Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Diplomová práce

Softwarové nástroje pro Identity management

Vypracoval: Bc. Milan Hořejš
Vedoucí bakalářské práce: doc. Ing. Vojtěch Merunka, Ph.D.

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Softwarové nástroje pro identity management" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne _____

Poděkování

Děkuji vedoucímu diplomové práce doc. Ing. Vojtěchu Merunkovi, Ph.D. za cenné rady, připomínky a metodické vedení práce.

Softwarové nástroje pro Identity management

Software tools for Identity management

Souhrn

Tato práce přináší sjednocený pohled na téma identity managementu a vybraných softwarových nástrojů pro jeho správu. V teoretické části jsou vysvětleny základní pojmy pro pochopení správy identit. Na uvedené pojmy navazují typické otázky (Proč se zajímat právě o tuto oblast? Co získáme studiem této oblasti? Jak konkrétně může pomoci správa identit právě mě nebo mojí společnosti? Jaké jsou výzvy, slabiny, rizika v oblasti řízení přístupu?). Základní pojmy jsou velmi důležité, jelikož na nich bude stavěno po zbytek celé diplomové práce. Další kapitolou je funkce identity managementu. Zde je vysvětlena základní funkce a cíle, kterých organizace dosáhne po úspěšné implementaci. Poté je vysvětlen pohled uživatele a bezpečnostního správce. Na tuto část navazují softwarové nástroje, jednak pro komerční sféru a nekomerční sféru.

V praktické části jsou demonstrovány teoretické poznatky na vybrané aplikaci (konkrétně ITIM - IBM Tivoli Identity Manager). Zvolená aplikace je detailněji popsána (procesní a technologická část). Dále je vysvětlena práce s touto aplikací a to z hlediska uživatele. Kde testuji nejvíce používané funkce v praxi, tzv. Self reset password. Zároveň s tímto testováním vznikla i příručka, tak, aby byl kdokoli schopen zvládnout práci v systému. Z pohledu administrátora jsou vysvětleny jednotlivé funkce systému. Ty jsou demonstrovány v příručce, která vznikla na základě smyšleného příkladu a popisuje řešení jednotlivých kroků. V praktické části jsou dále představeny úspěšně nasazené projekty.

Klíčová slova

identita, oprávnění, krádež identity, politika, role, proces, workflow, ITIM, RBAC

Summary

This work provides a unified document of identity management, and selected software tools for his management. In theoretical part explains the basic concepts for the understanding of identity management. On those terms follow the typical questions (Why just interested in this area? What we will get when we will study this area? Specifically, how identity management can help just me or my company? What are the challenges, weaknesses, risk in identity management?). The basic concepts are very important as they will be built for the rest of the graduation theses. Another chapter is a function of identity management. There is a basic functions and objectives that the organization will achieve successful implementation. After that is explain view of user and security admin. This part is followed by software tools, both commercial and noncommercial sector sphere.

In practical part of the theoretical findings are demonstrated in selected application (specifically ITIM - IBM Tivoli Identity Manager). Selected applications are described in more detail (process and technology section). It´s explained the work with this application from view of user. Where was the test most frequently used functions in practice, called Self-reset password. Along with this testing was produce guide, so that anyone can handle the work in the system. From view of administrator are explain the different functions of the system. They are demonstrated on a fictional example, where was produce next guide, which describes the individual steps. The practical part also presents successful deployment projects.

Keywords

identity, entitlement, identity thief, policy, roles, process, workflow, ITIM, RBAC

Obsah

Seznam obrázků

Seznam tabulek

1. Úvod

S rozvojem nových počítačových aplikací, které každý den „zaplavují“ uživatele, roste snaha o zjednodušení a zdokonalení firemních procesů. Největší snaha vychází z ekonomického předpokladu, tzv. maximalizace zisku. Cesta k dosažení maximálního zisku se skrývá v minimalizaci nákladů, dokonalých procesech a efektivním využívání času.

Benjamin Franklin měl naprostou pravdu, když tvrdil, že „Čas jsou peníze“. Z hlediska využívání počítačových aplikací to platí dvojnásobně. Snaha o dokonalé procesy, automatizace běžných rutinních prací, zefektivnění a všeobecný tlak na rychlost a přesnost, vedou k neustálému vymýšlení nových a nových konceptů. Současný svět prochází neustálým vývojem. Změny, které přináší nutnost být konkurenceschopný, jsou stále rychlejší. Pouze ta společnost, která je dokáže včas akceptovat, může být úspěšná.

Každá firma využívá identity management, ale na různých úrovních. Je nutné chránit svá data a zamezit přístupu těm, kteří nemají právo na tyto informace. S rostoucím počtem aplikací, roste počet uživatelů, stoupá počet přístupů a hesel. Uhlídat v tomto případě bezpečnost dat a zmapovat, kdo kam má přístup je velmi těžké. Je tedy vytvářen tlak pro vznik centralizované správy. V České republice vydala Česká národní banka opatření č. 2 ze dne 3. února 2004 k vnitřnímu řídícímu a kontrolnímu systému banky. Kde jedním z bodů bylo, že banka má zabezpečit jednoznačnou identifikaci a autentizaci uživatele, která musí předcházet aktivitám uživatelů v informačních systémech. Softwarové nástroje pro správu identity managementu toto samozřejmě řeší a banky tedy využívají tyto nástroje.

Softwarových nástrojů pro správu identity managementu je velmi mnoho. Na trhu spolu soupeří velké společnosti, jakými jsou IBM, Microsoft, Novell, Oracle, a každá z nich má své vlastní nástroje pro správu. Na trhu jsou i malé společnosti, které se zaměřují na tzv. „open source“ aplikace. V této práci představím postupně všechny a detailněji se zaměřím na produkt od IBM. Jedná se o ITIM (IBM Tivoli Identity Manager).

2. Cíl práce a metodika

2.1 Cíl práce

Cílem práce je popsat identity management a softwarové nástroje pro jeho správu. K pochopení této problematiky je nutné vysvětlit základní pojmy, které nám otevřou dveře do světa funkce identity managementu. Vysvětlit, proč je vlastně poslední dobou tolik skloňovaný v různých velkých korporátních společnostech. Proč jsou firmy „nucené“ přemýšlet o jeho zavádění. Jaké jim to přináší konkrétní výhody z ekonomického, informačního a zejména z procesního hlediska.

V praktické části budou demonstrovány teoretické poznatky na vybrané aplikaci (konkrétně ITIM - IBM Tivoli Identity Manager). Zvolená aplikace bude detailněji popsána (procesní a technologická část). Poté bude vysvětlena práce s touto aplikací a to z hlediska uživatele. Dalším cílem je otestování nejvíce používané funkce v praxi, tzv. Self reset password. Zároveň s tímto testováním bude vytvořena i příručka, tak, aby byl kdokoli schopen zvládnout práci v systému. Z pohledu administrátora budou vysvětleny jednotlivé funkce systému. Ty budou demonstrovány na smyšleném příkladu, kde bude vytvořena další příručka, která bude popisovat řešení jednotlivých kroků. V praktické části budou dále představeny úspěšné projekty, které jsou již v praxi nasazené.

2.2 Metodika

Data z níže uvedených zdrojů byla zpracována a na základě nich byla napsána tato diplomová práce. Je nutné si uvědomit, že trendy v tomto oboru jdou velmi rychle dopředu. Při psaní práce bylo využito zejména online zdrojů a praktických zkušeností, které byly získané na pozici systémový inženýr ve firmě Trask s.r.o.

V praktické části byly použity uvedené programy, a to konkrétně IBM Tivoli Identity Manager 4.6, IBM DB2, aplikační server IBM Websphere, databázový server LDAP a virtuální konzole VMware Sphere. Všechny tyto programové prostředky jsou nutné pro zprovoznění administrační konzole ITIM. Obrázky, které nepochází z aplikace ITIM nebo jiných uvedených zdrojů, byly vytvořeny pomocí Microsoft Office Visio 2007.

Závěry a zhodnocení byly provedeny na základě analýzy dle daných objektivních kritérií a dle vlastních zkušeností, které byly načerpány při aktivní činnosti v tomto oboru.

Část I.

Literární rešerše

3. Co je to Identity management?

Předtím než začneme psát o řízení a užívání identity v počítačových systémech, je třeba vysvětlit, co je to identita a jak je používaná. K ní se vážou další termíny, jakými jsou digitální identita, provisioning, de-provisioning, správa životního cyklu identit, synchronizace identit, security principal. Je nutné pochopit i vnímaní role, přístupových práv, procesů. A celou řadu základních pojmů uvedených v této kapitole.

3.1 Identita (Identity)

Pro pochopení identity si vezmeme např. typického českého občana, který je starší patnácti let. Ze zákona je povinen při sobě nosit identifikační kartu. V tomto případě se jedná o občanský průkaz. Jeho identita je z hlediska tohoto průkazu tvořena jedinečným rodným číslem, fotografií, podpisem a číslem průkazu. K této identitě se váží další náležitosti, zejména sociální a zdravotní pojištění, vzdělávání, odvod daní, volební právo, trestní rejstřík aj. Jedná se tedy o papírovou správu identit, která se u nás využívá od první republiky. Samotná identita je tedy velmi důležitá, ale zároveň je nezbytné zachovat její jedinečnost.

Abych tedy já jako student mohl využívat zvýhodněné služby (levnější jízdné, různé promo akce, karta ISIC, slevy na spotřební zboží, levnější kulturní akce, volné vstupy aj.), musím se prokázat. Jako nositel identity požaduji, aby mi na základě jejího ověření byly poskytnuty tyto služby, nebo jiné. Z hlediska poskytovatele služeb je nutná zpětná kontrola. Důvod je jednoznačný, poskytovatel nechce, aby někdo nečerpal na jeho úkor služby, které musí být následně uhrazeny. Proto poskytuje některé své služby pouze nositelům identity, kteří jsou s ním v nějakém právním svazku.

Pro potřeby počítačové problematiky identity nás bude zajímat tato definice, kdy je nutné si uvědomit, že: Identita, respektive identita uživatele, je jednoznačná identifikace, v podstatě jde o spárování fyzické osoby s virtuálním prostředím v počítačích.

3.2 Digitální identita (Digital identity)

Obohatíme-li pojem identita o slovo digitální, dostaneme pojem: Digitální identita (Digital identity), ta obsahuje samotnou identitu, která zahrnuje popis uživatele a jeho přístupová práva.

3.3 Poskytování (Provisioning)

Jedná se o proces, kdy dochází k tvorbě identity. Součástí procesu je i definování jejich přístupových práv a následné zahrnutí do úložiště identit.

3.4 Odejmutí (De-provisioning)

Jedná se o proces, kdy dochází k odstraňování identity z jejího úložiště. Smazáním identity dochází k ukončení všech přístupových práv, které identita měla k dispozici.

3.5 Správa životního cyklu identit (Identity lifecycle management)

Základní proces identity managementu je životní cyklus identity uživatele. Jak píše Martin Lízner ve svém článku, „tak tento cyklus zpravidla začíná nástupem zaměstnance do organizace, kdy jsou uživateli zřízeny základní přístupy, například na koncovou stanici, do firemní pošty a intranetu. V průběhu času uživatel získává další nové účty a oprávnění, nebo o oprávnění naopak přichází. Pokud dojde k přerušení pracovního poměru, jsou obvykle účty zaměstnance zneplatněny tak, aby se na ně nemohl přihlásit, přičemž účty fakticky dál existují. Při obnovení pracovního poměru je možné účty jednoduše znovu aktivovat a pokračovat v práci. Při definitivním odchodu zaměstnance jsou účty vymazány. Organizace také poměrně často zažívají změnu uživatelského jména uživatele (uživatelky) či změnu organizačního zařazení pracovníka a s ní související změny v oprávněních.“ [LÍZNER, 2010]

V citaci byl popsán typický proces nástupu pracovníka, kdy s nástupem do zaměstnání obdrží základní přístupy. Ty se s průběhem času mohou měnit. Identity lifecycle management se tedy váže k celé množině procesů a technologií, které udržují a aktualizují digitální identitu. Zahrnuje synchronizaci identit, provisioning, de-provisioning a průběžnou správu uživatelských atributů, ověřovacích údajů a oprávnění.

3.6 Synchronizace identit (Identity synchronization)

Tento proces slouží pro zajištění, aby různá úložiště identit obsahovala konzistentní data pro jednotlivé identity. Jde o to, aby se synchronizovaly identity a hesla napříč různými systémy. Cílem je poskytnout uživateli jedinou sadu pověření pro autentizaci od aplikací, databází a adresářových služeb.

3.7 Bezpečnostní princip (Security principal)

Digitální identita s jedním či více ověřovacími údaji, kterou lze autentizovat a autorizovat pro interakci se sítí.

3.8 Role (Roles)

Role, respektive uživatelská role, nám říká, jaká je naše role v daném prostředí. Nejlépe se dá pochopit význam na v informačním prostředí naší školy, České Zemědělské Univerzity. Momentálně mám roli, student. Abych mohl dosáhnout této role, musel jsem úspěšně projít přijímacím řízením a poté se zapsat do studia na mnou vybraný obor. V rámci svého studia však mohu spolupracovat se školou a stát se zaměstnancem. V informačním prostředí bych tedy získal dvě role. Vztah uživatele a role je 1:N, jeden uživatel tedy může mít víc rolí.

3.9 Oprávnění (Entitlement)

Oprávnění je přímo spjaté s danou rolí. Jak jsem již uvedl, tak moje role je student. Je patrné, že mám určitý druh povinností, které musím plnit, aby mi tato role zůstala zachována. Je tedy pro mě nezbytné docházet do školy a plnit studijní povinnosti. Ale je nutné si uvědomit, že jako student nemám přístup všude. Např. V rámci magisterského studia máme povinnost napsat diplomovou práci, kterou si vybíráme pomocí internetové aplikace BADIS (http://badis.czu.cz). Zde je uveden seznam témat pro jednotlivé katedry a poté dle vyučujících/vedoucích diplomové práce. Vzhledem k tomu, že moje role v daném prostředí je student, tak mé oprávnění je pouze prohlížet témata a poté se zapsat. Jak je již patrné, tak vyučují má oprávnění vypisovat témata, výběrová řízení, schvalování osnov a celkové práce. Takto bychom mohli pokračovat dalšími rolemi (studijní referentka, sekretářka,

administrátor aj.). Je tedy zřejmé, že každá role má jiný (někdy podobný, stejný) druh oprávnění. Záměrně jsem zvolil počítačovou aplikaci Badis, jelikož mi přijde na pochopení nejlepší. Rolí a přístupových oprávnění není tolik.

Ve velkých institucích/korporátních společnostech se však nepoužívá pár počítačových aplikací jako v rámci naší univerzity. Princip však zůstává stejný jako u aplikace Badis. Avšak počet rolí a přístupových oprávnění bude velmi mnoho.

Oprávnění (přístupová práva), pod tímto pojmem rozumíme možnost přístupu na daný systém, s tím, že oprávnění nám říká, co jsem schopen všechno dělat v daném prostředí.

3.10 Proces (Process)

Pod obecným významem pojmu proces (průběh, vývoj, děj) rozumíme posloupnost stavů nějakého systému.

Pro potřeby této diplomové práce si vysvětlíme proces na příkladu: Každá firma, instituce, obchod, škola aj. má definované své procesy. Z hlediska škol, institucí jsou procesy veřejně přístupné. Příkladem může být žádost o nový občanský průkaz. Důvodu je více, ale pro názornost si vyberu vypršení platnosti. Jakmile platnost skončí, průkaz se stává neplatný a nositel je povinen ho vyměnit na příslušném úřadě. Pro vydání nového, musí splnit předepsané náležitosti (řádně vyplnit žádost, mít novou fotografii o rozměrech 35mm x 45mm, která odpovídá jeho současné podobě, neplatný občanský průkaz a rodný list), poté může dojít k žádosti na příslušném úřadu. Zde zažádá o nový občanský průkaz. Pokud budou všechny náležitosti v pořádku, tak za 3-4 týdny obdrží nový. Je zřejmé, že toto je „ideální“ stav. Velmi často se stane, že je špatně vyplněná žádost, chybí rodný list, fotografie neodpovídá. Na prostředí firmy si proces vysvětlíme tak, že si představíme přijetí nového zaměstnance. Firma se rozhodne, že potřebuje nového administrátora pro platformu Windows 7. Vypíše tedy výběrové řízení, kde uvede požadavky na kandidáta. Kandidáti odešlou své životopisy a firma (pověřená osoba) si pozve vybrané na osobní pohovor. Na základě zkušeností, potřeb a předpokladů pro danou pozici, vybere toho pravého. Tomu nabídne odpovídající podmínky (mzdu, benefity, pracovní dobu, termín nástupu aj.) a pokud je spokojenost na obou

stranách, tak se podepíše smlouva. Opět mohou nastat různé komplikace jako v předchozím příkladu, nikdo nemusí mít o danou pozici zájem, malé zkušenosti, neodpovídající finanční ohodnocení, neznalost produktu aj.

Záměrně jsem zvolil tyto jednoduché příklady pro pochopení procesu, je totiž nezbytné začít přemýšlet o tom, jak funguje a mění se v jednotlivých krocích. Každá organizace má nastavené jiné procesy. Měla by to být jedna z klíčových věcí, proč je daná organizace úspěšná/neúspěšná. Správně nastavené procesy jsou klíčem k zisku a umožňují efektivní a pohotové plnění požadavků ať už ze strany zákazníků nebo interních zaměstnanců. Příkladem může být třeba internetový obchod a jeho procesy mohou být (způsoby a doba placení, způsoby a doba dopravy, možnosti odběru, vyřizování zakázky, kontrola plateb, komunikace se zákazníkem, objednávka nad 100000 Kč musí být schválená, možnosti placení záloh…).

Pro každý krok (ať už vytvoření uživatelské identity, získání nových přístupových práv, změna pracovního zařazení zaměstnance, povýšení, výpověď…) by měl být nastaven, co nejlepší, nejjednodušší a nejefektivnější proces.

3.11 Správa přístupu (Access management)

V praxi se téměř nestává, že se nasadí samostatně koncept identity managementu, aniž by nebyl podporován access managementem. Obojí je velmi důležité. Identity managementu je věnovaná kapitola uvedena níže. Samotný access management znamená v podstatě správu přístupových práv, který se váže k procesům a technologiím využívaných pro kontrolu a monitorování přístupu k síti. Mezi jeho funkce patří autentizace (jedná se o proces ověřování identity subjektu, stručně řečeno jde o zjištění identity), autorizace (proběhne-li proces autentizace, tak dojde k autorizaci, která umožní identitě přístup k požadovaným informacím) nebo auditování. Toto bývají nepostradatelné součásti systémů pro identity management.

Z dostupných zdrojů nejlépe shrnuje poznatky firma IBM[1], tak implementovat, nasadit a udržovat integrovaný systém správy identit. Takový systém umožňuje standardizaci správy přístupů na všech platformách pro uživatele, zařízení, aplikace

[1] Tyto poznatky vztahuje konkrétně na vlastní produkt, tak pro představu bohatě postačují.

a obchodní procesy, stejně jako míst fyzické bezpečnosti, jakými jsou čtečky biometrických údajů, smart karet či štítků. S pomocí IBM můžete získat:

- Bohaté portfolio produktů správy identit
- Řešení takřka veškerých aspektů správy identit, včetně ověřování, přidělování a kontroly přístupů
- Řešení komplexní správy identit na bázi politik, od vytváření uživatelských profilů až po jejich vyřazování z provozu
- Volbu mezi integrovaným řešením či samostatnými komponenty
- Efektivnější, cenově výhodnější procesy správy identit, které vyhovují nárokům na shodu s nařízeními [IBM-Identity and access management services, 2009]

3.12 Ověřovací údaje (Credentials)

Záleží vždy na dané organizaci jak má nastavené ověřovací údaje (credentials). Obecně lze říci, že se jedná o identifikátor využívaný uživatelem k získání přístupu do sítě. A to za pomocí uživatelského jména, hesla, domény, uživatelského certifikátů, různé biometrické informace (otisky prstů, barevné otisky prstů, autentizace na základě obličeje, autentizace na základě geometrie ruky, identifikace na základě duhovky, identifikace na základě sítnice, identifikace na základě DNA, identifikace na základě EEG křivky, analýza psaní na klávesnici, identifikace na základě chůze). Ty jsou jedinečně pro každý identifikovaný subjekt, proto se významně rozšiřuje jejich využití při autentizaci.

3.13 Resetování hesla (Password reset)

V tomto kontextu jde o funkci systémů identity managementu. Tato funkce umožňuje uživatelům samostatně resetovat (anulovat) heslo. Nepotřebuje k tomu tedy žádného správce sítě ani kontaktovat podporu help desku.

3.14 Identity management

V dřívějších dobách tedy nebylo tolik počítačových aplikací a ani uživatelů. V dnešní době lze říci, že každým dnem stoupá počet uživatelů a počítačových aplikací. Je to způsobeno zejména tím, že technologie je na jiné úrovni. Firmy musejí

být konkurence schopní a plnit požadavky zákazníku v co nejkratším čase. Klade se důraz na bezpečnost, rychlost, přesnost a zaměstnanci používají stále více počítačových aplikací. Dokonce si dovolím tvrdit, že je vyžadována i tzv. pohodlnost uživatele (snaha o to nechodit zbytečně tam, kam nemusím, nejlépe řešit vše online). Tento „boom" nastal s příchodem e-business řešení, které „představuje **elektronické podnikání**. Elektronické podnikání využívá zejména webové technologie a různé automatizované informační systémy. Rozmach e-businessu v posledních letech souvisí hlavně s rozvojem internetu, softwarových technologií, hardware a telekomunikací. Pojem e-business má poněkud širší záběr oproti **e-commerce**. Zatímco e-commerce se primárně soustřeďuje na elektronické obchodování, e-business se oboru elektronického podnikání věnuje komplexněji. E-business zahrnuje obchodní procesy zahrnující celý řetězec od elektronického nakupování, managementu zásobování, zpracovávání objednávek, zákaznickým servisem, vztahy se zákazníky (**CRM**), využívání **ERP** systémů, elektronické výměny dokumentů (**EDI**, **EDIFACT**) až po kooperaci obchodních partnerů. Komplexní nasazení aplikací a principů e-byznysu společnosti zajišťují buď prostřednictvím vlastních IT oddělení, nebo využívají alespoň částečně služeb s**ystémových integrátorů**. V praxi je často využito **outsourcingu IT řešení**." [E-business|ShopCentrik, c2010]

3.14.1 Proč by nás měl tedy identity management zajímat?

Nejlépe si situaci představíme na korporátní společnosti. Budeme předpokládat, že máme 1500 zaměstnanců. Ve firmě pro práci používáme na 100 aplikací. Máme tedy tisíce účtu a velké množství rolí. Tyto aplikace jsou používány v heterogenním prostředí na různých operačních systémech s IT službami poskytovány jak centrálně, tak distribuovaně. Každá aplikace má tedy jiné požadavky na správu uživatelů a přístupových oprávnění. Představte si tedy jak je složitá správa takového prostředí.

Čím je tedy organizace větší, tím více se zvyšuje počet spravovaných účtů a hesel. Proto je nutné zvýšit i počet administrátorů. V praxi to potom vypadá tak, že s rostoucím počtem aplikací roste i počet aplikačních správců, kteří spravují účty v přidělených programech. Jak píše pan Ing. Lukáš Jeník ve svém článku, tak „je to

způsobeno tím, že centrální útvar pro správu účtu nestíhá nebo neumí zakládat a rušit uživatelské účty ve všech provozovaných aplikacích, tato činnost se tedy deleguje na aplikační správce. Výsledkem pak obvykle jsou nekonzistentní procesy například při odchodu zaměstnance. Běžně se stává, že je zrušen pouze jeho „primární“ účet, zatímco účty v jiných aplikacích jsou dále aktivní a představují bezpečnostní riziko.“ [Jeník, 2004] Vznikají neefektivní procesy. Např. s příchodem nového zaměstnance do IT prostředí se stává složitý, pomalejší, hůře kontrolovatelný. Jeho odchodem. Změnou jeho role v organizaci. Úpravou role. Sledovat poté audit centrálně je velice náročné a složité. Zaměří-li se audit na konkrétního uživatele a jeho chování v celém prostředí, tak nastane problém. Protože účty se sledují pouze v oddělených aplikacích

Samotná správa identit úzce souvisí s bezpečnostní a produktivitou jakékoli organizace působící v oblasti s elektronických obchodních styků (viz E-business). Je tedy organizace dostatečně zabezpečená při ochraně svého digitálního majetku? Má dostatečnou obchodní produktivitu? Je administrace nákladná? Co je tedy hlavním úkolem identity managementu?

Jak uvádí a shrnuje Jaroslav Fojtík ze společnosti Convenio Consulting ve svém článku v časopise data v péči MHM tak „hlavním úkolem identity a access managementu (IAM) je stanovit a řídit, kdo a k jakým informacím bude mít v rámci informačního systému společnosti přístup v určitém časovém období. IAM procesy zahrnují vytváření identit pro jedince přistupující ke zdrojům informačního systému a jejich asociaci s uživatelskými účty jednotlivých systémů a aplikací, které organizace využívá. Nedílnou součástí IAM jsou rovněž nástroje umožňující komplexní auditování a monitoring. Co bylo kdysi jednoduchou záležitostí odehrávající se za zdmi výpočetního centra, se však postupem času stalo rostoucím problémem, se kterým se musejí vyrovnat společnosti všech velikostí. Jedním ze zdrojů rostoucí komplexity při řízení identit a přístupových práv je skutečnost, že ve většině společností existuje heterogenní prostředí zahrnující větší množství aplikací na různých operačních systémech s IT službami poskytovanými jak centrálně, tak distribuovaně. Každá platforma či aplikace pak vyžaduje vlastní správu uživatelů a přístupových oprávnění, což činí celý proces jejich správy komplikovanější. Ke zdrojům informačního systému navíc přistupují nejen vlastní

zaměstnanci, ale rovněž další skupiny uživatelů, jako jsou zákazníci, dodavatelé či partneři, přičemž samotný přístup se může realizovat několika různými způsoby, například přes terminál, klient-server či webové rozhraní. Decentralizovaná správa identit uživatelů a jejich privilegií prostřednictvím manuálních postupů nejen značně zatěžuje správce systémů, ale rovněž není sto zajistit patřičnou úroveň informační bezpečnosti společnosti na úrovni definované například mezinárodním standardem ISO27000. Společnosti musejí umožnit přístup ke zdrojům informačního systému rostoucímu počtu uživatelů, a to jak uvnitř, tak vně své organizace, a zajistit přitom pro uživatele co nejvyšší produktivitu a ochranu dat. Identity a access management přinášejí řešení uvedených úkolů prostřednictvím důsledné centralizace správy identit a privilegií v rámci jejich životního cyklu.“ [Fojtík, 2010]

Ať to na první pohled možná nevypadá, tak každá organizace musí řešit identity management. Je to dáno hlavně hierarchií společnosti, každá organizace má určité členění, které rozlišuje, zda daný subjekt (zaměstnanec) má právo na to, aby obdržel požadované informace nebo ne. Nelze dopustit, aby osoba z venčí měla přístup k citlivým informacím, nebo zaměstnanec na nejnižší pozici viděl údaje, které může vidět jenom top manažer (nebo jeho nadřízený). Je nutné řešit otázky spojené s identity managementem, rozpoznat kdo má anebo nemá přístup do systému, kam může přistupovat, co může a nemůže v daném systému vykonávat, apod. Pokud organizace neřeší tyto základní otázky, tak dochází k nekontrolovanému úniku dat, důležitých informací a je zde riziko vzniku velkých škod. Proto lze obecně říct, že řízení přístupu a (alespoň základní) identity management jsou nezbytné v jakékoliv organizaci bez ohledu na předmět podnikání (lišit se může pouze stupeň složitosti řešení a použité prostředky).

3.14.2 Jak tedy správa identit může konkrétně pomoci společnostem?

Implementací systémů pro identity management může poskytnout organizacím velkou konkurenční výhodu. Často se v této souvislosti hovoří o tzv. self reset password, kdy je uživatel si schopen sám resetovat heslo do dané aplikace, kde má přístupová práva. Na první pohled to působí velmi triviálně. Ve velkých podnicích tato zdánlivá maličkost se může pro firmu stát velice nákladnou a časově náročnou. Podle mých dosavadních pracovních zkušeností a statistik se přibližně polovina hovorů směřujících na help-desk svázána týká žádostí o reset hesla. Nasazením softwaru pro identity management se tato činnost dá automatizovat. To probíhá ve smyslu, že uživatel je schopen sám si resetovat heslo. Obzvláště větší podniky dosáhnout v této oblasti významných časových i finančních úspor.

Systém identity managementu přináší zvýšení bezpečnosti a kvalitnější kontrolu přístupu. Je však nutné zabezpečit co nejpřesnější definování organizačních rolí a následně přístupových politik. Je velmi důležité určit, kdo bude mít přístup k jakým informacím. Tato definice je základní částí digitální identity. Dobře spravované identity obnášejí lepší kontrolu přístupu uživatelů, což se projeví ve sníženém riziku vnitřních a vnějších bezpečnostních narušení. Systém pro správu identit může rovněž zlepšit dodržování souladu s vládními nařízeními (opatření ČNB č. 2 ze dne 3. února 2004 k vnitřnímu řídícímu a kontrolnímu systému banky), jedná se o tuto část:

Požadavky na informační systémy

III) Bezpečnost přístupu k informacím

Banka zabezpečí:

a) přidělení přístupových práv uživatelům v informačních systémech.
b) jednoznačnou identifikaci a autentizaci uživatele, které musí předcházet aktivitám uživatelů v informačních systémech.
c) přístup k informacím v informačních systémech pouze uživateli, který byl pro tento přístup autorizován.
d) ochranu důvěrnosti a integrity autentizační informace.
e) zaznamenávání událostí, které ohrozily nebo narušily bezpečnost informačních systémů, do bezpečnostních auditních záznamů, ochranu těchto záznamů před

neautorizovaným přístupem, zejména modifikací nebo zničením, a jejich archivaci.

f) vyhodnocování bezpečnostních auditních záznamů pracovníkem, který nemá možnost modifikovat v informačních systémech informace související s činností, o které je bezpečnostní auditní záznam pořízen. [Opatření České Národní Banky, 2004]

Společnostem poskytuje nástroje k implementaci komplexního zabezpečení, kvalitního auditorního procesu i vlastních pravidel pro přístup. Mnohé systémy dnes nabízejí funkce určené k zajištění fungování organizace v souladu s regulacemi.

3.14.4 Výzvy, slabiny, rizika v oblasti řízení přístupu?

Obecně se dá říci, že kdo neřeší identity management, tak je ohrožen nekontrolovatelným únikem dat. 8. Října v roce 2010 vyšel zajímavý článek na stránkách ICTsecurity.cz. Kdy redakce serveru pokládala otázky odborníkům z praxe (Roman Smolka, Technical architecture manager, Telefónica O2 Business Solutions, Miroslav Šedivý, Senior IT specialist, Telefónica O2 Business Solutions, Vladimir Kajs, Product development manager, Telefónica O2 Czech Republic.). Zajímavá je část, kdy byl položen dotaz: Jaké jsou největší výzvy, slabiny a rizika v oblasti řízení přístupu? „Největší slabiny spočívají v nekoncepčnosti řešení řízení přístupu, v jeho malé provázanosti na skutečné potřeby organizace v oblasti bezpečnosti informací. Příkladů je celá řada, uveďme některé:

1. nedostatečná efektivita řízení přístupu z pohledu uživatele – pokud má uživatel přístup do mnoha aplikací a ke každé z nich musí znát své přístupové jméno a heslo, končí to zpravidla tím, že má buď všude stejné heslo, nebo má hesla různá, avšak zpravidla napsaná na papíru a uložená pokud možno v dosahu – např. v šuplíku svého stolu
2. nedostatečná efektivita řízení přístupu z pohledu správce – pokud v organizaci, která má stovky uživatelů správci odpovědnému za řízení přístupů neposkytneme dostatečné nástroje, je velmi pravděpodobné, že dříve nebo později udělá chybu a s rovněž velkou pravděpodobností si jí nevšimne. Následky ovšem mohou být nedozírné.

3. neodpovídající oprávnění - v systémech, které nedisponují odpovídajícím nástrojem pro identity management, má velké procento uživatelů větší oprávnění, než ve skutečnosti potřebují – důvody bývají různé, od pohodlnosti administrátorů až po neoprávněné zasahování nadřízených.

4. špatná provázanost procesů řízení přístupu na životní cyklus zaměstnance – jestliže se o okamžité výpovědi zaměstnance dozví pracovník, který má na starosti správu přístupových oprávnění, s dvoudenním zpožděním, je téměř jisté, že si propuštěný zaměstnanec vytvořil kopie všeho, co potřeboval – situace může být ještě horší u administrátora důležitého systému.

Optimální identity management systém by proto měl disponovat alespoň následujícími vlastnostmi:

1. napojení na systémy řešící životní cyklus zaměstnance – tedy na HR systémy, protože oddělení lidských zdrojů má vždy nejblíže k informacím týkajících se aktuálního statutu zaměstnance (nástup, změna postavení, ukončení zaměstnání apod.) a může velice rychle založit proces vedoucí k okamžité aktualizaci příslušných oprávnění.
2. používání rolí – v organizacích, které mají stovky, či tisíce zaměstnanců není možné nastavovat oprávnění každému zaměstnanci do každé ze stovek aplikací organizace – jako optimální se jeví zařazení zaměstnanců do rolí a automatizované přidělení oprávnění podle profilu dané role. Zařazení do role může být součástí HR procesů.
3. používání standardních rozhraní a protokolů pro přihlašování – noční můrou administrátorů jsou systémy, které proprietárním způsobem řeší přihlašování uživatelů, optimální je použití standardních protokolů využívajících např. LDAP.

Již tyto výše uvedené vlastnosti identity management systému odbourávají zmíněné nedostatky, mnohé z nich pak toho umí nabídnout daleko více.“ **[O2, 2010]**

Popsány byly různé případy, ale nebyla zmíněna jedna z nejvážnějších hrozeb, kterou je krádež identity! V této souvislosti se používá pojem **Identity Thief (Identity Fraud[2]),** jedná se o nedovolené shromažďování a používání osobních údajů, obvykle za účelem kriminální činnosti. Obrázek č. 1 popisuje Identity Thief a jeho dělení (Krádež řidičského průkazu, sociálních dat, zdravotnických dat, osobních dat, finančních). Např. V USA je krádež identity jeden z nejrychlejších rostoucích zločinů. Důvod je jasný a to finanční prospěch. Zloději používají osobní data k získání řidičského průkazu na Vaše jméno a používají ho při porušení dopravních předpisů. Stejně jako používají SSN (sociální zabezpečení) k získání zaměstnání, na pojistná plnění, rentgeny, lékařské testy. Krade se i Váš charakter, který má krýt trestnou činnost jedince. Důsledek je, Vaše obvinění! Zloději používají Vaše osobní data k otevření nových bankovních účtů, nebo získávají přístup ke stávajícím.

Obrázek 1: Identity Thief se skládá z pěti uvedených typů [*ID Theft Instruction, c2010]*

Krádeže identity jsou dnes v kurzu. Jak píše Vojtěch Blažek na internetovém tuzemském serveru domaci.ihned, tak „policisté se za poslední půlrok setkali s pěti krádežemi nového typu. Někdo se dostane k cizím heslům do mailu, na Facebook nebo do internetových diskusí. A pak se za vás začne vydávat – aby rozšířil pomluvy nebo dokonce odsál peníze z účtů. "Hodně lidí si myslí, že co se děje na internetu, je jen taková legrace. Ale těchto činů bude přibývat a budou nebezpečnější," předpovídá Radim Polčák, právník z Masarykovy univerzity v Brně, který se na internetovou kriminalitu zaměřuje. V české republice nastupuje nový trend, potvrzuje i čerstvá

[2] V USA mapuje kriminalitu internetový server http://www.identitytheft.org

zpráva ministerstva vnitra o kriminalitě. "Jako nový fenomén se objevují krádeže identity a zneužití k diskreditaci osoby, za kterou se útočník vydává," stojí ve studii. Experti přitom čekají, že už brzo půjde také o peníze. "Zloději identity" totiž v cizině běžně útočí na účty svých obětí. Buď se snaží dostat do e-bankovnictví, nebo se jim alespoň pokouší "vysát" konta přes ukradená čísla platebních karet. Čísla jsou dnes běžně ke stažení na některých ruských serverech, ale už se objevují i v Česku. V severních Čechách nedávno policisté našli u jednoho člověka stovky čísel karet. Ale nedokázali mu, že je zneužíval.“ [Blažek, 2009]

Poslední dobou se to stalo běžnou věcí, jakou může být krádež auta. Většina lidí nevěnuje pozornost tomuto tématu. Představa že někdo převezme/vypůjčí vaše já již není tolik nereálná[3]. K největšímu krádeži identity v historii internetu došlo v USA, tu odhalily úřady pro bezpečnost, jak popisuje článek na stránkách ekonomika.ihned, tak „ukradena byla čísla zhruba 130 milionů kreditních a debetních karet, a to ze systémů firem Heartland Payment Systems, 7-Eleven a Hannaford Brothers, informovala agentura Reuters. Federální prokuratura oznámila, že obviněni byli v této souvislostitři lidé. Pětkrát údajně pronikli do počítačových systémů uvedených firem s cílem zmocnit se dat o platebních kartách a jejích majitelích. "Pravděpodobně se jedná o největší případ odcizení identity, který jsme kdy vyšetřovali,"potvrdila prokuratura. Podle agentur Reuters a Bloomberg jsou mezi obviněnými dva počítačoví hackeři a muž z Miami. Reuter přinesl informaci o 28letém Albertu Gonzalezovi, který má stanout před soudem se dvěma počítačovými piráty zřejmě ruského původu. “Vyšetřování dokazuje schopnost orgánů činných v trestním řízení odhalovat a sledovat aktivity hackerů po celém světě," cituje agentura Bloomberg státního návladního Ralpha Marru. Všichni tři se zaměřovali na největší americké společnosti, jejich názvy si vyhledávali v žebříčku 500 největších firem, ten sestavuje časopis Fortune. Nejprve si prý prohlédli internetové stránky těchto podniků a pak se pokusili najít slabá místa v jejich zabezpečení. Zločinci chtěli ukradená data prodat lidem, kteří by je využili k páchání trestné činnosti. Pravděpodobně by díky získaným číslům platebních karet prováděli nákupy přes internet.“ [iHNed.cz, 2009]

[3] Reportáž ČT 1 ze dne 8. 3. 2010 http://www.uoou.cz/files/reporteri_ct_08_03_2010.wmv

Je velké množství případů, které se staly. V budoucnu jejich počet bude stoupat. Spousta nás bere tuto hrozbu na lehkou váhu. Za přečtení stojí rozhodně i tyto články. První z nich popisuje hackery[4] a druhý se zaměřuje na otázku, zda se lidé bojí krádeže své identity[5]. Obecně bych doporučil dbát zvýšené opatrnosti při předávání osobních dat třetím stranám. A používal bych co nejvíce možných kombinací hesel. Nedržet se jednoho osvědčeného!

3.14.3 Výhody Identity managementu

V minulých kapitolách jsme obecně popisovaly různé výhody. Popisovaly jsme co je identity a access management. Zmiňovaly různé problémy. Cílem této podkapitoly je shrnout výhody.

Obecně se dá říci, že jeden z největších potenciálních přínosů IM (IAM) systémů je **bezpečnost založena na rolích** (systémem nadefinujeme uživatelské role, kterým přidáme příslušné aplikační přístupy. Praxe je taková, že role odpovídají pracovním pozicím, ale nemusí to být nepsané pravidlo. Při změně pozice pracovníka pak IDM (IAM) systém jednoduše opraví (nebo zruší) všechny jeho přístupy a účty automaticky.) Tímto se získá **kompletní přehled o přístupových právech uživatelů**. Dají se tedy zjistit potenciální bezpečnostní potenciální rizika.

Další nespornou výhodou je **centralizace a automatizace správy účtů**, ta probíhá na jednom místě, a to v IDM (IAM) systému. Správce účtů definuje role a jim přístupová oprávnění do konkrétních aplikací, které má určené zaměstnanec pro práci.

Pro manažery a nadřízené pracovníky, různé auditory je určitě jedna z nejvýznamnějších výhod **jednoduchý audit**. Všechny operace jsou ukládány na jednom místě, v databázi. A pomocí aplikace IM (IAM) se dají nastavit bezpečnostní reporty a audity dle požadavků nadřízeného, oddělení. Lze tedy získat velmi dobrý a rychlý přehled o pohybu pracovníků nebo vytvoření/smazání uživatele, změny rolí, změny hesel apod.

---

[4] http://www.lupa.cz/clanky/online-kradeze-citlivych-udaju-dobry-byznys-pro-hackery/

[5] http://www.lupa.cz/clanky/bojite-se-kradeze-sve-identity/

Velkým přínosem IAM (IM) je **automatizace procesu vytváření účtů** pro nové zaměstnance, změn přístupových oprávnění (změna pozice pracovníka) nebo rušení účtu (to je spojené s odchodem zaměstnance). Nový zaměstnanec má tedy ihned aktivní účty a „odchozí" zaměstnanec má ihned deaktivovány účty. Nedochází tedy ke zneužití zapomenutých, nepoužívaných, ale stále aktivních účtů. S tímto je spojené i **snížení pracovníků zabývajících se řízením přístupů** (většina procesů je automatizovaná).

V praxi se často stává, že někdo onemocní, má dovolenou apod. je tedy nutné ho zastoupit. K tomu slouží tzv. **delegace**, systémy IAM (IM) umožňují delegaci **bez účasti správce systému** nebo jiného specializovaného útvaru. Pomocí delegace je možné přenést odpovědnost za určité operace v IM na osoby, kterým dané oprávnění věcně přísluší. Často se jedná o řídícího nebo pověřeného pracovníka, který spravuje danou oblast nebo útvar. Některými oprávněními může být pověřen i samotný uživatel, který mění atributy spojené se svou osobou.

Již zmíněnou důležitou funkcí, která zní velmi triviálně, ale podle dodavatelů i analytiků může podnikům ušetřit zdaleka nejvíce financí. Jedná se o **samostatné resetování hesel** (v praktické části, v kapitole 6.1.4 Testování self-reset password je vytvořena příručka pro uživatele a zároveň je otestováno, že pro uživatele to není žádný problém. Nezáleží na konkrétním dodavateli, princip self-reset password bude obdobný). Zdánlivá trivialita však může v některých podnicích přerůst v neuvěřitelně komplexní, nákladnou a časově náročnou činnost.

Systém pro správu identit může rovněž zlepšit dodržování **souladu s vládními nařízeními**, neboť společnostem poskytuje nástroje k implementaci komplexního zabezpečení, kvalitního auditorního procesu i vlastních pravidel pro přístup.

Firmy nabízejí **relativně krátkou dobu implementace**, v závislosti zvolení dodavatelé (IBM, Novell, Oracle, Microsoft aj.). Je nutné si uvědomit, že produkty IM (IAM) jsou víceméně krabicová řešení. Pro které existují konkrétní postupy nasazení. Implementace je tedy kratší. Ale záleží na požadavcích organizace.

Výhod je velmi mnoho, zde jsou popsány ty nejzákladnější. Vzhledem k počtu firem, které nabízejí a dodávají řešení IM lze vytvořit jen tento základní přehled. Každá dodavatelská firma nabízí svojí přidanou hodnotu.

3.14.4 Pro koho jsou identity management systémy vhodné?

Jak bylo uvedeno výše, tak lze obecně říct, že řízení přístupu a (alespoň základní) identity management jsou nezbytné v jakékoliv organizaci bez ohledu na předmět podnikání (lišit se může pouze stupeň složitosti řešení a použité prostředky). Každá organizace tedy do jisté míry řeší identity management. Ale neřeší ho nasazováním různého/podpůrného softwaru (viz. Kapitola 5. Nástroje identity managementu). Máme-li malou organizaci (řádově do 100 zaměstnanců), tak je určitě větší pravděpodobnost uhlídání všech pohybu v rámci firmy. Ale to není pravidlo. Záleží na konkrétní organizaci.

Z praxe vím, že nasazování takových systému se vyplatí zejména ve společnostech:

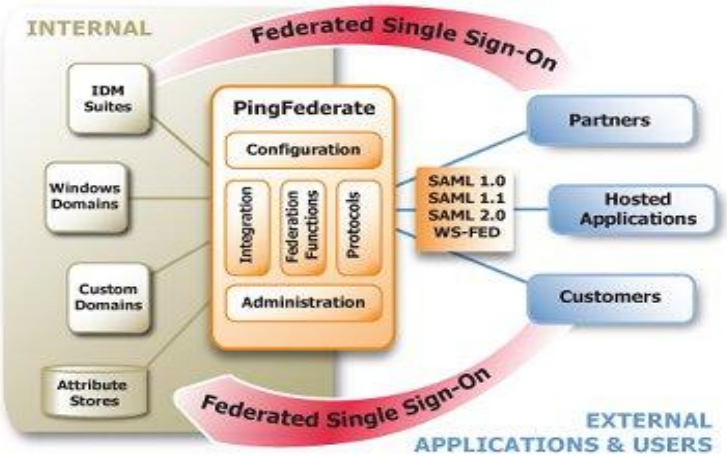
1. Mají více jak 800 uživatelů (zaměstnanců)
2. Pro práci používají velké množství aplikací
3. Autentizuje uživatele ke každé službě zvlášť
4. Provozují složité heterogenní prostředí (Aplikace jsou používány v heterogenním prostředí na různých operačních systémech s IT službami poskytovány jak centrálně, tak distribuovaně)
5. Firma má zavedeny nekonzistentní bezpečnostní politiky
6. Firmy požadují vyšší zabezpečení dat (postrádá bezpečnostní politiku účtů)
7. Firmy požadují spolehlivý audit (Operace (vytvoření/smazání uživatele, změna role, změna hesla atd.) jsou auditovány na jednom místě, u většiny produktů do databáze, ze které je pak možné dělat svoje vlastní reporty a výstup)
8. Firma spravuje různá organizační schémata využívaná jednotlivými aplikacemi

Těmi velkými společnostmi, které volí toto řešení, jsou hlavně tuzemské banky, pojišťovny (Komerční Banka, ČSOB, ING, aj.).

3.15 Federativní důvěra (Federated Identity Management)

V souvislosti s identity managementem se hovoří i o Federated identity managementu, které umožňuje sdílení digitálních identit s důvěryhodnými třetími stranami (např. když vybuduje silná korporace bezpečný kanál, může tento kanál sdílet se svými partnerskými společnostmi, ve výsledku budou se zákazníky také komunikovat zabezpečeně). Pro komunikaci se využívá tzv. Security Assertions Markup Language (SAML)[6], ten pomáhá bezpečně přenášet informace o jednotlivých identitách přes různé platformy a podniky.

Princip tedy spočívá ve využití jediného uživatelského jména, hesla a případných dalších údajů. Tento princip se obecně označuje jako Single Sign-On (viz Následující kapitola 3.16). Čili Federated Identity Management (FIM) je verzí SSO kde každé zařízení, systém a aplikační dotazy využívají centrální databáze pro autentizaci a autorizaci informací. FIM mají tedy za úkol umožnit autentizaci a autorizaci dat přes hranice organizace. Ve skutečných FIM systémech, autentizace dat prochází zabezpečenou doménou přes společnost k obchodním partnerům. Obrázek číslo 2 graficky popisuje vysvětlený princip.



Obrázek 2: Graficky popsaný princip Federated Single Sign-On [ID Theft Instruction, 2010]

[6] Ta definuje rámec XML pro bezpečnou výměnu mezi bezpečnostními autoritami. SAML bylo vyvinuto sdružením Liberty Alliance, které se zabývá vývojem specifikací, směrnic a best practices pro Federated identity management. Organizace přišla se specifikací SAML, aby umožnila vzájemnou interoperabilitu různých platforem pro autentizaci a pro poskytování autentizačních služeb.

Stejně jako většina jiných systémů vyžaduje standardizaci. Lídrem ve vývoji standardů je již zmíněná Liberty Aliance, jedná se o skupinu více než 150 organizací (Sun, Novell, Oracle, Intel, Fidelity, Aol, Isoc, Adobe, GSA, Bupa aj.)[7], neziskových organizací a vládních subjektů, které mají za úkol vytvářet otevřené standardy[8].

Název	Popis
ID-FF	The Identity Federation Framework
ID-WSF	The Identity Web Services Fram ework
ID-WSF DST	The Data Services Template
ID-SIS	A collection of Identity Services Interface Specifications

Tabulka 1: Příklady standardů s originálním popisem

Federovaný model identity managementu může usnadnit administraci a umožnit společnostem rozšířit správu identit a přístupu také na uživatele třetích stran a služby ostatních podniků.

[7] Úplný seznam členů na stránce http://www.projectliberty.org/ v sekci Membership

[8] Úplný seznam standardů na stránce http://www.projectliberty.org/v sekci Specifications

3.16 Systém jednotného přihlašování (Single Sign-On)

Single Sign On (SSO) je proces, který umožňuje uživateli zadat přihlašovací údaje (jméno, heslo) tak, že dostane přístup k mnoha aplikacím. Tento proces autentizuje uživatele ke všem aplikacím, ke kterým má v rámci systému povolený přístup a eliminuje další výzvy k zadání přihlašovacích údajů při přechodu z jedné aplikace do jiné. Uživateli odpadá nutnost pamatovat si hesla a přístupy pro různé aplikace (už víme, že heslo je jedině dobré, pokud je tzv. silné). Pokud si musíme pamatovat více silných hesel, hrozí, že je zapomeneme a začneme používat hesla slabší nebo dokonce stejná. To přináší rizika.

Proces Single-Sign-On je v současnosti nabízen v různých podobách přímo od výrobců PC či notebooků. Pokud ovšem uživatel nemá zabezpečený přístup do PC pomocí silného hesla (které často mění), zvyšuje se riziko zneužití tohoto systému při prvotním prolomení přístupu k PC. Proto se doporučuje systém SSO používat spolu s tokenem či čipovou kartou.

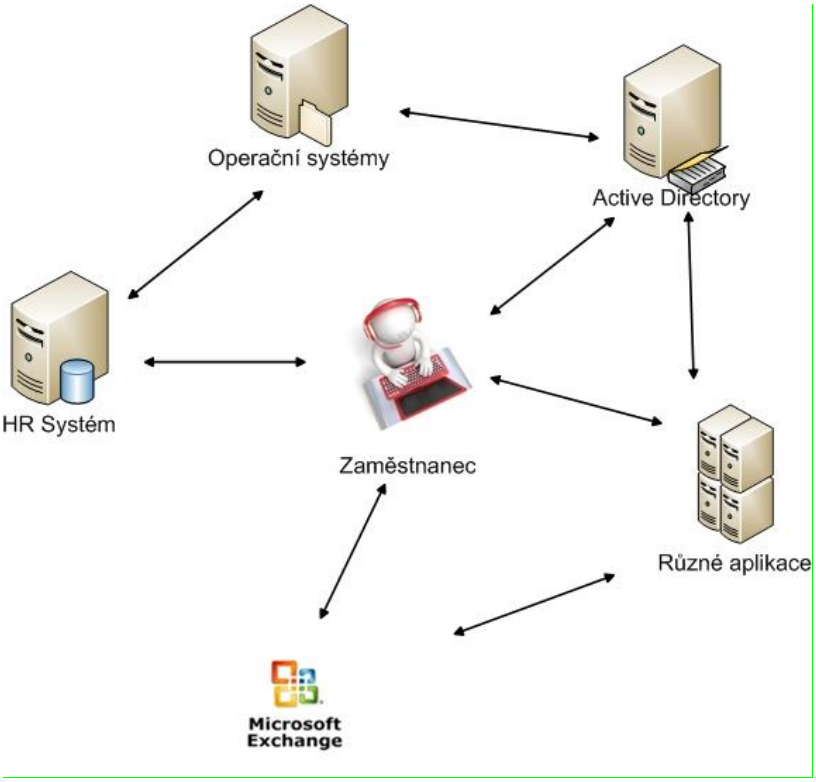
Výhody SSO je výrazná úspora času díky absenci mnoha přihlašování uživatelů denně, zvýšení bezpečnosti při nakládání s přihlašovacími údaji. Úspora nákladů na IT podporu snížením počtu uživatelských požadavků.

4. Jak funguje Identity management?

Cílem této kapitoly je vysvětlit funkci identity managementu.

4.1 Základní funkce a cíle

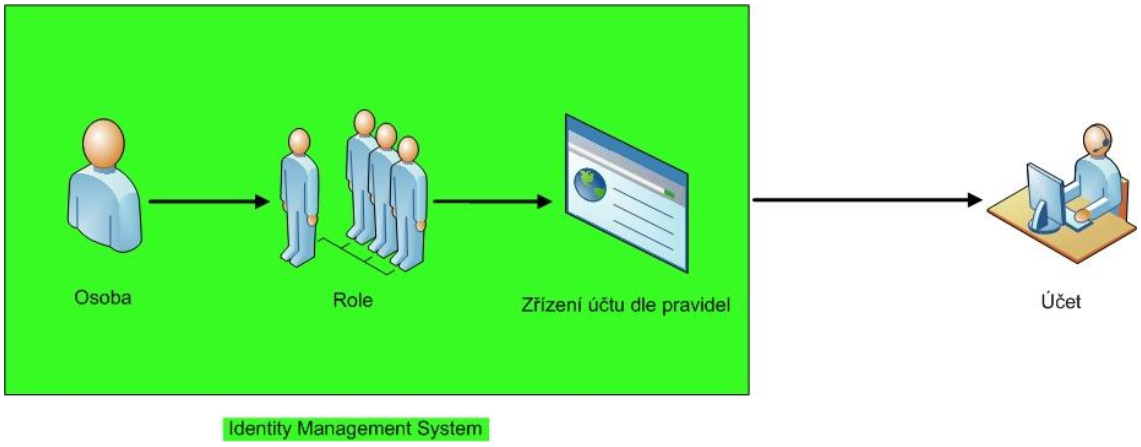
Ve většině velkých firem a organizací existuje heterogenní prostředí, kde jsou různé aplikace na různých operačních systémech, databázích, centralizované, decentralizované i lokální. Přístupy přes terminál, klient-server, webové rozhraní. Zní to velmi složitě. A ano, je to velmi složité a nepřehledné. Klasický protiargument je, ale ono to přece funguje. Je to dáno tím, že vedoucí pracovníky nezajímá pozadí, ale výsledek. Je nutné si uvědomit, že každá platforma, databáze, aplikace má svou vlastní správu, vlastní seznam uživatelů (jejich oprávnění), vlastní bezpečnostní pravidla. Celková správa tohoto prostředí je náročná. Jsou tedy kladeny nároky jak na samotné uživatele, vlastníky dat, tak i správce systémů. To vše stojí peníze a čas. Situace před nasazením IM se dá přiblížit na následujícím obrázku č. 3 (nejedná se o reálný podnik). V obrázku by se na první pohled nemělo dát vyznat.



Obrázek 3: Stav před nasazením řešení IDM

Cílem IM (viz zmíněné výhody IM v kapitole 3.14.3) je sjednotit správu přístupů do jedné aplikace. Získat jednotným interface. To eliminuje rozdíly ve správě jednotlivých systémů. Zjednoduší se celý proces přidávání, modifikace a mazaní přístupových oprávnění, při naplnění bezpečnostních pravidel v organizaci.

Co jsou tedy IM systémy? Jedná se o **aplikace definující vztah mezi osobou** (údaje o ní jsou získány z personálních systémů, HR databáze, nebo jiných zdrojů dat) **a účtem**, který poskytuje přístup k požadovaným informacím, aplikacím a systému. Po získání základních vstupních informací automaticky, popřípadě na žádost spouští procesy. Ty mají přesně stanoveny pravidla, která vedou k vytvoření (popřípadě modifikaci, zrušení) účtů a jiných nastavení. Na základě toho může osoba provádět požadované práce zajišťované oddělením Informačních technologií. Principiálně je to zachycené na obrázku číslo 4, kde je znázorněno schéma základního principu Identity managementu.

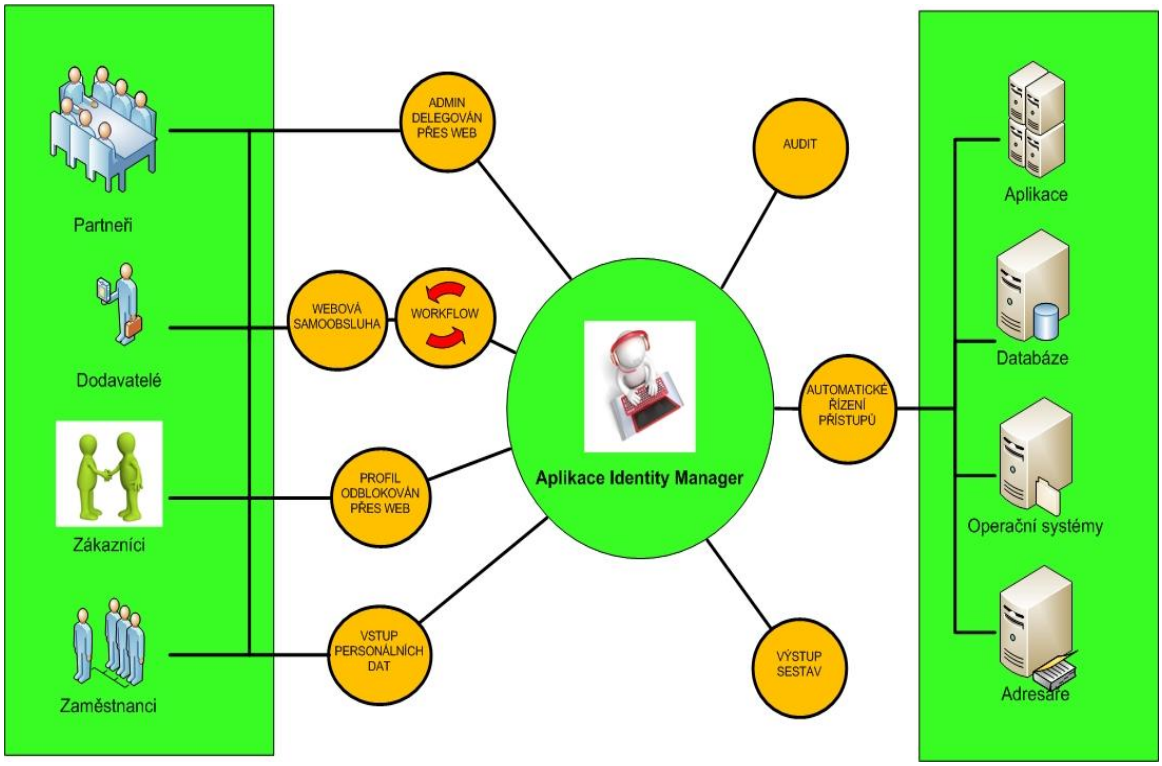


Obrázek 4: Schéma základního principu Identity Managementu

Obyčejně proces přidělení přístupů ke zdrojům probíhá tak, že ten kdo je pověřený (určitý pracovník) sepisuje žádost o přístupové oprávnění. Tu předává svému nadřízenému ke schválení. Po schválení žádost přechází k formálnímu posouzení na příslušné oddělení. Po schválení se provede její realizace. Zní to velmi jednoduše, ale v praxi to tak není. Žádost bývá nekompletní, obsahuje různé chyby (neoprávněný pracovník schválil, technické chyby, pracovník nemá nárok na přístup aj.). Tímto dochází k velkému prodloužení doby, než se požadavek realizuje.

V IM řešení se nesetkáme s chybami tohoto typu. Celý proces žádosti totiž proběhne pouze zadáním požadavku přímo v IM systému. Vše se nahradí pomocí elektronického formuláře, kterým pracovník (pověřená osoba) zažádá o vytvoření (změnu) přístupu. Dojde k automatickému doplnění potřebných údajů a žádost je v rámci systému předána ke schválení (pokud je to vyžadováno). To ovšem není vše, IM systém provádí kontrolu vyplněných údajů a zadavatele upozorňuje na případné nedostatky. Požadavek je schválen ihned, popřípadě v naplánovaný čas automaticky zrealizován. Jakmile je celý proces dokončen, tak je o tom zadavatel informován (po celou dobu může také sledovat, v jaké fázi se požadavek nachází). Dokončení tohoto procesu znamená přidělení přístupového oprávnění do dané aplikace (systému). Toto představuje pohled uživatele. Z pohledu bezpečnostního správce je situace složitější.

Na obrázků číslo 5 je situace po nasazení systému IM. Dojde k vytvoření uživatele jako identity, k identitě IM systém přidá uživatelské účty (veškeré) a hesla. Výhodou IM oproti SSO spočívá v ušetření nákladů, jelikož není potřeba upravovat existující aplikace. Uživatelské databáze zůstanou zachovány, správa účtů se zautomatizuje a transparentní (průhledné). Funguje to obdobně, jako když zavoláme například do O2 a objednáme si službu. Operátor call centra požadavek zanese do svého počítače. Po určité chvíli jsou upraveny prvky v telekomunikační síti. Zákazník tedy může využívat další služby.



Obrázek 5: Princip IM po nasazení do provozu (za účasti uživatelů, zdrojů a Identity manageru)

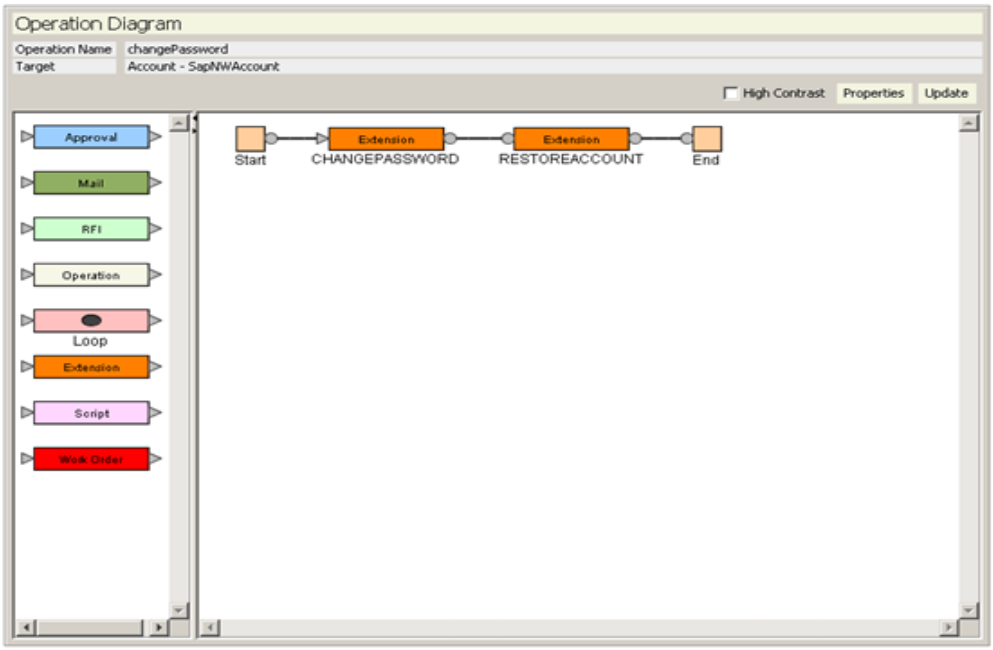
4.2 IM systémy z pohledu správce bezpečnosti

Na začátku tohoto dokumentu byly představeny různé základní pojmy. V souvislosti s funkcí IM systému se používají další pojmy. První a základní jednotka IM systému je **entita**. Jak je obecně známo, tak toto slovo vzniklo z latinského entitas (bytost), ens (jsoucí). Všeobecně s e entita označuje jako objekt. Pro systémy IM se definuje jako osoba, organizační jednotka, účet, nebo různé prvky. Pro tyto prvky jsou stanoveny vztahy prostřednictvím pravidel (policy). Entita jakéhokoli typu má určité atributy. Ty slouží pro jejich detailní popis. Stanovují se i další atributy. Tím vzniká ucelený popis vybrané entity. Návazné aplikace poté tyto data zpracovávají do výsledné podoby, která je požadována.

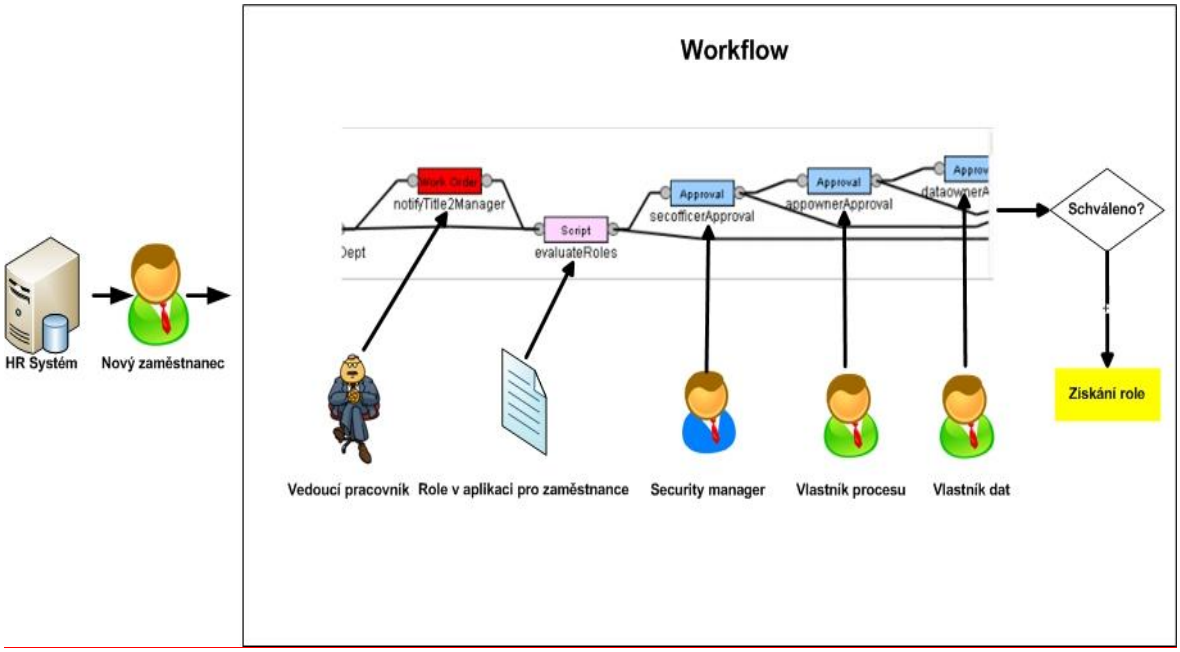
Na obrázku číslo 4, je znázorněn princip aplikace IM. Jednotlivé role jsou v IM systému dány podle typu přístupu, popřípadě druhu uživatele. Každá role je svázána s určitým typem pravidel (policy). Např. máme uživatele Milan Hořejš (entita typu Person), kterému přiřadíme roli pokladník. Pro tuto roli jsou nastaveny přístupová oprávnění do třech aplikací (systému) pokladna, fakturace, kniha jízd. IM systém

automaticky zajistí přidělení přístupových oprávnění, která jsou vázány na tuto roli. Pokud se později rozhodne nadřízená osoba (nebo jiná odpovědná osoba), že role pokladník by měl získat přístup do další aplikace (systému), která se v rámci podniku nově nasazuje (systém SAP). Tak se k roli pokladník přidají přístupová práva pro aplikaci (systém) SAP. Automaticky je tato změna aplikovaná na všechny osoby, které mají tuto roli přidělenou. Dojde-li ke zrušení role, tak dojde k automatickému odebrání přístupu. Řídí-li se přístup pomocí rolí, tak to velmi usnadňuje delegování pravomocí na jiné osoby. Je tedy zřejmé, že je velmi důležité přesně definovat a popsat role. Tomu předchází složité analýzy v rámci celé organizace/firmy. Chce-li budoucí organizace/firma využít všechny možnosti, které IM poskytuje, musí mít co nejlépe definované role.

Jeden ze základních prostředků IM je **workflow (Ukázka na obrázku číslo 6).** Tento prostředek se používá pro modelování procesů. Procesy mohou být různé, např. vedoucí k vytvoření účtu nebo nastavení atributů. Důležité je dodržet veškeré formální požadavky na proces v rámci organizace. Za primární cíl se považuje umožnění schválení požadavků definovaných uživateli IM (respektuje se organizační struktura a ostatní pravidla, ty mohou být stanovena i vně workflow). Pro další názorný příklad se nabízí ukázat schvalovací workflow na obrázku číslo 7. Kde je zachycen příchod nového zaměstnance (např. do oddělení pokladníků), který je přidělen do daného oddělení a je tedy nucen získat novou roli. Před samotným získáním role přichází žádost o přidělení na vedoucího pracovníka. Ten přístup zkontroluje, schvaluje anebo odmítá. Poté vše kontroluje security manager a pracovník získává danou roli.



Obrázek 6: Ukázka workflow z produktu IBM Tivoli Identity Manager



Obrázek 7: Ukázka schvalovacího workflow

4.1.2 Delegování, administrace, poskytování a rušení přístupu

Přístupová práva a jejich poskytování je další důležitá součást IM systému. Jedná se o zajištění vlastního procesu, kdy se přiděluje přístup na základě požadavku, který je zadán pomocí IM systému. Pokud má organizace nastavena pravidla pro manuální řešení procesu, řeší ho manuálně, jinak lze samozřejmě nastavit automaticky. V praxi se stává, že je třeba, aby určitá osoba zastoupila jinou osobu. K tomu slouží funkce **delegace administrace**, ta umožňuje přenést odpovědnost za určité operace v IM. Odpovědnost přenáší na osoby, kterým oprávnění náleží. Toto má velké pozitiva, protože to přinese ulehčení práce. Není nutné volat a žádat specializovaný útvar o přenesení odpovědnosti na někoho jiného (je to velmi zdlouhavý proces). Odpovědnost se takto přenese na pověřeného pracovníka. Ten bude spravovat danou oblast, nebo útvar.

4.1.3 Management hesel, srovnání, samoobslužné služby

Klasickou situaci, kterou zná každý uživatel je velké množství účtů. S tím je spojeno i velké množství hesel. Čím více přístupu používáte, tím je větší pravděpodobnost, že si heslo nevybavíte. Z vlastní zkušenosti vím a mohu potvrdit, že používám někdy i to samé heslo do různých aplikací. Ano, je to bezpečnostní hrozba, které by se mělo předcházet. IM systémy i na toto myslely, jelikož nabízejí možnost **management hesel** (centrální správu hesel) a to se týká všech definovaných účtů. Zní to možná na první pohled jednoduše, ale na všechny účty je aplikovaná politika. Ta splní bezpečnostní požadavky konkrétních systému. Pro uživatele (stejně tak i pro správce systému a oddělení zabývající se přístupem) je v případě nasazení IM systému velká výhoda, že získá-li přístup do IM aplikace, tak je schopen si změnit heslo na kterémkoliv systému (aplikaci). Změna hesla může být provedena pro jednu aplikaci, nebo třeba všech najednou. O přístupu rozhoduje jeho role.

Obrázek 8: Uživatel, který využívá více aplikací, zná zpaměti všechny hesla?

V předchozí podkapitole byla vysvětlena delegace. K tomuto pojmu se váže tzv. **samoobslužná služba**. Ta představuje speciální formu delegace, která umožní uživateli, aby mohl samostatně provádět změnu atributů spojených se svou osobou. Uživatel je schopen žádat o přidělení jiných zdrojů, modifikací nebo žádat o jejich zrušení. Tyto operace (všechny) lze samostatně povolovat nebo zakazovat a to pomocí přístupových oprávnění (k atributům, operacím IM). Tato možnost se v praxi pro koncové uživatele často nepoužívá. Přeci jenom běžný uživatel (pracovník) se nerad učí něco nového a pro něho to představuje zbytečnou práci. V praxi se tedy pro uživatele používá pouze změna vlastního hesla.

Další důležitou funkcí je **srovnání**. Jedná se o proces. Tento proces provádí zpětnou kontrolu proběhnutých operací a porovnává reálný stav spravovaných systémů (aplikací), které jsou definované systémem pro Identity management. Tímto procesem lze získat reálný obraz řízených zdrojů na cílovém systému. Poté jej lze porovnat s hodnotami tak, že se aplikují všechny politiky na danou entitu (včetně jejího nastavení). Budoucí správce (popřípadě auditor) tak může mít k dispozici přesný přehled o všech operacích, které byly provedeny mimo systém IM. Ty mohou představovat neoprávněný zásah do systému.

5. Nástroje identity managementu

Cílem této kapitoly je představit vybrané volně dostupné konkrétní systémy sloužící pro správu identit a single sign-on. A zejména systémy pro komerční využití. Popíšeme vybrané aplikace. Poté navážeme praktickou částí, kde si vybereme jeden software a ten detailněji popíšeme. Zejména po procesní a technické stránce. K vybranému softwaru vytvoříme základní administrátorskou příručku (demonstrace na příkladu) a představíme zmiňovanou funkci self-reset password. Jako zajímavost představíme open source single sign-on systémy.

5.1 Open source single sign-on systémy

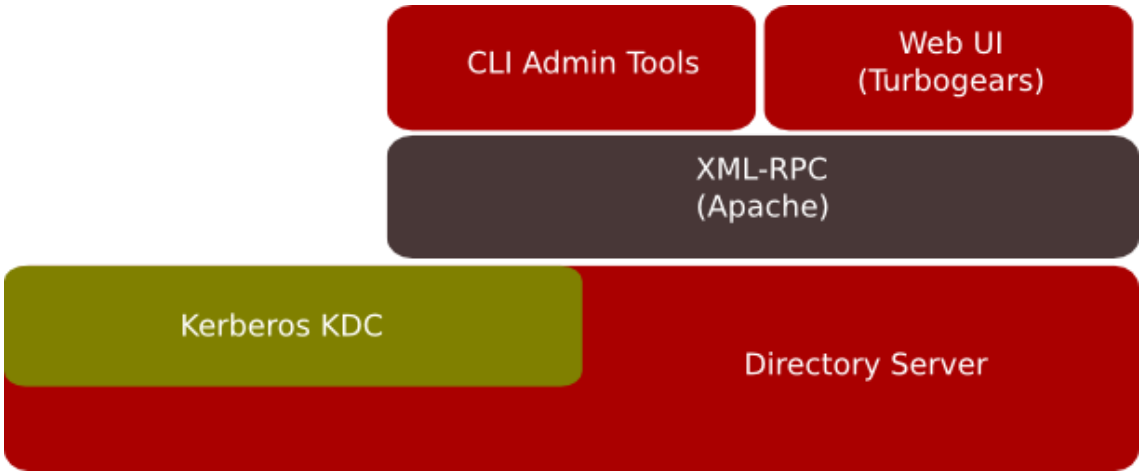
Open source (Open-source software) je počítačový software s otevřeným zdrojovým kódem. Otevřeností se rozumí technická a legální dostupnost. Jde o to, že ten kdo dodrží dané podmínky, tak má právo do kódu nahlížet a upravovat ho. Na rozdíl od komerčního softwaru nebo proprietárního softwaru[9]. Vybral jsem tři významné softwary, které jsou popsány v následujících kapitolách.

[9] Je takový software, kde autor upravuje licencí, nebo jiným způsobem možnosti jeho používání. Takový software tedy nemá k dispozici volné zdrojové kódy. Jejich úprava a následná distribuce není možná. Jedná se o synonymum komerčního softwaru, ale nemusí tomu vždy tak být.

5.1.1 FreeIPA

FreeIPA, písmeno I reprezentuje identitu (Identity), která v rámci řešení této aplikace obsahuje počítače, uživatele, virtuální počítače, skupiny, autentizaci osobních dokladů. P je politika (Policy), ta je řízená tzv. „Host Based Access Control“. A je audit (Audit), ale řešení této komponenty je dočasně odložené. FreeIPA používá k řešení kombinaci následujících technologií a prostředků (Architektura viz Obrázek 6):

- Linux (současně Fedora[10])
- 389 Directory Server
- MIT Kerberos
- NTP
- DNS (IPA v2)
- Webové a command-line nástroje pro správu uživatelů
- Dogtag Certificate System (IPA v2)



Obrázek 9: Architektura IPA serveru [FreeIPA, 2009]

[10] Nekomerční odnož Red Hat distribuce Linuxu, která se dá využívat a sdílet zdarma. Je sponzorována samotným Red Hatem.

Aktuální verze tohoto projektu má číslo 1.2.2, jedná se tedy o relativně nový projekt (aktivní vývoj probíhá od roku 2007). Jeho cílem do budoucna je konkurovat komerčnímu projektu Active Directory. Do budoucna se chystá verze 2.0.0, která prochází vývojem[11]. Je k dispozici 5 verzí Alpha a 2 verze Beta. Poslední dostupná verze je FreeIPA v2 Beta 2 (2.0.0.pre2), kde hlavní vlastnosti jsou:

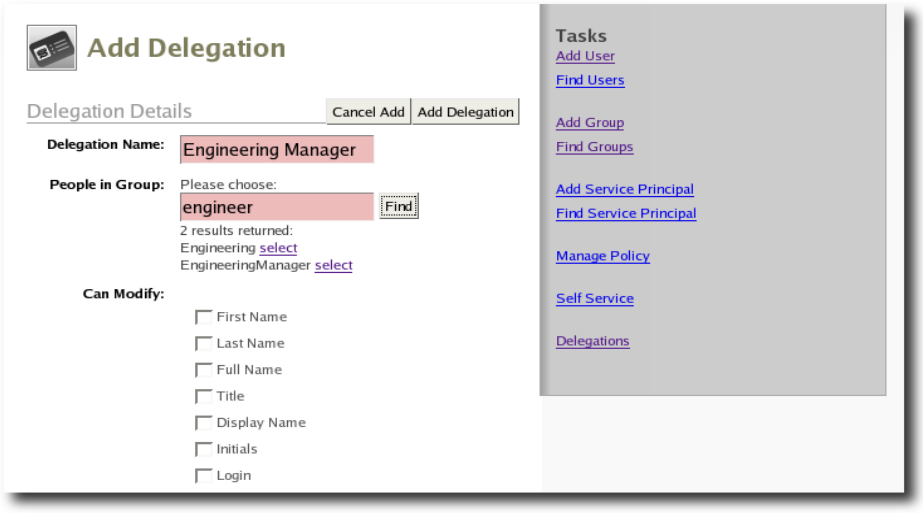
- Podpora posledních Dogtag balíčků.
- Fixace chyb
- Změny v DIT struktuře.
- Lepší inicializace a vypínání.
- Zlepšení replikace.
- Přidáno zlepšení v podporování IPv6.
- DNS zlepšení.
- Název balíku byl změněn na "freeipa", aby se předešlo kolizím s IPA v1.x a ostatními.

Již nyní jsou představeny hlavní vlastnosti připravované verze 2, která bude mimo jiné obsahovat tyto nové komponenty:

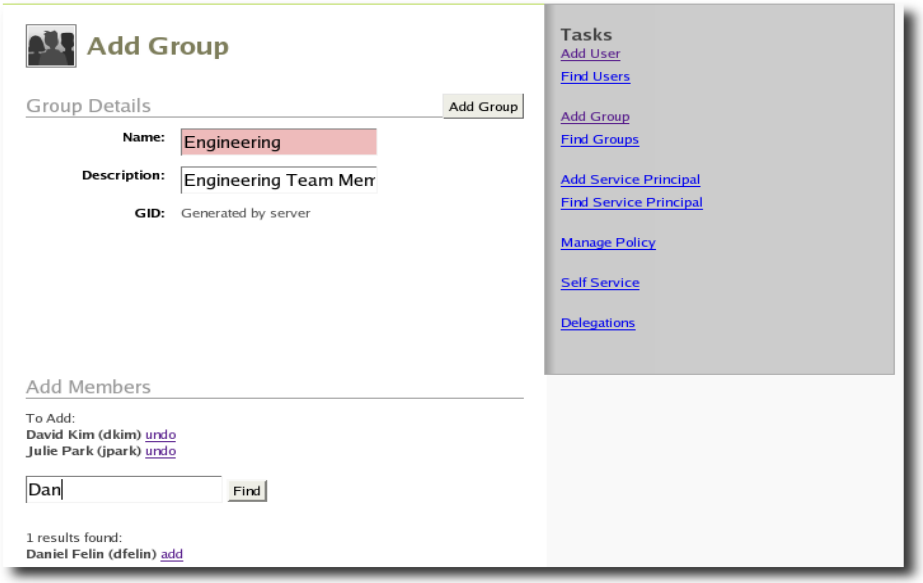
- Certifikační autorita podpora protokolu FreeRadius
- Centrální správa Kerberos principálů služeb
- Centrální auditovaní bezpečnostních událostí
- Centrální správa bezpečnostních politik

[11] Na internetových stránkách je přehled všech verzí http://www.freeipa.org/page/Main_Page

Ukázka prostředí (http://freeipa.org/docs/2.0.0/Administration_Guide/en-US/html/**):**



Obrázek 10: Přidávání delegáta



Obrázek 11: Přidání skupiny

Cíl firmy IPS je v prostředí Linuxu a Unixu jednoduše centrálně řídit identity, oprávnění a audit (jednoho dne). Samozřejmě, že firma má ambice pro vytvoření stejného nástroje pro Windows a mnoho dalších.

5.1.2 Samba

Samba původně vznikla jako volná implementace protokolu pro sdílení souborů a tiskáren SMB používaného společností Microsoft, díky čemuž i stanice postavené na OS Linux mohly přistupovat ke zdrojům poskytovaným servery v doménách Windows NT. Vývoj Samby probíhá od roku 1992. Stabilní verze číslo 3. Od 23. Ledna 2011 je k dispozici její nejaktuálnější podoba, kterou je verze 3. 4. 11.

Samba je důležitá komponenta k bezproblémovému integrování Linux/Unix serverů a desktopů do prostředí Active Directory[12], k tomu používá winbind démona (program, který je spuštěn dlouhodobě a není v přímém kontaktu s uživatelem, vyčkává v nečinnosti na nějakou událost, kterou obslouží a zajistí požadovaný úkol bez nutnosti interakce s uživatelem). Zjednodušeně řečeno je Samba sada programů, které umožňují součinnost mezi Linux/Unix servery a Windows klienty. Projekt Samba implementuje následující mechanismy:

- NetBIOS – jmenný protokol
- SMB – protokol pro sdílení souborů a tiskáren v sítích Microsoft
- CIFS – rozšíření protokolu SMB
- DCE/RPC (Distributed Computing Environment / Remote Procedure Call) – protokol pro vzdálené volání funkcí umožňující pracovat se vzdálenými systémy
- WINS Server (Windows Internet Name Service) – server přidělující NetBios jména
- NT Domain Suite – sada protokolů pro autentizaci a autorizaci

[12] Implementace adresářových služeb LDAP (definovaný protokol pro ukládání a přístup k datům na adresářovém serveru. Podle tohoto protokolu jsou jednotlivé položky na serveru ukládány formou záznamů a uspořádány do stromové struktury) firmou Microsoft pro použití v prostředí systému Microsoft Windows. Active Directory umožňuje administrátorům nastavovat politiku, instalovat programy na více počítačů nebo aplikovat kritické aktualizace v celé organizační struktuře. Své informace ukládá v centrální organizované databázi.

5.1.5 Josso

Josso neboli Java Open Single Sign-On řešení pro webové aplikace. Jedná se o open source J2EE[13] s cílem poskytovat řešení pro centralizovanou, platformou nezávislou, uživatelskou autentizaci a autorizaci.

Hlavní vlastnosti:

- SAML podpora pro bezproblémové Internetové/Federalizované SSO zkušenosti
- Framework povolující implementaci uživatelské identity komponentami využívající Spring nebo zabudovaný IoC container.
- Běžící v Apache Tomcat, JBoss aplikační server, BEA WebLogic 8, 9, 10, Websphere CE aplikační server, Apache Geronimo aplikační server, Windows IIS jako ISAPI konektor, JASPI-kompatibilní (JSR196) container jako JBoss 5 a GlassFish
- Kompatibilita s Liferay Portal, JBoss Portal, JBoss GateIn Portal, Alfresco CMS, OpenCMS, Wavemaker and phpBB
- Integrace se Spring Security pro umožnění tzv. „fine-grained“ autorizace.
- Poskytuje identity informace do Webové aplikace a EJB skrze standardní Servlet a EJB bezpečnostní API.
- Podporuje silnou autorizaci využívající X. 509 (klientský certifikát).
- Windows autorizace
- LDAP podpora pro ukládání informací a ověřovacích údajů uživatele.
- Podpora "Pamatování" a resetování hesla
- Client API pro PHP. To umožňuje budování SSO v PHP aplikacích.
- Client API pro Microsoft ASP. To umožňuje budování SSO v ASP aplikacích
- Standard Based: JAAS, Web Services/SOAP, EJB, Struts, Servlet/JSP, J2EE.

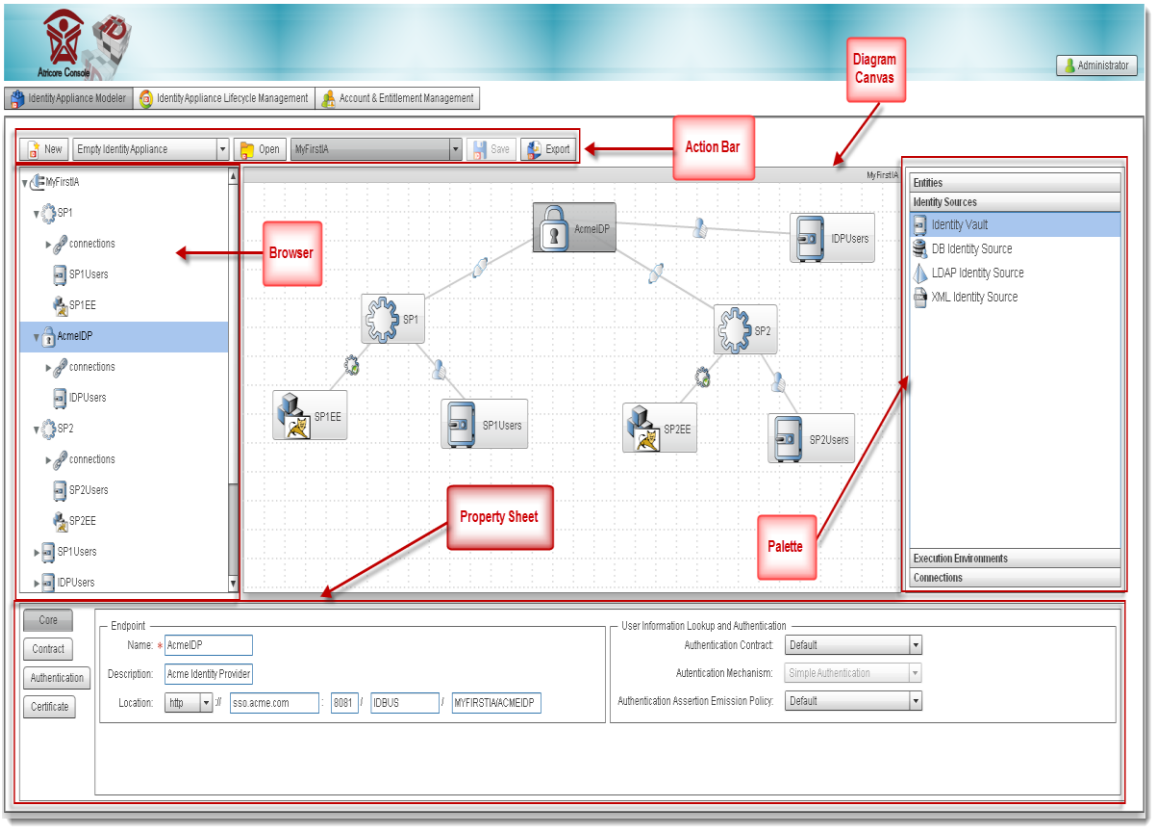
[13] Java 2 Enterprise Edition jedná se o přístup (sadu pravidel, technologií, metod, doporučení), jak provádět design, vývoj, nasazení a provozování vícevrstvých aplikací pomocí jazyka Java formou několika základních komponent. Patří sem: Platforma J2EE, Soubor testů kompatibility J2EE, Referenční implementace J2EE, J2EE BluePrints.

JOSSO v současnosti nabízí dvě generace produktu. Druhá generace[14] nabízí řešení, které je tzv. „all-in-one“. To umožňuje koncové doručení Internetové/Federativní SSO nastavení, vybudovaného pouze na model-driven přístupu pro snížení vstupních bariér a zkrácení trvání. Jestliže máte raději standardy a kontrolované zabezpečení a hledáte implementaci v out-of-the-box zkušenostech s nízkým zahrnutím od IT, JOSSO2 pro vás bude ta správná volba.

JOSSO1 využijete, jestliže máte více zákaznických scénářů, např. vyžadujete zavádění SSO plug-inu. Neortodoxní zdroje identit, nebo autentifikační mechanismus. Krom toho, budete mít větší šanci získat zdarma podporu.

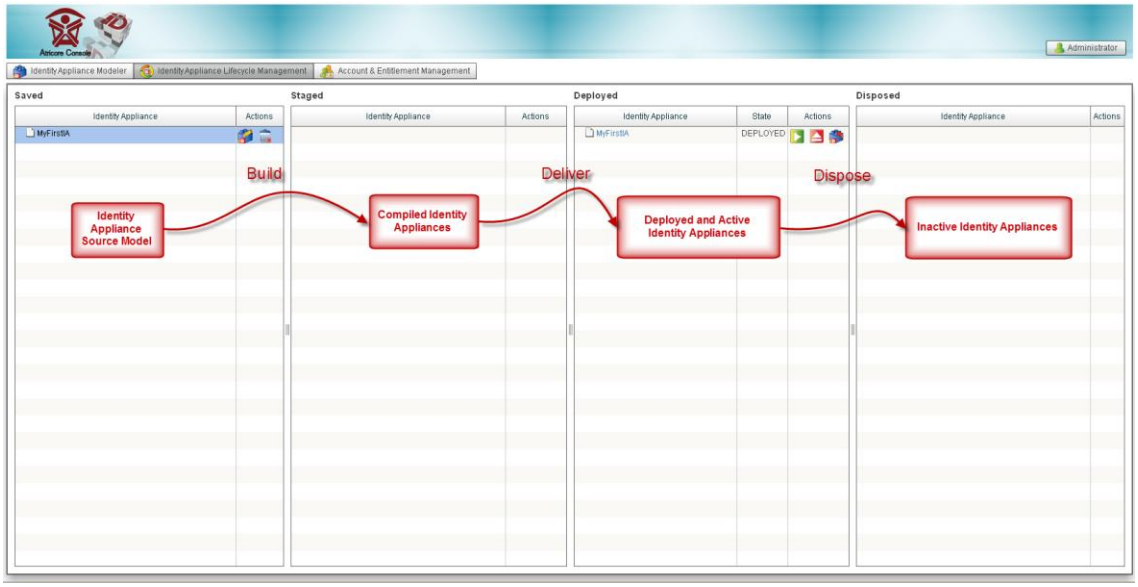
Ukázky prostředí JOSSO2:

http://www.josso.org/confluence/display/JOSSO1/JOSSO2+Birds-eye+View



Obrázek 12: Identity Appliance Modeler

[14] Detailněji se lze seznámit s druhou generací na internetových stránkách, kde je k dispozici tutorial: http://www.josso.org/confluence/display/JOSSO1/Video+Tutorial+-+Internet+SSO+Rollout+using+JOSSO2



Obrázek 13: Identity Appliance Lifecycle Management

5.2 Komerční systémy

Komerční software je takový software, za jehož užívání se musí tvůrci zaplatit. Často je také omezen počtem licencí, instalací, přenositelnosti licence nebo práva modifikací produktu. V této části představíme komerčně využívaný software. Poté navážeme další kapitolou, kde si vybereme jeden software. Ten detailněji popíšeme. Zaměříme se na procesní a technologickou stránku.

5.2.1 Novell identity manager

Firma Novell představuje své řešení pro poskytování a správu uživatelských účtů Novell Identity Manager pomáhá zákazníkům snižovat náklady na nasazení a správu uživatelských účtů v sítích organizací, zjednodušit složité přidělování účtů, bezpečněji spravovat role uživatelů a udržovat shodu s příslušnými předpisy. Novell Identity Manager nabízí vysoký stupeň integrace s ostatními řešeními Novellu pro ověřování uživatelů, jediné přihlášení k síti, sdílení bezpečnostních informací a monitorování bezpečnostních událostí. Identity Manager obsahuje flexibilní nástroje, jako vyspělé vizuální modelování, funkce pro návrh pracovního postupu a možnosti obsluhy uživatelem, které pomáhají snížit administrativní zátěž spojenou se zadáváním, aktualizacemi a odstraňováním uživatelských informací napříč heterogenními systémy organizací.

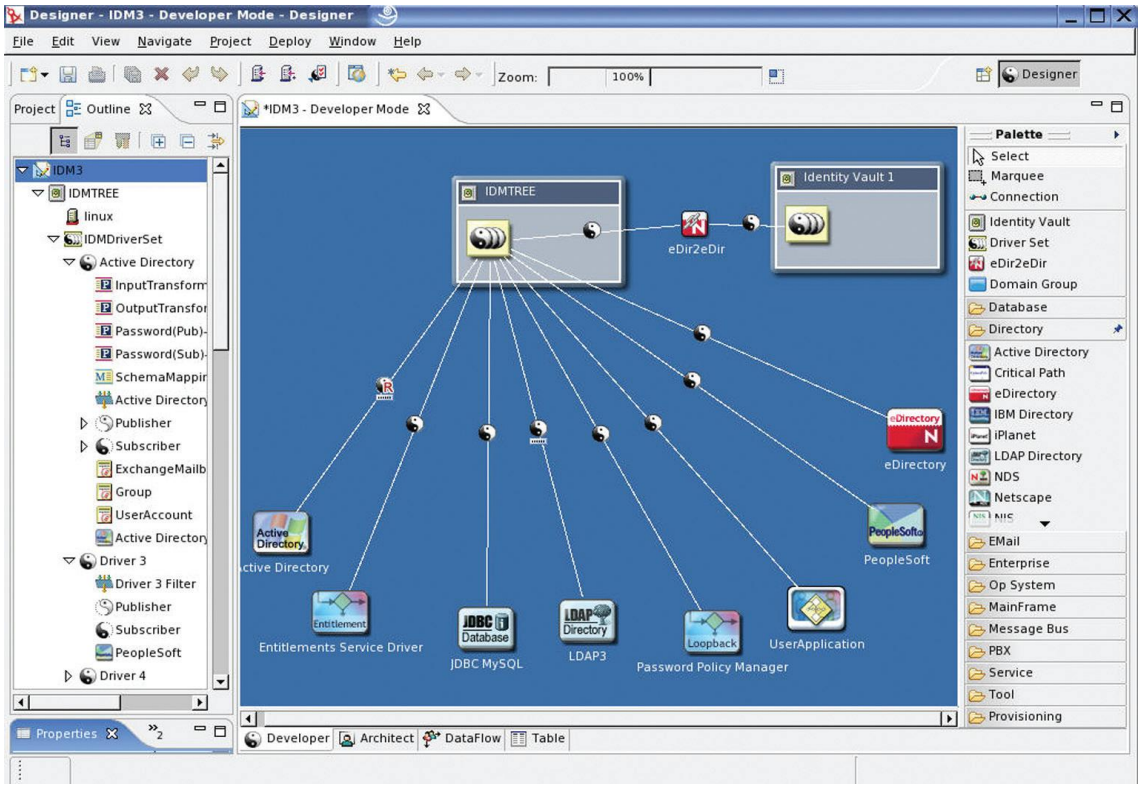
Hlavní přednosti řešení Novell Identity Manager:

1. Jednoduché a rychlé poskytování uživatelských účtů – Novell Identity Manager zajistí všem uživatelům přístup k aplikacím a službám v síti, které potřebují ke své práci.
2. Samoobslužné funkce pro uživatele – Operace, které snadno zvládne i běžný uživatel (jako např. změna hesla), není nutné řešit s asistencí helpdesku.
3. Snadný návrh politik a pravidel – Vizuální nástroje pro design, ladění a zavádění systémů řízení identit s intuitivním rozhraním dávají možnost kompletního náhledu a odzkoušení systému řízení identit před jeho implementací do sítě.
4. Široká kompatibilita – Díky rozsáhlé sadě ovladačů spolupracuje Novell Identity Manager se všemi běžně používanými podnikovými aplikacemi od různých výrobců.
5. Sjednocení identit – Novell Identity Manager sjednotí všechny digitální identity uživatele ve všech používaných systémech v organizaci. Jakákoliv změna v identitě je automaticky propagována do všech souvisejících systémů. [Novell: Worldwide, 2011]

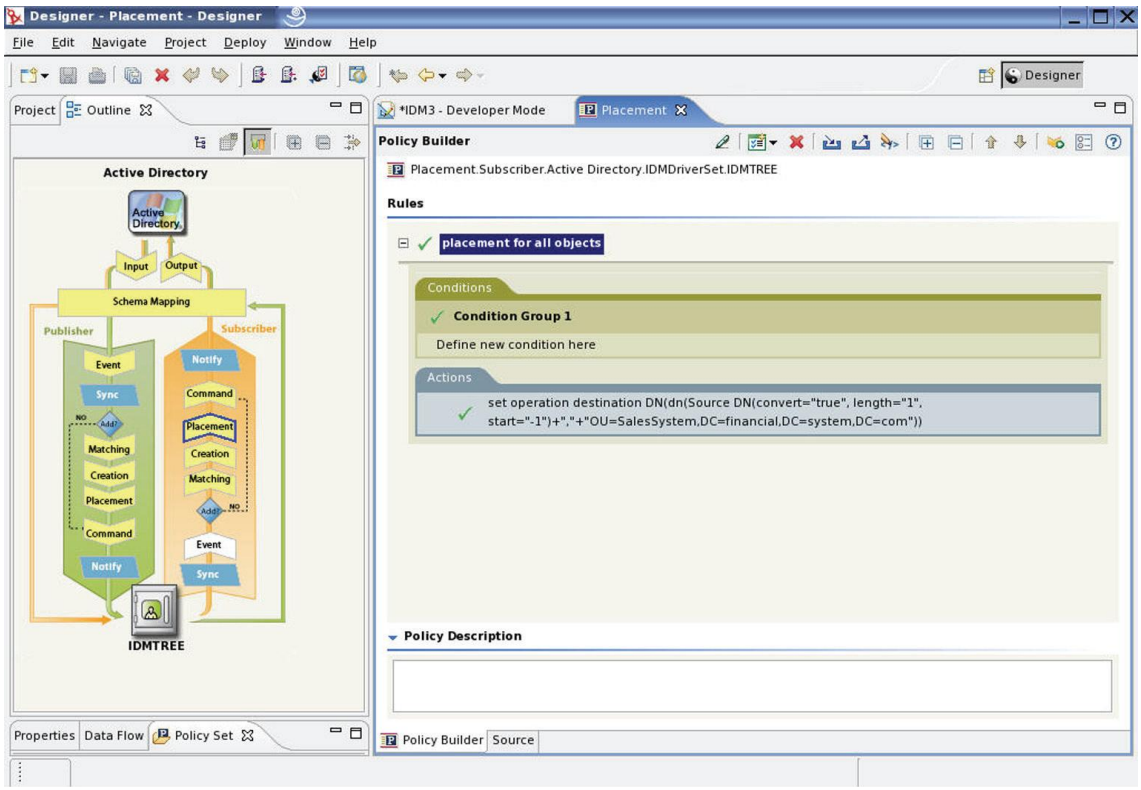
Ron Cook jako Vice prezident pro strategii a technické operace RadioShack[15] vyzdvihuje: „Řešení od Novellu je u nás z mnoha hledisek základním projektem. Vyhovělo našim bezprostředním potřebám připravovaných online výnosů a je skutečnou základnou pro řešení bezpečné správy identit v rámci všech našich prodejen.“ Novel Identity Manager prošel a prochází vývojem stejně jako konkurenční produkty. Jak informuje společnost, tak produkt byl prověřen ve významných společnostech po celém světě, včetně Gateway, zmíněný RadioShack, Allianz Suisse, Lufthansa a TRW.

[15] Firma zabývající se prodejem elektroniky ve Spojených státech, částech Evropy, Jižní Ameriky a Afriky. Má přes 34 700 zaměstnanců. V roce 2010 vykázala firma čisté tržby a provozní výnosy 4,81 miliard dolarů.

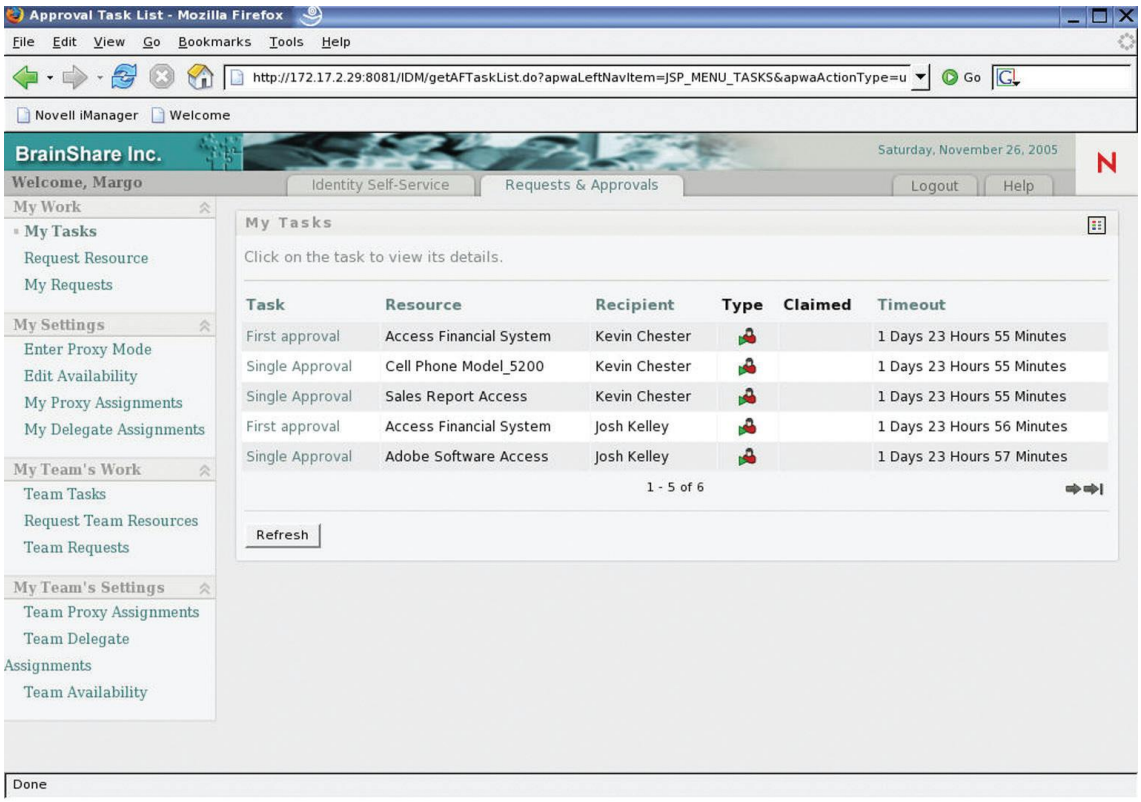
Ukázky prostředí Novell Identity Manager 3.6.1:



Obrázek 14: Vizuální modelování s nástrojem Designer for Identity Manager



Obrázek 15: Konfigurace politik Identity Manageru



Obrázek 16: Pohled na toky úkolů uživatele

V současné době je nejnovější verze 3.6.1, do nedávna byla používaná verze Novell Identity Manager 3.5. Oproti předchozím verzím (Novell Identity Manager 2.0, 3.0) došlo ke zdokonalení nových funkcí. Viz tabulka číslo 2. Je zde patrné, že došlo k velkému posunu aplikace. Je to dáno zejména konkurenčním prostředím, které panuje na trhu. Obrovská výhodou je, že s každou novou verzí je možné získat nové zákazníky a držet krok s konkurencí. Stejně tak i nová verze Identity manageru je zpravidla implementovaná (upgradovaná) k již stávajícím zákazníkům.

Za velkou zajímavost považuji, že firma Novell přichází na trh s novou verzí Identity Manageru, verze 4[16]. Uvedení pro komerční sféru se plánuje na září 2011.

[16] Demoverze IDM4 ke zhlédnutí na http://www.novell.com/products/identitymanager/demo.html

Funkce	IDM 2.0	IDM 3.0	IDM 3.5
Obousměrný proces obsluhy řízený událostmi	●	●	●
Politika založená na XSLT	●	●	●
Webové uživatelské rozhraní Novell iManager	●	●	▲
Reporty a oznamování	●	●	▲
Driver služby Workfl ow Request	●	●	●
Grafický nástroj Policy Builder a Novell DirXML® Script	●	●	▲
Správa hesel	●	●	▲
Bílé stránky a samoobslužné činnosti	●	●	▲
Reporty, logování a oznamování pomocí Novell Auditu	●	●	●
Oprávnění založená na rolích	●	●	●
Podpora doplňkových platforem	●	●	●
Zjednodušená instalace	●	●	▲
Zdokonalené uživatelské rozhraní pro správu	●	●	▲
Nástroj pro práci s verzemi	●	●	●
Vzorové reporty Auditu	●	●	●
Integrované schvalování toku úkolů	●	●	▲
Zdokonalené aplikace pro identity		●	▲
Atraktivní a pružný dodatkový produkt User Application		●	▲
Designer for Identity Manager		●	▲
Pokročilá škálovatelnost a bezpečnost dat		●	●
Podpora dalších jazyků		●	▲
Grafický Designer pro toky úkolů		●	●
Obsluha Secret Store Credential		●	▲
Samoobslužná registrace uživatelů		●	▲
Anonymní přístup			▲
Zdokonalená správa hesel zahrnující jejich plánované generování a kontrolu stavu synchronizace			▲
Aplikační programovací rozhraní pro webové služby toků úkolů a monitorování			▲
Podpora rolí: - pro organizace s maticovou a polyarchickou strukturou - dobře definované přípojné body pro integraci produktů třetích výrobců			▲
Plánování aktivit procesů obsluhy			▲
Plánovač prací			▲
Podpora synchronizace hesel pro drivery LDAP a Notes			▲
Oznamování synchronizace hesel			▲
Spojování skriptů ECMA a zdokonalených politik			▲

Tabulka 2: Porovnání jednotlivých verzí IDM,
LEGENDA: ●Ano ▲ Nová/zdokonalená [Novell: Worldwide, 2011]

Jak říká Larry Walsh (Channel Insider), „dlouho jsem tvrdil, že nejlepší pro bezpečné uchovávání dat je řešení od Novellu. Dnes Novell odhodil roušku tajemství a zveřejnil - Identity Manager 4 – které je opravdu unikátní ve dvou ohledech: Je nadesignován pro řízení identit na tzv. on-premises, poskytuje virtuální infrastrukturu a cloudové aplikace; a to integruje kmenový (log) a událostní (event) management pro posílení pravidel (policy enforcement) a auditu.

IDM 4 bude k dispozici ve dvou verzích. Jedna verze bude standardní, ta bude rozšiřovat možnosti řešení verze 3.6.1. Tím, že vylepší škálovatelnost a těsnou integraci se systémy Microsoft SharePoint, SAP ERP (Enterprise Resource Planning) a cloudovými aplikacemi Salesforce.com a Google Apps. Nabízí rovněž hotové funkce pro generování výkazů a nástroje pro čištění dat a návrh rámce zásad. Druhá verze bude nabízet pokročilé funkce. Novell Identity Manager 4 Advanced Edition nově definuje podnikové funkce poskytování uživatelských účtů, neboť integruje sofistikovanou správu rolí, vyspělé funkce pracovního toku a inteligentní reportovací funkce. Vyhoví těm nejnáročnějším potřebám velkých podniků a poskytovatelů spravovaných služeb v oblasti správy identit a shody s předpisy. Novell Identity Manager 4 Advanced Edition rovněž obsahuje nástroje pro čištění dat, návrh rámce zásad a možnost definovat role a oprávnění jednoduchým přetahováním myší, takže uživatel nemusí psát žádný kód.“ [Novell: Worldwide, 2011]

Tímto produktem se výrazně posílí pozice firmy Novell na trhu řešení v oblasti Identity managementu. Osobně si však nemyslím, že tímto produktem převezme klienty, které má konkurence. Velký potenciál vidím při oslovování nových klientů, kteří budou volit z nabízených alternativ na trhu.

5.2.2 Oracle identity mananager

Oracle Identity manager představuje kompletní, otevřené a integrované řešení. Nejnovější verzí softwaru od společnosti Oracle je Identity Manager verze 11g, které budoucím zákazníkům umožní efektivně plnit požadavky souladu, zabezpečit kritické aplikace, citlivá data a snížit provozní náklady. Podle oblasti působení nabízí své řešení (produkt). Např. Pro federační oblast slouží produkt Oracle Identity Federation, pro oblast ovládání identit a přístupů slouží Oracle Identity Analytics, pro řízení rolí Oracle Role Manager, pro informace o řízení přístupových práv nabízí produkt Oracle Information Rights Management, pro webové služby nabízí Web Services Manager. Oblast působení a konkrétní produkt zachycuje následující tabulka číslo 3.

Oblast	Oracle nabízí
Webový přístup	Oracle Access Manager
Risk-Based Access	Oracle Adaptive Access Manager
Role based User Provisioning	Oracle Identity Manager
Federation	Oracle Identity Federation
Identity and Access Governance	Oracle Identity Analytics
Virtual Directory	Oracle Directory Services Plus
Directory Server EE	Oracle Directory Services Plus
Internet Directory	Oracle Directory Services Plus
Role Management	Oracle Role Manager
Entitlements Management	Oracle Entitlements Server
Web Services	Oracle Web Services Manager
Enterprise SSO	Oracle Enterprise Single Sign-On Suite
Meta-Directory	Oracle Directory Integration Platform
Information Rights Management	Oracle Information Rights Management

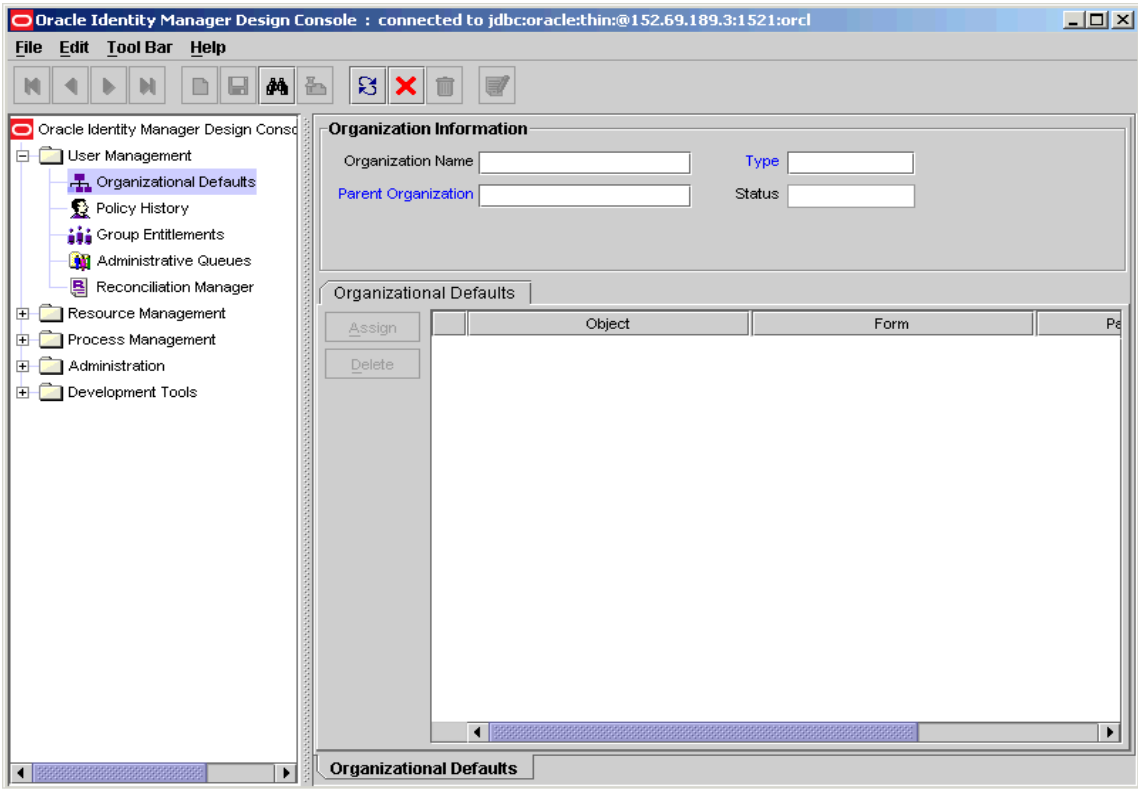
Tabulka 3: Oblast působení a řešení pomocí produktu [Oracle, c2011]

Oracle Identity Manager obsahuje všechny funkce uvedené v tabulce, to je velmi dobré pro budoucího zákazníka. Protože lze pokrýt (splnit) všechny jeho požadavky bez dodatečné úpravy produktu jako tomu je v ostatních konkurenčních firmách.

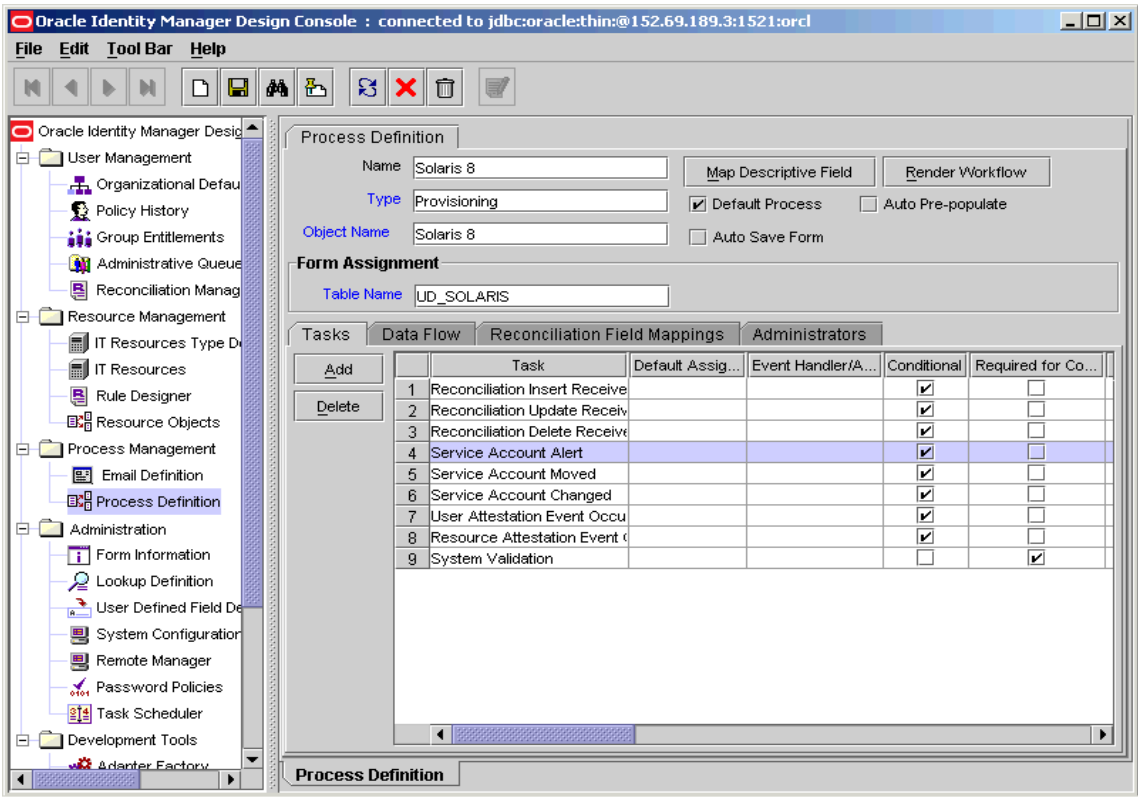
„Identity Manager 11 g přináší revoluční architekturu bezpečnosti, která je orientovaná na služby. Představuje první deklarativní bezpečnostní rámec v odvětví. Umožňuje vývojářům pohodlně integrovat prvky bezpečnosti do jejich aplikací, společnosti mohou urychlit vstup na trh a zvýšit obchodní efektivitu. Automatickým zaopatřením uživatelských účtů, dramaticky snižuje počet hovorů s oddělením podpory, zjednodušuje audit souladu a výkaznictví, konsolidaci sil identit, rychlou integraci s podnikovými aplikacemi a další.“ [Oracle, c2011]

Architektura bezpečnosti, která je orientovaná na služby (Service-Oriented Security), je v oblasti identity managementu revoluční. Jelikož dnešní aplikace musí splňovat celou řadu bezpečnostních požadavků, včetně autorizace, poskytování uživatelských účtů a federování, a soulad s průmyslovými standardy a předpisy. Vývojáři musí vzít v úvahu důsledky integrace těchto bezpečnostních složek nejen na základě žádosti, ale v rámci stávající bezpečnostní infrastruktury. Proto Oracle Identity Manager 11 g přináší Service-Oriented Security, který výrazně zjednodušuje zabezpečení aplikací tím, že bude funkce identit k dispozici jako diskrétní znovu použitelná webová služba. Toto umožňuje vývojářům provázat centralizovanou bezpečnostní infrastrukturu do aplikací namísto postupného přidávání komponent. Ve výsledku to vede k rychlejšímu rozvoji životních cyklů, lepší pružnosti IT a výraznému snížení nákladů. Jak to celé funguje? Shrnout to lze do třech částí, kde první je Identity function externalization, které umožňuje deklerativní připojení důležitých bezpečnostních artefaktů (autentizace, autorizace, audit a šifrování) přímo do aplikací, Service-Oriented Security umožňuje vývojářům oddělit bezpečnostní logiku od obchodní logiky aplikací. Toto urychlí vývojové cykly a firmám to umožní měnit politiku, aniž by bylo nutné zasahovat do aplikačního kódu. Druhou částí je Centralized policy administration (Centralizována správa politik) vývojáři mohou provazovat framework centralizované správy identit v aplikacích. Třetí částí je tzv. Run-time monitoring and audit (Monitorování a auditování za běhu (v čase)). Podniky tedy mohou účinněji kontrolovat zabezpečení, audit.

Ukázky prostředí Oracle Identity Manager:



Obrázek 17: Oracle Identity Manager design konzole

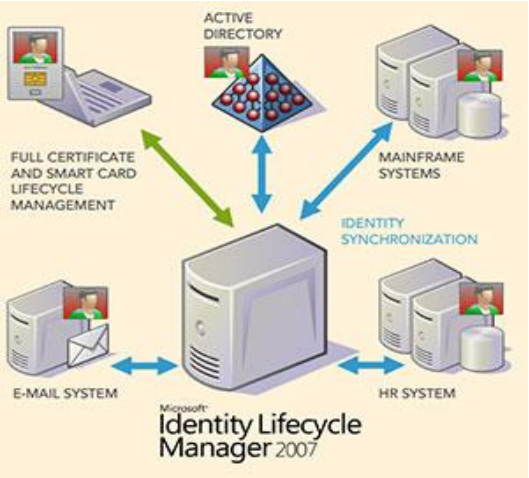


Obrázek 18: Oracle Identity Manager a ukázka prostředí

Firma Oracle stejně jako její konkurenti mají celosvětové pokrytí, za velmi úspěšné lze považovat práce pro společnost ING, SUNY, Verizon, Turkcell İletişim Hizmetleri A. Ş, radnice města Esbjerq, nemocniční okrsek Helsinky a Uusimaa. Všechny tyto společnosti zvýšily produktivitu, zabezpečení informačních technologií, snížily rizika a zabezpečení dat, včetně zisku. Detailnější popis vybraných projektů od společnosti Oracle je uveden v kapitole 6.2.

5.2.3 Microsoft Forefront Identity Manager 2010

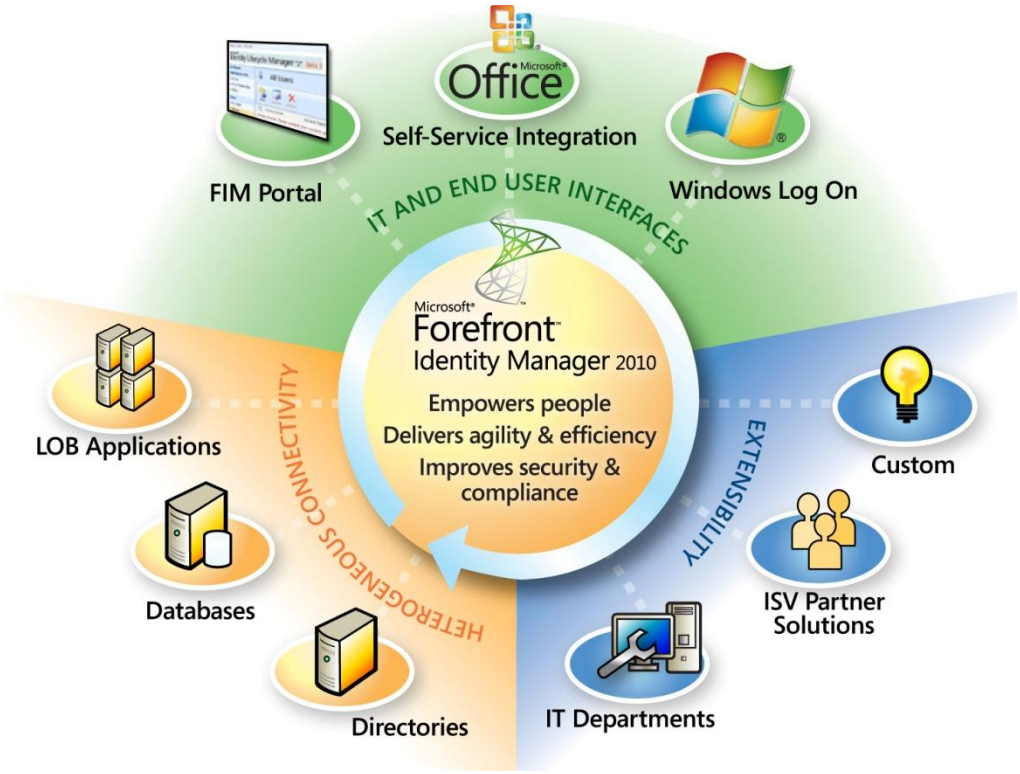
Microsoft Forefront Identity Manager (FIM) 2010 je ucelené řešení pro správu identit, pověření a zásad přístupu založených na identitách v rámci heterogenních IT prostředí. Tento produkt je nástupcem produktu Identity Lifecycle Manager 2007 (Princip na obrázku číslo 19). Na Americký trh byl uveden na konferenci RSA Conference 2010. Nesmírně zjednodušuje správu identit v rámci podniku a to tím, že využívá samoobslužné funkce pro koncové uživatele. Včetně nástrojů, které správcům IT umožňují automatizaci úloh.



Obrázek 19: Identity Lifecycle Manager [Microsoft Corporation, 2011]

Na konferenci RSA v roce 2010 firma Microsoft představila svůj nový produkt (viz obrázek č. 20, který je vysvětlen v následující citaci) a vyzdvihla jeho řešení. „FIM je důležitá část pro vytvoření obchodně zabezpečené strategie, která společnostem pomáhá řídit rizika a zplnomocňovat své pracovníky. Jedná se o základní součást našeho IAM řešení, jehož cílem je umožnit bezpečnější přístup k oběma on-site a cloud aplikací, prakticky z jakéhokoli místa nebo zařízení.

Celkově lze říci, že FIM má velkou cenu při neefektivnosti IM a pomáhá firmám zvýšit produktivitu zaměstnanců. Jakožto následník Lifecycle Manager 2007, výrazně zjednodušuje podnikovou správu identit prostřednictvím tzv. end-user samoobslužné funkce a administrátorské nástroje pro automatizaci úloh. To pomáhá společnostem spravovat uživatelské účty a přístup, hesla a identity politik v celých Windows a heterogenním prostředí. Krom toho FIM poskytuje základ pro vlastní řešení.



Obrázek 20: Originální popis FIM od Microsoftu [Microsoft Corporation, 2011]

První americká společnost, která se rozhodla použít FIM je pojišťovna. Ta pomocí tohoto řešení automatizuje poskytování a přístupy pro 14.000 zaměstnanců. Ve výsledku je společnost schopná pomáhat zaměstnancům. Snadněji se dostanou k informacím a aplikacím, které právě potřebují, zlepšil se i vnitřní audit a samozřejmě klesnul počet telefonátu na help desk. Předpokládané roční úspory jsou 66.000 dolarů.“ [Technet, 2010]

Ukázka prostředí:

Obrázek 21: Ukázka prostředí Microsoft FIM 2010

Jedná se o kvalitní software, kdy Microsoft říká, že je schopen zprovoznit základní verzi u zákazníka do 14 dnů. Toto je velmi zajímává informace, jelikož implementace ostatních firem trvají velmi dlouho. Ale jak bylo napsáno dříve, vše závisí na spolupráci se zadavatelskou firmou (vymyslet co nejpřesnější role, přístupy, usnadnit připojení cílových systému). V kapitole 6.2.3 budou popsány vybrané úspěšné projekty od firmy Microsoft.

5.2.4 IBM Tivoli Identity Manager

Tento software bude detailněji popsán v praktické části (Kapitola 6.1 IBM Tivoli Identity Manager).

5.2.5 Sun Identity Manager

Po dlouholetém partnerství firmy Oracle a Sun Microsystems se firma Oracle rozhodla koupit firmu Sun. A 20. Dubna 2009 zveřejnila, že za jednu akcii zaplatí 9,5 dolarů. Celkově tedy za celou firmu bylo zaplaceno 7, 4 miliardy dolarů. V roce 2009 to byla revoluční zpráva. Protože firma Sun jednala o spojení s počítačovou společností IBM. Jednání bohužel pro firmu IBM skončilo na ceně, kdy nabídly méně (kolem 7 miliard dolarů). Spojení přineslo i změnu v identity management systému, kdy firma Oracle posílila přední nabídku správy identit v odvětví.

„Zakoupení společnosti Sun společností Oracle dále posiluje přední nabídku správy identit v odvětví. Strategií společnosti Oracle je nabízet integrovanou řadu produktů Identity Managemenent, která kombinuje nejlepší produkty a schopnosti. Spojením sil dvou vůdčích společností v oblasti správy identit mohou zákazníci těžit ze zvýšených investic do výzkumu a vývoje, rychlých inovací, pokračující podpory otevřených standardů a mnohem většího ekosystému nezávislých prodejců softwarů, partnerů v integraci systémů a koncových uživatelů. Zákazníci produktu Sun Identity Management mají záruku, že jejich investice budou chráněny pokračující údržbou a nebudou nutné žádné migrace.“ [Oracle, c2011]

Část II.

Praktická část

6 Implementace v praxi

V této kapitole je detailněji představen produkt IBM Tivoli Identity Manager. Je zde vysvětlen a schematicky přiblížen technologický a procesní princip. Pro názornou ukázku seznamuje s prací administrátora. A to formou vymyšleného příkladu (Nezáleží na verzi softwaru, princip je stejný!). Kde krok za krokem je vysvětlen postup od naimportování agenta, vytvoření skupin, politik, po založení uživatele s automatickým přístupem do systému na základě přidělené role. Tento postup lze použít jako administrátorskou příručku. Druhá část této kapitoly je věnována testování self-reset password. Cílem je ukázat, že pro budoucí uživatele to není žádný problém. Testování je řešeno krok za krokem a opět lze použít i jako uživatelská příručka. V třetí části této kapitoly jsou představeny úspěšné projekty vybraných dodavatelských firem.

6.1 IBM Tivoli Identity Manager

IBM Tivoli Identity Manager je také známý pod svou zkratkou ITIM. Jeho funkce se dá zkráceně popsat jako snadné automatizování řízení životního cyklu uživatelských rolí, identit a přístupových práv. Tento software pro správu identit je zabezpečené a automatizované řešení založené na zásadách, které je určeno pro správu uživatelských oprávnění používaných pro prostředky heterogenního informačního systému.
Firma IBM shrnuje výhody následovně:

1. Pomáhá posílit vaši správu uživatelských přístupů o komplexní zajišťování založené na požadavcích. Je schopno zajišťovat požadavky a schvalování uživatelského přístupu k rolím, účtům či přesně stanoveným přístupovým nárokům, např. ke sdíleným složkám či webovým portletům.
2. Disponuje optimalizovaným samoobslužným rozhraním pro uživatele, jehož vzhled a celkovou grafickou koncepci lze snadno přizpůsobit potřebám vaší organizace, optimalizovat je pro konkrétní typy uživatelů (auditoři, vedoucí, pracovníci podpory atd.) a integrovat je s podnikovými portály.
3. Zahrnuje vylepšenou opětovnou certifikaci přístupových práv, jež poskytuje přesnější a pro potřeby auditorů přizpůsobené podrobnosti pro dodržování

předpisů, jakož i zásady, které lze snadno konfigurovat pomocí průvodců a šablon.

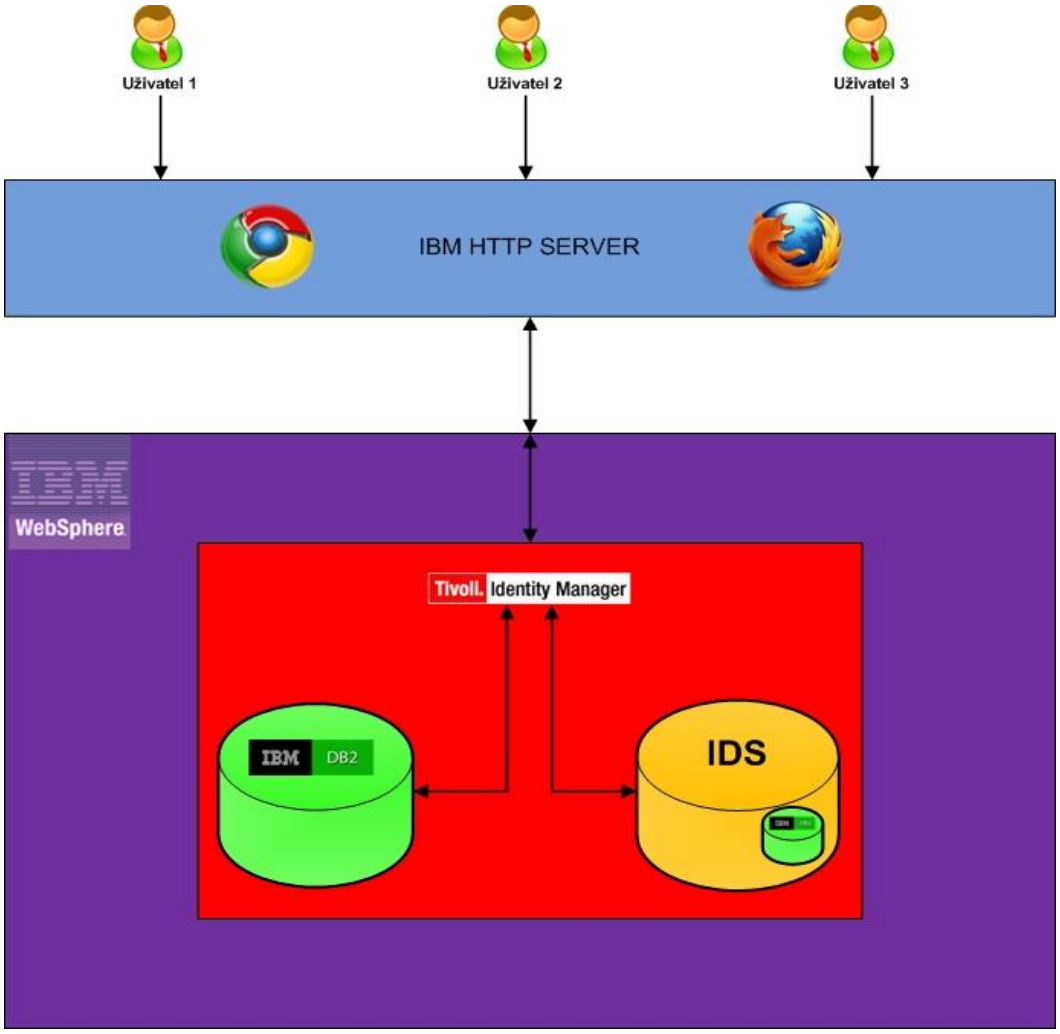
4. Poskytuje zásady, které lze snadno konfigurovat pomocí průvodců a šablon, jež jsou součástí softwarového balíku správy identit.
5. Poskytuje režim "pouze pro čtení" určený pro auditory, nově navrženou konzolu pro správu, další sestavy související s vykazováním dodržování předpisů, nástroj pro vytváření vlastních sestav a integraci s produktem Tivoli Compliance Insight Manager pro vytváření sestav pro účely auditu, které korespondují s předpisy a optimálními postupy.
6. Díky použití optimálních postupů urychluje vývoj a snižuje nároky na školení nových uživatelů. [IBM, 2011]

Proč zrovna firma IBM?

Z dlouhodobého hlediska je firma IBM považovaná za lídra v řešeních IM. IBM investuje každoročně víc jako 50 milionů dolarů na výzkum a vývoj v oblasti IM. Je to silná a stabilní technologická společnost, která může dodávat a podporovat svoje řešení a produkty v dlouhém časovém období. IBM má dostatek významných referencí a zkušeností s IM ve světě a v Evropě.

6.1.1 Technologický princip

Technologický princip aplikace ITIM vysvětlíme pomoci následujícího obrázku číslo 11. ITIM a všechny jeho součásti pracují pod WebSphere Aplication Serverem (WAS). Tento aplikační server pomáhá zvyšovat akceschopnost podniků tím, že vývojářům a architektům IT poskytuje pokrokovou na výkon zaměřenou základnu k sestavování, opakovanému využití, integraci a správě aplikací a služeb architektury SOA (Service Oriented Architecture). SOA určuje mantinely pro architekturu aplikace, anebo její části. WAS podporuje operační systémy různých platforem (AIX, HP Unix, i family, Linux, Sun Solaris, Windows, z/OS).



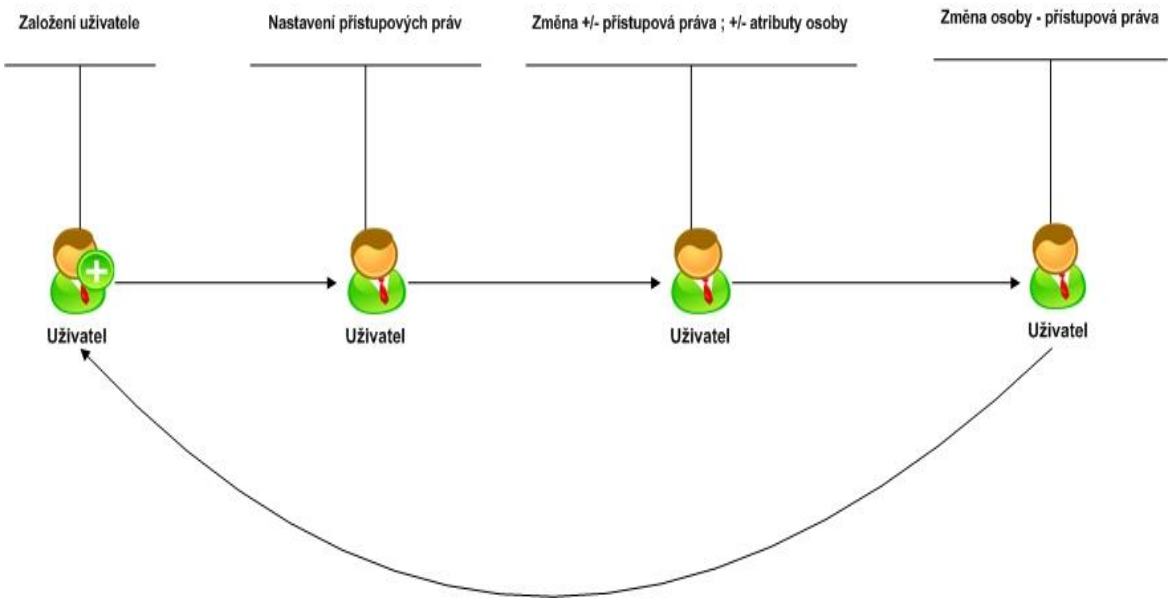
Obrázek 22: Technologický princip aplikace ITIM.

Koncový uživatel se připojuje přes libovolný prohlížeč (Firefox Mozilla, Google Chrome, Internet Explorer, Opera aj.) na IBM HTTP server. Aplikace ITIM využívá pro svou činnost dvě databáze. První databáze je **statická**, jedná se o IBM Directory Server[17] (částečně pro svou funkci používá databázi DB2). Tato databáze má funkci jako úložiště dat. Druhá databáze je **procesní.** Opět se jedná o produkt z firmy IBM, a to DB2 Universal Database. Slouží pro ukládání všech procesů v aplikaci ITIM.

[17] IDS je adresářový server, který umožňuje uchovávat různé typy dat. Nejlépe se optimalizuje pro data, jež nevyžadují časté aktualizace.

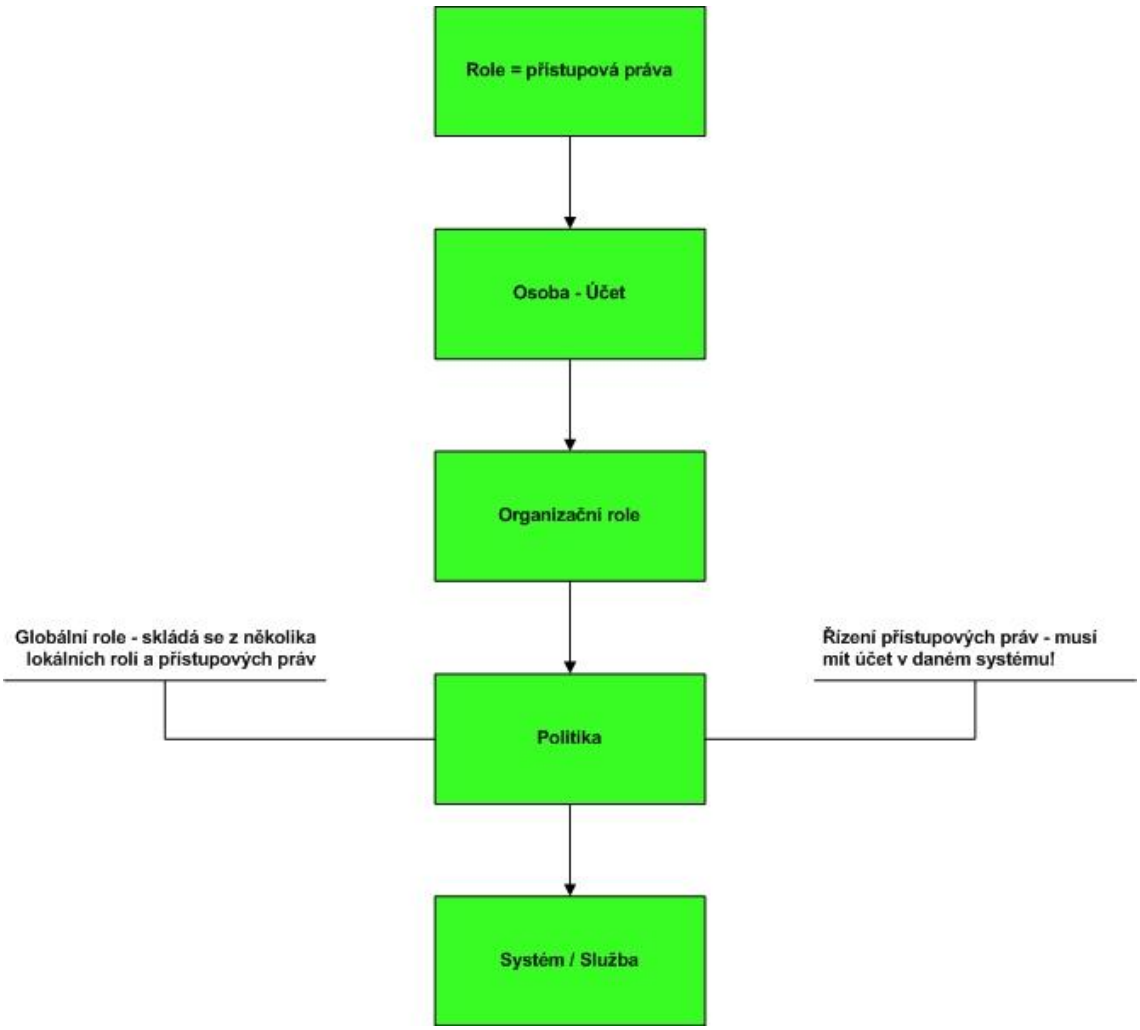
6.1.2 Procesní princip

ITIM je koncipován tak, že pracuje na principu RBAC (Role Based Access Control). Kde je vytvářen vztah mezi uživatelem a rolemi, ty mu přináleží. Uvnitř tedy pracuje s objekty. Role nám tedy dává právo na daný účet a přístupová práva. V aplikaci ITIM se nedá přidělit více schvalovatelů. Na obrázku číslo 12 je zachycen životní cyklus identity (jedná se o uživatele/člověka). Z obrázku vyčteme, že prvním krokem je založení uživatele, druhým krokem je přidělení přístupových práv. Třetím krokem se mohou stát různé modifikace účtů (odebrání/přidání přístupových práv nebo odebrání/přidání atributů osoby). Čtvrtým krokem je změna osoby, kterou rozumíme odebráním přístupových práv. Bez kterých nemá uživatel přístup.



Obrázek 23: Životní cyklus identity (uživatele/člověka). Osoba je začleněna do organizační skupiny.

Na obrázku číslo 13. je životní cyklus identity (uživatele/člověka) v aplikaci ITIM. Je zde i pojem, který nebyl doposud vysvětlen. Globální role představuje takovou roli, která se skládá z několika lokálních rolí a přístupových práv. Toto je nosnou myšlenkou správy identit. Globální účet můžeme přímo přiřadit konkrétnímu člověku a je nepřenosný. Pak nám již stačí přiřadit ke globálnímu účtu konkrétní účty z jednotlivých prostředí.



Obrázek 24: Životní cyklus identity (uživatele/člověka) v aplikaci ITIM.

6.1.3 Administrátorská příručka

V této části popisujeme základní administraci systému, formou zadání úkolů a postupného provázení řešením.

Service - Profil v ITIMu

Politika - Jsou jednotlivé skupiny v Active Directory

Organizační role (Globální role) - Např. Pokladník, Asistent

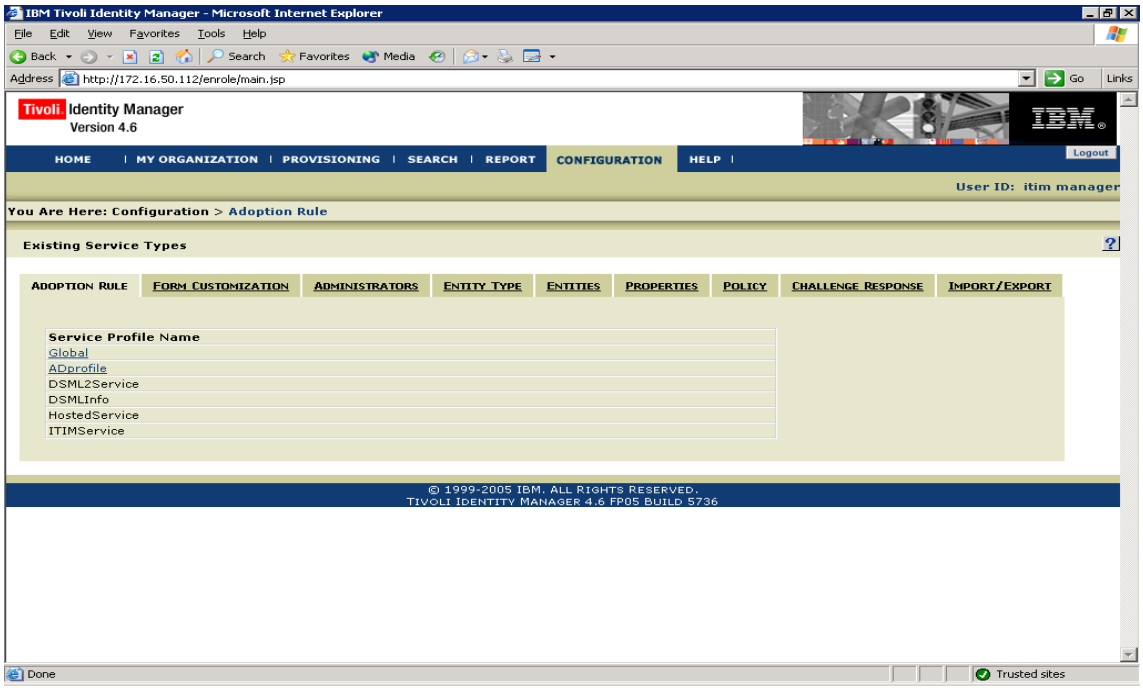
Zadání:

1. Naimportovat agenta Active Directory
2. Vytvořit skupiny v Active Directory – Office 2007, Kalkulačka, KBI, People Soft, CTS
3. Na základě skupin vytvořit Provisioning Policy
4. Vytvořit organizační role s přístupem dle tabulky č. 3.
5. Založení uživatele Jožko Mrkvička, jako IT-Specialistu s automatickým přístupem do systému, dle tabulky č. 3.

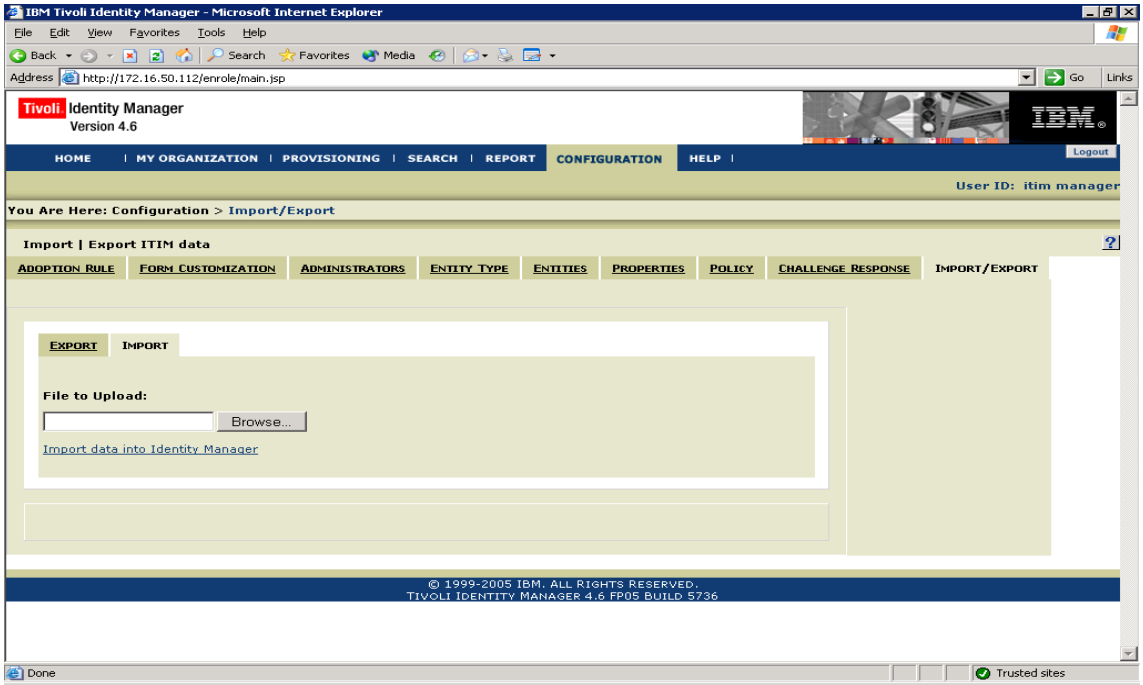
Role	Office 2007	Kalkulačka	Domain User	Account Operator	KBI	CTS
Asistent	X					
IT Specialista	X	X	X	X		
Pokladník		X	X		X	
Manager	X	X	X	X	X	X

Tabulka 4: Organizační role, X reprezentuje automatický přístup do daného systému

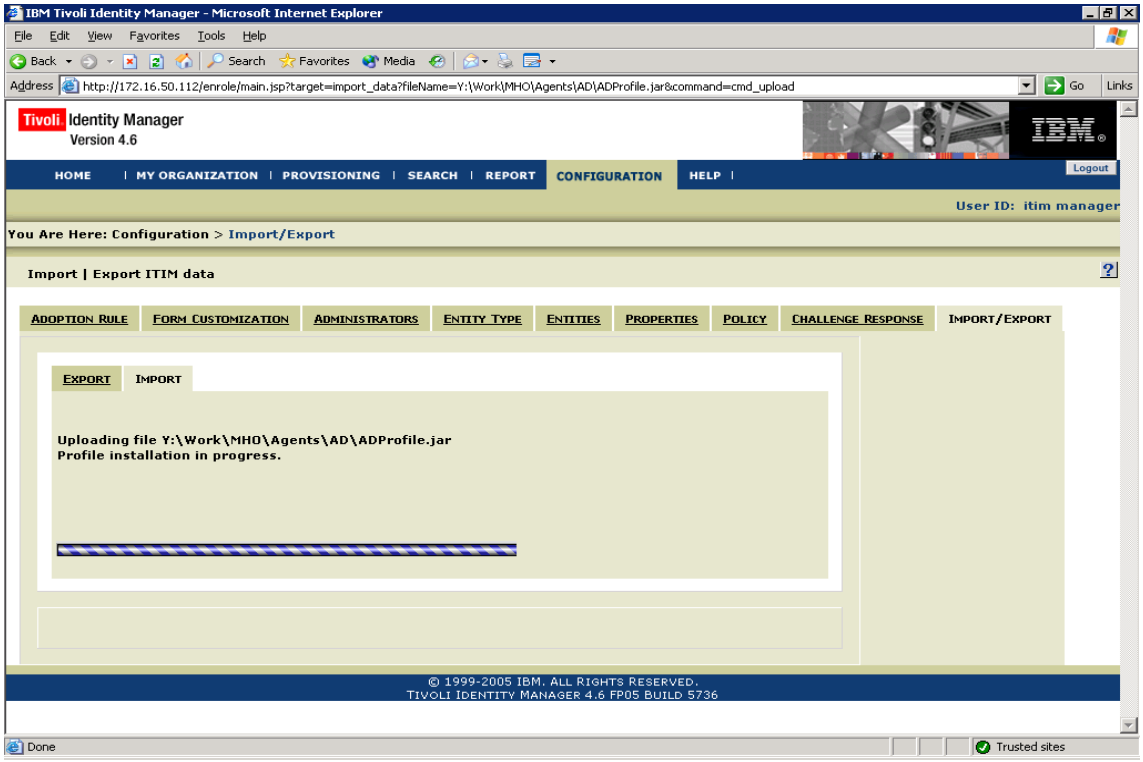
Active Directory – instalace a administrace



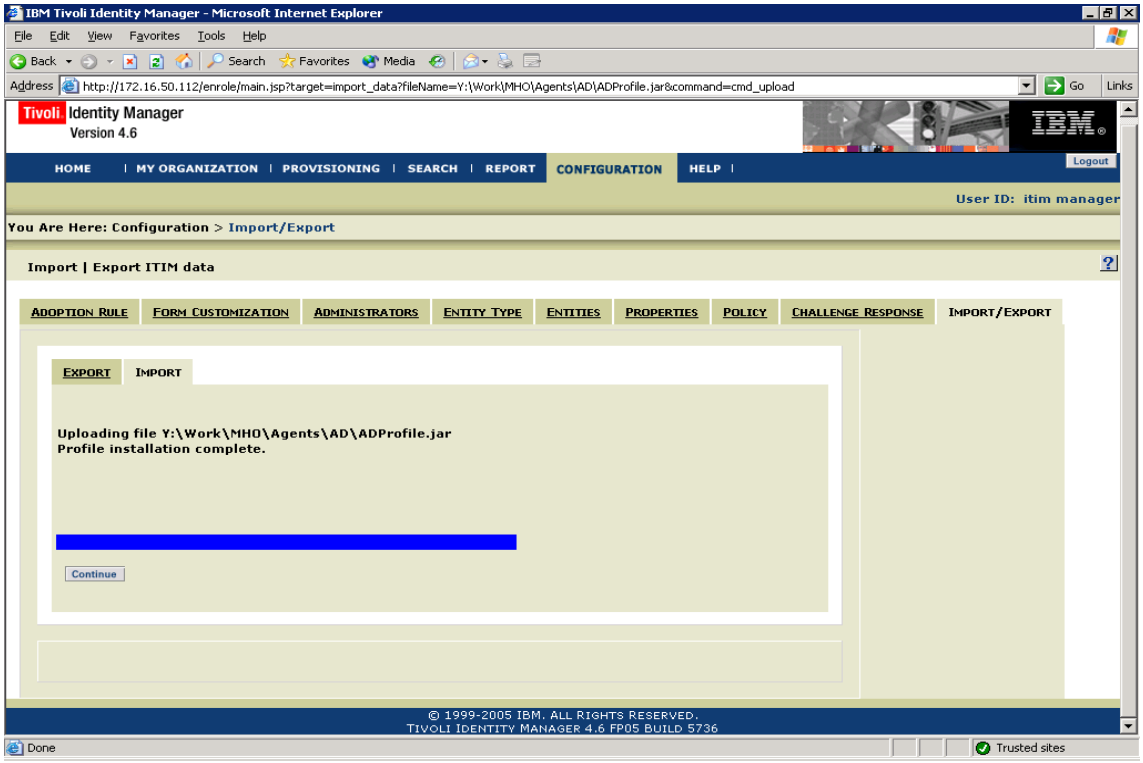
1. V hlavním panelu klikněte na **CONFIGURATION** a poté pokračujeme kliknutím na **IMPORT/ EXPORT**.



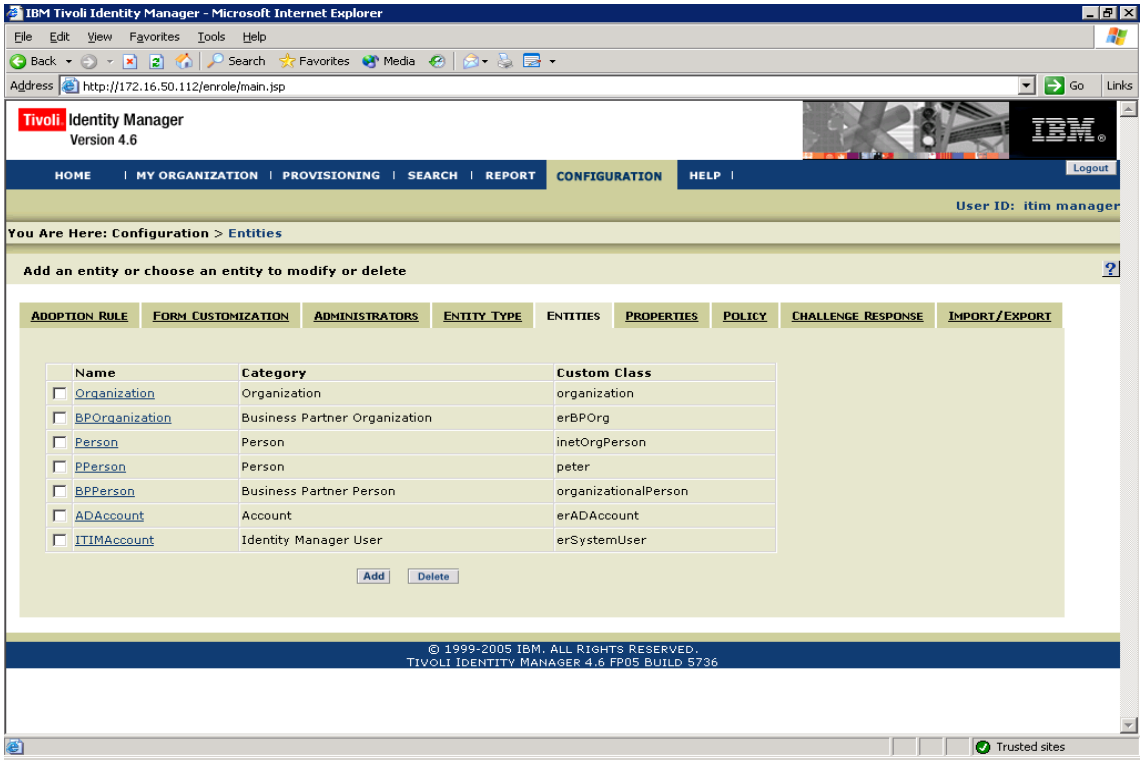
2. Pokračujte kliknutím na **IMPORT** a pomocí tlačítka **BROWSE** naimportujeme agenta **AD** (musí být ve formátu ***.jar**).



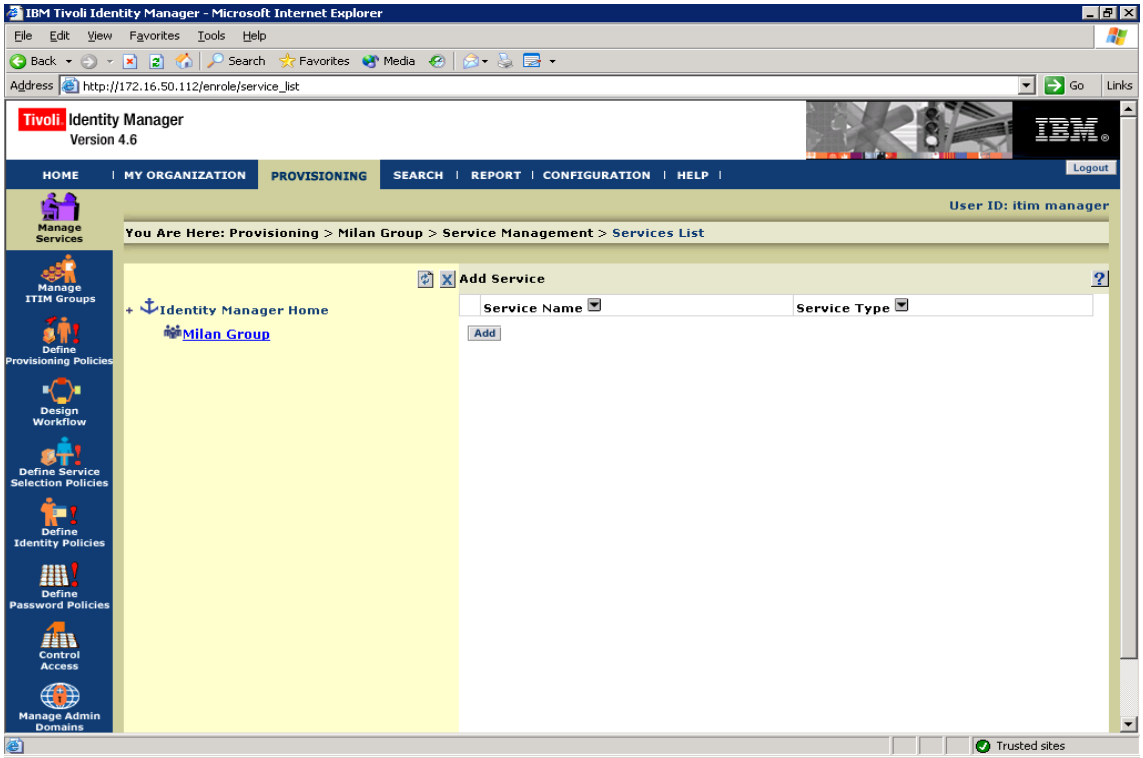
3. Načítají se data.



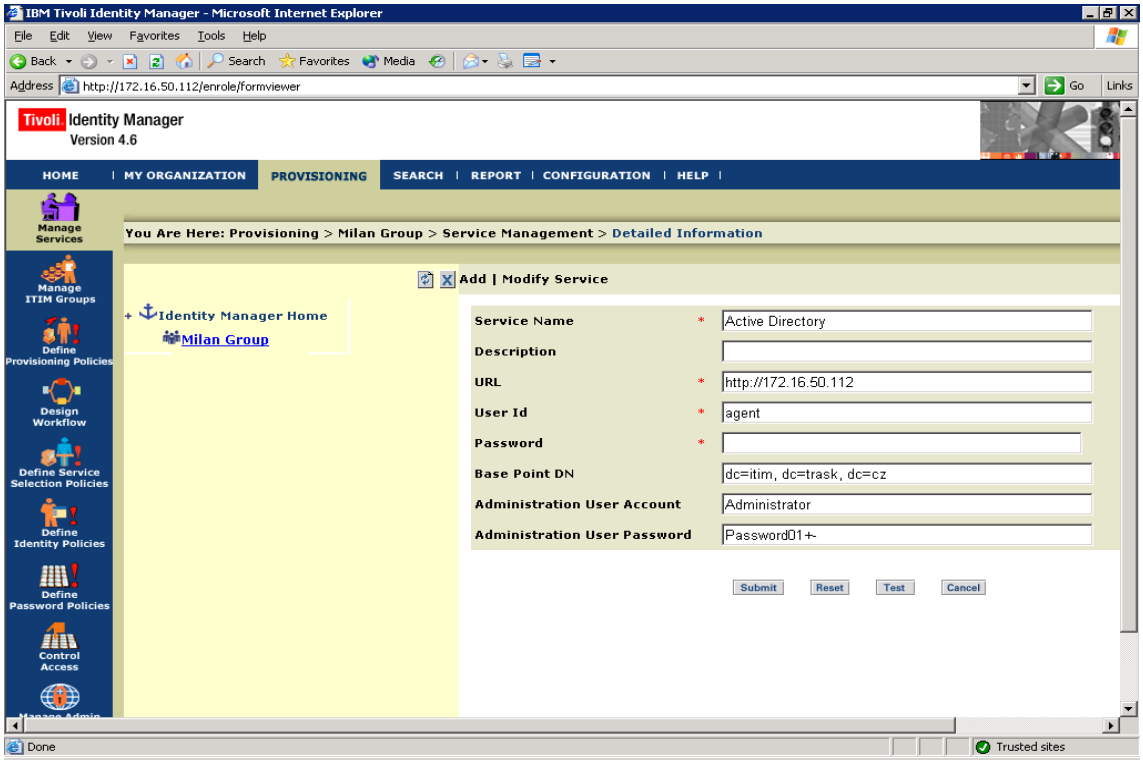
4. Import proběhl úspěšně, pokračujte kliknutím na **CONTINUE**.



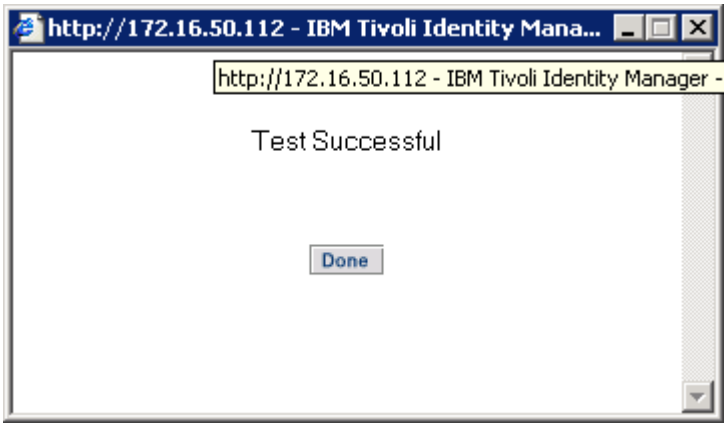
5. Zkontrolujte v záložce **ENTITIES** zda se přidal **ADAccount.**



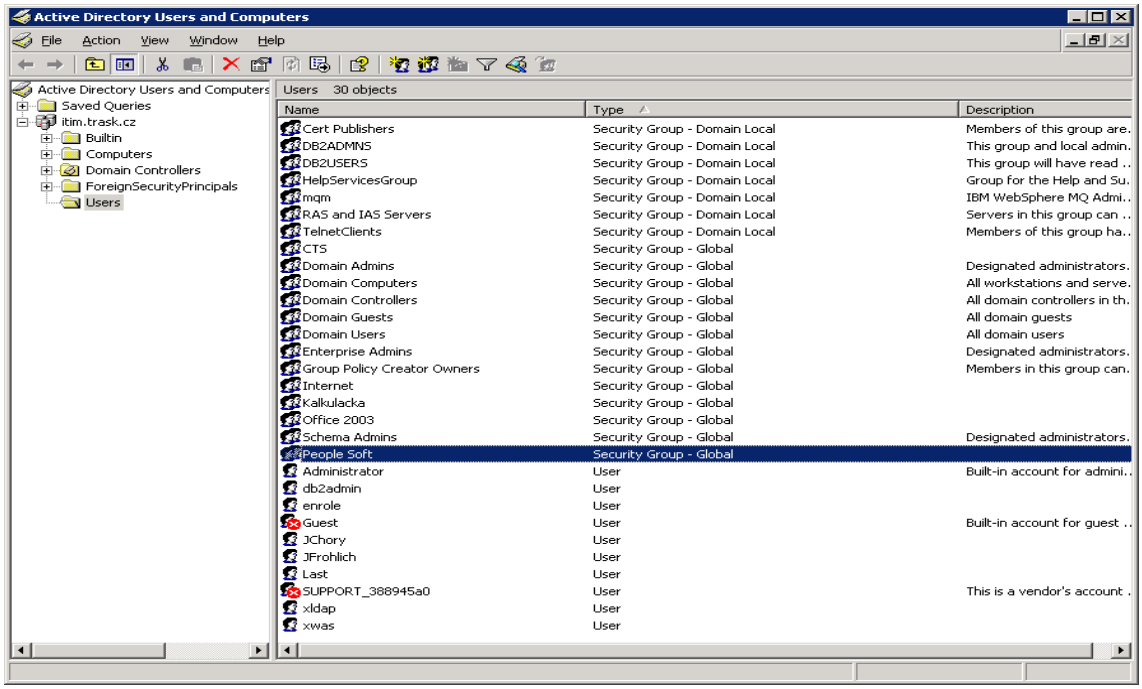
6. Naimportovaný ***.jar** pro AD, se nyní musí přidat pomocí **ADD** (Dále pomocí číselníku zvolit „**Active Directory Profile**“).



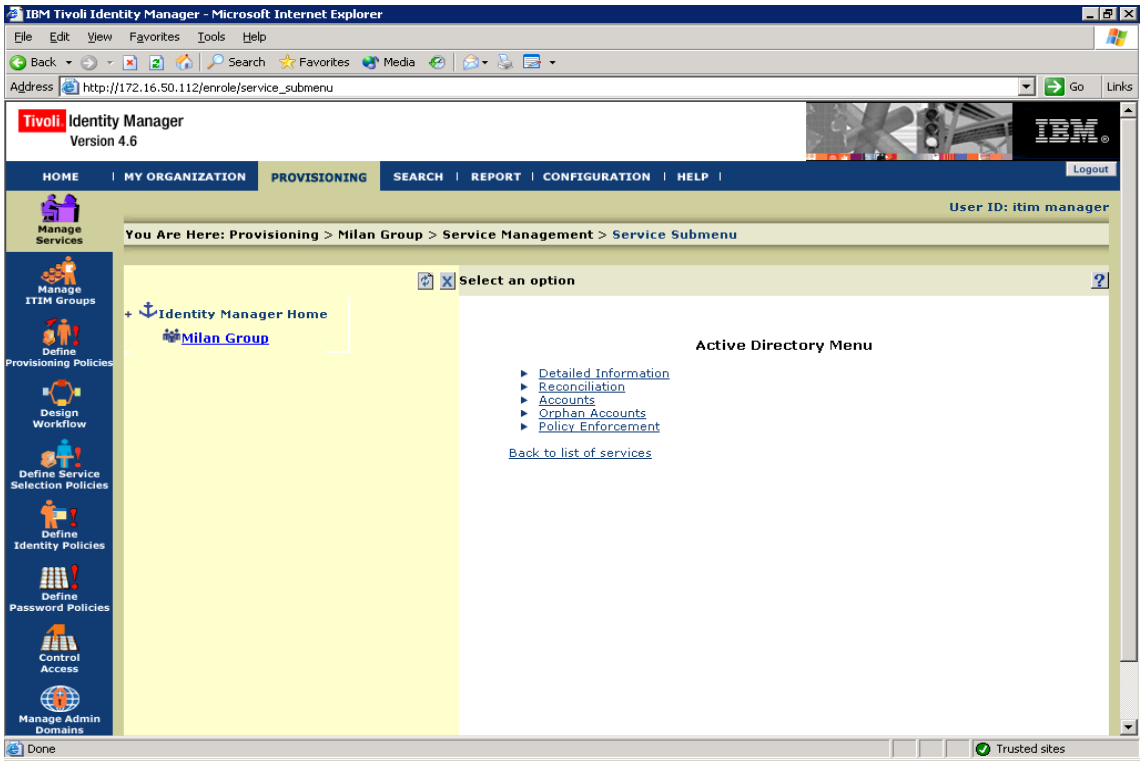
7. Hodnoty s * jsou povinné. Opsat obrazovku a heslo pro **Agent**a je **Agent.** Po vyplnění údajů klikněte na tlačítko Test. URL není standardní!!! A Base Point DN se mění dle domény počítače, to samé platí pro Administrátora i jeho heslo.



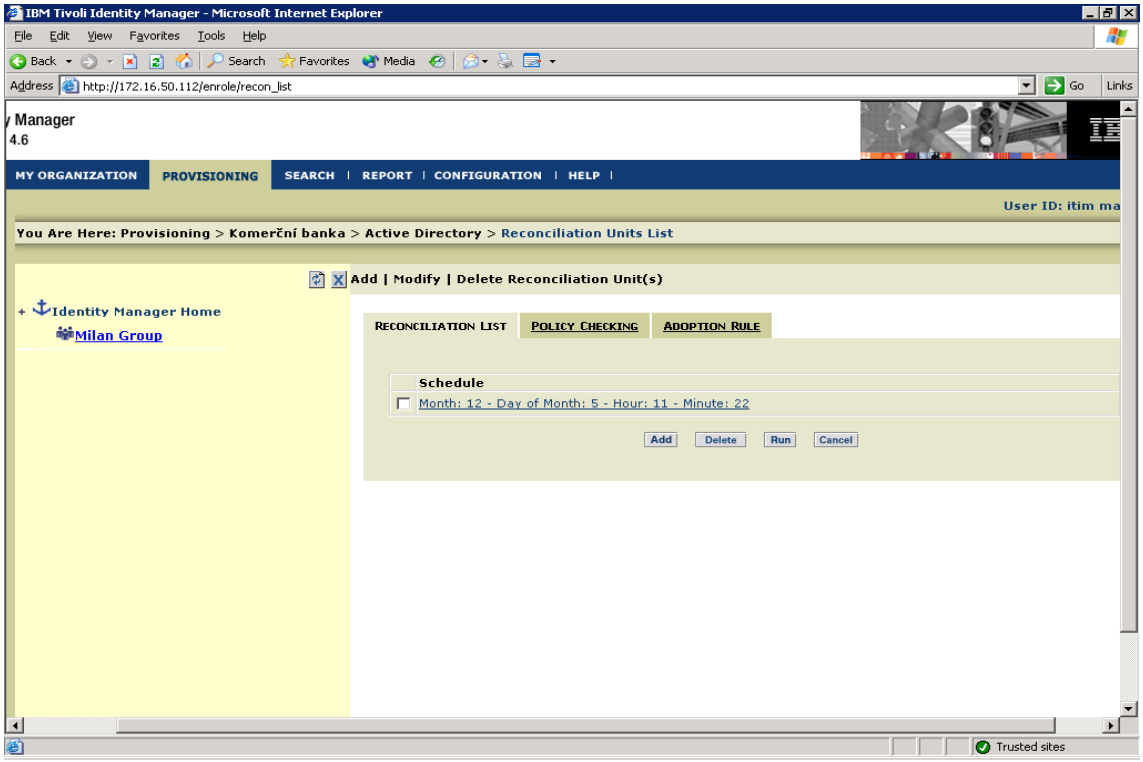
8. Při úspěšnosti testu se zobrazí následující okno. Pokračujte kliknutím na **DONE**.



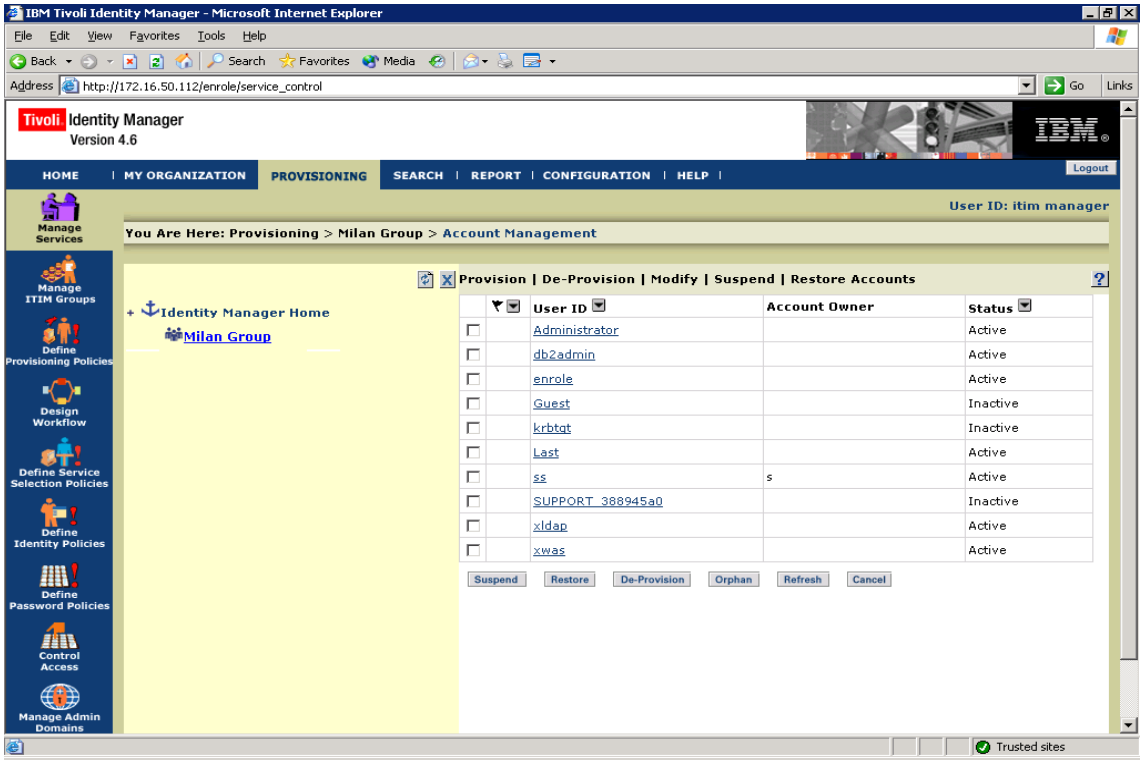
9. Pustíme si Active Directory (Run – **dsa.msc**) a založíme pět skupin – **CTS, KBI, People Soft, Kalkulačka, Office 2003 STD.**



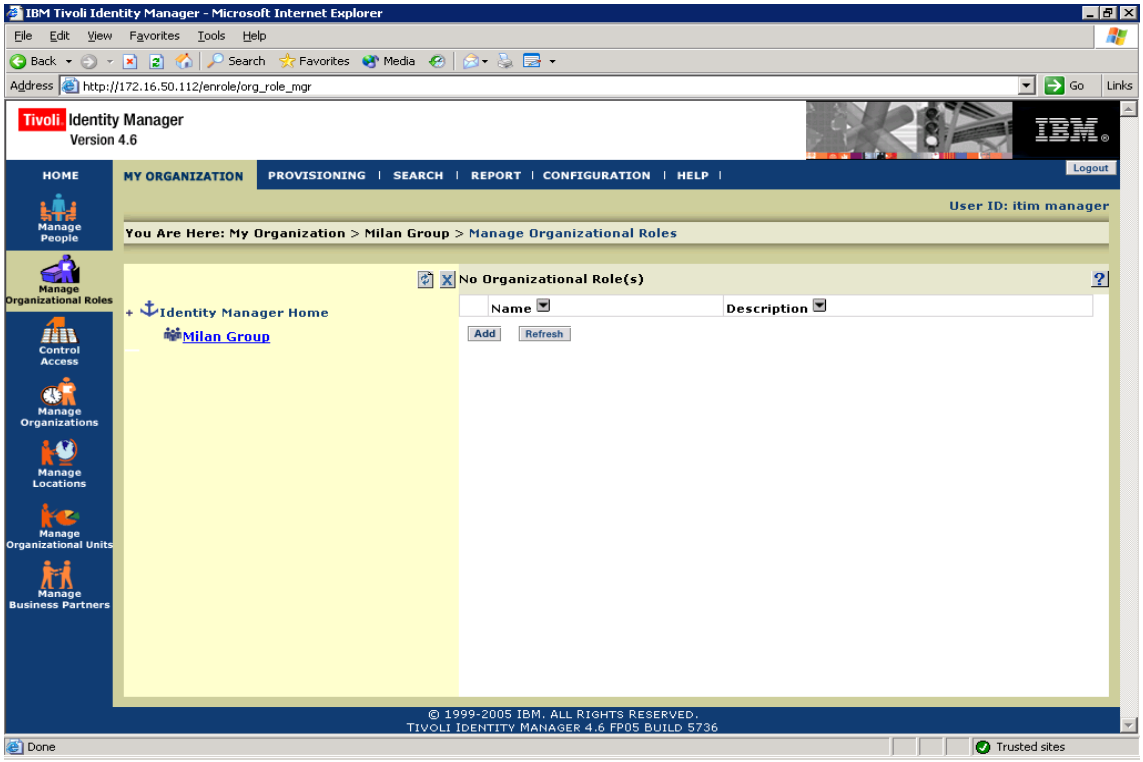
10. Po založení skupin je poté nutné pustit v ITIMu, v Active Directory Menu, **RECONCILIATION**, která načte potřebná data z Active Directory.



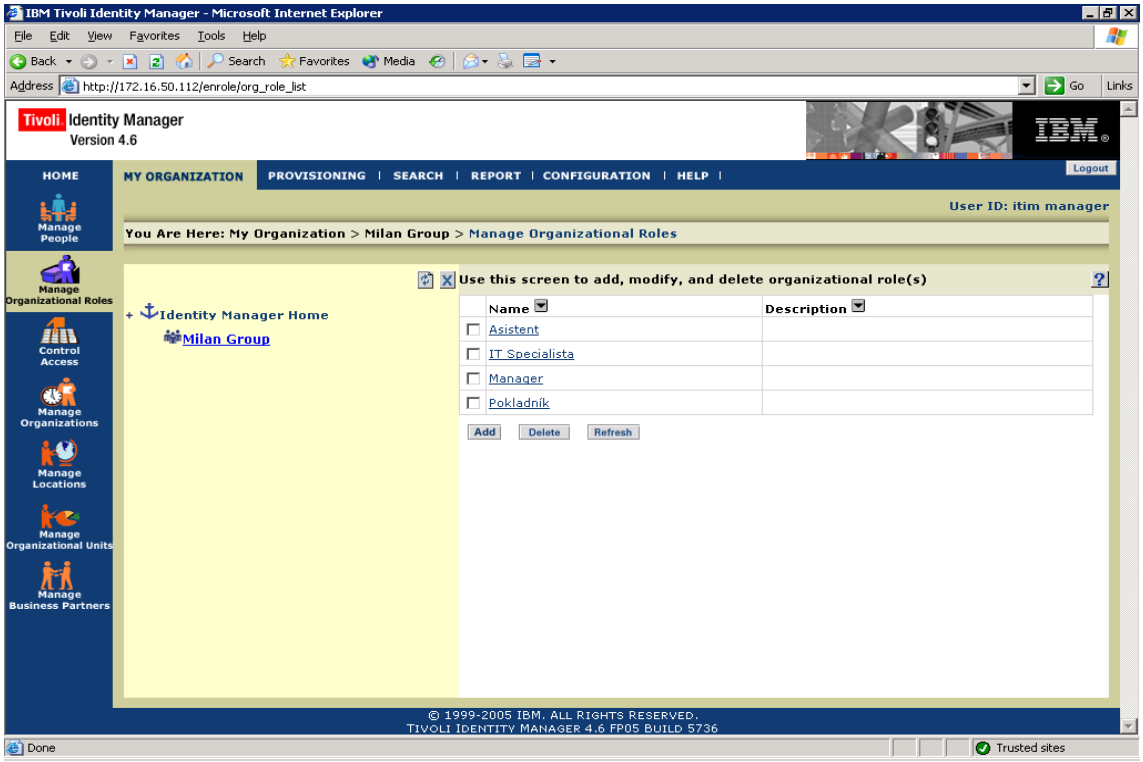
11. Kliknutím na **ADD** nastavíme (kdy začne) reconciliation a spustíme pomocí **RUN.**



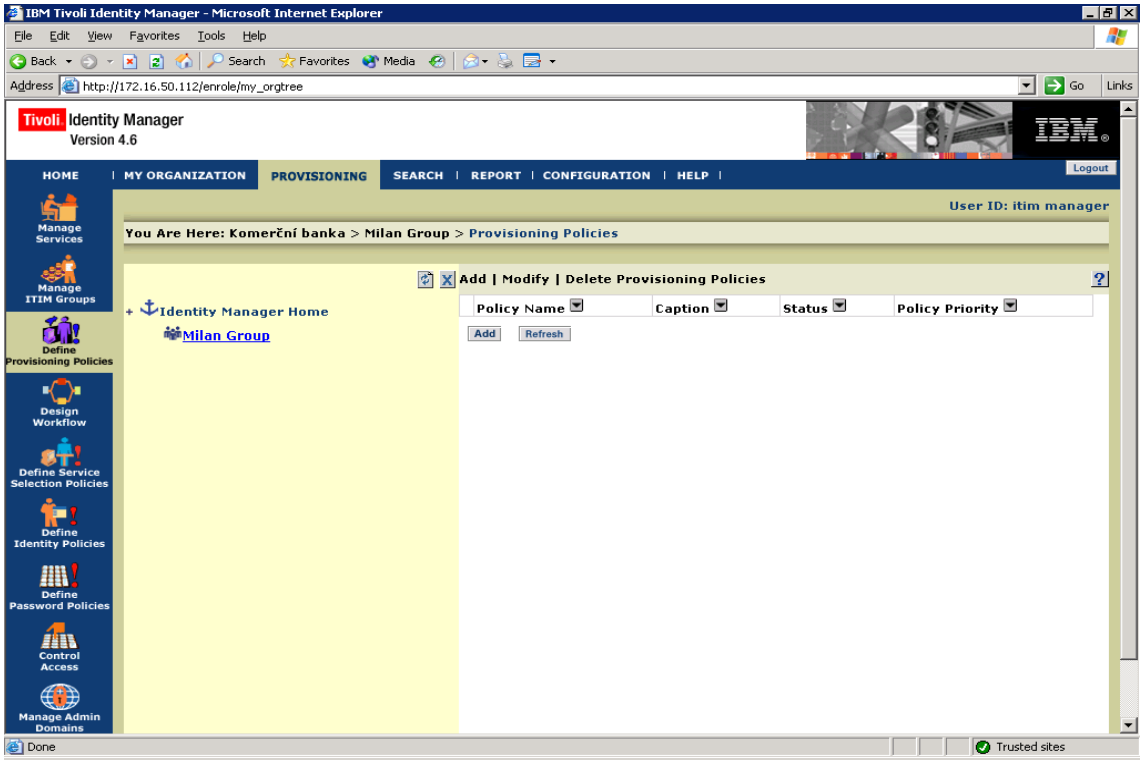
12. Pro ověření načtení se vrátíme zpět do **ACTIVE DIRECTORY MENU** (krok. 17) a klikneme na **ACCOUNTS**(Objeví se načtené účty podobné těm na obrázku).



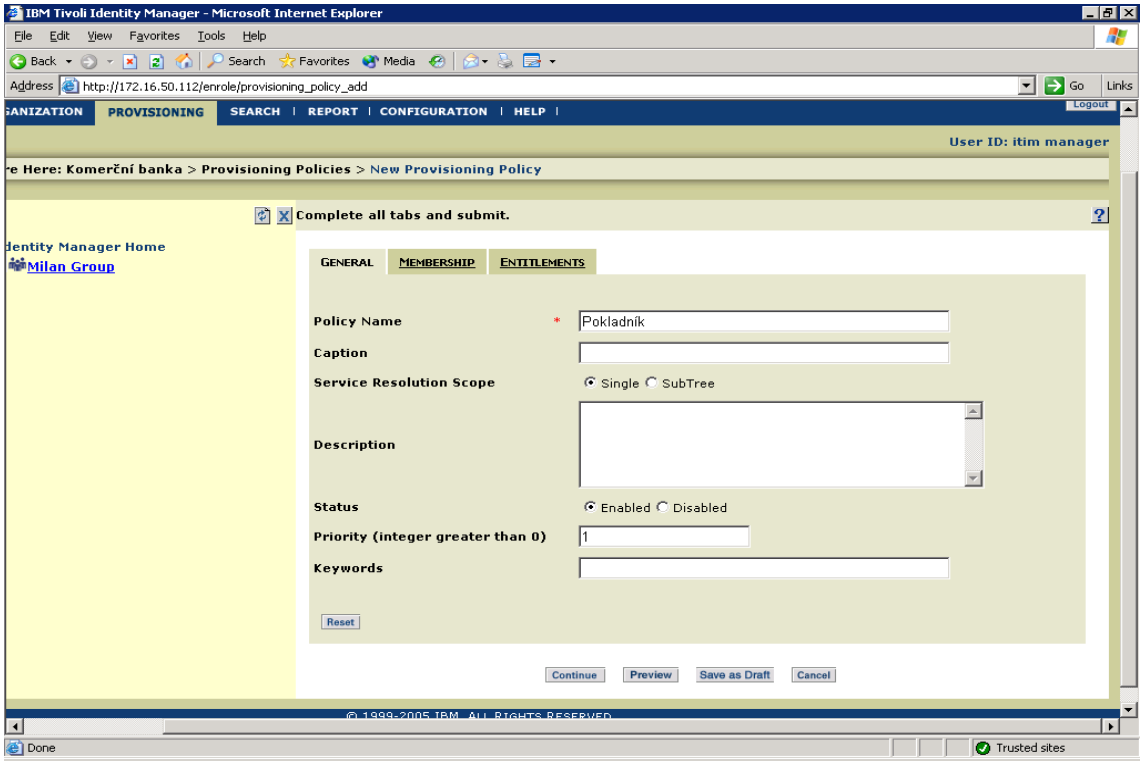
13. Vytvoříme čtyři organizační role pomocí **ADD**(typ role bude **STATIC**)přidáme postupně **IT SPECIALISTA**, **ASISTENT**, **POKLADNÍK**, **MANAGER**.



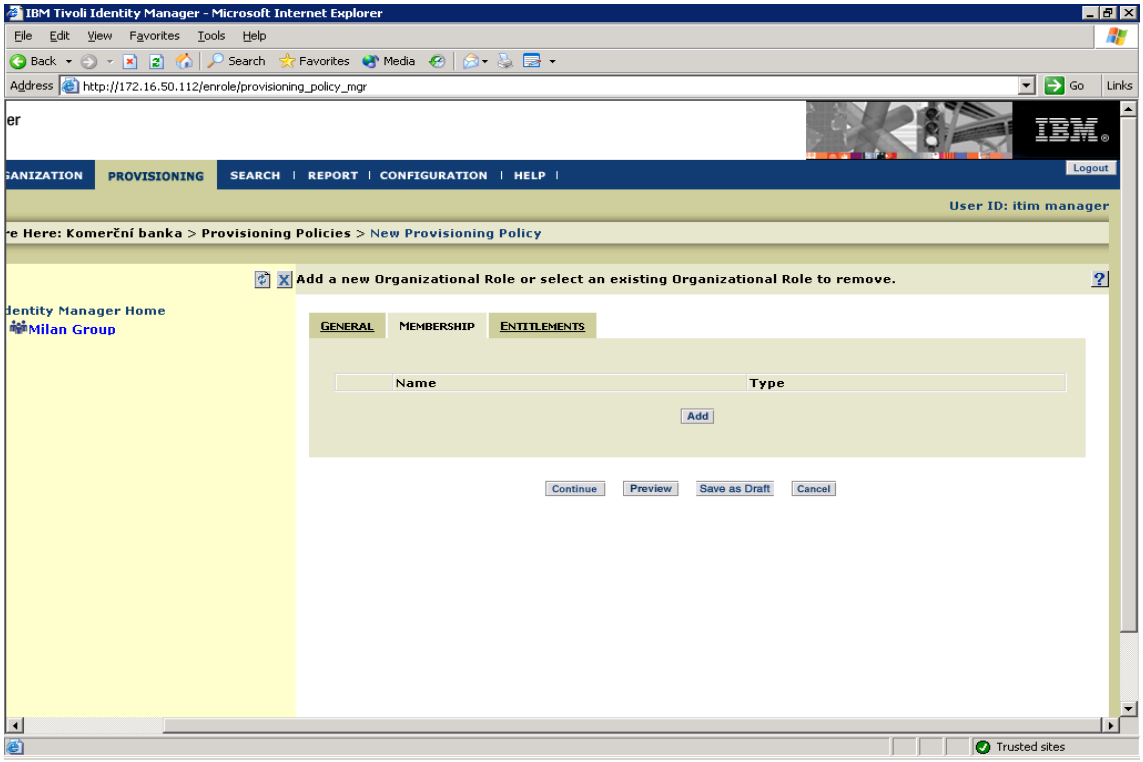
14. Výsledek bude stejný jako na obrázku.



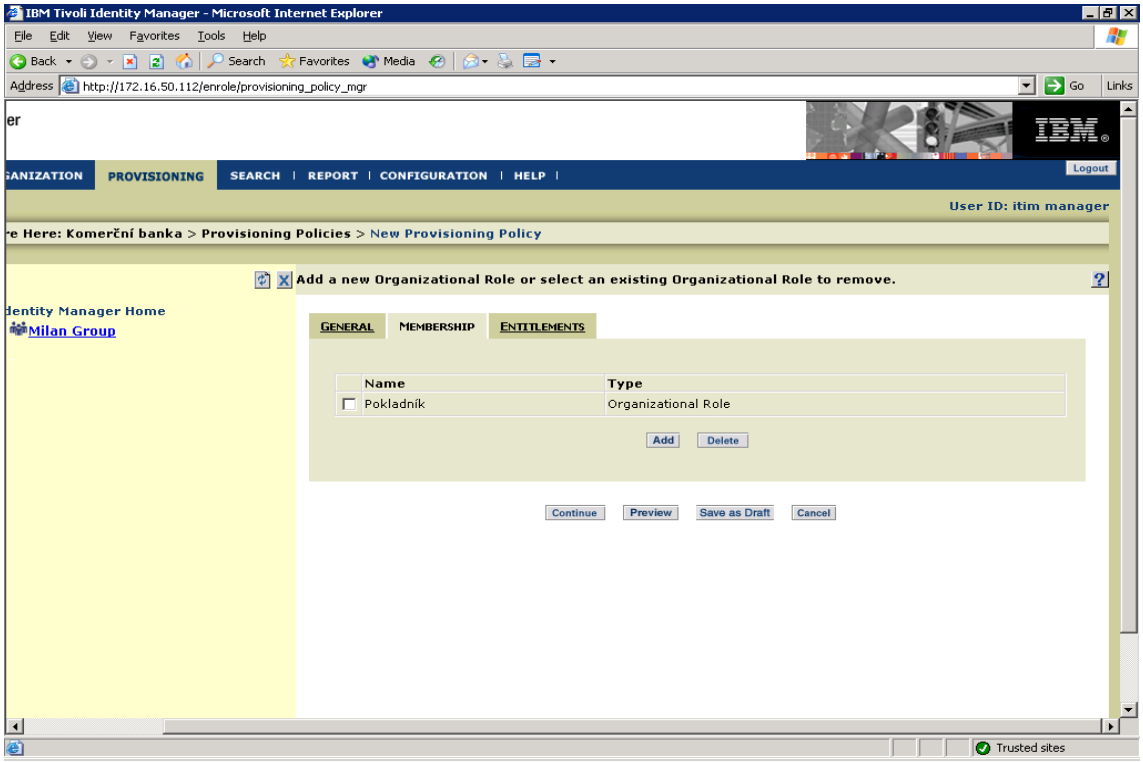
15. Na základě vytvořených skupin, vytvoříme jednotlivé politiky v **DEFINE PROVISIONING POLICIES**, stiskneme tlačítko **ADD**.



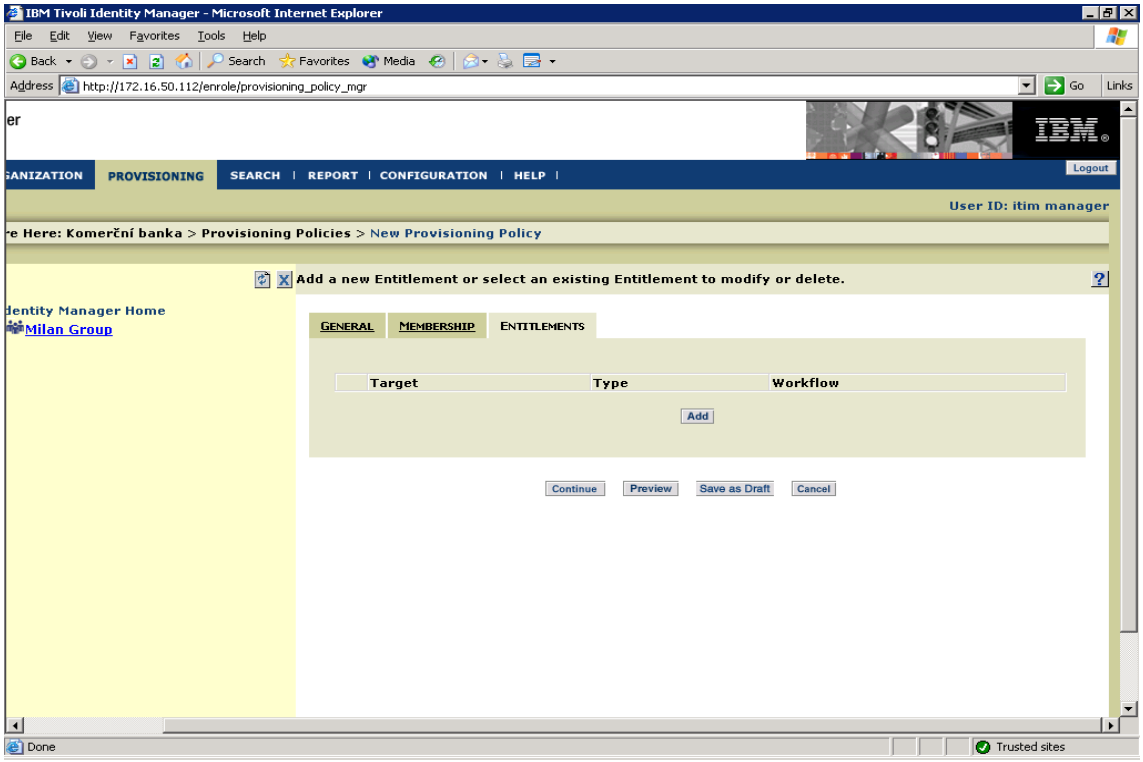
16. V záložce **GENERAL** vyplníme do **Policy Name** – „**Pokladník**“.



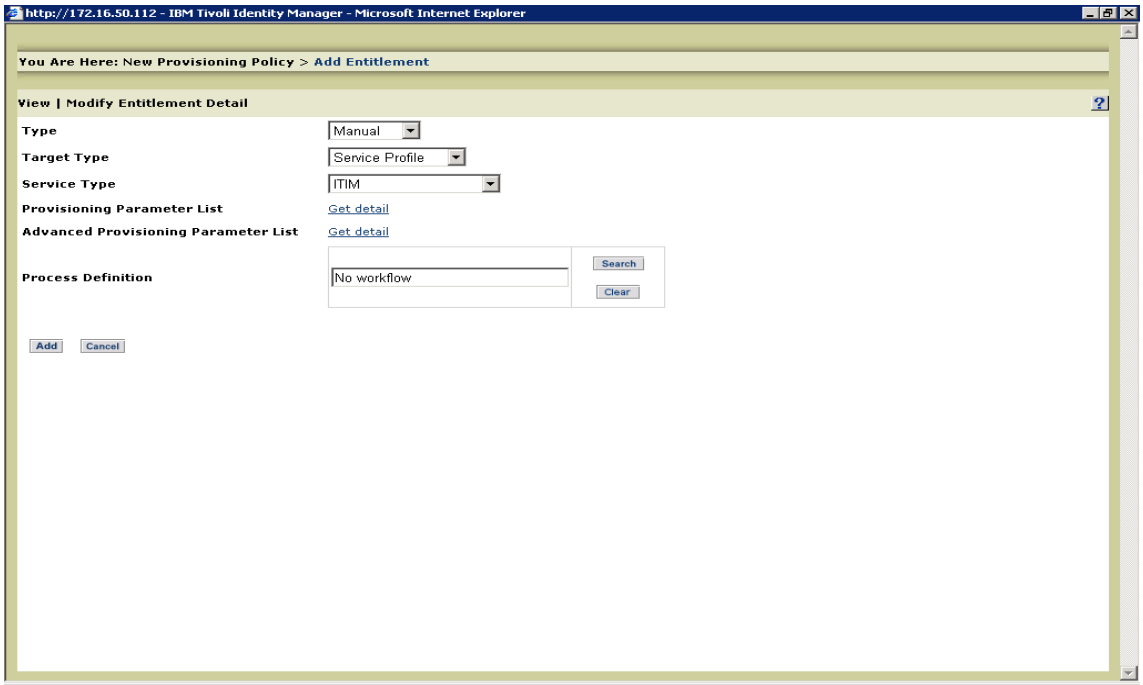
17. V záložce **MEMBERSHIP** přidáme pomocí tlačítka **ADD** organizační roli „**Pokladník**“.



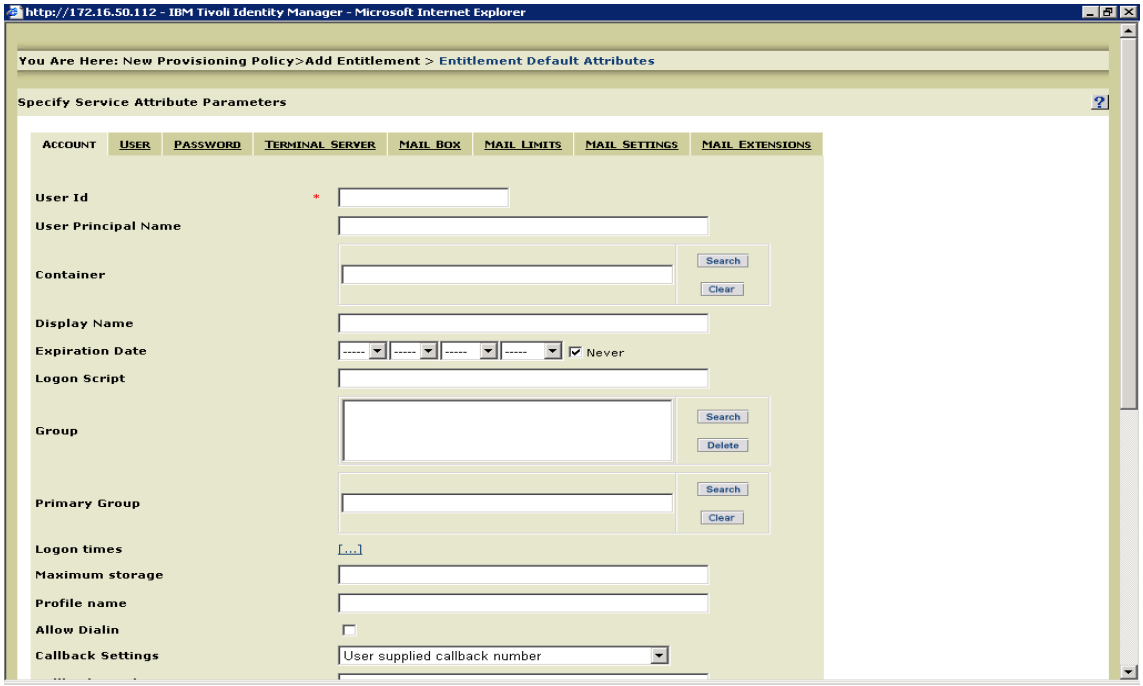
18. Výsledek vidíme na obrázku.



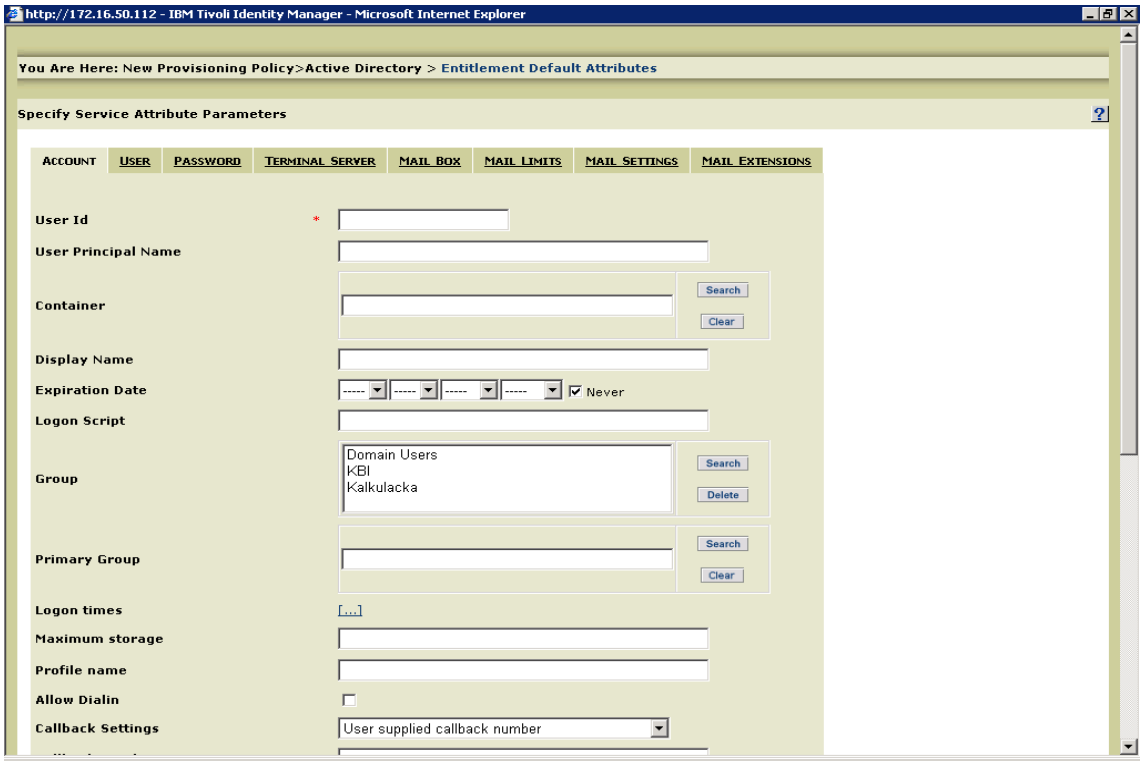
19. Pokračujme stisknutím tlačítka **ADD**.



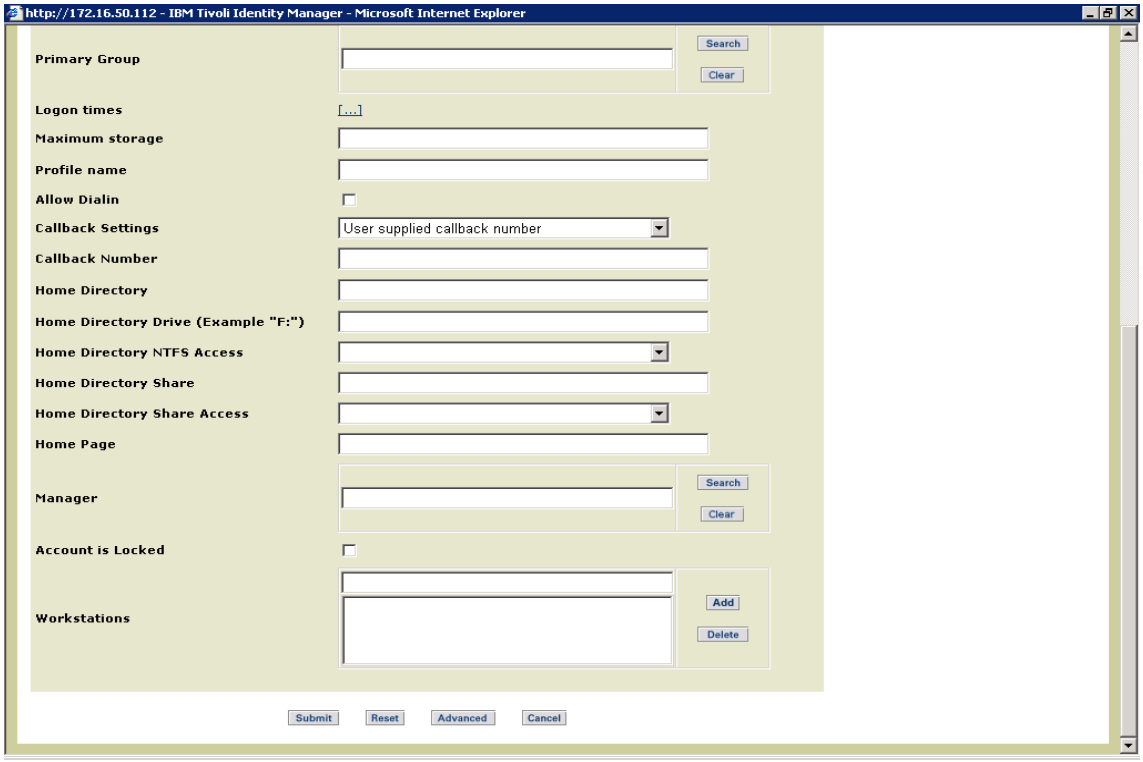
20. V číselníku **TYPE** zvolíme **AUTOMATIC**, v **TARGET TYPE** vybereme **SERVICE**, v **SERVICE TYPE** zvolíme **ACTIVE DIRECTORY**. Klikneme na **GET DETAIL** u **PROVISIONING PARAMETER LIST**.



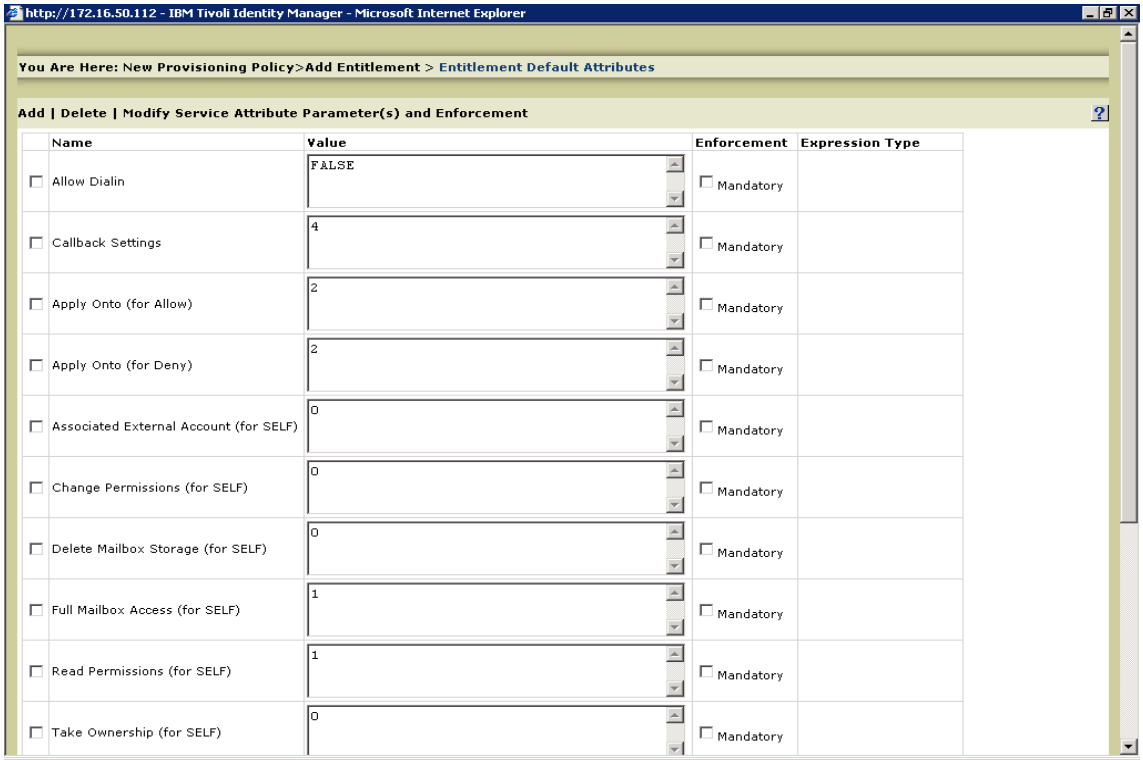
21. V části **GROUP** pomocí **SEARCH** přidáme jednotlivé skupiny pro **POKLADNÍKA** tj. „**KALKULAČKA**“, „**KBI**“, „**DOMAIN USER**“.



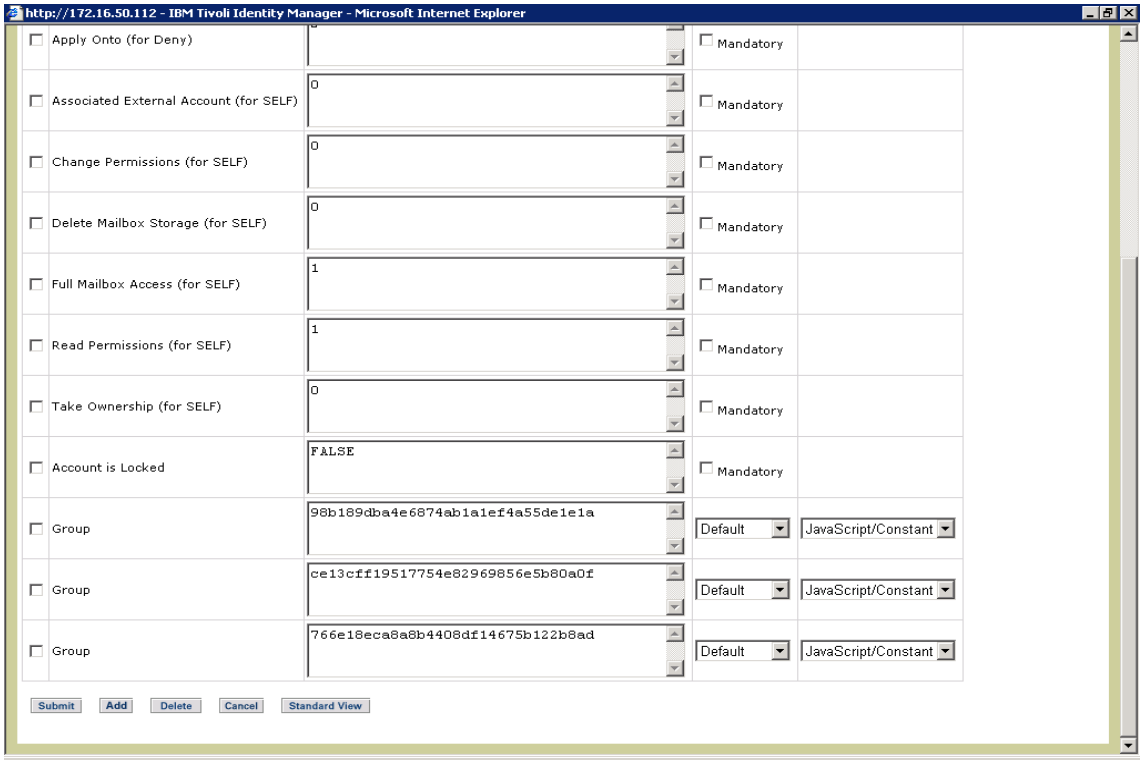
22. Výsledek vidíme na obrázku.



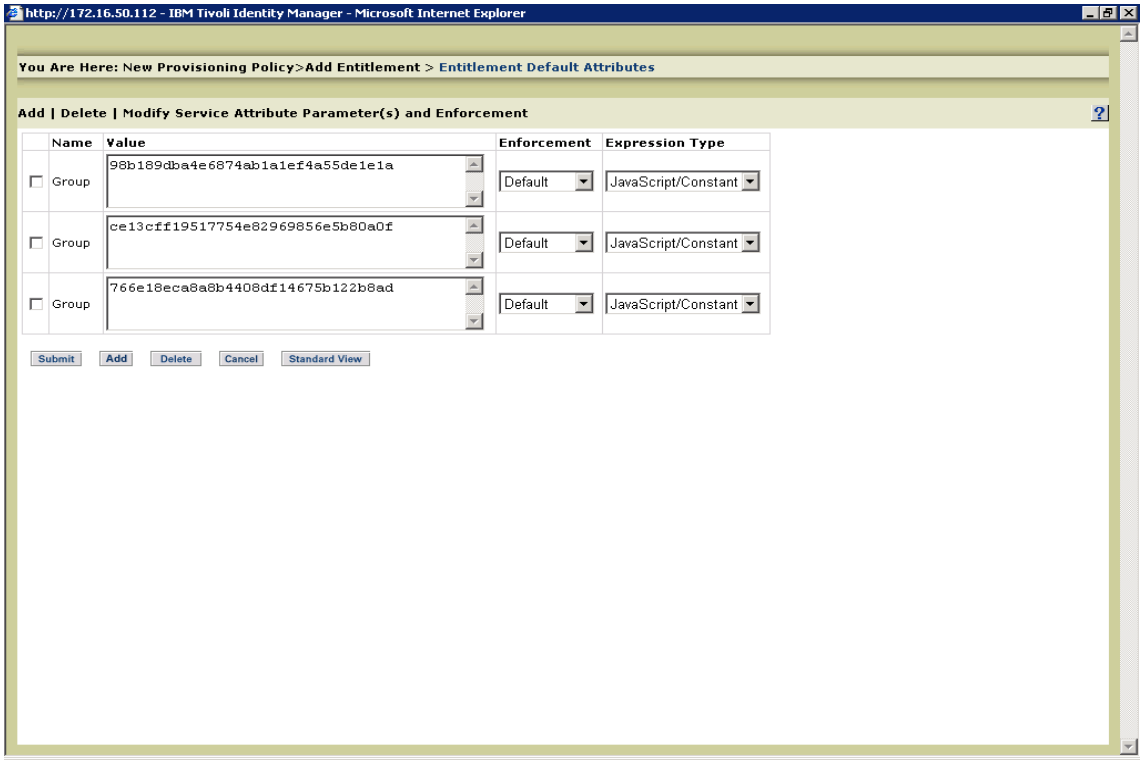
23. Sjedeme posuvníkem dolů a klikneme na **ADVANCED**.



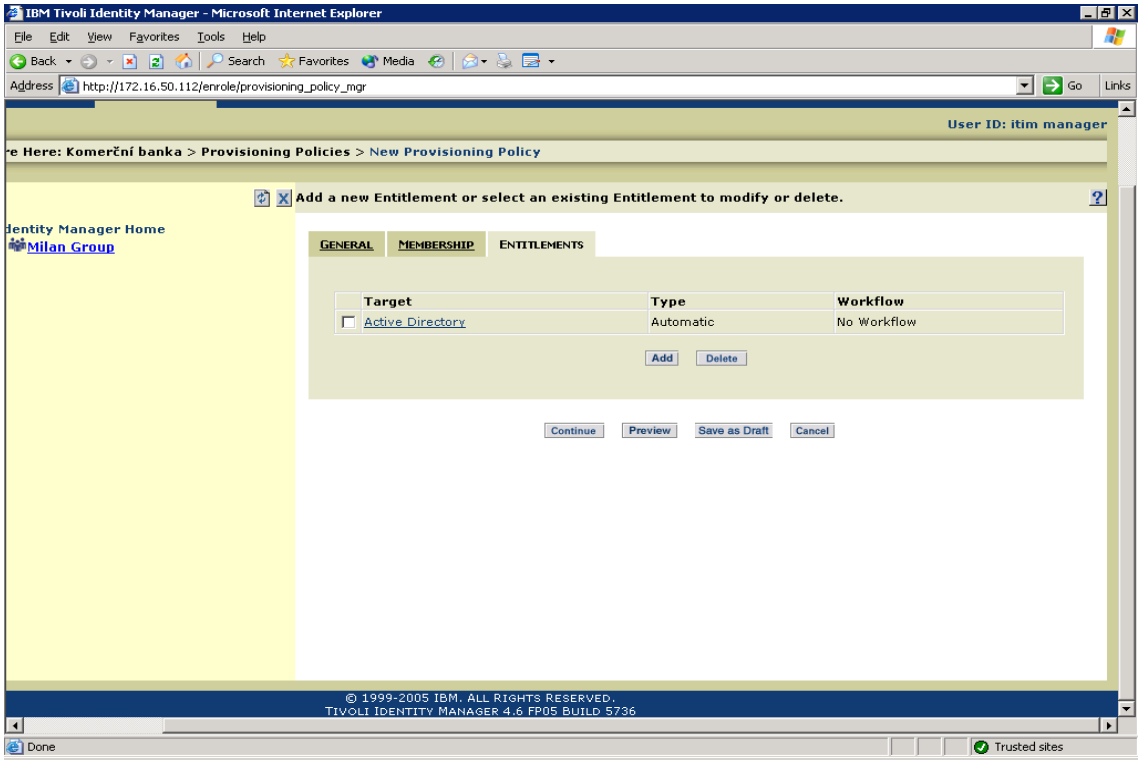
24. Všechny části viditelné části zaškrtneme a sjedeme posuvníkem dolů.



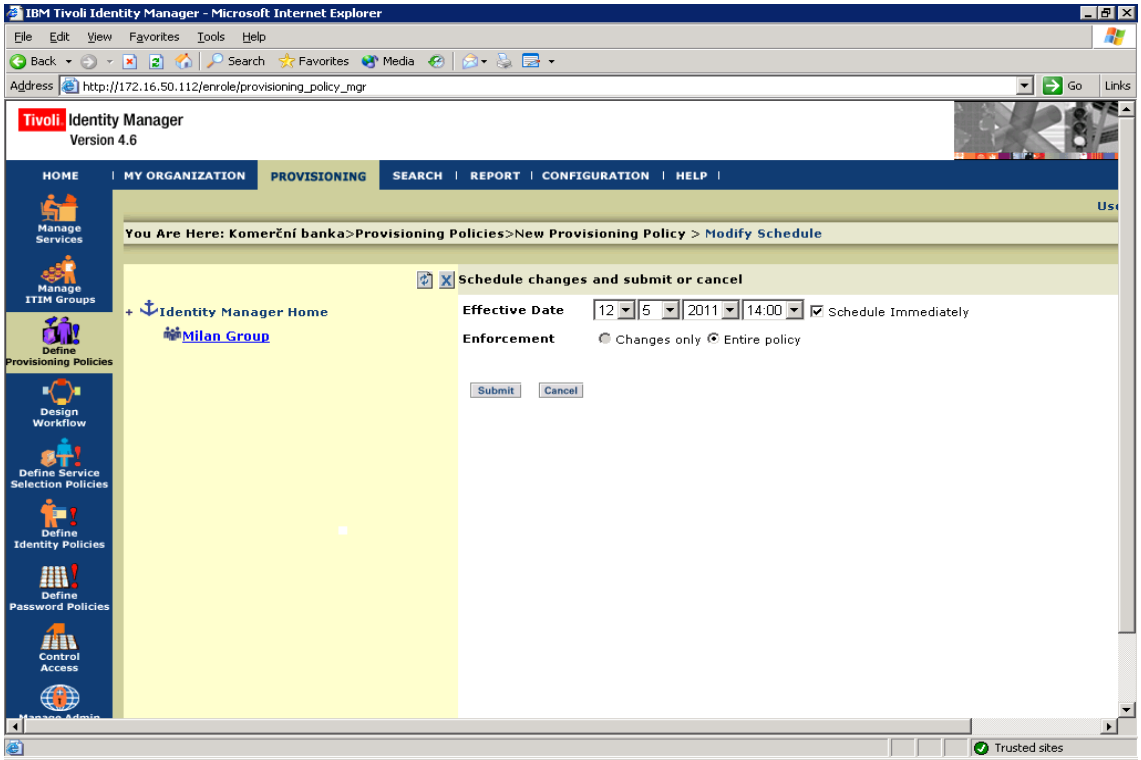
25. Označíme ještě část **Account is Locked** a všechny označené části smažeme pomocí tlačítka **DELETE**.



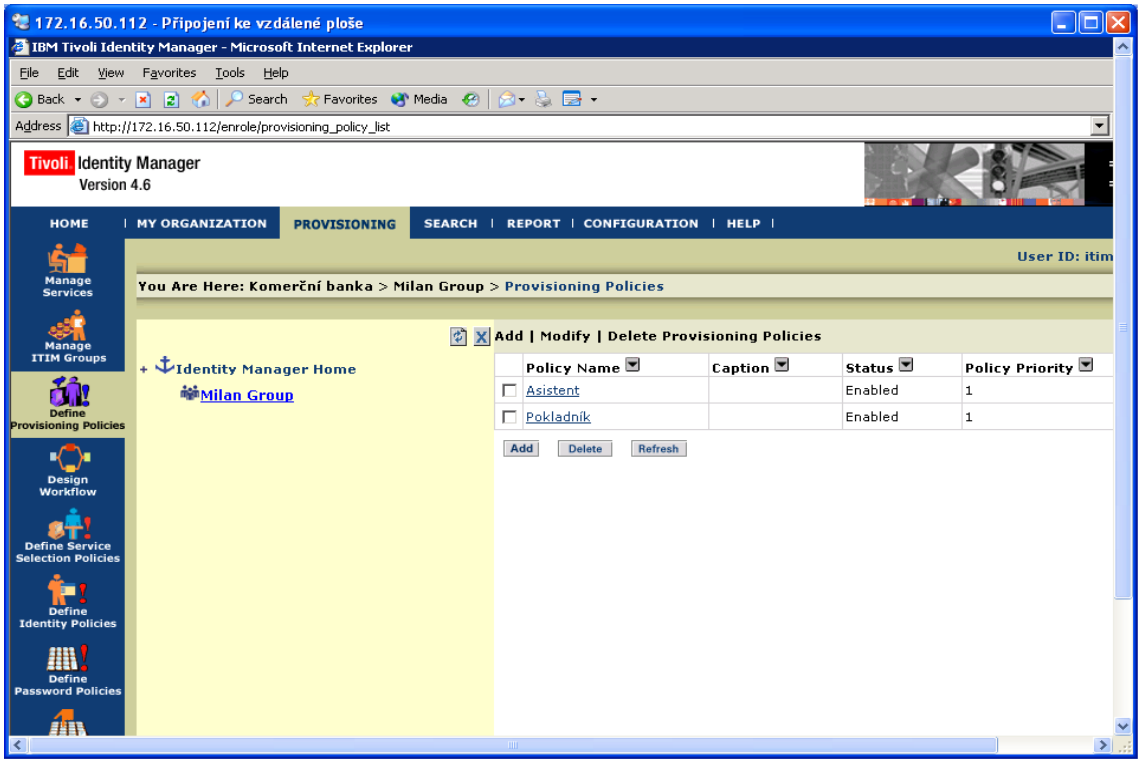
26. V části **Enforcement** pomocí číselníku vybereme pro všechny části **MANDATORY**(je na pevno dáno). Pokračujeme tlačítkem **SUBMIT** a vrátíme se k oknu v kroku **27** a dáme **ADD**.



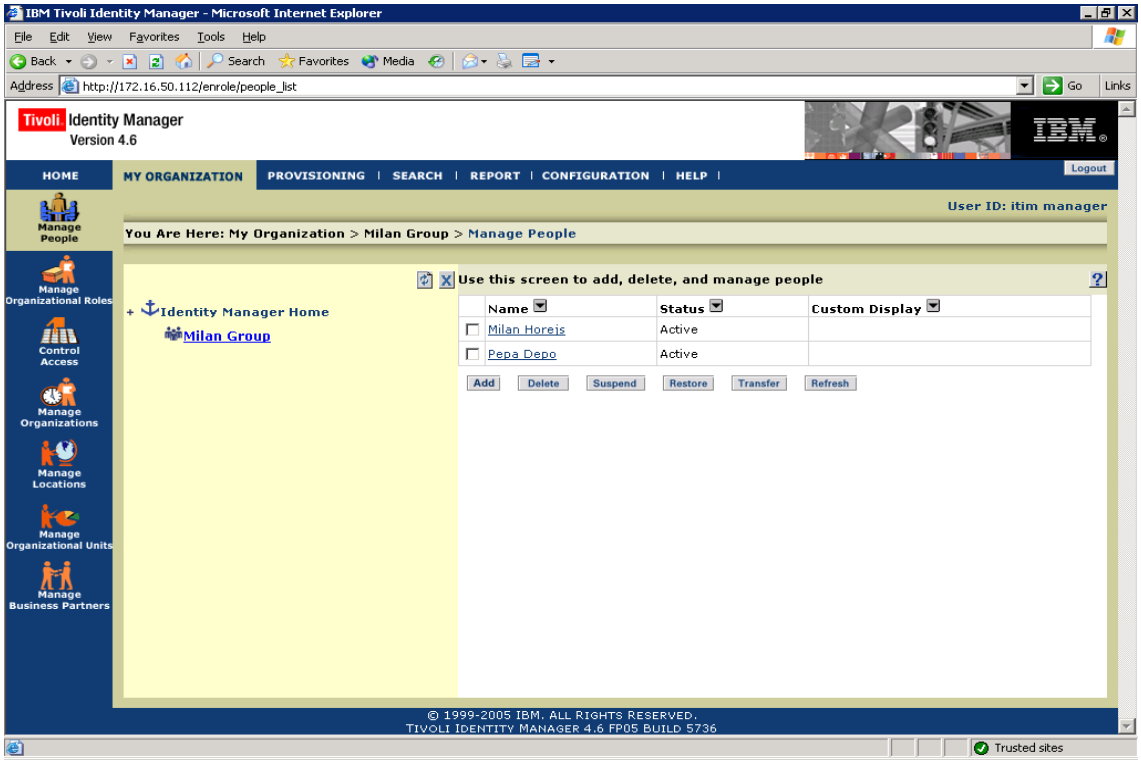
27. Po úspěšném přidání se objeví toto. Pokračujte tlačítkem **CONTINUE**.



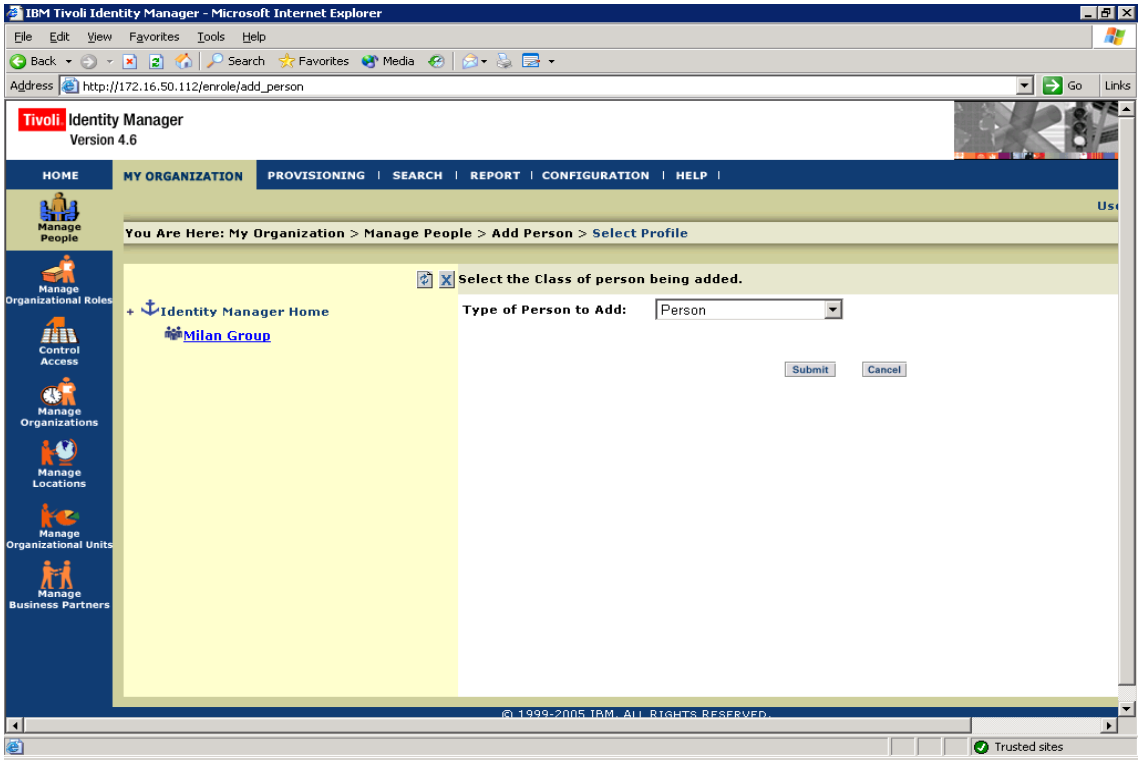
28. Pokračujte stisknutím tlačítka **SUBMIT.**



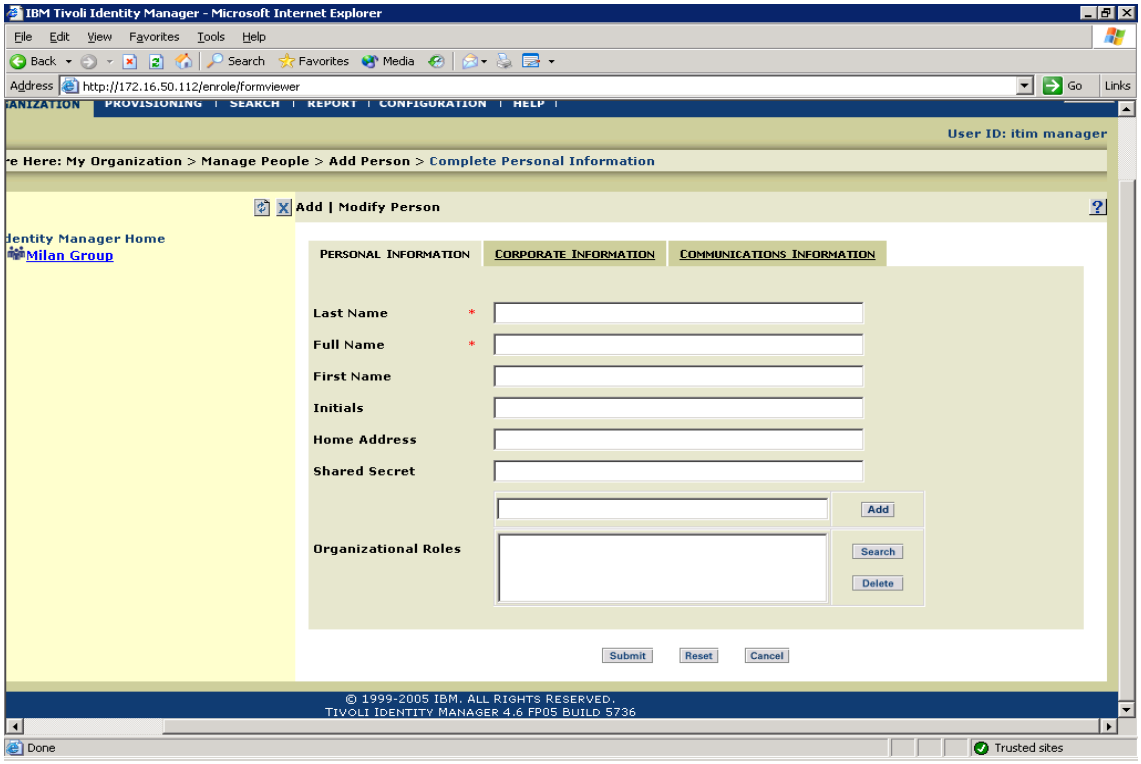
29. Po stisknutí tlačítka **REFRESH** se objeví nová politika „**Pokladník**“.



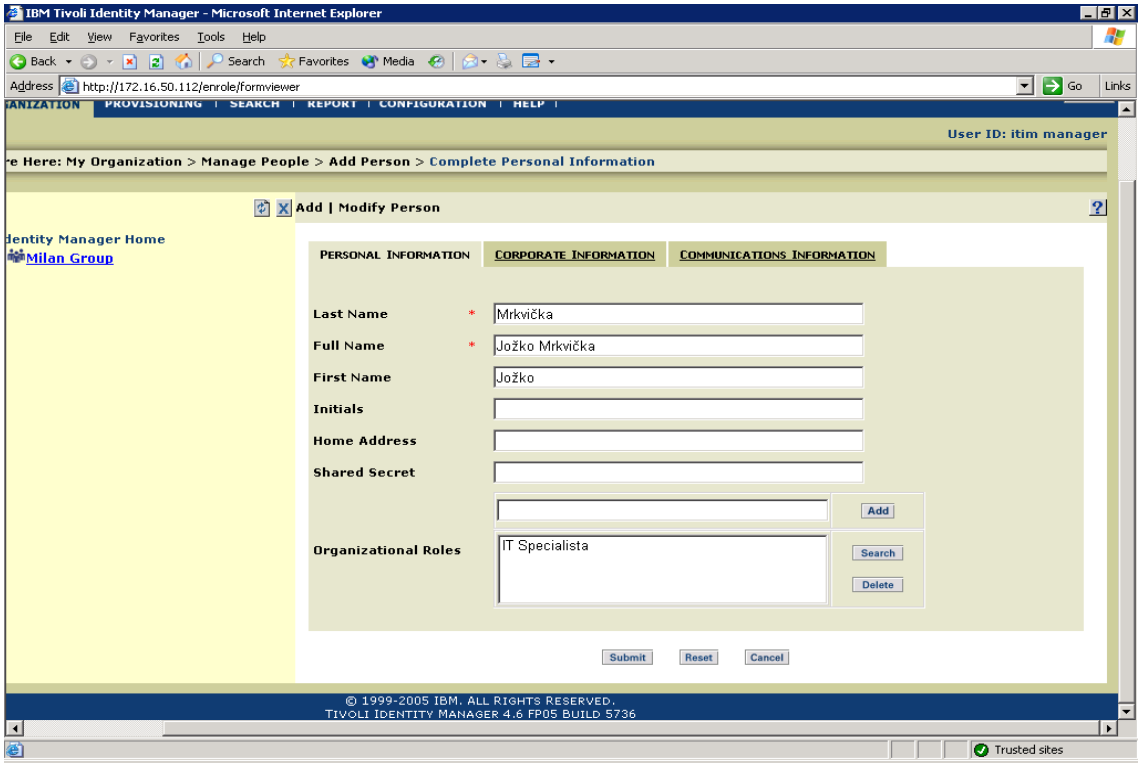
30. Nyní přidáme uživatele „**Jožku Mrkvičku**“, který bude „**IT-Specialista**“ a automaticky se mu vytvoří účet v AD, dle našeho předchozího nastavení. Klikneme na **ADD**.



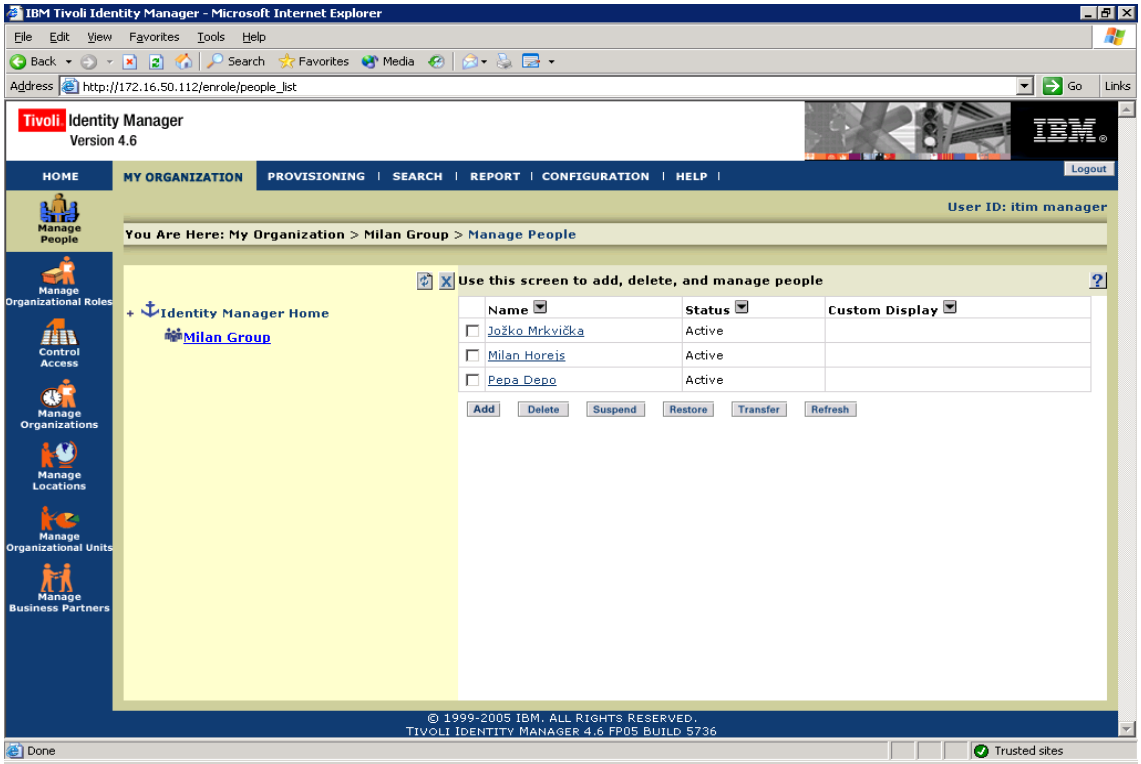
31. Typ osoby bude **PERSON**, pokračujte stisknutím tlačítka **SUBMIT**.



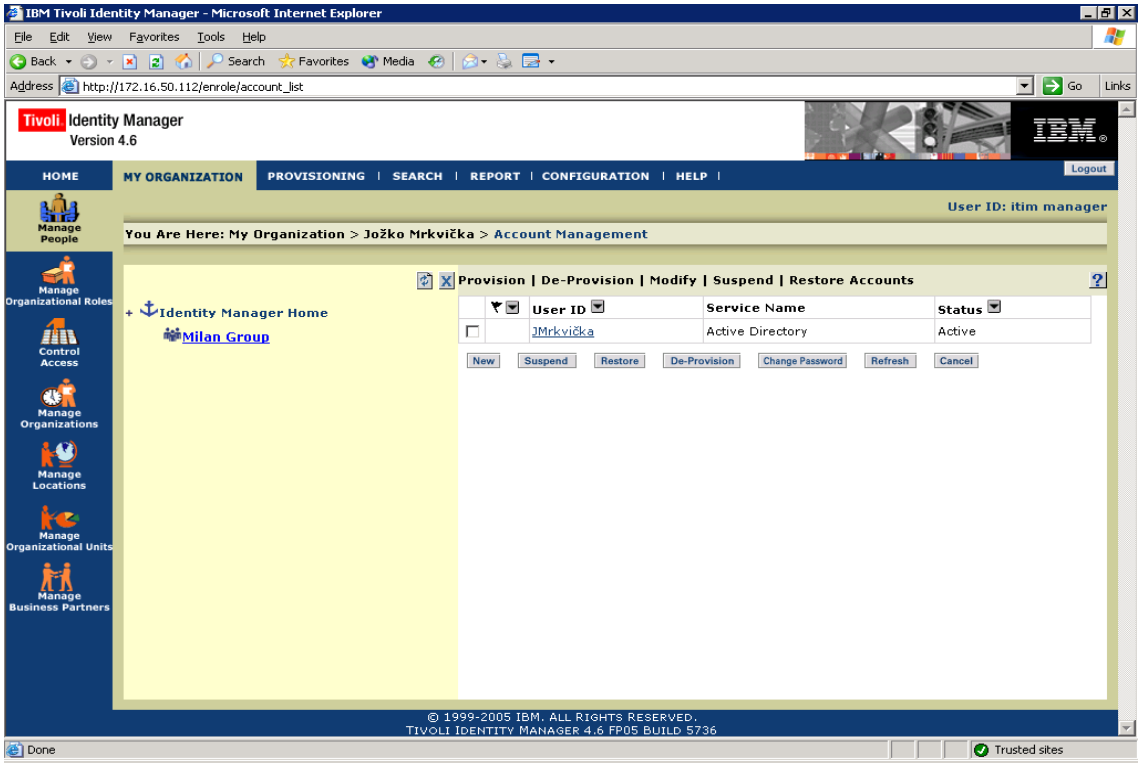
32. Vyplňte povinné údaje (*) a přiřaďte organizační roli Jožkovi Mrkvičkovi tj. IT-Specialist.



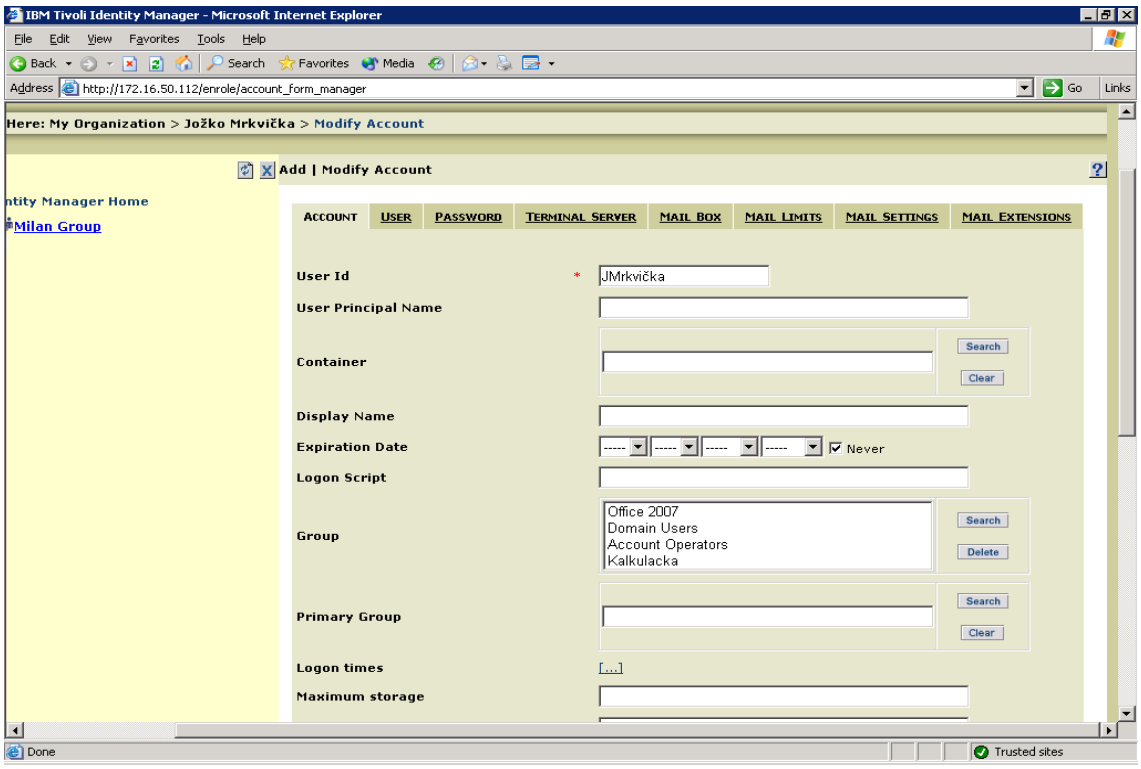
33. Takto by to mělo vypadat. Klikněte na SUBMIT.



34. Po kliknutí na tlačítko REFRESH se objeví vytvořený uživatel. Pokračujte kliknutím na něho a poté stiskněte MANAGE ACCOUNTS.



35. Automaticky se mu vytvořil účet. Pokračujte kliknutím na nově vytvořený účet.

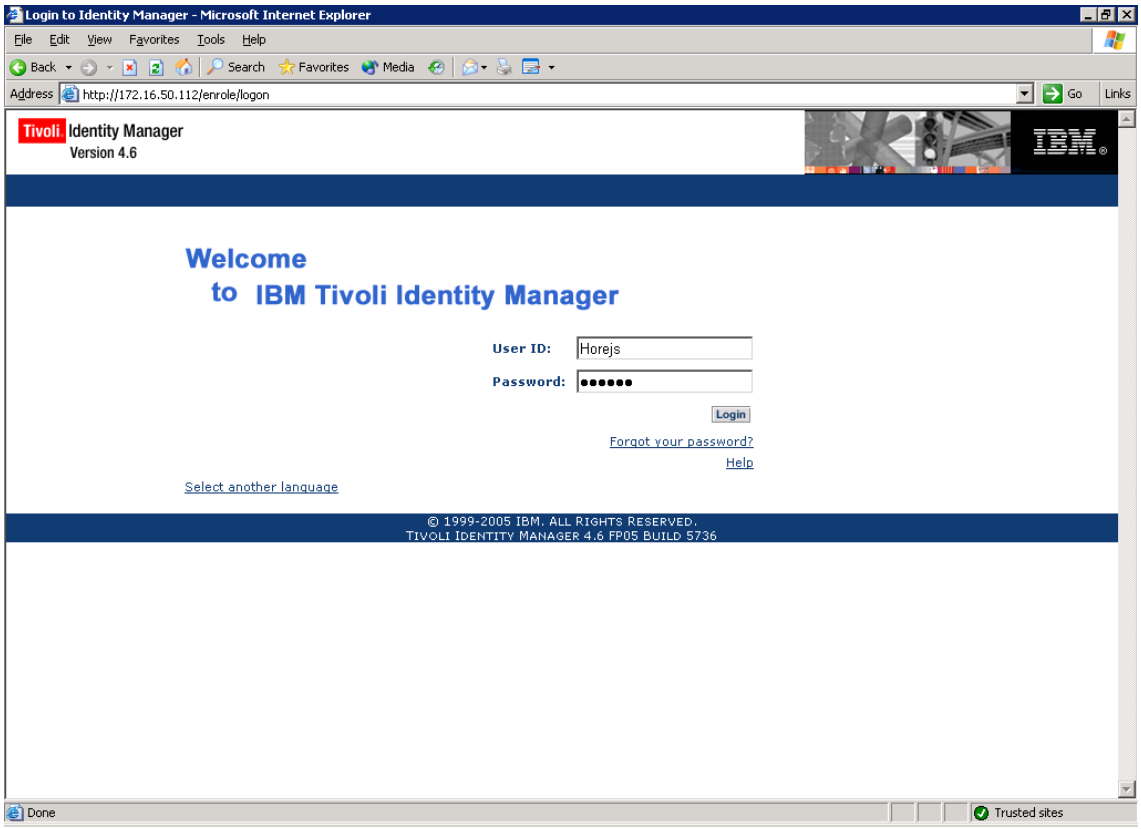


36. Vidíme, že uživatel JMrkvička dostal automatický přístup do zobrazených skupin.

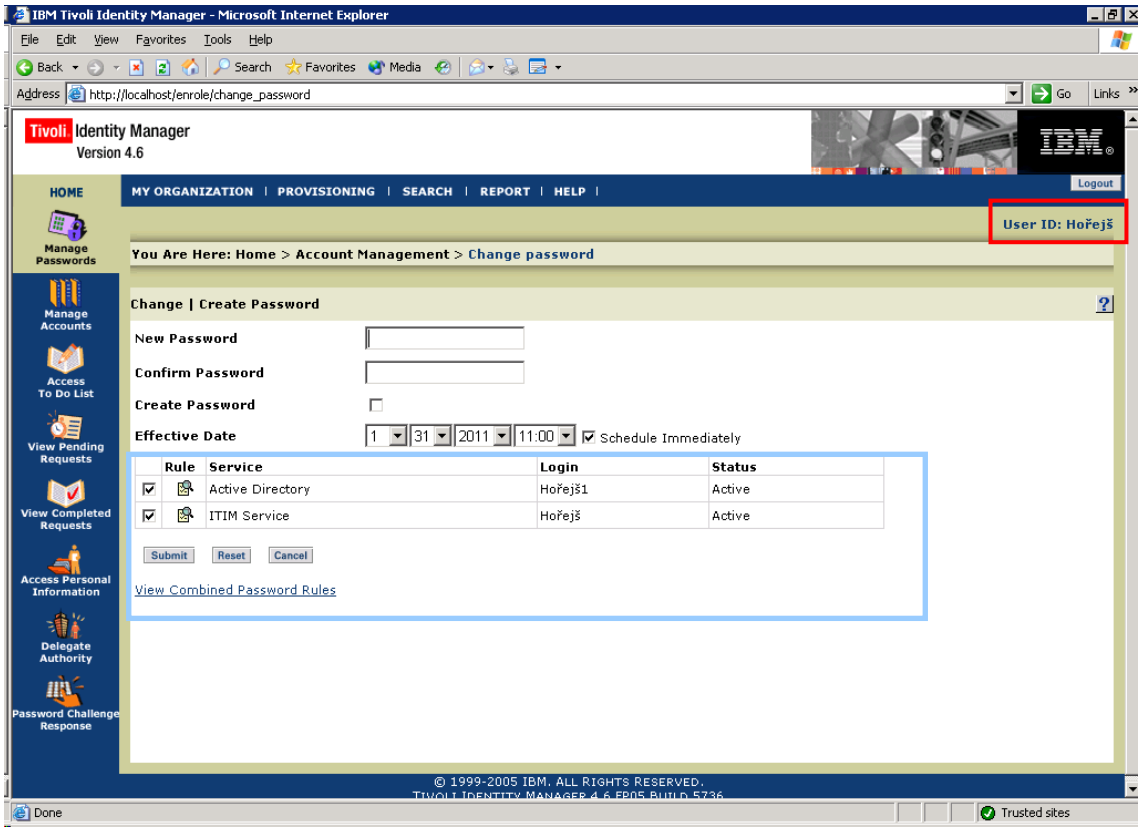
6.1.4 Testování self-reset password

V teoretické části se psalo o self-reset password. Princip spočívá v tom, že je uživatel schopen si sám resetovat heslo do dané aplikace, kde má přístupová práva. Na první pohled to působí velmi triviálně. Ve velkých podnicích tato zdánlivá maličkost se může pro firmu stát velice nákladnou a časově náročnou. Podle mých dosavadních pracovních zkušeností a statistik se přibližně polovina hovorů směřujících na help-desk týká žádostí o reset hesla.

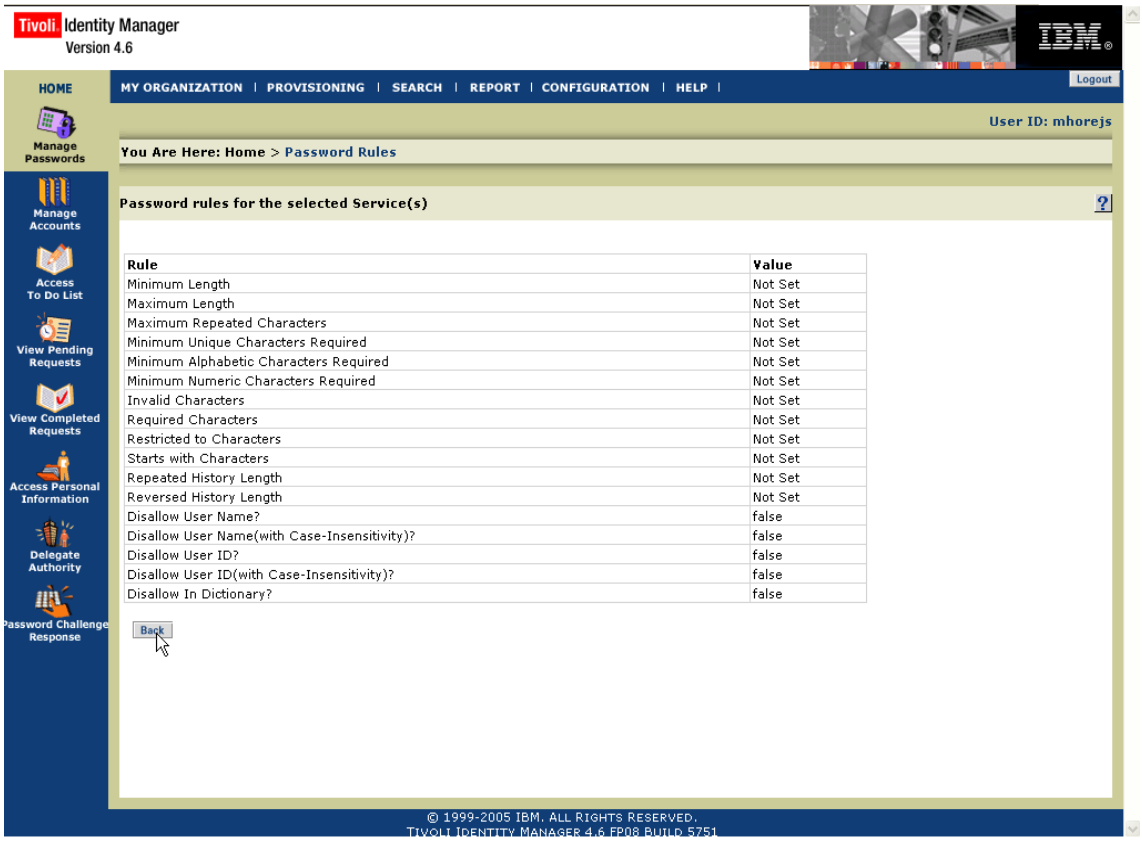
Rozhodl jsem se proto ukázat/otestovat jaká je složitost samostatného resetování hesla pro obyčejného uživatele. Na níže uvedeném postupu (dá se použít i jako návod pro budoucí uživatele aplikace) je vidět, že pro uživatele to není žádný problém. V aplikaci ITIM jsem založil uživatele Horejs, který má vytvořené dva účty. V aplikaci ITIM a v Active Directory. Následující postup popisuje změnu hesla krok za krokem.



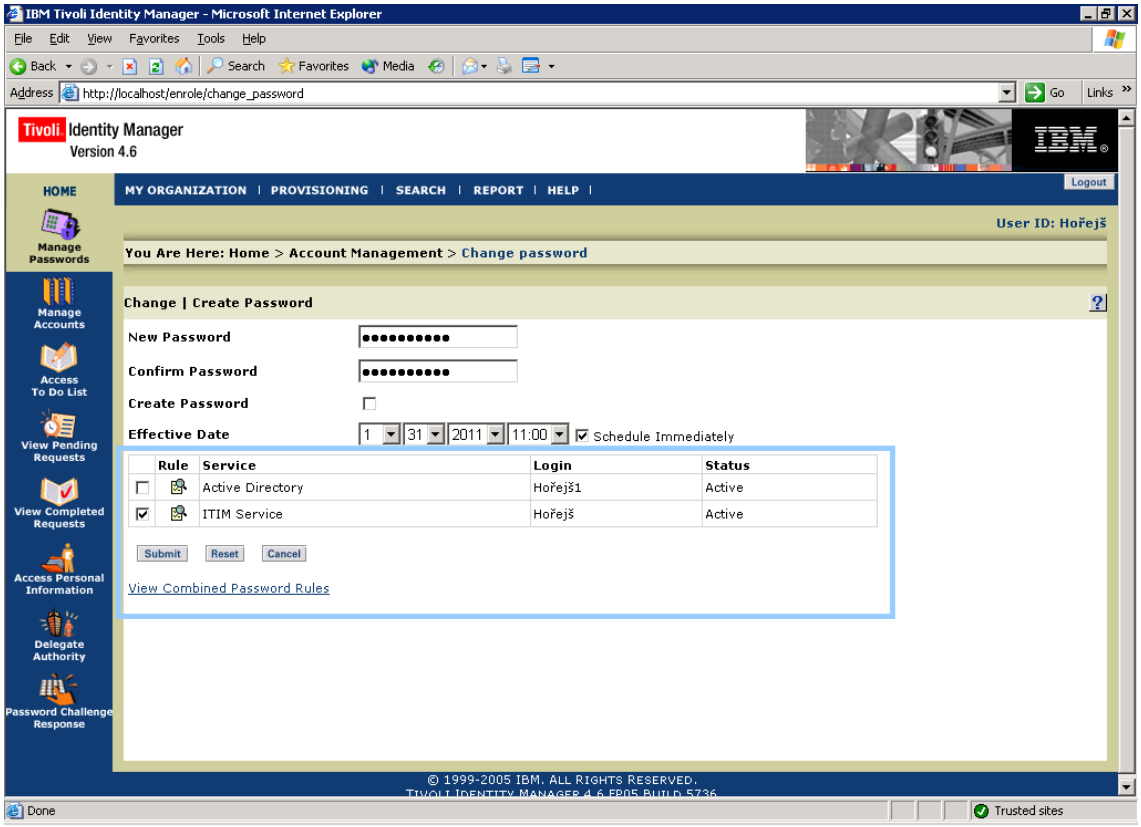
1. Otevřeme aplikaci ITIM a přihlásíme se. Použijeme založený účet: User ID=Horejs, Heslo=Horejs



2. V červeném obdélníku jsou informace o vás, tj. vidíte User ID, pod kterým jsme se přihlásily. V modrém obdélníku je seznam všech aplikací, ve kterých máte vytvořeny účty a pro ně si také můžete sami změnit heslo. Samozřejmě, že každé heslo podléhá určité politice (pravidel) pro jeho vytvoření. Pro zjištění pravidel pro daný systém, klikněte na  (Zobrazí se vám následující okno).

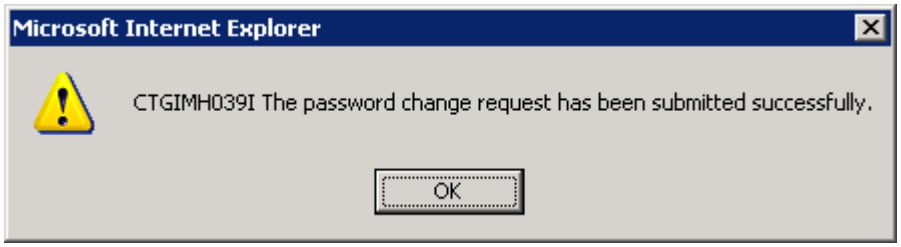


3. Zde je přehled všech pravidel pro změnu hesla do ITIMu. Jsou zde vidět různá pravidla, která zvyšují bezpečnost prolomení hesla (minimální a maximální délka, minimum unikátních znaků, čísel aj.). Ty má každá organizace nastavené jinak. Vrátíme se zpět pomocí kliknutí na tlačítko Back.



4. Když si chcete změnit heslo pro libovolný systém, tak si pomocí zaškrtávajícího checkboxu (☑ - aplikace byla vybrána, ☐ - aplikace nebyla vybrána), který je před daným systémem. Označíme systém, pro který chceme změnit heslo (Viz. Modrá elipsa).

5. Pro změnu hesla nemusíte znát své staré heslo. Po splnění všech předcházejících kroků klikněte na tlačítko Submit.



6. Po úspěšné změně hesla se objeví toto okno, které říká, že heslo bylo úspěšně změněno. Klikněte na OK.

6.2 Výsledky z praxe, před a po implementaci

6.2.1 Novell

Za jednu z nejzajímavějších případových studií se označuje případová studie Czech POINT, kde „cílem bylo vytvoření garantované služby pro komunikaci se státem prostřednictvím jednoho univerzálního místa, kde bude možné získat a ověřit data z veřejných i neveřejných informačních systémů, úředně ověřit dokumenty a listiny, převést písemné dokumenty do elektronické podoby a naopak. Czech POINTy jsou v současné době rozšířeny na více než 5000 obecních a krajských uřadů, vybraných pracovišť České pošty, zastupitelských uřadů, kancelářích Hospodářské komory a také v kancelářích notářů. Pro vyhledání Czech POINTů v konkrétní lokalitě můžete použít interaktivní mapku.“ [Czech POINT, 2010]

„Na počátku tohoto projektu byla myšlenka: Obíhat mají data, ne občan. Základním úkolem řešitelů bylo navrhnout, otestovat a posléze implementovat systém dostupný všude tam, kde je zaveden internet tak, aby umožňoval jednoduchou a efektivní komunikaci občana s úřady na kontaktních místech veřejné správy – „vše na jednom místě" – bez ohledu na místní příslušnost občana. Podmínkou bylo jednoduché ovládání, bez nutnosti větších investic do školení uživatelů. Samozřejmostí byla bezpečnost a dostupnost systému. Dalším požadavkem byly minimální hardwarové a softwarové požadavky na koncové stanice kontaktních míst, aby bylo možné systém provozovat na stávajících kontaktních místech veřejné správy bez dodatečných nákladů. „Když jsme s projektem začínali, mnozí si mysleli, že se jedná pouze o další marný pokus elektronizace veřejné správy. Naši lidé však myšlence projektu Czech POINT věřili již tehdy a jejich snaha a píle ve spolupráci s vysoce kvalifikovanými odborníky dodavatelů přinesla své ovoce. Dnes můžu říct, že Czech POINT pomohl rozhýbat eGONa.“ Ing. Jindřich Kolář, ředitel Odboru rozvoje projektů a služeb eGovernment, MV ČR. Po důkladné analýze požadavků a informací ze strany MV ČR a primárních poskytovatelů dat byl ve spolupráci se společností Software602 a.s. navržen systém postavený na operačním systému SUSE Linux Enterprise Server (SLES), formulářovém serveru 602XML FormServer a Novell Identity Manageru.“ [Novell: Worldwide, 2011]

Novell Identity Manager byl zvolen pro zajištění identifikace, autentizace a autorizace uživatelů přistupujících k systému. Společně s tímto produktem byl nasazen také Identity Manager Roles Based Module, který umožňuje třídit uživatele podle předem definovaných rolí (jak bylo psáno dříve, tak k roli se poté váže přístup). V systému byl tedy vytvořen jednotný identitní prostor pro správu všech uživatelů (Česká pošta, Hospodářská komora ČR, Notářská komora ČR a úřední orgány veřejné moci). Od 1. 3. 2009 je přístup do systému umožněn pouze uživatelům s platným certifikátem. Je to opatření pro zvýšení bezpečnosti. Za správu jednotlivých subjektů jsou zodpovědní lokální administrátoři (vedení uživatelských účtu, změny statusu uživatele, odebrání certifikátu).

Jaká je současnost? Použitím otevřených technologií v operačních systémech SUSE Linux dosáhl provozovatel systému – Ministe"rstvo vnitra ČR – výrazné úspory nákladů jak v oblasti nutných investic do pořízení hardwarového vybavení, tak v nákladech spojených se správou a údržbou potřebné infrastruktury. Novell je už druhým rokem správcem centrály Czech POINT. Systém Czech POINT byl vybudován za dodržení všech legislativních pravidel. Všechny služby, které nabízí, mají oporu v legislativě. Současně bylo při budování systému pamatováno na jeho další rozvoj a rozšiřitelnost v souladu s rozvojem eGovernmentu v České republice. Projekt Czech POINT, který v praxi naplňuje myšlenku z úvodu – „obíhat mají data, ne občan" –, je skutečně ojedinělým projektem i v rámci Evropy. Česká republika díky němu udělala viditelný kus práce v oblasti budování eGovernmentu. O využívání projektu občany České republiky svědčí statistiky vydaných výpisů. Miliontý výstup v projektu Czech POINT byl vydán již v průběhu prvního roku provozu, kdy systém poskytoval výpisy pouze ze čtyř ISVS (Katastr nemovitostí, Obchodní rejstřík, Živnostenský rejstřík a Rejstřík trestů). Největším přínosem systému je jednoznačně úspora času občana při komunikaci s veřejnou správou. [Novell: Worldwide, 2011]

Další úspěšné implementace naleznete na internetové adrese www.novell.cz/cs/aktuality/pripadove-studie/

6.2.2 Oracle

Firma Oracle má velmi úspěšné implementace (Suny, ING, Radnice města Esbjerq, Nemocniční okrsek měst Helsinki a Uusimaa, Turkcell İletişim Hizmetleri) další naleznete na internetové adrese www.oracle.com/cz/products/middleware/identity-management/index.html. Rozhodnout o nejzajímavější je velmi těžké, proto je uveden web, kde jsou k dispozici všechny případové studie.

6.2.3 Microsoft

Jedním z úspěšných projektů je implementace řešení produktu FIM 2010 do banky v Lucembursku. Jedná se o soukromou banku, která svým klientům nabízí služby správy majetku. IT oddělení udržuje IT infrastruktura, ta poskytuje nástroje k usnadnění klíčových bankovních úkolů včetně zpracování tisíce transakcí, které jsou na denní bázi. Mimo toho se spravuje 780 identit a přístupů, které využívají pro svoji práci více než 50 obchodních aplikací a několik heterogenních databází. Řízení identit a přístupu je tedy velmi důležité a to hlavně za účelem kontroly, kdy je třeba zjistit, kdo má jaký přístup k požadovaným datům.

Jak to tedy probíhalo před nasazením FIM 2010? Pro každou ze svých aplikací, které banka využívá, byly manuální procesy pro správu identit zaměstnanců a přístupu. Toto celé řídilo IT oddělení pro bezpečnost. Používaly tabulky pro Windows Server 2008, Active directory, pro vše měly speciální tabulky. Ty se sdíleli mezi dalších 30 osob (pomocí emailu), tak aby se zaznamenala změna role nebo přidání nového pracovníka. Nejenže tento způsob způsoboval dlouhé zpoždění a nepřesnosti, ale také to zvětšilo složitost zajištění bezpečnosti, protože banka musí ochránit citlivá data přístupu ke kritickým operacím. Banka tedy potřebovala centralizované řešení pro správu identit a přístupu. Ve snaze zlepšit elimanovat manuální procesy pro poskytování uživatelských účtů, zvýšit efektivitu IT oddělení a vnitřní soulad. A zejména chránit citlivé a důvěrné informace, tak aby se nemohl narušit provoz neoprávněným přístupem.

V únoru 2010 se banka rozhodla implementovat řešení Microsoft Forefront Identity Manager 2010. Oddělení pro řízení přístupu identifikovalo přes 300 rolí (pokrývající 20 nejvíce používaných bankovních aplikací). Dále byl použit Microsoft Office SharePoint Server (konzole součástí FIM), kde se snadno vytvořily pravidla pro upravení uživatelů a skupin. Poté pomocí aplikace FIM jsou brány informace o zaměstnancích z HR databáze. PeopleSoft se automaticky použije pro definování politik a pak se provede synchronizace s Active Directory. V budoucnu se plánuje implementovat funkce vedení skupiny v Forefront Identity Manager, který umožní zaměstnancům podávat žádosti o členství ve skupině, včetně vedení distribučního seznamu.

"Banka tedy získala následující výhody. Zvýšená produktivita zaměstnanců (automatické poskytování a rušení účtů z centrálního umístění), zjednodušené řízení IT, vylepšené kompliace (pravidelné synchronizování dat, zajištění konzistence a přesnosti dat). Celé řešení zhodnotil René Chevremont (vedoucí správy přístupu) z Banque de Luxembourg říká, „že díky produktu Forefront Identity Manager a službě Active Directory máme ucelené řešení pro správu identit a přístupu, které poskytuje potřebnou podporu pro naše bankovní operace“. [Microsoft Corporation, 2011]

Další úspěšné implementace (T Deutsch Telekom, Dow Corning aj.) naleznete na internetové adrese www.microsoft.com/forefront/identitymanager/en/us/case-studies.aspx

6.2.4 IBM

V České republice proběhla řada úspěšných projektu. Za jeden z nejvýznamnějších je dlouhodobě považováno řešení v bance ČSOB (Československá obchodní banka). K nastudování doporučuji případovou studii, kterou naleznete na následujících internetových stránkách: www.trask.cz/sprava-pristupovych-opravneni-v-csob. V současné době probíhá i projekt centrální administrace uživatelů v Komerční bance. Bohužel data ještě nejsou k dispozici.

7 Závěr

Ano, identity management je velký přínos pro firmy. Bohužel praxe je dnes taková, že firmy se rozhodují pro nasazení řešení správy identit až poté, co se stane nějaký průšvih. Po úspěšné implementaci IM systému získá firma velmi silný nástroj pro centralizaci správy uživatelů (dojde k automatizaci činností, které se správou souvisejí), zvýší se úroveň bezpečnosti, odstraní se byrokracie firmy a zprůhlední se veškeré operace, které uživatel provádí. Pro auditory se jedná o ideální nástroj. Při implementaci se objevují chyby, které se prakticky nedaly předtím zaznamenat. Jsou běžné případy, kdy tentýž uživatel má právo navrhnout nákup a zároveň ho i schválit. Chce-li budoucí organizace (firma) využít všechny možnosti a výhody, které IM poskytuje, tak musí mít co nejlépe definované role a k nim odpovídající přístupová práva. Je nutné předvídat a mít jasně naplánovanou strategii, vytyčené cíle, mít jasno v obchodních procesech, workflow. Pravidlo 2x měř a jednou řež zde platí na 100%. Jelikož implementovat řešení IM je v některých případech velmi složité.

Identity management však skrývá i určitá rizika, která nejsou publikovaná. Za hlavní riziko je třeba považovat centralizované operace. Ty mohou znamenat lákavý cíl pro hackery. Automatizací procesů týkajících se správy přístupů se prakticky usnadní práce správcům IT a pochopitelně i potencionálním útočníkům. Pokud se hackerovi podaří proniknout do systému IM, může si vytvořit vlastní identitu se všemi právy. Tím lze získat neomezený přístup do celopodnikové sítě. K tomuto se váže i zmiňovaný identity thief (krádež identity). Někdy je až velmi jednoduché ukrást identitu. Je to dáno lehkovážností uživatele při volbě hesla. S rostoucím počtem aplikací, které uživatel má k dispozici, roste frekvence opakování toho samého hesla. Z analytického výzkumu je známo, že nejoblíbenější hesla jsou: 123456, password, 12345678, qwerty, abc123, 0. Proto je nutné zvolit pro aplikace, které budou napojeny na IM systém kvalitní politiky hesel. Tím se dá toto riziko snížit.

V diplomové práci jsou představeny komerční a open source nástroje pro identity management. Kdy je patrné, že každá firma má určitou strategii při implementaci. A i své klíčové partnery. V praktické části jsou uvedeny i úspěšně

provedené implementace jednotlivých firem. To je velmi zajímavé, jelikož získáte i pohled zákazníka před a po implementaci. V praktické části je dále zvolen software od IBM. A to konkrétně IBM Tivoli Identity Manager (nejedná se o nejnovější verzi, principiální postup je však stejný). Tento software je vysvětlen po procesní a technologické stránce. Dále je otestován uživatelský pohled. Je velmi důležité, aby se budoucí uživatel (to může být kdokoli z nás) seznámil s nejvíce používanou věcí, tzv. self-reset password. Princip spočívá v tom, že je uživatel schopen si sám resetovat heslo do dané aplikace, kde má přístupová práva. Na první pohled to působí velmi triviálně. Ve velkých podnicích se tato zdánlivá maličkost může stát velice nákladnou a časově náročnou. Podle mých dosavadních pracovních zkušeností a statistik se přibližně polovina hovorů směřujících na help-desk týká žádostí o reset hesla. Je uveden postup, který se dá použít jako návod. Pro uživatele to není žádný problém.

V praktické části je i pohled administrátora, kde jsou vysvětleny jednotlivé funkce systému. Ty jsou demonstrovány na smyšleném příkladu. Smyslem tohoto příkladu je ukázat, jak v praxi probíhá instalace a připojení aplikace k IM systému. Poté vytváření skupin, na jejichž základě se vytvoří odpovídající provisioning policy. Dále organizační role a poté bude založen nový uživatel, který získá roli s automatickým přístupem do systému. Vše je vysvětleno krok za krokem, tento postup se opět dá použít jako samostatná administrátorská příručka. Z důvodu přehlednosti příruček nebyly obrázky uvedeny v seznamu obrázků na začátku diplomové práce.

Seznam použitých zdrojů

BLAŽEK, Vojtěch. V Česku se objevil nový zločin. Na internetu se krade vaše "já". *IHNed.cz : Online zprávy hospodářských novin* [online]. 2009-07-12, 0, [cit. 2011-02-28]. Dostupný z WWW: <http://domaci.ihned.cz/c1-37765240-v-cesku-se-objevil-novy-zlocin-na-internetu-se-krade-vase-ja>

Česko. Opatření České Národní Banky č. 2 ze dne 3. Února 2004 k vnitřnímu řídícímu a kontrolnímu systému bank. Věstník ČNB. Ze dne 16. února 2004, částka 3/2004, s. 16. Dostupný také z WWW: <http://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/legislativa/vestnik/2004/download/v_2004_03_10204510.pdf>

Czech POINT *[*online]. c2010 [cit. 2011-01-21]. Dostupné z WWW: <http://www.czechpoint.cz/web/index.php>

E-business|ShopCentrik [online]. c2010 [cit. 2011-02-28]. *E-business*. Dostupné z WWW: <http://www.shopcentrik.cz/slovnik/e-business.aspx>.

FOJTÍK, Jaroslav. Proč zavést identity a access management. *Data v péči MHM* [online]. 2009-11-30, 2009, č. 16, [cit. 2010-04-12]. Dostupný z WWW: <http://www.datavpeci.cz/webdvp.nsf/0/92A797DB18ED18C5C12576780030A3A3>.

FreeIPA. FreeIPA [online]. 2010-06-15 [cit. 2011-03-14]. Administration Reference. Dostupné z WWW: <http://freeipa.org/docs/2.0.0/Reference_Guide/en-US/html/>

IBM [online]. c2011 [cit. 2011-03-04]. Tivoli Identity Manager. Dostupné z WWW : < http://www-142.ibm.com/software/products/cz/cs/identity-mgr/>.

IBM-Identity and access management services [online]. 2009 [cit. 2011-02-28]. Identity and access management services. Dostupné z WWW: <http://www-935.ibm.com/services/cz/index.wss/offerfamily/gts/cz027701>.

ID Theft Instruction [online]. c2010 [cit. 2011-03-14]. 5 Common Types of Identity Theft. Dostupné z WWW: <http://www.idtheftinstruction.com/solutions.html>

iHNed.cz. Úřady v USA odhalily největší krádež identity v historii internetu. *IHNed.cz : Online zprávy hospodářských novin* [online]. 2009-08-17, 0, [cit. 2010-10-13]. Dostupný z WWW: <http://ekonomika.ihned.cz/c1-38083460-urady-v-usa-odhalily-nejvetsi-kradez-identity-v-historii-internetu>.

JENÍK, Ing. Lukáš. Zabezpečení IT infrastruktury a identity management. *IT SYSTEM* [online]. 2004-03-01, 2004, č. 3, [cit. 2010-08-28]. Dostupný z WWW: <http://www.systemonline.cz/clanky/zabezpseceni-it-infrastruktury-a-identity-management.htm>.

LÍZNER, Martin. Identity management – centrální správa uživatelských účtů. *Security World* [online]. 24. 05. 2010, č. 5, [cit. 2010-02-28]. Dostupný z WWW: <http://securityworld.cz/securityworld/identity-management-centralni-sprava-uzivatelskych-uctu-2780>.

***Microsoft Corporation** : Cloud Computing, Software, Online Games, IT Business Technology, Smartphones and Entertainment* [online]. c2011 [cit. 2011-01-12]. Dostupné z WWW: <http://www.microsoft.com/en-us/default.aspx>

Novell: Worldwide [online]. c2011 [cit. 2011-03-14]. Dostupné z WWW: <http://www.novell.com/home/>

O2 - Neřešení identity managementu znamená nekontrolovaný únik dat. *ICT Security : Nezávislý odborný on-line magazín* [online]. 2010-10-01, [cit. 2011-02-28]. Dostupný z WWW: <http://www.ictsecurity.cz/10/08/1-rizeni-pristupu-autent-a-identity-man/o2-nereseni-identity-managementu-znamena-nekontrolovany-unik-dat.html>.

Oracle: Hardware and Software, Engineered to Work Together [online]. c2011 [cit. 2011-01-14]. Administration Reference. Dostupné z WWW: <http://www.oracle.com/index.html>

Technet [online]. 2010-02-01 [cit. 2011-03-16]. RSA Conference 2010: Identity at the Forefront. Dostupné z WWW: <http://blogs.technet.com/b/forefront/archive/2010/03/02/rsa-conference-2010-identity-at-the-forefront.aspx>