SPŠ Jozefa Murgaša, Hurbanova 6, Banská Bystrica

Operačné systémy

Operačný systém Microsoft Windows Server 2008

Windows Active Directory

Služby Active Directory

Obsah:

Vypracoval: Ing. Jaroslav Karban Banská Bystrica 5.1.2012

Windows Server 2008 - Služba Active Directory Domain Services

1. Adresárové služby

1.1 Princíp adresárových služieb

Aplikácia zabezpečujúca tzv. adresárové služby spravuje hierarchickú databázovú štruktúru, v ktorej sa uchovávajú informácie o pomenovaných objektoch určitého systému. Pomenovanie objektov je v súlade s touto štruktúrou.

1.2 Objekty ako dáta pre adresárové služby

Rôzne systémy definujú funkčné prvky, ktoré v objektovom ponímaní nazývame ***objektami***. Objekt má svoju jednoznačnú identifikáciu (názov objektu, častejšie jednoznačný systémový identifikátor objektu - ***objekt ID***) v systéme a definované vlastnosti (atributy), ktorými je detailnejšie špecifikovaný. V oblasti operačných systémov implementovaných do sieťových technológií môžme za objkety považovať:

a/ Používateľa systému
b/ Prihlasovací účet
c/ Jednotlivé sieťové prvky (napr. počítač)

1.3 Databázové systémy adresárových služieb

1.3.1 Databáza LDAP (Lightweight Directory Access Protocol)

Protokolom LDAP je riadený prístup k dátam na adresárovom serveri. Jednotlivé záznami sú usporiadané do hierarchickej stromovej štruktúry podobne ako v adresárovej architektúre. Každý záznam je definovaný svojím menom a atributmi Jednotlivé záznami sú organizované do objektových tried.

1.3.2 Hierarchický objektový model LDAP

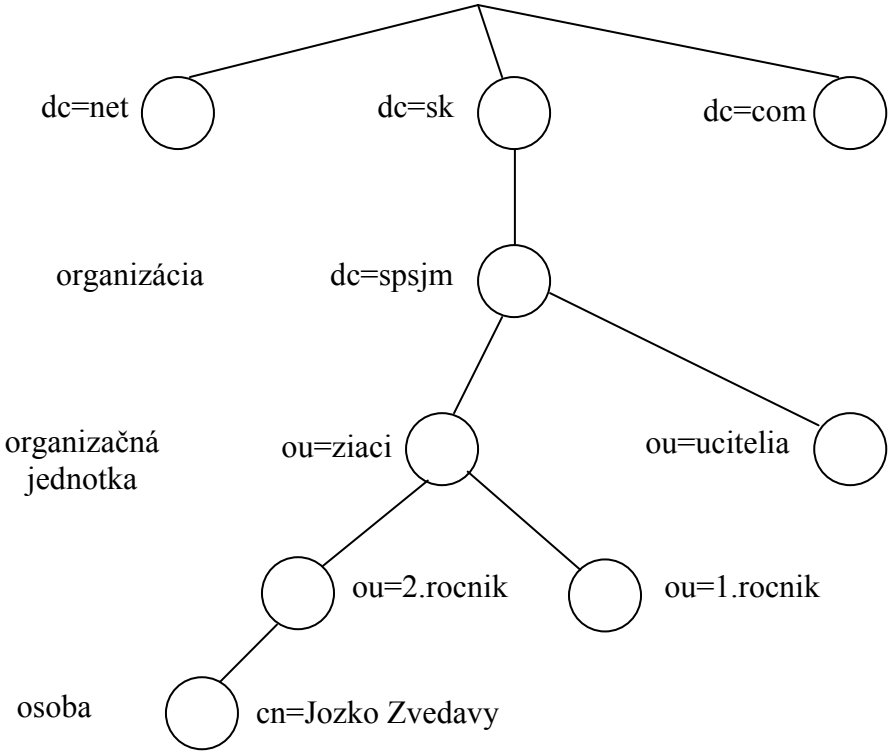
Databáza LDAP má hierarchiskú stromovú štrukrúru. Základnou informačnou jednotkou je objekt. Objekt jednoznačne pomenovaná kolekcia atribútov.

Objekt:
Pomenovanie objektu ***dn (Distinguished Name)***
Identifikátor objektu ***uid (Uniq ID)***

atributy objektu:
typ atribútu ***cn (Common Name)***
pomenovanie organizačnej jednotky ***ou (Organization Unit)***
domény, subdomény ***dc (Domain Component)***

Zoradenie atribútov vyjadruje pozíciu objektu v hierarchickej štruktúre smerom k jej vrcholu.

DN: cn= Jozko Zvedavy,ou=2.rocnik,ou=ziaci,dc=spsjm,dc=sk



1.3.3 Typy hierarchických organizačných štruktúr

a/ Funkčne orientovaná hierarchia

Je založená na funkciách pracovníkov organizácie. Štruktúra je nezávislá od geografického umiestnenia závodu, pobočky apod. (napr.: administrativa, vyroba, predajca zasobovac,……).

b/ Organizačne orientovaná hierarchia

Zohľadňuje organizačnú štruktúru na oddeleniach a vyšších organizačných celkoch.

c/ Hierarchia podľa geografického umiestnenia

Vytvárajú sa organizačné jednotky pre jednotlivé mestá poprípade štáty

d/ Hybridná hierarchia

Kombinácia štruktúr založených na geografickom umiestnení a organizačnej štruktúre

1.3.4 Výmena dát medzi databázami adresárových serverov

Na export a import dát medzi adresárovými databázami sa používa formát súborov označovaný ako LDIF (Data Interchange Format)

Druhý používaný formát dát je DSML (Directory Services Markup Language), založený na XML.

2. Aktívne adresárové služby Microsoft – Active Directory

Server so systémom Active Directory sa nazýva radič domény. Radičom domény je server na ktorom je nainštalovaný doménový radič - DC (Domain Controller). . Na jednej sieti môže pracovať viacej doménových radičov. Všetky sieťové objekty sú potom umiestnené v databáze Active Directory. Doménový radič spolu s centrálnym usporiadaním sieťových objektov v databáze AD vytvára v sieťach Microsoft doménové usporiadanie sietí typu klient – server.

Active Directory je databáza sieťových objektov založená na adresárových službách LDAP.

2.1 Doména a adresárové služby

Doménové usporiadanie siete s AD prináša nasledujúce výhody:

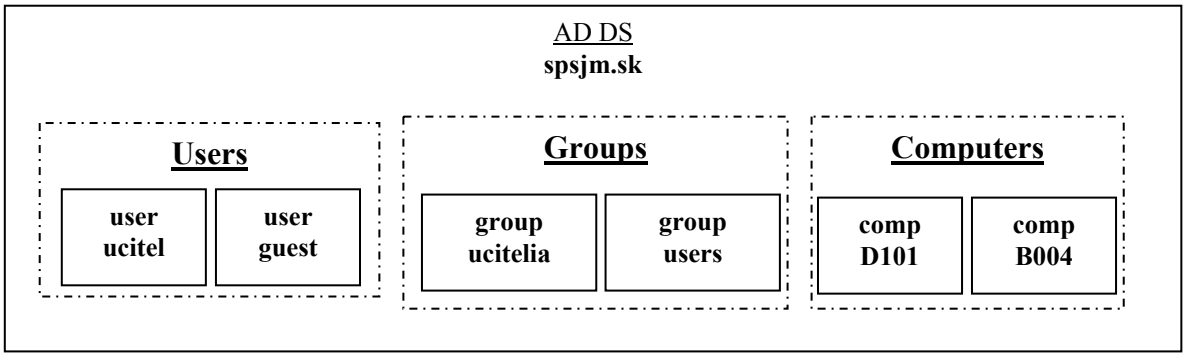
a/ Centrálna správa prostriedkov siete
b/ Jednotný prihlasovací proces ku všetkým prostriedkom podľa príslušného oprávnenia.

Do oblasti centrálnej správy v rámci domény patrí napr.:

a/ Správa používateľských účtov
b/ Správa účtov počítačov
c/ Správa zásad zabezpečenia

2.2 Účel služby Active Directory Domain Services (AD DS)

Služba AD DS poskytuje distribuovanú databázu, všetkých sieťových objektov danej domény. Správca domény vytvára logické hierarchiké usporiadanie týchto sieťových objektov. Spravuje interakciu medzi používateľom a doménou, pravidlá prihlasovania používateľov a ich overovania. Jednotlivé AD (domény) replikujú databázové údaje.



2.3 Spustenie služby AD DS

Na spustenie služby AD DS je potrebná inštalácia doménového radiča. Pretože DC je srdcom služby AD DS je dôležitá jeho bezpečnosť a stabilita. Akékoľvek poškodenie alebo nestabilita činnosti DC má kritické dôsledky pre všetkých pripojených klientov, serverov a bežiacich aplikácií.

3. Radič domény (DC-Domain Controller)

Radič domény je inštalovaná rola servera, ktorá má na starosti všetky činnosti spojené so sieťovými objektami domény a ich centrálnou správou. Riadí všetky funkcie Active Directory. Vo Windows server 2008 je možné inštalovať niekolko typov radičov domény.

3.1 Radič domény s možnosťou zápisu (Domain Controller)

Radič domény na správu a použitie v serveroch s dostatočnou fyzickou bezpečnosťou. Je to základný typ radiča pre bežnú inštaláciu.

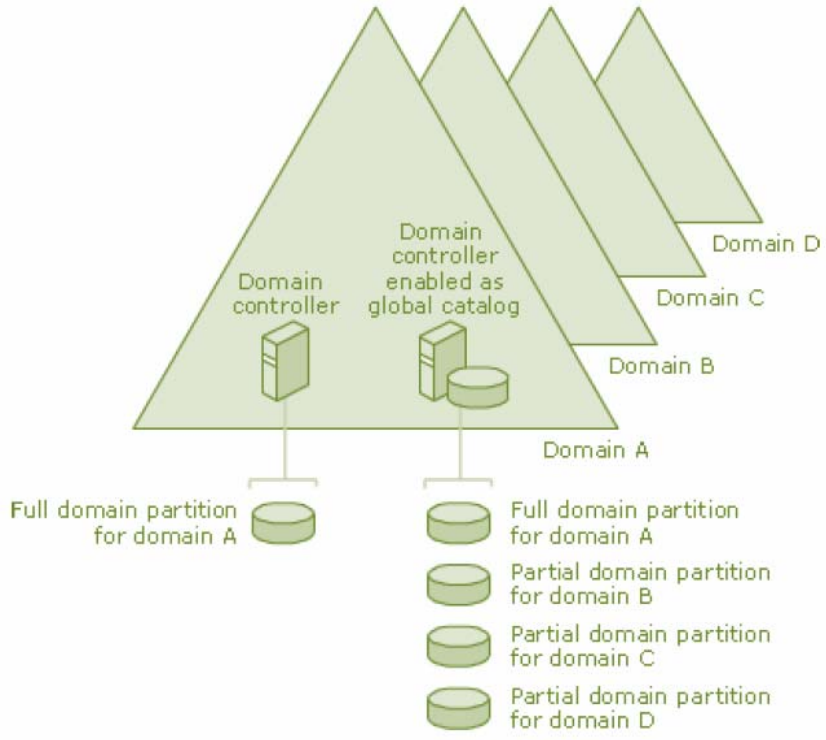
3.2 Řadič domény len na čítanie (Read Only Domain Controller)

Radič domény len na čítanie bez možnosti zapisovania je novým typom DC od Windows Server2008. Firmy alebo len firemné pobočky , ktoré nemôžu zaistiť fyzickú bezpečnosť doménového radiča majú možnosť inštalvať DC bez možnosti zápisu.

3.3 Globálny katalóg (Global Catalog)

Radič domény označovaný ako globálny katalóg je typom, ktorý ukladá kópie objektov Active Directory v adresároch hostiteľskej domény. Globálnym katalógom je štandardne prvý nainštalovaný radič domény minimálne jeden na doménu.

Globálny katalóg uchováva úplnú repliku objektov AD DS vlastnej domény a čiastočnú repliku všetkých ostatných domén lesa. Sú to objekty najčastejšie používané vo vyhľadávacích operáciách pužívateľov. Umožňuje rýchle vyhľadávanie informácií o objektoch AD bez potreby dotazov na iné domény.



4. Doménová štruktúra sietí

4.1 Doména a hierarchia domén

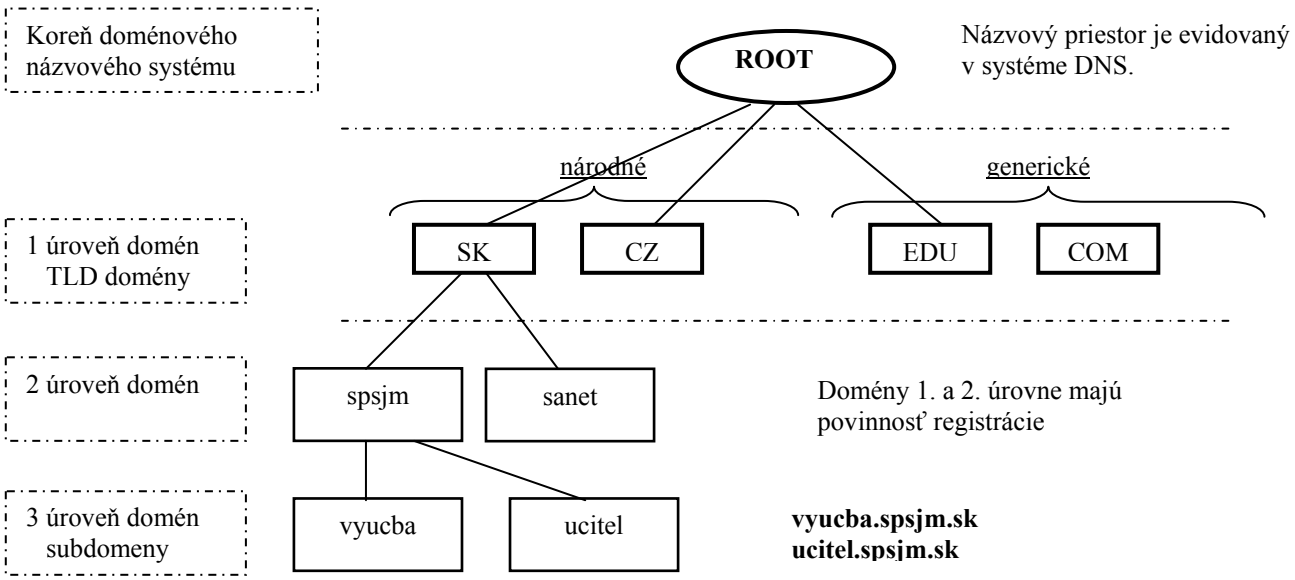
4.1.1 Doména

Doména Active Directory je logické zoskupenie počítačov zdielajúcich spoločnú databázu danej AD. Tvorí základnú jednotku AD a tvorí ju minimálne 1 doménový radič. V jednej doméne býva jeden počítač ako radič domény DC s Windows serverom a niekoľko podriadených klientských staníc s rôznymi OS, poprípade tzv. členské servre, ktoré nie su DC ale poskytujú len svoje prostriedky. Technické prostriedky domény môžu byť geograficky vzdialené ale sú objektami Active Directory na doménovom počítači.

Niektoré vlastnosti domény:

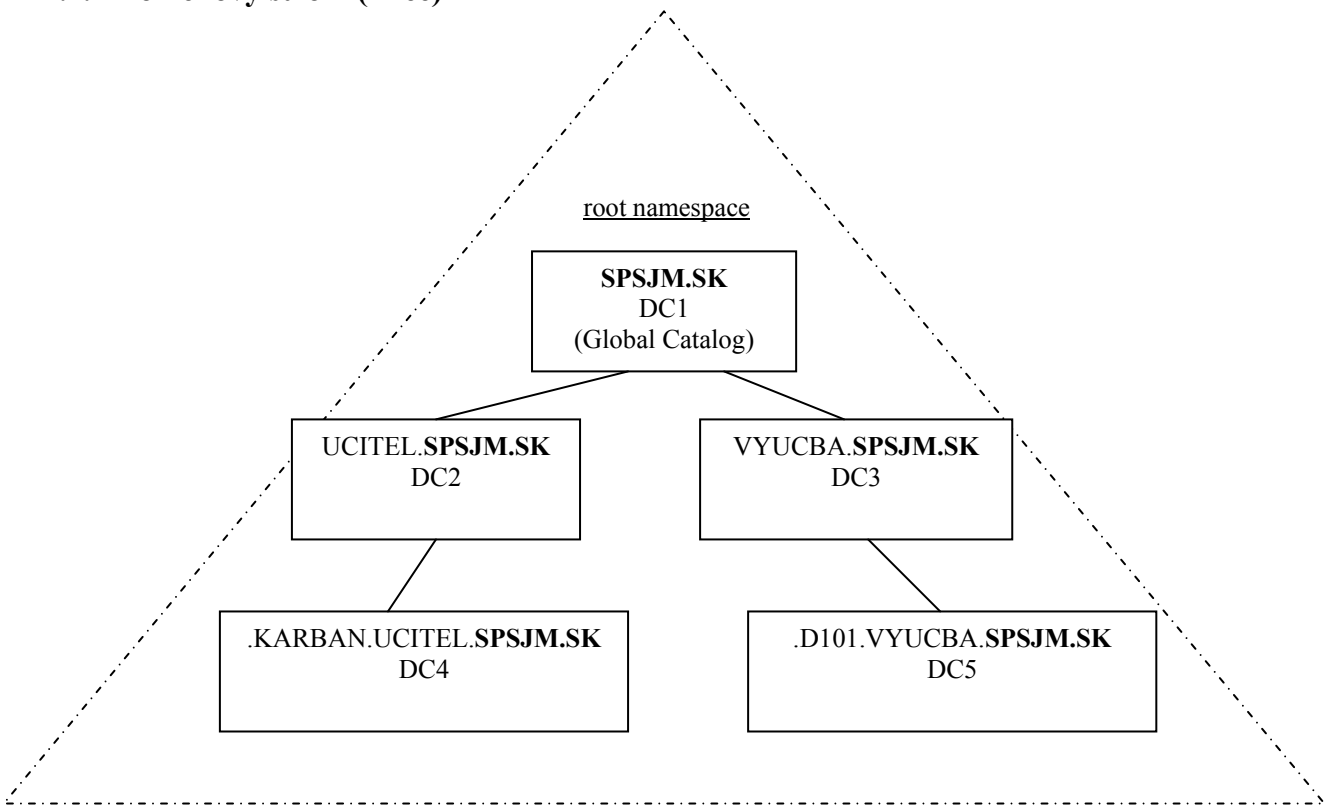
a/ Doména tvorí bezpečnostnú a replikačnú hranicu vymedzenú názvovým priestorom označenia domény
b/ Má definovaný jednoznačný názov. Názov je evidovaný v systéme DNS
c/ Sú v nej definované vlastné zásady zabezpečenia
d/ Vytvára vzťahy dôvery s ostatnými doménami

4.1.2 Hierarchická štruktúra domén – názvy domén



4.2 Lesy a stromy domén

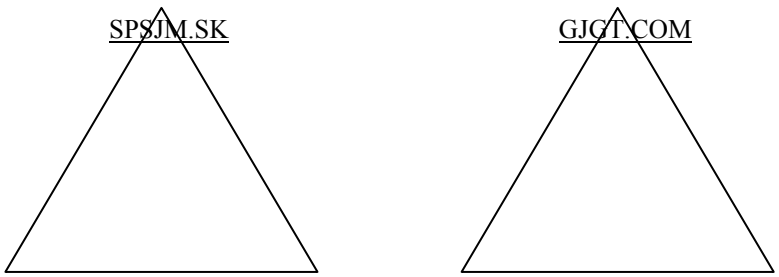
4.2.1 Doménový strom (Tree)



Doménový strom je hierarchické členenie domén, vytvorené vzťahom rodič – potomok. Všetky domény stromu zdielajú spoločný názvový priestor daný koreňom vytvorenej hierarchie (root namespace) – je to súvislá štruktúra názvov.

4.2.2 Les (Forest)

Les domén vytvára nesúvislý názvový priestor. Les vytvárajú samostatné stromy domén. Les môže obsahovať jeden alebo viacej stromov domén. Je to skupina doménových stromov.



.

5. Vzťahy dôvery (trust relationship)

Všetky funkcie vykonávané medzi doménami (prihlasovanie a overovania, replikácie a iné) sú činnosti vyžadujúce bezpečnosť. V technológiách microsoft je používaný ***vzťah dôvery*** medzi doménovými objektami

Na vzťah dôvery pozeráme z dvoch hľadísk:

a/ Vzťah dôvery podľa organizačnej štruktúry objektov

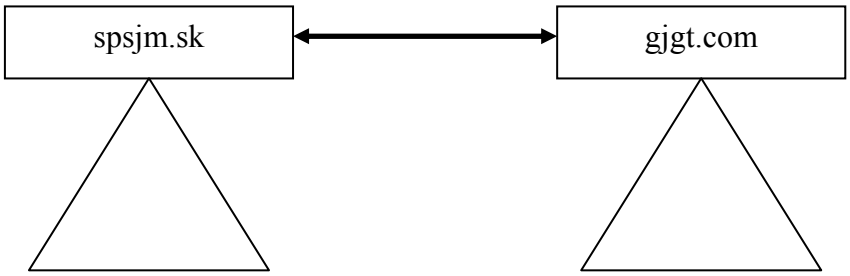
b/ Vzťah dôvery podľa funkcionality objektov

5.1 Vzťah dôvery podľa organizačnej štruktúry

Vzťahy dôvery medzi doménami podľa ich organizácie.

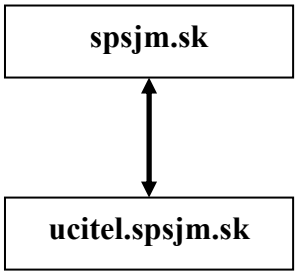
5.1.1 Domain root trust

Vzťah medzi dvoma rozdielnymi doménovými koreňmi jedného forestu.



5.1.2 Parent-child trust

Vzťah dôvery medzi doménami vo vzťahu rodič-potomok.



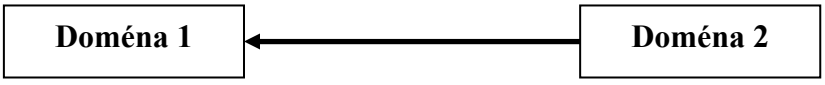
5.1.3 Forest trust

Vzťah dôvery domén jedného lesa k doménam iného lesa.

5.2 Vzťah dôvery podľa funkčnosti

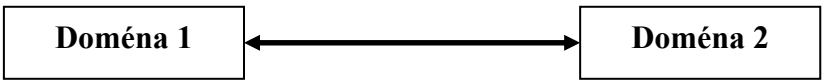
5.2.1 One-way trust

Jednocestná dôvera. ***Doména 1*** umožní prístup používateľom ***domény 2***, ale nie naopak.



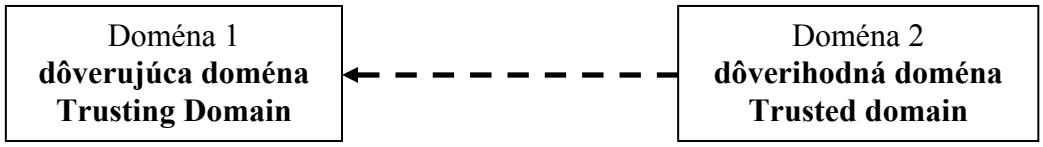
5.2.2 Two-way trust

Dvojcestná dôvera (vzájomna dôvera) medzi dvomi doménami. Používatelia obidvoch domén majú prístup do druhej domény.



5.2.3 Trusting domain

Dôverujúca doména. Umožní prístup z domény, ktorej dôveruje.

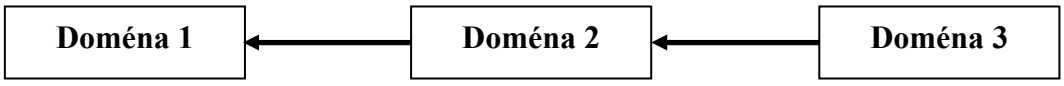


5.2.4 Trusted domain

Doména, ktorej je dôverované – dôverihodná doména. Používatelia tejto domény majú prístup do domény, ktorá jej dôveruje.

5.2.5 Transitive trust

Tranzitívna dôvera. Dôvera, ktorá môže presiahnuť dôveru medzi dvomi doménami k iným doménam v strome domén.



6. Organizácia Active Directory

6.1 Fyzická organizácia

AD rozlišuje ***logickú a fyzickú organizáciu***. Fyzická organizácia je založená na skutočnom umiestnení sieťových prostriedkov podľa sietí a podsietí Siete a podsiete ohraničujú sieťové prostriedky na základe rozsahov IP adries na rozdiel od logického členenia, ktoré definuje hierarchický názvový priestor. Priestor IP adries sieťových uzlov a názvový priestor spolu nesúviasia. Jedna sieť môže obsahovať viacej domén a naopak jedna doména môže preklenúť viacej sietí.

6.1.1 Sieť

Za sieť považujeme skupinu počítačov s IP adresami z jednej alebo viacerých podsietí.

6.1.2 Podsieť

Podsieť je fyzickou organizačnou podmnožinou siete so špecifickým rozsahom IP adries a maskou podsiete danými principmi vytvárania podsietí.

6.2 Logická organizácia

Základnou jednotkou logickej štruktúry Active Directory je **doména**. Logická štruktúra kopíruje organizačnú štruktúru firmy (organizácie). Nezaujíma sa o fyzické umistnenie sieťových objektov. Jednotlivé prvky Active Directory sa označuú ako **objekty**. Objekty zastupujú skutočné sieťové prostriedky v doméne. Objekty určené pre aplikovanie bezpečnostných pravidiel (user, group) majú pri vytvorení pridelený bezpečnostný identifikátor ***SID (Security Identifiers)***. Pri aplikovaní týchto objektov napr. v oprávnení k súborovému systému NTFS sú evidované pod SID. Po odstránení používateľa alebo skupiny sa definované opravnenie zobrazuje pod SID.

6.2.1 Les (Forest)

6.2.2 Strom domén (Tree)

Nejvyšší v dané hierarchii, skládá se z minimálně jedné domény. Určuje pomyslné hranice, kde môže správca zasahovať. V pôvodnom nastavení obsahuje strom len jednu doménu, nazývanú ako ***koreňová doména.***

6.2.3 Doména (Domain)

Doména je logické zoskupenie počítačov s jednoznačným označením názvu domény. Doména používa vlastné zásady zabezpečenia pre všetky členské sieťové prostriedky, ktoré zdielajú jednu spoločnú adresárovú databázu Active Directory. Doména obsahuje počítače, tlačiarne, používateľov a organizačné jednotky.

Medzi základné vlastnosti patrí vytváranie vzťahov dôvery s ostatnými doménami, aplikovanie zásad zabezpečenia a overovanie totožnosti (identity) používateľských účtov.

Overovanie identity:

a/ Autentizácia – overenie používateľa, ktorý sa snaží o pripojenie do adresárového servera. Spôsoby overenia:

- ***anonýmne overenie*** .. overenie bez informácii o pužívateľovi (anonymous)
- ***jednoduché overenie*** .. overenie na základe existujúceho účtu a definovaného hesla
- ***PKI overenie*** … overenie na základe digitálnych certifikátov

b/ Autorizácia – proces autorizácie sa spúšťa po pozitívnom overení používateľa. Výsledkom autorizácie je pridelenie nadefinovaných oprávnení prístupu k jednotlivým zdrojom systému, platných pre prihláseného používateľa.

5.2.4 Kontajner

Objekty sa zoskupujú do **kontajnerov**. Kontajner je objekt Active Directory, v ktorom sú uložené ďalšie kontajnery alebo iné objekty.

Preddefinované kantajnery:

- BuiltIn
Preddefinované miestne skupiny automaticky preddefinované systémom Windows

- Computers
Účty počítačov ako členov domény

- Domain Controllers
Počítače s radičom domény

- Users
Používateľské účty a spoločné globálne skupiny (Domain Admins, Domain Users)

5.2.5 Organizačná jedntka (OU – Organization Unit)

Na zoskupovanie objektov do organizačných skupín sa používa objekt s názvom organizačná jednotka (OU). OU uľahčuje správu veľkého množstva objektov. V hierarchickom členení OU sa odráža organizačná štruktúra. Na úrovni OU môžu byť uplatňované skupinové politiky zabezpečenia delegovaním právomocí. V OU sa môžu zoskupovať rôzne typy objektov.

Pre vytváranie OU v AD platia určité pravidlá a obmedzenia.

5.2.6 Doménový používateľ (Domain User)

Používateľ v AD DS je definovaný vytvoreným účtom s používateľským názvom a heslom. V rámci vytvoreného účtu je možné zadať nepovinné položky (atributy), ktoré bližšie špecifikujú používateľa.

5.2.7 Doménová skupina (Group)

Skupiny umožňujú organizačné zoskupenie používateľov za účelom hromadného pridelovania oprávnení členom skupiny alebo len k organizácii požívateľov bez bezpečnostných požiadaviek.

A. Delenie skupín podľa bezpečnosti:

a/ Distribučná skupina (Distribution group)

Táto skupina slúži na vytváranie nezabezpečených zoznamov používateľov napr. skupiny pre komunikačné účely (e-mail). Táto skupina nemá pridelený bezpečnostný identifikátor SID

b/ Skupiny zabezpečenia (Security group)

Tieto skupiny slúžia na riadenie prístupu k prostriedkom systému – definovanie oprávnení. Skupiny majú podobne ako používatelia pridelené SID.

B. Delenie podľa rozsahu platnosti:

a/ Miestna doménová skupina (Domain Local Group)
Definované pravidlá sú aplikované len na miestnu doménu.
b/ Globálna skupina (Global Group)
Pravidlá sú aplikované na ktorúkoľvek doménu doménovej štruktúry.
c/ Univerzálna skupina (Universal Group)
Pravidlá sú aplikované v každej doméne, ktorej je používateľ členom.

5.2.8 Počítač (Computer)

Objekt reprezentuje počítač v sieti s potrebnými informáciami. V AD sa vytvára automaticky po priradení počítača do domény.

5.2.9 Tlačiareň (Printer)

Zverejnené zdielané tlačiarne použiteľné v rámci AD.

6. Úložisko dát Active Directory

Databáza adresárových služieb AD je uložená v niekoľkých sôboroch. Ich umiestnenie sa rieší voľbou ponúkanou pri inštalácii doménového radiča. Zásady skupiny a niektoré iné informácie sú uložené v systémovom adresári SYSVOL.

7. Služby Active Directory

Active Directory ponúka prostriedky pre správu objektov a vzťahov medzi nimi v rámci organizácie . Adresárové služby AD ponúkajú niekoľko funkcií.

7.1 Služba Active Directory Domain Services (AD DS)

Služba Active Directory Domain Services (AD DS), v minulosti označovaná ako Active Directory Directory Services centrálne uchováva informácie o všetkých objektoch uložených v doménovej štruktúre. Pomocou tejto služby je možné efektívne centrálne spravovať používateľov, skupiny, počítače, tlačiarne, aplikácie a iné objekty registrované v adresárovej službe. Služba AD DS umožňuje jednotné nastavenie politík zabezpečenia pre danú doménu.

Všetky zmeny vykonané nad objektami AD je možné zaznamenávať (auditovať) na prípadné sledovanie daných zmien.

7.1.1 Inštalácia služby

Na inštaláciu služby používame príkaz dcpromo.exe. Po spusťení sa objaví wizard s nasledujúcou postupnosťou krokov inštalácie. Server s AD a DNS službou musí mať nastavenú pevnú nemennú IP adresu.

a/ Zaradenie domeny

aa/ do existujúceho lesa domém (pridanie do existujúcej doménovej štruktúry)
- ďalší DC v existujúcej doméne
- nová doména v existujúcom lese

ab/ vytvoriť novú doménu v novom lese

b/ Názov domény

ba/ Zadanie plne kvalifikovaného názvu domény (FQDN) pre DNS
bb/ Názov domény pre NetBIOS

c/ Úroveň funkcií pre spoluprácu s ostatnými doménami

Spolupráca s DC iných systémov Windows 2000, 2003, 2008

d/ Ďalšie voľby pre inštaláciu DC

da/ Inštalácia DNS servera
db/ DC s funkciou Global catalog
dc/ DC ako Read-only

e/ Cesta k databáze AD

7.2 Služba Active Directory Lightweight Directory Services (AD LDS)

Služba AD LDS v minulosti označovaná jako Active Directory Application Mode je určená na poskytovanie adresárových služieb pre aplikácie. Službu AD DS je možné pre aplikácie, ktoré potrebujú používať službu AD DS tým že ukladajú dáta do jej databázy, nahradiť službou AD LDS. AD LDS sprístupní aplikácii LDAP databázu vytvorením konkrétnej inštancie AD LDS pre danú aplikáciu.

7.3 Služba Active Directory Certificate Services (AD CS)

Väčšina organizácií využíva certifikáty na overenie identity používateľov a počítačov alebo na šifrovanie dát počas prenosu cez nezabezpečené sieťové pripojenia. Certifikačná služba AD CS umožňuje priradiť používateľom, zariadeniam alebo službám šifrovací kľúč pre kryptografické metódy zabezpečenia prístupu ku zdrojom alebo komunikácie.

7.4 Služba Active Directory Federation Services (AD FS)

Služba AD FS umožňuje bezpečný prístup k prostriedkom domény pre externých používateľov. Umožňuje s vysokou úrovňou zabezpečenia overovať používateľov partnerských organizácií.

7.5 Služba Active Directory Rights Management Services (AD RMS)

Služba AD RMS zabezpečuje oprávnený prístup k obsahu dokumenov a definuje pravidlá používania týchto dokumentov pre jednotlivých používateľov. Napr. právo otvoriť súbor, modifikovať, tlačiť, odoslať a iné operácie s dokumentami vo forme súborov.

Podpora tejto služby je i v aplikáciách fy Microsoft ako MS Office, Internet Explorer, a pod.

8. Správa Active Directory

8.1 Active Directory Users and Computers

Grafický nástroj určený na správu používateľov, skupín, počítačov a organizačných jednotiek

8.2 Active Directory Domains and Trusts

Nástroj je určený na správu domén a ich organizáciu do stromov a lesov domén. Zahŕrňa aj vzťahy dôverihodnosti medzi doménami.

8.3 Active Directory Sites and Services

Nástroj určený na správu sietí a podsietí.

8.4 Command Line

Textové príkazy na správu Active Directory - ***DScommand***.

DSadd – pridanie používateľa a skupiny (**add** Active Directory users and groups)

DSmod – úprava objektu AD (**modify** Active Directory objects)

DSrm – zrušenie objektu AD (**delete** Active Directory objects)

Dsmove – presun objektu AD (**relocate** Active Directory objects)

DSQuery – dotaz na hľadanie objektu AD (**find** Active Directory objects)

DSget – výpis vlastností objektu AD (**list** the properties of an objec)

8.5 Power Shell

Textové príkazy na správu AD so širokými možnosťami skriptovania.