

Active Directory

- slúži na spravovanie prístupu k jednotlivým častiam siete
- **Domain Services**
 - poskytuje informácie o užívateľoch a iných sieťových prostriedkoch
 - služby overovania totožnosti
 - umožňuje centrálnu správu
 - obsahuje info o zariadeniach, skupinách, doménach, ...
- **Certificate Services**
 - PKI - Public Key Infrastructure
 - vydávanie a správa verejných certifikátov, ktoré sa používajú pri šifrovaní a overovaní totožnosti
- **Federation Services**
 - umožňuje prístup k aplikáciám a zariadeniam, ktoré sa nachádzajú mimo domény
 - správa prístupu medzi viacerými organizáciami
- **Rights Management Services**
 - ochrana informácií udelením špecifického prístupu k jednotlivým súborom alebo aplikáciám
 - chráni pred kopírovaním, tlačením, odosielaním, čítaním neoprávnenými osobami
- **Lightweight Directory Services**
 - adresárová služba pre aplikácie
- **Domain Servicesprotokol**
 - LDAP - Lightweight Directory Access Protocol
 - protokol typu server-klient, ktorý je založený na TCP/IP
- **autentifikácia**
 - overenie totožnosti užívateľa na sieti

- interaktívne prihlasovanie - prístup k fyzickému počítaču
- overenie v sieti - prístup k sieťovým prvkom
- **autorizácia**
 - overenie oprávnenia na vykonanie istej akcie, overenie prístupu
 - SID - Security Identifier - jedinečný pre každého jednotlivca alebo skupinu
 - ACL - Access Control List obsahuje ACE - Access Control Entries
 - zoznm, v ktorom sú uložené všetky povolenia, zamietnutia prístupu a kontroly zabezpečenia
- **výhody**
 - centralizovaná správa systému
 - SSO - Single Sign-On - stačí sa raz prihlásiť do systému a získame prístup ku všetkým službám celej siete
 - škálovateľnosť
 - integrovaná bezpečnosť
- **požiadavky pre inštaláciu**
 - konfigurácia TCP/IP a DNS
 - administrátorské rozhranie
- **komponenty fyzické**
 - uľahčujú komunikáciu a fyzicky ohraničujú sieťové prostriedky
 - radiče domény
 - radič je server, na ktorom je nainštalovaná Domain Service
 - musí byť špeciálne povýšený
 - server globálneho katalógu
 - radič domény, ktorý obsahuje kópiu katalógu
 - globálny katalóg - obsahuje info o všetkých objektoch v lese
 - úložisko dát
 - obsahuje databázové súbory a procesy, ktoré pracujú s info o používateľoch službách, ...

- nie je možné k nemu pristupovať, pristupuje k nemu iba radič domény
- replikácia
 - zabezpečuje rovnaké informácie všetkým doménovým radičom
- siete
 - riadenie prenosu replikácie a prihlasovania klientov, ...
 - sú tvorené podsietami a IP adresami
- **logické**
 - pomáhajú pri organizácii objektov, správy účtov a zdieľaniach prostriedkov siete
 - objekty
 - užívateľ, počítač, tlačiareň, skupiny, kontakty, zdieľané adresáre, ...
 - organizačné jednotky
 - kontajnery, priečinky, v ktorých sa nachádzajú objekty
 - slúžia na hromadnú správu viacerých objektov
 - schéma
 - definuje každý typ objektu a jeho atribúty
 - príklad - trieda: počítač, atribút: meno
 - domény
 - územie, skupina počítačov so spoločnou adresárovou databázou
 - má jednoznačné označenie
 - spravuje sa radičom domény
 - určujú administratívne hranice pre politiky
 - určujú hranice pre autentifikáciu a autorizáciu
 - stromy
 - hierarchia domén
 - adlerka.sk - doména
 - student.adlerka.sk - pod doména
 - ucitel.adlerka.sk - pod doména

- domény a pod domény majú medzi sebou obojsmerný tranzitívny vzťah dôvery
- lesy
 - spojenie dvoch alebo viacerých doménových stromov
 - spoločná schéma, konfigurácia partície, globálny katalóg
 - povoľujú vzťahy dôvery medzi všetkými doménami v lese
- zťahy dôvery
 - umožňujú získať prístup ku sieťovým prvkom inej domény
 - dôvera môže byť rozšírená aj mimo les
 - direktívna - priamo medzi dvoma doménami
 - tranzitívna - rošíraná nad rámec dvoch domén