

Stratégia odľahčenia IAM - Dedikovaný STS pre integrácie

Slovensko.Digital

Manažérske zhrnutie

- Modul IAM (Identity Access Management) Ústredného portálu verejnej správy (ÚPVS) má podľa informácií MIRRI a NASES kapacitný problém, kvôli ktorému sa zdôvodňuje nákup novej neobmedzenej licencie pre modul IAM za cca 17 miliónov eur.
- Súčasný modul IAM je proprietárne a technologicky zastarané riešenie, ktorého licencie nie možné získať od iného ako súčasného dodávateľa. Súčasný riešenie je limitované aj tým, že musí byť nasadené v špeciálnom prostredí Oracle.
- Modul IAM zabezpečuje autentifikáciu používateľov ako aj iných informačných systémov (tzv. system-to-system integrácia pomocou technických účtov).
- Súčasná architektúra ÚPVS však umožňuje využívať na autentifikáciu viacero tzv. Security Token Service (STS), čo otvára priestor aj pre iné alternatívy riešenia problému záťaže modulu IAM.
- Odporúčame okamžite vykonať analýzu toho, koľko požiadaviek a záťaže generujú na modul IAM používatelia a koľko system-to-system integrácie. Za predpokladu, že výraznú časť záťaže generujú práve integrácie je vhodné zvážiť alternatívu vytvorenia paralelnej služby STS, ktorá by slúžila výhradne na autentifikáciu pre integrácie, ktoré nevyžadujú zložité zastupovania (ako je tomu v prípade prihlasovanie používateľov a niektorých integrácií).
- Vytvorenie novej paralelnej dedikovanej STS služby pre integrácie je možné pomocou existujúcich riešení vo veľmi krátkom časovom horizonte a zasadenie do súčasnej architektúry ÚPVS je možné bez zmeny na strane konzumentov služieb (integrátorov) a len s minimálnymi zmenami na strane súčasných služieb ÚPVS.
- Takéto krátkodobé riešenie umožní okamžité odľahčenie súčasného modulu IAM a horizontálnu škálovateľnosť dedikovanej služby STS pre integrácie a možnosť nasadiť ho v otvorenom prostredí neviazanom na jedného dodávateľa (Oracle).

Aktuálny stav

- Súčasný proprietárny modul IAM je podľa informácií MIRRI a NASES na hrane kapacity, pričom je limitovaný najmä licenčnou politikou, ktorá sa viaže na počet využívaných jadier.
- Modul IAM je nutné prevádzkovať v prostredí od spoločnosti Oracle, čo limituje možnosti nasadenia na nové moderné škálovateľné kontanerizačné a virtualizačné prostredia.
- Posudok 158/2024 od znalca z 10.7.2025 tvrdí, že licencie IAM sú limitované napočet jadier (vCPU alebo CPU) a prevádzka presahuje zazmluvnený počet 68, pretože sa využíva 48 (v prostredí fix) + 112 (v prostredí PROD) = 160 celkovo.
- Podľa z [verejne dostupných informácií](#) bol počet prihlásení v roku 2022 na slovenko.sk za deň maximálne (~117.000 prihlásení dňa 31.3.2022 - daňové priznania). Medián ~58.900 prihlásení, 90. percentil ~76.600 prihlásení). Z uvedeného je zrejmé, že modul IAM dokázal v minulosti spracovávať aj 2x vyššiu záťaž ako je bežná prevádzka.
- Pôvodné kapacitné plánovanie pre celý ÚPVS vychádza z predpokladov pôvodnej štúdie ÚPVS, podľa ktorej budú ÚPVS používať milióny ľudí.
- NASES plánuje nakúpiť neobmedzenú licenciu pre modul IAM od súčasného dodávateľa s predpokladanou hodnotou zákazky 17 miliónov eur.
- Architektúra ÚPVS bola navrhnutá tak, že umožňuje aj decentralizovanú správu prístupov k službám - t.j. je možné mať aj viac IAM modulov.
- Pôvodný plán prerábky ÚPVS rátal s postupným a úplným nahradením modulu IAM za štandardné a bežne dostupné riešenie.

Navrhované riešenie

Okrem alternatívy okamžitého nákupu proprietárneho a technologicky zastaralého modulu IAM v neobmedzenej licencií je potrebné zvážiť aj alternatívu dočasného odľahčenia súčasného modulu IAM tým, že sa vytvorí "ľahký horizontálne škálovateľný dedikovaný STS pre integrácie".

Súčasná architektúra ÚPVS umožňuje, aby prístupové tokeny boli vydávané viacerými službami (STS). Na koncových službách (napr. Schránky, G2G) je nutné len vytvoriť "trust", pridaním nového kľúča, ktorému služby dôverujú. Keďže táto operácia je pomerne bežná (rotácie kľúčov sa robia aj kvôli bezpečnosti), ide o jednoduchú konfiguračnú zmenu. Keďže všetky integrácie sú smerované cez dedikované ipsec tunely, výmena IAM modulu môže byť pre konzumentov (integrátorov) úplne transparentná.

Problematickejšie môžu byť integrácie, ktoré vyžadujú okrem "registrácie kľúča" aj špeciálne zastupovania (OnBehalfOfID), ktoré vyžadujú zložitejšiu logiku kontroly, avšak keďže ide o pomerne novú funkcionality, predpokladá sa, že nová dedikovaná STS služba sa obmedzí len na integrácie, ktoré túto funkcionality nepotrebujú.

Plán

1. Okamžite vytvoriť report, ktorý analyzuje akú časť záťaže na modul IAM generujú system-to-system integrácie (napr. analýzou prístupových logov). Zároveň vyhodnotiť, ktoré konkrétne systémy/integrácie generujú najväčšiu záťaž na modul IAM.
2. Ak sa preukáže, že integrácie generujú dostatočne veľkú záťaž, okamžite začať s vytváraním dedikovanej paralelnej STS služby. Tú je možné vytvoriť pomocou dostupných hotových riešení, ale pomerne jednoducho aj priamo interne (napr. implementáciou pomocou Apache CXF).
3. Nasadenie do FIX prostredia pre vybrané integrácie a testovanie.
4. Nasadenie do PROD prostredia pre vybrané integrácie a testovanie.

Silné a slabé stránky riešenia

Silné stránky

- Okamžité rýchle riešenie vysokej záťaže IAM
- Očakávané nízke vstupné a prevádzkové náklady oproti nákupu proprietárneho softvéru, ktorý je potrebné aj tak strednodobo úplne nahradiť.
- Možnosť horizontálne škálovať a prevádzkovať riešenie na novej modernej kontainerizačnej a virtualizačnej platforme.
- Plná kontrola štátu nad riešením, bez obmedzujúcich licenčných podmienok.
- Možnosť okamžite zvýšiť bezpečnosť pre integrácie oproti proprietárnemu zastaralému riešeniu.

Slabé stránky

- Len dočasné riešenie prípadného stavu vysokej záťaže.
- Paralelná evidencia prístupov - súčasný modul IAM má integrovanú samobslužnú správu kľúčov používateľmi.

Mitigácia: Synchronizácia autentifikačných kľúčov do nového riešenia je možná v súčinnosti so súčasným dodávateľom.

Záver

Táto alternatíva riešenia je explicitne navrhnuté ako **krátkodobé opatrenie**, ktoré zabezpečí okamžité riešenie potenciálnych výkonnostných problémov. Umožní získať čas na skutočne dlhodobé riešenie, ktoré by sa malo zamerať na **otvorené a široko podporované riešenia** namiesto drahých proprietárnych produktov a služieb.