

ČSOB Stavební: Bezproblémová migrace z OpenAM na Wren:AM

ČSOB Stavební potřebovala modernizovat svůj Identity Server, který po letech provozu na technologii OpenAM 13 přestal vyhovovat z hlediska dalšího rozvoje i náročnosti údržby. Pro zajištění kontinuity služeb pro více než milion klientů, téměř 1 500 obchodních zástupců a 19 napojených aplikací jsme navrhli a realizovali migraci na Wren:AM.



Výchozí situace

ČSOB Stavební od roku 2017 provozovala Identity Server (IDS) založený na upravené verzi OpenAM 13 a úložišti OpenDJ.

Na řešení byla napojena řada systémů včetně Klient-ské zóny, Nová eLiška či Salesforce. Přes IDS se ověřují klienti ČSOB Stavební (OIDC), obchodní zástupci ČSOB Stavební (OIDC), zaměstnanci ČSOB Stavební (Kerberos), klienti ČSOB (přenos autentizace) a zaměstnanci ČSOB (RADIUS).

Během let se potvrdila robustnost řešení postaveného na komerčně podporovaném open source softwaru i jeho schopnost pružně reagovat na nové požadavky. Po šesti letech provozu však OpenAM 13 pochopitelně zastaral a původní výrobce navíc ukončil open-source vývoj. To s sebou přineslo rostoucí náročnost údržby systému a potřebu buď upgradovat jádro řešení, nebo přejít na nový systém.

Cílem proto bylo odstranit technický dluh, zachovat bezproblémový provoz integrovaných systémů a připravit řešení na budoucí rozvoj.

Původní aplikace měla omezené možnosti dalšího rozvoje. Současně jsme potřebovali zavést systém pro autorizaci a autentizaci uživatelů do frontendových aplikací (Klientská zóna, NeL atd.)

— Pavel Jiránek, vedoucí IT Operations, ČSOB Stavební

Základ řešení: Wren:AM

Vzhledem ke komplexnosti celého systému a nákladům na jeho budování jsme spolu s GEM System, jakožto systémovým integrátorem, navrhli variantu, jak vyřešit problém vzniklého technického dluhu, aniž by ČSOB musela investovat do přechodu na zcela jiný systém.

Po zvážení alternativ se ČSOB Stavební rozhodla pro přechod na **Wren:AM**, **přímého open-source nástupce systému OpenAM** s dostupnou podporou v ČR. Toto řešení bylo nejdosazitelnější a nejvýhodnější z hlediska celkových nákladů na vlastnictví.

Náš přístup k řešení

Pro řízení přechodu tak byl vyvinut komplexní migrační plán postavený na automatizaci úloh a přístupu „Infrastructure as Code“ (IaC).

Celý postup byl ověřen na DEV prostředí, aby byla zajištěna správná funkčnost, a během procesu došlo k aktualizaci performance testů a byla poskytnuta asistence při upgradu na vyšších prostředích (TEST, PREP a PROD).

Implementace také zahrnovala provedení **performance a penetračních testů** v souladu se standardy ČSOB Stavební.

Klíčové výzvy

Přechod znamenal vybudování nového prostředí a zavedení jiného způsobu nasazování i provozu.

Největší výzvou bylo, že AM byl i v době migrace živý systém, s nímž bylo **integrováno 19 aplikací, které měly i po přechodu fungovat bez větší revize jejich integrací**. Při přechodu bylo dále potřeba:

- zachovat původní nastavení domén (realms) a **kontinuitu používání služeb na ESB** jako SMS Service a Mail Service;
- zajistit nepřetržité funkce registrovaných technických účtů pro integrované systémy;
- zachovat formát auditního logu – kompatibilita uložení ve formátu CEF;
- zajistit **opakovatelnost migrace** včetně možných přechodů mezi novým a starým řešením, pokud by některé integrované systémy vykazovaly problém.

Výsledky projektu

- Podařilo se přejít na podporovaný systém a zajistit **kontinuitu služeb** pro aplikace i audit.
- Výrazně se **snížily náklady a pracnost** díky automatizaci a snadným aktualizacím.
- Dostupnost služeb nebyla migrací prakticky ovlivněna a integrované aplikace nevyžadovaly žádné úpravy.
- Bezpečnost i propustnost systému se zvýšily.
- Nový systém bez problému zvládá vytíženost:
 - **1 000 požadavků na AM za minutu**
 - **1 000 paralelních session**
 - **10 000 aktivních paralelních tokenů (CTS)**
- Zavedené přístupy připravily řešení na případný budoucí provoz v kontejnerizovaném prostředí.

Vytvořili jsme další bezpečnostní prvek pro přístup do cílových systémů, který splňuje nejvyšší bezpečnostní standardy s možností rozšíření na širokou škálu dalších IT systémů. Součástí bylo i rozšíření o 2FA autentizaci. Pracovníci dodavatele byli kdykoliv na telefonu a technická úroveň lidí byla vysoká. Proaktivně navrhovali nová řešení a byli velmi ochotní předávat pracovníkům objednatelů potřebné know-how i z jiných IT oblastí.

— Pavel Jiránek, vedoucí IT Operations, ČSOB Stavební

O klientovi

ČSOB Stavební spořitelna, a.s. patří do skupiny ČSOB drží pozici nejvýznamnější stavební spořitelny v České republice s bilanční sumou 120,5 mld. Kč (téměř 30% podíl na trhu). O přes jeden milion klientů se na více než 200 obchodních místech stará téměř 1500 obchodních zástupců.

O Orchitechu

Pomáháme IT oddělením řídit přístup v komplexních prostředích. Specializuje se na řešení v oblasti Identity & Access Managementu.

Působíme na trhu přes 18 let a realizovali jsme více než 100 projektů pro 50 klientů z veřejného i soukromého sektoru.