Pianificare la trasformazione operativa con NSX

Best practice per casi d'uso reali

GUIDA

vmware®

Sommario

Introduzione

Questo white paper è destinato principalmente a dirigenti e responsabili di cloud, rete e sicurezza. È altresì utile per i responsabili e coloro che contribuiscono all'architettura, alla progettazione e alle operation e che partecipano alla trasformazione operativa della propria azienda tramite NSX.

La virtualizzazione della rete è un elemento importante per permettere alle aziende di migliorare la velocità, l'agilità e la sicurezza. I vantaggi che è possibile ottenere possono essere equivalenti o perfino superiori a quelli offerti dalla virtualizzazione del layer di elaborazione negli ultimi dieci anni. Per poter ottenere i vantaggi associati alla virtualizzazione della rete, le aziende devono valutare e applicare un piano operativo che tenga conto delle **persone**, dei **processi** e della **tecnologia**.

La collaborazione con i clienti NSX esistenti ha permesso a VMware di capire come inserire nella pratica la virtualizzazione della rete nell'ambiente di produzione. Questa conoscenza di prima mano di casi d'uso reali ci permette di offrire una guida dettagliata alla valutazione, alla distribuzione e all'operatività di NSX, una guida che può essere utilizzata come riferimento per le best practice da applicare alla propria situazione specifica.

Anche se questo documento propone numerose best practice, NSX può essere implementato con pochissime modifiche iniziali, indipendentemente dallo stato corrente dell'infrastruttura. Non è complicato inserire NSX nel proprio ambiente di produzione e i passi da compiere per avere successo sono chiari.

Questa guida si articola in tre sezioni principali, che illustrano le best practice e i punti di apprendimento principali per:

Persone

La virtualizzazione della rete offre le potenzialità per sbloccare i punti di forza dell'azienda e può realmente trasformare il modo di lavorare dell'organizzazione IT. Rappresenta inoltre un'innovazione che deve essere valutata con attenzione per assicurare chiarezza e allineamento a livello aziendale. La disponibilità di una struttura organizzativa agile, con team amalgamati in cui ruoli e responsabilità siano assegnati in modo chiaro, permetterà di ottenere risultati ottimali e valore per l'azienda e per il personale. Qui sono incluse informazioni e linee guida sulle strutture organizzative, il coinvolgimento interno e le strategie di comunicazione, nonché i ruoli e le responsabilità.

Processi

La virtualizzazione della rete crea opportunità straordinarie per aumentare la produttività tramite l'automazione dei processi manuali nel ciclo di vita delle applicazioni. Tramite la definizione di uno stato futuro ideale circa il provisioning, la gestione e il monitoraggio di applicazioni e servizi, sarà possibile eliminare processi e procedure esistenti non più necessari. VMware offre consigli su come pensare all'automazione, alla gestione dei processi e agli strumenti e presenta alcuni casi d'uso interessanti.

Tecnologia

Tra i principali vantaggi della virtualizzazione della rete vi è la separazione delle funzioni di rete e sicurezza dall'infrastruttura della rete fisica sottostante e la loro astrazione in un layer di virtualizzazione. Andando avanti, ciò permette di configurare e gestire al meglio l'infrastruttura. Forniremo linee guida sulle best practice per l'architettura, sull'implementazione incrementale dell'infrastruttura e sull'implementazione periodica di nuove funzionalità.

Ovviamente le best practice non sono prescrittive, né adatte a tutte le situazioni. Occorre scegliere quelle che si ritiene possano funzionare per la propria azienda sulla base delle caratteristiche, degli obiettivi e delle priorità che la definiscono. Non tentare un approccio troppo rivoluzionario, ma preferire di iniziare con un paio o solo alcune, aggiungendo le altre nel tempo.

Alcune aziende tendono ad adagiarsi sugli allori e si fermano in questo percorso prima di raggiungere prestazioni ottimali, pertanto limitano i successi che potrebbero invece ottenere. Tenere sempre in mente lo stato finale desiderato e lavorare per migliorare e raggiungerlo.

Persone

Il primo argomento di cui vogliamo occuparci sono le persone, ovvero l'azienda, i team e i singoli che compongono l'organizzazione IT e che sono responsabili della distribuzione e della gestione end-to-end di applicazioni e servizi e che, in ultima analisi, sono l'anello chiave per il successo dell'operatività della sicurezza e della virtualizzazione della rete.

Considerazioni iniziali sulla struttura aziendale

La virtualizzazione della rete e NSX non richiedono un tipo di struttura aziendale particolare, infatti la struttura ottimale dipende da fattori specifici alla propria azienda. NSX è stato implementato sia in aziende organizzate in sili sia in team cloud ben amalgamati e integrati, ma ovviamente esistono anche situazioni intermedie tra questi due estremi.

La struttura aziendale ideale dipende da diversi fattori. Quando si progetta la struttura, occorre considerare:

- Allineamento tra domini e discipline
- Maturità del flusso del valore
- Livello di leadership tecnica
- Esperienza e competenza del personale
- Esperienza e complessità operative
- Uso dell'outsourcing
- Quantità di infrastruttura e applicazioni
- Distribuzione in ambienti esistenti o in ambienti nuovi

Il nostro consiglio? Progettare una struttura con team amalgamati

L'esperienza ci ha insegnato che i team più produttivi sono strettamente interrelati, presentano un alto grado di collaborazione e sono autosufficienti. Questi team amalgamati hanno dimostrato di lavorare in modo più efficiente e rapido con circuiti di feedback condensati e amplificati e con più condivisione delle conoscenze e apprendimento continuo. Idealmente, il team si trova nello stesso luogo.

Abbiamo visto strutture organizzative di successo composte da team basati sul dominio (ad esempio, elaborazione, storage, rete e sicurezza) e basati sulla disciplina (ad esempio, architettura, sviluppo e integrazione, operation e assistenza). In entrambi i casi, i team sono responsabili dell'infrastruttura fisica e virtuale.

Con il trasferimento in continua crescita di infrastruttura e applicazioni dalla rete aziendale esistente al cloud, cambia anche l'allocazione del personale. Nel tempo, saranno più numerose le persone al lavoro sul cloud e meno numerose quelle che lavorano sulla rete aziendale esistente. È importante sviluppare un piano di comunicazione e formazione per aiutare l'azienda a capire e a prepararsi a questa evoluzione, nonché a cogliere nuove opportunità di crescita professionale. Altrettanto importante è comunicare che, indipendentemente dal fatto che una persona lavori sulla rete aziendale esistente o sul cloud, il suo contributo è essenziale al successo complessivo dell'azienda.

Allineamento con i parametri di successo condivisi

Un'altra importante considerazione per l'azienda è l'allineamento con una strategia condivisa che abbia obiettivi, misure e incentivi ben definiti. Il proprio team dovrebbe avere un approccio orientato ai servizi ed essere interamente responsabile dell'intero ciclo di vita della distribuzione dei servizi, dai requisiti aziendali al funzionamento e alla gestione di un carico di lavoro di produzione di alta qualità supportato da un accordo sui livelli di servizio.

Ogni team dovrebbe avere parametri di successo condivisi basati sui fattori che sono più importanti per l'azienda, come, ad esempio, il time-to-market, l'impatto sugli utili, il tempo di risposta del mercato, la velocità dell'innovazione e/o i vantaggi e la soddisfazione dei clienti. Gli obiettivi dovrebbero essere rivolti all'esterno, sull'attività e sugli utenti del servizio.

Consentire al team di sviluppare e monitorare i propri parametri di successo, assicurandosi che tali parametri siano rilevanti e in linea con gli obiettivi condivisi. Oltre all'allineamento agli obiettivi aziendali, i Key Performance Indicator dovrebbero essere specifici, chiari, quantificabili e misurabili. Qualsiasi essi siano, dovrebbero essere semplici e iniziare con alcune metriche di base intuitive e significative.

Dopo aver scelto i Key Performance Indicator, occorre confrontare e documentare la situazione attuale. Monitorare e valutare periodicamente i progressi, ad esempio su base mensile o trimestrale, verso il raggiungimento dello stato finale desiderato. Chiarire con il team che la valutazione non è finalizzata a criticare persone o prestazioni passate, bensì a dimostrare il successo del team e il nuovo valore che è in grado di offrire all'azienda. Queste misure possono inoltre essere utilizzate per rendere la revisione e la valutazione delle prestazioni più efficaci, tangibili e significative per il singolo.

Creazione di una cultura della responsabilità e del coinvolgimento

La cultura è importante per il successo con la sicurezza e la virtualizzazione della rete. È necessario avere una cultura che sostenga i principi di un Software-Defined Data Center. Piuttosto che imporre un cambiamento culturale a livello dirigenziale, cosa tra l'altro molto difficile, la cultura dovrebbe emergere in modo organico all'interno dei team tramite esperienze condivise, capacità e valori.

La definizione di parametri di successo condivisi permetterà la nascita di una nuova cultura, che si radicherà naturalmente. La nuova cultura si baserà su un obiettivo aziendale chiaro e incentrato sul cliente, su responsabilità e rischi condivisi, su collaborazione e cooperazione più strette e su fiducia e rispetto reciproci.

Il team: le competenze in materia di rete e sicurezza lavorano insieme

Tra i principali vantaggi della virtualizzazione della rete vi è la separazione delle funzioni di rete e sicurezza dall'infrastruttura della rete fisica sottostante e la loro astrazione in un layer di virtualizzazione. Questo cambiamento ha fatto porre alcune domande, come: “Quale team è responsabile della rete virtuale e della sicurezza nell'hypervisor?” e “In che modo la virtualizzazione della rete cambia le mie responsabilità?” Le risposte sono qui, in questa sezione.

Il personale esistente dedicato alle funzioni di rete e sicurezza si occuperà della virtualizzazione della rete e della sicurezza. NSX si basa su tecnologie e concetti della rete che richiedono competenze in ambito di rete. Solo i team addetti alla rete hanno le competenze necessarie. Gli esperti di rete e sicurezza sono necessari per progettare, distribuire e gestire le reti virtuali, così come lo sono per le reti fisiche.

La rete fisica non scompare, ma diventa più semplice e facile da gestire. Non è consigliabile creare un confine arbitrario per i team lungo le reti fisiche e logiche. Per ottimizzare la velocità e l'agilità, un team che includa architetti di rete, ingegneri e operatori dovrebbe essere responsabile del layer fisico sottostante e del layer virtuale sovrastante.

Tuttavia, è sempre possibile scegliere specialisti di rete dedicati al rack, allo stack e alla configurazione delle apparecchiature fisiche e altri dedicati al layer virtuale. Tutte queste persone dovrebbero comunque appartenere allo stesso team.

Le responsabilità funzionali della rete (ad esempio, architetti, ingegneri e operatori) si evolvono fino a includere la virtualizzazione della rete e la sicurezza. La maggior parte delle persone che si occupano di rete e sicurezza dovrà imparare qualcosa di nuovo per potenziare le proprie competenze e capacità. Con NSX, i servizi di rete vengono eseguiti nell'hypervisor. I professionisti della rete devono avere una qualche conoscenza della virtualizzazione del server e cosa significa per i servizi di rete logici.

Best practice per le persone: formazione

La priorità assoluta nelle fasi iniziali del processo di valutazione è assicurarsi che tutti capiscano i principi della virtualizzazione della rete e che vengano formati su NSX e sulle operation e gli strumenti di gestione correlati che fanno parte dell'ecosistema di cloud. VMware offre molti modi per farlo, inclusi Hands-on Lab, workshop e corsi. Queste risorse sono principalmente destinate ai professionisti della rete che non conoscono la virtualizzazione del server, ma sono adatte ai professionisti della virtualizzazione del server che desiderano acquisire informazioni sulla virtualizzazione della rete. È inoltre possibile implementare un programma per assicurare condivisione di conoscenze e formazione tra i team e all'interno di uno stesso team fornendo opportunità di leadership ai singoli per insegnare in modo informale le best practice ad altri team e gruppi.

Uno dei modi migliori per accelerare l'apprendimento è identificare e avviare un piccolo progetto pilota e una valutazione. Includere tutte le responsabilità funzionali necessarie (architettura, ingegneria e operatori) per l'elaborazione, lo storage, la rete e la sicurezza.

Iniziare con un piccolo team interfunzionale

Un'altra raccomandazione a basso rischio è di iniziare con un piccolo team interfunzionale nel percorso verso la virtualizzazione della rete. Se si è in grado di passare da team in sili a team amalgamati, procedere in modo graduale nel tempo. In generale, abbiamo visto due tipi di team interfunzionali ed è importante scegliere il modello più adatto alla propria situazione:

Team iniziale	Team avanzato
Se si è in grado di passare a un team amalgamato sul lungo periodo, utilizzare un team iniziale. Tale team diventerà infine un elemento permanente della struttura aziendale/dell'organigramma. Inoltre, destinare dei dipendenti a tempo pieno che trascorrano tutto il loro tempo con il team.	Se non si è in grado di passare a un team amalgamato sul lungo periodo, utilizzare un team avanzato. Il team avanzato può essere organizzato e sciolto secondo necessità. I membri lavorano nel team part-time e, formalmente, fanno capo a un altro team. I team avanzati vengono perlopiù utilizzati negli enti pubblici.

Il team interfunzionale ha di solito responsabilità end-to-end per un insieme di stack applicativi o uno stack applicativo specifico. Il team dovrebbe avere degli esperti in materia di elaborazione, storage, rete e sicurezza. Le capacità funzionali dovrebbero includere architettura, progettazione e operation. Il team deve essere in grado di gestire qualunque aspetto, dalla progettazione, sviluppo e testing alla distribuzione e alle operation di routine. Fare riferimento all'Appendice per le descrizioni dei ruoli e delle responsabilità per rete e sicurezza.

Scelta degli agenti del cambiamento per il primo team

È necessario scegliere i membri del team iniziale, che saranno agenti del cambiamento, esperti della materia, divulgatori e leader apprezzati. È opportuno trovare persone che tutti vogliano avere nel loro team, persone in grado di relazionarsi con gli altri, aprire percorsi di comunicazione e individuare e ridurre al minimo i punti di frizione. Persone capaci di stimolare gli altri a cambiare e che danno il buon esempio. Se i membri del team non si trovano nello stesso posto, fare in modo che si incontrino all'inizio del progetto per un paio di settimane.

I membri del team dovrebbero avere MBO personali allineati agli obiettivi del team. Ad esempio, se un membro del team trascorre il 50% del proprio tempo nel team iniziale, tale lavoro dovrebbe valere all'incirca il 50% del proprio MBO. Anche se potrebbe sembrare scontato, non è sempre così; si sono infatti verificati casi in cui il tempo trascorso in un team interfunzionale viene considerato più un hobby che non parte integrante del lavoro. È probabile che questo non sia il percorso giusto per il successo.

Best practice per le persone: evitare sorprese

Non sorprendere nessuno poco prima della distribuzione. Si sono verificate situazioni in cui persone addette alle attività di rete e sicurezza siano state coinvolte a processo già avviato, con conseguenti ritardi. Gli addetti alle operation devono sapere come monitorare, creare avvisi e risolvere i problemi relativi alla virtualizzazione della rete e alle modifiche di sicurezza, nonché in che modo processi e strumenti devono evolversi, aspetto che verrà discusso più avanti.

Festeggiare i successi e le opportunità di crescita

Quando il personale addetto a rete e sicurezza viene inserito nel progetto, spiegarne le implicazioni a livello personale e professionale. Con la virtualizzazione e l'automazione dell'infrastruttura, il personale avrà più tempo per lavorare su progetti nuovi e interessanti, potrà concentrarsi su iniziative strategiche capaci di dare più valore all'azienda. Ad esempio, piuttosto che svolgere il lavoro ordinario di configurare VLAN, unità di bilanciamento del carico o regole del firewall, potrà progettare nuovi servizi che danno valore all'attività, come l'automazione dei processi tra i domini, la progettazione per la resilienza, il capacity planning o altri progetti e iniziative interessanti.

Spiegare inoltre che chi propone soluzioni nuove e innovative potrà contribuire alla trasformazione di rete e sicurezza. I risultati saranno vantaggiosi per chi determina la trasformazioni, proprio come è accaduto a coloro che hanno colto l'opportunità e costruito la propria carriera sulle reti IP e, più di recente, sulla virtualizzazione del layer di elaborazione. In entrambi i casi, sono nate nuove schiere di amministratori con nuove capacità e conoscenze. Partecipare alla trasformazione permetterà alle persone di crescere professionalmente e ne accrescerà le opportunità e il valore nel mercato del lavoro.

Promozione del coinvolgimento attivo con gli utenti del servizio

Un altro modo positivo per promuovere il team è interagire con chi utilizza il servizio, ad esempio proprietari di applicazioni, aziende e infrastrutture, per informarli circa le nuove funzionalità. Richiederne la partecipazione attiva, i loro requisiti e il feedback. Vorranno capire come cambieranno le funzionalità e l'esperienza d'uso. Tra le varie attività di coinvolgimento di successo vi sono:

Punti di contatto periodici: organizzare workshop periodici durante i quali fornire aggiornamenti, conoscere requisiti e richiedere un feedback.

“Fatti e non solo parole”: definire e comunicare al team che esiste una cadenza periodica per lo sviluppo e il rilascio di nuove funzionalità, che aumenterà il coinvolgimento del cliente.

Comunicare i successi a livello aziendale è importante

Oltre a promuovere il progetto ai membri del team e agli utenti del servizio scelti, è anche utile informare del progetto le linee di business o l'intera azienda. L'obiettivo è creare una massa critica di persone che sostengono il progetto e rendere la piattaforma la modalità operativa standard. È utile condividere storie interessanti sull'attività e i risultati IT del progetto. È possibile effettuare questa promozione combinando presentazioni, discussioni, articoli, post di blog, social media, e-mail or dimostrazioni. Tutti nel team dovrebbero ritenersi promotori del progetto. Celebrare i successi, grandi o piccoli che siano, è quello che fanno le aziende altamente performanti e deve essere considerata una best practice importante nella gestione dei cambiamenti tecnologici.

Cambiare è difficile: trovare un intento comune

Tutti sappiamo che cambiare è difficile, soprattutto in aree e discipline dove i cambiamenti sono lenti o laddove il cambiamento può essere percepito come una potenziale minaccia a una carriera professionale o alla sopravvivenza. Questi fattori possono creare una certa resistenza ad andare avanti. Alcuni potrebbero addirittura ostacolare la trasformazione. L'approccio ottimale consiste nel cercare una comprensione condivisa del potenziale della virtualizzazione della rete tramite supporto e comunicazioni autentiche, nonché sostenendo i successi dell'azienda. Occorre essere trasparenti, aperti e pronti a domandarsi "Cosa ne guadagno? Cosa ne guadagniamo?" e a dare una risposta.

Processi

Questa sezione illustra l'impatto della virtualizzazione della rete sui processi operativi, descrive i passi da compiere per analizzare e comprendere i processi esistenti e offre dei suggerimenti su come far evolvere processi e strumenti per sfruttare appieno la sicurezza e la virtualizzazione della rete.

Inventario e analisi dei processi esistenti

Un'importante proposta di valore della virtualizzazione della rete è l'automazione dei processi solitamente manuali associati al ciclo di vita delle applicazioni. Ciò offre un'ottima opportunità per compiere una valutazione a tutto tondo dei processi esistenti per determinare come contribuiscono alla virtualizzazione della rete.

Suggerimento importante: non limitarsi a mantenere tutti i processi esistenti con la sicurezza e la virtualizzazione della rete NSX. Così facendo, infatti, si compromettono i vantaggi e i risparmi economici che sarebbe altrimenti possibile ottenere. Identificare e comprendere tutti i processi di rete e sicurezza esistenti. Comprendere l'impatto della virtualizzazione sui seguenti processi:

- Provisioning delle applicazioni
- Gestione della configurazione
- Gestione delle modifiche
- Gestione della capacità
- Gestione di incidenti e problemi

È bene comprendere come funzionano questi processi oggi, dall'inizio alla fine, e come possono essere semplificati e ottimizzati tramite automazione e orchestrazione. Si riscontrerà che i processi o le operazioni esistenti possono essere ottimizzati in modo significativo o perfino sconsigliati in alcuni casi.

Dopo aver realizzato un inventario dettagliato, è opportuno determinare le priorità per l'automazione di questi processi di rete e sicurezza. Per risultati immediati, concentrarsi sulle aree a più alto valore e che richiedono meno impegno. Non tentare di ottimizzare troppi processi nello stesso momento, ma sceglierne uno o due per iniziare.

Best practice per i processi: benchmarking

È importante fare un confronto prima di iniziare. Prima di cambiare qualcosa, analizzare e documentare quanto tempo richiedono attualmente i processi in uso; calcolare l'impegno in termini di attività e i cicli associati a ciascun processo; adottare queste stesse misure dopo aver automatizzato il processo; e infine confrontare e comunicare i risultati ottenuti. Comprendere le prestazioni aiuterà il team a raggiungere i suoi obiettivi, ad esempio ridurre il tempo del provisioning o il tempo per rilevare e isolare i problemi, e lo aiuterà a preparare accordi sui livelli di servizio adeguati per gli utenti.

Automazione del provisioning e della gestione

Dopo aver inventariato e valutato i processi attuali, il passo successivo consiste nell'analizzare la possibilità di automatizzare il provisioning e la gestione di applicazioni e servizi. Le aziende si servono di funzionalità di automazione intrinseche alla virtualizzazione della rete e a NSX per conseguire velocità, standardizzazione, coerenza e verificabilità. L'automazione riduce inoltre il downtime e rischi per la sicurezza associati agli errori di configurazione manuali. L'automazione migliora la produttività degli ambienti di sviluppo e test, rende più rapido il time-to-market per le nuove applicazioni, offre configurazioni standardizzate e coerenti e determina un minor numero di errori e risoluzioni più rapide.

Anche se NSX non richiede strumenti di automazione, la maggior parte dei clienti utilizza una combinazione di strumenti e API NSX per l'automazione del cloud. Questi strumenti e le API permettono di automatizzare il provisioning e la gestione dei servizi funzionali di NSX per le reti virtuali, ovvero switch logici L2, router L3, bilanciamento del carico, firewall e servizi perimetrali. La maggior parte delle aziende che utilizzano NSX automatizza più servizi.

La situazione tipica al giorno d'oggi è data da reti fisiche e VLAN il cui provisioning continua ad avvenire in modo manuale, su hardware specializzato, con tastiere e CLI. Di conseguenza, cambiamenti nella rete rientrano nel percorso critico per le distribuzioni delle applicazioni. Come noto, tali distribuzioni possono durare giorni, settimane o anche di più, fino a quando connettività della rete, prestazioni, disponibilità e sicurezza non sono pronti.

Procedendo con NSX, invece, le aziende possono automatizzare il provisioning, la configurazione, la gestione e la dismissione della virtualizzazione e della sicurezza della rete. Con NSX, i team di rete non devono configurare gli innumerevoli switch fisici con direzione del traffico e configurazioni di rete, quali VLAN, VRF, VDC, QoS, ACL e altri ancora.

Al termine della configurazione iniziale della rete fisica come rete sottostante, le frequenti e continue riconfigurazioni con distribuzioni di nuove applicazioni o modifiche dei requisiti delle applicazioni non sono più necessarie. Tutte queste modifiche ora avvengono nello spazio della rete logica tramite gli strumenti di automazione.

Best practice per i processi: attenzione sull'automazione IT

Si consiglia di iniziare dall'automazione per l'IT, per permettergli di soddisfare le richieste di servizi più velocemente. Una volta completata l'automazione dell'IT, è possibile aggiungere un portale self-service e un catalogo di servizi per sviluppatori di applicazioni e tecnici del controllo qualità per accedere ad ambienti completi con un clic. Ora esaminiamo alcuni degli strumenti di automazione utilizzati dai clienti NSX.

Considerazioni sugli strumenti

Come detto in precedenza, è importante innanzitutto identificare, comprendere e documentare le attività e i processi che si desidera rendere automatici. Questo è un passaggio fondamentale, poiché gli strumenti di automazione IT, come le Cloud Management Platform e gli orchestrator, offrono funzionalità diverse. Tutti questi strumenti richiedono un qualche investimento iniziale per l'apprendimento e la configurazione, ma i vantaggi che ne conseguono ripagano della spesa.

È possibile scegliere vRealize Suite e OpenStack per il provisioning, la gestione e l'orchestrazione dell'infrastruttura di rete. Per iniziare, è sufficiente automatizzare le singole attività per acquisire familiarità con lo strumento. Dopodiché, è possibile passare ai workflow, dove l'applicazione e i relativi servizi di rete e sicurezza vengono distribuiti e gestiti in uno stack completo. L'operatore della rete o l'operatore della rete cloud dovrebbe essere coinvolto nella valutazione e nell'utilizzo di tutti gli strumenti che consentono l'automazione della rete.

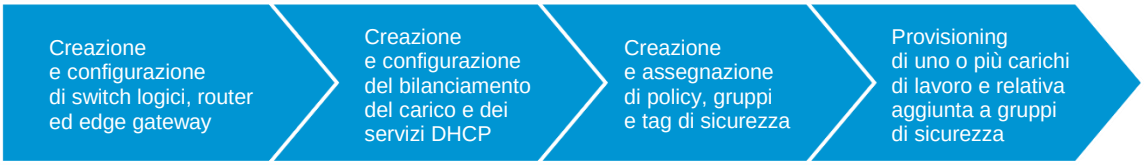
Standardizzazione e personalizzazione delle configurazioni

Le aziende possono standardizzare le configurazioni di elaborazione, storage, rete e sicurezza di interi stack applicativi utilizzando template e policy. Qualora fosse necessaria una modifica, modificano il template e lo inviano in produzione. Per tutti i carichi di lavoro che utilizzano il template, la modifica verrà applicata automaticamente. Viene conservato un record di tutte le modifiche per finalità di audit e conformità.

Il reparto di progettazione può pubblicare configurazioni statiche e/o personalizzabili. Gli ambienti statici vengono in genere utilizzati per stack certificati per la produzione, mentre gli ambienti personalizzabili sono destinati alle sandbox di test e sviluppo. Gli ambienti personalizzabili possono soddisfare anche più dell'80% dei requisiti dell'utente, ma possono essere modificati dallo sviluppatore o dal tecnico del controllo qualità in base alle esigenze. I carichi di lavoro possono essere attivati con nuove reti o per la connessione alle reti esistenti.

Esempio di automazione dei processi con blueprint

Diamo uno sguardo alle attività che è possibile automatizzare per un blueprint dell'applicazione standardizzato a tre livelli:



Dopo le fasi di test e convalida, il blueprint viene pubblicato nel catalogo dei servizi e messo a disposizione degli utenti. L'utente fa clic sull'elemento del servizio e l'intero stack applicativo, insieme alle sue caratteristiche di connettività, disponibilità e sicurezza, viene distribuito in pochi secondi.

Questo servizio automatizzato è di gran lunga più veloce di una rete fisica tradizionale senza NSX, che in genere richiede diversi giorni o settimane. Le aziende evitano tempi dei cicli lunghi e ritardi da workflow di ticketing complessi, modificano revisioni e approvazioni, l'individuazione e la convalida di requisiti ridondanti e la configurazione manuale.

Best practice per i processi: accesso basato sul ruolo

È utile implementare il controllo dell'accesso al portale self-service basato sul ruolo. Occorre definire inoltre le policy di prenotazione e allocazione delle risorse in base ai gruppi aziendali, tenere traccia dei costi per i chargeback e rispettare i livelli di servizio (accordi sui livelli di servizio).

Automazione delle policy di sicurezza con gruppi

NSX automatizza in modo nativo molte attività che vengono completate manualmente con l'infrastruttura di rete fisica e sicurezza. Ad esempio, offre nuovi modi per definire e applicare la policy di sicurezza alle VM nel layer di virtualizzazione.

Vecchio approccio: tradizionalmente, i team addetti alla sicurezza creano regole basate su indirizzi IP, porte e protocolli. Questo è anche noto come l'incubo di gestione “5-tupla”.

Nuovo approccio: nel nuovo modo, la policy di sicurezza si basa su gruppi di sicurezza. È possibile definire un gruppo di sicurezza composto da un insieme di VM e creare una policy di sicurezza intorno a questi carichi di lavoro. Se si aggiunge un'altra VM al gruppo, la policy di sicurezza viene applicata automaticamente ai nuovi carichi di lavoro senza alcun intervento manuale. L'appartenenza al gruppo può essere applicata in modo dinamico tramite tag di sicurezza e contesto come anche/invece. Le policy di sicurezza NSX possono includere, ad esempio, firewall, antivirus e IPS.

I gruppi di sicurezza possono essere statici o dinamici, programmati per attivarsi in caso di metadati arbitrari sul carico di lavoro, come, ad esempio, identità del gruppo di utenti, caratteristiche del SO, tag e nomi delle VM, la presenza di virus e così via. NSX assegna automaticamente il gruppo di sicurezza e la policy appropriati sulla base del contesto rilevante per la virtualizzazione piuttosto che sulla topologia fisica.

Le policy di sicurezza preapprovate vengono orchestrate e gestite a livello centrale, riducendo la proliferazione delle regole e assicurando l'applicazione precisa e uniforme della sicurezza. Questo nuovo livello di automazione riduce drasticamente la complessità operativa e le spese di gestione delle policy di sicurezza di tutti i carichi di lavoro.

Ogni team addetto alla sicurezza utilizza una combinazione originale di appliance di sicurezza della rete per soddisfare le esigenze del proprio ambiente. Oltre alla funzionalità di firewall distribuito di NSX, le aziende devono utilizzare al meglio la piattaforma per automatizzare le funzionalità di sicurezza delle reti avanzate dai partner tecnologici VMware.

I team addetti alla sicurezza della rete devono spesso coordinare servizi di rete e sicurezza completamente scollegati di più vendor. NSX consente di fare proprio questo. NSX distribuisce servizi di rete nel contesto vNIC per formare una pipeline logica di servizi applicati al traffico sulla rete virtuale. I servizi di rete di terze parti possono essere inseriti in questa pipeline logica, permettendo l'utilizzo di servizi fisici o virtuali. Le aziende utilizzano NSX per costruire policy che utilizzano al meglio l'inserimento, il concatenamento e l'indirizzamento dei servizi per consentirne l'esecuzione nella pipeline logica.

Gli strumenti di sicurezza integrati traggono inoltre vantaggio dal modello operativo offerto dalla piattaforma NSX. Queste integrazioni aumentano drasticamente l'efficienza operativa e la qualità del servizio mantenendo al tempo stesso la separazione dei compiti tra team addetti ai server, alla rete e alla sicurezza.

Le funzionalità di sicurezza avanzate sono disponibili tramite le integrazioni a livello di API con Palo Alto Networks, Intel Security, Trend Micro, Symantec, Checkpoint e molti altri partner VMware NSX.

Creazione di visibilità a livello di applicazione con gli strumenti moderni

L'hypervisor ha una posizione ideale e unica sul confine tra i mondi fisico e virtuale. Poiché il vSwitch NSX vede tutti i pacchetti che entrano ed escono da una VM, fornisce il livello più alto di visibilità e contesto ed è anche in grado di correlare le relazioni fluide tra applicazioni, reti virtuali, reti fisiche e altro.

Di seguito si riportano alcuni scenari esemplificativi che dimostrano le originali funzionalità di monitoraggio e risoluzione dei problemi di NSX:

Riepilogo in tempo reale	Monitoraggio e risoluzione dei problemi	Debugging
Un operatore può scegliere l'interfaccia di rete di una qualsiasi macchina virtuale e vedere un riepilogo in tempo reale di tutti i flussi e del loro stato. Non occorre configurare le acquisizioni dei pacchetti su uno strumento remoto, né analizzare gli indirizzi IP alla ricerca della VM.	Ogni aspetto di una rete virtuale è disponibile tramite il CLI centrale e l'API centrale di NSX. Le attività di monitoraggio e risoluzione dei problemi risultano pertanto estremamente semplificate, poiché non è più necessario capire dove cercare un problema nella rete. Inoltre, non è necessario andare su altre console per eseguire la risoluzione dei problemi.	Infatti, tutti i pacchetti vengono gestiti nel software dal vSwitch, offrendo quindi una visibilità superiore rispetto alle reti tradizionali. È possibile creare una transazione sintetica senza dover accedere alle VM guest. I pacchetti traceflow possono essere iniettati in una pipeline di inoltro per consentire il debugging granulare di problemi nel percorso dei dati, ad esempio policy ACL estremamente restrittive.

Gli operatori già si servono di molti strumenti per gestire e supportare l'infrastruttura del data center. Utilizzano diversi strumenti per le attività di monitoraggio, risoluzione i problemi e gestione delle modifiche. Grazie alla virtualizzazione della rete, gli strumenti esistenti possono essere utilizzati per ottenere visibilità nelle reti logiche.

Gli strumenti di monitoraggio in tempo reale sono importanti negli ambienti virtualizzati in continuo mutamento, dove infrastruttura e applicazioni si spostano dinamicamente da server a server e la rete viene riconfigurata automaticamente.

Best practice per i processi: strumenti

È importante individuare gli strumenti VMware o di terze parti che offrono visibilità sulle relazioni tra gli oggetti tra l'infrastruttura di rete, elaborazione e storage virtuale e fisica. La correlazione tra i domini dell'infrastruttura aiuta a limitare rapidamente l'ambito di un problema a un dominio specifico e a ridurre la necessità di avere più strumenti specifici per ciascun dominio.

Le opzioni migliori sono di solito gli strumenti moderni, come vRealize Operations, Arkin, Riverbed e altri, che sono appositamente progettati per gli ambienti virtuali e fisici. Questi strumenti offrono una visione end-to-end di topologia, applicazione, stato, utilizzo e capacità.

Ricordare che un approccio con un solo vendor non è necessariamente in grado di offrire la visibilità migliore. Potrebbe essere preferibile avere più strumenti per un monitoraggio, una generazione di avvisi e una risoluzione dei problemi ottimali, così come avviene oggi per la rete fisica. Ad esempio, è probabile che si utilizzino strumenti diversi per l'analisi del traffico, ad esempio SolarWinds e NetQoS, l'analisi dei pacchetti, ad esempio Wireshark e SteelCentral, e gli avvisi, ad esempio Netcool e OpenNMS.

Le reti virtuali offrono lo stesso livello di strumentazione della rete fisica tramite protocolli standard, ad esempio statistiche su pacchetti e byte tramite SNMP e API, SPAN/L3 SPAN, NetFlow/IPFIX, mirroring delle porte e Syslog. Ciò permette alle aziende di iniziare utilizzando gli strumenti di monitoraggio, avvisi e risoluzione dei problemi in loro possesso e di passare successivamente a uno strumento moderno, come quelli già menzionati.

Un'ultima nota sui processi

La virtualizzazione della rete e NSX sono un ottimo motivo per analizzare come si sta lavorando oggi e definire un modo di lavorare migliore e più efficiente per il futuro. Mettere a posto tutti i processi può sembrare un'impresa titanica, per questo è preferibile un approccio incrementale all'automazione dei processi per evitare la paralisi. Per andare avanti è opportuno utilizzare metodologie semplici e di miglioramento continuo.

Tecnologia

Questa sezione propone delle considerazioni sull'architettura e sull'infrastruttura da tenere presenti durante la pianificazione, la distribuzione e l'utilizzo della virtualizzazione della rete e di NSX. Verranno illustrati dei casi d'uso pratici sulla microsegmentazione e il Disaster Recovery.

Rete fisica progettata per essere semplice

Con NSX, l'architettura della rete fisica è progettata in modo semplice per assicurare connettività e prestazioni. Questa può essere semplice come un fabric L2 già in uso al momento oppure un fabric L3 basato su un'architettura leaf-spine. È possibile iniziare con la prima e passare gradualmente alla seconda.

NSX non impone requisiti complicati sui quali tracciare il confine delle reti L2. Le modifiche alla configurazione della rete fisica dovrebbero essere relativamente poco frequenti, poiché questa non fa altro che offrire connettività tra gli host, evitando così gli errori legati alla configurazione manuale.

La separazione di topologie e servizi di rete dall'hardware fisico ha permesso l'ampia diffusione dei fabric spine-leaf L3. Ciò permette di creare una piattaforma comune che utilizza lo stesso modello logico di rete, sicurezza e gestione.

Grazie all'astrazione della topologia della rete virtuale, come vista dalle VM, dalla topologia fisica, NSX rende più fattibile una modifica nell'architettura di rete. NSX dà più libertà ai progettisti delle reti, consentendo un più facile spostamento alle architetture spine-leaf che utilizzano router L3 con ECMP senza blocchi tra gli switch top-of-rack.

La rete fisica sottostante è libera di evolversi in modo indipendente dalla rete virtuale e la sua architettura è progettata intorno a criteri di scalabilità, throughput e solidità. Il guasto di un singolo dispositivo o link non compromette la connettività delle applicazioni.

La progettazione del fabric L3 ECMP offre uniformità di configurazione e migliora l'interoperabilità dei dispositivi. Gli aggiornamenti hardware, come, ad esempio, la distribuzione di nuovi switch, possono essere separati da NSX, evitando un impatto sui carichi di lavoro in esecuzione sulle proprie reti virtuali. NSX supporta gli switch di qualsiasi vendor, che possono essere interconnessi.

Gli overlay della virtualizzazione della rete abbinati ad architetture spine-leaf determinano resilienza ed efficienza operativa superiori, un utilizzo più efficiente della larghezza di banda e scalabilità per gestire la crescente quantità di comunicazioni est-ovest nel data center, mentre i domini di broadcast L2 più piccoli aumentano la stabilità della rete.

Implementazione incrementale della virtualizzazione della rete

La virtualizzazione della rete con NSX è una soluzione personalizzabile. Le reti virtuali NSX non richiedono modifiche alla rete fisica sottostante. La virtualizzazione della rete può coesistere in modo trasparente con le distribuzioni delle applicazioni esistenti sulla rete fisica.

Le organizzazioni IT hanno la flessibilità di virtualizzare parti della rete semplicemente aggiungendo nodi dell'hypervisor alla piattaforma NSX. Inoltre, i gateway del software NSX o gli switch top-of-rack (ovvero hardware dei partner VMware) offrono la possibilità di interconnettere senza problemi reti virtuali e fisiche. Questi possono essere utilizzati per supportare l'accesso a Internet in base ai carichi di lavoro connessi alle reti virtuali oppure per collegare direttamente le VLAN esistenti e i carichi di lavoro bare-metal alle reti virtuali.

Best practice per la tecnologia: iniziare con un solo progetto

È opportuno implementare la virtualizzazione della rete e gli aspetti legati alla sicurezza in maniera incrementale, iniziando con un singolo caso d'uso e un singolo set di applicazioni. Quindi è opportuno identificare i carichi di lavoro con un profilo rischio/vantaggio interessante per utilizzare al meglio le nuove funzionalità. Per la prima implementazione, scegliere carichi di lavoro a rischio più basso, ma sufficientemente complessi ai fini della convalida di NSX nel proprio ambiente.

Il caso d'uso che si sceglie di implementare sarà determinante per stabilire quali servizi funzionali di NSX si automatizzeranno per le proprie reti virtuali. Ad esempio, se si automatizza il provisioning della rete, è possibile iniziare con switch L2 logici, router L3 e servizi perimetrali. Se si implementa la microsegmentazione, si inizierà con il firewall logico.

Definire una strategia e un metodo per implementare in modo continuo le funzionalità di NSX per i propri clienti. Stabilire una cadenza periodica, nota a livello aziendale e su cui contare per i vari progetti. L'utilizzo di release periodiche aiuta ad accrescere il coinvolgimento degli utenti, l'adozione dei servizi e la soddisfazione dei clienti. Accettare l'adozione organica dei servizi piuttosto che forzare un'adozione di ampia portata.

Best practice per la tecnologia: workshop

La comunicazione con i colleghi addetti al business e alla tecnologia è un ottimo modo per assicurare il successo di qualunque iniziativa, inclusa la virtualizzazione della rete. È possibile organizzare workshop periodici con gli utenti allo scopo di informare e istruire le parti interessate sulla virtualizzazione della rete e i servizi di sicurezza disponibili e aggiornarli sui piani per la roadmap. Invitare i proprietari delle applicazioni e delle infrastrutture a collaborare fornendo i requisiti per le release future e un feedback sulle funzionalità già disponibili in produzione.

Caso d'uso: segmentazione intorno ai confini tra le applicazioni

Uno dei casi d'uso più implementati e utilizzati all'inizio dai clienti di NSX è la microsegmentazione. La microsegmentazione è da tempo considerata una best practice per l'architettura di sicurezza. Quando gli autori di attacchi ottengono accesso non autorizzato alla rete, la segmentazione aiuta a limitarne i movimenti e a prevenire la violazione dei dati. Tuttavia, la microsegmentazione non è stata molto utilizzata in passato, probabilmente a causa delle limitazioni dell'architettura nelle reti fisiche tradizionali, che la rendono difficile da implementare.

Con NSX la microsegmentazione diventa una cosa fattibile. La piattaforma offre isolamento e segmentazione nativi. L'inserimento di servizi avanzati consente alle appliance di sicurezza di terze parti di utilizzare al meglio il modello operativo NSX.

L'isolamento costituisce la base per la maggior parte delle strategie di sicurezza della rete, per la conformità, il contenimento o semplicemente per impedire l'interazione tra ambienti di sviluppo, test e produzione. Le reti virtuali vengono isolate le une dalle altre e dalla rete fisica sottostante per impostazione predefinita, a meno che non vengano appositamente connesse. Gli operatori non devono occuparsi di subnet fisiche, VLAN, ACL e regole per il firewall.

La segmentazione è correlata all'isolamento, ma applicata a livelli in una rete virtuale a più livelli. Storicamente, la segmentazione della rete è una funzione di un firewall o router fisico ed è progettata per consentire o vietare il traffico tra livelli o segmenti della rete. Ad esempio, router e firewall segmentano il traffico tra un livello Web, un livello applicativo e un livello di database.

Le sfide odierne: i processi tradizionali per la configurazione della segmentazione sono manuali, richiedono molto tempo e sono soggetti a errore umano, con conseguenti violazioni della sicurezza. L'implementazione richiede competenze specifiche della sintassi della configurazione dei dispositivi, dell'indirizzamento di rete, delle porte applicative e dei protocolli.

Soluzione per la virtualizzazione della rete: con la policy di sicurezza di NSX applicata nel layer di virtualizzazione. È arrivato il momento di dire addio ai trucchi per deviare il traffico est-ovest. La sicurezza viene applicata in modo trasparente prima che i pacchetti arrivino alla prima porta della rete virtuale. Dopo la protezione assicurata all'inizio, il traffico est-ovest sensibile alla latenza è libero di arrivare direttamente alla sua destinazione prendendo il percorso a più bassa latenza.

La combinazione di controllo centralizzato e implementazione distribuita dei servizi significa che è possibile applicare le policy granulari a ogni interfaccia virtuale in un modo operativamente fattibile. Ad esempio, le VM nello stesso livello di un'applicazione a tre livelli possono comunicare con gli altri livelli ma non tra di loro. Ciascun carico di lavoro può contare su una propria sicurezza.

NSX permette di impostare le policy di sicurezza sulla base di costrutti aziendali di alto livello, come applicazione, utente o gruppo, piuttosto che su costrutti di infrastruttura di basso livello, come indirizzo IP, porte applicative e protocolli. Le policy di sicurezza possono essere applicate con una precisione, un'accuratezza e un allineamento superiori alla policy aziendale senza lasciare spazio all'interpretazione.

Progettazione per il recupero e la mobility dei carichi di lavoro

In passato, le topologie e lo spazio di indirizzamento delle reti fisiche richiedevano la modifica degli indirizzi IP in caso di spostamento delle applicazioni. In alcuni casi, gli indirizzi IP sono codificati nelle applicazioni. Ciò comporta la necessità di apportare modifiche ed eseguire test di regressione con importanti ripercussioni sui costi.

NSX libera i carichi di lavoro da VLAN e indirizzi IP e ne permette il posizionamento e la mobility senza restrizioni nel fabric del data center. Con NSX, il posizionamento dei carichi di lavoro non dipende dalla topologia fisica e dalla disponibilità dei servizi della rete fisica in una determinata posizione.

Tutto ciò di cui una VM ha bisogno dal punto di vista della rete lo ottiene da NSX, ovunque risieda fisicamente. I carichi di lavoro sono liberi di muoversi tra subnet, zone di disponibilità o data center senza che le operation debbano reindirizzarli. Se un carico di lavoro viene spostato, vengono spostati automaticamente anche i relativi servizi di rete e sicurezza senza alcun intervento umano.

Le aziende usano la mobility e il posizionamento dei carichi di lavoro di NSX per, ad esempio:

- Eseguire il provisioning delle applicazioni più rapidamente
- Migrare i carichi di lavoro a un nuovo data center
- Aggiornare l'infrastruttura fisica sottostante

Caso d'uso: miglioramento dell'utilizzo delle risorse del server con la virtualizzazione della rete

Le aziende utilizzano NSX anche per accedere alla capacità dei server disponibile in altre posizioni nel data center o in un altro data center. Ciò permette un utilizzo e un consolidamento di gran lunga maggiori delle risorse del server. Tutti questi casi d'uso riducono in modo significativo i costi operativi e accrescono l'agilità, dando più valore all'investimento nella virtualizzazione della rete e in NSX.

Nelle topologie di rete tradizionali, ogni cluster o pod dispone di una propria capacità dei server. Riconfigurare la rete per accedervi da un altro pod o cluster richiede troppo tempo ed è soggetto a errore umano. La capacità dei server disponibile viene sprecata, un fenomeno anche detto come “capacità server non utilizzata”, poiché non è facilmente raggiungibile. In realtà, la complessità di apparecchiature e topologie di rete tradizionali limita la capacità dell'organizzazione IT di utilizzare al meglio la capacità dei server disponibile.

Con NSX è possibile estendere l'accesso alla rete per sfruttare la capacità disponibile ovunque nel data center senza toccare l'infrastruttura fisica esistente. Se si desidera aggiungere un'altra VM, ad esempio su un server in una subnet o zona di disponibilità diversa, è sufficiente richiamare la VM e collegarla al proprio switch logico. Questi due carichi di lavoro sono ora L2 adiacenti, anche se attraversano più subnet e zone di disponibilità sulla rete fisica.

Caso d'uso: Disaster Recovery

NSX può anche servire per completare soluzioni di Disaster Recovery esistenti. Con l'approccio tradizionale alla rete, l'utilizzo di un sito di backup per il Disaster Recovery richiede un equilibrio tra costi e funzionalità. Piuttosto che riprodurre fedelmente la topologia e i servizi di rete in una seconda ubicazione, la maggior parte delle aziende opta per una soluzione “sufficientemente buona”. I compromessi mirano a ridurre i costi, ma si traducono in funzionalità ridotte rispetto al data center principale.

Con NSX, il Disaster Recovery è senza compromessi. Invece di eseguire snapshot di macchine virtuali, NSX consente di eseguire una snapshot dell'intera architettura applicativa, inclusi i servizi di rete e sicurezza. È possibile inviarne una copia al sito di Disaster Recovery, dove rimane in standby sull'hardware senza compromettere la funzionalità.

In caso di emergenza, è sufficiente attivare la VM. La rete alla quale dovrebbe connettersi è già in esecuzione nel sito di ripristino. L'obiettivo di tempo di ripristino si riduce in modo significativo, poiché non occorre riconfigurare i carichi di lavoro e le appliance di sicurezza con nuovi indirizzi IP.

Considerazioni finali sulla tecnologia

La virtualizzazione della rete e NSX offrono una flessibilità superiore all'ambiente IT e aprono le porte a molteplici e preziosi casi d'uso. Invece di lasciarsi sopraffare dalle tante possibilità, è importante, all'inizio, concentrarsi sulla qualità del servizio per poi ampliare il footprint del caso d'uso iniziale e scegliere un secondo caso d'uso da implementare. È consigliabile fornire nuove funzionalità solo dopo che il proprio team e i propri utenti sono soddisfatti dei livelli di qualità.

Passaggi successivi

L'operatività della virtualizzazione della rete e della sicurezza dovrebbero essere considerati come un viaggio che permette all'azienda di maturare e avanzare nel passaggio al Software-Defined Data Center e di offrire sempre più valore al business.

I membri dell'azienda e dei singoli team hanno a disposizione molteplici opzioni per capire come cogliere tutti i vantaggi operativi offerti dalla virtualizzazione della rete e da NSX e in che modo questi si adattano e integrano con il resto dell'organizzazione IT.

Fase uno: Apprendimento

Un primo grande passo consiste nel fornire opportunità di apprendimento per l'azienda e i singoli. Abbinare diversi tipi di formazione e apprendimento, ovvero formale (workshop, corsi, Hands-on Lab, programmi) e informale (pranzi, coaching, mentoring). Per incentivare l'apprendimento, considerare modi per includere gli obiettivi formativi e di apprendimento negli MBO personali.

Per iniziare, il team può partecipare agli Hands-on Lab di VMware (labs.hol.vmware.com) e ai workshop e corsi con docente disponibili tramite VMware Education (vmware.com/education). VMware propone inoltre guide operative per NSX incentrate sulle attività di monitoraggio e risoluzione dei problemi.

Fase due: Servizi di trasformazione

Avere un punto di vista esterno durante la transizione alla virtualizzazione della rete e a NSX può accelerare il processo in modo significativo. VMware offre workshop e servizi di trasformazione delle operation (vmware.com/consulting). Ad esempio, Network-as-a-Service Envisioning aiuta a identificare in modo chiaro la vision e gli obiettivi del nuovo modello operativo per rete e sicurezza. NaaS Discovery permette di individuare quali funzionalità operative e aziendali occorre potenziare o creare per implementare il nuovo modello operativo e raggiungere gli obiettivi previsti.

Fase tre: Progetto pilota

Uno dei modi migliori per imparare a usare NSX è di avviare un progetto pilota di produzione con un singolo caso d'uso e pochi carichi di lavoro. Scegliere i carichi di lavoro a rischio più basso, ma sufficientemente complessi ai fini di ottimizzare l'apprendimento sull'operatività di NSX.

Contattare il proprio partner o account executive VMware per ricevere assistenza su come iniziare.

Appendice

Caratteristiche prestazionali finali

La tabella che segue riepiloga le caratteristiche finali dell'operatività di NSX per le persone, i processi e la tecnologia. È possibile utilizzarla come guida nel proprio viaggio:

Vettore	Stato corrente/iniziale	Stato futuro/finale
Struttura aziendale	• In sili con confini stabiliti che richiedono processi pesanti • Procedure di richiesta formali • Attribuzione all'IT • Individuazione delle responsabilità: noi o loro • Obiettivi e incentivi diversi e non allineati	• Amalgamata con interazioni immediate • Comunicazione aperta • Loop di feedback condensati • Collaborazione elevata • Obiettivi e KPI condivisi • Rischi e responsabilità condivisi
Persone	• Specializzazione • Competenze limitate a un dominio • Utilizzo di CLI e script • Conoscenze ampiamente disponibili • Crescita professionale limitata • Approccio basato sull'infrastruttura hardware	• Ruoli intersettoriali e interdisciplinari • Competenze di più domini • Utilizzo di API e strumenti di automazione • Apprendimento continuo • Opportunità per avere un impatto aziendale tramite progetti strategici • Approccio basato sui servizi e sulle applicazioni
Processi	• Manuali e soggetti a errori • Sistemi di ticketing complessi • Coordinamento e consegne • Complessità e colli di bottiglia • In attesa del servizio • OpEx elevato • Incentrati sull'infrastruttura	• Automatizzati, standardizzati, coerenti e verificabili • Basso rischio di errori manuali • Turnaround rapido/con accordi sui livelli di servizio • Interazioni in tempo reale • Riduzione dell'OpEx • Incentrati sui servizi e sulle applicazioni
Strumenti	• Preesistenti, specifici del dominio • Più strumenti in sili • Strumenti solo fisici • Incentrati sull'infrastruttura • Difficoltà a isolare i problemi con i servizi • CLI con componenti singoli	• Strumenti moderni interdominio • Progettati per la strumentazione virtuale e fisica • Incentrati sulle applicazioni • Monitoraggio integrato di infrastruttura e servizi • Facilità a isolare i problemi con i servizi • CLI e API centralizzati a e inefficiente dell'infrastruttura IT degli strumenti

Vettore	Stato corrente/iniziale	Stato futuro/finale
Architettura	• Tipiche limitazioni dell'architettura a 3 livelli • Vincoli dei carichi di lavoro • Firewall con strozzature • Core sovrautilizzato • Prestazioni dei link • Servizi centralizzati legati alla posizione	• Fabric spine-leaf con ECMP senza blocco • Overlay con separazione e astrazione • Portabilità e mobility dei carichi di lavoro • Isolamento e segmentazione nativi • Scalabilità e resilienza • Servizi distribuiti
Infrastruttura	• Fisica con modifiche lente nel livello sottostante • Sicurezza legata all'infrastruttura • DR “sufficientemente buono” • Interpretazione umana della policy • Policy incentrate sull'infrastruttura • Architettura dell'infrastruttura di basso livello • Gestione frammentata • Dipendenza dal vendor dell'hardware • Difficoltà a eseguire il concatenamento dei servizi	• Virtuale con modifiche dinamiche nell'overlay • Sicurezza incentrata sulle applicazioni • DR senza compromessi • Policy di sicurezza integrate leggibili da macchina • Policy incentrate sul business • Architettura dell'infrastruttura aziendale di alto livello • Gestione centralizzata • Scelta prezzo/prestazioni • Concatenamento dei servizi intuitivo

Ruoli per rete e sicurezza nel cloud

Le descrizioni che seguono aiuteranno a definire i ruoli e le responsabilità del personale addetto alle funzioni di rete e sicurezza. Questi ruoli nel cloud vengono affidati ai professionisti di rete e sicurezza tradizionali, ovvero persone già presenti nei propri team.

Nelle piccole e medie imprese, non è insolito che una stessa persona svolga due o più di questi ruoli. Ad esempio, uno stesso ingegnere di rete può essere responsabile dell'architettura di rete, dello sviluppo e/o delle operation. Non tutte le aziende dovranno avere persone diverse per ciascuno di questi ruoli.

Al contrario, è piuttosto comune per le grandi aziende avere più persone che svolgono lo stesso ruolo o un ruolo simile. Ad esempio, molte multinazionali hanno più architetti della rete cloud o ingegneri della rete cloud.

Ruoli nella rete cloud

Il *Cloud Network Architect (CNA)* si occupa di sviluppare architetture e standard di rete cloud end-to-end sulla base di un modello di utilizzo basato sui servizi (Network-as-a-Service). Il CNA ha le seguenti responsabilità:

- Determina i requisiti tecnici e operativi della rete
- Progetta reti fisiche e logiche che soddisfano i requisiti delle applicazioni, come capacità e prestazioni
- Sviluppa e convalida test per assicurare che i requisiti siano soddisfatti
- Guida la pianificazione e l'implementazione di soluzioni per la rete cloud

Il *Cloud Network Engineer (CNE)* ha la responsabilità della progettazione non avanzata di servizi di rete e infrastruttura, sviluppo e testing delle funzioni di rete, provisioning della capacità e definizione della configurazione della rete. Il CNE ha le seguenti responsabilità:

- Assicura il rispetto dei requisiti del cliente e dei livelli di servizio correlati
- Traduce i requisiti in blueprint logici e template di configurazione
- Progetta, sviluppa e testa script e workflow personalizzati per le attività di routine, come integrazione, distribuzione, monitoraggio e conformità
- Fornisce assistenza nella risoluzione dei problemi all'assistenza di livello 2 e 3 e propone e richiede soluzioni

Il *Cloud Network Operator (CNO)* ha la responsabilità complessiva per tutti gli aspetti delle operation successive, nel rispetto dei requisiti operativi dell'applicazione (ad esempio, prestazioni e capacità) e mantenendo l'infrastruttura di rete cloud, gli strumenti e le piattaforme. Il CNO ha le seguenti responsabilità:

- Esegue e controlla l'automazione per il provisioning, la gestione, il monitoraggio, gli avvisi e la risoluzione dei problemi
- Monitora attivamente l'infrastruttura della rete cloud e interviene sugli eventi prima che compromettano il servizio
- Esegue la risoluzione dei problemi, l'analisi della causa primaria e applica le soluzioni proposte dal CNE
- Fornisce assistenza di livello 2 e 3 e gestisce incidenti, problemi e tecniche di escalation

Ruoli per la sicurezza del cloud

Il *Cloud Security Architect (CSA)* ha la responsabilità complessiva di tutti gli aspetti legati all'architettura, alla progettazione e all'assistenza dell'infrastruttura di sicurezza del cloud per quanto riguarda la virtualizzazione, l'automazione, l'orchestrazione e il monitoraggio della sicurezza della rete. Il CSA ha le seguenti responsabilità:

- Valuta il rischio per la sicurezza per le applicazioni e l'infrastruttura cloud e fornisce una guida autorevole sulle strategie e le soluzioni per la sicurezza
- Determina le policy di sicurezza tecnica, i processi e le funzionalità di auditing richiesti per soddisfare gli obiettivi e i requisiti di sicurezza del cloud
- Sviluppa test di convalida per verificare le soluzioni di sicurezza del cloud e ne pianifica e guida l'implementazione
- Mantiene una conoscenza dettagliata delle minacce e delle strategie di mitigazione del rischio

Il *Cloud Security Engineer (CSE)* ha la responsabilità di tradurre le policy di sicurezza in controlli di sicurezza verificabili. Il CSE ha le seguenti responsabilità:

- Progetta e implementa soluzioni fisiche e logiche che realizzano i controlli di sicurezza del cloud
- Orchestra e automatizza i processi di sicurezza del cloud (controllo, monitoraggio e verifica)
- Integra e implementa gli strumenti e i servizi di sicurezza del cloud che soddisfano requisiti e livelli di servizio
- Coinvolge i diretti interessati, indaga sulle violazioni e consiglia e implementa le soluzioni

Il *Cloud Security Operator (CSO)* ha la responsabilità di comprendere, implementare, applicare, verificare e gestire controlli di sicurezza specifici, come richiesto dalla valutazione del rischio e dalle policy aziendali. Il CSO ha le seguenti responsabilità:

- Monitora, rileva e analizza le anomalie, le vulnerabilità e le minacce per la sicurezza
- Gestisce i registri della sicurezza, assicura la conformità agli standard di registrazione e collabora agli audit di sicurezza
- Indaga, diagnostica e risolve i problemi di sicurezza del cloud in risposta agli incidenti
- Implementa soluzioni di sicurezza ed elimina le vulnerabilità

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel. 877-486-9273 Fax 650-427-5001 www.vmware.com
VMware Inc. - Via Spadolini, 5 - Edificio A - 20141 Milano - Tel.: (+39) 02 3041 2700 Fax: (+39) 02 3041 2701 www.vmware.it