Лабораторна робота №20

Організація обміну файлами між Linux та Windows на основі протоколу SMB

Мета: організувати файловий сервер на базі Ubuntu Linux та налаштувати доступ до ресурсів цього серверу з домену Active Directory на основі протоколу SMB.

Інструменти: гіпервізор VirtualBox; (за потреби) мережний емулятор GNS3; модель комп'ютерної мережі та структура домену, побудовані у межах попередніх лабораторних курсу, а також віртуальна машина з Ubuntu Server, налаштована у межах лабораторної роботи №19.

Теоретичні відомості та завдання до лабораторної роботи

ПРОТОКОЛ SMB ТА ЙОГО РЕАЛІЗАЦІЯ SAMBA

Протокол **SMB** (Server Message Block) – протокол прикладного рівня, який використовується для організації спільного доступу до файлів, принтерів, серійних портів між вузлами мережі. Протокол відомий також під більш загальною назвою **SMB/CIFS**. CIFS є старішою версією цього протоколу і розшифровується як Common Internet File System).

SMB/CIFS найбільш активно використовувався для Windows мереж до появи Active Directory. Згодом потокол став основою для інших реалізацій, зокрема для Samba.

Samba – стандартний набір для спільної роботи програм Windows з програмами Linux і Unix, що дає змогу здійснювати взаємну інтеграцію цих систем. Так, на основі Samba можна організовувати спільне використання Windows-системами та Unix/Linux системами каталогів, принтерів. Samba підтримує інтеграцію Unix/Linux-систем в Active Directory, причому не лише як звичайних членів домену (робочих станцій чи серверів), а також за потреби і як контролерів домену.

Проект Samba є членом організації Software Freedom Conservancy, а відповідне програмне забезпечення поширюється під ліцензією GNU GPL.

Завдання №20.1

1. Запустіть віртуальну машину з Ubuntu Server, налаштовану у межах лабораторної роботи №19 та увійдіть у систему під адміністративний обліковим записом, створеним під час встановлення системи.
2. Використовуючи подані нижче теоретичні відомості, встановіть усі необхідні програмні пакунки (п. 1 теоретичних відомостей): samba, cifsutils, smbclient, sssdad, sssd-tools, realmd, adcli, winbind, libpam-winbind, libnss-winbind, krb5-config **Звіт має містити** скриншоти зроблених налаштувань та опис основних дій.

Налаштування Samba -серверу на Ubuntu

Samba дає широкі можливості для спільного доступу до файлів та інших ресурсів (наприклад, принтерів). У цій роботі буде розглянуто випадок файлового сервера з автентифікацією через Active Directory.

1. **Встановлення необхідних пакунків.** Встановимо пакунки, потрібні для функціонування Samba-серверу та його інтеграції в Active Directory. Варто інсталювати всі необхідні пакунки на цьому кроці – потім у вас може не бути доступу до Інтернету з-під цієї віртуальної машини.

   sudo apt update

sudo apt install samba cifs-utils smbclient

sudo apt install sssd-ad sssd-tools realmd

sudo apt install adcli krb5-user

Під час встановлення пакунку krb5-config для параметра realm задайте значення, яке відповідає імені вашого домену. Наприклад:

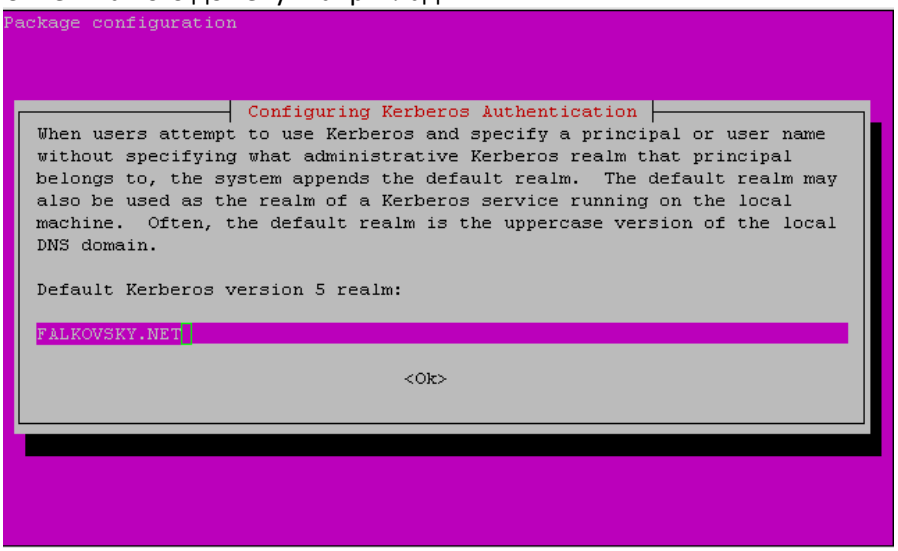


Рис.20.1.

Для параметрів Kerberos server необхідно відредагувати конфігураційний файл Kerberos /etc/krb5.conf. За потреби можливо зробити резервну копію старого файлу:

sudo cp /etc/krb5.conf /etc/krb5.conf.bak

Відкриваємо /etc/krb5.conf у редакторі. За Вашим бажанням видаліть або закоментуйте всі записи про публічні / сторонні realm'и (MIT, CSAIL тощо), або залиште їх. У секції [realms] додаємо записи про домен surname.net. Різниця між kdc і admin_server: kdc = ... — можна вказувати кілька разів — клієнт сам обере доступний з контролерів домену, admin_server = ... — за специфікацією має бути лише один (Kerberos не підтримує автоматичне перемикання між кількома admin_server):

```
[libdefaults]
        default_realm = SURNAME.NET
        dns_lookup_realm = true
        dns_lookup_kdc = true
[realms]
  SURNAME.NET = {
    kdc = serv-G-N-1.surname.net
    kdc = serv-G-N-2.surname.net
    admin_server = serv-G-N-1.surname.net
    default_domain = surname.net
  }
```

У секції [domain_realm] налаштовуємо відображення імен доменів:

```
[domain_realm]
  .yourdomain.local = SURNAME.NET
  yourdomain.local  = SURNAME.NET
```

Перезавантажуємо SSSD:

sudo systemctl restart sssd

Перевірте Kerberos-квиток:

kinit Administrator@SURNAME.NET

klist

Ви повинні побачити дійсний ticket (рис.20.2).

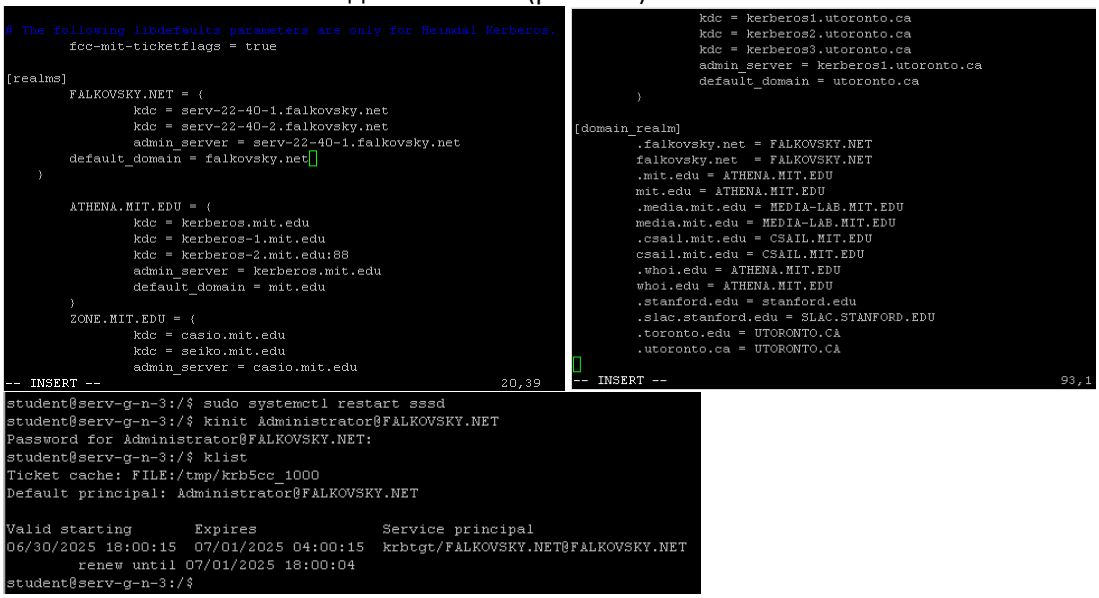


Рис.20.2.

<u>Завдання №20.2</u>

1. Відкорегуйте схему адресації, з якою ви працювали у лабораторній роботі №7, передбачивши статичну адресу для серверу з Ubuntu. **<u>Змінену схему адресації додайте до звіту.</u>**
2. Спираючись на подані нижче теоретичні відомості, змініть мережну конфігурацію серверу з Ubuntu та окремі налаштування Active Directory, щоб сервер з Ubuntu став частиною моделі мережі, з якою ви працювали у лабораторних роботах №1-19

<u>Звіт має містити</u> скриншоти зроблених налаштувань, опис основних дій та змінену схему адресації.

2. Виконання базових мережних налаштувань для серверу з ОС Ubuntu

2.1) **Внесення змін у схему адресації.** Виділимо серверу з ОС Ubuntu це одну статичну адресу у схемі адресації (лабораторна робота №7). У прикладі це буде адреса 192.168.40.246.

2.2) **Виключення адреси сервера з DHCP-пулу.** Цю адресу потрібно додатково виключити з DHCP-пулу на контролері домену. Для цього на контролері домену запустимо оснащення DHCP, оберіть відповідну область DHCP та в контекстному меню вузла Address Pool виберіть New Exclusion Range (рис. 20.3).

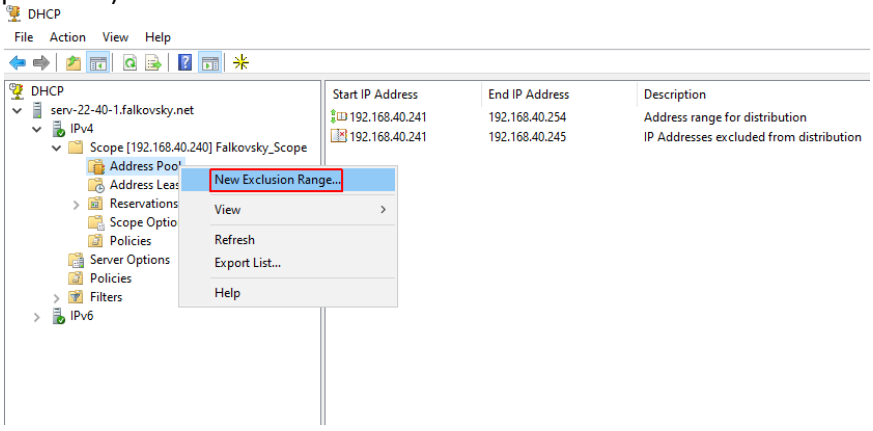


Рис.20.3.

У ролі початкової та кінцевої адреси діапазону, який необхідно виключити, введіть адресу сервера з ОС Ubuntu та натисніть Add (рис. 20.4).

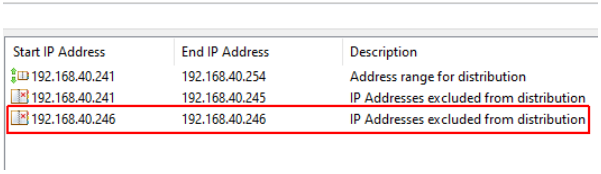


Рис. 20.4

2.3) (за потреби) **Корегування доменного імені серверу.** Для коректної роботи з доменним ім'ям Ubuntu сервера у цій лабораторній роботі переконайтеся, що довжина цього імені не перевищує 15 символів. Якщо символів в імені більше, це можна змінити, відредагувавши файл */etc/hostname* або перейменувавши сервер командою

sudo hostnamectl set-hostname New-Name-Server

Вносимо до файлу */etc/hosts* перелік хостів домену, з якими буде взаємодіяти сервер Ubuntu:

127.0.0.1 localhost

127.0.1.1 serv-G-N-3

192.168.40.246 serv-G-N-3

192.168.40.243 serv-G-N-1.surname.net

192.168.40.244 serv-G-N-2.surname.net

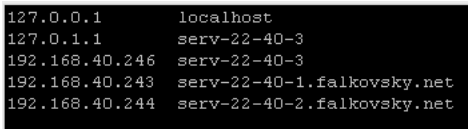


Рис. 20.5

Починаючи з Ubuntu 22.04+, система використовує systemd-resolved для динамічного керування DNS. Однак це може заважати інтеграції з внутрішнім Active Directory-доменом, оскільки /etc/resolv.conf постійно «скидається».

Щоб це виправити:

sudo systemctl disable systemd-resolved --now

Замінюємо символічне посилання /etc/resolv.conf:

sudo rm /etc/resolv.conf

echo "nameserver 192.168.40.243" | sudo tee /etc/resolv.conf

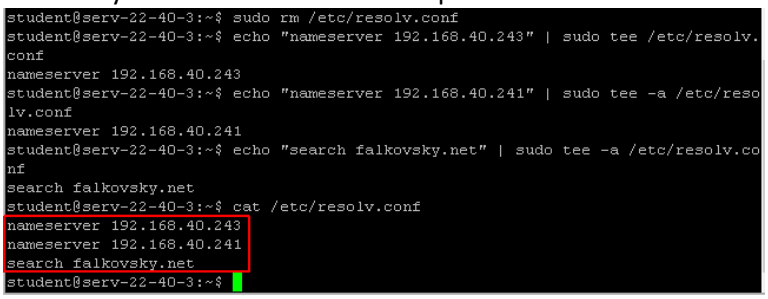
echo "nameserver 192.168.40.241" | sudo tee -a /etc/resolv.conf

echo "search surmane.net" | sudo tee -a /etc/resolv.conf

Це зробить файл статичним — systemd-resolved вже не перезапише його.

Перевіряємо вміст /etc/resolv.conf:

cat /etc/resolv.conf



Очікуваний результат - записи nameserver відповідають DNS-серверам, що використовуються у лабораторній роботі.

Перезавантажуємо сервер

sudo reboot

2.4) **Долучення ВМ з Ubuntu до моделі мережі.** Далі за допомогою віртуалізаційного ПЗ, яке ви використовуєте для моделювання мережі (GNS 3 і/або VirtualBox) приєднайте віртуальну машину з Ubuntu Server до моделі мережі, з якою ми працювали у попередніх лабораторних роботах.

2.5) **З'ясування імені віртуального інтерфейсу Ethernet.** Тепер треба дізнатися ім'я мережного інтерфейсу, який використовує мережа нашої моделі. В Ubuntu Server 20.04

мережні налаштування зазвичай здійснюються через Netplan і yaml-файли, тож для перегляду цих налаштувань можна скористатися командою ip:

ip addr show

або скорочено:

ip a

2.6) **Редагування yaml-файлів з налаштуваннями мережі.** Створюємо на сервері з ОС Ubuntu yaml-файл aksm-N.yaml (де N - варіант) у якому прописуємо мережні налаштування, включаючи обробника налаштувань (renderer: networkd), ім'я мережного інтерфейсу (типовий інтерфейс Ethernet зазвичай має ім'я enp0s3), IPадресу та префікс, шлюз за замовчуванням (ключове слово gateway4), ім'я DNSсервера (ключове слово nameservers).

Помилки у файлі Netplan можуть бути локалізовані за допомогою інструменту yamllint. Встановлення та приклад застосування:

sudo apt install yamllint
yamllint /etc/netplan/00-installer-config.yaml

Приклад yaml-файлу:

```
network:
  ethernets:
    enp0s3:
      addresses: [192.168.40.246/28]
      gateway4: 192.168.40.241
      nameservers:
        search: [falkovsky.net]
        addresses: [192.168.40.243, 192.168.40.241]
  version: 2
```

Примітка. У yaml-файлах для Netplan важливі відступи зліва. Йдеться не про кількість пробілів, а про дотримання рівневості. Так, якщо у зразку ключове слово gateway4 має такий самий відступ зліва, як ключове слово address (а не таке, як рядок – 220.19.40.246/28, наприклад) – то так само має бути і у вашому yaml-файлі.

У системі, ймовірно, є й інші yaml-файли. Наприклад, файл *50-cloud-init.yaml*. Закоментуйте рядки цього файлу і збережіть зміни, або перейменуйте його у файл з іншим розширенням. Наприклад *50-cloud-init.yaml.bkp*

2.6) **Застосування та перевірка мережних налаштувань.** Коли yaml-файли готові, застосовуємо мережні налаштування:

sudo netplan apply

Перевіряємо мережні налаштування шляхом пінгування.

2.7) **Приєднання Ubuntu Server 24.04 до домену Active Directory**. Перевіряємо доступність домену (рис.20.6).

realm discover falkovsky.net

Очікуваний результат:

type: kerberos
realm-name: FALKOVSKY.NET
domain-name: falkovsky.net
configured: no
…..

```
student@serv-22-40-3:~$ realm discover falkovsky.net
falkovsky.net
  type: kerberos
  realm-name: FALKOVSKY.NET
  domain-name: falkovsky.net
  configured: no
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: libnss-sss
  required-package: libpam-sss
  required-package: adcli
  required-package: samba-common-bin
student@serv-22-40-3:~$
```

Рис. 20.6

Годинник Ubuntu має бути синхронізований з DC, різниця не більше ±5 хв, інакше Kerberos не спрацює. Виконуємо (на всяк випадок ☺) примусову синхронізацію часу:

sudo timedatectl set-ntp true

Приєднуємось до домену (рис.20.7):

sudo realm join --user=Administrator surname.net

Вводимо пароль користувача Administrator (або іншого облікового запису з правами додавання комп'ютерів, що використаний у цьому рядку).

Перевіряємо успішність приєднання

realm list

Очікувано побачите щось на кшталт:

falkovsky.net

type: kerberos

realm-name: FALKOVSKY.NET

domain-name: falkovsky.net

configured: kerberos-member

server-software: active-directory

client-software: sssd ...

```
student@serv-22-40-3:~$ sudo timedatectl set-ntp true
student@serv-22-40-3:~$ sudo realm join --user=Administrator falkovsky.net
Password for Administrator:
student@serv-22-40-3:~$ realm list
falkovsky.net
  type: kerberos
  realm-name: FALKOVSKY.NET
  domain-name: falkovsky.net
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: libnss-sss
  required-package: libpam-sss
  required-package: adcli
  required-package: samba-common-bin
  login-formats: %U@falkovsky.net
  login-policy: allow-realm-logins
student@serv-22-40-3:~$
```

Рис. 20.7

Як бачимо, сервер повідомляє, що для повноцінної роботи приєднання через sssd необхідні встановлені пакунки (*required-package): sssd-tools, sssd, libnss-sss, libpam-sss, adcli ma samba-common-bin*

Можемо перевірити чи вони встановлені у системі:

dpkg -l sssd sssd-tools libnss-sss libpam-sss adcli samba-common-bin

Або одразу виконати спробу встановлення. Якщо щось із них не встановлено, додасться:

sudo apt install sssd-tools sssd libnss-sss libpam-sss adcli samba-common-bin

2.8) **Перевірка наявності серверу з Ubuntu у структурі домену Active Directory**.

На контролері домену запустимо оснащення Active Directory Users and Computers та перевіримо наявність серверу Ubuntu у організаційній одиниці Computers (рис.20.8).

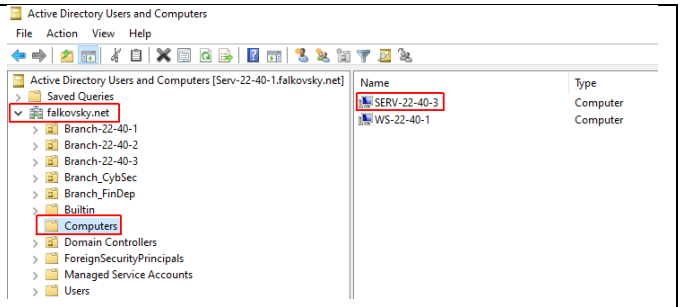


Рис. 20.8.

Якщо сервер відсутній у цій папці, виконуємо пошук у Computers домену (рис. 20.9). Сервер з Ubuntu має бути результатах пошуку.

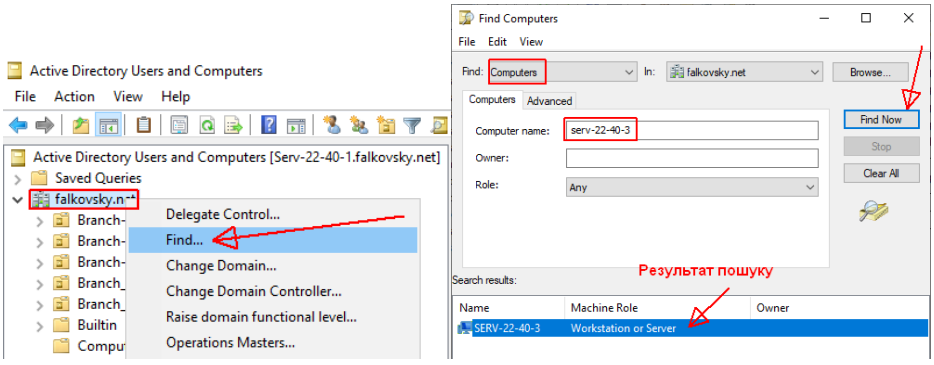


Рис. 20.9.

У властивостях серверу з Ubuntu обираємо опцію Trust this computer to delegation to any service (Kerberos only) - рис. 20.10.

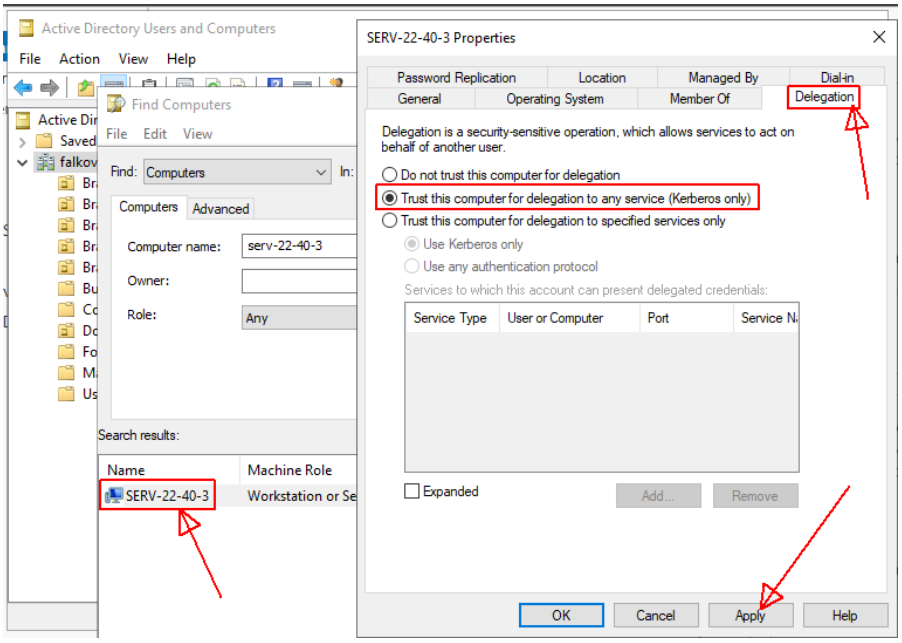


Рис. 20.10

2.8) **Створення DNS-запису для серверу з Ubuntu**. На контролері домену за допомогою оснащення DNS додайте до області прямого перегляду (Forward Lookup Zone) запис типу A для серверу з ОС Ubuntu (рис. 20.11).

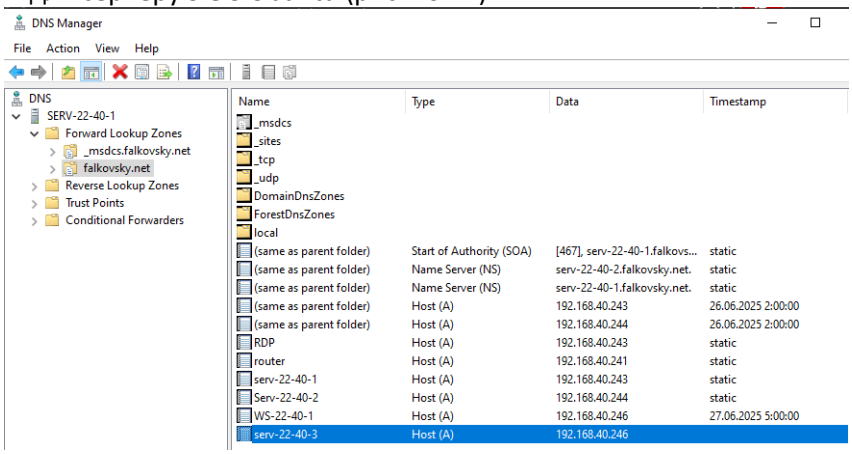


Рис. 20.11

Перевіряємо роботу Kerberos:

kinit administrator@SURNAME.NET

klist

та перевіряємо як SSSD розпізнає користувачів:

id administrator@surname.net

спроба входу під доменним користувачем на сервері:

su - 'administrator@surname.net'

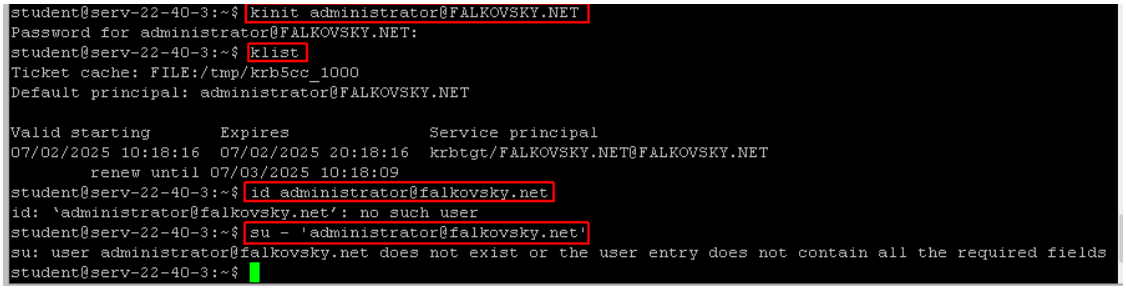


Рис. 20.12

Перевірка налаштувань на рис.20.12 показує успішно отриманий «квиток TGT» (krbtgt/FALKOVSKY.NET@FALKOVSKY.NET), а отже DNS налаштовано правильно (контролери домену знайшлися), час на сервері синхронізовано з контролерами домену (інакше Kerberos видає помилку Clock skew too great), пароль правильний, обліковий запис активний, krb5.conf налаштовано коректно (правильний realm, kdc, admin_server).

Команди id та su SSSD не надають інформацію про користувача, відповідно SSSD не відображає користувачів домену.

Перевіряємо статус SSSD (має бути active (running)

sudo systemctl status sssd

Перевіряємо */etc/sssd/sssd.conf*. У ньому має бути щось на кшталт:

[sssd]
domains = falkovsky.net
config_file_version = 2
services = nss, pam
[domain/falkovsky.net]
default_shell = /bin/bash
krb5_store_password_if_offline = True
cache_credentials = True
krb5_realm = FALKOVSKY.NET
realmd_tags = manages-system joined-with-adcli
id_provider = ad
fallback_homedir = /home/%u@%d
ad_domain = falkovsky.net
use_fully_qualified_names = True
ldap_id_mapping = True
access_provider = ad

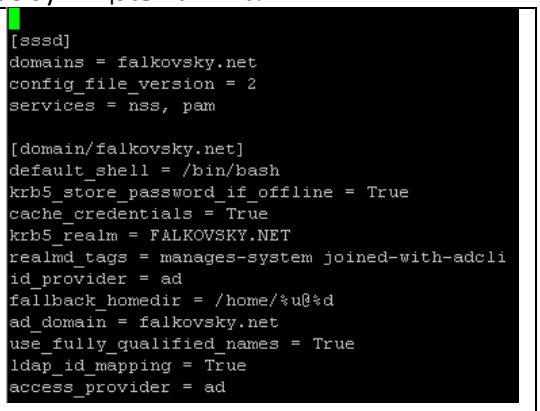


Рис. 20.13

Файл повинен мати права 600:

sudo chmod 600 /etc/sssd/sssd.conf
sudo systemctl restart sssd

Повторно перевіряємо як SSSD розпізнає користувачів:

id administrator@surname.net

та виконуємо спробу входу під доменним користувачем на сервері:

su - 'administrator@surname.net'

Команди працюють – отримана інформація про доменного користувача. Бачимо попередження, що не створено домашній каталог для користувача, хоча вхід під доменним користувачем відбувся успішно (рис.20.14):

su: warning: cannot change directory to /home/administrator@falkovsky.net: No such file or directory

```
student@serv-22-40-3:~$ sudo vi /etc/sssd/sssd.conf
student@serv-22-40-3:~$ sudo chmod 600 /etc/sssd/sssd.conf
student@serv-22-40-3:~$ sudo systemctl restart sssd
student@serv-22-40-3:~$ id administrator@falkovsky.net
uid=1451800500(administrator@falkovsky.net) gid=1451800513(domain users@falkovsky.net) groups=1451800513(domain
 users@falkovsky.net),1451800518(schema admins@falkovsky.net),1451800512(domain admins@falkovsky.net),145180057
2(denied rodc password replication group@falkovsky.net),1451800519(enterprise admins@falkovsky.net),1451800520(
group policy creator owners@falkovsky.net)
student@serv-22-40-3:~$ su - 'administrator@falkovsky.net'
Password:
su: warning: cannot change directory to /home/administrator@falkovsky.net: No such file or directory
administrator@falkovsky.net@serv-22-40-3:/home/student$
```

Рис. 20.14

Найпростіше рішення цієї проблеми – активація pam_mkhomedir через майстер

sudo pam-auth-update

Виходимо з сеансу доменного користувача *exit*. У меню, що з'явиться, необхідно відмітити [*] Create home directory on login переконатися, що також активовано [*] SSS authentication і натиснути Enter (OK)

```
administrator@falkovsky.net@serv-22-40-3:/$ exit
logout
student@serv-22-40-3:/$ sudo pam-auth-update
[sudo] password for student:
```

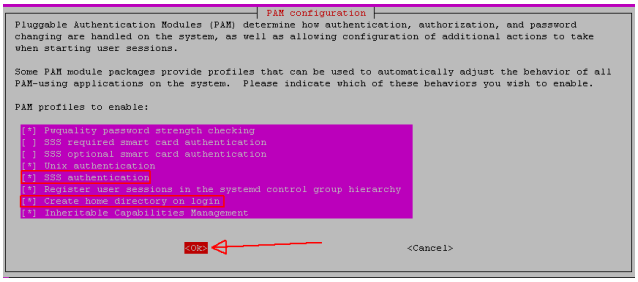


Рис. 20.15

Знову спроба входу під доменним користувачем на сервері:

su - 'administrator@surname.net'

Домашній каталог створився автоматично.

```
student@serv-22-40-3:/$ sudo pam-auth-update
[sudo] password for student:
student@serv-22-40-3:/$ su - 'administrator@falkovsky.net'
Password:
Creating directory '/home/administrator@falkovsky.net'.
administrator@falkovsky.net@serv-22-40-3:~$
```

Рис. 20.16

<u>Завдання №20.3</u>

1. Застосовуючи теоретичні відомості, наведені нижче, налаштуйте на сервері з Ubuntu інтеграцію з доменом Active Directory.
2. Переконайтеся, що користувач домену може здійснити вхід на сервері з Ubuntu (команда sudo login). Якщо це не вдається, перевірте зроблені налаштування. Такий вхід для користувача обов'язково має виконуватися успішно.

<u>Звіт має містити</u> скриншоти зроблених налаштувань та опис основних дій.

3. Налаштування інтеграції з Active Directory на сервері з Ubuntu

Щоб користувачі домену Active Directory могли під'єднуватися до ресурсів серверу з ОС Ubuntu, потрібно зробити цей сервер частиною домену та дозволити на ньому вхід користувачів цього домену. В Ubuntu це реалізується на основі сервісу SSSD (System Security Services Daemon), який підтримує автентифікацію через протоколи Kerberos та LDAP. У цій роботі буде використано автентифікацію через Kerberos. Про інші доступні налаштування можна почитати, наприклад, у документації Ubuntu Server [3].

3.1) **Редагування конфігураційних файлів сервісів Samba та Name Service Switch**. Йдеться про файли */etc/samba/smb.conf*, */etc/nsswitch.conf* відповідно. Також за бажанням можна додати створення домашніх каталогів користувачів Active Directory на сервері Ubuntu.

Файл */etc/nsswitch.conf* модифікуємо так, щоб він відповідав поданому нижче зразку. Тим часом файл */etc/samba/smb.conf* доцільно створити заново. У цьому файлі міститься багато варіантів готових налаштувань для різних випадків, і на початковому етапі вони радше заважатимуть, ніж допомагатимуть.

Якщо ви не хочете видаляти початковий варіант файлу */etc/samba/smb.conf*, можна перенести його задля майбутнього використання у домашній каталог:

sudo mv /etc/samba/smb.conf ~/smb.conf.bkp

а основний конфігураційний файл – перестворити:

sudo nano /etc/samba/smb.conf

Зразки конфігураційних файлів

На всіх поданих нижче зразках позначено основні зміни. Ваші зміни у цих файлах мають відповідати даним вашого варіанту та налаштуванням вашого домену.

Вміст файлу */etc/samba/smb.conf* створено наново, у чистому файлі. Відмінності позначено на рис. 20.17.

```
[global]
   workgroup = FALKOVSKY
   realm = FALKOVSKY.NET

   security = ads
   kerberos method = secrets and keytab
   dedicated keytab file = /etc/krb5.keytab

   server string = Samba Server with SSSD
   log file = /var/log/samba/%m.log
   log level = 1

   # Використовуємо SSSD, а не winbind ===
   idmap config * : backend = tdb
   idmap config * : range = 3000-7999

   idmap config FALKOVSKY : backend = sss
   idmap config FALKOVSKY : range = 10000-999999

   # winbind повністю не використовується:
   winbind enum users = no
   winbind enum groups = no
   winbind use default domain = no

   # Для підтримки Kerberos-автентифікації:
   kerberos method = secrets and keytab
   dedicated keytab file = /etc/krb5.keytab
```

[global]
workgroup = FALKOVSKY
realm = FALKOVSKY.NET
security = ads
kerberos method = secrets and keytab
dedicated keytab file = /etc/krb5.keytab
server string = Samba Server with SSSD
log file = /var/log/samba/%m.log
log level = 1

idmap config * : backend = tdb
idmap config * : range = 3000-7999
idmap config FALKOVSKY : backend = sss
idmap config FALKOVSKY : range = 10000-999999

winbind enum users = no
winbind enum groups = no
winbind use default domain = no

kerberos method = secrets and keytab
dedicated keytab file = /etc/krb5.keytab

Рис. 20.17.

```
student@serv-22-40-3:~$ testparm
Load smb config files from /etc/samba/smb.conf
Loaded services file OK.
Weak crypto is allowed by GnuTLS (e.g. NTLM as a compatibility fallback)

Server role: ROLE_DOMAIN_MEMBER

Press enter to see a dump of your service definitions

# Global parameters
[global]
        dedicated keytab file = /etc/krb5.keytab
        kerberos method = secrets and keytab
        log file = /var/log/samba/%m.log
        realm = FALKOVSKY.NET
        security = ADS
        server string = Samba Server with SSSD
        workgroup = FALKOVSKY
        idmap config falkovsky : range = 10000-999999
        idmap config falkovsky : backend = sss
        idmap config * : range = 3000-7999
        idmap config * : backend = tdb
```

Рис.20.18.

Зберігаємо файл */etc/samba/smb.conf.*

Пояснення значень рядків файлу надано у додатку 20.1 цього документу.

У кожному конкретному випадку будуть відрізнятись тільки рядки workgroup, realm та idmap config SURNAME

Виконуємо тестування поточних налаштувань командою *testparm*. Результати наведено на рис.20.18.

Файл /etc/nsswitch.conf.

Вміст цього файлу дещо відредаговано. Ключові зміни – значення рядків passwd: group: та shadow:, що тепер мають бути files sss. Вміст файлу показано на скриншоті (рис.20.19):

```
passwd:         files sss
group:          files sss
shadow:         files sss
gshadow:        files systemd

hosts:          files dns
networks:       files

protocols:      db files
services:       db files sss
ethers:         db files
rpc:            db files

netgroup:       nis sss
automount:  sss
```

Рис.20.19.

3.2) **Перезавантаження сервісів Samba та Nmbd.**

Для застосування змін у файлі /etc/samba/smb.conf, достатньо перезапустити служби smbd та nmbd:

sudo systemctl restart smbd.service nmbd.service
sudo systemctl status smbd
sudo systemctl status nmbd

У цій конфігурації winbind не використовується, оскільки систему приєднано до домену через sssd (рис. 20.20)

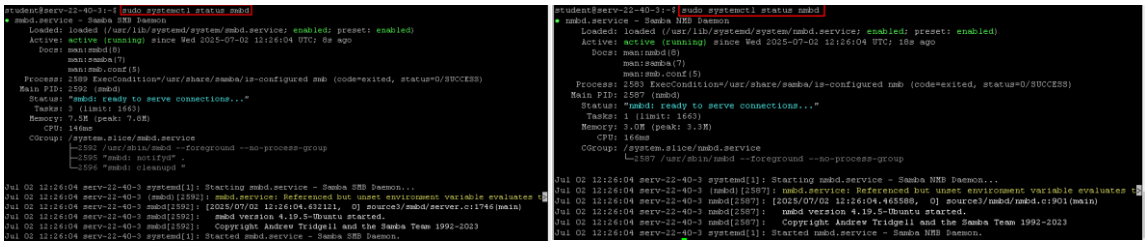


Рис. 20.20.

3.3) **Контроль доступності облікових записів домену Active Directory.** Наприклад, обліковий запис dep-rds-1 з домену falkovsky.net справді доступний на сервері Ubuntu. Також можна бачити, що цей користувач є членом двох груп користувачів домену.

Очистимо кеш SSSD та перезапустимо службу:

sudo sss_cache -E
sudo systemctl restart sssd

Перевіряємо доступ до серверу, членство у групах та входимо під доменним користувачем:

getent passwd dep-rds-1@falkovsky.net
groups dep-rds-1@falkovsky.net

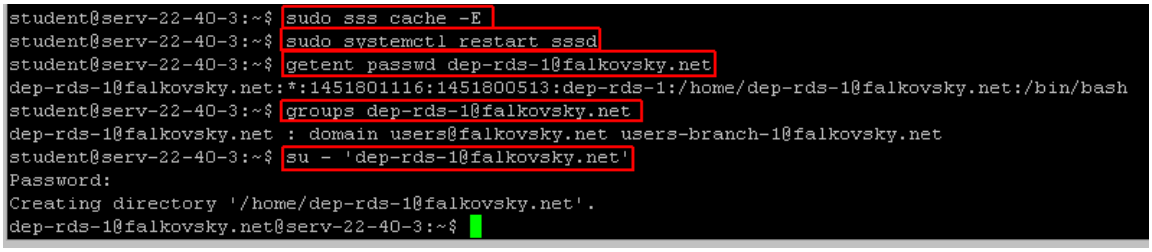


Рис. 20.21.

Увага! Цей етап перевірки (команди getent, groups, su) є критично важливим. Якщо автентифікація доменних користувачів із якихось причин не працює, то і доступ до спільних ресурсів Samba (шер, авторизація у службах тощо) також буде неможливим. Тому у разі будь-яких збоїв на цьому етапі необхідно ретельно перевірити налаштування SSSD, Kerberos, DNS та конфігураційні файли (sssd.conf, nsswitch.conf, smb.conf) перед тим, як переходити до наступних кроків.

Завдання №20.4

1. Користуючись поданими нижче інструкціями, налаштуйте на сервері з Ubuntu спільний каталог на основі Samba.

Вказівка до виконання п. 1. Коментар до спільного ресурсу (поле comment у файлі /etc/samba/smb.conf): Ubuntu File Server Share (Surname Name, Gr. GG, Var. NN), де – ваше прізвище та ім'я, GG – група, NN – варіант.

Звіт має містити скриншоти зроблених налаштувань та опис основних дій.

4. **Налаштування спільного каталогу на основі Samba.** Необхідні компоненти вже встановлено. Сервер з ОС Ubuntu вже приєднаний до домену. Лишилося підготувати майбутній спільний каталог та зробити його спільним ресурсом на основі Samba.

Повторно відкриваємо для редагування файл */etc/samba/smb.conf* і додаємо у кінці цього документа розділ *[share]* з адресою майбутнього спільного каталогу та налаштуваннями доступу до нього. Згідно з FHS (File Hierarchy Standard), для розміщення ресурсів сервера рекомендовано використовувати стандартний каталог */srv*. У каталозі */srv* створимо підкаталог *samba*, а всередині нього – підкаталог *share*:

sudo mkdir /srv/samba
sudo mkdir /srv/samba/share

Зробимо користувачем-власником каталогу системного користувача nobody, а групою-власником – системну групу nogroup:

sudo chown root:"domain users@surname.net" /srv/samba/share

Також дозволимо користувачу-власнику читання, запис і виконання, а групівласнику і решті користувачів – лише читання і виконання:

sudo chmod -R 0770 /srv/samba/share
sudo chgrp -R "domain users@surname.net" /srv/samba/share

Після виконання таких налаштувань для зміни вмісту спільного каталогу знадобляться права адміністратора, тим часом як читання вмісту каталогів та файлів буде дозволене всім користувачам, які пройшли автентифікацію. Налаштування можуть бути й іншими – залежно від потреб.

Приклад конфігураційного файлу */etc/samba/smb.conf* з доданими налаштуваннями спільного каталогу */srv/samba/share*:

```
[global]
   workgroup = FALKOVSKY
   realm = FALKOVSKY.NET
   security = ads
   kerberos method = secrets and keytab
   dedicated keytab file = /etc/krb5.keytab
   server string = Samba Server with SSSD
   log file = /var/log/samba/%m.log
   log level = 1
   # Використовуємо SSSD, а не winbind ===
   idmap config * : backend = tdb
   idmap config * : range = 3000-7999
   idmap config FALKOVSKY : backend = sss
   idmap config FALKOVSKY : range = 10000-999999
   # winbind повністю не використовується:
   winbind enum users = no
   winbind enum groups = no
   winbind use default domain = no
   # Для підтримки Kerberos-автентифікації:
   kerberos method = secrets and keytab
   dedicated keytab file = /etc/krb5.keytab

[share]
   path = /srv/samba/share
   read only = no
   browsable = yes
   guest ok = no
   valid users = @"FALKOVSKY\Domain Users"
   inherit acls = yes
   inherit permissions = yes
```

```
student@serv-22-40-3:~$ testparm
Load smb config files from /etc/samba/smb.conf
Loaded services file OK.
Weak crypto is allowed by GnuTLS (e.g. NTLM as a compatibility fallback)

Server role: ROLE_DOMAIN_MEMBER

Press enter to see a dump of your service definitions

# Global parameters
[global]
        dedicated keytab file = /etc/krb5.keytab
        kerberos method = secrets and keytab
        log file = /var/log/samba/%m.log
        realm = FALKOVSKY.NET
        security = ADS
        server string = Samba Server with SSSD
        workgroup = FALKOVSKY
        idmap config falkovsky : range = 10000-999999
        idmap config falkovsky : backend = sss
        idmap config * : range = 3000-7999
        idmap config * : backend = tdb


[share]
        inherit acls = Yes
        inherit permissions = Yes
        path = /srv/samba/share
        read only = No
        valid users = "@FALKOVSKY\Domain Users"
student@serv-22-40-3:~$
```

У додатку 20.1 наведено текст цього прикладу конфігураційного файлу *smb.conf* з поясненням значень конкретних рядків.

Рис. 20.21.

Виконуємо команду тестування вірності налаштувань *testparm.* У виводі має бути "Loaded services file OK"

Перевіряємо записи krb5.keytab

sudo klist -k /etc/krb5.keytab

Очікувані записи:

host/serv-G-N-3@SURNAME.NET
cifs/serv-G-N-3@SURNAME.NET

Якщо немає cifs/..., додаємо:

sudo net ads keytab add cifs -U administrator



Рис. 20.22.

Для застосування змін у файлі /etc/samba/smb.conf, перезапускаємо служби *sssd,* smbd та nmbd:

sudo systemctl restart sssd smbd nmbd
sudo systemctl status sssd smbd nmbd

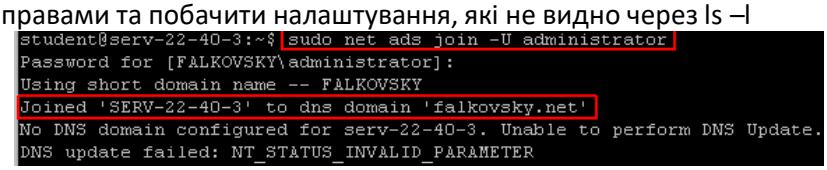
Результат цих команд має бути подібним рис.20.20.

У Samba або в більш складних файлових системах часто використовують **ACL**, щоб точно контролювати доступ до файлів/каталогів не лише для одного власника та групи, а для кількох конкретних користувачів або груп.

Встановлюємо пакети ACL та winbind:

sudo apt update
sudo apt install acl
sudo apt install winbind libnss-winbind libpam-winbind
sudo getfacl /srv/samba/share

Остання команда дозволяє перевірити, хто має доступ до спільної папки, відлагодити проблеми з правами та побачити налаштування, які не видно через ls –l



Для використання winbind з Samba вимагається *приєднання до AD-домену*. Оскільки вже все налаштовано (SSSD, DNS, SRV записи), достатньо виконати:

sudo net ads join -U administrator

Вводимо пароль адміністратора домену.

Машина успішно приєднана до домену. Попередження DNS update failed не є критичним, DNS-записи вже внесено вручну.

Перевірка доступності домену та отримання інформації про користувача
getent passwd dep-rds-1@falkovsky.net

Перевірка Kerberos - отримання Kerberos-квитка:
sudo kinit dep-rds-1@FALKOVSKY.NET
klist

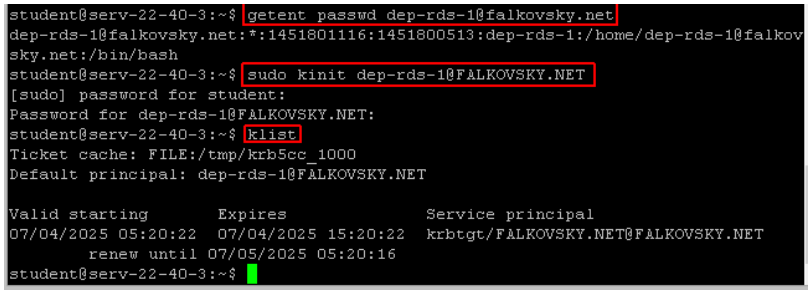


Рис. 20.23.

Знову перезапускаємо усі служби:

sudo systemctl restart sssd smbd nmbd

sudo systemctl restart winbind

winbind обов'язково потрібно запускати після sssd тоді він зможе використовувати бекенд sss для idmap.

Завдання №20.5

1. Спираючись на наведені далі теоретичні відомості, перевірте доступність спільного каталогу /srv/samba/share з довільного комп'ютера з ОС Windows, що належить до вашого домену. У випадку використання контролера домену в якості довільного комп'ютера з ОС Windows для доступу до Samba-ресурсу може знадобитись виконання дій, описаних у додатку 20.2.

Вказівка до виконання п. 1. Імена тестових файлу та каталогу має містити дані про вас: test-dir-ваші-ініціали та test-file-ваші-ініціали.txt **Звіт має містити** скриншоти зроблених налаштувань, опис основних дій.

5. **Перевірка доступу до спільного каталогу на основі Samba.** Аби переконатися, що спільний каталог працює як належне, створимо на сервері Ubuntu у каталозі /srv/samba/share тестові каталог та файл із довільним вмістом.

Створюємо тестовий каталог та тестовий файлу з вмістом:

sudo mkdir /srv/samba/share/test-dir

echo "Congratulations!
If you are reading this from a Windows machine, the Samba layer you purchased is working correctly!" | sudo tee /srv/samba/share/test-file.txt

Права повинні відповідати основним налаштуванням спільного каталогу:

sudo chown -R nobody:nogroup /srv/samba/share/test-dir /srv/samba/share/test-file.txt

sudo chmod 0755 /srv/samba/share/test-dir

sudo chmod 0644 /srv/samba/share/test-file.txt

Файл та каталог:

```
student@serv-22-40-3:/srv/samba/share$ ls -l
total 8
drwxr-xr-x 2 nobody nogroup 4096 Jul  2 14:30 test-dir
-rw-r--r-- 1 nobody nogroup  118 Jul  2 14:28 test-file.txt
student@serv-22-40-3:/srv/samba/share$
```

Вміст файлу test-file.txt:

Congratulations!
If you are reading this from a Windows machine, the Samba layer you purchased is working correctly!

```
student@serv-22-40-3:/srv/samba/share$ cat test-file.txt
Congratulations!
If you are reading this from a Windows machine, the Samba layer you purchased is working correctly!
```

Тепер необхідно внести зміни у системний реєстр на комп'ютері домену, з якого планується підключатися до спільного ресурсу на сервері Linux. Заходимо по гілці системного реєстру:

\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows

Шукаємо розділ реєстру **LanmanWorkstation**

Якщо він відсутній, його потрібно його створити.

У розділі **LanmanWorkstation** створюємо запис типу **DWORD 32** bit з назвою **AllowInsecureGuestAuth** та присвоюємо йому значення 1, як на рис.20.24.

Тепер на комп'ютері домену, де ми налаштували дозвіл **LanmanWorkstation**, запустимо Провідник і введемо в адресному рядку адресу серверу з Ubuntu:

\\serv-G-N-3\share

або

\\192.168.40.246\share

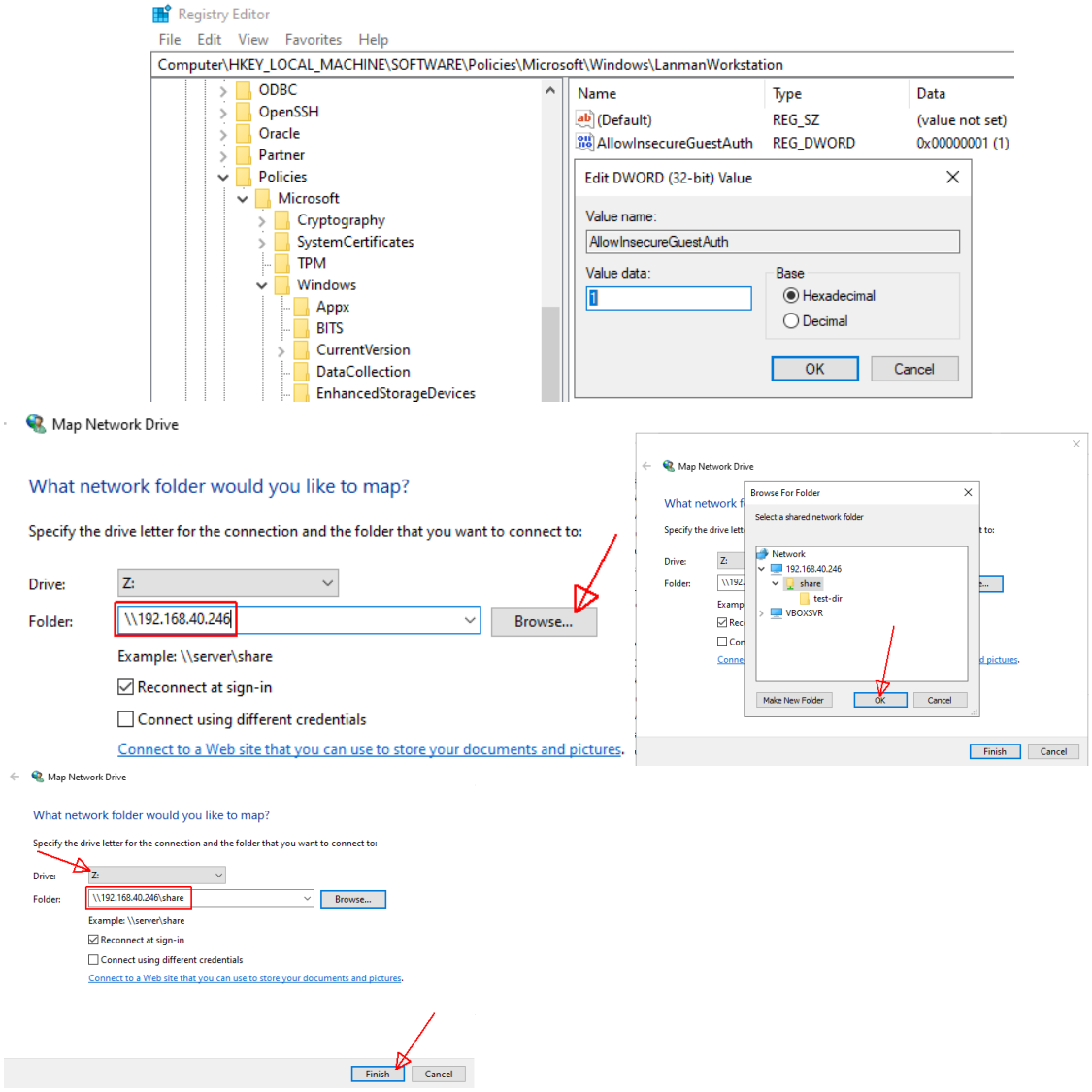


Рис.20.24.

Якщо все було зроблено правильно, має відобразитися спільний каталог (у нашому випадку share), і його вміст повинен бути доступним користувачу для читання.

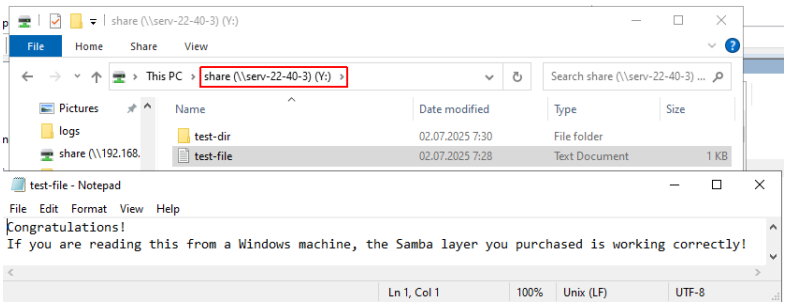


Рис.20.25.

Те ж саме можливо виконати за допомогою командного рядка net use (рис.20.26):

*net use * \\HostNameorIP\share /user:Surname\user-Login **

На рис. 20.26. показане підключення Samba-ресурсу для користувача домену Falkovsky.net dep-rds-1. У першому випадку доступ до Samba-серверу виконується по IP-адресі, у другому – по імені серверу.

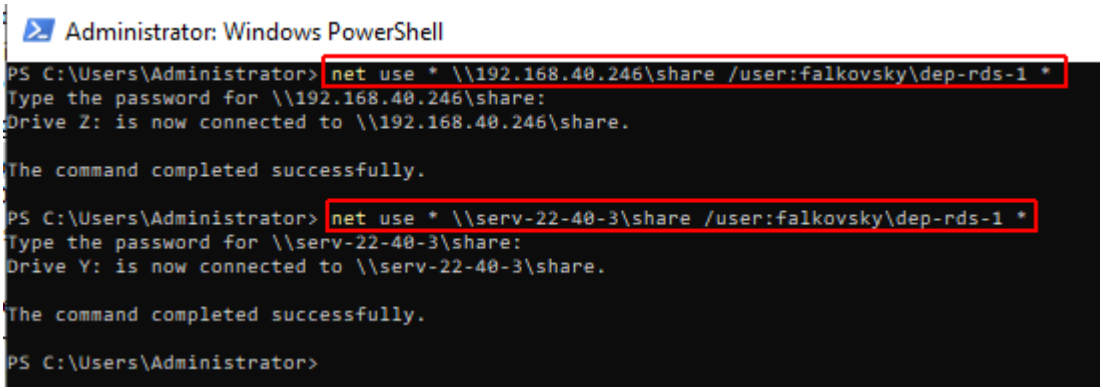


Рис.20.26.

Текст команд:

*net use * \\192.168.40.246\share /user:falkovsky\dep-rds-1 **

*net use * \\serv-22-40-3\share /user:falkovsky\dep-rds-1 **

Вимоги до звіту

Звіт має містити інформацію відповідно до завдань 20.1-20.5.

Додаток 20.1.

Пояснення рядків у секціях [global] та [share] конфігураційного файлу /etc/samba/smb.conf

[global] — загальні налаштування сервера

Параметр	Значення	Пояснення
workgroup = SURNAME	NetBIOS-домен	Ім’я робочої групи (NetBIOS). Має відповідати імені домену без суфіксу .NET.
realm = SURNAME.NET	DNS-домен	Повне ім’я Kerberos-домену (REALM), обов’язково у ВЕРХНЬОМУ регістрі.
security = ads	тип автентифікації	Вказує, що сервер є **членом Active Directory-домену**, і використовує AD для автентифікації.
kerberos method = secrets and keytab	спосіб Kerberos	Samba використовує /etc/krb5.keytab для Kerberos-токенів.
dedicated keytab file = /etc/krb5.keytab	шлях до keytab	Вказує Samba, який keytab-файл використовувати.
server string = Samba Server with SSSD	опис сервера	Інформація, що відображається клієнтам у мережі (необов’язково).
log file = /var/log/samba/%m.log	лог-файли	Індивідуальні логи для кожного клієнта (%m — NetBIOS-ім’я клієнта).
log level = 1	рівень логування	Мінімальний рівень логів. Вищі значення — докладніші, але створюють більше шуму.
idmap config * : backend = tdb	резервна база	Мапінг SID↔UID для невідомих доменів (локальний TDB).
idmap config * : range = 3000-7999	діапазон UID	UID/GID для облікових записів **не з домену FALKOVSKY**.
idmap config SURNAME : backend = sss	основний бекенд	Вказує, що Samba повинна брати мапінг із **SSSD**.
idmap config SURNAME : range = 10000-999999	діапазон UID	UID/GID для облікових записів з домену FALKOVSKY.
winbind enum users = no	не перелічувати	Забороняє Samba автоматично перераховувати користувачів через winbind.
winbind enum groups = no	не перелічувати	Те саме для груп.
winbind use default domain = no	без скорочень	Не обрізає доменне ім’я при вході (тобто потрібно user@domain).
passwd backend = sss	бекенд паролів	(Опціональний параметр) каже Samba звертатися до SSSD при перевірці паролів.

[share] — налаштування ресурсу

Параметр	Значення	Пояснення
path = /srv/samba/share	шлях до каталогу	Фізичне розташування расшареного ресурсу.
read only = no	запис дозволено	Користувачі можуть писати.
browsable = yes	видимий	Каталог видно в мережевому оточенні.
guest ok = no	без гостей	Доступ лише для авторизованих користувачів.
valid users = @"SURNAME\Domain Users"	хто має доступ	Доступ лише для членів групи **Domain Users**. Вказано у Windows-форматі (із лапками та зворотними слешами).
inherit acls = yes	наслідування ACL	Нові файли наслідують ACL від батьківського каталогу.
inherit permissions = yes	наслідування прав	Нові файли успадковують права rwx/rw- тощо від каталогу.

Додаток 20.2.

Налаштування доступу до Samba-ресурсу з Windows Server 2022 (роль: DC)

Відкрийте локальну політику безпеки secpol.msc. У дереві зліва перейдіть до:

Local Policies - Security Options

Змініть такі параметри:

Network access: Let Everyone permissions apply to anonymous users → Enabled

Network access: Do not allow anonymous enumeration of SAM accounts → Disabled

Network access: Do not allow anonymous enumeration of SAM accounts and shares → Disabled

Ці параметри дозволяють гостьовим або анонімним обліковим записам взаємодіяти з ресурсами Samba, що особливо важливо при використанні спільних папок з guest ok = yes.

Перевірте групові політики. Введіть gpedit.msc, перейдіть до:

Computer Configuration - Administrative Templates - Network - Lanman Workstation

Установіть

Enable insecure guest logons → Enabled

Цей параметр дозволяє Windows підключатися до SMB-ресурсів, які не потребують автентифікації (тобто гостьовий доступ), що за замовчуванням заборонено в нових версіях Windows через міркування безпеки.

Після змін перезапустіть політики командою:

gpupdate /force

Або перезавантажте сервер для гарантованого застосування налаштувань.

Перевірте доступ до Samba-ресурсу, наприклад через Провідник Windows або команду net use.

Додаток 20.3.

Налаштування статичної адреси для Ubuntu-server

Сервер Ubuntu після розгортання зконфігуровано на динамічну адресацію. Сервери, зазвичай, працюють на статиці, тому необхідно виконати зміну налаштування динамічної адреси на статичну. Шукаємо назву мережевого інтерфейсу, який необхідно відредагувати ***ip a***

Шукаємо конфігураційні файли Netplan (з розширенням YAML), що зберігаються в каталозі /etc/netplan. Ймовірно, у цьому каталозі є один або декілька файлів YAML. Назва файлу може відрізнятися залежно від налаштувань та версії операційної системи.

sudo dir /etc/netplan

Наприклад, у каталозі знайдено файл 50-cloud-init.yaml. Робимо його копію для редагування:

sudo cp /etc/netplan/50-cloud-init.yaml /etc/netplan/40-natnet.yaml

Відкриваємо для редагування

sudo vi /etc/netplan/40-natnet.yaml

Нижче наведено вміст файлу Netplan до та після редагування.

/etc/netplan/50-cloud-init.yaml --- DHCP

```
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: true
```

/etc/netplan/40-natnet.yaml Static 192.168.40.246/27

```
network:
  version: 2
  ethernets:
    enp0s3:
      addresses:
[192.168.40.246/27]
      gateway4: 192.168.40.241
      nameservers:
        addresses: [192.168.40.243]
```

Зберігаємо відредагований Netplan та застосовуємо внесені зміни:

sudo netplan apply

Помилки у файлі Netplan можуть бути локалізовані за допомогою інструменту yamllint. Встановлення та приклад застосування:

sudo apt install yamllint
yamllint /etc/netplan/40-natnet.yaml

Перевірка ip a покаже, що на інтерфейсі enp0s3 активні дві одночасні IPv4-адреси:

192.168.40.246/27— ручна статична адреса, задана через netplan;

192.168.40.xxx/27— динамічна (DHCP) адреса, отримана автоматично, і позначена як secondary dynamic.

Щоб не отримувати динамічну адресу, перейменовуємо (приховуємо ☺) цю конфігурацію та застосовуємо зміни:

sudo mv /etc/netplan/50-cloud-init.yaml /etc/netplan/50-cloud-init.bkp
sudo netplan apply

Рекомендовані джерела

- Network – Configuration – Ubuntu. URL: https://ubuntu.com/server/docs/network-configuration
- Samba – File Server – Ubuntu. URL: https://ubuntu.com/tutorials/install-and-configure-samba#1-overview
- Service – SSSD – Ubuntu. URL: https://documentation.ubuntu.com/server/how-to/sssd/with-active-directory/
- Samba – Active Directory – Ubuntu. URL: https://ubuntu.com/server/docs/samba-active-directory