Dispensa: Azure - Account e Subscription, Azure Active Directory, Utenti e Gruppi

1. Introduzione

Microsoft Azure è la piattaforma di cloud computing di Microsoft che offre servizi e risorse per l'implementazione di soluzioni IT flessibili e scalabili. In questa dispensa vedremo:

1. La differenza tra Azure **Account** e **Subscription**.
2. Il ruolo di **Azure Active Directory** (Azure AD) nell'autenticazione e autorizzazione.
3. Come gestire **Utenti** e **Gruppi** all'interno di Azure AD.

---

2. Azure Account e Subscription

2.1. Azure Account

- **Cos'è**
  Un Azure Account rappresenta la tua identità principale per accedere e gestire i servizi di Azure. L'account è tipicamente basato su un indirizzo email Microsoft (es. Outlook, Hotmail) oppure su un account aziendale collegato a un Azure AD tenant.

- **Tenant (o directory)**
  - Ogni account è associato a un tenant di Azure AD, che contiene gli utenti, i gruppi e le impostazioni di autenticazione.
  - Se hai un account aziendale, spesso c'è un tenant dedicato per l'intera organizzazione.

- **Creazione di un Azure Account**
  - Puoi registrarti qui (https://azure.microsoft.com) (sezione Try Azure for free) e ottenere un trial gratuito.
  - Viene richiesto di inserire una carta di credito per verificare l'identità (non verranno addebitati costi se non superi il credito o la durata del periodo di prova).

- **Ruoli principali dell'account**
  - *Account Administrator*: utente che possiede il controllo totale sull'account di fatturazione.

- *Service Administrator / Co-Administrator*: ruoli (meno usati oggi) che consentono la gestione delle risorse a livello classico.
- Con il *Role-Based Access Control (RBAC)*, i ruoli classici sono integrati da ruoli più granulari (Owner, Contributor, Reader, ecc.) gestibili a livello di Subscription, Resource Group e risorse.

2.2. Subscription

- **Definizione**
  Una **Subscription** è l'unità di fatturazione e di "contenimento" delle risorse in Azure. Ogni risorsa (VM, Database, App Service, ecc.) deve appartenere a una Subscription.

- **Tipi di Subscription**

  - **Free Trial**: offre un credito iniziale per testare il servizio.
  - **Pay-As-You-Go**: paghi solo per le risorse effettivamente utilizzate.
  - **Visual Studio/MSDN**: spesso inclusa con determinati abbonamenti di sviluppo.
  - **Enterprise Agreement (EA)**: per grandi aziende che acquistano un volume elevato di servizi Microsoft.

- **Relazione Account-Subscription**

  - Un Azure Account può gestire più Subscription.
  - Ogni Subscription ha un proprio ciclo di fatturazione, limiti di risorse e permessi assegnati.

2.3. Gestione di più Subscription

- **Management Groups**

  - Consentono di organizzare gerarchicamente più subscription.
  - Utili per applicare policy, controlli di sicurezza e regole di governance in modo centralizzato.

- **Best practice di governance**

  1. **Naming convention**: dare nomi chiari a subscription, resource group e risorse (es. `<Ambiente>-<Progetto>-<Funzione>`).
  2. **Azure Policy**: per imporre determinate configurazioni (ad es. regioni consentite).
  3. **Tag**: etichette (coppie chiave/valore) per raggruppare e organizzare le risorse, anche a scopo di rendicontazione costi.

---

3. Azure Active Directory (Azure AD)

3.1. Che cos'è un directory service?

- **Definizione**
  Un servizio di directory gestisce utenti, gruppi e dispositivi per scopi di autenticazione e autorizzazione.
- **Differenza con Active Directory tradizionale**

- L’Active Directory tradizionale (on-premises) richiede uno o più server (domain controller).
- Azure AD è un servizio cloud-based gestito da Microsoft che non richiede infrastruttura on-premises.

3.2. Funzionamento di Azure AD

- **Identity Provider (IdP)**
  - Azure AD fornisce l’autenticazione centralizzata (Single Sign-On) per le applicazioni Microsoft 365 e applicazioni SaaS di terze parti.
  - Ogni volta che un utente accede a un servizio, Azure AD verifica le credenziali e assegna eventuali token di accesso.
- **Tenant**
  - Lo spazio logico che identifica la tua organizzazione in Azure AD.
  - Puoi associare uno o più domini personalizzati (es. `contoso.com`) al posto di quello di default `onmicrosoft.com`.

3.3. Piani di Azure AD

1. **Azure AD Free**
   - Funzionalità base: gestione utenti, gruppi, SSO per Azure e Microsoft 365.
2. **Microsoft 365 Apps / Office 365**
   - Incluso con licenze Microsoft 365: aggiunge alcune funzionalità aggiuntive (reportistica, reset password self-service in modalità limitata, ecc.).
3. **Azure AD Premium P1**
   - Include *Conditional Access* di base, *MFA* avanzato, *Dynamic Groups*, possibilità di delegare l’accesso a risorse con politiche più sofisticate.
4. **Azure AD Premium P2**
   - Aggiunge *Identity Protection* (analisi di rischio e segnalazioni di account compromessi) e *Privileged Identity Management (PIM)*, per controllare e monitorare gli account con privilegi elevati.

3.4. Integrazione con on-premises (cenni)

- **Azure AD Connect**
  - Strumento per sincronizzare gli account di Active Directory locale su Azure AD.
  - Può gestire anche la sincronizzazione di password (Password Hash Sync), la pass-through authentication (PTA) o la federazione (AD FS).

---

4. Gestione di Utenti e Gruppi

4.1. Utenti in Azure AD

- **Tipologie**

1. **Utenti cloud-only**: creati direttamente in Azure AD (non hanno corrispondenza in AD locale).
2. **Utenti sincronizzati**: provengono dall'AD on-premises e sono sincronizzati tramite Azure AD Connect.

- **Attributi principali**
  - **UPN** (User Principal Name): di solito corrisponde all'indirizzo email aziendale.
  - **Password**: gestibile tramite MFA, SSPR (Self-Service Password Reset), e policies (es. scadenza password).
  - **Ruoli assegnati**: a livello di directory (es. Global Administrator, User Administrator) o a livello di risorsa (RBAC in Azure).
- **Sicurezza**
  - **Multi-Factor Authentication (MFA)**: aggiunge un secondo fattore (SMS, telefonata, app Authenticator) per rendere l'accesso più sicuro.
  - **Conditional Access**: regole che consentono l'accesso solo se rispettate alcune condizioni (posizione geografica, dispositivo compliant, ecc.).

4.2. Gruppi in Azure AD

- **Security groups vs Microsoft 365 groups**
  - **Security groups**: utilizzati per assegnare permessi e controlli di accesso (ad es. a una VM o una web app in Azure).
  - **Microsoft 365 groups**: includono anche funzionalità collaborative come mailbox condivisa, sito SharePoint, Planner, Teams.
- **Ruoli e Permessi**
  - In Azure, l'**RBAC (Role-Based Access Control)** consente di assegnare ruoli come *Owner*, *Contributor*, *Reader* a un gruppo (invece che a singoli utenti).
  - È un metodo molto più scalabile per la gestione dei permessi.
- **Gruppi dinamici (richiede P1/P2)**
  - Permettono di aggiungere o rimuovere automaticamente utenti in base a regole sugli attributi (es. reparto, job title, località).

---

5. Consigli pratici e best practice

1. **Usa l'MFA per tutti gli utenti**
   - Riduce drasticamente il rischio di compromissione dell'account.
2. **Organizza le Subscription con un criterio**
   - Ad esempio, una Subscription per l'ambiente di test, una per quello di produzione, oppure una per ogni reparto.
3. **Assegna ruoli a gruppi, non a utenti singoli**

    - Facilita la manutenzione e la revoca di autorizzazioni.
4. **Utilizza i tag e le policy**
    - Rendi più facile la governance e il controllo dei costi.
5. **Documenta le configurazioni**
    - Mantieni un elenco dei ruoli e dei gruppi, in modo da sapere sempre chi ha permessi su cosa.

---

6. Risorse e approfondimenti

- **Portale Azure**: https://portal.azure.com (https://portal.azure.com)
- **Documentazione ufficiale Azure**: https://docs.microsoft.com/azure/ (https://docs.microsoft.com/azure/)
- **Documentazione Azure Active Directory**: https://docs.microsoft.com/azure/active-directory/ (https://docs.microsoft.com/azure/active-directory/)
- **Microsoft Learn**: https://learn.microsoft.com/ (https://learn.microsoft.com/) - corsi e moduli interattivi gratuiti.
- **Azure AD pricing**: per dettagli sui piani Free, P1, P2, controlla la sezione di pricing sul sito Azure.

---

7. Breve Glossario

- **Account**: la tua identità con cui accedi ad Azure.
- **Tenant**: spazio logico (directory) in Azure AD che racchiude utenti, gruppi e impostazioni di autenticazione.
- **Subscription**: contenitore di fatturazione e gestione risorse in Azure.
- **Resource Group**: raggruppamento logico di risorse Azure (VM, storage, database, ecc.) appartenenti alla stessa subscription.
- **RBAC**: meccanismo di controllo degli accessi basato sui ruoli, applicabile a livello di subscription, resource group o risorsa singola.
- **MFA**: Multi-Factor Authentication, aggiunge un ulteriore livello di sicurezza oltre alla password.

---

8. Conclusioni

- Avere chiaro il modello di **Account** e **Subscription** è fondamentale per organizzare costi e risorse.
- **Azure AD** è il fulcro della sicurezza e dell'identità in Azure e Microsoft 365: tutti gli utenti, i gruppi e i meccanismi di autenticazione passano attraverso di esso.
- L'uso corretto di **Utenti e Gruppi** consente di gestire in modo efficace i permessi, evitando di creare configurazioni difficili da mantenere.
