|  |  |
| --- | --- |
|  | UNIVERZITA KARLOVA |
|  |

**Specifikace napojení midPoint**

**Projekt:**

RUK - OV - Dodávka, podpora a rozvoj CAFM systému na Univerzitě Karlově

**Fáze:**

VZ

Obsah

[1 Úvod 3](#_Toc171605088)

[2 Požadavky 3](#_Toc171605089)

[2.1 Požadavky na API koncového systému pro správu objektů z IdM midPoint 3](#_Toc171605090)

[2.1.1 Technické parametry 3](#_Toc171605091)

[2.1.2 Operace s objekty 3](#_Toc171605092)

[2.1.3 Seznam oprávnění 7](#_Toc171605093)

[2.1.4 Nefunkční požadavky 7](#_Toc171605094)

[2.1.5 Rychlost odezvy rozhraní koncového systému 7](#_Toc171605095)

[2.1.6 Ostatní 7](#_Toc171605096)

# Úvod

Cílem tohoto dokumentu je specifikovat požadavky a možnosti integrace pořizovaného CAFM systému s IdM midPoint.

# Požadavky

Předpokládáme, že veškeré integrace dat, která jsou svojí povahou založena na malých objektech, budou prováděny prostřednictvím IdM systému midPoint. Malým objektem se v tomto případě rozumí jednoznačně identifikovaná entita, která má pevně daný seznam možných vlastností (schéma). Vlastnosti jsou reprezentovány dvojicí název, hodnota (hodnoty pro vlastnosti stejného názvu mají stejný datový typ). Typickým příkladem takového malého objektu je uživatel, ale mohou jím být i další objekty (budova, skupina, oprávnění). Velké objekty (tj. objekty s vlastnostmi, jejichž datové typy jsou příliš velké - například obrázky, mapy atd.) se k integraci prostřednictvím midPointu nehodí a bude-li požadováno jejich sdílení s dalšími systémy, musí být realizováno jiným způsobem, stejně tak jako objekty, které nelze jednoznačně identifikovat.

## Požadavky na API koncového systému pro správu objektů z IdM midPoint

Vlastník koncového systému poskytuje na straně koncového systému technické rozhraní, které je voláno ze strany Identity management midPoint za účelem vzdálené správy uživatelských účtů a rolí registrovaných v koncovém systému (obecně objektů).

### Technické parametry

Rozhraní musí splňovat následující parametry:

* Aplikační rozhraní (WS SOAP, REST, Java API, SSH apod.) nebo rozhraní datového úložiště (LDAP, DB procedury, DB tabulka),
* bezpečný přenos dat mezi midPoint a rozhraním koncového systému (např. SSL/TLS),
* midPoint se k rozhraní autentizuje dedikovaným technickým uživatelem.

Použití DB tabulky/view pro rozhraní IdM-koncový systém je doporučováno pouze pro read-only systém. Pro připojení úložiště uživatelů prostřednictvím relační databáze doporučujeme použití uložených DB procedur, které vytváří vlastník koncového systému.

Preferovaný způsob napojení je pomocí aplikačního rozhraní koncového systému (WS, LDAP, API apod.).

V následujícím textu se primárně předpokládá zpracování uživatelů a rolí nebo skupin na koncovém systému. Ovšem rozhraní midPointu je navrženo tak, že umožňuje zpracovávat libovolné typy objektů (uživatelské profily, telefonní čísla apod.). Rozsah implementace aplikačního rozhraní konkrétního koncového systému vždy určuje konkrétní analýza.

### Operace s objekty

Níže je uveden rozsah operací, které musí podporovat rozhraní koncového systému (KS) tak, aby mohly být řízeny objekty uložené v tomto systému. Je uveden maximální požadovaný rozsah funkcionalit. Pokud některá operace v systému neexistuje, na rozhraní logicky existovat také nemusí – například zplatnění/zneplatnění účtu, změna hesla atd. nejsou v některých systémech implementovány. Zneplatnění je operace, která účet v koncovém systému fyzicky zachová, na účet se však není možné přihlásit ani pod ním v koncovém systému provádět žádné funkce. Operace zplatnění pak vrací účet do aktivního stavu se všemi původními možnostmi.

Jednotlivé operace rozhraní mohou být implementovány dle níže uvedené struktury jako samostatné pojmenované operace. Alternativně mohou být operace sdíleny v rámci jedné pojmenované operace rozhraní - příklad: Operace zplatnění je speciální případ aktualizace a je tak realizována v rámci operace update(), přičemž interní logika update() rozezná na základě měněného atributu, zda se jedná pouze o aktualizaci účtu nebo rovněž o zplatnění účtu.

Konkrétní implementaci operací rozhraní a jejich význam pro data koncového systému určuje vlastník koncového systému.

#### Create – založení objektu

**Popis:** Založení nového objektu na KS.

**Vstup:** uživatelské jméno nebo název objektu, ostatní atributy s vyplněnou hodnotou; atributy bez hodnoty nejsou zasílány

**Výstup:** unikátní ID objektu vygenerované koncovým systémem (není součástí vstupu z IdM)

**Možné návratové stavy:**

* úspěch – objekt byl v koncovém systému založen
* duplicita – pokus o založení již existujícího objektu
* jiná chyba – jiná nespecifikovaná chyba
* chyba syntaxe – (volitelné) pokus o vložení nepovolené hodnoty (např. řetězce do číselného atributu)

#### Delete – smazání objektu

**Popis:** Smazání objektu na KS.

**Vstup:** unikátní ID objektu evidované koncovým systémem (získaný dříve při operaci Create)

**Výstup:** zpráva o úspěchu nebo neúspěchu operace

**Možné návratové stavy:**

* úspěch – objekt byl v koncovém systému smazán
* neexistence – pokus o smazání neexistujícího objektu
* jiná chyba – jiná nespecifikovaná chyba

#### Search – seznam objektů daného typu

**Popis:** Výpis všech objektů daného typu (uživatelé, role) na KS, včetně neaktivních. Výpis musí obsahovat minimálně unikátní ID objektu a název objektu, volitelně může obsahovat i ostatní atributy.

Filtr: Preferujeme možnost volitelně zadat i filtrování podle názvu objektu (uživatelské jméno, název role apod.); filtrování na ostatní atributy (podle osobního čísla, podle zkratky role apod.) je vítané, ale není povinné

**Vstup:** typ objektu, který chceme získat; volitelně i filtr

**Výstup:** seznam všech objektů specifikovaného typu; pokud je zadán filtr tak jen těch, které odpovídají filtru

**Možné návratové stavy:**

* úspěch – seznam objektů
* jiná chyba – jiná nespecifikovaná chyba

#### LiveSync – seznam objektů, na kterých došlo v určeném časovém okně ke změně

**Popis:** Rozšířená akce Search, která poskytuje výpis objektů daného typu (uživatelé, role) na KS, na kterých došlo v definovaném časovém okně ke změně. Výpis musí v tomto případě obsahovat unikátní ID objektu název objektu a povinně i všechny atributy.

LiveSync může být součástí operace Search, pokud je možné v jejím filtru definovat časové okno od – do.

Operace LiveSync nemusí být implementována, pokud není nutné sledovat změny KS v reálném čase. Rozhodnutí o implementaci je provedeno na základě konkrétních požadavků a analýzy.

**Vstup:** typ objektu, který chceme získat a povinně i časové okno od - do

**Výstup:** seznam všech objektů změněných v časovém okně od - do

**Možné návratové stavy:**

* úspěch – seznam objektů
* jiná chyba – jiná nespecifikovaná chyba

#### Get – detail požadovaného objektu

**Popis:** Detail objektu z KS; Výpis musí obsahovat ID objektu, název objektu a ostatní (i nevyplněné) atributy. Může být součástí operace Search.

**Vstup:** unikátní ID objektu evidované koncovým systémem (získaný dříve při operaci Create)

**Výstup:** detail požadovaného objektu včetně unikátního ID

**Možné návratové stavy:**

* úspěch – detail objektu
* neexistence – pokus o získání neexistujícího objektu
* jiná chyba – jiná nespecifikovaná chyba

#### Update – aktualizace požadovaného objektu

**Popis:** Aktualizace objektu v KS; Z IdM jsou zasílány pouze atributy, které je nutné v KS aktualizovat, nezměněné atributy nejsou zasílány.

**Vstup:** unikátní ID objektu evidované koncovým systémem (získaný dříve při operaci Create) a měněné atributy

**Výstup:** unikátní ID objektu a návratový stav operace

**Možné návratové stavy:**

* úspěch – operace proběhla úspěšně
* neexistence – pokus o aktualizaci neexistujícího objektu
* jiná chyba – jiná nespecifikovaná chyba
* chyba syntaxe – (volitelné) pokus o vložení nepovolené hodnoty (např. řetězce do číselného atributu)

#### Rename – přejmenování objektu

**Popis:** Přejmenování objektu (změna uživatelského jména, změna názvu role) v KS.

Preferujeme, aby Rename objektu bylo součástí Update namísto samostatně volané operace.

**Vstup:** unikátní ID objektu evidované koncovým systémem (získaný dříve při operaci Create) a nové jméno objektu

**Výstup:** unikátní ID objektu a návratový stav operace

**Možné návratové stavy:**

* úspěch – operace proběhla úspěšně
* neexistence – pokus o přejmenování neexistujícího objektu
* duplicita – pokus o přejmenování objektu na jméno jiného objektu, který již v KS existuje
* jiná chyba – jiná nespecifikovaná chyba

#### Enable – zplatnění objektu

**Popis:** Zplatnění objektu (nejčastěji účtu) v KS.

Preferujeme, aby Enable objektu bylo součástí Update namísto samostatně volané operace.

**Vstup:** unikátní ID objektu evidované koncovým systémem (získaný dříve při operaci Create) a volitelně nový stav objektu

**Výstup:** unikátní ID objektu a návratový stav operace

**Možné návratové stavy:**

* úspěch – operace proběhla úspěšně
* neexistence – pokus o zplatnění neexistujícího objektu
* jiná chyba – jiná nespecifikovaná chyba

#### Disable – zneplatnění objektu

**Popis:** Zneplatnění objektu (nejčastěji účtu) v KS.

Preferujeme, aby Disable objektu bylo součástí Update namísto samostatně volané operace.

**Vstup:** unikátní ID objektu evidované koncovým systémem (získaný dříve při operaci Create) a volitelně nový stav objektu

**Výstup:** unikátní ID objektu a návratový stav operace

**Možné návratové stavy:**

* úspěch – operace proběhla úspěšně
* neexistence – pokus o zneplatnění neexistujícího objektu
* jiná chyba – jiná nespecifikovaná chyba

#### Check Alive – ověření platnosti session

**Popis:** Ověření platnosti session uživatele, pod kterým je přihlášené IdM ke KS.

Některé KS mají omezenou platnost session, kterou jsou identifikováni přihlášení uživatelé. Pokud je KS tento případ, je třeba v periodických intervalech kontrolovat platnost session a v případě ukončení platnosti ji obnovit. Operace je na straně IdM využita k vytvoření efektivního „connection poolingu“.

Tato operace, pokud je implementována, musí být velmi rychlá, neboť je volána často.

**Vstup:** ID session nebo uživatelské jméno technického uživatele

**Výstup:** informace o platnosti nebo neplatnosti zaslané session

**Možné návratové stavy:**

* úspěch – session je platná
* neúspěch – session není platná
* jiná chyba – jiná nespecifikovaná chyba

### Seznam oprávnění

Atributy uživatelského účtu zahrnují i seznam oprávnění (role, skupiny…) přiřazené účtu uživatele v koncovém systému. Atributy účtu mají obvykle textový formát, mohou existovat speciální případy – např. fotky (binární) či oprávnění (seznam/list/pole).

### Nefunkční požadavky

Koncový systém podporuje návratové kódy či fixní hlášky jako výsledek volání změnových operací.

### Rychlost odezvy rozhraní koncového systému

* Přečtení kompletního detailu jednoho uživatele (vč. navázání spojení) do 100ms
* Provedení zápisové operace nad jedním uživatelem do 200ms

### Ostatní

* Všechny atributy, které IdM zapisuje musí rozhraní poskytovat i pro čtení ve stejném formátu.

Podrobnější informace naleznete v [dokumentaci](https://wiki.evolveum.com/display/midPoint/Connector+Development+Guide) midPoint.