

IdM: Identity Management

6. 4. 2017
Josef Vybíhal



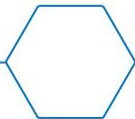
- Identita: jedna osoba, více účtů

- systém pro automatizaci běžných administračních úkonů
 - vytváření/mazání/přesuny uživatelů
 - nastavení/resety hesel
 - přidělování práv/rolí/přístupu k systémům
 - reakce na změny (např. organizační zařazení, příjmení, heslo, ...)
 - sledování identity (uživatel *abc123* v HR je *Franta Vopršálek* v AD)



IdM: K čemu je to dobré?

- zajištění čistoty dat ve zdrojových i cílových systémech
- zajištění integrity dat (data jsou ve všech systémech správná)
- IT má více času na produktivní práci:
 - nemusí řešit:
 - ruční změny v systémech
 - zakládání účtů
 - rušení účtů
 - přiřazování práv
 - a další operativní věci
- automatický přesun uživatelů/identit a jejich atributů mezi systémy
- vynucení podnikových pravidel (např. hesla)



> NetIQ Identity Manager 4.6 (původně DirXML od Novell)

- > Dlouho vyvíjený stabilní a robustní produkt
- > Novell/NetIQ/Micro Focus dlouhodobě nasazuje IdM celosvětově (nejen) pro vládní úřady a instituce (vysoké požadavky na zabezpečení):
 - > **Suite B** is a set of cryptographic algorithms standardized
 - > by the National Security Agency (NSA) to allow commercial products
 - > to protect traffic that is classified at secret or top secret levels.

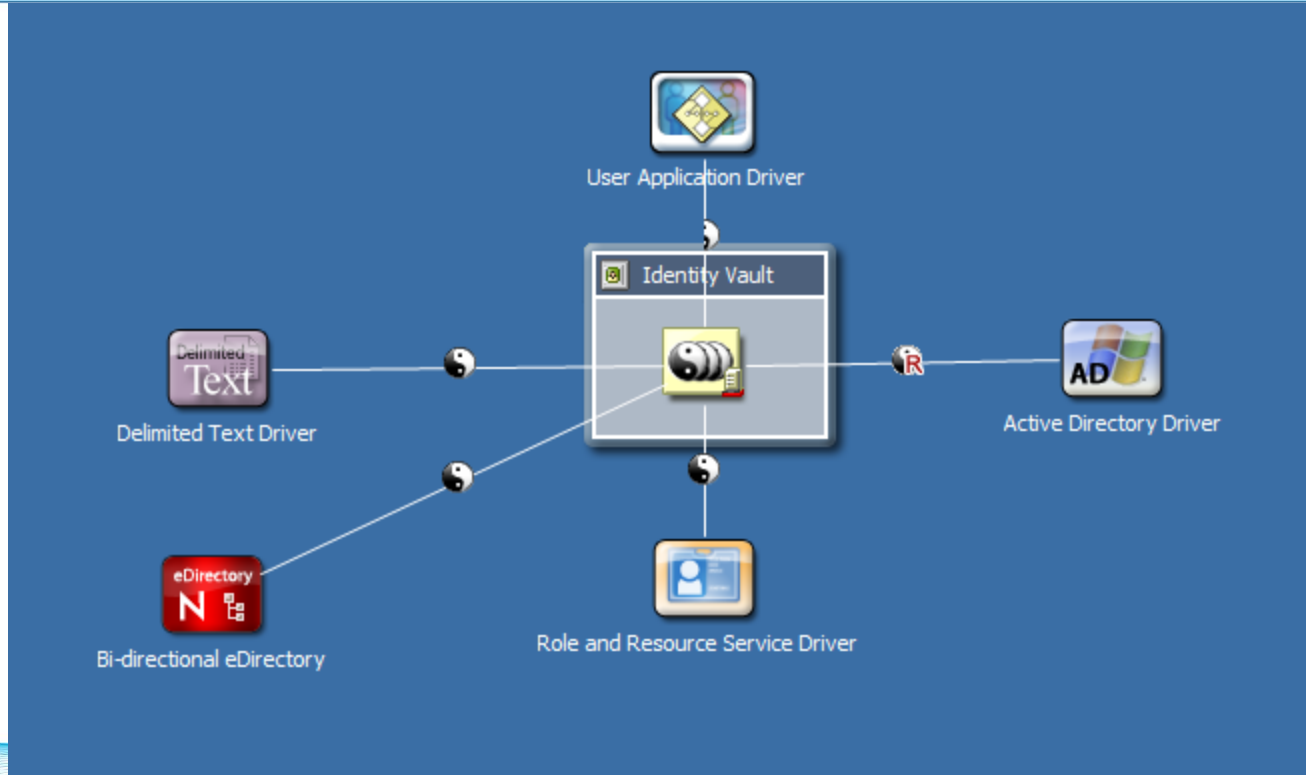
> Proč NetIQ Idm?

- > Akvizicemi společnosti Novell rozšířen o mnoho funkcionalitu
 - > Packaging Framework, security, SSO, Drivers, SSPR, EAS
- > Nadstandartní možnosti konfigurace politik (DirXML, XSLT, Xpath, ECMAScript)
- > Event oriented: každou událost lze odchytil a ihned na ni reagovat
- > Designer pro modelování celého systému (offline)
- > Velmi kvalitní dokumentace

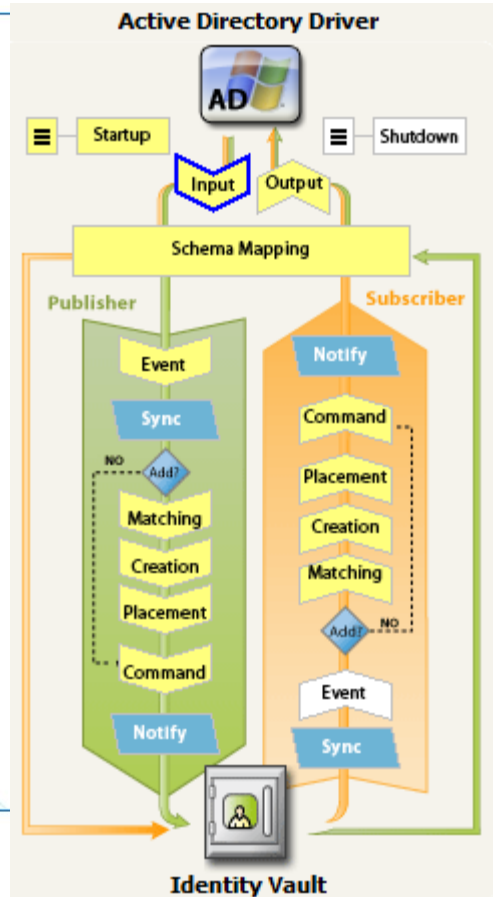
IdM: Jak to funguje (1)



IdM: Jak to funguje (2)



IdM: Jak to funguje (3)



 SUSQL-pub-ctp-UpdateFullName.Publisher.MSSQL.Driver Set.Identity Vault

Policy Description

Rules

Update Full Name

No description available.

Conditions

Condition Group 1

  if class name equal "User"

And

Condition Group 2

  if operation attribute 'Given Name' changing

Or

  if operation attribute 'Surname' changing

Or

  if destination attribute 'Full Name' not available

Actions

  set local variable("fullNameAccent", scope="policy", Source Attribute("Given Name", class name="User")+" "+Source Attribute("Surname", class name="User"))

  set destination attribute value("Full Name", class name="User", Local Variable("fullNameAccent"))

  set local variable("fullNameNoAccent", scope="policy", XPath("es:unaccentText(\$fullNameAccent)"))

  set destination attribute value("displayName", class name="User", Local Variable("fullNameNoAccent"))

IdM: Na čem to běží

- > Virtualizace: VMware, RHEV (KVM), Hyper-V, Xen
- > OS: linux (SLES, OES, RHEL), Windows Server
- > Použité technologie: X.500 (eDirectory), PostgreSQL, Java, Tomcat, XML, DirXML, XSLT, XPath, ECMAScript, CSV, Eclipse, a další



- > přiřazování rolí a zdrojů na základě nároků
 - > (roles, resources, entitlements)
- > skriptovací drivery
 - > Další rozšíření funkcionality. Na cílovém systému mohou spouštět libovolně složité skripty na základě nějaké události.
- > extrémně vysoká konfigurovatelnost
 - > s nadsázkou lze říct, že jde „cokoli“, jen je to vždy otázkou konfigurace politik a driverů
- > Inteligentní řízení událostí: např. „synthetic adds“
- > modelovací nástroj Designer
- > Workflows (schvalování žádostí)
- > Auditování - přehled o pohybech v systémech, kontrola (ne)přidělených oprávnění, reporty

> Děkuji za pozornost.

> jvybihal@uniscomp.cz

UNIS COMPUTERS, a.s.

Jundrovská 31, 624 00 Brno

tel.: +420 544 528 301

fax: +420 541 223 134

obchod@uniscomp.cz

Pobočka Praha

Zelený pruh 95/97, 140 00 Praha 4

tel.: +420 227 230 080

■ www.uniscomp.cz