

Novell Identity Manager

Ing. Zdeněk Stehlík
Technology Specialist, Novell-Praha
zstehlik@novell.cz

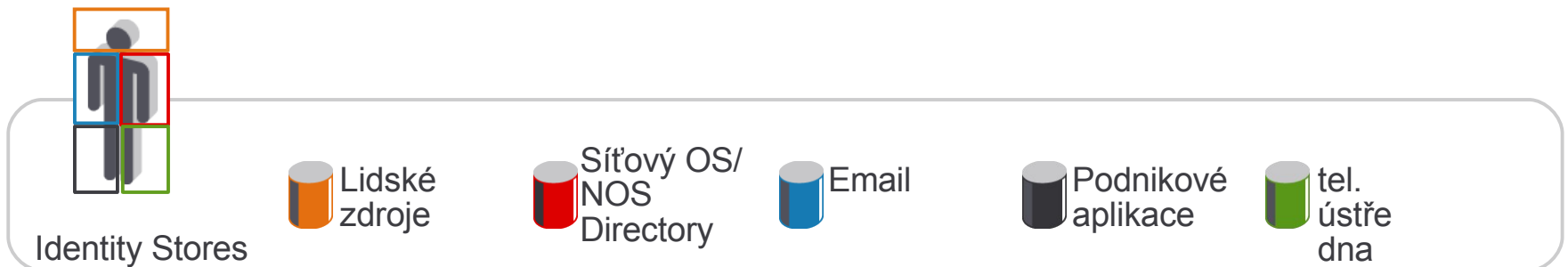
ISSS 2007

Novell.[®]

Co je správa identit?

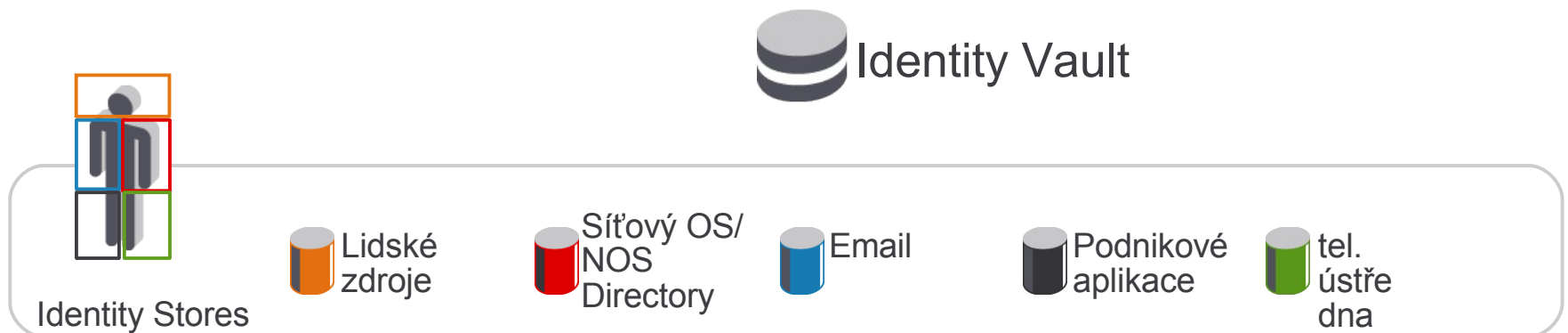
Vaše organizace má více systémů s vlastním úložištěm informací o identitách uživatelů.

- Mnoho podnikových aplikací vlastní a používá kus identity uživatelů
 - tato data:
 - > je drahé udržovat
 - > nemohou být plně sdílena těmi, kdo je potřebují
 - > mohou být nepřesná, nekonzistentní a neaktualizovaná



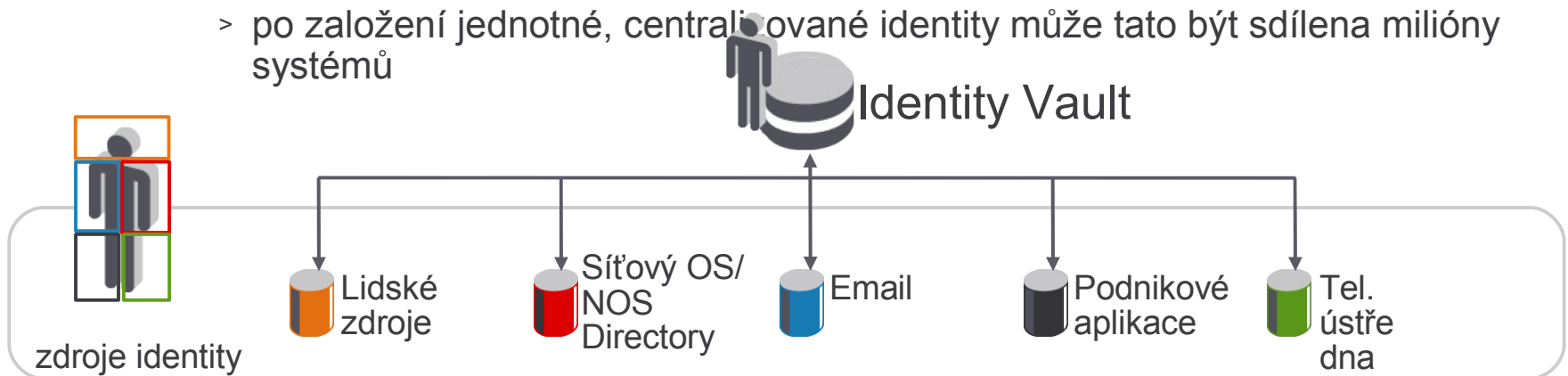
Centrální úložiště identit

- problémy s izolovanými identitami vyřeší centrální úložiště tzv. „Identity Vault“
 - místo pro centralizovanou správu identit
 - mnoho aplikací sdílí tytéž údaje o identitě a autentizace a autorizace je funkčně sjednocena
 - poskytuje základ pro centralizované řízení přístupu
 - umožňuje personalizaci založenou na rolích a jejich prostřednictvím přidělovaných právech



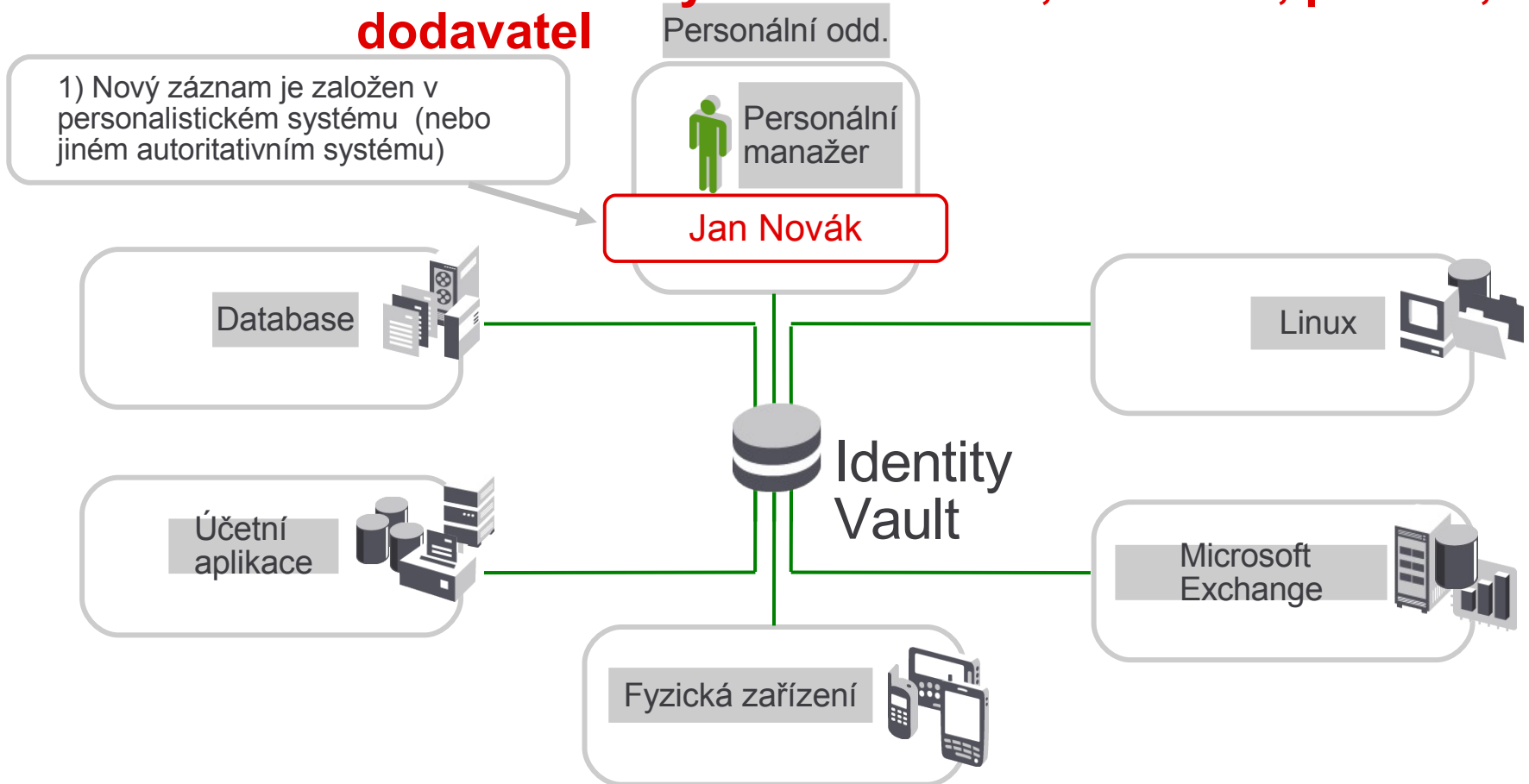
Metaadresářové služby

- Abychom mohli agregovat data související s identitou do centrálního úložiště, používáme techniku meta-directory (metadresáře), který
 - 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 milióny systémů



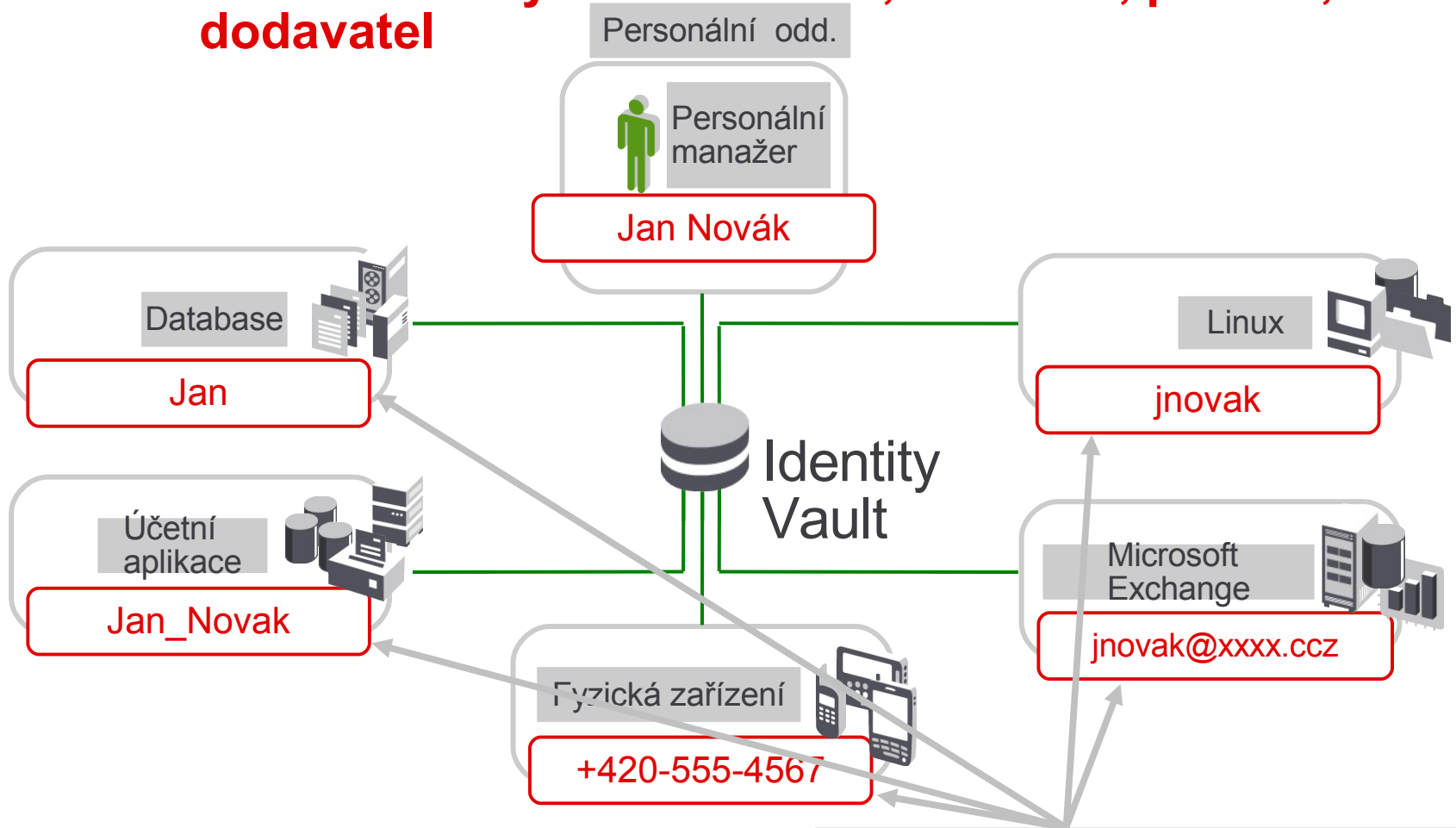
Založení uživatelského účtu na základě rolí

Scénáře: Nový zaměstnanec, zákazník, partner, dodavatel



Založení uživatelského účtu na základě rolí

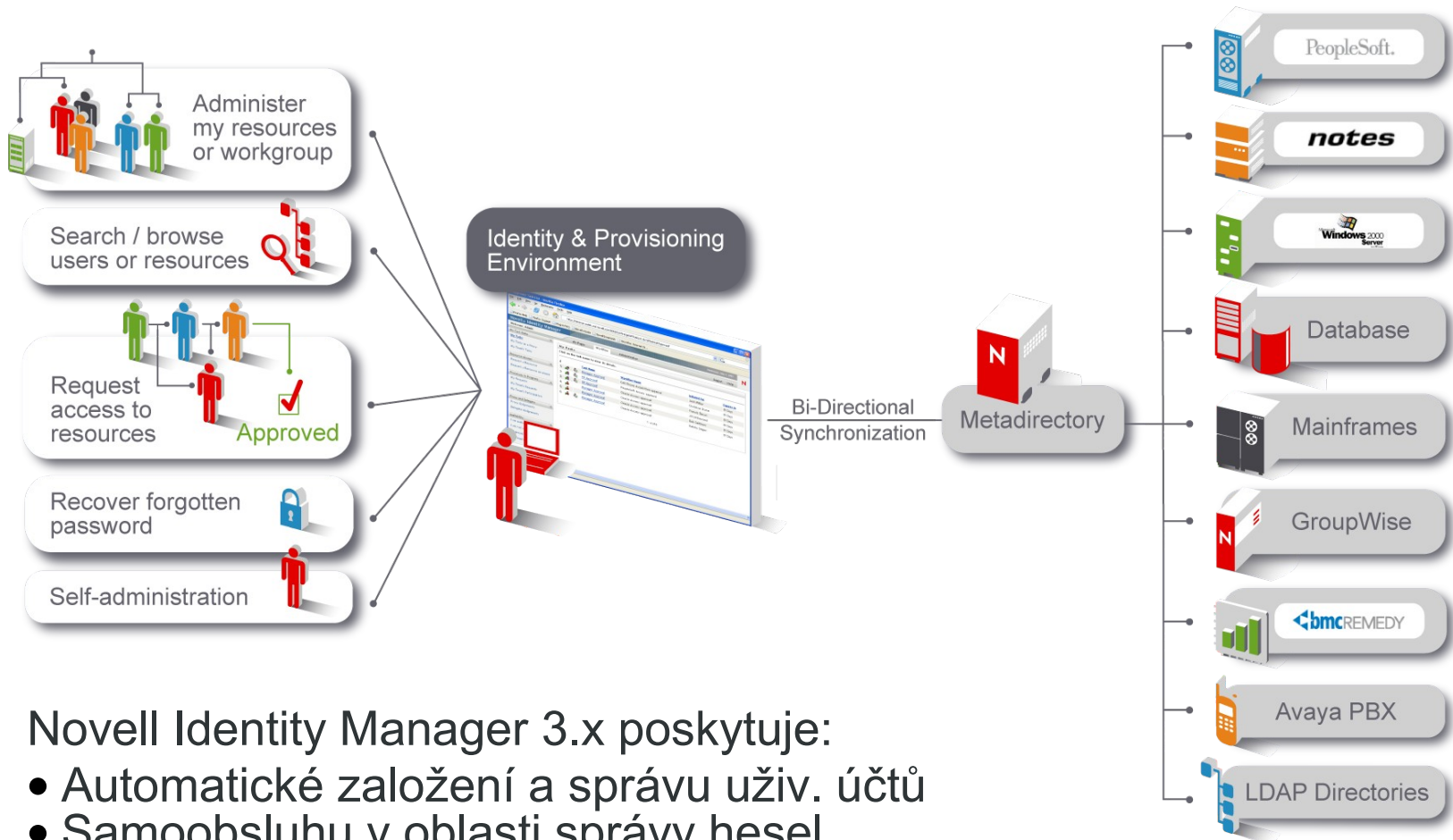
Scénáře: Nový zaměstnanec, zákazník, partner, dodavatel



- 2) Identity Manager zachytí událost
- 3) Identity Manager pak založí účty ve všech propojených systémech a synchronizuje je na základě definovaných pravidel

Novell® Identity Manager 3.x

Novell® Identity Manager 3.x



Novell Identity Manager 3.x poskytuje:

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

To vše napříč platformami: Linux, Windows, Solaris, HP-UX, AIX a NetWare®

Základní výhody řešení Novell

1. Využití technologických výhod vyspělého metadresáře založeného na Novell eDirectory a synchronizační technice DirXML
2. Integrovaný schvalovací proces pro algoritmizaci a automatizaci přidělování přístupových práv (workflow).
3. Webová aplikace iManager pro správu identity
4. Atraktivní a flexibilní uživatelské prostředí (webový portál)
5. Designer for Identity Manager - grafický návrhový systém
6. Nejvyšší počet propojitelných platforem a aplikací
7. Vysoká škálovatelnost a bezpečnost dat, audit a propojení s bezpečnostními a autentizačními systémy

Novell Identity Manager - propojitelné systémy (drivery):

database

IBM DB2
Informix
Microsoft SQL Server
MySQL
Oracle
Sybase
JDBC

directories

Critical Path InJoin Directory
IBM Directory Server (SecureWay)
iPlanet Directory Server
Microsoft Active Directory
Microsoft Windows NT Domains
Netscape Directory Server
NIS
NIS +
Novell NDS
Novell eDirectory
Oracle Internet Directory
Sun ONE Directory Server
LDAP

email systems

Microsoft Exchange 2000, 2003
Microsoft Exchange 5.5
Novell GroupWise
Lotus Notes

enterprise applications

Baan
J.D.Edwards
Lawson
Oracle
Peoplesoft
SAP HR
SAP R/3 4.6 and SAP Enterprise
Systems (BASIS)
SAP Web Application Server (Web
AS) 6.20
Siebel

enterprise message bus

BEA
IBM Websphere MQ
Open JMS
Oracle
JBOSS
Sun
TIBCO

mainframe

RACF
ACF2
Top Secret

midrange

OS/400 (AS/400)

operating systems

Microsoft Windows NT 4.0
Microsoft Windows 2000, 2003
SUSE LINUX
Debian Linux
FreeBSD
Red Hat AS and ES
Red Hat Linux
HP-UX
IBM AIX
Solaris
UNIX Files - /etc/passwd

other

Delimited Text
Remedy (for Help Desk)
SOAP
DSML
SPML
Schools Interoperability Framework (SIF)

pbx

Avaya PBX

***NOTE:** Identity Manager customers have integrated numerous other systems utilizing general purpose Identity Manager drivers such as JDBC, Delimited Text, or LDAP

Integrace schvalovacího postupu Z pohledu manažera



#	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

Uživatelská aplikace ukazuje schvalovací úkoly v jediném okně.

Je zde plně vybavený 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.)

Aplikace pro práci s identitami z pohledu uživatele

The screenshot displays the Novell Identity Manager web application interface. The top navigation bar includes the title "Novell Identity Manager", the date "Tuesday, November 22, 2005", and a user profile "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", "Organization Chart", "My Profile", "Directory Search", "Password Management", "Password Challenge", "Response", "Password Hint Definition", "Change Password", "Directory Management", and "Create User or Group". The main content area is titled "Org Chart" and features a "Lookup" search bar. The organization chart itself is a hierarchical tree structure. At the top level is "Timothy Swan, Director, Marketing, Vice President". Reporting to him are three directors: "Jane Smith, Marketing Research Director", "Margo MacKenzie, Director, Marketing", and "Allison Blake, Senior Creative Assistant". Under "Jane Smith" are "Josh Kelley, Marketing Assistant" and "Kevin Chester, Marketing Assistant". Each employee card includes a photo, name, title, and icons for information, search, and email.

Pokročilá webová aplikace používá sjednocená data.

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

Aplikace pro práci s identitami

pohled na výpis z vyhledávače osob

The screenshot shows a web browser window with the address bar displaying 'http://newman.qalab.wal.novell.com:8080 - DetailPortlet - Mozilla Firefox'. The main content area is titled 'Detail' and features a user profile for 'Chip Nano'. The profile includes a photo of a man with glasses and a blue turtleneck. To the right of the photo are three action links: 'Edit User', 'Send Identity Info', and 'Display Organization Chart'. Below the photo is a table of user details.

First Name:	Chip
Last Name:	Nano
Email:	test@novell.com
Region:	Northeast, U.S.
Telephone Number:	(555) 555-1222
Department:	Management
Manager:	Jack Miller
Cost Center:	US1122
Groupwise IM:	
Yahoo IM:	
AOL IM:	
Certification/Education:	MS - Massachusetts Institute of Technology, CNA - Certified Novell Administrator, CNE - Certified Novell Engineer, CLE - Certified Linux Engineer, PMP - Project Management Professional, HPCP - HP Certified Professional
Product Skills:	Novell exteNd, Novell IDM, Novell Groupwise, Novell SUSE, Novell eDirectory, Novell Ximian, Novell iChain, Novell BorderManager, Novell Netware
Assigned Devices:	Latitude D800 , HP Color LaserJet 3700 , Samsung 1700 Pocket PC , Motorola V710 , IBM ThinkCentre S9028

The browser status bar at the bottom shows 'Done'.

Pokročilá webová aplikace používá sjednocená data.

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

Aplikace pro práci s identitami pohled na výpis z vyhledávače osob

Directory Search - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://newman.qalab.wal.novell.com:8080/IDMProv/portal/cn/DefaultContainerPage/Company5k

Getting Started Latest Headlines

Novell Identity Manager Tuesday, June 21, 2005

Welcome, Admin Identity Self-Service Requests & Approvals Administration Logout Help

Information Management

- Organization Chart
- My Profile

Directory Search

Password Management

- Password Challenge Response
- Password Hint Definition
- Change Password

Directory Management

- Create User

Search List

Basic Search

Identity Location Skills Organization

Search for: User

With this criteria: First Name

User Group Device

Search

Saved Searches Save Search Advanced Search New Search

Pokročilá webová aplikace používá sjednocená data.

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

Aplikace pro práci s identitami pohled na výpis z vyhledávače osob

Directory Search - Mozilla Firefox

http://newman.qalab.wal.novell.com:8080/IDMProv/portal/cn/DefaultContainerPage/CompanySc

Novell® Identity Manager Tuesday, June 21, 2005

Welcome, Admin

Identity Self-Service Requests & Approvals Administration Logout Help

Information Management

- Organization Chart
- My Profile
- Directory Search

Password Management

- Password Challenge Response
- Password Hint Definition
- Change Password

Directory Management

- Create User

Search List

Results

Identity Location Skills Organization

User: (First Name starts with a) or
(First Name starts with b) or
(First Name starts with t) Sorted by: Last Name Total Matches: 13

First Name	Last Name	Telephone Number	Groupwise IM	Yahoo IM	Email
Bill	Bender	(555) 555-1320			
Allison	Blake	(555) 555-1222			
Bill	Brown	(555) 555-1225			
Bill	Burke	(555) 555-1210			
Angie	Chung	(555) 555-1208			
Admin	idmsample	(617) 555-1212			
Bob	Jenner	(555) 555-1314			
Brad	Jones	(555) 555-1313			
Terry	Mellon	(555) 555-1222			
Anthony	Palani	(555) 555-1202			

1 - 10 of 13

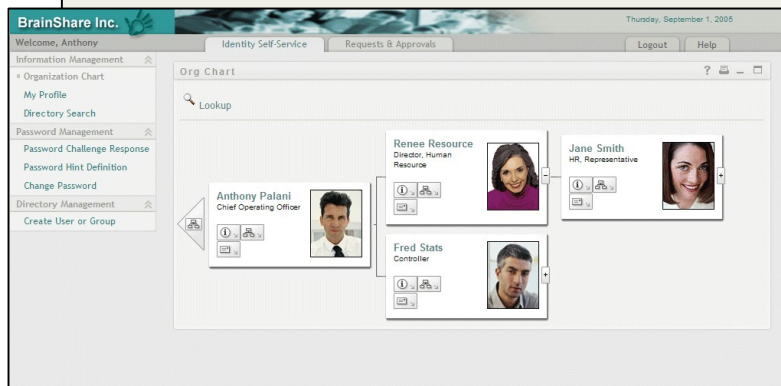
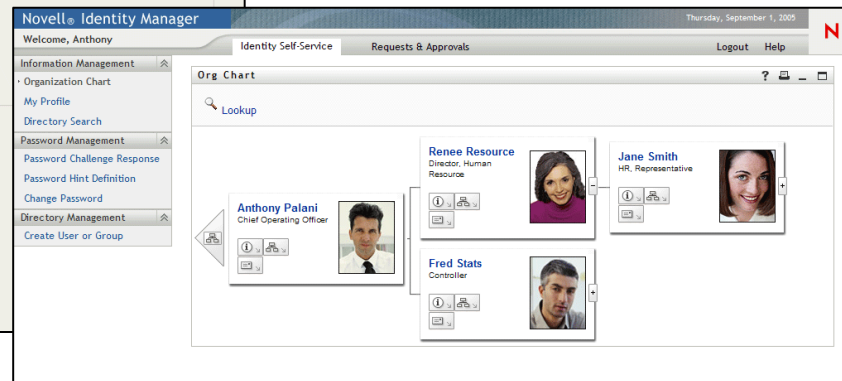
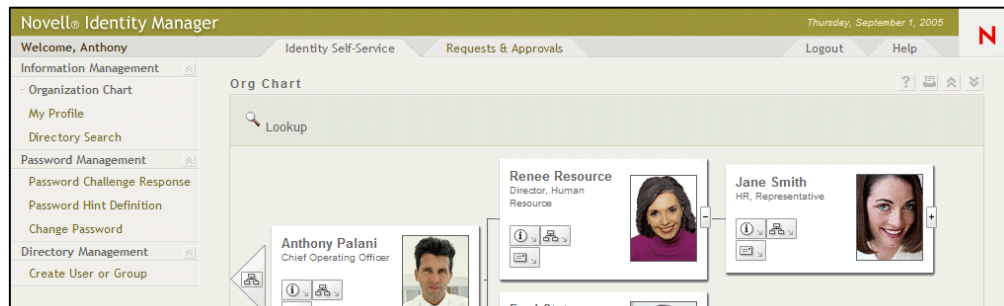
Next Last

Saved Searches Save Search Export Results Revise Search New Search

Pokročilá webová aplikace používá sjednocená data.

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

Atraktivní a flexibilní uživatelské prostředí



Webová aplikace zdělila funkce z Novell® SOA technologie.

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

Správa a konfigurace

Robustí a výkonná správa

Pohled administrátora

The screenshot displays the Novell iManager ADMIN interface. The left sidebar shows a navigation tree with categories like 'Roles and Tasks', 'Identity manager', 'Utilities', 'LDAP', 'NMAP', 'Novell Certificate Access', 'Novell Certificate Server', 'Partition and Replica Management', 'Passwords', 'PBX', 'Provisioning Request Configuration', and 'Rights'. The main content area is titled 'Provisioning Requests in 'UserApplication.IDMDriverSet.novell''. It contains a table of provisioning requests with columns for Name, Status, Category, and Description. The table lists 30 items, including 'Access Financial System', 'Adobe Software Access', 'Cell Phone Model_5100', 'Cell Phone Model_5200', 'Revoke Access Financial System', 'Revoke Adobe Software Access', 'Revoke Cell Phone Model_5100', and 'Revoke Cell Phone Model_5200'. A 'Close' button is visible at the bottom of the table area.

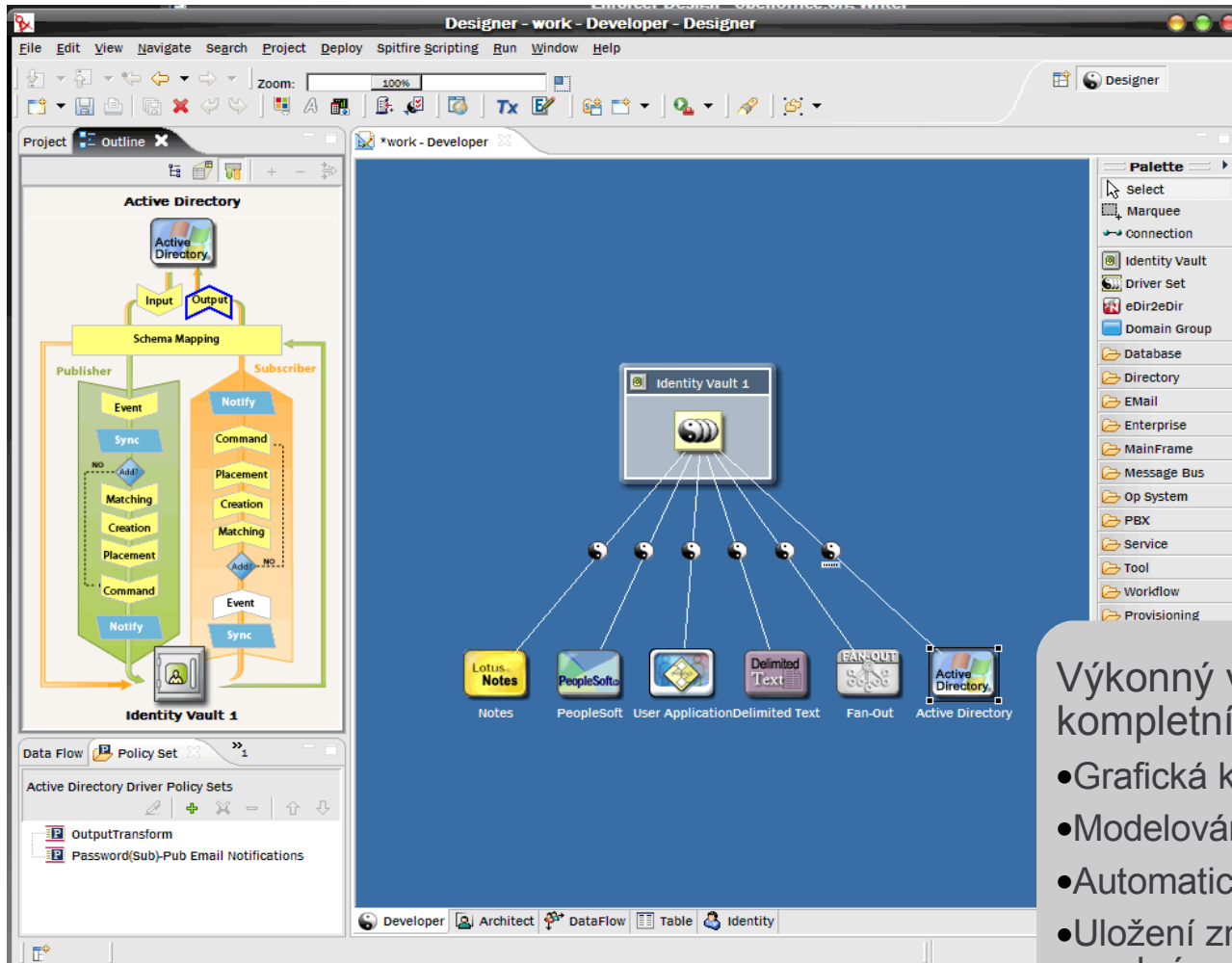
Name	Status	Category	Description
Access Financial System	Active	Accounts	Access Financial System - requires 2 levels
Adobe Software Access	Retired	Entitlements	Adobe Software Access - requires manager
Cell Phone Model_5100	Active	Entitlements	Cell Phone Model_5100
Cell Phone Model_5200	Inactive	Entitlements	Cell Phone Model_5200 - requires manager
Revoke Access Financial System	Active	Accounts	Revoke Access Financial System - requires
Revoke Adobe Software Access	Active	Entitlements	Revoke Adobe Software Access
Revoke Cell Phone Model_5100	Active	Groups	Revoke Cell Phone Model_5100
Revoke Cell Phone Model_5200	Active	G	

Plně vybavená webová administrační konzola.

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

Designer for Identity Manager

Pohled systémového architekta



Výkonný vizuální nástroj pro design kompletního prostředí.

- Grafická konfigurace složitého systému
- Modelování metodou "Co kdyby..?"
- Automaticky generovaná dokumentace
- Uložení znovu použitelných konfigurací pro zkrácení implementační doby
- Prostředí Eclipse

Editory použité v Designeru

- **Provisioning Request Definition Editor**

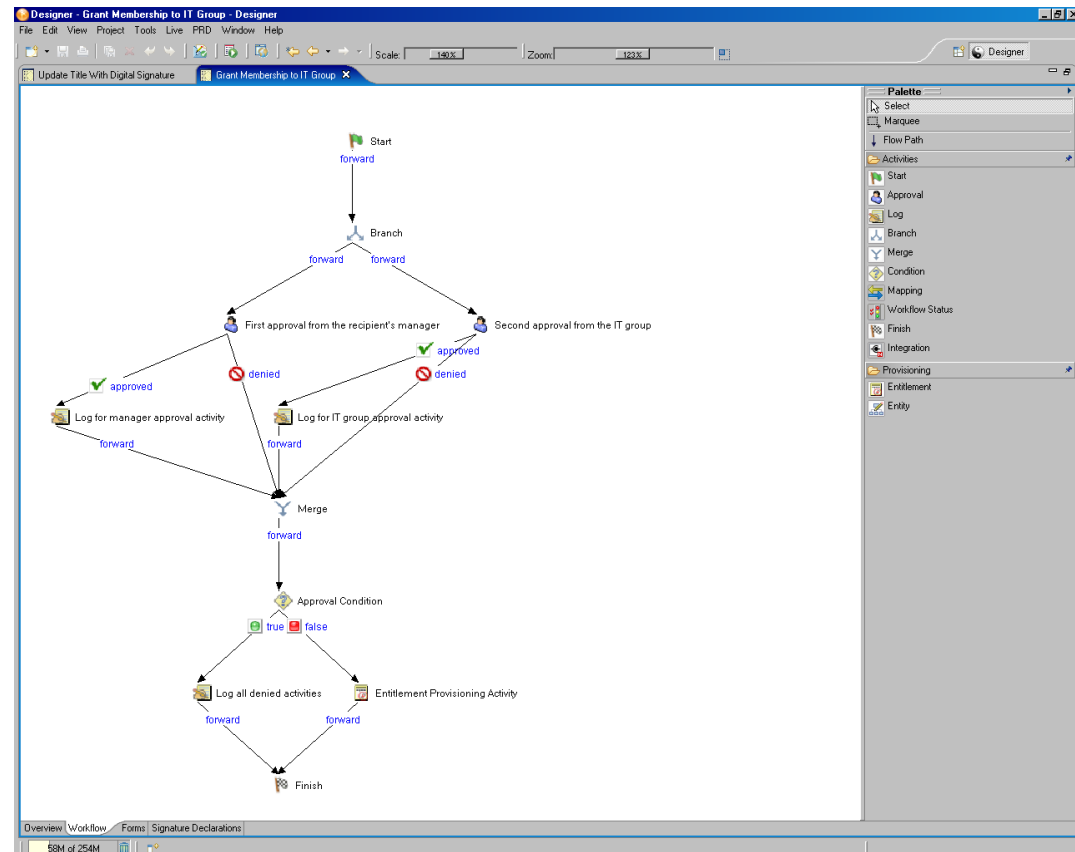
- dovoluje syst. architektovi vizuálně vytvářet schvalovací postupy v Designeru a instalovat je na IDM server.

- **Editor pro vytváření el. formulářů**

- pro schvalovací formuláře používané ve workflow

- **eDirectory Object Manager**

- zakládání, rušení, přejmenovávání, přesuny a modifikace všech druhů objektů a atributů



Otázky & odpovědi

Novell®

Award-Winning Technology

Ahead of the competition



InfoWorld The Identity Management Challenge

- October 10, 2005 Oliver Rist & Paul Venezia

In a recent shootout of competitive identity management solutions from Novell®, Courion*, IBM*, Microsoft*, Sun*, and Thor Technologies* **Novell emerged victorious.**

“Novell Identity Manager proved to be one of the **easiest-to-use** solutions in the roundup. The addition of Designer adds **even more intuitive functionality** on top of this suite.”

“Designer gives the Novell solution **a definite ooh-aah factor not found in any of the other products here.**”

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. 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. 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.

