Лабораторна робота
Служба доменів Active Directory та використання групових політик

Групові політики є потужним інструментом, за допомогою якого адміністратор може здійснювати централізоване конфігурування великої кількості робочих станцій в масштабах домену.

1. Оснащення Group Policy Object Editor

Оснащення Group Policy Object Editor (Редактор об'єктів групової політики) використовується для редагування параметрів об'єктів групової політики (group policy objects, GPO). Оснащення Group Policy Object Editor надає адміністратору більше можливостей по конфігурації параметрів групової політики в порівнянні з іншими оснащеннями, які передбачають роботу з груповою політикою, - оснащеннями Local Security Policy, Domain Controller Security Policy і Domain Security Policy. Зазначені оснащення забезпечують доступ тільки до обмеженої підмножини параметрів групової політики, розташованих в контейнері Security Setting (Параметри безпеки) відповідного об'єкта групової політики. Оснащення Domain Controller Security Policy і Domain Security Policy встановлюються на кожному контролері домену. Оснащення Local Security Policy присутнє на кожному звичайному комп'ютері під керуванням Windows.

2. Прив'язка оснащення до об'єкта групової політики

Оснащення Group Policy Object Editor може бути викликане з оснасток Active Directory Users and Computers і Active Directory Sites and Services. Для цього у вікні властивостей об'єкта, асоційованого з сайтом, доменом або підрозділом (Organizational Unit, OU) необхідно перейти на вкладку Group Policy (рис. 1).

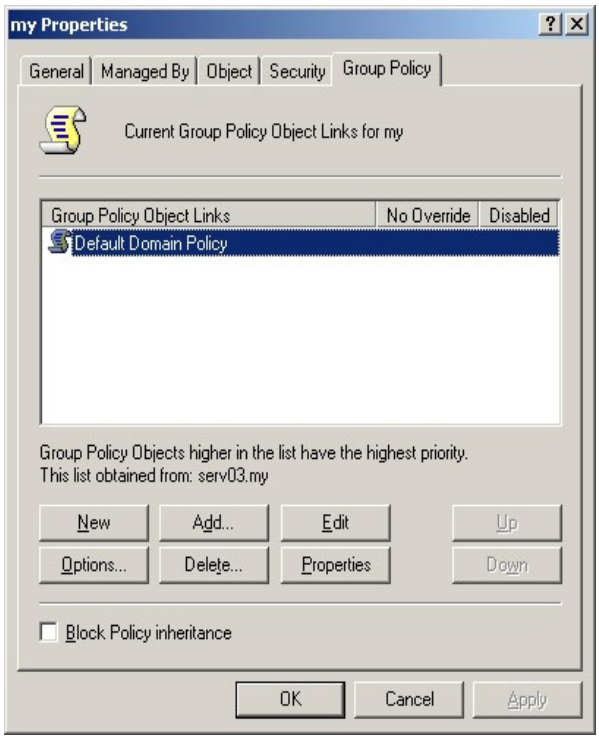

Рис. 1. Вкладка Group Policy вікна властивостей підрозділу

Необхідно розрізняти операцію прив'язки оснащення Group Policy Object Editor до деякого

об'єкту GPO і операцію прив'язки безпосередньо самого об'єкта GPO до деякого контейнеру каталогу.

Примітка: Оскільки при пошуку об'єктів групової політики виконуються звернення до DNS, помилки при запуску оснасток Group Policy Object Editor нерідко пояснюються неправильною роботою служби DNS. Тому при появі подібних помилок завжди перевіряйте конфігурацію DNS. Пам'ятайте про те, що DNS - це динамічна система, і ресурсні записи стають простроченими і вимагають періодичної перереєстрації.

3. Створення та видалення об'єктів групової політики

Для створення нового об'єкта групової політики досить клацнути на кнопці New (Створити) на вкладці Group Policy (див. Рис. 1) у вікні властивостей деякого контейнера. Система запропонує адміністратору дати ім'я створюваному об'єкту групової політики. Після цього системою буде створений об'єкт групової політики зі значеннями параметрів за замовчуванням.

Видалення об'єкта групової політики, не прив'язаного до якогось контейнеру каталогу, не викликає особливих труднощів. У разі, якщо подібна прив'язка існує, система вимагає дати додаткові вказівки:

- Remove the link from the list (Вилучити посилання зі списку, не видаляючи об'єкта). Вибираючи цей режим, адміністратор фактично тільки видаляє прив'язку обраного об'єкта групової політики до деякого контейнеру каталогу. Безпосередньо сам об'єкт групової політики залишається незмінним, і його можна використовувати згодом;

- Remove the link and delete the Group Policy Object permanently (Вилучити посилання і остаточно видалити об'єкт групової політики). Вибір даного режиму призводить до видалення безпосередньо самого об'єкта групової політики. При цьому також видаляються існуючі прив'язки зазначеного об'єкта до контейнерів каталогу.

4. Прив'язка об'єкта групової політики до контейнера Active Directory

Будь-який об'єкт групової політики може бути прив'язаний до певного сайту, домену або підрозділу (Organizational Unit, OU). Один об'єкт групової політики може бути прив'язаний до багатьох контейнерів. Для виконання прив'язки необхідно клацнути на кнопці Add на вкладці Group Policy вікна властивостей контейнера. У вікні Browse for a Group Policy Object всі об'єкти групової політики, що існують в домені, перераховані на вкладці All (Все).

Адміністратору достатньо вибрати необхідний об'єкт групової політики і клацнути по кнопці ОК.

Можлива і зворотна операція. Адміністратор може знайти контейнери, до яких прив'язаний обраний об'єкт групової політики. Для цього в оснащенні Group Policy Object Editor необхідно в контекстному меню кореневого об'єкта оснащення вибрати пункт Properties (Властивості), щоб відкрити вікно властивостей об'єкта групової політики. У вікні властивостей необхідно перейти на вкладку Links (рис. 2). Вибравши зі списку Domain потрібний домен і натиснувши кнопку Find Now (Знайти), адміністратор отримає список контейнерів, до яких до зараз прив'язаний даний об'єкт групової політики.

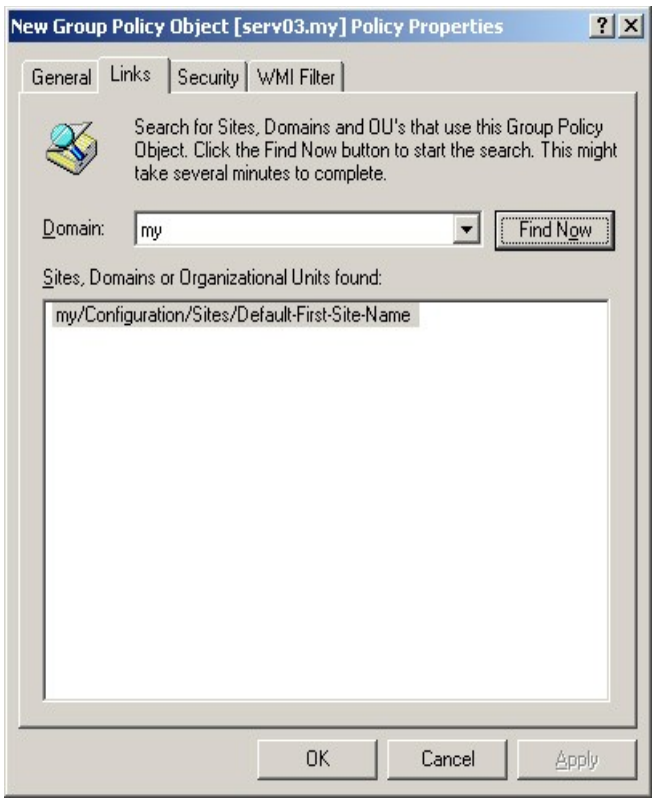

Рис. 2. Перегляд прив'язок обраного об'єкта групової політики

5. Структура об'єкта групової політики

Множина параметрів, що визначаються в рамках об'єкта групової політики, розділене на дві частини. Одна частина параметрів використовується для конфігурації комп'ютера (computer configuration), інша частина параметрів використовується для конфігурації середовища користувача (user configuration). Конфігурація комп'ютера передбачає визначення значень для параметрів, які впливають на формування оточення будь-яких користувачів, що реєструються на даному комп'ютері. Конфігурація середовища користувача дає можливість управляти процесом формування оточення конкретного користувача, незалежно від того, на якому комп'ютері він реєструється в мережі.

Незалежно від типу конфігурації, параметри групової політики організовані в спеціальні категорії. Кожна з категорій параметрів групової політики визначає окрему область середовища користувача. У свою чергу категорії параметрів групової політики організовані в три контейнера відповідно до свого призначення:

- Software Settings (Конфігурація програм). У контейнері розміщуються категорії параметрів групової політики, за допомогою яких можна управляти переліком застосунків, доступних користувачам;

- Windows Settings (Конфігурація Windows). У контейнері розміщуються категорії параметрів групової політики, що визначають настройку безпосередньо самої операційної системи. Вміст даного контейнера може бути різним, залежно від того, для кого визначаються параметри групової політики (для користувача або комп'ютера);

- Administrative Templates (Адміністративні шаблони). Цей контейнер містить категорії параметрів групової політики, які застосовуються для управління вмістом системного реєстру комп'ютера.

6. Адміністративні шаблони

Механізм адміністративних шаблонів дозволяє адміністратору за допомогою групової політики конфігурувати системний реєстр клієнтських комп'ютерів. Для будь-якої робочої станції, яка підпадає під дію деякого об'єкту групової політики, системний реєстр буде налаштований відповідно до адміністративного шаблону, визначеного у рамках даного об'єкта.

Адміністративні шаблони НЕ задіють весь реєстр цілком, а тільки два його ключа: HKEY_LOCAL_MACHINE і HKEY_CURRENT_USER.

Хоча, як було відмічено, адміністративний шаблон може використовуватися для конфігурації будь-яких ключів реєстру, кращим є використання ключів HKEY_LOCAL_MACHINE \ software \ Policies (для управління Параметрами комп'ютера) І HKEY_CURRENT_USER \ Software \ Policies (для управління середовищем користувачів). Дані ключі реєстру очищуються системою автоматично, при кожному застосуванні або відкликання об'єкта групової політики. Як наслідок, в разі, коли комп'ютер не підпадає під дію жодного об'єкта групової політики, для налаштування системи використовуються стандартні значення параметрів, визначених у відповідних ключах реєстру.

7. Сценарії

Під сценарієм (scripts) розуміється деяка зумовлена послідовність команд, здатних виконуватися в автоматичному режимі (тобто, без участі користувача). Адміністратори використовують сценарії в ситуаціях, коли необхідно багаторазово виконувати деяку послідовність дій. Використовуючи механізм групових політик, адміністратор може визначити послідовність операцій, які будуть виконуватися в момент включення або виключення комп'ютера, або при реєстрації користувача в системі або при виході з неї. Таким чином, можна виділити чотири групи сценаріїв:

- сценарії, що виконуються при ініціалізації системи (startup scripts);
- сценарії, що виконуються при реєстрації користувача в системі (logon scripts);
- сценарії, що виконуються при виключенні комп'ютера (shutdown scripts);
- сценарії, що виконуються при виході користувача з системи (logoff scripts).

Інтерпретація сценаріїв здійснюється сервером сценаріїв Windows Script Host. Цей стандартний компонент, що входить до складу Windows, дозволяє створювати сценарії, використовуючи спеціалізовані мови Visual Basic Scripting Edition, JScript.

8. Управління застосунками

Механізм групової політики може використовуватися як засіб управління процесом розгортання застосунків на Windows-клієнтах. Адміністратор може визначити перелік застосунків, які будуть доступні користувачам. Залежно від обраного режиму, в процесі застосування об'єкта групової політики на комп'ютері будуть встановлені всі необхідні застосунки. Можливі такі режими управління процесом розгортання застосунків:

- публікація застосунків;

- призначення застосунків користувачам ',
- призначення застосунків комп'ютерам.

Механізм управління процесом розгортання застосунків базується на технології Windows Installer. У складі більшості продуктів поставляються спеціальні інсталяційні пакети (installation package), які можуть бути використані для автоматичного встановлення цього застосунку.

Публікація додатків може здійснюватися виключно в конфігурації користувачів. При цьому користувачу, що підпадає під дію об'єкта групової політики, пропонується список доступних для установки додатків і користувач самостійно приймає рішення про те, чи потрібно виконувати установку додатка чи ні. Призначення додатків передбачає створення переліку додатків, обов'язкових для установки.

9. Побудова ієрархії об'єктів групової політики

Параметри, визначені в рамках об'єкта групової політики, впливають тільки на ті об'єкти каталогу, до яких вони застосовані. Щоб визначити множину об'єктів каталогу, що підпадають під дію того чи іншого об'єкта групової політики, необхідно виконати прив'язку останнього до одного або декількох контейнерів каталогу. Для будь-якого об'єкта групової політики (за винятком локальних) дозволяється прив'язка до будь-якого з трьох класів об'єктів каталогу - сайту, домену або підрозділу. Будь-які об'єкти, асоційовані з обліковими записами користувачів і комп'ютерів, розташовані всередині цих контейнерів, підпадають під дію прив'язаного об'єкта групової політики.

У ситуації, коли в рамках дерева каталогу є прив'язка декількох групової політики, цілком можлива ситуація, коли деякі об'єкти каталогу (або навіть всі) можуть підпадати під дію відразу декількох об'єктів групової політики. При цьому параметри, визначені в них, застосовуються до об'єктів каталогу відповідно до визначеного порядку:

- спочатку застосовуються об'єкти групової політики, прив'язані до сайту, в якому знаходиться об'єкт каталогу;
- після цього застосовуються об'єкти, прив'язані на рівні домену,
- останніми застосовуються об'єкти групової політики, прив'язані до підрозділів.

10. Блокування процесу спадкування параметрів об'єктів групової політики

Адміністратор може керувати процесом успадкування параметрів об'єктів групових політик. Для цього у вікні оснащення Active Directory Users and Computers необхідно відкрити вікно властивостей контейнера, до якого прив'язаний об'єкт групової політики. На вкладці Group Policy (Групова політика) необхідно встановити прапорець Block Policy inheritance (Блокувати спадкування політики). При цьому параметри групової політики, що визначені на рівні вищих контейнерів, не поширюватимуться на вміст контейнера, який налаштовується.

11. Заборона перевизначення параметрів об'єктів групової політики

Для заборони перевизначення параметрів об'єктів групової політики у вікні властивостей контейнера необхідно перейти на вкладку Group Policy і клацнути по кнопці Options (Параметри). У вікні, треба встановити прапорець No Override (Не перевизначати). При

цьому на вміст дочірнього контейнера будуть поширюватися параметри об'єкта групової політики, прив'язані до батьківських контейнерів, навіть в тому випадку, якщо аналогічні параметри перевизначені безпосередньо на рівні дочірнього контейнера. При встановленому прапорці No Override успадковані параметри мають перевагу над аналогічними параметрами об'єкту групової політики, прив'язаного до дочірнього контейнера, навіть якщо для цього контейнера встановлений прапорець Block Policy inheritance.

12. Заборона застосування параметрів об'єкта групової політики

Адміністратор може заборонити застосування параметрів будь-яких об'єктів групової політики до вмісту деякого контейнера каталогу. Для цього на вкладці Group Policy вікна властивостей контейнера необхідно клацнути по кнопці Options (Параметри) і у вікні, встановити прапорець Disabled (Відключено).

13. Обмеження дії параметрів групової політики

Хоча застосування параметрів об'єктів групової політики відбувається виключно на рівні окремих об'єктів каталогу, адміністратор може використовувати механізм належності групам для обмеження дії цих параметрів. На рівні певної групи безпеки адміністратор може заборонити (або навпаки - дозволити) застосування параметрів будь-якого об'єкта групової політики.

Для цього необхідно на вкладці Security (Безпека) вікна властивостей обраного об'єкта групової політики вказати потрібну групу безпеки і встановити прапорець Deny (Заборонити) навпроти дозволу Apply Group Policy (Застосовувати групову політику). Ця процедура називається фільтрацією групових політик (group policy filtering).

14. Надання повноважень на доступ до об'єктів групової політики

Адміністратор може делегувати деяким користувачам частину обов'язків по керванню об'єктами групової політики. Щоб надати користувачеві повноваження, необхідні для виконання прив'язки об'єкта групової політики на рівні певного контейнера, адміністратор повинен використовувати майстер Delegate of Control Wizard (Майстер делегування управління). При роботі майстра треба делегувати користувачам повноваження, необхідні для виконання завдання управління прив'язками об'єктів групової політики (прапорець Manage Group Policy links на сторінці майстра Tasks to Delegate). Крім того, зазначена категорія користувачів повинна мати дозвіл на читання об'єкта групової політики. За замовчуванням подібний дозвіл надається всім автентифікованим користувачам.

15. Визначення діючих політик

Для роботи з доменними груповими політиками в системах Windows Server є корисні утиліти командного рядка:

- GPUpdate.exe - виконайте цю команду, якщо ви змінювали групові політики і бажаєте, щоб вони негайно стали активними (спочатку запустіть її з параметром /?).

У системах Windows є зручний інструмент для роботи з груповими політиками, який особливо оцінять адміністратори великих доменів з багаторівневою ієрархією об'єктів GPO - це оснащення Resultant set of Policies (Результуюча політика).

Хід роботи:

Для виконання роботи будуть потрібні:

- віртуальна машина з Windows-Server.
- клієнтська ОС Windows.

1. Налаштуйте підключення до мережі між клієнтом і сервером та перевірте досяжність між хостами в мережі.

2. Встановити сервіс Active Directory на ваш сервер
    - Обліковий запис адміністратора домену – прізвище студента, який виконав роботу, а пароль - ім’я +прізвище з додатковою цифрою, великою буквою та спеціальним символом
    - Ім'я домену – прізвище + .com .

3. Використовуючи обліковий запис локального адміністратора, введіть клієнтську ОС в домен (Мій комп'ютер → Властивості → Ім'я комп'ютера → Змінити).

4. На контролері домену в оснащенні Active Directory Users and Computers створити обліковий запис користувача домену (і задати пароль). Дослідіть можливості налаштування облікового запису. Обмежте час входу користувача в домен і вкажіть дату закінчення дії облікового запису.

5. Делегуйте створеному користувачеві повноваження управління обліковими записами НЕ привілейованих користувачів і зміни їх властивостей.

6. На клієнтському комп'ютері дозвольте використання віддаленого підключення до робочого столу (Мій комп'ютер → Властивості → Дистанційні сеанси → Дозволити віддалений доступ до цього комп'ютера).

З сервера підключіться до робочого столу клієнта (Accessories → Communications → Remote Desktop Connections).

Примітка: Для віддаленого підключення до робочого столу в операційних системах Windows використовується протокол RDP (Remote Desktop Protocol).

7. У дереві каталогу домену Active Directory створіть контейнерний об'єкт-підрозділ (OU, Organizational Unit) і перемістіть в нього облікові записи раніше створеного вами користувача. Перемістіть в даний контейнер також обліковий запис комп'ютера клієнта.

8. Призначте створеному контейнерному об'єкту групову політику і змініть властивості даного об'єкта GPO (Properties → Group Policy → New).

Забороніть перевизначення параметрів даної групової політики (Group Policy Object Options → No Override і Block Policy Inheritance)

9. Налаштуйте групову політику даного контейнерного об'єкта (вимоги до паролю: обмеження мінімальної довжини і складності паролів),
а також:

- Привітання, яке буде виводитися при кожній реєстрації користувача;
- Профіль використання IPSec;
- Налаштування Internet Explorer (proxy-server);
- Видаліть команди Run (виконати) і Update з меню Start;

- Видаліть папки MyPictures і MyMusic з меню Start;
- Видаліть папку MyDocuments з робочого столу;
- Забороніть використання оснащень Add or Remove programs і Display в панелі управління;
- Забороніть виклик диспетчера задач і редактора реєстру;
- Забороніть виклик інтерфейсу командного рядка;
- Вкажіть список програм, заборонених для запуску.
- Видаліть пункт “Додані нещодавно” з меню;
- Видаліть історію нещодавніх документів;
- Застосуйте індивідуальний стиль меню в системі;
- Застосуйте картинку на профіль всіх користувачів за замовчуванням;
- Додайте Logoff до стартового меню;
- Забороніть Shutdown в системі;
- Видаліть “Help” з стартового меню;
- Видаліть ім’я користувача з стартового меню;
- Видаліть позначку, яка пов’язана з мережевим з’єднанням;
- Видаліть позначку, яка пов’язана з звуком;
- Видаліть позначки програм, які в таскбар (хз как перевести верно);
- Застосуйте класичний вигляд командного рядка;
- Приховайте системні диски, які є на хості;
- Видаліть меню файлів з File Explorer;

Командою ***gpupdate / force*** забезпечте негайне застосування внесених в групові політики змін.

10. Перевірте результуючу групову політику, яка буде застосована для створеного вами облікового запису в разі реєстрації на клієнтському комп'ютері, що належить створеному в п.7 підрозділу. Перевірте практично правильність зроблених налаштувань.

11. Ввімкніть Windows Remote Management (WinRM) за допомогою GPM (Group Policy Management) для адміністрування сервера віддалено.

12. За допомогою GPM (Group Policy Management) налаштуйте контроль за процесом входу (login) та виходу (logoff) користувачів у систему (через event logs).