Esempi di implementazione di Landing Zone

22 Luglio 2022 - 7 min. read

AWS Organizations *AWS Organizations* *governance and compliance* *Landing Zone*

Negli articoli precedenti abbiamo parlato di che cos'è una Landing Zone, perché è importante per qualsiasi azienda progettarla e capire su quali pilastri fondamentali costruirla.

Nei paragrafi di questo articolo proponiamo, a titolo esemplificativo, due differenti approcci alla Landing Zone, basati su due tipologie di aziende radicalmente differenti.

La prima - **Small IT** - riguarda le aziende con pochi workload e team IT ristretto, mentre la seconda è pensata per aziende con migliaia di workload e più team IT distribuiti e specializzati - **Large IT**.

Ad ognuna di queste, applicheremo ciascuno dei pilastri descritti in modo generale nella **parte due** della nostra serie.

Se pur da considerarsi come semplici esempi di declinazione di una Landing Zone, non riportabili così come sono all'interno di casi d'uso reali, i casi descitti nell'articolo sono in grado di sottolineare come organizzazioni diametralmente opposte per business e necessità, siano in realtà accumunate da un unico grande bisogno: la governance sui propri ambienti AWS.

Small IT

Organization

La semplificazione deve fare da padrona. In questi casi si può prevedere un'organizzazione light con una Organizatinal Unit (OU) principale in cui sono presenti uno o due account Foundational. Un account dedicato alle gestione della fatturazione e degli accessi, incaricato di gestire la nostra organizzazione. Un altro account potrebbe essere utilizzato per la gestione della parte di networking e security.

Una buona struttura iniziale, dunque, potrebbe essere basata su due OU fra servizi interni e servizi rivolti al pubblico in cui creare account dedicati alla produzione e account dedicati agli ambienti non produttivi.

Identity and Access management

Per partire con semplicità nella gestione degli accessi si può pensare di sfruttare direttamente il servizio AWS IAM censendo gli **IAM User** in un account centralizzato e creando **IAM Roles** negli account che contengono gli ambienti di sviluppo e di produzione dei workload. Se si volesse pensare ad una prima integrazione con il proprio IdP, si può procedere federandolo direttamente con AWS IAM.

Se siete interessati a questo argomento, ne abbiamo parlato in **questo articolo** descrivendo come è possibile, ad esempio, federare GSuite con AWS IAM.

Networking

In questi caso vanno previste connessioni dall'ufficio e dai nostri utenti verso le infrastrutture in Cloud. Per accentrare la gestione e le connessioni, si consiglia di sfruttare il servizio **Transit Gateway**. Questo oggetto ci permette anche di risparmiare senza rinunciare all'alta disponibilità implementando una configurazione che prevede **NAT Gateways centralizzati**.

Security

Per quanto riguarda la tracciabilità, è d'obbligo centralizzare tutti gli Audit Log provenienti dai vari account AWS.

Per quanto riguarda la sicurezza delle infrastrutture bisogna cercare di ridurre il più possibile la superficie di attacco, tenendo privati tutti i dati evitando di esporre al pubblico protocolli di interscambio deboli e vulnerabili.

Una corretta gestione dei backup dei propri dati e configurazioni è fondamentale per tutelarsi da attacchi rivolti contro i nostri servizi.

Governance e compliance

Per poter distribuire centralmente e in maniera standard le configurazioni di base dei vari account è imprescindibile l'applicazione del principio dell'**Infrastructure-as-Code** (**IaC**) tramite, ad esempio, il servizio **CloudFormation Stack Sets**. Questa modalità ci permette di controllare centralmente gli stack di configurazione di base dei vari account dell'organization aziendale.

Controllo dei costi

Per tenere sotto controllo i costi è di sicuro importante l'implementazione degli **allarmi sui budget** definiti per ogni workload o account.

I costi, poi, possono essere ottimizzati con l'applicazione dei **Saving Plans** che offrono uno sconto a fronte di un impegno almeno annuale e al più triennale.

Disaster recovery

Nel caso di aziende con pochi workload è meglio partire cercando di ridurre l'impatto del Disaster Recovery sui costi. Per fare questo la strategia corretta è quella del **Backup&Restore**. Vanno individuati i dati e replicati in maniera continua e l'infrastruttura deve venire codificata in modo tale di automatizzare le procedure di ripristino.

Large IT

Organization

Aziende con reparti digital che contano molti team esigono un'organizzazione complessa e molto stratificata. Occorre però evitare che la struttura esploda con il proliferare di troppi account.

Per quanto riguarda i Foundational account si può comunque pensare ad un'unica OU principale che conta diversi account divisi fra security, logging, gestione accessi, gestione fatturazione e networking.

L’alberatura si complica quando si passa alla classificazione dei workload. Va trovato un trade-off fra workload che hanno dignità di essere separati e workload che possono essere raggruppati, perchè gli account tendono ad esplodere in presenza di tanti ambienti di sviluppo.

Per chi vuole fornire ai propri **DevOps** la possibilità di sperimentare in ambienti sandbox si può costruire un’**Account Vending Machine** che sia in grado di fare il provisioning e il deprovisioning automatico di account.

Identity and Access management

Avere una dashboard centralizzata dove gestire i permessi alle varie OU o ai diversi account è di certo una necessità. Avere una Landing Page per facilitare gli accessi quotidiani di chi deve utilizzare la console è d’obbligo. Se aggiungiamo la possibilità di integrarci con il nostro IdP allora il servizio che fa al caso nostro è **AWS SSO**. Con AWS SSO è possibile gestire centralmente le identità e la autorizzazioni di accesso alla nostra struttura multi-account.

Networking

Per chi ha una topografia di rete complessa è difficile trovare una sintesi esaustiva. Sicuramente Transit Gateway è necessario ed è anche giusto sottolineare la possibilità di connettere due transit gateway presenti su region e account diversi.

L’**AWS VPN Client** si integrata a sua volta con AWS SSO per non dover gestire ulteriori credenziali di accesso.

Per quanto riguarda i nostri uffici o datacenter, al fine di ridurre latenze dovute al continuo trasferimento di dati vanno previsti collegamenti fisici tra le varie sedi e ambienti virtuali. La soluzione è creare una rete *mesh* di connessioni fisiche private tramite **Direct Connect**, supportate da **VPN SiteToSite** di backup.

In un’azienda complessa è conveniente definire i requisiti di accesso alle reti identificando percorsi che potenzialmente non rispettano i requisiti stessi. Per questo è utile sfruttare il servizio **Network Access Analyzer**.

Security

AWS Security Hub ci permette di avere una dashboard centralizzata su cui raccogliere e incrociare tutte le nostre metriche basate sulle regole di sicurezza.

Grazie al fatto che viene sfruttato **AWS Organization**, si dispone **Firewall Manager** che è un unico servizio per creare regole del firewall, creare policy di sicurezza e applicarle in modo coerente e gerarchico all'intera infrastruttura da un account amministratore centrale.

Governance e compliance

Nel caso di aziende molto grandi è utile fornire un portale self-service dal quale poter mettere in opera configurazioni validate dall'azienda. **Service Catalog** in tandem con **CloudFormation** consente di ottenere una governance coerente e di soddisfare i requisiti di conformità.

Le procedure vanno supportate dalla raccolta di metriche e con **Audit Manager**, è più facile valutare se le policy, procedure e i controlli stanno funzionando in modo efficiente.

Controllo dei costi

La ripartizione dei costi può essere fatta tramite il servizio **Billing Conductor** che permette di creare fatture ad hoc in caso di necessità complesse di ripartizione dei costi del business o dei clienti.

Necessaria è una strategia di controllo continuo dei costi che deve passare attraverso un processo di ottimizzazione della parte computazionale (**AWS Compute Optimizer**) e seguire le raccomandazioni automatiche per i piani di **Reservation** e per i **Saving Plans**.

Disaster recovery

Workload critici con requisiti di business continuity stringenti prevedono l'implementazione di una strategia **multi-site active-active**. Significa avere due workload situati in account e region differenti pronti a ricevere tutto il traffico di produzione, senza creare scenari di split-brain dei dati.

Per concludere

Il Cloud è uno strumento rivoluzionario, ma solo se usato bene; fondamentale è, quindi, avere un approccio informato e strutturato prima ancora che ai suoi servizi, alle dinamiche che ne stanno alla base. Da non sottovalurare quando si valuta un cambio di paradigma è un'adeguata formazione dei team IT finalizzata alla creazione, all'interno dell'azienda, di un Cloud Center of Excellence (CCoE). Questo gruppo deve essere in grado di guidare la trasformazione attraverso scelte strategiche sulla base delle nuove responsabilità e dei nuovi dati a disposizione.

In questa serie di articoli ci siamo focalizzati sul concetto di Landing Zone, il primo degli aspetti che il CCoE deve essere in grado di comprendere e declinare. La collaborazione tra il CCoE e un partner esperto consente alle aziende di progettare i propri ambienti Cloud nel modo migliore possibile personalizzandolo in base alle esigenze peculiari che ogni azienda ha. Il tutto sempre in ottica evolutiva: come qualsiasi progetto tecnologico, la Landing Zone non è un oggetto statico, ma qualcosa di dinamico che va adeguato alla continua mutazione aziendale e del mondo AWS.

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.
