

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 Research 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**

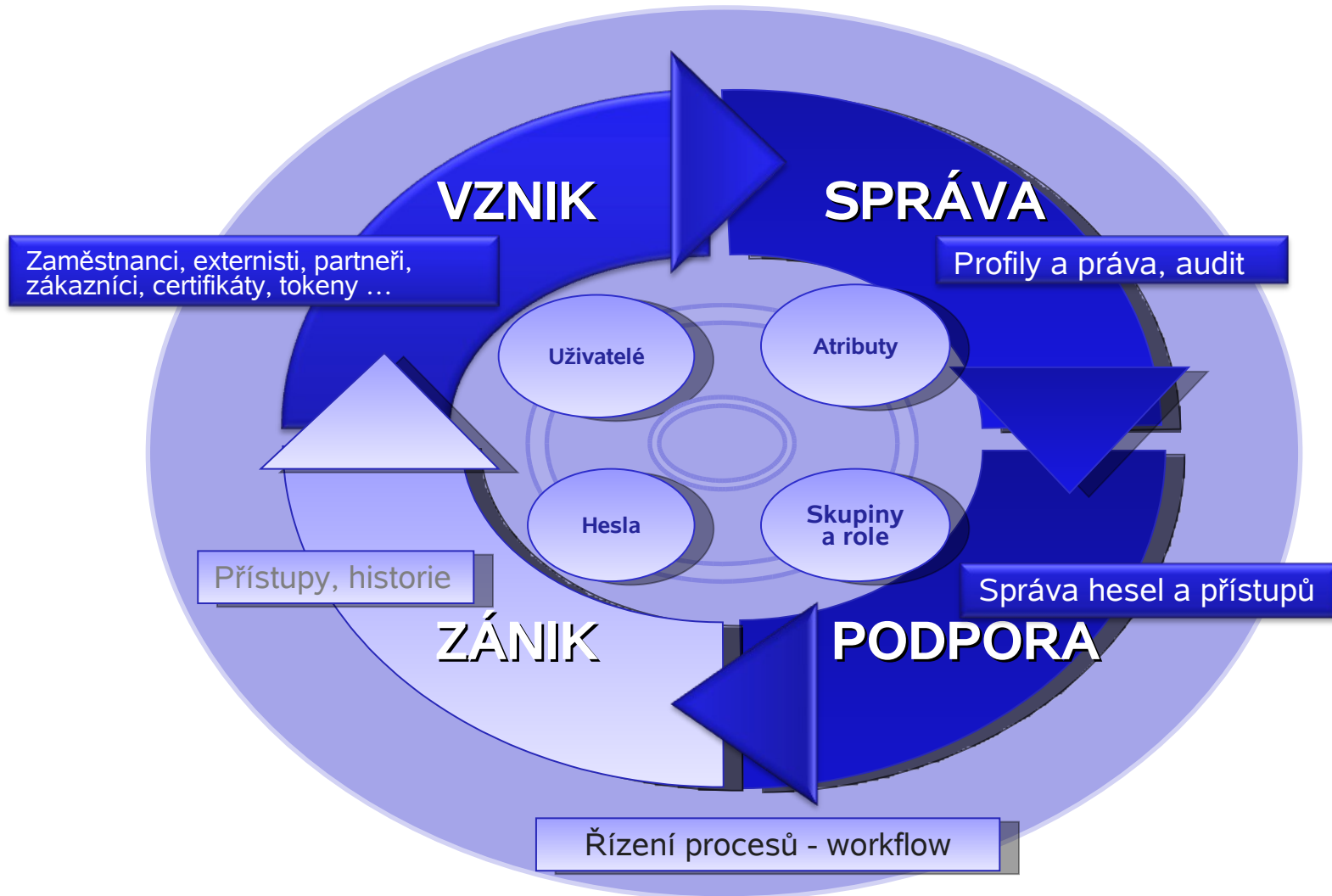
- První, který politiky řídí, definuje, vynucuje
- Druhý, který v reálném čase provádí kontrolu, audituje

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

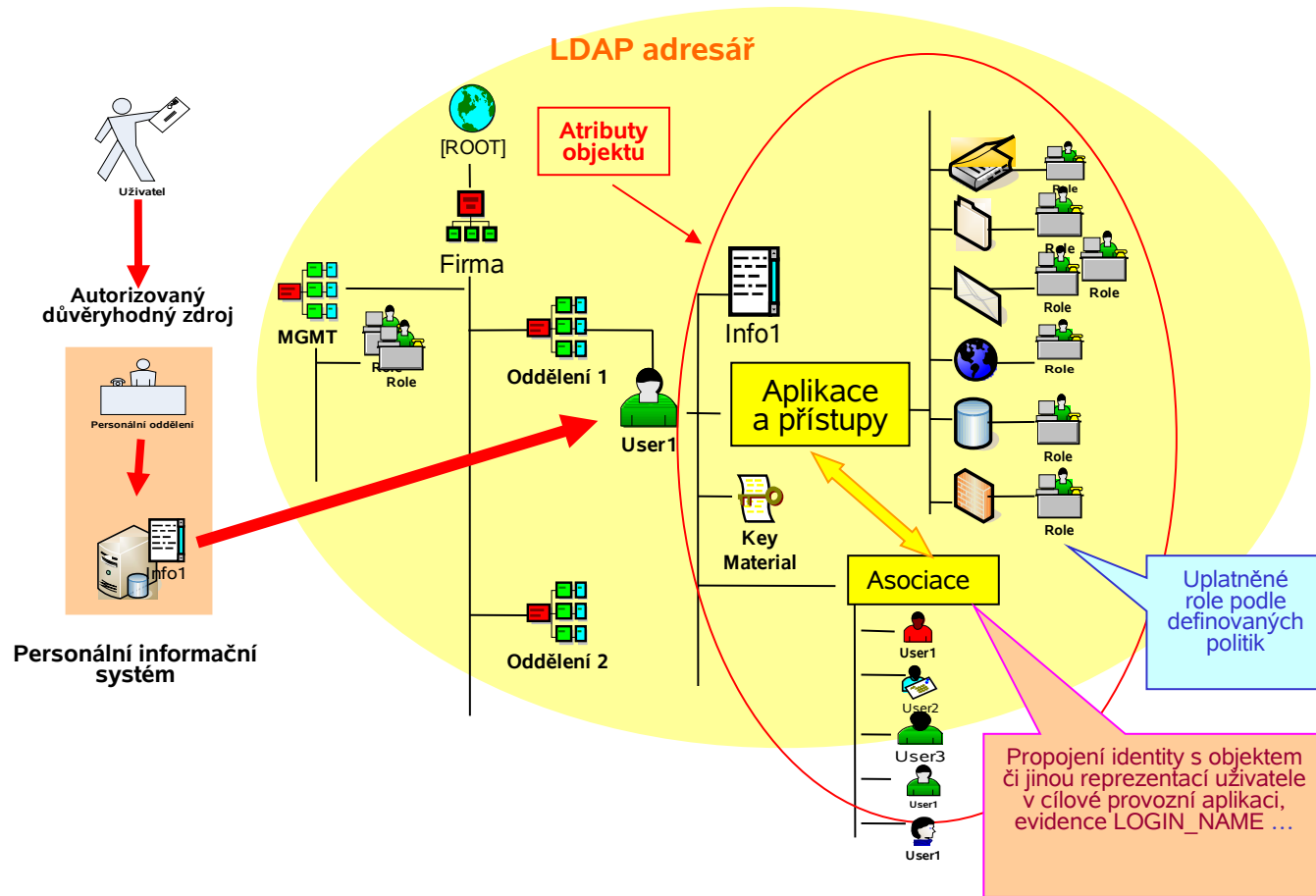
Centrální úložiště identit – trezor

- 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 personalizaci založenou na rolích a jejich prostřednictvím přidělovaných právech

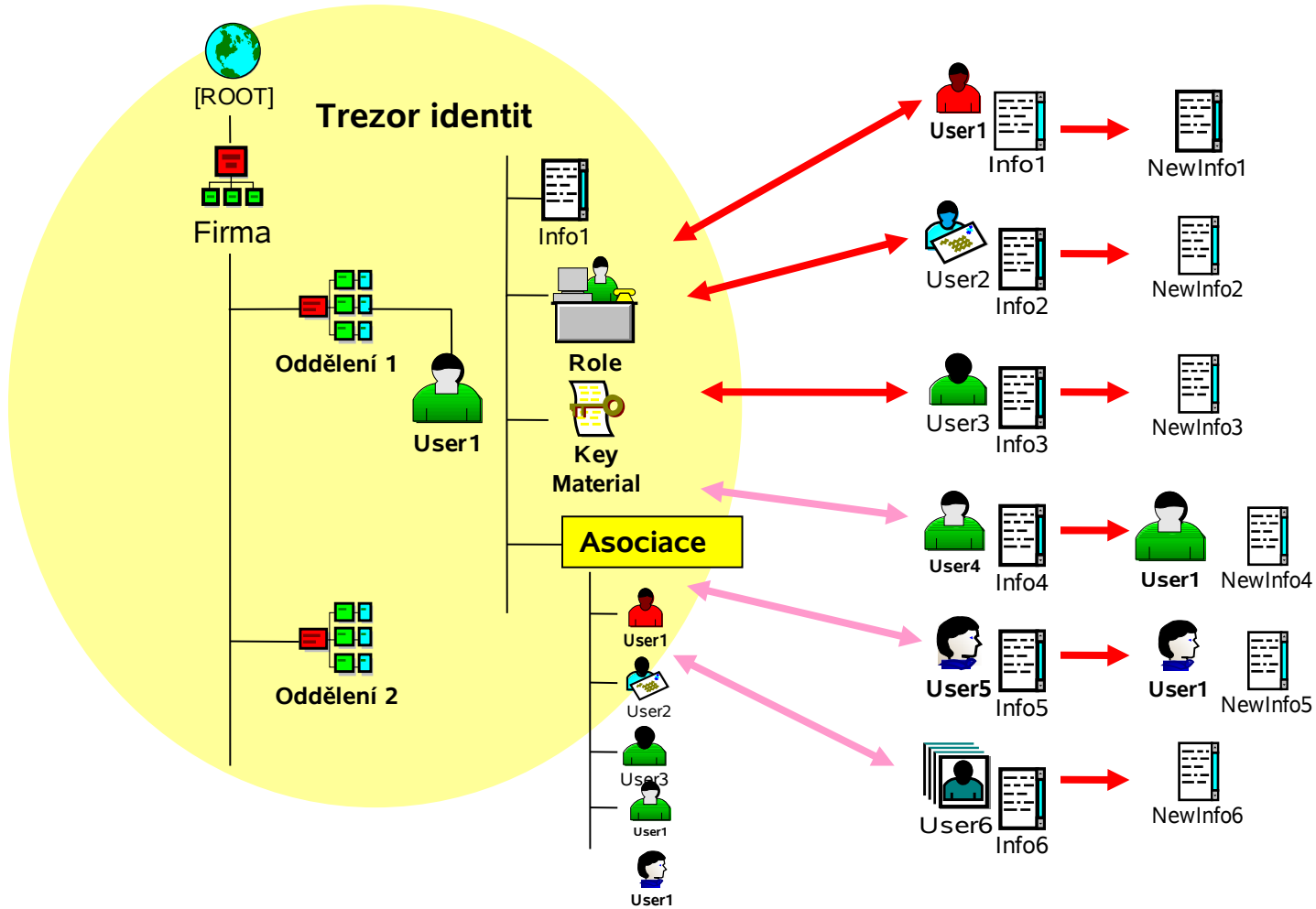
Metaadresářové služby

- 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

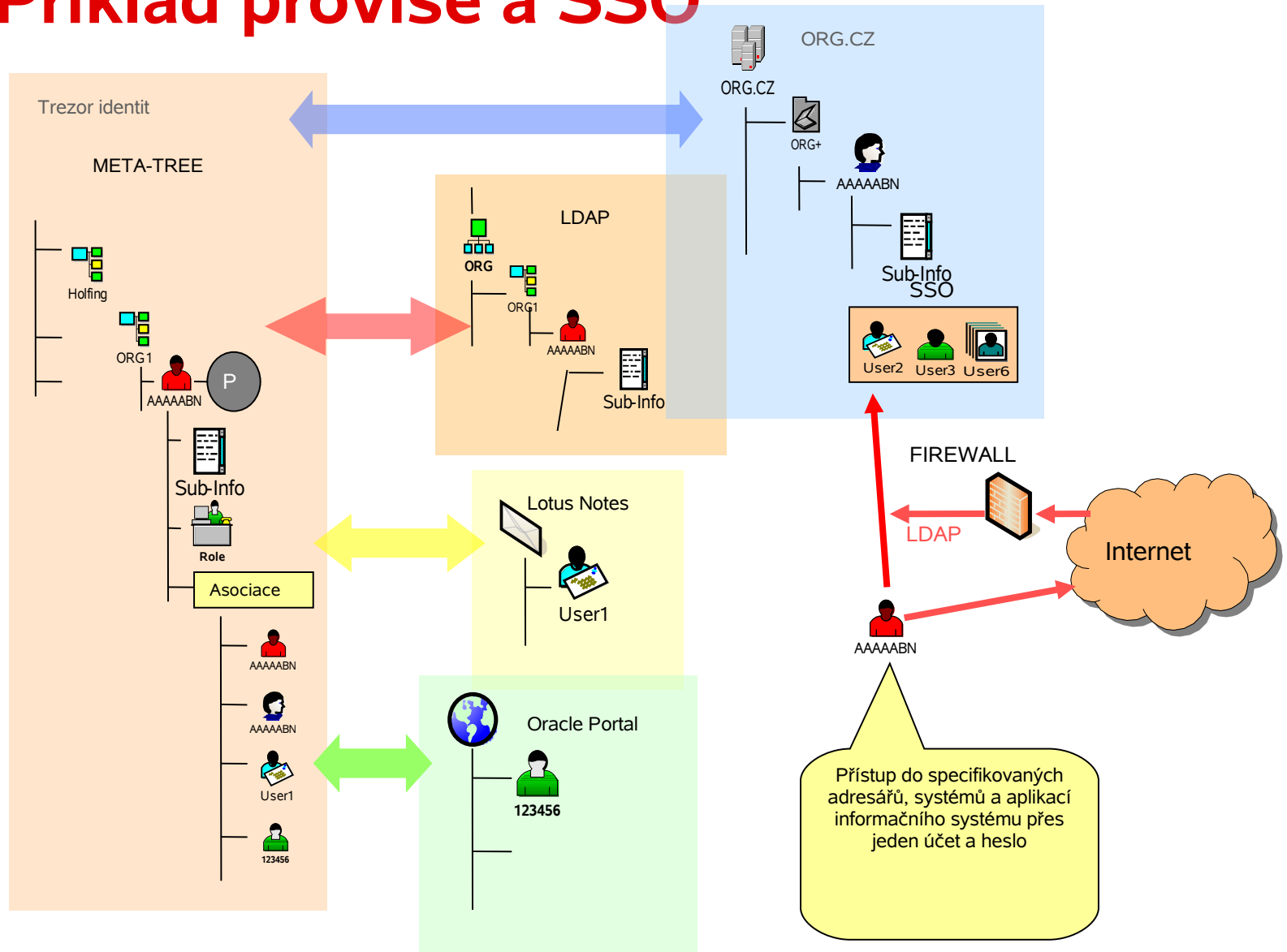
Trezor identit



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

The background of the slide is a solid blue color with a pattern of diagonal lines in various shades of blue, creating a sense of movement and depth. The lines are most prominent on the right side and fade towards the left.

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

Novell iManager
ADMIN
Unrestricted Access

Roles and Tasks

Provisioning Requests in 'UserApplication.IDMDriverSet.novell'

The following table lists the Provisioning Requests that are currently defined in 'UserApplication.IDMDriverSet.novell'. You can use the commands in the menubar to perform operations on these Provisioning Requests.

Provisioning Requests				
Create from... Delete Refresh Status▼ Actions▼				30 Item(s)
<input type="checkbox"/>	Name	Status	Category	Description
<input type="checkbox"/>	Access Financial System	Active	Accounts	Access Financial System - requires 2 levels
<input type="checkbox"/>	Adobe Software Access	Retired	Entitlements	Adobe Software Access - requires manager
<input type="checkbox"/>	Cell Phone Model_5100	Active	Entitlements	Cell Phone Model_5100
<input type="checkbox"/>	Cell Phone Model_5200	Inactive	Entitlements	Cell Phone Model_5200 - requires manager
<input type="checkbox"/>	Revoke Access Financial System	Active	Accounts	Revoke Access Financial System - requires
<input type="checkbox"/>	Revoke Adobe Software Access	Active	Entitlements	Revoke Adobe Software Access
<input type="checkbox"/>	Revoke Cell Phone Model_5100	Active	Groups	Revoke Cell Phone Model_5100
<input type="checkbox"/>	Revoke Cell Phone Model_5200	Active	Groups	Revoke Cell Phone Model_5200

Close

Plně vybavená webová administrační konzola.

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

The screenshot shows a Mozilla Firefox browser window displaying the Novell Identity Manager web application. The browser's address bar shows the URL: `http://newman.qalab.wal.novell.com:8080/Spitfire/getAFTaskList.do?afTaskListType=self`. The application interface includes a navigation menu on the left with categories like 'My Task Items', 'Resource Access', 'Processes in Progress', 'Proxy and Delegate', and 'Availability'. The main content area is titled 'My Tasks' and contains a table of pending approval tasks.

#	Task Name	Workflow Name	Initiated For	Expires in
1:	Manager Approval	Cell Phone Acquisition approval	Jack Miller	19 Days
2:	HR Approval	PeopleSoft Access approval	Christine Stone	19 Days
3:	HR Approval	Oracle Access approval	Francis Bacon	19 Days
4:	Manager Approval	Oracle Access approval	Jill Littlewood	19 Days
5:	Manager Approval	Oracle Access approval	Bob Smithers	19 Days
6:	Manager Approval	Oracle Access approval	Reikha Singer	19 Days

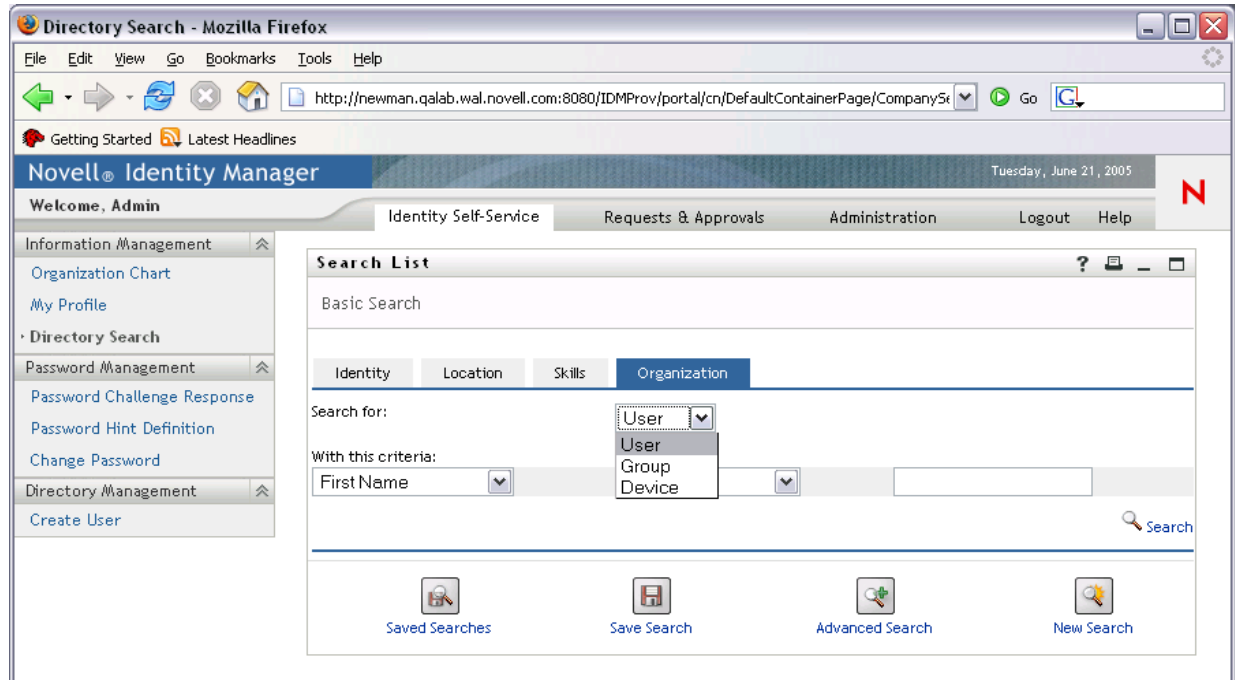
Below the table, it indicates '1 - 6 of 6' tasks.

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.

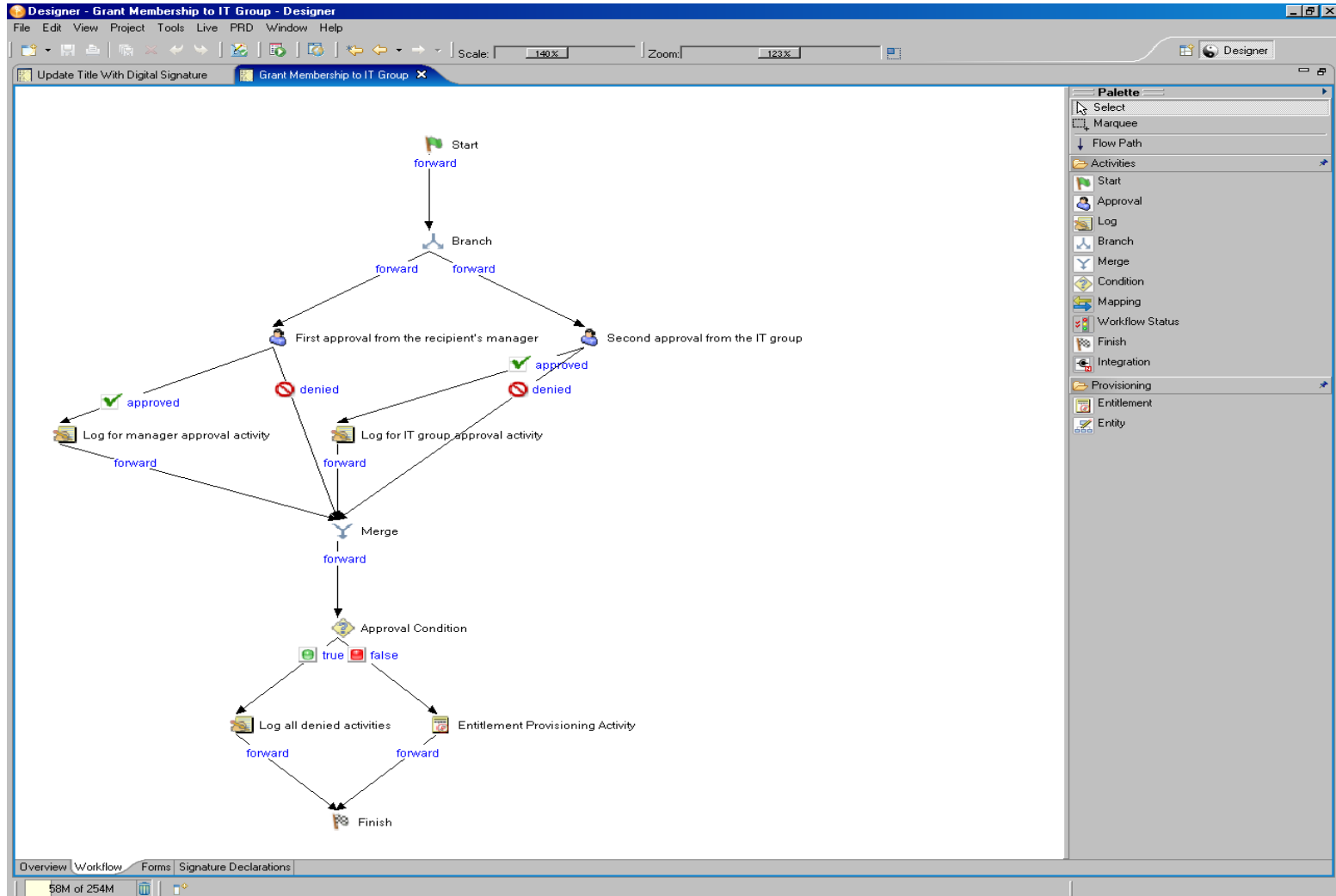
IDM – pohled na výpis z vyhledávače osob

The screenshot displays the Novell Identity Manager web interface. The top navigation bar includes the title 'Novell Identity Manager', the date 'Tuesday, November 22, 2005', and a user greeting 'Welcome, Allison'. Below this, there are tabs for 'Identity Self-Service' and 'Requests & Approvals', along with 'Logout' and 'Help' links. A left-hand sidebar menu lists various functions: 'Information Management' (with sub-items 'Organization Chart', 'My Profile', 'Directory Search'), 'Password Management' (with sub-items 'Password Challenge', 'Response', 'Password Hint Definition', 'Change Password'), and 'Directory Management' (with sub-item 'Create User or Group'). The main content area is titled 'Org Chart' and features a search box labeled 'Lookup'. The organization chart itself is a hierarchical tree structure. At the top level is 'Timothy Swan', Director, Marketing, Vice President. Reporting to him are 'Jane Smith', Marketing Research Director, and 'Margo MacKenzie', Director, Marketing. Under 'Margo MacKenzie' are 'Josh Kelley', Marketing Assistant, and 'Kevin Chester', Marketing Assistant. At the bottom level, reporting to 'Kevin Chester' is 'Allison Blake', Senior Creative Assistant. Each employee card includes a profile picture, name, title, and a set of small icons for actions like 'Info', 'Add', and 'Remove'.

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

File Actions Options

HP SD Remedy

Incident ID: 604

Title: Correlation

State: ASSIGNED

Severity: Severe (5)

Priority: Top (5)

Category: SECURITY WEAKNESS

Originator: ESEC_CORR

Responsible: esecadm

Description:

Valid Attack|HTTP WebDAV MSXML Attribute DoS Attack detected FROM Outside022:3770 TO eComm25:80

Resolution:

The vulnerability can be exploited when IIS is running and WebDAV is enabled.

Events Assets Vulnerability Advisor iTRAC History Attachments

iTRAC Process: Automatic Response

Process Monitor

Event Time	ID	InstanceID	EventType	Old State	New State
Tue Sep 26 1...	Automatic...	309_iTrac_iTr...	process_cre...		
Tue Sep 26 1...	Automatic...	309_iTrac_iTr...	process_cont...	{}	{containment...

Ready Refresh Created State: running

Děkuji za pozornost.
sbirnerova@novell.com

Novell®

Unpublished Work of Novell, Inc. All Rights Reserved.

This work is an unpublished work and contains confidential, proprietary, and trade secret information of Novell, Inc. Access to this work is restricted to Novell employees who have a need to know to perform tasks within the scope of their assignments. No part of this work may be practiced, performed, copied, distributed, revised, modified, translated, abridged, condensed, expanded, collected, or adapted without the prior written consent of Novell, Inc. Any use or exploitation of this work without authorization could subject the perpetrator to criminal and civil liability.

General Disclaimer

This document is not to be construed as a promise by any participating company to develop, deliver, or market a product. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. Novell, Inc. makes no representations or warranties with respect to the contents of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. The development, release, and timing of features or functionality described for Novell products remains at the sole discretion of Novell. Further, Novell, Inc. reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. All Novell marks referenced in this presentation are trademarks or registered trademarks of Novell, Inc. in the United States and other countries. All third-party trademarks are the property of their respective owners.

