Лабораторна робота №6

# Налаштування групових політик в Active Directory

**Мета:** навчитися основ роботи з груповими політиками в Active Directory (на прикладі Windows Server 2022).

**Інструменти:** гіпервізор VirtualBox; (за потреби) мережний емулятор GNS3; модель комп'ютерної мережі та структура домену, побудовані у межах лабораторних робіт №3-5.

**Теоретичні відомості та завдання до лабораторної роботи**

**Завдання №6.1. Аналіз групових політик на рівні домену**

1. Виконайте вхід на одному з контролерів домену під обліковим записомадміністратора та запустіть оснащення *Group Policy Management* (*Server Manager → Tools → Group Policy Management*).

2. Перегляньте та проаналізуйте вкладку *Scope* об'єкту групової політики *Default Domain Policy* для вашого домену. Дайте відповідь на наступні питання.

- Яких контейнерів (сайти, домени, OU), згідно з налаштуваннями, стосується даний об'єкт групової політики?
- Яких облікових записів, груп стосується даний об'єкт групової політики?
- Які WMI-фільтри наразі діють для даного об'єкту групової політики?

3. Перегляньте та проаналізуйте повний перелік налаштувань на вкладці*Settings* об'єкту групової політики *Default Domain Policy* для вашого домену. Дайте відповідь на наступні питання.

- Скільки останніх паролів користувача зберігаються в історії паролів?
- Якою є мінімальна довжина паролю?
- Чи повинен пароль відповідати вимогам складності?
- Який максимальний термін існування паролю?
- Чи встановлене блокування облікового запису у разі помилкового введення паролю? Якщо так, після скількох невдалих спроб відбувається блокування?

**Це допоможе вам виконати наступні завдання.** У дужках щодо кожної відповіді на запитання із п. 3 вкажіть вузол налаштувань, до яких належить відповідна групова політика. Наприклад: *Computer Configuration → Policies →*

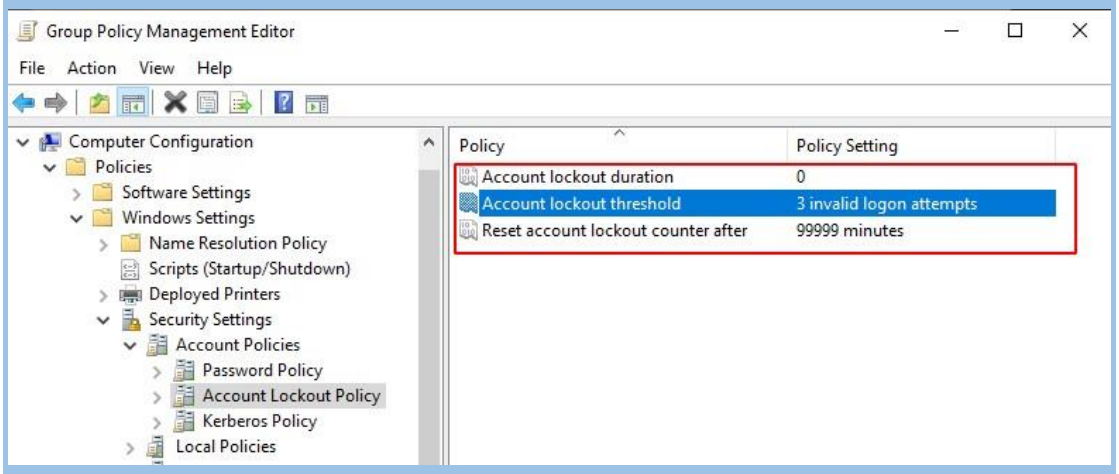
*Windows Setting → Security Settings → Account Policies/Password Policy → Minimum password length*.

**Звіт має містити** скриншоти зроблених налаштувань, опис основних дій, а також відповіді на поставлені запитання.

**Завдання №6.2**

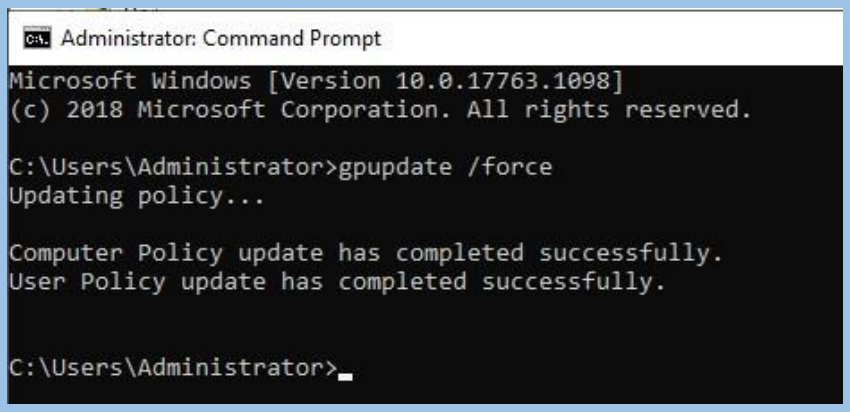
1. Спираючись на відомості, одержані вами під час виконання*завдання №6.1*, відредагуйте об'єкт групової політики *Default Domain Policy* так, щоб у межах вашого домену відбувалося блокування облікового запису після трьох підряд невдалих спроб входу, а розблокування мав робити адміністратор.

Підказка до п. 3:




2. Групові політики час від часу оновлюються автоматично (30-120 хвилин). Щоб не чекати, можна зробити наступне:

- Запустіть командний рядок на контролері домену і введіть команду gpupdate /force




- Коли оновлення групових політик на контролері домену завершиться, запустіть командний рядок на тестовій робочій станції і повторіть таку саму команду там

3. Після оновлення групових політик перевірте зроблені налаштування:

- З довільної робочої станції домену зробіть три поспіль невдалі спроби входу від імені будь-якого облікового запису і переконайтеся, що обліковий запис заблоковано.
- На контролері домену під обліковим записом адміністратора домену знайдіть заблокованого користувача у відповідній OU і розблокуйте його.
- Переконайтеся, що раніше заблокований користувач знову має можливість увійти.

**Звіт має містити** скриншоти зроблених налаштувань та опис основних дій.

## Делегування прав на керування OU локальним адміністраторам

### Етап I: Створення групи локальних адміністраторів

1) Відкрийте оснащення *Active Directory Users and Groups*.

2) У межах організаційної одиниці адміністраторів створіть нову групу локальних адміністраторів (рис. 6.1).

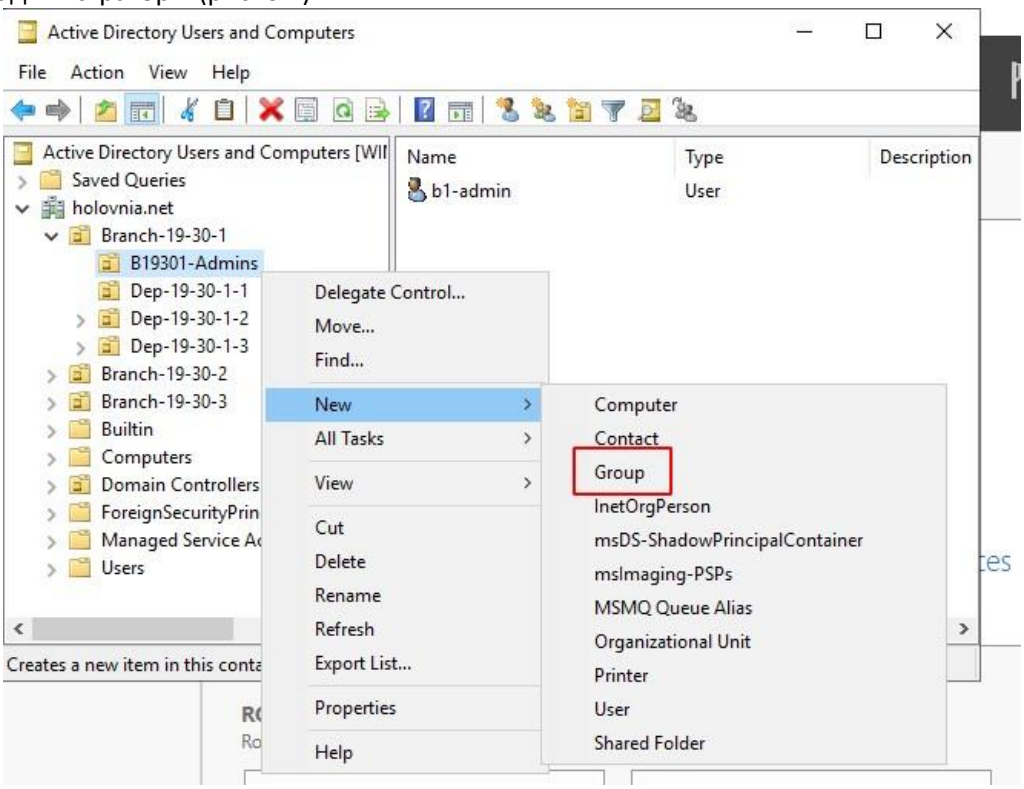



Рис. 6.1

3) Дайте групі ім’я, унікальне у межах домену. Межі дії групи - *Domain local* (рис. 6.2).

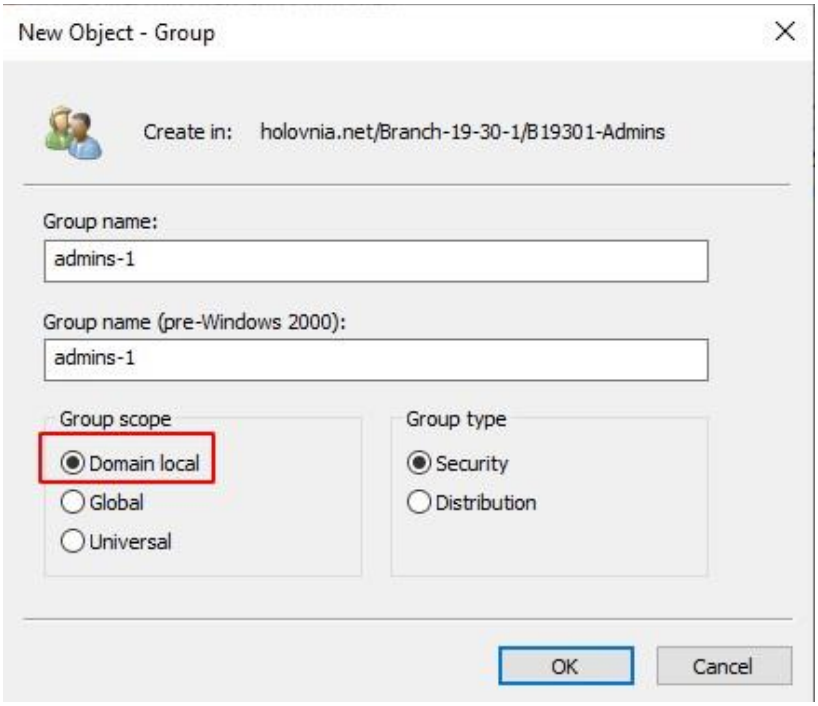



Рис. 6.2

4) Додайте наявні в даній організаційній одиниці облікові записи адміністраторів у новостворену групу (рис. 6.3).

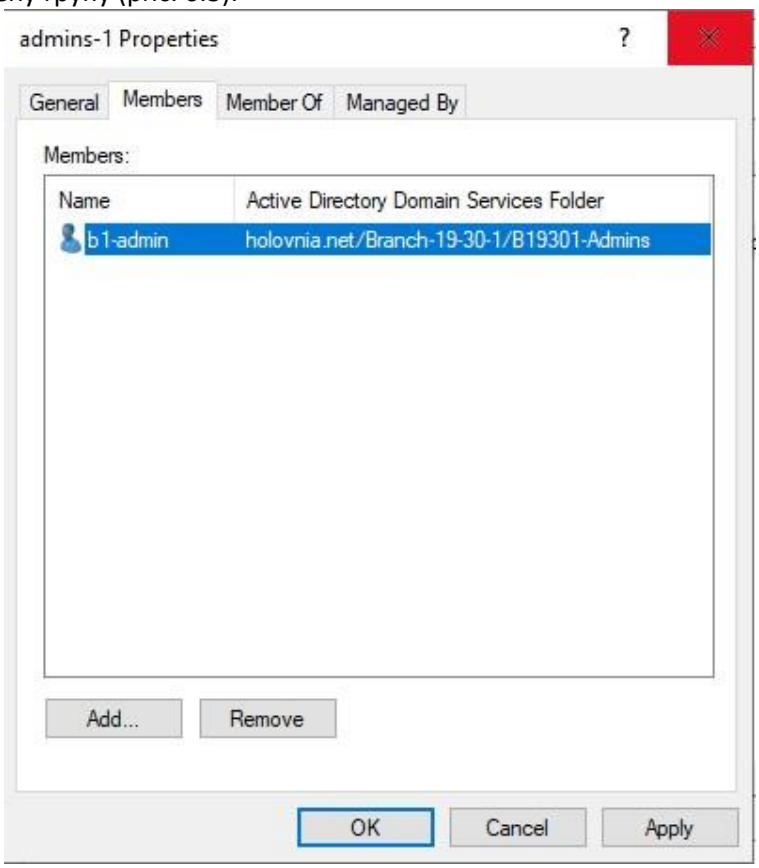



Рис. 6.3

5) Тепер у межах організаційної одиниці для локальних адміністраторів буде адміністративний обліковий запис (записи) і відповідна група (рис. 6.4).

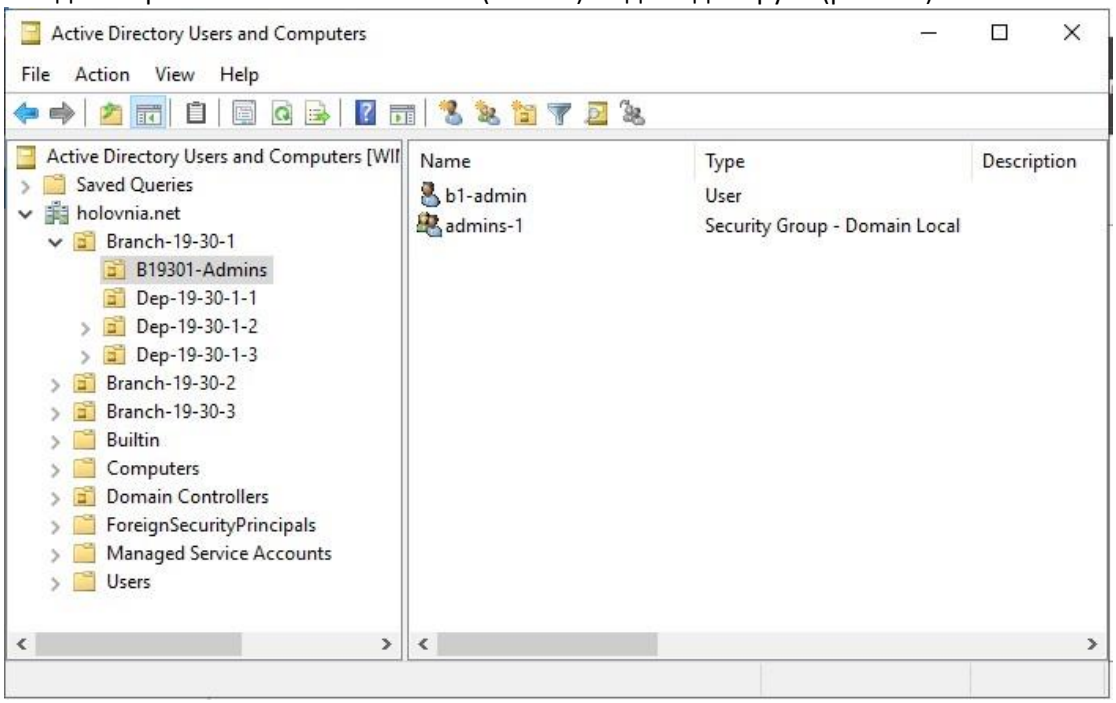



Рис. 6.4.

**Етап II: Делегування групі локальних адміністраторів відповідних прав**

1) Виберіть організаційну одиницю, яку мають адмініструвати члени новоствореної групи (*Branch-19-30-1* у прикладі). У контекстному меню клацніть по пункту *Delegate Control* (рис. 6.5).

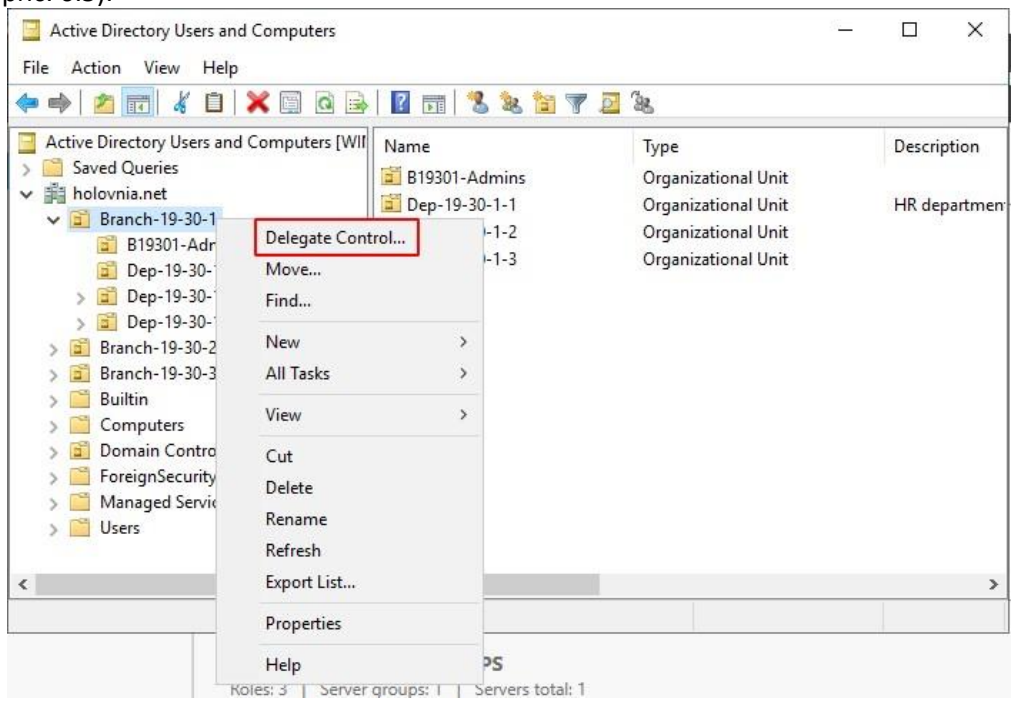



Рис. 6.5

2) Додайте до переліку користувачів та груп, яким треба делегувати контроль над цією організаційною одиницею, новостворену групу локальних адміністраторів (рис. 6.6).

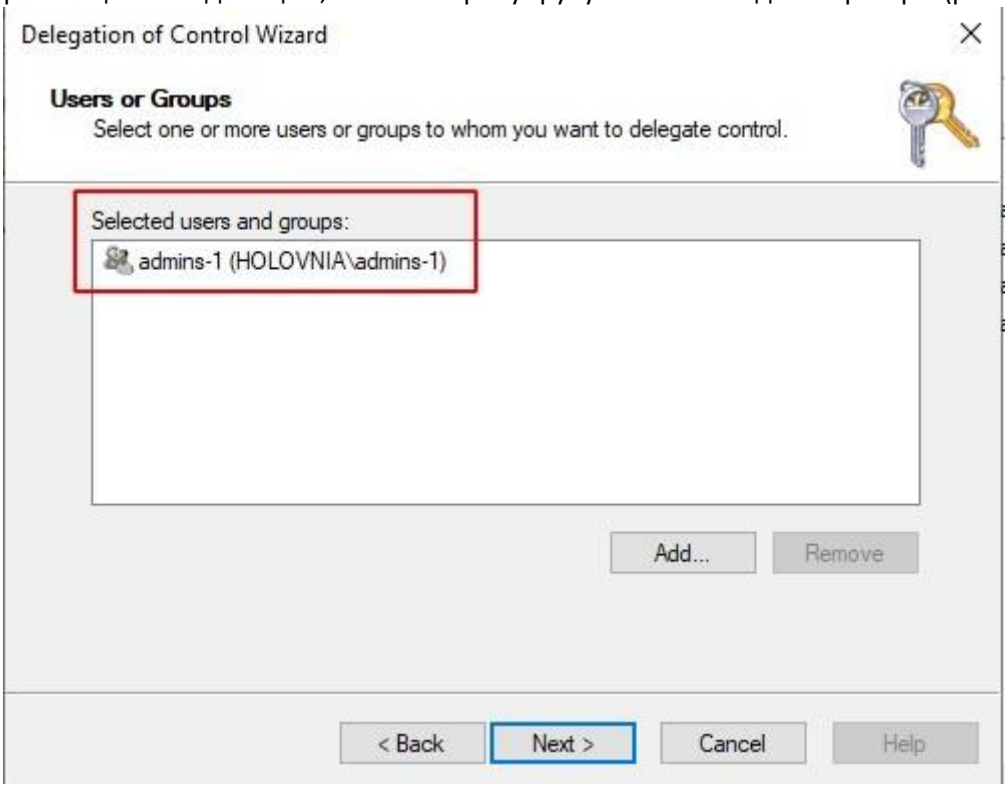



Рис. 6.6

3) Виберіть права, які треба делегувати групі. У прикладі обрано більшість адміністративних прав. Діятимуть вони лише у межах даної організаційної одиниці (рис. 6.7, рис. 6.8).

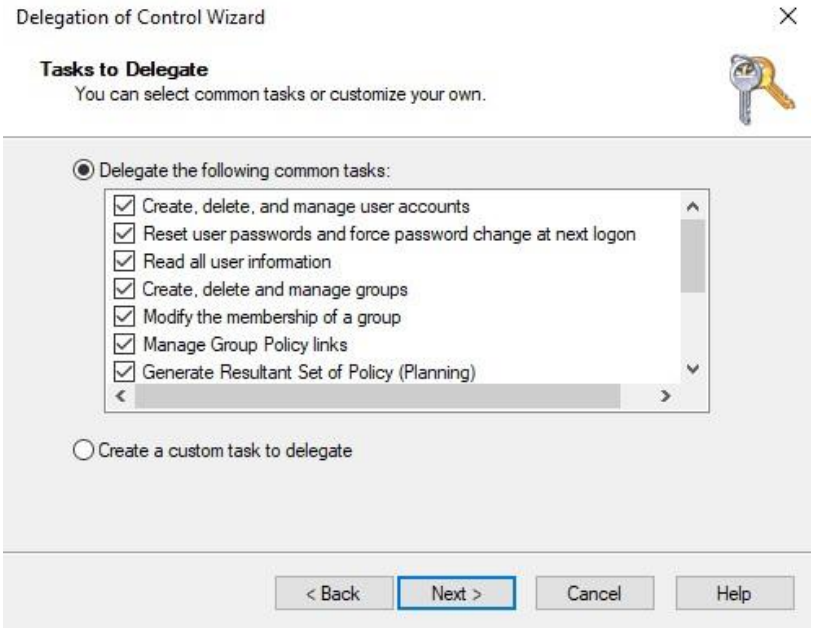



Рис. 6.7

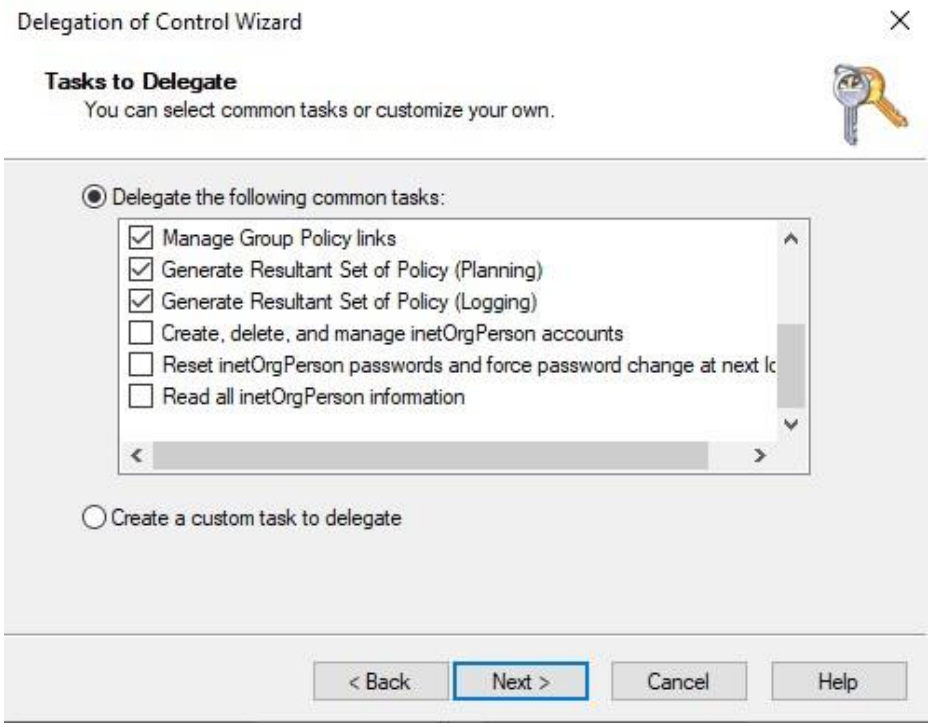



Рис. 6.8

4) Перевірте і підтвердіть зроблені налаштування (рис. 6.9).




Рис. 6.9

**Етап III: Надання групі локальних адміністраторів прав на локальний вхід на контролері домену (за потреби)**

1) Відкрийте оснащення *Group Policy Management*.

2) Оберіть потрібний ліс, домен та організаційну одиницю. У прикладі це організаційна одиниця *Domain Controllers* всередині домену *holovnia.net* (рис. 6.10). Знайдіть об'єкт групової політики *Default Domain Controller Policy* та у його контекстному меню виберіть *Edit*.

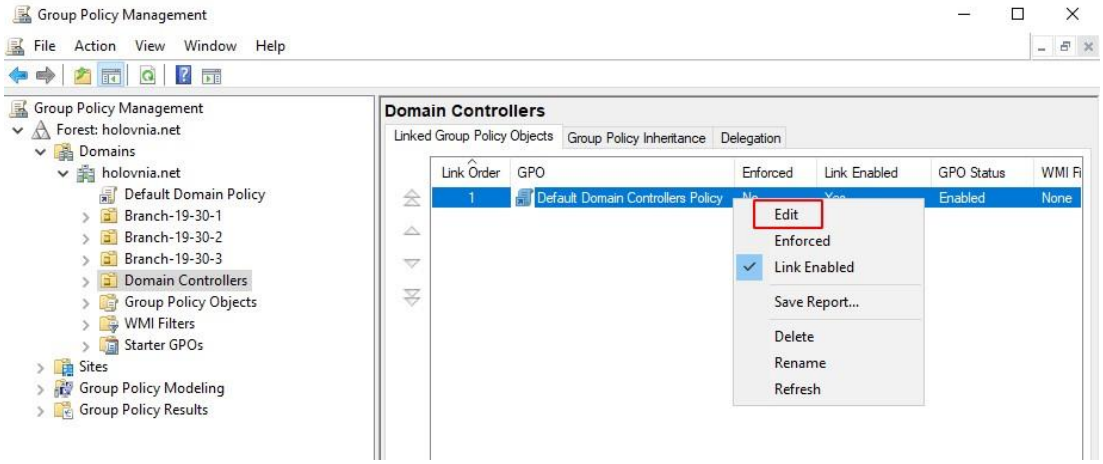



Рис. 6.10

3) Відкриється вікно *Group Policy Management Editor*. Оберіть *Computer Configuration* → *Policies* → Windows Settings → Security Settings → Local Policies → User Right Assingment та двічі клацніть по політиці Allow log on locally (рис. 6.11).

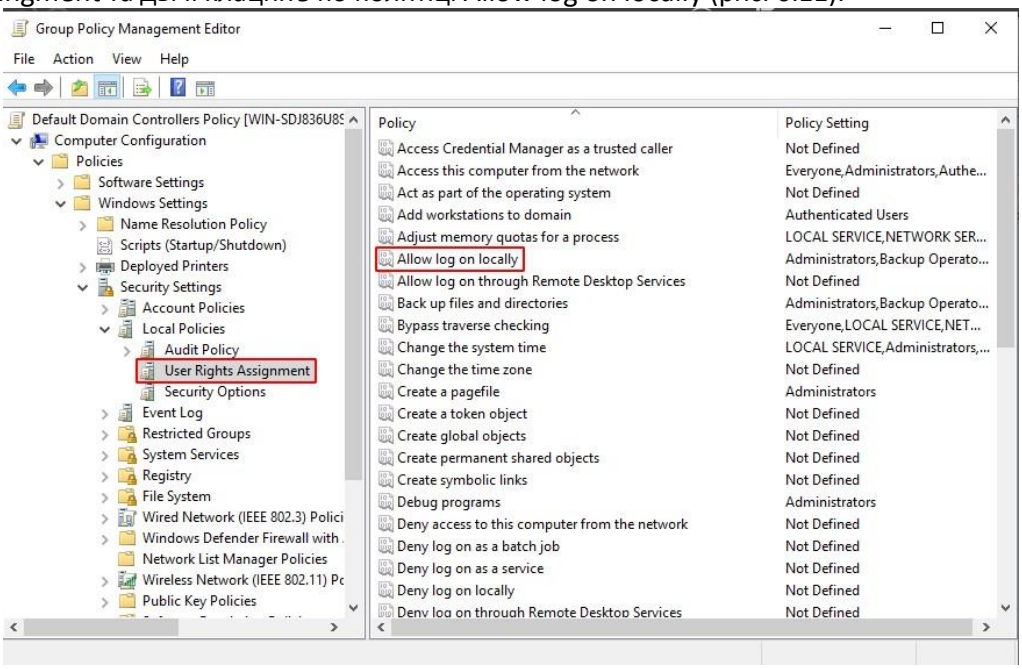



Рис. 6.11

4) Додайте до переліку користувачів та груп, яким дозволено локальний вхід на контролери домену, групу локальних адміністраторів (рис. 6.12).

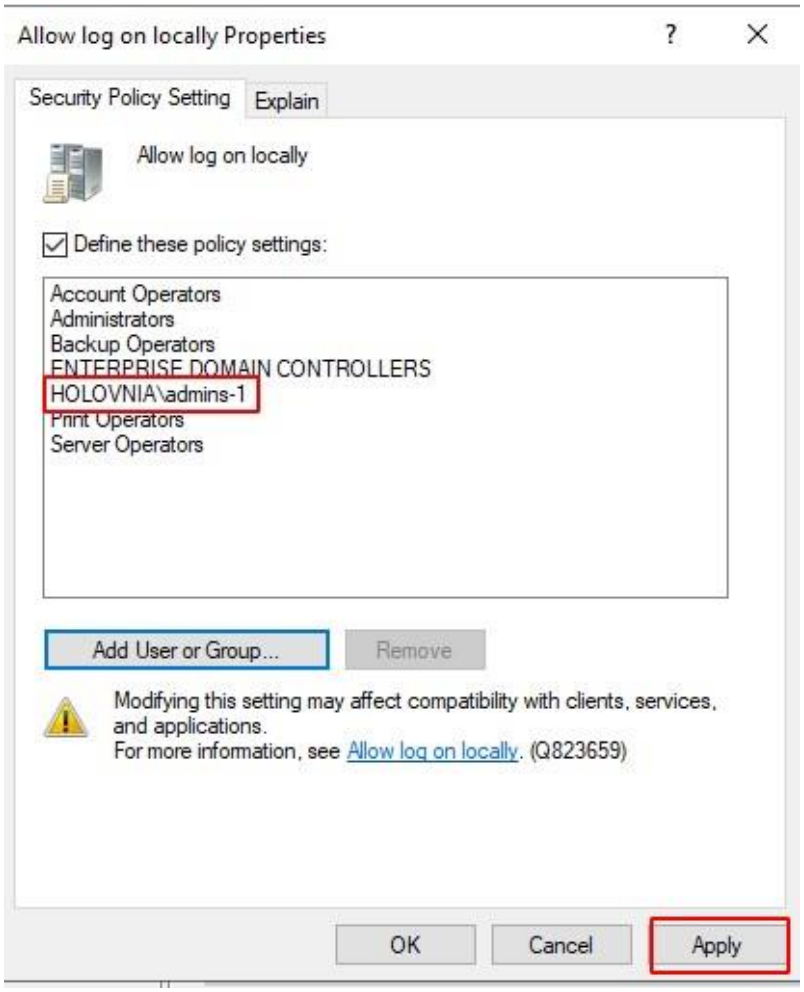



Рис. 6.12

5) Виконайте оновлення групової політики для контейнера *Domain Controllers*.

**<u>Завдання №6.3. Налаштування повноважень для локальних адміністраторів</u>**

1. Спираючись на подані вище теоретичні відомості, створіть в OU *Branch-GGNN-1* групу локальних адміністраторів та делегуйте їх адміністративні повноваження на рівні цієї організаційної одиниці.

2. Дозвольте членам новоствореної групи локальних адміністраторів локальний вхід на контролерах домену.

3. Перевірте зроблені налаштування, ввійшовши на контролері домену від імені одного з членів групи локальних адміністраторів OU *Branch-GG-NN-1* і спробувавши створити нового користувача у межах цієї організаційної одиниці. Чи вдається це зробити? Чи вдається створити користувача у межах іншої організаційної одиниці? Чому?

**<u>Звіт має містити</u>** скриншоти зроблених налаштувань, опис основних дій, а також відповіді на поставлені питання.

**Завдання №6.4. Налаштування традиційних політик для користувачів та комп'ютерів**

1. У лабораторній роботі №5 ми не створювали організаційні одиниці для комп'ютерів - через обмежену кількість робочих віртуальних машин. Однак для виконання наступного завдання нам знадобиться принаймні одна така організаційна одиниця.

За допомогою оснащення *Active Directory Users and Groups* створіть у вашому домені організаційну одиницю *Computers-GG-NN,* а в ній - дочірню організаційну одиницю *Comp-Branch-GG-NN-1.* Перемістіть одну з робочих станцій із контейнера *Computers* в організаційну одиницю *Comp-Branch-GG-NN1*.

2. Самостійно з'ясуйте, як в оснащенні *Group Policy Management* за допомогою вузла *Policies* (традиційні групові політики) **для комп'ютерів** зробити так, щоб*:*

- у межах OU *Comp-Branch-GG-NN-1* звичайні користувачі **були зобов'язані** встановлювати собі паролі довжиною принаймні 10 символів.

Виконайте описані вище налаштування.

3. Самостійно з'ясуйте, як в оснащенні *Group Policy Management* за допомогою вузла *Policies* (традиційні групові політики) **для користувачів** зробити так, щоб*:*

- у межах OU *Branch-GG-NN-1* звичайним користувачам не було дозволено запускати *Панель керування* (*Control Panel*);

- у межах OU *Branch-GG-NN-1* вимкнулося відображення значка *Смітника* / *Корзини* на робочому столі.

Виконайте описані вище налаштування.

***Підказки*.** Для окремих налаштувань вам може знадобитися вузол *Administrative Templates*. Для встановлення заборони на запуск *Панелі керування* існує більше одного шаблону. Оберіть той, що працюватиме.

4. Переконайтеся, що налаштування успішно застосовані.

**Звіт має містити** скриншоти зроблених налаштувань та опис основних дій.

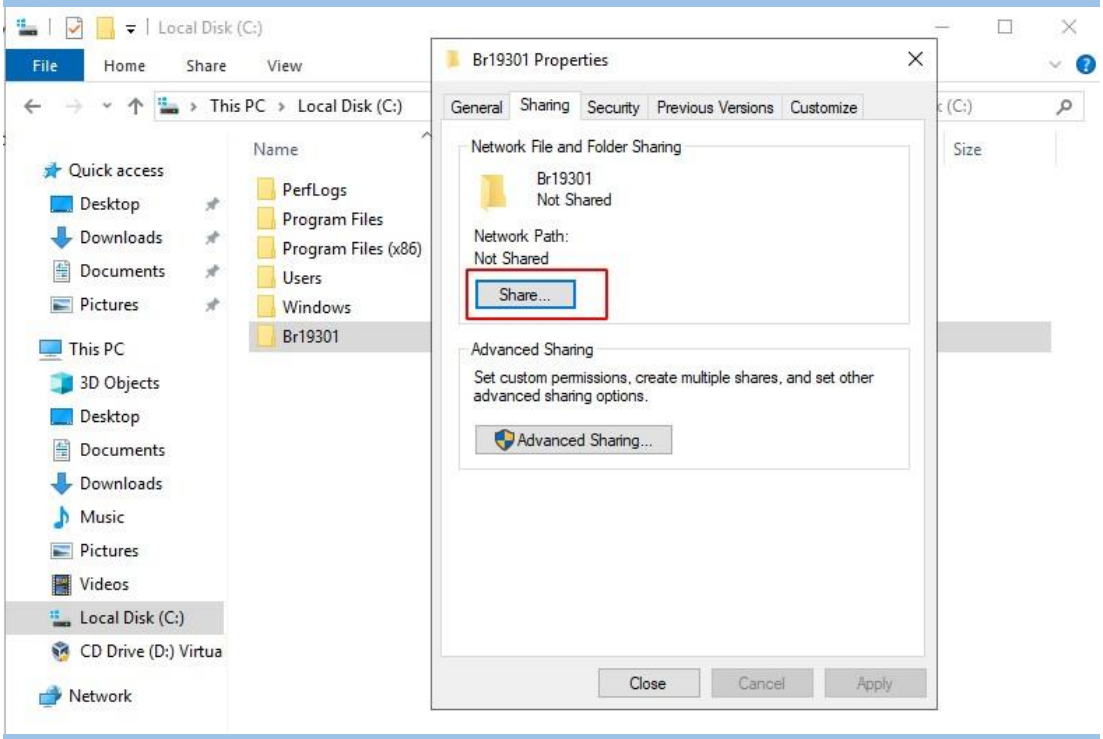
**Завдання №6.5. Налаштування *Preferences* для комп'ютерів**

1. Спираючись на матеріали лекції, самостійно з'ясуйте, як за допомогою вузла *Preferences* налаштувати для користувачів OU *Branch-GG-NN-1*:

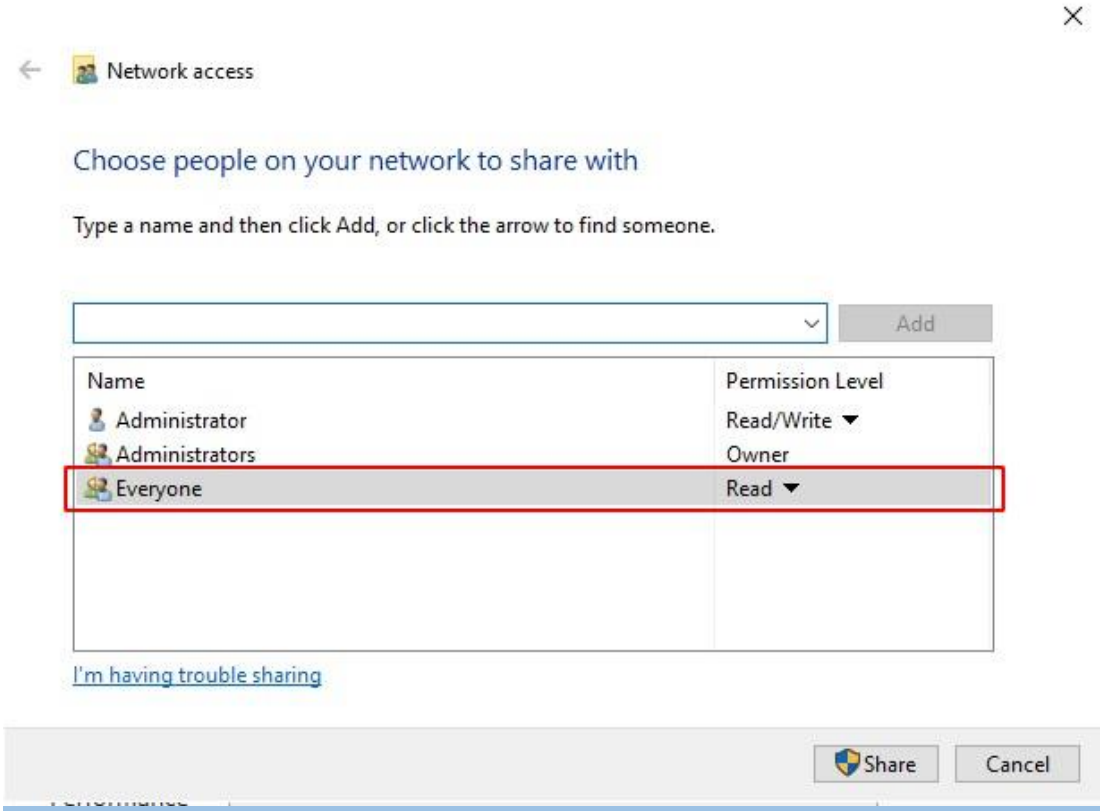
- підключення мережного диску з міткою *BrGGNN1*.

**Підказка.** Відповідну папку можна створити на контролері домену. Наприклад, так.

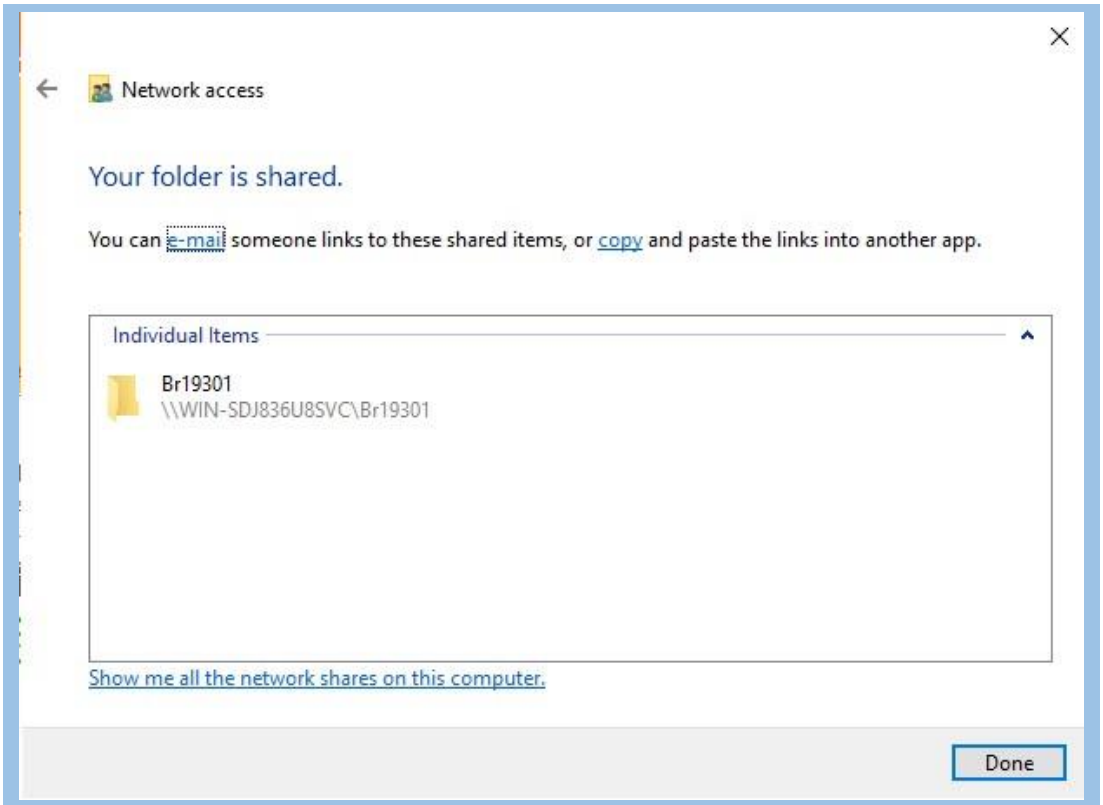
Створюємо папку і вибираємо *Properties -> Sharing -> Share*:




Дозволяємо групі *Everyone* (всім користувачам, які пройшли автентифікацію) читання вмісту цієї папки:




З’ясовуємо мережне ім’я спільної папки:




Дії, необхідні для підключення цієї папки як мережного диску, описані у лекції.

**Звіт має містити**скриншоти зроблених налаштувань та опис основних дій.

**Завдання №6.6**

1. За допомогою вузла *Group Policy Results* дослідіть права, які має один з локальних адміністраторів OU *Branch-GG-NN-1* у межах домену.

2. За допомогою вузла *Group Policy Modeling* змоделюйте ситуацію, що матиме місце, якщо того самого локального адміністратора OU *Branch-GG-NN-1* додати до групи *Domain Admins*.

**Звіт має містити** скриншоти зроблених налаштувань, опис основних дій, а також відповіді на поставлені питання.

## Вимоги до звіту

Звіт має містити інформацію відповідно до завдань 6.1-6.6.