**Popíšte 5 funkcii AD**

**Domain Services**

adresárová služba, ktorá poskytuje informácie o užívateľoch a iných sieťových prostriedkoch

poskytuje služby overovania totožnosti

umožňuje centrálnu správu

centrálny adresár obsahuje

objekty užívateľov

objekty skupín

objekty počítačov

informácie o službách

**Certificate Services**

* implementácia infraštruktúry verejných kľúčov (PKI – Public Key Infrastructure) od spoločnosti Microsoft
* PKI – Public Key Infrastructure obsahuje  komponenty a procesy pre vydávanie a správu digitálnych certifikátov, ktoré sa používajú pri šifrovaní a overovaní totožnosti. ​
* implementácia tejto služby nie je povinná

**Federation Services**

* umožňuje prístup iných systémov a aplikácií, ktoré sa nachádzajú mimo doménovej štruktúry, mimo organizácie​
* poskytuje zjednodušené, zabezpečené federácie identít a webové Single Sign-On (SSO) schopnosti. ​
* umožňuje vytváranie vzťahov dôveryhodnosti medzi dvoma organizáciami, ​
* poskytuje prístup k aplikáciám medzi organizáciami​
* poskytuje Single Sign-On (SSO) medzi dvoma rôznymi adresármi pre webové aplikácie

**Rights Management Services**

 je technológia ochrany informácií, ktoré pracuje s aplikáciami na ochranu digitálnych informácií

* umožňuje jednotlivcom a administrátorom špecifikovať prístupové oprávnenia na dokumenty, zošity a prezentácie ​
* chráni citlivé informácie pred vytlačením, odosielaním alebo kopírovaním neoprávnenými osobami ​
* súbory majú prístupové obmedzenia bez ohľadu na to, kde sa nachádzajú

**Lightweight Directory Services**

* adresárová služba pre aplikácie, ​
* nevyžaduje nasadenie domén ​
* táto služba bola navrhnutá tak, aby doplňovala doménovú službu Domain Services a nie tak, aby ju nahradila​
* služba Domain services poskytuje adresár pre správu a overovanie totožnosti prostredníctvom siete, zatiaľ čo služba Lighweight Directory services je navrhnutá čisto ako adresárová služba pre aplikácie

**Popíšte logické prvky AD**

**Objekty**

A screenshot of a computer

Description automatically generated with medium confidence

**Organizačné jednotky**

* kontajnery, ktoré môžu obsahovať jednotlivé objekty ako sú užívatelia, skupiny, počítače alebo iné organizačné jednotky​
* organizačné jednotky​
* reprezentujú logickú a hierarchickú štruktúru organizácie    ​
* umožňuje správu viacerých objektov konzistentným spôsobom​
* delegujú sa práva pre administráciu skupín objektov​
* používajú sa politiky

**Schéma**

* definuje každý typ objektu, ktorý môže byť uložený v adresári ​
* uplatňuje pravidlá týkajúce sa vytvorenia a konfigurácie objektu

A screenshot of a phone

Description automatically generated with medium confidence

**Domény**

* skupina počítačov, ktoré zdieľajú spoločnú adresárovú databázu so všetkými objektmi v organizácií​
* obsahuje veľké množstvo objektov​
* spravuje sa radičom domény​
* má  jednoznačné označenie   ​
* ​určuje administratívne hranice pre nastavenie politiky na skupiny objektov​
* určuje hranice replikácie dát medzi radičmi domény​
* určuje hranice autorizácie a autentifikácie pri prístupe k sieťovým prostriedkom ​
* vytvára vzťahy dôvery s ostatnými doménami

**Stromy**

* hierarchia domén v doménovej službe AD DS​
* stromy​
* zdieľajú priestor názvov s nadradenou doménou​
* môžu mať ďalšie podriadené domény   ​
* medzi doménami sa vytvára obojsmerný tranzitívny vzťah dôvery

**Lesy**

* jeden alebo viacero spojených doménových stromov, ktoré zdieľajú spoločné adresárové informácie  ​
* zdieľajú spoločnú schému​
* zdieľajú spoločnú konfiguráciu partície​
* zdieľajú spoločný globálny katalóg na vyhľadávanie ​
* povoľujú vzťahy dôveryhodnosti medzi všetkými doménami v lese

**Vzťahy dôvery**

* umožňujú užívateľom získať prístup ku sieťovým zdrojom v inej doméne​
* všetky domény  v lese dôverujú všetkých ostatným doménam v lese​
* dôvera môže byť rozšírená mimo les

A screenshot of a cell phone

Description automatically generated with low confidence

**Popíšte fyzické prvky AD**

**Radič domény**

server, na ktorom je nainštalovaná doménová služba Active Directory Domain Service a bol špeciálne povýšený (promoted) na radič domény

* obsahuje kópiu centrálneho adresára doménovej služby AD DS​
* poskytuje autorizáciu a autentifikáciu ​
* replikuje aktualizácie do ostatných radičov domény v doméne (Domain) a doménovej štruktúre (Forest) ​
* sprístupňuje administratívny prístup ku správe užívateľov a iných sieťových prostriedkov​
* podporuje radiče domény len pre čítanie (RODC)

**Server Globálneho katalógu**

* Radiče domény, ktoré obsahujú kópiu globálneho katalógu​
* Globálny Katalóg​
* obsahuje kópie všetkých objektov doménovej služby AD DS v lese, pričom pre každý objekt v lese obsahuje len niektoré z ich vlastností – atribútov. (Príklad: Mena všetkých ludí na našej škole)​
* zvyšuje výkonnosť  pri vyhľadávaní objektu  tým, že sa vyhnú  zbytočným požiadavkám k radičom domény ​
* potrebné pre prihlásenie sa užívateľov do domény

**Úložisko dát**

* obsahuje databázové súbory a procesy, ktoré ukladajú a spravujú adresárové informácie pre užívateľov, služby a iné aplikácie​
* úložisko dát​
* obsahuje Ntds.dit súbor, ktorý je uložený v prednastavenom adresári %SystemRoot%\NTDS na všetkých radičoch domény​
* nie je možné pristupovať k tejto databáze priamo žiadnou aplikáciou. Databáza je spravovaná radičom domény. ​
* 64-bitový hardvér môže poskytnúť významné zvýšenie výkonu pre radiče domény z dôvodu zvýšenia adresovateľnej pamäte.

**Replikácia**

* doménová služba AD DS kopíruje všetky aktualizácie databázy všetkým radičom domény v doméne alebo v lese​
* Replikácia​
* zabezpečuje rovnaké informácie všetkým doménovým radičom​
* používa multimaster model replikácie (v sieti je viacero prvkov schopných riadiť komunikáciu, no v danom okamihu riadi vždy iba jeden sieťový prvok a časom sa menia) ​
* môže byť riadená vytvorením doménovej siete (AD DS sites)   ​
* topológia AD DS replikácie je automaticky vytvorená hneď ako sú nové radiče domény pridané do domény

**Siete**

* predstavuje segment siete, kde sú všetky radiče domény rýchlo a spoľahlivo pripojené k sieti​
* Siete​
* sú tvorené podsieťami a IP adresami ​
* používajú sa pre riadenie prenosu replikácie​
* používajú sa pre riadenie prenosu prihlasovania klientov​
* používajú sa aplikáciami ako napríklad Microsoft Exchange Server alebo  Distribuované systémy súborov (DFS - Distributed File Systems)​
* používajú sa na pridelenie Zasad skupín (Group Policy)  užívateľom  a počítačom vo firme

**Popíšte uživateľské účty**

**Lokálny**

* môžu pristupovať k prostriedkom lokálneho počítača​
* nereplikujú sa do ďaľších doménových radičov​
* nemajú prístup k adresárovej službe Active Directory

**Doménový**

* Má prístup k adresárovej službe Active Directory​
* replikujú sa do ostatných doménových radičov

**Vstavaný**

* sú vytvorené automaticky na Windows serveri 2016​
  + Administrátorský účet ​
  + účet hosťa (Guest account)​
* môžu byť lokálne alebo doménové ​
  + Samostatný server: lokálny účet ​
  + Doménový radič: doménový účet

**Administrátorský**

* na samostatnom serveri má plný prístup ku všetkým súborom na serveri​
* na doménovom radiči má plný prístup k celej doméne ​
* Nemôže byť vymazaný, ale môže byť premenovaný alebo deaktivovaný ​
* bezpečnostné opatrenia ​
  + premenujte administrátorský účet ​
  + zvoľte silné heslo ​
  + obmedzte ľudí, ktorí poznajú administrátorské heslo ​

**Účet hosťa**

* používa sa len na dočasný prístup k sieti ​
* nemôže byť vymazaný​
* pôvodne je deaktivovaný ​
* nemá nastavené heslo ​
* bezpečnostné opatrenia ​
  + vytvorte jedinečný účet pre dočasných užívateľov ​
  + premenujte tento účet po deaktivovaní  tohto účtu  ​
  + nastavte silné heslo

**Popíšte rozdelenie skupín AD podľa typu a podľa rozsahu**

**Podľa typu**

* **Distribučná skupina**​
  + používa sa na šírenie medzi viacerých užívateľov ​
  + používa sa pre skupiny, ktoré nesúvisia s bezpečnosťou ​
* **Bezpečnostná skupina**​
  + používa sa na pridelenie práv prostriedkov jednému alebo viacerým užívateľom​
  + majú niekoľko funkcií ​
    - riadenie, ktoré objekty skupina môže obsahovať ​
    - limitujú objekty v rovnakej doméne ​
    - povoľujú prístup k objektom vzdialeným doménam​
    - určujú, kedy sa objekt používa v doméne alebo v lese

**Podľa rozsahu**

**Doménové lokálne skupiny**

* **Cieľ: prideľovanie oprávnení a práv k sieťovým prostriedkom v rámci vlastnej domény**​
* môžu obsahovať nasledujúce objekty​
  + užívateľské účty, účty počítačov, globálne skupiny z ľubovoľnej domény v lese a univerzálne skupiny ​
* používajú sa na pridelenie oprávnení v rovnakej doméne ​
* používajú sa na pridelenie oprávnení doménovým lokálnym skupinám​
* používajú sa na správu prideľovania oprávnení ​
* používajú sa na správu údržby opráv používajú sa na pridelenie povolení ​
* **sú viditeľné iba v doméne, v ktorej boli vytvorené a nikde inde**

**Globálne skupiny**

* **Cieľ: zoskupovanie užívateľov so spoločnými záujmami**​
* môžu obsahovať nasledujúce objekty​
  + užívateľské účty, účty počítačov, globálne skupiny z rovnakej domény​
* používa na pridelenie alebo zamietnutie práva na akýkoľvek prostriedok v lese alebo v doméne​
* replikáciu členstva medzi radičmi domén v rovnakej doméne​
* je možné meniť členstvo tak často ako je to nevyhnutné ​
* **je viditeľná vo vlastnej doméne a vo všetkých dôveryhodných doménach**

**Univerzálne skupiny**

* **Cieľ: slúžia k zlúčeniu globálnych skupín pre zjednodušenie prístupu k prostriedkom vo väčších prostrediach s väčším počtom domén v rámci lesa Active Directory**​
* používa sa pre prístup sieťovým prostriedkom v akejkoľvek doméne alebo v lese ​
* používa sa ku usporiadaniu skupín a užívateľských účtov v rámci domény alebo v rámci lesu​
* nemali by sa používať na časté zmeny členstva v skupine​
* zmeny sa replikujú na všetky servery globálneho katalógu​
* využívajú významnú šírku pásma počítačovej siete ak sa vykonáva často​
* účinok je horší v sieti WAN ako v sieti LAN​
* **je viditeľná v akejkoľvek doméne lesa Active Directory**

**Popíšte organizačné jednotky AD**

* môžu vytvoriť hierarchickú štruktúru, ktorá napodobňuje podnikovú štruktúru pre jednoduchšiu správu objektov ​
* umožňujú decentralizovať administráciu​
  + organizačným jednotkám je možné delegovať práva správcu, ktoré umožňujú užívateľom vykonávať administrátorské úlohy v danej organizačnej jednotke​
  + neumožňujú užívateľom vykonávať administrátorské úlohy na celej doméne​
  + minimalizuje počet užívateľov s globálnymi administrátorskými právami​
* na OU sa aplikujú Zásady skupín (Group Policy)

**Popíšte 5 ľubovolných zásad skupín**

* **Zásady hesla (Password Policy)​**
  + nastavenie vlastnosti hesla, dlžka hesla, znaky hesla
* **Zásady zamykania účtu (Account Lockout Policy)**
  + určujú počet nesprávne zadaných hesiel pre zamknutie účtu, poprípade čas, ako dlho bude účet zamknutý
* **Zásady Auditu (Audit Policy)**
  + určujú monitorovacie zásady pre doménu
* **Užívateľské práva (User Rights)**
  + priradenie užívateľských práv definuje napríklad práva pre miestne prihlásenie alebo vypínanie systému
* **Možnosti bezpečnosti (Security Options)​**

nastavenie zložitejšieho typu, ktoré sa v minulosti zadávalo v registroch, napríklad počet prihlásení, ktoré sa na desktopoch ukladajú do mezdipamäte

* **Zásady bezpečnosti (Security Policy)​**
  + zavedenie bezpečnostných nastavení pre účty, audit udalosti, politiku hesiel, systémové služby, registre a súborové systémy
* **Skripty (Scripts)​**
  + konfigurácia prihlasovacích/odhlasovacích skriptov a skriptov pre zapnutie/vypnutie počítača
* **Bezdrôtová sieť (Wireless Networking IEEE 802.1x)​**
  + nastavenie zásad prístupových bodov, klientov a preferovaných sietí pre bezdrôtové štandardy
* **Ovládací panel (Control Panel)**
  + nastavenie jednotlivých modulov ovládacieho panelu, ktoré budú povolené a ktoré budú zakázané
* **Desktop​**
  + konfigurácia plochy systému
* **Network Configuration​**
  + konfigurácia siete a nastavenia sieťových klientov, súborov offline

**Čo je GPO a popíšte rozdelenie GPO**

všetky nastavenia sú zoskupované do objektov zásad GPO – Group Policy Objects, ktoré dokážu meniť konkrétne parametre správania počítača alebo užívateľa

* **Vlastnosti GPO:​**
  + komponent globálnej politiky​
  + samotné nastavenie GPO sa viaže – linkuje na jednotlivé organizačné jednotky (OU), sieť (Site) alebo doménu (Domain) v Active Directory, neviažu sa na počítač alebo užívateľa​
  + jeden  GPO môže byť viazaný na viacero organizačných jednotiek
* **Rozdelenie GPO​**
  + Konfigurácia počítača (Computer configuration)​
  + Konfigurácia užívateľa (User configuration)​
* **Každá z uvedených častí rozdelenia GPO sa delí na​**
  + nastavenie softvéru (Softvér settings)​
  + inštalácia softvéru ​
  + nastavenie systemu Windows (Windows settings)​
  + obsahujú skripty (pri prihlásení a odhlásení) a nastavenie zabezpečenia pre užívateľa, počítač a Internet Explorer​
  + šablony pre správu  (Administrative templates)​
  + obsahujú stovky nastavení registrov pre ovládanie rôznych aspektov uživateľa alebo počítačového prostredia

**Popíšte delenie zásad skupín a prioritu zásad skupín.**

* **Zásady delíme na​**
  + **Lokálne ​**
    - každý počítač má lokálne zásady (local Group Policy), ktoré ovplyvňujú lokálny počítač a prihlásenie užívateľa​
    - obmedzené oprávnenia užívateľa vymedzujú lokálne zásady​
    - lokálne zásady sú uložené v skrytom adresári %systemroot%\system32\GroupPolicy​
    - používajú sa v prípade, keď počítač nie je pripojený do domény     ​
  + **Doménové  ​**
    - používajú sa u počítačov a užívateľov, ktoré sú členmi domény​
    - existujú dve základné doménové politiky​
      * 1) Default Domain Policy – pre všetky objekty v doméne ​
      * 2) Default Domain Controller Policy – pre všetky radiče v doméne​

ôObjekty zásad skupiny GPO sú aplikované v poradí​

1) Lokálne zásady​

2) Zásady pre siete​

3) Doménové zásady​

4) Zásady pre organizačné jednotky OU​

najnižšiu prioritu majú lokálne zásady a najvyššiu prioritu majú zásady organizačnej jednotky