Практична робота 5. Створення розподілених мережевих ресурсів засобами ОС Microsoft Windows Server

Мета: ознайомитись з можливостями Microsoft Windows по роботі з розподіленими ресурсами. Навчитись використовувати об'єкти групової політики з консолі керування груповою політикою для створення шаблонів управління та обслуговування ресурсів ОС

Теоретичні відомості

Розподіленим мережним ресурсом є папка, до якої організовано доступ через мережу і яка має унікальне мережне ім’я. Створення загального доступу до папки вказує Службі доступу до файлів і принтерів Microsoft (File And Printer Sharing For Microsoft Networks)на можливість підключеннядо цієї папки та її підпайок клієнтам, на комп’ютерах яких виконуєтьсяслужба Клієнт для мереж Microsoft (Client For Microsoft Networks).

Розподілені ресурси можна створювати з контекстного меню папки або за допомогою консолі MMC. Відкривши оснащення Загальні папки (Shared Folders)у консолі MMC або в консолі Керування комп’ютером (Computer Management),спостерігаємо, що у Windows Server 2003 вже налаштовано декілька стандартних адміністративних загальних ресурсів: системний каталог (зазвичай C:\Windows) і корінь кожного жорсткого диска. Ім’я ресурсу для таких загальних папок закінчується знаком долара ($). Знак «долар» наприкінці мережного імені позначає приховані загальні папки системного призначення. їх не можна побачити у програмі переглядачі(провіднику), але до них можна звернутися, вказавши їх ім’я на зразок:

\\ ім’я_сервера\ім’я_загального_ресурсу$

До адміністративних загальних ресурсів (наприклад, логічних дисків c$, d$ тощо) можна звернутися тільки з використанням облікового запису адміністратора.

Загальні папки до консолі MMC. У контекстному меню пункту Загальні папки або в меню Дія (Action) необхідно вибрати Новий загальний ресурс (NewShare). Майстер створення загальних ресурсів містить такі сторінки:

- Шлях до папки (Folder Path) – вказує шлях до загальної папки на локальному диску;
- Ім’я, опис і параметри (Name, Description and Settings) – задає ім’я загального ресурсу. Ім’я ресурсу разом з іменем сервера утворюють мережний шлях доспільної папки – \\ім’я_сервера\ім’я_загального_ресурсу;
- Дозволи (Permissions) – дає змогу вибрати користувачів, які матимуть доступ до ресурсу, та задати правила доступу (читання, запис).

Правила доступу до мережних ресурсів не такі детальні, як дозволи файлової системи NTFS, проте вони дають змогу налаштувати основні типи доступу до спільної папки (таблиця 5.1).

Таблиця 5.1 – Правила доступу до розподілених ресурсів

Правило	Опис
Читання (Read)	Користувачі можуть переглядати назви папок, а також імена, вміст та атрибути файлів, запускати програми й звертатися до інших підпапок у середині папки із загальним доступом.
Зміна (Change)	Користувачі можуть створювати папки, додавати файли й редагувати їхній вміст, змінювати атрибути файлів, видаляти файли і папки та виконувати дії, визначені дозволом Читання (Read).
Повний доступ (Full Control)	Користувачі можуть змінювати локальні правила доступу, отримувати права власності на файли і виконувати всі дії, допустимі дозволом Зміна (Change).

Іншим способом створення спільних ресурсів є використання вікна властивостей папки. Після виклику цього вікна потрібно перейти на вкладку Доступ (Sharring), у якій можна вказати:

- максимальну кількість одночасних з’єднань користувачів.
- правила доступу для окремих користувачів.

Параметри доступу до спільного ресурсу визначають максимальні діючі дозволи для всіх файлів і папок усередині нагальної папки. Призначаючи дозволи на рівні файлової системи NTFS для окремих файлів і папок, на рівні роботи через мережу, доступ можна посилити, але не розширити. Інакше кажучи, доступ користувача до файлу або папки визначається найбільш жорстким набором до. і поліп загального ресурсу й правил таблиці ACL. Це одна з причин, з якої, зазвичай, групі Всі (Everyone) надається дозвіл Повний доступ, (Full Control), а для захисту папок і файлів використовують тільки дозволи файлової системи NTFS.

Автентифікація при звертанні до розподіленого ресурсу будь-яким із запропонованих способів відбувається так:

- клієнт надсилає дані, які були введені користувачем у процесі реєстрації в системі;
- якщо логін і пароль збігаються із записом бази користувачів сервера, то сервер авторизує клієнта;
- якщо логін і пароль не збігаються з жодним записом бази користувачів сервера, то сервер надсилає запит клієнту на введення імені користувача та пароля.

Ще одним завданням, яке постає перед системним адміністратором, є конфігурування принтера для друку документів з віддаленого комп'ютера. Для цього потрібно встановити загальний доступ до принтера (за умови, що драйвер принтера вже встановлено на одному з комп'ютерів).

Порядок виконання роботи

1. Відкрити оснащення ттс Групова політика. Перейти у гілку Політика паролів, задати мінімальну довжину пароля. Після цього спробувати змінити власний пароль на такий, довжина якого менша за вказану у політиці, переконатись у неможливості такої дії. Повторити ці дії з параметрами: Пароль повинен відповідати вимогам складності.

2. Перейти у гілку Політика блокування облікового запису, задати граничне значення блокування. Після цього спробувати кілька разів зайти у систему з неправильним вводом пароля - переконатись у спрацюванні блокування. Увійти у систему як адміністратор - зняти блокування через оснащення Локальні користувачі та групи у властивостях облікового запису.

3. Перейти у гілку Локальні політики\Призначення прав користувача, задати привілей на вимкнення комп'ютера тільки для групи адміністраторів. Увійти до системи як користувач без адміністративних привілеїв; переконатись, що пункт Виключити комп'ютер зник з меню Пуск, а також, що завершення роботи системи з командного рядка теж неможливе.

4. Оглянути вміст гілки Адміністративні шаблони для частин: Конфігурація комп'ютера та Конфігурація користувача. У гілці Панель керування\Екран увімкнути політику видалення значка Екран з панелі керування. Спробувати змінити параметри екрана. Переконатись, що політики діють на усіх користувачів локальної системи.

5. Перейти у гілку Політики обмеженого використання програм. Створити нову політику. Не змінюючи політики за замовчуванням, створити нове правило (правила), що забороняє виконання програм з будь-якого іншого тому, окрім тому C: (за потреби створити логічні диски або розділи). Спробувати виконати будь-який файл з цього тому. Створити нове правило для хешу програми, яке дасть змогу виконувати саме цей вказаний файл. Спробувати запустити на виконання цей файл. Для яких потреб можуть використовуватись правила такого типу?

6. Відкрити оснащення Аналіз та налаштування безпеки. Створити нову базу даних, яка відображатиме стан налаштування політик комп'ютера за певним шаблоном. Для порівняння обрати один із вбудованих шаблонів безпеки (власні шаблони можна створювати за допомогою оснастки Шаблони безпеки). Проаналізувати параметри безпеки комп'ютера. Результати аналізу відображаються як порівняння параметрів комп'ютера з параметрами шаблона (створеної бази даних). Базу даних можна редагувати у цьому самому вікні, а

потім вибрати пункт контекстного меню Зберегти та за потреби, експортувати відредагований шаблон безпеки.

7. Налаштувати комп'ютер за певним шаблоном безпеки (привести у відповідність параметри бази даних і поточні налаштування комп'ютера), виконавши необхідні дії.

8. У звіті до лабораторної роботи описати та пояснити отримані результати.