

Esercizio di Pratica S10L3 – Cloud, Backup e RAID

Sergio Falcone

INTRODUZIONE

Ricerca sui principali fornitori di servizi cloud:

- 1) Effettuare una ricerca sui principali fornitori di servizi cloud (AWS, Azure, Google Cloud).
- 2) Descrivere brevemente ciascun fornitore e le sue caratteristiche principali.
- 3) Descrizione dei Modelli di Servizio Cloud:
- 4) Descrivere i tre modelli principali di servizio cloud: IaaS, PaaS e SaaS.
IaaS (Infrastructure as a Service): Fornire un esempio e descrivere i vantaggi.
PaaS (Platform as a Service): Fornire un esempio e descrivere i vantaggi.
SaaS (Software as a Service): Fornire un esempio e descrivere i vantaggi.

DEFINIZIONE DI CLOUD

Il **Cloud Computing** è un modello di erogazione di servizi informatici tramite Internet che consente di accedere a risorse condivise come server, storage, database, reti, software e servizi applicativi senza che ci sia il bisogno di possedere o gestire direttamente l'infrastruttura fisica (hardware)

Invece di installare hardware e software localmente, le risorse vengono fornite da un provider esterno e utilizzate tramite rete, con un modello di pagamento basato sulla quantità di risorse utilizzate. Le sue caratteristiche principali sono:

1. Attivazione autonoma delle risorse.
2. Utilizzo da qualsiasi dispositivo connesso.
3. Infrastruttura condivisa tra più utenti.
4. Risorse adattabili al carico di lavoro.
5. Monitoraggio e fatturazione in base all'utilizzo.

Nel Cloud la sicurezza si basa sul modello di responsabilità condivisa, cioè il provider del servizio Cloud protegge l'infrastruttura fisica mentre il cliente è responsabile della configurazione sicura dei servizi. I rischi per la sicurezza però sono molteplici.

Tra i principali rischi troviamo l'errata configurazione dei servizi, gli accessi non autorizzati quindi la potenziale violazione dei dati e la possibilità di attacchi DDos.

Le contromisure a questi rischi però sono la crittografia dei dati, autenticazioni multi-fattore (MFA), monitoraggio continuo e gestione delle identità (IAM)

PRINCIPALI FORNITORI DEL SERVIZIO

1) Amazon Web Services (AWS)

Amazon Web Services (AWS) è uno dei providers di servizi cloud più diffusi al mondo, lanciato appunto da Amazon nel 2006.

AWS offre una vasta gamma di servizi on-demand per computing, storage, database, networking, analytics, intelligenza artificiale, sicurezza e molto altro.

Le caratteristiche principali di AWS includono:

- **Scalabilità dinamica:** permette di aumentare o diminuire le risorse in base al carico di lavoro.
- **Servizi globali:** data center in numerose regioni geografiche per garantire bassa latenza e resilienza.
- **Ampio ecosistema** di servizi integrati e strumenti di automazione.
- **Sicurezza avanzata:** attraverso certificazioni di conformità e controlli di accesso granulare.

AWS è conforme a numerosi standard di sicurezza internazionali e implementa il modello di responsabilità condivisa e i suoi strumenti di sicurezza principali sono:

- **IAM (Identity and Access Management):** Gestione utenti e permessi.
- **AWS Shield:** Protezione DDoS.
- **AWS WAF:** Firewall applicativo.
- **GuardDuty:** Rilevamento minacce.
- **CloudTrail:** Logging e auditing.
- **KMS (Key Management Service):** Gestione chiavi crittografiche.

Amazon Web Services rappresenta una piattaforma cloud estremamente completa e scalabile, adatta sia a startup sia a grandi organizzazioni. In ambito sicurezza informatica, la corretta configurazione dei servizi e la comprensione del modello di responsabilità condivisa sono elementi fondamentali per garantirne sicurezza e compliance.

2) Microsoft Azure

Microsoft Azure è la piattaforma di cloud computing di Microsoft, lanciata nel 2010. È uno dei principali provider globali di servizi cloud e si distingue per la forte integrazione con l'ecosistema Microsoft e per il supporto agli ambienti aziendali e ibridi.

Tra i principali servizi di Azure troviamo i servizi di Compute (tutte le risorse di elaborazione messe a disposizione dal provider cloud, cioè di eseguire programmi, applicazioni o processi su server remoti), servizi di Storage, Database e Networking

Azure è conforme a standard internazionali e adotta il modello di responsabilità condivisa, simile a quello AWS.

I suoi strumenti di sicurezza principali sono:

- **Microsoft Entra ID (ex Azure Active Directory):** Identity & Access Management.
- **Microsoft Defender for Cloud:** Protezione workload e threat detection.
- **Azure Security Center:** Monitoraggio di sicurezza.
- **Azure Sentinel:** SIEM e SOAR cloud-native.
- **Azure Key Vault:** Gestione chiavi crittografiche e segreti.
- **DDoS Protection:** Protezione contro attacchi DDos

Microsoft Azure rappresenta una piattaforma cloud orientata al mondo aziendale, con forte integrazione ibrida e strumenti avanzati di sicurezza. In ambito della sicurezza, Azure offre soluzioni mature per l'identity management, monitoring e threat detection, rendendolo particolarmente adatto ad ambienti complessi e regolamentati.

3) Google Cloud Platform (GCP)

Google Cloud Platform (GCP) è la piattaforma di cloud computing di Google, lanciata nel 2008. È nota per le sue capacità avanzate nei big data, machine learning e intelligenza artificiale.

GCP offre servizi nei modelli IaaS, PaaS e SaaS, oltre a strumenti serverless, container e di gestione multi-cloud.

Il suo vantaggio principale è la scalabilità e l'innovazione tecnologica, sfruttando la stessa infrastruttura che supporta prodotti globali come Google Search, YouTube e Gmail.

Tra i principali servizi di GCP troviamo i servizi di Compute, di Storage, Database, Big Data e AI/ML, Networking

Google Cloud Platform adotta il modello di responsabilità condivisa, quindi Google gestisce sicurezza fisica, hardware e infrastruttura di rete e il Cliente gestisce la sicurezza dei dati, configurazioni delle VM, applicazioni e accessi.

I suoi strumenti principali sono:

- **Cloud IAM:** Identity & Access Management.
- **Cloud Key Management (KMS):** Gestione chiavi crittografiche.
- **Cloud Security Command Center (SCC):** Monitoraggio e rilevamento minacce.
- **DDoS Protection e Cloud Armor:** Protezione da attacchi volumetrici e Layer 7 (Livello Applicazione).
- **VPC Service Controls:** Controlli di sicurezza per dati sensibili.

GCP è una piattaforma cloud completa, orientata a innovazione e scalabilità globale. È ideale per aziende che necessitano di Big Data, AI, containerizzazione e infrastrutture globali, mantenendo un alto livello di sicurezza grazie al modello di responsabilità condivisa e agli strumenti integrati di gestione e monitoraggio.

MODELLI IAAS, PAAS E SAAS

In ambito cloud i servizi vengono raggruppati in modelli di servizio, ognuno dei quali definisce il livello di astrazione e gestione offerto al cliente.

1. IaaS (Infrastructure as a Service)

IaaS fornisce risorse infrastrutturali di base come server virtuali, storage, rete e sistemi operativi, gestite completamente dal provider. Il cliente può configurare e gestire l'ambiente come desidera.

Esempio: Amazon EC2 (Elastic Compute Cloud), che consente di avviare e gestire macchine virtuali scalabili.

Vantaggi principali:

- Flessibilità e controllo totale dell'infrastruttura.
- Scalabilità on-demand, pagando solo per le risorse effettivamente utilizzate.
- Riduzione dei costi hardware e tempo di provisioning.

NIST Special Publication 800-145:” *Infrastructure as a Service (IaaS)*

La capacità fornita al consumatore è quella di effettuare il provisioning di risorse fondamentali di calcolo come potenza di elaborazione, storage, reti e altre risorse informatiche di base, sulle quali il consumatore può distribuire ed eseguire software arbitrario, inclusi sistemi operativi e applicazioni.

Il consumatore non gestisce né controlla l’infrastruttura cloud sottostante, ma ha il controllo sui sistemi operativi, sullo storage e sulle applicazioni distribuite; inoltre può avere un controllo limitato su alcuni componenti di rete selezionati (ad esempio firewall host). ”

2. PaaS (Platform as a Service)

PaaS fornisce una piattaforma completa per lo sviluppo, il test e il deployment delle applicazioni, abstraendo la gestione dell’infrastruttura sottostante.

Esempio: Microsoft Azure App Services, che permette di distribuire web app senza gestire server fisici o virtuali.

Vantaggi principali:

- Semplificazione dello sviluppo, con tool e runtime già configurati.
- Deployment semplificato delle applicazioni.
- Aggiornamenti e manutenzione del sistema gestiti dal provider.

NIST Special Publication 800-145: “*Platform as a Service (PaaS)*

La capacità fornita al consumatore è quella di distribuire sull’infrastruttura cloud applicazioni create o acquisite dal consumatore, sviluppate utilizzando linguaggi di programmazione, librerie, servizi e strumenti supportati dal provider.

Il consumatore non gestisce né controlla l’infrastruttura cloud sottostante (rete, server, sistemi operativi o storage), ma mantiene il controllo sulle applicazioni distribuite e, possibilmente, sulle impostazioni di configurazione dell’ambiente che ospita le applicazioni. ”

3. SaaS (Software as a Service)

SaaS fornisce applicazioni complete accessibili via internet, gestite interamente dal provider. Gli utenti finali utilizzano il software senza preoccuparsi dell’infrastruttura o della piattaforma sottostante.

Esempio: Microsoft 365 o Google Workspace, suite di produttività accessibili via browser.

Vantaggi principali:

- Nessuna installazione locale richiesta.
- Accesso da qualsiasi luogo con una connessione internet.
- Aggiornamenti automatici e manutenzione gestita dal provider.

NIST Special Publication 800-145:” *Software as a Service (SaaS)*

La capacità fornita al consumatore è quella di utilizzare le applicazioni del provider in esecuzione su un’infrastruttura cloud.

Le applicazioni sono accessibili da vari dispositivi client tramite un’interfaccia leggera (thin client), come un browser web (ad esempio, la posta elettronica web-based), oppure tramite un’interfaccia programmatica.

Il consumatore non gestisce né controlla l’infrastruttura cloud sottostante, inclusi rete, server, sistemi operativi, storage o persino le singole funzionalità dell’applicazione, fatta eccezione per eventuali limitate impostazioni di configurazione specifiche per l’utente.”