Progettare una Landing Zone su AWS: i pilastri fondamentali

6 Luglio 2022 - 9 min. read

governance and compliance | Landing Zone

Nell'articolo precedente abbiamo visto che cos'è una Landing Zone e qualche nozione base su come aprocciare l'argomento.

In questo articolo analizzeremo e dettaglieremo gli aspetti su cui costruire una Landing Zone e i servizi AWS da sfruttare.

Di seguito verranno presi in considerazione gli aspetti che compongono la Landing Zone.

Organization

Il primo argomento che va preso in considerazione riguarda è la struttura degli account - ovvero l'Organization - che, come specificato dalla Legge di Conway (link ad articolo 1), deve rispecchiare la struttura organizzativa dell'azienda. Questo significa che diversi team hanno le loro responsabilità e le loro esigenze di risorse diverse.

Qui entra in gioco il servizio **AWS Organizations** che ci permette di organizzare gli account per *scope*, di creare *Organizational Units* (OU), semplificare l'allocazione dei costi e di automatizzare la creazione di nuovi Accounts. Un account è l'unico modo vero per separare i costi a livello di fatturazione. Più account aiutano a separare i volumi generati a livello di fatturazione tra business unit, team funzionali o singoli utenti.

La strategia multi-account porta al massimo livello di isolamento delle risorse e della sicurezza. L'isolamento, a seconda dei casi, deve avvenire anche a livello dati.

L'isolamento dei data store su un account limita il numero di persone che possono accedere e gestire quel data store aiutando a rispettare il Regolamento generale sulla protezione dei dati (GDPR).

Il primo passo sul percorso che ci porta ad una corretta configurazione, prevede di creare due macro gruppi di account: quelli **Foundational** e quelli dedicati a **Products and Workloads**.

I **Foundational** account sono, appunto, dedicati ai team di struttura, atti a soddisfare le esigenze dell'azienda stessa.

Per i **Product and Workloads** è conveniente creare delle OU per prodotti dove gli account vengono divisi secondo gli ambienti di sviluppo (da Dev a Produzione), ma anche OU dedicate ad ospitare gli ambienti dedicati a gruppi di workload come quelli di struttura. Business unit o prodotti diversi potrebbero avere scopi e processi diversi.

Da non sottovalutare è anche la presenza delle quote predefinite dei servizi negli account AWS. La separazione dei carichi di lavoro in account diversi impedisce loro di consumare limiti, snellendo i processi aziendali.

Identity and Access Management

Il principio dei privilegi minimi è il mantra di chi deve gestire gli accessi e i permessi ad infrastrutture o a parti di esse. Rispettare questo principio significa ridurre il *blast-radius* nel caso di sottrazione maliziosa dei diritti di accesso all'ambiente Cloud.

Questo principio non deve portarci ad una complicazione nella gestione, sottintendendo, quindi, la necessità di una gestione centralizzata delle credenziali.

Nello scenario AWS è possibile creare risorse sia mediante la console web che tramite l'utilizzo delle API REST Autenticate. La possibilità, quindi, di poter automatizzare le nostre azioni tramite l'utilizzo di queste API ci sottolinea ancora di più quanto sia attuale la gestione delle credenziali di accesso.

Vanno sicuramente implementate pratiche come quella della **Multi-Factor Authentication**, della **rotazione automatica** delle credenziali, di **password policy** forte e di autorizzazione ristretta.

Per **autenticazione** e **autorizzazione** AWS ci offre diverse possibilità: dall'utilizzo di **AWS IAM** alla possibilità di integrare l'**Identity Provider (IdP)** aziendale con **AWS SSO**. Questi servizi permettono sia una gestione centralizzata degli accessi sia di applicare tutte le pratiche di sicurezza descritte in precedenza.

Per l'accesso in console si può creare una landing page che ci permetta di discriminare le nostre credenziali e, magari, avere un client che ci aiuti a gestire i nostri accessi "programmatici" di tutti i giorni. Complementariamente ai servizi di gestione centralizzata di autorizzazione e autenticazione, per aiutare i nostri utenti ad essere efficienti ed efficaci in questi passaggi quotidiani, ci viene in soccorso **Leapp**, un tool open-source per gestire in modo sicuro e automatizzato le credenziali di accesso agli ambienti Cloud.

Networking

Fondamentale è la raggiungibilità dell'ambiente Cloud. Dalle connessioni degli utenti aziendali o dei collaboratori, alle connessioni dei nostri utenti esterni, come ad esempio integratori o utenti pubblici.

Prima di tutto bisogna strutturare la ripartizione del networking privato definendo i **CIDR** da assegnare alle varie reti virtuali presenti nei vari account definiti nella sezione *Organizations*. Qui è importante **evitare l'overlapping** per non incorrere in scenari complicati a livello implementativo e gestionale. Centralizzare i propri endpoint e il controllo delle loro rotte è importante per facilitare la gestione delle connessioni e la loro creazione.

Le nostre reti virtuali vengono definite tramite il servizio **AWS VPC** che vanno configurate a dovere tenendo conto dell'infrastruttura fisica del provider e dei requisiti di disponibilità delle infrastrutture. La connettività verso il pubblico è fornita tramite

l'**Internet Gateway** gestito e tramite l'implementazione di **AWS Managed NAT Gateway**.

Su AWS troviamo anche **AWS Transit Gateway** che ci permette di gestire centralmente e connetterci sia fisicamente, tramite **Direct Connect**, sia in maniera virtuale, tramite **AWS SiteToSite Managed VPN**. A questo concentratore possiamo collegare il nostro ufficio, i nostri data center e tutte le connessioni con i nostri partners, clienti e integratori. Transit Gateway ci viene in soccorso anche per le comunicazioni inter-vpc.

Da non trascurare sono anche gli accessi alle nostre reti virtuali da parte dei nostri utenti privati sparsi in giro per il mondo. In questi casi va tenuta in considerazione l'implementazione di una **VPN Dial Up** tramite **AWS Client VPN** che si integra con Transit Gateway.

Sotto il cappello del networking vanno considerati anche i DNS e la gestione dei domini. **AWS Route 53** e le sue peculiarità come il DNS Resolver vanno sfruttate sia per gestire i domini privati che pubblici oltre che determinare da che reti sia possibile risolvere i record.

Security

La security è un processo che implica pratiche che toccano in maniera basilare tutti gli aspetti dell'IT. Anche la terminologia si aggiorna e la pratica DevOps si trasforma in **DevSecOps**. Nel mondo delle buzzword serve a sottolineare l'importanza della security che va applicata su tutti i livelli.

Tra i canoni fondamentali su cui costruire la nostra Landing Zone spiccano in particolare la **tracciabilità**, la **protezione dei dati in transito e a riposo**, l'implementazione di **solide fondamenta sulle identità** e l'**isolamento**. Per quanto riguarda questi ultimi due argomenti, una corretta progettazione dell'organizzazione e una gestione centralizzata degli utenti ci facilitano nel far rispettare le best-practises in questo campo.

Come detto in precedenza, il Cloud AWS è costituito da API autenticate (sfruttate dalla console stessa). Ogni chiamata a queste API viene tracciata tramite il servizio **AWS CloudTrail** che può consolidare in un unico punto tutti i log.

Anche il traffico proveniente da internet può essere regolato tramite una gestione centralizzata delle regole di **AWS WAF**, il firewall web gestito del provider.

Security groups e Network ACL servono, invece, per controllare più puntualmente protocolli di comunicazione e specifiche connessioni tra reti. Con questi strumenti determiniamo quali comunicazioni, tra gli utenti interni e i workload aziendali, sono lecite.

Ciò non prescinde dal dover criptare tutte le nostre comunicazioni web pubbliche. Una gestione centralizzata dei certificati SSL collegati ai nostri domini può facilitare il controllo e la distribuzione.

Governance e Compliance

Mentre la **Governance** identifica chi ha potere e responsabilità e chi prende le decisioni, la **Compliance** è la conformità delle attività aziendali alle disposizioni normative, ai regolamenti, alle procedure ed ai codici di condotta.

Ogni azienda ha le proprie policy, i propri processi e deve poter implementare i propri controlli anche in ambiente Cloud. L'implementazione delle regole deve comunque permettere spazi di azione per i team, definendo quali guardrails in cui operare.

Abbiamo già parlato di quanto sia importante implementare la sicurezza nelle nostre pratiche. I dati, come già detto, non si devono esimere e devono venire criptati *at-rest*. Bisogna assicurarsi che, nel tempo, ogni workload rispetti questo canone. Anche evitare che vengano aggiunte regole di firewall che espongono la nostra infrastruttura a rischi è un altro canone fondamentale da far rispettare. Uno dei casi più classici prevede l'esposizione al pubblico di protocolli con vulnerabilità note.

L'automatizzazione dell'applicazione di queste regole e le rimediazioni automatiche si gestiscono centralmente affidandosi al servizio **AWS Config**.

AWS offre una vasta gamma di servizi adatti a scopi molto differenti. Non tutte le aziende hanno bisogno di sfruttare ogni servizio. Stessa cosa vale anche per le region globali su cui si possono mettere in opera i workload. Al fine di evitare che questi servizi e region vengano utilizzati vanno implementati dei guardrails tramite le **Service Control Policies**.

I controlli prevedono anche di implementare una classificazione delle risorse presenti in ambiente AWS. Una corretta strategia di tagging ci porta ad avere un'efficiente ripartizione dei costi e la possibilità di gestire i permessi su base **ABAC** (Attribute-based Access Control). A supporto di questa tematica esistono le **Tag Policies** che ci permettono di gestire centralmente i nostri Tag e di imporre che vengano utilizzati su tutte le risorse create.

Fin da subito vanno anche decise tutte le pratiche di deprovisioning delle risorse inutilizzate per non trovarsi in una situazione confusionaria in cui sia difficile attribuire e capire i propri costi.

Controllo dei costi

Le organizzazioni necessitano di un modo semplice e immediato per accedere alle **informazioni di fatturazione** di AWS, incluso un **riepilogo delle spese**, una **ripartizione di tutti i costi** di servizio sostenuti dagli account all'interno dell'organizzazione, insieme a **sconti** e **crediti**.

Fondamentale è la consolidazione delle fatture (consolidated billing) e predisporre protezioni adeguate in modo da poter mantenere il controllo su costi, governance e sicurezza. AWS consente alle organizzazioni di bilanciare la libertà e il controllo consentendo la governance delle autorizzazioni granulari dell'utente.

Per prendere decisioni consapevoli è necessaria una visibilità completa, quasi in tempo reale, dei costi e delle informazioni sull'utilizzo. AWS fornisce strumenti per organizzare le risorse in base alle esigenze, visualizzare e analizzare i dati di costi e di utilizzo in un unico riquadro. Oltre che controllare centralmente i costi, è possibile fornire in tempo reale informazioni sui costi, utili ai team di progettazione, applicazione e business. I dati dettagliati e allocabili sui costi consentono ai team di avere visibilità e informazioni per rendere conto della propria spesa.

AWS Cost Explorer presenta un'interfaccia di facile utilizzo che permette di visualizzare, analizzare e gestire i costi e l'utilizzo di AWS nel tempo. **AWS Budget** consente di impostare budget personalizzati per tenere traccia dei costi e dell'utilizzo dai casi d'uso più semplici a quelli più complessi.

Disaster Recovery

"Everything fails all the time" - Werner Vogel.

Tutto fallisce continuamente. Progettare con l'idea di fallimento in testa è fondamentale per costruire infrastrutture resilienti. Per questo motivo il **Disaster Recovery** è una strategia che va messa in campo già dalla progettazione della nostra Landing Zone.

Le tipologie di disastro che si possono verificare in cloud, e in generale, vengono divise in tre macro-categorie:

- Disastri naturali, come alluvioni o terremoti
- Fallimenti tecnici come interruzioni di connettività o di corrente
- Azioni umane, come configurazioni sbagliate o accessi non autorizzati

AWS non garantisce la resilienza delle nostre infrastrutture, ma ci fornisce tutti gli strumenti che dobbiamo sfruttare per poterle rendere resistenti ai fallimenti. Tutto questo è definito nello **Shared Responsibility Model** di AWS.

In questo contesto va prevista una strategia multi-region e multi-account, separando anche l'organization principale da quella preposta al Disaster Recovery. Anche gli accessi alle due strutture vanno separati e assegnati a personale differente.

Le strategie di Disaster Recovery disponibili sono categorizzabili in vari approcci, che vanno da costi bassi e complessità bassa per il backup&restore a strategie più costose e complesse di tipo active-active.

Determinante nella scelta di una strategia corretta è la definizione di due KPI: Recovery Time Objective (**RTO**) e Recovery Point Objective (**RPO**). Il primo definisce per quanto tempo si può interrompere la business continuity a valle di un disastro e il secondo identifica in termini di tempo quanti dati siamo disposti a perdere in caso di interruzione di servizio. I valori assegnati a questi KPI determinano quale strategia va applicata.

Per concludere

Come si evince da questa panoramica sui pillars della Landing Zone, a seconda della esigenze peculiari si possono ottenere un gran numero di personalizzazioni. Ogni caso va affrontato partendo sempre da una sessione di progettazione per la definizione dei requisiti che coinvolga tutti gli stakeholder aziendali e un partner esperto.

Nel prossimo articolo vedremo due esempi di come due realtà, una piccola e una grande, possono iniziare a pensare ad una Landing Zone proporzionata a loro.

Nicola Ferrari

Cloud Infrastructure Line Manager @ beSharp e AWS authorized instructor champion.Vivo la vita “un livello alla volta”. Ottengo i miei superpoteri raccogliendo caffeina nascosta qua e là nella mia mappa quotidiana. Sono un Internet surfer professionale (e ho visto tutto l’Internet per intero... almeno due volte!) e un appassionato di tecnologia, computer e networking. Costruire grandi cose IT - tutte precise e ordinate - contribuisce alla mia missione principale: la ricerca della perfezione!

Simone Merlini

CEO e co-fondatore di beSharp, Cloud Ninja ed early adopter di qualsiasi tipo di soluzione *aaS. Mi divido tra la tastiera del PC e quella a tasti bianchi e neri; sono specializzato nel deploy di cene pantagrueliche e nel test di bottiglie d'annata.
