Adresárové systémy

Správa identít a prístupov (*Identity and Access Management, IAM*) je relatívne široká oblasť, ktorá obsahuje množstvo spolupracujúcich technológií. Srdcom takmer každého riešenia IAM je nesporne adresárový systém (directory service).

Je to komponent, ktorý možno nájsť azda v každom nasadenom systéme. Pri menších podnikových riešeniach je to často známe Active Directory, pri väčších škálovateľných systémoch sa často používa systém dedikovaných LDAP serverov. Adresárový systém slúži na efektívne ukladanie a sprístupňovanie údajov o identitách, ktoré sú využívané ostatnými komponentmi riešenia IAM a veľmi často aj aplikáciami. De facto štandardom pri adresárových službách sa stal protokol LDAP. Tento protokol sa zaužíval do takej miery, že koncept adresárového systému sa často (hoci nesprávne) označuje ako LDAP.

Adresárový systém je teda v podstate databáza. Je to však úplne iná databáza ako bežné databázy SQL. Adresárový systém je od základu navrhnutý na masívnu škálovateľnosť. Keď počet záznamov prekročí niekoľko miliónov, v databázach SQL sa začínajú objavovať prvé problémy so škálovateľnosťou. Pre adresárové služby je milión záznamov takmer zanedbateľné číslo. Adresárové systémy s miliardami záznamov nie sú úplne výnimočné. Ale podstata škálovateľnosti adresárových služieb nie je v počte záznamov. Adresárové služby sú navrhnuté tak, aby umožňovali ľahkú replikáciu a distribúciu dát. Adresárový systém tvorený len jedným serverom je veľká výnimka. Bežný adresárový systém sa skladá aspoň z dvoch serverov, ktoré navzájom replikujú svoj obsah. Preto adresárové služby majú inherentne veľmi vysokú dostupnosť a ich výkon možno zvyšovať jednoducho pridaním ďalšieho servera. Toto sú vlastnosti, ktoré vo svete SQL nie sú zďaleka bežné. Ešte dôležitejší je však fakt, že adresárové služby dokážu škálovať veľmi lacno. Adresárový server má typicky relatívne malé výkonové nároky a nie je výnimočné, že replika adresárovej služby je umiestnená na rovnakom sieťovom uzle ako sama aplikácia, ktorá adresárové dáta používa.

Adresárové systémy majú takmer zázračnú škálovateľnosť a dostupnosť. No v technológii všetko má svoju cenu. Adresárové služby za to platia tým, že majú dosť silné obmedzenia týkajúce sa dát, ktoré sa v nich ukladajú. V prvom rade dátový model adresárových systémov je veľmi jednoduchý. Podobne je na tom aj systém vyhľadávania. Napríklad operácia join, ktorá je taká bežná v systémoch SQL, v adresárových službách bežne vôbec neexistuje. Podobne sú na tom indexy, transakcie a v podstate všetky pokročilé databázové operácie. Práve tieto zjednodušenia umožňujú veľmi efektívnu replikáciu dát a sú predpokladom na vysoký výkon systému. Aj keď adresárové služby sú často veľmi pomalé pri zápise údajov, tento nedostatok kompenzujú extrémne vysokou rýchlosťou pri čítaní. Preto sú ideálne na údaje, ktoré sa zriedka menia, ale veľmi často čítajú.

Toto všetko robí adresárové služby ideálnymi na ukladanie údajov o identitách. Tieto údaje potrebujú obrovskú škálovateľnosť a dostupnosť. Ak údaje o identitách nie sú dostupné, celý systém kriticky zlyháva, pretože používateľ sa do systému jednoducho nedostane. Údaje o identitách sa menia zriedka, ale čítajú sa veľmi často. Pri bežnej prevádzke systému je vyhľadávanie v týchto údajoch len veľmi jednoduché a transakcie nie sú potrebné. Preto je adresárový systém jadrom takmer každého riešenia IAM. Adresárový systém slúži ako rýchla, škálovateľná a vysoko dostupná databáza identít, ktorá je zdrojom pre autentifikačné a autorizačné rozhodnutia.

Adresárové systémy, ktoré komunikujú protokolom LDAP, majú však ešte jednu podstatnú výhodu. Tieto adresárové služby sú navrhnuté na to, aby boli zdieľané. Na rozdiel od „sveta SQL", kde každá aplikácia má svoju súpravu databázových tabuliek, „vo svete LDAP" jeden adresárový systém poskytuje zdieľané údaje množstvu aplikácií. Štandardizovaný nie je len prístupový protokol, ale aj podstatné časti dátového modelu. Aplikácie preto vedia, že objekty typu inetOrgPerson majú textový atribút givenName, ktorý obsahuje krstné meno osoby. Táto štandardizácia umožňuje aplikáciám jednoduchú integráciu s adresárovými systémami. Preto dnes už len veľmi zriedka možno nájsť modernú aplikáciu, ktorá by nemala podporu pre LDAP.

Adresárová služba sa dá využívať aj ako jednoduchý autentifikačný server. Veľa aplikácií priamo podporuje autentifikáciu pomocou protokolu LDAP, a preto sa táto metóda často využíva. A je spravodlivé priznať, že pre jednoduché riešenia správy identít je to takmer ideálna metóda. Pri zložitejších riešeniach si však treba uvedomiť, že adresárová služba je v podstate len databáza a nie je navrhnutá ako autentifikačný server. Adresárové servery napríklad neudržiavajú informácie o používateľskej relácii (session), a preto nemôžu priamo poskytovať službu jednotného prihlasovania (single sign-on, SSO). Okrem toho informácie o prihlasovaní nie sú replikované, autorizačné informácie slúžia len na obmedzenie prístupu k dátam v databáze adresárového systému a podobne. Preto takmer každé zložitejšie riešenie IAM potrebuje ďalší komponent: systém riadenia prístupu (access management).

Ďalšie obmedzenie adresárového systému je jeho jednoduchý dátový model. Jednoduchosť je obrovská výhoda pre výkon, škálovateľnosť a dostupnosť, ale je to aj nevýhoda pri správe systému. Adresárová služba typicky poskytuje len jednoduchý systém vnorených skupín. Komplikované prístupové modely založené na rolách (RBAC) sú podporované len veľmi slabo alebo vôbec. Adresárové služby nie sú navrhnuté na komplexnú delegovanú administráciu, správu administračných procesov, samoobslužné služby (ako napríklad reset hesla) a podobne. Adresárový server takisto typicky nie je primárny zdroj informácií, ktoré sú v ňom uložené. Takým zdrojom je väčšinou personalistický systém alebo podobná databáza zamestnancov, zákazníkov, brigádnikov, dodávateľov atď. Bežne je takých zdrojov dokonca niekoľko. A preto treba dáta v adresárovej službe synchronizovať. Na tieto účely je takmer v každom riešení IAM potrebný samostatný komponent: systém na správu identít (identity management, IDM) označovaný aj ako provisioning.

Adresárový systém je kľúčový komponent takmer každého riešenia IAM. S výnimkou veľmi jednoduchých nasadení však nedokáže efektívne pracovať úplne samostatne. V komplexnom riešení IAM je doplnený prvkami na riadenie prístupov (AM) a identít (IDM). A práve o týchto prvkoch budú nasledujúce časti nášho seriálu.

RADOVAN SEMANČÍK
Software architect,
radovan.semancik@evolveum.com
Evolveum, s. r. o.