Cloud & Business

n.66
Ottobre 2017

LA RIVISTA PER IL MANAGER CHE DEVE OTTIMIZZARE COSTI E PROCESSI

IN QUESTO NUMERO

COVER STORY

K5, IL CLOUD FUJITSU PER LA DIGITAL TRANSFORMATION DI PMI E ENTERPRISE

Cloud Service K5 è la piattaforma di Fujitsu che permette di accelerare la trasformazione digitale di ambienti Legacy

La trasformazione digitale avanza, ma il problema per le aziende, sia PMI che Enterprise, è come e con chi attuarla. Il cloud è di certo un approccio che abilita la esternalizzazione delle complessità insite nella digital transformation e oltre a facilitare una rapida messa in produzione di nuove applicazioni permette di ottimizzare Capex e Opex; ma è un approccio che va adottato in base a reali esigenze dell'azienda, coniugando in modo ottimale l'IT Legacy esistente e quanto progressivamente fruibile o migrabile sul cloud, e soprattutto gestendo il tutto in modo univoco e integrato.

Rispondere ai bisogni delle aziende impegnate in questo percorso, affiancarle e supportarle nella trasformazione digitale è quello che si è proposta di fare Fujitsu tramite la sua infrastruttura Fujitsu Cloud Service K5, un servizio cloud erogato tramite una rete di data center di proprietà e basato sul sistema operativo aperto OpenStack, ideato per le imprese e in grado di consentire sia la trasformazione degli ambienti

Reportec Cloud&Business - Numero 66 - Ottobre 2017 - Registrazione al tribunale n°574 del 5 Novembre 2010 -

Editore: Reportec Srl (www.reportec.it) - Direttore responsabile: Giuseppe Saccardi - In redazione: Gaetano Di Blasio - Grafica: Paola Saccardi - Immagini: Dreamstime.com

tradizionali di IT aziendale che la loro integrazione con applicazioni ospitabili nel cloud.

K5, piattaforma aperta per applicazioni cloud native

Cloud Service K5, che a sua volta costituisce un elemento fondamentale della piattaforma di orchestrazione Fujitsu Digital Business Platform MetaArc, mette a disposizione un insieme di tecnologie progettate al fine di consentire alle organizzazioni di sviluppare applicazioni cloud-native e continuare a fruire del valore delle installazioni tradizionali, integrando i due mondi nel cloud in modo coerente.

In sostanza, K5 permette alle aziende di modernizzare i propri ambienti IT, sfruttando il valore dei propri sistemi legacy e potendo contare sulle ampie potenzialità di MetaArc nel far leva su delivery e gestione multi-cloud automatiche, estese a tutte le piattaforme cloud più diffuse.

Cloud Service K5 è fruibile in quattro diversi modelli: public cloud, virtual private hosted, dedicated e dedicated on-premise.

Le diverse versioni si caratterizzano per una disponibilità del 99.99%, di SLA e di un servizio di assistenza di livello enterprise adatto a sostenere sistemi mission critical dal cloud.

K5 è erogato da data center di Fujitsu e operativo in Giappone, Regno Unito, Finlandia, Germania, Spagna, US.

In particolare, i data center attivi in Europa permettono di mantenere i dati all'interno dell'area comunitaria e di rispondere alle normative UE sulla protezione e riservatezza dei dati.

Oltre al servizio K5, compreso in MetaArc vi è anche la soluzione PRIMEFLEX Integrated Systems per le aziende che desiderano sviluppare un ambiente cloud come quello abilitato da K5 ma preferiscono per motivi strategici, di sicurezza o normativi, conservare ed elaborare i dati business sensibili all'interno dei propri data center.

MetaArc, la Business Platform per orchestrare Legacy e Cloud

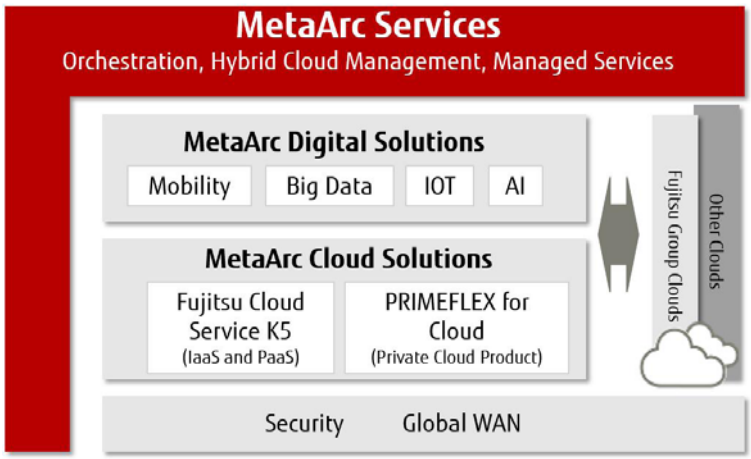
La Digital Business Platform MetaArc è una soluzione di orchestrazione delle risorse IT che permette alle aziende di digitalizzare le proprie attività e sfruttare tecnologie quali i Big Data, la mobility enterprise e l'IoT. Include le tecnologie, gli strumenti, i servizi e le partnership che occorrono per sviluppare un cloud strategico e aperto a diverse implementazioni, dal cloud pubblico al privato all'ibrido.

Il sistema supporta l'erogazione di ambienti Fast IT basati su cloud, solitamente conseguenti a iniziative intraprese da singole business unit e utilizzati in genere per esplorare e sfruttare soluzioni digitali innovative.

Allo stesso tempo supporta la modernizzazione di quelli che Fujitsu definisce sistemi di Robust IT e permette di monetizzare il valore insito nei sistemi Legacy, generalmente allocati in un data center on-premise oppure hosted, al fine di creare scenari IT ibridi.

Per supportare l'infrastruttura nell'evoluzione e nell'integrazione di sevizi legacy e cloud, e per-

mettere di farlo in modalità aperta, MetaArc supporta non solo le piattaforme cloud IaaS e PaaS della stessa Fujitsu, ma anche i servizi cloud di terze parti.
In questo modo, le aziende possono attingere facilmente a elementi chiave per la crescita come l'analisi dei dati, rendendo nel contempo mobili le applicazioni business e lo stesso ambiente aziendale.



K5, la strada semplice e flessibile per il cloud e la Smart Economy

Con l'offerta K5 di servizi e infrastrutture cloud, Fujitsu si propone di facilitare la digital transformation delle aziende e l'evoluzione verso una economia sempre più smart.
La migrazione al cloud richiede però - mette in guardia Bruno Sirletti, Presidente e AD di Fujitsu Italia - un approccio che sappia coniugare le soluzioni legacy esistenti con quanto di nuovo offre l'IT.
Se l'adozione del cloud è piuttosto facile per le nuove aziende nate con l'idea di sviluppare soluzioni cloud native, più complessa risulta essere la posizione di aziende come quelle di classe enterprise o grosse corporare con un IT consolidato. Per loro, anche se fortemente informatizzate, l'esigenza è quella di far coesistere quanto già presente (SAP, Mainframe, ecc.) e quanto rappresenta innovazione che,in quanto tale, deve essere inserita e integrata nei sistemi complessi e nei processi di business esistenti.


Bruno Sirletti, presidente e AD di Fujitsu

«Quello dell'integrazione e della coesistenza è uno dei compiti che si è assunta Fujitsu perché costruire una piattaforma digitale a partire da un green field è facile, fare in modo che si inserisca in un ambiente esistente è molto più complicato. Per questo abbiamo sviluppato una strategia che chiamiamo "Hybrid IT" che, da una parte, comprende il Cloud e una infrastruttura più moderna, e dall'altra è volta a supportare l'integrazione di queste infrastrutture moderne con SAP, mainframe e quanto esistente», ha evidenziato Bruno Sirletti, «Il nostro mestiere di base consiste nel gestire sistemi e infrastrutture IT. In questo caso l'approccio è un po' diverso: si tratta di abilitare la coesistenza della old e della new economy. Il Cloud è il passo fondamentale per andare verso la new economy, ma ciò non basta perché deve inserirsi nell'esistente: i nostri servizi di orchestrazione permettono la gestione legacy e cloud».

Una combinazione perfetta

FUJITSU Server PRIMERGY
e Windows Server 2016

FUJITSU

Microsoft

Windows Server: Power your business

Iperconvergenza, qualità e affidabilità: i Server PRIMERGY e Windows Server 2016 sono la perfetta combinazione per vincere le sfide del futuro. Cosa stai aspettando?

Info:

www.fujitsu.com/windowsserver2016
Numero verde: 800 466 820
customerinfo.point@ts.fujitsu.com
blog.it.fujitsu.com

shaping tomorrow with you

UCC COL VENTO IN POPPA CON I CENTRALINI 3CX

Con il software per UCC di 3CX e predisposto per il multi-tenant e il cloud è possibile comunicare ovunque sia su reti fisse che mobili e realizzare videoconferenze webRTC

Le comunicazioni unificate si confermano uno dei pilastri della trasformazione digitale e sono un forte abilitatore della proiezione di un'azienda sul mercato globale. Ma una soluzione di UCC deve rispondere adeguatamente ai principali paradigmi del mercato, e alle esigenze non solo del cliente finale che ne fruisce e le deve integrare nei suoi processi di business, ma anche del Canale e dei sui operatori, canale che la deve fornire, supportare ed adattare alle specifiche esigenze di settore o del singolo cliente.

Ma, mette in guardia **Loris Saretta**, regional sales manager per l'Italia e Malta di 3Cx, società specializzata nello sviluppo di centralini di UC software, un centralino di nuova generazione deve rispondere ai principali paradigmi del mercato in termini di mobilità, reperimento immediato del chiamato, comunicazione user frendly, sicurezza e fruizione su piattaforme il più possibile aperte, anche nel cloud, pur se in quest'ultimo caso deve essere posta estrema cura al come viene fatto.

Per favorire la digital transformation 3CX, ha evidenziato Saretta, ha adottato un approccio tecnologico e di commercializzazione che risponde alle esigenze del mercato, un mercato che richiede fondamentalmente soluzioni aperte e flessibili.

È una apertura e una flessibilità che nella vision strategica e di prodotto di 3CX inizia dal software. Il software che implementa le funzioni di centralino e di UCC di 3CX si basa sia su piattaforma Microsoft che Linux e dà la possibilità di supportare sia dispositivi fissi che mobili tramite connessioni di rete che supportano praticamente tutta la varietà di protocolli esistenti, a partire dall'IP e dallo standard SIP. Come software può poi girare su qualsiasi server standard di mercato ed essere allocato in server room, data center o stand alone.

Un'altra caratteristica che fa del software dei centralini 3CX una soluzione atta a favorire la digital transformation e la sua adozione come strumento per la modernizzazione delle comunicazioni delle PMI è di essere stato pensato in modo nativo per applicazioni multi-tenant e di conseguenza con la possibilità di essere fruito nel cloud e proposto dai partner di canale come servizio su cui costruire soluzioni a valore aggiunto o specializzate per servizi quali l'alberghiero, il sanitario o industriale.

«Costante attenzione dedichiamo al recepire le esigenze deli clienti, in modo da favorire l'attività propositiva dei partner. Ad esempio abbiamo attiva una diffusa Community che ci permette di recepire dai partner di canale le esigenze espresse dai loro clienti e quando le riteniamo significative o si tratta di richieste che ci sono segnalate da un certo numero di partner, le facciamo nostre e confluire negli sviluppi della nuova generazione di centralino», ha spiegato Saretta.

LA SICUREZZA DELLE RETI IOT È IL PUNTO CHIAVE DI UNA SOLUZIONE SMART

La trasformazione digitale e la diffusione di soluzioni IoT e Machine-to-Machine richiede sicurezza. Al come ottenerla ci ha pensato Barracuda Networks

Stefano Pinato - Barracuda Networks

Un tema correlato al cloud e che nel cloud trova un supporto atto a favorirne la diffusione è costituito dalle infrastrutture Smart atte a rendere semplice e dinamico il business. E' un tema che però si deve coniugare con la sicurezza, un problema che cresce soprattutto con il diffondersi di reti ad altissima velocità e di nuove classi di dispositivi personali o afferenti ad applicazioni IoT.

Nel complesso si tratta a breve di miliardi di oggetti intelligenti che generano informazioni, le utilizzano e le scambiano. E' una evoluzione tumultuosa che implica due aspetti di base, lo storage delle informazioni generate e la protezione dei dati sia quando sono in un repository che quando vengono scambiati in rete. In sostanza la domanda da porsi è: come posso proteggere i dispositivi IoT e soprattutto farlo in contesti anche molto diversi?

L'Internet of Things, osserva **Stefano Pinato**, country manager per l'Italia di Barracuda Networks, offre la possibilità di collezionare dati su larga scala e far su loro leva in una misura mai prima sperimentata e ciò crea enormi opportunità di business. Per la prima volta si prefigura una realtà in cui i dispositivi che verranno installati per applicazioni business potranno superare i numeri che di solito si riscontrano solo nel consumer. Dalla consegna di veicoli agli ATM, dai sistemi di condizionamento alle videocamere di protezione dell'ambiente e ad altre mille applicazioni, i numeri in gioco sono molto consistenti.

Il punto critico della Sicurezza

Tuttavia, evidenzia Pinato, persiste una forte barriera psicologica per questa diffusione, enfatizzata anche da cyber attacchi recenti, conseguenza del fatto che al momento gli strumenti che dovrebbero favorire l'adozione di dispositivi IoT e la loro fruizione sicura non appaiono adatti allo scopo. Il problema è enfatizzato dal fatto che dispositivi attaccati possono far parte di reti di erogazione dell'energia, dell'acqua, di sistemi di distribuzione del gas e quindi non si tratta di effrazione di dati, cosa pur grave, ma di possibili danni indotti nel campo del sociale o causare il blocco di interi settori industriali.

Ma c'è un'altra cosa che, osserva, preoccupa chi li ha in gestione quando si parla di oggetti IoT. Se in un dispositivo installato in decine di migliaia di esemplari (ad esempio i contatori del gas o della energia elettrica, semafori intelligenti o punti luce) si rivelasse una falla, come

si può intervenire rapidamente su tutti per porvi rimedio?
Prima di progettare e distribuire una rete di dispositivi IoT, suggerisce Pinato, una organizzazione dovrebbe analizzare come farlo, come gestirne il ciclo di vita, come intervenire se sorgono problemi e soprattutto come implementare politiche per renderli sicuri. Con una complessità aggiuntiva, aggiunge il manager: qualsiasi strumento progettato per fornire una sicurezza e una connettività scalabile per l'IoT deve condividerne le dimensioni ridotte, il basso costo, e la facilità di installazione. Non ultimo deve poter essere distribuito su larga scala e facile da gestire senza che sul territorio sia necessario uno stuolo di tecnici esperti.
La soluzione per IoT ideata da Barracuda Networks
Una soluzione per realizzare in modo sicuro la trasmissione e la raccolta dei dati generati da applicazioni IoT, nonché abilitare una interazione e una comunicazione protetta tra dispositivo intelligenti, è stata sviluppata da Barracuda Networks.
Alla base della sua vision c'è stata la considerazione che il semplice numero e la varietà dei dispositivi progressivamente on-line, conseguenza della diffusione dell'IoT, avrebbe offerto agli hacker e ai cyber criminali sponsorizzati anche da entità statali un ambiente aperto ad attacchi su larga scala estremamente profittevole. Con piccoli investimenti in sviluppi software, come già dimostrato dai fatti, si possono ottenere grandi profitti. La sfida che si sarebbe posta per le aziende sarebbe quindi stata quella di gestire e garantire la sicurezza del crescente numero di dispositivi remoti connessi tramite Internet.
L'analisi approfondita delle problematiche che le aziende avrebbero dovuto a breve termine affrontare, evidenzia Barracuda Networks, si è tradotta nella soluzione costituita da una nuova famiglia di dispositivi firewall di rete, NextGen Firewall F-Series, ideata appositamente per garantire la sicurezza di infrastrutture IoT distribuite.
Le caratteristiche dei dispositivi della F-Series, evidenzia l'azienda, vanno incontro alle necessità specifiche di una rete IoT: funzionalità atte a garantire una sicurezza elevate, un ridotto fattore di forma dei dispositivi di sicurezza, comunicazione criptata con robusti algoritmi di protezione, connettività cost-effective per ottimizzare contemporaneamente TCO, Capex e Opex. Per facilitare la gestione dei dispositivi, il management è integrabile in un centro di controllo in grado di supportare decine di migliaia di dispositivi remoti.
Robuste, come evidenziato, le funzioni sicurezza, che comprendono politiche basate su filtri, antivirus, sandboxing e anche la protezione da attacchi di tipo denial-of-service volti a bloccare una applicazione o una intera rete tramite un ammontare di messaggi contemporanei che la portano al collasso.
Fortemente automatizzata è anche la distribuzione degli aggiornamenti software. In ambienti IoT è possibile configurare i firewall mediante funzioni centralizzate basate su template predefiniti. Se si modifica un template perché cambiano le policy di sicurezza o le versioni software, i dispositivi connessi al centro di controllo vengono aggiornati automaticamente.

COME METTERE IN SICUREZZA L'AZIENDA CON G DATA

La sicurezza va affrontata come un processo riorganizzativo per proteggere il patrimonio informativo. Giulio Vada, di G Data, ne ha evidenziato le criticità

Giulio Vada, G Data Italia

Il mercato della sicurezza è forse l'unico settore dell'IT in costante crescita. I motivi è inutile elencarli e spaziano dalla crescita dei cyber attacchi all'apparire di nuove normative, da quelle che interessano la protezione dei dati personali come stabilito dal GDPR a quelle che hanno l'obiettivo di proteggere le reti su cui transitano le operazioni finanziarie come la rete SWIFT.

Non stupisce quindi che G Data, società tedesca che sviluppa soluzioni di sicurezza per reti e end-point, che commercializza in Italia tramite il Canale, veda, peraltro come altri operatori del settore, il futuro del mercato in modo positivo.

La positività del mercato per i fornitori di soluzioni di sicurezza non sempre corrisponde però a scelte corrette da parte delle aziende, soprattutto le PMI. **Giulio Vada**, Country Manager della società per l'Italia, mette in guardia contro approcci affrettati che possono portare a risultati ben lontani dalle aspettative e causare la perdita di dati che rappresentano un asset aziendale strategico.

«La sicurezza va affrontata come un percorso virtuoso che le aziende devono intraprendere in modo ponderato al fine di perseguire la compliance normativa. Va però posta attenzione al fatto che si tratta di un processo e non di un prodotto e in questo ci scontriamo con problemi culturali e realtà aziendali che evidenziano una scarsa conoscenza di quali siano e dove si trovino i dati sensibili e strategici per l'azienda, dove sono i dati dei clienti e a quali normative sono soggetti, o persino la documentazione riservata sui prodotti aziendali da cui il loro business dipende», evidenzia Vada.

Ci sono poi delle dinamiche del mercato come il cloud che, mette in guardia Vada, vanno affrontate e perseguite con cautela.

«Abbiamo una posizione attenta e critica allo stesso tempo nei confronti del cloud. Siamo focalizzati sulla protezione degli end-point e la nostra esperienza ci porta a suggerire un approccio misurato al cloud, soprattutto da parte delle PMI. Sovente una azienda di questo tipo si rivolge al cloud per esternalizzare una complessità, per dotarsi di una soluzione senza affrontare investimenti in conto capitale, ma se è una soluzione di comodo molto spesso si rivela una soluzione non adatta. Si ignorano ad esempio aspetti contrattualistici o i reali termini di un contratto, con i rischi connessi per quanto concerne riservatezza, garanzia di protezione, rispondenza alle normative, eccetera», mette in guardia Vada.

Se a livello di principio il ricorso al cloud, visto il basso livello di partenza, non può che contribuire ad aumentare il livello medio di protezione, quello che G Data suggerisce come strada praticabile e con il miglior rapporto prestazioni-rischi è quella del Cloud ibrido.

«Per supportare le aziende nel loro rivolgersi al Cloud abbiamo annunciato a SMAU la disponibilità della nostra offerta di servizi di sicurezza gestiti , in sostanza un modello di delivery che chiamiamo "Managed end-point security". E' una proposta importante per le aziende PMI e il canale e che allo stesso tempo ci permette di proporci come partner estremamente qualificati ai Managed Service Provider, un mercato che sino ad oggi non avevamo ancora indirizzato», ha spiegato Vada.

Mentre si opera per il presente e aiutare le aziende, gli operatori e il canale ad affrontare le criticità della trasformazione digitale, delle normative e del mercato, si deve però pensare al futuro, perlomeno quello prossimo.

«Oltre al Cloud, che ci vede fortemente impegnati con Microsoft e che ci ha visti impegnati assieme ad esempio anche in Germania per il lancio in una sua regione di Azure, un'altra linea di sviluppo su cui ci stiamo impegnando è quella dell'Intelligenza Artificiale. Già oggi le nostre soluzioni incorporano l'analisi comportamentale per l'individuazione di malware e altri tipi di attacchi. Ma ci muoveremo fortemente verso soluzioni basate sostanzialmente sul machine learning e l'AI, che sarà una delle nostre linee di sviluppo dell'immediato futuro», ha anticipato Vada.

Managed Endpoint Security: la sicurezza a consumo

Come accennato, G Data ha annunciato a SMAU una soluzione SaaS per la gestione del parco installato chiamata Managed Endpoint Security. In pratica, le aziende che non dispongono di uno staff dedicato alla sicurezza IT potranno affidare tale compito al proprio fornitore di servizi IT senza che lo stesso debba trovarsi presso l'azienda.

La piattaforma MES di G Data consente di gestire da remoto l'intero parco installato presso uno specifico cliente. Oltre a presentare tutte le funzioni centralizzate per la configurazione di policy e filtri applicabili a singoli client, gruppi o all'intera azienda, al deployment remoto di patch e al monitoraggio costante dello stato operativo dei sistemi, la soluzione assicura al fornitore di servizi IT e ai suoi clienti la trasparenza anche in merito ai costi.

IL NEXT GENERATION FIREWALL DI FORCEPOINT PROTEGGE IL CLOUD

Forcepoint Appliance di sicurezza serie 6200

Forcepoint ha annunciato la release di Next Generation FireWall basato sul concetto di Human Point direttamente nella rete e che protegge il cloud Azure e AWS

Forcepoint ha comunicato la disponibilità della nuova versione della soluzione Forcepoint Next Generation Firewall e ne ha illustrato le principali novità.

Focalizzata sulla Cybersecurity, la società si è posta l'obiettivo di approcciare il tema in un'ottica che integra a quanto già fatto nel passato una vision focalizzata sullo Human Point, ovverossia sulla protezione di quei luoghi virtuali dove utenti e dati vengono in contatto.

E' quello che si è proposta di concretizzare con il rilascio della nuova release del suo Next Generation Firewall 6.3, che dà visibilità direttamente a livello delle azioni operate dall'utente e permette di applicare le politiche di sicurezza ai NGFW virtuali anche su piattaforma Microsoft Azure, in modo da proteggere le applicazioni ed i servizi nel cloud. Nella soluzione, di cui seguono le principali novità, ha integrato anche gli aspetti salienti della sua tecnologia CASB (acronimo di Cloud Application Security Broker).

Endpoint Context Agent: Tramite l'installazione di un agente sugli endpoint presenti nella propria rete, è possibile ottenere informazioni sugli endpoint stessi ed utilizzare tali informazioni per regole di accesso direttamente nella SMC. Le informazioni vanno dallo stato dell'endpoint (come il sistema operativo ed i suoi aggiornamenti, lo stato dell'antivirus e del firewall locale), all'utente collegato al momento e alle applicazioni in uso

Cloud Application Discovery: I log del firewall possono essere utilizzati per avere visione delle applicazioni cloud utilizzate da ciascun utente e per valutare il rischio che ciascuna applicazione può comportare. La visibilità si basa sull'utilizzo della tecnologia CASB già citata e permette agli amministratori di un quadro esaustivo dei differenti profili di rischio.

Implementazione mista Layer2 – Layer3: E' possibile utilizzare la stessa appliance in due modalità differenti contemporaneamente. Ad esempio, si possono utilizzare alcune interfacce a Layer 2 (per ispezionare il traffico tramite il motore IPS) ed altre interfacce a Layer 3 (per utilizzare le funzionalità di firewalling avanzato).

Microsoft Azure e Hyper-V: E' possibile utilizzare NGFW virtuali per mettere in sicurezza le applicazioni su Microsoft Azure (in aggiunta al già supportato Amazon Web Services) così come su Hyper-V (in aggiunta al già supportato VMWare). Possono essere utilizzate le stesse policy, gli stessi report e le stesse viste utilizzate negli altri ambienti perché i NGFW sono gestiti centralmente.

Visibilità e controllo: Migliorate anche le funzioni di gestione e per quanto concerne lo stato dell'operatività delle appliance. E' possibile ad esempio personalizzare le dashboard scegliendo i widget di più significativo rilievo sia per ciascun componente che in modo aggregato.

IL CLOUD DI OVH SEMPRE ALWAYS-ON CON LA TECNOLOGIA VEEAM

Mehdi Bekkai - OVH

OVH garantisce la continuità di servizio nel cloud tramite l'integrazione nella sua infrastruttura di Veeam Cloud Connect per i backup dei dati aziendali

I dati parlano da soli: si stima che, a livello globale, il costo di violazioni e perdita di informazioni aziendali dovuto a malfunzionamenti software o hardware e furti di dati da parte di malintenzionati, potrebbero raggiungere i 2,1 miliardi di dollari già entro il 2019.

Per le aziende, quindi, la protezione e la disponibilità dei dati rappresentano un elemento economico cruciale al fine di garantire un rapido ripristino delle applicazioni critiche.

Quello della necessità di una robusta protezione è un approccio condiviso da OVH e Veeam Software, il cui obiettivo in fase di sviluppo delle soluzioni è quello di assicurare la continuità di servizio dei propri clienti.

Per garantire la protezione dei dati OVH ha fatto ricorso alla tecnologia Veeam Cloud Connect, con l'obiettivo dichiarato di fornire ai clienti una soluzione che permetta agli utenti di salvare facilmente i backup dei loro dati sulle sue infrastrutture. SI tratta in pratica di un'offerta volta a consentire alle aziende di consolidare la propria strategia di protezione dei dati con un backup in un sito remoto, senza la necessità di gestirlo ed esternalizzandone la complessità.

«La vision di Veeam sulla strategia di disponibilità dei dati e dei servizi è chiara e si basa sul modulo 3-2-1: tre copie di dati su due supporti, di cui uno remoto. L'infrastruttura di OVH consente di semplificare il backup remoto dei dati in un cloud sicuro, con una replica supplementare a livello infrastrutturale che costituisce l'elemento premium di questa soluzione. I clienti ne traggono un vero e proprio vantaggio», ha dichiarato Laurent Garcia, Cloud Senior Director di Veeam.

La progettazione della soluzione – disponibile inizialmente sulla piattaforma So you Start - si fonda sui feedback dei clienti e integra nativamente la crittografia end-to-end delle informazioni tramitea connessione SSL, la replica dei dati nel Cloud OVH e il WAN Accelerator per demoltiplicare il trasferimento dei dati. In linea con i principi del cloud la tariffazione si basata esclusivamente sulla quantità di storage utilizzata.

«Grazie alla partnership con Veeam offriamo una soluzione di backup esternalizzata in linea con le attese dalle aziende, che prevede una formula chiara e "all inclusive" e che semplifica le procedure per l'implementazione e la gestione della strategia di protezione dei dati. La stabilità della tecnologia Veeam, combinata alla qualità delle nostre infrastrutture Cloud, garantisce la ripresa delle attività aziendali», ha commentato **Mehdi Bekkai**, Product Manager Cloud di OVH.

IL CLOUD OF CLOUDS DI BT EVOLVE CON AWS DI AMAZON

BT e AWS si concentreranno sui servizi di networking, sicurezza e managed services per aumentare l'adozione del cloud da parte delle aziende

Bas Burger, CEO, Global Services di BT

BT ha annunciato una collaborazione strategica con Amazon Web Services (AWS), una mossa che è volta a rafforzare la sua posizione di leadership nei servizi cloud e ad aiutare le aziende a sfruttare meglio i benefici di AWS sia nel Regno Unito che nel resto del mondo.

L'annuncio rappresenta anche una tappa significativa nell'evoluzione della strategia di portfolio 'Cloud of Clouds' di BT, che fornisce connessioni sicure alle applicazioni e ai dati di cui necessitano. Va anche considerato che come Consulting Partner di AWS Partner Network, BT collega già numerose organizzazioni multinazionali al cloud di AWS.

L'annuncio di oggi sviluppa ulteriormente la collaborazione tra BT e AWS, che si concentra su networking, sicurezza e servizi cloud gestiti. In base all'accordo è previsto inoltre il lancio di nuove iniziative rivolte ai clienti, come l''hybrid cloud landing zone' di BT, oltre che attività di ricerca e innovazione in tema di evoluzione dei servizi di rete e un approccio integrato alla sicurezza nel cloud. L'obiettivo generale, ha osservato l'azienda, è di migliorare l'uso di AWS a livello globale per i clienti enterprise e consentire di accelerare l'adozione del cloud.

La hybrid cloud landing zone

La 'hybrid cloud landing zone' di BT è una proposta di mercato che comprende un insieme integrato di strumenti e modelli per dare vita a soluzioni cloud. Sarà costituita da progetti pronti all'uso per l'implementazione del cloud ibrido secondo le best practice, in diverse aree geografiche e diversi ambienti cloud, in particolare AWS. E' stata progettata per aiutare i clienti a gestire la complessità di ambienti cloud ibridi multipli, definire la rete virtuale tra più aree geografiche e mantenere i più alti livelli di sicurezza in ambienti hybrid cloud di grandi dimensioni.

I progetti predefiniti potranno far leva sulla dimensione globale della rete di BT, delle competenze in materia di sicurezza e delle funzionalità dei servizi gestiti così da dare ai clienti una maggiore visibilità e controllo di tutta la loro infrastruttura. BT utilizzerà componenti virtualizzati per implementare una connettività flessibile con sicurezza pre-embedded, allo scopo di consentire alle aziende clienti di avere una maggior velocità di deployment e ottimizzare le prestazioni complessive del cloudi. La fase di early adoption si aprirà nella prima metà del 2018.

Sicurezza integrata

BT e AWS collaboreranno anche su un approccio integrato alla sicurezza, per consentire di estendere al cloud i controlli di sicurezza esistenti, e supportarli in ambito compliance.

In proposito, BT creerà un catalogo di servizi di sicurezza di rete incorporati, anti-DDoS e threat intelligence disponibile sul Marketplace AWS.

In un prossimo futuro poi, i servizi includeranno anche identity e access management attraverso l'evoluzione dei servizi di sicurezza end-to-end. Sul tema BT ha già realizzato su AWS un case dedicato della sua Cyber Security Platform per un cliente multinazionale e sta lavorando a stretto contatto con AWS per farla diventare un'offerta standardizzata e replicabile per tutti i clienti.

Non ultimo, BT ha evidenziato che investirà ulteriormente sui servizi professionali per aiutare i clienti nel loro percorso di trasformazione digitale e nell'adozione di reti future, cloud ibrido e AWS.

«La nuova collaborazione strategica con AWS rappresenta una evoluzione molto importante per il Cloud of Clouds di BT. Insieme, BT e AWS hanno una posizione unica per aiutare i clienti in tutto il mondo a rimuovere la complessità dal loro percorso di trasformazione digitale. L'annuncio di oggi è solo l'inizio, e molto deve ancora venire», ha dichiarato **Bas Burger**, CEO, Global Services di BT.

Ma non è tutto per quella che si configura come una collaborazione a sempre più ampio orizzonte. BT e AWS collaboreranno anche all'evoluzione dei network services, sfruttando le tecnologie di rete emergenti per fornire nuove opzioni di connettività in linea con le esigenze dei clienti.

«Il cloud rappresenta ormai la norma e le organizzazioni di tutto il mondo stanno portando le loro applicazioni in AWS in modo da potersi concentrare su come offrire il meglio ai propri clienti. L'investimento e la competenza di BT nel cloud aiuteranno sempre più i clienti enterprise a sfruttare appieno le dimensioni, la sicurezza e l'agilità di AWS», ha dichiarato **Gavin Jackson**, UK Managing Director di AWS.

IL MERCATO CLOUD IN ITALIA SFIORA I 2 MILIARDI DI EURO

A trainare l'innovazione, i settori manifatturiero e bancario, seguiti da telco e media e utility oil&gas

Il mercato cloud in Italia continua il proprio processo di crescita: per il 2017 si stima un incremento del 18% negli ultimi 12 mesi, che lo porterà a raggiungere un valore di 1,978 miliardi di Euro. In relazione alla sola componente di Public & Hybrid Cloud - ovvero i servizi Cloud forniti da provider esterni (AWS, Google, Microsoft Azure e altri) e gli "ibridi" tra provider pubblici e privati - si stima che il mercato valga 978 milioni, in crescita del 24%.

Il ricorso al Virtual Private Cloud, ovvero l'esternalizzazione delle infrastrutture su porzioni dedicate di Cloud pubblico (che non rispondono quindi alla definizione tipica di Cloud), arriva a valere 520 Milioni di euro, con un tasso di crescita del 16%.

È quanto emerge dalla fotografia scattata dall'Osservatorio Cloud & ICT as a Service, giunto alla settima edizione e realizzata con il supporto di Alcatel Lucent Enterprise, Almaviva, Altran, Blueit, Cisco, Dedagroup, Fastweb, KPNQwest Italia, Vodafone; ASP Italia, Eteria, TWT, Wind Tre- La ricerca ha analizzato nel dettaglio l'evoluzione dell'offerta e i modelli di adozione di tale soluzione nelle aziende di grandi, medie e piccole dimensioni coinvolgendo oltre 1110 CIO e responsabili IT di imprese italiane.

La spesa in cloud per settore aziendale

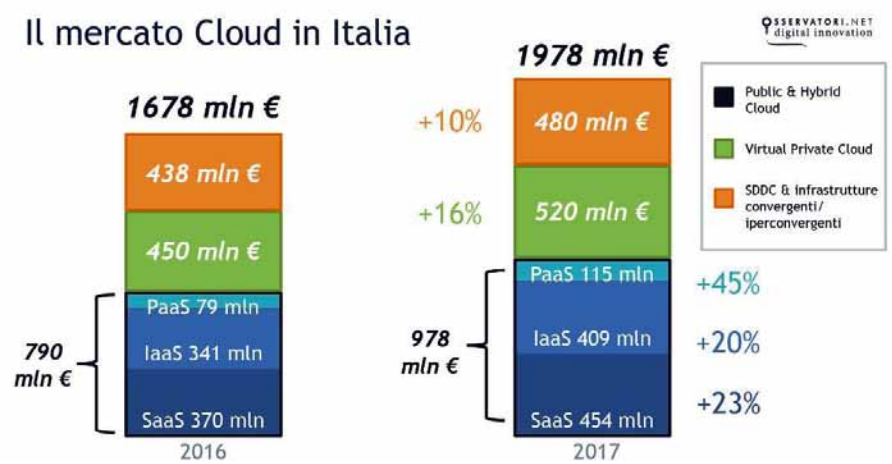
Il mercato del cloud è in salute, evidenzia la ricerca, e mostra tassi di crescita sostenuti in tutti i settori di impresa. Tra i settori più dinamici vi è il manifatturiero, interessato dalle evoluzioni relative al piano Industria 4.0, che hanno portato nuova spinta alla spesa in innovazione digitale. Il settore Telco e Media è caratterizzato da tassi di crescita sopra la media, in un percorso di progressivo arricchimento dell'offerta di servizi digitali e di allargamento a differenti canali di fruizione.

Anche nelle Utility/Oil & Gas la crescita del Cloud procede a ritmo sostenuto, con numerosi progetti strategici di Cloud Transformation.

Per quanto riguarda la Pubblica Amministrazione si attendono le implicazioni del nuovo piano triennale, che spinge in maniera decisa verso la razionalizzazione delle infrastrutture e i servizi in Cloud. Passando ad analizzare il mix di spesa nei diversi settori, il manifatturiero ha il peso maggiore (24%), seguito da bancario (20%), telco e media (15%), utility/ oil & gas (10%), altri servizi (10%). Completano il quadro PA e sanità (8%), grande distribuzione (8%) e assicurativo (5%).

Il grado di adozione

Con riferimento all'area geografica, il centro accelera rispetto allo scorso anno, divenendo l'area



con maggiore adozione, seguita da vicino da nord est e nord ovest. Il sud e le isole rimangono ancora attardati con una diffusione mediamente più bassa del 10%. L'intensità di spesa, misurata come percentuale della spesa IT dedicata al cloud, risulta, in continuità con lo scorso anno, più elevata nel nord ovest, seguita dal centro, dal nord est ed infine dal sud e isole. In conclusione, la crescita di spesa rispetto al 2016 risulta particolarmente robusta nelle aziende del centro, seguite dal nord ovest e dal sud, mentre nel nord est si assiste ad una fase di assestamento, con tassi di crescita più contenuti.

Per quanto riguarda le grandi aziende, il 41% del campione fa già ricorso a servizi IaaS e molto diffuse risultano le soluzioni di Virtual Private Cloud (utilizzate dal 55% del totale) che permettono di godere di alcuni benefici del Public Cloud mantenendo un maggior livello di isolamento rispetto agli altri utenti dello stesso servizio.

Gli investimenti nel cloud

Nell'anno in corso, mette in evidenza la ricerca, in Italia si è assistito a due principali atti di moto: da una parte il sostanziale consolidamento della parte di servizi applicativi fruiti in modalità SaaS, complice una diffusione massiccia sviluppata nel corso degli ultimi anni, dall'altra un arricchimento dell'utilizzo dei servizi infrastrutturali, che si stanno progressivamente spostando nella direzione delle piattaforme.

Le maggiori novità e i più alti tassi di crescita (+45%) riguardano i servizi di Piattaforma (PaaS): tra quelli più diffusi vi sono i database e data service ed i servizi a supporto dello sviluppo mobile e web. Ancora marginali, ma con trend di interesse superiore alla media, le funzionalità di abilitazione all'Artificial intelligence e ai Big Data Analytics.

I servizi applicativi (SaaS) consolidano la propria crescita (+23%) grazie all'ulteriore accelerazione nell'adozione di servizi di office automation e posta elettronica, arrivati a penetrare un'azienda su due nelle grandi organizzazioni, così come di servizi a supporto della gestione risorse umane ed e-learning (gestione documentale, firma elettronica). Un elemento di novità è la diffusione di servizi SaaS di Internet of Things (15%) e di artificial intelligence (10%), che pur mostrando un'adozione ancora limitata, sono caratterizzati da un interesse prospettico ben al di sopra della media.

Fra i servizi infrastrutturali (IaaS), nonostante il tasso di crescita più contenuto (+20%) si segnala un'ulteriore diffusione dei servizi rispetto al 2016, con l'ambito della continuity & disaster recovery in testa (20%) nelle intenzioni di investimento.

ENTER: UN APPROCCIO OPEN E AGNOSTICO AL BUSINESS CLOUD

Enter ha fatto di OpenStack il supporta per servizi cloud basati sul business. I benefici illustrati da Mariano Cunietti durante l'evento OpenStack Italy

Mariano Cunietti - Enter

L'arena dei fornitori di infrastrutture e servizi cloud è sempre più affollata. Ma non tutti i fornitori sono uguali e la differenza, mette in guardia **Mariano Cunietti**, CTO e Cloud & Hosting BU Manager di Enter, operatore e service provider con una propria rete paneuropea, la fa la infrastruttura software su cui i servizi si appoggiano e tramite la quale vengono erogati.

Il dato di fatto, evidenzia come punto di partenza nell'analisi delle considerazioni che hanno contribuito a definire la vision di Enter per il cloud, e illustrate nel corso dell'evento OpenStack Italy svolto proprio presso la sede di Enter a Milano, è che si tratta di un paradigma che sta evolvendo da un livello puramente infrastrutturale a qualcosa di diverso e più integrato con il business.

Il motivo di una tale evoluzione trova la sua genesi nel processo in atto che vede mettere sempre più automazione nei data center con il risultato che i software delle applicazioni possono parlare direttamente sia con altre applicazioni che con l'infrastruttura stessa. In questo l'evoluzione verso il Software Defined Data Center è stato un concreto aiuto.

Il risultato pratico e funzionale al business è che una applicazione può interagire direttamente con l'infrastruttura e autogestire le risorse che le servono liberando dal compito le risorse umane. Allo stesso tempo ne risulta una realtà meno complicata ma più complessa perché ciò apre la strada a un IT del tutto diverso e fortemente decentrato.

In sostanza, l'interazione diretta tra applicazioni e infrastruttura apre la strada al passare da una struttura generale dei sistemi da singola macchina monolitica e centralizzata ad una realtà distribuita costituita da numerosi e più piccole entità IT. «Il paradigma è passare dal grosso elemento che fa tutto a elementi molto più piccoli che svolgono compiti specifici, e che in quanto tali sono molto più facili da mantenere, con però il problema che sono tanti», osserva Cunietti.

Una vision per il cloud basata sulle esigenze del business

La velocità del cambiamento che va sotto il nome di digital transformation e i nuovi paradigmi che si susseguono, dal software defined all'IoT, alla virtualizzazione dei servizi di rete suggeriscono scelte precise e ponderate sia ai fornitori di servizi cloud che agli utilizzatori.

Una volta intrapresa una strada può essere diffi-

cile modificare la rotta, soprattutto se si è vincolati ad un hardware e a un software proprietario o limitatamente aperto.
«Per assicurare a noi stessi e di converso ai nostri clienti il massimo di indipendenza abbiamo scelto di sviluppare in house i nostri servizi cloud e di farlo basandoci su OpenStack, perché è la piattaforma software che assicura il massimo della indipendenza e garantisce un alto grado di portabilità di servizi e informazioni in un contesto molto ampio di fornitori di servizi cloud», ha evidenziato Cunietti.
La scelta di sviluppare quanto più possibile in house i servizi che propone è però solo una parte della vision di Enter volta a fornire al cliente il massimo di garanzia per quanto concerne la portabilità di applicazioni e servizi. Una seconda, non meno importante, è costituita dall'approccio che ha adottato nel confronto dei clienti, un approccio orientato non solo a soddisfare le necessità tecnologiche, comunque risolvibili, ma ad individuare il reale bisogno in relazione al business da perseguire.
«Quando incontriamo un cliente la prima cosa che facciamo è volta a recepire il suo reale bisogno, come possiamo aiutare a risolverlo e solo successivamente passiamo ad individuare gli strumenti e i servizi tecnologici che possono concretizzare la soluzione più adatta» spiega Cunietti.
Per supportare questa modalità di proposta centrata sui bisogni Enter ha sviluppato un insieme di servizi e tecnologie Cloud basate su OpenStack, un sistema operativo Cloud che ha oramai le medesime caratteristiche di Linux quanto a ampia accettazione, e che permette a Enter di costruirvi sopra infrastrutture molto liquide assemblando liberamente diverse componenti in grado nel loro complesso di rispondere in modo spinto e dinamico alle esigenze di business di una specifica azienda.
«È un approccio che in modo pragmatico abbiamo sviluppato andando "porta a porta" per recepire quali fossero i bisogni in termine di business, e che ci ha permesso di capire che i processi sono il punto centrale da affrontare e che sono i processi che devono essere stampati dentro il software. Il nostro lavoro è quindi centrato in primis sull'organizzazione dei processi e ciò ha incontrato ampio favore tra i nostri clienti. E' peraltro un approccio che vogliamo sviluppare e consolidare in modo che tramite i nostri partner possa essere proposto anche a chi non incontriamo direttamente», ha evidenziato Cunietti.
Non che tutto ciò sia stato facile, perché ha implicato un mutamento quasi genetico del convenzionale approccio adottato dai fornitori di servizi e infrastrutture.
«Quello che notiamo è che non parliamo più con il sistemista. Ora parliamo con il CTO, che non è l'IT manager che gestisce infrastruttura e relative problematiche, ma bensì la figura aziendale che determina la strategia. Ma non solo. Parliamo anche con il CEO che è lo stratega dell'azienda, e anche con il CFO, che ha la visione finanziaria. In sostanza, la mutazione quasi genetica che abbiamo intrapreso ci ha portato a parlare sempre meno di tecnologia e sempre più di processi di business. Ascoltiamo le necessità del business e identifichiamo, proponiamo e forniamo la soluzione più adatta», ha spiegato Cunietti.

SERVIZI APERTI O VENDOR LOCK-IN? LA SOLUZIONE NELLA OPEN CLOUD FOUNDATION

Cloud Foundation si è proposta di definire un quadro normativo per garantire la libertà delle scelte commerciali e contrastare vendor lock-in nel cloud

Il cloud è nato con l'obiettivo di esternalizzare la complessità dell'IT e favorire un utilizzo delle risorse centrato sul business e non viceversa. Implicita in questa evoluzione c'era l'intendimento da parte delle aziende di svincolarsi da legami vincolanti con fornitori di tecnologia, legami che se validi in un certo momento potevano finire con il costituire barriere all'evoluzione qualora le soluzioni fornite non vengano aggiornate con la dovuta rapidità o per quanto concerne le funzionalità.

Come sperimentato da molti non sempre questo assioma è stato rispettato e non sono stati pochi casi in cui il fornitore prescelto per servizi cloud ha finito con il prendere il posto del classico fornitore di tecnologie, con i medesimi problemi di lock-in.

Quello del lock-in è un problema molto sentito e che lo diventa sempre più con il diffondersi e l'accettazione dell'IT come servizio. In quanto tale, e dovendo rispondere a processi di business e sfide globali molto rapide, il settore impone ai fornitori di servizi una velocità di innovazione e industrializzazione finora mai sperimentata ma che contribuisce alla diffusione dei servizi IT in tutti i settori. E' facilmente prevedibile che il modello "as a service" che sottintende finirà con l'essere applicato alla quasi totalità di attività business, dall'infrastruttura ai livelli funzionali in un processo di esternalizzazione spinto sempre più in alto. «La chiave per erogare ai clienti il più alto livello possibile in termini di protezione dei dati, sicurezza e soddisfazione, è la condivisione di normative e standard che possono essere applicati, utilizzati e compresi da tutti. Continueremo a lavorare sull'apertura dell'ecosistema cloud affinché vengano abbattute le barriere tecnologiche e burocratiche», ha commentato **Stefano Cecconi**, CEO di Aruba.

Buona parte di dati, algoritmi, servizi e infrastrutture delle aziende che si rivolgono in toto o in parte al cloud per il loro IT, osserva la Open Cloud Foundation, sono o saranno ospitati presso i Cloud provider, cosa che sposta l'accento e il dibattito su temi che concernono la proprietà, il controllo, i segreti industriali, i vantaggi competitivi che abilitano se opportunamente fruiti.

Se da una parte cresce le aziende che si rivolgono al cloud, dall'altra si assiste per certi versi ad un processo inverso e cioè ad un consolidamento dei Cloud provider e all'emergere di realtà di grosse dimensioni che, come avvenuto agli albori dello sviluppo dei mainframe, hanno le dimensioni e l'impatto tale da portarli a cercare di imporre

Mark Collier -
Coo fondazione openstack

Stefano-Cecconi -
OPen Cloud Foundation

norme se non de jure perlomeno de facto, norme che potenzialmente o praticamente limitano il grado di libertà del mercato e con possibili impatti negativi anche sulla semplicità di utilizzo dei servizi, ad esempio in chiave ibrida.
E' un vincolo difficilmente accettabile dalle aziende, che in un mercato estremamente competitivo, desiderano essere del tutto libere di elaborare le proprie strategie d'impresa combinando le soluzioni offerte dai vari provider e integrando i diversi servizi a quelli già implementati internamente nelle proprie strutture.

Obiettivo cloud aperto

Per garantire la crescita continua delle imprese quello che è ritenuto necessario è in sostanza un Cloud aperto che permetta agli utilizzatori di migrare dati ed applicazioni liberamente e senza vincoli. Permettere agli utilizzatori di cambiare fornitore e assicurare libero accesso alle funzionalità dei modelli Cloud offerti al mercato significa consentire anche agli emergenti di dare impulso all'innovazione e stimolare gli incumbent, limitandone quello che potrebbe diventare uno strapotere in grado di condizionare il mercato.
Quello di definire normative aperte è l'obiettivo che si è prefisso la Open Cloud Foundation, da raggiungere tramite la collaborazione dei suoi principali attori nella redazione di direttive che permettano una gestione pratica della non semplice problematica. Il gruppo di lavoro ha infatti il compito di identificare le norme necessarie e colmare le lacune esistenti. Le direttive saranno applicate a livello globale e dovranno, in un secondo tempo, adattarsi alla legislazione locale come quanto concerne la "portabilità dei dati" nel regolamento definito dalla Commissione europea.
«Gli standard aperti stimolano l'innovazione, l'interoperabilità e l'integrazione. Sono fondamentali per la missione del progetto OpenStack e la collaborazione tra Community è la chiave per farne una realtà presso gli utenti. Siamo impazienti di collaborare con la Open Cloud Foundation per la progettazione e lo sviluppo del suo programma di lavoro per l'anno prossimo», ha dichiarato **Mark Collier**, COO della Fondazione OpenStack.
La fondazione per un cloud aperto non si preannuncia però come un sistema chiuso riservato ai fornitori di servizi, che in quanto tale finirebbe con il non recepire le esigenze delle aziende e le dinamiche del mercato. Il quadro di riferimento si baserà sui contributi che usciranno da una tavola rotonda che riunisce provider, clienti, organismi di ricerca e regolamentazione.
In un mercato in rapida evoluzione anche in questo caso la velocità è tutto. La Open Cloud Foundation verrà registrata ufficialmente e iniziare a operare già nel primo trimestre 2018., con un primo incontro preparatorio che si terrà a Parigi nel dicembre di quest'anno.
La disponibilità a lavorare in stretto contatto e a collaborare con la fondazione è stata espressa anche da OpenStack, che ha fatto dell'openess la propria vision.