Správa identit a bezpečnosti - cesta k bezpečnému IS

Stanislava Birnerová
Direct Account Manager
Novell-Praha, s.r.o.

Novell®

Novell a historie správy identit

- DirXML
  - v roce 2000 úplně první identity manager
  - spolupráce s Forrester Reseach a Burton Group na definici, co je to adresář (jako industry implementace X.500)
- Novell Identity Manager
- Novell Access Manager
  - rebranding produktů v roce 2003
- Novell Sentinel
  - akvizice společnosti eSecurity v roce 2006
- Novell je leaderem v oblasti Správy identit a bezpečnosti pro enterprise zákazníky

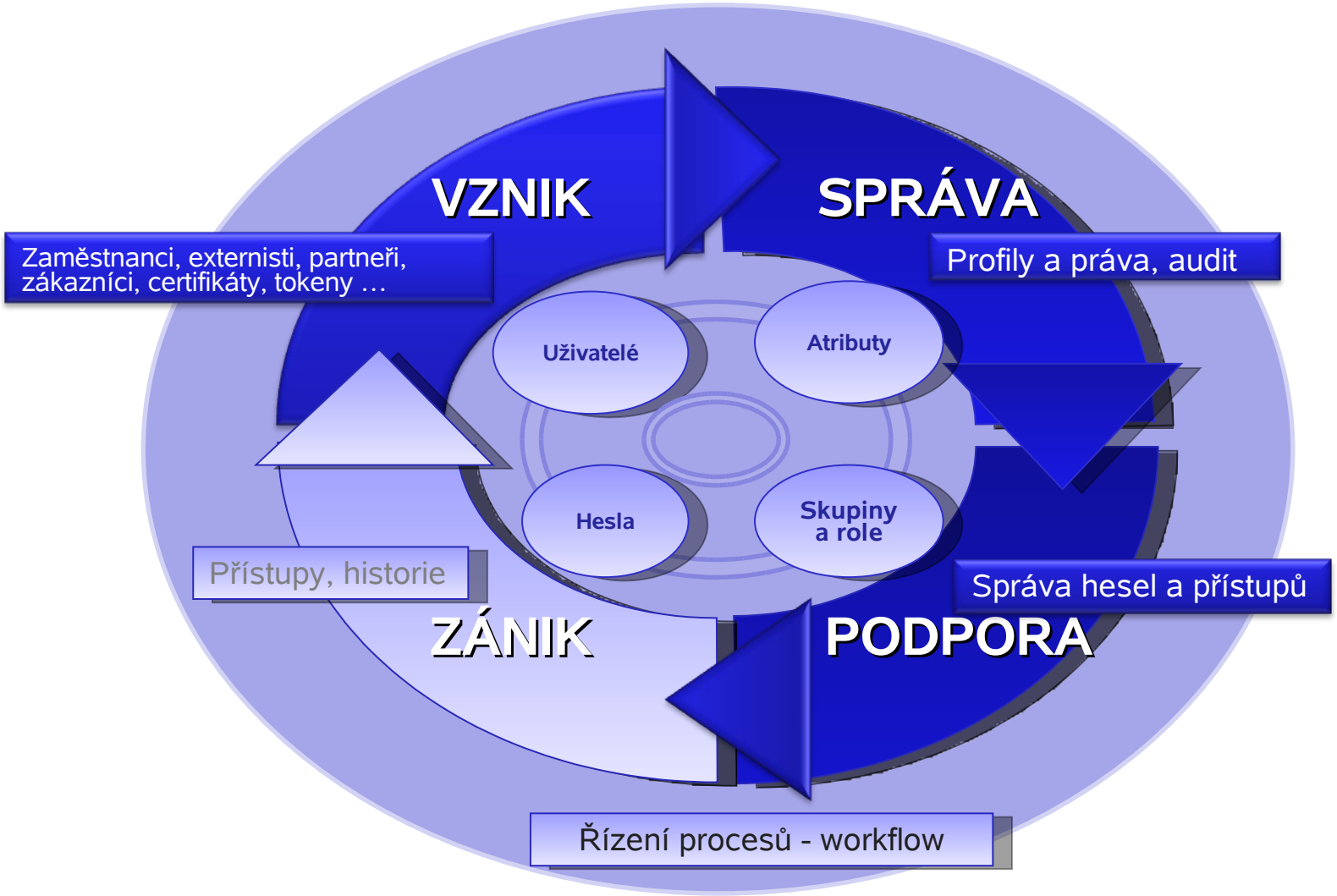
Důvod zájmu a hlavní cíl

- **Důvody**
  - vstupuje do popředí zájmu již několik let
  - důvodem jsou nároky nových předpisů a zákonů
  - nařízení regulátorů, ale i nároky z procesního řízení
- **Cíl**
  - Řešení jako celek je auditovatelné v každém okamžiku
- **Dva hlavní stavební kameny**
  - První, který politiky řídí, definuje, vynucuje
  - Druhý, který v reálném čase provádí kontrolu, audituje

Správa identit a bezpečnosti – sjednocení pojmů

- **Identita = totožnost, úplná shodnost**
  - IT identitou může být „cokoliv“ (člověk, místnost, program, …)
  - Trezor identit udržuje bezpečně všechny potřebné informace o identitě
- **Provisioning = poskytnutí, poskytování, propůjčení, zabezpečení**
  - Systém správy identit zajišťuje on-line kontrolované a řízené poskytování informací o identitě ostatním systémům v jimi požadované formě
  - Systém správy identit zajišťuje řízené a kontrolované provedení požadovaných operací závislých na změnách, které se dotýkají identity nebo její reprezentace v koncových systémech
- **Single Sign-On = jediné navázání, jediné označení, jediný podpis**
  - Pokud adresář se skladem účtů a hesel není napojen na trezor identit – není to řešení související se správou identit!
- **Password Synchronization = synchronizace hesla**
  - Může/nemusí souviset s řešením správy identit
- **Self Management = samospráva, samoobsluha**
  - Může/nemusí souviset s řešením správy identit

O čem správa identit a bezpečnosti je …



Architektura řešení

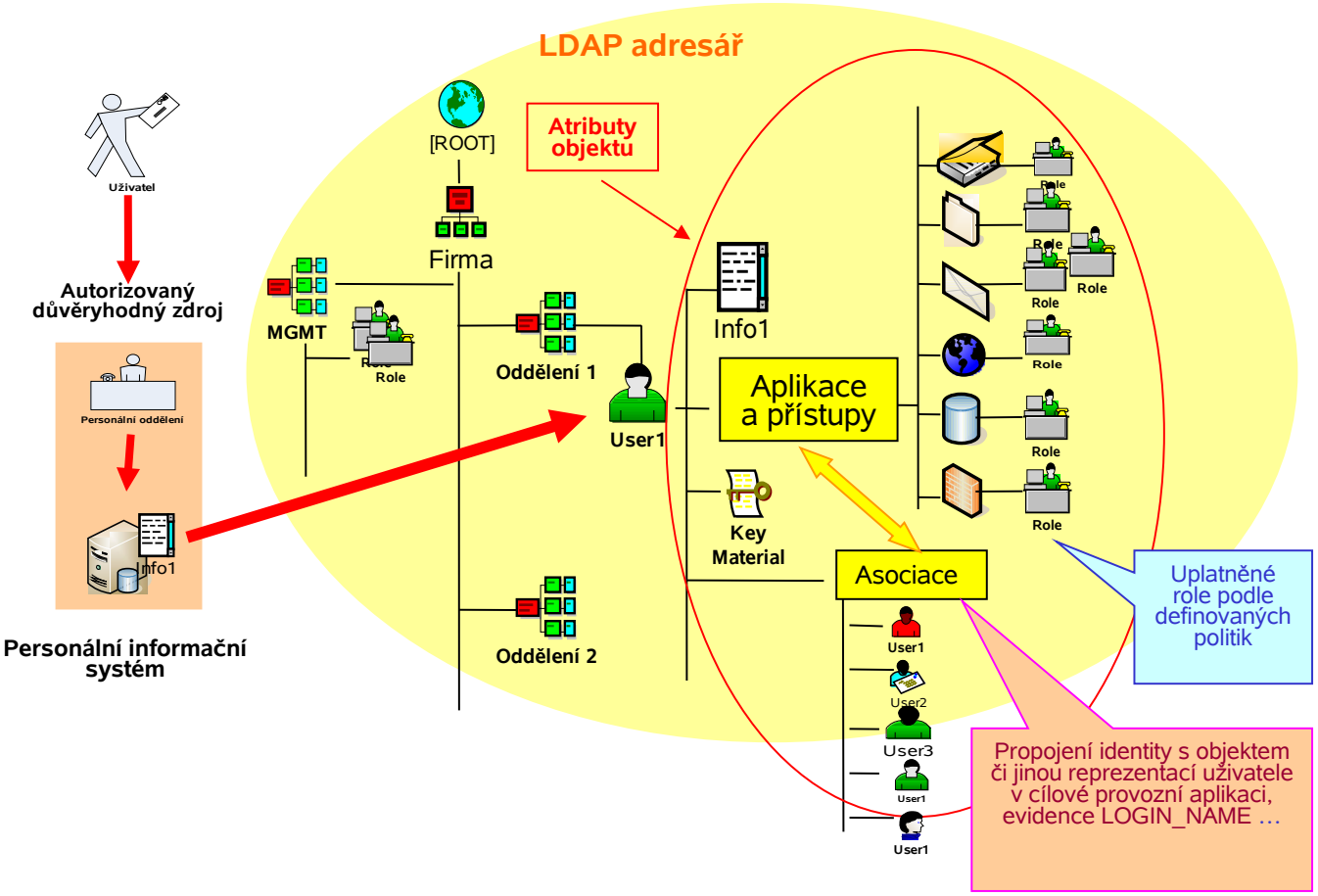
Centrální úložiště identit – trezor

- tzv. „Trezor identit”
  - řeší problémy s izolovanými identitami
  - centrální úložiště
  - místo pro centralizovanou správu identit
  - celá řada aplikací sdílí o identitě tytéž údaje
  - autentizace a autorizace je funkčně sjednocena
  - poskytuje základ pro centralizované řízení přístupu
  - umožňuje perzonalizaci založenou na rolích a jejich prostřednictvím přidělovaných právech

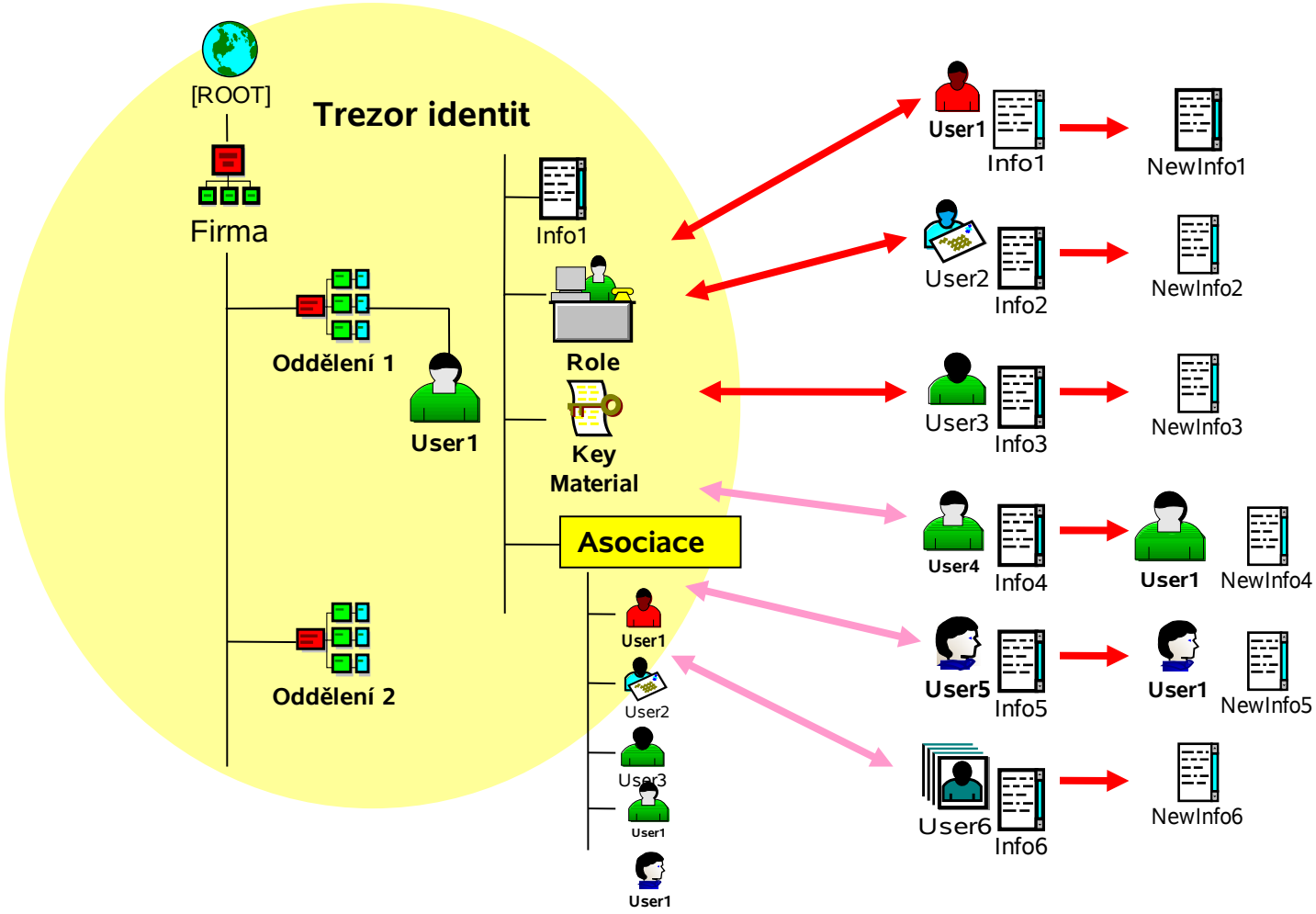
Metaadresářové služby

- metadirectory (metaadresáře)
  - tuto techniku používáme k agregaci dat souvisejících s identitou do centrálního úložiště
  - dovoluje na základě dat příslušejícím jednotlivým subsystémům založit jedinou, bohatou identitu pro každého uživatele, při zachování původních dat
  - umožňuje dále distribuované vlastnictví částí takto vzniklé identity...
    - po založení jednotné, centralizované identity může tato být sdílena mnoha systémy

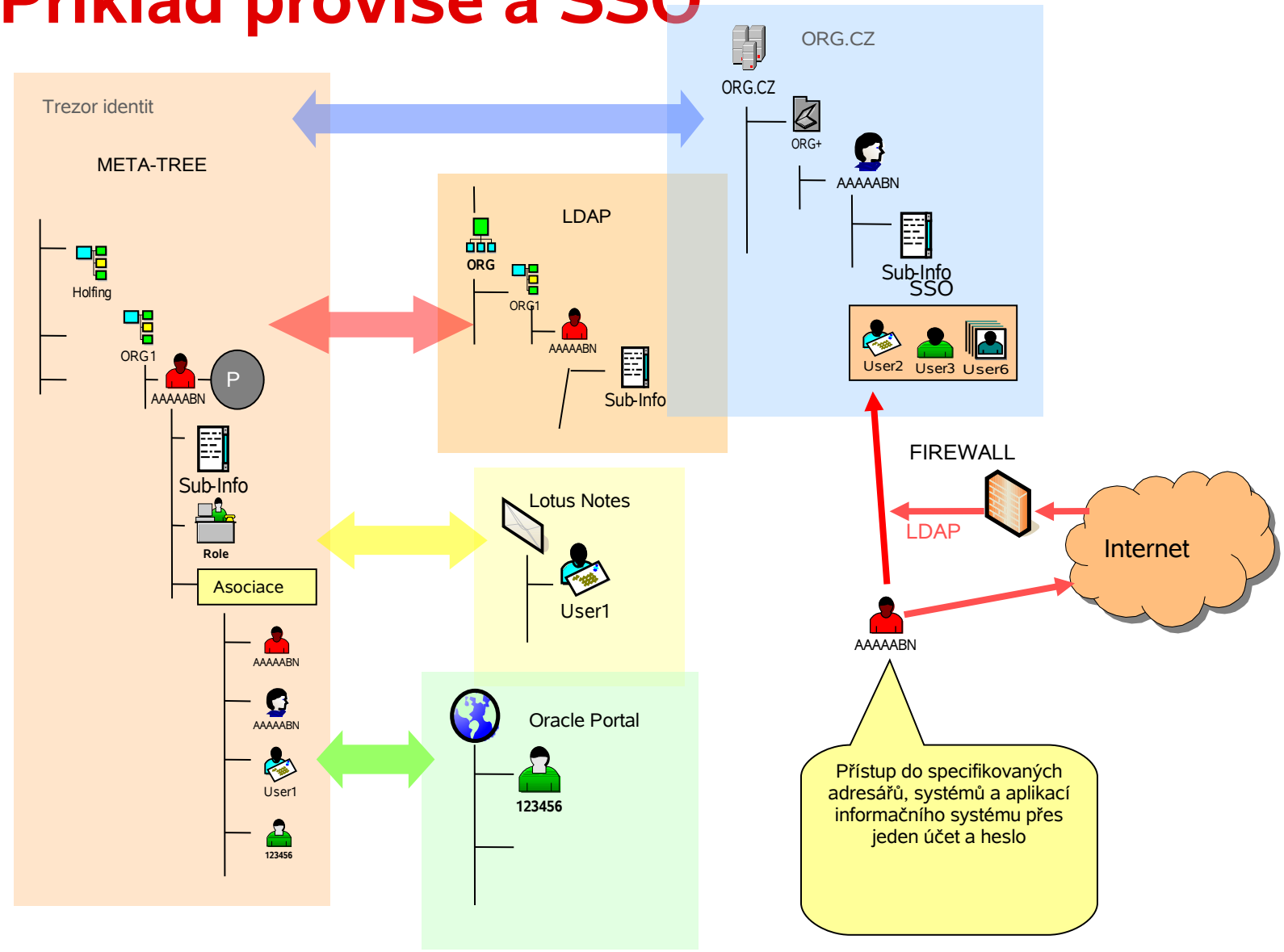
Trezor identit



Asociace identit, účtů a záznamů



Příklad provise a SSO



Správa identit a bezpečnosti umožňuje

- Automatické založení a správu uživ. účtů
- Samoobsluhu v oblasti správy hesel
- Bezpečný záznam událostí, auditování a generování výstupů

Z praxe

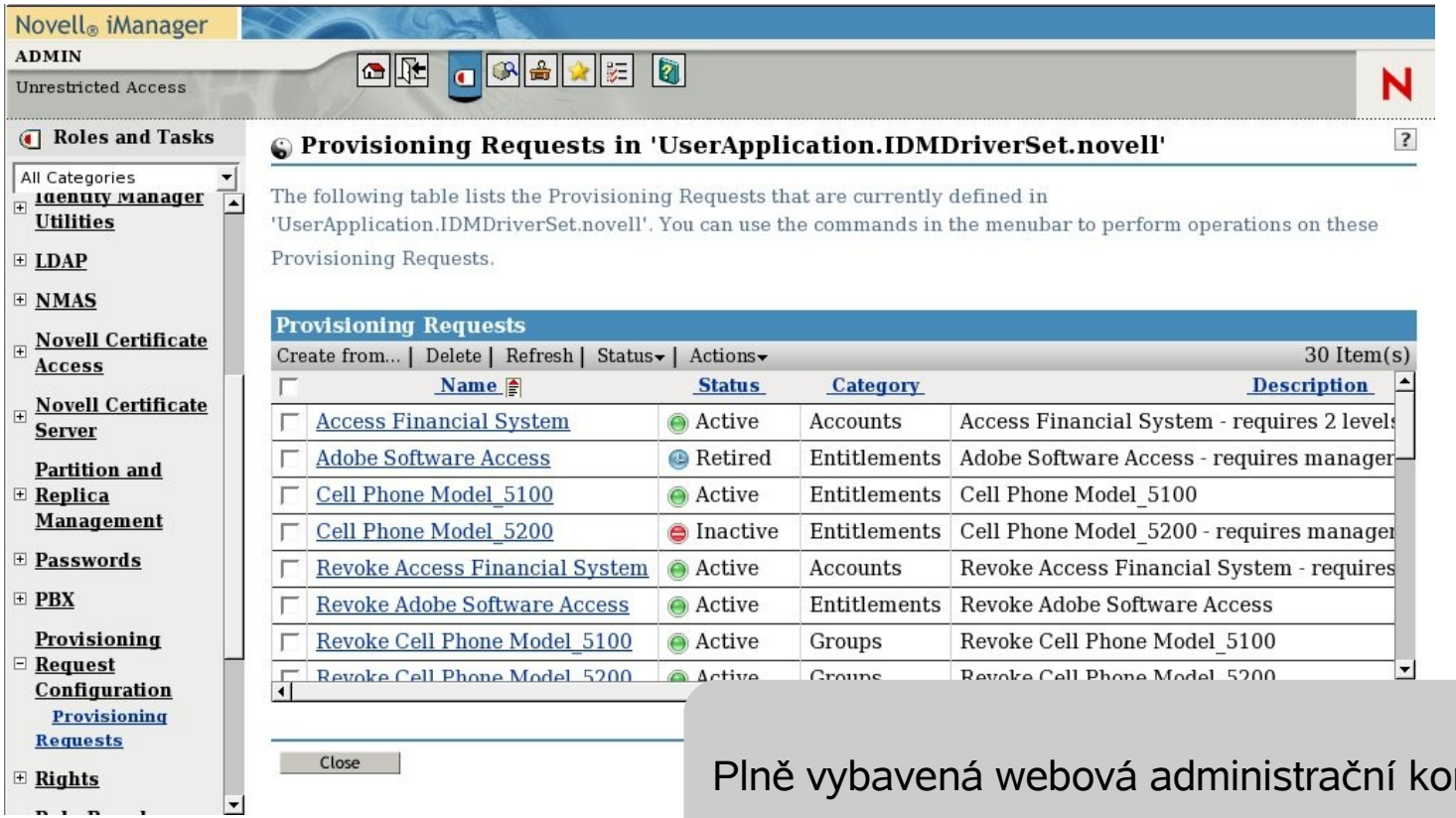
Produkty

- Dva hlavní stavební kameny

Novell Identity Manager
- zajišťuje správu identit
tj. produkt, který politiky řídí, definuje, vynucuje

Novell Sentinel
- nástroj pro bezpečnostní kontrolu
- auditovací nástroj
tj. produkt, který v reálném čase provádí kontrolu, audituje

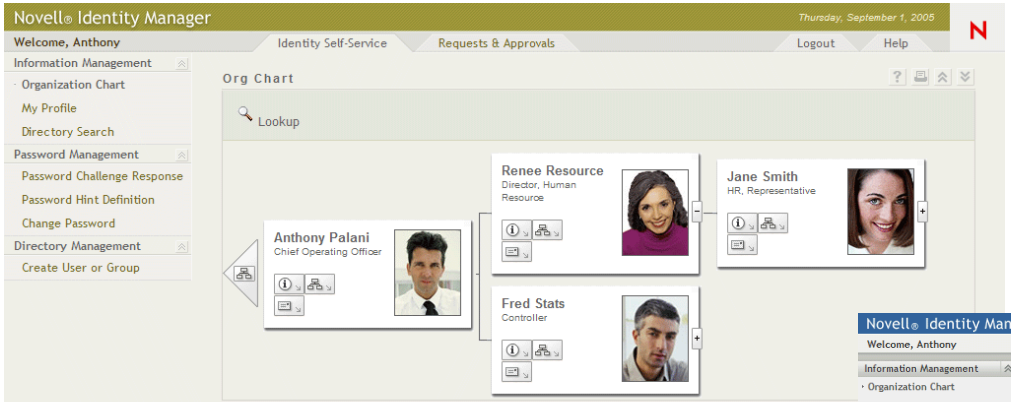
IDM
– pohled administrátora

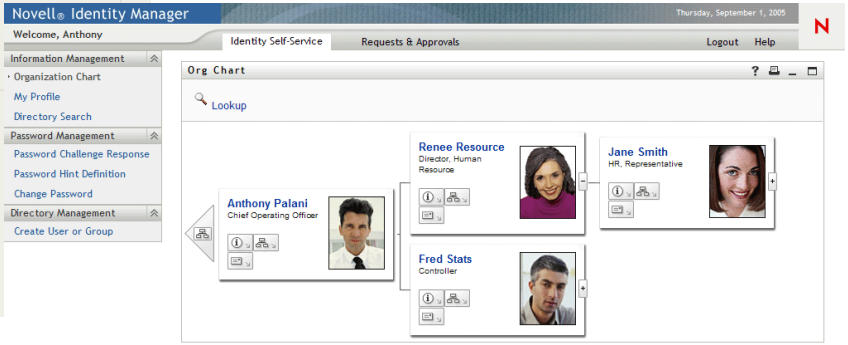


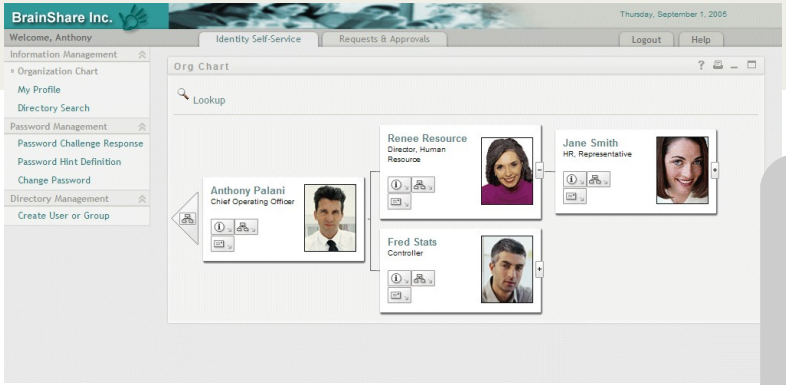
Plně vybavená webová administrační konzola.

- Monitorovací, tiskové a auditovací funkce
- Integrována do společného administračního portálu iManager (jednotná platforma CIM)
- Odděleno od nástrojů pro architekty /konzultanty

IDM
– atraktivní a flexibilní uživatelské prostředí



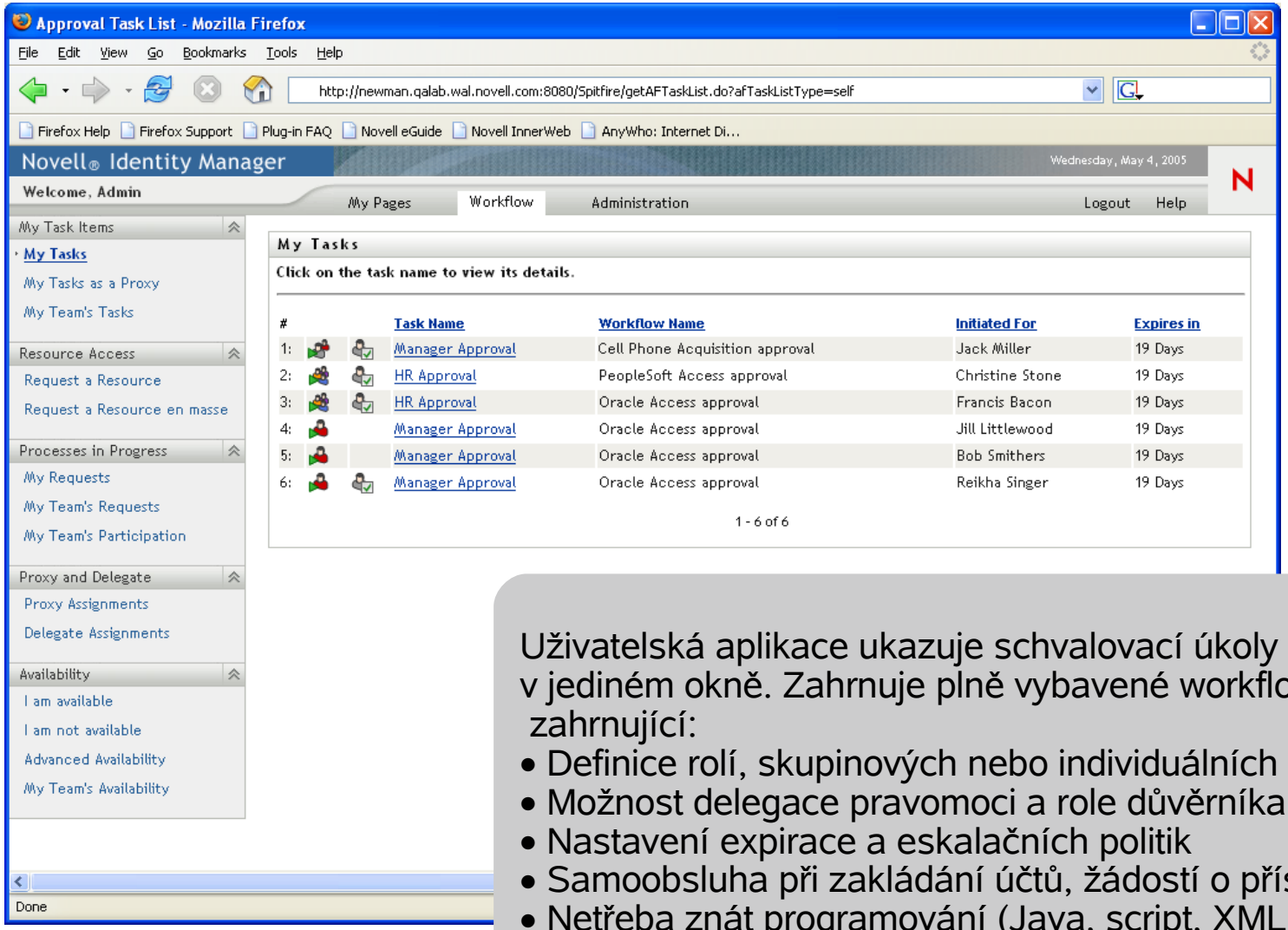




Webová aplikace zdědila funkce z Novell® SOA technologie.

- Robustní vybavení; přátelské pro správce
- Předefinované vzhledy; plně přizpůsobitelné.
- Respektuje standardy pro interoperabilitu

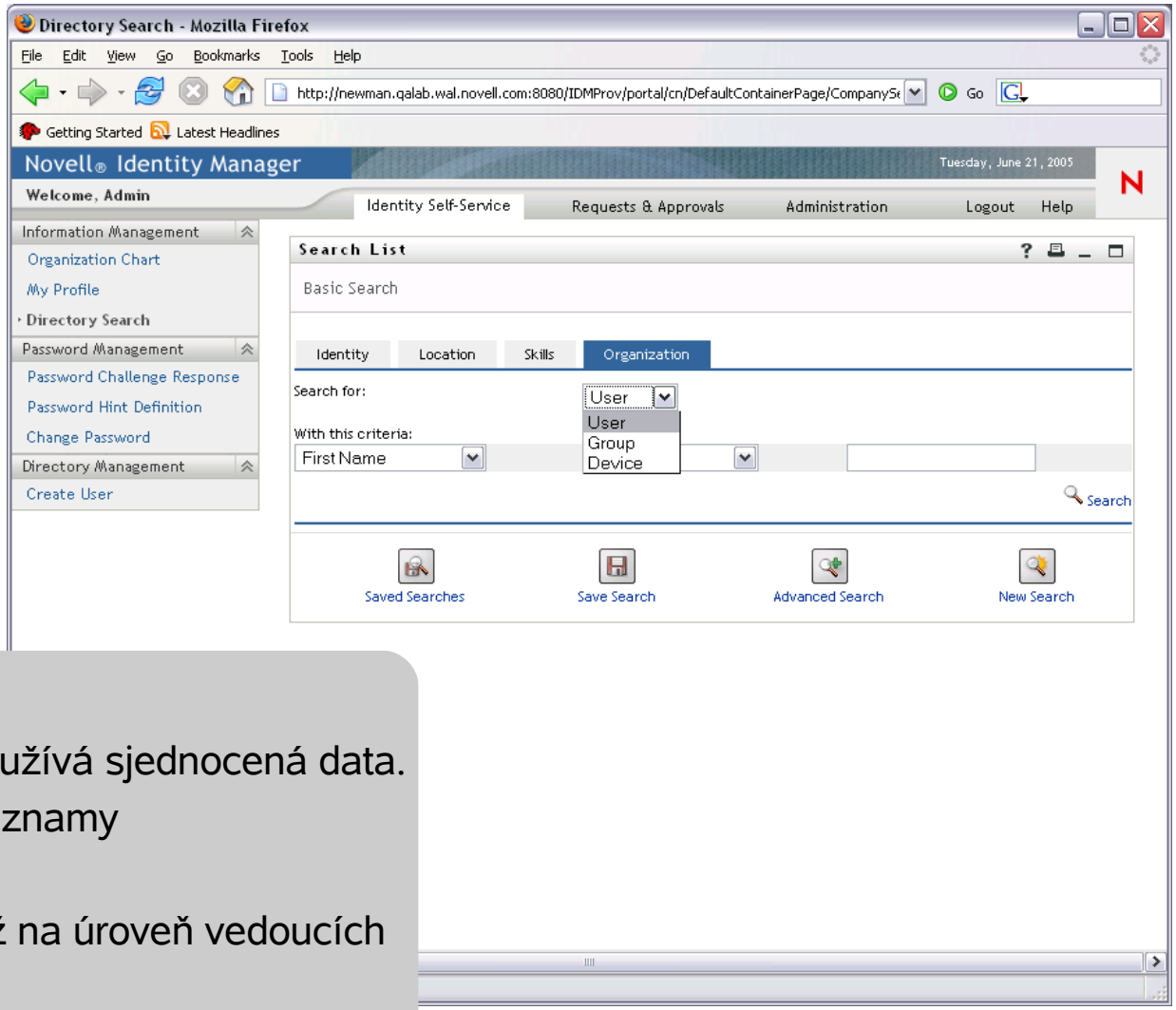
IDM z pohledu manažera
- Integrovaný schvalovací proces



Uživatelská aplikace ukazuje schvalovací úkoly v jediném okně. Zahrnuje plně vybavené workflow, zahrnující:

- Definice rolí, skupinových nebo individuálních přiřazení
- Možnost delegace pravomoci a role důvěrníka
- Nastavení expirace a eskalačních politik
- Samoobsluha při zakládání účtů, žádostí o přístupy
- Netřeba znát programování (Java, script, XML, atd.)

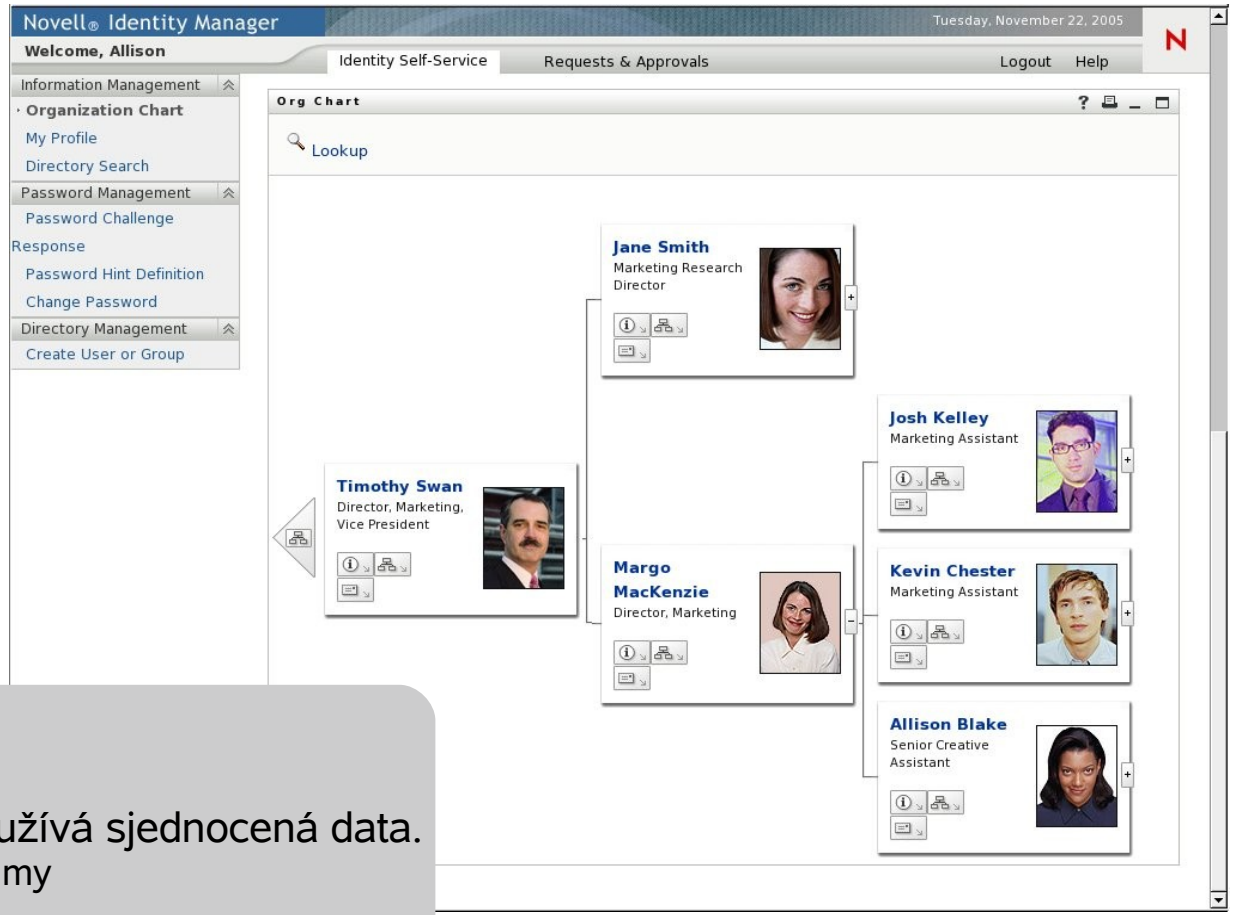
IDM 2x z pohledu uživatele
Aplikace pro práci s identitami - vyhledávač



Pokročilá webová aplikace používá sjednocená data.

- Přehledné org. schéma a seznamy
- Samoobsluha správy hesel
- Delegovaná administrace až na úroveň vedoucích jednotlivých pracovních týmů.

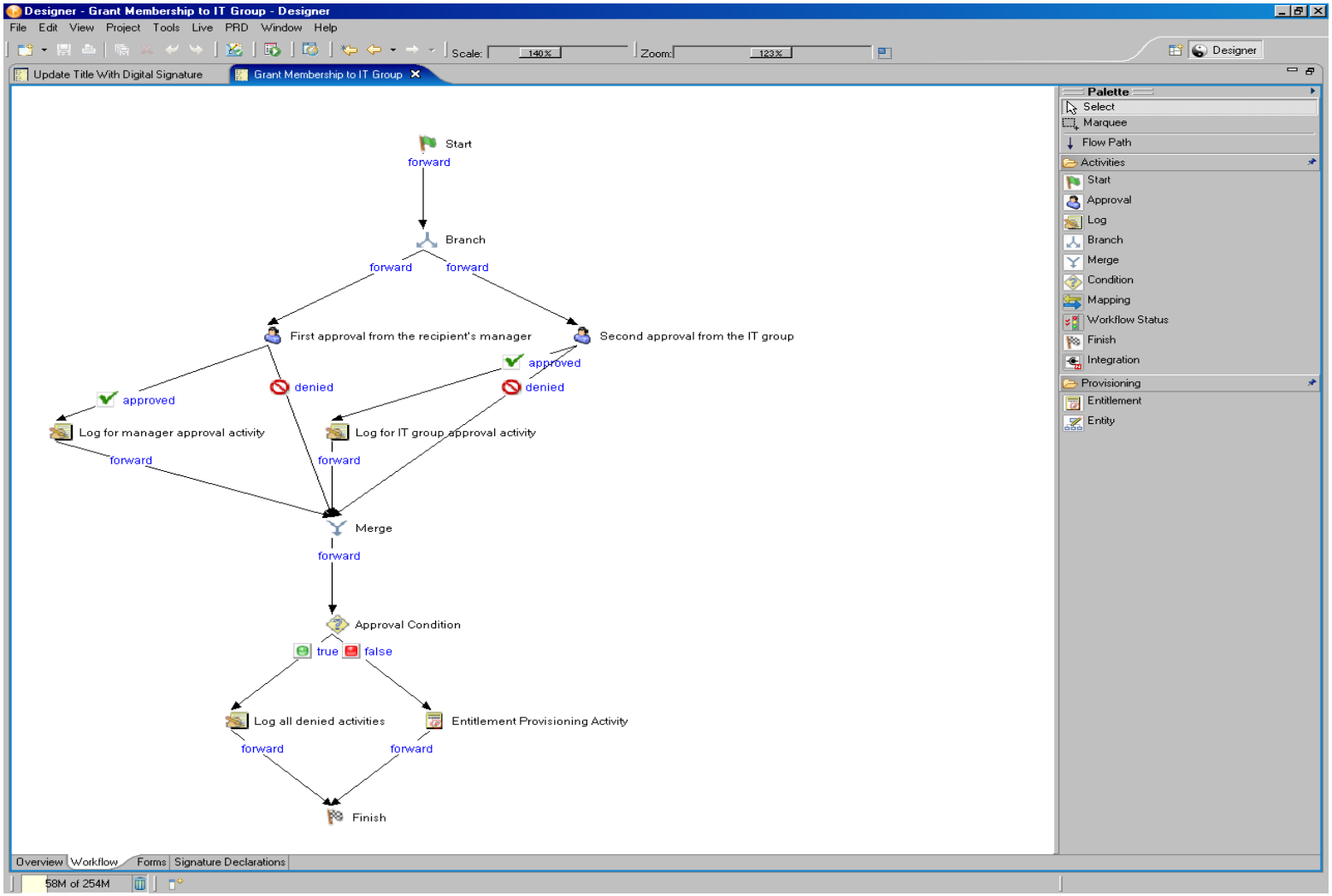
IDM – pohled na výpis z vyhledávače osob



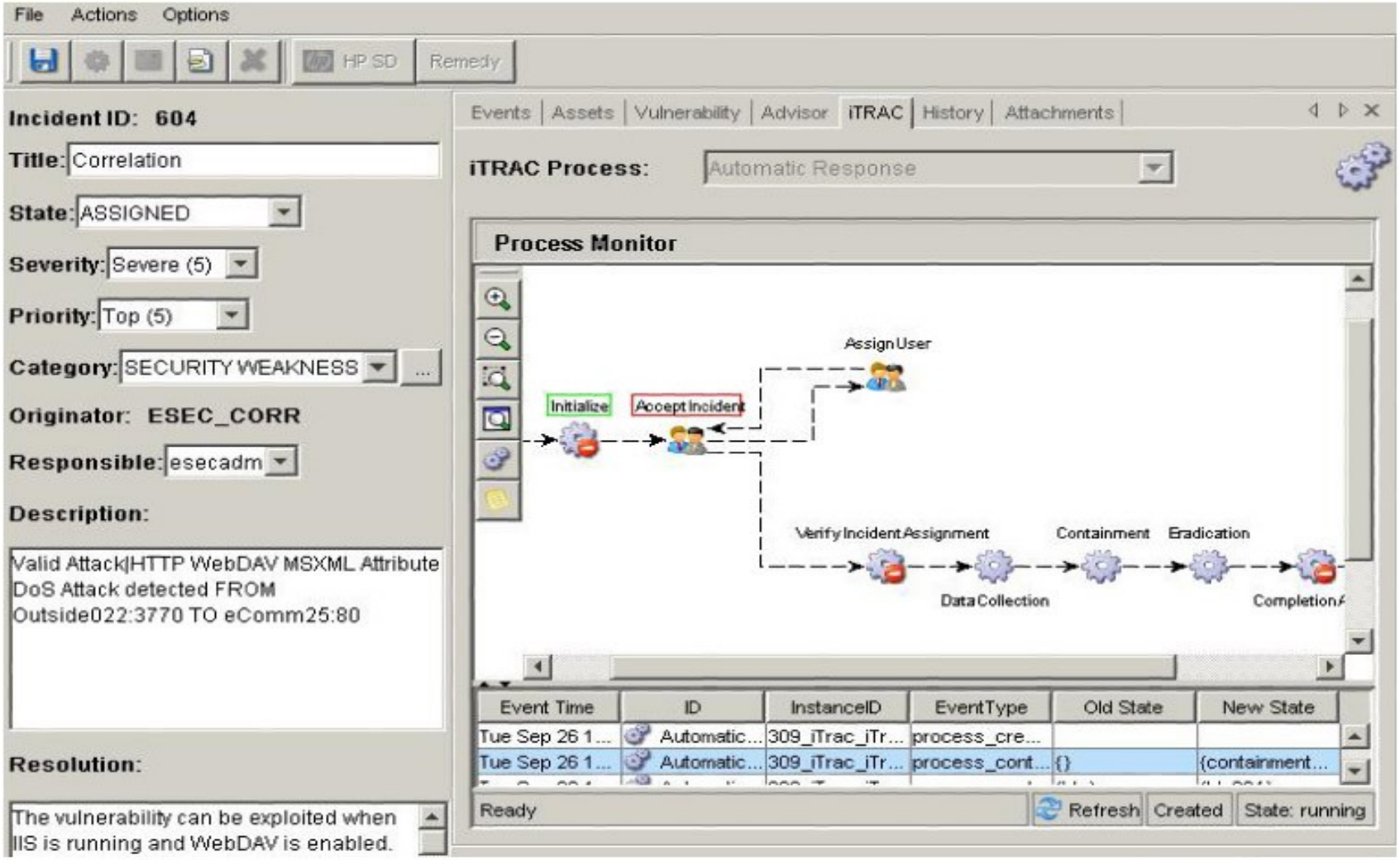
Pokročilá webová aplikace používá sjednocená data.

- Přehledné org. schéma a seznamy
- Samoobsluha správy hesel
- Delegovaná administrace až na úroveň vedoucích jednotlivých pracovních týmů.

IDM – z pohledu administrátora, Designer



Sentinel
– nástroj pro Compliance monitoring



Děkuji za pozornost.

sbirnerova@novell.com


Novell®