

# Nasazení Micro Focus IdM pro úplnou správu identit v univerzitním prostředí

**Jiří Provazník**

**e-mail: [jprovaznik@tdp.cz](mailto:jprovaznik@tdp.cz)**

**Továrna na dokonalé programy, s.r.o.**

**[www.tdp.cz](http://www.tdp.cz)**

# IDM

**IDM** (*IDentity Management*)

=

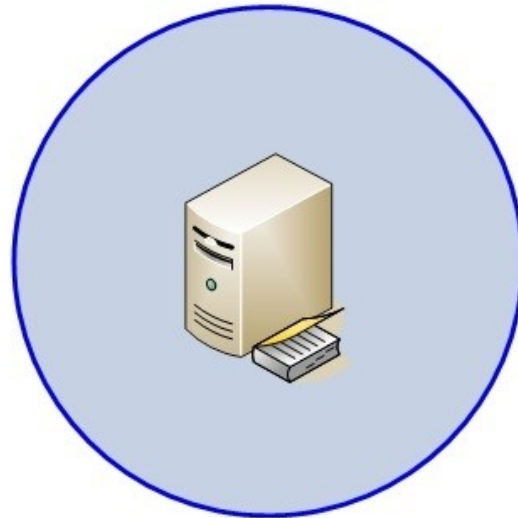
správa identit

=

Řízené propůjčování informací o lidech z jednoho zabezpečeného zdroje informací.  
Zdroj informací je plněn údaji z ověřených autoritativních zdrojů.

# Obečné schéma IDM

Dobře zabezpečené  
místo



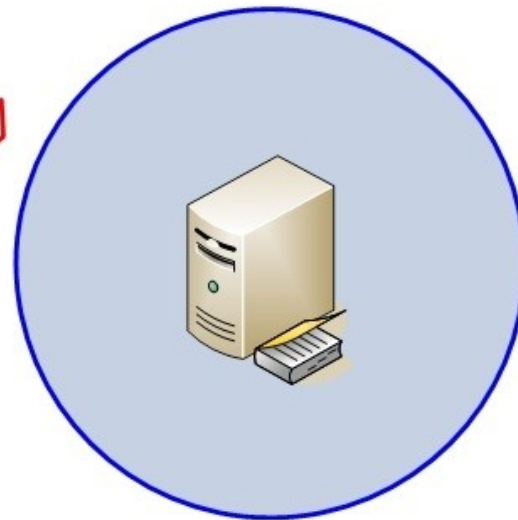
Trezor identit

# Obečné schéma IDM

Shromažďování  
informací



Dobře zabezpečené  
místo



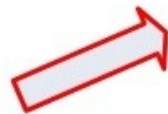
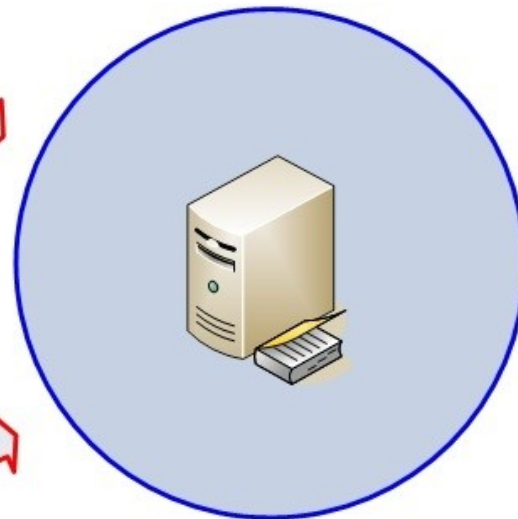
Autoritativní zdroje dat

Trezor identit

# Obečné schéma IDM

Shromažďování  
informací

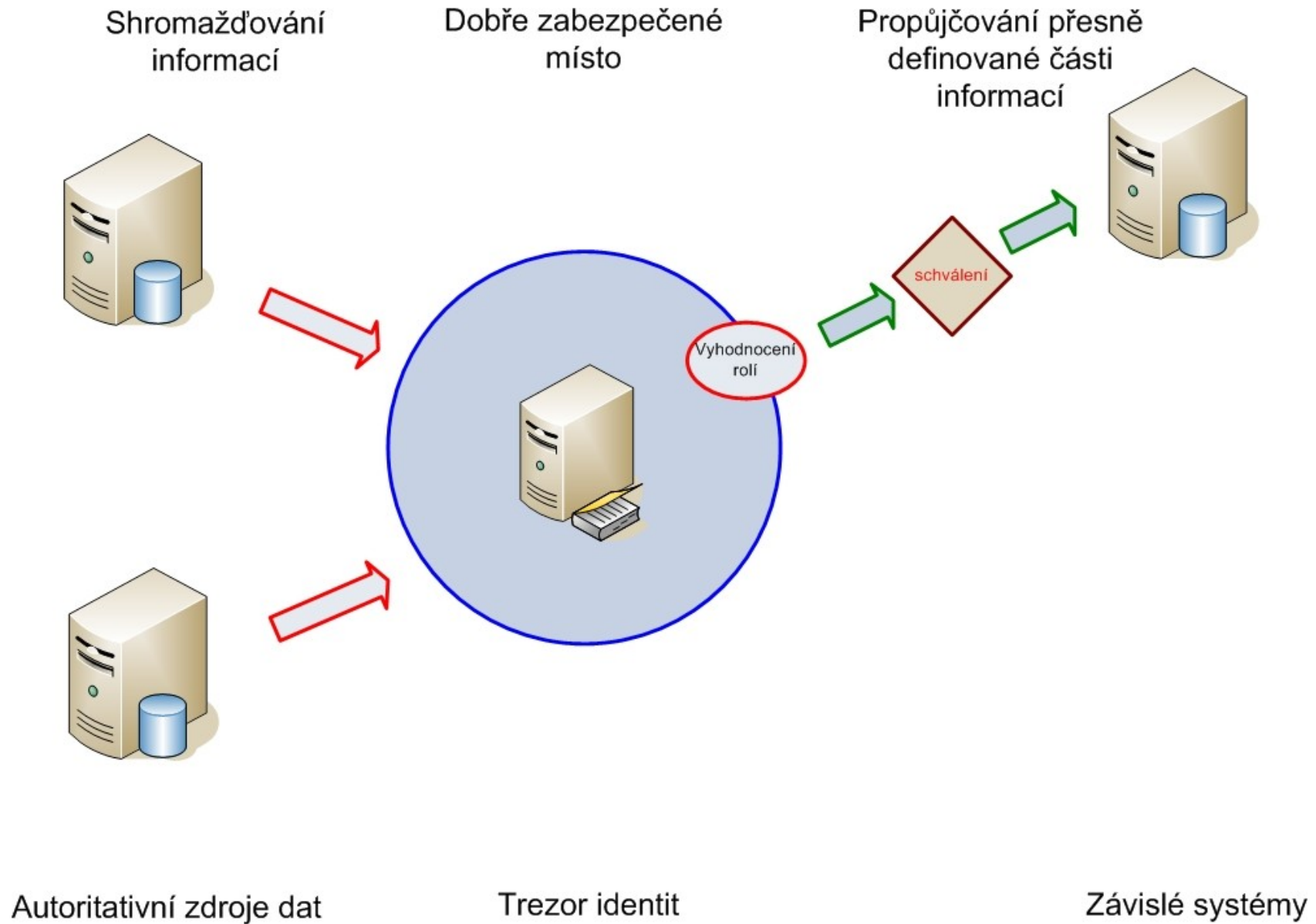
Dobře zabezpečené  
místo



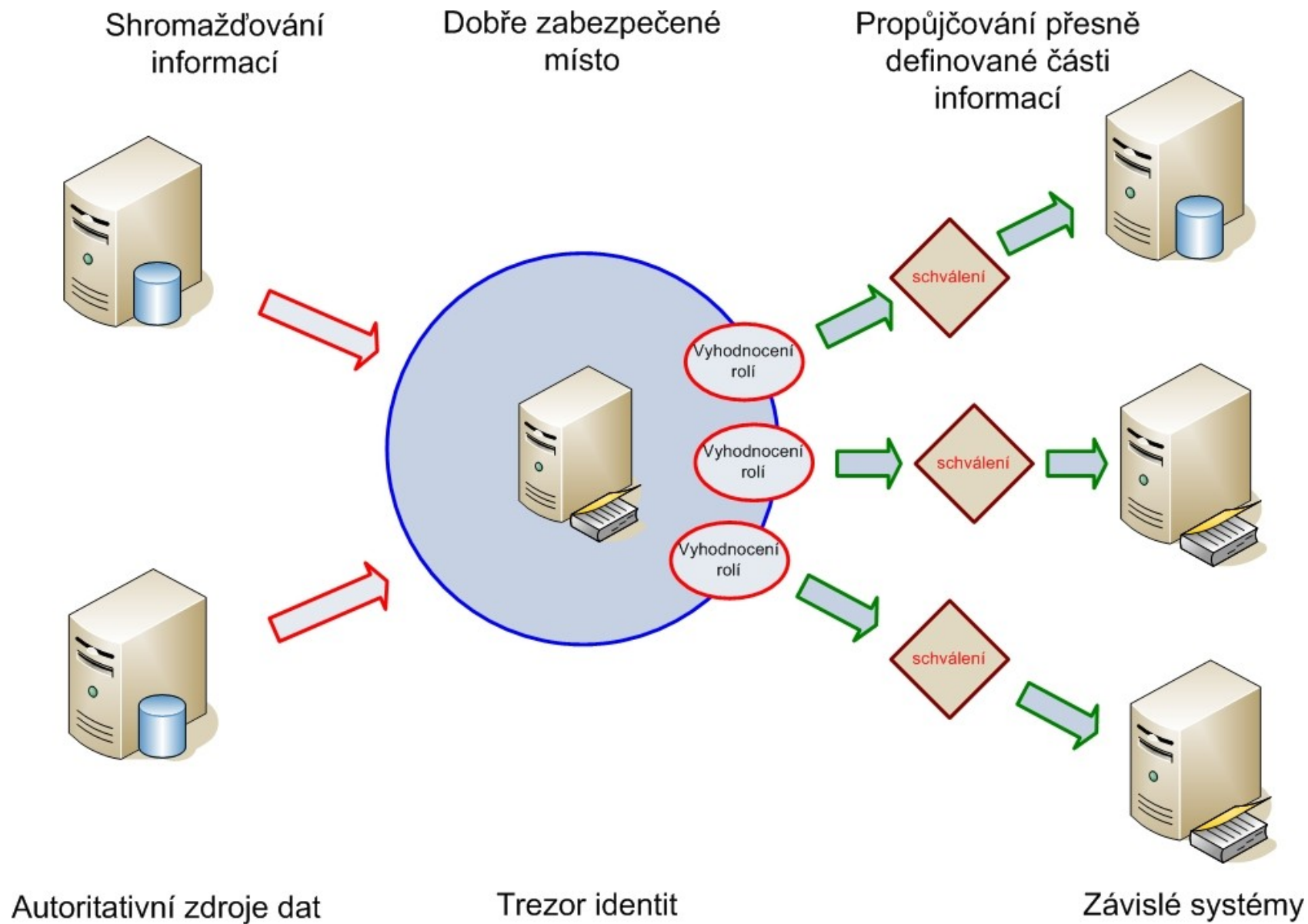
Autoritativní zdroje dat

Trezor identit

# Obečné schéma IDM



# Obečné schéma IDM

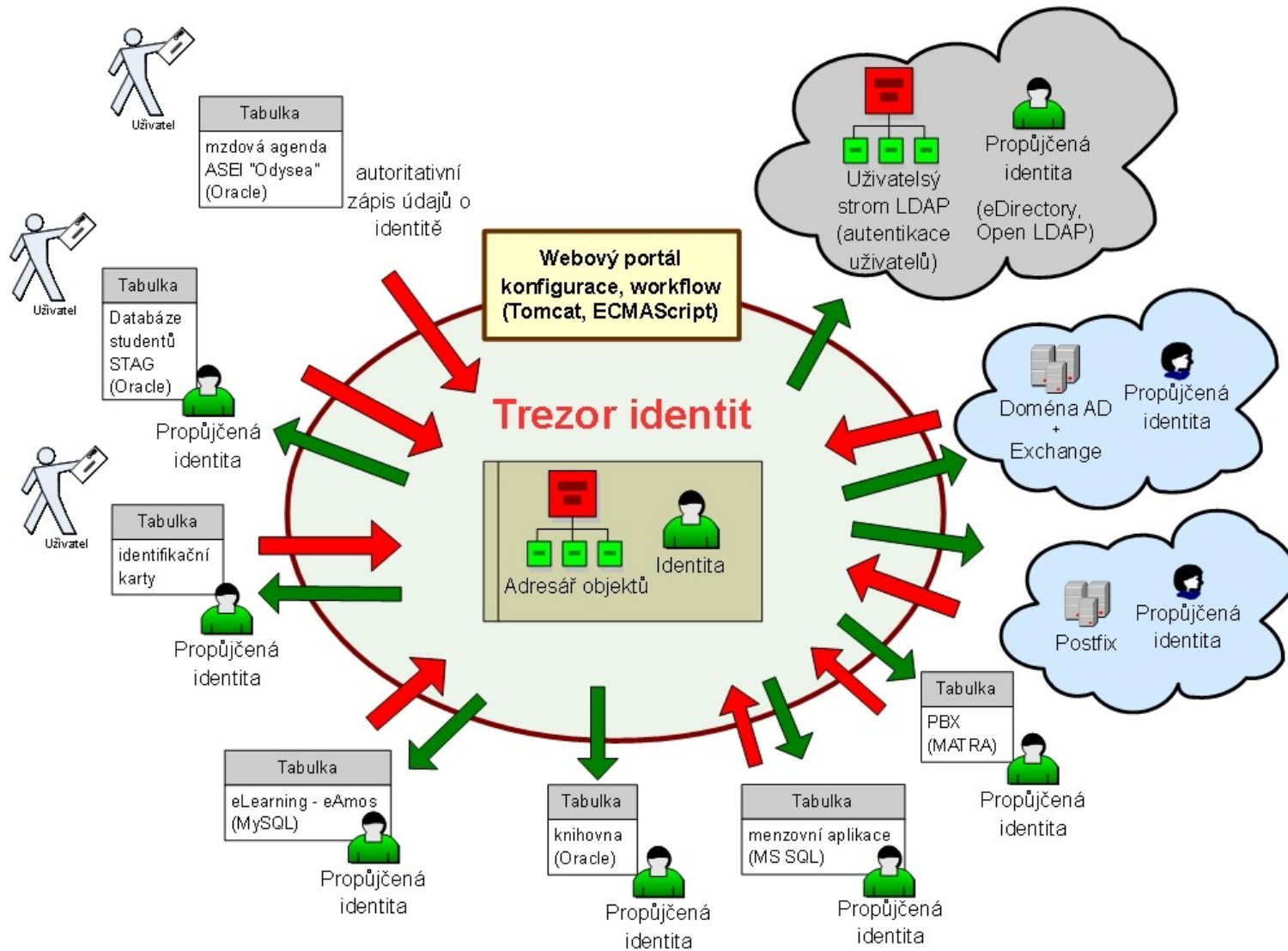


# Obečné schéma IDM

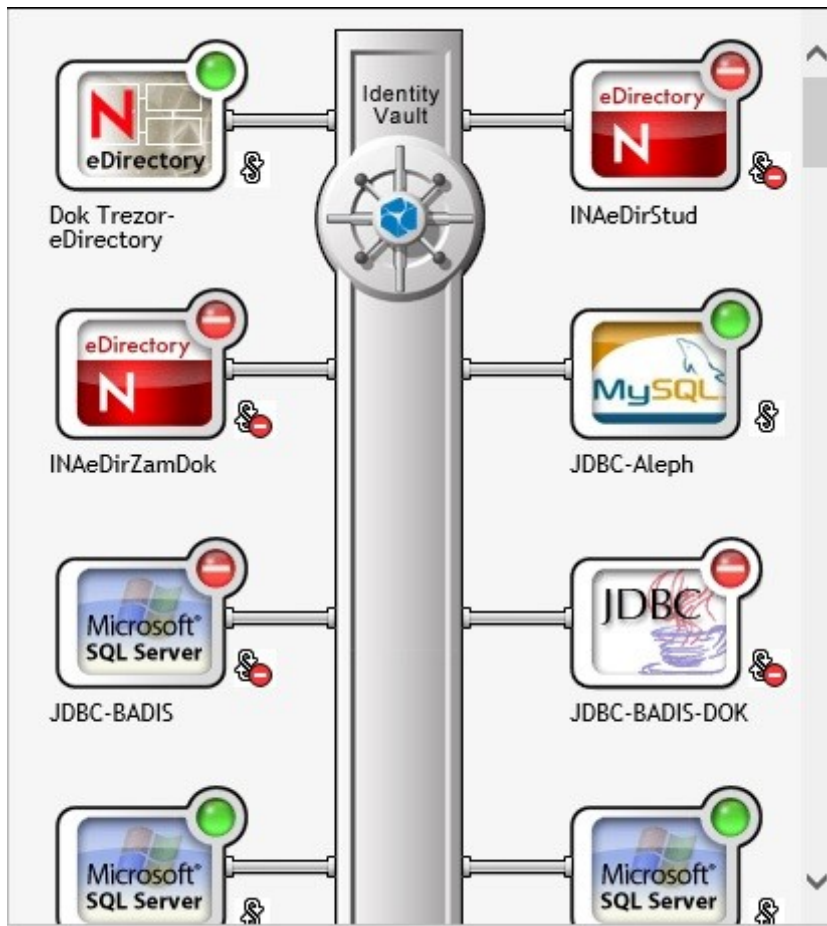
- **Dobře zabezpečené místo** – *trezor identit*  
(databáze, LDAP)
- **Shromažďování informací** – *autoritativní zdroj(e) informací*  
(personální systém)
- **Propůjčování přesně definované části informací** – *závislé systémy*  
(databáze, LDAP, API aplikace...)
- **Vyhodnocení rolí** – *pravidla zpracování požadavků*  
(skripty, utility)
- **Schválení (volitelné)** – *zásah obsluhy (administrátor, vedoucí)*  
(skripty, utility)



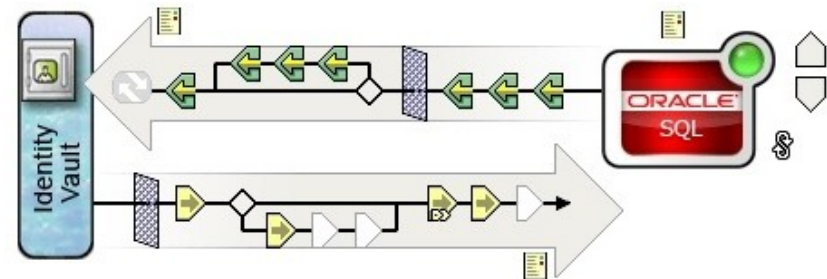
# Příklad realizace



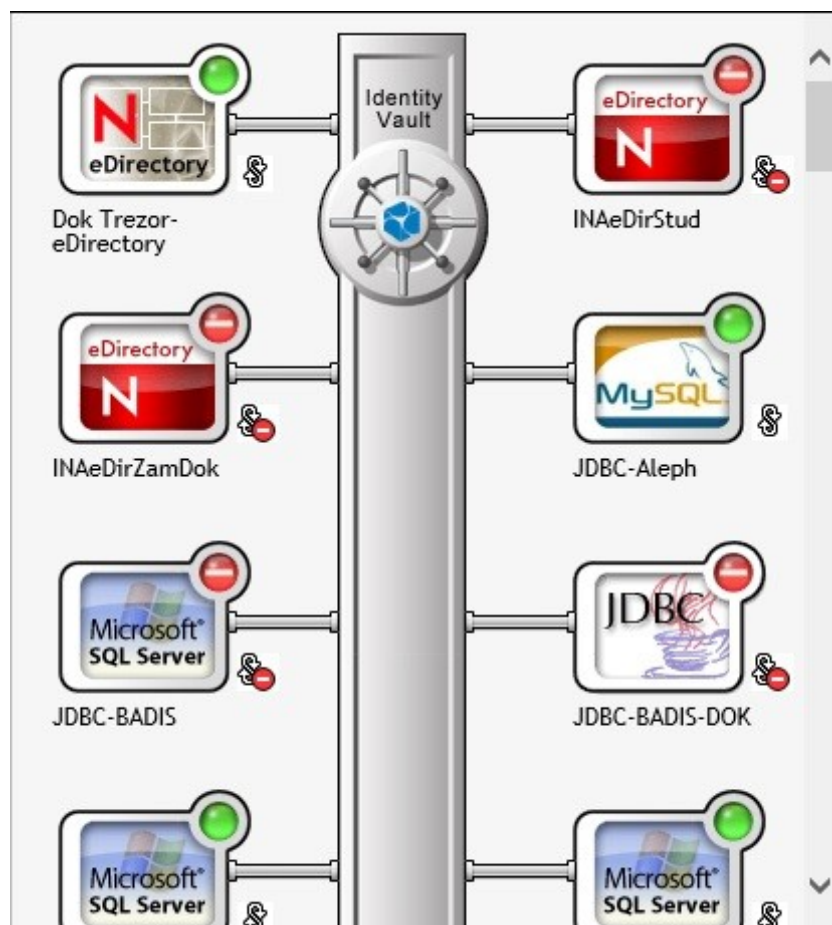
# Micro Focus implementace



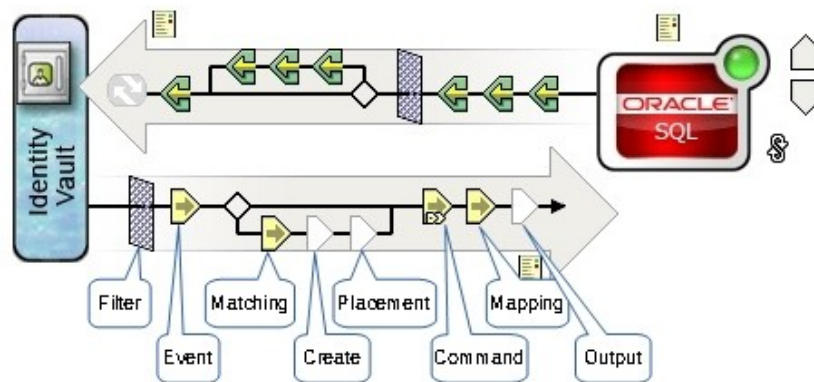
- *Původně Novell dirxml (synchronizace stromů NDS)*
- *Nyní systém s asi 40 konektory do nejrůznějších systémů a aplikací*
- *Obousměrná realtime synchronizace*
- *Webový portál pro spravování rolí a workflow*



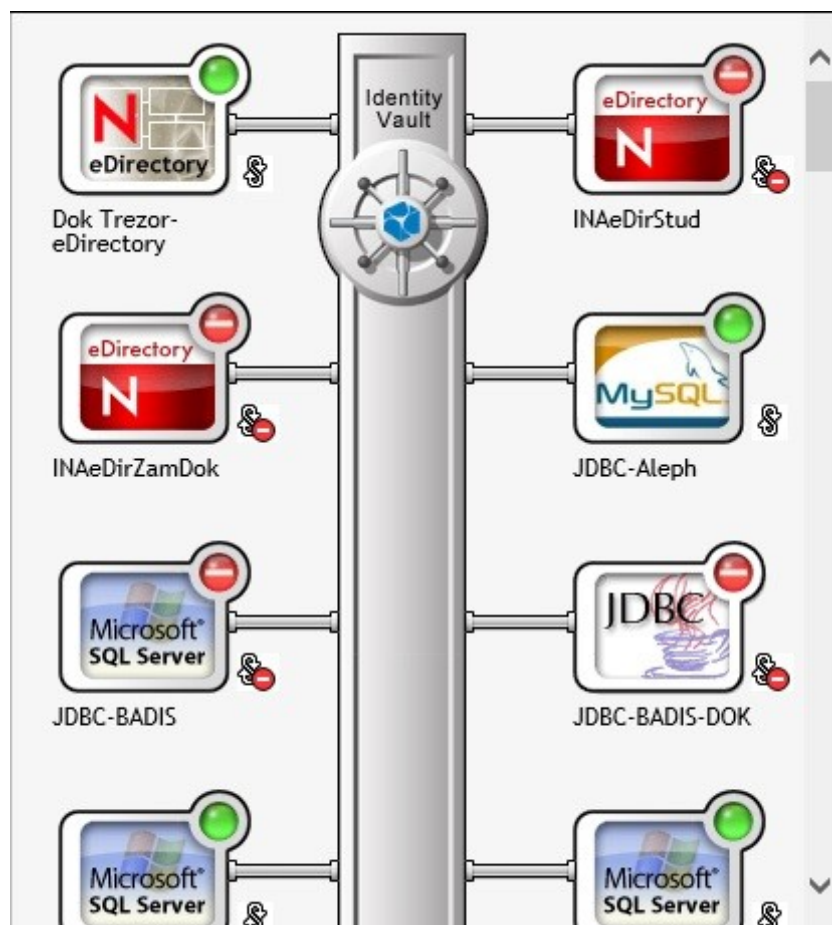
# Micro Focus implementace



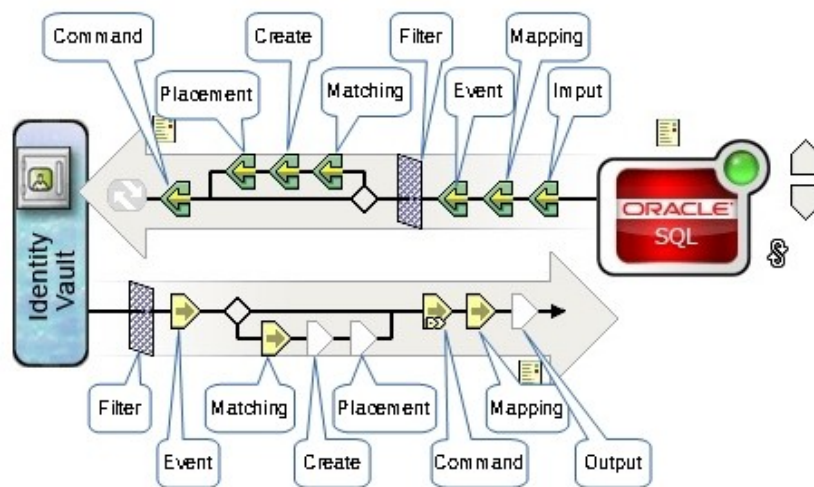
- *Původně Novell dirxml (synchronizace stromů NDS)*
- *Nyní systém s asi 40 konektory do nejrůznějších systému a aplikací*
- *Obousměrná realtime synchronizace*
- *Webový portál pro spravování rolí a workflow*



# Micro Focus implementace



- *Původně Novell dirxml (synchronizace stromů NDS)*
- *Nyní systém s asi 40 konektory do nejrůznějších systému a aplikací*
- *Obousměrná realtime synchronizace*
- *Webový portál pro spravování rolí a workflow*



# Trezor

The screenshot displays the web interface of the ČZU vault01 system. The browser window title is "ČZU vault01 - Internet Explorer" and the address bar shows "https://vault01.oikt.czu.cz:8443". The page header includes "ČZU vault01" and "ADMIN CZU-VAULT". The main content area is titled "IDENTITIES" and shows a list of 15969-16467 of 127296 identities. The left sidebar shows a tree view of the system structure, including "cz (1)", "czu (19)", "BASEUNITS (191)", "DOKTORAND (3864)", "IDENTITIES (127296)", "LNAMES-STU (62885)", "LNAMES-ZAM (14808)", "mgmt (46)", "OFFICEGROUPS (7)", "ORG\_GROUPS (2)", "PPV (57421)", "REFERENCE\_TABLES (12)", "RELATIONS (241798)", "ROOMS (8145)", "STUDIUM (180544)", "STUDIUM-EXAMS (236290)", "STUDIUM-SUBJECTS (7482)", "WORKORDEROFFICE (9275)", "Role Based Service 2 (106)", "Security (11)", and "Logging Services (4)".

Name
(current level)
Cmiral_Vladislav_164981
Cmiralova_Lenka_74917
Cmiralova_Petra_80032
Cmiralova_Rebeka_158823
Cmokova_Lucie_106557
Cmolik_Jan_74427
Cmolik_Petr_156600
Cmolikova_Cozlova_Klara_129843
Cmolikova_Lucie_144815
Cmuchalkova_Kamila_143212
Cmugr_Tomas_111435
Cmugrova_Renata_111434
Cmunt_Radek_136805
Cmuntova_Michaela_115024
Cmuntova_Vladimira_84157
Coat_Louis-Marie_169933
Cobanjan_Tigran_162630
Cobelens_Tara_141669
Cobena_Delgado_Yaira_Yisenia_61864
Cobr_Ondrej_147999
Cocek_Frantisek_50073
Cochin_Benjamin_92144
Cochova_Anna_107463

https://vault01.oikt.czu.cz:8443/nps/servlet/webacc?NPService=fw.LaunchService&NPAction=Delegate&delegate=fw.Tree...

# Trezor

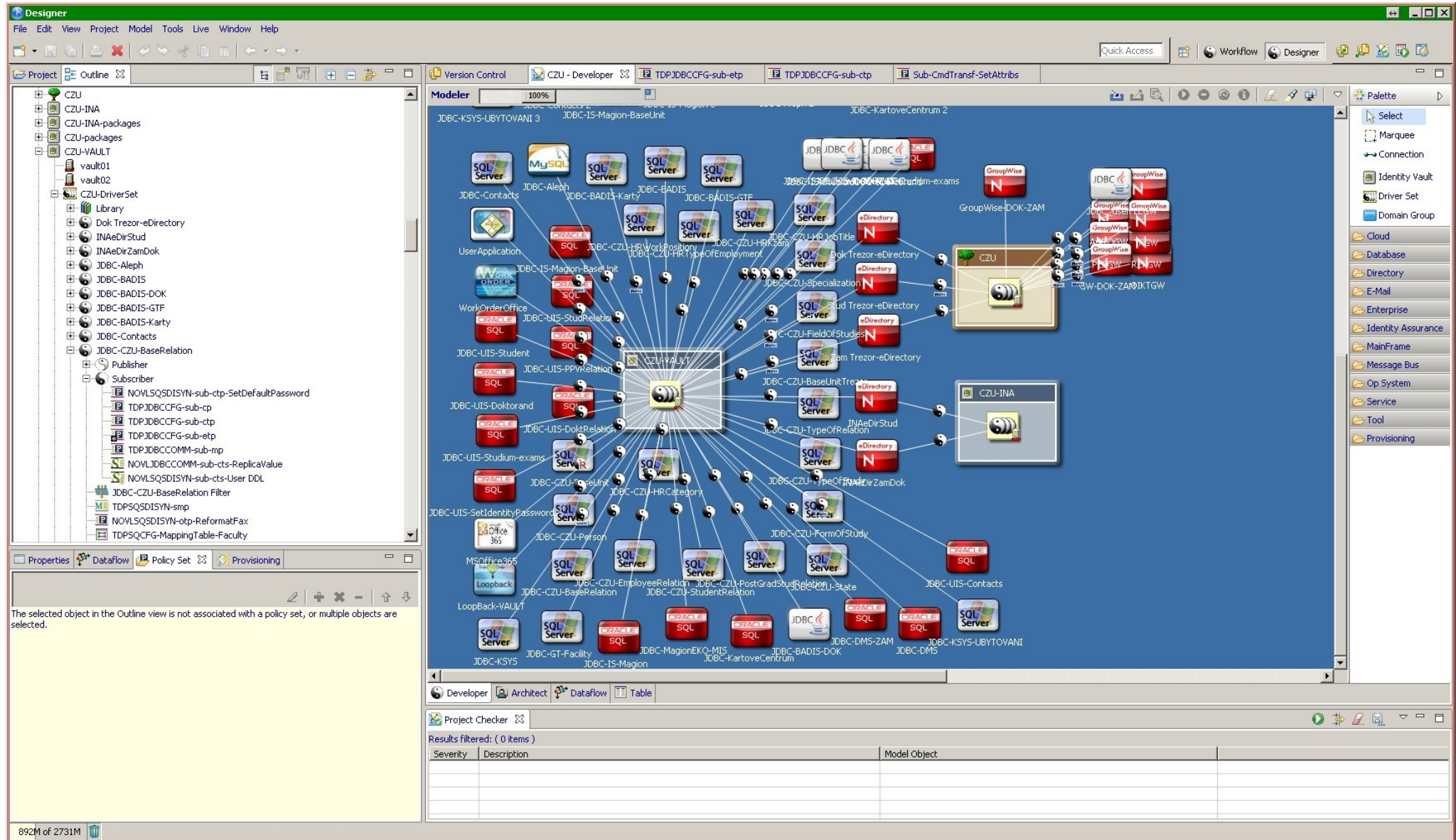
The screenshot displays the web interface of the ČZU vault01 system. The browser address bar shows the URL <https://vault01.oikt.czu.cz:8443>. The page title is "ČZU vault01" and the user is logged in as "ADMIN CZU-VAULT".

The interface is divided into two main sections:

- Tree View (Left):** A hierarchical tree structure showing organizational units. The "IDENTITIES (127296)" node is highlighted with a red box. Other highlighted nodes include "RELATIONS (241798)", "STUDIUM (180544)", and "STUDIUM-EXAMS (236290)".
- IDENTITIES List (Right):** A table displaying a list of identities. The table has a header "Name" and a search bar. The list contains 19 entries, each with a checkbox and a name followed by an ID number. The first entry is "(current level)".

The URL at the bottom of the browser window is <https://vault01.oikt.czu.cz:8443/nps/servlet/webacc?NPService=fw.LaunchService&NPAction=Delegate&delegate=fw.Tree...>

# Konfigurace - struktura



# Konfigurace - politiky

The screenshot displays the IBM Policy Designer interface. The main window shows the configuration for a policy named "Sub-CmdTransf-SetAttribs.Subscriber.JDBC-Aleph.CZU-DriverSet.CZU-VAULT-packages".

**Policy Description:** Sub-CmdTransf-SetAttribs.Subscriber.JDBC-Aleph.CZU-DriverSet.CZU-VAULT-packages

**Rules:**

- USER: Set Degree prefix
- USER: Set Telephone
- USER: Set Fullname
- USER: Set WorkforceID
- USER: Trim infoStudent
- USER: Trim infoDoktorand
- USER: Trim infoPPV
- USER: Trim ChipCard
- USER: Trim S
- USER: Trim Email

Nastavi atributy uzivatele.

**Conditions:**

- Condition Group 1
  - if class name equal "User"
  - if operation attribute 'Internet EMail Address' available
  - if attribute 'Internet EMail Address' available

**Actions:**

- set local variable("email", scope="policy", Attribute("Internet EMail Address"))
- strip operation attribute("Internet EMail Address")
- set destination attribute value("Internet EMail Address", Substring(length="60", Local Variable("email")))

**USER: Reset Login Name**

**Project Checker:** Results filtered: ( 0 items )

Severity	Description	Model Object

931M of 2731M



# Konfigurace - workflow

The screenshot displays the 'Designer' application window, which is used for configuring workflows. The main workspace shows a flowchart for the 'eDirectory Account Create' workflow. The flow starts with a 'Mapping 1' activity, followed by a 'Condition' node. If the condition is true, it proceeds to 'Mapping 2' and then to another 'eDirectory Account Create' activity. If the condition is false, it goes to 'Log for Manager Denied Activity'. From the 'eDirectory Account Create' activity, there are two paths: 'approved' leading to 'Log for Manager Approval Activity' and 'denied' leading to 'Log finish denied'. The 'Log finish denied' activity leads to 'Workflow Status Denied', which then leads to 'Manager is defined'. The 'approved' path from the second 'eDirectory Account Create' activity leads to 'Entity', then 'Log for approval activity', 'Resource Request', 'Workflow Status Approved', and finally 'Create GW Account'. The 'denied' path from the second 'eDirectory Account Create' activity leads to 'Log finish denied'.

The left-hand pane shows a tree view of provisioning request definitions, including various account creation and management tasks. The right-hand pane shows the properties of the selected activity, with a table of properties and values.

Property	Value
Name	eDirectory Account Create
Addressee	GCV.get(ua.edirectory.admins.r
Reminder Start	
Reminder Interval	
Escalation Addressee	
Escalation Count	0
Escalation Interval	172800000
Escalation Reminder S	
Escalation Reminder I	
Final Timeout Action	denied
Timeout	30
Timeout Units	Days
Form	approval_form
Exclude Requestor	false
Approver Type	Group
Notify by E-Mail	true
Digital Signature Type	not required
Priority	8

At the bottom of the window, there is a 'Data Item Mapping' table with columns for 'Source Expression', 'Target Form Field', and 'Data Type'. The 'Source Expression' column contains the expression 'Requestor.get(ua.edirectory.admins.r'.

# Co pro Vás uděláme

- **Připravíme pro Vás návrh řešení**
- **Vybereme odpovídající a vhodné produkty pro řešení IdM**
- **Profi produkt s ALA licencováním může vyjít tak dobře, že se vyplatí více, než investovat do nekonečna do práce**
- **Vybereme vhodný model licencování**
- **Zajistíme pro Vás speciální ceny**
- **Provedeme kompletní realizaci IdM**