IT BIMODALE/HYBRID E SICUREZZA

Giuseppe Paternò

Bimodale, hybrid-cloud o addirittura multi-cloud sono le diverse "sfacciettature" in cui l'IT si sta trasformando. E la sicurezza gioca un ruolo strategico.

Come consulente strategico in ambito OpenStack e private cloud, ho la fortuna di incontrare molti CIO e CEO di tutta Europa. Posso dire che. Ormai il cloud –che sia private o public- comincia ad essere "digerito" nelle aziende, ma spesso per la ragione sbagliata.

Molto spesso, infatti, è il **risparmio** il fattore trainante per cui vengo chiamato: l'obiettivo è di diminuire i costi di licenza di VMWare o trovare una forma di storage più conveniente rispetto alle SAN più tradizionali. Soprattutto in un mondo in cui i dati si moltiplicano a dismisura.

Mentre l'adozione di tecnologie come OpenStack sicuramente comportano un risparmio economico, il vero punto in cui c'è un maggior risparmio è nell'agilità di business e nello snellimento dei processi interni, che aiuta a snellire il quotidiano per potersi (finalmente) rifocalizzare sul vero core business dell'azienda.

E' questa la chiave per interpretare nella giusta maniera il cloud, ma **bisogna essere molto attenti all'aspetto sicurezza**, perche' in un ottica cloud/bimodale cambia radicalmente.

Vi faccio un esempio che non ammette interpretazioni. Un mio cliente bancario in Inghilterra per esempio impiegava 120 giorni per mettere a terra una singola virtual machine. In Italia le aziende spendono mediamente 60-80 giorni. Il motivo è presto detto: i processi interni sono così ingessati che per ogni operazione ci vuole un ticket. Basta sommare la creazione della virtual machine, l'installazione di sistemi operativi, la configurazione delle reti, compliance, sicurezza, l'installazione dell'applicativo e del relativo database e arriviamo facilmente a quei giorni.

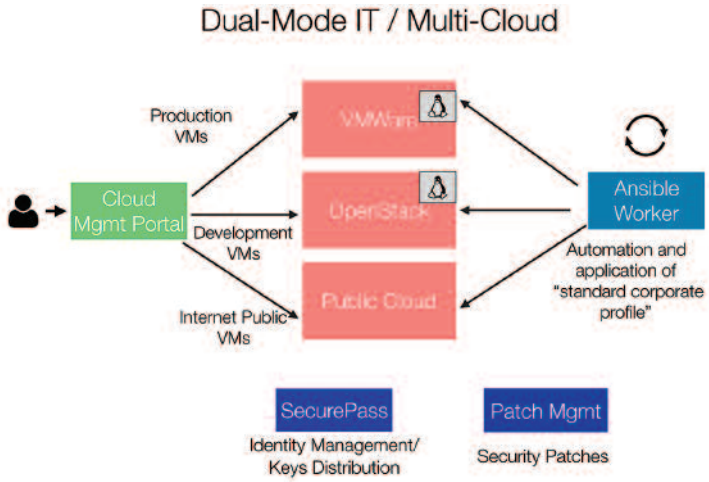
Una standardizzazione dell'infrastruttura porta numerosi vantaggi: l'accoppiata dell'uso di sistemi cloud e sistemi di automazione con tools quali Ansible, Puppet e Chef, per fare dei nomi ormai "industry standards"- aiuta a snellire e portare sia il provisioning che il change management, oltre all'integrazione automatica con il resto dei tools IT, mi vengono in mente ad esempio CMDB e monitoring. **La security e' quella che ne trae automaticamente vantaggio, perche' e' possibile anche fare "automatic compliance" dei sistemi**.

E' anche fuori discussione che possa essere fatto un cambiamento dall'oggi al domani. Quasi tutti i miei clienti mi chiedono di fare un "percorso" di cambiamento, che sia a lungo termine. Ecco che arriviamo a quello che viene chiamato "Dual-Mode IT" o "IT Bimodale", ovvero affiancare l'esistente con il nuovo.

Tipicamente quello che faccio con il mio team è partire dai sistemi di test e sviluppo, perche' non sono critici e quindi il cliente è più tranquillo nell'adottare nuove tecnologie, e man mano inserire nuove procedure "agili".

Vi faccio un esempio molto complesso di un mio cliente Italiano, tra l'altro molto conservativo, in cui Microsoft ha dato anche la possibilità di usare servizi Azure come parte del contratto.

Giuseppe Paternò, componente del Comitato Scientifico CSA Italy, è considerato da HP e dalla fondazione OpenStack **tra i migliori 30 consulenti al mondo in ambito Cloud**. La sua credibilità lo ha portato ad essere da Forrester Reserch nei loro report. Basato a Londra e a Zurigo, amministratore delegato di due aziende, la **GARL** e la **Alchemy Solutions**, è uno dei maggiori influencer del settore. Collabora con i più grandi brand mondiali come HP, Dell, RedHat, SuSE e RackSpace e i suoi clienti sono tra i più importanti dei settori telefonico e finanziario in Europa.



Tramite l'uso di un cloud management portal e di procedure di automation, possiede una zona di produzione interna su VMWare dove ha i workload tradizionali di "produzione" (tipicamente Oracle e SAP), una zona OpenStack interna dove fa test, sviluppo e produzione web "semplice", una parte su Azure dove ha i siti pubblici istituzionali in cui serve molta banda.

In questo scenario, in cui uniamo l'uso di un datacenter interno o esterno non "sposta" minimamente il modo in cui l'IT opera.

OpenStack e' nato già da subito affrontando le tematiche di disaster recovery e business continuity, che addirittura (se l'applicativo lo permette) è a praticamente zero downtime su ridondanza geografica. Meccanismi built-in di snapshotting geografico, di object storage e nuovi progetti come Freezer (backup dei dati interni alle VM) vanno proprio in quest'ottica, **rendendo la sicurezza del dato e la sicurezza di continuità del nostro business al centro del nostro IT**.

La sicurezza, così come la conosciamo oggi, però va rivista, e bisogna cambiarne l'approccio. Ci sono due livelli da tenere in considerazione. Il primo livello è quello della infrastruttura OpenStack stessa. In questa ottica è molto importante proteggere gli endpoint dei singoli servizi OpenStack da attacchi di tipo denial of service e da attacchi conosciuti con IPS e firewall che espongano solo le APIs della piattaforma. E' importante che questo tipo di protezione siano quasi wire-speed e reggano parecchio traffico.

Poi c'è da mettere la protezione a livello di tenant e di progetti che siano dentro la piattaforma OpenStack: andando sempre verso web services, è importante che questi tipi di tecnologie siano in grado di fare ispezione del traffico HTTP e HTTPS in modo da bloccare eventuali abusi all'applicativo stesso. In questo OpenStack offre un servizio di "firewall as a service" (FWaas), ma deve essere implementato da un vendor di sicurezza che sia in grado di affrontare queste tematiche. OpenStack, di base, offre comunque un firewall attraverso i security groups a protezione di ogni singola macchina, sia in traffico proveniente dall'esterno, che anche tra macchine nello stesso segmento di rete.

E' importante anche sottolineare che un ambiente "cloud oriented" la sicurezza va sempre implementata anche nell'applicativo, soprattutto se espone delle APIs pubbliche. Mentre in ambienti piu' tradizionali un firewall o il Deep Protocol Inspection (DPI) poteva bastare, ora e' importante segregare a livello applicativo l'accesso ai dati e fare audit di conseguenza. Inoltre, proprio in un'ottica cloud, e' importante anche che la resilienza sia spostata sempre di più nell'applicativo, come indicato anche dalle best practices del 12 factors (ref: http://12factor.net/).

E' indubbio che **i service provider e gli outsourcer** sono stati i primi che hanno capito che l'adozione di standard aperti e metodologie agili "DevOps" porta innumerevoli vantaggi, ma anche enterprises dalla piccola alla grande ne trarranno vantaggio sia in ambito di business che di sicurezza. ■