Лекція 1

Знайомство з Active Directory

План

1. Робочі групи і домени у Windows-мережах
2. Основні поняття Active Directory
3. Дерева і ліси в Active Directory
4. Відношення довіри

1. Робочі групи і домени у Windows-мережах

Комп’ютерні мережі з кінцевими вузлами під управлінням ОС Windows (повторення)

- **Робоча група Windows** (Windows Workgroup)

  Одноранговa організація мережі.
  Для невеликих мереж з простою структурою.
  Складається з одноранговиx вузлів + можуть бути окремі сервери, клієнти.

  \+ Простота реалізації та адміністрування (якщо завдання нескладні).
  – Відсутність централізованого управління; неможливість масштабування; невисокий рівень безпеки; невисока швидкодія.

- **Домен Windows** (Windows Domain)

  Клієнт-серверна організація мережі.
  Для більших мереж зі складнішою структурою.
  Складається з серверів, клієнтів та інших об’єктів.
  База, на основі якої здійснюється допуск всередині домену, зберігається на окремому сервері - контролері домену.
  Можуть також бути резервні контролери домену.

  \+ Вища керованість і захищеність мережі.
  – Складніші у реалізації та адмініструванні.

1. Робочі групи і домени у Windows-мережах

Облікові записи користувачів та групи у Windows можуть бути організовані:

- **На локальному рівні** (Security Account Manager, SAM; оснащення Локальні користувачі та групи)

  Користувач повинен мати окремий обліковий запис на кожному комп’ютері, за яким він працює.

  На кожному комп’ютері обліковий запис користувача налаштовується окремо.

- **На мережному рівні** (Active Directory)

  Всі облікові записи зберігаються у базі даних на контролері домену.

  Користувач має єдиний обліковий запис у домені.

Автентифікація та авторизація (повторення)

? Чим відрізняються автентифікація та авторизація?

Автентифікація (authentication): кожна дія виконується певним суб'єктом, ідентичність якого встановлено системою.

Авторизація (authorization): система регулює, які дії дозволені тим чи іншим суб'єктам.

2. Основні поняття Active Directory

Active **Directory**

Як це правильно читається:

британська англійська: dai·rEk·tuh·ree
американська англійська: dr·Ek·tr·ee

Active Directory (***AD***, дослівно: активний каталог) - служба каталогів для Windows-мереж, організованих як домен.

AD займається:

- автентифікацією та авторизацією користувачів і комп’ютерів,
- призначенням та застосуванням групових політик,
- встановленням ПЗ та оновлень до нього тощо.

AD використовує протоколи: LDAP (Lightweight Directory Access Protocol), Kerberos, DNS, RPC, а також низку інших протоколів для реалізації окремих функцій.

2. Основні поняття Active Directory

Домен (*domain*) - група комп'ютерів, які спільно використовують базу даних каталогу. У межах домену встановлюються спільні правила безпеки.

Домен може охоплювати всю мережу організацію, або у мережі організації може бути кілька доменів.

Контролер домену (*domain controller*) - комп'ютер мережі, спеціально виділений для реалізації єдиної політики безпеки в домені.

Тобто домен Windows і домен у мережі Інтернет - це не одне і те саме (хоча структура і справді схожа).

Саме на контролері домену працює доменна служба Active Directory (*Active Directory Domain Service*, *AD DS*).

Об'єкти Active Directory:

- **ресурси** (принтери, томи тощо)
- **учасники безпеки** (англ. *principals*; облікові записи користувачів та групи користувачів)

? Як називається ідентифікатор, що присвоюється учаснику безпеки?

SID (Securuty Identifier)

2. Основні поняття Active Directory

Всередині домену використовується деякий **простір імен** (*namespace*).

Простори імен у різних доменах можуть частково співпадати (тоді це вкладені простори імена). Але переважно різні домени мають різні простори імен.

Домен складається з **організаційних одиниць** (*Organizational Units*, *OU*) різних рівнів.

Структура організаційних одиниць відображає структуру організації (бізнес-структуру або функціональну структуру). OU бувають вкладеними.

До складу OU можуть входити:

- комп'ютери
- облікові записи користувачів
- групи користувачів

2. Основні поняття Active Directory

Початково служба AD встановлюється на одному із серверів домену. Цей сервер називається **основним контролером домену** (PDC, Primary Domain Controller).

Також задля більшої надійності та вищої продуктивності в домені налаштовують **резервні контролери домену** (BDC, Backup Domain Controller).

Якщо в домені є ще й інші сервери, то вони виконують роль ***відокремлених серверів*** (Standalone Servers).

Реплікація (*replication*) - процес синхронізації всіх копій бази даних домену між контролерами цього домену.

Групові політики (Group policies)

Згідно з рекомендаціями Microsoft, групові політики застосовуються до передусім об'єктів OU (для цього OU й потрібні). Завдяки груповим політикам, можна виконувати автоматичне встановлення ПЗ на задані комп'ютери, налаштовувати це ПЗ, керувати дозволами і заборонами на запуск програм, змінювати налаштування безпеки відповідного сегменту мережі тощо.

2. Основні поняття Active Directory

Також до складу Active Directory входять:

Схема (*schema*) - набір правил, які визначають класи об’єктів та атрибути у даному каталозі, а також формат імен екземплярів класу та обмеження, які накладаються на ці екземпляри.

Глобальний каталог (global catalog) містить інформацію про всі об’єкти в каталозі незалежно від домену.

Механізм запитів та індексування об’єктів для пошуку цих об’єктів та відомостей про них.

Сервіс реплікації (*replication service*) для передавання даних каталогу по мережі між контролерами домену.

Передається інформація про будь-які зміни.
У результаті всі контролери домену повинні містити точну копію інформації про всі каталоги домену.

2. Основні поняття Active Directory

Сервіси Active Directory:

Active Directory Domain Services (AD DS)

Основний та найвідоміший сервіс AD. Решта сервісів спираються на цей.

Зберігає відомості про пристрої і користувачів домену. Керує контолем доступу.

AD DS працює на контролері домену.

Залучається, коли користувач входить у систему чи намагається одержати доступ до іншого пристрою по мережі.

Lightweight Directory Services (AD LDS)

Це реалізація протоколу LDAP для AD DS.

Active Directory Certificate Services (AD CS)

Організовує локальну інфраструктуру публічних ключів (для внутрішніх потреб організації). Ключі можуть використовуватися для шифрування мережного трафіку (VPN, RDS, TLS), електронної пошти, файлів (файлова система EFS).

2. Основні поняття Active Directory

Сервіси Active Directory (продовження):

Active Directory Federation Services (AD FS)

Сервіс єдиного входу (single sign-on service).
Поширює ідею AD DS на зовнішні мережі.
Користувач може працювати з кількома мережними ресурсами чи вебсервісами на основі єдиних реквізитів.
Ці реквізити зберігаються централізовано.

Active Directory Rights Management Services (AD RMS)

Сервіс керування правами та інформацією.
Обмежує доступ користувачів до документів (Word, електронні листи, вебсторінки тощо).
Також шифрує ці документи.

3. Дерева і ліси в Active Directory

Дерево (*tree*) - один чи більше доменів,

які використовують спільний простір імен

та між якими встановлено *відношення довіри* (*trust relationships*).

Ліс *(forest)* - одне чи більше дерев, між якими здійснюється *обмін спільною інформацією каталогу*.

Ліс в AD є **найвищим організаційним рівнем**. У межах лісу використовується єдина база даних.

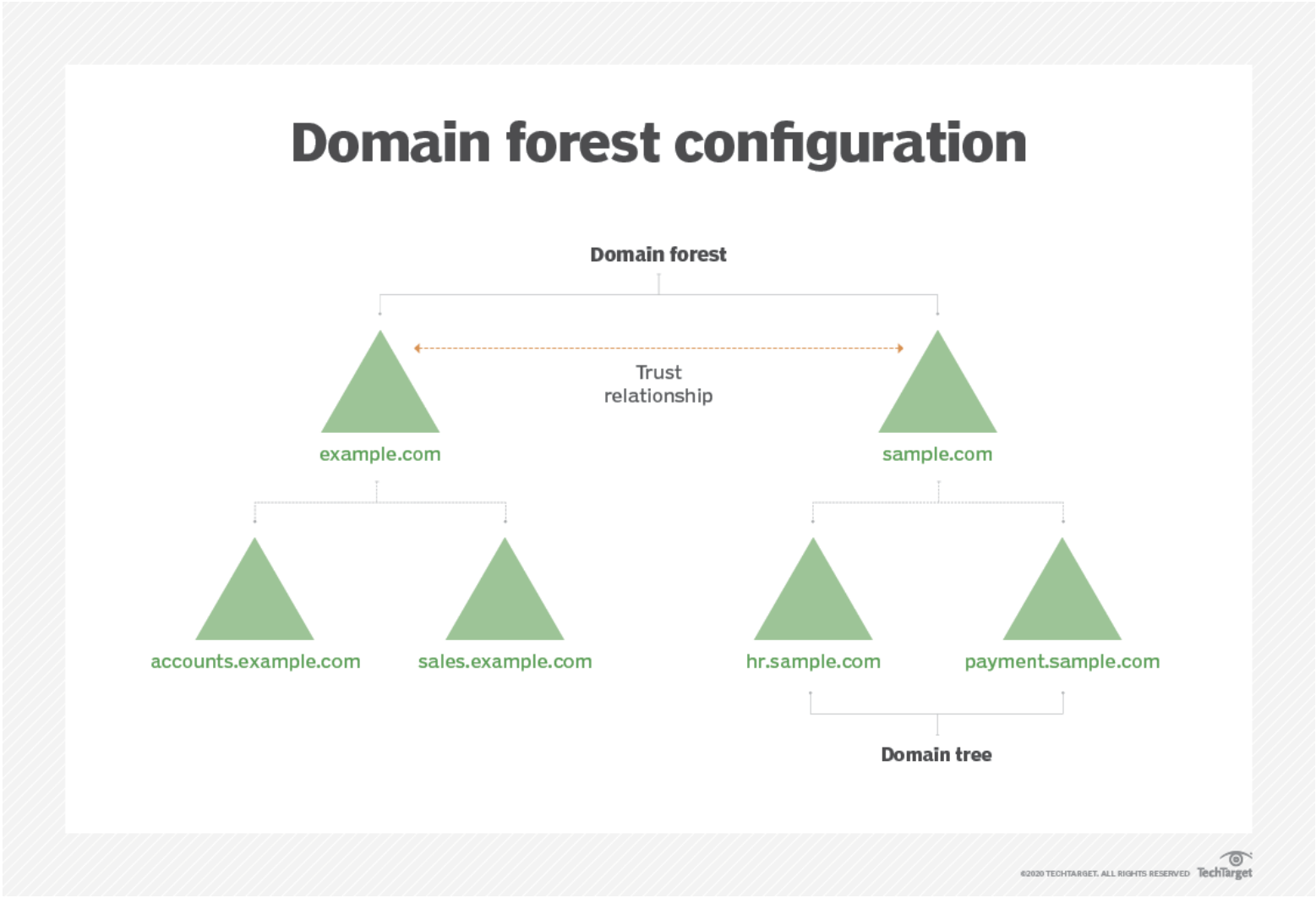
Ліс є **кордоном безпеки** (security boundary).

Тобто доступ до ресурсів лісу ззовні за замовчуванням відсутній і встановлюється лише тоді, коли у цьому є нагальна потреба.

Сайти (*sites*) вважаються компонентами фізичної структури Active Directory (на противагу доменам, деревам, лісу, організаційним підрозділам тощо).

Найчастіше сайт містить підмережу локальної мережі (або високошвидкісної глобальної мережі).

Тобто з’єднання в межах сайту має бути швидким і надійним.



Домени *example.com* і *sample.com* - **рівноправні**.
Домен *accounts.example.com* є **дочірнім** для домену *example.com* (використовує той самий простір імен).

Джерело схеми: https://searchwindowsserver.techtarget.com/definition/Active-Directory-forest-AD-forest

3. Дерева і ліси в Active Directory

Моделі розробки лісу

- Організаційна модель лісу (*organizational forest model*)
- Модель лісу для поділу ресурсів (*resource forest model*)
- Модель лісу для обмеження доступу (*restricted access forest model*)

Теза, на яку спираємося далі:

Ліс є кордоном безпеки.

Ліс ізолює дані та сервіси від будь-кого, хто є ззовні цього лісу.

Доступ зсередини одного лісу до іншого лісу за замовчуванням відсутній. Якщо треба організувати такий доступ, необхідно встановлювати відношення довіри рівня лісу.

Але іноді такий доступ організовувати не треба.

3. Дерева і ліси в Active Directory

Організаційна модель лісу (*organizational forest model*)

Найпростіша модель лісу.

Якщо організація невелика, такий ліс вміщує всі ресурси організації.

У більшій організації для кожного підрозділу може створюватися й окремий ліс.

Якщо різні підрозділу мають спільно використовувати ресурси, то між лісами встановлюються спеціальні *відношення довіри (trust relations) рівня лісу*.

Перевага: простота.

Модель лісу з поділом ресурсів (*resource forest model*)

Створюються окремі ліси для ресурсів (для кожного відділу, проєкту, підрозділу тощо) й окремий ліс - для облікових записів користувачів.

Ліс для облікових записів користувачів будується за організаційною моделлю. У ліс для ресурсів облікові записи не додаються (окрім тих, які потрібні для адміністрування цих ресурсів).

Перевага: добре ізолює проблеми з ресурсами (сервісами, даними) у межах відповідного лісу.

3. Дерева і ліси в Active Directory

Модель лісу з обмеженим доступом (*restricted access forest model*)

Модель з обмеженим доступом, як і організаційна модель для середніх і великих організацій, передбачає створення окремого лісу для кожного підрозділу. Але, на відміну від неї, організаційна модель лісу з обмеженим доступом не має відношень довіри між різними лісами.

Перевага: підходить для середовищ з підвищеними вимогами до безпеки.

За потреби ці підходи можуть поєднуватися.

Недоліки моделей з кількома лісами:

- складність
- висока вартість (додаткові сервери, додатковий персонал - рекомендовано)

У менших організаціях часто використовують моделі з одним лісом.

3. Дерева і ліси в Active Directory

Найкращі практики налаштування лісів в Active Directory

- Все, що може бути об'єднане в один ліс, має бути об'єднане в один ліс
- Ресурси і дані мають бути захищені через групові політики на основі *принципу мінімальних повноважень*
- Необхідно обмежити право користувачів на створення нових папок
- Якщо створюється ліс за моделлю з обмеженим доступом, то доступ справді має бути суворо обмеженим

4. Відношення довіри

Відношення довіри (*trust relations*, *trusts*) надають користувачам з одного домену доступ до ресурсів, розміщених в іншому домені.

Односторонні відношення довіри (One-way trust)

Перший домен дозволяє користувачам другого домену доступ до своїх ресурсів, а другий домен не дозволяє такого доступу користувачам першого домену.

Двосторонні відносини довіри (Two-way trust)

Перший і другий домен дозволяють доступ до своїх ресурсів користувачам одне одного.

Довірчий домен (Trusted domain)

Це домен, якому довіряє інший домен.

Транзитивне відношення довіри (Transitive trust)

Відношення довіри може поширюватися на інші довірчі домени всередині лісу.

Нетранзитивне відношення довіри (Intransitive trust)

Одностороннє віношення довіри, яке не поширюється на інші домени.

4. Відношення довіри

Відношення довіри (*trust relations*, *trusts*) надають користувачам з одного домену доступ до ресурсів, розміщених в іншому домені.

Розширене відношення довіри (Explicit trust)

Відношення довіри, створене адміністратором. Воно нетранзитивне і одностороннє.

Відношення довіри всередині лісу (Forest trust)

Застосовується до всього лісу. Транзитивне. Може бути одно- чи двостороннім.

Існують й інші відношення довіри.