Standard X.500 a protokol LDAP

Standard X.500 a protokol LDAP (Lightweight Directory Access Protocol) představují klíčové komponenty pro zajištění interoperability adresářových služeb v síťových prostředích. Tato prezentace přibližuje, jak X.500 vytvořil základní strukturu adresářových služeb s více typy protokolů a hierarchickým stromem DIT (Directory Information Tree) a jak LDAP přizpůsobil tento standard na protokol TCP/IP. Prozkoumáme také role jednotlivých protokolů v rámci X.500, rozdíly mezi DAP a LDAP, roli služby NIS a strukturu rozlišujících názvů (DN) v LDAP adresářích.

Standard X.500 - Základy a účel

1. **Definice a vývoj standardu X.500**
   - Vyvinut telekomunikačním průmyslem, aby sjednotil adresářové služby v síťových prostředích.
   - Standardizace prostřednictvím konsorcia The Open Group.
2. **Protokol DAP (Directory Access Protocol)**
   - Použitelný pro jakýkoliv typ sítě, komunikuje s agenty adresářového systému (DSA) v hierarchickém stromu DIT.
3. **Role agentů DUA (Directory User Agent)**
   - Klientské programy (např. WHOIS, FINGER) přistupují k adresářovým informacím prostřednictvím agentů DUA.
4. **Cíl X.500:**
   - Zajistit, aby různé adresářové služby byly vzájemně kompatibilní a mohly sdílet informace.

Protokoly v rámci standardu X.500

1. **Protokol DAP**
   - Operace jako Add, Bind, Compare, Delete, List, Modify, ModifyRDN, Read a Search.
   - Omezené rozšíření kvůli složitosti a použití OSI modelu.
2. **Protokol DISP (Directory Information Shadowing Protocol)**
   - Mechanismy replikace dat (stínové kopie a ukládání do mezipaměti).
   - Zvýšení spolehlivosti replikace pro efektivní zálohu a dostupnost informací.
3. **Protokol DOP (Directory Operational Bindings Management Protocol)**
   - Zajišťuje dohody o replikaci mezi servery.
4. **Protokol DSP (Directory System Protocol)**
   - Umožňuje komunikaci mezi DSA a dalšími DSA/DUA pro přístup k informacím v adresáři.

Přechod z DAP na LDAP

1. **Vznik LDAP (Lightweight Directory Access Protocol)**
   - Zjednodušený protokol vycházející z X.500, optimalizovaný pro TCP/IP sítě.
   - „Lehký“ přístup ke stejným adresářovým operacím jako DAP, ale s menší náročností.
2. **Význam zjednodušení na TCP/IP**
   - Odstranění složitosti OSI modelu, což umožnilo lepší rozšíření a kompatibilitu.
3. **Srovnání DAP a LDAP**
   - LDAP je méně náročný, rychlejší a rozšířenější než DAP, přičemž nabízí interoperabilitu v moderních sítích.

Služba NIS (Network Information Service)

1. **Úvod do služby NIS**
   - Adresářový systém založený na protokolu RPC, který uchovává názvy uživatelů a systémů.
2. **Role NIS v UNIX prostředí**
   - Používá se v sítích UNIX, umožňuje definování a správu společných konfiguračních souborů.
3. **Typy systémů v NIS**
   - Hlavní server NIS: Ukládá databázi pro domény NIS.
   - Sekundární server NIS: Obsahuje replikované kopie pro zajištění redundance.
   - Klient NIS: Využívá data uložená v NIS pro autentizaci.
4. **Bezpečnost a omezení NIS**
   - NIS uchovává informace ve formátu méně bezpečném než moderní adresářové služby na bázi LDAP.

LDAP servery a adresářové služby

1. **Moderní LDAP servery**
   - Microsoft Active Directory, Novell eDirectory, 389 Directory Server, OpenDS, Sun Java System Directory Server.
2. **Funkce LDAP v adresářových službách**
   - Dotazování adresářů přes TCP/IP, což zajišťuje flexibilní a kompatibilní komunikaci mezi různými systémy.
3. **Výhody LDAP**
   - Rozšířená kompatibilita mezi různými implementacemi, přestože existují omezení v interoperabilitě.

Formát výměny dat LDAP (LDIF)

1. **LDIF - LDAP Data Interchange Format**
   - Textový formát pro export a import dat mezi LDAP servery.
2. **Struktura LDIF záznamu**
   - Každý záznam obsahuje DN (Distinguished Name), typ objektu a atributy.
3. **Standardizace LDIF**
   - Udržován komisí IETF, využíván v OpenLDAP, Netscape, Microsoft a dalších systémech pro přenos a úpravy dat.
4. **Praktické příklady LDIF formátu**
   - Ukázka příkazů pro úpravu záznamů (Add, Replace, Delete).

Novell eDirectory

1. **Historie a funkce eDirectory**
   - Objektově orientovaná databáze s podporou uživatelů, skupin a síťových služeb.
2. **Hierarchická struktura a role objektů**
   - Rozdělení na oddíly, multimaster replikace.
3. **Interoperabilita**
   - Podpora pro systémy Windows, Linux, NetWare, Solaris, HP-UX a IBM AIX.
4. **Využití protokolů v eDirectory**
   - LDAP, SOAP, JDBC, ODBC, DSML, JNDI, ADSI.

Rozlišující názvy (DN) v adresářových službách

1. **Definice rozlišujícího názvu (DN)**
   - Jednoznačný identifikátor objektu v adresáři, který odkazuje na konkrétní objekt v adresářovém stromu.
2. **Struktura DN a komponenty**
   - Komponenty jako CN (Canonical Name), OU (Organizational Unit), DC (Domain Component).
3. **Význam DN pro adresářovou strukturu**
   - Umožňuje hierarchické uspořádání objektů a přehlednost přístupových práv.
4. **Příklady DN v Active Directory**
   - Například „/DC=společnost/O=organizační_jednotka/OU=oddělení/CN=server“.

Struktura adresářového stromu v LDAP

1. **Adresářový strom (Directory Information Tree - DIT)**
   - Hierarchická struktura pro uložení objektů a jejich vztahů.
2. **Uzly a atributy**
   - Uzly jako kontejnerové objekty s vlastnostmi, které mohou obsahovat více atributů.
3. **Možnosti rozšíření v LDAP**
   - Umožňuje definovat nové vlastnosti a specifické typy objektů.
4. **Význam rozlišujících názvů (RDN) v DIT**
   - Každý objekt má relativní rozlišující název (RDN), což podporuje jednoduchost a flexibilitu při správě objektů.

Shrnutí

- X.500 a LDAP jsou standardy, které definují strukturu a komunikaci v adresářových službách.
- LDAP, odlehčená verze X.500, umožňuje rychlé a kompatibilní operace v sítích TCP/IP.
- Role jednotlivých protokolů v X.500 a možnosti použití LDIF a rozlišujících názvů přispívají k efektivní správě adresářových služeb v síti.

Kontrolní otázky

1. Jaký je hlavní rozdíl mezi protokoly DAP a LDAP?
2. Jaké funkce nabízí protokol DISP v rámci standardu X.500?
3. Jaké typy systémů existují ve službě NIS?
4. Co je LDIF a k čemu slouží v prostředí LDAP?
5. Jaká je struktura rozlišujícího názvu (DN) a jaký je jeho význam?

Doporučená literatura

1. **RFC 4510 - Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map**
2. **Tanenbaum, A. S., & Wetherall, D. J.** - *Computer Networks*
3. **Microsoft Documentation** - Active Directory a LDAP
4. **Novell eDirectory Documentation**
5. **The Open Group** - Standardy pro X.500 a LDAP