Active Directory (AD)

Active Directory je adresářová služba vyvinutá společností Microsoft pro sítě typu doména. Slouží jako centrální databáze pro ukládání informací o uživatelích, počítačích, skupinách, tiskárnách a dalších prostředcích v síti.

Hlavním účelem AD je umožnit administrátorům spravovat oprávnění a přístup k síťovým zdrojům z jednoho centrálního místa.

Logická struktura Active Directory

AD organizuje objekty do hierarchické struktury, což umožňuje škálovatelnost od malých kanceláří až po nadnárodní korporace.

1. Objekty (Objects)

Základní jednotka v AD. Objekty představují konkrétní položky, jako jsou uživatelé, počítače, tiskárny nebo sdílené složky. Každý objekt má své **atributy** (např. jméno, příjmení, e-mail, telefonní číslo).

2. Organizační jednotky (Organizational Units - OU)

Kontejnery v rámci domény, do kterých se vkládají objekty. Slouží k:

- Logickému členění (např. OU „Marketing“, OU „IT“).
- Delegování práv (např. správce IT může spravovat jen uživatele v OU „Marketing“).
- Aplikaci skupinových politik (GPO).

3. Domény (Domains)

Hlavní administrativní jednotka. Všechny objekty v jedné doméně sdílejí společnou databázi a bezpečnostní politiku. Doména má obvykle název ve formátu DNS (např. `mojefirma.local`).

4. Stromy (Trees)

Seskupení jedné nebo více domén, které sdílejí společný jmenný prostor (např. `vyvoj.mojefirma.local` je součástí stromu `mojefirma.local`).

5. Lesy (Forests)

Nejvyšší úroveň hierarchie. Les sdružuje jeden nebo více stromů, které sdílejí společné **Schéma** (strukturu databáze) a **Global Catalog** (index všech objektů).

Fyzická struktura

Zatímco logická struktura řeší organizaci, fyzická struktura řeší výkon a dostupnost.

- **Domain Controller (DC):** Server, na kterém běží služba Active Directory. Obsahuje kopii databáze AD a provádí autentizaci uživatelů.
- **Sites (Lokality):** Reprezentují fyzickou topologii sítě (např. kancelář v Praze a pobočka v Brně). Slouží k optimalizaci replikace dat mezi DC, aby se zbytečně nezatěžovaly pomalé linky.

Klíčové mechanismy a funkce

Autentizace a Autorizace

AD využívá k ověřování uživatelů především protokol **Kerberos**, který je bezpečnější než starší NTLM. Po přihlášení uživatel obdrží „lístek“ (ticket), který mu umožňuje přístup k povoleným zdrojům bez nutnosti znovu zadávat heslo (Single Sign-On - SSO).

Group Policy (GPO)

Skupinové politiky umožňují hromadnou konfiguraci počítačů a uživatelů. Pomocí GPO lze například:

- Všem uživatelům nastavit stejné pozadí plochy.
- Zakázat používání USB disků.
- Automaticky instalovat software.

Schéma AD

Definuje pravidla pro to, jaké typy objektů a atributů mohou být v AD vytvořeny. Je to v podstatě „blueprint“ celé databáze.

Používané protokoly

Active Directory není uzavřený systém, ale využívá standardizované protokoly:

Protokol	Funkce
LDAP	(Lightweight Directory Access Protocol) Slouží k dotazování a úpravám objektů v AD.
DNS	(Domain Name System) Klíčový pro lokalizaci doménových řadičů v síti. Bez DNS AD nefunguje.
Kerberos	Hlavní protokol pro bezpečnou autentizaci uživatelů.
SMB/CIFS	Protokol pro sdílení souborů a tiskáren v rámci domény.

Služby AD (Role)

Moderní systémy Windows Server dělí AD do několika specifických rolí:

```
1. **AD DS (Domain Services):** Standardní správa uživatelů a počítačů.
2. **AD CS (Certificate Services):** Správa digitálních certifikátů.
3. **AD FS (Federation Services):** Umožňuje SSO přístup k aplikacím mimo firemní síť (např. Office 365).
4. **AD LDS (Lightweight Directory Services):** Ořezaná verze pro aplikace, které potřebují adresář, ale nepotřebují celou doménu.
```

Související pojmy: LDAP, Kerberos, DNS, Group Policy, Access Control.