Практична робота 9. Адміністрування домену Active Directory

Мета: Освоїти методи та засоби адміністрування доменів Active Directory.

Теоретичні відомості

Мережі Microsoft Windows підтримують дві моделі служб каталогів: робочу групу (workgroup) і домен (domain).

- Робочі групи - це вільні об'єднання комп'ютерів, в яких кожен комп'ютер управляється незалежно.

- Домени - це об'єднання комп'ютерів, колективно керованих за допомогою контролерів домену, тобто систем Windows Server 2003, що регулюють доступ до мережі, бази даних каталогу та загальних ресурсів.

Для організацій, які впроваджують Windows Server 2003, модель домену найбільш краща. Модель домену характеризується єдиним каталогом ресурсів підприємства - Active Directory, - якому довіряють всі системи безпеки, що належать домену. Тому такі системи здатні працювати з суб'єктами безпеки (обліковими записами користувачів, груп і комп'ютерів) в каталозі, щоб забезпечити захист ресурсів. Служба Active Directory, таким чином, відіграє роль ідентифікаційного сховища і повідомляє «хто є хто» в цьому домені.

Домени, дерева і ліси

Active Directory не може існувати без домену і навпаки. Домен - це основна адміністративна одиниця служби каталогів. Проте підприємство може включити в свій каталог Active Directory більше одного домену. Коли кілька моделей доменів спільно використовують безперервне простір імен DNS, вони утворюють логічні структури, звані деревами (tree). Наприклад, домени contoso.com, us.contoso.com і europe.contoso.com спільно використовують безперервне простір імен DNS і, отже, становлять дерево.

Домени Active Directory з різними кореневими доменами утворюють кілька дерев. Вони об'єднуються в найбільшу структуру Active Directory - ліс

(forest). Ліс Active Directory містить всі домени в рамках служби каталогів. Ліс може складатися з декількох доменів в декількох деревах або тільки з одного домену. Коли доменів кілька, набуває важливості компонент Active Directory, званий глобальним каталогом (global catalog): він надає інформацію про об'єкти, розташовані в інших доменах лісу.

Групова політика

Організаційні підрозділи (ОП) також використовуються для об'єднання однаково налаштованих об'єктів - комп'ютерів і користувачів. Групова політика Active Directory дозволяє централізовано керувати практично будь-якими конфігураційними змінами системи. З її допомогою можна вказати настройки безпеки, розгорнути ПО і налаштувати поведінку ОС і додатків, навіть не торкаючись до комп'ютерів користувачів. Ви просто реалізуєте свою конфігурацію в рамках одного об'єкта групової політики (ОГП).

ОГП складаються з сотень можливих конфігураційних параметрів: від прав і привілеїв користувача до ПЗ, яке дозволено запускати на системі. ОГП підключається до контейнера всередині Active Directory (зазвичай до ОП, але може і до доменів або навіть сайтам), і після цього його налаштування поширюються на всіх користувачів і комп'ютери усередині цього контейнера.

Будь сервер може підтримувати одну або більше наступних ролей.

- Контролер домену (Domain controller) - сервер, на якому працюють служби каталогів і розташовується сховище даних каталогу. Контролери домену також відповідають за вхід в мережу і пошук в каталозі. При виборі цієї ролі на сервері будуть встановлені DNS і Active Directory. Поштовий сервер (POPS, SMTP) [Mail server (POP3, SMTP)] - сервер, на якому працюють основні поштові служби POP3 (Post Office Protocol 3) і SMTP (Simple Mail Transfer Protocol), завдяки чому поштові POP3-клієнти домену можуть відправляти і отримувати електронну пошту. Вибравши цю роль, ви визначаєте домен за замовчуванням для обміну поштою і створюєте поштові скриньки. Ці служби зручні в невеликих компаніях або при віддаленому з'єднанні, коли електронна пошта необхідна, але цілком може обійтися без функціональності Microsoft Exchange Server.

- Сервер друку (Print, server) - сервер, організуючий доступ до мережевих принтерів і керуючий чергами друку і драйверами принтерів. Вибір цієї ролі дозволить вам швидко налаштувати параметри принтерів і драйверів.

- Сервер потоків мультимедіа (Streaming media server) - сервер, що надає мультимедійні потоки іншим системам мережі або Інтернету. Вибір цієї ролі приводить до установки служб Windows Media. Ця роль підтримується тільки у версіях Standard Edition і Enterprise Edition.

- Сервер додатків (Application server) - сервер, на якому виконуються Web-служби XML, Web-додатки та розподілені додатки. При призначенні сервера цій ролі на ньому автоматично встановлюються IIS, COM + і Microsoft. NET Framework. При бажанні ви можете додати до них серверні розширення Microsoft FrontPage, а також включити або виключити ASP.NET.

- Сервер терміналів (Terminal Server) - сервер, що виконує завдання для клієнтських комп'ютерів, які працюють в режимі термінальної служби. Вибір цієї ролі приводить до установки Terminal Server. Для віддаленого управління сервером встановлювати Terminal Server не потрібно. Необхідний для цього віддалений робочий стіл (Remote Desktop) встановлюється автоматично разом з ОС.

- Сервер віддаленого доступу або VPN-сервер (Remote access / VPN server) - сервер, що здійснює маршрутизацію мережевого трафіку і керуючий телефонними з'єднаннями і з'єднаннями через віртуальні приватні мережі (virtual private network, VPN). Вибравши цю роль, ви запустите Майстер настройки сервера маршрутизації та віддаленого доступу (Routing and Remote Access Server Setup Wizard). За допомогою параметрів маршрутизації та віддаленого доступу ви можете дозволити лише вихідні підключення, вхідні і витікаючі з'єднання або повністю заборонити доступ ззовні.

- Вузол кластера серверів (Server cluster node) - сервер, який діє у складі групи серверів, об'єднаних у кластер. Вибір цієї ролі призводить до запуску Майстра створення кластера (New Server Cluster Wizard), що дозволяє створити нову кластерну групу, або Майстра додавання вузлів (Add Nodes Wizard), який

допоможе додати сервер до існуючого кластеру. Ця роль підтримується тільки у версіях Enterprise Edition і Datacenter Edition.

- Файл-сервер (File server) - сервер, що надає доступ до файлів і керуючий ним. Вибір цієї ролі дозволить вам швидко налаштувати параметри квотування та індексування. Ви також можете встановити Web-прикладений і для адміністрування файлів. У цьому випадку буде встановлений IIS і включені сторінки ASP (Active Server Pages).

- DHCP-сервер (DHCP Server) - сервер, на якому запущений DHCP (Dynamic Hose Configuration Protocol), що дозволяє автоматизувати призначення IP-адрес клієнтам мережі. При виборі цієї ролі на сервері буде встановлений DHCP і запущений Майстер створення області (New Scope Wizard).

- DNS-сервер (DNS Server) - сервер, на якому запущена служба DNS, роздільна імена комп'ютерів в IP-адреси і навпаки. При виборі цієї ролі на сервері буде встановлена DNS і запущений Майстер налаштування DNS-сервера (Configure DNS Server Wizard).

- WINS-сервер (WINS server) - сервер, на якому запущена служба WINS (Windows Internet Name Service), роздільна імена NetBIOS у IP-адреси і навпаки. Вибір цієї ролі призводить до установкеWINS.

Управління обраними ролями сервера здійснюється за допомогою програми Керування даним сервером (Manage Your Server), у вікні якої зосереджені всі основні інструменти для управління Windows Server 2003. Зокрема, тут перераховані поточні ролі сервера (рис.1). Щоб відкрити це вікно, скористайтеся меню Адміністрування (Administrative Tools).

Хід роботи

1. У середовищі програмного емулятора створити проект комп’ютерної мережі.

2. Провести встановлення операційної системи ОС Windows 2003 ServerEnterpriseEdition/ОС Microsoft Windows Server 2019 Datacenter.

3. Розробити схему адресації пристроїв мережі. Для цього скористатися даними табл. 3.1. Під час розрахунку враховувати, що комутатору та інтерфейсу маршрутизатора мережі також виділяється по одній IP-адресі. Результати навести у вигляді таблиці.

Таблиця 3.1 – Параметри для розрахунку

№ варіанта	IP-адреса мережі	Префікс мережі	№ варіанта	IP-адреса мережі	Префікс мережі
1	191.G.N.0	/24	16	206.G.N.0	/24
2	192.G.N.0	/25	17	207.G.N.0	/25
3	193.G.N.0	/26	18	208.G.N.0	/26
4	194.G.N.0	/27	19	209.G.N.0	/27
5	195.G.N.0	/28	20	210.G.N.0	/28
6	196.G.N.0	/24	21	211.G.N.0	/24
7	197.G.N.0	/25	22	212.G.N.0	/25
8	198.G.N.0	/26	23	213.G.N.0	/26
9	199.G.N.0	/27	24	214.G.N.0	/27
10	200.G.N.0	/28	25	215.G.N.0	/28
11	201.G.N.0	/24	26	216.G.N.0	/24
12	202.G.N.0	/25	27	217.G.N.0	/25
13	203.G.N.0	/26	28	218.G.N.0	/26
14	204.G.N.0	/27	29	219.G.N.0	/27
15	205.G.N.0	/28	30	220.G.N.0	/28

4. Перевірити можливість інформаційного обміну між робочими станціями мережі. У разі виявлення проблем зв’язку знайти та усунути їх причини.

5. На сервері Serv_G_N_1 провести встановлення Active Directory, а сервер Serv_G_N_2 додати у домен та надати йому роль додатковий контролеру домену.

6. Додати в домен робочі станції(станцію).

7. На сервері Serv_G_N_1 в Active Directory створити групу користувачів GR_G_N. В цій групі створити нового користувача та, використовуючи цей обліковий запис, здійснити вхід у систему з робочої станції.