11. Adresářové služby

**1. Základní charakteristika adresářových služeb**

**1.1 Adresářové služby obecně**

* **Definice:**

Adresářové služby slouží k uchovávání, organizaci a správě informací o uživatelích, počítačích, aplikacích, službách a dalších síťových zdrojích. Umožňují centralizovanou správu přístupových práv a politik.

* **Výhody:**
  + **Centralizovaná správa:** Jediný zdroj pravdy, což usnadňuje správu velkých organizací.
  + **Efektivní autentizace a autorizace:** Umožňuje jednotné ověřování přístupu ke zdrojům napříč celou infrastrukturou.
  + **Škálovatelnost a replikace:** Informace jsou replikovány mezi doménovými řadiči, což zvyšuje dostupnost a odolnost proti selhání.

**1.2 Active Directory (AD)**

Active Directory je **adresářová služba** (pracujících na **LDAP**-rotokol) vyvinutá společností Microsoft, která se stala standardem pro správu prostředí Windows. Klíčové koncepty AD zahrnují:

* **Domény a pracovní skupiny:**
  + **Doména:**
    - Jedná se o logickou skupinu objektů (uživatelé, počítače, skupiny) spravovaných centrálně.
    - Doména má jedinečné jméno (DNS název) a bezpečnostní politiku, která se aplikuje na všechny její objekty.
  + **Pracovní skupina:**
    - Nezávislá skupina počítačů, kde každý systém má lokálně uloženou databázi uživatelů a přístupových práv.
    - Neexistuje centrální správa, což znamená, že autentizace probíhá lokálně.
* **Organizační struktura v AD:**
  + **Forest a Tree:**
    - **Forest** je nejvyšší logická jednotka, která může obsahovat více domén, jež jsou uspořádány do stromové struktury (tree).
    - Všechny domény v lese sdílejí společné schéma a konfigurační informace.
  + **Organizační jednotky (OU):**
    - Slouží k hierarchickému seskupování objektů uvnitř jedné domény.
    - Umožňují delegaci správy (např. různé oddělení mohou mít své OU a odpovědné administrátory).
  + **Důvěry (Trusts):**
    - Mezi doménami se mohou navazovat důvěry, které umožňují vzájemné ověřování uživatelů a sdílení zdrojů.
* **FSMO role (Flexible Single Master Operations):**
  + AD přiděluje některé kritické úlohy pouze jednomu řadiči v dané struktuře. Existuje pět hlavních FSMO rolí:
    - **Schema Master:**Řídí změny v AD schématu. Pokud dojde k potřebě rozšíření nebo úprav schématu (například při instalaci nových aplikací), tento řadič provádí příslušné aktualizace.
    - **Domain Naming Master:**Odpovídá za správu názvů domén uvnitř lesa, tedy umožňuje přidávání či odstraňování domén.
    - **RID Master (Relative Identifier Master):**Při vytváření nových objektů v doméně přiděluje unikátní identifikátory (RID), které se následně kombinují s GUID domény.
    - **PDC Emulator:**Slouží jako centrální bod pro synchronizaci času a kompatibilitu se staršími systémy; je také primárním kontaktním bodem při změnách hesel.
    - **Infrastructure Master:**Spravuje změny týkající se vztahů mezi objekty v různých doménách (například aktualizace informací o skupinách, jejichž členy jsou v jiné doméně).
* **Globální katalog:**
  + **Definice:**Obsahuje částečné kopie všech objektů v lese, což umožňuje rychlé vyhledávání informací napříč celou infrastrukturou.
  + **Funkce:**
    - Umožňuje klientům najít objekty a atributy, aniž by museli komunikovat s každým doménovým řadičem zvlášť.
    - Hraje klíčovou roli při autentizaci uživatelů z různých domén.
* **Úroveň funkčnosti (Functional Level):**
  + **Doménová a lesní úroveň funkčnosti** určuje minimální verzi operačního systému, kterou musí všechny řadiče v doméně nebo lese podporovat.
  + Vyšší úroveň funkčnosti umožňuje využití pokročilejších funkcí, jako je například rychlejší replikace nebo vylepšené bezpečnostní mechanismy.

**2. Základní objekty Active Directory a zásady skupiny**

**2.1 Základní objekty Active Directory**

* **Uživatelé (Users):**
  + Každý uživatel je reprezentován jako objekt s atributy jako jméno, heslo, email a další.
  + Správa uživatelů zahrnuje přiřazování oprávnění, členství ve skupinách a nastavení profilů.
* **Počítače (Computers):**
  + Reprezentují zařízení připojená do domény.
  + Umožňují centrální správu konfigurací, aktualizací a bezpečnostních zásad.
* **Skupiny (Groups):**
  + Skupiny slouží ke správě přístupových práv a mohou být typu bezpečnostních (Security Groups) nebo distribučních (Distribution Groups).
  + Umožňují zjednodušit správu oprávnění – místo individuálního nastavování oprávnění pro každého uživatele lze oprávnění přiřadit skupině.
* **Organizační jednotky (Organizational Units, OUs):**
  + Logické kontejnery, které slouží k organizaci objektů v rámci domény.
  + Umožňují delegaci správy a aplikaci specifických zásad (Group Policy) na konkrétní oddělení nebo geografické oblasti.
* **Další objekty:**
  + **Kontakty:** Uchovávají informace o osobách či subjektech, které nejsou přímo autentizované v doméně, ale mohou být referencovány v rámci adresáře.
  + **Tiskárny, sdílené složky, služby:** Mohou být také reprezentovány jako objekty v AD pro usnadnění jejich správy.

**2.2 Zásady skupiny (Group Policy)**

* **Group Policy Objects (GPO):**
  + **Definice:** GPO umožňují centralizovanou konfiguraci nastavení pro uživatele a počítače v doméně. Tyto zásady se vztahují na objekty umístěné v konkrétních OU, doménách nebo na celém lese.
  + **Možnosti nastavení:**
    - Konfigurace zabezpečení (např. nastavení hesel, auditování, firewall pravidla).
    - Konfigurace pracovního prostředí (např. nastavení plochy, instalace software, skripty při přihlášení/odhlášení).
    - Omezení přístupu a nastavení práv, které ovlivňují běžné operace uživatelů.
  + **Hierarchie a dědičnost:**
    - GPO se mohou dědit z vyšších úrovní (les, doména) a být přepsány nebo filtrované na nižších úrovních (OU).
    - Administrátoři mohou definovat, zda se konkrétní zásady mají aplikovat na určité objekty, což umožňuje velmi jemné ladění konfigurace.
* **Praktické aspekty správy:**
  + Pomocí nástrojů jako Group Policy Management Console (GPMC) lze snadno prohlížet, měnit a testovat GPO.
  + Testování a simulace výsledků zásad (Group Policy Modeling) pomáhá předcházet nechtěným konfiguracím.

**3. Konfigurace a správa služby LDAP v UNIX-like operačních systémech**

**3.1 Základní princip LDAP**

* **LDAP (Lightweight Directory Access Protocol):**
  + Je to protokol pro přístup k adresářovým službám, který definuje, jak klienti vyhledávají a modifikují informace uložené v adresářové databázi.
  + LDAP adresář je strukturován jako strom (Directory Information Tree – DIT) se záznamy (entry), které obsahují atributy (například jméno, email, telefon).

**3.2 OpenLDAP a jeho konfigurace**

* **OpenLDAP:**
  + Nejrozšířenější open-source implementace LDAP serveru.
  + Je využíván jako centrální úložiště pro autentizační informace, správu uživatelů, skupin a dalších síťových objektů.
* **Konfigurace a struktura:**
  + **Konfigurační soubory:**
    - Hlavní konfigurace bývá umístěna v adresáři /etc/openldap/ nebo /usr/local/etc/openldap/.
    - Soubor slapd.conf (v starších verzích) nebo konfigurace pomocí OLC (cn=config) u novějších verzí definuje schéma, přístupová práva (ACL) a další nastavení.
  + **Adresářová struktura (DIT):**
    - Hierarchická struktura, často založená na DN (Distinguished Name) formátu, např. dc=example,dc=com.
    - Uživatelé, skupiny a další objekty jsou organizovány do logických kontejnerů (např. ou=People, ou=Groups).
* **Nástroje pro správu LDAP:**
  + **ldapsearch:** Pro vyhledávání a ověřování struktury adresáře.
  + **ldapadd / ldapmodify:** Pro přidávání nebo úpravu záznamů.
  + **phpLDAPadmin:** Webové rozhraní, které zjednodušuje správu a vizualizaci dat v adresáři.
  + **GUI nástroje:** Například Apache Directory Studio poskytují kompletní správu adresářů s grafickým uživatelským rozhraním.
* **Integrace s dalšími systémy:**
  + LDAP se často kombinuje s Kerberos (pro centrální autentizaci), NFS nebo Samba, aby sloužil jako jednotný zdroj pro ověřování a autorizaci v heterogenních sítích.

**Shrnutí**

1. **Adresářové služby** poskytují centralizovaný správní model, který uchovává informace o uživatelích, počítačích a dalších síťových zdrojích. Tato centralizace umožňuje jednotnou správu autentizace a autorizace.
2. **Active Directory (AD):**
   * Umožňuje správu pomocí domén, organizačních jednotek (OU) a skupin, přičemž klíčové funkce zajišťují FSMO role, globální katalog a nastavení úrovně funkčnosti.
   * Zásady skupiny (Group Policy) umožňují detailní konfiguraci nastavení zabezpečení a pracovního prostředí, které se dědí a mohou být filtrované podle organizační struktury.
3. **LDAP v UNIX-like systémech:**
   * LDAP, nejčastěji implementovaný pomocí OpenLDAP, slouží jako adresářová služba, kde se informace ukládají hierarchicky.
   * Správa probíhá úpravou konfiguračních souborů a použitím nástrojů jako ldapsearch, ldapadd/modify či webových rozhraní (phpLDAPadmin), což umožňuje integraci s dalšími službami a centralizovanou správu identit.