



LIBERA UNIVERSITÀ DI BOLZANO UNA RETE POTENZIATA. DAL SOFTWARE.



LA SFIDA

Una rete che deve gestire un traffico sempre maggiore, una serie di apparati hardware che non riesce più a soddisfare le esigenze operative e altri che sono ormai vicini al loro fine vita, una gestione del network che si fa sempre più complessa. Il team IT della Libera Università di Bolzano era a un bivio.

LA SOLUZIONE

L'Università ha deciso di abbandonare un modello di rete tradizionale per passare a una Software Defined Network con VMware NSX.

SOFTWARE E TECNOLOGIA

- VMware NSX
- vSphere 6

“Abbiamo deciso di abbandonare un modello di rete tradizionale per passare a una Software Defined Network implementando una soluzione VMware NSX sui 16 nodi del nostro cluster ESX”.

CRISTIANO CUMER,
SYSTEMS ENGINEER,
LIBERA UNIVERSITÀ DI BOLZANO

La Libera Università di Bolzano nasce nel 1997 per volontà della Provincia Autonoma. La caratteristica principale di questo ateneo è l'insegnamento trilingue in italiano, tedesco e inglese.

L'Università è composta da cinque Facoltà, Economia, Design e Arti, Scienze e Tecnologie Informatiche, Scienze della Formazione e Scienze e Tecnologia per un totale di 3500 studenti distribuiti sulle tre sedi di Bolzano, Bressanone e Brunico. L'Università di Bolzano è certificata ISO 27001 e il Censis le ha assegnato nel 2015 il primo posto fra i piccoli atenei non statali in Italia.

I servizi IT dell'Università vengono erogati da due datacenter. L'infrastruttura di calcolo è composta principalmente da due nodi Cisco UCS e storage EMC. A partire dal 2008 i sistemi informativi e i servizi IT dell'Università sono stati gradualmente virtualizzati con VMware ESX 3.5, raggiungendo negli ultimi anni una quota di oltre il 95% di virtualizzazione, con oltre 600 macchine virtuali in produzione. Più recentemente è stata avviata la migrazione di alcuni servizi su cloud, come la posta elettronica.

La scoperta del Software Defined Network

Nel 2014 la Libera Università di Bolzano si è trovata ad affrontare un upgrade dei firewall interni, che gestiscono il traffico fra le reti campus e i datacenter. L'introduzione di nuove tecnologie, come lo streaming di video e applicazioni, l'uso di big data e VDI hanno fatto sì che l'hardware esistente, limitato a 2 GBit, non fosse più in grado di soddisfare le esigenze operative. “Ci siamo trovati a gestire parte del traffico con i firewall esistenti e parte con ACL sui core switch perdendo così la visione unica del nostro traffico interno, spiega Cristiano Cumer, Systems Engineer. “Stavamo considerando un upgrade dell'hardware esistente quando un nostro partner ci ha consigliato di valutare VMware NSX come soluzione alternativa”. L'idea di una Software Defined Network è subito una rivelazione per Cumer e il suo team, soprattutto per la sua scalabilità. “I nostri data center erano già basati su tecnologia VMware”, precisa Cumer. “La semplicità di integrazione di NSX nella nostra infrastruttura ha rappresentato un fattore importante per la nostra scelta, oltre agli aspetti economici, considerando che la soluzione NSX si è rivelata meno costosa dell'upgrade dei firewall esistenti”.

“Abbiamo deciso di abbandonare un modello di rete tradizionale per passare a una Software Defined Network, implementando una soluzione NSX sui 16 nodi del nostro cluster ESX”, racconta Cumer. “Abbiamo prima creato un cluster di test per acquisire familiarità con la tecnologia e verificare che rispondesse alle nostre esigenze. Passata con successo e soddisfazione la fase di test abbiamo poi implementato NSX sulla struttura di produzione, portando a termine contemporaneamente anche l'upgrade di vSphere alla versione 6.

“Con VMware NSX non solo ci siamo risparmiati i costi di acquisizione di nuovo hardware ma l'integrazione con vSphere rende più facile creare e mantenere le configurazioni di rete.”

CRISTIANO CUMER,
SYSTEMS ENGINEER,
LIBERA UNIVERSITÀ DI BOLZANO

Dai firewall distribuiti alla semplificazione delle attività di amministrazione

Rispetto ad un approccio classico, uno dei vantaggi principali che Cumer e il suo team hanno rilevato in VMware NSX è il distributed firewall. “Il firewall distribuito permette di non avere un singolo punto dove tutto il traffico generato dalle macchine virtuali viene analizzato e che potrebbe trasformarsi in un eventuale collo di bottiglia”, spiega Cumer. Questa tecnologia distribuisce il carico su tutti gli host che compongono i cluster ESX. In questo modo il throughput dei firewall scala orizzontalmente con il crescere degli host in cluster. Questo per noi è un elemento molto importante che ci permette di gestire i flussi di dati che i nostri istituti di ricerca analizzano e generano e che in passato eravamo costretti a limitare”.

Dal punto di vista dell'amministratore dell'infrastruttura virtuale, la disponibilità di un unico punto di management e l'applicazione di regole di firewall tramite tag permette di essere più efficienti nel deployment di nuove macchine virtuali, facilitandone l'automazione. “Abbiamo ridotto drasticamente il tempo necessario per mettere on line nuove virtual machine, mantenendo livelli di sicurezza molto elevati. Inoltre l'Università ha potuto sostituire i propri sistemi di load balancing, che avevano completato il proprio ciclo di vita, con i sistemi di NSX. “Con NSX non solo ci siamo risparmiati i costi di acquisizione di nuovo hardware ma l'integrazione con vSphere rende più facile creare e mantenere le configurazioni di rete”, aggiunge Cumer.

Verso la microsegmentazione

In futuro Cumer e il team IT della Libera Università di Bolzano si aspettano di poter abbandonare il classico modello di segmentazione della rete tramite VLAN grazie alle policy di sicurezza che sono applicate alle singole macchine. Queste policy permetteranno al personale IT di concentrarsi non più sul dove creare le macchine virtuali ma sulle reali policy necessarie al loro funzionamento, delegandone, ove possibile, la gestione.

Uno degli aspetti più innovativi di VMware NSX è rappresentato dalle funzionalità di micro-segmentazione. “Questa tecnologia si rivela d'importanza decisiva in vista del progetto VDI-Horizon che stiamo ultimando per quella che noi chiamiamo “Classroom 2.0”, ovvero la virtualizzazione di tutti le aule PC della nostra Università”, conclude Cumer. “In questa applicazione la limitazione della segmentazione per VLAN si fa sentire particolarmente, complicando il design dei pool di desktop. Potendo invece sfruttare le informazioni che NSX ha rispetto alle macchine virtuali in esecuzione, è possibile creare con estrema flessibilità policy di sicurezza in base all'utente che sta utilizzando un desktop virtuale, semplificando la progettazione dei pool e della rete”.

Risultati e benefici

- Maggiore scalabilità nell'erogazione di risorse elaborative sempre maggiori sulla rete
- Semplificazione e maggiore efficienza nelle attività di gestione delle reti, pur ottenendo un livello di sicurezza maggiore che in passato
- Distribuzione efficiente del carico elaborativo su tutti gli host
- Riduzione drastica dei tempi di rilascio di nuove virtual machine
- Riduzione dei costi per quanto riguarda l'acquisizione di nuovo hardware

