Come semplificare la gestione del DNS in ambienti cloud ibridi

4 Febbraio 2022 - 7 min. read

Amazon Route 53 *DNS management* *Hybrid Cloud*

Il DNS è un servizio fondamentale che permette il funzionamento dell'intera rete Internet.

Lo sviluppo del primo server DNS risale al 1984, poco dopo la pubblicazione delle RFC 882 e 883 da parte dell'Internet Engineering Task Force nel Novembre del 1983.

Il compito principale di un server DNS è di facilitare la vita agli esseri umani, associando un indirizzo IP ad un nome. Negli anni si sono aggiunte feature di sicurezza e nuovi tipi di record per soddisfare le esigenze di un mondo in costante evoluzione ma il suo design non è cambiato molto dai primi tempi: da allora ha sempre svolto un servizio eccellente.

Nel cloud il DNS ricopre un ruolo chiave: sarebbe impossibile offrire servizi scalabili ed affidabili utilizzando solamente indirizzi IP. Aggiungere e togliere istanze spot da un load balancer o promuovere una standby replica RDS in caso di fallimento sarebbe complesso e richiederebbe un enorme quantità di tempo, specialmente se fatto durante un'emergenza.

Spesso i servizi interni on-premise necessitano di accesso ai servizi cloud e viceversa. Il nostro scopo è riuscire a soddisfare questa esigenza con il minor sforzo.

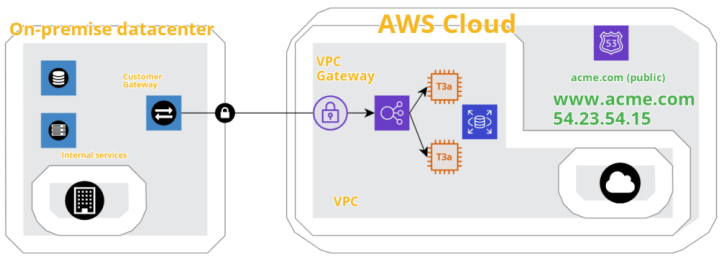
In un ambiente Cloud Ibrido utilizzare l'architettura che si adatta maggiormente al caso d'uso può aumentare l'affidabilità dei servizi e portare nel contempo anche a risparmi di tempo e di denaro.

È importante sapere che non esiste una soluzione migliore: in questo articolo prenderemo in esame alcune configurazioni DNS più comunemente utilizzate.

Per i nostri esempi esempi supporremo che applicazioni legacy siano ospitate nel datacenter on-prem del nostro business (ACME corp), mentre le applicazioni di cui è stato fatto refactor saranno ospitate nel Cloud AWS. Per l'interconnessione dei due ambienti supponiamo che sia stata configurata una connessione VPN.

Rimanete sintonizzati: nei prossimi articoli parleremo di come centralizzare e consolidare il networking in scenari complessi (Spoiler: si parlerà di Direct Connect e Transit Gateway !).

Utilizzeremo **Route53** per ospitare la zona pubblica ed il nostro dominio DNS sarà **acme.com**.



Ecco i tre possibili scenari che prenderemo in considerazione per il nostro business.

1. Usare solamente la zona pubblica

È possibile usare la zona acme.com per risolvere anche gli indirizzi IP interni, mantenendo in questo modo la gestione centralizzata.

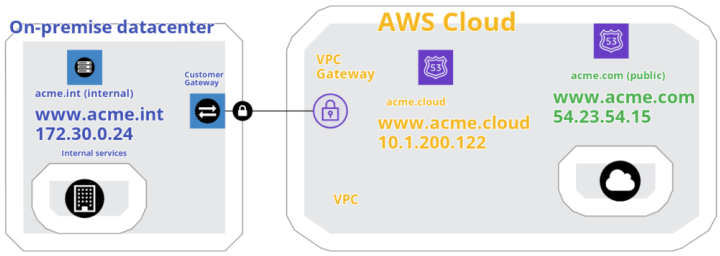
AWS usa questo metodo, ad esempio un'istanza RDS privata (test-instance-1) utilizza l'endpoint con nome test-instance-1.somerandomid.region.rds.amazonaws.com

Benefici: la gestione è centralizzata, non occorre mantenere server DNS aggiuntivi

Svantaggi: senza mantenere una nomenclatura standard si può generare confusione, ad esempio la versione di sviluppo del sito corporate può essere chiamata www-dev.acme.com o dev-www.acme.com da team differenti.

2. Usare lo stesso dominio in configurazione "split DNS"

Lo split DNS è una tecnica che permette di fornire valori diferenti quando una query DNS soddisfa alcuni criteri, come ad esempio la rete sorgente mediante l'uso di ACL (o views).
In questo modo è possibile che www.acme.com sia accessibile usando un ip privato dalla rete interna, mentre dall'esterno sia invece accessibile usando l'IP pubblico. Con le opportune restrizioni sul server web è possibile rendere acessibile solamente da rete interna l'interfaccia di amministrazione disito www.acme.com.

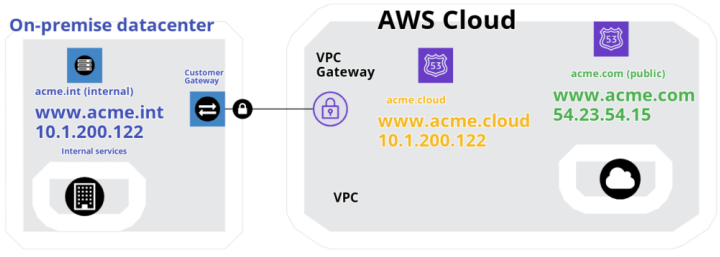


Benefici: la nomenclatura rimane consistente. Nel caso di spostamento di un servizio da on-premise al cloud non è necessario riconfigurare eventuali applicazioni dipendenti da esso.

Svantaggi: è facile dimenticare di aggiungere e mantenere record DNS in tutti i server coinvolti, portando a problemi applicativi inattesi (ad esempio alcuni servizi potrebbero risultare non disponibili o non configurati correttamente in alcuni ambienti).

3. Usare zone DNS differenti in ogni ambiente

Utilizzare nomi differenti aiuta a tenere traccia dell'ambiente in cui sono in esecuzione i servizi. Possiamo ad esempio usare *acme.int* per un ipotetico ambiente di sviluppo on-premise e *acme.cloud* per l'ambiente di test nel Cloud AWS.



È anche possibile usare sottodomini DNS, come ad esempio *acme.int* per l'ambiente di sviluppo e *cloud.acme.int* per l'ambiente di test.In questo caso è sufficiente creare un record di tipo NS nella zona acme.int che possa rendere autoritativo il DNS server della zona cloud.acme.int.

Benefici: è facile identificare l'ambiente in cui sono in esecuzione i servizi.

Svantaggi: aggiornare e spostare servizi nel cloud richiede modifiche applicative per riflettere l'ambiente di esecuzione.

Come risolvere zone private ospitate su Route53

È possibile associare una zona DNS privata su Route53 ad una o più VPC. AWS automaticamente fa in modo che le istanze EC2 ed i servizi possano risolvere i nomi delle zone private mediante l'utilizzo di un ip interno "magico", che si comporta come un server DNS privato: si tratta del terzo indirizzo riservato di ogni subnet. Ad esempio, se la subnet ha CIDR 192.168.0.0/24 l'ip riservato sarà 192.168.0.2, mentre per CIDR 192.168.0.16/28 sarà 192.168.0.18.

Questo indirizzo è utilizzabile solamente all'interno di una VPC e non è però raggiungibile mediante l'utilizzo di una connessione VPN o Direct Connect.

Vediamo quali servizi AWS possono aiutarci a risolvere questo problema. Ogni implementazione ha vantaggi e svantaggi, la scelta dello strumento migliore dipende solamente dai vostri requisiti di business ed usabilità.

1. Usare istanze EC2

Installando un server DNS (come ad esempio Bind, Microsoft DNS o Dnsmasq) su una coppia di istanze EC2 è possibile fare il forward delle query alla zona interna Route53 ed è possibile anche configurare il server DNS come *conditional forwarder* per i servizi on-premise.

Suggerimento: questa domanda è presente frequentemente negli esami di certificazione certificazione per la Advanced Networking Specialty.

.

Benefici: nel caso si abbia esperienza nella configurazione del server DNS si tratta di un task semplice e che può essere svolto in poco tempo.

Svantaggi: L'infrastruttura aggiuntiva va mantenuta, rendendo necessarie strategie di backup e di installazione degli aggiornamenti di sicurezza.

Costi: Assumendo che una coppia di istanze t3a.medium sia sufficiente per reggere il traffico, il costo mensile sarà di 44$.

2. Il nostro "piccolo hack: usare Simple AD

Il servizio Simple AD inoltra automaticamente le query DNS alle zone Route53 private. In questo modo, anche senza avere la necessità di utilizzare una directory gestita, è possibile utilizzare e configurare il servizio DNS dalle reti on-premise.

Benefici: Simple AD è un servizio totalmente gestito, quindi aggiornamento e alta disponibilità sono gestiti da AWS (ad esempio vengono automaticamente installati due domain controller)

Svantaggi: Essendo un servizio gestito non può avere un alto grado di personalizzazione (come ad esempio la redifinizione degli indirizzi host di Dnsmasq).

Costi: Il costo mensile di una istanza Simple AD (con HA multi-AZ disponibile di default) è di 36 $/mese.

3. Utilizzare gli endpoint Inbound ed Outbound di Route53 Resolver

Un endpoint inbound di Route53 mette a disposizione all'interno di una VPC una o più interfacce di rete con un indirizzo IP dedicato e raggiungibili da VPN, Direct Connect o un'altra VPC in peering, quindi anche dai server DNS presenti nelle reti on-premise. In scenari con topologie di rete complesse è la soluzione raccomandata e più facilmente gestibile per il lungo periodo.

Queste interfacce si occupano di fare da resolver DNS managed, facendo il forward delle query alle zone private.

Al contrario, se occorre inoltrare le richieste alla rete on-premise, sarà necessario un endpoint outbound, che creerà interfacce di rete in grado di comunicare con i DNS on-premise.

Benefici: si tratta di un servizio interamente gestito, configurabile totalmente usando la Console AWS.

Svantaggi: Costo alto.

Costi: Per una singola VPC sono necessari almeno due enpoint. La tariffa per delle query DNS è di 0,40$ per milione, per un costo minimo totale di 183$/mese.

Le tre configurazioni che abbiamo appena visto sono in grado di soddisfare la maggior parte delle implementazioni e possono essere utilizzate a piacimento: ad esempio è possibile usare sottodomini e delega DNS con un Inbound Endpoint di Route 53 Resolver, Simple AD per uno scnario di tipo split DNS o zone differenti installando un server DNS su istanze EC2.

Per concludere

Come sempre è necessario trovare un punto d'equilibrio fra la facilità di manutenzione ed i costi relativi ai servizi. Non esiste una implementazione perfetta e nemmeno la miglior pratica nell'assegnazione dei nomi DNS; si tratta anche di "gusto personale". Ad esempio in beSharp, spesso e volentieri, è possibile trovare colleghi impegnati in discussioni sull'utilizzo di Split DNS o delega di sottodomini, anche durante le pause caffè!

In uno scenario cloud ibrido è molto importante pianificare ed implementare l'architettura più appropriata, segliendo la soluzione che si adatta meglio all'ambiente e che non richieda di modificare radicalmente ciò che già esiste e funziona.

Quale architettura DNS state utilizzando ? Capita anche a voi di discutere con i colleghi sull'uso di delega, split DNS o zone differenti ? Fateci sapere nei commenti!

Damiano Giorgi

Ex sistemista on-prem, pigro e incline all'automazione di task noiosi. Alla ricerca costante di novità tecnologiche e quindi passato al cloud per trovare nuovi stimoli.L'unico hardware a cui mi dedico ora è quello del mio basso; se non mi trovate in ufficio o in sala prove provate al pub o in qualche aeroporto!

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.