Universitatea Politehnica Bucureşti

Facultatea Electronică,Telecomunicaţii şi Tehnologia Informaţiei

Retele de calculatoare si internet

Serviciul director ACTIVE DIRECTORY

Toader Bogdan

Master IISC, anul II

2013

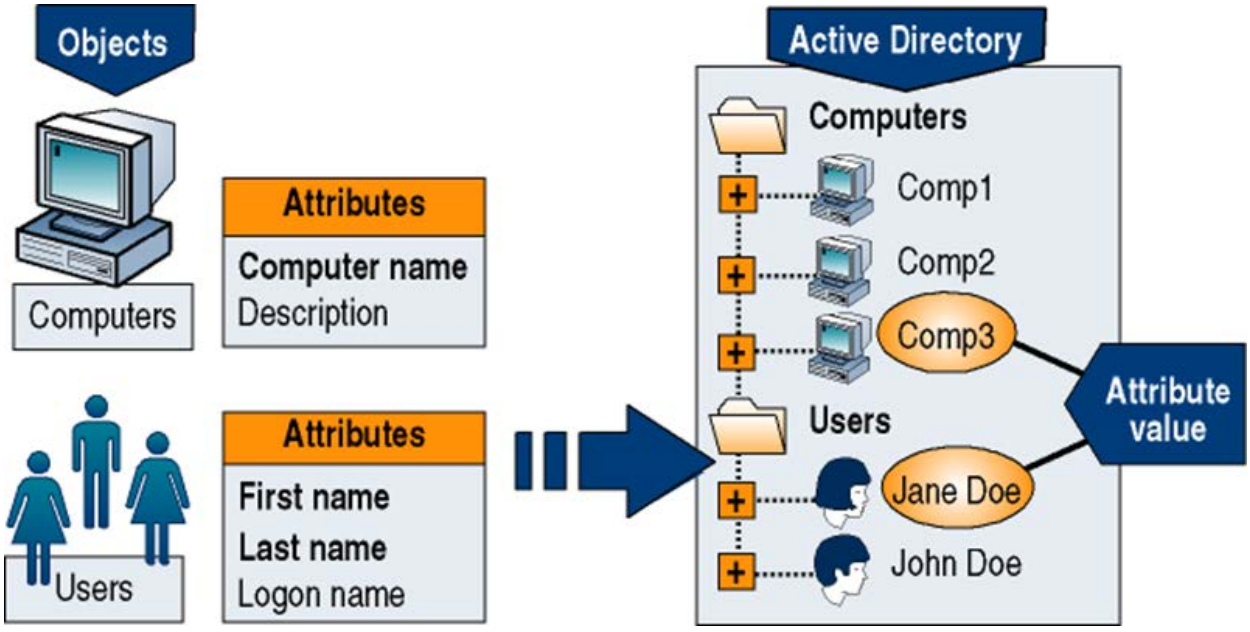
Cuprins

1.Noțiuni introductive. Problema.

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

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

Active directory este tehnologia creată de Microsoft pentru serviciul director Windows Server. Active Directory păstrează şi pune la dispoziţie informaţii despre resursele unei reţele, organizate în obiecte. Fiecare obiect are un set de atribute asociate, informaţii care identifică şi descriu obiectul.



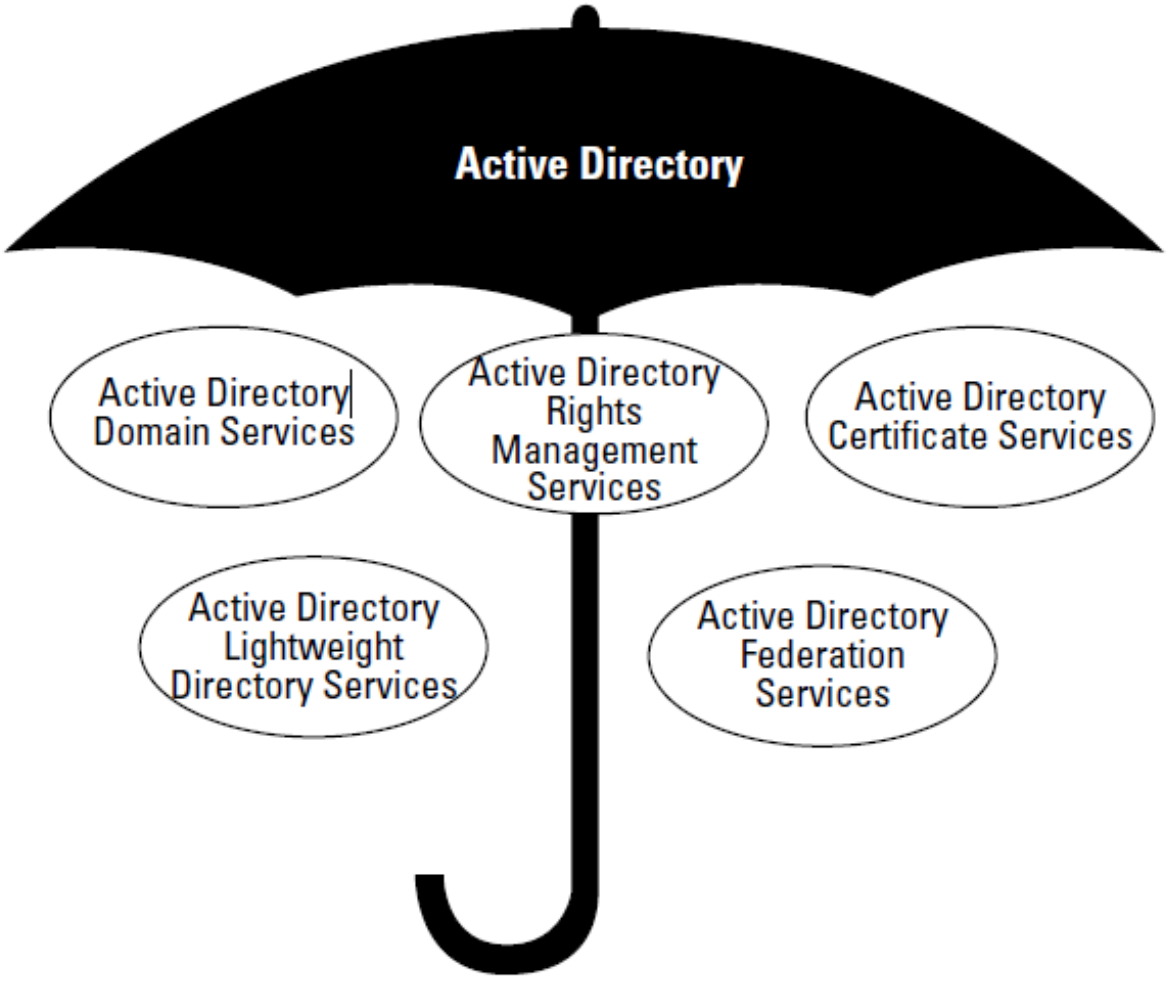
Arhitectura Active Directory

Sursa: site Microsoft

1.1. Serviciile Active Directory

Începând cu Windows Server 2003, Microsoft a creat o aplicație serviciu director separată de Active Directory numita *Active Directory Application Mode* sau *ADAM*. ADAM a fost construită ca să se adreseze nevoilor organizațiilor care vor să implementeze un serviciu director care nu necesită toate funcționalitățile pe care le oferă Active Directory.

Astfel toate aceste servicii separate sunt înglobate în Active Directory, care este ca o umbrelă sub care se desfășoară aceste servicii.

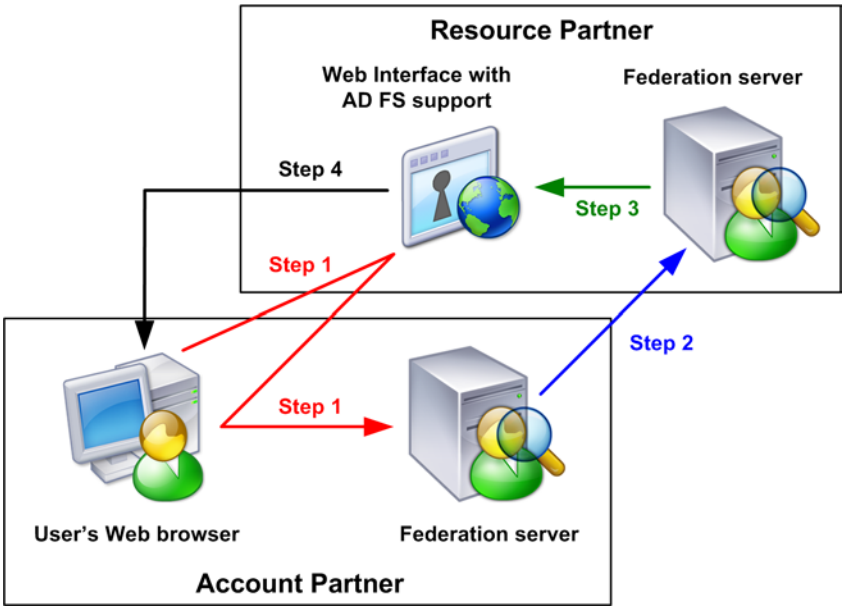


Serviciile Active Directory

Sursa: Active Directory For Dummies, 2nd edition

Active Directory Federation Services

Începând cu varianta R2 al Windows Server 2003, Microsoft a inclus un pachet software opțional numit *Federation Service*. Acesta oferă serviciul *Single Sign-on* (SSO) care ajută la minimalizarea numărului de ID-uri de logare si parole pe care utilizatorul trebuie să le introducă și simplifică modul în care utilizatorii pot accesa resursele în alte medii IT. Acest soft face acum parte din Windows Server si a fosr redenumit *Active Directory Federation Services* sau *AD FS*.

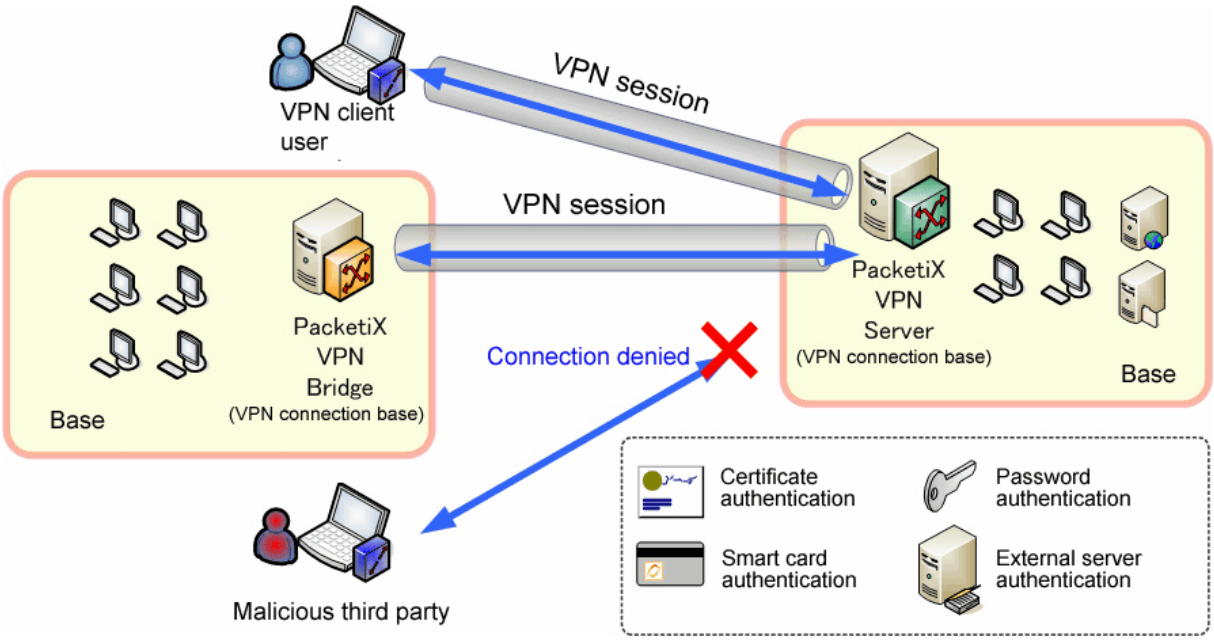


Active Directory Federation Services

Sursa: www.support.citrix.com

Active Directory Certificate Services

Certificate Services au fost în software-ul Windows Server de mai mult timp. Cu acest software se poate desemna o autoritate de certificare care poate emite chei publice folosite în autentificare prin smart cards sau criptarea datelor înainte de a fi trimise în rețea. Serviciul de certificare oferă de asemenea administrarea necesară acestor certificate astfel încât acestea pot fi reînnoite sau respinse.

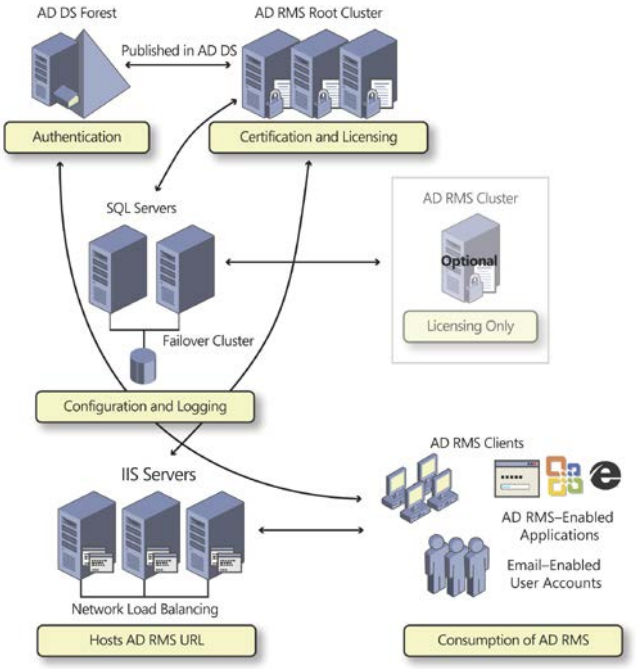


Active Directory Certificate Services

Sursa: www.plathome.com

Active Directory Rights Management Services

Administrarea utilizatorilor pentru a stabili anumite restricții în ceea ce aceștia fac cu datele a fost o problemă pentru cele mai multe organizații. Chiar dacă Active Directory a realizat un control în ceea ce privește dreptul de acces asupra unui document, nu se putea controla ce va face utilizatorul cu datele după ce acesta le accesează. Introducerea serviciului de management asupra drepturilor utilizatorilor a oferit organizațiilor controlul extins asupra documentelor. Spre exemplu un utilizator nu poate trimite prin e-mail un anumit document către utilizatori neautorizați.

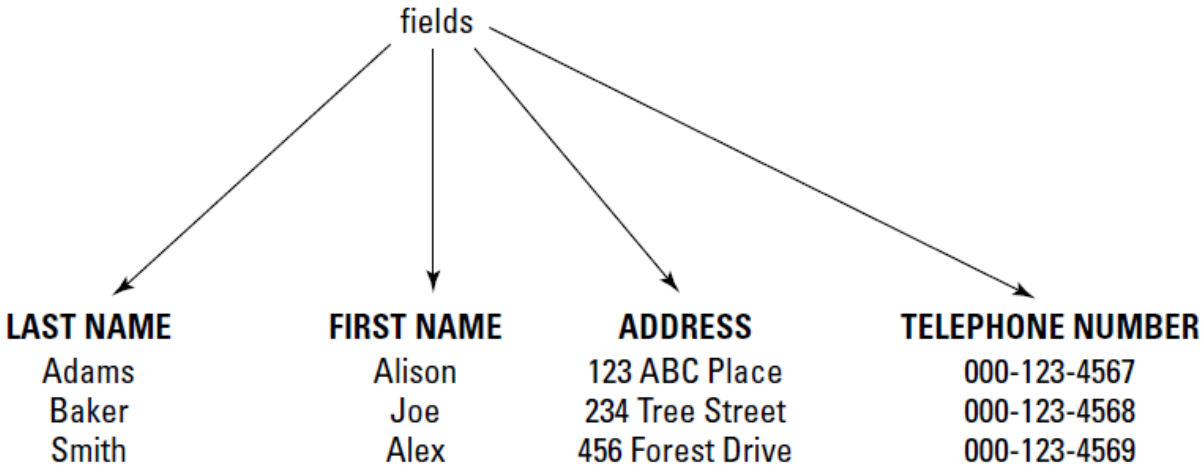


Active Directory Federation Services

Sursa: www.mscerts.programming4.us

1.2. Active Directory: director de informații

Informația este organizată în date care fac referință la obiecte, fiecare obiect având anumite seturi de atribute asociate. Să luăm spre exemplu informațiile din catalogul de telefoane Pagini Albe. Fiecare obiect din acst catalog reprezintă o adresa de locuință sau o firmă care conține informații precum numele, adresa sau numărul de telefon



Câmpurile de informații

Sursa: Active Directory For Dummies, 2nd edition

Capacitatea acestui catalog de a primi cât și de a modifica datele fac ca Active Directory să fie un serviciu director. De ce nu putem considera Active Directory o bază de date? Este cert că are anumite funcționalități comune bazelor de date incluzând stocarea, regasirea sau replicarea datelor, însă sunt anumite diferețe importante. În primul rând, serviciul de directoare este în mod normal optimiziat pentru citire deoare acestea reprezintă marea majoritate a operațiilor care sunt executate și de obicei datele nu se schimbă. Deasemena datele sunt structurate într-un mod ierarhic, lucru care permite atribuirea denumirii de serviciu director. Repetând analogia cu catalogul de telefoane, Pagini Aurii organizează obiectele în funcție de tipul de afacere. În acest mod se realizează căutarea mult mai rapid. Același lucru se poate spune și despre un serviciu director – obiectele se pot organiza în containere de informații care permit găsirea obiectelor mult mai ușor, în comparație cu o bază de date relațională cum ar fi Microsoft SQL Server, care este optimizată atât pentru citire cât și pentru scriere deoarece datele sunt des citite și scrise. Deasemenea o bază de date în general nu oferă un mod ierarhic de organizare a datelor așa cum se întâmplă în cazul serviciului director.

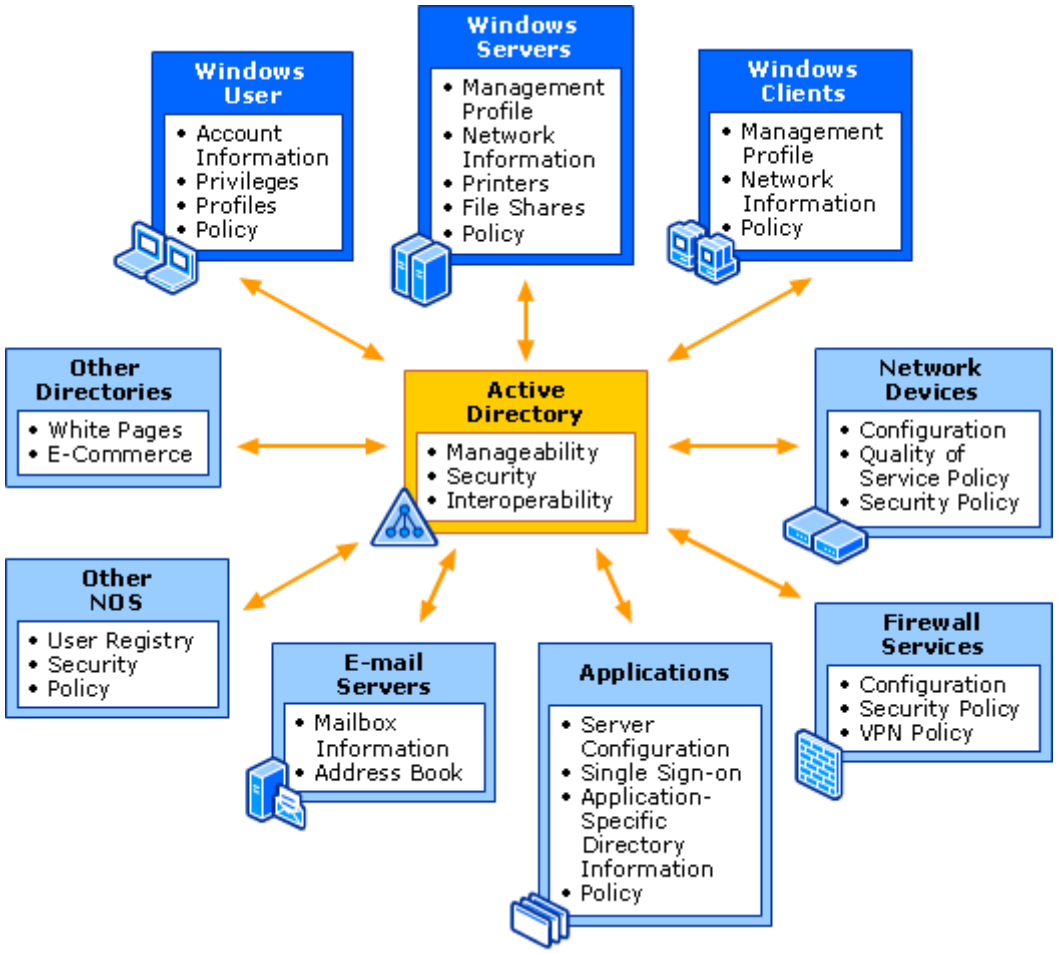
1.3. Structura Active Directory

Un serviciu director precum Active Directory permit stocarea obiectelor într-o structură ierarhică. Această structură este una din părțile care trebuiesc analizate atent dacă se dorește implementarea Active Directory. Această structură are două componente:

- **Partea logică:** structura logică oferă organizarea obiectelor. Aceste obiecte pot reprezenta utilizatori, calculatoare, grupuri și o varietate de alte entități care sunt în mediul IT. Această structură este în primul rând dependentă de modul în care se dorește administrarea infrastructurii IT cât și de modul în care este structurată organizația

- **Partea fizică:** toate serviciile de sub umbrela Active Directory sunt oferite de servere care rulează softul Active Directory. Aceste servere reprezintă obiecte fizice care trebuiesc plasate în rețea. După ce aceste servere sunt plasate, trebuie definit modul în care serverele vor comunica unele cu altele și cum vor fi direcționați utilizatorii către ele. Această topologie fizică este critică pentru o funcționare bună.

Dacă ne referim din nou la analogia cu catalogul de telefoane, dacă intrările nu sunt plasate în categoriile corecte (locuințe, restaurante, firme) nimeni nu poate găsi informația pentru a fi utilizată.



Structura logica si fizica Active Directory

Sursa: www.i.technet.microsoft.com

2. Functionalitati Active Directory

Active Directory ofera o serie de functionalitati. Dintre acestea vom descrie cautarea si gasirea facila prin administrare simplificata pe care o ofera, scalabilitatea si suportul standard pentru alte servicii.

2.1. Administrare simplificata

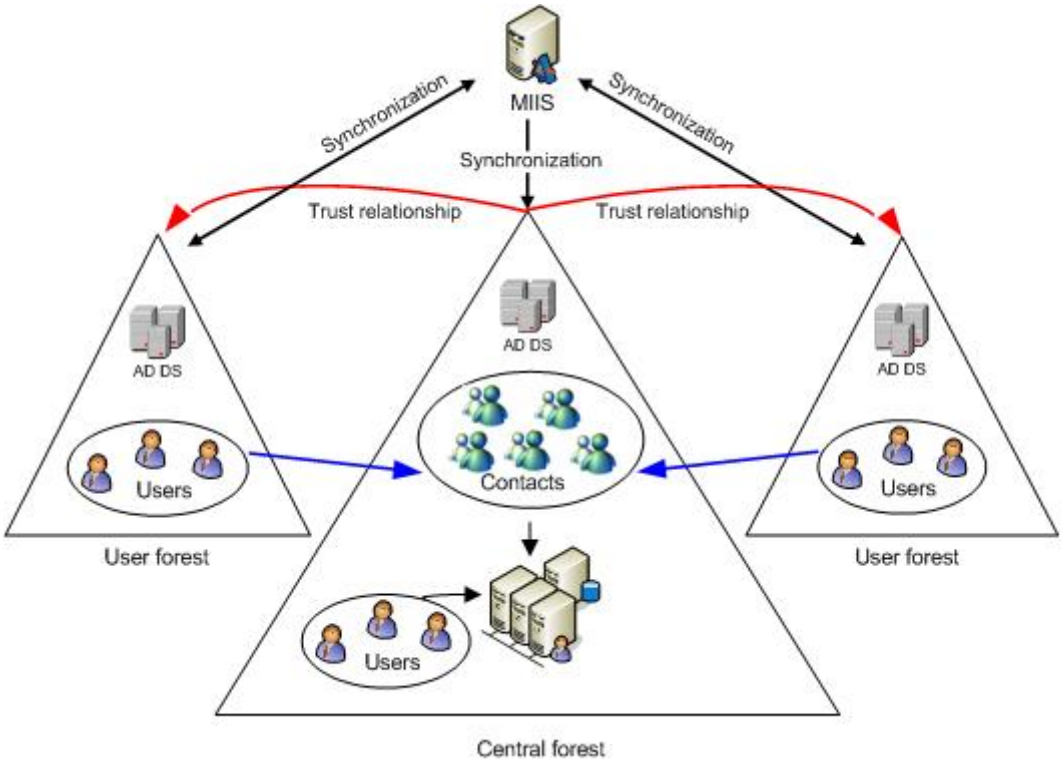
Active Directory este o implementare a serviciilor de directoare LDAP, folosită de Microsoft în cadrul sistemelor de operare Windows. Astfel „Active Directory” pune la dispoziția administratorilor un mediu flexibil cu efect global pentru: asignarea permisiunilor, instalarea programelor, înnoirea securității. Toate aceste operațiuni pot fi aplicate atât la rețele mici, cât și la rețele complexe.

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 proprietăţi, numite şi atribute. Unele obiecte sunt containere, deci conţin alte obiecte, inclusiv alte containere. De aici structura ierarhică Active Directory. La nivelul cel mai înalt al ierarhiei Active Directory se află forest (pădure). Un forest se compune din arbori (tree). La rândul lui un arbore este compus din domenii.

Domain controllerul detine toate configuratiile si proprietatile obiectelor din Active Directory.

Active Directory oferă posibilitatea de administrare a obiectelor si acces pentru toate resursele din rețea dintr-un singur punct. Folosind o singură bază de date, Active Directory oferă posibilitatea administrării centralizate a tuturor resurselor unei reţele.



Administrare Centralizata in Active Directory

Sursa: www.technet.microsoft.com

2.2. Scalabilitate

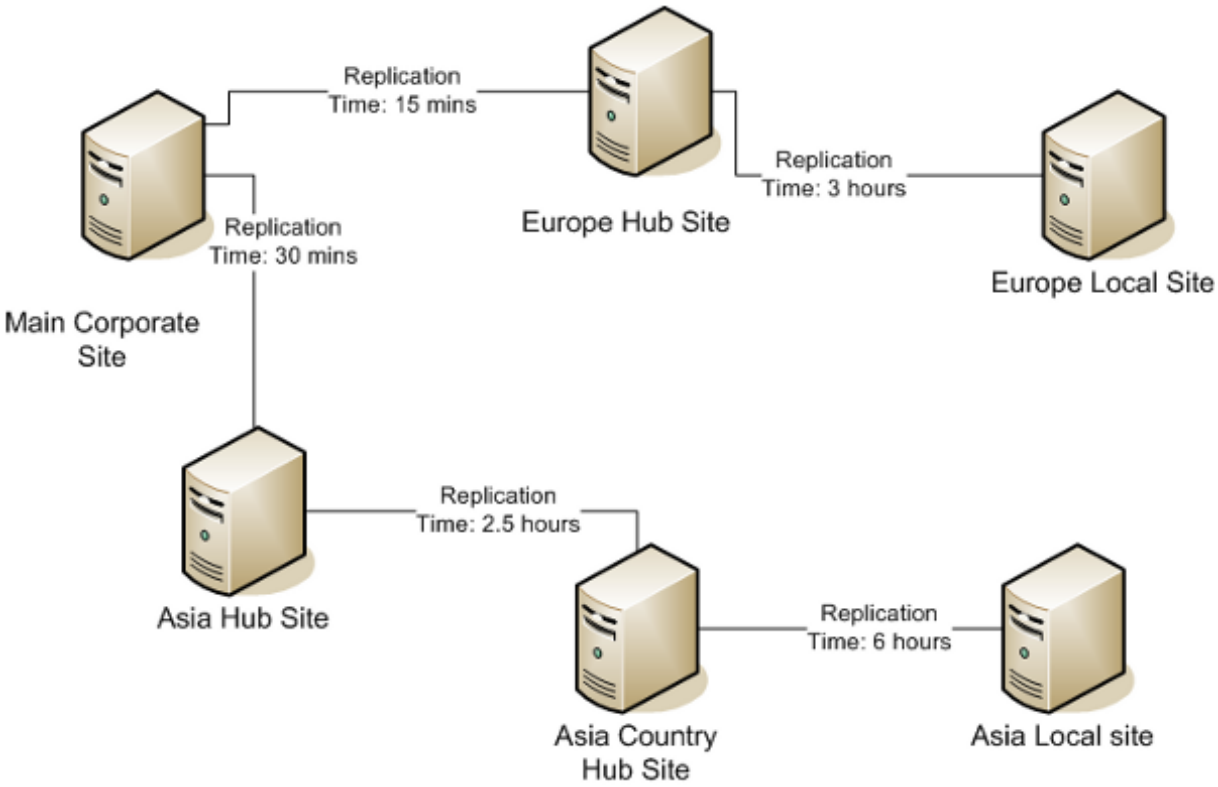
Stochează informația prin organizarea în secțiuni care permit stocarea unui număr nelimitat de obiecte.

Domeniile sunt scalabile: pot conţine un număr mic de calculatoare, dar pot găzdui la fel de bine mai multe mii de calculatoare.

Astfel directorul se poate extinde pentru a satisface cerințele diferitelor situații:

- **Instalări mici** cu un server și câteva sute de obiecte
  Pentru companiile mici si mijlocii sau organizatii mici.

- **Instalări mari** cu sute de servere și milioane de obiecte
  Pentru companii mari sau organizatii extinse.



Scalabilitate in Active Directory

Sursa: www.technet.microsoft.com

2.3. Suport standard pentru alte servicii

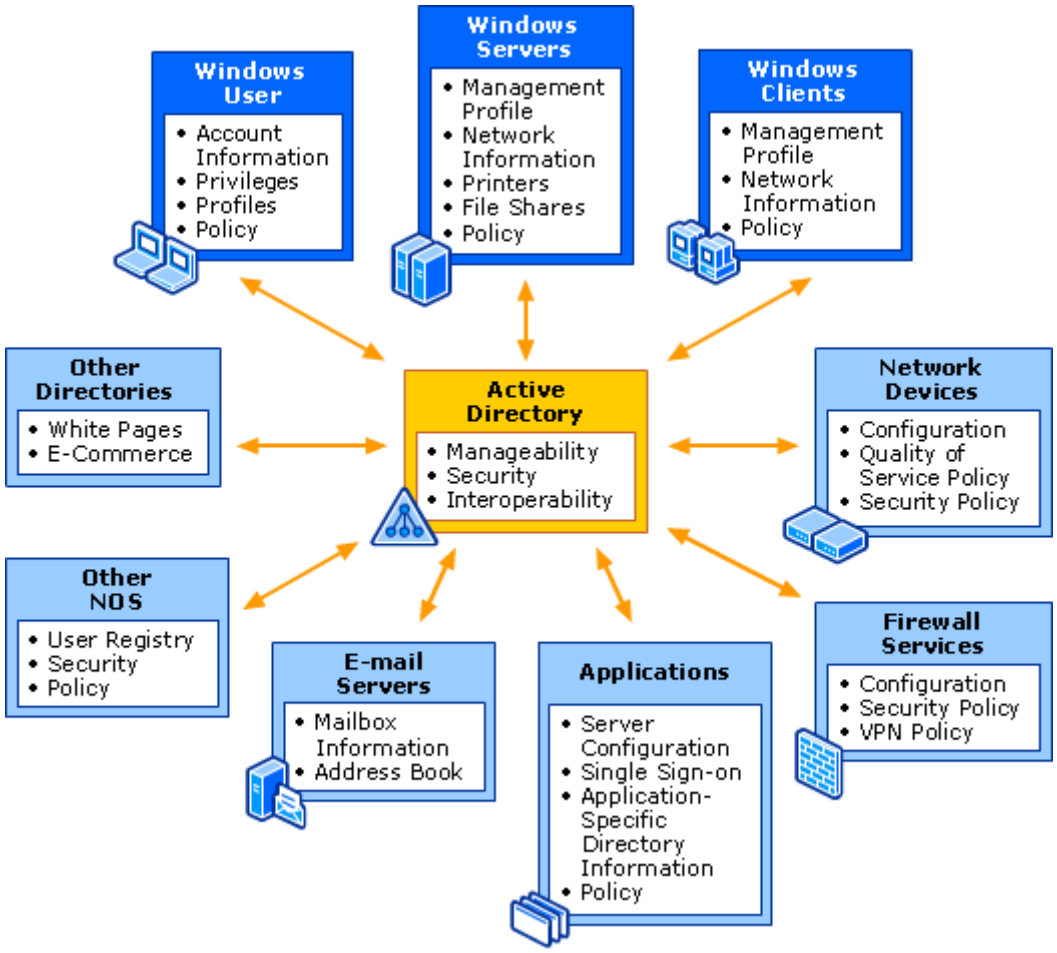
Active Directory integrează conceptele Internetului într-un spațiu de nume cu serviciul director Windows. Acesta oferă posibilitatea unificării și managementul multiplelor spații de nume.

Pentru numele sistemului se utilizează DNS. Sistemul de nume de domeniu (abreviat DNS, în engleză Domain Name System) este un sistem distribuit de păstrare și interogare a unor date arbitrare într-o structură ierarhică.

Active Directory schimbă informații cu orice aplicație sau director care utilizează LDAP sau HTTP.

Avantajul pe care il ofera este legat de posibilitatea clienților de a modifica tabelele DNS în mod dinamic. Prin folosirea serviciului DDNS se elimină nevoia de a desemna pe cineva care să redenumească serviciile.

Orice obiect din Acive Directory se poate afișa ca o pagina HTML în browser.



Suport standard pentru alte servicii in Active Directory

Sursa: www.i.technet.microsoft.com

3. Principiii de organizare

3.1. Obiecte in Active Directory

Active Directory (AD) - este o ierarhie de câteva obiecte, unde obiectele se împart în trei categorii: resurse (ex: imprimantă), servicii (ex: poșta electronică), resurse umane (ex: utilizatori, grupe de utilizatori). Scopul tehnologiei "Active Directory" este de a pune la dispoziție informații despre aceste obiecte, organizarea obiectelor, controlul accesului, setarea securității..

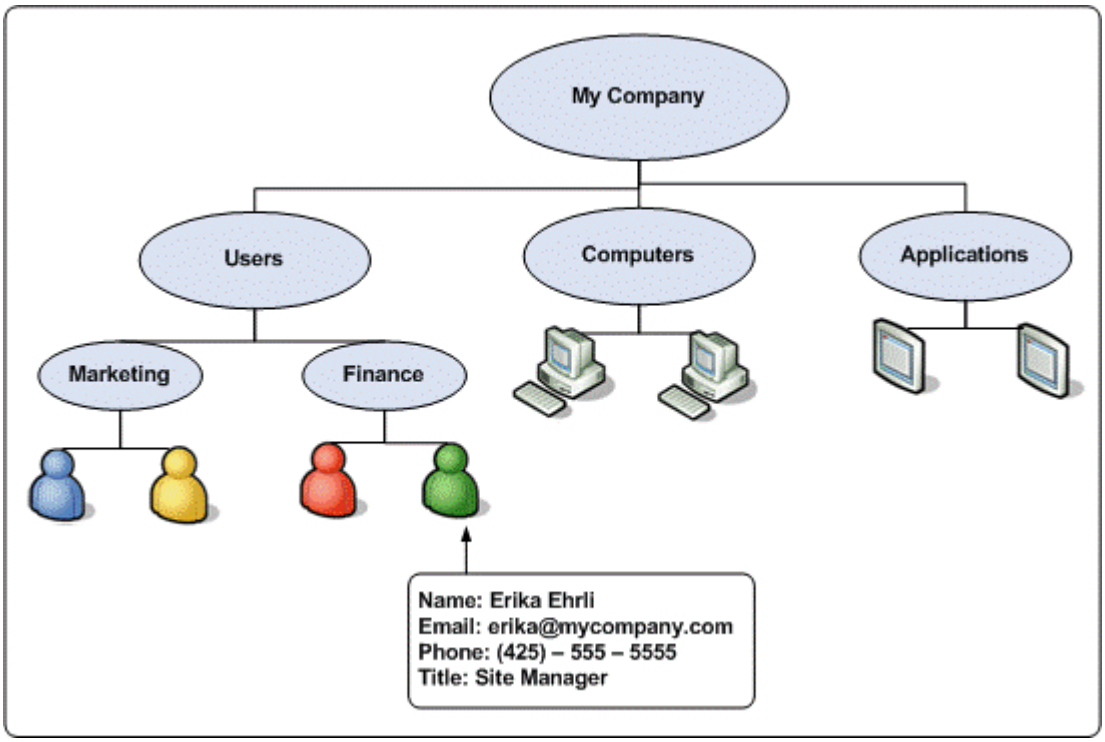
Fiecare obiect indiferent de categorie reprezintă o entitate și atributele ei, unde 'entitate' poate fi - "Utilizator", "Calculator", "Imprimantă", "Aplicație" sau "Resursă Partajată". Mai mult decât atât, un obiect poate să conțină și alte obiecte. Atributele obiectului (structura de bază a obiectului în sine) sunt definite de o "schemă", care la rîndul ei definește și tipul obiectelor care pot fi stocate ca subobiecte în obiectul dat.

Totul pare complicat, însă în realitate e mai simplu decât pare. Aceste reguli au fost inventate numai cu scopul ca să poată cumva să reflecte situațiile întâlnite de noi în fiecare zi. Pentru a le înțelege, e mai bine să ne închipuim o situație care trebuie cumva reflectată în lumea IT, și printr-o metodă de pseudo-inducție vom ajunge exact la ceea ce a fost expus mai sus.

O "schemă" e compusă din două tipuri de obiecte (sau meta-datele schemei): "clasa" și „atributele". Aceste metadate există cu scopul de a extinde sau modifica schema. Din motiv ce metadatele schemei sunt parte din obiectul pe care-l descriu (parte din obiectul la care a fost aplicată schemă), odata ce am modificat schema, efectele se raspândesc pe toate obiectele din Active Directory la care a fost aplicata schema dată - prin această caracteristică "Active Directory" este foarte puternic dar și foarte periculos - o modificare nechibzuită poate duce la efecte nedorite de nivel global (cum ar fi: scăderi din salariu de nivel esențial, imposibilitatea îndeplinirii lucrului oamenilor care sunt

dependenți de efectele modificării). O schemă creată poate fi numai deactivată, nu și ștearsă - deoarece crearea sau modificarea unei scheme este bazată pe motive serioase.

Mai jos este prezentata o figura in care sunt prezentate principalele tipuri de obiecte din Active Directory.



Obiecte in Active Directory

Sursa: www.i.msdn.microsoft.com

3.2. Structura logică

In Active Directory resursele sunt organizate într-o structură logică.

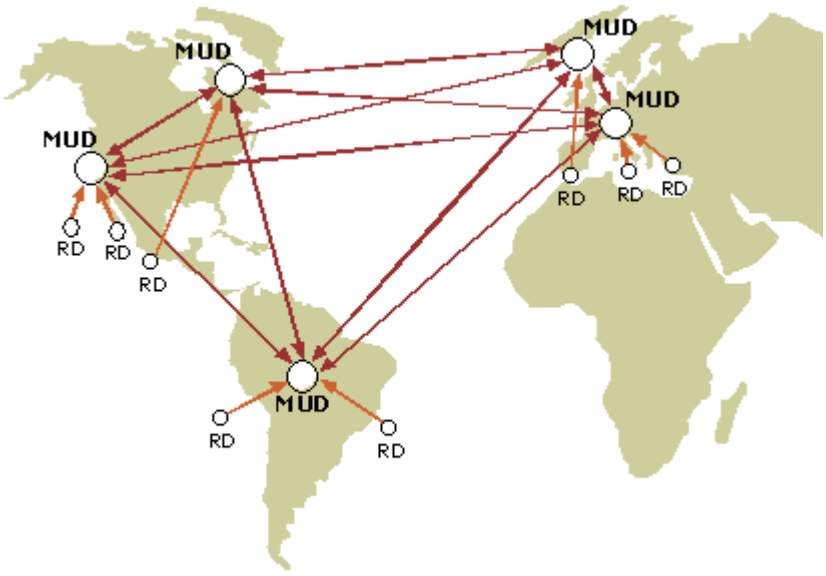
Resursele fiind grupate logic, structura fizică a reţelei devine transparentă utilizatorilor .

Structura logică este separată de structura fizică. Legătura dintre structura logică Active Directory şi structura fizică a reţelei se obţine prin folosirea conceptului şi a obiectului site.

Obiectul site din Active Directory descrie aşezarea fizică, geografică a reţelelor care găzduiesc resursele descrise prin obiecte din Active Directory.

Site-urile conţin obiecte numite subreţele (subnets). Obiectele site sunt folosite în legătură cu obiectele Group Policy, uşurează descoperirea resurselor, controlează replicarea Active Directory şi gestionează traficul în reţea. Site-urile pot fi legate unele de altele prin aşa-numitele legături între site-uri (site link). Din punct de vedere fizic un site constă în general din una sau, eventual, mai multe subreţele interconectate la viteză mare în care funcţionează servere controlere de domeniu.

Astfel resursele se găsesc după nume indiferent de locația unde se află.

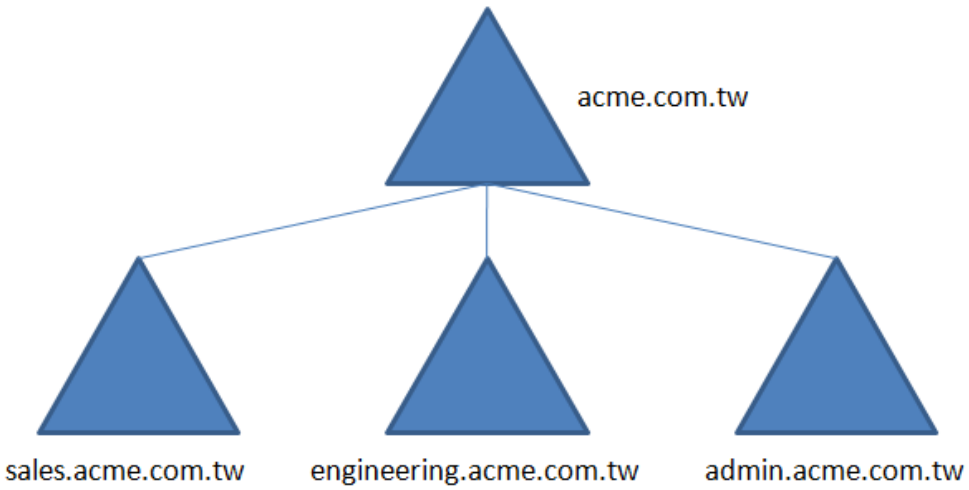


3.3. Domeniul

Conform terminologiei Microsoft, domeniul este reprezentat dintr-un grup de calculatoare care fac parte dintr-o reţea şi care folosesc în comun aceeaşi bază de date în care sunt reprezentate resursele reţelei. Domeniul este administrat ca entitate distinctă, cu reguli şi proceduri comune pentru toate calculatoarele care îl compun.

Domeniile sunt recunoscute prin nume. Calculatoarele membre ale domeniului respectă politica de securitate a domeniului. În plus, domeniul oferă şi soluţia administrării centralizate a tuturor resurselor reţelei, indiferent unde ar fi ele distribuite: administrarea bazei de date a domeniului este în fond soluţia pentru administrarea tuturor resurselor reprezentate prin obiecte înscrise în această bază de date. O singură operaţie de logon în domeniu (deschidere de sesiune) este suficientă pentru ca un utilizator să fie recunoscut în domeniu şi să aibă acces la resursele domeniului, în limita permisiunilor şi a privilegiilor de care dispune.

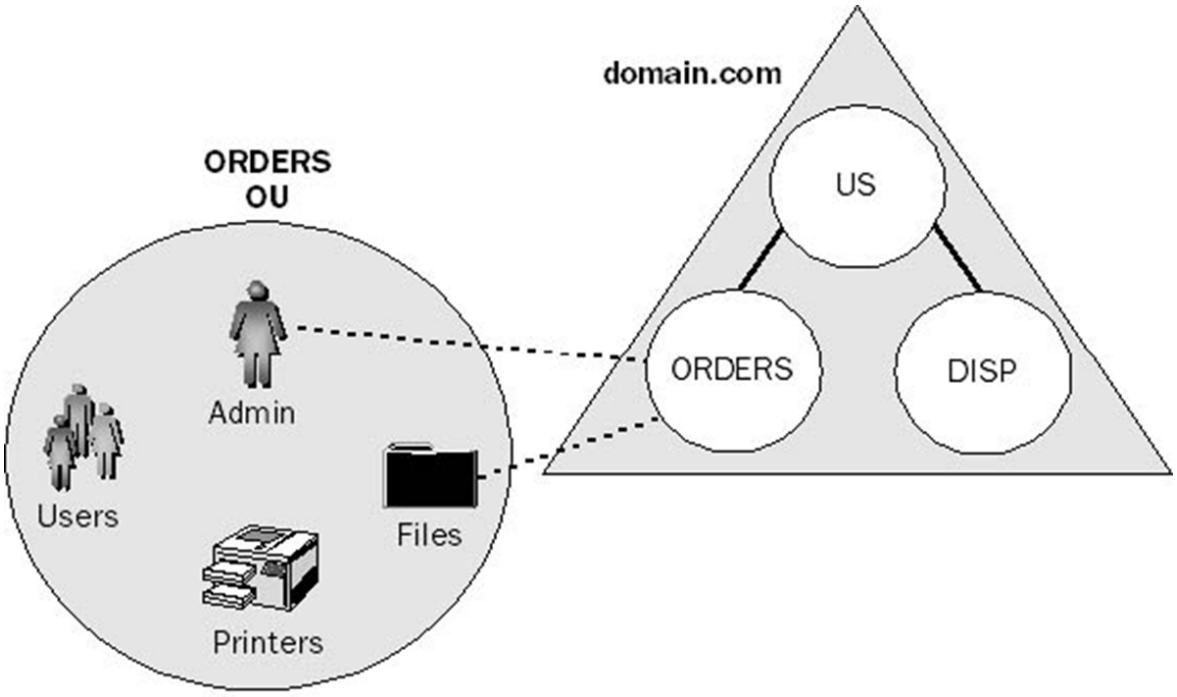
Reprezentarea grafică a domeniului este triunghiul care sugerează frontiera de administrare, frontiera de securitate şi aşezarea ierarhică a componentelor sale. Domeniul este construit în jurul unui controler de domeniu (domain controller). Într-un domeniu trebuie să existe cel puţin un controler de domeniu. El deţine toate informaţiile despre domeniu, despre resursele reţelei şi este serverul folosit pentru autentificarea în domeniu (logon în domeniu). Crearea unui domeniu se obţine prin crearea controlerului de domeniu. Instalarea serviciului Active Directory pe un server îl transformă în controler de domeniu.



3.4. Unitatea organizationala

Unitatea organizationala este un container folosit pentru a organiza obiecte în cadrul unui domeniu în grupuri administrative logice.

Aceasta furnizează un mod de a delega administrarea utilizatorilor şi a resurselor.



Obiecte in Active Directory

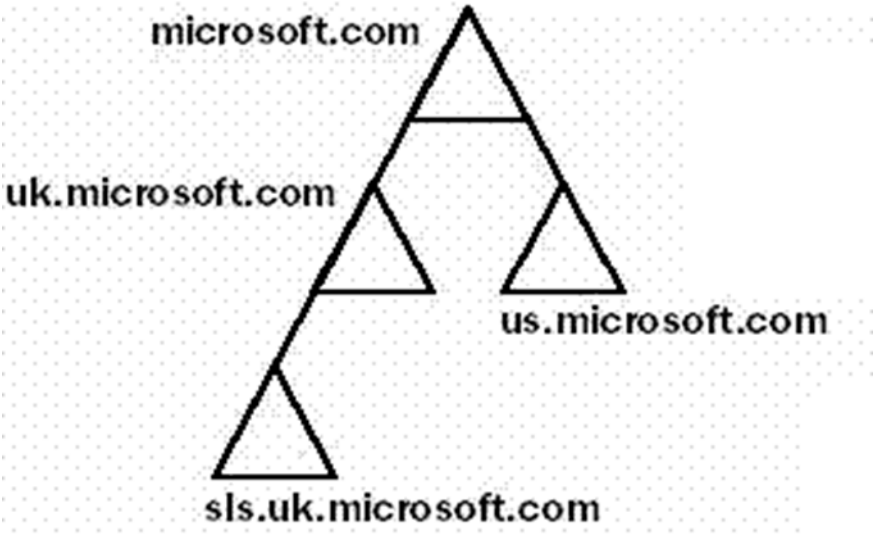
Sursa: www.msdn.microsoft.com

3.5. Arborele (Tree)

Un arbore (tree) este o grupare de domenii din acelaşi spaţiu de nume, deci o convenţie relativă la modul în care sunt denumite acestea. Între domenii există relaţii 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 relaţiile dintre ele: în acest caz sunt relaţii de genul „părinte-copil” (parent-child) sau domeniu-subdomeniu.



Structura de domenii cu un singur arbore

Sursa: www.microsoft.com

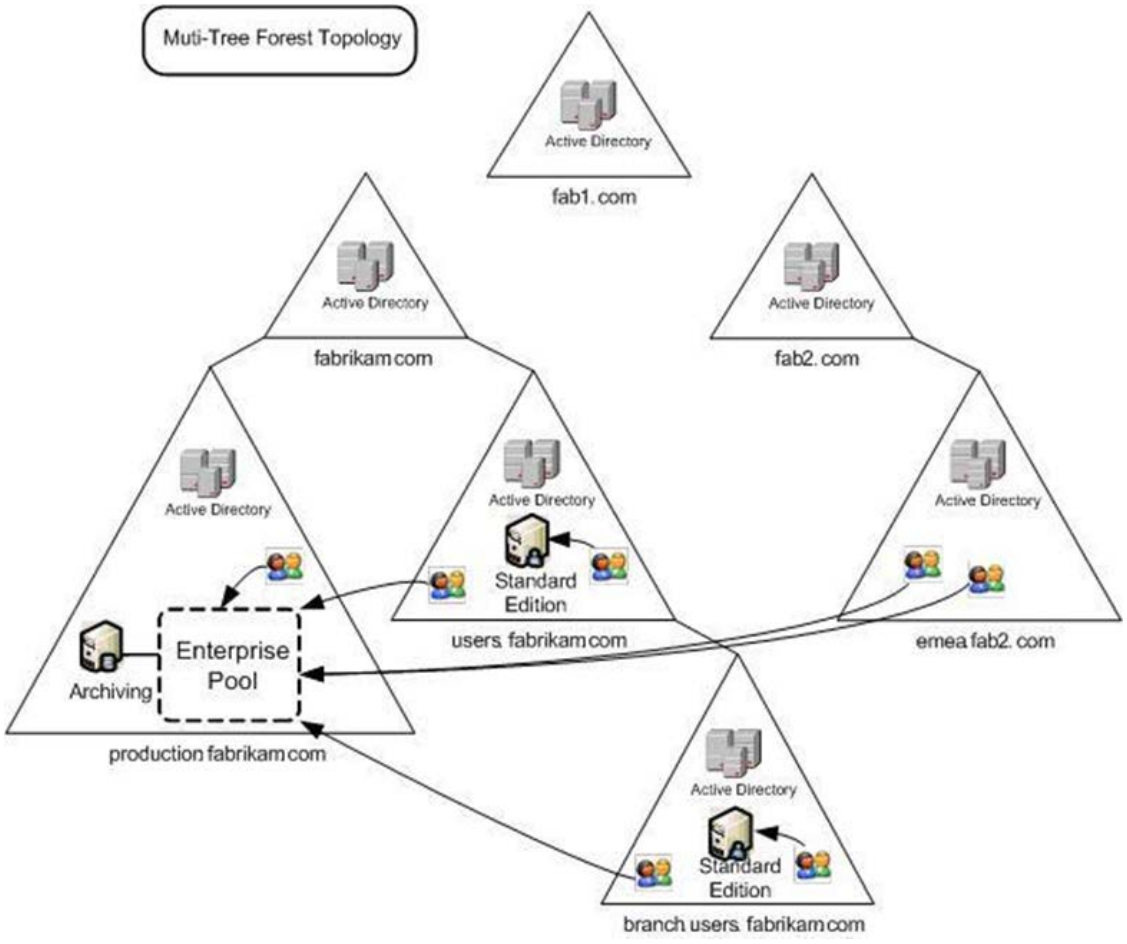
3.6. Pădurea (forest)

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

În această figură este reprezentat un forest cu cu două arborescenţe. Fiecare dintre ele are un spaţiu de nume independent.

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

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

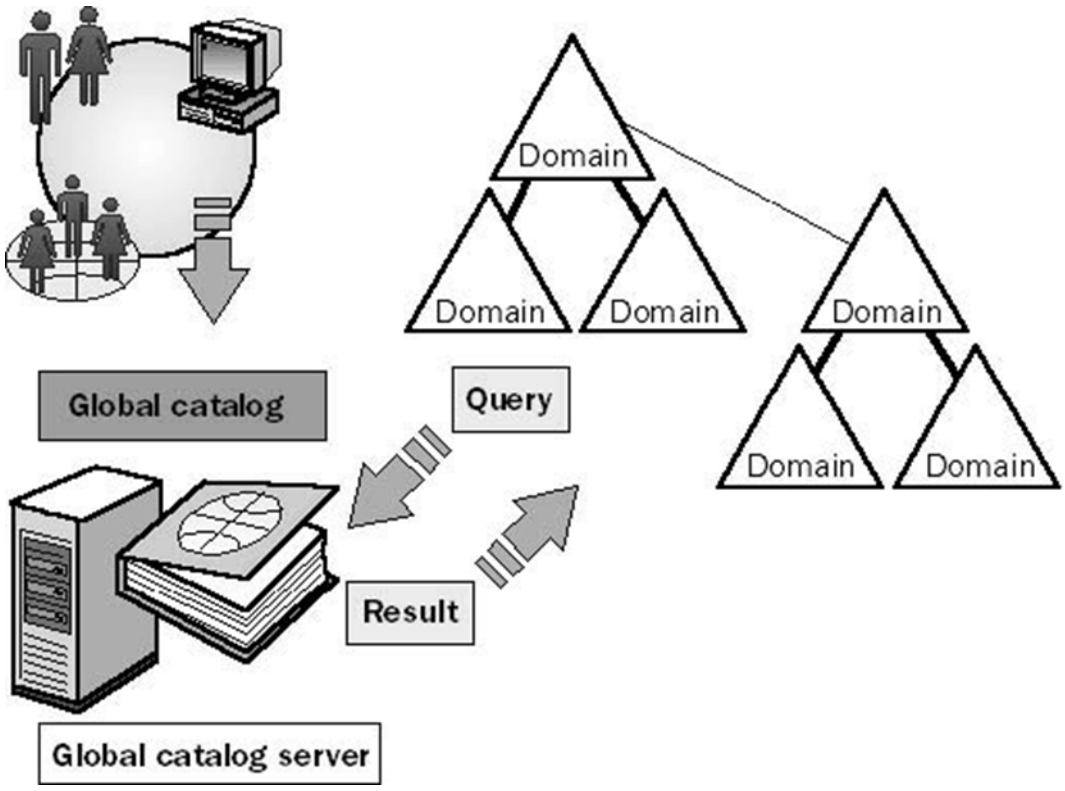


Padure cu doua arborescente in Active Directory

3.7. Catalogul global

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

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



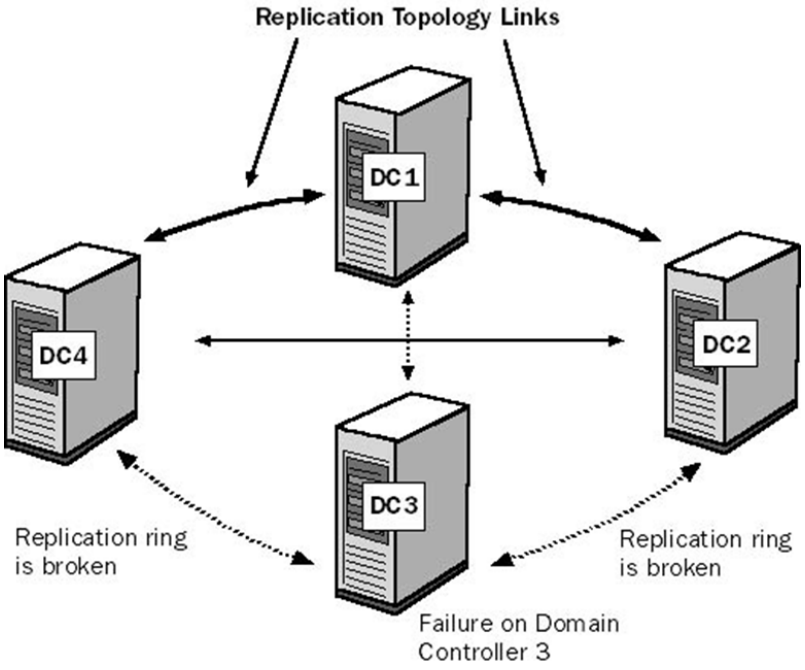
4. Replicarea

Serviciul Active Directory Service funcţionează pe baza informaţiile stocate pe controlerele de domeniu. Pentru existenţa unui domeniu este nevoie de un controler de domeniu.

Într-un domeniu pot funcţiona unul sau mai multe controlere de domeniu. Fiecare controler de domeniu deţine un exemplar al bazei de date Active Directory. Modificările efectuate într-un exemplar vor fi sincronizate cu celelalte exemplare Active Directory, în aşa fel încât toate exemplarele de pe toate controlerele din domeniu să fie identice. Operaţia de sincronizare a exemplarelor Active Directory este o replicare multi-master.

Fiecare controler de domeniu deţine un exemplar master al domeniului, adică fiecare exemplar poate fi modificat, prin crearea şi ştergerea de obiecte, prin modificarea valorilor asociate proprietăţilor (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 împărţită, separată din punct de vedere logic în partiţii. Fiecare partiţie este o unitate de replicare şi poate avea propria topologie de replicare.



5. Concluzii

In aceasta lucrare a fost prezentat Serviciul Director Active Directory. Principalele avantaje oferite de implementarea Active Directory în retea sunt descrise în continuare.

- Autentificarea utilizatorilor – permite identificarea fara echivoc a fiecarui utilizator al retelei pe baza de utilizator si parola unica.
- Autorizarea accesului la resurse – pentru fiecare resursa din retea pot fi configurate liste de acces care specifica explicit permisiunile pe care le au utilizatorii sau grupurile asupra resursei respective.
- Administrarea centralizata a tuturor serverelor si statiilor de lucru din retea.
- Aplicarea consistenta a unor politici de securitate în cadrul retelei. Acesta din urma este în particular un avantaj foarte important în procesul de securizare al retelei.
- Active directory ajuta la administrarea resurselor intr-un mod centralizat.
- Permite instalarea unor politici de securitate.
- Permite instalarea programelor in functie de grupul din care face parte utilizatorul.
- Permite utilizatorilor gasirea rapida a resurselor din intreaga retea.
- Domeniile sunt scalabile: pot conţine un număr mic de calculatoare, dar pot găzdui la fel de bine mai multe mii de calculatoare.

6. Bibliografie

1. Active Directory® For Dummies,® 2nd Edition, Published by Wiley Publishing, Inc.
2. Active Directory Cookbook 3rd Edition Dec 2008, Laura E. Hunter and Robbie Allen
3. Wikipedia
4. Active Directory: Designing, Deploying, and Running Active Directory by Brian Desmond, Joe Richards, Robbie Allen and Alistair G. Lowe-Norris (Mar 22, 2013)
5. Microsoft Technet Platform