Základy správy identít a prístupov

Správa identít a prístupov (Identity and Access Management, IAM) je kľúčová oblasť na zaručenie bezpečnosti a efektivity takmer akejkoľvek organizácie. Podnikové prostredie nedokáže efektívne existovať bez týchto technológií, sú nevyhnutné pre telekomunikácie a aj pre profesionálne navrhnutý „cloud".

Napriek tomu, že tieto technológie sú také dôležité, len veľmi málo ľudí im naozaj rozumie. Za viac ako desaťročie praxe s týmito technológiami sme sa stretli s množstvom mýtov a poloprávd, ktoré veľmi často ohrozujú a predražujú implementačné projekty. Pritom technológie správy identít a prístupov nie sú komplikované a možno ich veľmi efektívne nasadiť, ak sa použijú správne. Preto sme sa rozhodli zostaviť seriál o ich princípoch a efektívnom použití.

Základom porozumenia celej oblasti IAM je fakt, že nejde o jednu konkrétnu technológiu. IAM je súbor množstva spolupracujúcich technológií. Jednotlivé prvky riešenia sa kombinujú presne podľa potrieb konkrétneho prostredia. Preto projekty IAM majú veľmi vysokú variabilitu. Ale aj napriek tejto variabilite existujú tri technológie, ktoré možno nájsť v takmer akomkoľvek riešení:

- **Adresárová služba** (*directory service*) udržiava centrálnu databázu používateľov. Takmer všetky moderné adresárové služby využívajú protokol LDAP.
- **Systém riadenia prístupu** (*access management*) vykonáva centrálnu autentifikáciu (SSO), základnú autorizáciu, zaznamenávanie (audit) prístupov a podobne.
- **Provisioning systém** zabezpečuje správu databázy používateľov, jej synchronizáciu (napr. s personalistikou), riadi bezpečnostnú politiku a podobne.

Tieto tri technológie sa navzájom dopĺňajú. Akékoľvek netriviálne riešenie IAM nevyhnutne potrebuje všetky tri technológie, aby bolo kompletné. Ani jednu z nich nemožno vynechať alebo zanedbať. Napríklad adresárová služba môže slúžiť na autentifikáciu používateľov a často sa tak aj v jednoduchých riešeniach využíva. Táto metóda je však silne obmedzená a pri profesionálnych riešeniach ju treba nahradiť plnohodnotným systémom na správu prístupov. Ďalší príklad je synchronizácia používateľských databáz. Takmer každá organizácia má aspoň dve používateľské databázy: personalistiku a doménu (Active Directory). V jednoduchých riešeniach sa tieto databázy synchronizujú ručne, čo je pomalé, chybové a potenciálne otvára veľké bezpečnostné riziká. Zapojenie systému provisioningu do riešenia IAM tieto problémy odstráni. Preto len kombinácia všetkých troch technológií vytvorí uspokojivé riešenie.

Adresárová služba (directory service) je komponent, ktorý sa dá nájsť azda v každom nasadenom systéme. Pri menších podnikových nasadeniach je to často známe Active Directory, pri väčších škálovateľných systémoch sa často používa systém dedikovaných LDAP serverov. Nech je už použitý akýkoľvek produkt, základný princíp je rovnaký: adresárová služba je špecializovaná databáza používateľov. Adresárová služba je už svojím návrhom prispôsobená údajom o identitách. Výkon systému je vyladený na údaje, ktoré sa zriedka menia, ale zato veľmi často čítajú, sú tu špeciálne atribúty pre heslo, fotografiu a podobne. Použitie vhodnej adresárovej služby je základ azda každého riešenia IAM. No hoci je adresárová služba špecializovaná na údaje o identitách, stále je to len databáza. Adresárová služba ukladá a efektívne vyhľadáva údaje, ale možnosti transformácie údajov takmer neexistujú. Adresárová služba ukladá heslo a podobné „credentials", ale možnosti použitia týchto údajov na priamu autentifikáciu sú silne obmedzené. Kľúčový bod pri efektívnom riešení IAM je uvedomiť si, že adresárová služba je len databáza, a zložitú logiku prenechať ostatným komponentom.

Niektoré nedostatky adresárových služieb riešia systémy na správu prístupu (access management, AM). Tieto systémy spolupracujú s aplikáciami alebo aplikačnými bránami tak, aby dokázali spracovať akýkoľvek prístup k aplikáciám. Vo svete webových aplikácií sa to rieši najmä presmerovaním autentifikačných stránok aplikácie na systém AM. Ten vykoná autentifikáciu používateľa (a to aj viacfaktorovú) a presmeruje spojenie naspäť na aplikáciu. Systém AM dokáže vykonať aj čiastočnú autorizáciu prístupu, aj keď granularita autorizácie je zväčša obmedzená len na úroveň aplikácie ako celku. Udalosť vykonania autorizácie sa na strane systému AM zaznamená, čo slúži na účely auditu, ale aj na zjednodušenie prihlasovania. Používateľ prihlásený do jednej aplikácie môže pristúpiť na ďalšiu aplikáciu bez nutnosti prihlasovať sa znova. Moderné riešenia AM implementujú federáciu identít medzi organizáciami, integráciu na sociálne siete a podobne.

Služby poskytované systémami AM sú povestným svätým grálom technológií IAM. Tieto služby sú to, čo používatelia vidia, sú to, čo používatelia a vedenie firiem chcú dosiahnuť. No ako to už zvyčajne býva, ani toto nie je také jednoduché, ako by sa zdalo. Na to, aby systém AM dobre pracoval, musí mať k dispozícii zjednotenú databázu používateľov. To možno znie triviálne, ale v praxi to rozhodne nie je jednoduché. Pre veľa organizácií sú ťažké aj také zdanlivo jednoduché veci ako zabezpečiť jednotný identifikátor (login name) na prihlásenie do všetkých aplikácií. Niektoré aplikácie používajú priezvisko, iné osobné číslo, ďalšie kombináciu prvých písmen priezviska s náhodným číslom a podobne. Pritom pokiaľ sa nezjednotí identifikátor, systém na riadenie prístupu je takmer bezmocný. A ani po zjednotení identifikátora sa problémy nekončia. Ak je identifikátor založený na priezvisku, mení sa prekvapivo často, najmä vďaka svadbám. V tomto prípade treba zabezpečiť synchronizovanú zmenu identifikátora medzi centrálnou databázou (adresárová služba) a databázami všetkých relevantných aplikácií. A táto úloha je v praxi oveľa zložitejšia, ako sa zdá.

Tu vstupuje do hry posledný komponent: systém provisioningu. Hlavná zodpovednosť tohto systému je synchronizovať údaje v adresárovej službe, aplikáciách, personalistických systémoch a podobne. V ideálnom prípade by dáta mali existovať len v jednej databáze. Toto je však možné len v extrémne jednoduchých systémoch. V praxi je takýchto databáz niekoľko a systémy s desiatkami alebo aj stovkami databáz nie sú úplne výnimočné. Všetky tieto databázy musia zostať konzistentné, inak sa celý systém rozpadne. Konzistencia databáz je presne to, čo systém provisioningu zabezpečuje, preto je tento systém svojím spôsobom úplne najdôležitejším komponentom riešenia IAM. Okrem toho systém provisioningu aplikuje bezpečnostné politiky, transformuje údaje, riadi pracovné procesy, poskytuje samoobslužné služby a podobne.

Je takmer nemožné postaviť plnohodnotné riešenie IAM bez ktoréhokoľvek z týchto troch komponentov. Adresárový systém, riadenie prístupu a riadenie identít pomocou systému provisioningu sú kľúčové prvky riešenia IAM. Názov Identity and Access Management hovorí sám za seba.

V ďalších častiach seriálu podrobnejšie opíšeme každú z týchto troch technologických oblastí a neskôr sa budeme venovať aj tomu, ako z nich postaviť efektívne riešenie.

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