Univerzita Pardubice

Fakulta elektrotechniky a informatiky

Multiplatformní správa uživatelských účtů

Bubák Miroslav

Bakalářská práce

2008

ZDE BUDE ZADÁNÍ

ZDE BUDE ZADÁNÍ

Souhrn

Tato bakalářská práce se zabývá centralizovanou správou uživatelských účtů. Má za cíl navrhnout nekomerční řešení pro malé/střední firmy. Popsáno je několik nejrozšířenějších metod pro uložení informací o uživateli na straně serveru.

Klíčová slova

multipatformní, uživatelský účet, LDAP, Samba, správa

Title

Multiplatform user accounts management

Abstract

This bachelor work deals with central user accounts management. It aims to project noncommercial solution which could be used in small/middle company. This paper describes the most common methods used to store user informations on the server side.

Keywords

multipatform, user accounts, LDAP, Samba, management

Obsah

Seznam obrázků

Seznam tabulek

Seznam zkratek

AD – Active Directory.....adresářový server
API – Application Programming Interface.....rozhraní pro programování aplikací
BSD – Berkeley Software Distribution.....
.....odvozenina Unixu distribuovaná Kalifornskou univerzitou v Berkeley
CN – Common Name.....běžné jméno
CPU – Central Processing Unit.....centrální procesorová jednotka
DIT – Directory Information Tree.....stromová architektura LDAP
DN – Distinguished Name .....rozlišovací jméno
DNS – Domain Name Server.....jmenný server
GID – Group Identification.....číslo pracovní skupiny
GNU – GNU's Not Unix.....projekt vytváření svobodného operačního systému GNU
HA – High Availability.....vysoká dostupnost
HDD – Hard Disk Drive.....pevný disk
HTTP – Hypertext Transfer Protocol.....internetový protokol
HTTPS – Hypertext Transfer Protocol over Secure Socket Layer.....
.....internetový protokol se zabezpečením
LAN – Local Area Network.....místní síť
LDAP – Lightweight Directory Access Protocol.....
.....definovaný protokol pro ukládání a přístup k datům na adresářovém serveru
LDIF – Data Interchange Format.....formát dat serveru LDAP
NFS – Network File System.....
.....internetový protokol pro vzdálený přístup k souborům přes počítačovou síť
NSS – Name Service Switch
NT – New Technology.....nová technologie
NTFS – New Technology File systém.....typ souborového systémmu
OU – Organisation Unit.....organizační jednotka
PAM – Pluggable Authentication Modules.....
…..mechanizmus pro integraci více nízkoúrovňových autentizačních schémat do API
PC – Personal Computer.....osobní počítač
PDC – Primary Domain Controller.....primární doménový řadič
PHP – Hypertext Preprocessor.....hypertextový preprocesor
RAM – Random-Access Memory.....paměť s náhodným přístupem
RDN – Relative Distinguished Name .....relativní rozlišovací jméno
SMB – Server Message Block.....síťový komunikační protokol aplikační vrstv
SSL – Secure Sockets Layer.....vrstva bezpečných socketů
UID – User Identification.....uživatelské číslo
UNIX – Unary Information and Computing Service.....
.....víceúlohový a víceuživatelský operační systém
WWW – World Wide Web.....aplikace internetového protokolu HTTP

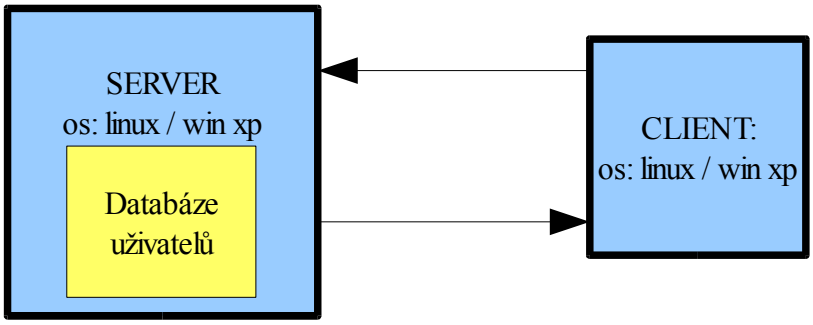
Úvod

Ve většině institucí se setkáme s osobními počítači zapojenými do lokální/místní počítačové sítě. Vždy mě zajímalo, co vlastně obnáší práce správce sítě. Mimo spravování sítě jako takové, mě zaujala zejména správa pracovních stanice. V ideálním případě bychom měli všechny počítače identické, nejen co se hardwarové stránky týče, ale zejména se stejným operačním systémem. S tím se ovšem v dnešní době setkáme v praxi zcela výjimečně. Většinou se jedná o heterogenní síť se stanicemi s operačními systémy nejen od společnosti Microsoft, ale i s poslední dobou rozrůstajícím se Linuxem. Pro uživatele je jednoznačně příjemnější, mohou-li se přihlašovat jak do operačního systému Linux, tak do operačních systémů Microsoft Windows se stejným přihlašovacím jménem a heslem.

Na úvod své bakalářské práce bych chtěl zmínit možné technologie pro vytvoření centrální správy uživatelských účtů. Následuje seznámení s technologií, kterou jsem si vybral pro vypracování své praktické části bakalářské práce. Za cíl si kladu vytvoření freewarového řešení centrálního serveru pro autentizaci a autorizaci uživatelů, který by byl použitelný pro nasazení v malé či středně velké lokální počítačové síti (LAN). V síti budou zapojeny stanice s operačními systémy Microsoft Windows XP Professional edition a Linux distribuce Debian ve verzi 4.0 (Etch). Řešení bude aplikovatelné i na jiné distribuce.

1. Teoretický rozbor

Všechna řešení mají společnou topologii. V síti bude centrální server, na němž budou uloženy informace o uživatelských účtech. K němu se budou připojovat pracovní stanice, které se skrze něj autentizují. Následně bude možno autorizovat uživatele, a tak mu umožnit přihlásit se na svůj uživatelský účet.



Obrázek 1: Topologie klient-server

Zdroj: vlastní

1.1. Co ukládat – informace o uživateli

O uživatelích budeme uchovávat, jak povinné, tak nepovinné informace. Každý operační systém se liší v tom, jaké informace jsou pro něj povinné.

1.1.1. Unix

Povinné údaje pro operační systémy Unix jsou přihlašovací jméno, heslo, user id, group id, cesta domácího adresáře a přihlašovací shell.

Mezi nepovinné údaje patří například jméno, příjmení nebo adresa bydliště.

1.1.2. Windows

Pro operační systémy Microsoft Windows si vystačíme s dvěma atributy. Povinné jsou přihlašovací údaje do systému, tedy přihlašovací jméno a heslo.

1.1.3. Společné informace

Mezi společné atributy tedy patří přihlašovací jméno a heslo, případně též plné jméno.

1.2. Možnosti uložení informací o uživatelských účtech na straně serveru

Je několik způsobů jak uchovávat informace o uživatelských účtech na straně serveru.

1.2.1. Textový soubor

Údaje o uživatelích jsou uloženy v textovém souboru v souborovém systému. Na každém řádku se nachází informace o jednom uživatelském účtě. Jednotlivé atributy účtu jsou odděleny speciálním znakem (středník, dvojtečka).

Příklad obsahu takového souboru:

```
gdm:heslo1:106:111:Gnome Display Manager:/var/lib/gdm:/bin/false
hplip:heslo2:107:7:HPLIP system user,,,:/var/run/hplip:/bin/false
mike:heslo3:1000:1000:mike,,,:/home/mike:/bin/bash
pc-01:heslo4:1002:1002:,,,:/home/pc-01:/bin/bash
winxp:heslo5:1001:1001:,,,:/home/winxp:/bin/bash
winxp$:heslo6:1003:103:Machine account:/dev/null:/bin/false
sshd:heslo7:108:65534::/var/run/sshd:/usr/sbin/nologin
openldap:heslo8:109:112:OpenLDAP Server Account,,,:/var/lib/ldap:/bin/false
```

Výhody:

- Soubor je snadno editovatelný v jakémkoliv prostředí na většině platforem.
- Zanedbatelné nároky na hardware serveru.

Nevýhody:

- Soubor je fyzicky dostupný v souborovém systému a je nebinární (v čitelné formě).
- Pomalé vyhledávání.
- Nižší přehlednost.

1.2.2. Formát Excelu

Údaje uživatelských účtů jsou přehledně uloženy v tabulce. Na každém řádku se nachází informace o unikátním účtu. Každý sloupec pak znamená jednotlivé informace/atributy příslušného účtu.

user name	password	uid	gid	comment	home	bash
gdm	heslo1	106	111	Gnome Display Manager	/var/lib/gdm	/bin/false
hplip	heslo2	107	7	HPLIP system user,,,	/var/run/hplip	/bin/false
mike	heslo3	1000	1000	mike,,,	/home/mike	/bin/bash
pc-01	heslo4	1002	1002	,,,	/home/pc-01	/bin/bash
winxp	heslo5	1001	1001	,,,	/home/winxp	/bin/bash
winxp$	heslo6	1003	103	Machine account	/dev/null	/bin/false
sshd	heslo7	108	65534		/var/run/sshd	/usr/sbin/nologin
openldap	heslo8	109	112	OpenLDAP Server Account,,,	/var/lib/ldap	/bin/false

Obrázek 2: Uživatelé uložení ve formátu Excelu

Zdroj: vlastní

Výhody:

- Soubor je přehledný.
- Nízké nároky na hardware serveru.

Nevýhody:

- Pro jeho editaci potřebujeme specifické nástroje.
- Nízká podpora ze strany vývojářů. Ve většině případů budeme muset doprogramovat aplikaci na získání dat.
- Nízká úroveň zabezpečení, soubor je opět nešifrované formě dostupný v souborovém systému.
- Nízká rychlost vyhledávání.

1.2.3. Relační databázové systémy

„Relační databáze je databáze, založená na relačním modelu. Často se tímto pojmem označuje nejen databáze samotná, ale i její konkrétní softwarové řešení.

Relační databáze je založena na tabulkách, které obvykle chápeme tak, že uchovávají informace o relacích mezi jednotlivými záznamy v matematickém slova smyslu.

Termín relační databáze definoval Edgar F. Codd v roce 1970.

Základem relačních databází jsou databázové tabulky. Jejich sloupce se nazývají atributy nebo pole, řádky tabulky jsou pak záznamy. Atributy mají určen svůj konkrétní datový typ – doménu. Řádek je řezem přes sloupce tabulky a slouží k vlastnímu uložení dat. Konkrétní tabulka pak realizuje podmnožinu kartézského součinu možných dat všech sloupců – relaci.

Index nebo též klíč je jednoznačný identifikátor záznamu, řádku tabulky. Klíčem může být jediný sloupec či kombinace více sloupců tak, aby byla zaručena jeho jednoznačnost. Pole klíče musí obsahovat hodnotu, tzn. nesmí se zde vyskytovat nedefinovaná prázdná hodnota NULL.

Dalším důležitým pojmem jsou nevlastní/cizí klíče. Slouží pro vyjádření vztahů, relací, mezi databázovými tabulkami. Jedná se o pole či skupinu polí, která nám umožní identifikovat, které záznamy z různých tabulek spolu navzájem souvisí.

Vztahy, neboli relace, slouží ke svázání dat, která spolu souvisejí a jsou umístěny v různých databázových tabulkách.“ [1]

Dostupné relační databáze jsou například:

- MySQL,
- MS SQL Server,
- Oracle,
- PostgreSQL.

Výhody:

- přehlednost,
- vyšší bezpečnost,
- vysoká podpora ze strany vývojářů.

Nevýhody:

- Oproti vyhledávání v LDAP musíme procházet každý záznam zvlášť.
- Vyšší nároky na hardware oproti použití textového/Excel formátu souboru.

1.2.4. Protokol LDAP

LDAP (Lightweight Directory Access Protocol) je protokol, který slouží k ukládání a přístup k datům na adresářovém serveru. Jednotlivé položky jsou na serveru ukládány formou záznamů a jsou uspořádány do stromové struktury (jako ve skutečné adresářové architektuře). Je vhodný pro udržování adresářů a práci s informacemi o uživatelích (např. pro vyhledávání adres konkrétních uživatelů v příslušných adresářích, resp. Databázích).

Protokol LDAP je založen na doporučení X.500, které bylo vyvinuto ve světě ISO/OSI, ale do praxe se ne zcela prosadilo, zejména pro svou „velikost“ a následnou „těžkopádnost“. Protokol LDAP již ve svém názvu zdůrazňuje fakt, že je „odlehčenou“ (lightweight) verzí, odvozenou od X.500. V aplikaci funguje na bázi klient server. V komunikaci využívá jak synchronní tak asynchronní mód. Součástí LDAP je autentizace klienta.

DIT

LDAP využívá tzv. strom objektů (DIT – Directory Information Tree). Ten je tvořen jednotlivými záznamy (entitami). Každý záznam má své jedinečné jméno (DN – distinguished name) skládající se z jeho relativního jména (relative distinguished name – RDN) a RDN jeho předchůdců. Každá entita má svoje atributy – povinné a nepovinné. Tyto atributy jsou definované pomocí objektů.

Formát LDIF

LDIF (Data Interchange Format) je speciální formát, ve kterém se uchovávají záznamy a jejich atributy. Jednotlivé záznamy jsou od sebe odděleny prázdným řádkem.

Příklad:

```
# LDIF zaznam pro uzivatele root
dn: uid=root,ou=People,dc=debianek
uid: root
cn:: cm9vdA==
sn:: cm9vdA==
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
```

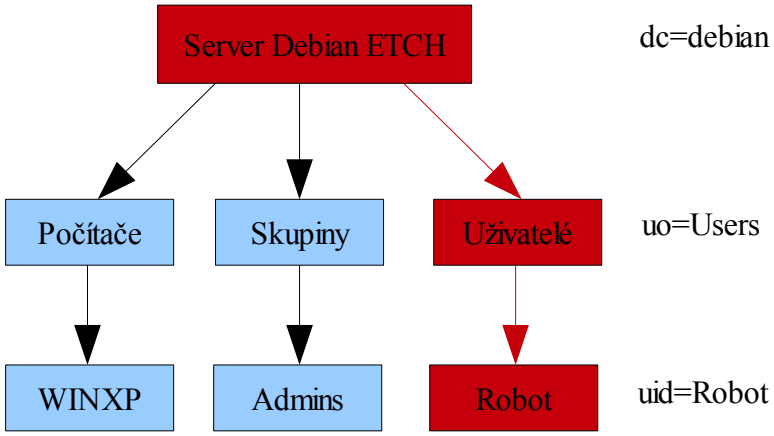
```
objectClass: top
objectClass: shadowAccount
userPassword: {crypt}$1$m0Q2Iz26$vsNx6d2pMcRVZg01XXahM/
shadowLastChange: 13995
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 0
gidNumber: 0
homeDirectory: /root
gecos: root
```

Schémata

LDAP využívá tzv. schémata, což je v podstatě soubor definic pravidel nad adresářovým stromem. Definuje množinu objektů a jejich atributy – povinné a nepovinné.
Při zvolení OpenLDAPu se nacházejí v /etc/ldap/schema (v distribuci Debian).

LDAP implementace

- OpenLDAP,
- Apache Directory Server,
- Fedora Directory Server,
- Red Hat Directory Server,
- Novell eDirectory,
- Sun Directory Server Enterprise Edition,
- IBM Lotus Domino,
- Windows Server 2003 Active Directory,
- Oracle Internet Directory,
- tinyldap.



Obrázek 3: Organizační diagram uspořádání dat protokolu LDAP

Zdroj: vlastní

Výhody:

- Data jsou uložena v hierarchické stromové struktuře.
- Dostupnost.
- Široká podpora ze strany vývojářů.
- Jeho použití je zdarma.
- Jednoduchá implementace.
- Vysoká rychlost vyhledávání.

Nevýhodou jsou:

- Vyšší nároky na hardware oproti použití textového/Excel formátu souboru.

1.2.5. Shrnutí kapitoly

Jako nejvýhodnější se jeví použít pro náš server aplikaci s implementací protokolu LDAP. Ve srovnání s ostatními možnostmi centrálního uchování dat vyniká především bezpečností a vysokou rychlostí vyhledávání. Díky široké podpoře ze strany vývojářů se dají z LDAP čerpat informace skoro do jakékoliv aplikace třetí strany a tam je využít dle potřeby.

Jakou aplikaci zvolíme, závisí především na tom, jaký operační systém se bude nacházet na serveru.

1.3. Operační systémy

Dalším důležitým krokem pro náš server s centralizovanou správou uživatelů je výběr operačního systému.

Máme několik možností:

- Microsoft Windows:
  - Windows 2000 Server,
  - Windows XP Professional,
  - Windows 2003 Server,
  - Windows Server 2008.
- Linux:
  - Debian,
  - Ubuntu,
  - Fedora Core,
  - Suse,
  - a další distribuce.
- BSD:
  - FreeBSD,
  - OpenBSD.
- Solaris,
- Mac OS X.

Ve své práci bych se zmínil o dvou nejdostupnějších operačních systémech a zohlednil je z hlediska našeho využití.

1.3.1. Microsoft Windows

Operační systémy od společnosti Microsoft jsou jednoznačně nejpoužívanější operační systémy vůbec.

Charakteristické rysy:

- komerční software,
- globálně nejpoužívanější operační systémy,
- jednoduchá správa přes uživatelsky přívětivé grafické rozhraní,
- silná podpora jak ze strany vývojářů software i hardware,
- relativní stabilita systému.

1.3.2. Linux

Poslední dobou se čim dál tím víc setkává s oblibou operační systém Linux.

Charakteristické rysy:

- nekomerční software,
- díky textovému režimu možnost nastavit prakticky cokoliv,
- vysoká stabilita a dostupnost (HA – high availability – není výjimkou, že systém běží několik let bez restartu s vynikajícími výsledky),
- slabší podpora ze strany vývojářů hardware (ovladače).

V podstatě bych se řídil pravidlem, že pokud chceme postavit kvalitní a stabilní server, který má za cíl běžet neustále, měli bychom využít možnosti nekomerčního řešení v podobě Linuxu.

Pokud se jedná o pracovní stanice, ve většině případů bych sáhl po operačních systémech značky Microsoft. Hlavním důvodem je široká podpora ze strany vývojářů a podpora hardware.

1.4. Server

Aplikační server využívající platformu Microsoft Windows, se nazývá Active Directory.

1.4.1. Active Directory

„Active Directory je implementace adresářových služeb LDAP firmou Microsoft pro použití v prostředí systému Microsoft Windows. Active Directory umožňuje administrátorům nastavovat politiku, instalovat programy na mnoho počítačů nebo aplikovat kritické aktualizace v celé organizační struktuře. Active Directory ukládá své informace a nastavení v centrální organizované databázi.

Adresářová služba Active Directory je rozšiřitelná a škálovatelná adresářová služba, která umožňuje efektivně uspořádat síťové prostředky.

- Vyžaduje instalaci služby DNS,
- je založena na standardních internetových protokolech,
- jednoznačně definuje strukturu sítě,
- organizuje skupiny počítačů a domén.

Vnější struktura Active Directory

Služba Active Directory obsahuje logické i fyzické struktury součástí sítě.

a) Logické

- Organizační jednotky – podskupiny domén, které často odpovídají obchodní nebo řídící struktuře organizace .
- Domény – skupiny počítačů sdílejících společnou adresářovou databázi.
- Stromy domén – jedna nebo více domén sdílejících souvislý obor názvů.
- Lesy domén – jeden nebo více stromů domén sdílejících společné adresářové informace.

b) Fyzické

- Podsítě – síťová skupina se specifickým rozsahem adres IP a masky podsítě.
- Sítě – jedna nebo více podsítí, slouží ke konfiguraci přístupu k adresářové službě a replikací.

Logické struktury pomáhají při organizaci objektů adresářové služby a při správě účtů a sdílených prostředků sítě. Fyzické struktury usnadňují komunikaci v síti a fyzicky ohraničují prostředky sítí.

Doména

Doména Active Directory je v podstatě skupinou počítačů sdílejících společnou adresářovou databázi.

- Základní jednotka AD, tvoří ji min. 1 DC (Domain Component).
- Je bezpečnostní hranice ve struktuře Active Directory.
- Reprezentuje replikační hranici.
- Má jednoznačné označení.
- Má vlastní zásady zabezpečení.
- Vytváří vztahy důvěry s ostatními doménami.

Doménový strom

- Hierarchické spojení domén vytvořené vztahem rodič-potomek.
- Všechny domény v doménovém stromu sdílejí stejný jmenný prostor (root namespace).
- Uživatelé mohou prohledávat informace v rámci doménového stromu.
- Schéma je stejné v rámci doménového stromu.

Organizační jednotky

Jsou to podskupiny v rámci domén, které často odráží řídící nebo obchodní strukturu organizace. OU si také můžeme představit jako logické kontejnery, do kterých si můžeme umístit:

- uživatelské účty,
- sdílené prostředky,
- další OU.

Vnitřní struktura adresářové služby

Služba Active Directory má mnoho součástí a je založena na mnoha technologiích. Její data jsou zpřístupněna uživatelům a počítačům prostřednictvím úložiště dat a globálních katalogů. Přestože většina úkolů služby Active Directory ovlivňuje úložiště dat, jsou globální katalogy stejně důležité, neboť se využívají při přihlašování a při hledání informací. Pokud není globální katalog k dispozici,

nemohou se běžní doménoví uživatelé přihlásit. Jediným způsobem, jak toto chování změnit, je ukládat členství v univerzálních skupinách do místní mezipaměti. Toto řešení má své výhody i nevýhody – viz dále. K datům služby Active Directory se přistupuje pomocí protokolů pro přístup k adresářové struktuře a její data se distribuují pomocí replikací. Protokoly pro přístup k adresářové službě umožňují klientským počítačům komunikovat s řadiči domény. Replikace zajišťuje distribuci aktualizovaných dat na řadiče domény. Přestože je replikace adresářových informací vždy typu *multimaster*, některé změny dat mohou provádět pouze individuální řadiče domény nazývané *operační servery*. Na replikace typu multimaster má také vliv nová vlastnost systému Windows Server 2003 nazvaná *Oddíl adresáře aplikace* (application directory partition). Správci velkých sítí (členové skupiny Enterprise Admins) mohou v lese domén vytvářet oddíly adresáře aplikací. Jedná se o logické struktury, pomocí kterých se řídí replikace dat v lese. Je např. možné vytvořit oddíl, který bude přesně určovat replikaci dat služby DNS v doméně. Ostatním systémům v doméně se tak zabrání v její replikaci.

Oddíly adresáře aplikací se mohou objevit jako:

- podřízený objekt domény,
- podřízený objekt jiného oddílu adresáře aplikací,
- nový strom ve stávajícím lese.

Úložiště dat

Úložiště dat (jinak nazývané jako *adresář*) obsahuje:

- informace o účtech,
- sdílené prostředky,
- organizační jednotky,
- zásady skupin.

Řadiče domény ukládají tento adresář v souboru Ntds.dit (umístění tohoto souboru se řeší při instalaci domény Active Directory a musí být na jednotce zformátované souborovým systémem NTFS. Adresářová data je také možné uložit odděleně od hlavního úložiště dat. To platí pro zásady skupiny, skripty a další typy veřejných informací, které jsou uložené ve sdílené systémové složce SYSVOL“ [2]

Výhody:

- Podpora ze strany výrobce.
- Využití LDAP protokolu.

Nevýhody:

- Jedná se o čistě komerční řešení. V Unixu se nabízí aplikační server OpenLDAP.

1.4.2. OpenLDAP

„OpenLDAP je svobodná implementace adresářového serveru a protokolu LDAP.“ [3]

Výhody:

- Freeware řešení.
- Jedná se o open source – podpora ze strany uživatelů.
- Využití LDAP protokolu.

Nevýhody:

- Složitější nastavení serveru.

1.5. Pracovních stanice

Pro pracovní stanice jsem zvolil dva operační systémy, které jsou dostupné v učebnách Fakulty elektrotechniky a informatiky Univerzity Pardubice.

1.5.1. Microsoft Windows XP Professional

Jedná se o prověřený stabilní operační systém. Verze professional je zvolena především z toho důvodu, že na rozdíl od levnější verze Home se dokáže připojit k doméně, což je v našem případě nutností.

1.5.2. Debian

Jako druhý operační systém jsem zvolil stejnou distribuci Linuxu jako je na našem serveru, a to ve verzi 4.0 (Etch). Tato distribuce je známá především díky dokonalému balíčkovacímu systému. Popisovaný postup instalace lze pak použít i na odvozené distribuce jako Linspire, Xandros nebo poslední dobou oblíbené Ubuntu (včetně klonů Kubuntu, Edubuntu či Xubuntu).

2. Vlastní řešení

Pro vypracování své bakalářské práce jsem použil svůj osobní počítač s následující konfigurací:

- CPU: Intel Q6600 (4 jádra),
- MotherBoard: Asus PK5,
- RAM: A-Data 4GB DDR2,
- HDD: 2x Quantum 250GB.

Pro virtualizaci serveru a pracovních stanic jsem použil software VMware Workstation. Vytvořil jsem virtuální server s Linuxem, tomu jsem alokoval 250 MB operační paměti. Dále jsem vytvořil dvě virtuální pracovní stanice s operačním systémem Microsoft Windows XP Professional a dvě virtuální pracovní stanice s Linuxem. Pro stanice s MS Windows XP jsem alokoval 512 MB a pro stanice s Linuxem 256 MB operační paměti.

2.1. Volba operačního systému

Za operační systém serveru jsem zvolil osvědčenou distribuci Linuxu Debian, především díky dokonalému balíčkovacímu systému.

Díky možnosti rychlého připojení k internetu jsem systém nainstaloval z image[1] verze netinstall a potřebné balíčky později stáhl přímo z repozitáře[2].

1 Obraz CD, který lze ve VMware přímo využít, aniž bychom ho museli vypálit na médium.
2 Úložiště distribuce pro software. Obvykle server typu FTP či HTTP.

2.2. Centrální databáze uživatelských účtů

Jako centrální úložiště informací o uživatelských účtech nám poslouží OpenLDAP server.

2.2.1. Stand-alone OpenLDAP daemon (slapd)

Podle návodu[3] nainstalujeme server OpenLDAP[4].

V Debianu využijeme balíčkovací systém a nainstalujeme balíček *slapd*.

```
apt-get install slapd
```

Nastavení serveru:

```
DNS domain name: debian
Name of organisation: debian
Admin password: heslo
Confirm password: heslo
Allow LDAP v2: yes
```

2.2.2. Apache 2.0 + PHP

Aby se dal spravovat strom LDAP přes webovou aplikaci PhpLDAPadmin, musíme nejdříve nainstalovat webový server Apache s podporou php-skriptů. Ten stáhneme na domácí stránce projektu[5]. Na stejné stránce najdeme i podrobně rozebrané možnosti nastavení serveru.

V Debianu opět využijeme vynikající příkaz apt-get a nainstalujeme balíček apache:

```
apt-get install apache
```

Díky balíčkovacímu systému je Apache plně přednastaven a zbývá pouze doinstalovat podporu php. Php si můžeme stáhnout na stránce projektu[6]. Potřebnou dokumentaci nalezneme na stejném serveru.

V Debianu nainstalujeme balíček *php5*.

```
apt-get install php5
```

3 Např. na adrese: http://phpldapadmin.wiki.sourceforge.net/en.doc.intro
4 http://phpldapadmin.sourceforge.net/
5 http://www.apache.org/
6 http://www.php.net/

Po instalaci je Apache server automaticky spuštěn, ale po doinstalování podpory php nebo změně v konfiguraci je potřeba jeho restart:

```
/etc/init.d/apache restart
```

2.2.3. Apache-SSL

Z důvodu vyšší bezpečnosti je ovšem lepší nainstalovat webový server Apache s podporou HTTPS. Tím bude zajištěn šifrovaný přenos komunikace mezi webovým serverem Apache a jednotlivými klienty připojenými přes webový prohlížeč.

Při instalaci na operačních systémech Linux bez podpory debianích balíčků budeme muset podporu šifrování SSL zapnout při kompilaci aplikace[7]. V některých případech stačí v konfiguraci Apache povolit modul SSL.

V distribuci Debian (případně odvozenin) máme k dispozici balíček *apache-ssl* s přednastavenou podporou šifrování.

```
apt-get install apache-ssl
```

Upravíme nastavení certifikátu, případně si platný certifikát zajistíme od certifikační autority.

2.2.4. PhpLDAPadmin

Jedná se o webovou administrační aplikaci, která je určená ke správě LDAP serveru. Práce s touto aplikací je opravdu snadná a značně zjednoduší práci při správě LDAP stromu.

Umožňuje následující funkce:

- prohledávání LDAP stromu,
- prohlížení LDAP schémat,
- vyhledávání záznamů,
- vytváření záznamů,
- kopírování záznamů,

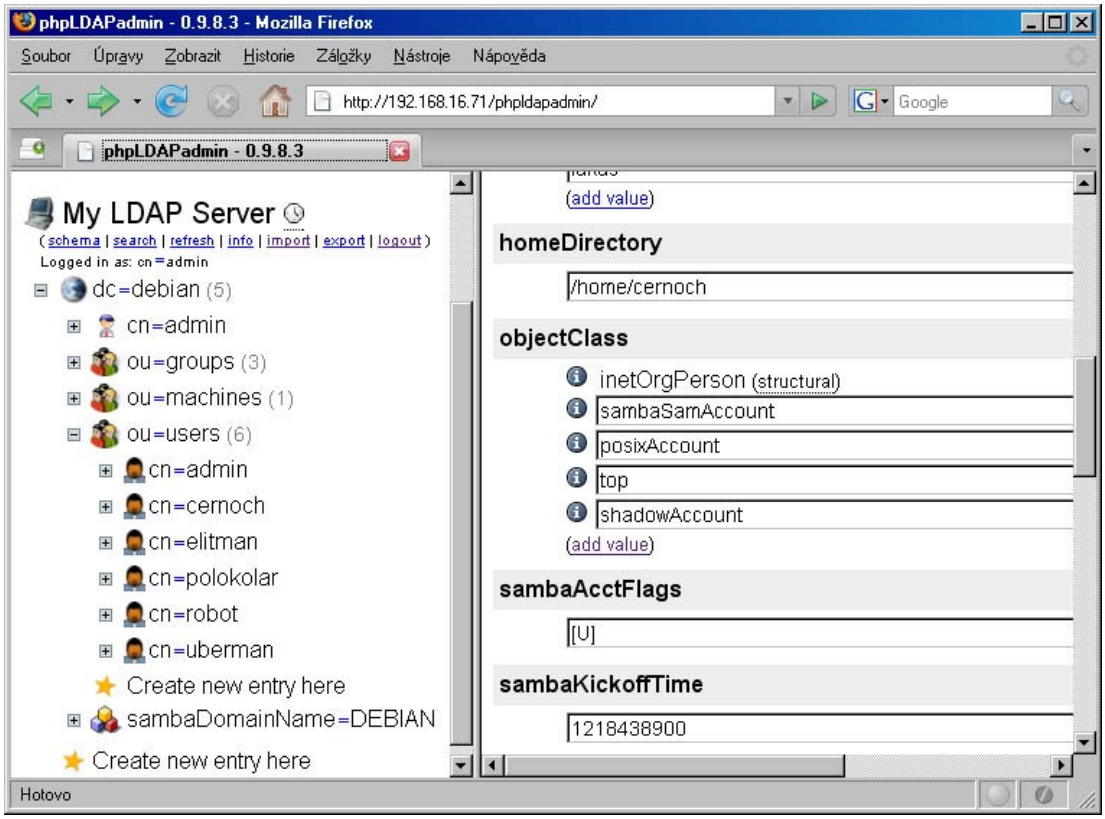
7 Více se dozvíme na adrese http://www.apache.org/.

- mazání záznamů,
- modifikaci záznamů.

Je volně ke stažení na domácí stránce projektu[8]. Tam se také nachází dostatečně podrobná dokumentace.

V Debianu se opět nachází přednastavený balíček *phpldapadmin*.

```
apt-get install phpldapadmin
```



Obrázek 4: PhpLDAPadmin – webová aplikace pro správu stromu LDAP

Zdroj: vlastní

2.3. Připojení pracovních stanic

Pro připojení pracovních stanic s operačním systémem Microsoft Windows XP nám poslouží aplikace Samba.

„Nastavíme Samba server, aby fungoval jako primární doménový řadič v naší síti. Vytvoříme doménu Windows NT s naším serverem, který bude pracovat jako řadič

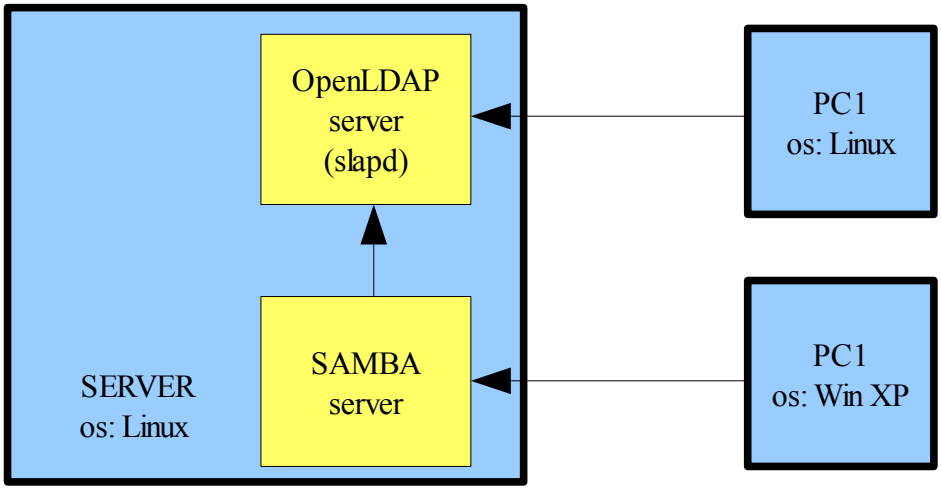
8 http://phpldapadmin.sourceforge.net/

domény, tzn., že bude poskytovat přihlašování do domény a autentizaci přístupu ke sdíleným prostředkům.“ [4]

Po přihlášení do domény NT bude uživateli k dispozici jeho domovský adresář na serveru. Ten bude moci využít pro ukládání jakýchkoliv dat. [4]

„Pomocí Samby můžeme na serveru či stanici sdílet další soubory či adresáře a poskytnout je ostatním klientům. To vše samozřejmě s využitím uživatelských práv.

Nastavíme Sambu k používání cestovních profilů. Cestovní profily slouží k poskytnutí lepšího pohodlí našim uživatelům tím, že po přihlášení na jakýkoliv počítač v naší síti jim bude k dispozici poslední nastavení jejich pracovního prostředí (ikony na ploše, nabídka Start, dokumenty apod.).“ [4]



Obrázek 5: Přihlašování pracovních stanic k serveru

Zdroj: vlastní

2.3.1. Samba

„Samba je svobodná implementace síťového protokolu SMB (Server Message Block, někdy též nazývaný NetBIOS), používaného především pro vzdálený přístup k souborům (sdílení) v systémech Microsoft Windows. Samba je distribuována pod licencí GNU General Public License.

V současné verzi 3 neposkytuje Samba pouze služby pro sdílení souborů a tiskových služeb pro klienty systému Windows, ale lze ji například využít pro integraci do domény Windows, buď jako primární doménový řadič (Primary Domain Controller, PDC) nebo jako běžného člena v doméně. Může být také součástí domény Active Directory.

Samba byla původně vyvinuta pro systém UNIX Andrewem Tridgellem, nyní běží na většině unixových systémů, které zahrnují GNU/Linux, Solaris, BSD, Mac OS X (od verze 10.2 je součástí OS X pro pracovní stanice – workstation) a jiné.

Dne 20.12.2007 obdržel Samba Team kompletní dokumentaci protokolu Microsoftu, viz [1] a [2]. Svět OSS tím získal důležité informace k implementaci otevřeného řešení s vysokou kompatibilitou.“ [5]

Samba server je volně ke stažení na adrese projektu[9], kde nalezneme i potřebnou dokumentaci aplikace.

Debian nabízí balíček *samba*.

```
apt-get install samba
```

Během instalování nastavíme:

```
Domain Name: debian
Use Password Encryption: Yes
Modify smb.conf to use WINS settings via DHCP: No
How to run Samba: daemons
Create password database: Yes
```

Protože budeme chtít používat autentizaci uživatele samby skrze OpenLDAP server doinstalujeme potřebný balíček samba-doc, ve kterém se nachází ukázka požadovaného souboru samba.schema. V něm nalezneme nadefinované potřebné třídy a jejich atributy.

```
apt-get install samba-doc
```

Abychom mohli využívat potřebné třídy objektů, musíme zkopírovat samba.schema do našeho slapd.

```
cd /usr/share/doc/samba-doc/examples/LDAP
cp samba.schema.gz /etc/ldap/schema/
gunzip samba.schema.gz
```

Dále ho musíme zahrnout v konfiguračním souboru /etc/ldap/slapd.conf, kam vložíme následující řádek:

```
include         /etc/ldap/schema/samba.schema
```

9 http://www.samba.org/

Nyní nám zbývá jen restartovat slapd, aby mohl načíst pozměněný konfigurační soubor:

```
/etc/init.d/slapd restart
```

Potřebujeme vytvořit kontejnery v LDAP pro uživatele, skupiny uživatelů a pracovní stanice. Přihlásíme se tedy do PhpLDAPadminu na adrese našeho serveru[10].

1. Přihlásíme se s heslem admina.
2. Rozbalíme kořenový strom a klikneme na „Create New Entry Here“, čímž se nám zobrazí obrazovka, kde si můžeme vybrat z tříd objektů.
3. Vybereme „Organization unit“ (ou).
4. Pojmenujeme ji „Users“.
5. A potvrdíme.

Kroky 2–5 opakujeme ještě 2× a vytvoříme „Organization unit“, kterou pojmenujeme „machines“ respektive „groups“.

Máme tedy vytvořené základní členění v našem LDAP stromu.

Následuje konfigurace samotného Samba serveru. Otevřeme si její konfigurační soubor /etc/samba/smb.conf a tento řádek:

```
passdb backend = tdbsam guest
```

nahradíme následujícími:

```
passdb backend = ldapsam:ldap://127.0.0.1
ldap suffix = dc=debian
ldap machine suffix = ou=machines
ldap user suffix = ou=users
ldap group suffix = ou=groups
ldap admin dn = cn=admin,dc=debian
ldap delete dn = no

# be a PDC
domain logons = yes

# allow user privileges
enable privileges = yes
```

10 Např. https://192.168.16.71/phpldapadmin (pokud náš server má adresu 192.168.16.71).

Pro kontrolu modifikovaného konfiguračního souboru Samby spustíme příkaz:

```
testparm
```

Dále musíme Samba serveru nastavit heslo, kterým se přihlásí k našemu OpenLDAP serveru.

```
smbpasswd -w password
```

Restartujeme Samba server, aby mohl z konfiguračního souboru načíst nové nastavení.

```
/etc/init.d/samba restart
```

Přihlásíme se přes PhpLDAPadmina a měl by se nám v kořeni stromu zobrazit záznam sambaDomainName=DEBIAN.

Všechno proběhlo v pořádku, a tak přidáme skupiny uživatelů do organizační jednotky uo=groups.

Unix name	Samba Name	gid	Samba Sid
Admins	Domain Admins	20000	Built-In -> Domain Admins
Users	Domain Users	20001	Built-In -> Domain Users
Guests	Domain Guests	20002	Built-In -> Domain Guests

Tabulka 1: Pracovní skupiny

Zdroj: vlastní

2.3.2. Libnss-ldap

„Tento balík poskytuje modul pro NSS (Name Service Switch), který umožňuje LDAP serveru vystupovat jako jmenná služba. To znamená, že může poskytovat informace o uživatelských účtech, skupinách, počítačích, aliasech, síťových skupinách a v zásadě čemkoliv, co byste získávali z ‚plochých' databázových souborů v /etc nebo NIS." [6]

Nainstalujeme tedy v Debianu balček *libnss-ldap*:

```
apt-get install libnss-ldap
```

S následujícím nastavením.

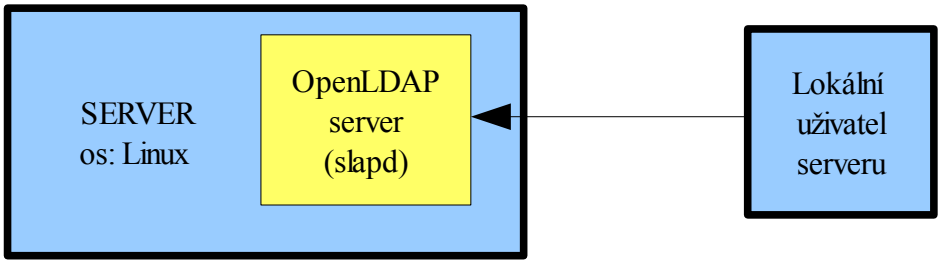
```
LDAP Server Host: 127.0.0.1
```

```
DN of Search Base: dc=nomis52,dc=net
LDAP Version: 3
Database requires login: no
Make config readable by owner only: yes
```

Upravíme konfigurační soubor /etc/nsswitch.conf.

```
Passwd:         compat ldap
group:          compat ldap
shadow:         compat ldap
```

Toto nastavení zajistí vyhledávání uživatelů nejprve v lokální databázi uživatelů (/etc/passwd) a poté v OpenLDAP (slapd).



Obrázek 6: Přihlášení lokálního uživatele (správce) serveru

Zdroj: vlastní

Pomocí příkazu getent ověříme, že byly vytvořeny naše skupiny z LDAP.

```
getent group
```

Měli bychom mj. dostat následující:

```
ssh:x:103:
users:x:20001:
guests:x:20002:
admins:x:20000:
```

2.3.3. PAM – Libpam-ldap

„Pluggable Authentication Modules neboli PAM je mechanizmus pro integraci více nízkoúrovňových autentizačních schémat do API, což umožňuje programům opírajícím se o autentizaci uložit uživatelské údaje nezávisle na použitém mechanizmu přihlášení. PAM byl poprvé vyvinut v roce 1996 firmou Sun Microsystems, později se stal standardním modulem UNIX/Linux systémů“ [7]

Nainstalujeme si balíček libpam-ldap:

```
apt-get install libpam-ldap
```

Nastavíme:

```
Make local root db admin: yes
Database requires logging in : no
Root login account : cn=admin,dc=nomis52,dc=net
Root password : password
Crypt : MD5
```

Dále musíme nakonfigurovat PAM pro náš server LDAP.

Upravíme soubor /etc/pam.d/common-account:

```
# Comment out the next line
#account        required        pam_unix.so
# and add these two
account         sufficient      pam_ldap.so
account         required        pam_unix.so try_first_pass
```

Dále soubor /etc/pam.d/common-auth:

```
# comment out the next line
#auth   required        pam_unix.so nullok_secure
# and add these two
auth    sufficient      pam_ldap.so
auth    required        pam_unix.so nullok_secure use_first_pass
```

A nakonec soubor /etc/pam.d/common-password:

```
# comment out the next line
#password   required   pam_unix.so nullok obscure min=4 max=8 md5
# and add these two
password   sufficient pam_ldap.so
password        required        pam_unix.so nullok obscure min=4 max=8 md5
use_first_pass
```

Nyní bude potřeba restartovat servery ssh a Samba.

```
/etc/init.d/ssh restart
/etc/init.d/samba restart
```

2.3.4. Name service caching daemon

„Použití cachovacího démona nscd (Name Service Cache Daemon) z glibc 2.1 sníží provoz na síti a urychlí vyhledávání záznamů.“ [8]

Nainstalujeme Name service caching daemon:

```
apt-get install nscd
```

2.4. Vytvoření uživatelů

Přes PhpLDAPadmina přidám do skupin dva uživatele. Uživatel Administrator musí mít uid=0.

Uid	First Name	User Name	User Password	Encryption	Windows Group
0	Admin	Administrator	heslo	MD5	Domain Admins
10000	Robot	robot	*****	MD5	Domain Admins

Tabulka 2: Tabulka uživatelů

Zdroj: vlastní

Opět si příkazem getent passwd ověřím, že se mi nově vytvoření uživatelé objeví i mezi unixovými uživateli:

```
robot:x:10000:20000:Simon Newton:/home/robot:/bin/bash
Administrator:x:0:20000:admin:/home/administrator:/bin/bash
```

Pro nově vytvořeného uživatele musím vytvořit domácí adresář.

```
mkdir /home/robot
cp /etc/skel/.* /home/robot/
chown -R robot:users /home/robot
```

Pro ověření správného nastavení se zkusíme na server nejdříve připojit přes ssh na uživatelský účet robot.

2.5. Vytvoření pracovních stanic

Abych se mohl připojit do domény (poskytované naším serverem Samba) pomocí stanice s operačním systémem Microsoft Windows XP Professional, musím nejprve vytvořit účty pracovním stanicím, ze kterých se budou uživatelé přihlašovat.

Jsou dvě možnosti jak to udělat:

2.5.1. Vytvoření pomocí nástroje PhpLDAPadmin

V aplikaci PhpLDAPadmin přidáme objekt třídy Samba 3 machine do organizační jednotky machines.

Machine Name	UID Number
winxp	30000

Tabulka 3: Pracovní stanice

Zdroj: vlastní

2.5.2. Smbldap-tools

V naší distribuci debian se nachází užitečná sada perl-skriptů.

Provedeme instalaci balíčku *smbldap-tools*.

```
apt-get install smbldap-tools
```

Zkopírujeme potřebné konfigurační soubory do adresáře /etc/smbldap-tools/ a rozbalím archiv smbldap.conf.gz.

```
mkdir /etc/smbldap-tools
cd /usr/share/smbldap-tools/
cp smbldap_bind.conf smbldap.conf.gz /etc/smbldaptools/
gunzip /etc/smbldaptools/smbldap.conf.gz
```

Upravíme konfigurační soubor /etc/smbldaptools/smbldap.conf:

```
SID="S-1-5-21-3131077580-1338128831-1697195685"
suffix="dc=debian"
usersdn="ou=users,${suffix}"
computersdn="ou=machines,${suffix}"
groupsdn="ou=groups,${suffix}"
sambaUnixIdPooldn="sambaDomainName=DEBIAN,${suffix}"
hash_encrypt="MD5"
```

Následuje nastavení souboru /etc/smbldap-tools/smbldap_bind.conf:

```
slaveDN="cn=admin,dc=debian"
slavePw="heslo"
masterDN="cn=admin,dc=debian"
masterPw="heslo"
```

Aby mohl skript automaticky určit id nově vzniklé pracovní stanice přidané pomocí skriptu, musíme objektu *sambaDomainName=DEBIAN* přidat třídu *sambaUnixIdPool*, z které zdědí atributy *gid* a *uid*. Gid v tomto případě nebude využito, ale z uid se vždy určí požadovaná hodnota.

Vyzkoušíme funkčnost skriptu.

```
./smbldap-useradd -w "winxp"
```

Přes PhpLDAPAdmina zjistíme, že se nám opravdu vytvořila nová pracovní stanice v organizační jednotce machines.

2.6. Nastavení pracovních stanic

Pracovní stanice musíme nastavit tak, aby „věděly“ na jaké adrese se mají dotazovat k autentifikaci uživatelů.

2.6.1. Microsoft Windows XP Professional

Nastavení pracovních stanic s operačním systémem Microsoft Windows XP Professional je velice jednoduché. Po spuštění pracovní stanice se přihlásíme na lokální účet administrátora. Klikneme na ikonku *Tento Počítač* pravým tlačítkem a dáme *Profiles/Vlastnosti*. Přejdeme na záložku *Computer Name/Název Počítače* a klikneme na tlačítko *Change/Změnit*.

1. V okně, které se nám otevřelo, nastavíme *Computer name/Název počítače* tak, aby souhlasil s účtem pracovní stanice vytvořené v našem OpenLDAP serveru. Dále vybereme selektor *Domain/Doména* a zadáme **DEBIAN**. Odsouhlasíme stiskem tlačítka OK.
2. Okno které se nám otevře po nás vyžaduje autentifikaci uživatele. Zadáme tedy uživatele, který už je vytvořen v OpenLDAP serveru, a příslušné heslo. Po kliknutí na OK se stanice pokusí přihlásit k Samba doméně.
3. Pokud vše proběhlo bez problému, systém nás uvítá v doméně DEBIAN a následně nás vyzve k restartu.
4. Po restartu je přihlašovací formulář rozšířen o listbox s naší doménou.

Podrobnější postup včetně obrázků je uveden v příloze A.

2.6.2. Unix

Nastavení pracovních stanic s operačním systémem Unix je o něco složitější. U každé stanice musíme nainstalovat balíček libnss-ldap (viz kapitola 2.3.2) a upravit konfigurační soubor /etc/nsswitch.conf.

Musíme nastavit adresu našeho OpenLDAP serveru. To provedeme přidáním následujícího řádku.

```
uri ldap://192.168.16.71
```

Dále musíme nastavit PAM pro připojení k LDAP (viz kapitola 2.3.3).

2.7. Migrace uživatelů

Pokud máme už vytvořené uživatele například v passwd, můžeme je jednoduše překopírovat do našeho OpenLDAP serveru.

2.7.1. Migrationtools

Sada perl skriptů pocházející od společnosti PADL Software Pty Ltd. Slouží pro zjednodušení importu (nejen) uživatelských účtů do databáze LDAP. Za pomoci skriptů si uložíme uživatele do formátu LDIF.
Tato sada skriptů je volně dostupná[11] spolu s podrobnou dokumentací.
V Debianu nainstalujeme balíček *migrationtools*.

```
apt-get install migrationtools
```

Vlastní export provedeme následujícími řádky.

```
export ETC_SHADOW=/etc/shadow
cd /usr/share/migrationtools
./migrate_base.pl > /tmp/base.ldif
./migrate_group.pl /etc/group /tmp/group.ldif
./migrate_hosts.pl /etc/hosts /tmp/hosts.ldif
./migrate_passwd.pl /etc/passwd /tmp/passwd.ldif
```

2.7.2. Ldap-utils

Tento balíček obsahuje důležité nástroje pro naši správu LDAP serveru jako ldapsearch, ldapadd a další.

Je volně ke stažení na stránce http://sourceforge.net/projects/ldaputils/.

Debian nám nabízí balíček *ldap-utils*.

```
apt-get install ldap-utils.
```

11 http://www.padl.com/OSS/MigrationTools.html

Nyní již máme soubory „stravitelné“ serverem LDAP. Záznamy přidáme pomocí následujících řádků:

```
ldapadd -D "cn=admin,dc=debian" -x -W -f /tmp/base.ldif
ldapadd -D "cn=admin,dc=debian" -x -W -f /tmp/group.ldif
ldapadd -D "cn=admin,dc=debian" -x -W -f /tmp/passwd.ldif
ldapadd -D "cn=admin,dc=debian" -x -W -f /tmp/hosts.ldif
```

2.8. Cestovní profily a domácí adresáře

Užitečnou záležitostí jsou cestovní profily. Po přihlášení uživatele z pracovní stanice se nám vytvoří na straně serveru profil nastavení uživatelského rozhraní systému. Zároveň se nám připojí domácí adresář uživatele, který se rovněž nachází na serveru. Při odhlášení se uloží změny opět na server a jsou k dispozici pro další přihlášení uživatele.

2.8.1. Samba

O cestovní profily a přidělení domácích adresářů pracovních stanic s operačním systémem Microsoft Windows se nám postará aplikace Samba.

Proto upravíme konfigurační soubor.

```
# formát v jakém se budou ukládat cestovní profily
logon path = \\%L\profiles\%U\%m
#nastavíme logický disk pro připojení domácího adresáře
logon drive = H:

[profiles]
# adresa kam se budou ukládat cestovní profily
path = /home/roaming
browsable = no
writable = yes
create mask = 0600
directory mask = 0700

[homes]
comment = Home
# adresa domácích adresářů
path = /home/%U/smbhome
read only = No
create mask = 0750
browseable = No
delete readonly = Yes
```

Nyní se můžeme přihlásit z pracovní stanice s operačním systémem Microsoft Windows XP Professional. Nastavení systému se nám uloží na straně serveru v nastaveném adresáři.

2.8.2. Pam_mkhomedir

„Jednou z možností, jak zajistit uživateli domácí adresář, je jeho vytvoření při prvním přihlášení do systému. Toto řešení je použitelné například když zakládáte uživatele zápisem do LDAP z nějakého webového rozhraní a nechcete řešit vytváření domácích adresářů. Pozor, adresář se vytvoří na každém stroji, kde neexistuje. pam_mkhomedir není zrovna dobrý nápad, pokud chcete centralizovat domácí adresáře uživatelů, ale hodí se třeba na serveru, kde chcete automaticky vyrábět domácí adresáře při prvním přihlášení uživatele. Při vytvoření se uživateli do domácího adresáře automaticky nakopíruje obsah /etc/skel/.

Použití pam_mkhomedir je docela jednoduché, stačí v souboru /etc/pam.d/common-session upravit říst session přibližně do podoby:

```
session required      pam_ldap.so
session required      pam_unix.so
session required      pam_mkhomedir.so skel=/etc/skel/ umask=077“ [9]
```

2.8.3. Pam_mount

„Pokud máte více počítačů propojených do sítě a chcete umožnit přístup k uživatelským datům z kteréhokoliv počítače, lze využít PAM modul pam_mount. pam_mount po ověření uživatele umí namountovat adresáře třeba ze sítě nebo z nějakého šifrovaného souboru. Je možné mountovat svazky pomocí SMB protokolu a podobně.“ [9]

2.8.4. Autofs

„Klasický unixový nástroj autofs (automounter) umožňuje automatické připojování svazků ze sítě. Po přihlášení uživatele se namountuje jeho domácí adresář přes NFS z nějakého centrálního fileserveru. Autofs má jednu velkou výhodu, umožňuje definovat konfiguraci v LDAP a tím i centralizovanou správu.

V distribuci Debian je autofs dostupný v samostatném balíčku. Instalace je jednoduchá.“ [9]

```
apt-get install autofs
```

„Konfigurace autofs se provádí v soubour /etc/auto.master, pravděpodobně tam budete mít zakomentované nastavení pro adresář /net, pokud tuto volbu odkomentujete a autofs restartujete, budete mít možnost ‚procházet‘ sítí NFS serverů. Procházení je docela příjemné a rychle se na něj zvyká. Prostě jen napíšete cd /net/server/ a vidíte co má server nasdílené. Jako server lze uvést buď IP adresu nebo přímo doménový název počítače.“ [9]

Auto.master přímo v LDAPu

Automounter umožňuje držet kompletní konfiguraci v LDAP. Pro aktivaci této funkce je třeba zapsat do /etc/nsswitch.conf

```
automounter: ldap
```

Samozřejmě je možné kombinovat ldap i soubory, ale musíte to do /etc/nsswitch.conf zapsat:

```
automounter: ldap files
```

Pokud řádek pro automounter neexistuje, vytvořte ho.

Obsah nahrazující původní /etc/auto.master v LDAP vypadá následovně:

```
dn: ou=auto.master,dc=debian
ou: auto.master
objectClass: top
objectClass: automountMap

dn: cn=/home,ou=auto.master,dc=debian
objectClass: automount
cn: /home
automountInformation: ldap://ldap.debian/ou=auto.indirect,dc=debian

dn: cn=/-,ou=auto.master,dc=debian
objectClass: automount
cn: /-
automountInformation: ldap://ldap.debian/ou=auto.direct,dc=debian
```

V naší konfiguraci direct mapy nepoužíváme, ale přesto zde uvedu příklad.

```
dn: ou=auto.direct,dc=debian
objectClass: top
```

```
objectClass: automountMap
ou: auto.direct

dn: cn=/usr/local,ou=auto.direct,dc=debian
objectClass: automount
cn: /usr/local
automountInformation:   file.debian:/usr/local/
```
[9]

2.9. Blokování uživatelských účtů

Při správě uživatelských účtů je důležité mít nad účty plnou kontrolu. Nejedná se tedy jen o jejich vytváření nebo upravování, ale především o možnost blokovat jednotlivé účty.

Pro každý operační systém budeme muset přidat do objektu uživatelského účtu atribut, který nám určí kdy účet expiruje. Pro administraci dat v LDAP využijeme aplikaci PhpLDAPadmin.

2.9.1. Pro stanice s operačním systémem Microsoft Windows

Přihlásíme se do webové aplikace PhpLDAPadmin a proklikáme se LDAP stromem přec *cn=debian, ou=users* až ke konkrétnímu uživateli. Když se podíváme na vlastnosti objektu, vidíme záložku *objectClass*, která nám určuje z jakých tříd objekt dědí atributy.

V tomto případě je pro nás důležitá třída *sambaSamAccount*. Musíme k objektu připojit atribut, z něhož Samba server pozná, kdy má účet expiraci. Klikneme tedy na odkaz *Add new attribute* a v následujícím formuláři vybereme atribut *sambaKickoffTime*. Tomu přidělíme čas v unixové podobě. Pro převod nám postačí stránka dostupná na adrese http://www.epochconverter.com/ nebo unixový příkaz date.

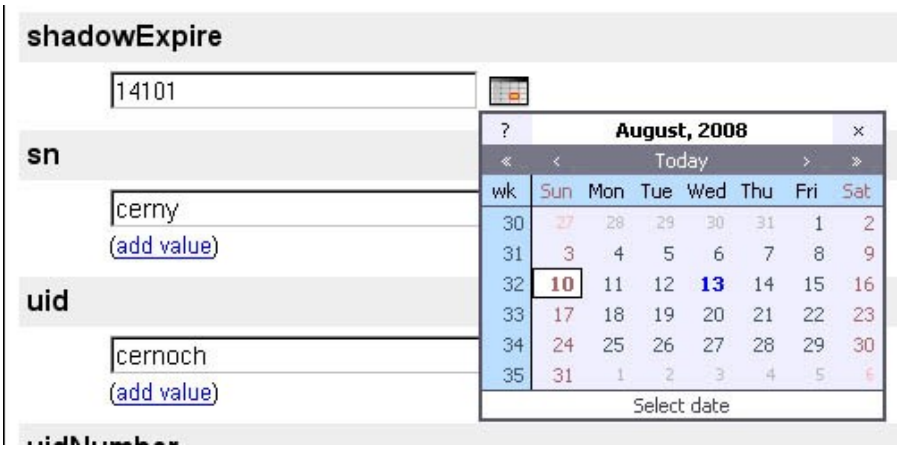
Obrázek 7: PhpLDAPadmin – Atribut expirace s unixovým formátem času

Zdroj: vlastní

2.9.2. Pro stanice s operačním systémem Unix

Pro blokování uživatelů na stanicích s operačním systémem Unix je situace velice podobná jako u stanic s Microsoft Windows.

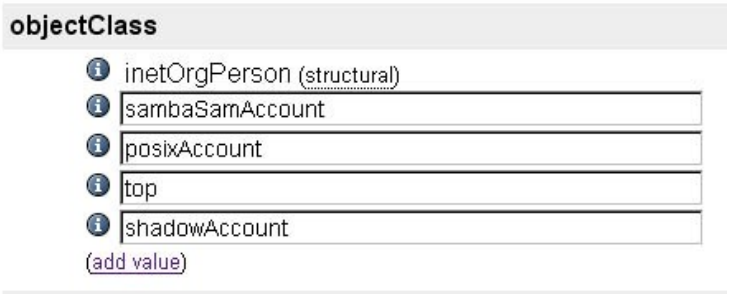
Opět si najedeme v PhpLDAPadminu na konkrétního uživatele. Nyní budeme potřebovat přidat objektu třídu *shadowAccount*, aby nám byl dostupný atribut *shadowExpire*. Pod záložkou *objectClass* klikneme na odkaz *add value* a vybereme zmíněnou třídu *shadowAccount*. Potom klikneme na odkaz *Add new attribute* a vybereme *shadowExpire*. Zadání hodnoty expirace v tomto atributu nám PhpLDAPadmin značně usnadňuje, protože se dá zadat pomocí grafického kalendáře.



Obrázek 8: PhpLDAPadmin – Nastavení expirace účtu pro Unix

Zdroj: vlastní

Díky podpoře schémat v OpenLDAP serveru pro nás není problém rozšířit objekt o prakticky jakýkoliv atribut. Díky kombinaci jednotlivých tříd můžeme vytvořit velice praktický objekt s potřebnými údaji jak pro Unix, tak pro operační systémy Microsoft Windows.



Obrázek 9: PhpLDAPadmin – Výsledné třídy objektu pro uživatele obou OS

Zdroj: vlastní

Závěr

Použití operačního systému Unix (distribuce Debian Etch) pro server s centrální databází uživatelských účtů, je velice výhodné díky nulovým nákladům, nízkým nárokům na hardwarové vybavení serveru a jeho variabilitě.

Centrální databáze uživatelů uložená v aplikaci OpenLDAP přináší zjednodušení práce pro administrátora i pro uživatele samotné. Administrátor může díky podpoře schémat vytvářet a kombinovat jednotlivé třídy objektů v závislosti na dalším využití dat. Uživatelé mají na všechny stanice s různými operačními systémy a ke všem službám v síti stejné přihlašovací údaje a administrátor spravuje jen jednu databázi uživatelů. Díky výborné aplikaci PhpLDAPadmin je správa záznamů LDAP opravdu jednoduchá, rychlá a velice efektivní.

Největší pozitivum řešení popsaného v této práci shledávám jednoznačně v možností propojení OpenLDAP serveru s širokým spektrem aplikací. Díky této možnosti ve spojení s dokonalým balíčkovacím systémem distribuce Debian zde bez výčitek můžeme mluvit o dokonale jednoduchém a efektivním řešení centrální správy uživatelských účtů.

Použitá literatura

[1] *Relační databáze* [online]. Wikipedia. 4. července 2008 [cit. 2008-8-3]. Dostupný z WWW: http://cs.wikipedia.org/wiki/Rela%C4%8Dn%C3%AD_datab%C3%A1ze

[2] *ACTIVE DIRECTORY* [online]. Wikipedia. 2. července 2008 [cit. 2008-8-1]. Dostupný z WWW: http://cs.wikipedia.org/wiki/Active_directory

[4] Kamil Kantar. *Soukromá síť – III* [online]. 21. září 2004 [cit. 2008-8-11]. Dostupný z WWW: http://www.abclinuxu.cz/clanky/site/soukroma-sit-iii

[5] *Samba (software)* [online]. Wikipedia. 2. července 2008 [cit. 2008-8-2]. Dostupný z WWW: http://cs.wikipedia.org/wiki/Samba_%28software%29

[6] *Details of package libnss-ldap in dapper* [online]. Wikipedia. [cit. 2008-8-1]. Dostupný z WWW: http://packages.ubuntu.com/dapper/libnss-ldap

[7] *Pluggable Authentication Modules* [online]. Wikipedia. 2. července 2008 [cit 2008-8-1]. Dostupný z WWW: http://cs.wikipedia.org/wiki/Pluggable_Authentication_Modules

[8] Zbyněk Hubínka. *Poznámky k LDAP* [online]. 30. srpna 2005 [cit. 2008-8-1]. Dostupný z WWW: http://www.root.cz/clanky/poznamky-k-ldap/

[9] Zdeněk Burda. *Využití LDAP v praxi.* [online]. 2005 [cit. 2008-8-12]. Dostupný z WWW: http://www.root.cz/clanky/poznamky-k-ldap/

[10] *LDAP.* Wikipedia [online]. 15. února 2008 [cit. 2008-8-1]. Dostupný z WWW: http://cs.wikipedia.org/wiki/LDAP

[11] Zdeněk Burda. *Využití LDAPu v praxi* [online]. 22. července 2007 [cit. 2008-8-1]. Dostupný z WWW: http://ldap.zdenda.com/

[12] Markus Amersdorfer. *Using OpenLDAP on Debian to serve System Users*

[online]. 10. května 2007 [cit. 2008-4-28]. Dostupný z WWW: http://home.subnet.at/~max/ldap/

[13] Nick Barkas. *LDAP Auth on Debian Sarge HOWTO* [online]. 17. října 2006 [cit. 2008-8-1]. Dostupný z WWW: http://moduli.net/sysadmin/sarge-ldap-auth-howto.html

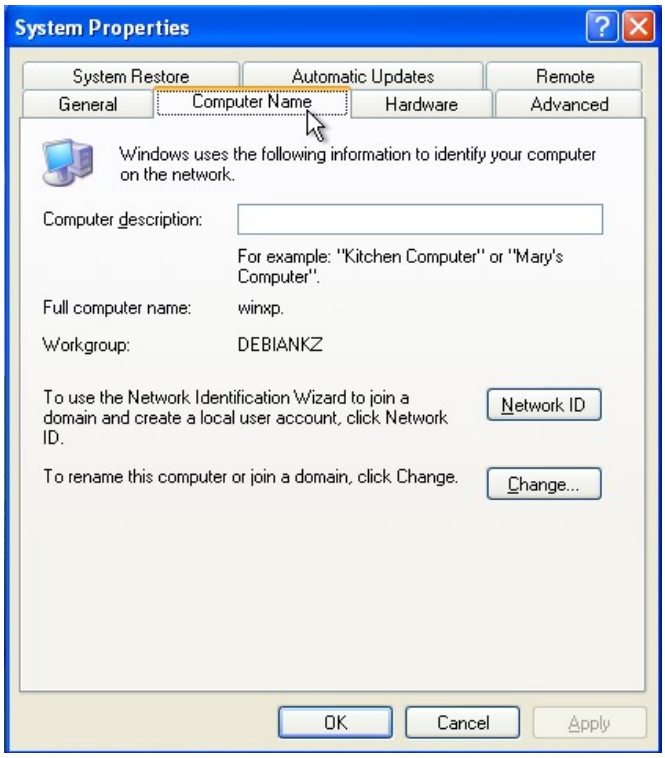
[14] Lukáš Malý, DiS. *LDAP v praxi s MUA* [online]. 2006 [cit. 2008-8-1]. Dostupný z WWW: http://ldap.smejdil.cz

[15] *Slapd* [online]. OpenLDAP. 19. února 2008 [cit. 2008-8-1]. Dostupný z WWW: http://www.openldap.org/software/man.cgi?query=slapd

[16] Mike. *Co je co IT > Základy v LDAP* [online]. 14. října 2004 [cit. 2008-8-1]. Dostupný z WWW: http://hps.mallat.cz/view.php?cisloclanku=2004101401

Příloha A: Nastavení pracovní stanice s operačním systémem Microsoft Windows XP Professional

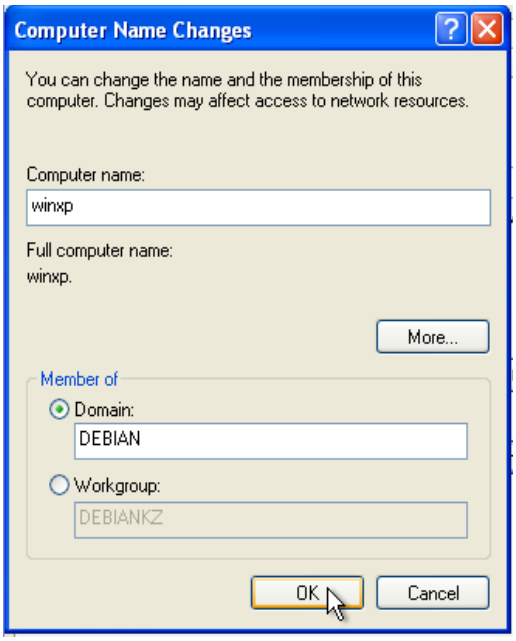
Nastavení pracovních stanic s operačním systémem Microsoft Windows XP Professional je velice jednoduché. Po spuštění pracovní stanice se přihlásíme na lokální účet administrátora. Klikneme na ikonku *Tento Počítač* pravým tlačítkem a dáme *Profiles/Vlastnosti*. Přejdeme na záložku *Computer Name/Název Počítače* a klikneme na tlačítko *Change/Změnit*.



Obrázek 10: Windows XP Pro – System Profiles

Zdroj: vlastní

1. V okně, které se nám otevřelo, nastavíme *Computer name/Název počítače* tak, aby souhlasil s účtem pracovní stanice vytvořené v našem OpenLDAP serveru. Dále vybereme selektor *Domain/Doména* a zadáme **DEBIAN**. Odsouhlasíme stiskem tlačítka OK.



Obrázek 11: Windows XP Pro – Computer Name Changes

Zdroj: vlastní

2. Okno které se nám otevře po nás vyžaduje autentifikaci uživatele. Zadáme tedy uživatele, který už je vytvořen v OpenLDAP serveru, a příslušné heslo. Po kliknutí na OK se stanice pokusí přihlásit k Samba doméně.

Obrázek 12: Windows XP Pro – Autentifikace

Zdroj: vlastní

3. Pokud vše proběhlo bez problému, systém nás uvítá v doméně DEBIAN a následně nás vyzve k restartu.

Obrázek 13: Windows XP Pro – Welcome to domain

Zdroj: vlastní

4. Po restartu je přihlašovací formulář rozšířen o listbox s naší doménou.

Příloha B: Konfigurační soubory

Kompletní konfigurační soubory jsou přiloženy na kompaktním disku u bakalářské práce.