Microsoft Active Directory

Microsoft Active Directory (AD) je jedna z nejrozšířenějších adresářových služeb, poprvé uvedená v systému Windows Server 2000. S postupnými verzemi byla aktualizována a dnes se nachází ve své třetí hlavní verzi. Prezentace představí základní koncepty Active Directory, strukturu objektů, význam domén a organizačních jednotek, použití protokolu LDAP a replikace. Také se zaměří na roli různých oddílů v AD databázi a moderní možnosti správy identit prostřednictvím rolí, jako jsou AD LDS a AD RMS.

Úvod do služby Microsoft Active Directory

1. **Co je Active Directory?**
   - Adresářová služba vyvinutá společností Microsoft pro centrální správu uživatelů a síťových zdrojů.
2. **Historie a vývoj AD**
   - Poprvé se objevila v systému Windows Server 2000 a od té doby prošla významnými aktualizacemi.
3. **Verze Active Directory**
   - Třetí hlavní verze je v současnosti dostupná v nejnovějších edicích Windows Server.
4. **Účel AD**
   - Poskytuje jednotnou správu uživatelských účtů, skupin, počítačů, zabezpečení a síťových prostředků.

Základní pojmy a struktura AD

1. **Doména a její role**
   - Základní logická jednotka v Active Directory, která sdružuje systémy s jednotným zabezpečením.
2. **Členové domény a servery**
   - Člen domény: Každý systém připojený k doméně.
   - Server domény: Poskytuje služby členům domény, zatímco ostatní servery mohou být aplikační nebo členské servery.
3. **Příklad logického uspořádání**
   - Struktura domén a organizačních jednotek (OU) pro oddělení a uspořádání podle funkcí či geografických umístění.

Typy objektů v Active Directory

1. **Objekty a jejich role v AD**
   - AD spravuje širokou škálu objektů, jako jsou uživatelé, skupiny, počítače, domény, kontakty a další.
2. **Příklady objektů**
   - **Uživatelé**: Jednotlivci s přístupem do sítě.
   - **Skupiny**: Skupiny uživatelských účtů.
   - **Počítače**: Pracovní stanice a servery.
   - **Doména a organizační jednotka** (OU): Kolekce a organizační struktury v AD.
3. **Identifikátory objektů**
   - Každý objekt má GUID (Globally Unique Identifier), který zajišťuje jeho jedinečnost v AD.
4. **Rozlišující název (DN)**
   - Struktura DN jako jednoznačného identifikátoru v adresářové hierarchii, např. /DC=organizace/OU=oddělení/CN=server.

Protokol LDAP a X.500

1. **LDAP jako protokol pro přístup k AD**
   - AD používá protokol LDAP založený na schématu X.500, což umožňuje kompatibilitu se standardizovanými adresářovými službami.
2. **Struktura LDAP názvů**
   - DN (Distinguished Name) se skládá z několika komponent, jako je DC (Domain Component) a OU (Organizational Unit).
3. **Hlavní název uživatele (UPN)**
   - Ve formátu Uživatelské_jméno@Název_domény, slouží jako jednoznačný identifikátor uživatele.
4. **Výhody použití LDAP**
   - Široká kompatibilita, flexibilita v dotazování a správa informací ve velkých adresářových systémech.

Doménové struktury a vztahy důvěryhodnosti

1. **Kořenová doména**
   - První vytvořená doména v AD, slouží jako základ pro celou doménovou strukturu.
2. **Podřízené domény a hierarchie**
   - Subdomény a jejich vztahy vůči kořenové doméně, což umožňuje rozčlenění AD struktury do menších jednotek.
3. **Vztahy důvěryhodnosti mezi doménami**
   - Tranzitivní vztahy důvěryhodnosti (A důvěřuje B a B důvěřuje C, tudíž A důvěřuje i C).
4. **Praktické využití vztahů důvěryhodnosti**
   - Zajišťuje bezpečný a řízený přístup mezi různými částmi organizace v rámci doménové struktury.

Oddíly v databázi Active Directory

1. **Configuration oddíl**
   - Obsahuje fyzickou strukturu doménové struktury, informace o serverech a síťové konfiguraci.
2. **Domain oddíl**
   - Uchovává topologii a nastavení jednotlivých domén, tedy informace specifické pro doménu.
3. **Schema oddíl**
   - Definuje objekty a jejich atributy, standardizuje typy objektů pro celou doménovou strukturu.
4. **Praktický význam oddílů**
   - Každý oddíl má specifickou úlohu v řízení a udržování konzistence dat v AD.

Služby rolí v Active Directory

1. **Vývoj rolí v AD**
   - Se zavedením Windows Server 2008 byly představeny nové služby rolí v rámci AD.
2. **Certifikační služby (AD CS)**
   - Správa certifikátů, umožňuje vytvoření PKI infrastruktury pro zabezpečenou komunikaci.
3. **Služby pro správu práv (AD RMS)**
   - Řízení přístupu k dokumentům a datům na úrovni aplikací.
4. **Federované služby (AD FS)**
   - Umožňuje jednotné přihlášení mezi doménami a cloudovými službami, což zjednodušuje přístup k externím aplikacím.
5. **AD LDS (Active Directory Lightweight Directory Services)**
   - Odlehčená verze AD pro aplikace, které nevyžadují plnou doménovou strukturu.

Replikace v Active Directory

1. **Řadiče domény a replikace**
   - Kritické servery, které ukládají a replikují informace pro doménu, aby zajistily dostupnost a konzistenci.
2. **Primární a záložní řadiče domény**
   - První verze AD umožňovala PDC a BDC, zatímco pozdější verze přešly na multimaster replikaci.
3. **RODC (Read-Only Domain Controller)**
   - Řadič domény s omezeným přístupem pouze pro čtení, vhodný pro zabezpečené prostředí s nižší šířkou pásma.
4. **Optimalizace replikace pro WAN**
   - RODC nabízí optimalizované funkce pro vzdálené pobočky s omezeným přístupem k síti.

Shrnutí

- Microsoft Active Directory poskytuje komplexní adresářové služby pro řízení a zabezpečení síťových zdrojů.
- Struktura AD obsahuje různé typy objektů, jako jsou uživatelé, skupiny, počítače a domény, které jsou organizovány do logických a hierarchických jednotek.
- Protokol LDAP podporuje přístup k datům v AD, zatímco replikace a služby rolí poskytují flexibilitu, bezpečnost a efektivní správu v rámci celého síťového prostředí.

Kontrolní otázky

1. Jakou roli hraje doména v Active Directory?
2. Jaký je rozdíl mezi oddíly Configuration a Domain v AD databázi?
3. Jaký je význam LDAP pro přístup k Active Directory?
4. K čemu slouží vztahy důvěryhodnosti mezi doménami?
5. Jaké funkce plní služba AD RMS?

Doporučená literatura

1. **Microsoft Documentation - Active Directory** - Oficiální dokumentace Microsoftu k Active Directory.
2. **Tanenbaum, A. S., & Wetherall, D. J.** - *Computer Networks* - Příručka s detailními informacemi o sítích a adresářových službách.
3. **RFC 4510 - Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map**
4. **Novell eDirectory Documentation** - Kompatibilní adresářová služba pro srovnání s AD.
5. **The Open Group - Standardy X.500 a LDAP**