**Popis aktuálního IdM řešení MZe**

Verze: 1.0

Datum: 7. 4. 2017

Zpracovali: Dodavatel aktuálního řešení, xxxxxxxxxxxxx, xxxxxxxxxxxxxxxxx

# Obsah

[1. Obsah 2](#_Toc479076310)

[2. Definice pojmů 3](#_Toc479076311)

[3. Úvod – o řešení IDM na MZe 4](#_Toc479076312)

[4. Popis současného řešení 5](#_Toc479076313)

[4.1 Popis IdM procesů 5](#_Toc479076314)

[4.2 Import z HR systému 7](#_Toc479076315)

[4.3 Provisioning do řízených systémů 8](#_Toc479076316)

[4.3.1 MS Active Directory 8](#_Toc479076317)

[4.3.2 MS Exchange 8](#_Toc479076318)

[4.3.3 LDAP (Oracle Internet Directory – OID) 9](#_Toc479076319)

[4.3.4 SAP CUA (SAP Central User Administration) 9](#_Toc479076320)

[4.4 Admin rozhraní 9](#_Toc479076321)

[4.5 Integrace se systémem SIEM 9](#_Toc479076322)

[4.6 Notifikace 9](#_Toc479076323)

[4.7 Licence a maintenance 10](#_Toc479076324)

[5. Vybrané technické údaje o implementaci 10](#_Toc479076325)

[5.1 Zdrojová data 10](#_Toc479076326)

[5.1.1 Metodika konsolidace údajů o zaměstnancích 10](#_Toc479076327)

[5.2 Datový model 11](#_Toc479076328)

[5.3 Integrované systémy 11](#_Toc479076329)

[5.4 Podporované procesy 12](#_Toc479076330)

[5.5 Administrátorské rozhraní 13](#_Toc479076331)

[5.6 Notifikace 13](#_Toc479076332)

[5.7 Komponenty řešení 13](#_Toc479076333)

[5.8 Integrace se SIEM 14](#_Toc479076334)

# Definice pojmů

|  |  |
| --- | --- |
| **Zkratka / Pojem** | **Popis** |
| cílový systém | Systém, do kterého jsou objekty synchronizovány (např. MS AD). |
| implicitní synchronizace | Při uložení změn spravovaného objektu dochází k aplikování všech mapování pro daný objekt. |
| korelační pravidla | Pravidla, podle kterých je možné navázat systémový existující objekt na spravovaný objekt. |
| mapování | Definice synchronizace konkrétních objektů mezi systémy (např. managedUser\_adAccount). |
| NAME / \_\_NAME\_\_ | OpenICF – externí identifikátor systémového objektu (např. DN pro LDAP konektor). |
| OIM | Oracle Identity Manager – původní nahrazený IdM systém. |
| OpenIDM | Open-source projekt, který využívá nasazený IdM systém (Orchitech OpenIDM). |
| OpenICF | Framework pro konektory a sada standardních předpřipravených konektorů (CSV, LDAP, ...). |
| spravovaný objekt / managed object | Objekt spravovaný v rámci IdM (např. identita / uživatel). |
| synchronizace | Proces IdM, při kterém dochází k synchronizaci objektů mezi dvěma systémy. |
| synchronizační akce | Akce nad cílovým objektem, prováděná obvykle v návaznosti na detekovanou synchronizační situaci (např. CREATE pro ABSENT). |
| synchronizační politiky | Definice synchronizačních akcí (a případného *postAction* skriptu) pro jednotlivé synchronizační situace.  |
| synchronizační situace | Situace detekovaná při synchronizaci mezi systémy, např. ABSENT (objekt je ve zdroji, ale není v cíli), CONFIRMED (objekt je ve zdroji i v cíli), MISSING (objekt je ve zdroji, má být v cíli, ale není). |
| systém | Z pohledu IdM jde o integrovaný systém. Každý systém je identifikován jednoznačným identifikátorem. |
| systémový objekt | Objekt v cílovém (nebo zdrojovém) systému. Každý objekt je plně definovaný identifikátorem systému a typem (např. adAccount – účet v MS AD). |
| UID / \_\_UID\_\_ | OpenICF – primární klíč / stabilní identifikátor systémového objektu systému (např. entryUUID pro LDAP konektor). |
| validační pravidla | Pravidlo, které musí synchronizovaný objekt splňovat. |
| zdrojový / cílový objekt | Systémový nebo spravovaný objekt z pohledu synchronizace. |
| zdrojový systém | Systém, ze kterého jsou objekty synchronizovány (např. SAP HR nebo samotné IdM při synchronizaci účtů do MS AD). |

# Úvod – o řešení IDM na MZe

Řešení IdM na Ministerstvu zemědělství (MZe) vychází z nasazení Oracle Identity Manager, které bylo později reimplementováno a nahrazeno sadou open-source projektů založených na projektu OpenIDM, komponentách společnosti Orchitech Solutions a přizpůsobení Orchitech MZe Extension vytvořeného na míru MZe.

Implementace pokrývá procesy správy identit interních zaměstnanců MZe v několika vybraných systémech – Active Directory, Exchange, SAP CUA a Oracle Internet Directory.

SAP HR

IdM

MS AD

MS Exchange

OID

SAP CUA

*Obr. 1: Přehled integrovaných systémů*

Správci IdM mohou v rámci administrátorského rozhraní vybrané identity blokovat, dočasně povolovat nad rámec platnosti pracovního vztahu nebo povolovat založení účtů v konkrétním systému (více o implementovaných procesech dále v textu).

# Popis současného řešení

## 4.1 Popis IdM procesů

Implementace IdM převzala a doplnila původní procesy, které jsou naznačeny na diagramech níže. S ohledem na přehlednost diagramy neobsahují všechny detaily jako např. notifikace.


*Obr. 2: Založení nového uživatele*


*Obr. 3: Změna atributů uživatele*


*Obr. 4: Administrátorské uzamčení / odemčení účtu*

## 4.2 Import z HR systému

Import uživatelů je realizován načítáním CSV souboru, který je v pravidelném intervalu exportován SAP HR systémem do vybrané sdílené složky.

Importované osoby/kontrakty jsou celkem čtyř typů:

1. HPP - Hlavní Pracovní Poměr
2. SP – Služební poměr
3. DPČ - Dohoda o Pracovní Činnosti
4. DPP - Dohoda o Provedení Práce

IdM systém automaticky zakládá účty v řízených systémech pouze pro kontrakty typu SP a HPP. Jedna osoba může mít maximálně jeden SP nebo HPP, může mít však více poměrů DPČ/DPP. Proto nejsou účty na koncových systémech pro kontrakty typu DPČ/DPP zakládány automaticky, ale jsou pouze (před)vytvořeni v IdM systému a až na základě potvrzení administrátorem je pro takového IdM uživatele vytvořen uživatelský účet ve vybraném řízeném systému (administrátor zvolí v jakých řízených systémech bude účet vytvořen).

V rámci importního procesu je implementován ochranný mechanizmus, který přeruší import v případě, že je detekováno příliš velké množství změn, přičemž tento počet je definován jako konfigurovatelný parametr.

Kromě ochranného mechanismu se spoléhá na standardní validaci, která zajišťuje, že načítaný CSV soubor obsahuje smysluplný obsah.

## 4.3 Provisioning do řízených systémů

Uživatelům importovaným do IdM systému jsou provisionovány uživatelské účty do řízených systémů, dle nastavených pravidel, která přímo vycházejí z popsaných procesů.

Provisioning je implementován tak, aby odpovídal aktuálnímu stavu, popsanému níže. Napojeny jsou následující 4 systémy:

1. Microsoft Active Directory
2. Microsoft Exchange
3. LDAP (OID)
4. SAP CUA

Před samotným napojováním (těchto nebo dalších) řízených systémů IdM umožňuje mapování uživatelů na existující uživatelské účty na řízených systémech. Mapování je umožněno podle jednoznačného uživatelského jména, které je v podobě čísla zaměstnance. Toto mapování podléhá revizi a schválení MZe.

Integrace na každý z řízených systému podporuje speciální pilotní režim, v rámci kterého nejsou do řízeného systému propagovány žádné změny, ty jsou pouze logovány tak, aby mohla být provedena analýza chování provisioningu a nebyl přitom ohrožen provoz těchto napojených řízených systémů.

### 4.3.1 MS Active Directory

AD je provozováno na doménových kontrolérech verzí:

* Microsoft Active Directory 2008 R2 SP1,
* Microsoft Active Directory 2012,
* Microsoft Active Directory 2012 R2.

V AD je IdM systémem řízena jedna doména. Uživatelé jsou automaticky vytvářeni/aktualizováni v jednom kontejneru. Uživatelům je nastavena sada atributů, které přímo vycházejí z hodnot atributů osoby ze SAP HR systému. Uživatelům je taktéž nastaveno členství v základních AD skupinách dle definovaných podmínek (typ zaměstnance, členství v org. jednotce).

V AD je dohledán manažer IdM uživatele dle osobního čísla, které je dostupné ve vlastním atributu. DN manažera je doplněno do atributu AD uživatele. Pokud manažer není dohledán, je vyplněna defaultní hodnota a je odeslána notifikace.

Nové DN AD účtu je vyplněno do atributu IdM uživatele (a je dále použito při provisioningu LDAP účtu, který má v jednom ze svých atributů právě tuto hodnotu kvůli funkčnosti externí autentizace).

K dispozici je produkční a testovací prostředí AD.

### 4.3.2 MS Exchange

Jedná se o Microsoft Exchange Server 2013 CU7.

Po úspěšném založení uživatele v doméně je mu vygenerována unikátní mailová adresa a aktivována mailová schránka. Mailová adresa je uložena také do atributu IdM uživatele.

Při změně příjmení uživatele je vygenerována nová unikátní mailová adresa, která je přidána jako nový primární alias (původní alias je zachován).

MS Exchange prostředí je pouze jako **produkční**, bez testovacího prostředí.

### 4.3.3 LDAP (Oracle Internet Directory – OID)

Jedná se o Oracle Internet Directory 11.1.1.5.0.

K LDAPu je přistupováno standardním protokolem LDAPs. Po úspěšném založení uživatele v AD doméně je založen účet stejného jména v OID. Uživateli nejsou systémem IdM přidělovány žádné skupiny.

LDAP je instalován celkem ve třech prostředích: **produkční**, **testovací** a **vývojové**.

### 4.3.4 SAP CUA (SAP Central User Administration)

Jedná se o SAP CUA, který je součástí SAP Solution Manager SM 7.1 SPS12

Systém SAP CUA je napojen IdM konektorem vyvinutým na míru. Uživateli je v systému SAP CUA založen neaktivní účet bez hesla a oprávnění se základní sadou atributů, která přímo vychází z atributů IdM uživatele. Uživatel je aktivován a dále nastaven manuálně administrátorem na základě notifikace odeslané IdM systémem.

SAP Solution Manager je instalován celkem ve dvou prostředích: **produkční** a **testovací**.

## 4.4 Admin rozhraní

IdM systém disponuje webovým administrátorským rozhraním, prostřednictvím kterého je administrátorům umožněno provádět mimo jiné následující akce:

* Přehled IdM uživatelů, včetně jejich účtů spravovaných na koncových systémech.
* Okamžitá blokace IdM uživatele, včetně jeho navázaných účtů. Tato blokace nebude ovlivněna HR importem.
* Aktivace IdM uživatele, který byl zablokován HR importem. Tato aktivace nebude ovlivněna HR importem.
* Aktivace konkrétního účtu na koncovém systému, který je navázán na neaktivního IdM uživatele. Tato aktivace nebude ovlivněna HR importem.

Veškeré tyto administrátorské akce jsou řádně auditovány a přeposílány spolu s ostatními auditními logy do systému SIEM.

Webové admin rozhraní je kompatibilní s prohlížečem **Internet Explorer ve verzi 10 a vyšší.**

## 4.5 Integrace se systémem SIEM

IdM systém loguje jak veškeré aktivity prováděné administrátory, tak i veškeré automatické operace nad uživateli IdM a účty v řízených systémech prováděné IdM systémem. Všechny tyto logované záznamy jsou v reálném čase přenášeny do systému pro bezpečnostní monitoring MZe (SIEM - HP Arcsight 6.1.0.1389.0) k jejich vyhodnocení a uložení na centrálním bezpečném místě pro případnou zpětnou analýzu.

Události je možné vyčítat systémem SIEM jednou z následujících metod:

* Syslog
* SNMP TRAP
* Textový soubor
* JDBC
* Microsoft Event Log

## 4.6 Notifikace

Součástí IdM systému je notifikační engine, který umožňuje naplánovat mailové notifikace na základě definovaných událostí. Objednatel má k dispozici rozhraní, pomocí kterého může libovolně měnit obsah notifikačních mailů nebo adresátů. Dále je mu umožněno notifikace deaktivovat nebo znovu aktivovat.

V rámci dodávky budou nastaveny následující notifikace:

1. Notifikace o založení nového uživatele do SAP CUA
2. Notifikace o zamknutí účtu v SAP CUA
3. Notifikace o odemknutí účtu v SAP CUA
4. Notifikace o založení IdM uživatele
5. Notifikace o vytvoření nového emailového účtu
6. Notifikace o vytvoření nového účtu v MS AD
7. Notifikace o novém uživateli bez platného manažera
8. Notifikace o odpojení mailboxu

Definice e-mailu je obsahem nastavení, která jsou spravovaná administrátory systému.

## Licence a maintenance

* Časově a množstevně (počtem uživatelů, administrátorů či aktivních i neaktivních identit) neomezená licence k užívání IdM systému;
* Následná technická podpora standardních (generických) softwarových produktů tvořících součást IdM systému, včetně zajištění technické podpory ze strany subjektu, který pro daný produkt zastřešuje vývoj a údržbu;
* Oprávnění ke všem v úvahu přicházejícím způsobům užití autorského díla a bez jakéhokoliv omezení, a to zejména pokud jde o územní, časový nebo množstevní rozsah užití;
* Oprávnění práva tvořící součást licence zcela nebo zčásti jako podlicenci poskytnout třetí osobě;
* Oprávnění bez dalšího upravit či jinak měnit autorské dílo, jeho název nebo označení autorů, stejně jako spojit autorské dílo s jiným dílem nebo zařadit autorské dílo do díla souborného nebo na jeho základě či při jeho využití vytvořit dílo nové, a to přímo nebo prostřednictvím třetích osob, přičemž tato oprávnění trvají i po ukončení účinnosti smlouvy.

# 5. Vybrané technické údaje o implementaci

## 5.1 Zdrojová data

IdM načítá data ze systému SAP HR. Ten publikuje data o zaměstnancích skrze webové služby. IdM nicméně nekomunikuje se systémem napřímo. Místo toho data ze SAP HR načítá externí ETL komponenta, která jednou denně do sdílené složky nahrává CSV soubor s konsolidovanými zaměstnaneckými daty.

### 5.1.1 Metodika konsolidace údajů o zaměstnancích

SAP HR

Osoba A – poměr 1

Osoba A – poměr 1

Osoba B – poměr 1

**ETL**

CSV

Osoba A – poměr 1

Osoba B – poměr 1

*Obr. 5: Konsolidace údajů o zaměstnancích*

SAP HR v prostředí MZe využívá funkcionality tzv. Central Person. Každý pracovně-právní vztah tak má vazbu na záznam reprezentující fyzickou osobu. ETL je zodpovědné za to, aby se do IdM dostal pro jednu fyzickou osobu právě jeden zaměstnanecký vztah a nevznikaly tak duplicitní identity.

## 5.2 Datový model

Podporované případy užití nevyžadují složitý datový model. Z procesního pohledu jsou významné pouze dvě entity:

* User – identita / reprezentace fyzické osoby
* Role – přidělovaná role řídící propagaci do podřízených systémů

Objekt *User* eviduje standardní sadu atributu, jako je jméno osoby, tituly, typ zaměstnaneckého poměru, pozice v organizačním stromě, profese, konstantní údaje a další. Atributy specifické pro jednotlivé procesy jsou popsány dále v textu.

Objekt *Role* je využit pouze ve čtyřech instancích:

* interní zaměstnanec – základní role povolující vytvoření účtu ve všech spravovaných systémech
* přístup do AD – technická role povolující vytvoření účtu v MS AD a mailbox v MS Exchange
* přístup do LDAP – technická role povolující vytvoření účtu v Oracle Internet Directory
* přístup do SAP CUA – technická role povolující vytvoření účtu v SAP CUA

IdM neeviduje organizační strukturu (pouze jako atributy identit).

## 5.3 Integrované systémy

|  |  |  |
| --- | --- | --- |
| **Cílový systém** | **Způsob integrace** | **Technologie** |
| MS AD | LDAP konektor | konfigurace |
| MS Exchange | .NET PowerShell konektor | aplikace v PowerShell |
| LDAP (OID) | LDAP konektor | konfigurace |
| SAP CUA | Groovy konektor | aplikace v Groovy; SAP JCo |

#### Dva druhy rekonciliace

Systém implementuje současně dva přístupy k synchronizaci spravovaných objektů:

* automaticky okamžitě při změně atributů
* plná rekonciliace – porovnání a synchronizace všech relevantních spravovaných objektů

#### Specifika integrace MS AD

* IdM v systému zakládá účty a případně řídí jejich blokaci.
* Pro založení nebo povolení účtu v AD musí mít uživatel roli *interní uživatel* nebo *přístup do AD*.
* IdM účty ukončených identit nemaže, ale je schopno detekovat, že takový účet byl smazán a pro danou identitu zrušit příslušnou vazbu.
* IdM oproti standardní synchronizaci účtů kontroluje, zda před založením uživatele existuje záznam jeho nadřízeného (referenční integrita nad atributem *manager*).
* Při založení jsou přiřazovány výchozí skupiny a je správcům AD je posílán notifikační e-mail.

#### Specifika integrace s MS Exchange

* IdM v systému zakládá, připojuje a odpojuje mailboxy.
* Právo na mailbox mají všechny identity, které mají právo na účet v AD.
* IdM ukončeným identitám odpojuje připojený mailbox. V případě, že se ukončená identita vrátí zpátky do aktivního stavu, tak je místo založení nového mailboxu připojen mailbox původní (pokud již nedošlo k jeho smazání).
* IdM podporuje správu mailboxů ve více Exchange databázích, nicméně zakládání je podporováno pouze v jedné konkrétní.
* Při změně jména IdM generuje a přiřazuje primární e-mailovou adresu.
* Při změně e-mailu nebo odpojení mailboxu (tedy odebrání e-mailu) je odesílána notifikace správcům personálního systému.

#### Specifika integrace s Oracle Internet Directory

* IdM v systému zakládá účty a případně řídí jejich blokaci.
* OID je jediný systém, který má mírně odlišnou konfiguraci mezi produkčním a testovacím prostředím. V testovacím prostředí IdM řídí účty ve speciálním kontejneru a pro unikátní atributy používá speciální prefix (IdM-). Toto opatření je implementováno proto, aby IdM nemohlo ovlivnit fungování testovacích aplikací napojených na OID.
* V ostatních ohledech jde o standardní napojení LDAP systému.

#### Specifika integrace se SAP CUA

* IdM v systému zakládá účty a případně řídí jejich blokaci.
* Při vytváření účtu odesílá IdM notifikaci na správce systému SAP CUA, kteří založené účty dále zpracovávají pro předání cílovému uživateli.

## 5.4 Podporované procesy

Kapitola popisuje procesy podporované řešením IdM.

#### Řízení přístupů

IdM řídí přístupy pouze na úroveň založení / nezaložení (nebo blokace) účtu. IdM neřídí přiřazení práv v jednotlivých systémech.

Právo na zřízení účtu nebo vedení aktivního účtu v daném systému je řízeno přiřazením role v IdM. IdM má jedinou základní roli – *interní zaměstnanec*. Tato role je automaticky přiřazována všem zaměstnancům s pracovním poměrem. Zaměstnanci na DPP / DPČ nemají ve výchozím stavu právo na účet v žádném z integrovaných systémů. Správci IdM mohou uživatelům manuálně přiřadit role, které uživatele opravňují k založení účtu v konkrétním systému.

#### Příchod zaměstnance

Načtení nové identity zaměstnance je doprovázeno odesláním e-mailové notifikace na správce IdM. Jde-li o zaměstnance s pracovním poměrem, je identitě automaticky přiřazena základní role *interní zaměstnanec* (viz kapitola *Řízení přístupů*). Pokud jde o DPP/DPČ zaměstnance, je na zvážení správce IdM, zda mu ručně přiřadí role umožňující vznik účtu v jednotlivých systémech.

#### Blokování identity

Správce IdM má možnost vybranou identitu zablokovat. Zablokované identitě jsou s okamžitou platností zakázány přístupy do všech integrovaných systémů. Správce IdM má možnost blokaci identity kdykoliv zrušit.

#### Aktivace neaktivní identity

Správce IdM má možnost aktivovat neaktivní identitu (zaměstnanec na v dlouhodobé nečinnosti nebo ukončený zaměstnanec). Ručně aktivované identita nabývá právo mít účty v integrovaných systémech. Ručně aktivované identitě není přiřazována automatická základní role *interní zaměstnanec* a jednotlivé systémy musí správce IdM povolit ručně (viz kapitola *Řízení přístupů*).

## 5.5 Administrátorské rozhraní

Řešení IdM poskytuje rozhraní pro správce IdM. Ti se k rozhraní autentizují jménem a heslem. Řešení v tuto chvíli nerozlišuje role správců.

Administrátorské rozhraní primárně podporuje následující případy užití:

* přihlášení správce IdM
* hledání v identitách a zobrazení detailu identity
* administrátorské zamknutí nebo odemknutí identity
* administrátorská aktivace nebo deaktivace identity
* změna přístupů identity (nastavení systémových rolí)
* ruční vyvolání rekonciliace se SAP HR

Zmíněné případy užití korespondují s procesy popsanými v předešlé kapitole.

## 5.6 Notifikace

V současnosti jsou nastaveny notifikace dle seznamu níže. Notifikace umožňují i dynamickou volbu adresáta, zejména manažera příslušného uživatele.

* Vytvoření nového účtu v SAP CUA
* Zamknutí účtu v SAP CUA
* Odemknutí účtu v SAP CUA
* Vytvoření nového uživatele
* Přiřazení e-mailové adresy
* Odebrání e-mailové adresy
* Vytvoření nového účtu v MS AD
* Uživatel bez platného manažera
* Změna typu kontraktu
* Chyba při HR importu
* Chyba při synchronizaci uživatele

## 5.7 Komponenty řešení

Řešení IdM se skládá z několika základních artefaktů:

* OpenIDM + záplaty od Orchitech Solutions verze 4.0.1-orchi – základní platforma pro správu identit (vystupuje i v roli běhového prostředí pro OpenICF konektory psané v jazyce Java)
* Orchitech IdM Extensions – knihovna rozšíření IdM
* Orchitech MZe IdM – knihovna přizpůsobení a zákaznické logiky implementující IdM procesy MZe
* PostgreSQL – databáze pro Orchitech OpenIDM
* Apache HTTP Server – reverzní proxy pro přístup k administrátorskému rozhraní OpenIDM
* .NET Connector Server verze 1.4.0.0-orchi a PowerShell konektor verze 1.4.2.0 – běhové prostředí pro OpenICF konektory založené na platformě .NET

Zmíněné artefakty jsou nasazeny na dvou strojích:

* RedHat Server – základní Linux server pro Java artefakty
* Windows Server – konektor server pro .NET artefakty



*Obr. 6: Diagram nasazení*

Řešení je provozována ve dvou prostředích – produkční a testovací. Tato prostředí jsou navzájem víceméně identická:

* RedHat server – 2 jádra CPU, 80 GB disk, 4 GB RAM, RHEL 7+
* Windows server – 1 jádro CPU, 80 GB disk, 4 GB RAM, MS Windows Server 2012+

## 5.8 Integrace se SIEM

Řešení je integrováno se SIEM platformou MZe – HP Arcsight 6.1.0.1389.0. Integrace je provedena na úrovni vydefinovaných a zpřístupněných databázových struktur.