Správa sietí a operačných systémov Linux a Windows

Richard Ostertág

UNIVERZITA KOMENSKÉHO V BRATISLAVE
2022

Správa sietí a operačných systémov Linux a Windows

Autor: RNDr. Richard Ostertág, PhD.
Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky
Katedra informatiky
Oddelenie kryptológie a informačnej bezpečnosti

Recenzenti: doc. Ing. Pavel Segeč, PhD.
doc. Ing. Anton Baláž, PhD.

Vydavateľ: Univerzita Komenského v Bratislave
Bratislava 2022
1. vydanie, 81 strán

Materiál je výstupom Rozvojového projektu Univerzity Komenského a Ministerstva školstva, vedy, výskumu a športu SR č. 002UK-2-1/2018 – *„Vzdelávanie pre informačnú spoločnosť“* v oblasti Podpora vysokých škôl pri plnení záväzkov prijatých v rámci Národnej koalície pre digitálne zručnosti a povolania SR.

ISBN 978-80-223-5405-9

Obsah

Zoznam obrázkov

Kapitola 1

Úvod

Svety počítačov postavených na operačnom systéme Windows a Linux zostávali dlho oddelené. Dnes sa však čoraz častejšie stretávame s použitím oboch systémov v rámci jednej siete. V takomto prípade je interoperabilita týchto systémov dôležitou otázkou. Našťastie obe strany postupne k sebe nachádzajú cestu.

Cieľom tohto materiálu je ukázať, ako je možné oba systémy nakonfigurovať tak, aby spolu zdieľali údaje a plnohodnotne spolupracovali v jednej doméne s využitím autentifikácie a adresárových služieb poskytovaných druhou platformou (ktorou môže byť platforma Windows, tak aj na platforma Linux).

Najprv v samostatnej kapitole demonštrujeme, ako pripojiť Linuxový počítač s Ubuntu 20.04 do domény riadenej Windows Serverom 2019. Ukážeme konfiguráciu radiča domény na Windows a ako nastaviť autentifikáciu používateľov na Linuxe voči tejto doméne. Na záver tejto kapitoly predvedieme, ako sa môže doménový používateľ prihlásiť na Linuxový počítač, pričom sa mu automaticky vytvorí domovský priečinok a správne sa namapuje jeho doménový identifikátor na Linuxový.

V ďalšej kapitole vykonáme inštaláciu a konfiguráciu radiča domény postaveného na Linuxovom balíku Samba 4. Demonštrujeme niektoré možnosti správy takejto domény z Linuxu, ale ukážeme aj jej správu natívnymi nástrojmi operačného systému Windows. Na záver pridáme počítač s operačným systémom Windows do Samba domény a ukážeme vytvorenie a aplikovanie skupinových politík.

Nakoniec si popíšeme pripojenie z jedného operačného systému na vzdialenú pracovnú plochu druhého. Najprv v samostatnej kapitole popíšeme projekt Cygwin, pričom sa zameriame na SSH a X server. Oba programy použijeme na pripojenie sa z operačného systému Windows na Unixový počítač. V nasledujúcej kapitole použijeme program PuTTY, ako náhradu za SSH z Cygwinu. Toto riešenie sa hodí, pokiaľ nepotrebujeme celú funkčnosť prostredia Cygwin a chceme šetriť priestorom na disku. V poslednej kapitole ukážeme s použitím programov rdesktop a FreeRDP, ako sa možno pripojiť z operačného systému Linuxu na vzdialenú pracovnú plochu Windows.

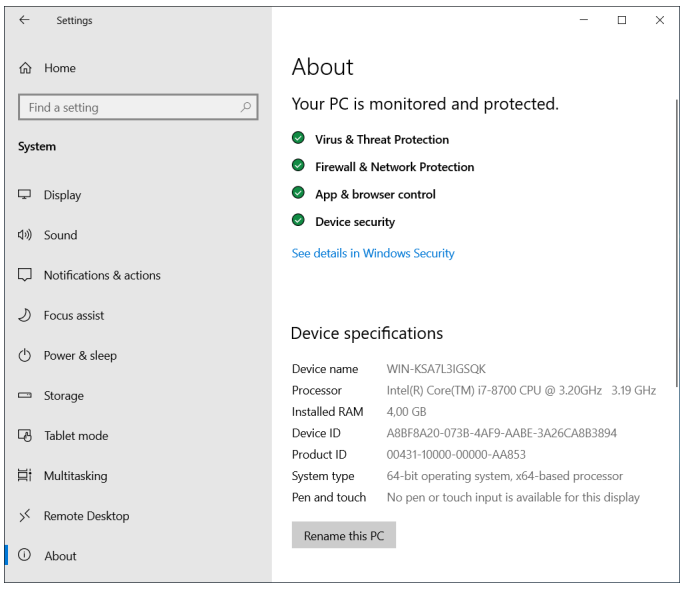
Kapitola 2

Prístup k Windows AD DS z Linuxu

Prvým problémom, ktorého riešenie si popíšeme, je využitie adresárových služieb poskytovaných doménovým radičom bežiacim na operačnom systéme Windows z Linuxových pracovných staníc. Prezentované riešenie umožní doménovým používateľom prihlásiť sa aj na Linuxové počítače pridané do domény bez toho, aby niekto musel pre nich najprv vytvoriť lokálne Linuxové konto.

2.1 Inštalácia Active Directory Domain Services na Windows Server

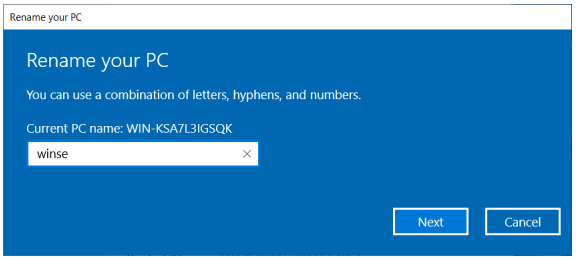
Pre účely vyskúšania pridania Linuxových počítačov do domény si najskôr spravíme základnú inštaláciu doménových služieb na Windows Server 2019 Standard.



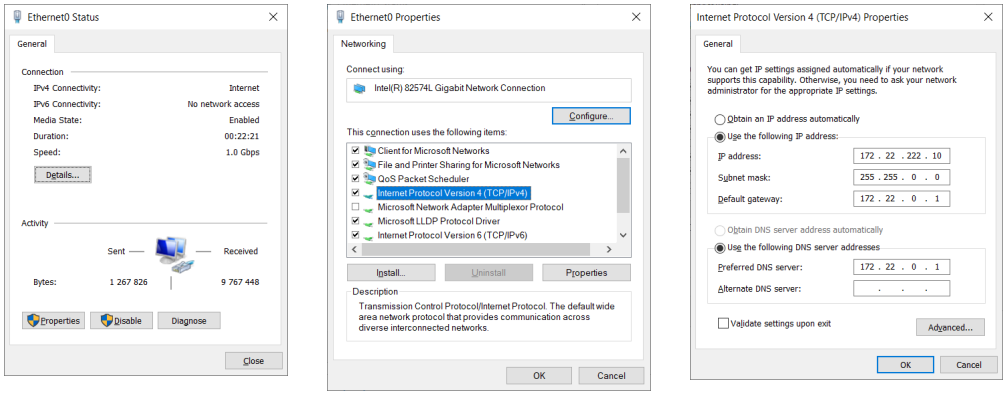
2.1.1 Základná konfigurácia počítača

Pred inštaláciou Active Directory Domain Services na Windows Server je potrebné mať nastavené silné heslo pre správcu (účet Administrator), zvolené meno počítača, pridelenú pevnú IP adresu a aktualizovaný operačný systém s poslednými záplatami. Nastavenie mena počítača vykonáme v aplikácii „Settings“ (prístupnej zo štart-menu) stlačením tlačidla Rename this PC v časti „System ▸ About“.

V zobrazenom dialógovom okne „Rename your PC“ zadáme meno počítača. Pre meno sme si zvolili winse (ako WINdows SErver). Po potvrdení zmeny mena tlačidlom Next je potrebné pre aplikovanie tejto zmeny počítač reštartovať, kliknutím na tlačidlo Restart now.

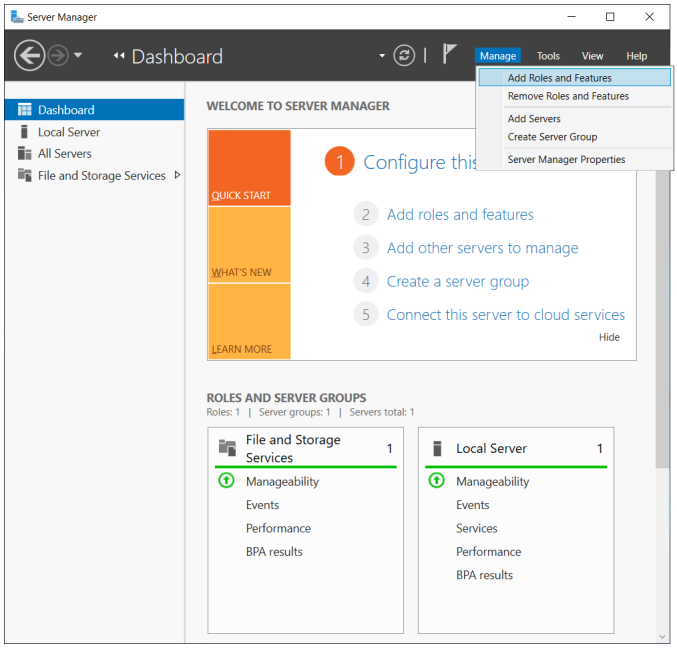


Po reštartovaní počítača ešte potrebujeme nastaviť pevnú IP adresu, pretože štandardne sa používa adresa získaná od DHCP servera. Nastavenie pevnej IP adresy je možné cez nastavenie v časti „⚙ ▸ Network & Internet ▸ Change adapter options“. Tu si dvojklikom vyberieme pripojenie Ethernet0. V dialógovom okne „Ethernet0 Status“ stlačíme tlačidlo Properties. V novom okne „Ethernet0 Properties“ si zvolíme v zozname „Internet Protocol Version 4 (TCP/IPv4)“ a opäť stlačíme tlačidlo Properties. V poslednom okne s názvom „Internet Protocol Version 4 (TCP/IPv4) Properties“ zvolíme „Use the following IP address“ a „Use the following DNS server address“. Potom zadáme údaje podľa obrázku nižšie. V tomto prípade sme zvolili pre server IP adresu `172.22.222.10/16`, pričom predvolená brána je `172.22.0.1`. Brána v našom prípade slúži aj ako DNS server. Tieto údaje treba samozrejme prispôsobiť konkrétnemu prostrediu, v ktorom sa server inštaluje.



Obr. 2.1: Nastavenie pevnej IP adresy servera

2.1.2 Inštalácia „Active Directory Domain Services“

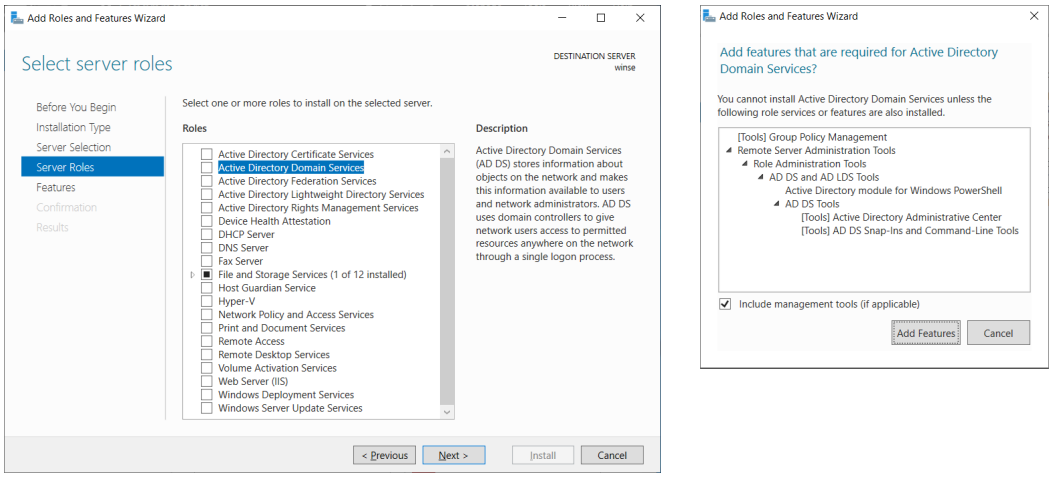


Po základnej konfigurácii počítača pridáme serveru rolu pre „Active Directory Domain Services“ (v skratke AD DS). Role môžeme pridávať napríklad pomocou aplikácie „Server Manager“, ktorá sa automaticky spustí po prihlásení. V menu si vyberieme položku „Manage“ a následne v rozbalenom menu položku „Add Roles and Features“. Po jej odkliknutí sa zobrazí okno so sprievodcom „Add Roles and Features Wizard“.

Sprievodca najprv upozorní na potrebu silného hesla pre správcu, nastavenie statickej IP adresy a posledných aktualizácií. Tieto kroky sme už vykonali v základnej konfigurácii, takže stlačením tlačidla Next > prejdeme na ďalší krok.

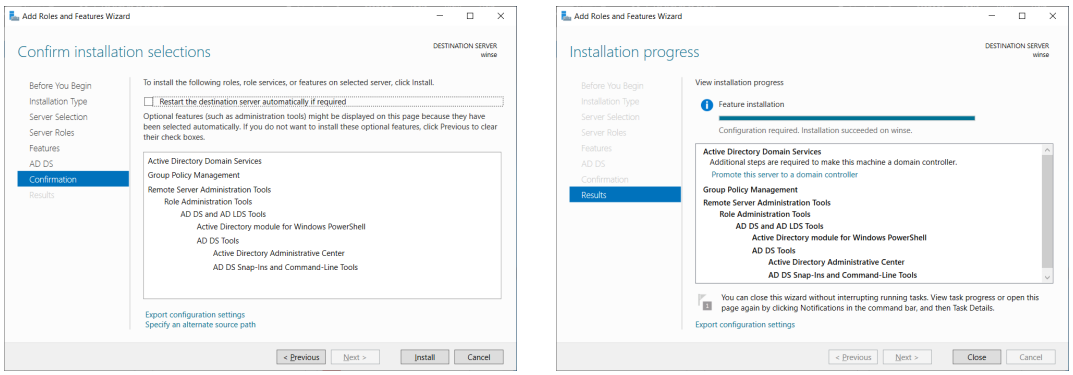
V tomto kroku s názvom „Installation Type“ si vyberieme možnosť „Role-based or feature-based

installation“. Druhá možnosť („Remote Desktop Services installation“) nás momentálne nezaujíma. Po prechode na ďalší krok (s názvom „Server Selection“) vyberieme zo zoznamu serverov riadok s naším serverom (`winse`, IP: `172.22.222.10`). V nasledujúcom kroku (s názvom „Server Roles“) vyberieme zo zoznamu rolí položku „Active Directory Domain Services“, ako znázorňuje obrázok nižšie.



Obr. 2.2: Pridanie „Active Directory Domain Services“

Pridáme aj všetky ostatné komponenty, ktoré Windows požaduje pre túto rolu, vrátane nástrojov pre správu (pozri obrázok vyššie). V ďalšom kroku sprievodcu („Feature“) už nemusíme nič pridávať, pretože potrebné komponenty už boli zvolené automaticky v predošlom kroku. V kroku AD DS sa odporúča prevádzkovať minimálne dva radiče domény, aby sa bolo možné do domény prihlásiť aj v prípade výpadku jedného z radičov. V našej skúšobnej inštalácii budeme toto odporúčanie ignorovať. V predposlednom kroku („Confirmation“) potvrdíme inštaláciu zvolených komponentov. Možnosť „Restart the destination server automatically if required“ nebudeme zaškrtávať, keďže si server reštartujeme radšej sami.

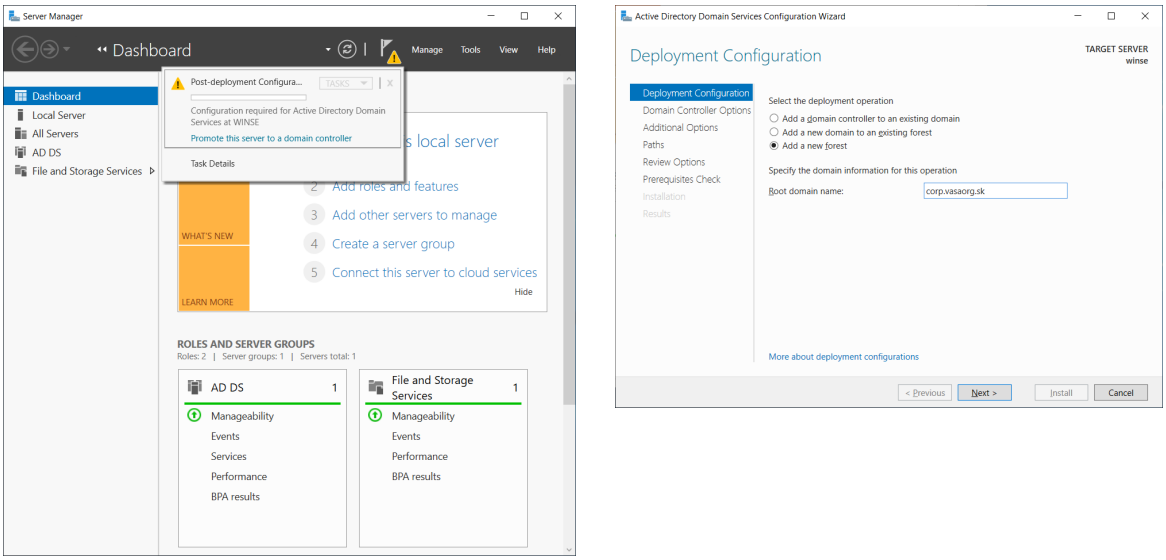


Obr. 2.3: Inštalácia „Active Directory Domain Services“

Na posledný krok („Results“), ktorým je samotná inštalácia sa dostaneme po stlačení tlačidla Install. Po dokončení inštalácie reštartujeme server. V tomto okamihu je radič domény nainštalovaný, ale ešte nepracuje, pretože je ho potrebné najprv nastaviť.

2.1.3 Konfigurácia „Active Directory Domain Services“.

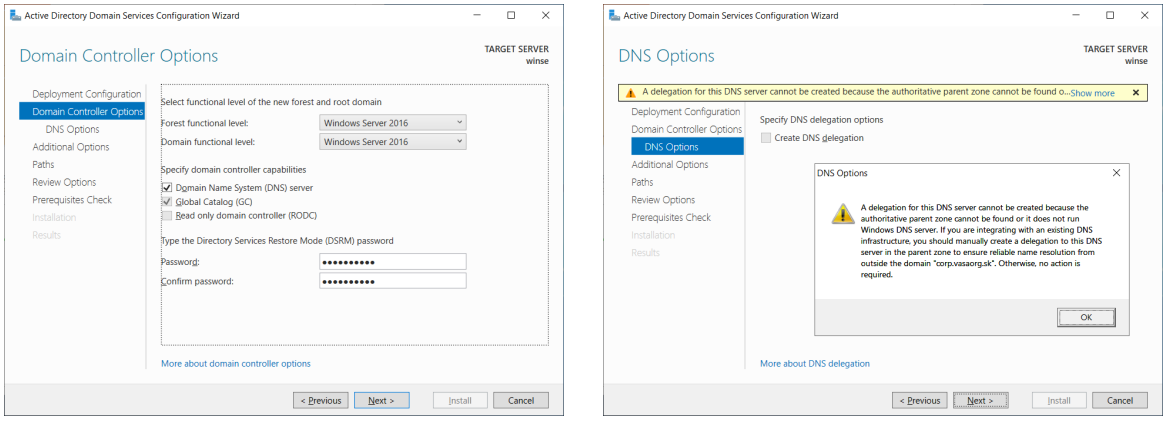
Po reštartovaní servera sa automaticky spustí „Server Manager“. Kliknutím na ikonu vlajky rozbalíme „Post-deployment Configuration“. Následne kliknutím na modrú linku „Promote this server to a domain controller“ spustíme sprievodcu „Active Directory Domain Services Configuration Wizard“. V prvom kroku („Deployment Configuration“) vyberieme možnosť „Add a new forest“, keďže v našom testovacom príklade vytvárame novú sieť, v ktorej ešte nie je žiadny iný doménový radič. Tým vznikne nový doménový les, v ktorom sa vytvorí nový doménový strom s jedinou (a to koreňovou) doménou, ktorú budeme pri testovaní používať.



Obr. 2.4: Spustenie „Active Directory Domain Services Configuration Wizard“

Názov koreňovej domény („Root domain name“) nemôže byť tzv. „single-labelled“. To znamená, že nemôže byť iba v tvare „`vasaorg`“, ale mal by mať aspoň dve časti, ako napríklad „`vasaorg.sk`“. Neodporúča sa vytvárať domény s rovnakým menom, ako je externé DNS meno organizácie. Napríklad, ak externá web stránka je na adrese `http://vasaorg.sk`, tak pre interné domény je potrebné zvoliť iné meno, napríklad `corp.vasaorg.sk`. Po zadaní mena koreňovej domény pokračujeme stlačením tlačidla Next >.

V ďalšom kroku („Domain Controller Options“) je potrebné zadať „Directory Services Restore Mode“ (DSRM) heslo. Toto heslo by sme použili v obnovovacom režime doménového radiča. V našom prípade túto možnosť nebudeme využívať, ale aj tak je potrebné si nejaké heslo zvoliť. Ako z obrázku nižšie vidieť, predvolená minimálna funkčná úroveň (pre les aj doménu) je „Windows Server 2016“. Aj v tomto najvyššom nastavení sa podarilo komunikáciu Linuxu s doménou nakonfigurovať. Sprievodca automaticky zvolil inštaláciu DNS servera, ktorý je potrebný pre klientov, aby mohli dynamicky lokalizovať doménový radič pre doménu, v ktorej sa nachádzajú. Keďže toto je prvý radič v lese, je automaticky zvolená aj možnosť „Global Catalog“ (GC) a nie je možné vybrať „Read only domain controller“ (RODC). Na ďalší krok prejdeme stlačením tlačidla Next >.



Obr. 2.5: Nastavenie možností pre doménový radič

V nasledujúcom kroku („DNS Options“) sprievodca informuje, že nevie vytvoriť previazanie medzi rodičovskou zónou vasaorg.sk a vytváranou zónou `corp.vasaorg.sk`. V našom testovacom prípade to nevadí, pretože rodičovská zóna ani neexistuje a klientov nakonfigurujeme tak, aby komunikovali priamo s DNS serverom na radiči domény, ktorý bude priamo obsahovať požadovanú zónu `corp.vasaorg.sk`. Pokračujeme stlačením tlačidla Next >.

V ďalších dvoch krokoch („Additional Options“ a „Paths“) sa zobrazí NetBIOS doménové meno („CORP“) a ponúkne sa možnosť zmeniť preddefinované umiestnenie priečinka s databázou adresárovej služby (`C:\Windows\NTDS`), log záznamami (`C:\Windows\NTDS`) a so SYSVOL (`C:\Windows\SYSVOL`), na ktorom sa nachádzajú napríklad skupinové politiky. Štandardné hodnoty nebudeme meniť a pokračujeme 2× stlačením tlačidla Next >.

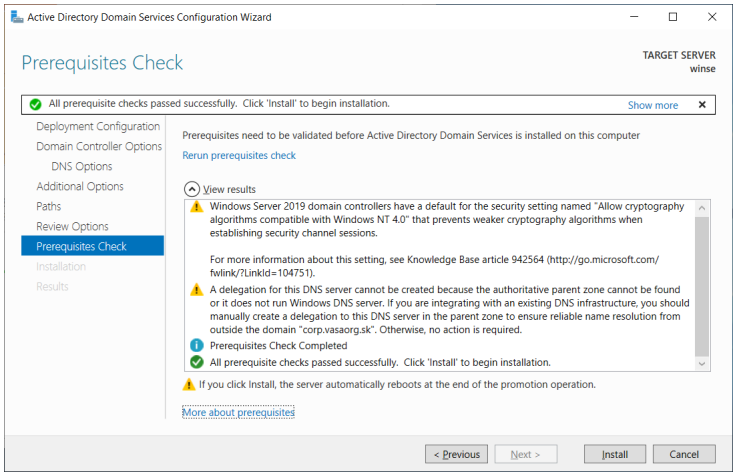
Nasleduje rekapitulácia konfigurácie (krok „Review Options“):

- Configure this server as the first Active Directory domain controller in a new forest.
- The new domain name is "corp.vasaorg.sk". This is also the name of the new forest.
- The NetBIOS name of the domain: CORP
- Forest Functional Level: Windows Server 2016
- Domain Functional Level: Windows Server 2016
- Additional Options — Global catalog: Yes, DNS Server: Yes, Create DNS Delegation: No
- Database folder: `C:\Windows\NTDS`
- Log file folder: `C:\Windows\NTDS`
- SYSVOL folder: `C:\Windows\SYSVOL`
- The DNS Server service will be configured on this computer.
- This computer will be configured to use this DNS server as its preferred DNS server.
- The password of the new domain Administrator will be the same as the password of the local Administrator of this computer.

V tomto okamihu je možné nechať si zobraziť pomocou tlačidla View script príkaz pre „Windows PowerShell“, ktorým je možné vykonať rovnakú konfiguráciu priamo z príkazového riadku bez preklikávania sa grafickým používateľským rozhraním:

```
# Windows PowerShell script for AD DS Deployment
Import-Module ADDSDeployment
Install-ADDSForest `
-CreateDnsDelegation:$false `
-DatabasePath "C:\Windows\NTDS" `
-DomainMode "WinThreshold" `
-DomainName "corp.vasaorg.sk" `
-DomainNetbiosName "CORP" `
-ForestMode "WinThreshold" `
-InstallDns:$true `
-LogPath "C:\Windows\NTDS" `
-NoRebootOnCompletion:$false `
-SysvolPath "C:\Windows\SYSVOL" `
-Force:$true
```

Po stlačení tlačidla Next > nasleduje kontrola splnenia všetkých predpokladov pre konfiguráciu AD DS. Aj keď je kontrola úspešná, tak zobrazí dve upozornenia:



Obr. 2.6: Kontrola splnenia všetkých predpokladov pre konfiguráciu AD DS

Prvé sa týka skutočnosti, že Windows Server 2019 má štandardne vypnutú podporu pre slabšie kryptografické algoritmy kompatibilné s Windows NT 4.0. Druhé upozornenie sa týka chýbajúceho prepojenia DNS servera, ktoré sme spomínali vyššie. Obe varovania v našom prípade nepredstavujú žiadny problém. Preto môžeme tlačidlom Install spustiť inštaláciu. Po jej skončení sa server automaticky reštartuje a máme pripravenú novú doménu. V prípade reálnej inštalácie by bolo potrebné ďalej pokračovať v konfigurácii AD. Napríklad premenovať štandardnú lokalitu Default-First-Site-Name, nastaviť synchronizáciu času a tak podobne.

2.1.4 Otestovanie funkčnosti servera

Na otestovanie funkčnosti DNS servera použijeme iný počítač so základnou inštaláciou operačného systému Linux (konkrétne Ubuntu 20.04.2 LTS). Necháme si DNS serverom na radiči domény (IP adresa: `@172.22.222.10`) vypísať SRV záznam pre službu LDAP nad protokolom TCP pre doménu `corp.vasaorg.sk` (čo zodpovedá požiadavke na záznam: `_ldap._tcp.corp.vasaorg.sk`). Dosiahneme to nasledovným príkazom:

```
tester@ubuntu:~$ dig @172.22.222.10 srv _ldap._tcp.corp.vasaorg.sk
;; ANSWER SECTION:
_ldap._tcp.corp.vasaorg.sk. 600 IN SRV 0 100 389 winse.corp.vasaorg.sk.

;; ADDITIONAL SECTION:
winse.corp.vasaorg.sk.     3600 IN A   172.22.222.10
```

Vidíme, že ako odpoveď dostaneme náš doménový server: `winse.corp.vasaorg.sk`. Otestovať funkčnosť radiča domény môžeme aj overením funkčnosti samotného LDAP subsystému. Najprv si musíme na Linux nainštalovať utility pre prácu s LDAP príkazom:

```
tester@ubuntu:~$ sudo apt install ldap-utils
```

Následne pomocou príkazu `ldapsearch` môžeme získať informácie uložené v adresárovej službe. Napríklad nasledovný príkaz vypíše informácie o používateľovi Administrator:

```
tester@ubuntu:~$ ldapsearch -LLL -H ldap://172.22.222.10 -x -D
↪"CORP\Administrator" -W -b
↪"cn=Administrator,cn=Users,dc=corp,dc=vasaorg,dc=sk"
Enter LDAP Password: ********** (heslo pre používateľa CORP\Administrator)
dn: CN=Administrator,CN=Users,DC=corp,DC=vasaorg,DC=sk
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Administrator
description: Built-in account for administering the computer/domain
distinguishedName: CN=Administrator,CN=Users,DC=corp,DC=vasaorg,DC=sk
...
memberOf: CN=Group Policy Creator Owners,CN=Users,DC=corp,DC=vasaorg,DC=sk
memberOf: CN=Domain Admins,CN=Users,DC=corp,DC=vasaorg,DC=sk
memberOf: CN=Enterprise Admins,CN=Users,DC=corp,DC=vasaorg,DC=sk
memberOf: CN=Schema Admins,CN=Users,DC=corp,DC=vasaorg,DC=sk
memberOf: CN=Administrators,CN=Builtin,DC=corp,DC=vasaorg,DC=sk
uSNChanged: 12779
name: Administrator
objectGUID:: oP40raFzQ0WRlGBYy5S81Q==
userAccountControl: 66048
badPwdCount: 0
...
primaryGroupID: 513
objectSid:: AQUAAAAAAAUVAAAAqxUkd9H8yyT84uHU9AEAAA==
adminCount: 1
...
sAMAccountName: Administrator
sAMAccountType: 805306368
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=corp,DC=vasaorg,DC=sk
isCriticalSystemObject: TRUE
...
```

2.2 Dekódovanie SID

Ako vidieť na predošlom výpise, niektoré hodnoty sú vypísané v zakódovanom tvare (napr. objectGUID alebo objectSid). Ukážeme si, ako dekódovať hodnotu objectSid. Najprv musíme base64 dekódovať reťazec „AQUAAAAAAAUVAAAAqxUkd9H8yyT84uHU9AEAAA==“. Výsledkom ale bude postupnosť bajtov, ktorá nepredstavuje len ASCII znaky. Preto si ich nasledovným príkazom necháme zobraziť ako čísla v hexadecimálnej sústave:

```
1 tester@linse:~$ echo "AQUAAAAAAAUVAAAAqxUkd9H8yyT84uHU9AEAAA==" | base64 -d |
    ↪hexdump -v -e '/1 "%02x "'
2 01 05 00 00 00 00 00 05 15 00 00 00 ab 15 24 77 d1 fc cb 24 fc e2 e1 d4 f4 01 00 00
```

Teraz rozdelíme získanú postupnosť bajtov na jednotlivé časti tak, ako je naznačené zmenou farby pozadia. Získame nasledovné polia:

Názov časti	Dĺžka (B)	Bajty	Hodnota	Komentár
revízia SID štruktúry	1 ↔	01	1	aktuálne vždy 1
počet „SA“ záznamov	1 ↔	05	5	maximálne 15
IdentifierAuthority	6 →	00 00 00 00 00 05	5	NT SID authority
1. SubAuthority (SA)	4 ←	15 00 00 00	21	
2. SubAuthority (SA)	4 ←	ab 15 24 77	1998853547	
3. SubAuthority (SA)	4 ←	d1 fc cb 24	617348305	
4. SubAuthority (SA)	4 ←	fc e2 e1 d4	32470361374	
5. SubAuthority (SA)	4 ←	f4 01 00 00	500	Relative ID (RID)

Všetky viac-bajtové čísla sú v postupnosti bajtov reprezentované tak, že najprv sa uloží najmenej významný bajt (little-endian, LSB, ←). Výnimkou je IdentifierAuthority, ktorý začína najvýznamnejším bajtom (big-endian, MSB, →). Bezpečnostný identifikátor (SID) používateľa Administrator (v tvare aký na jeho reprezentáciu používa Windows) získame zadaním príkazu `whoami /user` na serveri `winse`. Identifikátor môžeme získať aj spojením číselných reprezentácií jednotlivých častí:

$$\underbrace{\text{S-1-5-21-1998853547-617348305-3571573500}}_{\text{SID domény}}\text{-}\underbrace{\text{500}}_{\text{RID}}$$

Prvá časť je SID domény a druhá časť je jednoznačný relatívny identifikátor (RID) používateľa Administrator v rámci tejto domény.

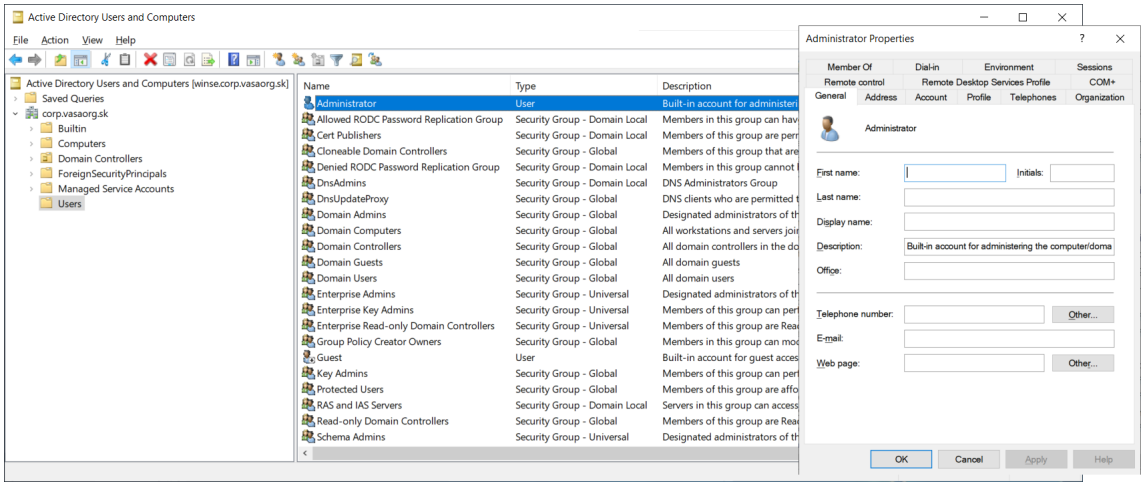
2.3 Základné používanie AD DS

V nasledujúcich dvoch častiach si ukážeme niektoré základné nástroje pre prácu s „Active Directory Domain Services“ (AD DS).

2.3.1 Správa používateľov a počítačov v AD

Pre správu používateľov a počítačov v „Active Directory“ (AD) sa používa aplikácia „Active Directory Users and Computers“ (v skratke ADUC). Na ľavej strane jej okna je strom domény `corp.vasaorg.sk`, ktorého časťou je napríklad zložka s používateľmi. Keď si v tejto zložke nájdeme používateľa Administrator a dáme si zobraziť jeho vlastnosti, tak sa zobrazí dialógové okno „Administrator Properties“. V tomto okne je možné zadávať údaje (ako napríklad meno, priezvisko, e-mail, skupiny a tak podobne). Všimnime si, že v tomto okamihu neobsahuje dialógové okno záložku s názvom „UNIX Attributes“. Do starších Windows Serverov

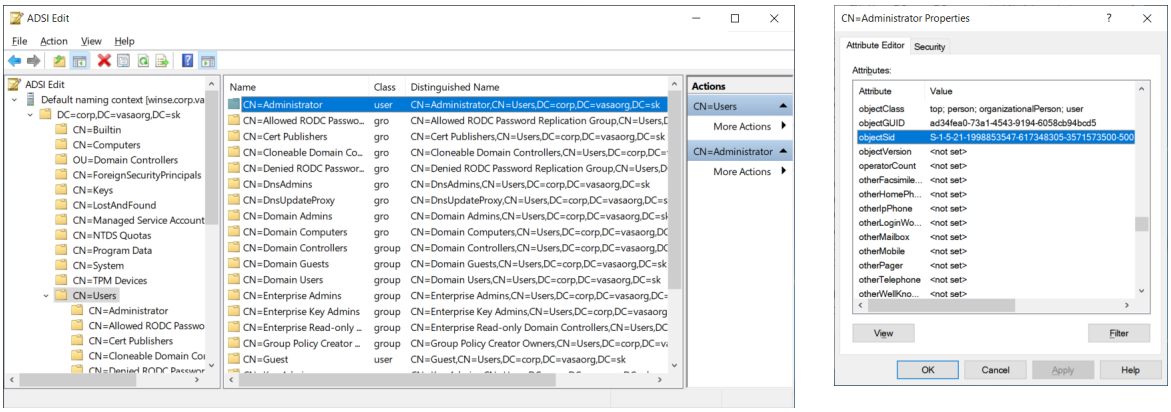
(pred verziou 2016) túto záložku neskôr doinštalujeme pomocou nástroja „Identity Management for UNIX“ (pozri časť 2.13 na strane 26).



Obr. 2.7: Aplikácia „Active Directory Users and Computers“

2.3.2 Pohľad do obsahu LDAP

Pre detailnejší pohľad do obsahu adresárovej služby je možné použiť napríklad nástroj „ADSI Edit“ (celým názvom „Active Directory Services Interfaces Editor“). Po jeho prvom spustení je potrebné kliknúť pravým tlačidlom myši na „ADSI Edit“ v koreni stromu (v ľavej časti obrazovky) a vybrať možnosť „Connect to...“. Po prvotnom nastavení spojenia na náš doménový radič (stačí potvrdiť tlačidlom OK) sa v ľavej časti okna rozbalí strom domény.



Obr. 2.8: Aplikácia „Active Directory Services Interfaces Editor“

Opäť si nájdeme priečinok s používateľmi a v ňom používateľa Administrator. Po zobrazení vlastností tohto používateľa sa dozvieme zoznam všetkých atribútov, ku ktorým môže mať tento objekt priradenú nejakú hodnotu. Pre nás je zaujímavý napríklad atribút objectSid, ktorý prezrádza SID zvoleného objektu (v tomto prípade používateľa). Tiež vidno, že mnohé atribúty sú nenastavené (<not set>).

Teraz si môžeme overiť, že hodnota objectSid, ktorú sme získali cez `ldapsearch` príkaz pre používateľa Administrator, korešponduje s hodnotou objectSid, ktorú vidíme cez „ADSI Edit“ priamo na Windows serveri.

2.4 Samba

Samba je open-source projekt, ktorého cieľom je integrácia medzi Windows a Unix prostredím. Umožňuje zdieľať súbory a tlačiarne medzi Windows a UNIX systémami. Implementuje Server Message Block (SMB) protokol (známy tiež ako Common Internet File System – CIFS) pre UNIX systémy. Dokáže emulovať radič domény na UNIX serveri a umožňuje UNIX počítačom využívať služby ponúkané AD DS, ako sú napríklad autentifikácia a adresárové služby.

Samba je slobodný softvér pod GNU GPL v3 licenciou. Môže byť komerčne použitý, ale autori nemôžu byť braní na zodpovednosť. Pozostáva z viacerých balíkov, ktoré popíšeme v nasledujúcich častiach.

2.4.1 Balík: samba

Samotný balík samba obsahuje komponenty potrebné pre súborový server, tlačový server a radič domény (či už vo verzii NT4 alebo AD). Pre použitie v doméne je potrebný aj balík winbind, popísaný nižšie. Balík samba nie je potrebný pre „interaktívne“ pripojenie k existujúcim súborovým alebo tlačovým serverom na báze SMB/CIFS protokolu. Na tento účel stačí balík smbclient. Taktiež balík samba nie je potrebný pre lokálne pripojenie vzdialeného súborového systému. Na to stačí balík cifs-utils.

2.4.2 Balík: winbind

Balík winbind obsahuje winbindd démona, ktorý integruje do systému Linux doménové mechanizmy pre autentifikáciu a adresárové služby pre vyhľadanie používateľov a skupín. Sprostredkováva komunikáciu medzi Pluggable Authentication Modules (PAM) a Name Service Switch (NSS) subsystémom Linuxu a adresárovými službami. Pre komunikáciu s AD DS používa Kerberos protokol pre autentifikáciu (cez PAM – vyžaduje balík libpam-winbind) a LDAP pre získanie informácií o používateľoch a skupinách (cez NSS – vyžaduje balík libnss-winbind). Umožňuje aj lokalizáciu radiča domény pomocou algoritmu DC Locator, ktorý vychádza z už spomínaných DNS SRV záznamov. To je jeho výhoda oproti priamemu použitiu PAM s Kerberosom, kde by bolo nutné napevno nastaviť adresu DC. Pri zmene hesla v AD komunikuje s doménovým radičom (DC) cez Remote Procedure Call (RPC).

2.4.3 Balíky: libnss-winbind a libpam-winbind

Balík libnss-winbind obsahuje zásuvný modul nss_winbind pre Name Service Switch (NSS), ktorý cez lokálny winbind server poskytuje systému vyhľadávanie používateľov a skupín. Okrem toho obsahuje aj zásuvný modul nss_wins pre NSS, ktorý poskytuje vyhľadávanie

názvu hostiteľa (hostname) cez NetBIOS Name Service (NBNS)[1] a NetBIOS broadcast protokoly. Tento modul nebudeme používať.

Balík libpam-winbind obsahuje zásuvný modul pam_winbind pre PAM, ktorý cez lokálny winbind server poskytuje systému autentifikáciu používateľov vo Windows doméne.

2.4.4 Balík: smbclient

Balík smbclient umožňuje „interaktívne“ pripojenie k existujúcim súborovým alebo tlačovým serverom na báze SMB/CIFS protokolu (či už Microsoft Windows alebo Samba). Obsahuje nasledovné príkazy:

smbclient: pre prístup k zdieľaným zdrojom (podobným štýlom ako FTP)

smbspool: pre posielanie súborov na zdieľanú tlačiareň

smbtree: pre zobrazenie sieťového stromu

Nástroje pre lokálne pripojenie zdieľaných sieťových adresárov sa štandardne nachádzajú v distribúcii operačného systému Ubuntu v balíku cifs-utils.

2.4.4.1 Zoznam zdieľaných priečinkov

Pomocou príkazu `smbclient` vieme získať zoznam zdieľaných priečinkov na zvolenom serveri nasledovným spôsobom (prepínač `-U` umožňuje zvoliť meno používateľa):

```
tester@ubuntu:~$ sudo apt install smbclient
tester@ubuntu:~$ smbclient -U "CORP\Administrator" --list=winse
Enter CORP\Administrator's password: **********

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
SMB1 disabled -- no workgroup available
```

SMB1 je už skoro 40 ročný protokol (vznikol v roku 1983) a dnes je už dávno považovaný za zastaraný (firmou Microsoft od roku 2015), keďže nie dostatočne efektívny a bezpečný. Od Windows 10 verzie 1511 („November Update“) je podpora pre SMB1 protokol štandardne vypnutá. Windows 10 od verzie 1709 („Fall Creators Update“) už nepovoľuje inštaláciu SMB1 klienta. Preto aj na Linux vidíme, že SMB1 je štandardne zakázaný.

2.4.4.2 Chybové hlásenia

Pre testovanie si najprv na Windows serveri vyrobíme neprivilegovaného lokálneho používateľa `ric` pomocou nasledovného príkazu v PowerShelli:

[1] Stretneme sa aj s názvom: Windows Internet Name Service (WINS).

```
PS C:\Users\Administrator> New-LocalUser -Name "ric"

cmdlet New-LocalUser at command pipeline position 1
Supply values for the following parameters:
Password: **********

Name Enabled Description
---- ------- -----------
ric  True
```

Používateľ `ric`, ako neprivilegovaný používateľ, nemá prístup k ukrytému (spoznáme podľa znaku $ na konci názvu) zdieľaniu disku C a preto získa nasledovné chybové hlásenie:

```
tester@ubuntu:~$ smbclient -U "CORP\ric" //winse/c$
Enter CORP\ric's password: **********
tree connect failed: NT_STATUS_ACCESS_DENIED
```

Ak používateľ zadá zlý názov zdieľaného priečinka, tak získa iné chybové hlásenie:

```
tester@ubuntu:/etc/samba$ smbclient -U "CORP\ric" //winse/neexistuje
Enter CORP\ric's password: **********
tree connect failed: NT_STATUS_BAD_NETWORK_NAME
```

Ak zadáme zlého používateľa alebo heslo, tak získame nasledovné chybové hlásenie:

```
tester@ubuntu:/etc/samba$ smbclient -U "CORP\neexistuje" //winse/c$
Enter CORP\neexistuje's password: **********
session setup failed: NT_STATUS_LOGON_FAILURE
```

Môžeme vyskúšať, že Windows Server v súlade s dobrými bezpečnostnými praktikami nerozlišuje v chybovom hlásení (alebo svojím správaním) medzi neexistujúcim používateľom a existujúcim používateľom so zlým heslom. Tým predchádza napríklad pokusom o overenie existencie účtu bez znalosti hesla alebo o enumerovanie všetkých účtov.

2.4.4.3 „FTP“ prístup k súborom

Primárne využitie príkazu `smbclient` je pre interaktívny prístup k súborom na vzdialenom počítači v štýle bežných FTP klientov:

```
tester@ubuntu:~$ cd ~/Pictures/
tester@ubuntu:~/Pictures$ touch foto1.jpg
tester@ubuntu:~/Pictures$ smbclient -U "CORP\Administrator" //winse/c$
Enter CORP\Administrator's password: **********
Try "help" to get a list of possible commands.
smb: \> cd Users\Administrator\Documents\
smb: \Users\Administrator\Documents\> dir
  .                                   DR        0  Sun Mar ...
  ..                                  DR        0  Sun Mar ...
  desktop.ini                        AHS      402  Tue Mar ...
  My Music                           DHS        0  Tue Mar ...
  My Pictures                        DHS        0  Tue Mar ...
  My Videos                          DHS        0  Tue Mar ...

                15570943 blocks of size 4096. 11201316 blocks available
smb: \Users\Administrator\Documents\> get desktop.ini (stiahni zo servera)
getting file \Users\Administrator\Documents\desktop.ini of size 402 as
  ↪desktop.ini (392,5 KiloBytes/sec) (average 392,6 KiloBytes/sec)
smb: \Users\Administrator\Documents\> recurse (choď aj do podadresárov)
smb: \Users\Administrator\Documents\> mput *.jpg (nahraj na server)
Put file foto1.jpg? y
```

```
putting file foto1.jpg as \Users\Administrator\Documents\foto1.jpg (0,0 kb/s) (average 0,0 kb/s)
smb: \Users\Administrator\Documents\> quit
```

2.4.4.4 Tlač na zdieľanú tlačiareň (smbclient)

Aby sme mohli pokračovať, tak potrebujeme najprv mať nejakú zdieľanú tlačiareň. Na Windows serveri môžeme tlačiareň nazdieľať pomocou programu „Print Management“. Nech teda máme nazdieľanú tlačiareň pod názvom `\\winse\canon`. Tlačiť na túto zdieľanú tlačiareň z Linuxu môžeme napríklad pomocou príkazu `smbclient`. Nie je to však pohodlné:

```
tester@ubuntu:~$ smbclient -U "CORP\Administrator" //winse/canon
Enter CORP\Administrator's password:
Try "help" to get a list of possible commands.
smb: \> print sprava.txt
putting file sprava.txt as sprava.txt (0,1 kb/s) (average 0,1 kb/s)
```

2.4.4.5 Tlač na zdieľanú tlačiareň (smbspool)

Príkaz `smbspool` umožňuje pohodlnejšiu tlač z príkazového riadku. Formát príkazu je nasledovný: `smbspool [DEVICE_URI] job-id user title copies options [file]`. Parameter `DEVICE_URI` nie je potrebné zadávať, ak je definovaná premenná prostredia s rovnakým menom `DEVICE_URI`. Tvar tohto parametra je:

`smb://[username:password@][workgroup/]server[:port]/printer`.

Konkrétny príkaz pre tlač súboru môže vyzerať napríklad nasledovne:

```
tester@ubuntu:~$  smbspool smb://Administrator:***********@winse/canon 3 Tester "Nadpis" 1 "" sprava.txt
DEBUG: Try to connect using username/password ...
DEBUG: SMB connection established.
```

2.4.5 Balík: cifs-utils

Balík cifs-utils slúži na lokálne pripojenie zdieľaných adresárov cez CIFS protokol. Najprv je potrebné nainštalovať balíček cifs-utils a vytvoriť bod pripojenia:

```
tester@ubuntu:~$ sudo apt install cifs-utils
tester@ubuntu:~$ sudo mkdir /mnt/cifs
```

Potom je možné pripojiť zdieľaný adresár pomocou príkazu `mount`:

```
tester@ubuntu:~$ sudo mount -t cifs //172.22.222.10/C$ /mnt/cifs/ -o username=Administrator,password=***********
```

alebo pomocou príkazu `mount.cifs`:

```
tester@ubuntu:~$ sudo mount.cifs //172.22.222.10/C$ /mnt/cifs/ -o username=Administrator,password=***********
```

Zrealizovanie pripojenia si môžeme následne overiť pomocou príkazu `mount` a `ls`:

```
tester@ubuntu:~$ mount
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
```

```
...
/dev/sda5 on / type ext4 (rw,relatime,errors=remount-ro)
...
//172.22.222.10/C$ on /mnt/cifs type cifs
    (rw,relatime,vers=3.1.1,cache=strict,username=Administrator,uid=0,
    noforceuid,gid=0,noforcegid,addr=172.22.222.10,file_mode=0755,
    dir_mode=0755,soft,nounix,serverino,mapposix,rsize=4194304,
    wsize=4194304,bsize=1048576,echo_interval=60,actimeo=1)
tester@ubuntu:~$ ls -la /mnt/cifs/
total 1441800
drwxr-xr-x 2 root root       4096 mar 16 11:33  ./
drwxr-xr-x 3 root root       4096 mar 21 16:23  ../
drwxr-xr-x 2 root root          0 sep 15  2018 '$Recycle.Bin'/
drwxr-xr-x 2 root root          0 mar 16 10:23 'Documents and Settings'/
-rwxr-xr-x 1 root root 1476395008 mar 21 15:03  pagefile.sys*
drwxr-xr-x 2 root root          0 mar 16 10:55  PerfLogs/
drwxr-xr-x 2 root root          0 mar 21 00:50  ProgramData/
dr-xr-xr-x 2 root root          0 mar 16 11:32 'Program Files'/
drwxr-xr-x 2 root root          0 mar 16 10:27 'Program Files (x86)'/
drwxr-xr-x 2 root root          0 mar 16 10:23  Recovery/
drwxr-xr-x 2 root root          0 mar 20 23:12 'System Volume Information'/
dr-xr-xr-x 2 root root          0 mar 16 10:27  Users/
drwxr-xr-x 2 root root          0 mar 21 00:40  Windows/
```

2.4.5.1 Pripojenie bez hesla alebo mena

Pripojenie je možné zrealizovať aj bez zadania hesla na príkazovom riadku, ale potom je ho potrebné zadať interaktívne:

```
tester@ubuntu:~$ sudo mount.cifs //172.22.222.10/C$ /mnt/cifs/ -o
    username=Administrator
Password for Administrator@//172.22.222.10/C$:  **********
```

Pokiaľ sa v príkazovom riadku nezadá ani meno používateľa, tak sa použije meno aktuálne prihláseného používateľa:

```
tester@ubuntu:~$ sudo mount.cifs //172.22.222.10/C$ /mnt/cifs/
Password for root@//172.22.222.10/C$:  **********
mount error(13): Permission denied
Refer to the mount.cifs(8) manual page (e.g. man mount.cifs) and kernel log
    messages (dmesg)
```

V zozname parametrov za `-o` môže byť aj parameter `credentials=filename`. Použitie súboru s heslom zamedzuje zobrazeniu hesla pri výpise procesov v systéme alebo histórie zadaných príkazov. Formát súboru je jednoduchý:

```
username=value
password=value
domain=value
```

2.5 Doménová autentifikácia vo Windows

Doménový radič Windows NT poskytoval autentifikačné služby klientom pomocou NT LAN Manager protokolu. Elegantne vyriešil problém s udržovaním duplicitných používateľských účtov na rôznych serveroch v sieti. Žiaľ, časom sa ukázalo, že NTLM protokol má bezpečnostné slabiny.

Preto od Windows 2000 Microsoft prešiel z NTLM protokolu na službu Active Directory, ktorá v sebe integruje Kerberos protokol pre autentifikačné služby a LDAP. Kerberos je podstatne bezpečnejší protokol ako NTLM a bol už predtým používaným štandardom na UNIXe.

2.6 Tri autentifikačné stratégie voči AD

Na UNIXe je možné nasadiť tri autentifikačné stratégie voči doméne.

2.6.1 LDAP autentifikácia

LDAP autentifikácia je najjednoduchšie riešenie (ale nie je vyhovujúce). Samotný Windows používa pre autentifikáciu protokol Kerberos. Pokiaľ sa Kerberos protokol nedá použiť, tak núdzovo prejde na NTLM protokol, nie LDAP. Na rozdiel od protokolu Kerberos, kde sa heslo po sieti neposiela vôbec, pri LDAP sa posiela meno aj heslo po sieti v otvorenom tvare. Toto riziko sa dá zmierniť vytvorením bezpečného kanálu medzi klientom a serverom, napríklad pomocou protokolu SSL/TLS, ale toto riešenie zas vyžaduje dodatočnú starostlivosť o certifikáty na oboch koncoch spojenia.

2.6.2 Autentifikácia pomocou LDAP a Kerberos

Druhá možnosť je autentifikácia cez Kerberos protokol pomocou Pluggable Authentication Modules – PAM[2]. Okrem autentifikácie cez Kerberos, sa používa aj LDAP (pomocou Name Service Switch – NSS[3]), ale iba pre získavanie informácií o používateľoch a skupinách. Na druhej strane však toto riešenie nevyužíva DNS SRV záznamy, ktoré radič domény zverejňuje a preto je nutné vybrať konkrétny radič domény, s ktorým sa má komunikovať. Taktiež toto riešenie neposkytuje intuitívny spôsob spravovania exspirujúcich hesiel.

2.6.3 Autentifikácia pomocou winbind

Ideálnym riešením, ktoré budeme aj ďalej popisovať, je využitie winbind autentifikácie. Vtedy PAM[2] a NSS[3] komunikujú s lokálne bežiacim winbind démonom. Ten preloží ich rôzne požiadavky do zodpovedajúcich požiadaviek na doménový radič. Tieto požiadavky pritom môže realizovať použitím LDAP, Kerberos protokolu alebo RPC, podľa toho, čo je v tom ktorom jednotlivom prípade najvhodnejšie.

2.7 Linux – konfigurácia siete

Pokiaľ nie je korektne nastavená delegácia pre DNS server vytvorenej domény, tak je potrebné, aby Linuxový počítač používal priamo DNS server domény, do ktorej sa pripája. Vo

[2]PAM (subsystému Linuxu pre autentifikáciu) sa budeme podrobnejšie venovať v časti 2.9 na strane 19.
[3]NSS budeme podrobnejšie opisovať v časti 2.10 na strane 23.

väčšine prípadov sa používa DNS integrované do Active Directory. Potom radič domény prevádzkuje aj DNS a treba teda použiť jeho IP adresu ako adresu DNS servera.

Pokiaľ používate Ubuntu pred verziou 20.04, tak v súbore `/etc/network/interfaces` je nutné pridať konfiguráciu pre rozhranie, ktorým sa počítač pripája do domény (v tomto prípade eth0):

```
auto eth0
iface eth0 inet static
  address 172.22.222.30
  netmask 255.255.0.0
  gateway 172.22.0.1
  dns-search corp.vasaorg.sk
  dns-nameservers 172.22.222.10
```

Ubuntu od verzie 20.04 prešlo na konfiguráciu siete pomocou netplan. V tomto prípade treba do adresára `/etc/netplan` pridať súbor s názvom `02-static-ip.yaml` s nasledovným obsahom (následne obsah možno otestovať príkazom `sudo netplan try`) a zmeny aplikujeme príkazom `sudo netplan apply`:

```
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens33: # aktuálny názov sa dá zistiť napríklad pomocou: ip link
      dhcp4: false
      addresses: [172.22.222.30/16]
      gateway4: 172.22.0.1
      nameservers:
        search: [corp.vasaorg.sk]
        addresses: [172.22.222.10]
```

Oba postupy majú rovnaký výsledný efekt, treba si zvoliť ten, ktorý je vhodný pre použitý operačný systém. Ďalším krokom je nastavenie mena počítača tak, aby zodpovedalo jeho menu v doméne. Pokiaľ by bolo iné, tak po pridaní počítača do domény by sa mohol v AD vytvoriť nesprávny objekt pre tento počítač. Pre Linuxový počítač si zvolíme meno linwo (ako LINux WOrkstation). Preto obsah súboru `/etc/hostname` zmeníme na linwo a v súbore `/etc/hosts` nahradíme riadok so starým menom týmto riadkom:

```
#127.0.1.1      ubuntu
172.22.222.30   linwo.corp.vasaorg.sk  linwo
```

2.8 Linux – konfigurácia synchronizácie času

Protokol Kerberos vyžaduje, aby server a klient mali zosynchronizovaný čas. Štandardne Active Directory povoľuje maximálne päť minútový časový posun medzi serverom a klientom. Pre zaistenie synchronizácie času medzi klientom a serverom treba nakonfigurovať Linux tak, aby využíval službu NTP (Network Time Protocol) radiča domény. Najprv skokom zosynchronizujeme čas medzi klientom a serverom pomocou príkazu:

```
tester@linwo:~$ sudo apt install ntpsec-ntpdate
tester@linwo:~$ sudo ntpdate winse
```

Túto metódu ale nechceme používať stále, pretože pri synchronizácii skokom dochádza k nespojitosti času, čo je nežiaduci efekt okamžitej skokovej synchronizácie. To môže viesť napríklad k tomu, že v logoch budú záznamy, ktorých čas kontinuálne nerastie, ale napríklad sa zrazu skokom vracia späť. Preto chceme čas synchronizovať priebežne pomocou NTP démona. Úvodná synchronizácia skokom má ale svoje opodstatnenie. Ak by na začiatku bola časová odchýlka medzi klientom a serverom príliš veľká, tak NTP démon by tento časový rozdiel príliš dlho vyrovnával. NTP démona nainštalujeme príkazom:

```
tester@linwo:~$ sudo apt install ntpsec
```

Do konfiguračného súboru NTP démona `/etc/ntpsec/ntp.conf` pridáme odkaz na náš doménový radič:

```
server 172.22.222.10 iburst prefer
```

Odkazy na iné servery (riadky začínajúce `pool` alebo `server`) by sme mali odstrániť alebo zakomentovať, pretože pre nás je dôležitejšie, aby sme mali rovnaký čas ako radič domény, než aby sme mali skutočne presný reálny čas. Po zmene konfiguračného súboru potrebujeme, aby démon svoju konfiguráciu opätovne načítal, čo zabezpečíme príkazom:

```
tester@linwo:~$ sudo systemctl restart ntpsec
```

Bežiaci NTP démon môžeme skontrolovať príkazom:

```
tester@linwo:~$ ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 172.22.222.10   .LOCL.          1 u   30   64    3    0.4311  152.0706   3.5918

```

alebo môžeme použiť aj príkaz:

```
tester@linwo:~$ ntpmon
```

2.9 Linux PAM

Pluggable Authentication Modules (v skratke PAM) boli navrhnuté firmou Sun v roku 1995 ako riešenie, ktoré poskytuje množinu autentifikačných programových rozhraní využiteľnú všetkými aplikáciami v systéme. Správcom systému zároveň umožňuje nastaviteľný spôsob poprepájania autentifikačných modulov do požadovanej autentifikačnej schémy. Táto schéma je na Linuxe konfigurovateľná cez súbory nachádzajúce sa v priečinku `/etc/pam.d`.

Väčšina Linuxových distribúcií obsahuje niekoľko autentifikačných modulov. Napríklad modul pam_ldap.so podporuje autentifikáciu na základe LDAP. Tento modul umožňuje použiť ľubovoľný LDAP v2 alebo v3 server, napríklad OpenLDAP, prípadne Microsoft Active Directory na autentifikáciu používateľov. Ďalší modul, pam_krb5.so, umožňuje použiť ľubovoľný Kerberos server, napríklad MIT Kerberos, Heimdal Kerberos, prípadne Microsoft Active Directory. My však budeme používať modul pam_winbind.so z balíka libpam-winbind (poskytuje súbor `/lib/x86_64-linux-gnu/security/pam_winbind.so`), ktorý autentifikuje používateľov s využitím radiča domény.

2.9.1 Autentifikačné služby

PAM poskytuje štyri autentifikačné služby: auth, account, password a session. Prvá z nich, auth, umožňuje aplikácii overiť identitu používateľa (napríklad zadaním hesla) a získa poverenia účtu (UID, skupiny, ...). Druhá, account, rieši dostupnosť účtu, ktorá priamo nesúvisí s autentifikáciou. Napríklad obmedzenie na základe času, kedy sa môže používateľ prihlásiť, systémových zdrojov (napríklad maximálny počet používateľov) alebo spôsobu pripojenia (napríklad root sa môže prihlásiť iba na konzole). Tretia, password, umožňuje zmenu hesla (napríklad pri jeho exspirácii alebo z vôle používateľa). Posledná, session, vykonáva úlohy spojené s vytvorením a likvidáciou sedenia ako napríklad logovanie, vytvorenie domovského adresára alebo pripojenie adresárov.

2.9.2 Formát súborov

Adresár `/etc/pam.d` obsahuje textový súbor pre každú aplikáciu, ktorá používa PAM pre autentifikáciu, napríklad `/etc/pam.d/login`. Každý riadok v PAM konfiguračnom súbore má nasledovný formát:

```
1 <group> <control> <module> <params>
```

Význam jednotlivých častí je nasledovný:

<group> určuje jednu z autentifikačných služieb auth, account, password a session
<control> riadi, akým spôsobom sa interpretuje návratová hodnota modulu
<module> určuje modul, ktorý sa má zavolať, napríklad pam_unix.so alebo pam_winbind.so
<params> hodnoty parametrov, ktoré sa odovzdajú modulu, napr.: krb5_ccache_type=FILE

Každá skupina služieb má spravidla niekoľko záznamov. To znamená, že je viac riadkov s rovnakým poľom <group>. PAM spracuje záznamy v poradí, v akom sú uvedené v súbore. Pre ich spracovanie zavolá uvedený modul <module> s parametrami <params>. Modul vráti návratovú hodnotu (success, ignore, ...) a PAM na základe nej a riadiacej časti <control> pokračuje v spracovaní.

V rámci súboru je možné vložiť aj iný súbor pomocou riadku `@include filename`, ktorý akoby vložil súbor s názvom filename namiesto riadku s `@include` a výsledný súbor sa spracuje v takomto tvare.

2.9.2.1 Význam poľa <control>

Riadiaca časť <control> má tvar zoznamu priradení oddelených medzerou:

```
1 [hodnota1=akcia1 hodnota2=akcia2 ...]
```

Ľavá časť priradenia (hodnota) je návratovou hodnotou z modulu. Napríklad: success predstavuje úspešné vykonanie funkcie. Hodnota new_authtok_reqd indikuje, že autentifikácia bola úspešná, ale je požadovaný nový autentifikačný token. Takáto situácia môže nastať napríklad preto, lebo je potrebné zmeniť exspirované heslo. Hodnota ignore znamená, že modul nechce ovplyvňovať výsledok autentifikácie (napr. mohol niečo iba zapísať do logov).

Hodnota default je špeciálna hodnota, ktorá určuje, aká akcia sa má vykonať pre všetky hodnoty, ktoré neboli explicitne uvedené v zozname priradení.

Akcie v poli <control> môžu byť ignore, bad, die, ok, done, N alebo reset. Ich význam je nasledovný:

ignore Znamená, že modul neovplyvní úspešnosť/neúspešnosť celkovej autentifikácie (nezávisle na tom, akú mal návratovú hodnotu).

bad Indikuje, že modul zlyhal. Ak je to prvý modul, ktorý zlyhal, tak jeho stav bude stavom celej autentifikácie. Vyhodnocovanie zostávajúcich modulov pokračuje ďalej.

die Podobné ako bad, len s tým rozdielom, že vyhodnocovanie sa okamžite preruší.

ok Ak predošlý stav bol úspešný, tak návratová hodnota modulu ho prepíše. Ak predošlý stav bolo zlyhanie, tak sa tento stav nezmení. Vyhodnocovanie zostávajúcich modulov pokračuje ďalej.

done Podobné ako ok, len s tým rozdielom, že vyhodnocovanie sa okamžite preruší.

N predstavuje prirodzené číslo > 0. Jeho význam je podobný ok, len s tým rozdielom, že pred vyhodnocovaním zostávajúcich modulov sa preskočí nasledujúcich N modulov.

reset Zahodí aktuálny stav a začne s ďalším modulom s čistým stavom.

Keďže niektoré zoznamy kombinácií hodnota=akcia sa často vyskytujú, tak je pre ne aj skrátený zápis v podobe riadiaceho kľúčového slova. Poznáme nasledovné riadiace slová:

required [success=ok new_authtok_reqd=ok ignore=ignore default=bad]
Ak modul uspeje, PAM pokračuje vyhodnocovaním zostávajúcich záznamov. Výsledok bude určený výsledkom ostatných modulov. Ak modul zlyhá, tak PAM pokračuje vo vyhodnocovaní, ale výsledkom bude zlyhanie.

requisite [success=ok new_authtok_reqd=ok ignore=ignore default=die]
Ak modul uspeje, PAM pokračuje vyhodnocovaním zostávajúcich záznamov. Výsledok bude určený výsledkom ostatných modulov. Ak modul zlyhá, tak PAM zastaví vyhodnocovanie a výsledkom bude zlyhanie. Použiteľné napríklad na ochranu pred zadaním hesla cez nezabezpečené médium.

sufficient [success=done new_authtok_reqd=done default=ignore]
Ak modul uspeje, tak PAM zastaví vyhodnocovanie a vráti úspech (ale len ak žiadny predchádzajúci required modul nezlyhal). Ak modul zlyhá, tak PAM pokračuje vo vyhodnocovaní. Výsledok bude určený výsledkom ostatných modulov.

optional [success=ok new_authtok_reqd=ok default=ignore]
PAM ignoruje výsledok modulu, okrem prípadu ak ide o jediný modul v skupine.

2.9.3 Konfigurácia PAM

Najprv treba nainštalovať balíky `winbind` a `libpam-winbind`:

```
1 tester@linwo:~$ sudo apt install winbind libpam-winbind
```

Po ich nainštalovaní sa na Ubuntu 20.04 automaticky vhodne nakonfiguruje ich integrácia do PAM. Pokiaľ by táto integrácia z akýchkoľvek dôvodov neprebehla, tak je ju možné vykonať ručne nasledovnými úpravami PAM konfiguračných súborov v priečinku `/etc/pam.d`. V súbore `common-auth` je potrebné nahradiť riadok:

```
auth        [success=1 default=ignore]        pam_unix.so nullok_secure
```

nasledovnými dvomi riadkami:

```
auth        [success=2 default=ignore]        pam_unix.so nullok_secure
auth        [success=1 default=ignore]        pam_winbind.so krb5_auth
    krb5_ccache_type=FILE cached_login try_first_pass
```

Táto zmena zabezpečí, že pokiaľ modul pam_unix nedokáže používateľa autentifikovať (lebo to nie je štandardný lokálny používateľ), tak sa pokúsime o jeho autentifikáciu v doméne pomocou modulu pam_winbind.so. Ako ďalší krok treba v súbore `common-account` nahradiť riadok:

```
account [success=1 new_authtok_reqd=done default=ignore] pam_unix.so
```

nasledovnými dvomi riadkami:

```
account [success=2 new_authtok_reqd=done default=ignore] pam_unix.so
account [success=1 new_authtok_reqd=done default=ignore] pam_winbind.so
```

Táto zmena zabezpečí, že v prípade, že používateľ nie je lokálny, tak sa PAM obráti cez winbind na radič domény. V súbore `common-password` treba zmeniť riadok:

```
password [success=1 default=ignore] pam_unix.so    obscure sha512
```

na nasledovné dva riadky:

```
password [success=2 default=ignore] pam_unix.so    obscure sha512
password [success=1 default=ignore] pam_winbind.so try_authtok[5] try_first_pass
```

Táto zmena umožní zmenu hesla nie len lokálnym používateľom (cez pam_unix.so), ale aj používateľom z domény (cez pam_winbind.so). V súbore `common-session` a v súbore `common-session-noninteractive` je potrebné za riadok:

```
session        required                        pam_unix.so
```

vložiť nový riadok:

```
session        optional                        pam_winbind.so
```

2.9.4 Automatické vytvorenie domovského adresára

Keď sa do Linuxu prihlási používateľ, systém očakáva, že už bude mať vytvorený domovský adresár. Keďže používateľov vytvárame v AD, Linux automaticky nevytvorí ich domovské adresáre pri ich pridaní do domény. Našťastie, PAM je možné nakonfigurovať tak, aby domovský adresár vytvoril ako súčasť prípravy sedenia pri prvom prihlásení. V súbore `/etc/pam.d/common-session` za riadok:

[5] Pre správnu činnosť tohto modulu pri zmene hesla, je v Ubuntu potrebné parameter try_authtok vynechať. Pozri podčast 2.17.2 na strane 32.

```
session optional pam_umask.so
```

je treba pridať riadok:

```
session optional pam_mkhomedir.so skel=/etc/skel
```

Tento riadok zabezpečí vytvorenie domovského adresára (pokiaľ už neexistuje), pričom sa použije vzor (kostra, skeleton) z adresára `/etc/skel`.

Automatické vytvorenie domovského adresára nie je súčasťou štandardnej inštalácie v operačnom systéme Ubuntu 20.04. Preto, na rozdiel od predošlej časti, je potrebné ho nakonfigurovať ručne.

2.10 Linux NSS

Name Service Switch (NSS) poskytuje programové rozhranie pre získanie informácií o používateľoch, skupinách, službách (mapovanie názvu služby na port/protokol) a podobne. Spája rôzne zdroje do jedného zdroja a zároveň skrýva ich špecifiká pred aplikáciou, ktorá chce pristupovať k týmto údajom.

Ako príklady zdrojov možno uviesť zdroj „files“ (`/lib/x86_64-linux-gnu/libnss_files.so.2`) alebo zdroj „winbind“ (`/lib/x86_64-linux-gnu/libnss_winbind.so.2`), ktorý treba nainštalovať zadaním:

```
tester@linwo:~$ sudo apt install libnss-winbind
```

NSS poskytuje správcom ľahko konfigurovateľný spôsob poprepájania rôznych zdrojov informácií cez modifikáciu konfiguračného súboru `/etc/nsswitch.conf`. Špeciálne nás zaujíma konfigurácia spôsobov získavania informácie o používateľoch a skupinách.

2.10.1 Konfigurácia NSS

Potrebujeme NSS nastaviť tak, aby aplikácie vyhľadávali informácie o používateľoch a skupinách v Active Directory použitím winbind. Preto musíme do konfiguračného súboru NSS (`/etc/nsswitch.conf`) pridať modul winbind:

```
passwd:         files systemd winbind
group:          files systemd winbind
```

Ostatné riadky v súbore necháme nezmenené.

2.11 Interná reprezentácia objektov

Na platforme Microsoft Windows sa pre internú reprezentáciu objektov používa Security Identifier (SID). Je to štruktúra s premenlivou dĺžkou. SID obsahuje aj jednoznačný identifikátor domény, v ktorej sa objekt nachádza. Preto Windows môže rozlíšiť objekty z rôznych domén a SID je jednoznačný identifikátor objektu aj medzi doménami.

Na platforme Unix sa používa jednoduchšia schéma. Každý objekt má svoj identifikátor, ktorým je 32-bitové celé číslo. Tento identifikátor je jednoznačný iba v rámci jedného počítača. Preto nič nezaručuje, že používateľ s User ID (UID) 1234 na jednom počítači má také isté UID aj na druhom počítači. Navyše na druhom počítači môže mať pridelené UID 1234 úplne iný používateľ.

2.12 winbind: Mapovanie SID na Unix ID

Vzhľadom na rôznu štruktúru SID a UID nie je možné použiť SID ako UID. Preto winbind poskytuje mapovanie SID na Unix ID ako jednu zo svojich služieb. Toto mapovanie môže robiť pomocou rôznych „backend“-ov. Najčastejšie používané sú asi nasledovné tri: idmap_tdb, idmap_rid a idmap_ad, ktoré si bližšie popíšeme. Odporúčame použiť idmap_ad a ako záložné riešenie používať idmap_tdb.

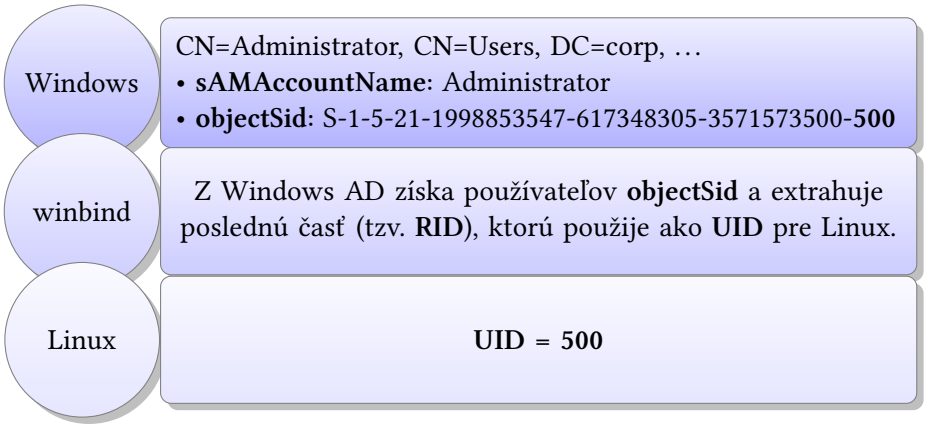
2.12.1 idmap_tdb

Mapovanie idmap_tdb interne vytvára a udržiava mapovanie SID na UID. Má pridelený rozsah Unix identifikátorov, na ktoré môže mapovať jednotlivé externé SID. Postupne, ako winbind vyhľadáva používateľov a skupiny v doméne, tak ich táto metóda mapuje na ďalší (zatiaľ nepoužitý) Unix ID z prideleného rozsahu a ukladá toto mapovanie do tdb databázy. Mapovanie sa vykonáva v poradí, v akom prichádzajú požiadavky na identifikáciu externých objektov. Okrem požiadavky na konkrétny objekt, môže prísť aj požiadavka na vymenovanie všetkých objektov (napríklad používateľov). Pri vykonaní tejto požiadavky prebehne namapovanie všetkých objektov (napríklad používateľov).

Toto riešenie je jednoduché a automatické, ale má svoje nedostatky. Jediné miesto, kde je mapovanie uložené, je tdb databáza. Ak sa táto databáza poškodí alebo zmaže, tak sa už nedá zrekonštruovať mapovanie SID na Unix ID. Ďalšou nevýhodou je, že na rôznych počítačoch veľmi pravdepodobne vzniknú rôzne mapovania. To môže spôsobovať problémy, napríklad pokiaľ tieto počítače zdieľajú časť svojich súborových systémov, pretože externý počítač bude interpretovať UID podľa svojej internej tdb databázy. To môže spôsobiť napríklad vypisovanie nekorektných vlastníkov súborov a nesprávne interpretovanie prístupových práv.

2.12.2 idmap_rid

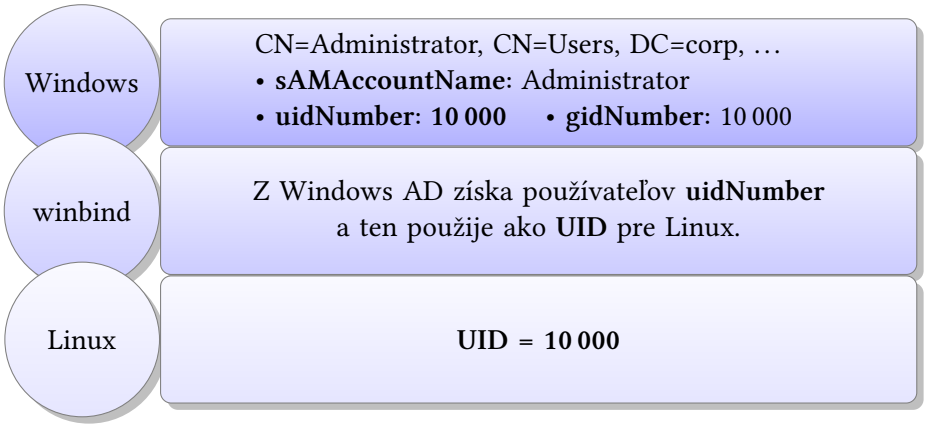
Winbind označuje stratégiu idmap_rid ako „RID mapping“. Pripomeňme si, že posledná časť SID, ktorá jednoznačne určuje objekt v rámci domény, sa nazýva „Relative Identifier“ (RID). RID je 32-bitové celé číslo (ako všetky „SubAuthority“ záznamy v reťazci). Pri tomto mapovaní sa vychádza z toho, že Unix ID je tiež 32-bitové číslo a preto je možné RID mapovať priamo na SID.



Toto riešenie je ale nepoužiteľné pre prostredie s viacerými doménami. V tomto prípade totiž môžu mať dvaja používatelia s rôznym SID rovnaké RID. Ďalším problémom je, že RID nie je možné na danom počítači mapovať priamo na rovnaké Unix ID, lebo toto ID už môže byť obsadené (napríklad lokálnym používateľom). Preto je pri tomto mapovaní vhodné špecifikovať rozsah, ktorý bude pre mapovanie RID rezervovaný. Pokiaľ sa objaví RID mimo rezervovaný rozsah, tak sa toto mapovanie nepoužije. Preto je dôležité mať aj záložné mapovanie, ktoré by sa mohlo použiť v takomto prípade. Štandardne sa na tento účel používa mapovanie idmap_tdb.

2.12.3 idmap_ad

Winbind označuje idmap_ad ako „Active Directory ID mapping“. Pri tomto mapovaní sa pre každého používateľa a skupinu uloží jeho Unix ID v prislúchajúcom objekte v Active Directory. Keď winbind autentifikuje používateľa, vyhľadá jeho Unix ID v AD a poskytne ho Linuxu ako interný identifikátor.



Nevýhodou tohto riešenia je, že je nutné toto mapovanie v AD udržiavať a zaručiť, že je v celom lese jednoznačné. Aj pri tomto mapovaní sa špecifikuje rozsah, ktorý sa používa ako filter. Pokiaľ je identifikátor z Active Directory mimo tento rozsah alebo sa vôbec nenájde,

tak sa toto mapovanie nepoužije. Preto opätovne treba mať pripravené záložné mapovanie. Štandardne sa na tento účel používa mapovanie idmap_tdb. Týmto spôsobom sa Linuxový systém chráni pred chybnými údajmi v AD (napríklad, ak by niekto zadal ako uidNumber pre niektorého používateľa číslo 0).

2.13 Identity Management for UNIX

„Identity Management for UNIX“ obsahuje sadu nástrojov pre synchronizáciu hesiel, integráciu NIS (Network Information Service) a rozšírenie Active Directory o RFC 2307[6] atribúty a používateľské rozhranie pre ich správu. Toto rozšírenie bolo potrebné pre staršie verzie Windows Servera. Napríklad Windows Server 2012 R2 tieto atribúty už priamo obsahuje a samotná inštalácia „Identity Management for UNIX“ sa preto vytratila z grafických sprievodcov tohto operačného systému.

2.13.1 Windows Server 2012 R2

My inštalujeme Identity Management for UNIX jedine z dôvodu príjemnejšieho používateľského rozhrania na správu UNIX-ových atribútov. Toto rozhranie je možné nainštalovať na Windows Server 2012 použitím DSIM (Deployment Image Servicing and Management tool), ktorý sa spúšťa z príkazového riadku pod právami správcu nasledovne:

```
PS> DISM /Online /Enable-Feature /FeatureName:adminui /All
Deployment Image Servicing and Management tool
Version: 6...
Image Version: 6...
Enabling feature(s)
[==========================100.0%==========================]
The operation completed successfully.
Restart Windows to complete this operation.
Do you want to restart the computer now? (Y/N)
```

Význam jednotlivých parameterov:

/Online určuje, že cieľom je bežiaci operačný systém,
/Enable-Feature povolí špecifikovanú vlastnosť v obraze,
/All povolí aj všetky nadradené vlastnosti k uvedenej vlastnosti.

Ak chceme, aby sa v nástroji ADUC (pri zobrazení vlastností používateľov alebo skupín) pridala záložka „UNIX Attributes“, tak treba nainštalovať aj „Server for NIS“:

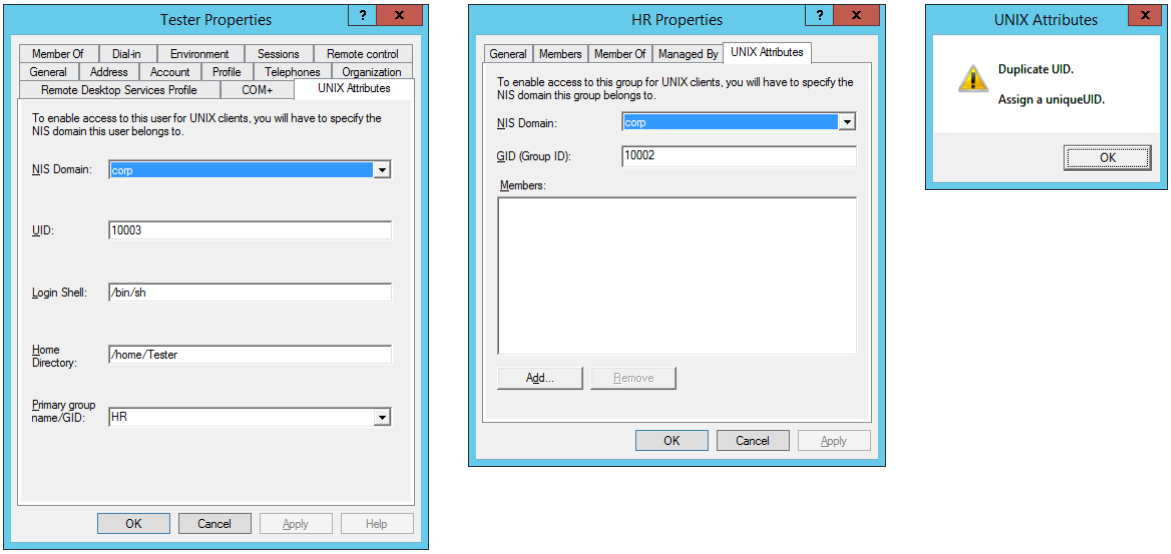
```
PS> DISM /Online /Enable-Feature /FeatureName:nis /All
```

Synchronizáciu hesiel (password synchronization) možno nainštalovať pomocou príkazu:

```
PS> DISM /Online /Enable-Feature /FeatureName:psync /All
```

Túto časť ale netreba inštalovať, pretože pre zobrazenie UI ju netreba. Heslá meníme cez winbind priamo pomocou RPC volaní. Nainštalované používateľské rozhranie pre správu UNIX-ových atribútov je zobrazené na obrázku 2.9.

[6] RFC 2307: An Approach for Using LDAP as a Network Information Service



Obr. 2.9: Záložka UNIX Attributes zo „Server for NIS“

Okrem (pre niektorých používateľov príjemnejšieho) grafického prostredia, systém aj automaticky generuje nové Unix ID pre nových používateľov/skupiny. V prípade ručnej zmeny automaticky kontroluje duplicitu Unix ID. Umožňuje nastaviť primárnu skupinu pre používateľa. Dá sa vybrať zo skupín s prideleným GID (group ID). Okrem toho je možné nastaviť aj domovský adresár a login shell.

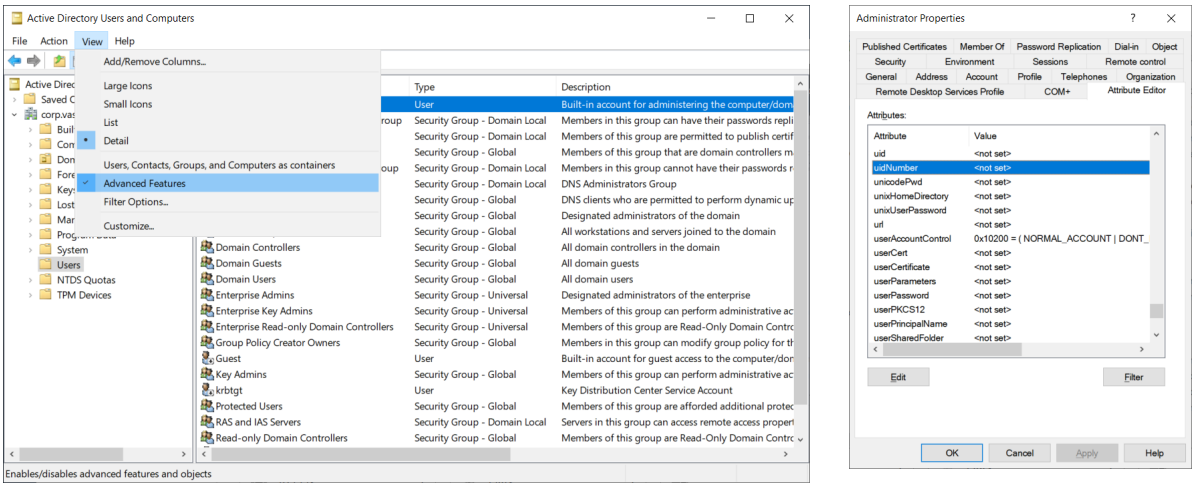
2.13.2 Windows Server 2016 a vyššie

Windows 10 a Windows Server 2016 (a vyššie) nepodporujú rozšírenie „Server for NIS“. Bez tejto funkcie „Active Directory User and Computer“ (ADUC) nezobrazuje záložku „Unix Attributes“ pre používateľov a skupiny. Táto situácia sa dá vyriešiť manuálnym nastavením potrebných atribútov v Active Directory (AD). Mapovanie položiek zo záložky na atribúty je uvedené v nasledovnej tabuľke:

Položka na záložke „Unix Attributes“	**Zodpovedajúci atribút v Active Directory**
NIS Domain	msSFU30NisDomain
UID	uidNumber
Logon Shell	loginShell
Home Directory	unixHomeDirectory
Primary group name/GID	primaryGroupID
GID (Group ID)	gidNumber

Aby sme získali k týmto atribútom prístup, tak musíme najprv aktivovať novú záložku „Attribute Editor“ vo vlastnostiach používateľov a skupín. Jej zobrazenie docielime zaškrtnutím voľby „View ▸ Advanced Features“ v ADUC. Potom môžeme v ADUC ručne vybrať používateľa (napríklad Administrator) a z jeho kontextového menu zvoliť „Properties“. Zo-

brazí sa okno „Administrator Properties“ už aj s novou záložkou „Attribute Editor“ (pozri obrázok 2.10 na strane 28). Následne v zobrazenom zozname atribútov treba vyhľadať atribúty z tabuľky vyššie a nastaviť im požadované hodnoty. Nevýhodou je, že okrem toho, že musíme ručne nastavovať UID a GID, tak si tiež musíme sami pamätať naposledy použité UID a GID a aj sami garantovať ich jednoznačnosť.



Obr. 2.10: Aktivovanie pokročilých nastavení v ADUC

Pokiaľ nechceme zadávať paremetre pre používateľa `ric` ručne, je možné dosiahnuť rovnakého efektu aj nasledovnými PowerShell príkazmi:

```
PS> $u = Get-ADUser -Filter "Name -eq 'ric'" -Properties *
PS> $u.msSFU30NisDomain = "CORP"
PS> $u.uidNumber = 10000
PS> $u.loginShell = "/bin/bash"
PS> $u.unixHomeDirectory = "/home/CORP/ric"
PS> $u.primaryGroupID = 513 # RID pre Domain Users
PS> Set-ADUser -Instance $u
```

```
PS> $g = Get-ADGroup -Filter "Name -eq 'Domain Users'" -Properties *
PS> $g.msSFU30NisDomain = "CORP"
PS> $g.gidNumber = 10000
PS> Set-ADGroup -Instance $g
```

2.14 Samba – konfigurácia

Na záver konfigurácie Linuxového počítača treba ešte nastaviť samotnú Sambu pomocou jej konfiguračného súboru `/etc/samba/smb.conf`. Všetky nastavenia, ktoré popisujeme, treba uviesť v prvej časti označenej ako `[global]`. Táto časť obsahuje globálne nastavenia. Za ňou nasledujú časti pre jednotlivé zdieľané priečinky. Týmito časťami sa teraz nebudeme zaoberať. V globálnej časti treba pridať (alebo zmeniť ak už existujú) nasledovné parametre:

```
workgroup = CORP
realm = CORP.VASAORG.SK
security = ADS
```

Týmto sa zaručí, že Samba sa správa ako člen domény vo vyššie uvedenej oblasti (realm).

```
server role = member server
```

Nastaví overovanie používateľov cez ADS. Server ale najprv musí byť pridaný do domény.

```
winbind enum users = yes
winbind enum groups = yes
```

Hodnota „no“ by zakázala vymenovanie (enumerovanie) všetkých používateľov, respektíve skupín. Vypnutie enumerovania môže byť vhodné pre veľké systémy s veľkým počtom používateľov a skupín.

```
winbind nss info = rfc2307
```

Toto nastavenie informuje Sambu, že adresárový server používa rozšírenú schému pre ukladanie informácií potrebných pre Linux.

```
template homedir = /home/%D/%U
template shell = /bin/bash
```

Pokiaľ by sa v adresárovej službe aj tak nenašiel údaj špecifikujúci domovský adresár alebo login shell, tak štandardný domovský adresár bude `/home/domena/pouzivatel` a shell bude `/bin/bash`.

```
idmap cache time = 1
idmap negative cache time = 1
winbind cache time = 1
```

Pre naše testovanie chceme rýchlu reakciu na zmenu údajov v AD, preto ich budeme ukladať do medzipamäte (cache) len na jednu sekundu.

```
idmap config * : backend = tdb
idmap config * : range = 1000000-1999999
```

Tento preddefinovaný (`*`) spôsob mapovania identifikátorov slúži ako záložný mapovací spôsob, pokiaľ sa nedá aplikovať nasledovný:

```
idmap config CORP : backend  = ad
idmap config CORP : range = 10000-999999
```

V tomto prípade `range` pracuje ako filter. To znamená, že ak je ID v AD mimo rozsah filtra, tak je toto mapovanie ignorované a nepoužije sa. Za takýchto okolností sa na mapovanie použije tdb. Zmyslom tohto opatrenia je ochrana pred nechceným prekryvom medzi lokálnymi a vzdialenými identifikátormi.

```
idmap config CORP : schema_mode = rfc2307
```

Určuje schému, ktorú idmap_ad použije pri vyhľadávaní informácií o používateľoch a skupinách v AD. Môže byť použitá aj staršia schéma sfu (Windows Services for UNIX).

Skontrolovať korektnosť upraveného `smb.conf` súboru je možné príkazom:

```
tester@linwo:~$ testparm
Load smb config files from /etc/samba/smb.conf
Loaded services file OK.
Server role: ROLE_DOMAIN_MEMBER

Press enter to see a dump of your service definitions
```

```
7
8  # Global parameters
9  [global]
10         idmap cache time = 1
11         idmap negative cache time = 1
12 ...
```

2.15 Pridanie Linuxového počítača do domény

Po vykonaní všetkých vyššie uvedených nastavení zostáva iba pridanie Linuxového počítača do domény. Samotné pridanie je jednoduché a vykoná sa nasledovným príkazom:

```
1 ester@linwo:~$ sudo net ads join -U Administrator
2 Enter Administrator's password:
3 Using short domain name -- CORP
4 Joined 'LINWO' to dns domain 'corp.vasaorg.sk'
```

Po pridaní počítača do domény je ešte potrebné reštartnúť službu winbind:

```
1 tester@linwo:~$ sudo systemctl restart winbind
```

2.16 Používanie domény

Po pridaní počítača do domény a spustení služby winbind môžeme vyskúšať nástroje, ktoré nám nainštalované balíky ponúkajú pre prácu s doménou.

```
1 tester@linwo:~$ wbinfo --ping-dc
2 checking the NETLOGON for domain[CORP] dc connection to
    ↪"winse.corp.vasaorg.sk" succeeded
```

Vypísať zoznam používateľov domény môžeme pomocou nasledovného príkazu:

```
1 tester@linwo:~$ wbinfo -u
2 CORP\administrator
3 CORP\guest
4 CORP\krbtgt
5 CORP\ric
```

Obdobne zoznam skupín v doméne získame príkazom:

```
1 tester@linwo:~$ wbinfo -g
2 CORP\domain computers
3 CORP\domain controllers
4 CORP\schema admins
5 CORP\enterprise admins
6 CORP\cert publishers
7 CORP\domain admins
8 CORP\domain users
9 CORP\domain guests
10 ...
```

Teraz môžeme overiť integráciu viacerých zdrojov informácií o používateľoch (podľa konfigurácie v NSS) zadaním príkazu:

```
1 tester@linwo:~$ getent passwd
2 root:x:0:0:root:/root:/bin/bash
3 ...
```

```
tester:x:1000:1000:Tester,,,:/home/tester:/bin/bash
CORP\ric:*:10000:10000::/home/CORP/ric:/bin/bash
→ CORP\ric:*:10002:10001:Richard Ostertag:/home/ric:/bin/sh
```

Vidíme, že sme dostali jeden zoznam, ktorý obsahuje lokálnych používateľov (tester, UID:1000), ako aj doménových používateľov (`CORP\ric`, UID: 10000).

2.17 Prihlásenie používateľa z AD

Na záver vyskúšame prihlásenie používateľa z domény na Linuxový počítač. Používateľ `ric` z domény `CORP` sa prihlási na `localhost` pomocou príkazu[7]:

```
tester@linwo:~$ sudo apt install openssh-server
tester@linwo:~$ ssh CORP\\ric@localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:....
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
CORP\ric@localhost's password:
Creating directory '/home/CORP/ric'.
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.8.0-48-generic x86_64)
...
```

Používateľ sa po zadaní hesla úspešne prihlásil a systém mu aj automaticky vytvoril domovský adresár podľa nastavenia v AD. Pri vypísaní obsahu domovského adresára vidno, že vytvorené súbory majú správneho vlastníka a že systém pozná mapovanie identifikátorov aj pre doménových používateľov a skupiny (ako napríklad `CORP\domain users`).

```
CORP\ric@linwo:~$ ls -la
total 32
drwxr-xr-x 5 CORP\ric CORP\domain users 4096 mar 24 09:22 .
drwxr-xr-x 3 root     root              4096 mar 24 09:22 ..
-rw-r--r-- 1 CORP\ric CORP\domain users  220 mar 24 09:22 .bash_logout
-rw-r--r-- 1 CORP\ric CORP\domain users 3771 mar 24 09:22 .bashrc
drwxr-xr-x 4 CORP\ric CORP\domain users 4096 mar 24 09:22 .cache
drwx------ 4 CORP\ric CORP\domain users 4096 mar 24 09:22 .config
drwxr-xr-x 3 CORP\ric CORP\domain users 4096 mar 24 09:22 .local
-rw-r--r-- 1 CORP\ric CORP\domain users  807 mar 24 09:22 .profile
```

Správnosť mapovania môžeme overiť aj príkazom `id` a `pwd`:

```
CORP\ric@linwo:~$ id
uid=10000(CORP\ric) gid=10000(CORP\domain users) groups=10000(CORP\domain users)
CORP\ric@linwo:~$ pwd
/home/CORP/ric
```

2.17.1 Autentifikácia cez AD pre smbclient

Aj keď sme prihlásení na Linuxový počítač ako doménový používateľ, tak po zadaní príkazu:

```
CORP\ric@linwo:~$ smbclient //winse/C$
Enter ric@CORP.VASAORG.SK's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
```

[7] Symbol \ treba pre shell zapísať ako \\.

vidíme, že systém vyžaduje opätovné zadanie hesla. To ale nie je nutné, pokiaľ použijeme doménový Kerberos protokol pre autentifikáciu. V takomto prípade získame rovnaké výhody jediného prihlásenia, ako majú aj používatelia Windows v doméne. Pripojenie s použitím Kerberos autentifikácie vyžaduje pri príkaze smbclient zadanie parametra `--kerberos`:

```
CORP\ric@linwo:~$ smbclient --kerberos //winse/C$
tree connect failed: NT_STATUS_ACCESS_DENIED
```

Z výpisu vidíme, že spojenie by sa úspešne nadviazalo aj bez zadania hesla. Ale aby sme sa mohli pripojiť aj keď nie sme Administrator, tak si najprv vytvoríme na serveri zdieľaný adresár users:

```
CORP\ric@linwo:~$ smbclient --kerberos //winse/users
Domain=[CORP] OS=[Windows Server ...] Server=[Windows Server ...]
smb: \>
```

2.17.2 Zmena hesla v AD

Z dobre nakonfigurovaného Linuxového počítača pridaného do domény si môžu doménový používatelia zmeniť aj svoje doménové heslo pomocou štandardného príkazu `passwd`:

```
CORP\ric@linwo:~$ passwd
Changing password for CORP\ric
(current) NT password:
Enter new NT password:
Retype new NT password:
passwd: Authentication token manipulation error
passwd: password unchanged
```

Ako vidno z výpisu vyššie, tak zmena skončila chybou. Pre korektnú činnosť zmeny hesla je nutné zo štandardnej konfigurácie vytvorenej na systéme Ubuntu 20.04 odstrániť parameter try_authtok[8] v súbore `/etc/pam.d/common-password` na nasledovnom riadku[9]:

```
password  [success=1 default=ignore]  pam_winbind.so  try_authtok try_first_pass
```

Podľa dokumentácie je zmysel parametra use_authtok v tom, že nastaví nové heslo na heslo poskytnuté predošlým password modulom. Parameter try_authtok robí to isté, ale ak nie je heslo platné, tak sa predsa len znovu opýta. Táto voľba bolo použitá preto, aby používateľ nemusel po zlyhaní modulu pam_unix.so zadávať heslo ešte raz. V skutočnosti systém s týmto parametrom pri zmene hesla zlyhá. Po jeho odstránení sa systém správa korektne:

```
CORP\ric@linwo:~$ passwd
Changing password for CORP\ric
(current) NT password:
Enter new NT password:
Retype new NT password:
passwd: password updated successfully
```

[8] Zo starších verzií Ubuntu je potrebné odstrániť use_authtok.

[9] Po zmene riadku v konfiguračnom súbore sú zmeny okamžite aktívne (bez reštartovania).

Kapitola 3

Samba 4 ako Linuxový radič domény

Druhý problém, ktorého riešenie si popíšeme, je nasadenie adresárových služieb na počítač s operačným systémom Linux. Prezentované riešenie umožní používať Linuxový server ako radič domény. Tento radič domény môžu použiť ako Linuxoví, tak aj Windowsoví používatelia. Obom skupinám umožní prihlásenie na základe údajov spravovaných centrálne týmto radičom domény. Tento Linuxový server je možné administrovať jednak pomocou Linuxových, ale čo je možno ešte zaujímavejšie, aj pomocou klasických Windowsových nástrojov. Pri popise spôsobu pripojenia sa zameriame na Windowsových používateľov (pripájajúcich sa k doméne). Riešenie pre Linuxových používateľov je rovnaké ako v predošlej časti, keď používali radič domény postavený na operačnom systéme Windows.

3.1 Konfigurácia siete

Najprv musíme na Linuxovom serveri (Ubuntu 20.04) vykonať základnú konfiguráciu siete. Potrebný postup sme už podrobnejšie popísali v časti 2.7 na strane 17. Do adresára `/etc/netplan` treba pridať súbor s názvom `02-static-ip.yaml` s nasledovným obsahom (následne obsah možno otestovať príkazom `sudo netplan try`) a zmeny aplikujeme príkazom `sudo netplan apply`:

```
network:
  version: 2
  ethernets:
    ens33: # aktuálny názov sa dá zistiť napríklad pomocou: ip link
      dhcp4: false
      addresses: [172.22.222.11/16]
      gateway4: 172.22.0.1
      nameservers:
        search: [corp.vasaorg.sk]
        addresses: [172.22.0.1]
```

Ďalej nastavíme meno Linuxového servera na linse (ako LINux SErver). Preto zmeníme obsah súboru `/etc/hostname` na linse a v súbore `/etc/hosts` nahradíme riadok so starým menom (začína IP adresou 127.0.1.1) týmto riadkom:

```
172.22.222.11  linse.corp.vasaorg.sk linse
```

Pretože Samba AD DC používa vlastný DNS server, ktorý potrebuje mať voľný port 53, tak potrebujeme zastaviť a následne deaktivovať službu systemd-resolved:

```
tester@linse:~$ sudo systemctl stop systemd-resolved
tester@linse:~$ sudo systemctl disable systemd-resolved
Removed /etc/systemd/system/dbus-org.freedesktop.resolve1.service.
Removed /etc/systemd/system/multi-user.target.wants/systemd-resolved.service.
```

Keďže `/etc/resolv.conf` je len symbolickou linkou na súbor `/run/systemd/resolve/stub-resolv.conf`, tak túto linku zmažeme:

```
tester@linse:~$ sudo rm /etc/resolv.conf
```

Potom vytvoríme nový súbor `/etc/resolv.conf` s nasledovným obsahom:

```
domain corp.vasaorg.sk
search corp.vasaorg.sk
nameserver 172.22.0.1
```

3.2 Odporúčania pre Samba AD DC

Pri väčšom počte používateľov sa odporúča prevádzkovať viac radičov domény, aby sa zabránilo znefunkčneniu domény pri výpadku jediného servera. Pokiaľ sa bude v sieti používať aj súborový server postavený na platforme Linux, odporúča sa prevádzkovať súborový server ako samostatný členský server (nie priamo na AD DC). Oddelenie umožňuje aktualizovať radič domény a súborový server samostatne bez narušenia činnosti druhého servera. Taktiež sa vyhneme problémom s winbind integrovaným v radiči domény. Samba má svoju vlastnú implementáciu Kerberos a LDAP servera. Neodporúča sa používanie externých implementácií týchto serverov spolu so Sambou.

3.3 Základná inštalácia

Tam, kde budú umiestnené zdieľané priečinky (`/var/lib/samba/sysvol`), je potrebné použiť súborový systém s podporou rozšírených atribútov (pre uloženie NTFS práv, DOS atribútov a Posix ACL). Prítomnosť podpory rozšírených atribútov v jadre Linuxu je možné overiť pomocou príkazu:

```
tester@linse:~$ cat /boot/config-5.4.0-70-generic | grep "EXT._FS_"
```

Výsledkom by mal byť zoznam obsahujúci nasledovné voľby:

```
CONFIG_EXT4_FS_XATTR=y      # nemusí byť (pozri text nižšie)
CONFIG_EXT4_FS_POSIX_ACL=y
CONFIG_EXT4_FS_SECURITY=y
```

V jadrách Linuxu od verzie 3.8 je voľba CONFIG_EXT4_FS_XATTR odstránená a podpora XATTR je automaticky prítomná. V tomto prípade je v poriadku, ak nebude táto voľba vypísaná. Ak sa používa jadro, v ktorom chýba podpora pre niektoré z uvedených volieb, je potrebné získať jadro s ich podporou (napríklad prekompilovaním). Ubuntu od verzie 14.10 štandardne obsahuje podporu všetkých týchto volieb.

Ďalej sa treba uistiť, že v súbore `/etc/fstab` sú pri správnom súborovom systéme prítomné atribúty user_xattr, acl a barrier=1. Namiesto barrier=1 stačí aj samotné barrier. Súborový systém ext4 nemá od verzie 3.2 jadra Linuxu atribúty user_xattr a acl. Tieto sú štandardne povolené. Na ich zakázanie je možné použiť atribúty nouser_xattr a noacl. Tieto by sa teda pri vybranom súborovom systéme nemali nachádzať. Taktiež barrier je štandardne pri ext4 zapnuté (na rozdiel od ext3). Tento atribút zaistí, že tdb transakcie zvládnu aj neočakávaný výpadok napájania.

Pre prácu s Kerberos serverom bežiacom na AD DC potrebujeme nainštalovať používateľské nástroje kerberosu (ako napríklad `kinit`, či `klist`) pomocou príkazu:

```
tester@linse:~$ sudo apt install krb5-user
```

Počas inštalácie odpovieme na nasledovné tri otázky:

```
Default Kerberos version 5 realm: CORP.VASAORG.SK
Kerberos servers for your realm: linse.corp.vasaorg.sk
Administrative server for your Kerberos realm: linse.corp.vasaorg.sk
```

Inštalačný program na základe odpovedí na tieto tri otázky vytvorí nižšie uvedený obsah konfiguračného súboru `/etc/krb5.conf`:

```
[libdefaults]
    default_realm = CORP.VASAORG.SK

[realms]
    CORP.VASAORG.SK = {
        kdc = linse.corp.vasaorg.sk
        admin_server = linse.corp.vasaorg.sk
    }
```

Správna konfigurácia Kerberosu v tomto okamihu nie je zásadná, pretože neskôr, počas konfigurácie Samba radiča domény, vznikne konfiguračný súbor aj pre Kerberos, ktorým prepíšeme v tomto bode vytvorenú konfiguráciu. Na záver nasleduje inštalácia samotného balíka samba (momentálne je v Ubuntu 20.04 samba vo verzii 4.11.6):

```
tester@linse:~$ sudo apt install samba
...
Samba is not being run as an AD Domain Controller: Masking samba-ad-dc.service
...
Failed to preset unit: Unit file /etc/systemd/system/samba-ad-dc.service is
↪masked.
...
samba-ad-dc.service is a disabled or a static unit, not starting it.
...
```

Vybrané správy uvedené vyššie by mohli vzbudzovať znepokojenie, ale je to očakávané správanie, vzhľadom na skutočnosť, že sme ešte nenastavili sambu do role doménového radiča.

3.4 Zriadenie domény (DCPROMO)

Nainštalovanie balíku samba ešte nevytvorí samotnú doménu. Za týmto účelom môžeme použiť príkaz `samba-tool`, ktorý okrem iného vie vytvoriť základnú konfiguráciu domény, vrátane základnej Active Directory databázy. Ak už súbor `/etc/samba/smb.conf` existuje,

treba ho najprv zmazať. Inak ho `samba-tool` neprepíše a nevytvorí sa nová konfigurácia zohľadňujúca zadané parametre. Vytvorenie domény spustíme nasledovným príkazom:

```
tester@linse:~$ sudo samba-tool domain provision --use-rfc2307 --interactive
↪--option="interfaces=lo ens33" --option="bind interfaces only=yes"
↪--function-level=2008_R2
```

Parameter `--use-rfc2307` povolí použitie RFC 2307 (An Approach for Using LDAP as a Network Information Service), čím sa do schémy AD doplní rozšírenie o atribúty potrebné pre správu Unixových účtov (ako napríklad uidNumber). Bez tohto parametra sa tieto atribúty nepridajú.

Parameter `--interactive` hovorí, že `samba-tool` sa bude interaktívne pýtať na hodnoty potrebných parametrov. Preddefinované hodnoty budú ponúknuté v hranatých zátvorkách. Pre ich použitie stačí stlačiť klávesu Enter.

Minimálnu funkčnú úroveň domény a celého lesa je možné zvoliť z nasledovných možností: 2000, 2003, 2008 a 2008_R2. Preddefinovaná hodnota je 2003. Nastaviť inú hodnotu je možné pomocou parametra `--function-level`.

Parameter `--site=SITENAME` nastaví meno fyzickej lokality. Túto možnosť, podobne ako pri Windows serveri, ponechávame na štandardnej hodnote (Default-First-Site-Name).

Posledným spomínaným parametrom je parameter `--option=OPTION`. Pomocou neho je možné pridať zadanú `OPTION` priamo do konfiguračného súboru `smb.conf`. V našom príklade pridávame dve voľby `interfaces=lo eth0` a `bind interfaces only=yes`. Tým sa obmedzia rozhrania, kde bude Samba počúvať. To je vhodné napríklad v situácii, keď je server priamo pripojený na Internet a má jedno rozhranie smerom von a druhé smerom dnu a potrebujeme, aby Samba server počúval iba na vnútornom rozhraní.

3.4.1 Interakcia so samba-tool pri zriadení domény

Po spustení príkazu `samba-tool` z predošlej podčasti prebehne nasledovný interaktívny dialóg (červený text treba zadať, šedý sa vypíše automaticky):

```
Realm [CORP.VASAORG.SK]: Enter
Domain [CORP]: Enter
Server Role (dc, member, standalone) [dc]: Enter
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]: Enter
DNS forwarder IP address (write 'none' to disable forwarding) [172.22.0.1]: Enter
Administrator password: ****
Administrator password does not meet the default minimum password length requirement (7
↪characters).
Administrator password: ********
Administrator password does not meet the default quality standards.
Administrator password: ***********
Retype password: ***********
INFO: Looking up IPv4 addresses
INFO: Looking up IPv6 addresses
WARNING: No IPv6 address will be assigned
INFO: Setting up share.ldb
INFO: Setting up secrets.ldb
INFO: Setting up the registry
INFO: Setting up the privileges database
INFO: Setting up idmap db
```

```
INFO: Setting up SAM db
INFO: Setting up sam.ldb partitions and settings
INFO: Setting up sam.ldb rootDSE
INFO: Pre-loading the Samba 4 and AD schema
INFO: Adding DomainDN: DC=corp,DC=vasaorg,DC=sk
INFO: Adding configuration container
INFO: Setting up sam.ldb schema
INFO: Setting up sam.ldb configuration data
INFO: Setting up display specifiers
INFO: Modifying display specifiers and extended rights
INFO: Adding users container
INFO: Modifying users container
INFO: Adding computers container
INFO: Modifying computers container
INFO: Setting up sam.ldb data
INFO: Setting up well known security principals
INFO: Setting up sam.ldb users and groups
INFO: Setting up self join
INFO: Adding DNS accounts
INFO: Creating CN=MicrosoftDNS,CN=System,DC=corp,DC=vasaorg,DC=sk
INFO: Creating DomainDnsZones and ForestDnsZones partitions
INFO: Populating DomainDnsZones and ForestDnsZones partitions
INFO: Setting up sam.ldb rootDSE marking as synchronized
INFO: Fixing provision GUIDs
INFO: A Kerberos configuration suitable for Samba AD has been generated at
  /var/lib/samba/private/krb5.conf
INFO: Merge the contents of this file with your system krb5.conf or replace it with this
  one. Do not create a symlink!
INFO: Setting up fake yp server settings
INFO: Once the above files are installed, your Samba AD server will be ready to use
INFO: Server Role:           active directory domain controller
INFO: Hostname:              linse
INFO: NetBIOS Domain:        CORP
INFO: DNS Domain:            corp.vasaorg.sk
INFO: DOMAIN SID:            S-1-5-21-4159030542-4152435832-3415138938
```

3.4.2 Význam zadaných parametrov

Parameter `realm` (CORP.VASAORG.SK) predstavuje meno pre Kerberos oblasť (realm). Prvá časť tejto hodnoty sa automaticky použije aj ako DNS meno pre AD. Tento parameter by mal byť zadaný veľkými písmenami. Parameter `domain` (CORP) predstavuje meno domény. Obyčajne je to prvá časť AD DNS mena, ale na tomto mieste je to možné zmeniť. Tiež by mal byť napísaný veľkými písmenami.

Úlohu, akú bude server plniť v doméne, nastavíme pomocou parametra `server role`. Možné hodnoty sú `dc`, `member` a `standalone`. V tomto prípade zvolíme `dc` (active directory Domain Controller).

Ďalej si musíme zvoliť DNS backend. Na výber sú možnosti `SAMBA_INTERNAL`, `BIND9_DLZ`, `BIND9_FLATFILE` alebo `NONE`. Preddefinovaná a najlepšia voľba (pokiaľ nie sú kladené špeciálne požiadavky na DNS) je `SAMBA_INTERNAL`. `SAMBA_INTERNAL` je interný DNS server, ktorý je súčasťou Samba balíka a nevyžaduje žiadne ďalšie konfigurovanie. BIND9 je vhodný pre komplexnejšie požiadavky na DNS. Možnosti sú buď `BIND9_DLZ`, keď sú informácie o zónach uložené v AD, čo je odporúčané, alebo `BIND9_FLATFILE`, keď sú informácie uložené v textovej databáze. Túto možnosť sa neodporúča používať, keďže je nedokumentovaná a nepodporovaná a v budúcich verziách balíka Samba bude odstránená, rovnako ako `NONE`.

Parameter `DNS forwarder IP address` je nastaviteľný iba vtedy, ak sa používa interný DNS server. Definuje IP adresu DNS servera, kam sa posielajú požiadavky, pre ktoré interný server nie je autoritatívny. V našom prípade sme zvolili 172.22.0.1.

Posledným zadávaným údajom je heslo správcu domény (`Administrator password`). Toto heslo musí mať aspoň 7 znakov a musí obsahovať aspoň tri z nasledujúcich skupín znakov: veľké písmená, malé písmená, číslice a symboly (to sú všetky znaky na klávesnici, ktoré nie sú definované ako písmená alebo číslice). Ako vidno z vyššie uvedeného protokolu, ak heslo nespĺňa tieto požiadavky, tak je používateľ požiadaný o zadanie iného hesla.

3.4.3 Popis vytvoreného konfiguračného súboru

Po skončení interaktívneho dialógu vytvorí `samba-tool` konfiguračný súbor `/etc/samba/smb.conf`. Jeho obsah sa dá pozrieť priamo alebo cez príkaz `testparm`:

```
[global]
   dns forwarder = 172.22.0.1   # používa sa iba pri internom DNS
   bind interfaces only = Yes   # ručne pridané riadky pre naviazanie
   interfaces = lo ens33        # servera iba na vybrané rozhrania
   netbios name = LINSE         # NetBIOS meno Samba servera
                                # (štandardne prvá časť DNS mena PC)
   realm = CORP.VASAORG.SK      # názov Kerberos oblasti
   server role = active directory domain controller
                                # lebo sme zadali dc; iné možnosti sú:
                                # standalone, member server, classic primary
                                # alebo netbios backup domain controller
   workgroup = CORP             # meno domény
   idmap_ldb:use rfc2307 = yes  # zabuduje do LDAP atribúty z RFC2307

[sysvol]
   path = /var/lib/samba/sysvol
   read only = No

[netlogon]
   path = /var/lib/samba/sysvol/corp.vasaorg.sk/scripts
   read only = No
```

3.4.4 Konfiguračný súbor – implicitné parametre

Zadaním príkazu `testparm` (ktorý bol súčasťou aj staršieho balíka Samba 3) získame ešte niektoré ďalšie implicitné parametre:

```
passdb backend = samba_dsdb    # Samba directory services database
rpc_server:tcpip = no          # yes je momentálne iba pre testovanie
rpc_daemon:spoolssd = embedded
rpc_server:spoolss = embedded  # Network Printing Spooler
rpc_server:winreg = embedded   # Remote Registry Service
rpc_server:ntsvcs = embedded   # Plug and Play Services
rpc_server:eventlog = embedded # Event Logger
rpc_server:srvsvc = embedded   # Remote Server Services
rpc_server:svcctl = embedded   # Service Control
rpc_server:default = external
winbindd:use external pipes = true
idmap config * : backend = tdb
map readonly = no              # testparm -v
```

```
14 map archive = No # nepoužíva špeciálne mapovanie týchto atribútov do
     ↪štandardných UNIX atribútov, ale používa mapovanie DOS atribútov
     ↪(S,H,A,RO) do rozšíreného atribútu FS s názvom user.DOSATTRIB
15 store dos attributes = Yes # testparm -v
16 vfs objects = dfs_samba4 acl_xattr
17   # dfs_samba4: Distributed File System založený na doméne
18   # acl_xattr: ukladá NTFS ACL do rozšíreného atribútu security.NTACL
```

3.5 Spustenie a kontrola Samba AD-DC procesov

Po konfigurácii balíka Samba a vytvorení súboru `/etc/samba/smb.conf` je vhodné overiť funkčnosť radiča domény. Najprv treba skontrolovať bežiace procesy pomocou príkazu:

```
1 tester@linse:~$ ps axf | grep -E "samba|smbd|nmbd|winbindd"
2   18428 ?        Ss     0:00 /usr/sbin/nmbd --foreground --no-process-group
3   18438 ?        Ss     0:00 /usr/sbin/smbd --foreground --no-process-group
4   18440 ?        S      0:00  \_ /usr/sbin/smbd --foreground --no-process-group
5   18441 ?        S      0:00  \_ /usr/sbin/smbd --foreground --no-process-group
6   18444 ?        S      0:00  \_ /usr/sbin/smbd --foreground --no-process-group
```

Správne by sme mali dostať jeden samba proces, pod ktorým bežia ďalšie samba procesy. Pokiaľ dostaneme výpis podobný vyššie uvedenému, tak sme v zlom stave, z ktorého sa dostaneme vypnutím starých služieb (smbd a nmbd) a zapnutím novej samba služby pomocou:

```
1 tester@linse:~$ sudo systemctl stop smbd nmbd
2 tester@linse:~$ sudo systemctl disable smbd nmbd
3 Synchronizing state of smbd.service with SysV service script with
    ↪/lib/systemd/systemd-sysv-install.
4 Executing: /lib/systemd/systemd-sysv-install disable smbd
5 Synchronizing state of nmbd.service with SysV service script with
    ↪/lib/systemd/systemd-sysv-install.
6 Executing: /lib/systemd/systemd-sysv-install disable nmbd
7 Removed /etc/systemd/system/multi-user.target.wants/smbd.service.
8 Removed /etc/systemd/system/multi-user.target.wants/nmbd.service.
9 tester@linse:~$ sudo systemctl unmask samba-ad-dc
10 Removed /etc/systemd/system/samba-ad-dc.service.
11 tester@linse:~$ sudo systemctl start samba-ad-dc
12 Job for samba-ad-dc.service failed because the control process exited with
     ↪error code.
13 See "systemctl status samba-ad-dc.service" and "journalctl -xe" for details.
```

Vidíme, že službu sa nepodarilo naštartovať. Preto sa pozrieme do záznamov:

```
1 tester@linse:~$ journalctl -u samba-ad-dc
2 systemd[1]: Starting Samba AD Daemon...
3 ...
4 samba[10128]:   /usr/sbin/winbindd: Failed to exec child - No such file or
    ↪directory
5 samba[10128]: ../../source4/winbind/winbindd.c:46(winbindd_done)
6 samba[10128]:   winbindd daemon died with exit status 255
7 ...
8 systemd[1]: samba-ad-dc.service: Failed with result 'exit-code'.
9 systemd[1]: Failed to start Samba AD Daemon.
```

Dôvodom zlyhania je neexistujúci súbor `/usr/sbin/winbindd`. Tento je súčasťou balíka winbind, ktorý nainštalujeme príkazom:

```
1 tester@linse:~$ sudo apt install winbind
```

Teraz sa opätovne pokúsime o spustenie služby:

```
tester@linse:~$ sudo systemctl start samba-ad-dc
```

Tentokrát sa spustenie služby síce podarilo, ale keď skontrolujeme záznamy pomocou príkazu `journalctl -u samba-ad-dc`, tak zistíme, že:

```
systemd[1]: Starting Samba AD Daemon...
samba[12402]: ../../source4/smbd/server.c:622(binary_smbd_main)
samba[12402]:   samba version 4.11.6-Ubuntu started.
samba[12402]:   Copyright Andrew Tridgell and the Samba Team 1992-2019
samba[12402]: ../../source4/smbd/server.c:865(binary_smbd_main)
samba[12402]:   binary_smbd_main: samba: using 'prefork' process model
smbd[12423]: ../../lib/util/become_daemon.c:135(daemon_ready)
systemd[1]: Started Samba AD Daemon.
smbd[12423]:   daemon_ready: daemon 'smbd' finished starting up and ready to
  serve connections
winbindd[12457]:
  ../../source3/winbindd/winbindd_cache.c:3164(initialize_winbindd_cache)
winbindd[12457]:   initialize_winbindd_cache: clearing cache and re-creating
  with version number 2
winbindd[12457]: ../../lib/util/become_daemon.c:135(daemon_ready)
winbindd[12457]:   daemon_ready: daemon 'winbindd' finished starting up and
  ready to serve connections
samba[12460]: ../../lib/util/util_runcmd.c:352(samba_runcmd_io_handler)
samba[12460]:   /usr/sbin/samba_dnsupdate: ERROR(runtime): uncaught exception
  - (9711, 'WERR_DNS_ERROR_RECORD_ALREADY_EXISTS')
...
```

Tento problém vyriešime tým, že v súbore `/etc/resolv.conf` zmeníme DNS server z externého 172.22.0.1 na interný 172.22.222.11 (ktorý je súčasťou balíka samba):

```
domain corp.vasaorg.sk
search corp.vasaorg.sk
nameserver 172.22.222.11
```

Po reštartovaní služby samba-ad-ac znovu overíme hierarchiu procesov. Už získame požadovaný správny stav:

```
tester@linse:~$ sudo systemctl start samba-ad-dc
tester@linse:~$ ps axf | grep -E "samba|smbd|nmbd|winbindd"
    820 ?        Ss     0:00 samba: root process
    890 ?        S      0:00  \_ samba: tfork waiter process
    891 ?        S      0:00  |   \_ samba: task[s3fs] pre-fork master
    893 ?        S      0:00  |       \_ samba: tfork waiter process
    895 ?        Ss     0:00  |           \_ /usr/sbin/smbd -D ...
    944 ?        S      0:00  |               \_ /usr/sbin/smbd -D ...
    945 ?        S      0:00  |               \_ /usr/sbin/smbd -D ...
    946 ?        S      0:00  |               \_ /usr/sbin/smbd -D ...
    892 ?        S      0:00  \_ samba: tfork waiter process
    894 ?        S      0:00  |   \_ samba: task[rpc] pre-fork master
    899 ?        S      0:00  |       \_ samba: tfork waiter process
    902 ?        S      0:00  |       |   \_ samba: task[rpc] pre-forked worker(0)
    903 ?        S      0:00  |       \_ samba: tfork waiter process
    906 ?        S      0:00  |       |   \_ samba: task[rpc] pre-forked worker(1)
    908 ?        S      0:00  |       \_ samba: tfork waiter process
    912 ?        S      0:00  |       |   \_ samba: task[rpc] pre-forked worker(2)
    913 ?        S      0:00  |       \_ samba: tfork waiter process
    920 ?        S      0:00  |           \_ samba: task[rpc] pre-forked worker(3)
    896 ?        S      0:00  \_ samba: tfork waiter process
    897 ?        S      0:00  |   \_ samba: task[nbt] pre-fork master
    898 ?        S      0:00  \_ samba: tfork waiter process
```

```
24      900 ?        S      0:00  |   \_ samba: task[wrepl] pre-fork master
25      901 ?        S      0:00  \_ samba: tfork waiter process
26      904 ?        S      0:00  |   \_ samba: task[ldap] pre-fork master
27      951 ?        S      0:00  |       \_ samba: tfork waiter process
28      952 ?        S      0:00  |       |  \_ samba: task[ldap] pre-forked worker(0)
29      953 ?        S      0:00  |       \_ samba: tfork waiter process
30      954 ?        S      0:00  |       |  \_ samba: task[ldap] pre-forked worker(1)
31      955 ?        S      0:00  |       \_ samba: tfork waiter process
32      956 ?        S      0:00  |       |  \_ samba: task[ldap] pre-forked worker(2)
33      957 ?        S      0:00  |       \_ samba: tfork waiter process
34      958 ?        S      0:00  |          \_ samba: task[ldap] pre-forked worker(3)
35      905 ?        S      0:00  \_ samba: tfork waiter process
36      907 ?        S      0:00  |   \_ samba: task[cldap] pre-fork master
37      909 ?        S      0:00  \_ samba: tfork waiter process
38      910 ?        S      0:00  |   \_ samba: task[kdc] pre-fork master
39      916 ?        S      0:00  |       \_ samba: tfork waiter process
40      917 ?        S      0:00  |       |   \_ samba: task[kdc] pre-forked worker(0)
41      918 ?        S      0:00  |       \_ samba: tfork waiter process
42      922 ?        S      0:00  |       |   \_ samba: task[kdc] pre-forked worker(1)
43      925 ?        S      0:00  |       \_ samba: tfork waiter process
44      927 ?        S      0:00  |       |   \_ samba: task[kdc] pre-forked worker(2)
45      928 ?        S      0:00  |       \_ samba: tfork waiter process
46      935 ?        S      0:00  |          \_ samba: task[kdc] pre-forked worker(3)
47      911 ?        S      0:00  \_ samba: tfork waiter process
48      914 ?        S      0:00  |   \_ samba: task[drepl] pre-fork master
49      915 ?        S      0:00  \_ samba: tfork waiter process
50      919 ?        S      0:00  |   \_ samba: task[winbindd] pre-fork master
51      923 ?        S      0:00  |       \_ samba: tfork waiter process
52      929 ?        Ss     0:00  |          \_ /usr/sbin/winbindd -D ...
53     2070 ?        S      0:00  |              \_ winbindd: domain child [CORP]
54     2071 ?        S      0:00  |              \_ winbindd: domain child [BUILTIN]
55     2072 ?        S      0:00  |              \_ winbindd: idmap child
56      921 ?        S      0:00  \_ samba: tfork waiter process
57      924 ?        S      0:00  |   \_ samba: task[ntp_signd] pre-fork master
58      926 ?        S      0:00  \_ samba: tfork waiter process
59      930 ?        S      0:00  |   \_ samba: task[kcc] pre-fork master
60      931 ?        S      0:00  \_ samba: tfork waiter process
61      933 ?        S      0:00  |   \_ samba: task[dnsupdate] pre-fork master
62      934 ?        S      0:00  \_ samba: tfork waiter process
63      936 ?        S      0:00      \_ samba: task[dns] pre-fork master
```

Nakoniec povolíme službu, aby sme mali zabezpečené jej aktivovanie počas štartovania operačného systému:

```
tester@linse:~$ sudo systemctl enable samba-ad-dc
Synchronizing state of samba-ad-dc.service with SysV service script ...
Executing: /lib/systemd/systemd-sysv-install enable samba-ad-dc
Created symlink
  ↪ /etc/systemd/system/multi-user.target.wants/samba-ad-dc.service ...
```

3.5.1 Kontrola portov

Ďalším krokom by mala byť kontrola správneho priradenia portov potrebných pre činnosť radiča domény. Priradenie portov pre jednotlivé procesy môžeme získať pomocou príkazu:

```
tester@linse:~$ sudo apt install net-tools # ak netstat ešte nie je nainštalovaný
tester@linse:~$ sudo netstat -tulpn | egrep "samba|smbd|nmbd|winbindd"
tcp  0  0  172.22.222.11:464    0.0.0.0:*     LISTEN      910/samba: task[kdc]
tcp  0  0  127.0.0.1:464        0.0.0.0:*     LISTEN      910/samba: task[kdc]
tcp  0  0  172.22.222.11:53     0.0.0.0:*     LISTEN      936/samba: task[dns]
tcp  0  0  127.0.0.1:53         0.0.0.0:*     LISTEN      936/samba: task[dns]
```

```
 7 tcp  0  0 172.22.222.11:88      0.0.0.0:*     LISTEN      910/samba: task[kdc]
 8 tcp  0  0 127.0.0.1:88          0.0.0.0:*     LISTEN      910/samba: task[kdc]
 9 tcp  0  0 172.22.222.11:636     0.0.0.0:*     LISTEN      904/samba: task[ldap]
10 tcp  0  0 127.0.0.1:636         0.0.0.0:*     LISTEN      904/samba: task[ldap]
11 tcp  0  0 127.0.0.1:445         0.0.0.0:*     LISTEN      895/smbd
12 tcp  0  0 172.22.222.11:445     0.0.0.0:*     LISTEN      895/smbd
13 tcp  0  0 172.22.222.11:49152   0.0.0.0:*     LISTEN      894/samba: task[rpc]
14 tcp  0  0 127.0.0.1:49152       0.0.0.0:*     LISTEN      894/samba: task[rpc]
15 tcp  0  0 172.22.222.11:49153   0.0.0.0:*     LISTEN      902/samba: task[rpc]
16 tcp  0  0 127.0.0.1:49153       0.0.0.0:*     LISTEN      902/samba: task[rpc]
17 tcp  0  0 172.22.222.11:49154   0.0.0.0:*     LISTEN      902/samba: task[rpc]
18 tcp  0  0 127.0.0.1:49154       0.0.0.0:*     LISTEN      902/samba: task[rpc]
19 tcp  0  0 172.22.222.11:3268    0.0.0.0:*     LISTEN      904/samba: task[ldap]
20 tcp  0  0 127.0.0.1:3268        0.0.0.0:*     LISTEN      904/samba: task[ldap]
21 tcp  0  0 172.22.222.11:3269    0.0.0.0:*     LISTEN      904/samba: task[ldap]
22 tcp  0  0 172.22.222.11:389     0.0.0.0:*     LISTEN      904/samba: task[ldap]
23 tcp  0  0 127.0.0.1:3269        0.0.0.0:*     LISTEN      904/samba: task[ldap]
24 tcp  0  0 127.0.0.1:389         0.0.0.0:*     LISTEN      904/samba: task[ldap]
25 tcp  0  0 172.22.222.11:135     0.0.0.0:*     LISTEN      902/samba: task[rpc]
26 tcp  0  0 127.0.0.1:135         0.0.0.0:*     LISTEN      902/samba: task[rpc]
27 tcp  0  0 127.0.0.1:139         0.0.0.0:*     LISTEN      895/smbd
28 tcp  0  0 172.22.222.11:139     0.0.0.0:*     LISTEN      895/smbd
29 udp  0  0 172.22.222.11:464     0.0.0.0:*                 910/samba: task[kdc]
30 udp  0  0 127.0.0.1:464         0.0.0.0:*                 910/samba: task[kdc]
31 udp  0  0 172.22.222.11:53      0.0.0.0:*                 936/samba: task[dns]
32 udp  0  0 127.0.0.1:53          0.0.0.0:*                 936/samba: task[dns]
33 udp  0  0 172.22.222.11:88      0.0.0.0:*                 910/samba: task[kdc]
34 udp  0  0 127.0.0.1:88          0.0.0.0:*                 910/samba: task[kdc]
35 udp  0  0 172.22.222.11:137     0.0.0.0:*                 897/samba: task[nbt]
36 udp  0  0 172.22.255.255:137    0.0.0.0:*                 897/samba: task[nbt]
37 udp  0  0 127.0.0.1:137         0.0.0.0:*                 897/samba: task[nbt]
38 udp  0  0 127.255.255.255:137   0.0.0.0:*                 897/samba: task[nbt]
39 udp  0  0 172.22.222.11:138     0.0.0.0:*                 897/samba: task[nbt]
40 udp  0  0 172.22.255.255:138    0.0.0.0:*                 897/samba: task[nbt]
41 udp  0  0 127.0.0.1:138         0.0.0.0:*                 897/samba: task[nbt]
42 udp  0  0 127.255.255.255:138   0.0.0.0:*                 897/samba: task[nbt]
43 udp  0  0 172.22.222.11:389     0.0.0.0:*                 907/samba: task[cldap]
44 udp  0  0 127.0.0.1:389         0.0.0.0:*                 907/samba: task[cldap]
```

Pre lepšiu prehľadnosť sú použité porty zhrnuté v nasledovnej tabuľke (iba IPv4):

TCP	UDP	Local Address	Port	Service	PID	Program
●	●	127.0.0.1, 172.22.222.11	53	DNS	936	samba task[dns]
●	●		88	Kerberos	910	samba task[kdc]
●	○		135	MS End Point Mapper[1]	902	samba task[rpc]
○	●	127.0.0.1, 127.255.255.255, 172.22.222.11, 172.22.255.255	137	NetBIOS Name Service	897	samba task[nbt]
○	●		138	NetBIOS Datagram Service	897	samba task[nbt]
●	○		139	NetBIOS Session Service	895	smbd
●	○	127.0.0.1, 172.22.222.11	389	LDAP	904	samba task[ldap]
○	●		389	LDAP	907	samba task[cldap]
●	○		445	SMB nad TCP	895	smbd
●	●		464	Kerberos kpasswd	910	samba task[kdc]
●	○		636	LDAP nad SSL (LDAPS)	904	samba task[ldap]
●	○		3268	MS Global Catalog	904	samba task[ldap]
●	○		3269	MS Global Catalog nad SSL	904	samba task[ldap]
●	○		49152 – 65535	Dynamické RPC porty	894, 902	samba task[rpc]

Ak niektorý z týchto portov chýba (proces nebeží, alebo port používa iný proces), tak treba vykonať nápravu (napr. odinštalovanie konfliktného procesu alebo jeho rekonfiguráciu).

[1] Microsoft End Point Mapper je tiež známy ako DCE/RPC Locator Service.

3.5.2 Kontrola konfigurácie zdieľaných priečinkov

Po overení činnosti všetkých služieb môžeme skontrolovať, či AD DC poskytuje základné priečinky netlogon a sysvol. Najprv nainštalujeme príkaz `smbclient`:

```
tester@linse:~$ sudo apt install smbclient
```

Príkaz `smbclient` používa parameter `-U`, ktorým sa špecifikuje meno a prípadne heslo prihlasovaného používateľa. Tieto údaje sa zadávajú v tvare `-Uusername[%password]`. Napríklad parameter `-Uuser` znamená používateľa `user`. Pokiaľ sa heslo nezadá na príkazovom riadku, tak si ho `smbclient` vypýta. Ak je heslo prázdne (napríklad pri anonymnom prístupe), tak možno výzvu potlačiť parametrom `-N`. Pri vypísaní zdieľaných prostriedkov pomocou príkazu `smbclient --list` by sa mali zobraziť priečinky netlogon a sysvol:

```
tester@linse:~$ smbclient --list localhost -N
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        sysvol          Disk
        netlogon        Disk
        IPC$            IPC       IPC Service (Samba 4.11.6-Ubuntu)
SMB1 disabled -- no workgroup available
```

3.5.3 Kontrola autentifikácie a prístupových práv

Po úspešnom zobrazení zdieľaných priečinkov sa pokúsime s anonymným prístupom vypísať obsah priečinku sysvol. Tento pokus by mal skončiť úspešným prihlásením ale s odopretím prístupu, ako ukazuje nasledovný príklad:

```
tester@linse:~$ smbclient //localhost/sysvol -N -c 'ls'
Anonymous login successful
tree connect failed: NT_STATUS_ACCESS_DENIED
```

Pokiaľ sa o to isté pokúsi používateľ Administrator, tak by sa výpis adresára mal podariť:

```
tester@linse:~$ smbclient //localhost/sysvol -UAdministrator -c 'ls'
Enter CORP\Administrator's password:
             (heslo zadané pri zriadení domény - pozri podčasť 3.4.1, strana 36)
  .                                   D        0  Sat ...
  ..                                  D        0  Sat ...
  corp.vasaorg.sk                     D        0  Sat ...

   19475088 blocks of size 1024. 13793992 blocks available
```

3.6 Konfigurácia DNS a kontrola funkčnosti

Pre správnu činnosť AD je nutná aj korektná funkčnosť DNS. Napríklad bez správnych záznamov nebude korektne pracovať Kerberos protokol (AD používa algoritmus DC Locator pre nájdenie Kerberos servera). Preto overíme, či Samba AD DC poskytuje cez svoj interný DNS server (ktorý sme v podčasti 3.5 na strane 40 nastavili pre náš systém ako východzí) správne záznamy pre algoritmus DC Locator na nájdenie jednotlivých serverov:

```
tester@linse:~$ host -t SRV _ldap._tcp.corp.vasaorg.sk.
_ldap._tcp.corp.vasaorg.sk has SRV record 0 100 389 linse.corp.vasaorg.sk.
tester@linse:~$ host -t SRV _kerberos._udp.corp.vasaorg.sk.
_kerberos._udp.corp.vasaorg.sk has SRV record 0 100 88 linse.corp.vasaorg.sk.
tester@linse:~$ host -t A linse.corp.vasaorg.sk
linse.corp.vasaorg.sk has address 172.22.222.11
```

Pokiaľ by niektorý príkaz zlyhal, tak DNS nepracuje správne a chybu je potrebné opraviť.

3.7 Konfigurácia Kerberosu

Kerberos protokol je dôležitou súčasťou AD. Umožňuje jednorazové prihlásenie v rámci domény. Vďaka tomu nie je nutné opakované prihlasovanie na ostatné servery v doméne. Počas zriadenia domény vznikla konfigurácia pre používateľské programy Kerberosu odrážajúca nastavenia domény. Preto treba nahradiť konfiguračný súbor Kerberosu `/etc/krb5.conf` súborom vytvoreným Sambou `/var/lib/samba/private/krb5.conf`:

```
tester@linse:~$ sudo ln -sf /var/lib/samba/private/krb5.conf /etc/krb5.conf
```

Obsah tohto súboru je nasledovný:

```
[libdefaults]
    default_realm = CORP.VASAORG.SK
    dns_lookup_realm = false
    dns_lookup_kdc = true
```

Po konfigurácii Kerberosu vykonáme skúšobné prihlásenie:

```
tester@linse:~$ kinit Administrator
Password for Administrator@CORP.VASAORG.SK:
Warning: Your password will expire in 41 days on ...
```

Prihlásením vznikol „ticket“, ktorý si môžeme vypísať pomocou príkazu:

```
tester@linse:~$ klist -fe
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: Administrator@CORP.VASAORG.SK

Valid starting      Expires         Service principal
...                 ...             krbtgt/CORP.VASAORG.SK@CORP.VASAORG.SK
  renew until ..., Flags: RIA
  Etype (skey, tkt): aes256-cts-hmac-sha1-96, aes256-cts-hmac-sha1-96
```

3.7.1 Test pripojenia cez Kerberos

V predošlej časti sme sa autentifikovali voči Kerberos serveru a získali sme špeciálny „ticket“ nazývaný „ticket granting ticket“ (TGT). Počas jeho platnosti sa môžeme autentifikovať bez zadania hesla voči iným službám v doméne. Napríklad môžeme vyskúšať prihlásenie na súborový server:

```
tester@linse:~$ smbclient //linse/sysvol --kerberos -c 'ls'
  .                                   D        0  Sat ...
  ..                                  D        0  Sat ...
  corp.vasaorg.sk                     D        0  Sat ...

    19475088 blocks of size 1024. 13793992 blocks available
```

V tomto prípade parameter `--kerberos` spôsobil, že pre autentifikáciu sa použil Kerberos protokol. Preto nebolo potrebné zadať heslo a používateľ sa autentifikoval vďaka svojmu platnému TGT. Po autentifikácii voči súborovému serveru používateľ získal ďalší „ticket“ použiteľný pre priamu komunikáciu so súborovým serverom. Na nasledovnom výpise je označený hrubým písmom:

```
tester@linse:~$ klist -fe
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: Administrator@CORP.VASAORG.SK
Valid starting      Expires         Service principal
...                 ...             krbtgt/CORP.VASAORG.SK@CORP.VASAORG.SK
  renew until ..., Flags: RIA
  Etype (skey, tkt): aes256-cts-hmac-sha1-96, aes256-cts-hmac-sha1-96
...                 ...             cifs/linse@CORP.VASAORG.SK
  Flags: ATO, Etype (skey, tkt): aes256-cts-hmac-sha1-96, aes256-cts-hmac-sha1-96
```

Každý „ticket“ má svoje príznaky (flags). Ich význam je nasledovný:

Príznak	Názov	Popis
R	Renewable	Použitelný pre získanie nového kľúča sedenia bez potreby opätovného zadania hesla.
I	Initial	Vydaný na základe aktuálnej autentifikácie a nie na základe „ticket-granting ticket“ (TGT).
A	preAuthenticated	Vydaný po tom, ako bol používateľ autentifikovaný voči „key distribution center“ (KDC).
T	Transit policy checked	Vydávajúci KDC skontroloval platnosť celej reťaze medzi prvým „ticketom“ a aktuálnym „ticketom“.
O	Okay as delegate	Politika ho dovoľuje použiť ako delegáta.

3.8 NTP server pre AD

AD vyžaduje synchronizáciu času medzi počítačmi v doméne z dôvodu riešenia konfliktov pri replikácii, ale aj pre zabránenie útokov opakovaním v Kerberos protokole. Maximálny povolený časový rozdiel medzi dvomi počítačmi je štandardne 5 minút.

Windows klienti požadujú NTP server s podporou MS-SNTP (Microsoft Simple Network Time Protocol). Tento protokol používa Network Time Protocol (NTP) Authentication Extensions. Jeho špecifikáciu je možné nájsť (aj so špecifikáciou ostatných Windows protokolov, 458 PDF súborov ≈ 1,24 GB) na adrese:

`http://go.microsoft.com/fwlink/?LinkId=389156`.

Samba štandardne poskytuje pre ntpd server službu podpisovania paketov (server services = +ntp_signd), aby Linuxový NTP server nemusel riešiť, odkiaľ má získať kľúč na podpísanie paketov. Na komunikáciu s ntpd používa Samba socket (ntp signd socket directory = `/var/lib/samba/ntp_signd`). Je nutné použiť ntpd vo verzii aspoň 4.2.6 s podporou ntp_signd (`--enable-ntp-signd`). NTP server nainštalujeme nasledovným príkazom:

```
tester@linse:~$ sudo apt install ntp
```

3.8.1 Konfigurácia NTP servera

Po inštalácii NTP servera je potrebné upraviť prístupové práva k adresáru so Samba socketom tak, aby mohol z neho čítať aj používateľ, pod ktorým beží NTP server:

```
tester@linse:~$ sudo chown root:ntp /var/lib/samba/ntp_signd
tester@linse:~$ sudo ls -ld /var/lib/samba/ntp_signd/
drwxr-x--- 2 root ntp 4096 Mar 27 15:22 /var/lib/samba/ntp_signd/
```

Následne upravíme konfiguračný súbor servera (`/etc/ntp.conf`) do nasledovného tvaru:

```
driftfile /var/lib/ntp/ntp.drift
leapfile /usr/share/zoneinfo/leap-seconds.list
ntpsigndsocket /var/lib/samba/ntp_signd # bez /socket na konci!

# vyberieme jeden alebo viac NTP serverov
pool 0.ubuntu.pool.ntp.org iburst prefer
...

# pseudo IP lokálnych hodín (využije sa v prípade problémov so sieťou)
server 127.127.1.0
fudge  127.127.1.0 stratum 10

# štandardne každému povolíme synchronizáciu času (vrátane MS-SNTP)
# ale nepovolíme mu konfiguráciu servera
restrict -4 default kod notrap nomodify nopeer noquery limited mssntp
restrict -6 default kod notrap nomodify nopeer noquery limited mssntp

# lokálny používateľ môže NTP server aj konfigurovať
restrict 127.0.0.1
restrict ::1

# pre externé časové servery je slušné povoliť dopytovanie (queries)
restrict source notrap nomodify noquery nopeer
```

Je vhodné použiť viac externých časových serverov. Tie je možné doplniť na miesta označené symbolom „…“. V uzavretej doméne nie je potrebné, aby na všetkých počítačoch bol presný reálny čas. Je len nutné, aby v každom okamihu, bol rozdiel medzi časmi na dvoch počítačoch menší ako päť minút. Na druhej strane, keď už riešime synchronizáciu času, je rozumné udržiavať na všetkých počítačoch presný reálny čas. Po ukončení konfigurácie ntp server reštartneme príkazom:

```
tester@linse:~$ sudo systemctl restart ntp
```

3.9 Použitie samba-tools

Príkaz `samba-tools` má široké použitie pri správe domény a jej radiča. Napríklad pomocou nasledovného príkazu je možné skontrolovať integritu lokálnej AD databázy:

```
tester@linse:~$ sudo samba-tool dbcheck
Checking 267 objects
Checked 267 objects (0 errors)
```

Databáza je momentálne bez chýb. Pomocou príkazu `samba-tool fsmo show` je možné zobraziť všetky „Flexible Single Master Operations“ (FSMO) role, ktoré sú v doméne a na akých serveroch bežia:

```
tester@linse:~$ sudo samba-tool fsmo show
SchemaMasterRole owner: ...
InfrastructureMasterRole owner: ...
RidAllocationMasterRole owner: ...
PdcEmulationMasterRole owner: ...
DomainNamingMasterRole owner: ...
DomainDnsZonesMasterRole owner: ...
ForestDnsZonesMasterRole owner: ...
```

kde ... predstavujú nasledovnú úplnú cestu:

```
CN=NTDS Settings,CN=LINSE,CN=Servers,CN=Default-First-Site-Name,CN=Sites,
    CN=Configuration,DC=corp,DC=vasaorg,DC=sk
```

Aktuálne všetky role bežia na jedinom serveri v doméne: linse. Tieto role sa vyznačujú tým, že nie sú vhodné pre beh na viacerých DC (preto sa volajú Single Master). Pomocou tohto príkazu je možné ich nielen zobraziť, ale aj spravovať.

Zoznam všetkých používateľov domény sa dá získať príkazom:

```
tester@linse:~$ sudo samba-tool user list
Administrator
krbtgt
Guest
```

Zvolenú funkčnú úroveň domény a lesa je možné overiť pomocou príkazu:

```
tester@linse:~$ sudo samba-tool domain level show
Domain and forest function level for domain 'DC=corp,DC=vasaorg,DC=sk'

Forest function level: (Windows) 2003
Domain function level: (Windows) 2003
Lowest function level of a DC: (Windows) 2008 R2
```

Pokiaľ pri zriadení domény bola zvolená nízka úroveň (v tomto príklade 2003) je možné ju dodatočne zvýšiť príkazom:

```
tester@linse:~$ sudo samba-tool domain level raise --forest-level=2008_R2
    --domain-level=2008_R2
Domain function level changed!
Forest function level changed!
All changes applied successfully!
```

Po jeho vykonaní môžeme overiť, či sa funkčná úroveň naozaj zvýšila:

```
tester@linse:~$ sudo samba-tool domain level show
Domain and forest function level for domain 'DC=corp,DC=vasaorg,DC=sk'

Forest function level: (Windows) 2008 R2
Domain function level: (Windows) 2008 R2
Lowest function level of a DC: (Windows) 2008 R2
```

Pri zriadení domény bolo potrebné zadať heslo pre administrátora domény v súlade s politikou hesiel v doméne. Zobraziť (a následne aj spravovať) aktuálnu politiku hesiel v doméne je možné pomocou príkazu `samba-tool domain passwordsettings`:

```
tester@linse:~$ sudo samba-tool domain passwordsettings show
Password information for domain 'DC=corp,DC=vasaorg,DC=sk'

Password complexity: on
Store plaintext passwords: off
```

```
Password history length: 24
Minimum password length: 7
Minimum password age (days): 1
Maximum password age (days): 42
Account lockout duration (mins): 30
Account lockout threshold (attempts): 0
Reset account lockout after (mins): 30
```

3.10 Pridanie Windows do domény

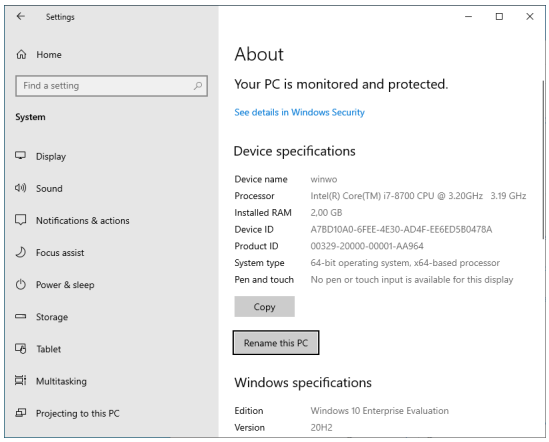
V tejto kapitole popíšeme pridanie počítača so systémom Microsoft Windows do novej domény, ktorú sme získali po úspešnej inštalácii a konfigurácii AD DS na báze Samba servera.

3.10.1 Predpoklady

Na to, aby bolo možné počítač s operačným systémom Windows pridať do domény, musia byť splnené niektoré základné predpoklady. Prvým z nich je správna edícia Windows. Do domény nie je možné pridať tie edície Windows, ktoré sú určené pre domáce (nefiremné) použitie. Presnejšie povedané, z posledných verzií operačného systému Windows je možné pridať do domény nasledovné edície: Windows 10 Pro, Enterprise a Education, Windows 8 / 8.1 Pro a Enterprise, Windows 7 Professional, Ultimate a Enterprise, Windows Vista Business, Ultimate a Enterprise.

Pre pridanie počítača do domény sú potrebné práva lokálneho správcu (na PC, ktoré sa pripája). Ďalej je potrebná znalosť mena a hesla doménového účtu, ktorý má oprávnenie pridávať počítače do domény (napríklad Domain Administrator).

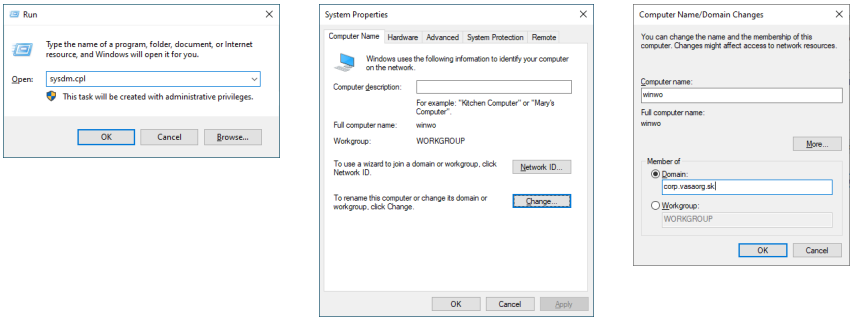
Ďalšou podmienkou je DNS nastavené tak, aby sa dala zistiť IP adresa pre radič domény, LDAP, Kerberos a tak podobne. V našom prípade DNS nastavíme priamo na radič domény, ktorý prevádzkuje vlastný interný DNS server.



Poslednou podmienkou je správny čas na pripájanom počítači. Synchronizácia času s PDC (serverom s PdcEmulationMasterRole) sa na počítači nastaví automaticky po jeho pripojení do domény.

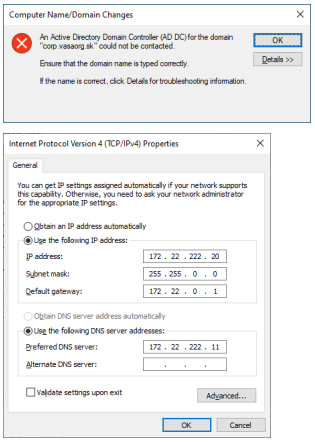
3.10.2 Pridanie do domény

V nasledovnom príklade postupu budeme vychádzať z čerstvej inštalácie Windows 10 Enterprise Evaluation. Počítač nazveme winwo (ako WINdows WOrkstation) stlačením tlačidla Rename this PC v okne „⚙ ▸ System ▸ About“. Windows sa v základnej konfigurácii štandardne pripája do preddefinovanej pracovnej skupiny WORKGROUP. Pre pridanie počítača do domény spustíme program „System Properties“ stlačením ⊞ + R a zadaním `sysdm.cpl` (pozri obrázok 3.1):



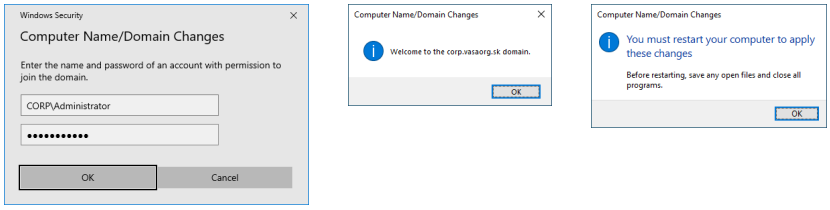
Obr. 3.1: Pridanie počítača do domény

V okne „System Properties“ na záložke „Computer Name“ stlačíme tlačidlo Change ... . Následne v dialógovom okne „Computer Name/Domain Changes“ klikneme na „Member of ▸ Domain“ a zadáme názov domény. V tomto prípade: „corp.vasaorg.sk“. Pridanie do domény potvrdíme tlačidlom OK (premenovať počítač sme mohli aj v tomto okne).



Systém však oznámi chybu zobrazenú na obrázku na okraji. Táto chyba je spôsobená tým, že sme ešte správne nenastavili DNS server na interný DNS server radiča domény. Z tohto dôvodu nevedel algoritmus DC Locator nájsť radič domény k zadanej doméne. Preto v nastaveniach TCP/IP protokolu (+ R , `ncpa.cpl`, „Ethernet0 ▸ Properties ▸ Internet Protocol Version 4 (TCP/IPv4)“, Properties) do poľa „Preferred DNS server“ zadáme IP adresu linse: 172.22.222.11. Rovno hneď nastavíme aj fixnú IP adresu v časti „Use the following IP address“ (pozri obrázok na okraji).

Po nastavení správneho DNS servera zopakujeme postup z obrázku 3.1. Teraz sa po potvrdení názvu domény zobrazí okno „Windows Security“ so žiadosťou o zadanie mena a hesla používateľa, ktorý má právo pridať počítač do domény (nie lokálny administrátor, ale správca domény). Po zadaním správneho mena a hesla pre správcu domény sa počítač pridá do domény (pozri obrázok 3.2). Po pridaní do domény je počítač potrebné reštartovať.



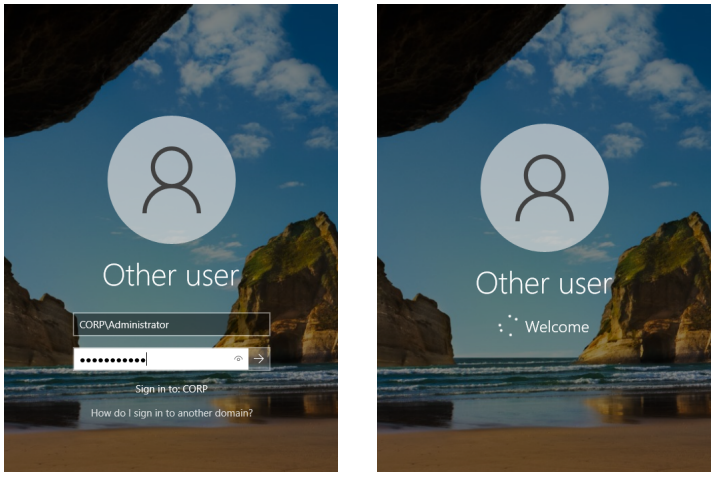
Obr. 3.2: Dokončenie pridania počítača do domény

Po reštarte sa používateľ môže do počítača prihlásiť pod lokálnym (v tvare `WINWO\User`), ako aj pod doménovým účtom.

3.10.3 Prihlásenie ako používateľ domény

Keď je počítač súčasťou domény, tak sa na ňom môže používateľ prihlásiť zadaním doménového mena v štandardnom tvare (v tomto prípade napríklad `CORP\Administrator`). Pre

zmenu prihlasovaného používateľa treba kliknúť do ľavého dolného rohu na „Other user“. Do akej domény sa používateľ prihlasuje, je zobrazené aj pod poľom pre zadanie hesla (Sign in to: CORP). Informácie o tom, ako sa prihlásiť do zvolenej domény alebo na lokálny počítač je možné získať aj kliknutím na linku „How do I sign to another domain?“.



Obr. 3.3: Pridanie do domény

Ak sa používateľ prihlási doménovým účtom, tak je meno domény súčasťou jeho používateľského mena (pred lomítkom), ako aj domovského adresára (v tvare `Meno.DOMENA`), ktorý bude používateľovi na počítači automaticky vytvorený.

Po prihlásení je vhodné skontrolovať dostupné aktualizácie (aj keď bol počítač pred pridaním do domény plne aktualizovaný), pretože po jeho pridaní do domény môžu byť pre neho k dispozícii ďalšie aktualizácie.

3.10.4 Kontrola synchronizácie času

Pridaním počítača do domény by sa mala automaticky nastaviť synchronizácia času počítača s radičom domény. Synchronizáciu času môžeme skontrolovať zadaním príkazu `w32tm` z príkazového riadku. Pre prístup k príkazovému riadku je možné použiť klasické `cmd`, ale v nasledujúcich príkladoch používame novší „Windows PowerShell“:

```
PS C:\Users\Administrator.CORP> w32tm /resync
Sending resync command to local computer
The computer did not resync because no time data was available.
```

Pokiaľ synchronizácia skončí neúspešne (ako v predošlom prípade), treba skontrolovať, či náhodou v súbore `/var/log/syslog` na Ubuntu serveri poskytujúcom NTP server sa nevyskytuje záznam podobajúci sa na:

```
... linse kernel: ... apparmor="DENIED" operation="connect" profile="/usr/sbin/ntpd" name="/var/lib/samba/ntp_signd/socket" pid=879 comm="ntpd" requested_mask="wr" denied_mask="wr" fsuid=112 ouid=0
```

Ak áno, tak je pravdepodobné, že AppArmor má zle nastavenú cestu k socketu v konfiguračnom súbore `/etc/apparmor.d/usr.sbin.ntpd` pre službu NTP:

```
# samba4 ntp signing socket
/{,var/}run/samba/ntp_signd/socket rw,
```

Chybu opravíme pridaním nasledovných riadkov do lokálneho konfiguračného súboru `/etc/apparmor.d/local/usr.sbin.ntpd` (ktorý je inak prázdny):

```
# Site-specific additions and overrides for usr.sbin.ntpd.
# For more details, please see /etc/apparmor.d/local/README.
/var/lib/samba/ntp_signd/socket rw,
```

Po opravení AppArmor konfigurácie pre NTP server a jej znovunačítaní pomocou príkazu:

```
tester@linse:~$ sudo apparmor_parser -r /etc/apparmor.d/usr.sbin.ntpd
```

by už mala synchronizácia času na winwo prebehnúť správne:

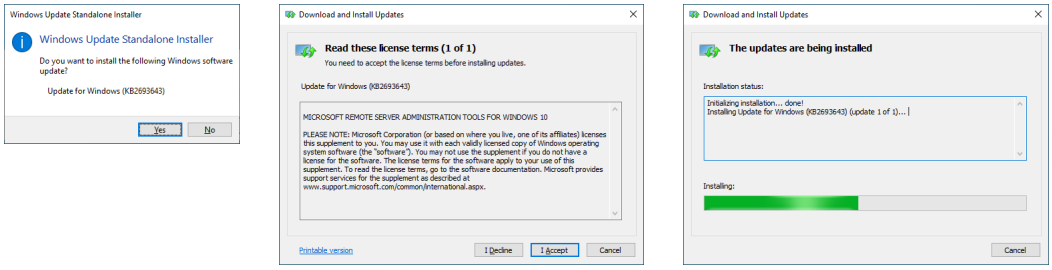
```
PS C:\Users\Administrator.CORP> w32tm /resync
Sending resync command to local computer
The command completed successfully.
```

3.11 Inštalácia RSAT

Ak chceme spravovať doménu z klientskej Windows stanice, tak je potrebné na ňu najprv nainštalovať RSAT („Remote Server Administration Tools“). Zároveň je to aj najjednoduchší spôsob, ako spravovať Samba doménu. Výhodou je, že sú to nástroje priamo od Microsoftu s dobrou dokumentáciou, na ktoré sú správcovia domén zvyknutí. Aj keď sme si ukázali, že sa dá Samba doména spravovať pomocou príkazu `samba-tool`, tak tento nástroj ešte nie je plnohodnotnou náhradou nástrojov dostupných pre Windows od Microsoftu. RSAT vo verzii pre Windows 10 sa dá voľne stiahnuť z adresy:

`https://www.microsoft.com/en-us/download/details.aspx?id=45520`

Je to súbor `WindowsTH-RSAT_WS_1803-x64.msu` s veľkosťou približne 95,1 MB.[2] Po spustení stiahnutého súboru sa zobrazí okno „Windows Update Standalone Installer“. Súhlasom s inštaláciou aktualizácie KB2693643 (kliknutím na tlačidlo Yes) sa dostaneme k licenčným podmienkam. Ich prijatím (kliknutím na tlačidlo I Accept) sa vykoná samotná inštalácia.



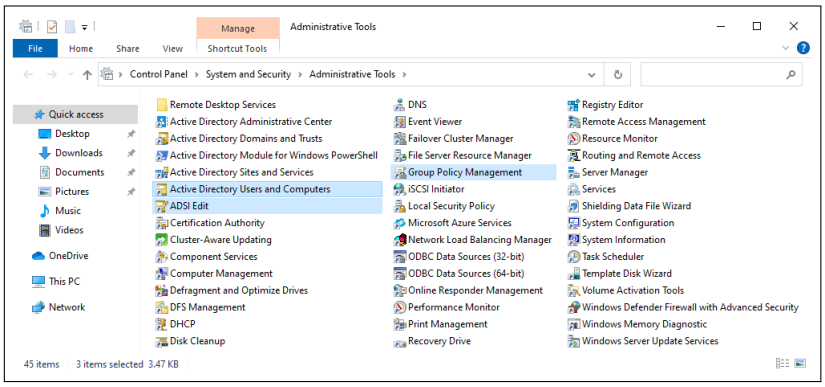
Obr. 3.4: Inštalácia RSAT na Windows 10

Alternatívne na Windows 10 je možné RSAT inštalovať po jednotlivých nástrojoch cez „⚙ ▸ Apps ▸ Optional features ▸ Add a feature“, kde do poľa „Find an available optional feature“ zadáme RSAT a zaškrtneme možnosti, ktoré chceme (napríklad „RSAT: Group Policy

[2] Súbory WindowsTH-RSAT_WS_1709-x64.msu a WindowsTH-RSAT_WS2016-x64.msu sú staršie verzie.

Management Tools“ a „RSAT: Active Directory Domain Services and Lightweight Direcotry Services Tools“ – okrem iného obsahujú ADSI Edit a ADUC) a stlačíme tlačidlo Install.

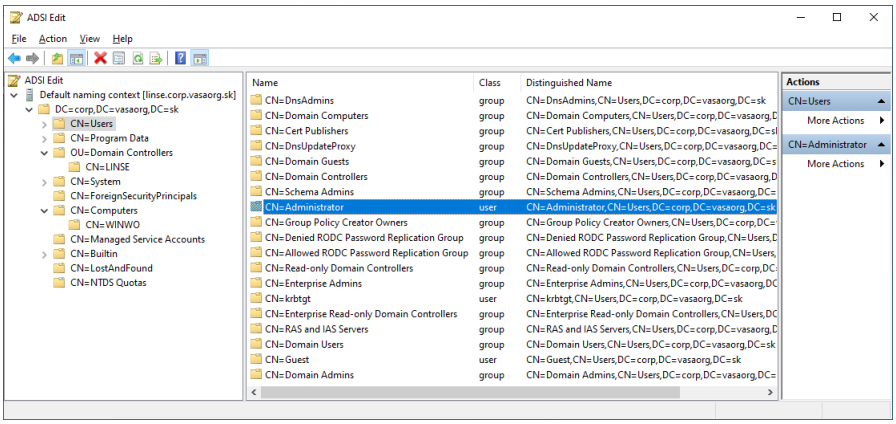
Po nainštalovaní RSAT je cez ovládací panel (v časti „Control Panel ▸ System and Security ▸ Administrative Tools“) dostupných vyše dvadsať nových programov pre správu domény (pozri obrázok 3.5). Bližšie si ukážeme ADSI Edit, GP Management a ADUC.



Obr. 3.5: Windows 10 Administrative Tools (vrátane RSAT nástrojov)

3.12 ADSI Edit

„Active Directory Service Interfaces Editor“ (ADSI Edit) je nízko-úrovňový nástroj pre priame prezeranie a editovanie (vytváranie, modifikovanie a mazanie) obsahu doménovej adresárovej služby. Najprv je potrebné pripojiť sa k severu cez položku v menu „Action ▸ Connect to...“. Ak sme prihlásení ako používateľ domény, tak stačí potvrdiť predvolené nastavenia.

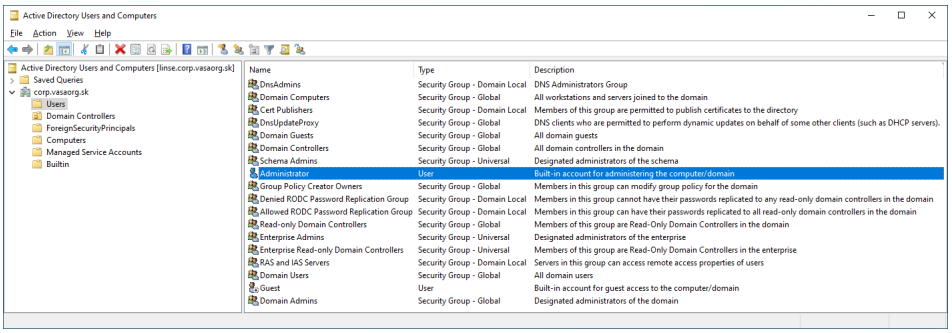


Obr. 3.6: RSAT – ADSI Edit

Na obrázku vyššie je zobrazený obsah uzla „Users“, v ktorom sa nachádzajú štandardní používatelia domény. Ďalej pod týmto uzlom sa nachádza uzol „Computers“, pod ktorým je možné vidieť počítače pridané do domény (v tomto prípade iba WINWO). Tieto dve časti adresára sa lepšie spravujú cez nástroj ADUC, ktorý je na to špeciálne určený.

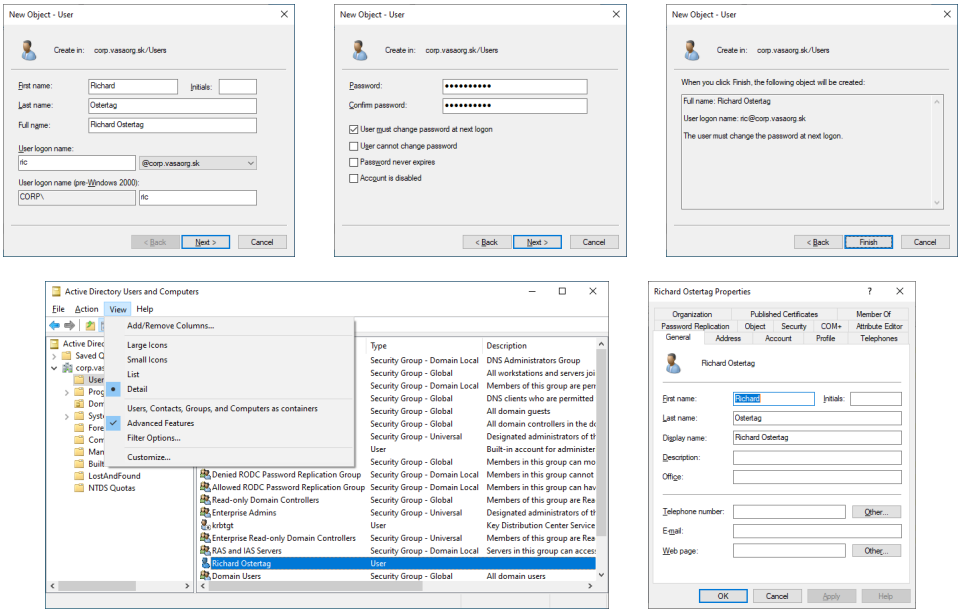
3.13 ADUC – pridanie nového používateľa

Nástroj „Active Directory Users and Computers“ (v skratke ADUC) slúži na pohodlnú správu doménových používateľských účtov a počítačov pridaných do domény. Práca s týmto nástrojom je pre bežné činnosti pohodlnejšia ako práca s nízko-úrovňovým ASDI Edit. Nasledujúci obrázok zobrazuje zoznam doménových používateľov a skupín v ADUC:



Obr. 3.7: RSAT – ADUC

Po kliknutí pravým tlačidlom myši na adresár „Users“ a vybratí možnosti „New ▸ User“ sa zobrazí dialógové okno „New Object - User“. Pomocou neho je možné vytvoriť nového používateľa domény. Nasledujúce obrázky demonštrujú vytvorenie doménového používateľa „Richard Ostertag“ s prihlasovacím menom `CORP\ric`.



Obr. 3.8: ADUC – vytvorenie nového doménového používateľa

Po stlačení tlačidla Finish v treťom okne sa nový používateľ pridá do adresára. Pokiaľ v menu „View“ je zapnutá možnosť „Advanced Features“ (pozri obrázok 3.8), tak po zobrazení vlastností používateľa sa ukáže viac podrobností (záložky „Published Certificated“, „Password

Replication“, „Object“, „Security“ a „Attribute Editor“). Okrem toho aj v samotnej adresárovej štruktúre (v ľavej časti okna) sa zobrazuje viac podrobností.

Ak by sme potrebovali, aby sa používateľ mohol prihlasovať na Linuxové počítače s jednoznačným unikátnym UID v rámci celej domény, tak je nutné pre nového používateľa ručne nastaviť potrebné RFC 2307 parametre cez „Attribute Editor“.

3.14 Exspirované heslo

Pri pokuse o prihlásenie sa môže stať, že použité heslo exspirovalo (podľa toho, ako je nastavená politika hesiel v doméne). Štandardne je exspirácia nového hesla nastavená na 42 dní. V prípade exspirácie je používateľ o tom upovedomený a je vyzvaný, aby zadal nové heslo:

```
tester@linse:~$ kinit ric  # nesprávne zadané heslo
Password for ric@CORP.VASAORG.SK:
kinit: Password incorrect while getting initial credentials
tester@linse:~$ kinit ric  # správne zadané heslo
Password for ric@CORP.VASAORG.SK:
Password expired.  You must change it now.
Enter new password:
Enter it again:
Password change rejected: Try a more complex password, or contact your
    administrator..  Please try again.

Enter new password:
Enter it again:
Warning: Your password will expire in 42 days on ...
```

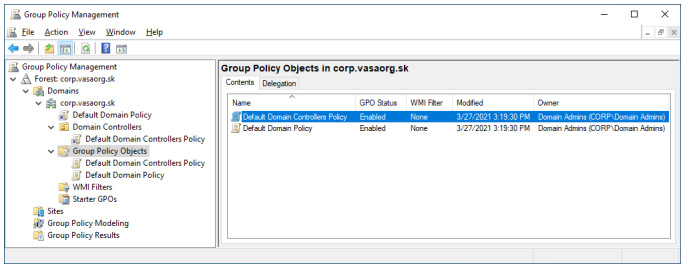
Ak nové heslo nespĺňa požiadavky aktuálnej politiky hesiel, tak je odmietnuté a používateľ musí zadať nové heslo. Po zadaní vhodného nového hesla je používateľ upozornený na dátum jeho exspirácie.

3.15 Samba 4 – skupinové politiky

Samba 4 vie obsluhovať skupinové politiky (group policy objects – GPO) pre klientov na platforme Microsoft Windows. Sama však ignoruje nastavenia GPO, ktoré by boli pre ňu aplikovateľné (napríklad minimálna dĺžka hesla). Existujú však produkty tretích strán (napríklad Centrify), ktoré aplikujú skupinové politiky v heterogénnych systémoch. Aj samotná Samba má ambíciu, aby od verzie 4.14 vedela o GPO, ktoré sú na Linuxe aplikovateľné a pravidelne (nie len pri štarte) aplikovala uvedené nastavenia s ohľadom na hierarchiu GPO (politika hesiel, plánovanie úloh, sudoers, …).

3.15.1 Group Policy Management

Posledným administratívnym nástrojom, ktorý si popíšeme, je nástroj „Group Policy Management“. Po jeho spustení (napríklad  + R, `gpmc.msc`) sa zobrazí nasledovné okno:



Obr. 3.9: Nástroj pre správu skupinových politík

Objekty skupinovej politiky (GPO) sa nachádzajú v adresári „Group Policy Objects“. V základnej inštalácii sú prítomné iba dva objekty: „Default Domain Controllers Policy“ a „Default Domain Policy“. Prvá politika je aplikovaná na všetky radiče domény (lebo odkaz na ňu je vytvorený v adresári „Domain Controllers“). Druhá je aplikovaná na všetko v doméne (lebo odkaz na ňu sa nachádza v adresári „corp.vasaorg.sk“). Obe politiky sú však štandardne prázdne, teda nič nemenia, nevynucujú.

3.15.2 Výpis všetkých skupinových politík

Na Samba serveri je možné vypísať všetky objekty skupinovej politiky príkazom:

```
1  tester@linse:~$ sudo samba-tool gpo listall
2  GPO          : {31B2F340-016D-11D2-945F-00C04FB984F9}
3  display name : Default Domain Policy
4  path         : \\corp.vasaorg.sk\sysvol\corp.vasaorg.sk\Policies\
     ↪{31B2F340-016D-11D2-945F-00C04FB984F9}
5  dn           : CN={31B2F340-016D-11D2-945F-00C04FB984F9},
     ↪CN=Policies,CN=System,DC=corp,DC=vasaorg,DC=sk
6  version      : 0
7  flags        : NONE
8
9  GPO          : {6AC1786C-016F-11D2-945F-00C04FB984F9}
10 display name : Default Domain Controllers Policy
11 path         : \\corp.vasaorg.sk\sysvol\corp.vasaorg.sk\Policies\
     ↪{6AC1786C-016F-11D2-945F-00C04FB984F9}
12 dn           : CN={6AC1786C-016F-11D2-945F-00C04FB984F9},
     ↪CN=Policies,CN=System,DC=corp,DC=vasaorg,DC=sk
13 version      : 0
14 flags        : NONE
```

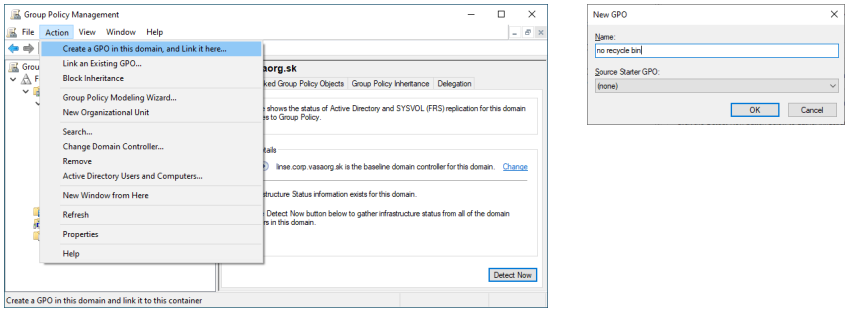
Vo výpise môžeme identifikovať obe základné skupinové politiky „Default Domain Policy“ a „Default Domain Controllers Policy“. Okrem iných podrobností je možné zistiť ich umiestnenie v zdieľanom adresári `sysvol`. Za predpokladu, že poznáme lokálnu cestu k zdieľanému adresáru `sysvol` (štandardne `/var/lib/samba/sysvol`), tak vieme zistiť aj to, kde sa GPO nachádza na lokálnom súborovom systéme.

3.15.3 Vytvorenie nového GPO

Pre demonštráciu spôsobu práce s GPO vytvoríme novú politiku, ktorá odstráni odpadkový kôš (Recycke Bin) z pracovnej plochy operačného systému Microsoft Windows.

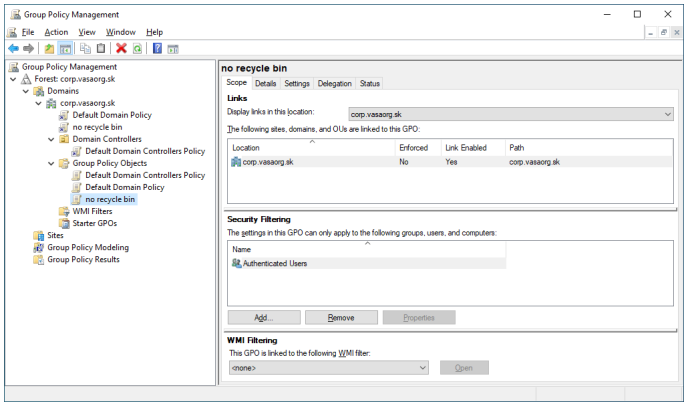
Vytvorenie GPO prebieha v dvoch krokoch. Najprv spustíme nástroj „Group Policy Management“ a zvolíme adresár „corp.vasaorg.sk ▸ Group Policy Objects“ (pozri obrázok 3.9), kde vytvoríme nový GPO. Potom treba vytvoriť zástupcu GPO na nejakom mieste adresárovej štruktúry. Následkom toho sa bude GPO aplikovať na všetky objekty nachádzajúce sa v tomto adresári a pod ním. Ak by sme nevytvorili žiadneho zástupcu, tak by GPO síce existoval, ale na nič by nemal vplyv. Vo všeobecnosti môže byť na GPO aj viacero odkazov.

Skoro vždy chceme vykonať obe činnosti a preto, keď sme na „corp.vasaorg.sk“, tak je v menu „Action“ položka „Create a GPO in this domain, and Link it here...“, ktorá vytvorí nové GPO v adresári „Group Policy Objects“ a zároveň umiestni odkaz naň do vybraného adresára. Po zvolení tejto možnosti je používateľ vyzvaný na zadanie mena pre nové GPO:



Obr. 3.10: Vytvorenie a pomenovanie nového objektu skupinovej politiky

Potvrdením zvoleného mena sa vytvorí nový objekt skupinovej politiky. Zároveň sa vytvorí aj odkaz naň vo vybranom adresári:

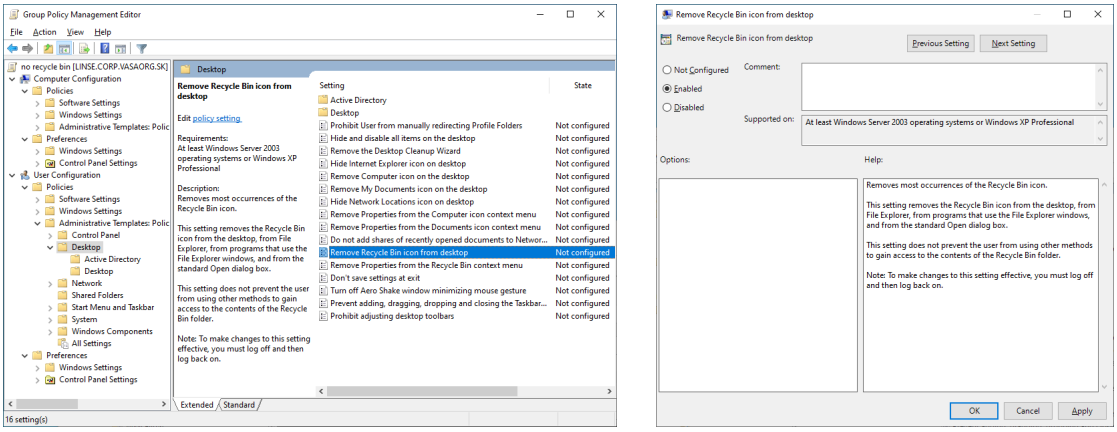


Obr. 3.11: Umiestnenie nového GPO aj s jeho odkazom

Pokiaľ nechceme ponechať skupinovú politiku prázdnu, tak ďalším krokom je jej editácia.

3.15.4 Editácia obsahu GPO

Editácia skupinovej politiky je možná po kliknutí na ňu alebo ktoréhokoľvek jej zástupcu. Následne z menu zvolíme položku „Action ▸ Edit...“, čím sa otvorí editor skupinovej politiky:

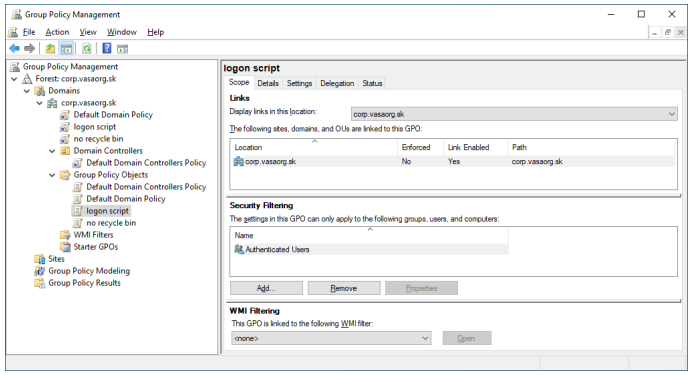


Obr. 3.12: Editor skupinovej politiky

V okne „Group Policy Management Editor“ otvoríme na ľavej strane cestu „User Configuration ▸ Policies ▸ Administrative Templates[3] ▸ Desktop“. Potom na pravej strane urobíme dvojklik na „Remove Recycle Bin icon from desktop“, čím otvoríme okno „Remove Recycle Bin icon from desktop“ (na obrázku 3.12 vpravo). V tomto okne povolíme odstránenie ikony koša kliknutím na „Enabled“ a uložíme zmeny kliknutím na tlačidlo OK. Ak sa teraz prihlásime na nejaký počítač v doméne, tak na jeho pracovnej ploche nebude zobrazená ikona odpadkového koša. Overiť vytvorenie novej skupinovej politiky na Samba serveri môžeme pomocou postupu, ktorý uvedieme v podčasti 3.15.6 na strane 58.

3.15.5 Vytvorenie prihlasovacieho skriptu

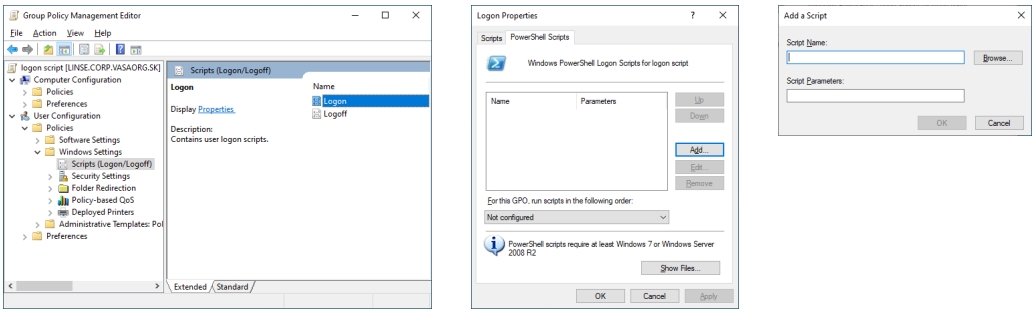
Ako ďalší príklad skupinovej politiky si ukážeme vytvorenie prihlasovacieho skriptu, ktorý sa automaticky spustí na každom počítači v doméne po prihlásení používateľa. Rovnako ako v predošlom prípade, najprv v nástroji „Group Policy Management“ vyberieme adresár „corp.vasaorg.sk“ a potom z menu vyberieme položku „Action ▸ Create a GPO in this domain, and Link it here...“. Ako meno pre nové GPO zadáme: „logon script“. Po potvrdení mena bude vytvorená nová politika spolu so zástupcom (pozri obrázok na okraji strany).



Po vybraní skupinovej politiky (alebo ktoréhokoľvek jej zástupcu) cez menu „Action ▸ Edit...“ otvoríme okno pre editáciu skupinovej politiky, v ktorom na ľavej strane otvoríme

[3]Definície týchto šablón sa nachádzajú v ADMX súboroch na lokálnom počítači. ADMX súbory sú vlastne XML súbory, ktoré umožňujú definovať šablónu pre skupinové politiky založené na modifikácii databázy Registry. Šablóna zjednodušuje prácu tým, že skrýva technické detaily modifikácie tejto databázy a poskytuje definíciu používateľského rozhrania s možnosťami a nápovedou.

cestu „User Configuration ▸ Policies ▸ Windows Settings ▸ Scripts (Logon/Logoff)“. Potom na pravej strane dvojklikom na „Logon“ otvoríme okno „Logon Properties“ a prepneme sa na záložku „PowerShell Scripts“. Po kliknutí na tlačidlo Add... sa zobrazí okno „Add a Script“ pre výber súboru. Stlačíme tlačidlo Browse... a z otvoreného okna nakopírujeme cestu, v ktorej sa očakáva umiestnenie prihlasovacieho skriptu (pozri obrázky nižšie).



Obr. 3.13: Editovanie politiky pre prihlasovací skript

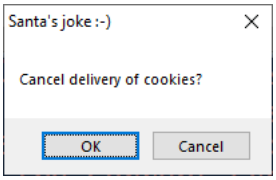
V našom prípade bola cesta nasledovná:

```
\\corp.vasaorg.sk\SysVol\corp.vasaorg.sk\Policies\
  ↪{45A9653F-BDC6-4CD3-9CD3-90328FE8B3CD}\User\Scripts\Logon
```

Časť medzi kučeravými zátvorkami bude zakaždým iná. Do tohto adresára uložíme skript, ktorý po spustení vytvorí dialógové okno a v ňom zobrazí otázku, či chceme zrušiť doručenie koláčikov s možnosťami OK alebo Cancel. Takýto skript napísaný v jazyku PowerShell môže vyzerať nasledovne:

```
#Set-ExecutionPolicy -ExecutionPolicy Unrestricted

$wshell = New-Object -ComObject Wscript.Shell
$wshell.Popup("Cancel delivery of cookies?", 0, "Santa's joke :-)", 0x1)
```



Po jeho uložení pod menom `hello.ps1` (do vyššie uvedenej cesty) ho vyberieme v otvorenom okne „Add a Script“ pre výber skriptu a voľbu potvrdíme tlačidlom OK. Následne stlačením OK zavrieme aj okno „Logon Properties“. Odteraz sa každému používateľovi po prihlásení do domény ukáže „mikulášske“ dialógové okno zobrazené na okraji.

3.15.6 Nové politiky z pohľadu samba-tool

Pre kontrolu môžeme v predchádzajúcich bodoch vytvorené bezpečnostné politiky zobraziť na Linuxe pomocou príkazu `samba-tool` (prvé dve politiky sme vynechali lebo ide o štandardné politiky, ktoré sme už spomínali):

```
tester@linse:~$ sudo samba-tool gpo listall
GPO          : {31B2F340-016D-11D2-945F-00C04FB984F9}
display name : Default Domain Policy
...

GPO          : {6AC1786C-016F-11D2-945F-00C04FB984F9}
display name : Default Domain Controllers Policy
...
```

```
GPO           : {8E7D77C9-2724-4C6A-AC3F-00F4FAB59876}
display name  : no recycle bin
path          : \\corp.vasaorg.sk\SysVol\corp.vasaorg.sk\Policies\{8E7D77C9-2724-4C6A-AC3F-00F4FAB59876}
dn            : CN={8E7D77C9-2724-4C6A-AC3F-00F4FAB59876},CN=Policies,CN=System,DC=corp,DC=vasaorg,DC=sk
version       : 65536
flags         : NONE

GPO           : {45A9653F-BDC6-4CD3-9CD3-90328FE8B3CD}
display name  : logon script
path          : \\corp.vasaorg.sk\SysVol\corp.vasaorg.sk\Policies\{45A9653F-BDC6-4CD3-9CD3-90328FE8B3CD}
dn            : CN={45A9653F-BDC6-4CD3-9CD3-90328FE8B3CD},CN=Policies,CN=System,DC=corp,DC=vasaorg,DC=sk
version       : 65536
flags         : NONE
```

3.16 Rozšírené atribúty súborov

Pri inštalácii balíka Samba sme spomínali, že je potrebné, aby súborový systém, na ktorom bude uložený obsah zdieľaného priečinka sysvol podporoval rozšírené atribúty. Je to z toho dôvodu, že Samba využíva rozšírené atribúty pre uloženie dodatočných informácií o súboroch. Aké rozšírené atribúty sú použité na zvolenom súbore, môžeme zistiť napríklad nasledovným príkazom:

```
tester@linse:~$ sudo getfattr -m- /var/lib/samba/sysvol/corp.vasaorg.sk/Policies/\{45A9653F-BDC6-4CD3-9CD3-90328FE8B3CD\}/User/Scripts/Logon/hello.ps1
getfattr: Removing leading '/' from absolute path names
# file: var/lib/samba/sysvol/corp.vasaorg.sk/.../Logon/hello.ps1
security.NTACL
system.posix_acl_access
user.DOSATTRIB
```

Bez voľby `-m-` by príkaz `getfattr` nezobrazil atribúty z kategórie security a system. Preto by nebolo vidno napríklad pre Sambu dôležitý `security.NTACL` atribút. Jeho obsah je možné získať príkazom:

```
tester@linse:~$ sudo getfattr -n security.NTACL /var/lib/samba/sysvol/corp.vasaorg.sk/Policies/\{45A9653F-BDC6-4CD3-9CD3-90328FE8B3CD\}/User/Scripts/Logon/hello.ps1
getfattr: Removing leading '/' from absolute path names
# file: var/lib/samba/sysvol/corp.vasaorg.sk/.../Logon/hello.ps1
security.NTACL=0sBAAEAAAAAgAEAAIAAQAukVmQS7EwKWq20coMKVARybikieYkb+Vbk/h2VdX5B
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAcG9zaXhfYWNsAP7b2wqrJNcBw9s9je5
    YrTBzq4AVgHcINLyYBW5ZVukj9AfMbD3I+8QAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAEABIS0AAAAxAAAAAAAAADgAAAAQIAAAAAAAUgAAAAIAIAAAEFAAAAAAAFFQAAAA7F5fd
    4JIH3euKOywECAAACAKQABgAAAAQJAD/AR8AAQUAAAAAAAUVAAAADsXl93gkgfd64o7LAAIAA
    AAQJAD/AR8AAQUAAAAAAAUVAAAADsXl93gkgfd64o7LBwIAAAAQGAD/AR8AAQIAAAAAAAUgAAA
    AIAIAAAAQFAD/AR8AAQEAAAAAAAUSAAAAABAUAKkAEgABAQAAAAAABQsAAAAAEBQAqQASAAEBA
    AAAAAAFCQAAAA==
```

Tento obsah je však pre bežného používateľa nečitateľný. Bežný používateľ si práva môže pozrieť cez klasické Windowsové nástroje zobrazením vlastností tohto zdieľaného súboru.

Kapitola 4

Cygwin

Cygwin poskytuje pre Windows veľkú zbierku štandardných GNU a „open source“ nástrojov, ktoré sú bežné pre mnohé Unixové distribúcie. Okrem toho poskytuje knižnicu (DLL) implementujúcu POSIX API, to znamená systémové volania a prostredie, ktoré Unixové aplikácie očakávajú. Vďaka tomu je možné portovať mnohé Unixové programy na Windows bez výraznejších zmien v zdrojovom kóde. Cygwin neumožňuje priame spúšťanie „binárie“ Unixových aplikácií na Windows. Aplikácie treba minimálne prekompilovať zo zdrojových súborov s použitím Cygwin knižnice.

Domovská stránka Cygwin projektu je na adrese https://www.cygwin.com/. Cygwin je k dispozícii zadarmo v podstate pod GPL licenciou. Avšak pre portovanie proprietárnej aplikácie (t.j. bez následného zverejnenia jej zdrojového kódu) na Windows pomocou Cygwinu je potrebné mať zakúpenú špeciálnu licenciu od firmy Red Hat. Podrobnosti je možné nájsť na stránke https://cygwin.com/licensing.html.

4.1 Cygwin – inštalácia

Inštalačný súbor pre 64-bitový Windows sa nachádza na adrese (oficiálna stránka projektu):

https://cygwin.com/setup-x86_64.exe

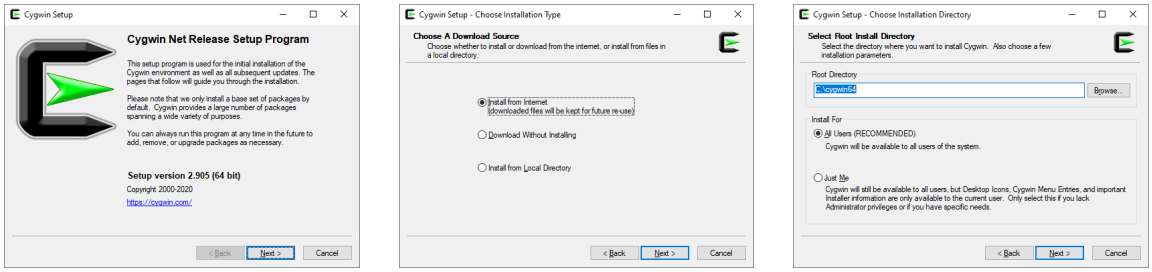
Tento program je možné kedykoľvek spustiť. Pri prvom spustení sa vykoná nová inštalácia Cygwinu. Pri ďalších spusteniach sa už urobí iba aktualizácia existujúcej inštalácie. Staršiu inštaláciu je možné aktualizovať aj novšou verziou inštalačného programu setup-x86_64.exe.

Inštalácia je možná aj bez administrátorských oprávnení. Tie sú potrebné len pre inštaláciu pre všetkých používateľov na danom PC. Pokiaľ používateľ nemá administrátorské oprávnenia, tak je možné inštaláciu spustiť s parametrom `--no-admin`:

```
1 PS C:\Users\Ric\Downloads> .\setup-x86_64.exe --no-admin
```

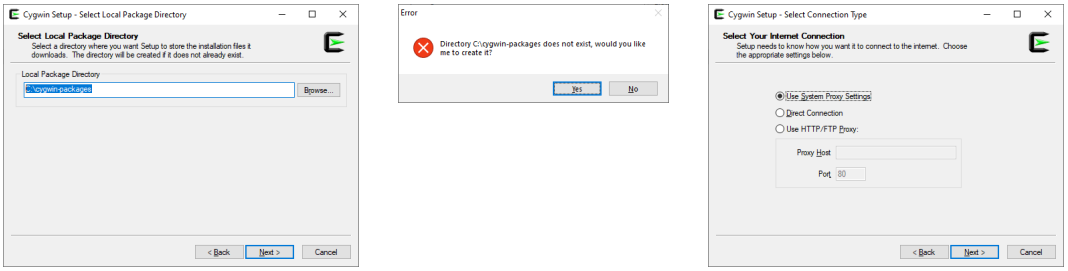
Po spustení inštalácie sa zobrazí úvodné okno s číslom verzie inštalátora. Samotný inštalátor neobsahuje všetky dáta potrebné na nainštalovanie Cygwinu. Preto ďalšie okno umožňuje zvoliť typ inštalácie. Prvá možnosť stiahne inštalačné balíčky jednotlivých programov

z Internetu a potom ich nainštaluje. Druhá možnosť ich iba stiahne ale nenainštaluje. Posledná možnosť slúži na nainštalovanie už stiahnutých balíčkov z lokálneho adresára. Vyberieme teda prvú možnosť. V nasledujúcom okne zvolíme inštalačný adresár pre samotný Cygwin (štandardne `C:\cygwin64`).



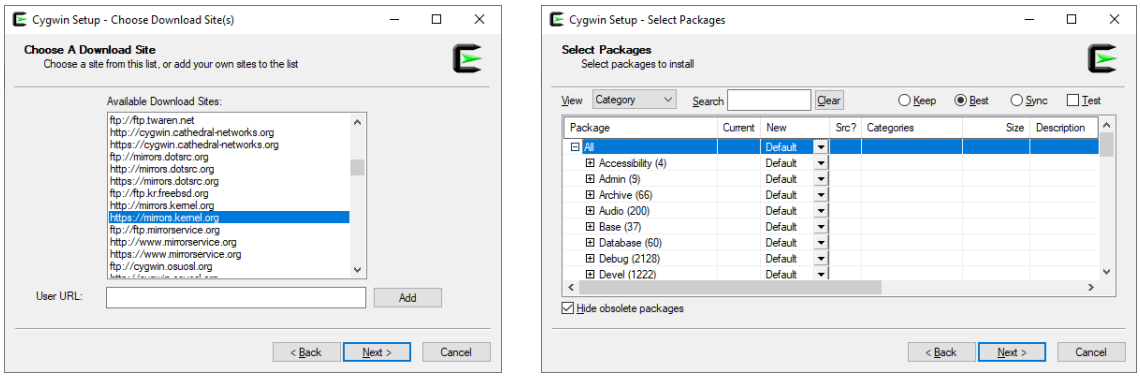
Obr. 4.1: Spustenie inštalácie systému Cygwin

V ďalšom okne zas vyberieme adresár pre lokálne uloženie stiahnutých balíčkov (navrhujeme zvoliť `C:\cygwin-packages`), pričom potvrdíme vytvorenie nového adresára. Pred samotným stiahnutím zoznamu dostupných balíčkov je potrebné zvoliť spôsob pripojenia. Navrhujeme ponechať štandardné nastavenie „Use System Proxy Settings“ .



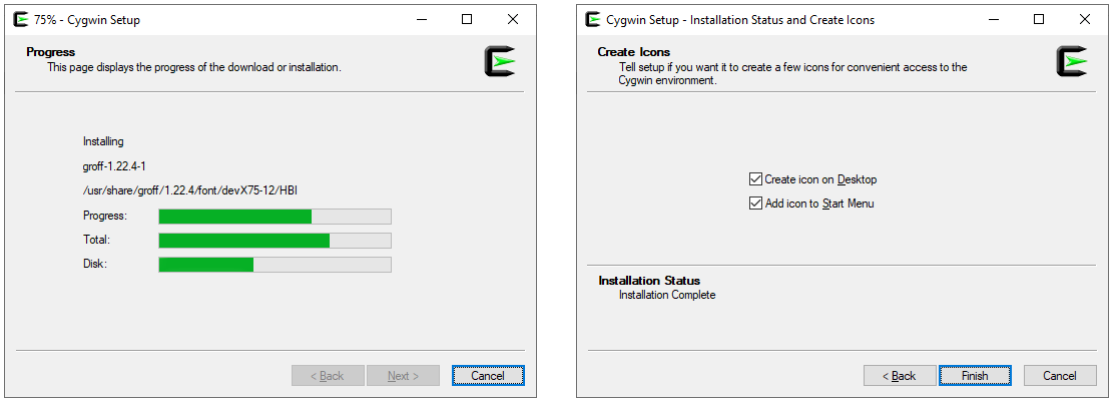
Obr. 4.2: Zmena adresára s balíčkami a nastavenie pripojenia k Internetu

Ďalším krokom je výber servera, z ktorého sa budú balíčky sťahovať. Jeden z dlhodobo najspoľahlivejších serverov je server `https://mirrors.kernel.org`. Po stiahnutí zoznamu balíčkov si používateľ môže vybrať, aké balíčky si chce nainštalovať. Základný výber je už spravený, preto používateľ môže prejsť rovno na ďalší krok stlačením Next >.



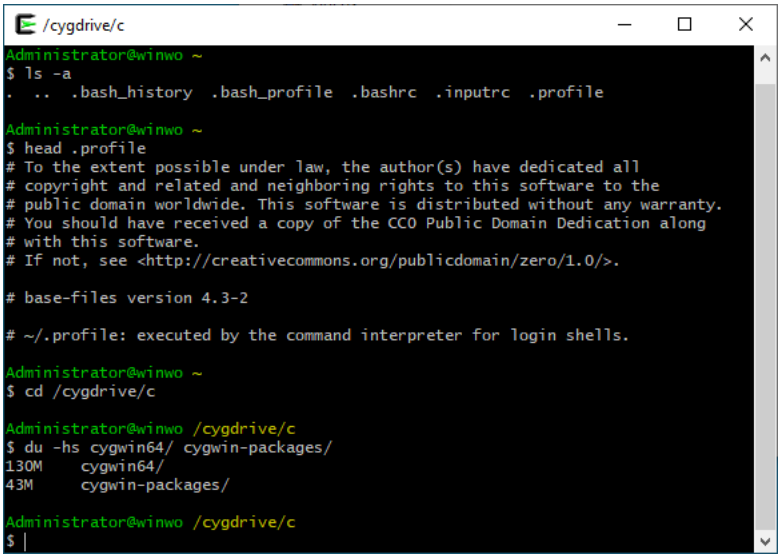
Obr. 4.3: Zvolenie servera s balíčkami a ich základný výber

Nasleduje potvrdenie výberu v okne „Review and confirm changes“ stlačením tlačidla Next >. Potom začne sťahovanie všetkých vybraných balíčkov. Po ich stiahnutí sa automaticky prejde k inštalácii. Nakoniec je ponúknutá možnosť vytvoriť ikonu na pracovnej ploche a v zozname programov. Inštaláciu dokončíme kliknutím na tlačidlo Finish.



Obr. 4.4: Dokončenie inštalácie Cygwinu

Pomocou ikony vytvorenej na ploche je možné spustiť „Cygwin64 Terminal“, ktorý je vstupným bodom do Unixového sveta Cygwinu na Windows:

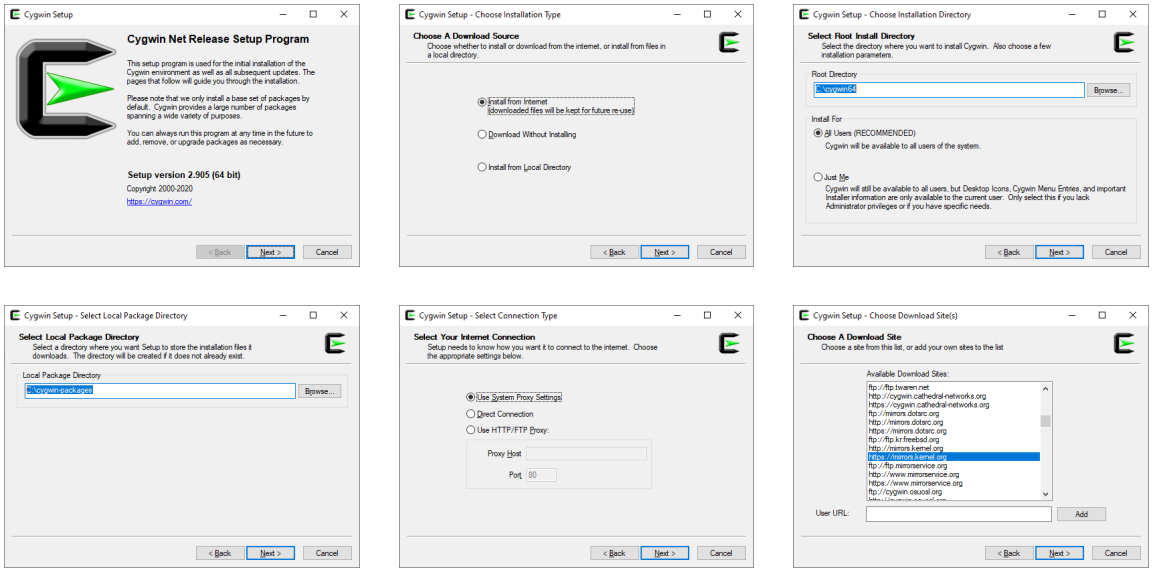


Obr. 4.5: Cygwin64 Terminal

Koreňový adresár Cygwinu je mapovaný do inštalačného adresára Cygwinu – v tomto prípade teda do adresára `c:\cygwin64`. Preto nie je možné v terminálovom okne pomocou príkazu `cd` opustiť tento priečinok. Do koreňového adresára akéhokoľvek Windows disku sa však dá dostať pomocou cesty `/cygdrive/disk` (napríklad `/cygdrive/c`). Základná inštalácia obsahuje mnohé užitočné Unixové nástroje, ako napríklad príkaz `ssh`. Žiaľ editor `vim` do tohto výberu nepatrí. Preto si v nasledujúcej časti ukážeme, ako ho doinštalovať.

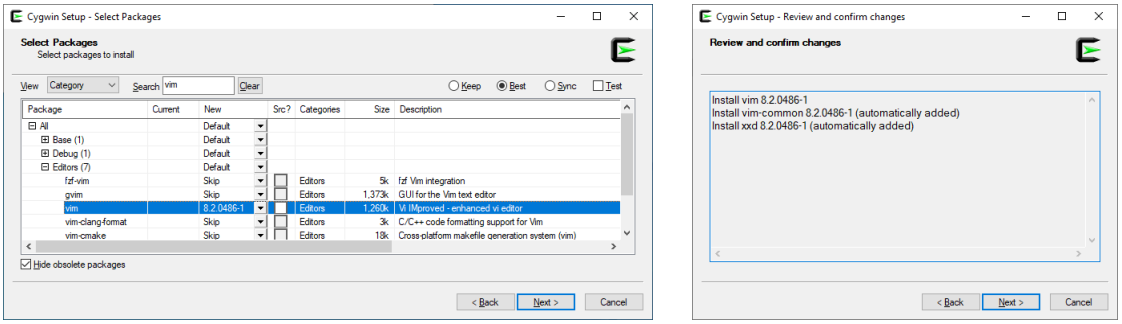
4.2 Cygwin – inštalácia balíčka

Rozhodli sme sa, že si chceme do Cygwinu doinštalovať náš obľúbený editor Vim. Preto opätovne spustíme `setup-x86_64.exe`. Tentokrát však za účelom aktualizácie/doplnenia nainštalovaných balíkov. Prvé kroky inštalácie sú úplne rovnaké ako v predošlom príklade:



Obr. 4.6: Opätovné spustenie inštalácie Cygwin

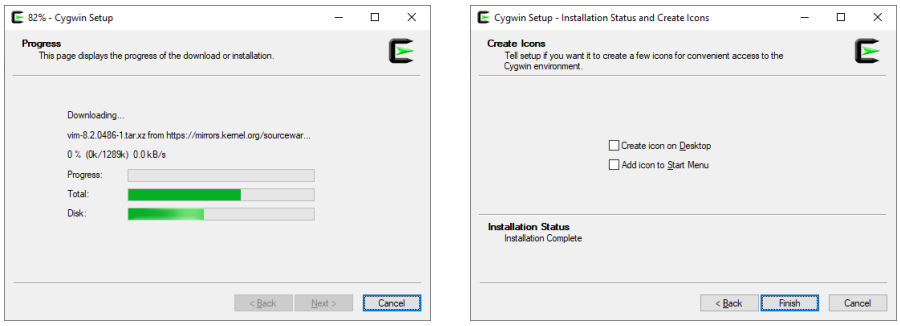
V momente, keď inštalačný program ponúkne aktualizovaný zoznam dostupných balíkov, tak „View“ nastavíme na „Category“. Do poľa „Search“ zadáme „vim“, čím zúžime zoznam ponúkaných balíkov na rozumnú mieru. Následne rozbalíme adresár „Editors“ a klikneme na „Skip“ pri balíku „vim“, a vyberieme verziu, ktorú chceme nainštalovať. Ku každému balíčku obsahuje Cygwin aj niekoľko starších verzií. Namiesto (prípadne popri) binárnej distribúcii balíka je možné dať nainštalovať aj zdrojový kód balíka (voľba „Src?“). Túto možnosť teraz nevyužijeme. Mala by zmysel, ak by sme chceli program meniť, či skompilovať s inými nastaveniami, ako sú štandardné. Ďalej pokračujeme stlačením Next >.



Obr. 4.7: Výber balíčka vim pre inštaláciu do systému Cygwin

Po odsúhlasení inštalácie potrebných závislostí sa spustí sťahovanie a inštalácia nanovo vybraných balíkov. Ak sa medzičasom objavila aktualizácia na niektorý už nainštalovaný

balík, tak aj táto sa automaticky stiahne a nainštaluje. V poslednom kroku sa, na rozdiel od prvotnej inštalácie, štandardne neponúka vytváranie ikon (pozri obrázok 4.8 vpravo).



Obr. 4.8: Priebeh inštalácie balíčka vim do systému Cygwin

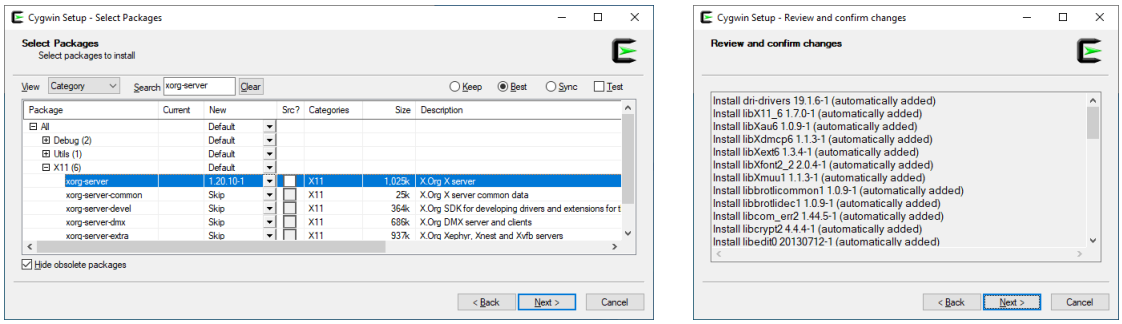
Po dokončení inštalácie a otvorení Cygwin terminálu je už možné z príkazového riadku spustiť vim. Jeho funkcionalita je rovnaká ako je zvykom na Unixových počítačoch (ide o ten istý program, len portovaný na Cygwin).

4.3 Cygwin/X

Ak potrebujeme na vzdialenom počítači používať aj aplikácie, ktoré majú grafické používateľské rozhranie, tak okrem SSH potrebujeme na lokálnom počítači mať nainštalovaný aj X server. Súčasťou Cygwin je Cygwin/X (`https://x.cygwin.com/`). X server však štandardne nie je nainštalovaný.

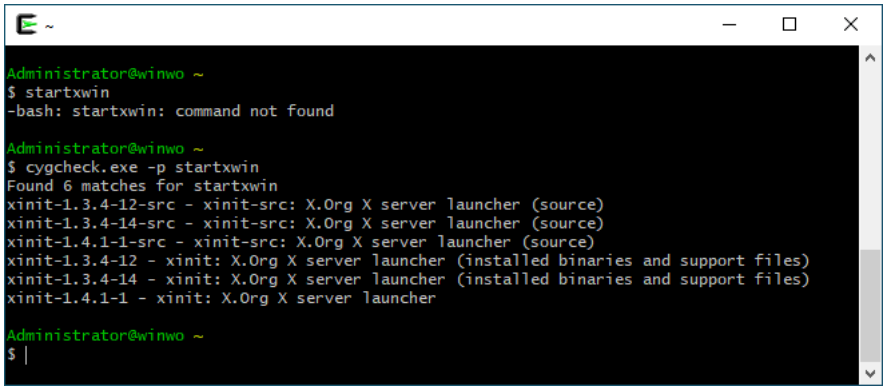
4.3.1 Inštalácia

Po opätovnom spustení inštalačného programu a preklikaní sa úvodnými obrazovkami (pre podrobnosti pozri obrázok 4.6) treba k inštalácii pridať balík xorg-server a doinštalovať aj všetky jeho závislosti:



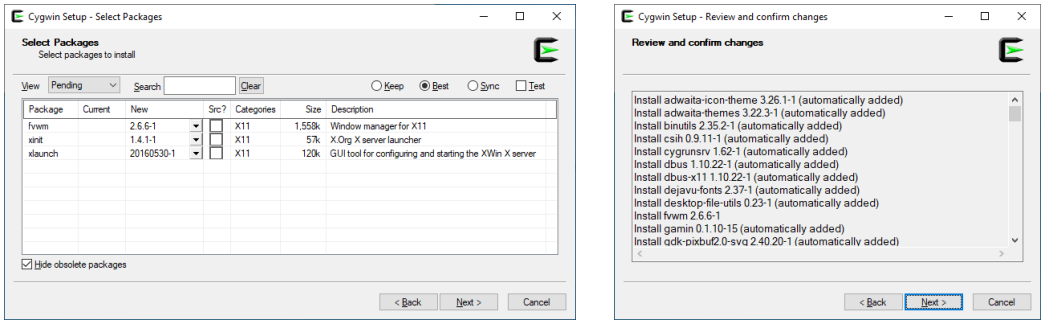
Obr. 4.9: Výber balíčka xorg-server

Po skončení inštalácie môžeme vyskúšať spustiť X server príkazom `startxwin` z terminálového okna systému Cygwin:



Obr. 4.10: Výber balíčka xorg-server

Tento príkaz však neexistuje, pretože sme pri inštalácii nezvolili všetky potrebné balíky. Na tomto príklade demonštrujeme, ako sa dá pomocou príkazu `cygcheck.exe -p REGEXP` prehľadať celý repozitár balíkov a zistiť, aké balíky obsahujú zadaný regulárny výraz. V tomto prípade sme zistili, že výraz startxwin obsahujú rôzne verzie balíka xinit. Pridáme teda ešte najnovšiu verziu (v tomto prípade 1.4.1-1) balíka xinit. Okrem toho rovno pridáme aj balíky xlaunch a fvwm, ktoré budeme neskôr potrebovať.



Obr. 4.11: Výber balíčkov fvwm, xinit a xlaunch

Inštalácia Cygwin v tomto okamihu zaberá 575 MB a ďalších 133 MB zaberá repozitár so stiahnutými balíkmi. Po dokončení tejto inštalácie je Cygwin/X kompletne nainštalovaný. Pred jeho spustením je ale potrebné ozrejmiť základné možnosti jeho používania.

4.3.2 Integrácia s Windows

Cygwin/X má schránku (clipboard) integrovanú s operačným systémom Windows. Preto je možné kopírovať medzi Windows oknami a X oknami pomocou príkazov kopíruj a vlož. Samotný X server je možné spustiť v troch (windowing) módoch: zakorenenom (rooted), viacoknovom (multiwindow) alebo bezkoreňovom (rootless).

V zakorenenom móde (rooted mode) je každá X obrazovka (screen) zobrazená ako jedno Windows okno. Všetky X okná tejto obrazovky sa zobrazujú v rámci tohto Windows okna.

V zakorenenom móde si môže používateľ zvoliť vlastného správcu okien (window manager), napríklad „F Virtual Window Manager“ (`/usr/bin/fvwm2`).

Vo viacoknovom móde (multiwindow mode) je použitý interný správca okien a každé X okno najvyššej úrovne (top-level) je samostatné Windows okno. Tento mód najnatívnejšie integruje okná vzdialenej pracovnej plochy do lokálneho operačného systému.

V bezkoreňovom móde (rootless mode) sa koreňové (root) X okno nezobrazuje, ale zobrazujú sa okná najvyššej úrovne (top-level) ako samostatné okná. Tento mód je kombináciou predošlých dvoch módov. Umožňuje natívnejšiu integráciu s Windows, ale s použitím vybraného správcu okien.

4.3.3 Možnosti spustenia

Spôsob spustenia X servera sa líši práve podľa toho, v akom móde chceme X server prevádzkovať. Spustenie vo viacoknovom móde (multiwindow mode) sa vykoná príkazom `startxwin` z terminálového okna. Alternatívne je možné spustiť program „XWin Server“ cez štartmenu. Konfiguráciu X servera je možné prispôsobiť v súbore `~/.startxwinrc`. Jeho základnú verziu je možné vytvoriť príkazom:

```
1 $ cp /etc/X11/xinit/startxwinrc ~/.startxwinrc
```

Vo viacoknovom móde X server beží aj po skončení tohto skriptu.

Spustiť X server v zakorenenom móde (rooted mode) je možné príkazom `startx`. Tento príkaz však hneď skončí lebo štandardne nie je nakonfigurované nič, čo by spustil. Ak chceme spustiť iba jeden program, môžeme ho odovzdať ako parameter, napríklad príkazom `startx /usr/bin/fvwm2` sa spustí X server so správcom okien fvwm2. Podrobnejšie sa dá X server v tomto móde konfigurovať (vrátane aplikácií ktoré sa majú spustiť) v súbore `~/.xinitrc`. Jeho základnú verziu môžeme vytvoriť príkazom:

```
1 $ cp /etc/X11/xinit/xinitrc ~/.xinitrc
```

Príkaz `startx` skončí hneď, ako skončí skript `~/.xinitrc`.

X server je možné spustiť aj cez program „XLaunch“ zo štart menu. Po jeho spustení sa najprv zobrazí grafický sprievodca, v ktorom je možné jednoducho zvoliť mód a iné parametre spustenia X servera.

4.3.3.1 XWin Server

V tejto časti podrobnejšie popíšeme, ako spustiť X server a pripojiť sa na vzdialenú pracovnú plochu vo viacoknovom móde. Najprv je potrebné spustiť „XWin Server“ a „Cygwin64 Terminal“ alebo použiť „xterm“. Ak sa používa „Cygwin64 Terminal“, je ešte potrebné nastaviť premennú prostredia `DISPLAY`:

```
1 $ export DISPLAY=:0.0
```

Tento krok nie je nutný, pokiaľ sa používa „xterm“, pretože v tomto prípade už musí byť premenná `DISPLAY` nastavená, keďže „xterm“ sa spúšťa cez „XWin Server“. „Cygwin64

Terminal“ nie je X-ová aplikácia. Ďalším krokom je spustiť v termináli SSH pripojenie na vzdialený počítač s parametrom `-Y` pre presmerovanie X-ov na lokálny počítač:

```
$ ssh -Y tester@linse
```

Potom na vzdialenom počítači spustíme nejakú X windows aplikáciu, napríklad xcalc:

```
tester@linse:~$ xcalc &
```

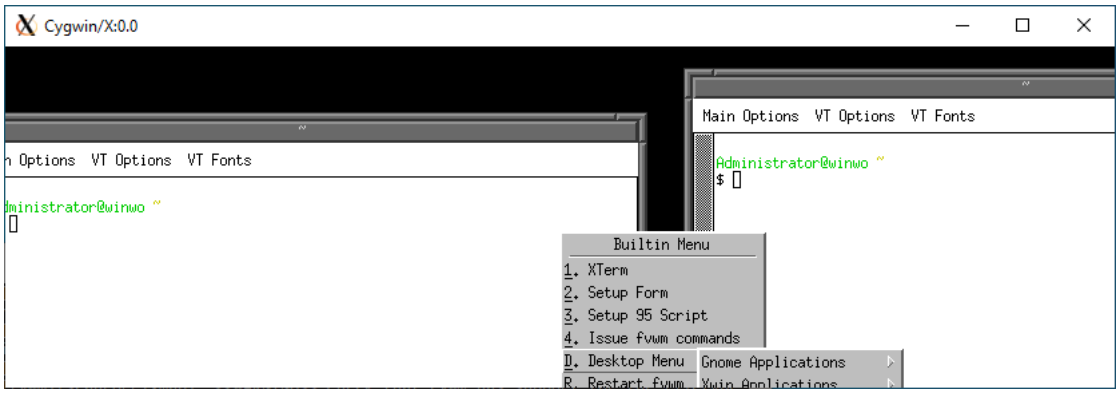
Pokiaľ vzdialený SSH server nedovoľuje preposielanie X-ov, tak je potrebné upraviť jeho konfiguračný súbor `/etc/ssh/sshd_config` tak, aby obsahoval `X11Forwarding yes`. Ak všetko prebehlo správne, tak sa na pracovnej ploche Windows objaví nové okno s kalkulačkou xcalc (pozri obrázok na okraji strany).

4.3.3.2 startx /usr/bin/fvwm2

V tejto časti ukážeme, ako vyzerá X server spustený v zakorenenom móde. Najprv spustíme Cygwin64 Terminal, v ktorom zadáme príkaz:

```
$ startx /usr/bin/fvwm2
```

Po spustení X servera sa zobrazí prázdne koreňové okno. Všetky okná sa budú zobrazovať v tomto okne. Kliknutím na plochu sa zobrazí ponuka, z ktorej vyberieme spustenie terminálu XTerm. V terminálovom okne by sme sa potom mohli pomocou príkazu `ssh` prihlásiť na vzdialený počítač. V tomto prípade nie je potrebné ručne nastaviť premennú prostredia `DISPLAY`, keďže XTerm už beží na X serveri a táto premenná je teda už nastavená.

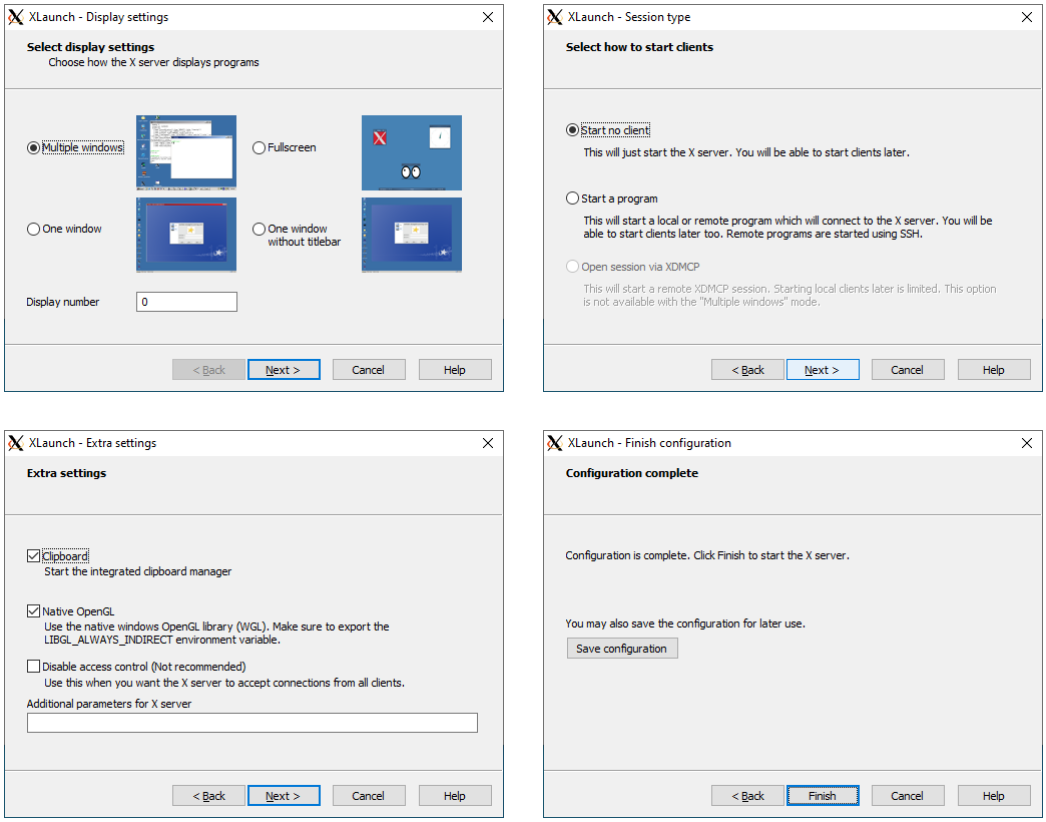


Obr. 4.12: X server v zakorenenom móde

Ako vidno na obrázku vyššie, okná aplikácií v tomto móde nemôžu opustiť koreňové okno. Používajú zvoleného Unixového správcu okien, preto nemajú natívny Windows-vzhľad.

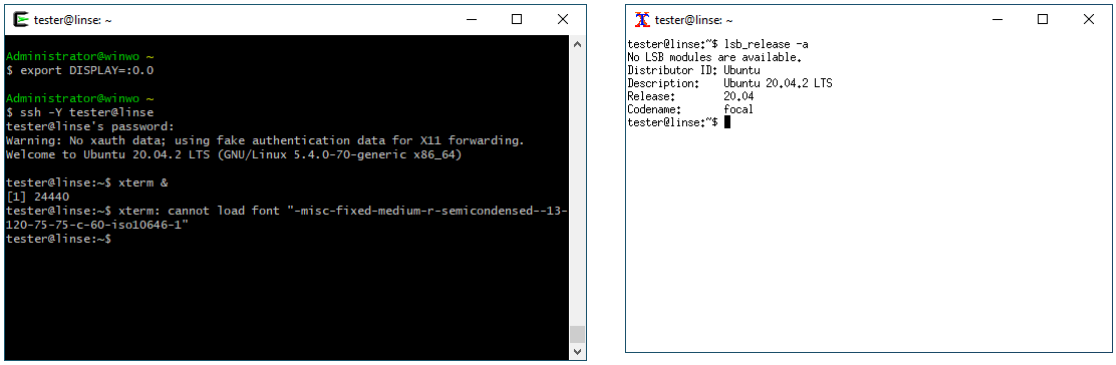
4.3.3.3 XLaunch

Pre niektorých používateľov bude najpohodlnejším spôsobom spustenia X servera aplikácia „XLaunch“, ktorú je možné spustiť cez štart menu. V niekoľkých dialógových oknách vedie používateľa cez rôzne konfiguračné možnosti X servera až po jeho spustenie, pričom zmysel jednotlivých možností je graficky znázornený alebo podrobnejšie popísaný.



Obr. 4.13: Spustenie X servera cez XLaunch

V tomto príklade sme spustili X server opäť vo viacoknovom móde s podporou integrácie schránok a OpenGL akcelerácie. Po spustení X servera je potrebné otvoriť „Cygwin64 Terminal“ a nastaviť premennú `DISPLAY`. Potom sa môžeme pripojiť cez SSH na vzdialený počítač a spustiť napríklad xterm.



Obr. 4.14: Spustenie xterm vo viacoknovom móde

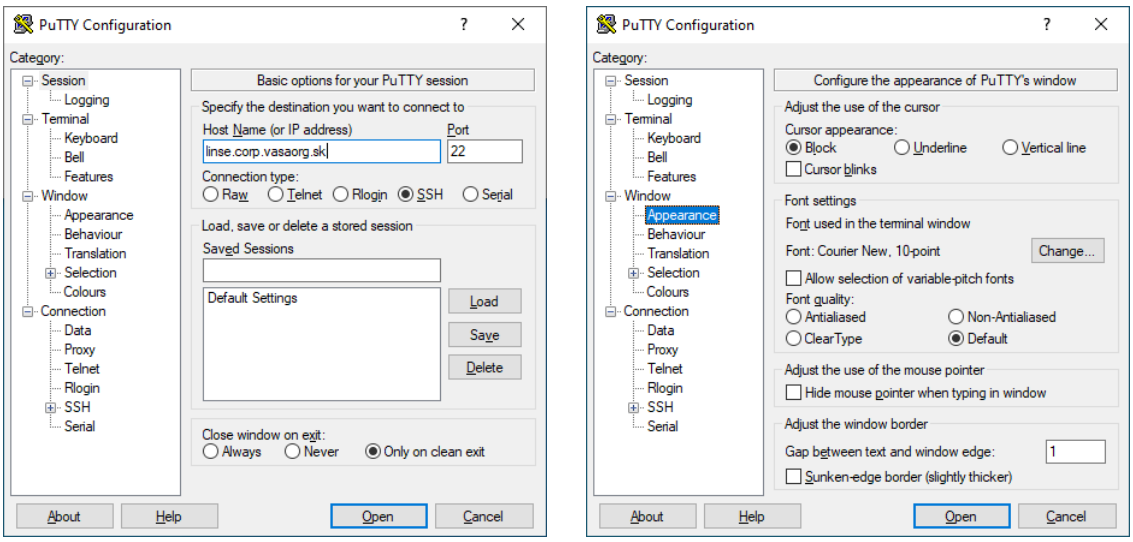
Kapitola 5

PuTTY

Pokiaľ je potrebné pripájať sa z operačného systému Windows na Unixové počítače, ale nevyužije sa široká škála možností, ktoré Cygwin ponúka, tak nemá zmysel inštalovať Cygwin, pretože jeho veľkosť sa pohybuje v stovkách MB. V tomto prípade je lepšou alternatívou program PuTTY. Jeho veľkosť je iba 1 152 kB a je k dispozícii pod MIT licenciou. Stiahnuť sa dá zdrojový kód, inštalačný program (MSI) alebo len samotný spustiteľný súbor (EXE). V tomto prípade netreba nič inštalovať a program stačí len spustiť. Posledná verzia je dostupná na nasledovnej adrese:

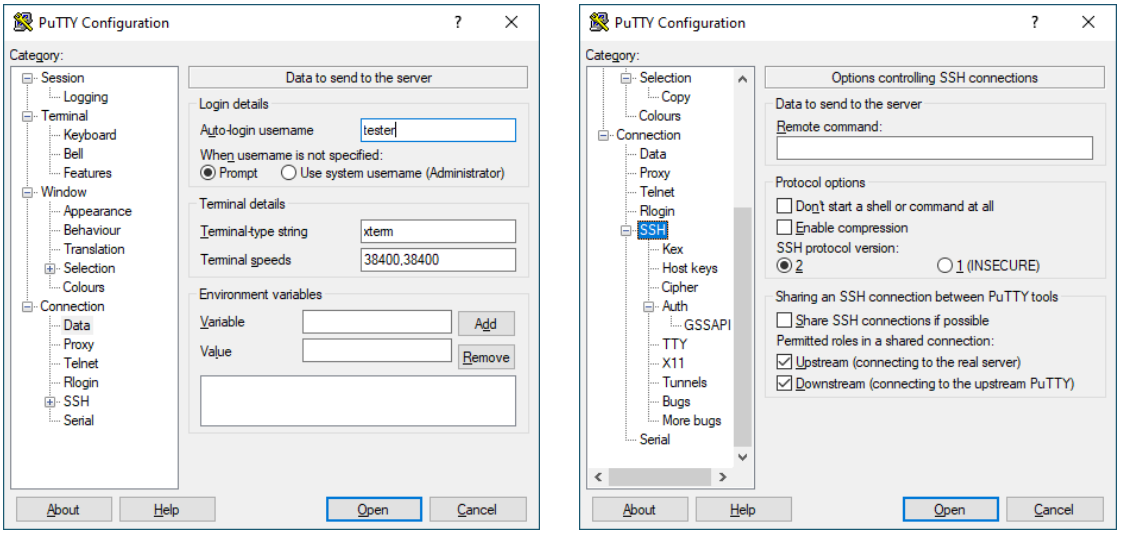
`https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html`

Práca s PuTTY začína dialógovým boxom, v ktorom sa nakonfigurujú rôzne parametre spojenia. V časti „Session“ do poľa „Host Name (or IP address)“ zadáme meno alebo IP adresu vzdialeného počítača (linse.corp.vasaorg.sk). V časti „Appearance“ môžeme zmeniť font (stlačením tlačidla Change...), spôsob vyhladzovania písma (voľby pod „Font quality“), či tvar kurzora (voľby pod „Cursor appearance“). V tejto časti nám vyhovujú štandardné nastavenia.



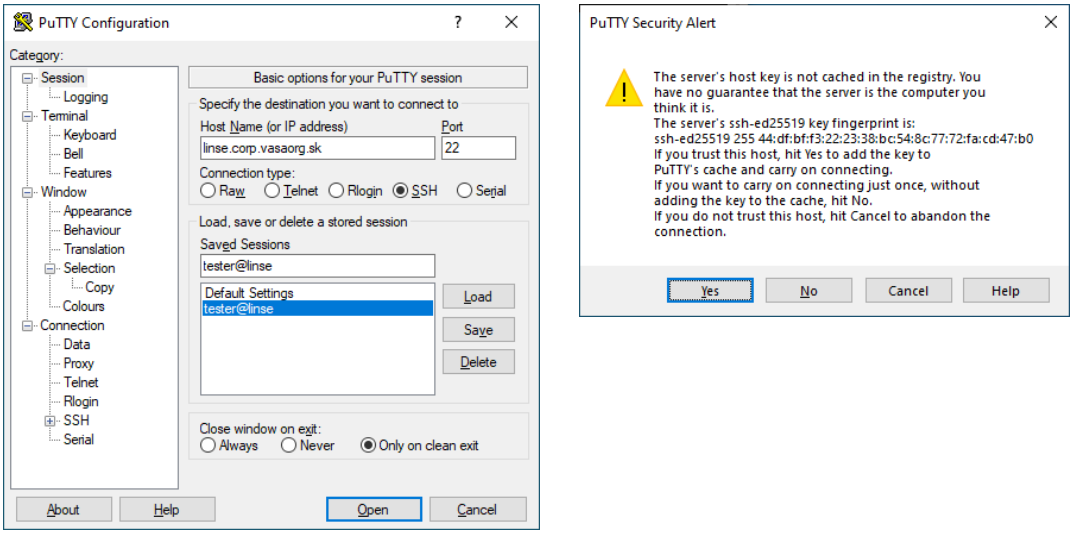
Obr. 5.1: PuTTY – nastavenie mena počítača a vzhľadu terminálového okna

Pod časťou „Data“ sa ukrýva položka „Auto-login username“, ktorá umožňuje pevne zvoliť používateľské meno pre prihlásenie. Vyplníme `tester`, aby sme meno nemuseli zakaždým ručne zadávať. V časti „SSH“ je možné nakonfigurovať podporovanú verziu protokolu. Ponecháme zvolenú verziu 2, keďže verzia 1 už nie je bezpečná.



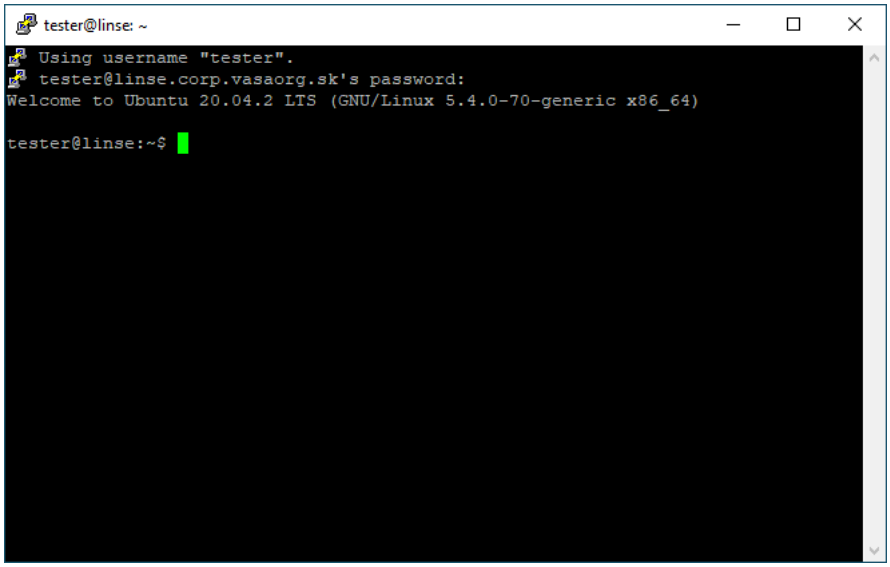
Obr. 5.2: PuTTY – nastavenie pevného používateľského mena a verzie SSH protokolu

Nastavenia zvolené vo všetkých častiach sa dajú nakoniec v časti „Session“ uložiť pre budúce jednoduché použitie. Pod „Saved Sessions“ treba vyplniť názov ukladanej konfigurácie (tester@linse) a potvrdiť tlačidlom Save.



Obr. 5.3: PuTTY – uloženie nastavení a potvrdenie autentickosti pri prvom prihlásení

Dvojklikom na uložené nastavenia (alebo výberom a kliknutím na tlačidlo Open) sa PuTTY pokúsi nadviazať spojenie s vybraným počítačom. Pri prvom prihlásení na počítač sa zobrazí okno pre potvrdenie autentickosti počítača, na ktorý sa pripájame (analogicky je to aj na Unixe). Po potvrdení autentickosti sa zobrazí terminálové okno.



Obr. 5.4: PuTTY – terminálové okno po nadviazaní spojenia

PuTTY je možné použiť aj na presmerovanie portov a v súčinnosti s X serverom (napríklad z Cygwin) aj vzdialenej pracovnej plochy na lokálny počítač.

Kapitola 6

Pripojenie na plochu Windows z Linuxu

Operačný systém Windows v edíciách, ktoré sú schopné pripojenia do domény, štandardne poskytuje možnosť pripojiť sa vzdialene na ich grafickú pracovnú plochu pomocou protokolu Remote Desktop Protocol (RDP). Pre operačný systém Linux existuje niekoľko implementácií tohto protokolu. V nasledovných častiach spomenieme dve z nich: „rdesktop“ a „FreeRDP“. Najprv si však popíšeme „Network Level Authentication“, ktorá tvorí dôležitú súčasť mechanizmu pripojenia na vzdialenú pracovnú plochu.

6.1 RDP a Network Level Authentication

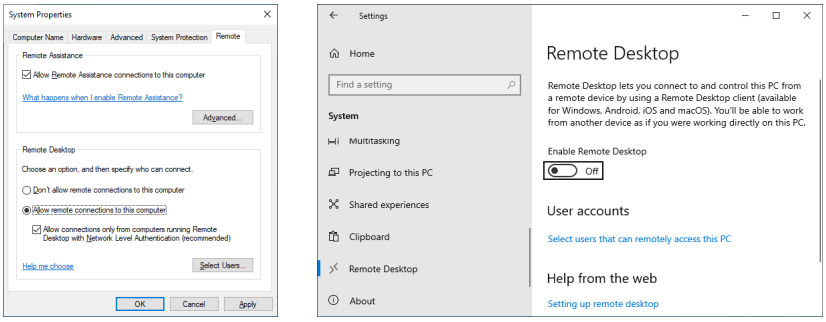
Pri pokuse klienta o pripojenie vytvorí operačný systém Windows pre neho nové sedenie s grafickým používateľským rozhraním. Potom sa klient v tomto rozhraní môže prihlásiť rovnakým spôsobom, ako keby fyzicky sedel za počítačom, na ktorý sa prihlasuje. Toto riešenie bolo pre klienta intuitívne. Umožňovalo však útočníkom žiadať počítač o vytvorenie sedenia bez toho, aby vedeli akékoľvek prihlasovacie údaje. Na základe jednoduchej sieťovej požiadavky musel počítač vykonať zložitú prípravu sedenia a grafického prostredia. Útočník potom mohol spojenie zavrieť a postup dokola opakovať. Týmto spôsobom mohol útočník voči počítaču vykonať relatívne „lacný“ útok „Denial of Service“ (DoS).

Preto bol od verzie Windows Vista a RDP 6.0 zavedený nový spôsob autentifikácie klienta, tzv. „Network Level Authentication“ (NLA). Táto autentifikácia na sieťovej úrovni umožnila overiť identitu používateľa ešte pred zložitou prípravou sedenia s grafickým prostredím. Týmto spôsobom sa zamedzilo vyššie spomínanému DoS útoku, pretože útočník, ktorý nepoznal prihlasovacie údaje, zaťažil systém oveľa menej. NLA zavádza „CredSSP“, čo je nový „Security Support Provider“ (SSP). CredSSP sa dá použiť v kombinácii s „NT LAN Manager“ (NTLM) alebo Kerberos autentifikáciou, podľa toho, či je počítač mimo domény, alebo je pripojený do domény (v tom prípade je podporované aj SSO).

Novšie verzie Windows štandardne vynucujú použitie NLA pri pripojení cez RDP. Pre kompatibilitu s niektorými programami môže byť potrebné povoliť aj starší spôsob autentifikácie (aj keď lepším riešením by rozhodne bola aktualizácia nekompatibilných programov).

6.1.1 Povolenie vzdialeného prístupu

Operačný systém Windows štandardne nepovoľuje vzdialený prístup k počítaču. Ak chceme používať RDP na pripojenie, tak musíme tento prístup najprv povoliť. Prvá možnosť je dostať sa cez „⚙ ▸ System ▸ About ▸ Advanced System Settings“ k oknu „System Properties“. Na záložke „Remote“ (zobrazenej na obrázku 6.1 vľavo) môžeme povoliť vzdialený prístup zvolením možnosti „Allow remote connections to this computer“.



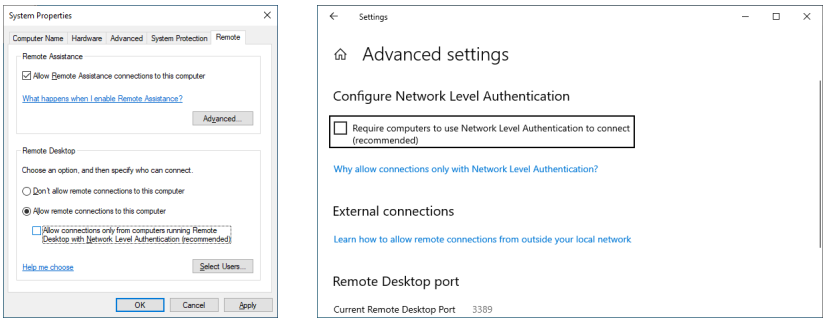
Obr. 6.1: Povolenie vzdialeného prístupu

Alternatívne môžeme postupovať cez „⚙ ▸ System ▸ Remote desktop ▸ Enable Remote Desktop“ (obrázok 6.1 vpravo). Povolenie potvrdíme kliknutím na tlačidlo Confirm v dialógovom okne „Remote Desktop Settings“.

6.1.2 Vypnutie vynucovania NLA

Windows štandardne pri vzdialenom prístupe k počítaču vyžaduje použitie nového NLA protokolu. Avšak, dá sa nakonfigurovať tak, aby použitie NLA nevynucoval. Potom bude možné použiť aj starý spôsob autentifikácie. Z dôvodov uvedených v časti 6.1 to však *neodporúčame*.

Opäť máme dve možnosti ako vypnúť vynucovanie NLA. Prvá možnosť je dostať sa cez „⚙ ▸ System ▸ About ▸ Advanced System Settings“ k oknu „System Properties“. Na záložke „Remote“ (zobrazenej na obrázku 6.2 vľavo) môžeme povoliť vzdialený prístup zrušením zaškrtnutia možnosti „Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)“.



Obr. 6.2: Vypnutie vynucovania NLA

Alternatívne môžeme postupovať cez „⚙ ▸ System ▸ Remote desktop ▸ Advanced settings“ (obrázok 6.2 vpravo). Následne zrušíme zaškrtnutie políčka „Require computers to use Network Level Authentication to connect (recommended)“. Zrušenie potvrdíme kliknutím na tlačidlo Proceed anyway v dialógovom okne „Remote Desktop Settings“. Po potvrdení zmien sa už môžeme pripojiť na počítač bez použitia NLA.

6.2 rdesktop

Jedným z prvých Windows RDP klientov pre Linux je program `rdesktop`. Pôvodne nepodporoval NLA, ale od verzie 1.8.0 je implementovaná podpora CredSSP s Kerberos autentifikáciou. Ak je Linuxový počítač pripojený do domény, tak môže využiť Kerberos autentifikáciu na doménovom radiči s protokolom NLA. Žiaľ, možnosť CredSSP s NTLM nie je implementovaná, preto pokiaľ počítač nie je pripojený do domény, tak nemôžeme použiť NLA. Aj potom je možné použiť `rdesktop`, je však nutné vypnúť NLA, čo *neodporúčame* (v takom prípade je lepšie použiť FreeRDP).

Pre otestovanie pripojenia pomocou `rdesktop` s NLA je potrebné sa najprv na Linuxovom počítači prihlásiť ako doménový používateľ:

```
tester@linwo:~$ ssh CORP\\tester@localhost
CORP\tester@linwo:~$ klist -fe
Ticket cache: FILE:/tmp/krb5cc_10010
Default principal: tester@CORP.VASAORG.SK

Valid starting   Expires   Service principal
...              ...       krbtgt/CORP.VASAORG.SK@CORP.VASAORG.SK
  renew until ..., Flags: FRIA
  Etype (skey, tkt): aes256-cts-hmac-sha1-96, aes256-cts-hmac-sha1-96
...              ...       LINWO$@CORP.VASAORG.SK
  Flags: A, Etype (skey, tkt): aes256-cts-hmac-sha1-96, aes256-cts-hmac-sha1-96
```

Vidíme, že prihlásením vznikol Kerberos TGT, ktorý potrebuje CredSSP s Kerberos autentifikáciou. Bez prihlásenia do domény by sme pri pokuse o pripojenie pomocou `rdesktop` a NLA dostali chybu:

```
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
```

Program `rdesktop` nainštalujeme príkazom `sudo apt install rdesktop`. Po nainštalovaní je možné nadviazať pripojenie k vzdialenej pracovnej ploche príkazom:

```
CORP\tester@linwo:~$ rdesktop -u tester -z -x l winse
```

Parameter `-u meno` určuje meno používateľa, pod ktorým sa chceme pripojiť. Obdobne `-d doména` určuje doménu pripájaného doménového používateľa. Parameter `-z` povolí kompresiu dátového toku, čím sa získa lepšia rýchlosť pri pomalom spojení. Šírku dátového toku (l[an], b[roadband], m[odem]) je možné nastaviť parametrom `-x`.

```
...
Connection established using CredSSP.
Core(error): tcp_recv(), gnutls_record_recv() failed with -54: Error in the
  pull function.
```

K vzdialenej pracovnej ploche na Windows sa nám, žiaľ, nepodarilo dopracovať. Aj keď sa spojenie pomocou CredSSP nadviazalo, tak sa zdá, že `rdesktop` má problém s TLS 1.2 použitým operačným systémom Windows. Skúsme preto nadviazať spojenie bez NLA.

6.2.1 Pripojenie cez rdesktop bez NLA

Najprv potrebujeme na vzdialenom Windows počítači vypnúť vynucovanie NLA postupom uvedeným v podčasti 6.1.2. Potom sa na tento počítač môžeme prihlásiť už aj bez toho, aby sme boli na Linuxe prihlásení ako doménový používateľ. Použijeme príkaz:

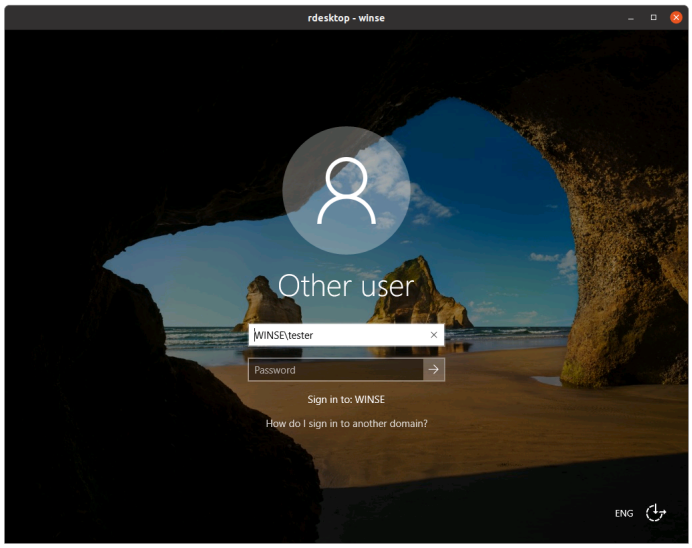
```
tester@linwo:~$ rdesktop -u tester -z -x l winse
...
ATTENTION! The server uses and invalid security certificate which can not be
   trusted for the following identified reasons(s);

 1. Certificate issuer is not trusted by this system.
     Issuer: CN=winse.corp.vasaorg.sk

Review the following ... info before you trust it to be added as an exception.
If you do not trust the certificate the connection atempt will be aborted:

    Subject: CN=winse.corp.vasaorg.sk
     Issuer: CN=winse.corp.vasaorg.sk
...
  Certificate fingerprints:
       sha1: ac07bc9f4dde3f5476428126605c56b1801c227a
...
Do you trust this certificate (yes/no)? yes
...
Connection established using SSL.
```

Uvidíme okno s plochou vzdialeného počítača, na ktorej sa môžeme prihlásiť:



Obr. 6.3: Prihlasovacie okno po pripojení sa programom rdesktop bez NLA

6.3 FreeRDP

Program FreeRDP, na rozdiel od programu rdesktop, podporuje CredSSP s NTLM. Nainštalujeme ho príkazom `sudo apt install freerdp2-x11`. Potom sa nasledovným príkazom pripojíme na vzdialenú plochu:

```
tester@linwo:~$ xfreerdp /compression /network:lan /rfx /sec:nla
↪/u:Administrator /v:winse.corp.vasaorg.sk
```

Parameter `/u:meno` určuje meno používateľa, pod ktorým sa chceme pripojiť a parameter `/v:server[:port]` zas meno a port počítača, na ktorý sa chceme pripojiť. Obdobne `/d:doména` určuje doménu pripájaného doménového používateľa. Parameter `/compression` povolí kompresiu dátového toku, čím sa získa lepšia rýchlosť pri pomalom spojení. Šírku dátového toku je možné nastaviť parametrom `/network:lan`. Parameter `/rfx` povolí RemoteFX, čo je technológia pre zlepšenie vizuálneho zážitku pri RDP. Nakoniec parametrom `/sec:nla` vynútime použitie NLA zo strany klienta.

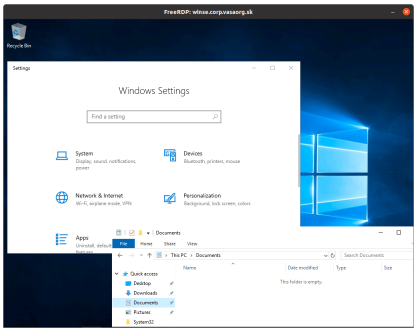
Po odoslaní príkazu budeme na príkazovom riadku vyzvaní na potvrdenie autentickosti vzdialeného počítača a zadanie hesla:

```
...
Certificate details for winse.corp.vasaorg.sk:3389 (RDP-Server):
        Common Name: winse.corp.vasaorg.sk
        Subject:     CN = winse.corp.vasaorg.sk
        Issuer:      CN = winse.corp.vasaorg.sk
        Thumbprint:  eb:af:4b:77:e7:c0:5a:b4:9a:91:12:a7:...:40:9f:1a
The above X.509 certificate could not be verified, possibly because you don't have
the CA certificate in your certificate store, or the certificate has expired.
Please look at the OpenSSL documentation on how to add a private CA to the store.
Do you trust the above certificate? (Y/T/N) Y
Password:
```

Po potvrdení autentickosti sa vzdialený počítač pridá do zoznamu známych počítačov a už nebude nutné opätovne potvrdzovať jeho autentickosť (podobne ako pri ssh):

```
tester@linwo:~$ cat ~/.config/freerdp/known_hosts2
winse.corp.vasaorg.sk 3389 eb:af:4b:77:e7:c0:5a:b4:9a:91:12:a7:...:40:9f:1a
↪Q04gPSB3aW5zZS5jb3JwLnZhc2Fvcmcuc2s= Q04gPSB3aW5zZS5jb3JwLnZhc2Fvcmcuc2s=
```

Po skončení dialógu na príkazovom riadku sa otvorí okno so vzdialenou pracovnou plochou, na ktorú už bude používateľ rovno prihlásený:



Obr. 6.4: Pracovná plocha po pripojení sa programom xfreerdp s NLA

Kapitola 7

Záver

Naším cieľom bolo demonštrovať rôzne možnosti integrácie operačných systémov Windows a Unix. Najprv sme popísali, akým spôsobom je možné pripojiť Linuxový počítač s Ubuntu 20.04 do domény riadenej Windows Serverom 2019. Začali sme konfiguráciou radiča domény na Windows a potom sme nastavili autentifikáciu používateľov na Linuxe voči tejto doméne. Na konci tejto kapitoly sme predviedli, ako sa môže doménový používateľ prihlásiť na Linuxový počítač, pričom sa mu automaticky vytvorí domovský priečinok a správne sa namapuje jeho doménový identifikátor na Linuxový. Rovnako sme spomenuli rôzne možnosti riešenia pridelenia jednoznačného Linuxového UID tomu istému používateľovi z domény na rôznych Linuxových počítačoch v doméne.

V ďalšej kapitole sme popísali inštaláciu a konfiguráciu radiča domény postaveného na Linuxovom balíku Samba 4. Uviedli sme niektoré možnosti správy takejto domény z Linuxu, ale ukázali sme aj jej správu natívnymi nástrojmi operačného systému Windows. Túto kapitolu sme uzavreli pridaním počítača s operačným systémom Windows do Samba domény a ukázali sme, ako naň aplikovať dve vybrané skupinové politiky.

Poslednou témou bolo pripojenie sa z jedného operačného systému na vzdialenú pracovnú plochu druhého systému. Najprv sme v samostatnej kapitole popísali projekt Cygwin so zameraním na použitie SSH a X servera. Ukázali sme, ako použiť tieto programy na pripojenie sa z operačného systému Windows na Unixový počítač a spúšťať nielen konzolové, ale aj grafické aplikácie. V nasledujúcej kapitole sme spomenuli program PuTTY, ktorý nahrádza SSH (nie však X server) z Cygwinu, pričom je podstatne kompaktnejší. V poslednej kapitole sme ukázali, ako sa možno pripojiť z Linuxu na vzdialenú pracovnú plochu Windows. Na pripojenie sme najprv použili starší program rdesktop, ktorý je možné použiť pokiaľ nepotrebujeme pripojenie cez NLA a potom novší program FreeRDP s podporou NLA.

Správa sietí a operačných systémov Linux a Windows

Autor: RNDr. Richard Ostertág, PhD.
Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky
Katedra informatiky
Oddelenie kryptológie a informačnej bezpečnosti

Recenzenti: doc. Ing. Pavel Segeč, PhD.
doc. Ing. Anton Baláž, PhD.

Vydavateľ: Univerzita Komenského v Bratislave
Bratislava 2022
1. vydanie, 81 strán

Materiál je výstupom Rozvojového projektu Univerzity Komenského a Ministerstva školstva, vedy, výskumu a športu SR č. 002UK-2-1/2018 – *„Vzdelávanie pre informačnú spoločnosť“* v oblasti Podpora vysokých škôl pri plnení záväzkov prijatých v rámci Národnej koalície pre digitálne zručnosti a povolania SR.

ISBN 978-80-223-5405-9