AWS Landing Zone e networking centralizzato: un matrimonio ben riuscito

15 Settembre 2023 - 9 min. read

Advanced Networking | Amazon VPC | Amazon VPC | governance and compliance | Landing Zone

Introduzione

Quando ci si trova a dover progettare una Landing Zone, uno dei temi più salienti è sicuramente la configurazione del networking. (Se non sei familiare al concetto di Landing Zone parti dalla nostra serie di articoli per saperne di più).

La scelta di configurazione della rete che andremo a implementare sia in ambienti fully cloud, che in ambienti ibridi influirà moltissimo su sicurezza e operatività aziendale, che sulla comunicazione tra il Cloud e l'on-premise.

Networking design

Per quanto riguarda il networking della nostra organizzazione, AWS mette a disposizione diverse possibili soluzioni e approcci, ognuna con particolari benefici e use case specifici. Dobbiamo sempre ricordarci che, anche se possediamo molteplici possibilità tra cui scegliere, non sempre tutte faranno al caso nostro, ma dovremo cercare di capire quale di queste si adatterà meglio alle nostre esigenze, rispecchiando anche i pilastri portanti della nostra infrastruttura.

La soluzione che decideremo di adottare potrebbe anche essere una versione aggiornata nella nostra attuale infrastruttura e non per forza una nuova configurazione: dovremo tenere in considerazione i nostri trascorsi per capire dove la soluzione si adattava alle nostre esigenze e dove invece c'erano problematiche o margini di miglioramento.

Nel corso dell'articolo vedremo quelle che vengono considerate le migliori soluzioni per la **realizzazione di un'infrastruttura di rete condivisa e centralizzata su AWS**. Come avremo modo di vedere esistono due filoni principali quando si parla di infrastrutture di rete in un approccio multi-account: utilizzo di una singola VPC, oppure di molteplici VPC. Analizziamo entrambi gli approcci.

Singola VPC con AWS RAM

Se parliamo di singola VPC è difficile riuscire ad adattarla ad un contesto multi-account, eppure, grazie al servizio **AWS RAM**, questa soluzione risulta sia efficiente, che molto funzionale.

Pur essendo uno degli approcci meno conosciuti, consiste nell'utilizzo di una **singola VPC centralizzata per erogare connettività a tutta la nostra Organization su AWS**. Come vedremo tra poco, questa soluzione fornisce moltissimi vantaggi spesso messi in secondo piano, ma che talvolta possono fare la differenza.

Prima di tutto, però, cerchiamo di capire come realizzare una VPC centralizzata e come adattarla ai nostri requisiti.

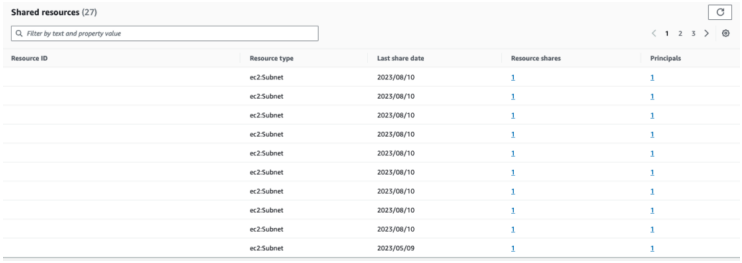
Implementazione

Per la realizzazione di questa infrastruttura avremo bisogno di pochi servizi: una singola VPC e il servizio AWS RAM.

Come piccolo tip, consigliamo di utilizzare una **VPC con un ampio indirizzamento CIDR**. Questo ci permetterà di creare numerose subnet senza dover ricorrere all'estensione dell'indirizzamento associato alla VPC.

Per cominciare basterà **configurare un account adibito alle gestione del networking** dal quale successivamente condivideremo tutte le subnet verso gli account della nostra Organization (nel corso dell'articolo lo chiameremo "*network-account*"). Una volta creata la nostra VPC e un piccolo sottoinsieme di subnet, potremo procedere con la loro condivisione tramite l'utilizzo di AWS RAM verso l'account desiderato.

Come ultimo step basterà collegarsi all'account di destinazione e accettare la condivisione delle subnet.

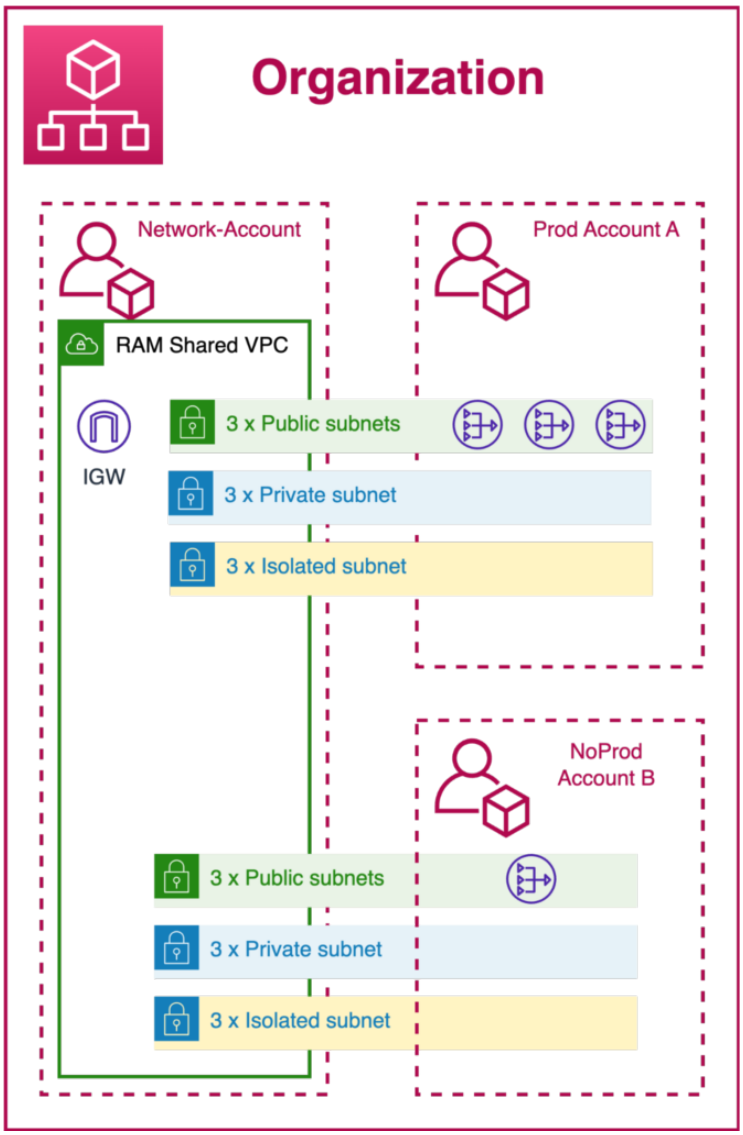


Per tutto quello che riguarda la condivisione, utilizzeremo il servizio di AWS RAM adibito proprio a questo genere di attività e che ci permetterà anche di configurare determinati parametri per differenziare come verranno condivise, e quindi utilizzate, le nostre risorse.

Se tutto sarà andato per il verso giusto, nell'account applicativo dovremmo vedere comparire le subnet che abbiamo appena condiviso e la loro VPC.

Non vi preoccupate se anche la VPC risulterà visibile dato che, comunque, ogni account avrà accesso solo alle subnet che si è deciso di condividere.

Ora che abbiamo le subnet sull'account di destinazione sarà possibile creare le risorse utilizzando network condiviso, pur non essendo gli owner della suddetta VPC. Ovviamente, non possedendo l'ownership di queste subnet, non potremo creare rotte o eliminarne altre dato che non siamo i detentori delle varie routing tables. Per tutte queste attività sarà necessario avere un amministratore di rete con gli accessi al *network-account*, facendoci anche intuire uno dei vantaggi che vedremo successivamente.



Nello schema possiamo vedere un esempio della struttura che potrebbe avere la nostra Organization. In questo esempio il *Network-Account* condividerà 3 subnet di ogni tipo con i vari account (produzione e non produzione). L'unica differenza che vediamo tra gli ambienti sarà il numero di Nat Gateway. Se per l'account di produzione sarà necessario avere almeno 2 NAT così da mantenere l'alta disponibilità, per quello di non produzione ne avremo soltanto uno, così da ridurre i costi.

Per ottimizzare ulteriormente i costi si potrebbe pensare di creare 3 NAT Gateway centralizzati che verranno utilizzati da tutti gli account al posto di averne uno dedicato per ogni ambiente non di produzione.

Queste configurazioni ci fanno capire che la soluzione risulta davvero versatile per adattarsi al meglio alla nostra idea di Landing Zone e di Business.

Dopo aver compreso l'impostazione che prenderà la nostra struttura di rete su AWS, sicuramente inizieremo a porci delle domande per quanto riguarda **sicurezza** e segregazione. Purtroppo la soluzione a singola VPC con AWS RAM non ci viene

particolarmente in contro in questo ambito, bensì ci costringe ad utilizzare Security group e Network ACL in maniera molto puntuale per evitare spiacevoli eventi.

Tratteremo le questioni inerenti alla security in un successivo articolo più tecnico e dettagliatto.

Approccio multi-VPC

Dopo esserci focalizzati sull'utilizzo di un unica VPC è doveroso capire anche quali altre possibilità ci vengono messe a disposizione da AWS.

Se prima avevamo una sola VPC per tutti gli account ora invece avremo almeno **una VPC per ogni account**. Un approccio di questo tipo viene chiamato multi-VPC e, come la sua controparte, ha pregi e difetti che non sempre lo rendono la soluzione perfetta per noi.

Quando parliamo di approcci multi-VPC la scelta molto spesso ricade sull'utilizzo di AWS Transit Gateway oppure del VPC Peering.

AWS Transit Gateway

Ormai sdoganato negli ultimi anni, l'utilizzo del Transit Gateway è lo "standard" per quanto riguarda la progettazione di una landing zone. (Abbiamo parlato di AWS Transit Gateway in maniera dettagliata in alcuni nostri articoli)

Per la realizzazione di un'infrastruttura che sfrutti il Transit Gateway avremo bisogno soltanto di: un Transit gateway, Transit Gateway Route table e Transit Gateway Attachment.

Il Transit Gateway possiamo immaginarlo come **un router virtuale che mette in comunicazione tutte le VPC della nostra Landing Zone in maniera semplice ed efficace**.

Anche per adottare questa soluzione avremo bisogno del cosiddetto network-account su cui riesiederà effettivamente il Transit Gateway. Essendo un approccio Multi-VPC ci serviranno anche almeno 2 VPC, una nell'account A e una nell'account B (anche il network account può avere la sua VPC). A differenza della soluzione proposta precedentemente, in questo caso tutte le VPC saranno indipendenti dal punto di vista della loro configurazione e gestione mentre solo il Transit Gateway in sé per sé sarà riservato agli amministratori di rete.

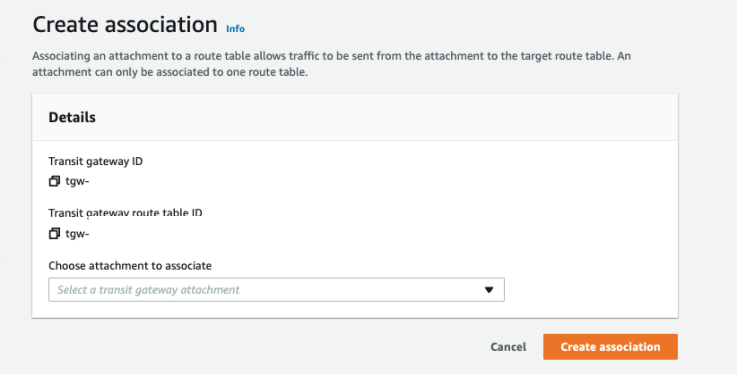
Ricordiamo che, dovendo utilizzare numerose VPC, dovremo evitare il più possibile di utilizzare CIDR sovrapposti tra di loro e soprattutto che vadano a coprire reindirizzamenti pubblici.

Per agganciare una delle nostre VPC al Transit Gateway dovremo creare un **Attachment** sia che questa VPC si trovi nel network-account o che si trovi in uno degli altri account della landing zone. Anche in questa occasione ci avvarremo del servizio AWS RAM per poter condividere il nostro Transit Gateway appena creato con uno o più account della nostra Landing Zone (ogni account avrà il proprio attachment). Una volta che avremo accettato la condivisione potremo procedere, dal nostro account A, con la creazione del nostro Transit Gateway attachment per poi collegarlo alla nostra VPC. **Così facendo avremo creato un collegamento "virtuale" tra la nostra VPC e il Transit Gateway centralizzato.** Se si desiderasse utilizzare l'Infrastructure-as-Code (IaC) potremmo automatizzare questi passaggi direttamente Tramite AWS CloudFormation.

Allo stato attuale avremmo una o più VPC che afferiscono allo stesso Transit Gateway, ma senza la possibilità di comunicare fra di loro.

Come ogni router, per gestire il percorso dei nostri pacchetti di rete, bisognerà **configurare le rotte** che nel nostro caso risiedono **nelle Transit Gateway Route Table**. In generale potremmo avere una routing table per ogni attachment così da poter meglio dividere le varie rotte e la segregazione delle VPC di account specifici e particolarmente critici.

Per agganciare una Route Table ad un Attachmen basterà creare un association direttamente dalla console di AWS specificando i vari ID richiesti.



Segregazione delle rotte

Purtroppo, come per ogni altra soluzione multi-VPC, anche questa avrà bisogno di molto effort a livello gestionale per assicurarsi che col proliferare delle VPC venga comunque mantenuto un buon isolamento a livello di sciruezza. Ricordiamo che, se pur dobbiamo mantenere un certo livello di sicurezza, dovremo anche permettere ai nostri applicativi di funzionare in maniera ottimale, senza andare ad impattare sui loro normali flussi operativi. Molto dell'effort, infatti, sarà da spendere nella configurazione precisa e puntuale delle rotte i ogni singola Routing Table. Una buona gestione di tutte le VPC afferenti al nostro Tranist

Gateway ci permetterà di essere tutelati anche qualora una delle nostre istanze venisse infettata da malintenzionati.

VPC Peering

L'approccio che meglio si contrappone a quello del Transit Gateway è quello di utilizzare i VPC Peering.

Il VPC Peering altro non è che un "ponte" virtuale creato per mettere in comunicazione due VPC diverse, sia che queste si trovino in un solo account, sia che siano dislocate in account differenti.

Di solito questo è un approccio che risulta valido quando si possiedono pochi account e non si vuole investire troppo effort nella gestione della rete.

Avendo le VPC collegate potremo anche utilizzare i security group che non appartengono alla VPC di cui siamo i proprietari, aiutandoci a rendere più sicura la nostra infrastruttura con regole ad hoc e ben mirate.

Ricordiamo che se referenziamo un security group di un altra VPC questo non ci comparirà come suggerimento direttamente dalla console ma dovremo inserirlo manualmente. Inoltre, nel caso in cui ci trovassimo cross-region non sarebbe possibile referenziare i security group delle varie VPC.
Una cosa molto importante da tenere a mente quando si utilizza il VPC peering è che quest'ultimo **non è transitivo**. Se abiliteremo il Peering tra la VPC-A e la VPC-B e successivamente tra la VPC-B e la VPC-C, la VPC-B potrà comunicare con tutte le altre VPC ma le altre VPC non potranno comunicare tra loro dato che la VPC-B non riesce a ruotare il traffico verso il "next hop".

Questo ci fa subito capire che il numero di peering che dovremo creare crescerà esponenzialmente mano a mano che creeremo nuove VPC.

Conclusione

Come spesso ci si sente dire, la risposta a quale approccio sia il più adatto alle nostre esigenze è "Dipende".

Tutto dipende da quale architettura abbiamo intenzione di adottare, quanto grande sarà la nostra organizzazione e soprattutto quanto effort saremo in grado di sostenere nella sola gestione della rete.

Ricordiamo sempre che una buona infrastruttura poggia le sue fondamenta su una rete ben progettata e scalabile, in grado di evolversi di pari passo con l'evoluzione e con la crescita della organization.

Per capire meglio vantaggi e svantaggi delle varie possibilità introdotte in questo articolo, entreremo nel dettaglio del loro utilizzo in un articolo dedicato. Prenderemo ad esempio alcuni degli use-case più comuni delineando una mappa di soluzioni a seconda dal caso.

Seguiteci dunque per non perdervi la seconda parte del nostro viaggio nella centralizzazione del networking in ambienti Cloud multi-account su AWS!

About Proud2beCloud

Proud2beCloud is a blog by beSharp, an Italian APN Premier Consulting Partner expert in designing, implementing, and managing complex Cloud infrastructures and advanced services on AWS. Before being writers, we are Cloud Experts working daily with AWS services since 2007. We are hungry readers, innovative builders, and gem-seekers. On Proud2beCloud, we regularly share our best AWS pro tips, configuration insights, in-depth news, tips&tricks, how-tos, and many other resources. Join the discussion!

Riccardo Fragnelli

DevOps @beSharp.Ho un passato on-prem prima di redimermi con il Cloud. Molto pignolo e abbastanza pigro. Mi piace passare il tempo fra videogiochi e GDR. Con AWS ho scoperto una branca dell'informatica tutta nuova che mi affascina sempre di più.
