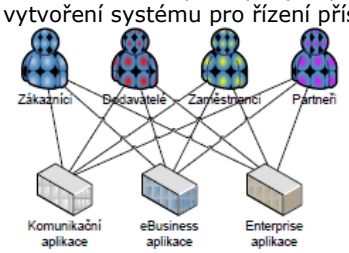
LDAP adresářové servery pro správu uživatelských
Identit

Správa uživatelských identit

Identity management „IDM" je infrastruktura a business procesy pro správu celého životního cyklu a následného využití, zahrnující definici prvků, ověřování a oprávnění. IDM pokrývá firemní procesy aplikované na všechny provozní operace v celé ICT infrastruktuře. Identita v rámci IDM může být spojena s uživatelem, službou, zařízením nebo komunitou.

Vývoj a popis IDM

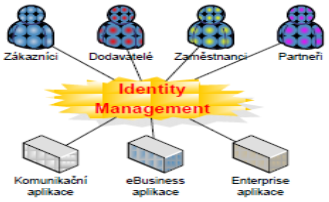
S rostoucím počtem uživatelských aplikací a potřebou definice přístupových pravidel a rolí pro různé uživatele a komunity bylo poukázáno na nutnost vytvoření systému pro řízení přístupů k síťovým zdrojům.



Obrázek 1 Heterogenní IDM

Typicky každý podnik využívá při vývoji a implementaci aplikací vlastní uživatelské a IDM rozhraní a vlastní schémata pro zabezpečení těchto aplikací. Tato metoda nasazení vede k vytvoření heterogenního systému bez centrální správy systémů a s tím související neexistence flexibility při dalším růstu a plnění pozdějších úkolů spojených s nasazováním nových aplikací či prostředí. Tento trend může například negovat výhody vývoje internetových aplikací a dostupnosti v rámci celé firemní infrastruktury včetně připojení k dalším subjektům. Následně dochází ke zvyšování nákladů na nasazení, administraci a údržbu takto řešených systémů. Další nevýhodou je zvýšené bezpečnostní riziko a prakticky zmražený další vývoj některých důležitých částí takto řešeného systému. Informace o uživatelských identitách a bezpečnostních politikách jsou distribuovány přes velké množství aplikací a datová úložiště jsou dostupná a kontrolována různými interními i externími skupinami. Potřeba větší flexibility přístupů a silnějšího zabezpečení omezuje nadbytečnost administrativních úkonů a nekonzistentnost dat přes celou společnost včetně problematického nastavování ad-hoc bezpečnostních strategií. Prostředí s různorodými zdroji identifikačních informací implementují rozdílné přístupy pro organizaci uživatelských entit, bezpečnostních praktik, řízení přístupů a dalších aspektů potřebných v informační architektuře. Komplikovanost interního prostředí v rámci IDM může být dále rozšiřováno za hranice prostředí uvnitř jedné firmy. V tomto případě je architektura rozšiřována z individuální sféry na úroveň tzv. federativních modelů IDM – „FIDM". Modely FIDM jsou užívány pro propojování a správu zdrojů a s tím související zajišťování efektivní a bezpečné spolupráce mezi dalšími subjekty, kterými mohou být zákazníci, obchodní partneři či dodavatelé. To vše s ohledem na soukromí, snadné využití spotřebiteli a musí splňovat požadavky na rozšiřitelnost a aplikační nenáročnost správy od jednotek až po tisíce až milióny entit. V případě, že je nasazována nová aplikace bez použití společné infrastruktury IDM, bezpečnostní rozhodnutí a řízení je typicky ve správě týmu vývoje aplikací a systémových administrátorů. Přímo nadřízení manažeři nemohou zajistit, aby správní lidé viděli to, co přesně mají a ve správný čas.

Manažeři musí uplatnit bezpečnostní politiku centrálně a aplikovat ji lokálně. Bezpečnostní politiky definují, jak jsou uživatelé identifikováni, ověřeni a současně definují, kteří uživatelé mohou přistupovat k jakým zdrojům – autorizace. Některé služby neb transakce potřebují jiné formy ověření nežli jiné. Pro některé aplikace může být dostačující použití uživatelského jména a hesla, pro jiné je možné přístupy dále kategorizovat v rámci bezpečnostních politik. Silnější úrovně mohou mít formát digitálních certifikátů a osobních identifikačních čísel „PIN", v závislosti na povaze informací a transakcí. Autorizace je identifikována pomocí jednoznačné lokalizace zdroje „URL" a může být přidružena k množině či skupině uživatelů a uživatelských rolí. Pokud se změní vlastnost uživatelské role, tato změna se projeví současně ve všech systémech využívajících IDM.



Obrázek 2 Centralizovaný IDM

Rozšířením stávající infrastruktury může IDM přinést sloučení roztříštěných identifikačních dat do jednoho celku s dalšími možnostmi, které lze využít v podnikové sféře:

- Konzistentní bezpečnostní politika přes celou síť
- Centralizované ověřování a autorizace
- Řízení celého životního cyklu identity
- Využití možnosti single sign-on pro jednorázové přihlášení do systému
- Pro obchodní partnery poskytuje IDM řešení podnikových vztahů se snížením rizika podvodných transakcí

Přesun k novým *inteligentním* aplikacím a operačním systémům požaduje implementaci systémů zahrnujících správu uživatelů i přístupů. Takové systémy dovolují administrátorům centralizovat jejich správu jak na úrovni řízení uživatelů, uživatelských rolí, přístupů a bezpečnostních politik v rámci organizace s ohledem na nepřeberné množství různých zdrojů.

Úkoly a cíle systémů pro IDM

Sloučení všech prvků infrastruktury řízení identit umožňuje administrátorům snižovat množství duplicitních úkolů napříč všemi spravovanými aplikacemi a systémy. Toto sloučení umožňuje delegování úkolů k dalším subjektům v závislosti na konkrétních požadavcích. Výsledkem takového prostředí je integrální, flexibilní, bezpečný a jednoduše řízený systém.Systémy IDM poskytují integrální platformu, která zahrnuje nepřeberné množství dílčích částí:

- Bezpečné ověřování
- Kontrola přístupů
- Audity
- Zajištění synchronizace identit s delegováním možností
- Federativní řízení identit

☐☐Podpora Security Assertion Markup Language „SAML"
☐☐Vysoký výkon
☐☐Vysokou dostupnost
☐☐Snadnou rozšiřitelnost

Implementací IDM získává společnost výhody v silnější bezpečnosti ve všech síťových aplikacích, zvýšení produktivity a snížení nákladů na administraci. Společné řešení pomáhá společnosti zaměřit se na jejich hlavní činnosti a vyvíjet aplikace jako část integrálního celku se zapojením dalších moderních technologií. IDM poskytuje společnosti možnosti pro identifikování problémů a současně dokáže tyto problémy řešit. Poskytuje také základ pro nasazování nových služeb v budoucnosti. Pro dosažení stále se rozvíjejících požadavků enterprise, musí systémy pro správu identit splnit:

☐☐*Hloubka* – společnosti vyžadují přínos IDM na mnoha úrovních, od základního provisioningu, řízení přístupů, možností zabezpečení pro zautomatizování poskytování a delegování na základě rolí a pravidel, federativní SSO a bezpečnost internetových služeb.

☐☐*Shoda* – dnešní společnosti vyžadují infrastrukturu, která napomáhá zajistit shodu s požadavky regulátorů a interních politik, a musí být schopna dalšího rozšiřování a změn.

☐☐*Rozšiřitelnost* – řešení IDM musí být schopny rozvíjení přes celý enterprise segment.

☐☐*Integrace* – komponenty IDM jsou vyvíjeny pro úzkou spolupráci s dalšími prvky v IT infrastruktuře.

Lightweight Directory Access Protocol

Lightweight Directory Access Protocol „LDAP" je protokol vytvořený pro ukládání a přístup k datům umístěných na adresářovém serveru „DS".

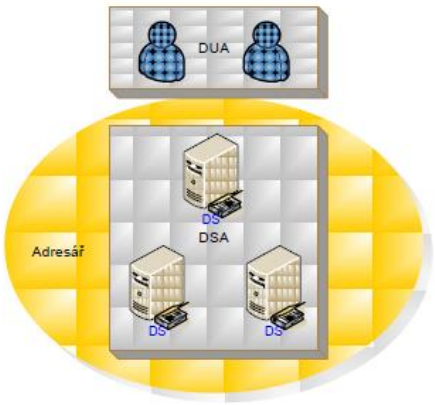
Standardy a doporučení DAP a LDAP

Protokol LDAP vychází z Directory Access Protocol „DAP", který byl vytvořen na základě doporučení X.500, které bylo vyvinuto a přijato organizací International Consultative Committee of Telephony and Telegraphy „ICCTT". Vzhledem ke složitosti protokolu DAP byla vytvořena organizací Internet Engineering Task Force „IETF" odlehčená verze, LDAP, která byla akceptována jako standard ve světě ICT. Jednotlivé standardy a doporučení vztahující se k DAP a LDAP lze nalézt v přílohách *15.1 Seznam standardů DAP* a *15.2 Seznam doporučení LDAP*. Služby poskytované adresářovým serverem je možné nalézt v ITU-T Rec. X.511.

Popis a cíle LDAP

Rozlehlé firemní počítačové sítě s velkým množstvím terminálů, síťových komponent, aplikací a uživatelů vždy vyžadovali informační systém, který poskytuje jména, adresy a další důležité atributy o lidech a objektech zahrnutých k komunikaci. Z pohledu uživatele je adresář databáze, kde jsou uloženy informace o skutečných objektech a tyto informace jsou dostupné na vyžádání. Tato databáze je označována jako adresářová informační báze „DIB". Každý známý objekt v adresářové službě je reprezentován záznamem v DIB.

Jednotlivé entity adresáře X.500 jsou na adresářovém serveru uspořádány do stromové struktury pod společnou entitou *root*. Hierarchie obsahuje prvky (anglicky): country, organization, organization unit a person. Záznam v každé z těchto větví musí obsahovat určité atributy, z nichž některé jsou povinné a jiné volitelné. V každém firemním prostředí může být adresář implementován jinou cestou tak, aby bylo dodrženo základní schéma nebo určitý plán.

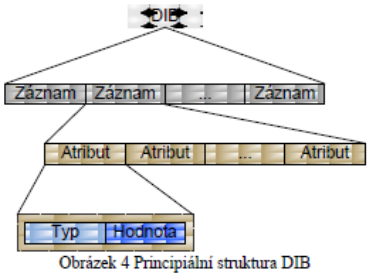


Obrázek 3 Distribuovaný globální adresář X.500

Distribuované globální adresáře pracují skrze registrační proces a jedno nebo více centrálních míst, které spravují adresáře. V X.500 je každý lokální adresář nazýván Directory System Agent „DSA". DSA může být reprezentován jednou nebo skupinou organizací. Jednotlivé DSA jsou vzájemně propojeny v Directory Information Tree „DIT". Uživatelský program přistupující k jednomu nebo více DSA je nazýván Directory User Agent „DUA".

Directory Information Base „DIB"

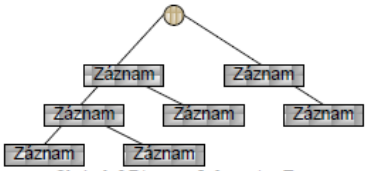
Soubor všech informací uložených v adresáři je znám jako Directory Information Base „DIB". Skládá se ze záznamů, kde každý jednotlivý obsahuje informaci o jednom objektu. Objekt je identifikován atributy, které můžou být definovány různým typem a jednou nebo několika hodnotami. Typ atributu záleží na třídě objektu, který popisuje záznam. Objekty mající podobné vlastnost jsou identifikovány vlastní třídou objektů. Každý záznam v adresáři je členem minimálně jedné třídy objektu. DIB a jeho struktura je definována v ITU-T Rec. X.501.



Obrázek 4 Principiální struktura DIB

Directory Information Tree „DIT"

Informace uložené v DIB mají přesnou strukturu a hierarchii využívající stromovou strukturu. DIB je tedy reprezentován jako Directory Information Tree „DIT", kde každý uzel ve stromě reprezentuje záznam adresáře.



Obrázek 5 Directory Information Tree

Jmenná konvence

Každý objekt uložený v adresáři je rozeznán od ostatních objektů svým jednoznačným názvem, které se označuje jako Distinguished Name „DN". Každý jednotlivý záznam přebírá od svého nadřazeného záznamu jeho název, který je připojen k jeho vlastnímu názvu Relative Distinguished Name „RDN".

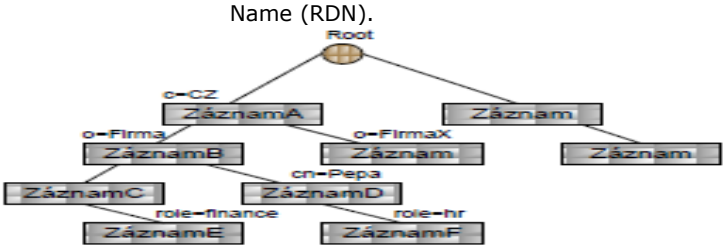
Sufix (jmenný kontext)

Sufix (přípona) je DN, které identifikuje nejvyšší záznam v lokální adresářové hierarchii. Protože LDAP používá relativní jmenné schéma, toto DN je také sufixem každého dalšího záznamu v adresářové hierarchii. Adresářový server „DS" může obsahova několik různých sufixů, každý identifikující vlastní adresářovou hierarchii.

Příkladem může být o=Firma,c=CZ.

Relative Distinguished Name „RDN"

V hierarchicky organizovaném adresářovém stromu jsou objekty identifikovány unikátní cestou jmen patřící nadřazenému objektu. Například v hierarchii poštovní adresy, objekt *ulice* může zahrnovat jméno města, stát a zemi. Tento název se označuje jako Distinguished Name (DN). Název jednoho objektu z pohledu objektu druhého je označován jako Relative Distinguished Name (RDN).

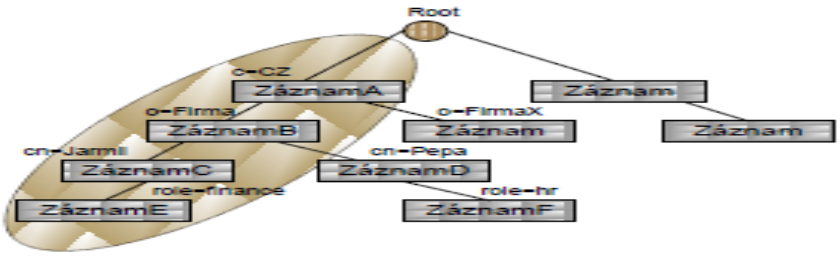


Obrázek 6 Relative Distinguished Name „RDN"

Na obrázku výše je například RDN záznamu *ZáznamA* název *c=CZ*.

Distinguished Name „DN"

Distinguished Name (DN) je globální autoritativní název instance v adresáři dle OSI X.500. DN je obsahem globální unikátní identifikace uživatelů nebo systémů. DN například zajišťuje, že digitální certifikát vydaný konkrétnímu člověku nemůže být použit jinou osobou stejného jména. DN unikátně identifikuje záznam vztahující se k rootu objektu, případně je DN celé jméno objektu. DN se skládá ze setříděného seznamu RDN, začínající rootem objektu



Obrázek 7 Distinguished Name „DN": c=CZ, o=Firma,cn=Jarmil,role=finance

DN záznamu *ZáznamC* je tedy *c=CZ,o=Firma,cn=Jarmil*.

Adresářové schéma

Adresářové schéma je množina pravidel zaručující, že DIB zůstane z pohledu dalších změn stále ve stejné podobě. Obsah záznamů ve strumě je určen právě adresářovým schématem. Díky těmto pravidlům se předchází možnosti mít špatně nastavené atributy pro jednotlivé třídy objektů. Schéma definuje typy atributu, které může adresářový záznam obsahovat. Schéma definuje třídy objektu. Každý záznam musí mít atribut *objectClass*, obsahující pojmenovanou třídu definovanou v adresářovém schématu. Typicky je atribu objectClass vícehodnotový a obsahuje třídu *top* stejně jako čísla dalších tříd. Definice schématu pro každou třídu záznamu vymezuje, jaký druh objektu může záznam reprezentovat. To znamená, že členství v konkrétní třídě dává záznamu možnost obsahovat alternativní množinu atributů a povinnost obsahovat další povinný soubor atributů.

Například záznam reprezentující osobu může patřit třídám *top* a *person*. Členství v třídě *person* vyžaduje nutnost vyplnit atributy *sn* a *cn*, a dovoluje *userPassword*,
telephonNumber a další.

objectclass (2.5.6.6 NAME 'person'
DESC 'RFC2256: a person'
SUP top STRUCTURAL
MUST (sn $ cn)
MAY (userPassword $ telephoneNumber $ seeAlso $ description))
attributetype (2.5.4.3 NAME ('cn' 'commonName')
DESC 'RFC2256: common name(s) for which the entity is known by'
SUP name)

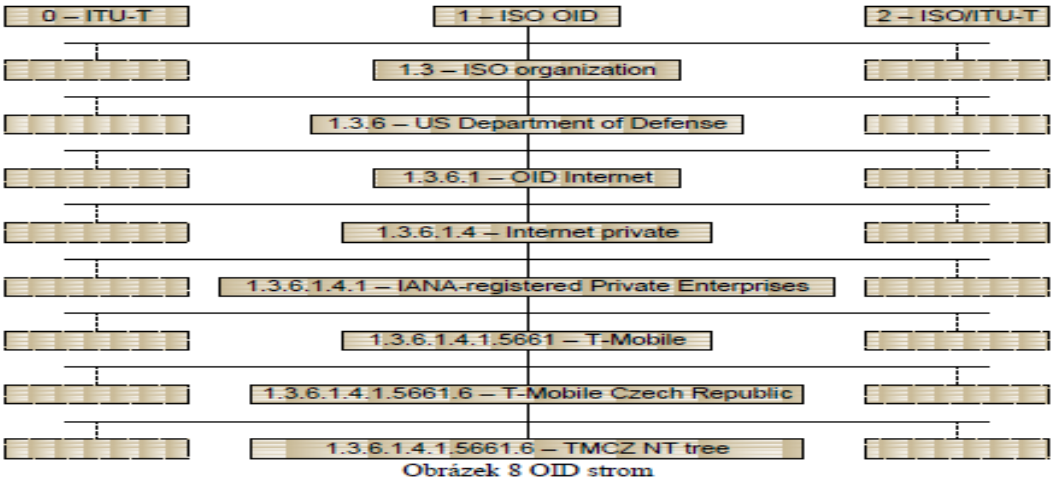
Jelikož můžou záznamy náležet do několika tříd, každý záznam obsahuje směs volitelných a povinných množit atributů sjednocených tříd objektů, které obsahují. Většina adresářových schémat obsahuje jméno a globální unikátní identifikátor objektu OID (Object Identifier).

Identifikátor objektu

Každá třída objektu, atribut nebo typ atributu musí mít unikátní identifikátor umožňující adresářové službě správné rozlišení. Tento unikátní identifikátor se nazývá OID (Object Identifier). OID poskytuje informaci, jak jsou atributy uloženy v adresáři stejně jako vodítko pro správné pojmenování. Strukturálně se OID skládá z hierarchicky poskládaných uzlů namapovaných ve jmenném prostoru.

attributetype (1.3.6.1.1.1.1.0 NAME 'uidNumber'
DESC 'An integer uniquely identifying a user
in an administrative domain'
EQUALITY integerMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE)
attributetype (1.3.6.1.1.1.1.1 NAME 'gidNumber'
DESC 'An integer uniquely identifying a group
in an administrative domain'
EQUALITY integerMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE)
attributetype (1.3.6.1.1.1.1.2 NAME 'gecos'
DESC 'The GECOS field; the common name'
EQUALITY caseIgnoreIA5Match
SUBSTR caseIgnoreIA5SubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE)
attributetype (1.3.6.1.1.1.1.3 NAME 'homeDirectory'
DESC 'The absolute path to the home directory'
EQUALITY caseExactIA5Match
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE)

Formálně jsou OID definovány dle standardu ITU-T ASN.1. Následná čísla uzlů, začínající rootem stromu, identifikují každý jednotlivý uzel ve stromě. Návrháři umisťují nové uzly pomocí registrace pod registrační autoritou každého jednoho uzlu.



Obrázek 8 OID strom

Uvnitř schémat LDAP, každá třída a každý atribut má unikátní OID.

Bezpečnost LDAP

Vzhledem k důležitosti a s ohledem na informační hodnotu dat uložených v adresářovém serveru je nedílnou součástí LDAP bezpečnostní politika. Celý bezpečnostní model je popsán v konkrétních dokumentech RFC.

RFC 2829 – Authentication Methods for LDAP definuje základní hrozby pro LDAP adresářové služby:

☐☐Neautorizovaný přístup přes operaci data-fetching
☐☐Neautorizovaný přístup s použitím informací získaných monitoringem cizích přístupů
☐☐Neautorizovaný přístup k datům získaných monitoringem cizích přístupů
☐☐Neautorizovaná úprava dat
☐☐Neautorizovaná úprava konfigurace
☐☐Neautorizované nebo nadměrné využití zdrojů – DoS
☐☐Vydávání se za adresářový server

LDAP v3 uplatňuje čtyři typy ověřování:

☐☐Bez ověření – anonymní přístup

Anonymní přístup slouží pro přístup do adresáře bez poskytnutí ověřovacích informací. S řízením kontroly přístupů můžeme nastavit anonymním uživatelům přístupová práva dle našeho uvážení. Často jsou anonymním uživatelům zpřístupněny pouze data takové povahy, která nejsou citlivá, jako jména, telefonní čísla a emailové adresy. Lze tedy například zabezpečit přístup pouze k určitému typu atributů, obsahující pouze informace o kontaktech.

☐☐Základní ověření

Ověření se uskutečňuje na základě znalosti DN (Distinguished Name) a hesla. Data jsou přenášena v textovém formátu nebo zakódována pomocí Base64.

Obrázek 9 Ověření založené na hesle

☐☐Ověřování pomocí PKI

Pro ověření klient digitálně podepíše náhodně vygenerovaný řetězec dat a pošle je spolu s certifikátem na server. Na serveru se provede ověření certifikátu porovnáním s certifikátem uloženým na serveru.

Obrázek 10 Ověření založené na certifikátu

☐☐Jednoduché ověření a s použitím SASL

Simple Authentication and Security Layer „SASL" je framework zásuvných modulů pro použití alternativních bezpečnostních mechanismů. Tyto mechanismy zahrnují: Kerberos v4, S/Key, GSSAPI, CRAM-MD5, TLS, ANONYMOUS

Zabezpečení komunikace je možné díky StartTLS/SSL. SSL je protokol, který je určen pro zabezpečení komunikace a provádění ověřování. Primárně slouží pro zabezpečení TCP/IP jako transparentní mezivrstva mezi aplikací a sítí.

Další prvkem zabezpečení adresářových služeb LDAP je tzv. řízení přístupů k obsahu uloženému v adresáři. Toto řízení se provádí pomocí ACI (Access Control Instructions). Mechanismus, kterým se definuje přístup k datům, se nazývá řízení přístupu (Access Control). V případě že adresářový server přijme požadavek, použije ověřovací informace poskytnuté uživatelem v operaci *bind* a ACI definované v adresáři pro povolení nebo zakázání přístupu k adresářovému obsahu. Server muže povolit nebo zakázat přístup pro operace čtení, zápisu, vyhledávání nebo porovnání. Úroveň zabezpečení může záležet na poskytnutých ověřovacích informacích.

Za použití ACI můžeme řídit přístup k celému adresáři, stromu, části stromu, jednotlivým záznamům nebo specifické množině atributů. Práva lze nastavit pro jednotlivé uživatele, skupinu uživatelů nebo všechny uživatele v adresáři. Lze také řídit přístup pro klienty s určitou IP adresou nebo doménovým jménem. ACI jsou uloženy v adresáři jako atributy záznamů. Atribut *aci* je atributem operativním. Je použit adresářovým serverem pro vyhodnocení informace, jaká práva jsou povolena nebo zakázána v případě obdržení LDAP požadavku ze strany klienta. Atribut *aci* je také vracen na vyžádání operace *ldapsearch*.

Třemi hlavními částmi pravidla ACI jsou:

☐☐Cíl – určuje záznam nebo atributy, na které se pravidlo vztahuje

☐☐Práva – určuje, které operace jsou povoleny nebo zakázány

☐☐Uživatel – určuje pro koho je ACI pravidlo určeno. Uživatel je identifikován pomocí DN.

Každý adresářový produkt používá vlastní syntaxi ACI (příklad OpenLDAP a OpenDS):

```
# users can authenticate and change their password
access to attrs="userPassword,sambaNTPassword,sambaLMPassword"
by dn="cn=samba,ou=DSA,dc=firma,dc=cz" write
by dn="cn=smbldap-tools,ou=DSA,dc= firma,dc=cz" write
by dn="cn=nssldap,ou=DSA,dc= firma,dc=cz" write
by dn="uid=root,ou=People,dc= firma,dc=cz" write
by dn="cn=syncuser,ou=DSA,dc= firma,dc=cz" write
by anonymous auth
by self write
by * none
access to *
by dn="cn=samba,ou=DSA,dc= firma,dc=cz" write
by dn="cn=syncuser,ou=DSA,dc= firma,dc=cz" read
by * read
(target="ldap:///")(targetscope="base")(targetattr="objectClass||
namingContexts||supportedAuthPasswordSchemes||supportedControl||
supportedExtension||supportedFeatures||supportedLDAPVersion||
supportedSASLMechanisms||vendorName||vendorVersion")
(version 3.0; acl "User-Visible Root DSE Operational Attributes";
allow (read,search,compare) userdn="ldap:///anyone";)
```

Replikace

Replikace adresářového obsahu umožňuje dosahovat vyšší dostupnosti a výkony adresářových služeb. Replikace je mechanismus, kdy jsou data z jednoho adresářového serveru automaticky kopírována do jiného adresářového serveru. S použitím replikace může být jakýkoli DIT, nebo část DIT, kopírován mezi servery. Adresářový server plnící funkci master, automaticky kopíruje informace o změnách do ostatních replik. Replikací adresářových dat můžeme snižovat zatížení jednoh serveru, snižovat čas odpovědí a poskytovat vyšší stabilitu. Replikace záznamů adresáře co nejblíže k uživateli nebo aplikaci můžeme více snižovat latenci. Replikace není primárně určena pro rozšiřování možností zápisu do adresáře. Jakákoli databáze účastnící se replikace se nazývá *replika*. Používají se tři typy replik:

☐☐*Master replika* je replika sloužící jak pro čtení tak i pro zápis. Obsahuji hlavní kopii adresářových dat. Master replika vykonává následující úkony:

o Odpovídá za změny uvnitř adresáře a čtení záznamů klienty
o Udržuje historické informace o replice a udržuje protokol o dotazech
o Inicializuje replikaci do ostatních replik

☐☐*Slave replika* je podřízenou replikou, která slouží pouze pro čtení záznamů z adresáře. Slave replika vykonává následující úkony:

o Odpovídá za čtení záznamů klienty
o Udržuje historické informace o replice a udržuje protokol o dotazech
o Mění data ve své databázi na základě požadavků master repliky

☐☐*Centrální slave replika* je službou určenou pouze pro čtení. Tato replika je podobná slave replice s tím rozdíle, že je na adresářovém serveru umístěno více slave replik.

Centrální slave replika vykonává následující úkony:

o Odpovídá za čtení záznamů klienty
o Udržuje historické informace o replice a udržuje protokol o dotazech
o Inicializuje replikaci do slave replik
o Mění data ve své databázi na základě požadavků master repliky

Replikace poskytuje následující výhody:

☐☐*Fault tolerance a failover* – replikace DIT přes několik serverů, kdy je adresářová služba dostupná i v případě výpadku některého z adresářových serverů.

☐☐*Load balancing* – replikace DIT přes několik serverů snižující zatížení jednoho stroje, což má za následek zvýšení rychlosti odezvy na dotazy.

☐☐*Vysoký výkon a zvýšení rychlosti odezvy* – replikace adresáře blíže k uživatelům nebo aplikacím přímo zvyšuje rychlost odezvy na dorazy.

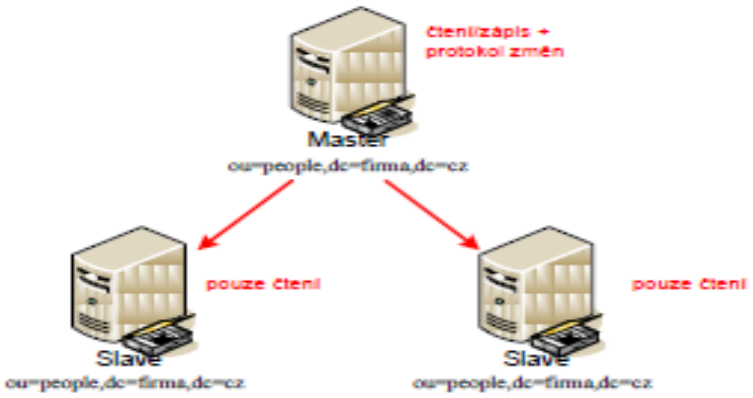
☐☐*Místní správa dat* – replikace dovoluje lokální správu a vlastnictví DIT a současné sdílení v rámci enterprise sítě.

Nejmenší jednotkou určenou k replikaci je *suffix*. Nicméně není možno replikovat dva jmenné kontexty uložené na master replice do jednoho uloženého na slave replice. Pro odlišení master replik se používá unikátní identifikátor, kterým je 16b číslo mezi 1 – 65534. Slave repliky používají 65535. Toto číslo slouží k identifikaci replik sloužících k zápisu. Pokud je na master adresářovém serveru použito několik jmenných kontextů, mohou používat stejný identifikátor pro identifikaci serveru, na kterém se změny provádí. Vztahy mezi repliky jsou řešeny v konfiguraci replikace. Tato konfigurace je uložena na master replice a obsahuje následující parametry:

☐☐*Suffix* určený k replikaci
☐☐Slave server, na který jsou data odesílána
☐☐Plán replikací
☐☐DN a heslo pro komunikaci mezi replikami
☐☐Nastavení zabezpečení
☐☐Nastavení atributů zahrnutých v případě částečné replikace
☐☐Skupina a velikost okna definující množství dat odeslané slave replice před potvrzením přijetí
☐☐Případné nastavení stupně komprese u některých systémů

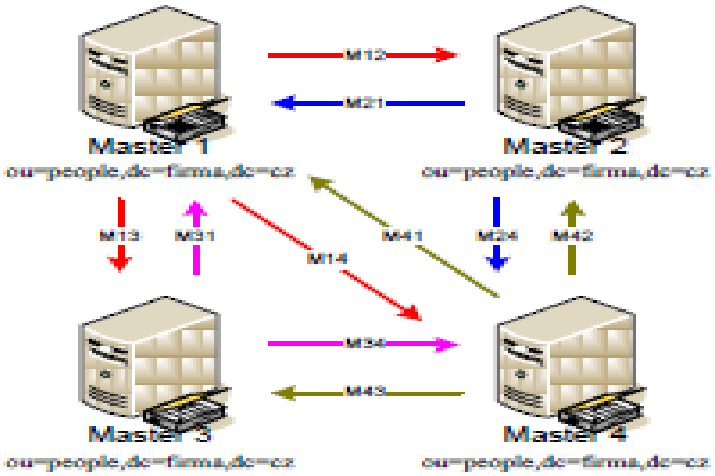
Na základě požadavků na topologii replik a vzájemné konfiguraci existuje několik scénářů replikací:

☐☐*Single master replikace* jejíž použití ne nejzákladnější replikační konfigurací obsahuje master repliku kopírující data přímo do jednoho nebo více podřízených serverů, které slouží pouze pro obsluhu dotazů klientů. Veškeré změny klienty jsou prováděny pouze v master replice.



Obrázek 11 Single master replikace

☐☐*Multi-master replikace* neobsahuje žádné slave repliky. V tomto prostředí master repliky obsahují stejná data. Tato data mohou být současně upravována na několika různých geografických místech. Změny jsou poté replikovány na ostatní adresářové servery.

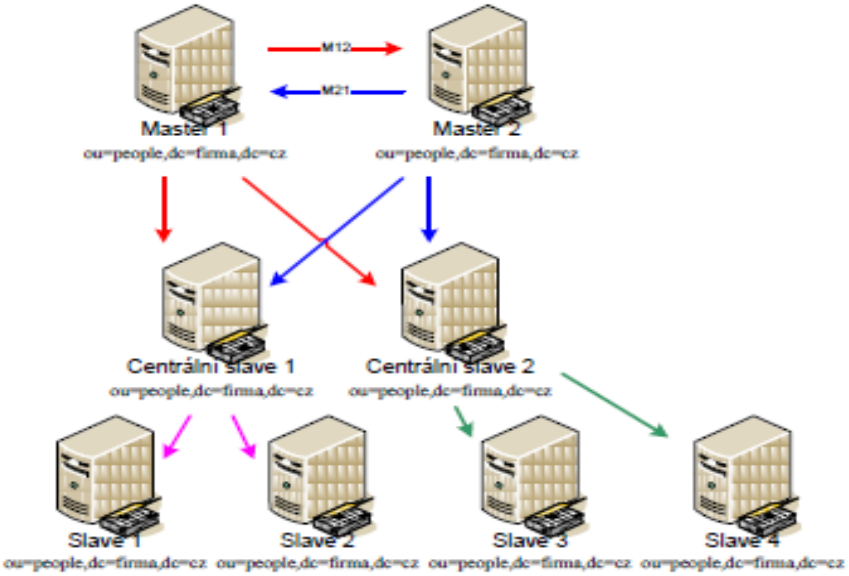


Obrázek 12 Multi master replikace

□□*Kaskádní replikace* využívá centrální slave repliky, která přebírá změny z master repliky a poskytuje je dále slave replice. Centrální slave replika se tedy chová jako slave replika v kombinaci s master replikou, která je pouze pro čtení.

Obrázek 13 Kaskádní replikace

□□*Smíšená topologie* obsahuje všechny výše zmíněné scénáře, od multi-master až po kaskádní konfiguraci replik.



Obrázek 14 Smíšená topologie

Dostupná LDAP řešení

Na základě specifikací a doporučení bylo vyvinuto nepřeberné množství LDAP řešení. Všechna tato řešení mají několik zásadních cílů, a těmi jsou dostupnost pro určitou skupinu zákazníků, dostupné vlastnosti a otevřenost. V dnešním enterprise světě pomalu začíná převládat množství open-source řešení, která umožňují poskytovat velice výkonná řešení podporovaná komunitními vývojáři a přispěvovateli. Tato strategie návrhu a vývoje umožňuje šetřit další peněžní zdroje. Tato otevřená řešení je možné nalézt i v komerčním světě, kde je možné k přesně cílenému produktu dokoupit potřebnou podporu ze strany

přispěvovatelů nebo správců komunitních řešení. Vedoucí pozici v tomto segmentu zaujímají společností Sun Microsystems, Red Hat a Novell.

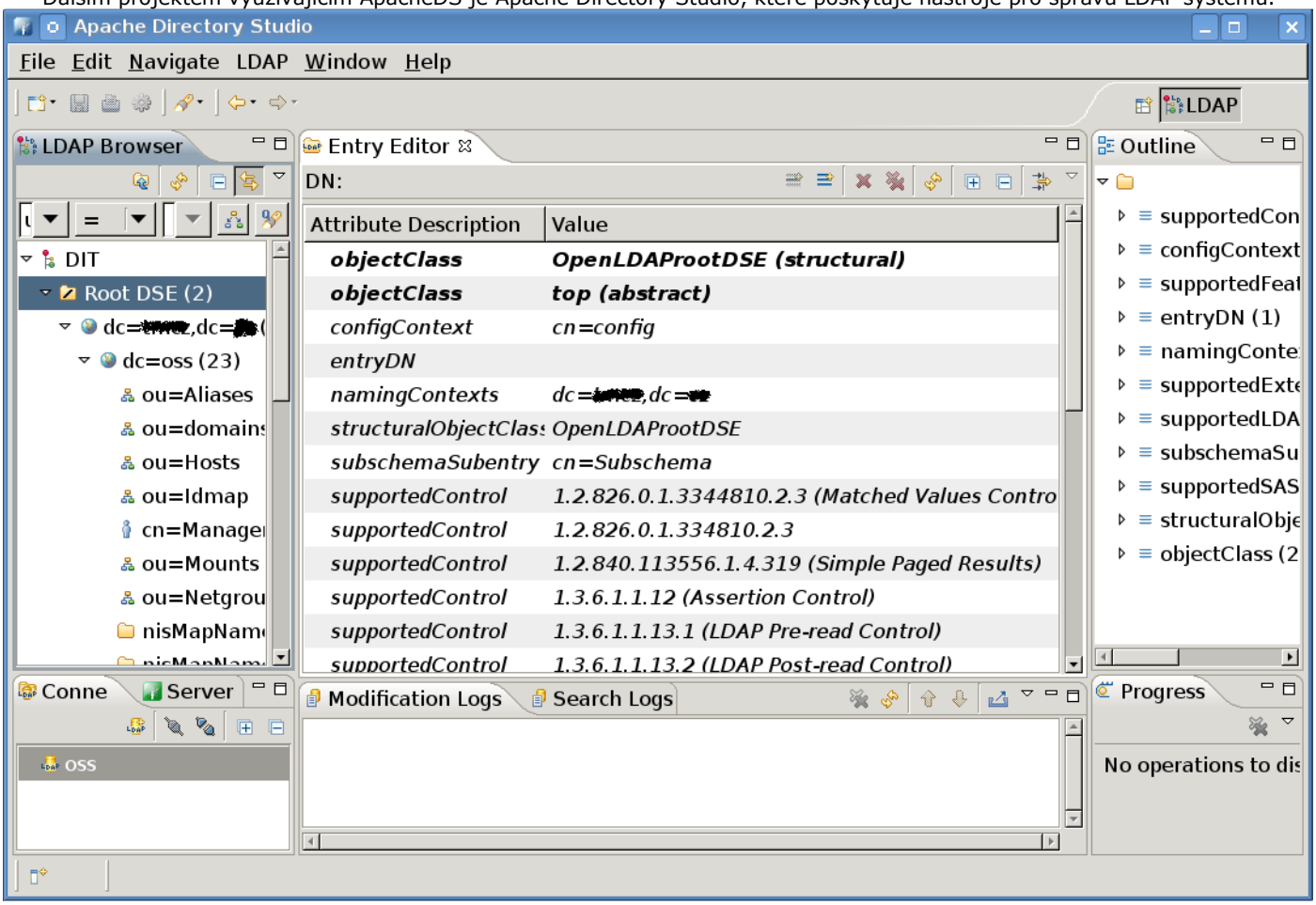
Apache Directory Server

Apache Directory Server je malý, rozšiřitelný moderní LDAP server, který vyvíjen jako open-source pod záštitou Apache Software Foundation. Tento adresářový server je kompletně vyvíjen pomocí technologií založených na jazyce Java. Projekt je dostupný pod licencí Apache Software License.

ApacheDS je možno používat jako součást jiných Java projektů, běžících uvnitř stejného prostředí JVM, ať se jedná o aplikační servery jako GlassFish, Sun Web Server, Apache Tomcat, Apache Geronimo, Oracle Application Server, Oracle – BEA Weblogic, IBM WebSphere, jBoss Application Server, nebo samostatně jako služba Windows. Díky své přenositelnosti a nezávislosti na platformě, může být adresářový systém ApacheDS provozován pod různými operačními systémy, zahrnující Microsoft Windows, Sun Solaris, OpenSolaris, Ubuntu GNU Linux, Redhat Enterprise Linux, HPUX a IBM AIX. Apache Directory Server obsahuje některé vlastnosti, které jsou unikátní pouze pro tento produkt. Některými z těchto vlastností jsou:

- ApacheDS je založen na platformě X.5000
- Extrémní modularita díky existenci rozhraní pro externí zásuvné moduly
- Možnost vytvářet virtuální adresáře, proxy servery a brány do dalších X.500 kompatibilních adresářových serverů
- Možnost rozdělit logický adresářový strom do několika sekcí
- Administrace systému přes specifické rozhraní a jmenný kontext ou=system
- Vzájemně oddělený backend a frontend
- Interně založené rozhraní JNDI LDAP poskytující přímý transakční přístup mezi jednotlivými bloky adresářového systému
- Kompatibilita s ASN.1 a kodeky BER, které jsou méně náchylné k DoS
- Procedury a triggery interně uložené v LDAP
- LDAP verze 3 kompatibilní certifikace od OpenGroup

Dalším projektem využívajícím ApacheDS je Apache Directory Studio, které poskytuje nástroje pro správu LDAP systémů.



Obrázek 15 Ovládací konzole Apache Directory Studio

Apache Directory Studio je možné použít pro jakýkoli LDAP kompatibilní produkt. Na obrázku *Obrázek 15 Ovládací konzole Apache Directory Studio* je uveden příklad spolupráce s OpenLDAP adresářovým serverem.

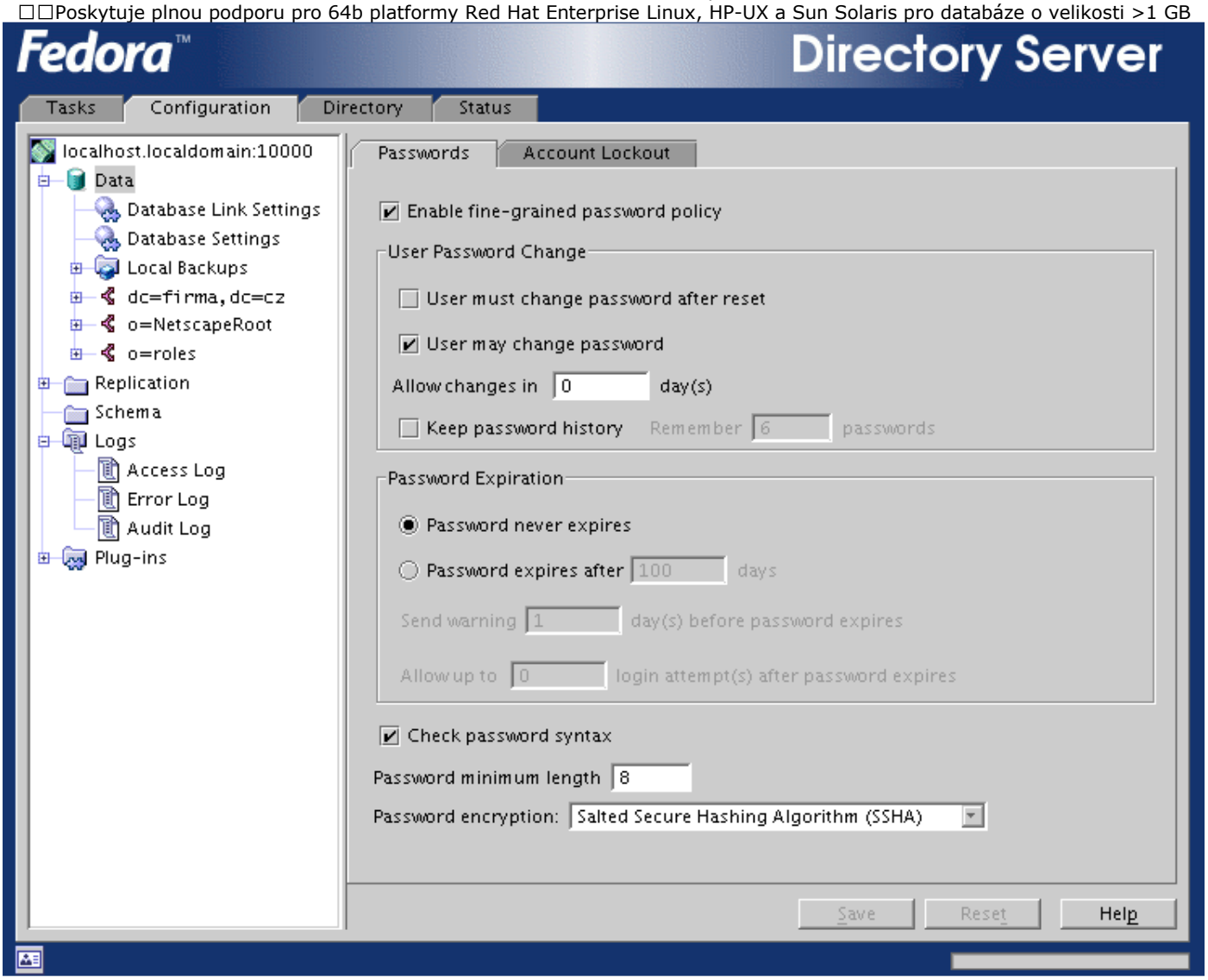
Red Hat Directory Server

Red Hat Directory Server je LDAP kompatibilní server centralizující aplikační nastavení, uživatelské profily, politiky a kontrolu přístupu do síťového registru. Je vyvíjen společností Red Hat jeko součást komerčního operačního systému Red Hat Enterprise Linux. Otevřené řešení je dostupné pod licencí GPL a spravováno komunitou okolo distribuce Fedora, kde nese adresářový server název 389 Directory Server (původně Fedora Directory Server).

Adresářový server zjednodušuje správu uživatelů eliminací nadbytečné údržby a automatizacemi. Red Hat Directory Server také zlepšuje bezpečnost tím, že umožňuje administrátorům uchovat politiky a informace pro řízení přístupů v jediném adresáři. Jedná se jak pro interní data, tak i pro data extranetových aplikací. Mezi vlastnosti produktu Red Hat Directory Server patří:

- Implementace LDAP verze 2 a 3
- Logické rozdělení adresáře mezi několik serverů
- Centralizovaná správa uživatelů a jejich profilů
- Centrální repositář pro uživatelské profily a nastavení, umožňující ukládání osobních i aplikačních dat

☐☐Čtyřcestná, multi-master flexibilní replikace dat uvnitř společnost, poskytující centralizovaný konzistentní zdroj dat pro podnikové aplikace
☐☐Možnosti Single-Sign On
☐☐Možnost lineárního rozšíření počtu CPU
☐☐Poskytuje plnou podporu pro 64b platformy Red Hat Enterprise Linux, HP-UX a Sun Solaris pro databáze o velikosti >1 GB



Obrázek 16 Ovládací konzole 389 Directory Server

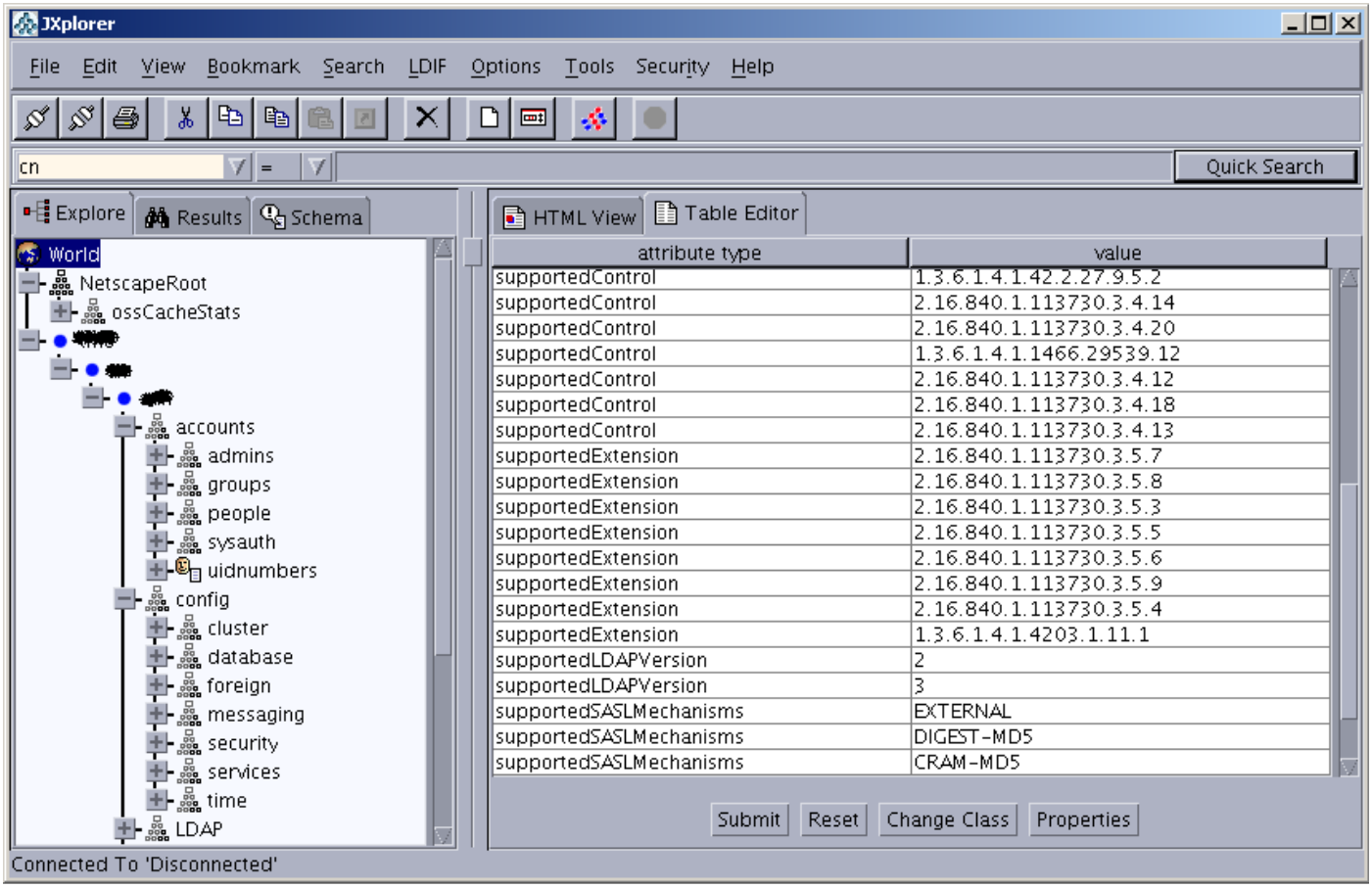
5.5.3 Novell eDirectory

Adresářová služba Novell eDirectory je adresářovým systémem vyvíjeným společností Novell. Vychází z produktu Novell Directory Services, který byl založen na standardu X.500. Služba Novell Directory Services byla poprvé uvedena v systému Novell NetWare 4.

Novell eDirectory je systémem otevřeným, distribuovaným a multiplatformním. eDirectory je možné provozovat jak v prostředí NetWare, tak i na jiných operačních systémech, jako jsou SUSE Linux, RedHar Linux, Sun Solaris, HP-UX, AIX a Microsoft Windows. Díky této adresářové službě je možné realizovat centrální správu heterogenních sítí. V současné době Novell eDirectory podporuje většinu vlastností LDAP verze 3.

5.5.4 OpenLDAP

OpenLDAP je open-source implementací LDAP vyvíjené komunitními vývojáři. Celý projekt je uvolněn pod svobodnou licencí BSD. Tento software je možné provozovat na operačních systémech jako Microsoft Windows, Sun Solaris, OpenSolaris, Ubuntu GNU Linux, Redhat Enterprise Linux, HPUX a IBM AIX. OpenLDAP je jedním z nejznámějších adresářových serverů v prostředí alternativních operačních systémů jako Linux/GNU a derivátů BSD. Jeho neocenitelnou výhodou je jednoduchá konfigurace, ale na straně druhé je zde absence nativních grafických nástrojů pro správu. Tuto mezeru se snaží vyplnit například JXplorer, LDAP Browser, phpLDAPadmin nebo třeba LAM.



Obrázek 17 Ovládací konzole Explorer

OpenLDAP nabízí podporu jak LDAP verze 2, tak i verze 3. Samozřejmostí je podpora zabezpečení SASL, ACI a replikace. Výkonem, funkcemi a robustností však OpenLDAP nedosahuje předností konkurenčních enterprise řešení. Nevýhodou zůstává i nutnost restart adresářového serveru v případě změny některého z konfiguračních parametrů.

Sun Directory Server

Sun Java System Directory Server Enterprise Edition je vysoce výkonný adresářový server poskytující základní adresářové služby a velké množství dílčích datových služeb. Zahrnuje několik klíčových komponent, které společně poskytují adresářové služby:

☐☐Adresářový server poskytující LDAP adresářové služby

☐☐Adresářový proxy server umožňující load-balancing, vysokou dostupnost, virtualizaci a další distribuční možnosti

☐☐Synchronizaci identit pro Microsoft Windows umožňující synchronizaci identifikačních dat, hesel a skupin mezi Microsoft Active Directory a Sun Java System Directory Server

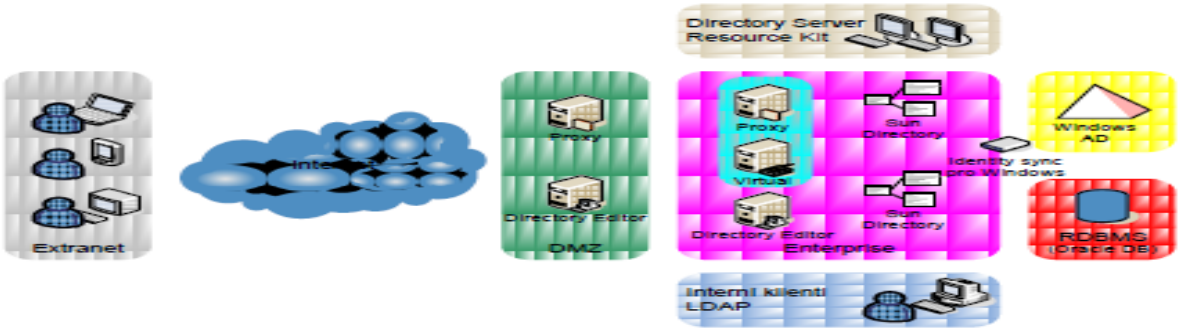
☐☐Adresářový editor pro přímé úpravy adresáře

☐☐Resource Kit pro ladění a optimalizaci výkonu adresářového serveru

S rostoucím počtem identifikačních dat a aplikací vzniká velká potřeba nasazovat vysoce výkonná enterprise adresářová řešení poskytující množství funkcí a vlastností. Tento adresářový server představuje 64b enterprise-class adresářový systém poskytující a zachovávající výkonné vyhledávání a výkonný zápis přibližující se výkonu relačních databází. V prostředí kde je tak velké množství dat, že musí být rozděleny přes několik serverů, Sun Java System Directory Server Enterprise Edition nabízí možnosti distribuované integrace pro konsolidaci těchto dat, které tím pádem mohou být zpracovávány efektivněji.

Sun Java System Directory Server Enterprise Edition podporuje operační systémy Microsoft Windows, Sun Solaris, OpenSolaris, Ubuntu GNU Linux, Redhat Enterprise Linux, HPUX a IBM AIX. Podporovanými databázemi pro virtualizaci jsou MySQL 5.0, Oracle 9i a 10g a IBM DB2 verze 9. Sun Java System Directory Server Enterprise Edition obsahuje virtuální adresář a službu adresářového proxy serveru, a byl navržen pro jednodušší integraci do stávající technologické infrastruktury. Adresářový server je možno například připojit do stávající topologie Microsoft Active Directory synchronizovat identity, hesla a skupiny mezi Microsoft Active Directory a Sun Java System Directory Server Enterprise Edition. Jako kritická komponenta enterprise infrastruktury pro správu identit, musí dnešní adresářové servery poskytovat konzistentní a spolehlivý přístup k datům identit za všech okolností a v jakýkoli čas. Sun Java System Directory Server Enterprise Edition přináší vysoce flexibilní replikační prostředí napomáhající zabezpečit dostupnost dat. Integrovaný proxy server zabraňuje tzv. single point of failure pro adresářové služby, a také poskytuje operativní routing, load balancing a vlastnosti failover zabezpečující, že data uložená v adresářovém serveru budou vždy dostupná pro uživatele a aplikace vždy když jsou potřeba.

Sun Java System Directory Server Enterprise Edition poskytuje jak vertikálnítak i horizontální rozšiřitelnost bez nutnosti přepracování návrhu systému. 64b enterpriseclassadresářový systém představuje možnosti lineární rozšiřitelnosti počtu procesorůaž do 18.Základní vlastností dnešních adresářových služeb je citlivost identity dat. To pověřujeadresářový server, že bude poskytovat robustní zabezpečení chránící proti neoprávněnémupřístupu, útokům DoS a dalším bezpečnostním rizikům. Mimo šifrované komunikacea ochraně hesly, Sun Java System Directory Server Enterprise Edition zabezpečuje přístupk datům pomocí ACI (Access Control Instructions), který definuje přístupová práva na úrovni atributů. Integrovaný proxy server také minimalizuje riziko neautorizovaného přístupu k datům pomocí ACI na úrovni adresářové proxy, limitací využití zdrojů bránící útokům typu DoS a vynucenému šifrování a ověření.



Obrázek 18 Sun Directory Server Enterprise Edition

Mezi vlastnosti Sun Java System Directory Server Enterprise Edition patří:

- Centralizovaný repositář pro identity, aplikace a informace o síťových zdrojích
- Služby adresářového proxy serveru
- Neomezený počet master serverů
- Editor objektů založený na webovém rozhraní
- Centralizovaná správa globálního adresáře
- Sjednocený pohled na identity
- Virtuální adresáře

Obrázek 19 Ovládací konzole Sun Directory Server

OpenDS

OpenDS je otevřený projekt postavený na produktu Sun Directory Server. Hlavním přispěvovatelem a správcem je Sun Microsystems. Projekt byl vydán pod open-source licencí CDDL (Common Development and Distribution License) s cílem umožnit komunitě vývojářů vytvořit kompletní adresářový systém nové generace. OpenDS umožňuje členům komunity vytvářet standardizované adresářové služby pro internetové aplikace používané uvnitř nebo vně organizace. Internetové aplikace spoléhající se na adresářové služby zahrnují vysoce propustné webové sítě jako email, kalendář, instant messaging, jmenné služby, řešení AAA používané u poskytovatelů např. internetových poskytovatelů nebo telekomunikačních operátorů a portálů určených pro zaměstnance, zákazníky a partnery. V současné době podporuje OpenDS velké množství operačních systémů a distribucí, zahrnující Microsoft Windows, Sun Solaris, OpenSolaris, Ubuntu GNU Linux, Redhat Enterprise Linux, HPUX a IBM AIX. OpenDS je malý adresářový Java server, který je volně dostupný a může být použit na velkém množství platforem. Vývojáři jej mohou jednoduše použít jako součást jejich aplikačních řešení, na rozdíl od většiny jiných řešení, která vyžadují zakoupení licencí nebo nutnost vytvoření dohody o poskytování určitých možností aplikací na trhu nebo v podnicích.

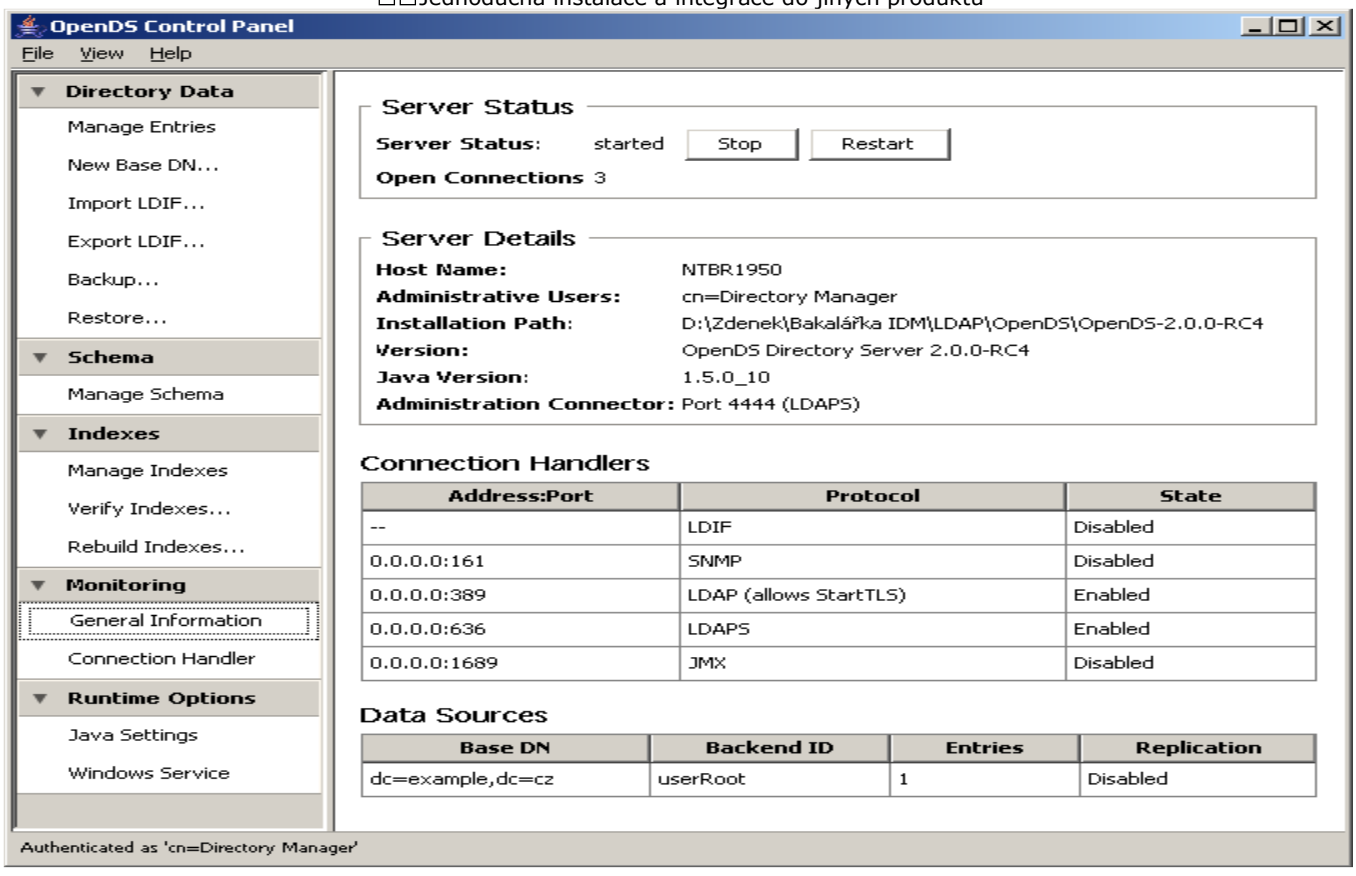
OpenDS je bezplatný SW vyvíjený pod CDDL licencí, nicméně je možno využít podpory od společnosti Sun. Tato podpora je určena zpravidla společnostem a poplatek za OpenDS Standard Edition je za jednoho uživatele $1,25. OpenDS je software navržen poskytovat dnes velmi požadovaný výkon s podporo možnosti rozšiřitelnosti, která se v pohledu budoucích strategií stává stále důležitější. Adresář využívá horizontální strukturu, která je optimální pro ukládání uživatelských dat a zvyšuje výkon systému. Přímo tedy zlepšuje latence, zvyšuje dostupnost pro koncového uživatele nebo aplikaci a snižuje riziko nevykonání požadavku. OpenDS také uspokojuje přísnější výkonnostní požadavky přes různá odvětví, od repositáře telekomunikačních zákazníků až po milióny uživatelů extranetových aplikací. OpenDS splňuje standardy zajišťující maximální

spolupráci s LDAP klientskými aplikacemi a jednoduchou integraci do topologicky odlišných infrastruktur. Řešení implementuje všechny dnešní specifikace, včetně mnoha konceptů LDAP rozšíření od IETF, které začínají být vyvíjeny pro budoucí verze tohoto protokolu. Mimo to, toto malé řešení adresářového serveru je velmi vhodné pro integraci do jiných aplikací a zařízení, a poskytuje sadu API pro rozšíření funkcionality vedoucí k přidávání nových služeb a zvyšující rozsah využití. Základní vlastností dnešních adresářových služeb je citlivost identity dat. To pověřuje adresářový server, že bude poskytovat robustní zabezpečení chránící proti neoprávněnému přístupu, útokům DoS a dalším bezpečnostním rizikům. Zabezpečení OpenDS zahrnuje podporu pro několik politik správy hesel, dávající společnostem více možností jak zvýšit celkovou bezpečnost. Také poskytuje rozsáhlé možnosti zabezpečení v dalších oblastech, jako je kontrola přístupů, šifrování a audit.
Hlavní úlohou adresářového serveru je správa dat a tato vlastnost musí být vždy dostupná. OpenDS poskytuje moderní nástroje pro zálohování a obnovu těchto dat. Tyto nástroje umožňují přírůstkové zálohování, komprimaci, šifrování, elektronické podepsání, ověření a online obnovení vedoucí k vyšší dostupnosti a spolehlivosti dat.

Obrázek 20 Sun OpenDS Standard Edition

Následující verze produktu budou obsahovat vlastnosti jako virtuální adresáře, proxy server, editor, synchronizaci identit pro Windows (synchronizace záznamů v Active Directory) a průzkumníka adresáře – vše bude zahrnuto v jediném uceleném produktu. Například Oracle licencuje svůj Virtual Directory Server odděleně, což zvyšuje celkové náklady na licence pro enterprise segment. OpenDS se také stává klíčovou komponentou kompletního portfolia IDM produktů od společnosti Sun. Vlastnosti produktu OpenDS:

☐☐LDAP v3 adresářový server založený pouze na Java technologiích
☐☐Rozšířená replikace
☐☐Rozšířená politika správy hesel
☐☐Rozšířená podpora zálohování a obnovy dat
☐☐Vyspělé ovládání z příkazové řádky
☐☐Vyspělé ovládání z ovládací konzole, viz *Obrázek 21 Ovládací konzole OpenDS*
☐☐Jednoduchá instalace a integrace do jiných produktů

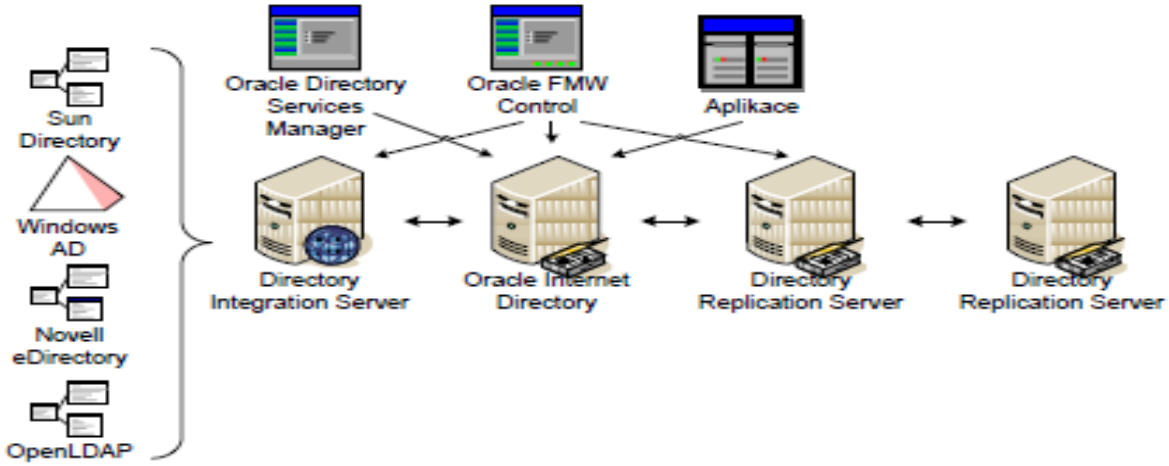


Obrázek 21 Ovládací konzole OpenDS

Oracle Directory Services

Produkty z portfolia Oracle Directory Services poskytují řešení adresářových služeb, které nabízí enterprise řešení zahrnující virtualizaci, úložiště a synchronizaci adresářových dat. Produkt Oracle Virtual Directory poskytuje agregaci a transformaci identit bez synchronizace, zatímco Oracle Internet Directory poskytuje služby pro uložení dat a synchronizaci.

Oracle Internet Directory je pouze adresářovou službou, která poskytuje možnosti uspokojit požadavky na moderní adresářové úložiště. Oracle Internet Directory je navržen poskytovat vysoce dostupný rozšiřitelný a výkonný adresářový systém. Jako produkt je součásti Oracle Identity Management Suite. Oracle Internet Directory (*Obrázek 22 Komponenty Oracle Internet Directory*) poskytuje unikátní, robustní a bezpečnou platformu pro adresářové služby. Implementací služeb LDAP na technologii databáze Oracle, může tento adresářový server poskytnout velké úrovně rozšiřitelnosti, vysoké dostupnosti a bezpečnosti uložených dat.



Obrázek 22 Komponenty Oracle Internet Directory

Oracle Internet Directory využívá možností Oracle Database 10g/11g umožňující podporu velkého množství internetových aplikací. Adresářová služba také podporuje LDAP reference, což je technologie, kdy může být adresář fyzicky rozdělen na několik částí. Toto rozdělení umožňuje další delegaci administrace takto odděleného segmentu adresáře, zatímco z logického pohledu zůstává adresář v celku. Vlastnosti jako *Server Chaining* dovolují integrovat externí adresáře jako Sun Java System Directory Server Enterprise Edition nebo Microsoft Active Directory, a poskytovat transparentní adresářové služby klientům.

Klíčovými vlastnostmi Oracle Internet Directory jsou:

☐☐Implementace LDAP doporučení IETF verze 2 a 3
☐☐Implementace informačního modelu X.500
☐☐Rozšiřitelné adresářové schéma
☐☐Podpora online změn v adresářovém schématu bez výpadku
☐☐Podpora Unicode, UTF-8 a národních znaků
☐☐Rozšiřitelnost pomocí Java a PL/SQL modulů
☐☐Řetězení jiných nežli Oracle adresářů

Oracle Virtual Directory naproti tomu není LDAP serverem pro uložení identit, ale virtualizační službou. Umožňuje konsolidovat a využívat stávajících adresářových služeb bez kopírování či migrace. Jedná se o systém, který poskytuje jednotný pohled na různé adresářové služby uvnitř organizace. Díky LDAP rozhraní do ne LDAP datových zdrojů mohou aplikace a internetové služby využívat jedno datové rozhraní, které je shodné pro přístup do všech zdrojů.

Klíčovými vlastnostmi Oracle Virtual Directory jsou:

☐☐Jednotné rozhraní pro aplikace a klienty
☐☐LDAP rozhraní do ne LDAP datových zdrojů zahrnující databáze a internetové služby
☐☐Transformace dat a aplikačně specifické pohledy
☐☐Rozšiřitelnost
☐☐Vysoká dostupnost

Oracle Virtual Directory obsahuje dvě rozhraní. První slouží k přístupu ke zdrojům uloženým v jiných adresářových systémech, databázích nebo internetových službách. Ke druhému rozhraní se připojují klienti nebo aplikace pomocí podporovaných protokolů. Těmi v současné době jsou LDAP, HTTP a DSML.

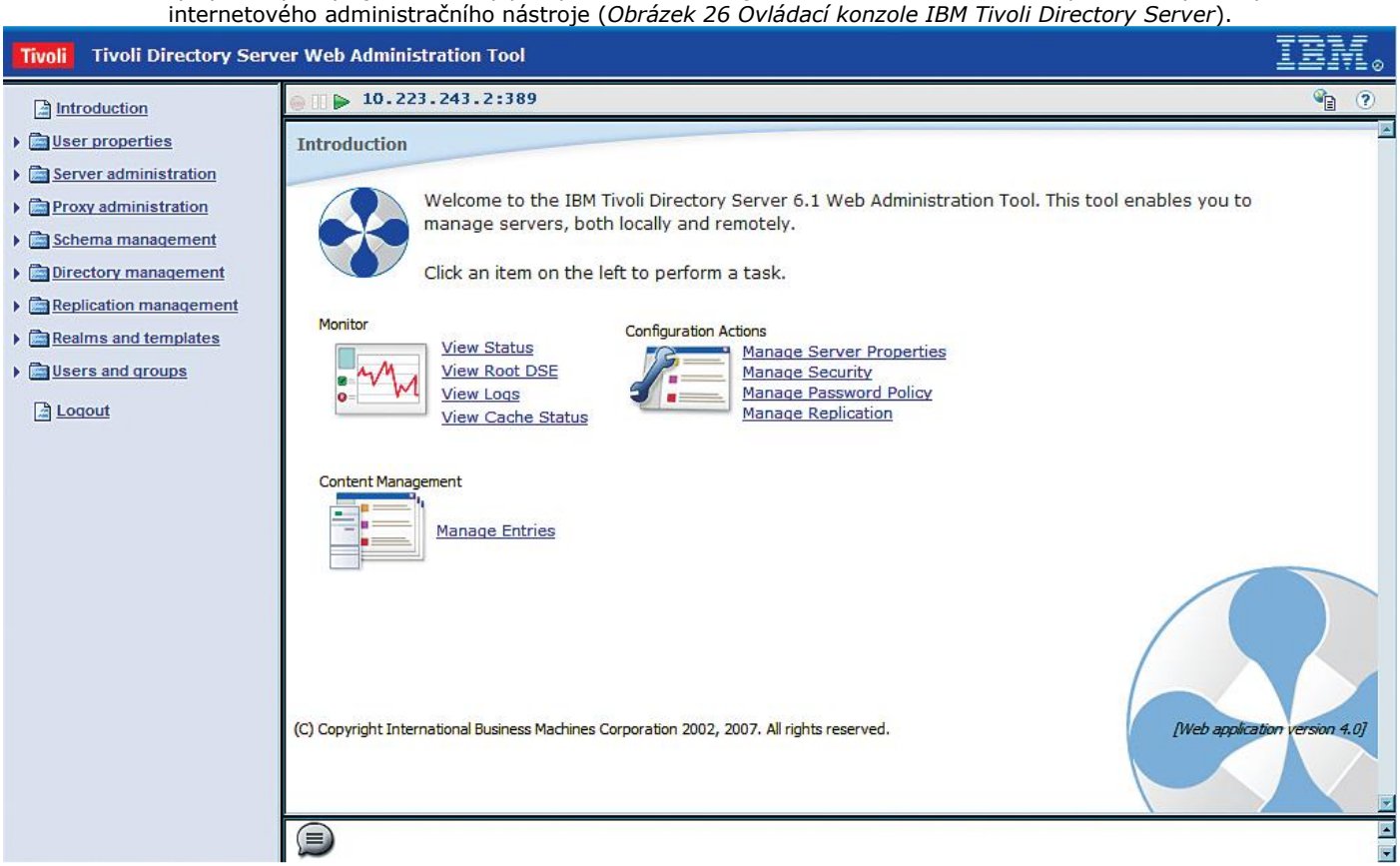
Obrázek 24 Architektura Oracle Virtual Directory

Na následujícím obrázku je zobrazena komunikace, kdy je pro aplikaci užívající LDAP použito zdrojů například z databáze.

Obrázek 25 Komunikace mezi aplikací a Oracle Virtual Directory

IBM Tivoli Directory Server

IBM Tivoli Directory Server (ITDS) je další implementací LDAP adresářového serveru, a je součástí skupiny produktů IBM Tivoli Identity and Access Management. Adresářový server poskytuje funkce rozšířeného zabezpečení, vysoké dostupnosti a je vyvíjen dle standardů pro enterprise segment adresářových systémů. Jako datové úložiště je použit databázový systém IBM DB2, dosahující vysokých výkonů s možností replikace, vertikální rozšiřitelnosti a pokročilých funkcí pro zálohování a obnovu dat. Podporovanými operačními systémy jsou Microsoft Windows, Sun Solaris, Redhat Enterprise Linux, HP-UX a IBM AIX. Adresářový systém poskytuje vestavěný proxy server, umožňující další rozšíření a možnost spravovat systém pomocí internetového administračního nástroje (*Obrázek 26 Ovládací konzole IBM Tivoli Directory Server*).



Obrázek 26 Ovládací konzole IBM Tivoli Directory Server

Microsoft Active Directory

Active Directory je technologie vytvořená společností Microsoft jako kombinace několika síťových služeb, zahrnující adresářový server založený na LDAP, ověření Kerberos a systém DNS. Jedná se o distribuovanou adresářovou službu, která je součástí operačních systémů Microsoft Windows Server. Active Directory poskytuje centralizovanou zabezpečenou správu celé sítě o velikosti serveru, budovy, města nebo několika lokalit na světě. Systém Active Directory byl představen v roce 1999, kdy se stal součástí operačního systému Microsoft Windows 2000 Server. Později byl přepracován, rozšířena funkcionalita a možnosti administrace, a to jako součást Microsoft Windows 2003 Server a Microsoft Windows 2003 Server R2. Následně byl kód pročištěn v Microsoft Windows 2008 Server a Microsoft Windows 2008 Server R2. Ve verzi Microsoft Windows 2008 Server byl přejmenován na Active Directory Domain Services. Active Directory byl v předchozích verzích označován jako NT Directory Services (NTDS).

Active Directory je logické seskupení uživatelů, počítačů v doméně a dalších entit, centrálně spravované servery zvanými Domain Controller (Windows DC). Struktura Active Directory je hierarchická soustava objektů, které jsou rozdělení do třech kategorií:

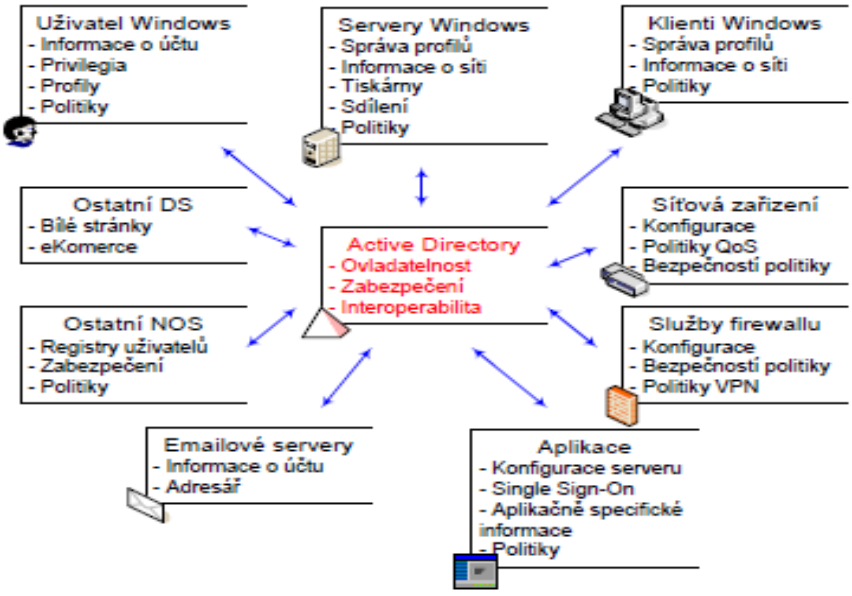
- Zdroje: např. tiskárny
- Služby: např. web, email, FTP
- Uživatelé: uživatelská konta, skupiny a počítače

Každý objekt v Active Directory reprezentuje jednu entitu s jejími atributy. Některé objekty mohou obsahovat další, podřízené objekty. Objekt je unikátně identifikován názvem a skupinou atributů charakteristickými informacemi, které může objek obsahovat. Všechny objekty a atributy jsou popsány v adresářové schématu, které je blíže rozpracováno v kapitole *16 Adresářové schéma*.

Active Directory může udržovat objekty v několika úrovních. Vrcholem hierarchické struktury je tzv. *les* (forest). Dalším logickými částmi jsou strom (tree) a doména. Produkt Active Directory zahrnuje:

- Active Directory v rámci sítě serverů Microsoft Windows
- Aplikační režim Active Directory
- Strukturální a odkládací technologie
- Role doménových řadičů
- Technologie replikací
- Technologie vyhledávání a publikování
- Instalace, upgrade a technologie pro migraci Systém Active Directory je nejčastěji použit pro jeden ze tří účelů:
- Interní adresář: použit v enterprise síti pro publikování informací o uživatelských účtech a technologických zdrojích. Interní adresář je dostupný pro zaměstnance společnosti přímo, nebo přes připojení VPN, ale není dostupný pro ostatní.
- Externí adresář: tyto adresáře jsou umístěné většinou na serverech ve speciální demilitarizované zóně (DMZ) na hranici enterprise sítě uvnitř společnosti (LAN) a veřejnou sítí Internet. Externí adresáře jsou zpravidla používány pro ukládání informací o zákaznících a obchodní partneři mohou těchto informací využívat.
- Aplikační adresář: aplikační adresář slouží pro uložení dat relevantních pouze příslušné aplikaci. Tyto adresáře se umisťují na stejný server, kde je nainstalována příslušná aplikace.

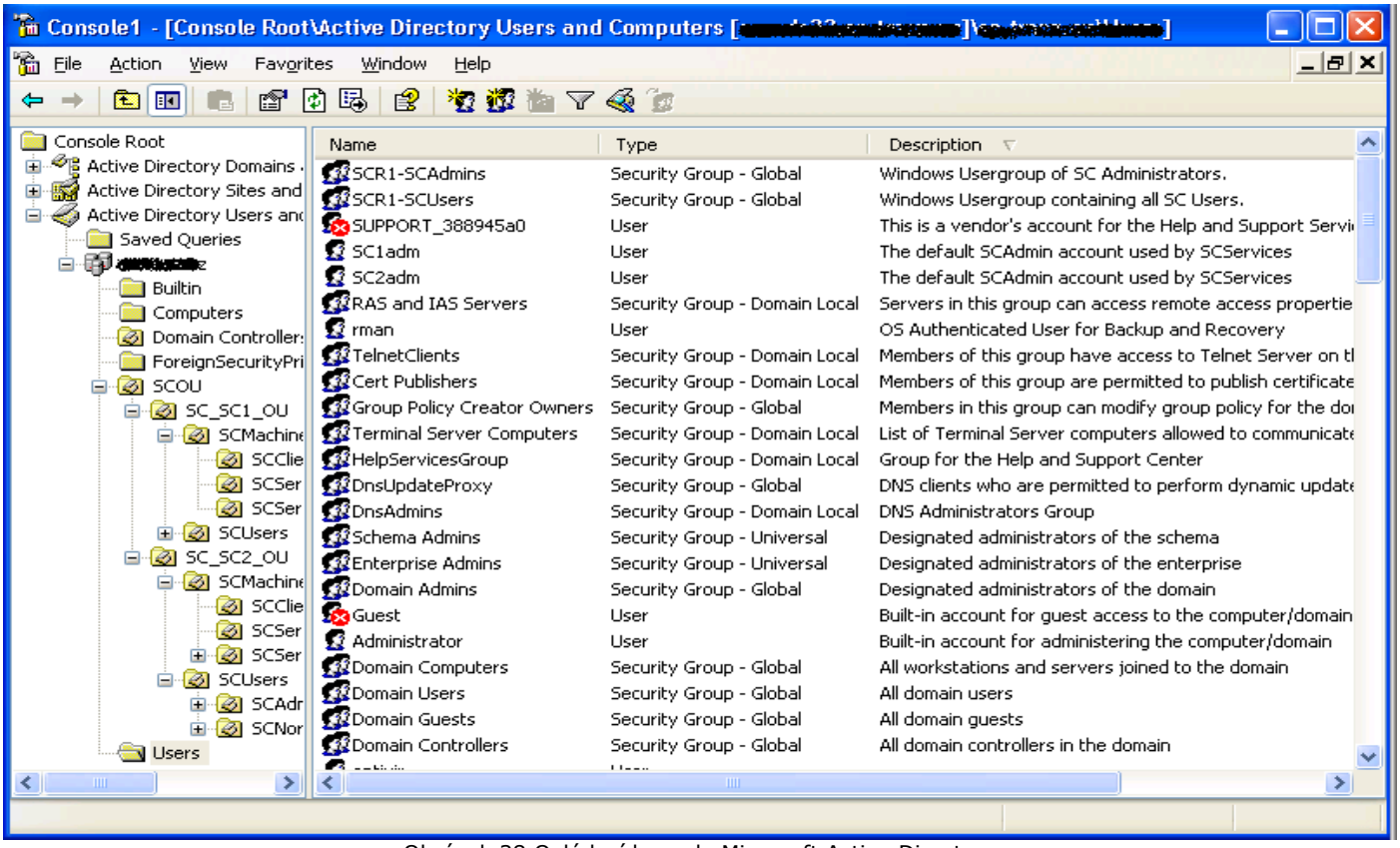
Active Directory je informační centrum systémů primárně založených na operačních systémech Microsoft Windows. Tento adresářový systém je nepřenosný na jiné operační systémy či hardwarové platformy. Následující obrázek ukazuje Active Directory v síti Microsoft Windows a vztahy mezi jednotlivými distribuovanými zdroji, které mohou spolupracovat.



Obrázek 27 Active Directory v síti Windows

Active Directory dovoluje přístup z jedné domény ke zdrojům domény druhé, pokud je použito nastavení tzv. důvěryhodnosti (trust). Nové domény vytvořené uvnitř objektu forest, mají automaticky přístup do všech ostatních domén pod stejným objektem forest. Důvěryhodnost ve Windows 2000 a výše může být následující:

- *One-way trust* – povoluje přístup z jedné domény do druhé, ale opačný přístup je zakázán
- *Two-way trust* – je povolen obousměrná komunikace (přístup) mezi doménami
- *Trusting domain* – do domény je povolen přístup z *trusted domény*
- *Trusted domain* – z domény je povolen přístup do *trusting domény*
- *Transitive trust* – důvěryhodnost může být rozšířena do ostatních domén v AD
- *Intransitive trust* - *one-way trust*, který nemůže být rozšířen do dalších domén
- *Explicit trust* – důvěryhodnost vytvořená administrátorem
- *Cross-link trust* – explicitní vazba mezi doménami v případě, že nejsou ve stejném stromu nebo není nastaven vztah potomek/rodič



Obrázek 28 Ovládací konzole Microsoft Active Directory

Řešení systémů pro správu uživatelských identit

Jak společnosti přidávají více aplikací a internetových služeb, někdy spolupracujících přes několik servisních organizací, stojí tváří v tvář obtížné výzvě. Na jedné straně se snaží najít cestu jak minimalizovat podnikatelské riziko vztahující se ke spolupráci s mnoha partnery z pohledu přístupu ke klíčovým zdrojům, tak na straně druhé musí současně umožnit rozšířit rozsah podnikatelských aktivit, které jsou základem podnikatelské soutěže v ekonomii internetu a extranetu. Existuje celé portfolio řešení IDM, která pomáhají rozvíjet a udržovat tyto klíčové zdroje. Mezi nejznámější a nejpoužívanější patří Sun Java System Access Manager, Oracle Identity Management, IBM Tivoli Access Manager, CA Siteminder a Sun OpenSSOEnterprise. Jedná se o řešení, která slouží k efektivní správě uživatelských identit primárně uložených v LDAP adresářových serverech.

	OpenSSO Enterprise	Oracle Access Manager	CA Siteminder	IBM Tivoli Access Manager
Správa přístupů	x	x	x	x
Federace (FIDM)	x	Oracle Identity Federation	CA Federation Manager	Federated Identity Manager
Podpora WEB	x	Web Services Manager	CA Web Services Manager	Federated Identity Manager
Vynucené oprávnění	Léto 2009	Oracle Entitlements Manager	CA Entitlements Manager	Security Policy Manager
SSO	Léto 2009	OEM: Passlogic	CA Single Sign-On	Access Manager for ESSO

Tabulka 1 Matice produktů a dostupná řešení

Sun Identity Management

Portfolio produktů IDM společnosti Sun zahrnuje celou skupinu programů pro správu identit v enterprise prostředí.

Obrázek 29 Sun Identity Management

☐☐*Sun Identity Manager* poskytuje kompletní funkce pro užití a vynucení bezpečností politiky se zaručením shody s požadavky auditu. Poskytuje moderní, integrovaný provisioningu a audit zahrnující jednoduchý reporting a poskytující automatické přehledy.

Možnosti produktu Sun Identity Manager:

- o Provisioning uživatelů
- o Správa hesel
- o Služby pro synchronizaci dat
- o Audit přístupů s automatizovanou nápravou

☐☐*Sun Role Manager* je řešení pro řízení přístupů ke zdrojům na základě rolí.
Možnosti produktu Sun Role Manager:
- o Návrh rolí
- o Obsluha rolí
- o Certifikace rolí

☐☐*Sun Identity Compliance Manager* pomáhá organizacím v přístupu k certifikacím, které jsou vyžadovány státními regulátory nebo interní bezpečnostní politikou. Zároveň pomáhá snižovat rizika spojená s řízením přístupů a usnadňuje provádění auditů stálým monitorováním aktuálního stavu a porovnáváním vůči předem definovaným bezpečnostním politikám.
Možnosti produktu Sun Identity Compliance Manager:
- o Certifikace přístupů
- o Monitorování přístupů vzhledem k politikám SoD

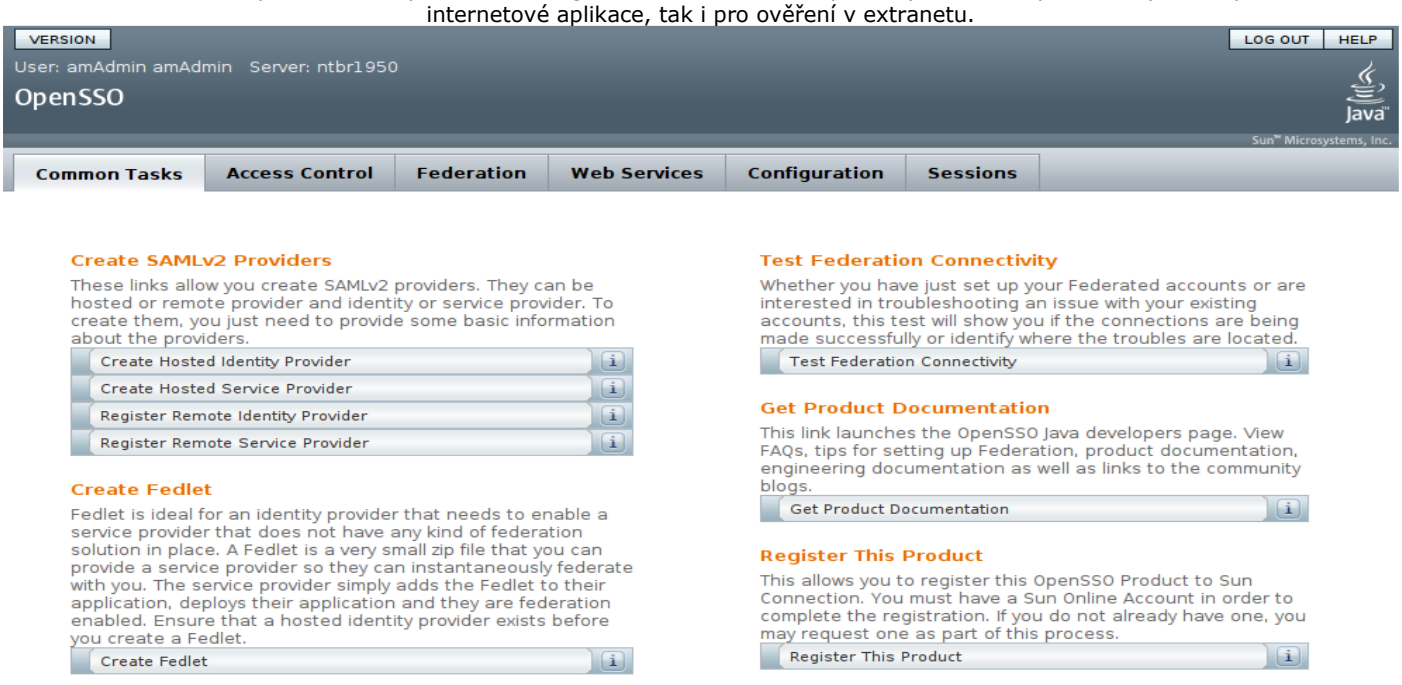
☐☐*Sun OpenSSO Enterprise* je systém umožňující doručit každý aspekt problému single-on. Je založen na OpenSSO komunitním projektu a je jediným produktem kombinujícím zabezpečený přístup pro internetové aplikace, federativní SSO pro spolupráci s dalšími partnery a řízení přístupů. Produkt OpenSSO je popsán v kapitole *6.2 OpenSSO*.
Možnosti produktu Sun OpenSSO Enterprise:
- o Řízení přístupů pro internetové aplikace
- o Federativní SSO
- o Služby pro zabezpečení internetových služeb

☐☐*Sun Directory Server Enterprise Edition* je výkonný adresářový server s dalším přidanými vlastnostmi, zahrnující proxy, virtuální adresáře a redistribuci dat, pro poskytování adresářových služeb s vysokou dostupností a rozšiřitelností s možností jednoduše spravovat milióny záznamů v rostoucím a dynamickém enterprise prostředí. Produkt Sun Directory Server Enterprise Edition je blíže popsán v kapitole *30 Sun Directory Server*.
Možnosti produktu Sun Directory Server Enterprise Edition:
- o Adresářové služby
- o Vysoká dostupnost
- o Synchronizace hesel s Microsoft Active Directory a virtuálními adresáři

☐☐*Sun OpenDS Standard Edition* je prvním komerčně dostupným čistě Java řešením adresářového serveru, založeným na vývoji open-source komunitního projektu OpenDS. Nabízí společnostem všech velikostí nasadit nové technologie v rychlém vývojovém cyklu a další výhody plynoucí s použití open-source řešení, ale s plnou podporou komerčního řešení, které má jednoduchou instalaci, použití, správu a rozšíření. Produkt OpenDS je popsán v kapitole *33 OpenDS*.
Možnosti produktu Sun OpenDS Standard Edition:
- o Adresářové služby
- o Pokročilé služby replikací, zálohování a obnovy
- o Integrován v OpenSSO

OpenSSO

Projekt OpenSSO je založen podobně jako OpenDS na zdrojových kódech uvolněných společností Sun Microsystems, konkrétně se jedná o produkt Sun Java Systém Access Manager 7.0, který zahrnuje komponenty z vývojové verze 7.1, a Sun Java System Federation Manager. S komunitou vývojářů a inženýrů Sunu je OpenSSO světově největší open-source SW pro správu uživatelských identit poskytující vysoce výkonný a rozšiřitelný systém pro SSO, management přístupů, federační služby (FIDM) a zabezpečené Web služby.
Práce OpenSSO komunity vyústila v roce 2008, kdy byla vydána komerční verze Sun OpenSSO Enterprise 8.0, čistě Java řešení, kde se uplatňuje komplexní bezpečnostní politika pro Webové aplikace a služby nasazované ve společnostech místo používání jednoúčelově vytvořených služeb. Jelikož se jedná o systém založený na technologiích Java, OpenSSO Enterprise je možno jednoduše nasadit na jakémkoli operačním systému zahrnující Sun Solária, Redhat Enterprise Linux, Ubuntu GNU Linux, IBM AIX, Microsoft Windows a Apple Macintosh. Také je možno využít možnosti běhu na Java aplikačních serverech jako GlassFish, Sun Web Server, Apache Tomcat, Apache Geronimo, Oracle Application Server, Oracle – BEA Weblogic, IBM WebSphere a nebo jBoss Application Server. OpenSSO Enterprise je IDM poskytující management přístupů jak pro intranet, tak i pro extranet., podporující FIDM a umožňující Webovým službám využít bezpečnostního modelu. To vše bez potřeby odděleného produktu nebo dalších licencí. S OpenSSO Enterprise mohou organizace centralizovat vynucený SSO a bezpečnostní politiku pro interní internetové aplikace, tak i pro ověření v extranetu.



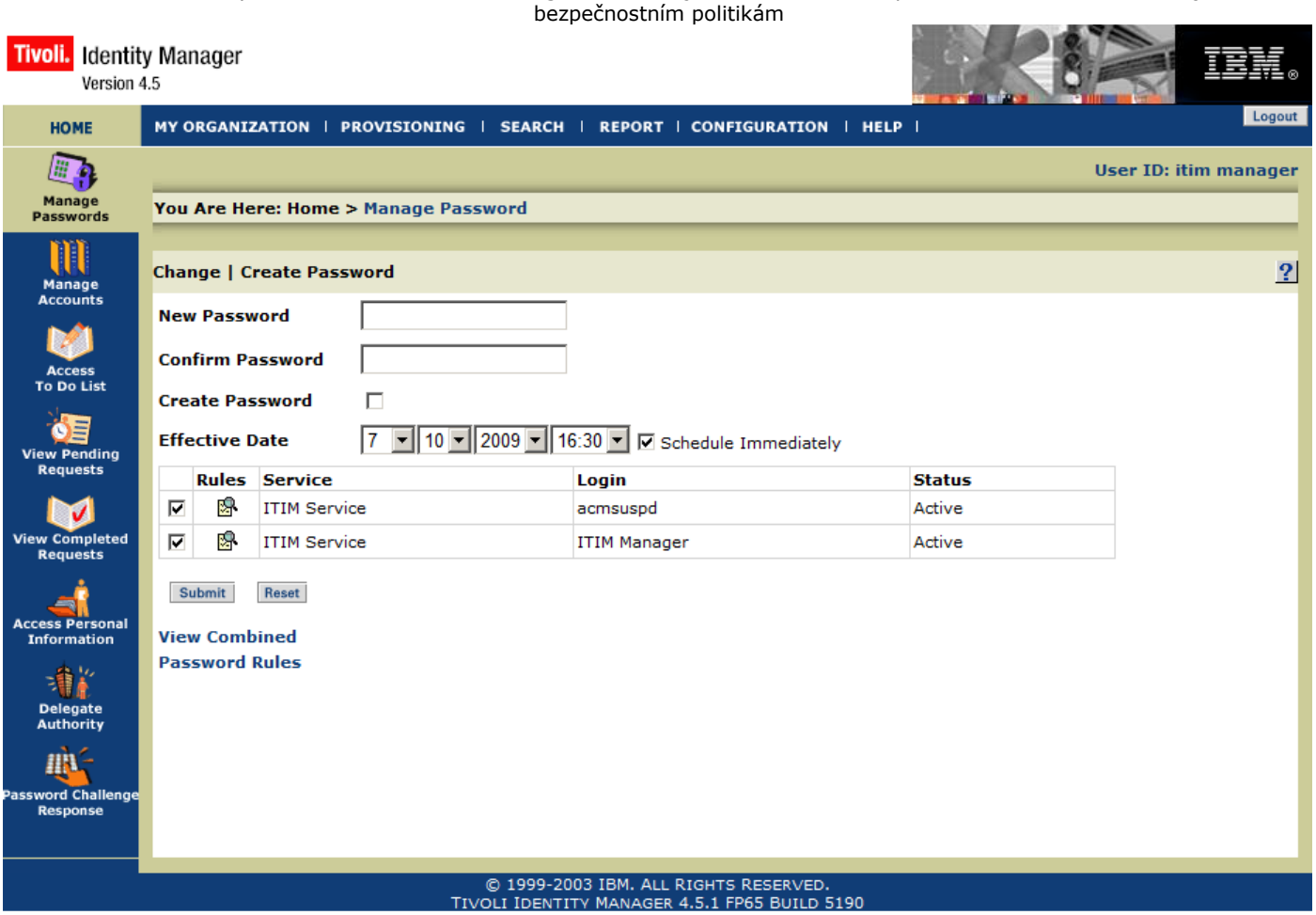
IBM Identity and Access Management

Řešení IBM Identity and Access Management napomáhá udržovat uživatelské a systémové identity stále online a pod kontrolou. Nepřímo tak napomáhá ke zvyšování produktivity práce a dynamickému rozvoji společností. Zároveň přispívá k udržení flexibility a bezpečnosti v heterogenním IT prostředí, zatímco pomáhá snižovat náklady a maximalizovat návrat investic (ROI). Rychlé a jednoduché zavádění služeb využívajících identit a systém řízení přístupů může automatizovat a více zjednodušovat správu uživatelských identit a politik napříč společností. Tyto řešení slouží k efektivnímu řízení interních uživatelů stejně jako narůstající počet zákazníků či obchodních partnerů přes celý Internet. Možnosti skupiny produktů IBM Identity and Access Management jsou:

☐☐Řízení životního cyklu identity včetně samoobslužných systémů
☐☐Řízení identity zahrnující řízení přístupů, rolí, profilů a audit
☐☐Federativní služby spojené s identitami
☐☐Centralizované řízení a správa umožňující konzistentní nastavení bezpečnostních politik pro více uživatelů a aplikací

Produkty zahrnuté v tomto portfoliu jsou:

☐☐*IBM Tivoli Access manager for eBusiness* je centrum pro ověřování a autorizaci pro internetové služby a další aplikace. Access Manager centralizuje správu zabezpečení a vytváří další možnosti pro nasazování bezpečných aplikací
☐☐*IBM Tivoli Access Manager for Enterprise Single Sign-On* zjednodušuje, posiluje a sleduje přístupy integrací technologie SSO uvnitř společnosti
☐☐*IBM Tivoli Federated Identity Manager* poskytuje centrální federativní SSO pro bezpečné sdílení informací mez důvěryhodnými partnery a zjednodušuje integraci aplikací za použití SOA a internetových služeb napříč distribučními portály
☐☐*IBM Tivoli Identity and Access manager* řeší efektivní životní cyklus uživatelů a řízení přístupů pro interní i externí uživatele, centralizuje řízení zabezpečení a automatizuje správu uživatelských účtů, přístupových práv a hesel
☐☐*IBM Tivoli Identity Manager* poskytuje zabezpečenou a automatizovanou správu uživatelů založenou na politikách, napomáhající efektivnímu řízení uživatelských přístupů, účtů, práv a hesel, od vytváření až po zrušení, napříč IT prostředím
☐☐*IBM Tivoli Privaci Manager for eBusiness* pomáhá chránit důvěru zákazníků implementací vlastních politik, které ochraňují citlivé osobní informace
☐☐*IBM Tivoli Security Policy Manager* přináší další generaci zabezpečení napomáhající snižovat složitost a cenu zabezpečeného přístupu k aplikacím a internetovým službám v heterogenní IT a SOA infrastruktuře
☐☐*IBM Tivoli Unified Single Sign-On* zjednodušuje používání SSO aplikacemi a internetovými službami přistupující ke zdrojům jiného partnera (federativní SSO)
☐☐*IBM Tivoli Security Information and Event Manager* centralizuje informace o zabezpečení včetně událostí vztahujících se k bezpečnostním politikám



Obrázek 31 Ovládací konzole IBM Tivoli Identity Manager

Oracle Identity Management

Oracle Identity management poskytuje sjednocenou bezpečnou platformu vytvořenou pro správu uživatelských identit, oprávnění a poskytování zdrojů uživatelům a aplikacím. Současně zajišťuje integritu velkého množství aplikací umožněním dalších stupňů zabezpečení a úplnost přístupu k chráněným podnikovým zdrojům. Následně umožňuje řízení procesů pro nakládání s těmito zdroji. Oracle Identity Management poskytuje vylepšené efektivní metody pro integraci, konsolidaci a automatizaci zabezpečení, řízení a správy. Oracle Identity Management podporuje celý životní cyklus podnikových aplikací a identit od založení až po zrušení. Do portfolia produktu Oracle Identity Management patří následující komponenty:

☐☐*Oracle Identity Manager* slouží ke správě intranetových i extranetových uživatelských identit
☐☐*Oracle Role Manager* poskytuje kompletní sadu vlastností pro správu životního cyklu rolí
☐☐*Oracle Access Manager* poskytuje centralizovaný systém služeb pro řízení přístupů a SSO
☐☐*Oracle Web Services Manager* je nástroj pro řízení přístupů k internetovým službám a zdrojům
☐☐*Oracle Identity Federation* obsahuje řešení pro centrální federativní SSO pro bezpečné sdílení informací mezi důvěryhodnými partnery a zjednodušuje integraci aplikací za použití SOA a internetových
☐☐*Oracle Enterprise Single Sign-On* je řešení poskytující vlastnosti SSO pro desktopové a serverové platformy založené na operačním systému Microsoft Windows
☐☐*Oracle Entitlements Server* umožňuje ověřování aplikací díky unifikované jednoduché správě kompletních ověřovacích politik
☐☐*Oracle Adaptive Access Manager* Poskytuje zdroje pro ochranu před podvodným jednáním zahrnující softwarové vícefaktorové ověřování
☐☐*Oracle Management Pack for Identity management* je rozšířením možností nástroje Oracle Enterprise Manager, který slouží pro správu celé řady Oracle produktů včetně Oracle Database

Vzájemná spolupráce řešení

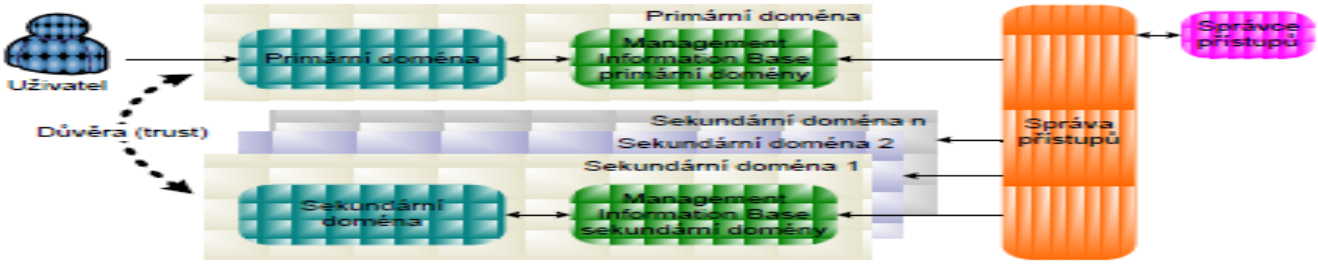
Vzájemná spolupráce řešení adresářových serverů se stává v dnešním globálním světě stále více důležitou vlastností všech adresářových služeb založených na LDAP. Vzájemná slučitelnost systémů a služeb hraje nedílnou roli nejenom v případě komunikace s obchodními partnery, rozšiřování vlastní infrastruktury, ale také při spojování společností, akvizicích nebo outsourcingu IT.

Single Sign-on

Single Sign-On je mechanismus, pomocí něhož jednou ověřený uživatel má povolen přístup ke všem zdrojům, ke kterým by se jinak musel opětovně přihlašovat (*Obrázek 32 Přístup ke zdrojům bez SSO*). Umožňuje tedy využívat jediné uživatelské identity ke všem zdrojům, které to vyžadují a zároveň být přihlášen pouze jednou (*Obrázek 33 Přístup ke zdrojům s SSO*).

Obrázek 32 Přístup ke zdrojům bez SSO

Historicky byly distribuované systémy sestaveny z komponentů v odlišných bezpečnostních doménách. Tyto domény obsahovaly individuální platformy skládající se z různých operačních systémů a aplikací. Tento koncept nezávislých domén měl za následek, že se každý uživatel musel identifikovat a ověřit nezávisle do každé takové domény, kde vyžadoval použití příslušných zdrojů. Takový uživatel, který byl přihlášen do primární domény, musel pro přístup do jiných bezpečnostních domén zadávat své uživatelské jméno a heslo.



Obrázek 33 Přístup ke zdrojům s SSO

Služby SSO vznikly pro eliminaci nutnosti přehlašování uživatelských identit mezi bezpečnostními doménami. Po ověření identity primární doménou již není uživatel vyzýván k přihlašování do dalších domén za předpokladu, že mezi doménami je nastavena důvěryhodnost (trust), a vložená identita je platná i pro sekundární domény. Pro služby SSO se primárně využívá protokolu Kerberos, který slouží pro distribuci a ověřování identit mezi bezpečnostními doménami – oblastmi (realm).

OpenID

OpenID je otevřeným, decentralizovaným standardem pro ověřování uživatelů a řízení přístupů, dovolující využívat přístup na sdílené internetové a intranetové aplikace a služby s jednou digitální identitou. Nahrazuje zavedený systém nutící uživatele k přihlášení svým uživatelským jménem a heslem, kdykoli přistupuje ke sdílené službě. Pomocí OpenID je uživatel přihlášen pouze jednou a nadále využívá přístupu ke zdrojům umístěným v různých systémech. Není tedy pro každé přihlášení potřeba sdělovat citlivé informace jako je kombinace uživatelské jméno a heslo. Ověřování pomocí OpenID je podporováno a využíváno velkým množstvím poskytovatelů služeb, jako například Google, IBM, Microsoft, AOL, BBC, MySpace, Yahoo! a VeriSign.
OpenID je ve své podstatě jednoznačné URL a je ověřováno poskytovatelem, kde je uživatel registrován. Proces ověřování začíná u internetové aplikace, která vyžádá OpenID identifikátor. Běžné formuláře pro přihlašování k digitálnímu obsahu obsahují pole pro zadání uživatelského jména a hesla. V případě OpenID je uživatel požádán o vložení jeho jednoznačného identifikátoru OpenID. Vedle příslušné řásky ve formuláři je zobrazen malý piktogram . Ten označuje, že formulář využívá klientské knihovny OpenID pro ověřování identity. Internetová služba požadující ověření provede transformaci uživatelova OpenID do formátu URL. URL je použito k získání informací o identitě. Pokud není identita ověřena, je systémem provozovatele služby OpenID zobrazen dialog vyzývající k vložení uživatelského hesla. Po jeho vložení a ověření je umožněn přístup pod jednoznačnou identitou k internetovému obsahu.

Bezpečnost

Veškeré ze zde popsaných adresářových systémů a systémů pro správu uživatelských identit umožňují použití nejmodernějších bezpečnostních doporučení a protokolů, které jsou založeny na modulech SASL a Kerberos. Zároveň je celá datová komunikace

zpravidla šifrována protokoly SSL nebo TLS. Úroveň zabezpečí je ale velmi důležitá v případě, že komunikace probíhá v rámc extranetu, kde může dojít k narušení citlivosti nebo autentičnosti přenášených dat. Tyto transportní kanály je ale možno dál zabezpečit
například pomocí technologie VPN nebo IPsec.
Vždy ale záleží na jednoznačném rozhodnutí správce systému, zda a jakého zabezpečení bude použito. O zabezpečení adresářových sužeb přímo pojednává kapitola 5.3 *Bezpečnost LDAP*.

Integrace produktů

Jednou z mnoha předností je možnost využití LDAP adresářových serverů a uložených identit jako zdroj dat pro další služby a aplikace. Lze tedy nastavit služby pro centrální ověřování, ale také pro ukládání aplikačních nastavení vztahujících se k jednotlivým uživatelům, ale samozřejmě i dalším zdrojům umístěným v enterprise prostředí a internetu.
LDAP adresářové servery je tedy možno integrovat s operačními systémy, aplikačními servery sloužící pro poskytování obsahu v rámci intranetu i extranetu, ale i jednotlivými aplikacemi.

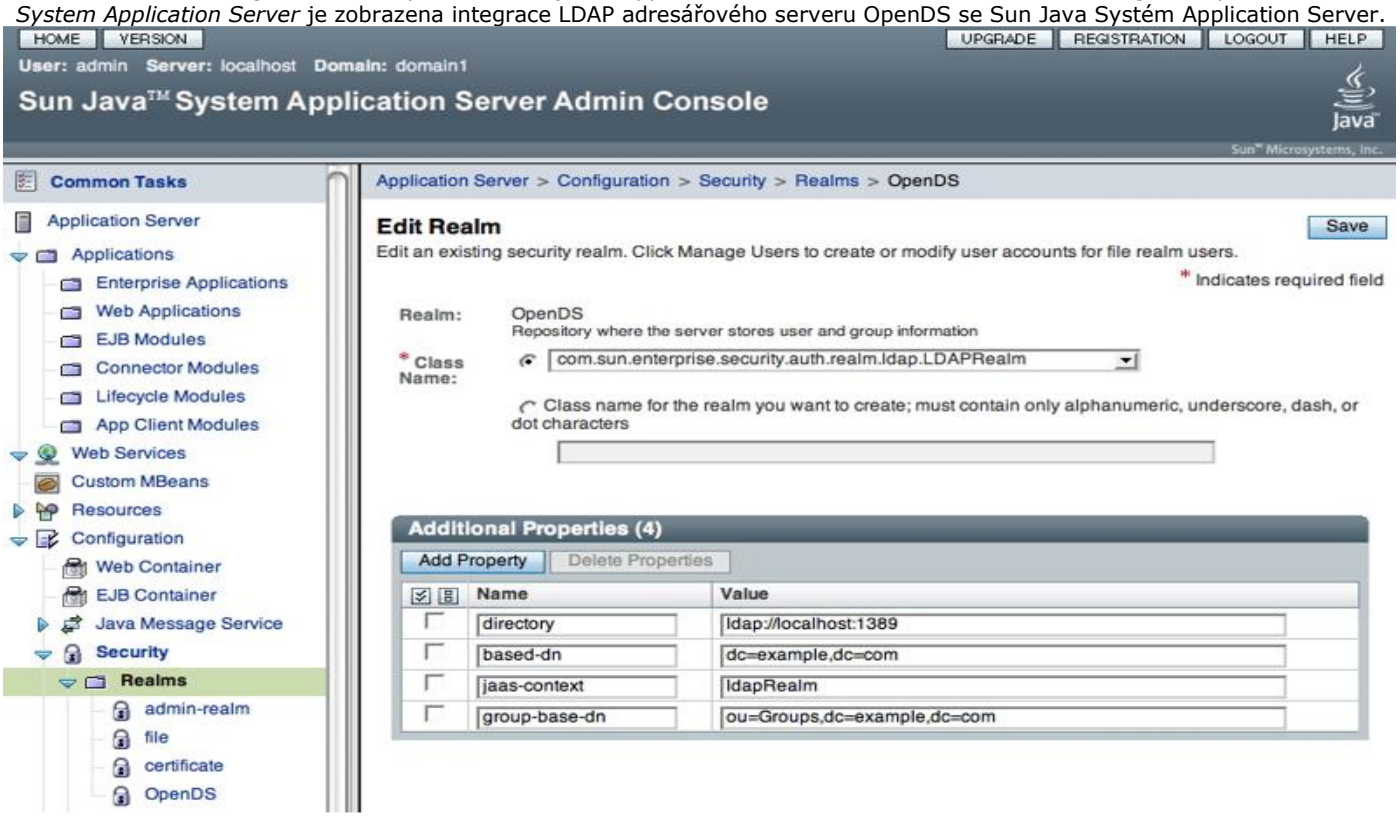
Integrace v operačních systémech

V současné době je možné integrovat LDAP adresářové služby prakticky do všech operačních systémů UNIXového typu, i Microsoft Windows. V případě systémů typu UNIX je možné použít přímé podpory těchto operačních systémů, tj. bez použití adaptérů a konvertorů. V případě Microsoft Windows je nutné použít vrstvu, která emuluje Windows Domain Controller a překládá patřičné OID z použitých schémat na identifikátory, které jsou běžné ve světě Windows. Takovým software je kupříkladu open-source produkt Samba, jež je komunitním projektem a obsahuje velkou část vlastností kompatibilních s Microsoft Windows. Za použití služeb založených na Single Sign-On se z takového řešení systému stává plnohodnotné řešení pro nasazení ve firemním prostředí.
Na příkladu je možné vidět jednoduchou konfiguraci LDAP adresářových služeb použitých pro ověřování uživatelů a jako zdroj informací o účtech v operačním systémy Linux/GNU. Tato konfigurace se nachází v souboru /etc/ldap.conf a využívá adresářových služeb LDAP verze 3.

```
host ldap2.firma.cz ldap.firma.cz
uri ldap://ldap2.firma.cz ldap://ldap.firma.cz
base dc=firma,dc=cz
ldap_version 3
ssl on
ssl start_tls
scope sub
bind_policy soft
pam_password exop
pam_filter objectclass=posixAccount
pam_login_attribute uid
pam_member_attribute memberUid
pam_check_host_attr yes
nss_base_passwd ou=People,dc=firma,dc=cz
nss_base_group ou=Group,dc=firma,dc=cz
```

Integrace v aplikačních serverech

Přínos aplikačních serverů je se v dnešní době stává stále více výhodnější, a to vzhledem k novým technologiím, ale také jako možnost šetřit další výdaje na pořizování nových technologií. I v tomto prostředí je výhodné nasazovat technologie pro centrální správu uživatelských identit a centrální adresářové služby. Veškeré současné Java aplikační servery umožňují integraci LDAP adresářových služeb založených na LDAP verze 3 a dalšími rozšířeními, jako jsou federativní služby a podpora SSO. Těmito Java aplikačními servery jsou například GlassFish, Sun Web Server, Apache Tomcat, Apache Geronimo, Oracle Application Server, Oracle – BEA Weblogic, IBM WebSphere a nebo jBoss Application Server. Na obrázku *Obrázek 34 Integrace OpenDS s Java System Application Server* je zobrazena integrace LDAP adresářového serveru OpenDS se Sun Java Systém Application Server.



Integrace v aplikacích

Integrace adresářových služeb přímo do aplikací umožňuje snižovat počet administrativních úkonů v případě správy uživatelských identit a aplikačních úložišť. Není tedy potřeba zabezpečit synchronizaci identit mezi aplikacemi, které podporují protokol LDAP. S tím dále souvisí i uživatelská transparentnost ověřování v případě nasazení služeb SSO.

Následující příklad ukazuje použití řízení přístupů u internetového serveru Apache http Server. Nastavení je uloženo v souboru .htaccess příslušné složky, kde má mýt použito ověření identity.

```
AuthType Basic
AuthName "Restricted zone: MSISDN Localization"
AuthBasicProvider ldap
AuthBasicAuthoritative On
AuthLDAPURL
ldap://ldap.firma.cz:389/ou=People,dc=firma,dc=cz?uid?sub?(objectClass=*)
Require valid-user
AuthzLDAPAuthoritative off
```