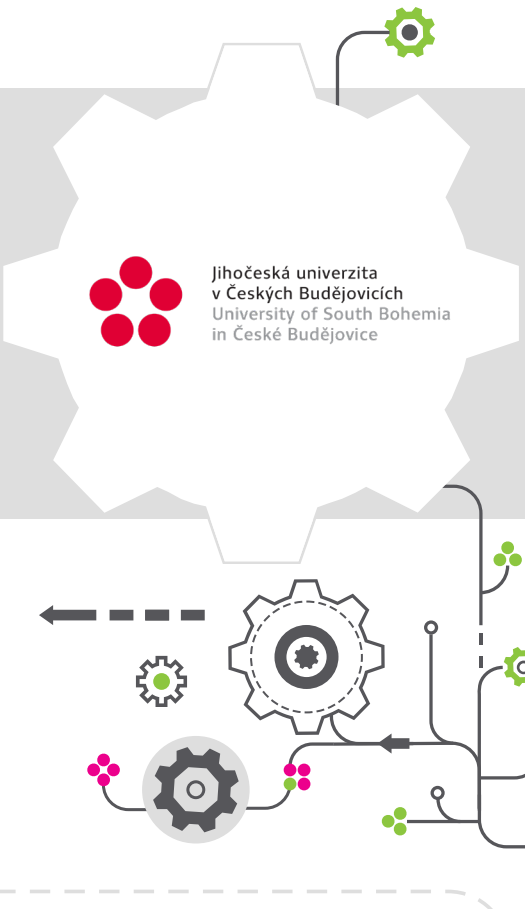
Případová studie

Jihočeská univerzita: Efektivní správa identit s Wren:IDM

Jihočeská univerzita v Českých Budějovicích z důvodu neudržitelnosti původního řešení potřebovala nový spolehlivější způsob řízení identit pro prostředí s tisíci studenty, pravidelnými nástupy a odchody i množstvím systémů. Orchitech uspěl s řešením Wren:IDM díky jeho flexibilitě, rychlosti, transparentním nákladům a schopnosti přizpůsobit se specifickým procesům univerzity bez zbytečné složitosti.



Když staré řešení nestačí

Původní IDM od společnosti Novell přestalo Jihočeské Univerzitě vyhovovat. Implementace procesů zastarala, byla chybová a jakkoliv upravit konfiguraci bylo složité.

„V původní implementaci bylo v podstatě nemožné provést rekonciliaci, tj. srovnání chtěného a aktuálního stavu systému, který se z nějakého důvodu rozsynchronizoval," uvádí k původnímu stavu pan Marek, vedoucí Útvaru informační infrastuktury Jihočeské univerzity. Dále došlo ke změně cenové politiky výrobce původního systému na nacenění dle počtu identit. Těch má univerzita desítky tisíc, čímž se licence neúměrně a neudržitelně prodražily. Univerzita tak musela přistoupit ke změně systému.

Tím se otevřelo okno příležitosti k implementaci procesů dle aktuálních potřeb a řadě vylepšení. *„Univerzita dopředu tušila, že bude lepší přejít na nový systém. Hlavním parametrem pro výběr nového systému přitom bylo TCO, tedy snížení nákladů oproti původnímu řešení,"* říká pan Marek.

Total Cost of Ownership

Univerzita v rámci výběru dodavatele kalkulovala pětileté celkové náklady zahrnující licenční poplatky, maintenance, podporu a opci na rozvojové práce v rozsahu až 1000 hodin. Podmínkou bylo předání kompletních konfigurací tak, aby nevznikla závislost na dodavateli. Kvůli tomu také preferovali open-source platformu. Řešení od Orchitechu nabídlo transparentní cenovou politiku a univerzita nový systém získala za cenu jednoho roku licenční podpory předchozího řešení.

Orchitech zvítězil ve výběrovém řízení a dodal řešení postavené na produktu Wren:IDM, open-source nástupci projektu OpenIDM. Flexibilita Wren:IDM umožnila snadno implementovat i požadavky dané specifickým univerzitním prostředím, včetně přizpůsobeného uživatelského rozhraní.

> *Získali jsme zcela nový systém, který je spolehlivější, rychlejší, predikovatelnější a v případě havárií lze stav jednoduše narovnat, ať už na vstupu do IDM, kdy si IDM "dohraje" změny ze zdrojového systému, nebo naopak když zkontroluje a sjednotí stav v cílovém systému.*
>
> — Ing. Jan Marek
> vedoucí Útvaru správy informační infrastruktury
> Jihočeská univerzita

Problémy odhaleny již při implementaci

Při implementaci jsme s využitím synchronizace v režimu simulovaného zápisu („dry run") objevili řadu problémů konzistence dat, které přetrvávaly z původního IDM:

- V Active Directory jsme odhalili řadu nekonzistencí v atributech (mezery za jménem, čárky v DN apod.).
- Konvence pro uživatelské jméno v některých případech generovaly jméno delší než 20 znaků, a docházelo tak k překročení limitu v AD (původní nahrazované IDM jméno bez chyby zkrátilo).
- Hesla obsahovala řadu neshod, neboť heslové politiky původního IDM nebyly sladěny s požadavky AD. Data v původním IDM tak nebyla v souladu s daty AD.
- Další nepřesnosti byly v e-mailových adresách vygenerovaných původním IDM, které neodpovídaly požadovanému algoritmu. Nové IDM tyto problémy napravilo.
- LDAP pro FreeRADIUS obsahoval vícehodnotové záznamy v atributech, které měly být single-value. Původní IDM problém nehlásilo, a některé účty tak mohly být interpretovány mylně.
- Některé systémy vynucovaly referenční integritu, kterou IDM mělo zohlednit mj. správným pořadím zakládání a modifikace záznamů. Jelikož se toto nedělo, operace původního IDM mohly končit chybou a data nebyla řádně synchronizovaná.

Díky včasné identifikaci jsme tyto problémy vyřešili začištěním dat a úpravou IDM skriptů, a tak následný přechod do produkce proběhl hladce.

Specifika řešení

- **70 000 identit** (15 000 aktivních)

5 zdrojových systémů:

- systém pro studijní agendu IS/STAG
- personální systém EGJE
- systém pro celoživotní vzdělávání
- karetní systém
- evidence budov a místností

10 řízených systémů:

- MS Active Directory
- LDAP
- PostgreSQL DB
- RADIUS LDAP
- karetní systém
- knihovní systém
- a další

Udržení kontinuity při opuštění univerzity

Uživatelé mohou využívat některých služeb i určitou dobu po opuštění univerzity – třeba přistupovat k univerzitní emailové schránce.

Toto jsme vyřešili zavedením konfigurovatelných karenčních lhůt. Lhůty jsou specifické pro různé typy identit a jejich parametry lze libovolně upravovat. Pro každou identitu je při jejím ukončení vypočítána doba uchování. Až po jejím uplynutí dojde ke skutečnému ukončení identity a zablokování přístupů. Na vypočítanou dobu uchování jsou navázány i další procesy, např. nastavení přesměrování pošty na osobní e-mail.

Skartace osobních údajů

Správa identit je ze své podstaty vhodným nástrojem pro automatickou správu osobních údajů v řízených systémech, zejména často opomenutých procesů skartace, stanovených GDPR. Skartaci osobních údajů vyžaduje také ÚOOÚ.

V univerzitní praxi se ale objevují specifické výzvy. Může jít třeba o studenty nastupující na navazující studia nebo zaměstnance, kteří se vracejí pouze na jeden semestr. Okamžitá skartace dat by přinášela problémy při zachování kontinuity dat ve všech systémech organizace. Proto ji nejprve nahrazuje tzv. pseudonymizace. Ta sice smaže nepotřebné osobní údaje z identity, ale stále je možné provádět korelaci s využitím hashe unikátního identifikátoru identity. V takovém případě se identita obnoví načtením dat z personálního systému.

Až po uplynutí nastavené lhůty dochází ke skartaci, tedy ke kompletnímu smazání identity a navázaných vztahů.

Správa hostovských identit

Na veřejných vysokých školách je běžná velká fluktuace identit. Kromě studentů jde třeba o hosty konferencí a externí spolupracovníky, kteří potřebují vybrané přístupy jako WiFi a přístupové karty. Proto IDM umožňuje správu dočasných identit, resp. hostovských identit. Správu provádí administrátoři v rámci jednotlivých fakult, kde mohou pro každou fakultu definovat omezení – třeba maximální platnost či prefix uživatelského jména.

Celouniverzitní administrátoři mohou spravovat hostovské identity pro všechny fakulty. IDM se po založení hostovské identity postará o celý životní cyklus, přidělí všechny potřebné přístupy a ve správný čas zařídí jejich odebrání.

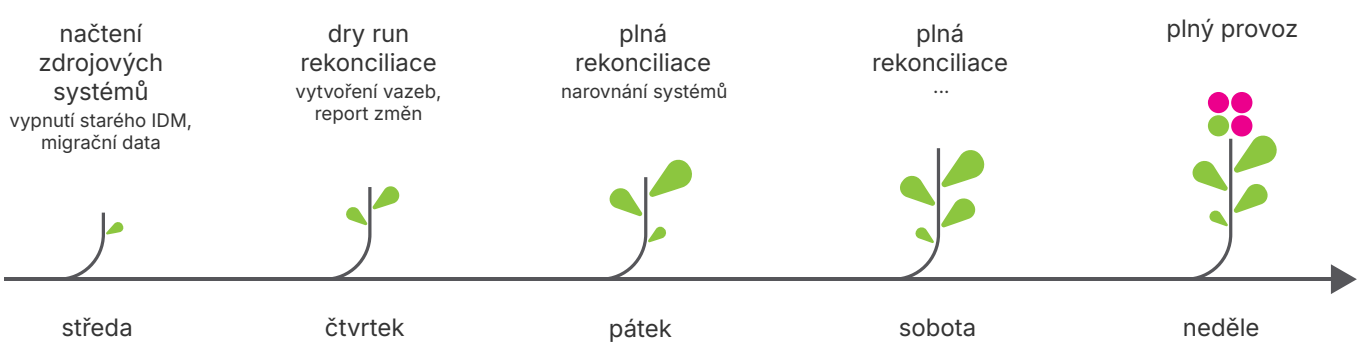
Migrace

Díky pečlivé přípravě proběhla kompletní produkční migrace během necelého týdne. Přechod na nové IDM proběhl bez výpadku a bez dopadu na koncové systémy a uživatele. Po přechodu dramaticky klesla chybovost zpracování IDM procesů.

Statistiky celé migrace:

- **14 000** korektně napárovaných validních účtů
- **33 000** zakázaných účtů bez vlastníka (účty bývalých studentů)
- **80** nesprávně povolených účtů (účty, které měly být zakázány, ale nebyly)
- **8** chybějících účtů (účty, které dle IDM měly existovat, ale neexistovaly)

Průběh migrace:



Přínosy pro univerzitu

Cílem projektu bylo zvýšit spolehlivost, snížit provozní náklady a získat plnou kontrolu nad životním cyklem identit v celé univerzitní infrastruktuře. To vše se podařilo v rámci projektu naplnit.

Implementace Wren:IDM na Jihočeské univerzitě ukázala, že moderní řízení identit dokáže výrazně zlepšit provozní efektivitu, bezpečnost i dlouhodobou udržitelnost IT prostředí, a to i v organizaci s velmi specifickými nároky a vysokým počtem identit.

> *IDM nasazený firmou Orchitech si nás získal svojí rychlostí a spolehlivostí. Dle systému RT teď řešíme o 80 % méně požadavků. Zbylých 20 % pak tvoří převážně jen zapomenutá hesla. Řešení pokrylo všechny naše potřeby, a to ve slíbeném termínu.*

— Ing. Jan Marek
vedoucí Útvaru správy informační infrastruktury
Jihočeská univerzita

o 80 %

méně incidentů souvisejících se správou identit a přístupů

Nižší TCO

díky open-source platformě a transparentnímu modelu provozu

Snížení zátěže IT

většina procesů nad identitami je nyní plně automatizovaná

Připravenost

na audit a legislativní požadavky (GDPR, bezpečnost dat)

Zajímá vás, jak může IDM pomoci i vaší organizaci?

Rádi se podělíme o další zkušenosti z univerzitního, veřejného i soukromého sektoru.

O klientovi

Jihočeská univerzita v Českých Budějovicích patří mezi deset největších univerzit v ČR. Navštěvuje ji přes deset tisíc studentů, jejichž výuka zaměstnává stovky pracovníků.

Řízení přístupů k IS/IT je na JU náročné nejen kvůli počtu identit, ale i díky pravidelnému nárazovému příchodu a odchodu studentů v jednotlivých studijních obdobích.

S Orchitechem spolupracuje již od roku 2014.

O Orchitechu

Pomáháme IT oddělením:

- efektivně řídit identity a přístupy
- automatizovat rutinní činnosti
- zvyšovat bezpečnost
- šetřit čas a náklady

Naše řešení zajišťují soulad s legislativními požadavky, včetně GDPR, NIS2, nového kybernetického zákona a dalších. Působíme na trhu od roku 2008 a realizovali jsme již více než 100 projektů pro 50 klientů z veřejného i soukromého sektoru.

https://orchi.tech/ +420 216 216 850 info@orchitech.cz

orchitech