Katedra informatiky
Přírodovědecká fakulta
Univerzita Palackého v Olomouci

BAKALÁŘSKÁ PRÁCE

Linux a doména a služby MS Windows?

Integrace Linuxového klienta do domény Windows Active Directory

2023

Kryštof Baksa

Vedoucí práce:
doc. Mgr. Jan Outrata, Ph.D.

Studijní program: Informační technologie, kombinovaná forma

Bibliografické údaje

Autor:	Kryštof Baksa
Název práce:	Linux a doména a služby MS Windows? (Integrace Linuxového klienta do domény Windows Active Directory)
Typ práce:	bakalářská práce
Pracoviště:	Katedra informatiky, Přírodovědecká fakulta, Univerzita Palackého v Olomouci
Rok obhajoby:	2023
Studijní program:	Informační technologie, kombinovaná forma
Vedoucí práce:	doc. Mgr. Jan Outrata, Ph.D.
Počet stran:	31
Přílohy:	elektronická data v úložišti katedry informatiky
Jazyk práce:	český

Bibliographic info

Author:	Kryštof Baksa
Title:	Linux and domain and services of MS Windows? (Integration of Linux client into Windows Active Directory)
Thesis type:	bachelor thesis
Department:	Department of Computer Science, Faculty of Science, Palacký University Olomouc
Year of defense:	2023
Study program:	Information Technologies, combined form
Supervisor:	doc. Mgr. Jan Outrata, Ph.D.
Page count:	31
Supplements:	electronic data in the storage of department of computer science
Thesis language:	Czech

Anotace

Tato bakalářská práce se zabývá integrací klientského počítače s operačním systémem Linux do domény Windows Active Directory. Součástí je porovnání a volba vhodné linuxové distribuce, postup pro připojení počítače k doméně pomocí služby SSSD a nastavení uživatelů a domovských adresářů včetně přístupových práv.

Synopsis

This thesis is researching integration of client computer with Linux OS into Windows Active Directory domain. This thesis includes comparison and choice of appropriate Linux distribution, guide for connecting computer to domain via service SSSD and configuration of users and home directories including permissions.

Klíčová slova: závěrečná práce; dokumentace; Linux; Active Directory; SSSD; Samba;

Keywords: thesis; documentation; Linux; Active Directory; SSSD; Samba;

Děkuji vedoucímu mé práce doc. Mgr. Janu Outratovi, Ph.D. a správci sítě Ivovi Fridrichovi.

Odevzdáním tohoto textu jeho autor/ka místopřísežně prohlašuje, že celou práci včetně příloh vypracoval/a samostatně a za použití pouze zdrojů citovaných v textu práce a uvedených v seznamu literatury.

Obsah

1 Úvod

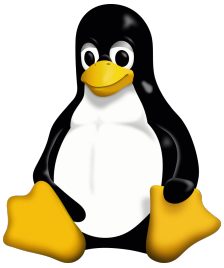
V českém pracovním a školním prostředí dominuje operační systém Windows. Mnoho programů bohužel podporuje pouze systém Windows a mnoho velkých organizací používá Windows Active Directory pro správu počítačů a uživatelských účtů. Licence k Windows ovšem mohou být nákladné a dochází k tzv. "vendor lock-in", kdy je organizace závislá na jednom dodavateli softwaru (v tomto případě Microsoft).

Dalším blížícím se problémem je končící podpora Windows 10 v roce 2025. Jeho následovník Windows 11 vyžaduje v počítači bezpečnostní čip TPM 2.0, který se začal do počítačů vkládat teprve v roce 2014. Všechny počítače vyrobené před tímto rokem a také mnoho levnějších počítačů vyrobených po tomto roce tento modul nemají a nelze tedy na ně Windows 11 oficiálně nainstalovat. Windows 11 také oficiálně nepodporuje některé nepříliš staré procesory, např. Athon 220GE z roku 2018. Po roce 2025 tyto počítače mohou být zranitelné a obsahovat bezpečnostní díry kvůli neudržovanému systému Windows 10, přestože jejich hardware funguje v pořádku.

Řešením, jak se vyhnout zbytečnému vyřazení těchto funkčních počítačů a nadále je bezpečně používat, je přechod na operační systém Linux.

1.1 Linux

Operační systém Linux je bezplatný, vysoce upravitelný a málo náročný na výkon. Starým počítačům, na kterých je Windows již příliš pomalý či zastaralý, lze vrátit život právě systémem Linux.



Linux má otevřené kódy a lze jej tak jakkoliv upravovat. Některé státy si dokonce vyvíjí své vlastní Linuxové distribuce uzpůsobené dle svých potřeb jako např. BOSS (Indie), MaX (Španělsko) či Pardus (Turecko).

1.2 Cíl práce

Cílem této práce je prozkoumat možnosti integrace Linuxu do domény Windows Active Directory a připravit ukázkový systém Linux připojený k doméně Windows Active Directory.

Cíle práce v bodech:

- Prozkoumat běžné Linuxové distribuce a posoudit vhodnost pro integraci
- Připojit Linuxový počítač do domény Active Directory
- Zajistit přihlašování uživatelů s doménovým jménem a heslem
- Automaticky připojovat SMB adresáře bez opětovného vyžadování jména a hesla
- Prozkoumat možnosti zpracování speciálních souborů (např. symbolické odkazy)
- Prozkoumat možnost zobrazení omezení zabrané kapacity (kvóta)
- Umožnit změnu hesla doménového účtu z Linuxového počítače
- Automatizace integrace Linuxového klienta do domény Active Directory

2 Výběr Linuxové distribuce

Narozdíl od Windows má Linux mnoho tzv. distribucí. Distribuce mohou být zaměřené na různé použití. Například systém SystemRescue je uzpůsoben pro diagnostiku a opravu počítačů, systém Kali Linux je uzpůsoben pro digitální forenziku a testování bezpečnosti sítě či systém Edubuntu, který je uzpůsoben pro výuku bez přístupu k internetu (např. v rozvojových zemích).

Dostupný software a délka podpory se u každé distribuce může lišit. Jelikož se jedná o klientský počítač, distribuce musí obsahovat desktopové prostředí a software potřebný k integraci s doménou.

Jedná se o následující software:

- System Security Services Daemon (SSSD)
- Samba
- GVfs

Důležitými parametry jsou stabilita a délka podpory. Při hromadném nasazení chceme, aby systém bez problému fungoval a dostával po co nejdelší dobu bezpečnostní aktualizace.

2.1 Ubuntu

Ubuntu je distribuce vyvíjená společností Canonical. Jedná se o nejpopulárnější Linuxovou distribuci. LTS verze Ubuntu mají standardní podporu po vydání 5 let, v rámci komerční podpory ESM (zdarma pro osobní použití) je možné prodloužit podporu o dalších 5 let.

Tato distribuce je tedy velmi vhodná pro hromadné nasazení, jelikož po instalaci mohou klientské počítače dostávat bezpečnostní aktualizace až 10 let.

2.2 Debian

Debian je distribuce vyvíjená komunitou Debian Project. Standardní doba podpory u jednotlivé verze po vydání jsou 3 roky, v rámci dlouhodobé podpory LTS 5 let a v rámci komerční podpory ELTS může dosáhnout až 7 let.

Debian v základní instalaci obsahuje pouze plně svobodný software, i z jádra Linux jsou odstraněny veškeré nesvobodné moduly a ovladače. Nesvobodný software lze získat z repozitářů contrib a non-free. Absence nesvobodného softwaru může být nevýhoda oproti jiným distribucím, jelikož některé důležité součásti počítačů, zejména v noteboocích, nemusí fungovat bez nesvobodných ovladačů či firmwaru, např. Wi-Fi, GPU, reproduktory atd. a je potřebná dodatečná instalace. Jiné distribuce, které již v základu obsahují nesvobodné ovladače z mé zkušenosti většinou fungují bez problému a není potřebná žádná dodatečná instalace. Představenstvo Debianu rozhodlo, že instalátory budoucích verzí budou obsahovat nesvobodný firmware, tudíž by instalace v budoucnu měla být jednodušší. Nesvobodné ovladače ovšem nadále nebudou základní součástí Debianu. [1]

2.3 Fedora

Fedora je distribuce vyvíjená společností Redhat. Podpora jednotlivých verzí je pouze jeden rok. Upgrade na novější verze je možný, tento proces by se ovšem neměl automatizovat, jelikož může rozbít funkčnost systému kvůli zastaralým konfiguracím nebo nekompatibilitě. Pro hromadné nasazení klientských počítačů tedy tato distribuce příliš vhodná není kvůli nutnosti častých upgradů.

2.4 Archlinux

Archlinux je distribuce vyvíjená komunitou Archlinux. Archlinux používá takzvaný "rolling-release"model vydání. Verze jsou odvozeny dle data vydání a podpora verze automaticky zaniká vydáním novější verze. Nová verze je vydávána každý měsíc.

Každé vydání obsahuje nové verze programů, které mohou být náhle nekompatibilní s původní konfigurací a tím rozbít funkčnost systému. Tato verze tedy pro hromadné nasazení klientských vhodná není.

3 Adresářová služba

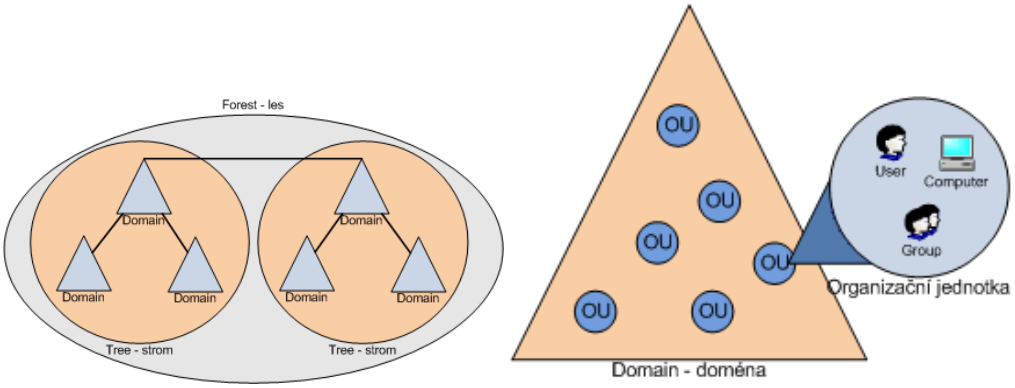
Adresářová služba je aplikace či skupina aplikací, které ukládají a organizují informace o uživatelích a zdrojích v počítačové síti. Adresářová služba také funguje jako centrální autentizační autorita, která umožňuje autentizaci zdrojů (uživatelů, služeb, počítačů). [2]

Použití adresářové služby je nezbytné ve větších organizacích. Umožňuje přihlašování jednotným uživatelským účtem ke všem počítačům připojeným do domény. Další funkcí je hromadná správa počítačů v doméně, např. hromadná instalace programů či úprava nastavení.

3.1 Windows Active Directory

Active Directory (AD) je adresářová služba od Microsoftu. Active Directory Domain Controller (DC či doménový řadič nebo pouze řadič) je server na kterém běží Active Directory Domain Services (AD DS). AD DS poskytuje distribuovanou databázi, která v hierarchické struktuře obsahuje síťové objekty (jako je uživatel, počítač, skupina). Zajišťuje také autentizaci a autorizaci uživatelů a počítačů v síti. Využívá se LDAP protokol, rozšířený Kerberos verze 5 a DNS (Domain Name System).[3]

Logická struktura Active Directory (organizace zdrojů) je tvořena pomocí lesa, stromů, domén a OU. Na vrcholu struktury je les - Forest. Ten může obsahovat jeden nebo více stromů - Trees. Strom je tvořen jednou či více doménami - domains. Uvnitř domén již máme jednotlivé organizační jednotky - OU (Organizational Unit). Uvnitř OU se nachází jednotlivé objekty (počítače, uživatelé, tiskárny, apod.).[4]



[4]

Active Directory je nejrozšířenější adresářová služba v organizacích, kde se používá systém Windows. Integrace systému Windows s doménou je rychlá a jednoduchá. Kromě správy uživatelů umožňuje i rozháhlou správu počítačů pomocí tzv. Skupinových zásad. Lze např. odepřít uživatelům přístup k některým programům, nastavit mazání nepoužívaných uživatelských profilů či nastavit cestovní profily. Software na doménových počítačích lze hromadně instalovat či aktualizovat pomocí balíčků MSI.

3.2 Samba

Samba je open-source reimplementace protokolu SMB původně vyvíjená Andrewem Tridgellem. Může sloužit jako souborový a tiskový server pro počítače Windows nebo se naopak připojovat k SMB serverům. [5] Umožňuje i integraci do domény Windows pomocí služby Winbind. Od verze 4.0 může sloužit jako doménový řadič Active Directory.

3.3 FreeIPA

FreeIPA je open-source verze produktu Red Hat Directory Server, který slouží jako adresářová služba pro systémy Redhat. Zajišťuje podobné služby jako Active Directory. Skládá se z programů jako např. 389 Directory Server, MIT Kerberos, NTP či DNS.

4 Připojení k doméně Windows Active Directory

Tato kapitola popisuje postup pro připojení Linuxového klienta k doméně Windows Active Directory. Pro připojení k doméně se v Linuxu lze použít buď System Security Services Daemon (SSSD) nebo Samba Winbind. Zatímco SSSD podporuje kromě Active Directory i FreeIPA a LDAP, Samba Winbind umí pracovat pouze s Active Directory. V této práci se používá SSSD.

4.1 SSSD

SSSD je sada programů využívána k integraci Linuxového systému do doménových a přihlašovacích služeb. SSSD byl původně vyvíjen open-source projektem FreeIPA, postupem času získal dostatek funkcí na to, aby mohl nahradit Winbind. SSSD projekt je sponzorován společností Redhat. [6]

4.2 Postup připojení

Je nutné nainstalovat software realmd.

Instalace v Ubuntu/Debian:

```
1 sudo apt install realmd
```

Instalace v Fedora:

```
1 sudo dnf install realmd
```

Nyní dojde k samotnému připojení do domény pomocí příkazu realm. Je nutné mít k dispozici přístup správce na Linuxu a doménový účet oprávněný k připojování počítačů do domény.

Připojení k doméně přes SSSD:

```
1 sudo realm join -U domenovy_uzivatel domena.lan
```

Po zadání tohoto příkazu systém vyzve k zadání hesla k doménovému účtu a hesla k účtu správce, doinstaluje potřebné balíčky a poté bude počítač připojen k doméně.

Pokud se připojení nepodaří kvůli chybě "Insufficient permissions to join the domain", je potřeba zadat `rdns = false` do souboru `/etc/krb5.conf`[7].

Systém Debian nevytvoří konfigurační soubor `/etc/krb5.conf`. Tento soubor je potřeba ručně vytvořit:

```
1 [libdefaults]
2 udp_preference_limit = 0
3 rdns = false
```

Po připojení je ještě potřeba ještě udělat nějaké úpravy. V základní konfiguraci se používají tzv. plně kvalifikované názvy. To znamená, že názvy doménových uživatelů se ukládají ve formátu uzivatel@domena.local a v tomto formátu se musí i přihlašovat. Pro zjednodušení a podobné používání jako v systému Windows lze názvy zkrátit, tedy názvy doménových uživatelů se ukládají ve formátu uzivatel.

Plně kvalifikovaný název	**Zkrácený název**
uzivatel@domena.local	uzivatel

Je důležité mít na vědomí, že zkrácení názvů lze provést pouze pokud je Linux připojen k jedné doméně. Při připojení více domén by mohlo docházet ke konfliktu jmen a zde je nutné názvy dodatečně rozlišovat pomocí přípony @domena.local.

Plně kvalifikovaný název	**Zkrácený název**
uzivatel@domena1.local	uzivatel
uzivatel@domena2.local	uzivatel

Pokud je to možné, je doporučeno vypnout používání plně kvalifikovaných názvů, protože je pro uživatele mnohem jednodušší používat jen přihlašovací jméno místo celého názvu.

Pro vypnutí používání plně kvalifikovaných názvů se nastaví hodnota `use_fully_qualified_names = False` v konfiguračním souboru `/etc/sssd/sssd.conf`

Pokud se vyskytují problémy s připojováním SMB adresářů, lze vypnout cachování hesel doménových účtů nastavením hodnoty `cache_credentials = False`.

V Ubuntu/Debian je také potřeba zapnout vytváření domovských adresářů u nových uživatelů následujícím příkazem:

```
1 sudo pam-auth-update --enable mkhomedir
```

Když SSSD nedokáže přečíst některé skupinové zásady v doméně, v základním nastavení odepře přihlašování doménovým uživatelům.
Pro povolení přihlašování se nastaví hodnota `ad_gpo_ignore_unreadable = True` v souboru `/etc/sssd/sssd.conf`

Nyní se lze přihlašovat doménovými účty na Linuxového klienta.

5 Sdílené SMB adresáře

Tato kapitola popisuje postup pro připojení sdílených SMB adresářů pro doménové uživatele a správné nastavení práv pomocí softwaru Samba. Cílem je umožnit uživatelům přístup k SMB adresářům co nejblíže podobný přístupu v systému Windows. Je nežádoucí, aby musel uživatel po přihlášení znovu zadávat své přihlašovací údaje pro připojení k SMB adresáři, proto využijeme přihlašovací metodu Kerberos.

5.1 Kerberos V5

Kerberos V5 (Kerberos Network Authentication Service (V5)) je nejpoužívanější autentizační metoda pro Active Directory. Definuje autentizační proces, který poskytuje metody pro ověření identity, například pro pracovní stanici či uživatele. Pro autentizaci klienti používají Kerberos tickets (lístky), které reprezentují síťové credentials (pověření) pro klienta. Klient získá ticket od KDC (Kerberos Key Distribution Center) a ukazuje tento lístek, když se vytváří síťové spojení. Kerberos představuje identitu klienta pomocí jména domény, uživatelského jména a hesla.[8]

5.2 mount.cifs

Nejprve jsem se snažil připojování adresářů implementovat pomocí mount.cifs. Tento způsob má ovšem několik problémů. Mountovat lze pouze s root oprávněním, které rozhodně nechceme běžným uživatelům přidělovat. Tento problém lze sice vyřešit definováním SMB adresářů do `/etc/fstab` s parametrem user, který dovolí adresáře mountovat bez root oprávnění, zde jsem ovšem narazil na to, že nelze do souboru `/etc/fstab` vkládat proměnné a proto se adresáře mohou připojovat jen do jedné společné složky.

Společná složka by nevadila u počítačů pouze s jedním uživatelem, pokud ovšem počítač používá více uživatelů, musíme implementovat i odhlašovací skript, který by se pokaždé spustil při odhlášení či přepnutí uživatele což je ovšem zbytečně komplikované a může uživatelům způsobit ztrátu dat.

Například když by měl uživatel rozpracovaný dokument v SMB adresáři, uzamknul počítač a k počítači se přihlásil jiný uživatel, systém by z důvodu bezpečnosti musel SMB adresář odpojit a znovu připojit přes údaje současného uživatele, dokument minulého uživatele by mohl být ztracen.

5.3 GVfs

Vhodnějším způsobem je použití GVfs. GVfs (GNOME virtual file system) je virtuální souborový systém, který pracuje s knihovnou GIO. [9] GVfs nevyžaduje root oprávnění a připojuje SMB adresáře do soukromé složky uživatele v `/run/user`, nehrozí tedy žádná kolize s ostatními uživateli.

5.4 Instalace softwaru

Nejprve musíme nainstalovat potřebný software:

Instalace v Ubuntu a Debian:

```
1 sudo apt install samba gvfs
```

Instalace v Fedora:

```
1 sudo dnf install samba gvfs
```

Následně lze připojovat SMB adresáře pomocí tohoto příkazu.

```
1 gio mount smb://smb_server/adresar
```

Po zadání příkazu GVfs zkontroluje, zdali lze pro přihlášení použít Kerberos ticket, v opačném případě vyzve k zadání hesla.

Po úspěšném připojení se SMB adresář připojí do složky `/run/user/uid/gvfs/` a automaticky se vytvoří odkaz v souborovém prohlížeči.

5.5 Přihlašovací skript

Pro automatické připojení SMB adresářů je nutné vytvořit přihlašovací skript. Zde přikládám skript použitý v mé práci. Tento přihlašovací skript přidáme do složky: `/opt/`

5.5.1 variables.sh

```
1  #!/bin/bash
2  # Doménový server
3  ADSERVER="kourilkova8.lan"
4
5  # Název administrátorského účtu, přes který se bude připojovat počí
       tač do domény, k zadání hesla budete vyzváni po spuštění skriptu
6  ADMIN="admin"
7
8  # Adresa SMB serveru
9  SMBSERVER="bakskr00-inf.kourilkova8.lan"
10
11 # NEMĚNIT: Pro případ, že se používají plné názvy včetně domény, je
       nutné odebrat název @prfad.upol.cz za jménem.
12 # Použijte tuto proměnnou pro určení cesty k osobnímu adresáři.
13 USERNAME=${USER%@*}
14
15 # Primární doménová skupina, ke cd které se budou automaticky př
       ipojovat SMB adresáře
16 SMBGROUP1="_g_ucitele"
17
18 # Seznam připojovaných SMB adresářů k primární skupině
19 SMBSHARES1=(
20   "disk-O"
21   "disk-U"
22   "Dokumenty-Ucitele/$USERNAME"
23 )
24
25 # Sekundární doménová skupina, ke které se budou automaticky př
       ipojovat SMB adresáře
26 SMBGROUP2="_g_studenti"
27
28 # Seznam připojovaných SMB adresářů k sekundární skupině
29 SMBSHARES2=(
30   "disk-O"
31   "Dokumenty-Studenti/$USERNAME"
32 )
```

5.5.2 mount.sh

```
1  #!/bin/bash
2
3  #Načtení proměnných z variables.sh
4  source /opt/variables.sh
5
6  # SSSD automaticky překládá doménové skupiny na unixové, takže je mů
       žeme ve skriptu jednoduše používat pomocí příkazu groups.
7  if [ ! -z "$(groups $USER | grep $SMBGROUP1)" ]
8  then
9    # Připojit SMB adresáře z array $SMBSHARES1
10   for i in "${SMBSHARES1[@]}"
11   do
12     # V Ubuntu/Debian se momentálně vyskytuje chyba, která způsobuje,
           že gvfs nepoužívá Kerberos ticket pro připojení SMB adresáře
           bez hesla.
13     # Lze opravit restartováním gvfs démona po přihlášení dokud
          nedojde k úspěšnému přihlášení.
14     while [[ ! -z $(timeout 10 gio mount smb://$SMBSERVER/$i | grep '
          equired\|ověření') ]]
15     do
16       systemctl --user restart gvfs-daemon.service
17     done
18   done
19 fi
```

```
# SSSD automaticky překládá doménové skupiny na unixové, takže je mů
    žeme ve skriptu jednoduše používat pomocí příkazu groups.
if [ ! -z "$(groups $USER | grep $SMBGROUP2)" ]
then
  # Připojit SMB adresáře z array $SMBSHARES2
  for i in "${SMBSHARES2[@]}"
  do
    # Momentálně se vyskytuje chyba, která způsobuje, že gvfs nepouží
       vá Kerberos ticket pro připojení SMB adresáře bez hesla.
    # Lze opravit restartováním gvfs démona po přihlášení dokud
       nedojde k úspěšnému přihlášení.
    while [[ ! -z $(timeout 10 gio mount smb://$SMBSERVER/$i | grep '
       equired\|ověření') ]]
    do
      systemctl --user restart gvfs-daemon.service
    done
  done
fi
```

Tento skript je nutné spouštět na pozadí, aby nedošlo k zaseknutí systému během přihlašování, proto je umístěn ve složce `/opt/` a do složky `/etc/profiles.d/` se umístí následující skript:

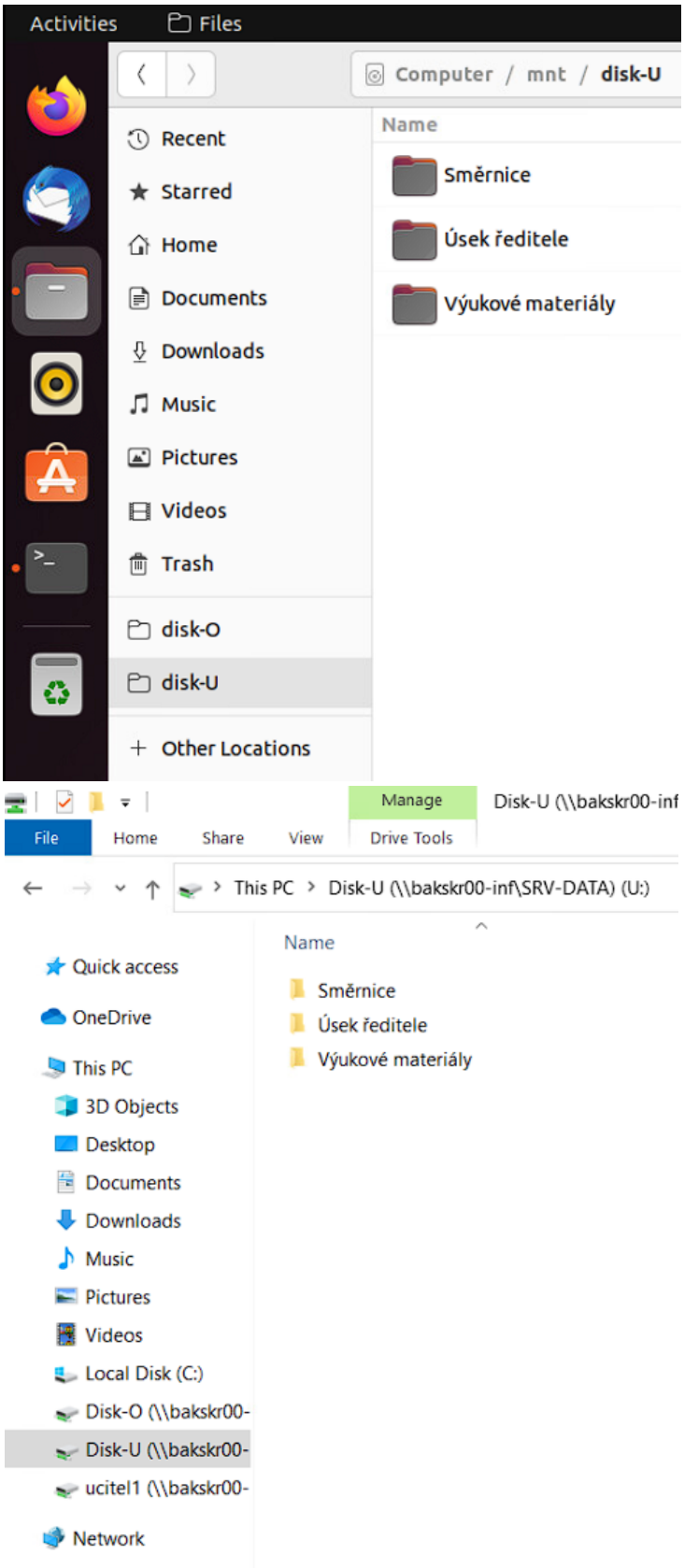
```
#!/bin/bash
/opt/mount.sh &
```

Nyní mohou uživatelé přistupovat k SMB adresářům.

5.6 Vzhled

Na následujícím obrázku můžete vidět, jak přístup na SMB adresáře vypadá ve Windows a v Linuxu.

Postup přístupu na disky je velice podobný - uživatel otevře průzkumníka souborů a v levém panelu najde odkaz na SMB adresáře. Uživatel si tedy rychle zvykne na přístup k SMB adresářům v Linuxu.


Activities
Files
Computer / mnt / disk-U
Recent
Starred
Home
Documents
Downloads
Music
Pictures
Videos
Trash
disk-O
disk-U
Other Locations
Name
Směrnice
Úsek ředitele
Výukové materiály
Manage
Disk-U (\\bakskr00-inf
File
Home
Share
View
Drive Tools
This PC
Disk-U (\\bakskr00-inf\SRV-DATA) (U:)
Quick access
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Disk-O (\\bakskr00-
Disk-U (\\bakskr00-
ucitel1 (\\bakskr00-
Network

5.7 Poznámky k připojování

5.7.1 Chyba v Ubuntu

Kvůli spouštění GVFS démona v nesprávný čas momentálně GVFS neumí správně používat Kerberos ticket po spuštění.[10] Po restartování démona po načtení plochy lze již připojovat SMB adresáře bez problému.

Lze předpokládat, že tato chyba bude v budoucnu opravena. Prozatím jsem do skriptu přidal smyčku, která automaticky restartuje démona dokud nedojde k úspěšnému připojení SMB adresáře.

5.7.2 Osobní adresáře žáků

V mém zaměstnání jsou osobní adresáře studentů rozděleny dle tříd, aby k nim mohli učitelé rychleji přistupovat. Systém Windows cestu k osobnímu adresáři jednoduše získá pomocí atributu `homeDirectory`.

Bohužel jsem nenašel žádný jednoduchý způsob, jak získávat atributy přes SSSD. Můžeme ovšem číst skupiny uživatele pomocí příkazu `groups`, proto jsem vytvořil pro každou třídu skupinu s prefixem `trida_`. Poté jsem již jednoduše získal název třídy, do které student patří a dle toho vytvořil odkaz v průzkumníku souborů.

Osobní adresáře všech studentů na katedře jsou umístěny v jedné složce, tudíž k zjištění cesty adresáře stačí znát jen uživatelské jméno.

5.8 Odkazy

Odkazy ve Windows mají jiný formát než v Linuxu a tudíž jsou nekompatibilní. Linuxový klient nemůže vytvářet odkazy v SMB adresáři.

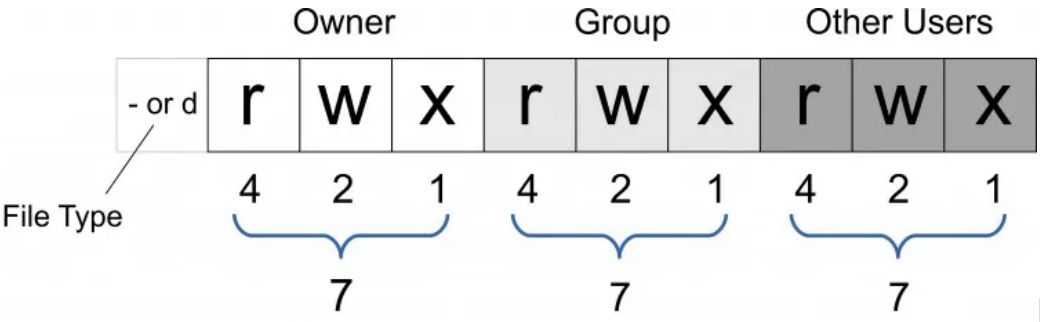
Z Windows odkazů (soubory .lnk) je ovšem možné získat cestu k odkazovanému souboru či složce pomocí skriptu. Cesta se ovšem musí pro použití v Linuxu upravit.

```
1 #!/bin/bash
2
3 # Získání řetězců textu ze souboru .lnk | filtrování řetezce s
    adresou serveru | Smazání adresy serveru | Nahrazení zpětných
    lomítek běžnými lomítky | Malá písmena u kořenového adresáře,
    Linux u cest rozlišuje malá a velká písmena
4 path=$(strings $1 | grep 'dragon.inf.upol.cz' | sed 's/\\\\dragon.
    inf.upol.cz\\//g' | sed 's/\\/\//g' | sed 's/Data-Students/data-
    students/g')
5
6 echo /run/user/$UID/gvfs/smb-share:server=dragon.inf.upol.cz,share=
    $path
7 nautilus /run/user/$UID/gvfs/smb-share:server=dragon.inf.upol.cz,
    share=$path
```

5.9 Oprávnění

5.9.1 Linux

Linux používá POSIX systém oprávnění. Uživatelé jsou rozděleni do tří kategorií - vlastník, skupina a ostatní. Každá kategorie může mít tři základní druhy oprávnění - čtení(číslo 4), zápis(číslo 2) a spouštění(číslo 1). Ze součtu čísel oprávnění lze odvodit veškerá oprávnění.



[11]

5.9.2 Windows

Windows používá Access-Control List (ACL) oprávnění. Soubory či složky mají vlastní seznam oprávnění, který přiděluje či odepírá uživatelům a skupinám různé druhy oprávnění, např. čtení, zápis, spouštění atd.

5.9.3 Kompatibilita

Linuxový klient rozpozná základní druhy oprávnění v SMB adresářích. Při pokusu o přístup do složky bez oprávnění oznámí chybu o odepřeném přístupu. Při otevření souboru bez oprávnění k zápisu oznámí uživateli, že je soubor nezapisovatelný.

Změnu oprávnění ovšem SMB klient neumožňuje, tento krok se musí učinit z Windows klienta či SMB serveru.

5.10 Kancelářský software

5.10.1 Microsoft Office

Microsoft Office v základním nastavení používá formát Office Open XML (.docx, .xlsx, .pptx). Tento formát se dělí na 2 druhy - Transitional(přechodný) a Strict(striktní).

Strict formát je plně otevřený a v souladu se standardem ISO/IEC 29500.

MS Office ovšem v základním nastavení používá Transitional OOXML, který není plně otevřený a 100% kompatibilní s jiným kancelářským softwarem.

Novější MS Office verze podporují i formáty ODF.

	Office 2003	Office 2007	Office 2010	The New Office
Binary format (.doc, .xls, .ppt)	Open, Edit, Save	Open, Edit, Save	Open, Edit, Save	Open, Edit, Save
Transitional Open XML	Open, Edit, Save	Open, Edit, Save	Open, Edit, Save	Open, Edit, Save
Strict Open XML			Open, Edit	Open, Edit, Save
ODF 1.1		Open, Edit, Save	Open, Edit, Save	Open, Edit
ODF 1.2				Open, Edit, Save
PDF		Save	Save	Open, "Edit", Save

[12]

5.10.2 LibreOffice

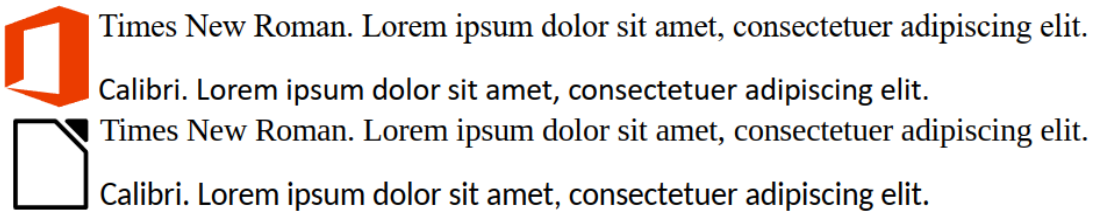
LibreOffice je nejběžnější open-source kancelářský software v Linuxu. Používá v základním nastavení Open Document format (.odt, .ods, .odp). Formát Strict OOXML je také plně podporován.

Transitional OOXML sice LibreOffice také umí zpracovat, během práce s dokumentem v tomto formátu se ovšem mohou vyskytovat chyby, jelikož se nejedná o plně otevřený formát a vývojáři LibreOffice se museli uchýlit k reverse-engineeringu

5.10.3 Kompatibilita mezi MS Office a LibreOffice

Pro plnou kompatibilitu mezi MS Office a LibreOffice je nutné ukládat soubory ve formátu Strict OOXML nebo Open Document Format.

Je také nutné dávat pozor na používané fonty. MS Word používá ve výchozím nastavení font Calibri, který ovšem není svobodný. Při otevření dokumentu v LibreOffice se font nahradí náhradním, který dodržuje rozměry původního fontu, ovšem trochu se liší.



Pokud chcete někomu sdílet dokument jen pro čtení či výtisk, je vždy nejvhodnější dokument exportovat do formátu PDF. Tak jak vidí PDF soubor odesílatel, tak ho uvidí i adresát.

6 Změna hesla

Doménový uživatel může změnit heslo stejným způsobem jako lokální uživatel, tedy příkazem passwd.

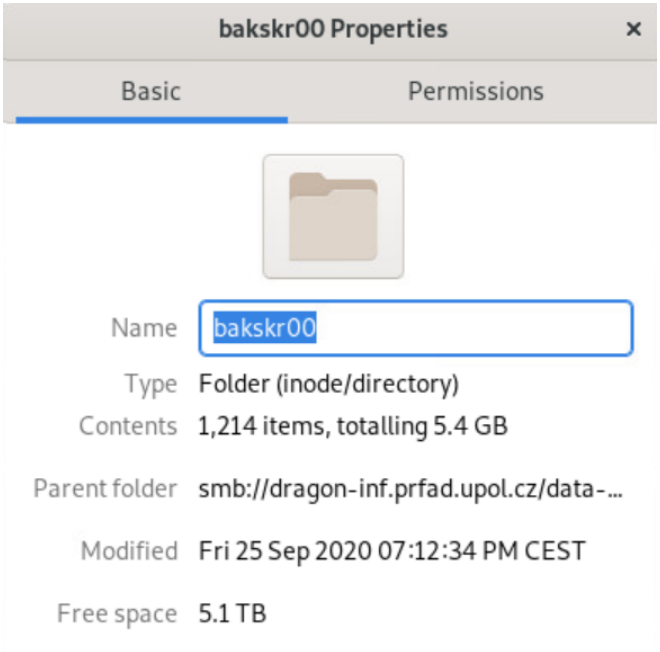
Po zadání příkazu program vyzve uživatele k zadání starého hesla, nového hesla a informuje o úspěšné změně.

```
1 passwd
2 Stávající heslo:
3 stareheslo
4 Nové heslo:
5 noveheslo
6 Zadejte znovu nové heslo:
7 noveheslo
8 passwd: Heslo úspěšně aktualizováno.
```

7 Disková kvóta

Bohužel jsem nenašel způsob, jak zobrazit diskovou kvótu osobního adresáře.

Lze zobrazit celkovou kapacitu SMB adresáře, a to i přímo pomocí souborového průzkumníka.



Závěr

Výsledkem této práce je automatická integrace Linuxového počítače do domény Active Directory pomocí bash skriptů. Skripty lze jednoduše přizpůsobit pro různá prostředí pomocí proměnných uložených v odděleném skriptu variables.sh. Skripty podporují systémy Debian, Ubuntu a Fedora. Skripty automaticky připojí počítač do domény a připraví přihlašovací skript pro připojování SMB adresářů. Po úspěšném provedení skriptu install.sh je počítač připraven pro použití.

Linuxový klient v doméně Active Directory může sloužit jako alternativa k Windows pro běžné uživatele. Přihlašovací stránku i uživatelské prostředí lze upravit tak, aby bylo velmi podobné systému Windows. SMB adresáře lze automaticky připojovat a provádět v nich běžné operace.

Problém může nastat, když je potřeba provozovat programy, které nemají k dispozici Linuxovou verzi. Tyto programy lze spouštět přes rozhraní WINE či virtualizaci Windowsu. Při provozu programu přes WINE se ovšem mohou vyskytovat chyby a virtualizace zvyšuje komplikovanost a zátěž na systém.

Ideální je používání webových aplikací místo lokálních, pokud je to možné. V Linuxu mohu uživatelé používat webové aplikace přes prohlížeč Firefox, případně Chromium. Data aplikace jsou ukládány na serveru, tudíž není ani potřeba řešit sdílení souborů mezi Windows a Linuxem. Např. webová verze Microsoft Office 365 funguje bez problému na Linuxu a open-source alternativa Collabora CODE funguje bez problému na Windows.

Problematická je také kompatibilita dokumentů mezi různým kancelářským softwarem, jelikož je většina MS Office dokumentů vytvořena v nesvobodném Transitional OOXML formátu. Řešením je používání webových aplikací zmíněných v předchozím odstavci.

Conclusions

The outcome of this thesis is an automatic integrations of a Linux computer to Active Directory domain via bash scripts. Scripts can be easily adapter for various environments via variables saved in separated script variables.sh. Scripts support system Debian, Ubuntu and Fedora. Scripts automatically connect the computer to the domain and prepare login script for connecting SMB shares. After successful execution of install.sh script, the computer is ready for deployment.

A Linux client in Active Directory can serve as an alternative for Windows for common users. Login screen and user environment can be modified to imitate Windows environment as close as possible. SMB shares can be automatically mounted and common operations can be done in them.

We can encounter some problems, when we need to run programs that do not support Linux. These programs can be run via WINE interface or in Windows VM. However we could encounter some problems when running programs via WINE and virtualization increases complexity and performance requirements.

It's ideal to use web applications instead of local ones, if it is possible. In Linux, users can use web applications via browser Firefox, eventually Chromium. Data of the application are saved on the server, so it's not necessary to care about file sharing between Windows and Linux. For example, the web version of Microsoft Office 365 works without problems on Linux and open-source alternative Collabora CODE works without problems on Windows.

Compatibility of document formats between various Office software is problematic as well, because most MS Office documents are created in non-free Transitional OOXML format. It can be resolved by using web applications mentioned in previous paragraph.

A Obsah elektronických dat

text/
: Adresář s textem práce ve formátu PDF, vytvořený s použitím závazného stylu KI PřF UP v Olomouci pro závěrečné práce, včetně všech (textových) příloh, a všechny soubory potřebné pro bezproblémové vytvoření PDF dokumentu textu (případně v ZIP archivu), tj. zdrojový text textu a příloh, vložené obrázky, apod.

README.txt
: Textový soubor s informacemi o opakovatelném způsobu připojení Linuxového klienta do domény.

skripty/
: Adresář se skripty, který je nutné zkopírovat do počítače, který se má připojit do domény. Instalační skript se následně spouští z tohoto adresáře.

skripty/variables.sh
: Soubor s proměnnými, které je potřeba nastavit. Proměnné jsou nastaveny pro testovací doménu kourilkova8.lan.

skripty/install.sh
: Instalační skript po jehož úspěšném provedení bude počítač připojen do domény. Také se nastaví přihlašovací skript pro automatické připojování SMB adresářů. Skript je nutné spouštět s oprávněním root.

skripty/krb5.conf
: Konfigurační soubor potřebný pro úspěšné připojení počítače do domény. Je umístěn do /etc/krb5.conf

skripty/mount.sh
: Skript pro automatické připojení SMB adresářů používaných studenty na katedře informatiky PřF. Tento skript se musí spouštět na pozadí skriptem mountbg.sh.

skripty/mountbg.sh
: Skript, který spouští skript mount.sh na pozadí. Spouštění na pozadí je nutné, aby nedošlo k zaseknutí systému při přihlašování.

skripty/link.sh
: Skript, který lze použít pro otevírání Windows odkazů .lnk. Skript se spouští s cestou k odkazu, po spuštění skript spustí průzkumníka souborů ve složce, na kterou odkazoval odkaz.

skripty_prf/
: Adresář s identickými soubory ze složky skripty/. Soubor variables.sh je ovšem upraven pro připojení do domény Katedry informatiky.

Literatura

[1] *Debian Votes To Add Non-Free Firmware to Official Install Media | Tom's Hardware*. Dostupný z: ⟨https://www.tomshardware.com/news/debian-includes-proprietary-code⟩.

[2] Bouška, Petr. *Adresářové služby a LDAP*. Dostupný z: ⟨https://www.samuraj-cz.com/clanek/adresarove-sluzby-a-ldap/⟩.

[3] Bouška, Petr. *Kerberos část 1 - Active Directory Komponenty*. Dostupný z: ⟨https://www.samuraj-cz.com/clanek/kerberos-cast-1-active-directory-komponenty/⟩.

[4] Bouška, Petr. *Active Directory Komponenty - domain, tree, forest, site*. Dostupný z: ⟨https://www.samuraj-cz.com/clanek/active-directory-komponenty-domain-tree-forest-site/⟩.

[5] *Samba (software)*. Dostupný z: ⟨https://en.wikipedia.org/wiki/Samba_(software)⟩.

[6] Lawrence, Kearney. *Introducing SSSD: You Should See Polyscheme PAM*. Dostupný z: ⟨https://web.archive.org/web/20190127004209/http://www.lawrencekearney.com/files/OpenHorizons_Issue_27_Intro_to_SSSD_Polyscheme_PAM.pdf⟩.

[7] *realm: Couldn't join realm: Insufficient permissions to join the domain example.local*. Dostupný z: ⟨https://stackoverflow.com/questions/73517112/realm-couldnt-join-realm-insufficient-permissions-to-join-the-domain-example⟩.

[8] Bouška, Petr. *Autentizace v LDAPu (AD)*. Dostupný z: ⟨https://www.samuraj-cz.com/clanek/autentizace-v-ldapu-ad/⟩.

[9] *GVfs*. Dostupný z: ⟨https://wiki.gnome.org/Projects/gvfs⟩.

[10] *gvfsd process does not have the KRB5CCNAME environment set*. Dostupný z: ⟨https://bugs.launchpad.net/ubuntu/+source/tracker-miners/+bug/1779890⟩.

[11] *File permissions mode 0777 vs 777 - Digital Fortress*. Dostupný z: ⟨https://digitalfortress.tech/php/difference-file-mode-0777-vs-777/⟩.

[12] *New file format options in The New Office*. Dostupný z: ⟨https://blogs.office.com/2012/08/13/new-file-format-options-in-the-new-office/⟩.