Planificación de la transformación operativa con NSX

Prácticas recomendadas en un entorno real

GUÍA

vmware

Índice

Introducción

Este documento técnico está dirigido principalmente a ejecutivos y responsables de cloud, redes y seguridad. También es útil para responsables y colaboradores individuales en las áreas de arquitectura, ingeniería y operaciones que participan en la puesta en marcha de NSX en su organización.

La virtualización de red representa un avance importante que ayuda a las organizaciones a aprovechar las ventajas de la velocidad, la agilidad y la seguridad. Equivale o supera a las ventajas que la virtualización del entorno de TI proporcionó a lo largo de la última década. A fin de obtener las ventajas de la virtualización de red, las organizaciones deberán evaluar y ejecutar un plan operativo que abarque el **personal**, el **proceso** y la **tecnología**.

VMware ha desarrollado una estrecha colaboración con clientes existentes de NSX para entender las realidades que implica llevar la virtualización de red a la producción. Estos conocimientos del mundo real le guiarán a través de la evaluación, la implementación y la puesta en marcha de NSX. Usted y su organización pueden analizar y utilizar las prácticas recomendadas que tengan más sentido para su situación en concreto.

Si bien este documento abarca un amplio espectro de prácticas recomendadas, para comenzar, NSX puede ponerse en marcha con cambios mínimos, independientemente de su estado actual. La puesta en marcha de NSX no es complicada y supone un camino claro hacia el éxito.

Esta guía está dividida en tres secciones principales en las que se tratan la información clave y las prácticas recomendadas para las siguientes áreas:

Personal

Con la virtualización de red, se pueden descubrir las fortalezas organizativas y las grandes ventajas que se obtienen al transformar la forma en que se trabaja en la organización tecnológica. También representa un cambio que debe considerarse detenidamente a fin de garantizar claridad y coordinación en toda la organización. Al asegurarse de contar con una estructura organizativa ágil, con equipos combinados que tengan funciones y responsabilidades bien definidas, podrá obtener los mejores resultados y el mayor valor para la organización y el personal. Brindamos información y orientación con respecto a estructuras organizativas, estrategias internas de participación y comunicación, así como funciones y responsabilidades.

Proceso

La virtualización de red proporciona oportunidades importantes para aumentar la productividad a través de la automatización de procesos manuales en el ciclo de vida de las aplicaciones. Al definir un estado futuro ideal para la forma en que despliega, gestiona y supervisa tanto aplicaciones como servicios, podrá alejarse de los procesos y las prácticas existentes que no son necesarios.
Le proporcionaremos orientación sobre la automatización, la gestión de procesos, las herramientas y algunos casos de uso interesantes.

Tecnología

Una de las ventajas principales de la virtualización de red es la separación de las funciones de red y seguridad de la infraestructura de la red física subyacente, así como su abstracción a una capa de virtualización. Esto le permitirá diseñar y gestionar la infraestructura con mayor eficacia según avanza. Proporcionaremos orientación sobre las prácticas arquitectónicas recomendadas, la implementación incremental de la infraestructura y la puesta en marcha periódica de nuevas prestaciones.

No se pretende que estas prácticas recomendadas sean prescriptivas ni adecuadas para todos los casos. Debe elegir aquellas que considere que funcionarán para su organización, dadas sus características, metas y prioridades. No intente aplicar un enfoque global. Comience con solo un par de aspectos o unos pocos y después, con el tiempo, céntrese en otros.

Algunas organizaciones se confían demasiado y se detienen antes de tiempo en su trayecto hacia el rendimiento óptimo. Como resultado, limitan el éxito que pueden alcanzar para su organización. Tenga siempre en mente la meta final y luche continuamente por mejorar y alcanzarla.

Personal

El primer tema que queremos tratar es el de las personas: la organización, los equipos y los individuos que componen su organización tecnológica responsable de la distribución y gestión integrales de aplicaciones y servicios y que, en última instancia, constituyen la fuerza impulsora de la puesta en marcha de la seguridad y la virtualización de red.

Reflexiones iniciales sobre la estructura de la organización

La virtualización de red y NSX no requieren un tipo específico de estructura organizativa. La estructura óptima depende de factores que son específicos de la organización. NSX se ha puesto en marcha tanto en organizaciones tradicionalmente aisladas como en equipos de cloud completamente mixtos e integrados. También existen términos medios entre los equipos estrictamente aislados y aquellos que son totalmente mixtos.

La estructura organizativa ideal dependerá de diferentes factores. En el diseño de la estructura, se deben tener en cuenta los siguientes elementos:

- Coordinación entre dominios y disciplinas
- Madurez del flujo de valor
- Nivel de liderazgo técnico
- Experiencia y conocimientos especializados del personal
- Experiencia y sofisticación operativas
- Uso de la externalización
- Cantidad de infraestructura y aplicaciones
- Implementación en una estructura nueva o existente

Nuestra recomendación: diseñar una estructura de equipo combinado

La experiencia demuestra que los equipos más productivos están estrechamente entrelazados, tienen un alto nivel de colaboración y son autosuficientes. Estos equipos combinados han demostrado trabajar con mayor eficiencia, tiempos de ciclos más cortos, bucles de comentarios condensados y amplificados, además de mayor grado de intercambio de conocimientos y aprendizaje continuo. Lo ideal sería que el equipo esté físicamente en el mismo lugar.

Hemos visto estructuras organizativas con éxito compuestas por equipos basados en el dominio (p. ej., recursos informáticos, almacenamiento, redes y seguridad) y basados en la disciplina (p. ej., arquitectura, desarrollo e integración, operaciones y soporte). En ambos casos, los equipos son responsables de la infraestructura virtual y física.

A medida que mueva una mayor parte de la infraestructura y más aplicaciones de la red corporativa existente a la cloud, la asignación del personal también cambiará. Con el tiempo, habrá más miembros del personal trabajando en la cloud y una cantidad menor trabajando en la red corporativa existente. Es importante desarrollar un plan de comunicación y formación para que la organización entienda esta evolución y esté preparada para la misma, así como para nuevas oportunidades laborales. También es importante comunicar el hecho de que, independientemente de si una persona trabaja en la red corporativa existente o en la cloud, la contribución de esta persona es fundamental para el éxito general de la organización.

Coordinación con medidas de éxito en común

La siguiente consideración organizativa importante es la coordinación con una estrategia compartida que tenga metas, objetivos, medidas e incentivos bien definidos. El equipo debe tener un enfoque orientado al servicio y debe ser responsable colectivamente de todo el ciclo de vida de la prestación de servicios: desde los requisitos del negocio hasta el funcionamiento y la gestión de una carga de trabajo en producción de alta calidad que cuente con el respaldo de un acuerdo de nivel de servicio (SLA).

Además, cada equipo debe tener medidas de éxito en común que se basen en los factores que sean más importantes para la organización. Entre los ejemplos se incluyen: plazo de comercialización, impacto en los ingresos, capacidad de respuesta del mercado, tasa de innovación o ventajas y satisfacción del cliente. Las metas deben enfocarse hacia el negocio y los consumidores del servicio.

Permita que el equipo desarrolle sus propias medidas de éxito y realice un seguimiento de estas. Sin embargo, asegúrese de que las medidas sean relevantes y se ajusten a las metas y los objetivos en común. Además de que estén en línea con las metas de la organización, los indicadores clave de rendimiento deben ser específicos, claros, cuantificables y medibles. Independientemente de qué indicadores clave de rendimiento elige el equipo, deben ser simples y se debe comenzar con algunos parámetros básicos que sean significativos y fáciles de entender.

Una vez elegidos los indicadores clave de rendimiento, determine los valores de referencia y documente el punto en el que se encuentra en la actualidad. Realice un seguimiento y una evaluación periódicos de su progreso (p. ej., normalmente por mes o por trimestre) en el avance hacia el estado final deseado. Deje en claro al equipo que esto no se hace para criticar a las personas ni el rendimiento pasado, sino para mostrar pruebas del éxito del equipo y el nuevo valor que brindan al negocio. Estas medidas también pueden usarse para que la revisión y la evaluación del rendimiento sean más eficaces, tangibles y significativas para las personas.

Creación de una cultura responsable y comprometida

La cultura es un puntal importante del éxito en la seguridad y la virtualización de red. Contar con una cultura que apoye los principios de un centro de datos definido por software es crucial. En lugar de que el cambio cultural parta de los ejecutivos o responsables, que entra su dificultad, la cultura debería surgir de forma natural desde el interior de los equipos a través de la experiencia, los conocimientos y los valores que comparten.

Al establecer medidas de éxito en común, una nueva cultura surgirá y arraigará de forma natural. La base de la nueva cultura estará constituida por una meta clara centrada en el negocio y el consumidor, responsabilidades y riesgos compartidos, colaboración y cooperación más estrechas, además de confianza y respeto mutuos.

El equipo: colaboración en conocimientos especializados sobre seguridad y redes

Una de las ventajas principales de la virtualización de red es la separación de las funciones de red y seguridad de la infraestructura de la red física subyacente, así como su abstracción a una capa de virtualización. El cambio ha creado algunas preguntas, tales como las siguientes: «¿Qué equipo es responsable de las redes virtuales y la seguridad en el hipervisor?» y «¿de qué manera la virtualización de red cambia mis responsabilidades?» En esta sección, respondemos estas preguntas.

Su personal de redes y seguridad existente se encarga de la seguridad y la virtualización de la red. NSX se basa en conceptos y tecnologías de redes para los que se requieren conocimientos especializados en redes. Solo los equipos de redes cuentan con los conocimientos requeridos. Al igual que con las redes físicas, se necesitan expertos en redes y seguridad para diseñar, implementar y operar las redes virtuales.

La red física no desparece, pero se torna mucho más simple y fácil de gestionar. No recomendamos crear un equipo arbitrario de límite entre las redes físicas y lógicas. A fin de maximizar la velocidad y la agilidad, el equipo responsable de la capa base física y la capa superpuesta virtual debe incluir arquitectos, ingenieros y operadores de redes.

Sin embargo, también puede optar por incluir ingenieros de redes que se centren más en el montaje en rack, el apilamiento y la configuración de los equipos físicos, además de otros que se centren más en la capa superpuesta virtual. De todas formas, la totalidad de estas personas deben formar parte del mismo equipo.

Las funciones relacionadas con las redes (p. ej., arquitectos, ingenieros y operadores) evolucionan para incluir la seguridad y la virtualización de red. La mayoría del personal del área de redes y seguridad deberá aprender algo nuevo para incrementar sus conocimientos especializados. Con NSX, los servicios de red se ejecutan en la capa del hipervisor. Los profesionales de las redes deben tener un cierto conocimiento sobre virtualización de servidores y lo que significa para los servicios de red lógicos.

Práctica recomendada para el personal: formación

En la etapa inicial del proceso de evaluación, la mayor prioridad es asegurarse de que todos entiendan los principios de la virtualización de red y cuenten con formación sobre NSX y las herramientas relacionadas con las operaciones y la gestión que forman parte del ecosistema de la cloud. VMware ofrece diversas formas de hacerlo, como los laboratorios prácticos, los talleres y los cursos. Estos recursos están principalmente enfocados para profesionales de redes que no tienen experiencia en virtualización de servidores, pero son adecuados también para profesionales de la virtualización de servidores que desean aprender sobre la virtualización de red. También puede poner en práctica un programa que garantice el intercambio de conocimientos y la formación dentro y entre equipos, al proporcionar oportunidades de liderazgo a personas que enseñen, de manera informal, las prácticas recomendadas a otros equipos y grupos.

Una de las mejores maneras de acelerar el aprendizaje es identificar e iniciar un pequeño proyecto piloto y una evaluación. Haga partícipes a todas las divisiones funcionales necesarias (arquitectura, ingeniería y operadores) de las áreas de recursos informáticos, almacenamiento, redes y seguridad.

Comience con un equipo interdisciplinar reducido

Otra recomendación de bajo riesgo es que comience con un equipo interdisciplinario reducido en la evolución hacia la virtualización de red. Si puede pasar de equipos aislados a combinados, hágalo por etapas, a lo largo del tiempo. Principalmente, hemos visto dos tipos de equipos interdisciplinarios. Elija el modelo que sea más adecuado para usted:

Equipo permanente	Equipo temporal
Si puede pasar a un equipo combinado a largo plazo, use un equipo permanente. Con el tiempo, el equipo permanente se convertirá en una parte fija de la estructura organizativa u organigrama. Además, incluya empleados de jornada completa que pasen el 100 % de su tiempo con el equipo.	Si no puede pasar a un equipo combinado a largo plazo, use un equipo temporal. Los equipos temporales se forman y se disuelven, según sea necesario. Los miembros trabajan a tiempo parcial en el equipo y rinden cuentas formalmente a otro equipo. Según lo que hemos visto, los equipos temporales se usan principalmente en las organizaciones gubernamentales.

En general, el equipo interdisciplinar tiene la responsabilidad integral sobre una determinada pila de aplicaciones o un conjunto de ellas. El equipo debe contar con expertos en las áreas de recursos informáticos, almacenamiento, redes y seguridad. Sus conocimientos deben abarcar las áreas de arquitectura, ingeniería y operaciones. El equipo debe ser capaz de encargarse de todo: desde el diseño, el desarrollo y las pruebas hasta la implementación y las operaciones continuas. Consulte el apéndice para ver descripciones de las funciones y responsabilidades de redes y seguridad.

Selección de los especialistas en cambios para el primer equipo

Para el equipo inicial, elija personas que sean especialistas en cambios, expertos en el tema, impulsores y líderes respetados. Busque personas que todos quieran para su equipo: individuos que sepan cómo establecer relaciones interpersonales, abrir vías de comunicación e identificar y minimizar puntos de fricción; líderes que incentiven a los demás a hacer el cambio y que den ejemplo. Si el equipo no se encuentra físicamente en el mismo lugar, reúnalo al comienzo del proyecto durante un par de semanas.

Los miembros del equipo deben tener planes personales de gestión por objetivos (MBO) en línea con las metas del equipo. A modo de ejemplo, si un miembro del equipo dedica el 50 % de su tiempo en el equipo permanente, ese trabajo debería representar aproximadamente el 50 % de sus MBO. A pesar de que puede parecer obvio, hemos visto casos en los que el tiempo que alguien dedica a un equipo interdisciplinario se trata más como un pasatiempo que como una parte esencial de su trabajo. No es probable que este sea un camino al éxito.

Práctica recomendada para el personal: evitar sorpresas

Avise con tiempo para no sorprender a nadie justo antes de realizar la implementación. Ha habido casos en los que se tardó demasiado en hacer partícipes del proceso a personas de operaciones de red y seguridad. Como resultado, los proyectos sufrieron demoras importantes. El área de operaciones deberá conocer cómo la seguridad y la virtualización de red modifican las tareas de supervisión, las alertas y la solución de problemas, así como la forma en la que los procesos y las herramientas deben evolucionar, tema que trataremos más adelante en este documento.

Celebración del éxito y las oportunidades de crecimiento

Cuando incluya personal de redes y seguridad en el proyecto, explique el potencial personal y profesional. A medida que la infraestructura se virtualiza y automatiza, el personal de redes y seguridad obtendrá más tiempo para trabajar en proyectos nuevos e interesantes. Tendrán la oportunidad de centrarse en iniciativas estratégicas que aporten mayor valor al negocio. Por ejemplo, en lugar de realizar el trabajo rutinario de configurar VLAN, equilibradores de carga o reglas de cortafuegos, pueden trabajar en el diseño de servicios nuevos que aporten valor al negocio: automatización de procesos entre dominios, creación de diseños para la adaptabilidad, planificación de la capacidad u otros proyectos e iniciativas interesantes.

Además, explique que las personas innovadoras y de criterio avanzado de la organización tienen la oportunidad de contribuir a la transformación de redes y seguridad. El resultado será beneficioso para aquellos que impulsen la transformación, al igual que lo fue para aquellos que defendieron las redes IP y crearon sus carreras en función de estas y, de manera más reciente, la virtualización del entorno de TI. En ambos casos, las nuevas generaciones de administradores nacieron con nuevos conocimientos. Al participar en la transformación, las personas se enriquecerán profesionalmente y aumentarán sus oportunidades y su valor en el mercado laboral.

Promoción de la participación activa de los usuarios del servicio

Otra manera positiva de incentivar el desarrollo del equipo es hacer partícipes a los consumidores del servicio (p. ej., responsables de aplicaciones, del negocio y de la infraestructura) para enseñarles las nuevas prestaciones. Solicíteles que participen activamente y que proporcionen sus requisitos y comentarios. Los consumidores querrán conocer cómo cambiarán las funciones y la experiencia de usuario. Entre las diversas actividades con éxito de participación se incluyen:

Contactos regulares: llevar a cabo talleres periódicos para ofrecer novedades, conocer los requisitos y solicitar comentarios.

«Mostrar sin decirlo»: establecer e informar de que el equipo desarrolla y lanza nuevas prestaciones de forma periódica, con lo que se incrementará el interés del cliente.

Informar del éxito en toda la organización es positivo

Además de promover el proyecto ante los miembros elegidos del equipo y los consumidores del servicio, también se recomienda difundir el proyecto en las líneas del negocio o en toda la organización. La meta es crear una masa crítica de personas que apoye el proyecto y establecer la plataforma como la forma de facto de hacer las cosas. Comparta historias interesantes sobre la empresa y los resultados de TI del proyecto. Puede promocionarlo mediante una combinación de presentaciones, charlas, artículos, publicaciones en blogs, redes sociales, correo electrónico o demostraciones. Todos los componentes del equipo deben considerarse a sí mismos como impulsores del proyecto. Celebrar los éxitos, tanto pequeños como grandes, es el distintivo de las organizaciones de alto rendimiento, por lo que debe considerarse una práctica recomendada importante en la gestión de los cambios tecnológicos.

Cambiar es difícil: cómo lograr un entendimiento común

Todos sabemos que cambiar es difícil, especialmente en áreas y disciplinas en las que el cambio es lento o en lugares en los que el cambio se podría percibir como una posible amenaza para una carrera o una forma de sustento. Estos factores pueden crear una resistencia al progreso. Incluso, algunas personas pueden trabajar activamente en contra de la transformación. La mejor estrategia es lograr un entendimiento en común con respecto al potencial de la virtualización de red a través de una comunicación y un apoyo auténticos, así como la defensa de los éxitos de la organización.
Debe mostrar transparencia, apertura y disposición para expresar y responder las preguntas: «¿Qué ventajas obtengo? ¿Qué ventajas obtenemos?»

Proceso

En esta sección, explicaremos el impacto que la virtualización de red tiene en los procesos operativos, describiremos los pasos que debe realizar para examinar y entender los procesos existentes, y haremos recomendaciones sobre cómo desarrollar sus procesos y herramientas a fin de aprovechar al máximo la seguridad y la virtualización de red.

Inventario y análisis de los procesos existentes

Una de las propuestas de valor clave de la virtualización de red es la automatización de los procesos generalmente manuales asociados con el ciclo de vida de las aplicaciones. Esto constituye una gran oportunidad para llevar a cabo una evaluación integral de los procesos existentes para determinar qué futuro tendrán con la virtualización de red.

Una sugerencia importante: no mantenga todos los procesos existentes a la hora de aplicar la seguridad y la virtualización de red de NSX. Si se hace, degradará las ventajas y el ahorro de costes que obtendría de otra manera. Identifique y comprenda todos los procesos de redes y seguridad existentes. Comprenda el efecto que la virtualización de red tiene en los siguientes procesos:

- Despliegue de aplicaciones
- Gestión de la configuración
- Gestión de cambios
- Gestión de la capacidad
- Gestión de incidencias y problemas

Comprenda la forma en que estos procesos funcionan en la actualidad, de principio a fin, además de cómo se pueden simplificar y optimizar a través de la automatización y coordinación. Descubrirá que los procesos o pasos existentes se pueden optimizar en gran medida o incluso, en algunos casos, se pueden dejar de usar.

Una vez que haya realizado un inventario exhaustivo, determine las prioridades para automatizar estos procesos de red y seguridad. Para obtener resultados satisfactorios rápidamente, céntrese en áreas que impliquen un alto valor y un esfuerzo reducido. No intente optimizar demasiados procesos a la vez; elija uno o dos para comenzar.

Práctica recomendada para el proceso: establecer parámetros de referencia

Antes de empezar, es importante establecer parámetros de referencia. Antes de realizar ningún cambio, determine los valores de referencia y documente el tiempo que tardan los procesos en la actualidad. Calcule el esfuerzo de las tareas y los tiempos de ciclo asociados a cada proceso. Realice estas mismas mediciones después de haber automatizado el proceso. Así podrá comparar y comunicar los resultados que se han logrado. Comprender el rendimiento ayudará a que el equipo logre sus objetivos (p. ej., reducir el tiempo de despliegue o el tiempo para detectar y aislar problemas) y a que establezca acuerdos de nivel de servicio adecuados para los usuarios.

Automatización del despliegue y la gestión

Después de haber realizado un inventario y una evaluación de los procesos actuales, el paso siguiente es la automatización del despliegue y la gestión de las aplicaciones o los servicios. Las organizaciones usan las funciones de automatización inherentes de la virtualización de red y NSX para lograr velocidad, estandarización, uniformidad y permitir auditorías. La automatización también permite reducir el tiempo de inactividad y los riesgos de seguridad asociados con los errores de configuración manuales. La automatización mejora la productividad del desarrollo y las pruebas, acelera el plazo de comercialización para las aplicaciones nuevas, ofrece configuraciones estandarizadas y uniformes, además de causar menos errores y ofrecer resoluciones más rápidas.

Si bien no se requieren herramientas de automatización para NSX, la mayoría de los clientes usan una combinación de herramientas y API de NSX para la automatización de la cloud. Estas herramientas y API se usan para automatizar el despliegue y la gestión de los servicios funcionales de NSX para redes virtuales (es decir, conmutación lógica de capa 2, enrutamiento de capa 3, equilibrio de cargas, cortafuegos y servicios perimetrales). La mayoría de las organizaciones que usan NSX automatizan varios servicios.

La situación actual típica es la siguiente: las redes físicas y las VLAN se siguen desplegando manualmente, en hardware especializado, mediante el uso de teclados y CLI. Como resultado, los cambios de red se encuentran en la ruta crítica del despliegue de aplicaciones. Como sabe, estos despliegues pueden durar días, semanas o más tiempo, hasta que la conectividad, el rendimiento, la disponibilidad y la seguridad de la red estén listos.

Además, las organizaciones usan NSX para automatizar el despliegue, la configuración, la gestión y la retirada de la virtualización de red y la seguridad. Con NSX, los equipos encargados de la red no necesitan configurar la multitud de conmutadores físicos con direccionamiento de tráfico y configuraciones de red, como VLAN, enrutamiento y reenvío virtual (VRF), centro de datos virtual (VDC), calidad de servicio (QoS), ACL, etc.

Una vez que se realiza la configuración inicial de la red física como una red subyacente, ya no se requiere la reconfiguración constante y frecuente con implementaciones de aplicaciones nuevas o cambios de requisitos de las aplicaciones. Ahora, todos estos cambios ocurren en el espacio de la red lógica utilizando herramientas de automatización.

Práctica recomendada para el proceso: centrarse en la automatización de TI

Le recomendamos que comience por automatizar el entorno de TI para poder cumplir con las solicitudes de servicio de manera más rápida. Una vez que se haya automatizado el entorno de TI, podrá añadir un portal de autoservicio y un catálogo de servicios para que los desarrolladores de aplicaciones e ingenieros de control de calidad (QA) tengan acceso a entornos completos con tan solo un clic. Ahora veamos algunas de las herramientas de automatización que usan los clientes de NSX.

Consideraciones sobre las herramientas

Según lo analizado anteriormente, es importante que primero identifique, comprenda y documente las tareas y los procesos que desea automatizar. Este paso es clave porque las herramientas de automatización de TI, como las plataformas de gestión de la cloud y los coordinadores, ofrecen diferentes características y funcionalidades. Todas estas herramientas requieren cierta inversión inicial para conocerlas y configurarlas; pero las ventajas valen la pena.

Puede utilizar vRealize Suite y OpenStack para el despliegue, la gestión y la coordinación de la infraestructura de red. Comience por automatizar tareas separadas para familiarizarse con la herramienta. Una vez que haya aprendido a usar la herramienta, puede pasar a flujos de trabajo en los que la aplicación y sus redes y seguridad se desplieguen y gestionen en conjunto en una pila completa. El operador de red local o de la cloud debe participar en la evaluación y la operación de cualquier herramienta que se use para la automatización de la red.

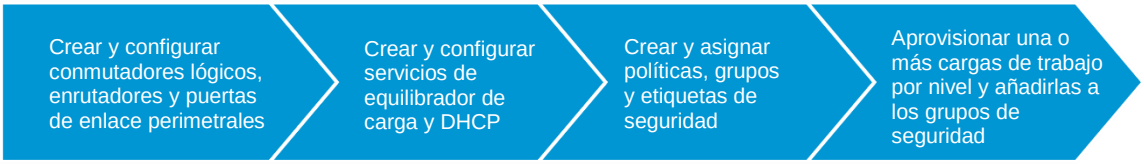
Estandarización y personalización de las configuraciones

Las organizaciones pueden estandarizar las configuraciones de recursos informáticos, almacenamiento, redes y seguridad de pilas de aplicaciones completas usando plantillas y políticas. Si necesitan hacer un cambio, modifican la plantilla y la envían a producción. El cambio se reflejará automáticamente en todas las cargas de trabajo que utilicen la plantilla. Se mantiene un registro de todos los cambios con fines de auditoría y conformidad.

El departamento de ingeniería puede publicar configuraciones estáticas o personalizables. En general, los entornos estáticos se usan para pilas con certificación para producción. Y los entornos personalizables son para los entornos de pruebas y de desarrollo. Con los entornos personalizables se pueden abordar el 80 % o más de los requisitos del usuario. Sin embargo, el desarrollador o el ingeniero de control de calidad pueden modificar estos entornos según sea necesario. Las cargas de trabajo se pueden activar con redes nuevas o conectar a redes existentes.

Ejemplo de automatización del proceso de un modelo

Veamos las tareas que se pueden automatizar para el modelo estandarizado de una aplicación de tres niveles:



Una vez que el proyecto se ha probado y validado, se publica en el catálogo de servicios para que lo usen los usuarios. El usuario hace clic en el elemento de servicio y la pila completa de aplicaciones (con toda su conectividad, disponibilidad y seguridad) se implementa en segundos.

Este servicio automatizado es mucho más rápido que una red física tradicional sin NSX, que suele tardar días o semanas. Las organizaciones evitan los tiempos de ciclo prolongados y las demoras en flujos de trabajo de tiques complejos, revisiones y aprobaciones de cambios, la detección y la validación de requisitos redundantes, además de la configuración manual.

Práctica recomendada para el proceso: acceso basado en funciones

Implemente el control de acceso basado en funciones en el portal de autoservicio según las funciones empresariales. Además, debería definir las políticas de reserva y de asignación de recursos de acuerdo con los grupos de negocio, realizar un seguimiento de los costes para la imputación de gastos y cumplir los niveles de servicio (SLA).

Automatización de las políticas de seguridad con grupos

NSX automatiza en forma nativa muchas tareas que se realizan manualmente con infraestructura de red física y seguridad. Por ejemplo, ofrece nuevas formas de definir y aplicar las políticas de seguridad a las máquinas virtuales en la capa de virtualización.

Estrategia antigua: de la manera antigua, los equipos de seguridad crean reglas de forma manual en base a direcciones IP, puertos y protocolos. La temida pesadilla de gestión «5-tupla».

Estrategia nueva: de la manera nueva, las políticas de seguridad se basan en grupos de seguridad. Puede definir un grupo de seguridad que contenga un conjunto de máquinas virtuales y crear una política de seguridad en torno a esas cargas de trabajo. Si añade otra máquina virtual al grupo, la política de seguridad se aplica automáticamente a las nuevas cargas de trabajo sin ninguna intervención manual. La pertenencia a los grupos puede aplicarse dinámicamente mediante etiquetas de seguridad y contexto o, alternativamente, solo contexto. Por ejemplo, las políticas de seguridad de NSX pueden incluir cortafuegos, antivirus y sistemas de prevención de intrusiones (IPS).

Los grupos de seguridad pueden ser estáticos o dinámicos y estar programados para activarse con cualquier metadato arbitrario sobre la carga de trabajo; por ejemplo, la identidad del grupo de usuarios, características del sistema operativo, nombres y etiquetas de máquinas virtuales, la presencia de un virus, etc. NSX asigna automáticamente el grupo y la política de seguridad adecuados en función del contexto relevante de virtualización, en lugar de solo la topología física.

Las políticas de seguridad previamente aprobadas se coordinan y gestionan de forma centralizada, lo cual reduce la expansión de las reglas y garantiza que la seguridad se aplique de manera precisa y uniforme. Este nuevo nivel de automatización reduce considerablemente la complejidad y los gastos operativos que conlleva la gestión de políticas de seguridad en las cargas de trabajo.

Cada equipo de seguridad usa una combinación única de dispositivos de seguridad de red para satisfacer las necesidades de su entorno. Aparte de la posibilidad de utilizar el cortafuegos distribuido de NSX, las organizaciones también deberían aprovechar la plataforma para automatizar las funciones avanzadas de seguridad de redes que están disponibles a través de los partners de tecnología de VMware.

Los equipos de seguridad de red suelen enfrentarse al desafío de coordinar servicios de seguridad de redes de varios proveedores, que no están relacionados en absoluto. Con NSX, esto es posible. NSX distribuye los servicios de red en el contexto de vNIC para formar una cadena de procesamiento lógica de servicios que se aplica al tráfico de red virtual. Se pueden insertar servicios de red de terceros en este canal lógico para permitir que se usen servicios físicos o virtuales. Las empresas usan NSX para crear políticas que utilicen la inserción, el encadenamiento y el direccionamiento de servicios de NSX con el objetivo de impulsar la ejecución de los servicios en el canal lógico.

Las herramientas de seguridad integradas también se benefician del modelo operativo que proporciona la plataforma de NSX. Gracias a estas integraciones, se genera un aumento considerable de la velocidad de despliegue, la eficacia de la gestión y la calidad del servicio, a la vez que se mantiene la separación de tareas entre los equipos de servidores, redes y seguridad.

Las prestaciones de seguridad avanzadas están disponibles por medio de integraciones con Palo Alto Networks, Intel Security, Trend Micro, Symantec, Checkpoint y otros partners de VMware NSX.

Creación de visibilidad a nivel de la aplicación con herramientas modernas

El hipervisor cuenta con una posición ideal y excepcional en el límite entre el entorno físico y el virtual. El vSwitch de NSX proporciona el mayor nivel de visibilidad y contexto, ya que detecta cada paquete según entra y sale de una máquina virtual. Además puede correlacionar las relaciones fluidas entre las aplicaciones, las redes virtuales, las redes físicas, etc.

A continuación, se detallan algunos ejemplos de escenarios en los que se demuestran las excepcionales funciones de supervisión y solución de problemas de NSX:

Resumen en tiempo real	Supervisión y solución de problemas	Depuración
Un operador puede elegir la interfaz de red de cualquier máquina virtual y ver un resumen en tiempo real de todos los flujos y su estado. No es necesario configurar capturas de paquetes completos en una herramienta remota ni cribar direcciones IP en busca de la máquina virtual.	Todos los aspectos de una red virtual están disponibles a través de la CLI y API centrales de NSX. De esta forma, se simplifican considerablemente las actividades de supervisión y solución de problemas, porque ya no es necesario averiguar la ubicación de un problema en la red. Además, no es necesario ir a diferentes consolas para solucionar problemas.	El vSwitch maneja en software cada paquete, ofreciéndole mayor visibilidad que en las redes tradicionales. Puede crear una transacción sintética sin necesidad de tener acceso a las máquinas virtuales invitadas. Los paquetes de Traceflow pueden introducirse en un canal de envío para permitir la depuración detallada de problemas en la ruta de datos (p. ej., políticas extremadamente restrictivas de ACL).

Los operadores ya usan muchas herramientas para gestionar y dar soporte a la infraestructura del centro de datos. Utilizan diferentes herramientas para las actividades de supervisión, solución de problemas y gestión de cambios. Con la virtualización de red, se puede usar el mismo conjunto de herramientas existentes para obtener visibilidad de las redes lógicas.

Las herramientas de supervisión en tiempo real son importantes en los entornos virtualizados que cambian constantemente, en los que la infraestructura y las aplicaciones migran de un servidor a otro de forma dinámica y la red se reconfigura automáticamente.

Práctica recomendada para el proceso: herramientas

Identifique las herramientas de VMware o de terceros que le den visibilidad de las relaciones de los objetos entre la infraestructura virtual y física de red, almacenamiento y recursos informáticos. La correlación entre los dominios de la infraestructura ayuda a limitar rápidamente el alcance de un problema a un dominio en particular y a reducir la necesidad de tener herramientas específicas de múltiples dominios.

Las mejores opciones suelen ser herramientas modernas, como vRealize Operations, Arkin, Riverbed, entre otras, que están específicamente diseñadas para entornos virtuales y físicos. Estas herramientas proporcionan una visión integral de la topología, el estado de las aplicaciones, la utilización y la capacidad.

Tenga en cuenta que es posible que una estrategia de un único proveedor no siempre proporcione la mejor visibilidad. Puede que para contar con un nivel óptimo de supervisión, alertas y solución de problemas, lo más adecuado sea usar varias herramientas, al igual que ocurre con la red física en la actualidad. Por ejemplo, es probable que use herramientas diferentes para el análisis del flujo de tráfico (p. ej., SolarWinds, NetQoS), el análisis de paquetes (p. ej., Wireshark, SteelCentral) y las alertas (p. ej., Netcool, OpenNMS).

Las redes virtuales proporcionan el mismo nivel de instrumentación que la red física a través de protocolos estándar (p. ej., estadísticas de paquetes y bytes a través de SNMP y las API, SPAN/SPAN de nivel 3, NetFlow/IPFIX, creación de reflejo de puerto y Syslog). Esto permite a las organizaciones dar el primer paso con las herramientas existentes de supervisión, alertas y solución de problemas, para más adelante realizar las transición a una herramienta moderna, como las mencionadas anteriormente.

Mensaje final sobre los procesos

La virtualización de red y NSX le ofrecen un motivo importante para evaluar la forma en que hace las cosas hoy en día, así como definir una forma mejor y más eficaz para avanzar hacia el futuro. Corregir todos los procesos se percibe como una tarea titánica: adopte una estrategia incremental para automatizar los procesos y así evitar la paralización. Las metodologías ágiles y de mejora continua son formas ideales de avanzar.

Tecnología

En esta sección, examinaremos las consideraciones sobre la arquitectura y la infraestructura al planificar, implementar y poner en marcha la virtualización de red y NSX. También trataremos casos de uso prácticos en torno a la microsegmentación y la recuperación ante desastres.

Diseño de la red física para ofrecer sencillez

Con NSX, la arquitectura de la red física está diseñada de manera simple para ofrecer conectividad y rendimiento. Eso puede ser tan simple como una estructura de capa 2 que ya esté usando en la actualidad o una estructura de capa 3 basada en una arquitectura leaf-spine. Puede comenzar con la primera y pasar gradualmente a la última.

NSX no impone requisitos estrictos con respecto a dónde se establecen los límites de la capa 2. Debido a que solo proporciona conectividad entre hosts, los cambios de configuración realizados en la red

física deberían ser relativamente poco frecuentes. Esto ayuda a evitar errores de configuración manuales.

La separación entre las topologías y los servicios de red del hardware físico, ha permitido que las estructuras leaf-spine de capa 3 se hayan generalizado. Esto le permite establecer una plataforma común con el mismo modelo lógico de redes, seguridad y gestión.

Con NSX es más viable realizar un cambio en la arquitectura de red, ya que abstrae la topología de red virtual (como las máquinas virtuales la ven), de la topología física. NSX libera a los diseñadores de redes para realizar una transición más sencilla a arquitecturas de leaf-spine que se usan el enrutamiento de capa 3 con múltiples rutas de igual coste (ECMP) sin bloqueo entre conmutadores de la parte superior del rack.

La red física subyacente tiene libertad para evolucionar independientemente de la red virtual; además su arquitectura está diseñada en torno a criterios de escalabilidad, rendimiento y solidez. El fallo de un enlace o un dispositivo no afecta a la conectividad de las aplicaciones.

El diseño de la estructura de capa 3 de ECMP ofrece uniformidad en cuanto a la configuración y mejora la interoperabilidad de los dispositivos. Las actualizaciones de hardware (p. ej., implementación de conmutadores nuevos) pueden separarse de NSX, con lo que no afecta a las cargas de trabajo en las redes virtuales. NSX es compatible con conmutadores de cualquier proveedor, que se pueden interconectar.

Las capas superpuestas de virtualización de red combinadas con arquitecturas de leaf-spine dan lugar a un mayor nivel de adaptabilidad y eficiencia operativa, un uso más eficaz del ancho de banda y escalabilidad para manejar la cantidad cada vez mayor de comunicación de este a oeste dentro del centro de datos. A la vez, los dominios de difusión de capa 2 más pequeños incrementan la estabilidad de la red.

Implementación incremental de la virtualización de red

La virtualización de red de NSX no es una propuesta de tipo «todo o nada». Las redes virtuales de NSX no precisan cambios en la red física subyacente. La virtualización de red puede coexistir de manera transparente en la red física con despliegues de aplicaciones existentes.

Las organizaciones tecnológicas cuentan con la flexibilidad de virtualizar partes de la red con simplemente añadir nodos de hipervisor a la plataforma de NSX. Además, mediante las puertas de enlace de software de NSX o los conmutadores de la parte superior del rack (es decir, hardware de partners de VMware), se ofrece la posibilidad de interconectar redes virtuales y físicas sin problemas. Se pueden usar para permitir el acceso a Internet de las cargas de trabajo conectadas a redes virtuales o para conectar directamente VLAN heredadas y cargas de trabajo nativas a redes virtuales.

Práctica recomendada para la tecnología: comenzar con un solo proyecto

La puesta en producción de la virtualización de red y la seguridad se debe realizar de forma progresiva. Le recomendamos comenzar con un solo caso de uso y un conjunto de aplicaciones. Identifique las cargas de trabajo que tengan un perfil de riesgo-recompensa interesante con el fin de aprovechar nuevas prestaciones. Para la primera implementación, elija cargas de trabajo que impliquen un riesgo bajo pero que sean lo suficientemente complejas como para validar NSX en el entorno.

El caso de uso que elija implementar determinará en gran medida cuáles serán los servicios funcionales de NSX que automatizará para las redes virtuales. Por ejemplo, si desea automatizar el despliegue de la red, puede comenzar con la conmutación de capa 2, el enrutamiento de capa 3 y los servicios perimetrales lógicos. Si desea implementar la microsegmentación, comenzará con el cortafuegos lógico.

Defina una estrategia y un método para poner continuamente nuevas características y funcionalidades de NSX en producción para los clientes. Establezca un sistema de información periódica, para que la empresa pueda saber de antemano qué está por venir y con qué puede contar para sus proyectos. Verá que los lanzamientos periódicos ayudan a incrementar la participación del usuario, la aceptación de los servicios y la satisfacción

del cliente. Dé opción a que los servicios se acepten de forma natural, en lugar de intentar forzar artificialmente una adopción generalizada.

Práctica recomendada para la tecnología: talleres

Mantener la relación con sus homólogos de negocio y tecnología en la organización es una manera excelente de garantizar el éxito de cualquier iniciativa, incluida la virtualización de red. Considere llevar a cabo talleres periódicos con los usuarios para informar e instruir a las partes interesadas sobre los servicios disponibles de seguridad y virtualización de red, además de ofrecerles información actualizada sobre los planes de desarrollo. Incentive a los propietarios de las aplicaciones y la infraestructura a que colaboren proporcionando requisitos para las versiones futuras, así como comentarios sobre las prestaciones que ya están disponibles en producción.

Caso de uso: segmentar en torno a los límites de las aplicaciones

Uno de los principales casos de uso que la mayoría de los clientes de NSX implementan y ponen en práctica desde un principio es la microsegmentación. La microsegmentación se ha considerado una arquitectura de seguridad recomendada durante mucho tiempo. Cuando los atacantes obtienen acceso a la red sin autorización, la segmentación puede ayudar a limitar su movimiento y evitar la vulneración de los datos. Sin embargo, la microsegmentación no alcanzó un uso generalizado en el pasado. Esto se debió a las limitaciones arquitectónicas en las redes físicas tradicionales que dificultan la puesta en marcha.

Con NSX, la microsegmentación es operativamente viable. La plataforma ofrece prestaciones nativas de segmentación y aislamiento. Al añadir servicios avanzados, es posible aprovechar el modelo operativo de NSX en dispositivos de seguridad de terceros.

El aislamiento es la base de la mayor parte de la seguridad de la red, ya sea con fines de conformidad, contención o simplemente evitar la interacción entre los entornos de desarrollo, prueba y producción. De manera predeterminada, las redes virtuales están aisladas de otras redes virtuales y de la red física subyacente, a menos que estén conectadas entre sí específicamente. No es necesario que los operadores gestionen subredes físicas, VLAN, ACL ni reglas de cortafuegos.

La segmentación está relacionada con el aislamiento, pero se aplica a niveles dentro de una red virtual con varios niveles. Tradicionalmente, la segmentación de la red es una función de un cortafuegos o enrutador físicos y se diseña para permitir o rechazar el tráfico entre segmentos o niveles de la red. Por ejemplo, los enrutadores y cortafuegos segmentan el tráfico entre un nivel web, un nivel de aplicación y un nivel de base de datos.

Desafíos actuales: los procesos tradicionales para configurar la segmentación son manuales, lentos y propensos a errores humanos, lo que puede dar lugar a vulneraciones de la seguridad. Para la implementación se requieren conocimientos especializados sobre sintaxis de configuración de los dispositivos, direccionamiento de redes, puertos de aplicaciones y protocolos.

Solución de virtualización de red: con NSX, la política de seguridad se aplica en la capa de virtualización, por lo que puede deshacerse de los métodos para desviar el tráfico este-oeste. La seguridad se aplica de manera transparente, incluso antes de que los paquetes lleguen al primer puerto de la red virtual. Al estar protegido desde el comienzo, el tráfico este-oeste sensible a la latencia puede desplazarse libre y directamente a su destino a través de la ruta de menor latencia.

La combinación del control centralizado con la implementación distribuida de servicios significa que se pueden aplicar políticas muy detalladas a cada interfaz virtual de forma operativamente viable. Por ejemplo, las máquinas virtuales en el mismo nivel que una aplicación de nivel tres pueden comunicarse

con otros niveles, pero no entre sí. De hecho, cada carga de trabajo está protegida con su propia seguridad.

Con NSX, puede configurar políticas de seguridad basadas en estructuras empresariales de alto nivel (p. ej., aplicación, usuario o grupo) en lugar de estructuras de infraestructura de bajo nivel (p. ej., dirección IP, puertos de aplicaciones y protocolos). Las políticas de seguridad se pueden aplicar con mayor precisión, exactitud y coordinación con la política corporativa, sin interpretación humana.

Diseño con movilidad y capacidad de recuperación de las cargas de trabajo

Tradicionalmente, las topologías de red física y el espacio de direcciones requerían que el departamento de TI cambiara las direcciones IP cuando se movían las aplicaciones. En algunos casos, las direcciones IP tienen códigos fijos en las aplicaciones, lo cual es aún más costoso porque se deben realizar cambios en los códigos y en las pruebas de regresión.

Usando NSX, las cargas de trabajo se liberan de las VLAN y de las direcciones IP, además se permiten la movilidad y la asignación sin restricciones de las cargas de trabajo en la estructura del centro de datos. Con NSX, la asignación de las cargas de trabajo no depende de la topología física ni de la disponibilidad de los servicios de la red física en una ubicación determinada.

NSX proporciona todo lo que necesita una máquina virtual desde el punto de vista de las redes, independientemente de su ubicación física. Las cargas de trabajo pueden moverse libremente entre subredes, zonas de disponibilidad o centros de datos, sin tener que efectuar operaciones para cambiar su IP. Si se mueve una carga de trabajo, todos sus servicios de red y seguridad se mueven con esta automáticamente, sin intervención humana.

Las organizaciones usan la movilidad y la asignación de cargas de trabajo de NSX para hacer lo siguiente:

- Desplegar las aplicaciones con mayor rapidez
- Migrar las cargas de trabajo a un centro de datos nuevo
- Actualizar la infraestructura física subyacente

Caso de uso: mejorar el uso de recursos de servidor con la virtualización de red

Las organizaciones también usan NSX para acceder a la capacidad del servidor disponible en otras ubicaciones del centro de datos u otro centro de datos. Esto permite un grado significativamente mayor de utilización y consolidación de los recursos de servidor. Todos estos casos de uso reducen considerablemente el coste operativo y mejoran la agilidad, además de aumentar el valor general de la inversión en virtualización de red y NSX.

En las topologías de red tradicionales, cada clúster o módulo tiene su propia capacidad de servidor. La reconfiguración de la red para acceder a ella desde otro módulo o clúster es demasiado lenta y propensa a errores humanos, por lo que se desperdicia la capacidad disponible en el servidor. A veces, nos referimos a esto como «capacidad de servidor sin utilizar» debido a que no se puede acceder a ella con facilidad. De hecho, la complejidad de los equipos y las topologías de red tradicionales limita la posibilidad de la organización tecnológica de usar mejor la capacidad disponible del servidor.

NSX permite ampliar la red para acceder a la capacidad disponible en cualquier lugar del centro de datos, sin modificar la infraestructura física existente. Si desea añadir otra máquina virtual, por ejemplo, en un servidor ubicado en otra subred o zona de disponibilidad, ponga en funcionamiento la máquina virtual y conéctela con el conmutador lógico. De esta forma, esas dos cargas de trabajo son adyacentes de la capa 2, a pesar de que pasan por varias subredes y zonas de disponibilidad en la red física.

Caso de uso: recuperación ante desastres

También puede usar NSX para complementar las soluciones de recuperación ante desastres existentes. Con el enfoque tradicional de las redes, para utilizar un sitio de seguridad para la recuperación ante desastres se precisa encontrar un equilibrio entre costes y funciones. En lugar de reproducir fielmente los servicios y la topología de red en una segunda ubicación, la mayoría de las organizaciones optan por una solución «lo suficientemente buena». Se hacen concesiones para reducir los costes, lo que implica una disminución de las prestaciones en relación con el centro de datos principal.

NSX permite una recuperación ante desastres sin concesiones. En lugar de tomar instantáneas de las máquinas virtuales, NSX le permite tomar una instantánea de la arquitectura de aplicaciones completa, incluidas las redes y la seguridad. Se envía una copia a un sitio de recuperación ante desastres, donde se mantendrá en espera, en cualquier hardware y sin ninguna disminución en la funcionalidad.

En caso de desastre, solo hay que activar la máquina virtual. La red a la que espera conectarse ya se está ejecutando en el sitio de recuperación. El objetivo del tiempo de recuperación se reduce significativamente, ya que no es necesario volver a configurar las cargas de trabajo ni los dispositivos de seguridad con direcciones IP nuevas.

Última reflexión sobre las consideraciones de la tecnología

La virtualización de red y NSX aportan una nueva y enorme flexibilidad para el entorno tecnológico, además de hacer posibles una serie de casos de uso valiosos. En lugar de sentirse abrumado con todas las posibilidades, céntrese primero en la calidad del servicio y amplíe el alcance del caso de uso inicial. Luego, elija un segundo caso de uso que desee poner en marcha. Ofrezca prestaciones nuevas solo después de que su equipo y los usuarios estén satisfechos con los niveles de calidad.

Pasos siguientes

La puesta en marcha de la seguridad y la virtualización de red debe considerarse un proceso; un proceso en el que la organización adquiera cada vez mayor madurez y sofisticación a medida que avance hacia el centro de datos definido por software y genere mayor valor a la empresa.

Su organización y los miembros del equipo cuentan con una variedad de opciones para obtener más información sobre cómo hacer realidad todas las ventajas operativas que están disponibles con la virtualización de red y NSX. Además conocerán cómo encaja la solución en el resto de la organización de TI y la complementa.

Paso uno: aprendizaje

Un excelente primer paso es ofrecer oportunidades de formación a la organización y las personas. Combine diferentes tipos de capacitación y formación: tanto formales (p. ej., talleres, cursos, laboratorios prácticos, programas) como informales (p. ej., sesiones de aprendizaje durante el almuerzo, consultoría, orientación). A fin de incentivar el aprendizaje, considere algunas formas de incluir los objetivos de capacitación y formación en los MBO personales.

Para comenzar, el equipo puede participar en los laboratorios prácticos de VMware (labs.hol.vmware.com), además de en los cursos y talleres impartidos por instructores disponibles a través de VMware Education (vmware.com/education). VMware también proporciona guías de operaciones de NSX enfocadas a la supervisión y la solución de problemas.

Paso dos: servicios de transformación

Obtener una perspectiva externa como ayuda para realizar la transición a la virtualización de red y NSX puede acelerar el proceso considerablemente. VMware proporciona servicios y talleres de transformación de las operaciones (vmware.com/consulting). Por ejemplo, el taller Envisioning para

la red como servicio (NaaS), permite identificar con claridad la visión, las metas y los objetivos de su nuevo modelo operativo de red y seguridad. Con el taller Discovery para NaaS puede identificar las funciones operativas y organizativas que necesita mejorar o crear a fin de hacer realidad el nuevo modelo operativo y lograr las metas y los resultados esperados.

Paso tres: prueba piloto sencilla

Una de las mejores formas de aprender sobre NSX y ver cómo se puede poner en práctica es comenzar una prueba piloto de producción con un solo caso de uso y algunas cargas de trabajo. Elija cargas de trabajo que impliquen un riesgo bajo pero que sean lo suficientemente complejas para maximizar el aprendizaje sobre la forma en que NSX funciona.

Póngase en contacto con el ejecutivo de cuentas de VMware o de un partner para que le ayude a comenzar.

Apéndice

Características de rendimiento final

La tabla siguiente resume las características de funcionamiento final de NSX para las áreas de personal, proceso y tecnología. Puede usarla como guía durante el proceso:

Vector	Estado actual/inicial	Estado futuro/final
Estructura org.	• Aislada con límites rígidos que necesitan muchos procesos • Procedimientos formales de solicitud • Traspaso a otro grupo • Búsqueda de responsables: nosotros frente a ellos • Metas, objetivos e incentivos diferentes y mal alineados	• Combinada con interacciones inmediatas • Comunicación abierta • Bucles de comentarios condensados • Alto nivel de colaboración • Metas e indicadores clave de rendimiento en común • Riesgos y responsabilidades compartidos
Personal	• Especialización • Conocimientos especializados limitados a un dominio • Uso de CLI y scripts • Conocimientos ampliamente disponibles • Crecimiento profesional limitado • Hardware centrado en la infraestructura	• Interdisciplinario y de varios dominios • Conocimientos especializados sobre varios dominios • Uso de herramientas de automatización y API • Aprendizaje continuo • Oportunidad de influir en la empresa a través de proyectos estratégicos • Centrado en el servicio y la aplicación
Procesos	• Manuales y propensos a errores • Sistemas complejos de tiques • Coordinación e interacción • Complejidad y embotellamientos • Espera para recibir servicio • Gastos operativos elevados • Centrado en la infraestructura	• Automatizado, estandarizado, uniforme y auditable • Bajo riesgo de errores manuales • Respuesta rápida/con respaldo de SLA • Interacciones en tiempo real • Gastos operativos reducidos • Centrado en el servicio o en la aplicación
Herramientas	• Heredadas, específicas del dominio • Herramientas múltiples y aisladas • Instrumentación solo física • Centradas en la infraestructura • Dificultad para aislar los problemas del servicio	• Herramientas modernas para varios dominios • Diseñadas para instrumentación virtual y física • Centradas en la aplicación • Supervisión integrada de servicios e infraestructura

Vector	Estado actual/inicial	Estado futuro/final
	• CLI de componentes individuales	• Facilidad para aislar los problemas del servicio • CLI y API centralizadas para instrumentar la infraestructura
Arquitectura	• Limitaciones arquitectónicas clásicas de nivel 3 • Obstrucciones de cargas de trabajo • Cortafuegos de puntos críticos • Núcleo sobrecargado • Rendimiento de enlaces • Servicios centralizados que dependen de la ubicación	• Estructura leaf-spine con ECMP sin bloqueo • Capa superpuesta con separación y abstracción • Portabilidad y movilidad de las cargas de trabajo • Aislamiento y segmentación nativos • Escalabilidad y adaptabilidad • Servicios distribuidos
Infraestructura	• Física con cambios lentos en la capa subyacente • Seguridad dependiente de la infraestructura • DR reducida, «lo suficientemente buena» • Interpretación humana de las políticas • Políticas centradas en la infraestructura • Estructuras de infraestructura de bajo nivel • Gestión fragmentada • Dependencia de proveedores de hardware • Dificultad para el encadenamiento de servicios	• Virtual con cambios dinámicos en la capa superpuesta • Seguridad centrada en la aplicación • DR sin concesiones • Políticas de seguridad legible por máquinas • Políticas centradas en la empresa • Estructuras empresariales de alto nivel • Gestión centralizada • Relación precio-rendimiento • Facilidad para el encadenamiento de servicios

Funciones de seguridad y redes de la cloud

Las siguientes descripciones le ayudarán a definir las funciones y las responsabilidades del personal de redes y seguridad de la cloud. Estas funciones de la cloud están a cargo de profesionales «tradicionales» de redes y seguridad, es decir, personas que ya forman parte de sus equipos.

En las pequeñas o medianas empresas, es habitual que una sola persona esté a cargo de dos o más de estas funciones. Por ejemplo, un solo ingeniero de red puede ser responsable de la arquitectura, el desarrollo y las operaciones de la red. No todas las organizaciones tendrán la necesidad de contar con una persona diferente en cada una de estas funciones.

Al otro extremo del espectro, es bastante común que las grandes empresas tengan varias personas a cargo de la misma función u otra similar. Por ejemplo, hemos visto muchas empresas multinacionales que tienen varios arquitectos o ingenieros de red de la cloud.

Funciones de red de la cloud

El *arquitecto de red de la cloud (CNA)* es responsable del desarrollo integral de las arquitecturas y los estándares de redes de la cloud de acuerdo con un modelo de consumo basado en servicios (red como servicio). El CNA está a cargo de las siguientes responsabilidades:

- Determina los requisitos técnicos y operativos de la red.
- Diseña redes físicas y lógicas que respondan a los requisitos de las aplicaciones (p. ej., capacidad y rendimiento).
- Desarrolla y valida pruebas para garantizar el cumplimiento de los requisitos.
- Guía la planificación e implementación de soluciones de redes de la cloud.

El *ingeniero de red de la cloud (CNE)* es responsable del diseño de bajo nivel de los servicios y la infraestructura de red, el desarrollo y la prueba de las funciones de red, el aprovisionamiento de la capacidad y la definición de la configuración de la red. El CNE está a cargo de las siguientes responsabilidades:

- Garantiza que se cumplen los requisitos del cliente y los niveles de servicio relacionados.
- Convierte los requisitos en proyectos lógicos y plantillas de configuración.
- Diseña, desarrolla y prueba flujos de trabajo y scripts personalizados para tareas rutinarias (p. ej., integración, implementación, supervisión y cumplimiento).
- Proporciona asistencia a la solución de problemas de soporte de nivel 2 y 3, además de proponer soluciones y solicitar correcciones.

El *operador de red de la cloud (CNO)* posee la responsabilidad global de todas las facetas de las operaciones posteriores, el cumplimiento con los requisitos operativos de las aplicaciones (p. ej., rendimiento y capacidad) y el mantenimiento de la infraestructura, las herramientas y las plataformas de red de la cloud. El CNO está a cargo de las siguientes responsabilidades:

- Ejecuta y controla la automatización para el despliegue, la gestión, la supervisión, las alertas y la solución de problemas.
- Supervisa proactivamente la infraestructura de red de la cloud y toma medidas con respecto a los eventos, antes de que afecten al servicio.
- Lleva a cabo la solución de problemas y el análisis de las causas principales, y aplica las soluciones y correcciones propuestas por el CNE.
- Proporciona soporte de nivel 2 y 3, además de gestionar incidentes, problemas y sus notificaciones.

Funciones de seguridad de la cloud

El *arquitecto de seguridad de la cloud (CSA)* posee la responsabilidad global de todas las facetas de la arquitectura, el diseño y el soporte de la infraestructura de seguridad de la cloud, en lo que respecta a la virtualización, la automatización, la coordinación y la supervisión de la seguridad de la red. El CSA está a cargo de las siguientes responsabilidades:

- Evalúa el riesgo de seguridad para las aplicaciones y la infraestructura de cloud, además proporciona orientación autorizada sobre las estrategias y soluciones de seguridad.
- Determina las funciones que se precisan de las políticas, procesos y auditoría de seguridad técnicos para cumplir con las metas y los requisitos de seguridad de la cloud.
- Desarrolla pruebas de validación para verificar las soluciones de seguridad de la cloud, además planifica y guía su implementación.
- Mantiene un conocimiento profundo sobre las amenazas y las estrategias de mitigación de riesgos.

El *ingeniero de seguridad de la cloud (CSE)* es responsable de convertir las políticas de seguridad en controles de seguridad que puedan auditarse. El CSE está a cargo de las siguientes responsabilidades:

- Diseña e implementa soluciones físicas y lógicas para implementar los controles de seguridad de la cloud.
- Coordina y automatiza los procesos de seguridad de la cloud (control, supervisión y auditoría).

- Integra e implementa servicios y herramientas de seguridad de la cloud que cumplen con los requisitos y los niveles de servicio.
- Participa en la notificación de problemas, investiga vulneraciones y recomienda e implementa soluciones de corrección.

El *operador de seguridad de la cloud (CSO)* es responsable de comprender, implementar, aplicar, verificar y mantener controles de seguridad específicos, según lo requerido por la evaluación de riesgos y las políticas de la organización. El CSO está a cargo de las siguientes responsabilidades:

- Supervisa, detecta y analiza anomalías, vulnerabilidades y amenazas de seguridad.
- Gestiona los registros de seguridad, garantiza el cumplimiento de los estándares de registro y ayuda en las auditorías de seguridad.
- Investiga, diagnostica y soluciona los problemas de seguridad de la cloud en respuesta a los incidentes.
- Implementa soluciones de seguridad y correcciones para vulnerabilidades.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
C/ Rafael Botí, 26 - 2ª planta, 28023 Madrid, España. Tel. +34 914125000 Fax +34 914125001 www.vmware.es