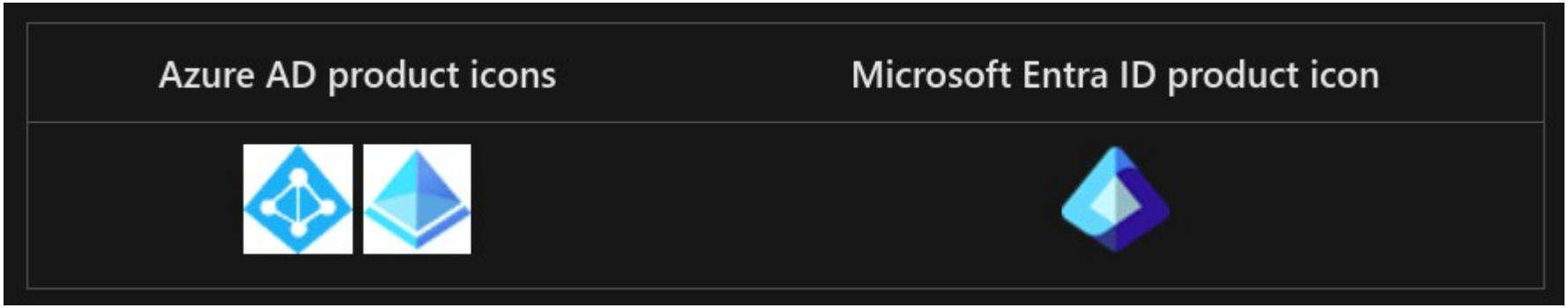
*Лекція 12*

# Огляд Microsoft Entra ID

Ребрендинг (липень 2023 року):

Microsoft Azure Active Directory ⇢ **Microsoft Entra ID**




Детальніше про зміни:
https://learn.microsoft.com/uk-ua/entra/fundamentals/new-name

# План

1. Ключові поняття MS Enra ID.
2. Основні можливості MS Enra ID.

# 1. Ключові поняття MS Enra ID

**?** AD все, тепер лише хмара?

Ні. AD — локально, Entra ID (Azure AD) — у хмарі, а також гібридні варіанти (є інтеграція).

**?** Що добре з хмарами? / Що не так із хмарами?

**Що добре:**

+ на потрібно обслуговувати обладнання

+ можна платити лише за використаний обсяг ресурсів

+ (потенційно) безпека

**Що не так:**

- залежність від умов постачальника

- менша гнучкість щодо деталей реалізації

- (якщо особливі вимоги) безпека

У різних випадках — різні пріоритети й різні потреби. Тому ці переваги та недоліки умовні.

# 1. Ключові поняття MS Entra ID

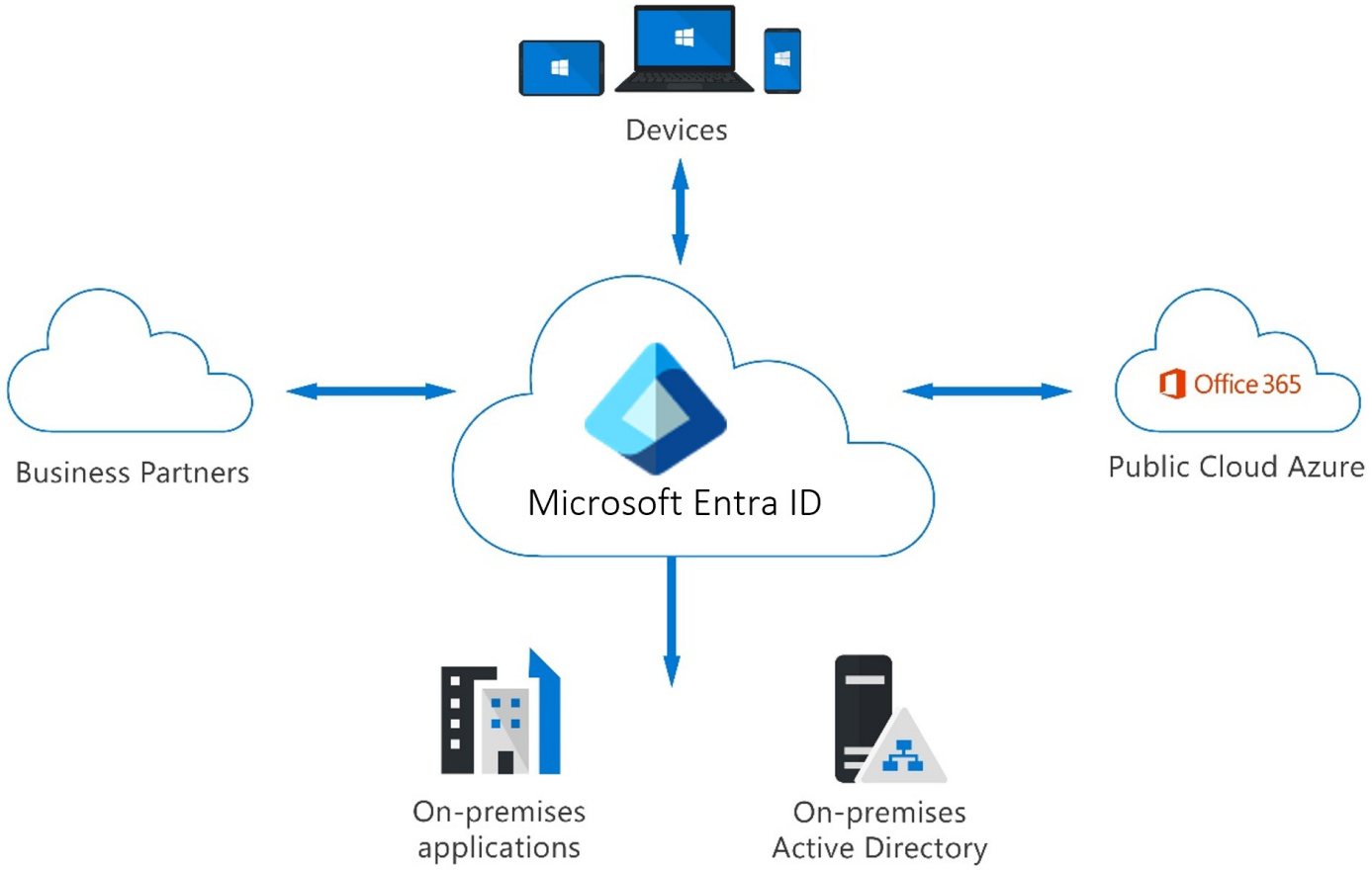
MS Entra ID (раніше — Azure Active Directory) — хмарний сервіс керування ідентичностями та доступом до ресурсів.

Приклади ресурсів, доступ до яких може бути організовано через MS Entra ID:

- застосунки в корпоративній мережі;
- власні хмарні застосунки;
- Microsoft Office 365;
- хмарна платформа MS Azure;
- сторонні SaaS-застосунки тощо.

**А як бути з локальною інфраструктурою на базі Active Directory?**
*Є інтеграція. Дані можна синхронізувати. Або повністю мігрувати в хмару (хмари), якщо потрібно.*

# 1. Ключові поняття MS Entra ID




Джерело картинки: https://learn.microsoft.com/en-us/training/modules/explore-basic-services-identity-types/2-describe-azure-active-directory

# 1. Ключові поняття MS Entra ID

**Ідентифікація / автентифікація**

☺ **Ідентифікація** (identification) — вирізнення певного суб’єкта з-поміж інших суб’єктів, зазвичай за допомогою логіну.

Суб’єктом найчастіше є користувач, але це може бути процес, пристрій тощо.

Мета ідентифікації — пов’язати з суб’єктом певну ***ідентичність (identity)***.

Одне з гасел прибічників технології ідентичностей:

*Identity is a new security perimeter*

☑ **Автентифікація** (authentication) — процедура підтвердження ідентичності суб’єкта (через пароль чи в інший спосіб).

Автентифікація може здійснюватися локально або через мережу.

У разі мережної автентифікації може використовуватися:

- власний сервер автентифікації (зокрема й контролер локальної AD);
- послуги зовнішніх провайдерів ідентичностей (зокрема хмарних).

# 1. Ключові поняття MS Entra ID

**Провайдери ідентичностей**

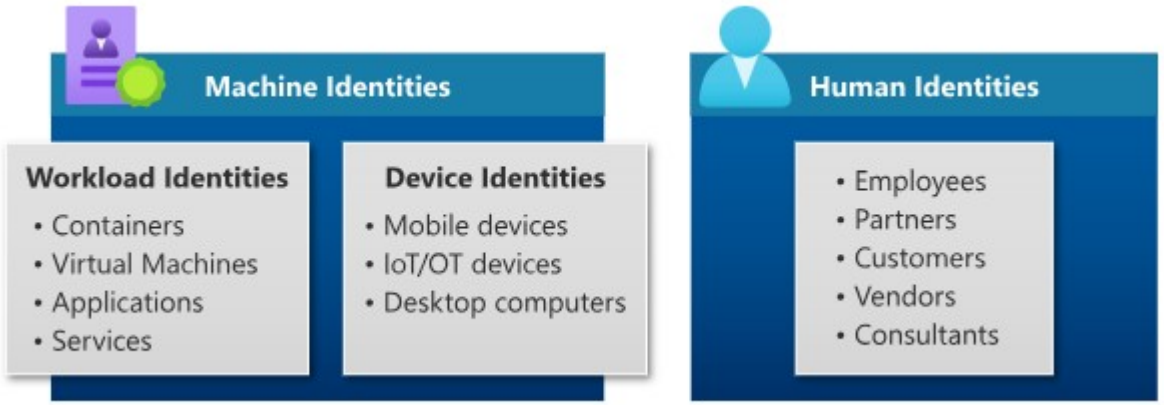
**Провайдер ідентичностей** (постачальник ідентичностей, identity provider) — система, яка здійснює автентифікацію ідентичностей суб’єктів для авторизації їхнього доступу до різноманітних застосунків та сервісів.

Для можливості здійснювати автентифікацію суб’єктів провайдер ідентичності повинен мати їхні **реквізити входу** (credentials).

Приклади провайдерів ідентичностей: MS Entra ID, Octa, Google, Facebook.

Провайдери ідентичностей активно використовуються у **сервісах єдиного входу** (SSO, Single Sign-On).

**Приклади суб’єктів, які можуть мати ідентичності в Entra ID:**



# 1. Ключові поняття MS Enra ID

## Базові терміни Entra ID

**Тенант**, або **обліковий запис організації** (**tenant**) — конкретний екземпляр Microsoft Entra ID, що зберігає дані певної організації (користувачі, групи, пристрої, реєстрація застосунків), а також відповідні політики доступу та сумісності.

Тенант має власні доменне ім’я (наприклад, *contoso.onmicrosoft.com*) та ідентифікатор (Tenant ID).

Тенант є адміністративним кордоном і кордоном безпеки.

**?** Щось нагадує? ;)

*Дещо схоже на ліс (бо ліс — кордон безпеки для локальної AD).*

*Але: тенант не тотожний лісу! Є багато варіантів того, як ліси у локальній AD може співвідноситися з тенантами в Entra ID. Більше — тут:* https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/plan-connect-topologies

*Продовження ↪*

# 1. Ключові поняття MS Enra ID

**Базові терміни Entra ID (продовження)**

**Каталог (directory)** — логічний контейнер всередині тенанту, який містить ресурси та об’єкти, пов’язані з керуванням ідентичностями та доступом (користувачі, групи, пристрої, застосунки та інші об’єкти).

У MS Entra ID терміни «каталог» і «тенант» часто вживаються як синоніми. Бо **тенант містить лише один каталог** (не зовсім ліс!)

**Мультитенант (multi-tenant)** — кілька тенантів, які належать одній організації.

*Але: мультитенант також не тотожний лісу!*

# 1. Ключові поняття MS Enra ID

**Zero Trust**

Zero Trust Security Model — модель з нульовою довірою, архітектура з нульовою довірою.

**За означенням NIST:**

**Архітектура з нульовою довірою (zero trust architecture, ZTA)** — це кібербезпекова архітектура рівня організації, яка базується на принципах нульової довіри і розроблена для попередження витоків даних та обмеження можливості зловмисників переміщуватися всередині мережі.

Джерело: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

# 1. Ключові поняття MS Enra ID

**Основні положення Zero Trust**

- **Перевіряти все.** Сприймати будь-яку мережу, як недовірену, навіть коли її захищено фаєрволом.
- **Принцип мінімальних повноважень.** Кожній програмі чи користувачу у системі має бути надано мінімальний набір повноважень, необхідний для виконання поставлених перед ними завдань.
- Інша назва принципу мінімальних повноважень — **JEA (Just Enough Access)**
- **Припускати наявність порушення.** Застосовувати шифрування (і під час передавання даних, і під час їх зберігання), використовувати сегментування користувачів, пристроїв, мереж та застосунків, виявляти загрози та вдосконалювати безпекові налаштування.

# 1. Ключові поняття MS Entra ID

## Шість принципів моделі нульової довіри

**1) Дані.** Захищати дані важливо і всередині інфраструктури, і за її межами.

**2) Застосунки.** Доступ до застосунків має бути керований та контрольований. Відстежувати діяльність застосунків.

**3) Мережі.** Використовувати сегментування та мікросегментування мережі, шифрувати дані в мережі, здійснювати моніторинг мережі, виявляти загрози.

**4) Інфраструктура.** Підтримувати безпеку інфраструктури. Вчасно оновлювати інфраструктуру. Застосовувати додаткові механізми (наприклад, JIT / Just-in-time access — обмежений у часі привілейований доступ).

Гарна практика: JIT + JEA

**5) Ідентичності.** Ідентичність може мати користувач, служба, пристрій. Якщо суб'єкт, який володіє ідентичністю, претендує не деякий ресурс, він має підлягати надійній автентифікації.

**6) Пристрої.** Необхідно здійснювати моніторинг загального стану пристроїв та їхньої відповідності політикам безпеки.

# 1. Ключові поняття MS Entra ID

**MFA / Multi-Factor Authentication**

MFA / Multi-Factor Authentication — мультифакторна автентифікація, багатофакторна автентифікація

Використовує додаткові фактори під час автентифікації.

Наприклад, логін + пароль + операція на власному телефоні користувача (застосунок, повідомлення з кодом, дзвінок тощо).

2FA / Two-Factor Authentication — двофакторна автентифікація.

Мультифакторна автентифікація **належить до сучасних рекомендацій** з безпеки, оскільки знижує ймовірність, що зловмиснику вдасться заволодіти одразу всіма факторами.

MFA в Microsoft Server: з 2019 року локально не пропонується, лише в хмарі (зокрема в Azure Active Directory / MS Entra ID).

# 2. Основні можливості MS Entra ID

## Основні сервісні плани MS Entra ID

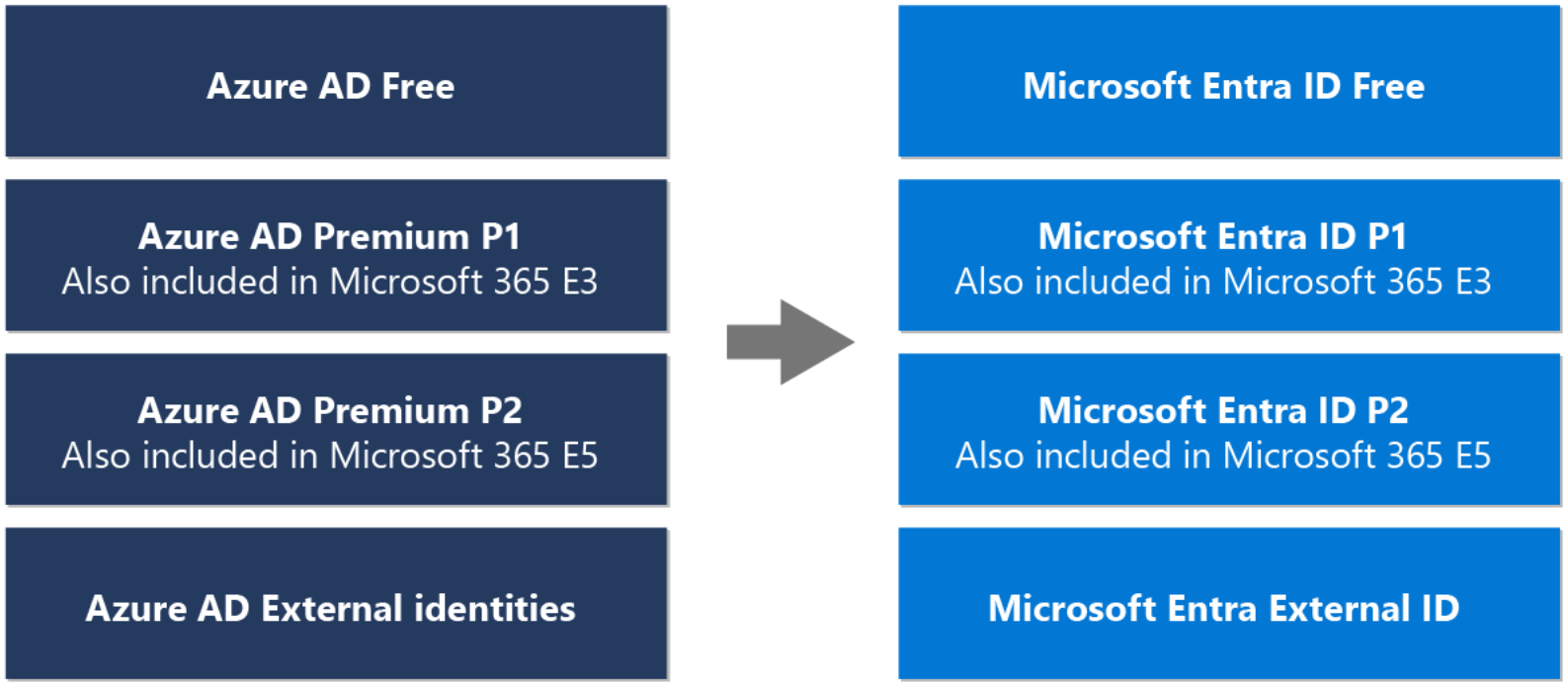
**Microsoft Entra ID** Free
Керування користувачами, групами, синхронізація з локальним AD, основні звіти, MFA, SSO, сервіс самообслуговування для зміни паролю хмарними користувачами
Не зовсім безкоштовно :) ⇠ *Безкоштовно* надається користувачам інших хмарних сервісів Microsoft, наприклад Microsoft 365, Microsoft Azure
**Microsoft Entra ID P1**
Те саме, що й у *Free*, + користувацький доступ і до локальних ресурсів AD, і до ресурсів у хмарі; групи з динамічним членством, Microsoft Identity Manager, сервіс самообслуговування для скидання паролю локальними користувачами
**Microsoft Entra ID P2**

Те саме, що й у *Free* та *P1*, + Microsoft Entra ID Protection, Privileged Identity Management.

Більше ліцензій для Entra ID — тут:
https://learn.microsoft.com/en-us/entra/fundamentals/whatis

# 2. Основні можливості MS Entra ID

**Основні сервісні плани MS Entra ID: нові назви**




Джерело:
https://learn.microsoft.com/uk-ua/entra/fundamentals/media/new-name/azure-ad-new-name-high-res.png#lightbox

# 2. Основні можливості MS Entra ID

**Основні безпекові механізми в Entra ID:**

- MFA
- керування доступом на основі умов (conditional access)
- виявлення аномальної поведінки користувача (у межах Identity Protection)
- PIM (Privileged Identity Management)
- SSO (Single Sign-On) ⇠ *для інтеграції*

**PIM (Privileged Identity Management)**

Інструмент керування адміністративними обліковками.

Ключові підходи в основі PIM:

- використовується принцип мінімальних повноважень;
- час доступу з-під адміністративних облікових записів обмежено;
- дії з-під адміністративних обліковок логуються.

# 2. Основні можливості MS Entra ID

**Conditional Access (умовний доступ, доступ на основі умов)**

Передбачає застосування різних політик на основі різних сигналів. Мета — знайти баланс між безпекою та продуктивністю.

***Сигнали*** прив’язуються до ідентичностей.

***Політики*** мають формат «якщо — то».

***Рішення*** мають формат «заблокувати» або «дозволити» (дозвіл може передбачати додаткові умови, наприклад дозволити у разі успішного проходження MFA).

Приклади сигналів: користувач та його членство в групах, IP, клієнтський застосунок, клієнтський пристрій тощо.

Приклади рішень: блокування ризикованих входів, вимога MFA для адміністративних облікових.

# Корисні посилання

- Офіційна сторінка MS Entra ID: https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-id
- Офіційна документація MS Entra ID: https://learn.microsoft.com/uk-ua/entra/fundamentals/
- Електронні курси про MS Entra ID на Microsoft Learn: https://learn.microsoft.com/en-us/training/entra/
- Zero Trust Architecture (за NIST): https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf