Cloud & Business

n.72

Giugno-Luglio 2018

LA RIVISTA PER IL MANAGER CHE DEVE OTTIMIZZARE COSTI E PROCESSI

IN QUESTO NUMERO

COVER STORY

HYPER AVAILABILITY E CLOUD I PARADIGMI PER UN'AZIENDA A PROVA DI FUTURO

Il business nel cloud richiede soluzioni sempre attive e l'assoluta disponibilità e sicurezza dei dati

La diffusione di un IT basato su cloud o multi-cloud ha fatto emergere l'esigenza di modificare in profondità l'approccio adottato sino ad ora nella gestione del dato, passando da uno reattivo ad uno proattivo basato sull'intelligenza artificiale e su analytics.

Si tratta di realtà, sia che si parli di reti di sensori IoT inerenti infrastrutture di tipo sanitario, dei trasporti, di grid per l'erogazione di energia o per servizi pubblici, che richiedono di essere orchestrate e garantite sia per quanto concerne la loro disponibilità assoluta che per i tempi in cui rispondono in termine di latenza e velocità alle richieste di dati inoltrate. Ciò ha portato alla coniazione del nuovo termine di Hyper-Availability, che ha come obiettivo chiave quello di facilitare una orchestrazione dei dati pilotata dal comportamento delle applicazioni su infrastrut-

Reportec Cloud&Business - Numero 72 - Giugno-Luglio 2018 - Registrazione al tribunale n°574 del 5 Novembre 2010 - Tutti i marchi sono di proprietà delle relative società- Editore: Reportec Srl (www.reportec.it) - Direttore responsabile: Giuseppe Saccardi - In redazione: Gaetano Di Blasio - Grafica: Paola Saccardi - Immagini: Dreamstime.com

ture multi-cloud anche di grandi dimensioni.
«La Hyper-Availability è la nuova frontiera nel trattamento del dato e nella sua fruizione per il business. La Hyper-Availability Platform di Veeam, già utilizzata da numerose grandi aziende ed operatori mondiali e italiani è una soluzione completa di Intelligent Data Management che permette di sviluppare e fornire rapidamente e in modo sicuro servizi digitali innovativi on-premise e nel cloud», ha evidenziato Albert Zammar, Regional Vice President della Southern EMEA Region di Veeam.
La protezione e la gestione dei dati pensata come salvaguardia attraverso policy puramente reattive è in sostanza superata dai fatti e nella vision di Veeam si è concretizzata in un sistema che fornisce in modo proattivo valore di business.

Albert Zammar, Regional Vice President della Southern EMEA Region di Veeam

Cloud ibrido e multi-cloud sempre disponibili con Veeam Availability Suite

La vision per il cloud di Veeam trae la sua genesi dalla considerazione che nell'odierna economia digitale le aziende adottano una strategia multi-cloud per incrementare l'innovazione, accelerare il time-to-market ed ottimizzare i costi, tutti aspetti a cui Veeam ha inteso dare una risposta .
Per supportare le aziende nella esternalizzazione della complessità dell'IT basata sul Cloud la società ha inglobato nella sua soluzione Veeam Availability Suite un insieme di funzionalità che permettono di gestire in pratica la totalità dei dati aziendali e di assicurarne la disponibilità per tutti i carichi di lavoro possibili, virtuali, fisici o nel cloud, il tutto gestendoli da un pannello di controllo Veeam centralizzato.
In sostanza, con la sua soluzione, ha perseguito l'obiettivo di consentire alle aziende in fase di transizione al cloud di sostituire le soluzioni legacy di backup , business continuity e data recovery legacy, che rallentano la business transformation, con un approccio innovativo centrato sul cloud e che assicura la disponibilità dei dati tramite una singola piattaforma ad elevata affidabilità.
Le funzioni di gestione dei dati atte a garantire la "Always-on Availability" per i carichi di lavoro virtuali in ambito premise, comprendono anche il supporto multi-cloud per Microsoft Azure, Azure Stack, Amazon Web Services, IBM Cloud nonché applicazioni SaaS, ad esempio per quanto concerne il Backup su ambienti Office 365 di Microsoft.

Al sicuro i dati su Microsoft Office 365

Veeam Backup for Microsoft Office 365 è una funzione che aggiunge un nuovo supporto di scalabilità e multi-tenancy per le implementazioni aziendali e i provider di servizi che offrono servizi di backup gestiti da Office 365. Lanciata in ottobre con la versione, ha già raggiunto più di 25.000 aziende che lo stanno utilizzando, estendendo la protezione dei dati ad oltre 2,3 milioni di caselle postali Office 365.
La positiva accettazione da parte delle aziende trova spiegazione nel fatto che Veeam Backup for Microsoft Office 365 fornisce alle aziende varie opzioni aggiuntive per proteggere i loro

dati, oltre alla replica automatica dei dati che Microsoft fornisce nei suoi data center e ai controlli nativi di resilienza disponibili in Office 365. E una combinazione che consente alle aziende di mantenere un controllo completo dei propri dati nel cloud e garantirne la disponibilità ai propri utenti.

Veeam Backup for Microsoft Office 365 v1.5, ha evidenziato l'azienda, ha avuto una massiccia adozione da parte del mercato Enterprise grazie alle sue numerose funzioni per garantire la scalabilità e ad una architettura multi-repository e multi-tenant che consente di proteggere le implementazioni Office 365 di grandi aziende con un'unica installazione.

Servizi subito in produzione con Veeam DataLabs

L'impegno di Veeam nel cloud, come chiave per una digital transformation di successo e la salvaguardia dei dati, si è esteso sino a comprendere il ricorso all'intelligenza artificiale e a quanto necessita per avere una un'azienda always-on.

Per questo, oltre alla elevata disponibilità, entra in gioco anche il fattore tempo correlato ai processi produttivi e a cosa necessità a livello di dati per passare dalla formulazione di una idea al suo passaggio in produzione, sia che si tratti di un bene materiale che di un servizio immateriale.

Un aiuto concreto Veeam si è proposta di darlo con lo sviluppo della piattaforma per l'alta disponibilità Veeam DataLabs, una soluzione per la gestione delle copie di dati che permette alle aziende di creare rapidamente e on-demand nuove istanze dei propri ambienti di produzione.

La soluzione, ha spiegato Zammar, abilita casi d'uso che vanno oltre i classici scenari di protezione dei dati, come DevTest, DevOps e DevSecOps, e include test di sicurezza e di analisi forense e sandbox on-demand per le operations IT. In sostanza, rende disponibile un contesto per sperimentare e accelerare l'innovazione, migliorare l'efficienza operativa, ridurre i rischi e ottimizzare le risorse.

AUTOMATIZZARE LA RETE COMMERCIALE? PIÙ SEMPLICE CON AXIOMA CLOUD

Axioma Cloud CPQ automatizza la rete commerciale delle aziende e personalizza e semplifica i processi di configurazione, preventivo e offerta

Con la competizione sempre più globale e dove soddisfazione del cliente, rapidità di risposta, flessibilità e customizzazione sono i fattori chiave per aumentare il fatturato, un fattore chiave è disporre di soluzioni IT che permettano alla rete commerciale di automatizzare i processi di configurazione dell'offerta, preventivazione e gestione degli ordini, rendendo in sostanza il ciclo di vendita più veloce ed efficiente.

A renderlo possibile ci ha pensato Axioma, attiva da oltre 30 anni nello sviluppo di soluzioni software gestionali, nella fornitura di servizi professionali e nella consulenza.

Il fulcro della sua proposta per automatizzare la rete commerciale è Cloud CPQ, una soluzione ideata dalla società per le aziende che propongono prodotti e/o servizi da configurare, ovvero non presenti in un catalogo già definito ma che vanno a comporre un'offerta personalizzata in base alle specifiche esigenze e richieste del cliente.

Questo tipo di azienda, ha osservato Axioma, si trova spesso ad affrontare il problema di identificare la migliore offerta per il cliente tra le varie combinazioni possibili, consultando listini e cataloghi ed inserendo in seguito l'ordine manualmente, incrementando sensibilmente il margine di errore. Ciò comporta investimenti onerosi in termini di tempo e risorse e rischia di rallentare o addirittura compromettere l'esito della trattativa commerciale.

«Sempre più aziende oggi mettono al primo posto la soddisfazione del cliente, ecco perché è molto importante fornire risposte immediate e corrette, ma soprattutto in linea con le loro specifiche esigenze», ha commentato **Andrea Maserati**, Presidente di Axioma. «Grazie alla nostra soluzione CPQ, la forza vendita può configurare offerte più precise e senza errori ed i clienti ricevono esattamente quello che vogliono. Le aziende possono così elaborare preventivi più veloci, più accurati e trasformati in ordine in un semplice clic. Con questa soluzione ci rivolgiamo in particolar modo alle aziende che hanno l'esigenza di semplificare i processi e di essere supportate nell'attività di preventivazione poiché trattano prodotti complessi e con un numero elevato di varianti che vanno personalizzate in base alle richieste dai clienti».

Ai fini pratici, ha spiegato l'azienda, Cloud CPQ consente di ridurre sensibilmente i tempi configurando il prodotto o il pacchetto di servizi ed emettendo il preventivo direttamente insieme al cliente o inviandoglielo via e-mail: con la garanzia aggiuntiva che il prodotto sia effettivamente realizzabile in produzione o che il servizio sia erogabile dalle risorse aziendali e consentendo un passaggio diretto degli ordini nel sistema gestionale e di produzione.

CYBERARK AL TOP NELLA SICUREZZA DEVOPS

CyberArk Conjur è uno strumento open source di classe Enterprise che permette di far fronte alle esigenze di sicurezza di ambienti cloud nativi e DevOps

John Walsh, Community Manager & Evangelist di CyberArk

L'interesse che sempre più attraggono fa sì che i tool DevOps vengano rilasciati con crescente frequenza. Per districarsi tra le proposte XebiaLabs ha ideato la "Periodic Table of DevOps Tools", giunta alla sua versione 3, una sorta di equivalente della tavola degli elementi di liceale o universitaria memoria. Entrarvi a far parte è un eccellente riconoscimento per entrare nel mercato DevOps.

La "Periodic Table of DevOps Tools", osserva **John Walsh**, Community Manager & Evangelist di CyberArk, è un ottimo strumento di riferimento che aiuta i professionisti IT nel navigare tra le offerte di un mercato in forte espansione.

Nella tavola, CyberArk è stata posizionata di recente tra le società che sviluppano soluzioni per la Security DevOps, (elemento CK, numero 118), grossomodo laddove nella tavola di Mendeleev si trova invece l'elemento 101, il Mendelevio. Va osservato che CyberArk vi figura assieme a un numero ristrettissimo di una decina di altre aziende attive nella security DevOps con la sua soluzione di sicurezza CyberArk Conjur.

Si tratta di uno strumento open source di classe e posizionamento Enterprise, ha spiegato l'azienda, ideato espressamente per far fronte alle esigenze di sicurezza di ambienti cloud nativi e ambienti DevOps. La soluzione incorpora principi fondamentali per la sicurezza DevOps, come ad esempio quelli di "least privilege" e di "segregation of duties", riferentisi rispettivamente ai privilegi minimi e alla separazione dei compiti in modo da ridurre incidenti o frodi, e gestire e rendere sicuri dati riservati utilizzati da identità non umane, dai container ai microservizi, così come da utilizzatori umani lungo tutta la pipeline DevOps.

Il prodotto si integra con altri diffusi strumenti DevOps come ad esempio Ansible, Jenkins, Docker, Chef e Puppet, tutti tool che tramite Conjuar hanno la possibilità di accedere ed utilizzare le credenziali gestite da CyberArk Conjur.

Si integra anche, ha evidenziato la società, con le piattaforme Platform-as-a-Service leader di mercato, comprese tra queste Red Hat OpenShift, Kubernetes (K8S), Pivotal Cloud Foundry (PCF) e Cloud Foundry (CF).

«Con CyberArk Conjur, segreti e credenziali possono essere gestiti in modo consistente attraverso l'ambiente DevOps indipendentemente dalle capacità di loro gestione degli strumenti DevOps originali o della piattaforma, che può variare in modo anche molto significativa e non essere della classe Enterprise adatta. Ad esempio, alcuni tool non dispongono della rotazione delle credenziali o di funzioni di audit. Non ultimo, Conjur elimina le "isole di sicurezza" che si creano quando strumenti DevOps individuali non possono condividere segreti tra loro in modo sicuro», ha commentato Walsh.

CONTAINER PIÙ PROTETTI CON L'APP CONTAINER SECURITY

Una nuova cloud App di Qualys consente di monitorare la sicurezza dei container, partendo dall'interno dei cicli DevOps fino alle implementazioni applicative

Qualys, società che sviluppa soluzioni di sicurezza e compliance basate su cloud, ha annunciato Qualys Container Security (CS). La nuova cloud App, già disponibile, si propone di consentire le implementazioni di container globali e di processi DevOps con controlli continui sulla security, e di integrarne i risultati in una visualizzazione unificata dello stato di sicurezza e conformità dell'ambiente IT ibrido globale.

La App CS, integrata nella Qualys Cloud Platform, è una soluzione di sicurezza e compliance specifica per container che, ha spiegato l'azienda, estende la visibilità a questo tipo di ambienti, integrando la visibilità continua dei processi DevOps e dei flussi CI/CD con quella degli ambienti di virtualizzazione tradizionali.

la piattaforma esegue l'inventario ed il monitoraggio in tempo reale delle modifiche ai container distribuiti in ambienti on-premise ed elastic cloud, estendendo rilevamento di vulnerabilità e controlli di policy compliance ai registri delle immagini, ai container e agli host.

«La nostra nuova App Container Security è progettata per aiutare i clienti a estendere in modo trasparente le funzionalità di sicurezza continua e compliance ai nuovi flussi di lavoro cloud tramite l'uso di DevOps e container, integrando la security all'interno dei progetti di trasformazione digitale», ha commentato l'annuncio del rilascio Philippe Courtot, Presidente e CEO di Qualys.

Tra le caratteristiche salienti dell'App Qualys Container Security vi sono:

- **Visibilità dei container**: sono raccolte informazioni sui progetti con container (immagini, registri di immagini e container generati dalle immagini). Tramite dashboard dinamiche e personalizzabili gli utenti possono visualizzare l'intero inventario e lo stato di sicurezza dai container fino agli host.
- **Pipeline DevOps:** I team di sicurezza possono attivare policy per bloccare l'uso di copie che presentano particolari vulnerabilità oppure il cui livello di vulnerabilità supera una specifica soglia di criticità..
- **Minacce:** i team di sicurezza possono cercare immagini con vulnerabilità gravi, pacchetti non approvati e tag vecchi o di test.
- **Protezione runtime:** è possibile identificare le variazioni di configurazione e sicurezza in fase runtime che violano il comportamento codificato dell'immagine principale. Qualys CS usa anche una orchestrazione basata su policy al fine di impedire che i container con immagini vulnerabili vengano attivati nei cluster Kubernetes.

In sintesi, osserva Qualys, la Cloud Platform è una architettura per il consolidamento della security tra ambienti container e non, il cui obiettivo primario è di abilitare una drastica riduzione della complessità dell'IT.

LA SICUREZZA DELLA UCC IN RETE E NEL CLOUD INIZIA DAL TELEFONO IP

Nell'implementazione di una nuova piattaforma per le UC si deve valutare il livello di sicurezza garantito sia dalla soluzione sia dai terminali IP

Nelle aziende l'adozione di una piattaforma di Unified Communication (UC) integrata con l'infrastruttura IP, il cloud e le applicazioni di rete deve oramai necessariamente affrontare una ulteriore sfida: tutelare le conversazioni interne e esterne contro eventuali intercettazioni e proteggere lo scambio di dati tra la soluzione UC, i terminali e le applicazioni condivise, come i CRM.
Snom, produttore berlinese di telefoni IP da tavolo, cordless e da conferenza, ha identificato in proposito tre criteri discriminanti che un team aziendale dovrebbe esaminare prima di procedere all'adozione di una nuova soluzione completa per la telefonia via IP. Vediamoli in sintesi
Un primo punto chiave è Il "provisioning automatico", ossia il processo che consente alla soluzione di UC di distribuire con un click la configurazione e i parametri utente impostati ai più diversi terminali, un processo che deve essere sicuro e protetto.
Durante il processo, dati particolarmente sensibili vengono trasmessi attraverso un protocollo di trasporto sicuro (TLS/SSL). Ma questo può non bastare per proteggersi da attacchi del tipo "man in the middle". Per farlo, questo richiede che la soluzione UC e il terminale si scambino un certificato atto a garantire una corretta autenticazione del dispositivo nei confronti del server di telefonia.
Allo stesso tempo, osserva SNOM, è necessario che la trasmissione dei dati di utente dal centralino IP al terminale non sia intercettabile e/o che i dati non siano leggibili in chiaro. Una soluzione può consistere nell'autorizzare esclusivamente l'accesso di terminali IP alla rete previa autenticazione quale client.
Quanto discusso nel paragrafo precedente si basa su un assunto: che l'accesso al terminale sia protetto tramite una password robusta, che non necessariamente deve essere nota all'intero staff. Ciò implica che si debba valutare quali addetti possono avere accesso a quale telefono IP e se l'accesso debba essere granulare o meno (utente/admin).
Un aspetto chiave è la cifratura, che andrebbe applicata in modo esteso, a partire dall'invio di segnali tra le diverse connessioni e al trasferimento di dati vocali. Va però osservato che una cifratura totale d un sistema UC su base end-to-end che coinvolga le connessioni, i terminali, la rete e le applicazioni è più o meno inesistente nella telefonia business e il motivo risiede nel fatto che da un lato vi è l'obbligo di consentire eventuali intercettazioni su richiesta di un giudice, dall'altro vi è l'elevata complessità tecnica legata all'impiego di un sistema di cifratura "end-to-end".
In sostanza, se è richiesto un alto livello di sicurezza, spiega Snom, l'unico modo è implementare una VPN come è possibile con i telefoni IP Snom, o una rete MPLS.

AUTOMIUM, UN SERVIZIO SAAS CHE ABILITA LA CLOUD TRANSFORMATION

Il software di Continuous Deployment di Enter gestisce l'automazione dell'infrastruttura cloud e del deployment applicativo. Semplificata la gestione delle applicazioni

Le architetture a microservizi sono di fatto lo standard per le applicazioni cloud-native. Lo stile architetturale a microservizi è un approccio allo sviluppo di una singola applicazione come insieme di piccoli servizi, ciascuno dei quali viene eseguito da un proprio processo e comunica con un meccanismo snello, spesso una HTTP API. Le parole chiave di questo paradigma sono automazione, API, microservizi e sistemi distribuiti.

Automium, ha spiegato **Mariano Cunietti**, CTO di Enter, è stato ideato proprio con l'obiettivo di semplificare lo scenario complesso della gestione delle applicazioni e permettere alle aziende di intraprendere la cloud transformation con semplicità lasciando che sia Automium a gestire le complessità.

Si tratta, in particolare, di un servizio che fa parte di Enter Cloud Suite, un insieme di tecnologie open source che presiedono a tutta la filiera (dalla gestione del codice sorgente fino alla produzione), e che consente di fare DevOps fin da subito, fornendo gli strumenti per costruire la propria pipeline di continuous deployment.

È anche una piattaforma di automazione che consente di creare e gestire la propria infrastruttura cloud, e fruirne con facilità sin dal primo momento. In sostanza, può essere visto come un collante che rende accessibili le tecnologie open source di uso più diffuso e consolidato, come Terraform, Ansible, Docker, Kubernetes, Consul, Vault, Golang.

«Vogliamo portare gli utenti a fare un passo evolutivo, facendo loro comprendere che il design architetturale e la comprensione del processo produttivo di un'applicazione sono il loro vero business value, e non la tecnologia che lo concretizza. La tecnologia e la semantica di ogni tool sono il valore dei provider, non dei clienti», evidenzia Cunietti, «Il nostro business value è gestire questa complessità, selezionare (quindi scartare) e semplificare quello che secondo noi è più utile, e presentarlo ai clienti in modo che lo possano usare, senza bisogno di essere degli esperti del settore. Nascondiamo e riduciamo la complessità, senza limitare la libertà».

L'aspetto chiave della soluzione è che non serve più fare tutto a mano. Sia che si stia costruendo la propria nuova infrastruttura cloud o riprogettando quella esistente in ottica cloud, osserva Cunietti, Automium mette a disposizione i "mattoni" che servono, e permette di partire dal punto in cui ci si trova: si disegna quello che serve e sarà poi Automium ad automatizzare la costruzione e il deployment della infrastruttura direttamente su Enter Cloud Suite, la piattaforma cloud europea multi-region basata su OpenStack di Enter.

In linea con il concetto di "cloud portability" Automium è multi-cloud, e in quanto tale può funzionare anche su VMWare, AWS, GCP, Azure ed altri cloud, una apertura che evita il rischio di un lock-in su un fornitore se si dovesse cambiare strategia.

BT APRE LA STRADA ALLE FUTURE RETI ULTRA-SICURE

BT insieme ad alcuni importanti partner fa un salto "quantico" per lo sviluppo di reti future ultra-sicure

BT ha annunciato di aver realizzato la prima rete in fibra ottica ad alta velocità di massima sicurezza (quantum-secured) del Regno Unito che collega Cambridge ai BT Labs di Adastral Park. Il progetto è frutto della collaborazione con il Quantum Communications Hub, nell'ambito del UK Quantum Technologies Programme.

Formulata negli ultimi due anni dai ricercatori di BT, dell'Università di York e di Cambridge, la connessione "ultra-sicura", garantita dalle leggi della fisica, è stata realizzata come parte di un progetto cofinanziato dall'Engineering and Physical Sciences Research Council (EPSRC),e si collegherà al Cambridge Metropolitan QKD Network che sarà lanciato domani a Cambridge.

Il quantum-secured link corre attraverso una connessione in fibra standard mediante molteplici BT exchange per una distanza di 120 km.

Si tratta della prima implementazione di una rete ad alta velocità "reale" di sicurezza quantum-based nel Regno Unito. Il collegamento di rete, che è in grado di trasferire 500 Gbps di dati, esaminerà e ratificherà i casi d'uso per le tecnologie Quantum Key Distribution (QKD). Incluso in questo il modo in cui la tecnologia può essere implementata per garantire la sicurezza dell'infrastruttura critica nazionale, nonché per proteggere il trasferimento di dati critici, come informazioni mediche e finanziarie sensibili.

Un sistema teoricamente inattaccabile

Si ritiene che un collegamento quantistico sia virtualmente "non attaccabile" perché si basa sull'uso di singole particelle di luce (fotoni), per trasmettere "chiavi" di crittografia dei dati attraverso la fibra. Se la comunicazione dovesse essere intercettata, il mittente è in grado di rilevarlo e segnalare che il collegamento è stato manomesso e che i fotoni rubati non possono essere utilizzati come parte della chiave, rendendo così il flusso dei dati incomprensibile per l'hacker.

I partner utilizzano apparecchiature di ID Quantique per trasmettere la chiave di crittografia dei dati utilizzando un flusso di singoli fotoni attraverso la rete in fibra.

In parallelo, i dati crittografati attraversano la stessa fibra, alimentata da apparati attraverso reti ottiche ADVA. La fibra va dal Cambridge University Engineering Department's Centre for Photonic Systems attraverso le "stazioni di ripetizione" quantum a Bury St Edmunds e Newmarket prima di arrivare ai laboratori BT in meno di un millesimo di secondo. Il collegamento è frutto di un'iniziativa congiunta di BT con il Quantum Communications Hub, guidato dall'università di York - uno dei quattro hub del programma nazionale UK Quantum Technologies. L' Hub nasce dalla collaborazione tra otto università del Regno Unito, aziende private e stakeholder del settore pubblico che hanno interessi comuni nello sfruttamento della fisica quantistica per lo sviluppo di tecnologie e servizi di comunicazione sicuri.

DATA CENTER SEMPRE ONLINE CON SWITCH TOP OF RACK

Switch di aggregazione e top of the rack di Raisecom permettono di creare una connessione tra data center altamente ridondata e sicura

Il progresso della trasformazione digitale e la globalizzazione di clienti e risorse pone sempre più all'attenzione e al centro degli interessi dei CIO il problema di come garantire la continuità operativa e l'accessibilità a dati ed applicazioni allocate sui data center, nonché a come, tramite essi, assicurare un servizio di business continuity e di disaster recovery.

A facilitare la realizzazione di una rete per data center senza punti di guasto ci ha pensato Raisecom, le cui soluzioni sono distribuite in Italia da CIE Telematica, società di ingegneria specializzata nella progettazione, realizzazione e supporto di reti di accesso fisse e mobili.

La soluzione sviluppata da Raisecnm si basa su switch di aggregazione della categoria Top of the Rack (ToR) che sono già in uso in diversi grandi data center mondiali. La soluzione mette a disposizione apparati e link ridondati.

Un progetto di questo tipo richiede di base che ogni server sia connesso a due diversi switch e che ogni punto di aggregazione sia basato su un doppio switch in modo da assicurare la ridondanza per le connessioni.

Per soddisfare sia le esigenze di ridondanza che di capacità di gestione dei consistenti flussi di dati che afferiscono da/verso un data center e tra i centri ridondati, gli switch Raisecom si caratterizzano per una capacità complessiva di 176 Gbps e sono equipaggiati con 48 porte a 1 G e 4 porte a 10G per la funzione di ToR , mentre prevedono una capacità complessiva di 1,2 Tbps con 48 porte a 10G e 4/6 porte a 40G per applicazioni di ToR o di aggregazione.

Dal punto di vista topologico e di gestione gli switch, ha spiegato CIE Telematica, possono essere connessi in stack e funzionare come un unico switch virtuale multiporta. L'aggregazione in un unico switch virtuale permette di espandere anche fortemente la capacità e la configurazione in porte complessiva senza aggiungere complessità di gestione.

Ogni stack viene in sostanza ad essere costituito da uno switch che opera come master, da uno switch di backup e da più switch slave. Nel caso di guasto del master lo switch di backup entra in funzione automaticamente. L'affidabilità delle connessioni tra apparati è invece assicurata dalla connessione cross dei link tra gli switch.

Per rispondere alle esigenze dei data center, estremamente ridotto è il tempo di commutazione tra uno switch guasto e quello di backuo, che è inferiore ai 50 ms.

«Si tratta di architettura altamente scalabile e la commutazione a caldo tra switch in esercizio e di riserva in caso di guasto, o l'espandere l'architettura, non impatta sul servizio. Quando uno switch è aggiunto allo stack, quello master si aggiorna automaticamente prendendolo in carico», ha evidenziato **Lugi Meregalli**, general manager di CIE Telematica.