Infrastrutture cloud ridondate geograficamente

Alta disponibilità sulla infrastruttura di Seeweb

Marco d'Itri
<md@seeweb.it>
@rfc1036

Seeweb s.r.l.

SMAU Milano 2016 - 25 ottobre 2016

Chi è Marco d'Itri?

- Usa Linux e Internet dal 1995.
- È uno sviluppatore Debian dal 1997.
- Dalla fine degli anni '90 si occupa in vari modi di Internet in Italia.
- Gli piace programmare in Perl.

Dal 2006 progetta e gestisce l'infrastruttura di rete, le piattaforme di posta ed altri servizi di Seeweb.

seeweb

Chi è Seeweb?

Il principale fornitore italiano di infrastruttura cloud

- 1998: fondata a Frosinone come hosting provider puro, dopo una esperienza come ISP.
- 2005: apre il secondo datacenter a Milano nel campus di Via Caldera.
- 2015: fonda Dominion Hosting Holding e la quota alla Borsa di Milano.

Ha 4 datacenter a Frosinone, Milano e Sesto San Giovanni.

seeweb

La rete di Seeweb

Un anello ridondato a 10 Gbps

- Datacenter Milano 1.
- Datacenter Frosinone 1 e 2.
- POP a Roma presso NAMEX.

Oltre 60 Gbps di connettività aggregata

- 40 Gbps di transiti a Milano e Roma.
- 10 Gbps di peering al MIX. Più NAMEX, AMS-IX e MINAP.
- 4 + 4 Gbps di peering privato con Telecom Italia (Milano e Roma).

seeweb

Il servizio

Abbiamo sviluppato un sistema di proxy e caching per uno dei più grandi portali italiani.
Il cliente richiede altissima disponibilità del servizio.

Più livelli di ridondanza

- Due datacenter.
- Ogni datacenter contiene due blade (in enclosure differenti).
- Ogni blade server contiene 4 macchine virtuali con i proxy.

Il portale è composto da più domini, distribuiti tra gli 8 proxy di ciascun datacenter.

seeweb

Alta disponibilità locale

In caso di guasto, il traffico è gestito dal proxy gemello nell'altro server.

Guasto di un proxy

keepalived monitora Varnish: se questo non funziona cede l'IP di servizio locale.

Guasto di un server

keepalived monitora il nodo gemello locale: se questo non funziona prende l'IP di servizio locale.

Ridondanza attivo-attivo

Ogni server gestisce parte del traffico del sito e in caso di guasto può gestire anche quello del gemello.

seeweb

Alta disponibilità geografica

In caso di guasto, il traffico è gestito dai server replicati nell'altro datacenter.

Guasto di un datacenter

I normali meccanismi di routing fanno in modo che gli utenti raggiungano solo i datacenter funzionanti.

Ridondanza attivo-attivo

Ogni datacenter gestisce il traffico degli utenti più vicini e in caso di guasto può gestire anche quelli dell'altro.

seeweb

L'architettura

Infrastruttura composta da prodotti standard di Seeweb

Prodotto	**Ruolo**
Web accelerator HA	Proxy e caching
Foundation server	Private cloud
IP failover	Routing anycast

Abbiamo creato un sistema di private cloud direttamente connesso ai nostri core router per isolarlo da possibili interferenze dovute ad altri clienti.

Prodotti: web accelerator

Appliance: servizio installato e gestito da Seeweb. Normalmente disponibile sulla nostra piattaforma di public cloud.

Varnish

Reverse proxy HTTP.

nginx

Terminatore TLS.

Valore aggiunto

Sistema proprietario di gestione, configurazione basata su moduli standard.

seeweb

Il web accelerator: perché?

Un sito senza caching non può reggere traffico significativo.

Se il visitatore arriva a PHP ormai è tardi per migliorare le prestazioni.

Facendo caching delle pagine intere il web accelerator permette di gestire traffico altissimo con poca spesa.

Variante istantanea

Può essere attivato in pochi minuti in condizioni di emergenza per gestire picchi di traffico improvvisi o attacchi DoS.

seeweb

Web accelerator: altre funzioni

Terminatore TLS avanzato

- Client integrato per Let's Encrypt.
- TLS moderno con OCSP stapling.
- HTTP/2!

Inoltre

- Load balancer.
- Router HTTP.
- Front end IPv6.
- TCP Fast Open.
- Configurazioni pronte per i CMS più comuni.

seeweb

Esempio: `blogseeweb.yaml`

```
backends:
  - host: 217.64.194.157

frontends: vm4635.cloud.seeweb.it

modules: [ ssl, selective_caching,↩
           wordpress, error_seeweb ]

variables:
  healthcheck_domain: blog.seeweb.it
  force_https_re: '^/'
```

Prodotti: foundation server

Raccomandato per costruire infrastrutture di private cloud.

Blade server dedicati al cliente

- 2 CPU da 16 core.
- 48 o 128 GB di RAM.
- Connettività 10GE.
- Storage su SAN Fibre Channel.
- Accesso alla console dal pannello Seeweb.

I foundation server: perché?

Evoluzione dei tradizionali server dedicati.

Storage su SAN Fibre Channel

- Altissime prestazioni.
- Possibile variare lo spazio allocato.
- Server stateless sostituibili via software in caso di guasto.

seeweb

Prodotti: IP failover

Sposta un IP da un datacenter all'altro con una API REST.

Il cliente può scegliere autonomamente se inviare il traffico ai propri server di Milano, Frosinone o entrambi.

seeweb

IP failover: modalità anycast

Routing anycast:

Annunciando al resto di Internet una route da più punti, il traffico viene ricevuto dal nodo topologicamente più vicino.

Approssimazione di routing geografico

Grazie alla nostra presenza a MIX e NAMEX possiamo ricevere con buona approssimazione a Milano il traffico proveniente dal nord Italia e a Frosinone quello dal centro-sud.

Domande?

https://www.linux.it/~md/text/cloudha-smau2016.pdf

(Google . . . Marco d'Itri . . . I feel lucky)

seeweb