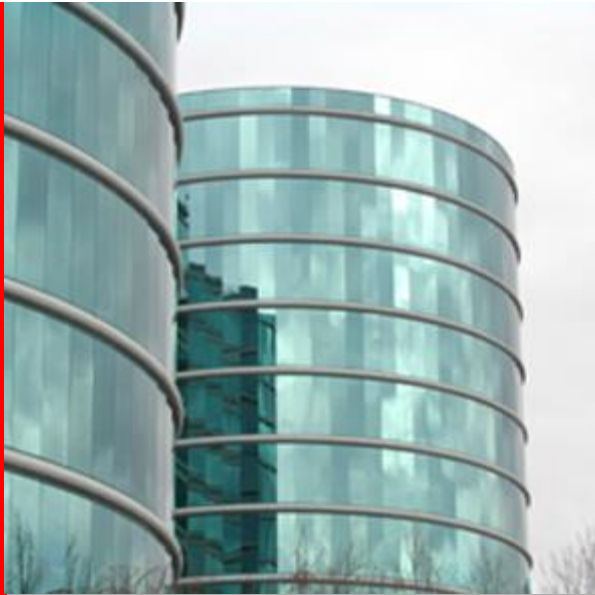




ORACLE®

Oracle Identity Management a jeho použití v praxi

Aleš Novák, Oracle
ales.novak@oracle.com

Agenda

- Úvod do IdM
- Ukázka
- Popis projektu
- Analytici

Co je Identity Management?

Inspirováno wikipedií

Řízení životního cyklu identity:

- Workflow
- Uživatelská samoobsluha
- Password reset
- Provisioning a de-provisioning identit ze systémů

... zavedením elektronických – automatizovaných procesů



Potřebujeme Identity Management?

Q: Kdo má ve vaší organizaci nejvíce přístupových práv?



- a – Správce bezpečnosti
- b – Finanční ředitel
- c – Brigádník, který přes léto zapojoval naši novou síť

Q: Jak přidělujete přístupová práva?

- a – Dejte Alici to co má Wally
- b – Na základě business role
- c – To co řekne její manager



DILBERT © Scott Adams, Inc. / Dist. by UPS, Inc.



DILBERT © Scott Adams, Inc. / Dist. by UPS, Inc.

Q: Co je napsáno na nálepkách,
přilepených k monitoru?

- a – Hesla
- b – Vzkazy
- c – Úkoly



A co ČR / SK?

- 2008, ČR, finanční instituce, vnitřní útok, pokus o ukradení cca 270 milionů
- 1999 - 2002, ČR, finanční instituce, 200 milionů ukradeno zaměstnancem (a většinou vráceno)
- SK, telekomunikace, root heslo na serverech připojených k internetu, žádná password policy, zneužito bývalým zaměstnancem

Důvody nasazení - audit, compliance

- SOX – podléhají mu firmy obchodované na US burze
- PCI
- Bezpečnostní audit – cyklus audit, nález, náprava, ...

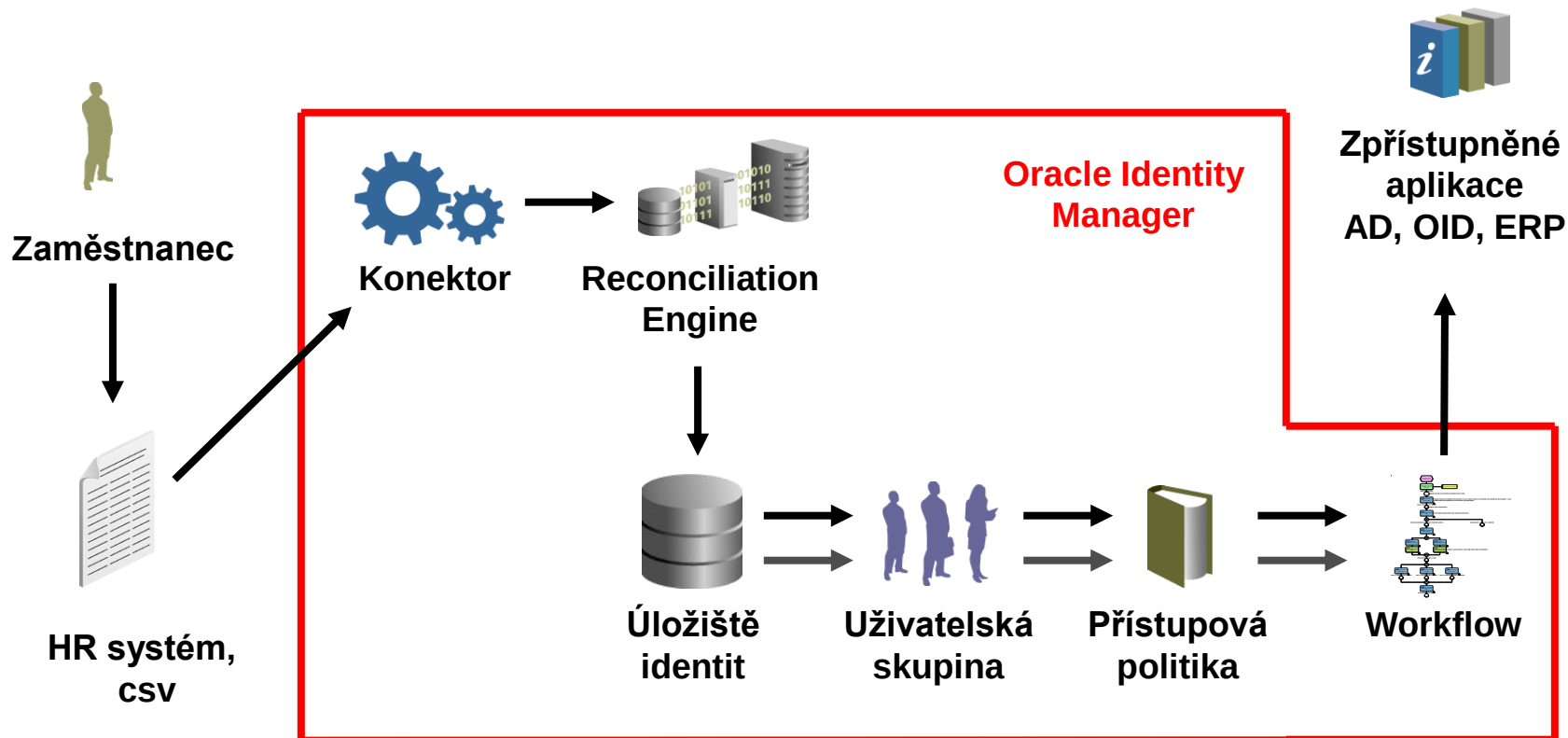
Úspora nákladů

- Self service, password reset
 - Příklad „pondělní amnézie“
- Nástup, změna pracovní pozice
- Správa kontraktorů
- Správa externistů – hypoteční a pojišťovací agenti, obchodní partneři

Oracle Identity Manager

- J2EE aplikace – aplikační server + Oracle DB
 - SoD podporováno a doporučeno
- Webové rozhraní pro uživatele
- Design console pro vývojáře
- Workflow engine
- Formuláře
- Konektory

Zapojení



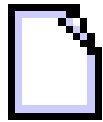
Přístupové politiky - RBAC

fmetelka, Franta, Metelka, **Full-Time**, ...

Skupina „Full-Time Employee“



Full-Time Employee



Role == Full-Time

- Definice přístupové politiky
 - AD, DB přístup



DEMO

DEMO

- Oracle IdM
- Active Directory
- Oracle BI Publisher
- Reporty – disabled users, partially disabled, rogue accounts, entitlement exception

Reconciliation

Usmíření

Identity Manager

Active Directory

Počáteční AD
Reconciliace - linkování

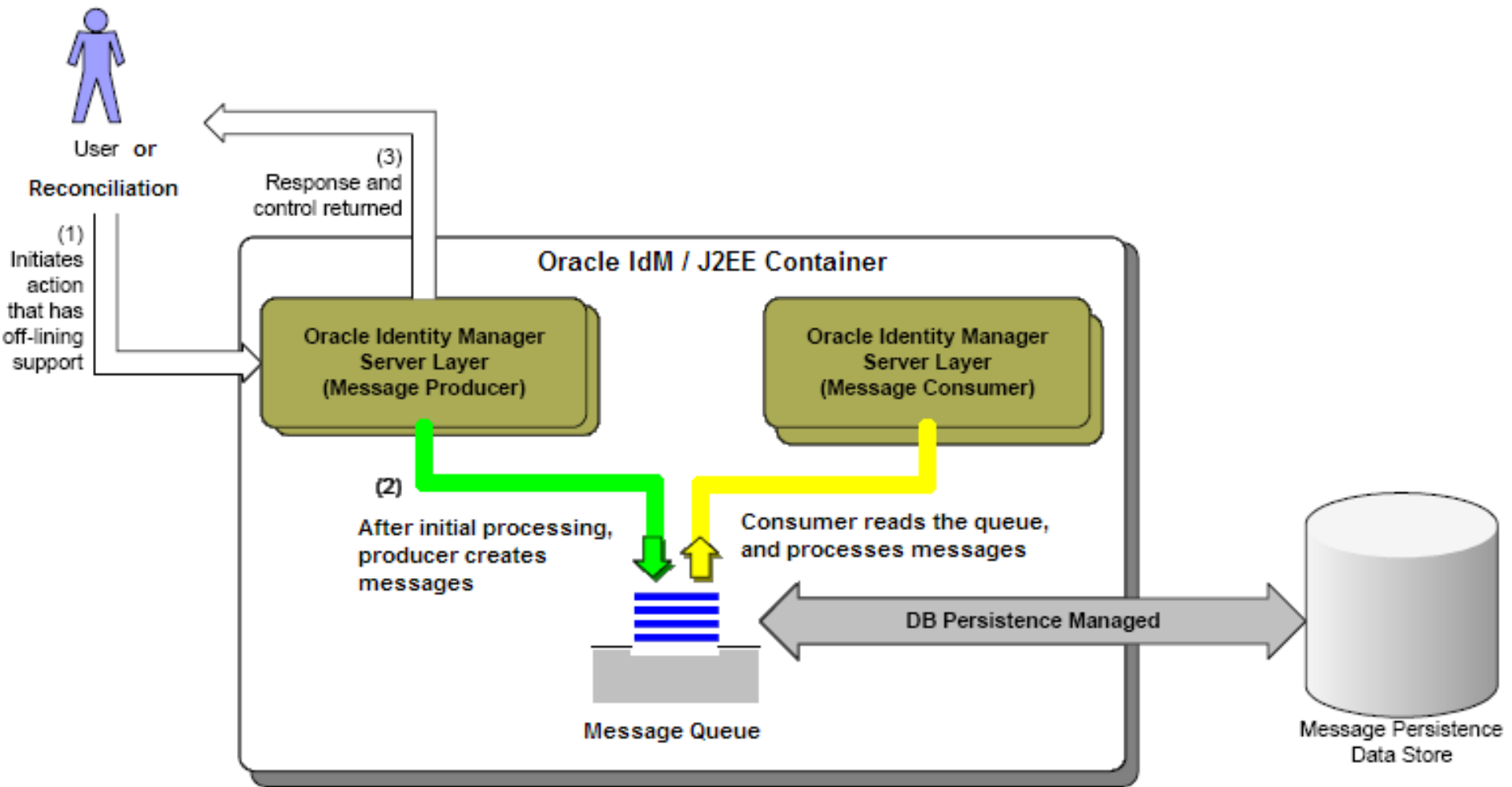
baseline

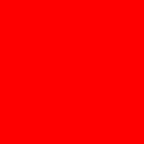
Počáteční recon
(Trusted)

Následné AD
Reconciliace



IdM Architektura



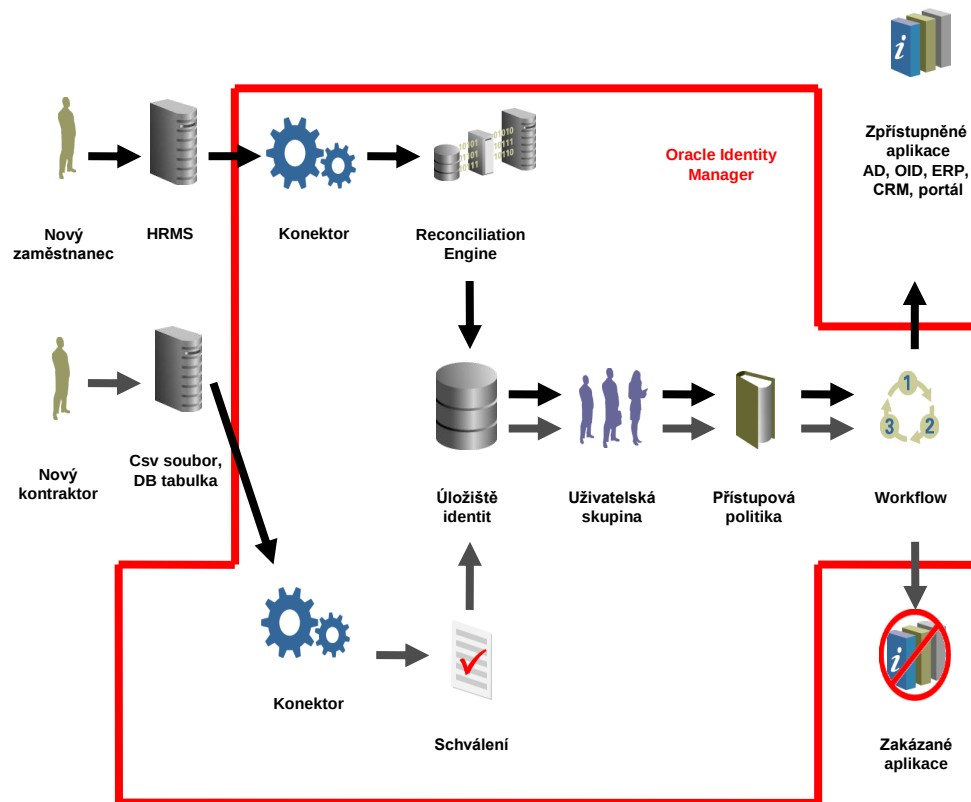


Případová studie

Ministerstvo Zemědělství

Motivace

- Portal access pro zaměstnance
- Blokování přístupu
- Konsolidace hesel



Zadání

- Vstup SAP HR
- Výstup AD, OID, SAP CUA
- Incremental a full recon
- HA infrastruktura

Návrh implementace

- Dev, test, produkce
- Rozšíření data modelu v OIM
- Konektor na SAP HR, SAP CUA, AD, OID
- Workflow
- Dodatečná BAPI

Implementace – SAP HR

- Konektor + úpravy
- 1 x týdně full reconciliace, 1 x denně inkrementální
- Volání custom BAPI
 - Vývoj BAPIletů, unit testy...

PERNR, VORNA, NACHN, USRID_LONG, ORGEH, STTEXT, ...

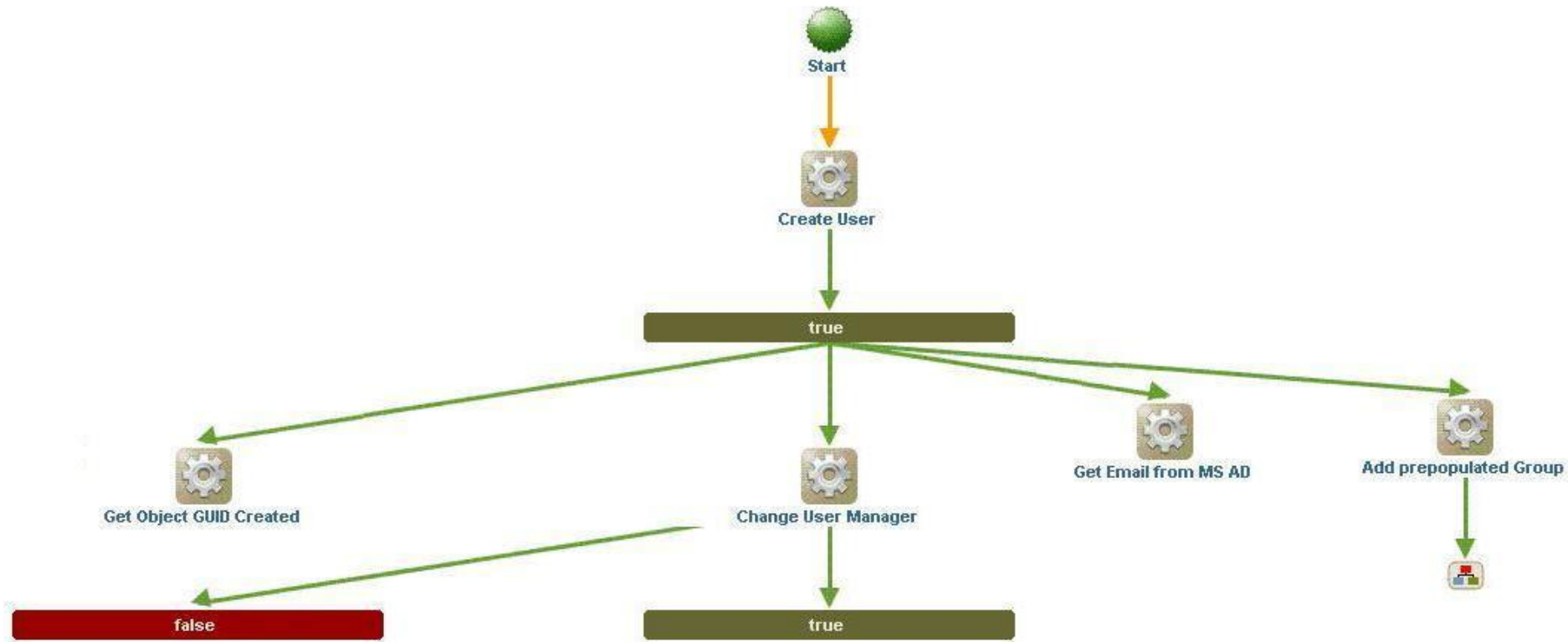
SAP CUA

- Spravované systémy, profily a role do číselníků OIM
-
- | | |
|--------------|--------------|
| • BNAME | • ROOMNUMBER |
| • NAME_LAST | • FLOOR |
| • NAME_FIRST | • BUILDING |
| • TITLE_ACA1 | • TEL_NUMBER |
| • TITLE_ACA2 | • SMTP_ADDR |
| • DEPARTMENT | • CODVN |
| | • LOCL |

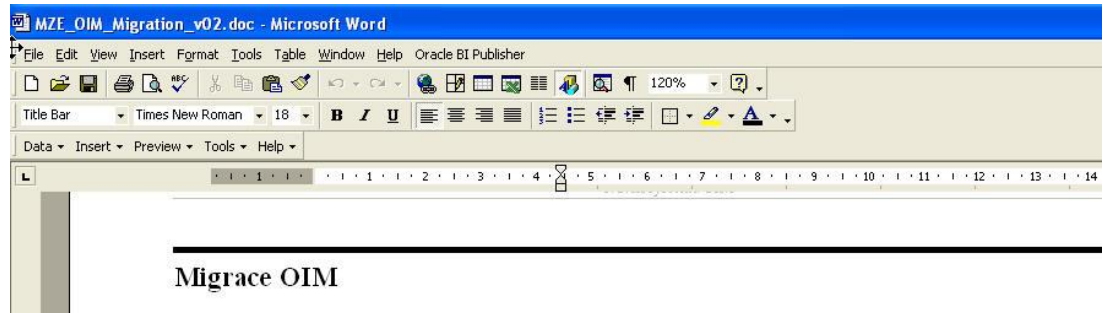
Implementace – AD, OID

- OID – objectclasses pro portál
- Department change -> AD moddn
- AD generuje mail

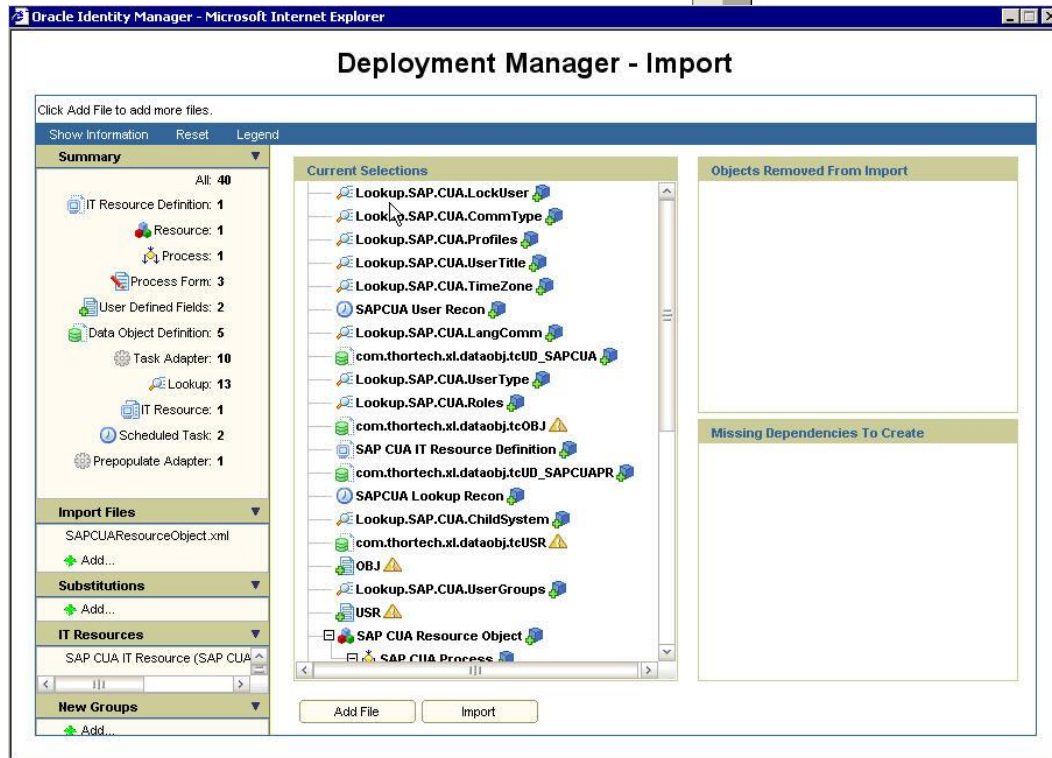
MS AD jako zdroj pro emailové adresy



Deployment Management



Migrate OIM



Dokument detailně popisuje postup migrace konfigurací a customizací na OIM prostřed

V rámci migrace se provádí dva typy operací:

- přenos custom jar souborů
- export a import xml souborů pomocí OIM Admin Console

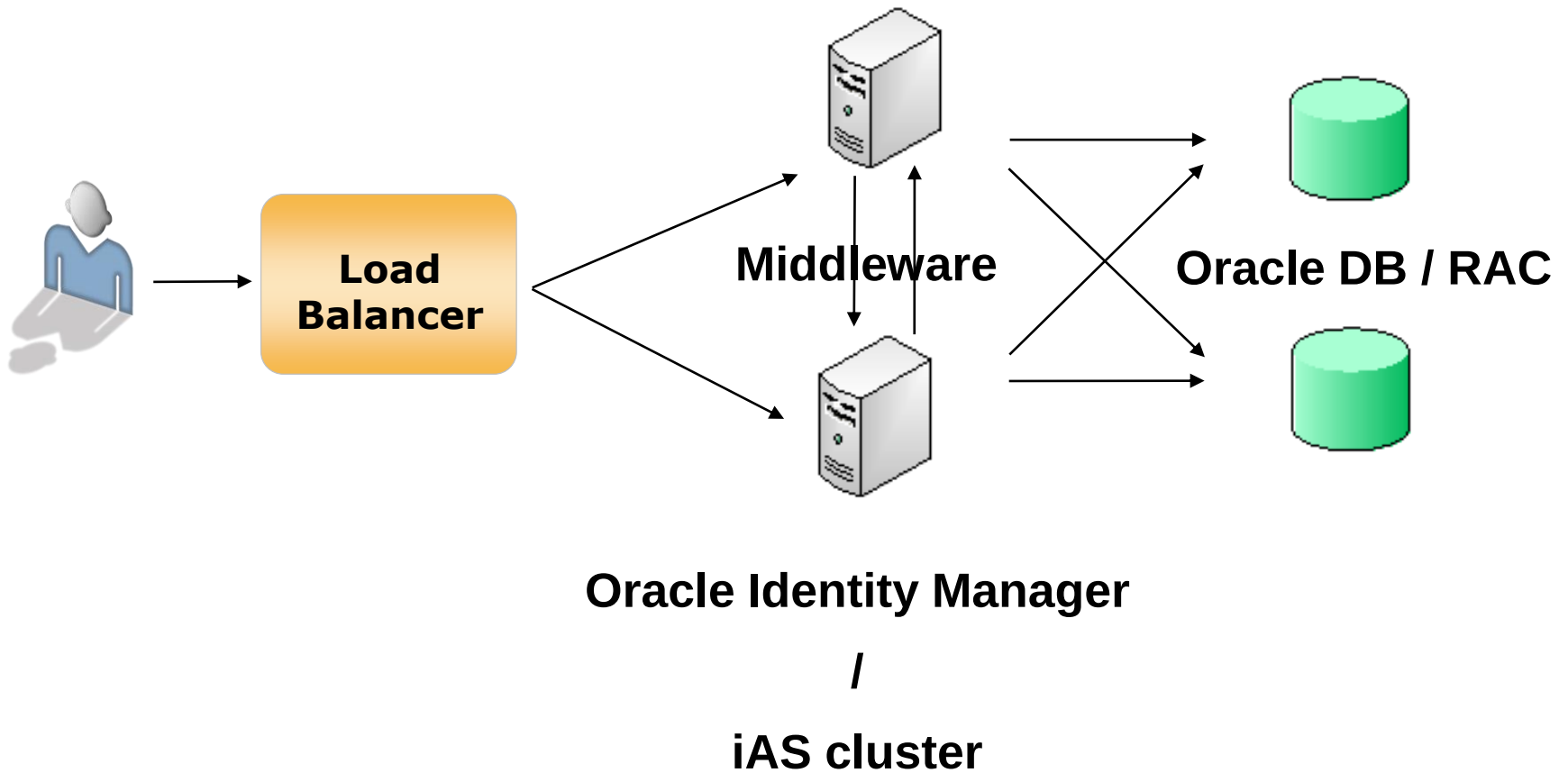
Kompletní „release“ OIM řešení je tedy zachycen sestavou jar souborů a xml souborů.

Dokument popisuje

- přehled migrovaných objektů
- postup migrace (zohledňující závislosti)

Pořadí importu xml objektu je dáno pořadím xml souboru v tabulce !

Infrastruktura



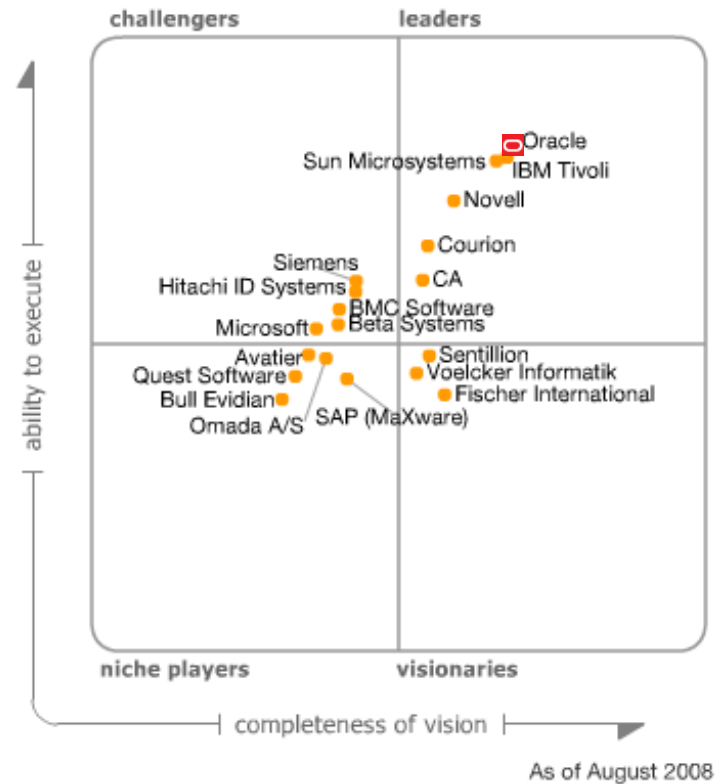
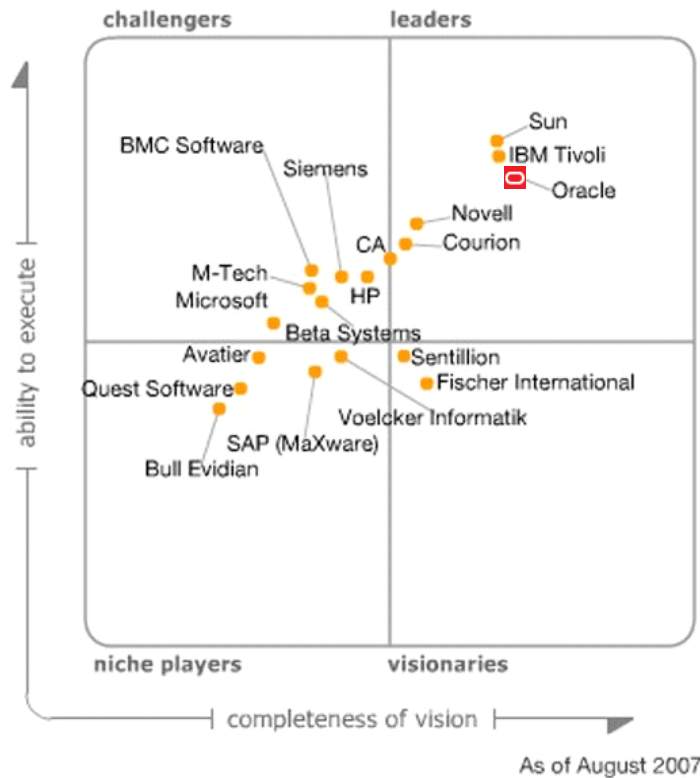
Projekt

- Cca 2,5 měsíce
- 2 – 5 lidí
- Analýza, dokumentace, testy, akceptace

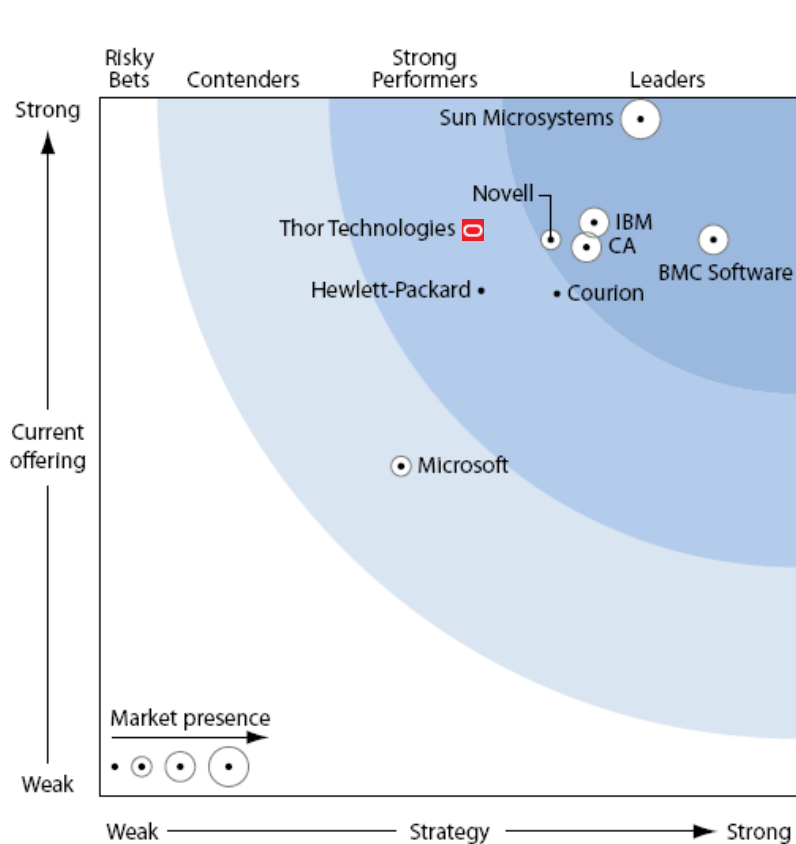
Analytici

Gartner

User Provisioning (Oracle Identity Manager)

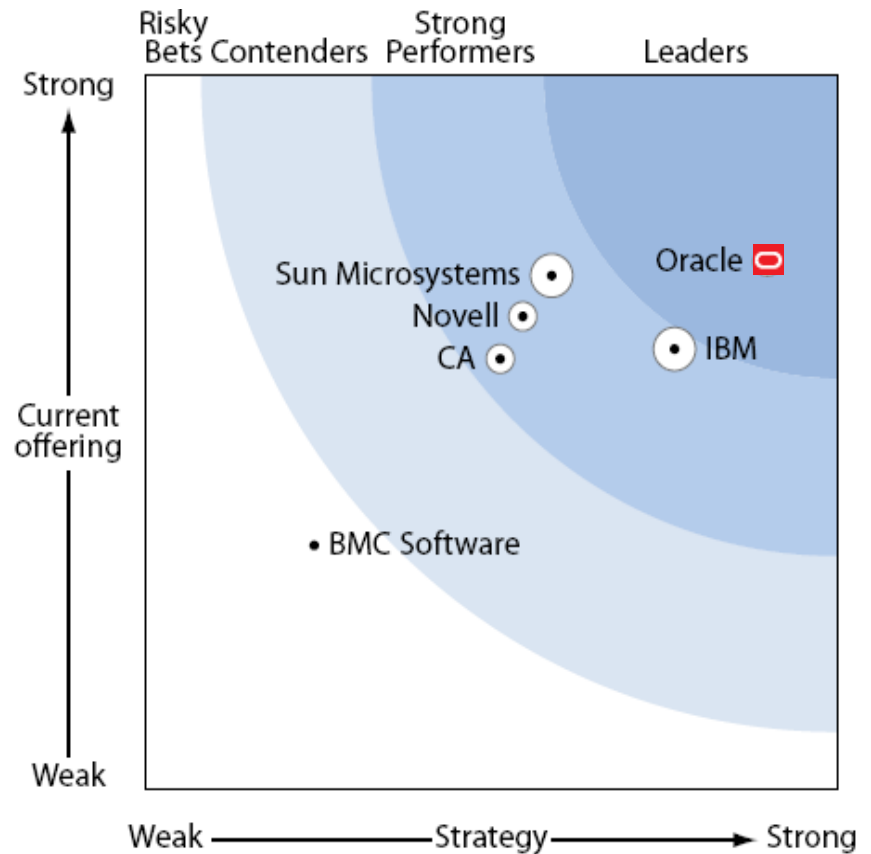


Forrester Wave 2006 - 2008



by **Jonathan Penn**

with Laura Koetzle, Paul Stamp, Simon Yates,
and Adele Sage



by **Andras Cser**

with Jonathan Penn, Paul Stamp, and Allison
Herald

Závěr

- Co a k čemu je identity management
- Demo
- Studie
- Analytici

ORACLE®