Тема 2

Створення структури домену в Active Directory

План

1. Гарні практики створення структури домену
2. Облікові записи користувачів у домені
3. Групи в домені

1. Гарні практики створення структури домену

Основна теза:

Структура домену безпосередньо впливає на групові політики (тобто на те, як саме будуть потім здійснюватися налаштування - і чи буде зручно це робити).
Тому структуру OU варто побудувати з урахуванням гарних практик.

У цьому пункті нас зокрема цікавить:

- як побудувати **ієрархію організаційних одиниць (OU)** (тобто як взаємно розташувати комп’ютери, облікові записи користувачів, групи в логічній структурі)
- як реалізувати іменування (**простори імен**)

1. Гарні практики створення структури домену

Простори імен (*namespaces*)

Гарні практики:

- Не використовувати для домену верхнього рівня загальні імена на зразок *.local*
- Якщо організація використовує публічну DNS-адресу, то не бажано використовувати точно таке саме ім’я для домену AD верхнього рівня.
  Це можливо, але у такому разі доведеться налаштовувати DNS із розділеним горизонтом (split-horizon DNS).
- Натомість, рекомендованими є два наступні способи:

  1) Використати для домену AD верхнього рівня ***неактивний піддомен публічного домену*** вашої організації

     Наприклад: internal.company.com (*company.com* - публічний домен)

     Плюси: зручність управління, забезпечення унікальності імені.

     Мінуси: дещо довші імена у домені AD :)

  2) Виділити під домен AD верхнього рівня ***окремий домен з унікальним ім’ям***

     Наприклад: company.net (тимчасом як company.com - публічне ім’я)

     Плюси: окреме унікальне ім’я для домену AD

     Мінуси: знадобиться два окремих доменних імені

1. Гарні практики створення структури домену

Ще про іменування

Правила іменування доменів, комп’ютерів, сайтів, OU в Active Directory (офіц.): https://docs.microsoft.com/uk-UA/troubleshoot/windows-server/identity/naming-conventions-for-computer-domain-site-ou

1. Гарні практики створення структури домену

Організаційні одиниці (*Organization Units, OUs*)

Гарні практики:

- Використовувати єдиний підхід до іменування OU у межах домену
- Не лишати користувачів і комп’ютери поза OU (у контейнері за замовчуванням)
- Документувати нові OU (заповнювати поле опису об’єктів)
- Захищати OU від випадкового видалення
- Розглянути можливість створення окремої OU для серверів
- Використовувати вкладені групи замість того, щоб додавати того самого користувача чи комп’ютер у кілька груп
- Відокремити облікові записи адміністраторів від решти облікових записів
- Не додавати користувачів до адміністративних груп без потреби

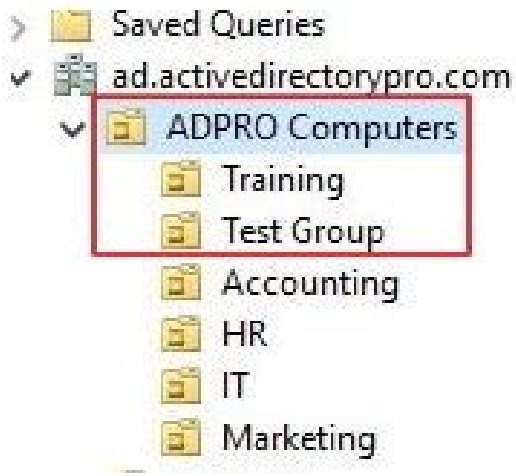
1. Гарні практики створення структури домену

- Розділяти OU для користувачів і OU для комп’ютерів:



- Створювати окремі OU для структурних підрозділів та напрямів діяльності:





1. Гарні практики створення структури домену

Організаційні одиниці (*Organization Units, OUs*)

Гарні практики (продовження):

- Розглянути можливість створення окремої OU для виділених робочих станцій адміністратора (administrators dedicated workstations) без доступу до Інтернету https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-accounts#create-dedicated-workstation-hosts-without-internet-and-email-access
- Обмежити можливість адміністраторів входити в систему на серверах і робочих станціях (але тоді в адміністраторів обов’язково має бути або локальний доступ до контролера домену, або налаштована виділена робоча станція.

2. Облікові записи користувачів у домені

Деякі стандартні локальні облікові записи в AD

- **Administrator** (S-1-5-<domain>-500)

Вбудований. Не може бути видалений чи заблокований. Але може бути перейменований чи відключений. Має повний доступ до ресурсів (локально).

- **Guest** (S-1-5-<domain>-501)

Вбудований. Не бажано лишати ввімкненим (погано для безпеки). Якщо необхідно - не дозволяти нічого зайвого.

- **HelpAssistant** (спеціальний обліковий запис для віддаленої допомоги)

Деякі сервісні локальні облікові записи в AD (під ними не входять користувачі)

- **Local System** (має такі ж привілеї, як в адміністратора)
- **Local Service** (має такі ж привілеї, як у стандартного користувача**)**
- **Network Service** (те саме, що й Local Service + робота у мережі від імені цього комп’ютера)

3. Групи в домені

Деякі стандартні групи

- **Account Operators** - користувачі цієї групи можуть керувати обліковими записами користувачів та групами
- **Administrators** - вбудована група адміністраторів
- **Backup Operators** - члени цієї групи можуть обходити обмеження для виконання резервного копіювання та відновлення
- **Cryptographic Operators** - члени цієї групи можуть виконувати криптографічні операції
- **DNSAdmins** - група адміністраторів DNS
- **Domain Admins** - члени цієї групи можуть адмініструвати домен; вони автоматично належать до локальної групи Administrators на кожному комп’ютері домену; за замовчуванням володіють всіма об’єктами в Active Directory
- **Domain Computers** - до цієї групи належать всі комп’ютери даного домену
- **Domain Controllers** - всі контролери даного домену
- **Domain Guests** - до цієї групи належить вбудована обліковка гостя (Guest)
- **Domain Users** - містить обліковки всіх користувачів у домені

3. Групи в домені

Деякі стандартні групи (продовження)

- **Enterprise Admins** - група наявна лише в кореневому домені лісу; мають право вносити зміни на рівні лісу
- **Event Log Readers** - можуть переглядати вміст журналів подій
- **Group Policy Creator Owners** - члени цієї групи можуть створювати і змінювати об’єкти групової політики
- **Hyper-V Administrators** - адміністратори Hyper-V на локальному комп’ютері
- **Network Configuration Operators** - члени цієї групи можуть змінювати налаштування мережі
- **Print Operators** - члени цієї групи можуть адмініструвати принтери на контролері домену
- **Read-Only Domain Controllers** - контролери домену, налаштування яких захищені від запису
- **Replicator** - група для реплікації на рівні домену
- **Server Operators** - члени групи можуть адмініструвати сервери, які належать до даного домену
- **Users** - вбудована група звичайних користувачів

3. Групи в домені

Групи можна організувати залежно від:

- спільно виконуваних завдань (напр., група, яка разом працює над певним проєктом)
- ресурсу, до якого вони можуть мати доступ (наприклад, користувачі, які можуть робити SQL-запити до бази даних)