este ca înainte de crearea unui utilizator să creați întâi un nou grup organizațional care poate include şi stații de lucru, şi asupra căruia se poate crea o politică de securitate centralizată.

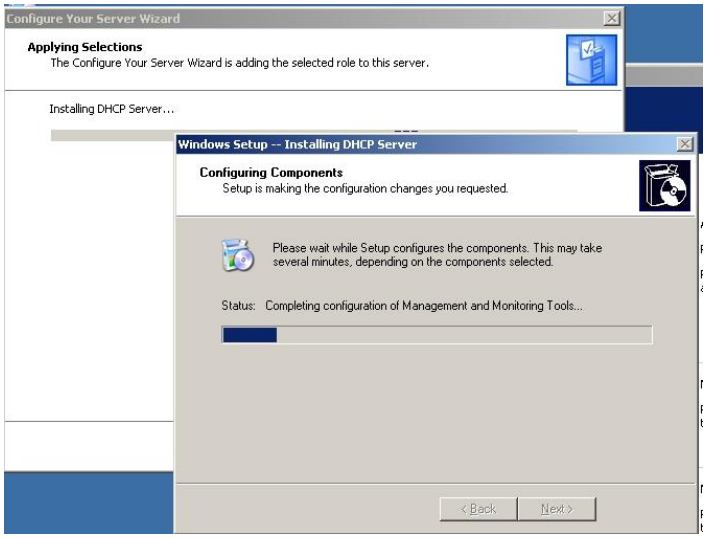
La proprietățile unui grup organizațional putem specifica următoarele informații:

• informații generale (General). Conține informații privind descrierea grupului şi adresa la care poate fi localizat acesta;

• informații despre persoana / utilizatorul care gestionează grupul respectiv (Managed By).

• politicile de securitate aplicate grupului respectiv (Group Policy) unde avem posibilitatea de creare a unei noi politici de securitate sau importul unei politici deja existente. Nu activați opțiunea Block Policy inheritance pentru că aceasta nu se va mai propaga automat asupra altor subsisteme organizaționale din grupul respectiv.

## Fișa 3.3. Instalarea serverului DHCP




Instalarea şi configurarea de principiu a serverului DHCP se realizează cu ajutorul vrăjitorului care poate fi rulat din fereastra Manage my computer, Add remove roles.

Vrăjitorul ne va ajuta printr-o serie de paşi simpli să configurăm un server DHCP funcțional şi foarte util în dezvoltarea şi managementul rețelei.

Ce informații trebuie dumneavoastră să-i dați vrăjitorului:

1. Numele „rezervorului de adrese” şi o scurtă descriere a acestuia (ex. adrese pentru laboratorul de informatică)
2. Apoi trebuie să ştim adresa de început, adresa de sfârşit şi masca de subrețea. Dacă în această gamă de adrese avem adrese pe care dintr-un motiv sau altul nu dorim să le alocăm dinamic, la pasul următor vom fi întrebați care sunt acestea.
3. „Închirierea” de adrese de IP se face pe perioadă determinată (8 zile implicit).
4. Deoarece un server DHCP trebuie să lucreze împreună cu un server DNS vom fi întrebați de adresa sau numele serverului DNS respectiv.

În ceea ce priveşte proprietățile generale ale serverului, este deosebit de important să cunoaşteți următoarele trei lucruri:

♦ cum se activează jurnalul pentru serviciul DHCP;

♦ cum este implicat serviciul DHCP în actualizarea înregistrărilor DNS pentru clienții DHCP;

♦ cum se configurează detectarea conflictelor.

Pe pagina de proprietăți Advanced puteți activa proprietatea Conflict Detection Attempts. Această configurare defineşte de câte ori serverul DHCP lansează în

rețea comanda PING pentru a obține un răspuns la o adresă pe care urmează să o aloce unui client. Dacă este detectat un răspuns, atunci serverul DHCP ştie că un alt client utilizează adresa şi încearcă să aloce alta. Prin opțiune prestabilită, această proprietate nu este activată (este stabilită la valoarea 0), dar dumneavoastră puteți să măriți această valoare pentru a verifica adresele. Într-o rețea LAN, o singură încercare trebuie să fie suficientă pentru a controla existența unei adrese duplicat în rețea.
Pentru a configura opțiunile Server TCP/IP, efectuați clic dreapta pe linia Server Options şi selectați opțiunea Configure Options din meniul care apare.

Opțiuni:

♦ ruter;

♦ server DNS;

♦ numele domeniului DNS;

♦ server WINS;

♦ tipul de nod NetBIOS.

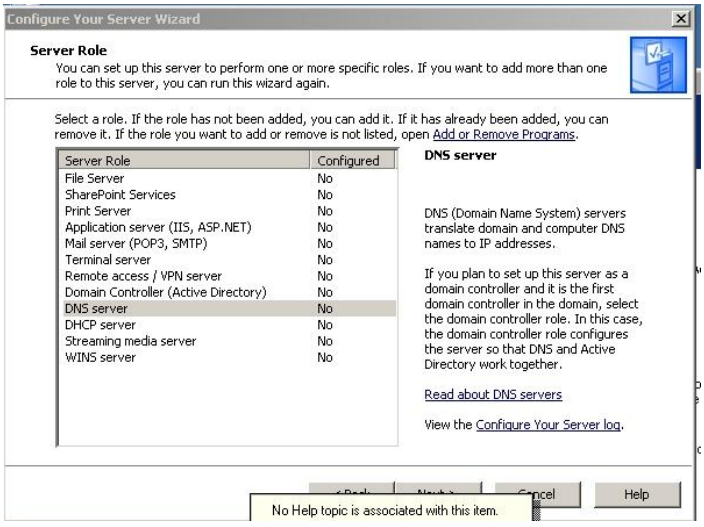
În plus, clienții DHCP Windows 2000 acceptă şi configurarea opțiunilor Perform Router Discovery şi Static Route. Toate celelalte setări ale configurației vor fi ignorate de către clienții Microsoft.

Se pot configura anumite calculatoare care să obțină anumite adrese atunci când cer o adresă de la serverul DHCP. Aceste alocări de adrese se numesc rezervări. Printr-o rezervare se realizează o corespondență între adresa MAC a unei plăci de rețea şi o adresă TCP/IP. Aceasta are ca efect crearea unei configurații statice, fără a fi necesară, de fapt, modificarea proprietăților TCP/IP de pe client. Rezervările de adrese sunt utile în mai multe situații. De exemplu, dacă aveți o imprimantă de rețea, care obține adresa TCP/IP prin intermediul unui server DHCP, dar trebuie să aibă întotdeauna aceeaşi adresă, atunci puteți utiliza o rezervare. În plus, dacă doriți să stabiliți explicit adresa TCP/IP a unui calculator, deoarece acesta are instalat un anumit serviciu, dar dumneavoastră doriți să beneficiați de parametrii de configurare oferiți de serverul DHCP, atunci puteți utiliza de asemenea o rezervare.

Pentru a crea o rezervare, este necesară adresa hardware (MAC) a plăcii de rețea pentru care doriți să rezervați adresa. Aceasta este uşor de obținut; adresa TCP/IP poate fi obținută fie local, pe calculatorul cu placa de rețea, fie de la distanță. În ambele cazuri, calculatorul trebuie să aibă instalat protocolul TCP/IP şi trebuie să aibă o adresă TCP/IP. Local, dacă lansați comanda IPCONFIG/all de la un prompt de comandă, va fi afişată o linie cu eticheta Physical Address şi un număr de tipul 00-60-97-D5-22-CA asociat acesteia. Aceasta este adresa MAC şi, dacă ştergeți liniuțele, obțineți numărul pe care serverul DHCP îl doreşte asociat cu rezervarea.

Dacă nu puteți accesa local calculatorul, atunci puteți determina adresa de la distanța, folosind comanda PING şi utilitarul ARP. Utilitarul ARP descoperă şi păstrează adresa hardware asociată unei adrese TCP/IP contactate de către calculatorul local. Dacă lansați comanda PING pentru calculatorul pe care încercați să-l configurați şi apoi verificați memoria cache pentru utilitarul ARP, atunci veți descoperi adresa MAC.

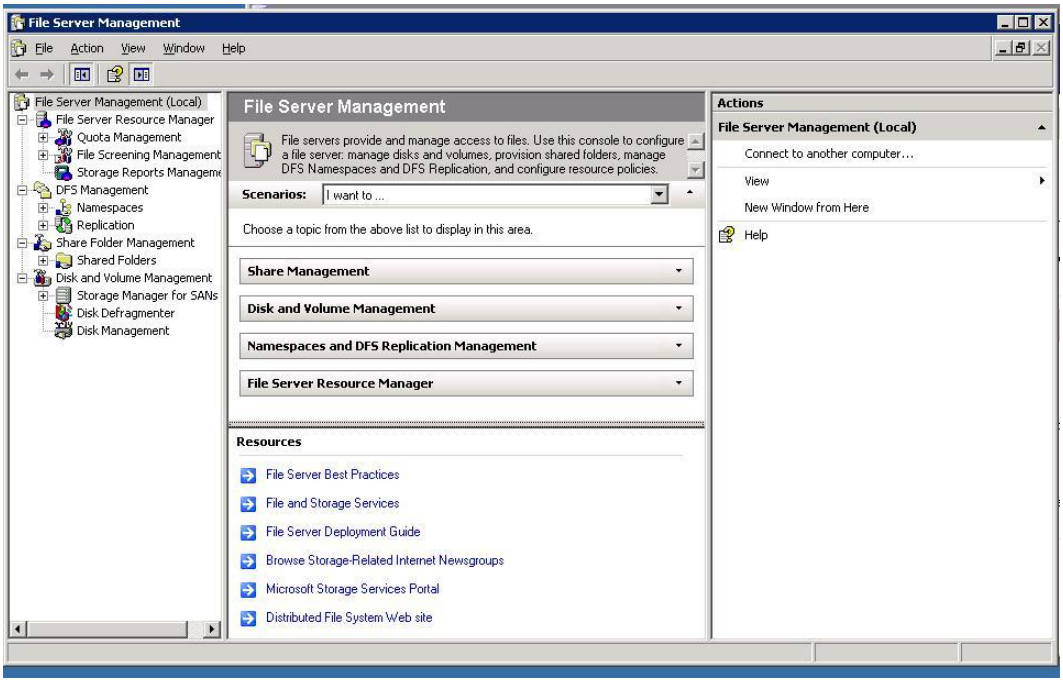
## Fișa 3.4 Instalarea  serverului DNS




Serverul DNS este unul din cele mai importante servere, server fără de care internetul şi rețelele de calculatoare, aşa cum le ştiți dumneavoastră, ar fi un coşmar. Închipuiți-vă doar că ar trebui să țineți minte toate numerele de telefon din memoria telefonului dumneavoastră mobil! Acelaşi lucru se întâmplă şi în calculatoare: închipuiți-vă că ar trebui să țineți minte câte o adresă IP pentru fiecare site care vă place! Instalarea preliminară a unui server DNS se realizează relativ simplu în Windows 2003 Server urmând ca setările de finețe să fie făcute ulterior. Aşa cum v-ați obişnuit adăugarea rolului de server DNS se realizează tot din fereastra Manage Your Server.

## Fișa 3.5 Instalarea  serviciului file server.

În principiu, orice calculator care oferă partajare de fișiere poate fi considerat un server de fișiere. Problema se pune în situația în care avem mulți utilizatori și multe fișiere. În acest caz, se impune existența unui server special creat pentru așa ceva. Începând cu ediția R2 a windows 2003 server au fost introduse concepte noi legate de stocarea de fișiere:




- Quota Management – facilitate destinată limitării spațiului de stocare utiliyat de unul sau mai mulți utilizatori / grupuri de utilizatori pe discurile serverului de fișiere
- File screening – facilitate care oferă posibilitatea administratorilor să blocheze depozitarea anumitor tipuri de fișiere pe discurile serverului de fișiere. Implicit serverul vine cu câteva templateuri predefinite care acoperă o mare parte din nevoile unui administrator. Dar există și posibilitatea foarte simplă a creerii de noi template-uri în funcție de necesități.
- DFS – permite crearea de resurse partajate centralizate folosind suportul de stocare a diferitelor componente fizice din rețeaua de date. Acest serviciu oferă un acces mai rapid la resurse precum și o utilizare mai eficientă a spațiului de stocare.

# Tema 4 Instalarea sistemului de operare Windows 2003 server

## Fișa 4.1. Operațiuni pregătitoare

Windows Server 2003 solicită în cazul minimal un hardware relativ modest. Pentru prioritatea edițiilor, îl puteți instala la calculatoarele pe care altfel nu le-ați putea utiliza ca stație de lucru. Pentru un server folosit efectiv în producție ar fi mai bine să utilizați un calculator destinat să fie folosit ca server. Calculatoarele de clasa server sunt proiectate şi construite astfel încât să fie mai fiabile şi mai serviabile decât calculatoarele desktop.

Pentru **Web Edition** a Windows Server 2003, iată configurația minimală recomandată pentru hardware:

- Procesor de clasă Pentium (doar) cu frecvența minimă de lucru de 133 MHz (Microsoft recomandă 550 MHz).

- Cel puțin 128MB de RAM. (Microsoft recomandă cel puțin 256MB)

- Cel puțin 1,5GB de spațiu liber pe disc.

Pentru **Standard Edition**:

- Procesor de clasă Pentium (doar) cu frecvența minimă de lucru de 133 MHz (Microsoft recomandă 550 MHz). Ediția standard poate utiliza până la 4 procesoare de clasă Pentium.

- Cel puțin 128MB de RAM. (Microsoft recomandă cel puțin 256MB şi personaj recomand cel puțin 512MB.) Ediția standard poate utiliza până la 4GB de RAM instalat.

- Cel puțin 1,5GB până la 2GB de spațiu liber pe disc.

Pentru **Enterprise Edition**:

- Procesor de clasă Pentium (doar) cu frecvența minimă de lucru de 133 Mhz (Microsoft recomandă 550 MHz). Ediția Enterprise poate utiliza până la opt calculatoare echipate procesoare de clasă Pentium sau Itanium.

- Cel puțin 128MB de RAM. Ediția Enterprise poate utiliza până la 32GB de RAM instalat.

- Cel puțin 1,5GB pentru calculatoarele echipate cu procesoare de clasă Pentium şi 2GB de spațiu liber pe disc pentru calculatoarele echipate cu procesoare de clasă Itanium.

După ce ați verificat că echipamentul hardware corespunde cerințelor minimale, ar trebui să vă asigurați de asemenea că acel hardware pe care intenționați să-l utilizați este atestat a fi utilizat pentru Windows Server 2003. Puteți face acest lucru fie adresându-vă producătorului echipamentului hardware pe care intenționați să-l utilizați, fie căutând în Microsoft Hardware Compatibility List, la adresa http:// www.microsoft.com/hcl.

Pregătirea calculatorului server

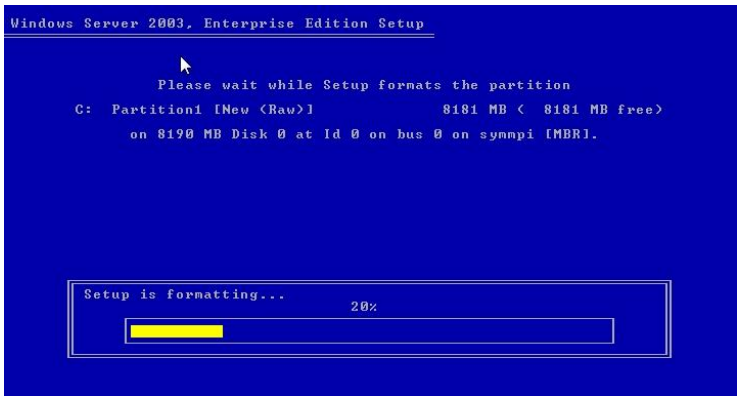
Pentru un server folosit efectiv în producție, este important să acordați o atenție specială în pregătirea echipamentului hardware. Acest proces presupune următoarele etape:

- Testarea riguroasă a calculatorului, utilizând programe de diagnoză furnizate de fabricant.
- Existența unei liste a tuturor componentelor utilizate pe server
- Existența driverelor pentru componente

## Fișa 4.2 Instalarea sistemului de operare

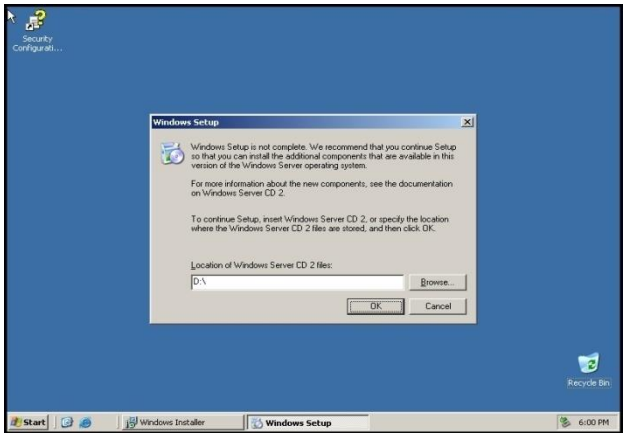
Pentru început trebuie să intrați în BIOS-ul sistemului de calcul și să îl configurați astfel încât să booteze de de CD/DVD. Apoi introduceti CD-ul de instalare Windows 2003 Server in unitatea CD ROM. Cand sistemul porneste, urmariti mesajul “Press any key to boot from CD..” (Apasati orice tasta pentru a boot-a de pe CD)

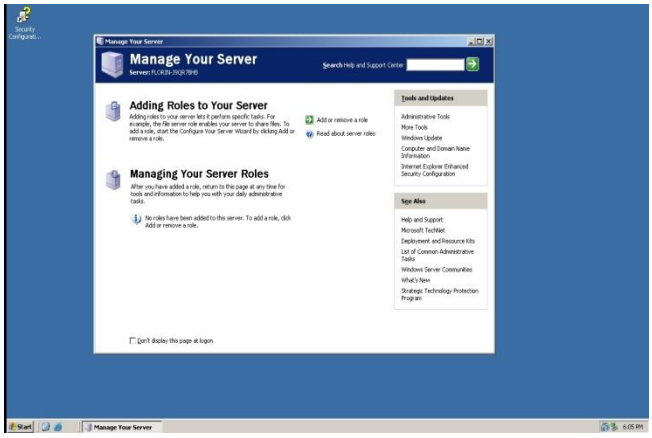

Daca mesajul apare, apăsați orice tasta de pe tastatură pentru ca sistemul sa booteze de pe CD. Sistemul va începe acum sa inspecteze configurația hardware. Daca mesajul nu apare, unitatea de hard disk este goala şi sistemul va începe sa inspecteze configurația hardware. Va trebui să fim de acord cu termenii de licențiere și apoi dacă totul este în regulă vom avea acces la programul de partiționare și vom realiza partițiile necesare. Datorită avantajelor evidente formatarea partiției se va realiza în sistemul de fișiere NTFS. Va începe apoi procesul de copiere al fișierelor, sisstemul se va restarta și procesul de instalare va continua în mod grafic:




Vor trebui apoi configurate setările regionale, modul de licențiere (pe server sau pe stație de lucru), numele calculatorului și setările de rețea.

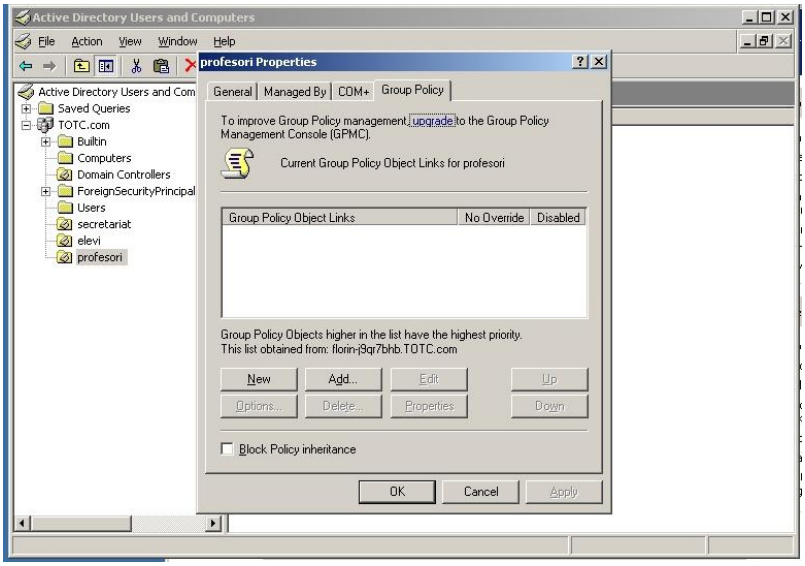
Cu aceasta s-a încheiat prima parte a procesului de instalare. Dacă doriți să instalați Windows 2003 server R2, procesul de instalare va continua cu cererea celui de-al 2-lea CD. După ce instalarea celui de-al 2-lea CD s-a încheiat va apare ecranul binecunoscut



# Tema 5 - Configurarea sistemelor de operare în rețea

## Fisa 5.1. Configurarea Active Directory




Deoarece securitatea şi managementul securității este un element cheie în ceea ce înseamnă Active Directory pentru un domeniu, vom prezenta în continuare, pe scurt, câteva noțiuni şi opțiuni pe care trebuie să le cunoaşteți atunci când abordați un server Windows 2003.

Fereastra Group Policy este împărțită în două mari categorii:

• Computer Configuration (politica stațiilor de lucru şi a serverelor din domeniu);

• User Configuration (politica de securitate pentru utilizatorii din grupul organizațional respectiv).

Dacă un grup organizațional conține numai utilizatori sau numai calculatoare, cealaltă opțiune poate fi blocată din fereastra de proprietăți a politicii de securitate.

În momentul în care activați una dintre cele 2 opțiuni, va apărea pe ecranul d-voastră o fereastră de atenționare cu privire la consecințele care pot fi generate în urma acestei operațiuni, respectiv faptul că stațiilor de lucru din acest grup organizațional le va fi aplicată politica de securitate locală. Vă recomandăm să creați o politică de securitate cu preponderență orientată spre utilizator, pentru că pe aceeaşi stație se pot conecta diferite

categorii de utilizatori care pot avea diferite niveluri de acces la aceasta, anumite operațiuni fiindu-le private de o eventuală politică de securitate eronat specificată.

O primă subcategorie întâlnită la ambele categorii este Software Settings ce conține opțiunea Software installation, care presupune instalarea automată a unor aplicații împachetate în prealabil în mod administrativ. Pachetele utilizate în acest scop sînt recunoscute sub extensia MSI. Aceste pachete se salvează într-un director pus la dispoziție în rețea. Instrumentele respective se bazează pe crearea unei imagini (snapshot) a regiştrilor sistemului de operare, instalarea şi configurarea aplicațiilor, repornirea sistemului, împachetarea aplicației prin preluarea fişierelor de pe disc, precum şi a cheilor introduse în regiştri.

În subcategoria Windows Settings există opțiunea Scripts care, pentru Computer Configuration, include opțiunile Startup şi Shutdown, iar la User Configuration include Log on şi Log off. Aici se pot specifica diferite script-uri care să se declanşeze în momentul în care stația sau utilizatorul se autentifică în rețea.

O opțiune din politica de securitate poate avea 3 stări:

• Nedefinită/neconfigurată (not defined/not configured);

• Definită/Activă (specificarea unei valori/Enabled);

• Indisponibilă (Disabled).

În continuare, vom încerca să explicăm câteva dintre opțiunile politicii uzuale de securitate, valorile aferente şi, înainte de toate, calea de a ajunge la opțiunea respectivă.

**Computer Configuration\ Windows Settings\ Security Settings\ Account Policies\ Password Policies:**

• Maximum password age (durata maximă de valabilitate a unei parole) - forțează utilizatorul ca după un anumit număr de zile (implicit 70) să-şi schimbe parola. Este în strînsă legătură cu Minimum Password age (durata minimă de valabilitate a unei parole) (implicit 30 de zile).

• Passwords must meet complexity requirements (parola trebuie să aibă un format complex) - care înseamnă că aceasta nu trebuie să conțină o parte sau tot numele de utilizator; să nu fie mai mică de 6 caractere; să conțină caractere mari, mici, numere şi caractere non-alfanumerice (de exemplu, !, $—>, %). De asemenea, se recomandă folosirea caracterelor speciale sau a caracterului spațiu în crearea parolelor. Activarea acestei opțiuni forțează utilizatorul să nu mai folosească data naşterii, numărul de la maşină sau nume familiare în crearea parolelor.

**Computer Configuration\ Windows Settings\ Security Settings\ Account Policies\ Account Lockout Policy:**

• Account lockout threshold (blocarea contului de utilizator) - se configurează pentru a preveni încercările repetate de conectare la rețea în condițiile de necunoaştere a parolei. Valorile pe care le poate lua sînt de la 1 la 999. Implicit această opțiune nu este configurată, iar valoarea 0 elimină posibilitatea de blocare a contului. Recomandăm valoarea 3 pentru această opțiune.

• Account lockout duration (timpul de blocare a unui cont) - specifică durata de blocare a unui cont care a fost blocat automat prin opțiunea anterioară. Intervalul de valori este cuprins între 1 şi 99999 minute, valoarea implicită fiind de 30 de minute, configurabilă automat în momentul în care se configurează opțiunea anterioară.

**Computer Configuration\ Windows Settings\ Security Settings\ Local Policies\ User Rights Assignment:**

• Add workstations to domain (adăugarea de stații în domeniu) - se configurează pentru a permite utilizatorilor sau unui grup de utilizatori să adauge stații de lucru în domeniu. Implicit, grupul de utilizatori care poate adăuga stații în domeniu este Authenticated Users, dar în această categorie pot intra toți utilizatorii creați în Active Directory, ceea ce diminuează controlul asupra stațiilor din domeniul respectiv.

• Change the systern time (schimbarea timpului din sistem) - în mod implicit, fiecare utilizator poate să schimbe data şi ora sistemului, dar nu recomandăm acest lucru pentru că poate duce la înregistrarea greşită din punctul de vedere al timpului a unor evenimente

din rețea. Schimbați asemănător exemplului anterior această opțiune, definind dreptul de acces grupurilor administrative la nivel de domeniu.

**Computer Configuration\ Windows Settings\ Security Settings\ Local Policies\ Security Options:**

• Additional restrictions for anonymous access (Acces limitat conexiunilor anonime). Orice utilizator din domeniul curent sau din alte domenii poate vedea, în mod implicit, resursele puse la dispoziție în rețea. Pentru a oferi o mai bună protecție domeniului recomandăm opțiunea Do not allow enumeration of SAM accounts and shares, care înlocuieşte grupul de utilizatori Everyone cu Authenticated Users în definirea politicilor locale de acces la diferite resurse. În acest fel, numai utilizatorii din Active Directory pot avea acces la resursele domeniului: share-uri, imprimante etc.

• Automatically log off users when logon time expires (Deconectarea automată de la rețea în momentul expirării timpului de lucru). Pentru anumite categorii de utilizatori sau în mod individual poate fi configurat un interval orar de acces în rețea. În momentul în care utilizatorul depăşeşte timpul alocat, acesta este deconectat automat de la resursele rețelelor. De asemenea, şi versiunea următoare (local) trebuie activată pentru ca sistemul să deconecteze automat utilizatorul.

• Do not display last user name in logon screen (Neafişarea numelui ultimului utilizator conectat pe stația curentă). În cazul rețelelor cu mulți utilizatori, activarea acestei opțiuni aduce un spor de siguranță la conectarea în rețea, mulți utilizatori nefiind destul de atenți la ultimul User Name scris în fereastra de Log On. În cazul în care într-o rețea acelaşi utilizator lucrează cu preponderență pe aceeaşi stație, activarea acestei opțiuni nu este recomandată.

• Message text for users attempting to log on (Mesajul pentru utilizatorii care doresc să se conecteze în rețea). Aici se poate trece un mesaj de informare a utilizatorilor care se conectează în rețea. Opțiunea Message title for users attempting to log on specifică tipul ferestrei de mesaj (de exemplu, Bun venit în cadrul rețelei TOTC).

• Number of previous logons to cache (in case domain controller is not available) (Numărul conectărilor anterioare salvate local în cazul în care serverul de domeniu nu este

disponibil) - permite conectarea pe staţii folosind utilizatorii de domeniu chiar şi în cazul în care serverul de autentificare este temporar indisponibil. Această opţiune este recomandabilă numai în cazul în care domeniul conţine puţini utilizatori, şi aceştia se conectează cu precădere pe aceeaşi staţie. În cazul domeniilor cu mulţi utilizatori, crearea profilurilor de utilizatori locali duce la o diminuare a spaţiului disponibil pe disc. Valoarea 0 este corespondentă cazului al doilea.

• Prompt user to change password before expiration (Atenţionarea utilizatorului pentru a-şi schimba parola cu un anumit timp înainte de expirare). Se exprimă în zile, valoarea implicită fiind 14. Vă recomandăm însă o valoare mai mică, 5 sau 7, pentru a nu deranja utilizatorul la fiecare conectare. Schimbarea parolei acestuia duce la anularea apariţiei mesajului de avertizare pînă la următorul termen.

• Restrict CD-ROM access to locally logged-on user only (Blocarea accesului la CD-ROM utilizatorilor autentificaţi de staţie şi nu de serverul de domeniu). Se utilizează pentru prevenirea instalării unor aplicaţii, copierii de fişiere etc. de alţi utilizatori decît cei autentificaţi în domeniu. De asemenea, se poate interzice accesul către unitatea de dischetă prin următoarea opţiune : Restrict floppy access to locally logged-on user only.

**Computer Configuration\ Windows Settings\ Security Settings\ Restricted Groups** este destinată limitării drepturilor anumitor grupuri de utilizatori, prin adăugarea acestora în această categorie

**Computer Configuratiom Windows Settings\ Security Settings\ System Services** este destinat configurării serviciilor care vor rula pe staţiile de lucru din domeniu. Se pot defini modul de pornire a serviciului, precum şi grupurile de utilizatori care au dreptul de pornire a respectivului serviciu.

Atenţie la modul de pornire a anumitor servicii. Testaţi în prealabil pe o staţie obişnuită care dintre servicii vă pot asigura o funcţionalitate optimă şi care pot fi oprite. Este bine cunoscut că un număr mai mic de servicii aduce cu sine şi o memorie RAM suplimentară.

**Computer Configuration\ Windows Settings\ Security Settings\ Registry** este opţiunea prin intermediul căreia administratorii pot defini permisiuni de acces utilizatorilor pe anumite secţiuni din regişţrii sistemului de operare de pe staţiile de lucru.

**Computer Configuration\ Windows Settings\ Security Settings\ File System** permite administratorilor adăugarea şi definirea politicii de securitate la nivelul directoarelor şi fişierelor de pe stațiile de lucru.

**Computer Configuration\ Administrative Templates** conține o serie de şabloane de opțiuni predefinite configurabile. Şabloanele implicite sînt conf, inetres, system.

• încetarea apariției ferestrei de bun venit la conectarea în rețea: Computer Configuratori Administrative Templates\ System\ Don't display welcome screen at logo.

• Blocarea rulării automate a unui CD în momentul introducerii acestuia în unitatea de CD-ROM : Computer Configuration\ Administrative Templates\ System\ Disable Autoplay.

• În cazul în care aveți mai multe servere de autentificare pentru domeniu, propagarea schimbărilor care se efectuează pe acestea poate fi configurată din: Computer Configuration\ Administrative Templates\ System\ Group Policy\ Group Policy refresh interval for domain controllers. Valoarea implicită este de 5 minute.

**Prezentarea principalelor categorii din User Configuration**

• Personalizarea titlului pentru Internet Explorer şi a imaginii de pe bara cu instrumente: User Configuration\ Windows Settings\ Internet Explorer Maintenance\ Browser User Interface\ Browser Title

• Specificarea unui proxy pentru comunicarea pe Internet: User Configuration\ Windows Settings\ Internet Explorer Maintenance\ Connection\ Proxy Settings

• Personalizarea paginii de start (home page), a paginii de căutare şi a paginii pentru asistența tehnică: User Configuration\ Windows Settings\ Internet Explorer Maintenance\ URLs\ Important URLs  Această opțiune este foarte importantă pentru configurarea unei pagini HTML drept desktop al stațiilor din domeniu.

• Pentru specificarea altei locații directorului My Documents: User Configuration\ Windows Settings\ Folder Redirection\My Documents. În lista Settings există opțiunea Basic - Redirect everyone 's folder to the same location (redirecționarea tuturor utilizatorilor către

aceeaşi locație), iar la Target folder location treceți adresa la care va fi redirecționat automat directorul My Documents pentru fiecare utilizator în parte.

• Interzicerea schimbării paginii de start (home page): User Configuration\ Administrative Templates\ Windows Components\ Internet Explorer\ Disable changing home page settings.

• Ascunderea opțiunii Folder Option din meniul Tools din Windows Explorer cu scopul de a nu permite utilizatorilor vizualizarea unor fişiere ascunse, sau fişiere sistem, în scop distructiv, sau a eliminării lor din necunoştință de cauză: User Configuration\ Administrative Templates\ Windows Components\ Windows Explorer\ Removes the Folder Option menu item from the Tools menu. Opțiunea ascunderii fişierelor şi eliminarea posibilității de dezascundere poate fi depăşită cu utilitarul Command Prompt, comanda attrib.

• Ascunderea anumitor discuri în My Computer, pentru a restricționa accesul la acestea: User Configuration\ Administrative Templates\ Windows Components\ Windows Explorer\ Hide these specified drives in My Computer. Foarte multe erori care se întâmplă la utilizarea calculatoarelor sunt cauzate de mutarea accidentală prin drag-and-drop a directoarelor dintr-o locație în alta. Pentru protejarea sistemului de operare, dar şi pentru a păstra o ordine în organizarea fişierelor de pe discul C:, vă recomandăm să activați opțiunea Restrict C drive only. De asemenea, puteți bloca accesul la discurile A: sau B: pentru a vă proteja şi prin această cale de utilizatorii care pot transporta viruşi pe dischete (Restrict A, B and C drives only). În cazul în care doriți blocarea accesului la CD-ROM, trebuie să activați opțiunea Restrict D drive only, cu specificarea faptului că trebuie să vă configurați partițiile de pe stațiile de lucru (Administrative Tools\ Computer Management\ Disk Management) în aşa fel încît discul de CD-ROM să aibă asignată litera D. Dacă stația d-voastră face parte dintr-un domeniu public, gen i-cafe, puteți ascunde toate discurile de pe stație, prin activarea opțiunii Restrict all drives. Chiar dacă activați această politică de securitate, accesul la discuri este posibil din Command Prompt numai dacă nu ați dezactivat această opțiune.

• Eliminarea iconiței My Network Places din Windows Explorer pentru a preveni accesul neautorizat în rețea: User Configuration\ Administrative Templates\ Windows Components Windows Explorer\ No „Entire Network" in My Network Places.

• Specificarea numărului maxim de documente stocate în lista documentelor recent apelate: User Configuration\ Administrative Templates\ Windows ComponentsX Windows ExplorerX Maximum number of recent documents (valoare implicită: 15).:

• Eliminarea opțiunii Run din meniul Start: User Configuration\ Administrative Templates\ Start Menu & Taskbar\ Remove Run Menu from Start Menu.

• Ascunderea iconiței de acces la rețea de pe Desktop : User Configuration\ Administrative Templates\ Desktop\ Hide My Network Places icon on desktop.

• Interzicerea schimbării destinației directorului sistem My Documents: User Configuration\ Administrative Templates\ Desktop\ Prohibit user from changing My Documents path.

• Ascunderea resursei Active Directory în rețea: User Configuratori Administrative Templates\ Desktop\ Active Directory\ Hide Active Directory folder.

• Interzicerea accesului la tabloul de bord al calculatorului (Control Panel): User Configuratori Administrative Templates\ Control Panel\ Disable Control Panel.

• Dacă doriți în schimb să păstrați numai anumite componente în Control Panel, puteți alege opțiunea Show only specified control panel applets şi specificați numele componentelor pe care le doriți. Componentele pe care le puteți folosi le găsiți în directorul în care a fost instalat sistemul de operare, subdirectorul System32, sub forma unor fişiere cu extensia CPL. Pot exista în schimb şi neclarități în legătură cu aceste componente pentru că, de exemplu, nu există nici un CPL care să deschidă fereastra de configurare a tastaturii, şi nici a imprimantelor.

• Interzicerea modificării setărilor pentru display : User Configuration\Administrative Templates\ Control Panel\ Display\ Disable Display în Control Panel. Această regulă poate fi considerată una dintre cele mai drastice pentru utilizatorul final. Folosirea acestei politici de securitate diminuează posibilitatea de apariție a unor cazuri de acest gen, pentru că în utilitarul Paint există încă posibilitatea de setare a unei imagini drept fundal al desktop-ului d-voastră.

• Interzicerea modificării parametrilor TCP/IP : User Configuratori Administrative Templates\ Network\ Network and Dial-up Connections\ Allow TCP/IP advanced configuration

• Blocarea accesului la utilitarul pentru comenzi (Command Prompt): User Configuratori Administrative Templates\ System\ Disable the command prompt. În această secțiune, la opțiunea Enabled foarte important este modul în care se vor executa script-urile. Dacă la procesul de autentificare de rețea aveți script-uri de tip BAT pentru diferite operațiuni, alegeți din lista Disable the command prompt script processing also opțiunea No.

• Interzicerea accesului la regiştrii sistemului de operare, activați opțiunea Disable registry editing tools.

• Interzicerea accesului către anumite aplicații: Do not run specified Windows applications

• Limitarea accesului la aplicația de gestiune a proceselor (Task Manager): User Configuratori Administrative Templates\ System\ Logon\ Logoff\ Disable Task Manager; recomandăm această opțiune în momentul în care rulați aplicații de monitorizare pe stațiile de lucru sub formă de servicii, pentru a preveni oprirea neautorizată a acestora de către utilizatori.

# Tema 6: Securitatea NOS

## Fisa 6.1. Securizarea sistemului

Securitatea se referă la menținerea sistemului în stare de funcționare în regi continuu şi la parametri normali. Securitatea nu se referă doar la protejarea împotriva diferitelor tipuri de atacuri, ci şi la protecția împotriva căderilor hardware (a harddisk-urilor), a ştergerii accidentale a datelor.

Un server este supus permanent riscurilor unor atacuri de diferite feluri, aceste provenind de la distanță sau chiar de pe propria maşină. Atacurile pot fi:

• atacuri de refuz al serviciilor (Denial of Service), care degradează sau defecteas anumite servicii ale programului;

• atacuri în vederea obținerii de privilegii asupra sistemului;

• atacuri în vederea copierii sau distrugerii de informații.

Principalele tipuri de atacuri:

Poate fi stopat prin introducerea în fişierele de configurare a accesului din cadrul MTA a unei directive de refuzare a mesajelor provenind de pe maşina sau de la utilizatorul respectiv. Această soluție nu rezolva însă problema traficului prin rețea.

2. Spam (e-mail spamming)

De obicei, adresa expeditorului este falsă (pentru a nu putea fi descoperit), astfel că acest tip de atac poate fi prevenit configurând serviciul de e-mail pentru a respinge e-mail-urile provenite de pe domenii care nu pot fi rezolvate.

3. Falsificarea adresei expeditorului (E-mail spoofing)

Serverul (sau serverele, în unele cazuri) de mail care a transmis mesajul poate fi determinat prin analiza antetului mesajului. Se recomandă contactarea administra torului serverului respectiv şi solicitarea de informații privind originea mesajului (acestea pot fi obținute din fişierele jurnal ale sistemului)'.

4. Abonarea nesolicitată la liste de discuții

Reprezintă înscrierea unei adrese e-mail pe una sau mai multe liste de discuții fără ca persoana căreia îi aparține adresa să fi cerut explicit acest lucru. Nu există soluții rapide pentru stoparea acestor atacuri, ci doar trimiterea de cereri de dez-abonare. :

5. Atacuri pentru refuzul serviciilor (Denial of Service) '

Prevenirea atacurilor de tip DoS se poate face prin instalarea de firewalluri (care să filtreze pachetele către porturi care trebuie protejate, precum şi pachetele ICMP) instalarea

de conexiuni de siguranță (backup) şi dezactivarea serviciilor care n necesare (pentru a diminua expunerea acestora la potențialele atacuri).

6. Depăşirea zonelor tampon

Acest tip de atac nu poate veni însă din afara maşinii, ci din interiorul și nu poate fi prevenit. Pe măsură ce asemenea erori sunt descoperite, sunt generate actualizări ale programelor.

7. Interceptarea rețelei (IP sniffing)

Un asemenea atac se poate preveni doar din interiorul rețelei locale. Pentru a preveni, este bine să utilizăm, cel puțin pentru transmiterea parolelor din protocoale sigure, criptate, cum ar fi SSH.

8. Cai troieni (Trojan horses)

Toate fişierele executabile sau arhivele conținând programe descărcate de pe Internet (chiar şi de pe şiturile oficiale) trebuie verificate înainte de a fi instalate și executate. De asemenea, se recomandă realizarea periodică de copii de siguranță a sistemelor de fişiere, pentru a putea restaura fişierele executabile originale în alterării acestora de către cai troieni.

9. Uşi ascunse

Uşile ascunse sunt cazuri particulare de cai troieni. Un asemenea program creează o „poartă" (de exemplu, un utilizator nou) care să permită accesul ulterior la calculatorul în cauză sau să acorde unui anumit utilizator privilegii speciale. Spre exemplu, un cal troian poate înlocui fişierul /bin/login, care are rolul de a autentifica utilizatorii, pentru a salva parolele tastate de aceştia într-un fişier ascuns;

10. Viruşi

Viruşii sunt programe care pot efectua operațiuni nedorite, de obicei distructive, şi care au capacitatea de a se „multiplica", adică de a infecta şi alte programe. Viruşii rezidă în general în cadrul fişierelor executabile. Sistemele UNIX nu sunt vulnerabile la viruşi, datorită gestiunii stricte a memoriei şi a proceselor care se execută. Este recomandat, în

orice caz, să nu se execute ca root nici un fişier executabil despre care nu se cunoaşte ce face.

11. Viermi (Worms)

Viermii sunt programe de sine stătătoare, capabile să se multiplice, să se transfere pe alte calculatoare şi, eventual, să efectueze operații distructive. Sistemele FreeBSD nu sunt afectate de viermi.

12. Ghicirea parolelor (password guessing)

Acest tip de atac se referă la folosirea unui program pentru a determina parolele prost alese, denumit în genere spărgător de parole (cracker). Un astfel de program poate determina, printr-o analiză comparativă, o corespondență între variantele de presupuse parole criptate.

13. Folosirea de anumite vulnerabilități (bugs) a programelor / serviciilor existente pe server

De obicei, problema securității nu se pune la nivel de nucleu al sistemului de operare, ci la nivelul aplicațiilor. La anumite perioade de timp sunt descoperite vulnerabilități în aplicațiile instalate în sistem, în servicii, unele dintre ele putând fi folosite pentru a obține accesul în sistem.

Reuşita atacurilor este de cele mai multe ori cauzată de configurări slabe ale sistemului sau de neglijarea erorilor (bugs) de securitate descoperite şi de lipsa update-uui la timp a programelor ce prezintă vulnerabilități. De aceea trebuie acordată o importanță mare configurărilor de după instalare.

Acțiuni ce trebuie întreprinse pentru a se asigura securizarea unui sistem de operare în rețea:

- Siguranța fizică a sistemului - Instalarea maşinii trebuie realizată într-un loc sigur, să nu fie expusă contactului cu persoane neautorizate. Acestea nu trebuie să aibă posibilitatea sau timpul necesar de a înlătura carcasa, de a modifică configurația hardware, de a opri şi apo

reporni maşina (eventual în modul single), de a înlocui sau copia informațiile discuri sau de a inocula programe răuvoitoare (cai troieni). De asemenea, mediile de stocare a salvărilor de siguranță trebuie să fie păstrate într-un loc închis, fără posibilitate de acces (e.g., un seif).

- Salvările de siguranță - Se recomandă salvarea periodică cel puțin a fişierelor importante şi, dacă este posibil a întregului conținut al sistemelor de fişiere.
- Drepturile de acces la fişierele importante - Trebuie acordată o atenție sporită drepturilor de acces la fişierele importante: fişierele de configurare ale diverselor servicii instalate în sistem, fişierele jurnal (log-uri), executabilele care nu trebuie să poată fi apelate de către utilizatorii obişnuiți, precum şi alte fişiere importante (spre exemplu, baze de date MySQL, PostreSQL etc.), executabilele şi scripturile de inițializare ale sistemului nu trebuie să poată fi modificate decât de root / administrator.
- Execuția daemonilor / proceselor - Se recomandă ca numai daemonii / procesele utilizați(te) curent să ruleze pe sistem. Mai mulți(te) daemoni / servicii înseamnă o încărcare mai mare a sistemului, precum şi un nivel de vulnerabilitate mai mare. De asemenea, o mare parte a daemonilor / serviciilor (care oferă diverse servicii) nu trebuie executați sub root / administrator, ci sub utilizatorii speciali (de exemplu, daemonul HTTP rulează sub utilizatorul www).
- Scripturile CGI - Scripturile CGI nu trebuie executate ca root. Acestea trebuie plasate într-un singur director, în care nu se va permite accesul utilizatorilor, iar modificările asupra scripturilor trebuie monitorizate.
- Porturile - Anumite servicii pot fi accesate prin rețea, de pe alte maşini. Pentru aceasta, ele aşteaptă conexiuni pe anumite porturi (e.g., serverul HTTP pe portul 80). Aceste porturi pot constitui puncte vulnerabile ale sistemului (datorită vulnerabilităților care pot exista în aceste programe), putând fi detectate de la distanță cu ajutorul scanerelor. Aceste porturi trebuie protejate fie prin configurarea respectivelor servicii să accepte conexiuni doar de pe o anumită interfață de rețea, considerată sigură (e.g.,

rețeaua locală), fie prin configurarea unui firewall care să nu permită accesarea din exterior a porturilor în cauză.

- Accesul utilizatorului root / administrator în sistem - Din principiu, nu se recomandă permiterea accesului cu root / administrator decât de la consolele sistemului. Accesul de la distanță (cu SSH) va fi făcut cu un utilizator obişnuit, iar apoi va fi folosită comanda su. Sistemul FreeBSD nu permite accesul la distanță prin SSH folosind autentificarea ca root şi, de asemenea, nu permite su decât din contul utilizatorilor ce aparțin grupului wheel.

# Fişa rezumat

**Numele elevului**: _____

**Numele profesorului:** _____

| **Competențe care trebuie dobândite** | **Activități efectuate şi comentarii** | **Data activitatii** | **Evaluare** | | |
|---|---|---|---|---|---|
| | | | **Bine** | **Satis-făcător** | **Refacere** |
| Identifică dispozitive şi circuite electronice analogice şi digitale utilizate în realizarea echipamentelor de telecomunicații | Activitate 1 | | | | |
| | Activitate2 | | | | |
| Interpretează parametrii ce caracterizează funcționarea circuitelor electronice din echipamentele de telecomunicații | | | | | |
| Citeşte scheme cu circuite electronice din echipamentele de telecomunicații | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| Depanează subansamble electronice din echipamentele de telecomunicații | | | | | |
| **Comentarii** | | **Priorități de dezvoltare** | | | |
| **Competențe care urmează să fie dobândite (pentru fişa următoare)** | | **Resurse necesare** | | | |

- **<u>Competențe care trebuie dobândite</u>**

  Această fişă de înregistrare este făcută pentru a evalua, în mod separat, evoluția legată de diferite competențe. Acest lucru înseamnă specificarea competențelor tehnice generale şi competențelor pentru abilități cheie, care trebuie dezvoltate şi evaluate. Profesorul poate utiliza fişele de lucru prezentate în auxiliar şi/sau poate elabora alte lucrări în conformitate cu criteriile de performanță ale competenței vizate şi de specializarea clasei.

- **<u>Activități efectuate şi comentarii</u>**

  Aici ar trebui să se poată înregistra tipurile de activități efectuate de elev, materialele utilizate şi orice alte comentarii suplimentare care ar putea fi relevante pentru planificare sau feed-back.

- **<u>Priorități pentru dezvoltare</u>**

  Partea inferioară a fişei este concepută pentru a menționa activitățile pe care elevul trebuie să le efectueze în perioada următoare ca parte a viitoarelor module. Aceste informații ar trebui să permită profesorilor implicați să pregătească elevul pentru ceea ce va urma.

- **<u>Competențele care urmează să fie dobândite</u>**

  În această căsuță, profesorii trebuie să înscrie competențele care urmează a fi dobândite. Acest lucru poate implica continuarea lucrului pentru aceleaşi competențe sau identificarea altora care trebuie avute in vedere.

- **Resurse necesare**

  Aici se pot înscrie orice fel de resurse speciale solicitate:manuale tehnice, rețete, seturi de instrucțiuni şi orice fel de fişe de lucru care ar putea reprezenta o sursă de informare suplimentară pentru un elev care nu a dobândit competențele cerute.

***Notă**: acest format de fişă este un instrument detaliat de înregistrare a progresului elevilor. Pentru fiecare elev se pot realiza mai multe astfel de fişe pe durata derulării modulului, aceasta permițând evaluarea precisă a evoluției elevului, în acelaşi timp furnizând informații relevante pentru analiză.*