15. Služby Azure pro zajištění identity, přístupu a zabezpečení

**1. Azure Active Directory (Azure AD) a Azure AD Domain Services**

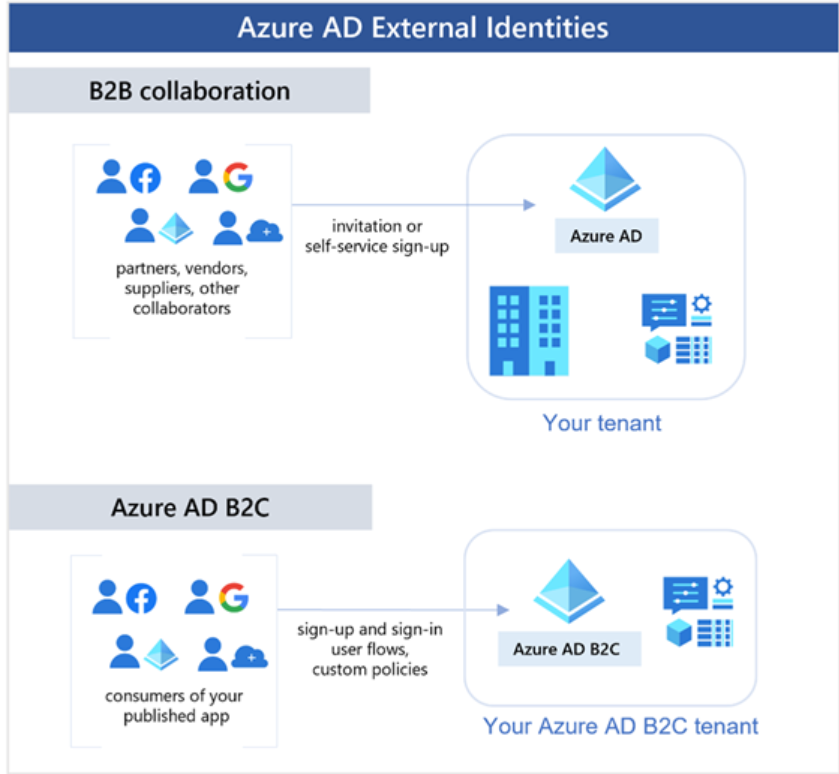
**1.1 Azure Active Directory (Microsoft Entra ID)**

**Definice**

* Cloudová služba pro správu identit a přístupu.
* Klíčový prvek pro přihlášení a řízení oprávnění uživatelů v Azure, Microsoft 365 i dalších SaaS aplikacích.

**Klíčové funkce**

1. **Ověřování**
   * **Vícefaktorové ověřování (MFA)**: kombinace hesla a dodatečného faktoru (mobilní aplikace Microsoft Authenticator, SMS kód, FIDO2 klíč).
   * **Samostatné resetování hesla**: uživatelé si mohou hesla resetovat bez zásahu administrátora (Self-Service Password Reset).
2. **Single Sign-On (SSO)**
   * Jednotné přihlášení k aplikacím Microsoft 365 a dalším SaaS řešením (Salesforce, Dropbox), i k vlastním aplikacím pomocí SAML, OAuth apod.
3. **Správa zařízení**
   * Registrace zařízení (Windows, iOS, Android) do Azure AD, možnost řídit jejich stav (compliance) pomocí Microsoft Intune.
   * Podmíněný přístup na základě zabezpečení zařízení (šifrování, heslo/PIN, správa aktualizací).
4. **Externí identity**
   * **Azure AD B2B**: spolupráce s partnery a externími uživateli ve formě hostů.
   * **Azure AD B2C**: správa identit zákazníků (např. pro e-shopy), možnost přizpůsobit přihlašovací rozhraní.



1. **Integrace s on-premises**
   * **Microsoft Entra Connect**: synchronizace uživatelů, skupin a hesel z místního Active Directory do Azure AD.
   * Umožňuje hybridní identitu (jedno uživatelské jméno a heslo pro on-prem i cloudové služby).

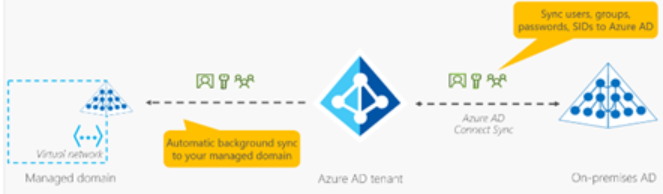
**1.2 Microsoft Entra Domain Services**

**Definice**

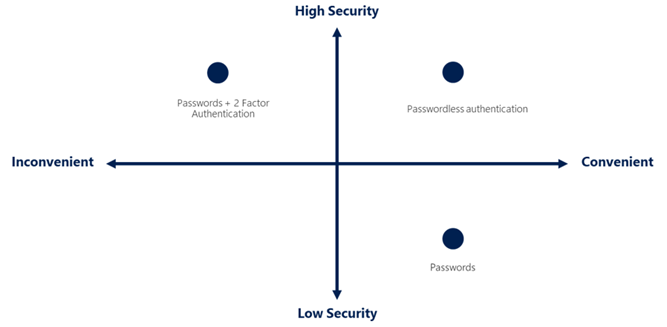
* Spravovaná služba v Azure, která poskytuje funkce tradiční domény Active Directory (LDAP, Kerberos/NTLM, Group Policy) bez nutnosti provozovat vlastní doménové řadiče.

**Vlastnosti**

* **Kompatibilita s Windows Server Active Directory**: podpora autentizačních protokolů (Kerberos/NTLM), Group Policy, LDAP.
* **Automatická správa**: Microsoft zajišťuje údržbu (aktualizace, zálohování) a vysokou dostupnost DC.
* **Legacy aplikace**: vhodné pro migraci starších aplikací do cloudu, pokud vyžadují tradiční doménové funkce.
* **Synchronizace s Azure AD**: jednosměrná synchronizace (uživatelé, skupiny) z Microsoft Entra do Microsoft Entra DS.



**2. Možnosti ověřování ve službě Azure**



**2.1 Single Sign-On (SSO)**

* **Federované ověřování**: propojení Azure AD s externími poskytovateli identity (Google, Facebook) přes SAML 2.0, OpenID Connect.
* **Integrované aplikace**: předpřipravené šablony pro SaaS aplikace (Zoom, Slack, ServiceNow).

**2.2 Vícefaktorové ověřování (MFA)**

* Typy ověření:
  1. **Něco, co znáte** (heslo),
  2. **Něco, co máte** (telefon, FIDO2 klíč),
  3. **Něco, co jste** (biometrie – otisk prstu, rozpoznání obličeje).
* **Podmíněné spouštění MFA**: např. vyžadovat MFA jen při přihlášení z neznámé sítě či vysokého rizika.

**2.3 Ověřování bez hesla (Passwordless)**

* **Windows Hello for Business**: biometrické přihlášení (otisk prstu, obličej) nebo PIN chráněný v TPM čipu.
* **Microsoft Authenticator**: potvrzení notifikací namísto zadávání hesla.
* **FIDO2 klíče**: fyzické USB/NFC klíče (např. YubiKey) – bezpečná metoda bez nutnosti hesla.

**3. Podmíněný přístup a Role-Based Access Control (RBAC)**

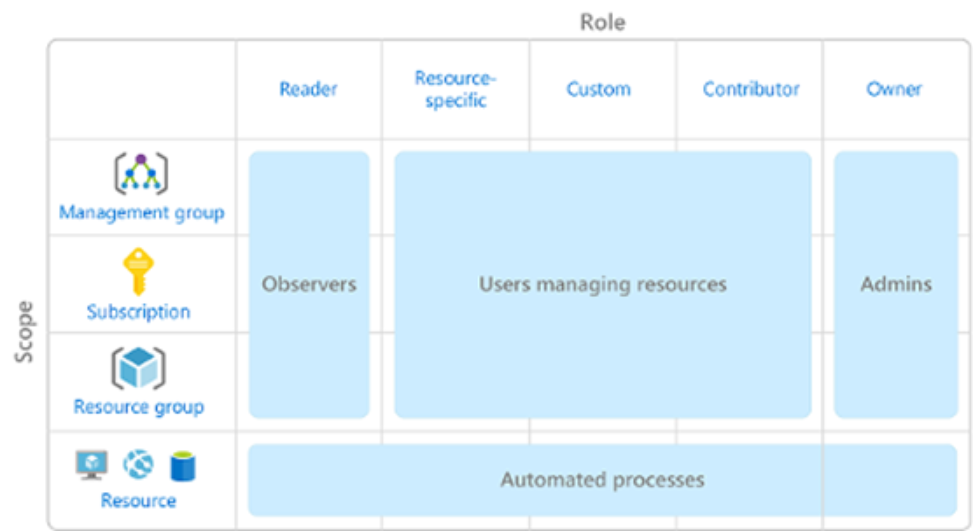
**3.1 Podmíněný přístup (Conditional Access)**

* **Princip**: Dynamické rozhodování o přístupu k aplikacím a datům na základě kontextu (identita uživatele, typ zařízení, geografická poloha atd.).
* **Signály pro vyhodnocení**:
  + Uživatel/role (např. globální administrátor),
  + Umístění (IP, zeměpisná poloha),
  + Typ a stav zařízení (OS, compliance s Intune),
  + Riziko přihlášení (podezřelá IP, netypická geolokace).
* **Příklady politik**:
  + Blokovat přístup ze zemí s vysokým rizikem.
  + Vyžadovat MFA pro přístup k citlivým aplikacím.
  + Povolit přístup jen z firemních (compliant) zařízení.



**3.2 Role-Based Access Control (RBAC)**

* **Princip**: Přiřazení uživatelů či skupin do rolí, které určují oprávnění k prostředkům v Azure.
* **Předdefinované role**:
  + **Owner (Vlastník)**: úplná kontrola nad zdroji, včetně přiřazování oprávnění,
  + **Contributor (Přispěvatel)**: správa zdrojů (vytváření, mazání), ale nemůže měnit přístupová práva,
  + **Reader (Čtenář)**: pouze prohlížení,
  + **Security Admin (Správce zabezpečení)**: správa bezpečnostních zásad.
* **Vlastní role (Custom Roles)**: definice specifických povolení dle potřeby.
* **Dědičnost**: role přiřazené na úrovni subscription se dědí i do resource groups a konkrétních resource.



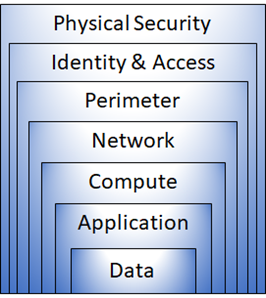
**4. Model Zero Trust a Defense-in-Depth**

**4.1 Model Zero Trust**

* **Zásady**:
  1. **Explicitní ověření**: neustálé ověřování identity a kontextu, i uvnitř firemní sítě,
  2. **Nejnižší možná oprávnění**: každý má přístup jen k nutnému minimu,
  3. **Předpoklad narušení**: mikrosegmentace, pravidelný audit a detekce anomálií.
* **Nástroje**:
  + Conditional Access, MFA, RBAC, šifrování dat, monitorování a audit.

**4.2 Defense-in-Depth (Vícevrstvé zabezpečení)**

* **Hlavní vrstvy** (příklady):
  1. **Fyzická vrstva**: zabezpečená datacentra Azure (biometrie, CCTV).
  2. **Identita a přístup**: Azure AD, MFA, audit přihlášení.
  3. **Perimeter**: Azure DDoS Protection, Azure Firewall.
  4. **Síť**: segmentace pomocí VNet, NSG (Network Security Groups).
  5. **Výpočetní vrstva (Compute)**: ochrana VM (Azure Security Center, Endpoint Protection).
  6. **Aplikace**: Web Application Firewall (WAF), testování zranitelností.
  7. **Data**: šifrování disku (Azure Disk Encryption), šifrování při přenosu (TLS), klasifikace citlivých dat (Microsoft Purview).



**5. Doplňkové nástroje pro zabezpečení**

1. **Microsoft Defender for Cloud**
   * Kontinuální hodnocení zabezpečení, doporučení pro nastavení, detekce hrozeb.
   * Integrace s Azure Policy pro vynucování bezpečnostních standardů.
2. **Azure Policy**
   * Tvorba zásad pro compliance (např. povinné šifrování storage účtů).
   * Automatické nasazení oprav nebo upozornění, pokud prostředek nevyhovuje zásadě.
3. **Azure Blueprints**
   * Předdefinované šablony pro nasazení politik, rolí, ARM šablon a dalších konfigurací pro konkrétní standardy (HIPAA, GDPR).
4. **Microsoft Purview**
   * Správa dat a data governance, klasifikace a ochrana citlivých informací, sledování přístupu.
5. **Service Trust Portal**
   * Portál s dokumentací k zabezpečení a compliance Azure (audity, certifikace jako ISO 27001).

**Shrnutí**

* **Azure Active Directory** (Microsoft Entra ID) je základem pro správu cloudových identit a řízení přístupu. Poskytuje SSO, MFA, napojení na on-premises, externí identity a podporu pro ověřování bez hesla.
* **Azure AD Domain Services** přináší do cloudu tradiční doménové služby, kompatibilní s LDAP a Group Policy, bez nutnosti spravovat vlastní doménové řadiče.
* **Conditional Access** a **RBAC** umožňují flexibilní a granulární řízení přístupových práv na základě kontextu a rolí.
* **Zero Trust** a **Defense-in-Depth** definují moderní přístupy k architektuře zabezpečení, kombinující více ochranných vrstev a neustálé ověřování.
* **Doplňkové nástroje** jako Microsoft Defender for Cloud, Azure Policy, Azure Blueprints, Microsoft Purview a Service Trust Portal výrazně rozšiřují možnosti správy, zabezpečení a compliance v cloudu.