Planification de la transformation opérationnelle avec NSX

Meilleures pratiques concrètes

GUIDE

vmware®

Sommaire

Introduction

Ce livre blanc s'adresse principalement aux directeurs et responsables du Cloud, du réseau et de la sécurité. Il peut également s'avérer utile aux responsables et contributeurs individuels en charge de l'architecture, de l'ingénierie et des opérations, qui participent à l'exploitation de NSX au sein de l'entreprise.

La virtualisation du réseau est une avancée majeure qui aide les entreprises à gagner en rapidité, en flexibilité et en sécurité. Ses avantages sont au moins équivalents à ceux apportés par la virtualisation de l'environnement informatique ces dix dernières années. Pour tirer pleinement parti de la virtualisation du réseau, les entreprises ont tout intérêt à définir et à mettre en œuvre un plan opérationnel portant à la fois sur le **personnel**, les **processus** et la **technologie**.

VMware a travaillé en étroite collaboration avec des clients NSX existants pour comprendre les réalités de la virtualisation du réseau en environnement de production. Ces connaissances concrètes nous permettront de vous guider dans l'évaluation, le déploiement et l'exploitation de NSX. Vous et votre entreprise pourrez vous appuyer sur les meilleures pratiques qui vous semblent les mieux adaptées à votre cas particulier.

Même si ce livre blanc couvre un large éventail de meilleures pratiques, il est tout à fait possible de commencer à exploiter NSX sans procéder à des changements majeurs, quelle que soit votre situation actuelle. NSX étant d'une grande simplicité d'utilisation, vous n'aurez aucun mal à le mettre en œuvre.

Ce guide est divisé en trois sections principales fournissant des informations clés et décrivant les meilleures pratiques dans les domaines suivants :

Personnel

La virtualisation du réseau vous permet de libérer le potentiel de votre entreprise et de bénéficier d'avantages significatifs en transformant le mode de fonctionnement de votre département technologique. Ce changement doit être soigneusement préparé pour être bien compris et déployé de manière cohérente à tous les niveaux de l'entreprise. La mise en place d'une structure organisationnelle agile, reposant sur des équipes mixtes aux rôles et responsabilités clairement définis, est le meilleur moyen pour votre entreprise et votre personnel d'obtenir des résultats optimaux. Nous vous fournirons des informations et des conseils sur les structures organisationnelles, les stratégies d'implication et de communication internes, et les rôles et responsabilités.

Processus

La virtualisation du réseau ouvre de nouveaux horizons en matière de productivité via l'automatisation de processus manuels tout au long du cycle de vie des applications. La définition de la stratégie idéale de provisionnement, de gestion et de surveillance des applications et des services vous permettra de vous délester de vos processus et pratiques inutiles. Nous vous expliquerons comment aborder l'automatisation, la gestion des processus et les outils, avec, à l'appui, des cas d'utilisation instructifs.

Technologie

L'un des principaux avantages de la virtualisation du réseau est la séparation des fonctions de sécurité et réseau de l'infrastructure réseau physique sous-jacente, et leur abstraction dans une couche de virtualisation. Elle vous permet de mieux concevoir et gérer votre infrastructure. Nous vous fournirons des conseils sur les meilleures pratiques architecturales, la mise en œuvre progressive de l'infrastructure et le déploiement périodique de nouvelles fonctionnalités.

Ces meilleures pratiques ne constituent en aucun cas des exigences normatives ni des solutions universelles. Libre à vous de choisir celles qui, selon vous, correspondent le mieux aux caractéristiques, objectifs et priorités spécifiques de votre entreprise. N'adoptez pas une approche de changement radical. Commencez par un petit nombre de meilleures pratiques, puis déployez-en d'autres au fur et à mesure.

Certaines entreprises présument de leurs forces et déclarent forfait avant d'atteindre des performances optimales. Elles se privent ainsi de bon nombre d'avantages. Ne perdez jamais de vue l'objectif final : ne relâchez pas vos efforts et progressez pour l'atteindre.

Personnel

Le premier sujet que nous allons aborder est le personnel, à savoir l'organisation, les équipes et les collaborateurs qui composent le département technologique responsable de la fourniture et de la gestion de bout en bout des applications et des services. C'est sur le personnel que repose la mise en œuvre réussie de la virtualisation et de la sécurité du réseau.

Réflexions préliminaires sur la structure organisationnelle

La virtualisation du réseau et NSX n'exigent pas un type particulier de structure organisationnelle. La structure optimale dépend de facteurs spécifiques à votre entreprise. NSX a été exploité aussi bien au sein d'organisations cloisonnées traditionnelles que d'équipes Cloud mixtes parfaitement intégrées. Il est également possible de trouver un compromis entre des équipes entièrement cloisonnées et des équipes parfaitement mixtes.

La structure organisationnelle idéale sera fonction de plusieurs facteurs. Tenez compte des points suivants lors de la constitution de la structure :

- alignement des domaines et des disciplines ;
- maturité de la chaîne de valeur ;
- niveau de maîtrise technique ;
- expérience et expertise du personnel ;
- expérience et sophistication opérationnelles ;
- externalisation ;
- étendue de l'infrastructure et quantité d'applications ;
- déploiements existants et nouveaux.

Nos recommandations : concevez une structure d'équipe mixte

L'expérience sur le terrain indique que les équipes les plus productives sont étroitement intégrées, hautement collaboratives et autonomes. Ces équipes mixtes ont démontré une plus grande efficacité, avec des durées de cycle plus courtes, des boucles de rétroaction condensées et amplifiées, un meilleur partage des connaissances et un apprentissage continu. Dans l'idéal, l'équipe est colocalisée.

Nous avons vu des structures organisationnelles performantes composées d'équipes basées sur le domaine (calcul, stockage, réseau, sécurité, etc.) ou sur la discipline (architecture, développement et intégration, opérations, support, etc.). Dans les deux cas, les équipes sont responsables de l'infrastructure physique et virtuelle.

À mesure que vous migrerez l'infrastructure et les applications de votre réseau d'entreprise existant vers le Cloud, la répartition du personnel changera. Au fil du temps, les employés se consacreront davantage au Cloud qu'à votre réseau d'entreprise existant. Il est important de mettre en place un plan de communication et de formation pour aider l'organisation à comprendre cette évolution, à s'y préparer et à saisir de nouvelles opportunités de carrière. De même, vous devez faire clairement comprendre aux employés que leur contribution est essentielle au succès global du projet, qu'ils travaillent sur le réseau d'entreprise existant ou le Cloud.

Alignement sur des indicateurs de succès communs

L'alignement sur une stratégie commune reposant sur des objectifs, indicateurs et mesures incitatives clairement définis constitue un autre aspect clé de l'organisation. Votre équipe doit adopter une approche orientée services et être collectivement responsable du cycle de vie complet de la fourniture de services, depuis la réponse aux besoins de l'entreprise jusqu'à l'exécution et la gestion d'une charge de travail de production de haute qualité régie par un SLA.

Des indicateurs de succès doivent également être définis pour chaque équipe en fonction des facteurs qui comptent le plus pour votre organisation. Par exemple : délai de mise sur le marché, impact sur le chiffre d'affaires, meilleure réactivité face au marché, capacité d'innovation et/ou avantages pour les clients et satisfaction de la clientèle. Les objectifs doivent être ouvertement axés sur l'entreprise et les consommateurs du service.

Aidez l'équipe à définir et suivre ses propres indicateurs de succès, mais assurez-vous aussi qu'ils sont pertinents et alignés sur les objectifs communs. Outre leur conformité aux objectifs organisationnels, les indicateurs de performances clés doivent être précis, clairs, quantifiables et mesurables. Quels que soient les indicateurs de performances clés choisis par l'équipe, ils doivent être simples et commencer par un petit nombre de mesures de base judicieuses et faciles à comprendre.

Une fois les indicateurs de performances clés choisis, documentez votre situation actuelle pour établir une référence de base. Suivez et évaluez régulièrement votre progression (par exemple tous les mois ou les trimestres) par rapport à l'objectif final. Faites clairement comprendre aux membres d'équipe que le but n'est pas de dénigrer le travail de leurs collaborateurs ni les performances passées, mais de démontrer le succès de l'équipe et la valeur qu'elle apporte à l'entreprise. Ces mesures peuvent également être utilisées pour un examen et une évaluation plus efficaces, tangibles et pertinents des performances de chaque collaborateur.

Création d'une culture d'engagement et de responsabilisation

En matière de virtualisation et de sécurité du réseau, la culture est un facteur de succès important. La mise en place d'une culture qui soutient les principes du Software-Defined Data Center est cruciale. Le changement culturel ne doit pas émaner de la direction ou des cadres supérieurs, un défi très difficile à relever, mais des équipes au travers de leurs expériences, compétences et valeurs communes.

La définition d'indicateurs de succès communs permettra à une nouvelle culture d'émerger et de s'enraciner tout naturellement. La nouvelle culture reposera sur un objectif clair orienté entreprise et consommateurs, des responsabilités et risques communs, une collaboration et une coopération plus étroites, et des valeurs de confiance et de respect mutuels.

L'équipe : étroite collaboration entre les experts de la sécurité et du réseau

L'un des principaux avantages de la virtualisation du réseau est la séparation des fonctions de sécurité et réseau de l'infrastructure réseau physique sous-jacente, et leur abstraction dans une couche de virtualisation. Ce changement a soulevé un certain nombre d'interrogations, notamment : « Quelle équipe sera responsable de la sécurité et du réseau virtuel au niveau de l'hyperviseur ? » et « En quoi la virtualisation du réseau modifie-t-elle mes responsabilités ». Nous répondrons à ces questions dans cette section.

Le personnel actuellement en charge du réseau et de la sécurité s'occupera de la virtualisation et de la sécurité du réseau. NSX repose sur des concepts et technologies réseau qui exigent une expertise en matière de réseau. Seules vos équipes réseau possèdent les compétences techniques requises. Des experts en réseau et en sécurité sont nécessaires pour concevoir, déployer et exploiter les réseaux virtuels, tout comme cela est le cas pour les réseaux physiques.

Le réseau physique ne disparaît pas. Il devient juste beaucoup plus facile à gérer. Nous ne recommandons pas la création arbitraire d'équipes séparées pour les réseaux physiques et virtuels. Pour plus de rapidité et de flexibilité, une même équipe composée d'architectes, d'ingénieurs et d'opérateurs réseau doit être responsable à la fois de l'infrastructure physique sous-jacente et de l'infrastructure virtuelle superposée.

Cela n'empêche pas certains ingénieurs réseau de se consacrer davantage à la mise en rack, l'assemblage et la configuration de l'équipement physique, et d'autres à l'infrastructure virtuelle superposée. L'essentiel est que chacun d'eux fasse partie de la même équipe.

Les fonctions liées au réseau (architectes, ingénieurs, opérateurs, etc.) évoluent simplement pour inclure la virtualisation et la sécurité du réseau. La plupart des collaborateurs en charge du réseau et de la sécurité devront se former pour parfaire leur expertise et leurs compétences. Avec NSX, les services réseau s'exécutent dans la couche de l'hyperviseur. Les professionnels du réseau doivent posséder une certaine connaissance de la virtualisation des serveurs et comprendre ses enjeux pour les services réseau logiques.

Meilleure pratique en matière de personnel : formation

Au début du processus d'évaluation, la priorité est de s'assurer que tout le monde comprend les principes de la virtualisation du réseau et est formé à NSX ainsi qu'aux outils d'exploitation et de gestion associés qui font partie de l'écosystème du Cloud. VMware propose à cet effet plusieurs formules, dont des laboratoires d'essai pratique, des ateliers et des cours. Ces ressources s'adressent principalement aux professionnels du réseau non formés à la virtualisation des serveurs, mais conviennent aussi aux professionnels de la virtualisation des serveurs souhaitant s'initier à la virtualisation du réseau. Vous pouvez également mettre en place un programme favorisant le partage des connaissances et la formation interéquipes et intra-équipes en permettant à des collaborateurs de former d'autres équipes et groupes aux meilleures pratiques dans un cadre informel.

L'une des meilleures façons d'accélérer l'apprentissage est de commencer par un petit projet pilote et de l'évaluer. Impliquez toutes les fonctions requises (architectes, ingénieurs et opérateurs) dans les domaines du calcul, du stockage, du réseau et de la sécurité.

Démarrez avec une petite équipe transverse

Afin de limiter les risques de la transition vers la virtualisation du réseau, il est également recommandé de débuter avec une petite équipe transverse. Pour passer d'équipes cloisonnées à des équipes mixtes, procédez par étapes progressives. Nous avons observé deux types d'équipes transverses. Choisissez le modèle le mieux adapté à votre situation :

Équipe d'incubation	Équipe ad hoc
Si la migration, à terme, vers une équipe mixte est envisageable, mettez en place une équipe d'incubation. L'équipe d'incubation fera au final partie intégrante de la structure organisationnelle/l'organigramme. Elle doit être composée d'employés à plein-temps dédiés à 100 % à l'équipe.	Si la migration, à terme, vers une équipe mixte n'est pas envisageable, mettez en place une équipe ad hoc. L'avantage de ce type d'équipe est qu'elle peut être constituée et démantelée au gré des besoins. Ses membres travaillent à temps partiel et rendent compte de manière formelle à une autre équipe. Les équipes ad hoc ont surtout été observées au sein des organismes publics.

En général, l'équipe transverse est entièrement responsable d'une pile d'applications donnée ou d'un ensemble de piles d'applications. Elle doit être composée de spécialistes du calcul, du stockage, du réseau et de la sécurité. Leurs compétences couvrent l'architecture, l'ingénierie et les opérations. L'équipe doit être capable de prendre en charge tous les aspects du projet, depuis la conception, le développement et le test jusqu'au déploiement et aux opérations courantes. (Pour une description des rôles et responsabilités en matière de réseau et de sécurité, reportez-vous à l'annexe.)

Choix des agents du changement pour la première équipe

L'équipe initiale doit être composée d'agents du changement, de spécialistes, d'ambassadeurs et de leaders respectés. Choisissez des personnes que tout le monde aimerait voir faire partie de son équipe. Elles doivent savoir comment bâtir des relations interpersonnelles, favoriser la communication, et détecter et désamorcer les points de friction. Il doit s'agir d'experts qui encouragent le changement et donnent l'exemple. Si l'équipe n'est pas colocalisée, réunissez-la au début du projet pendant quelques semaines.

Les objectifs personnels des membres de l'équipe doivent être alignés sur ceux de l'équipe. Par exemple, si un membre d'équipe passe 50 % de son temps dans l'équipe d'incubation, ce travail doit représenter environ 50 % de ses objectifs personnels. Cela peut sembler évident, mais nous avons observé plusieurs cas où des personnes traitaient leur rôle dans l'équipe transverse davantage comme un hobby que comme une part importante de leurs attributions. Ce n'est pas l'un des meilleurs critères de réussite.

Meilleure pratique en matière de personnel : éviter tout effet de surprise

Ne prenez personne au dépourvu avant le déploiement. Nous avons vu des cas où les personnes en charge des opérations de réseau et de sécurité ont été impliquées trop tard dans le processus, ce qui a considérablement retardé les projets. Les équipes opérationnelles ont besoin de comprendre l'incidence de la virtualisation et de la sécurité du réseau sur la surveillance, les alertes et le dépannage. Il est également important pour elles de savoir comment leurs processus et outils doivent évoluer, un point que nous aborderons plus loin dans ce document.

Célébration des réussites et des opportunités de croissance

Lors de l'implication des équipes de sécurité et réseau dans le projet, expliquez-leur les avantages potentiels de ce dernier au niveau personnel et professionnel. La virtualisation et l'automatisation de l'infrastructure permettront au personnel en charge de la sécurité et du réseau de consacrer davantage de temps à de nouveaux projets intéressants. Il pourra se concentrer sur des projets stratégiques à plus forte valeur ajoutée pour l'entreprise. Par exemple, au lieu d'effectuer des tâches de routine, comme la configuration des VLAN, des équilibreurs de charge ou des règles de pare-feu, il pourra concevoir de nouveaux services générateurs de valeur pour l'entreprise, comme l'automatisation des processus interdomaines, le renforcement de la résilience, la planification de la capacité, ainsi que d'autres projets intéressants.

Expliquez également l'opportunité pour les innovateurs et visionnaires du département technologique de participer à la transformation du réseau et de la sécurité. Les résultats profiteront à tous ceux qui contribuent à la transformation, comme cela a été le cas pour ceux qui ont bâti leur carrière sur les réseaux IP et, plus récemment, sur la virtualisation de l'environnement informatique. Dans les deux cas, cela a donné naissance à de nouvelles catégories d'administrateurs, dotés de nouvelles compétences et connaissances. Participer à la transformation permettra non seulement au personnel de s'enrichir sur le plan professionnel, mais aussi d'accroître ses opportunités et sa valeur sur le marché du travail.

Susciter l'implication active des utilisateurs du service

Une autre manière positive de promouvoir l'équipe consiste à sensibiliser les consommateurs du service (par exemple les propriétaires d'application/d'infrastructure et les responsables métiers) aux nouvelles fonctionnalités. Invitez-les à participer activement, et à vous faire part de leurs besoins et commentaires. Ils voudront certainement connaître les répercussions du changement sur les fonctionnalités et l'expérience utilisateur. Il existe plusieurs activités efficaces pour favoriser leur implication :

Points de contact réguliers : organisez des ateliers périodiques pour informer et recueillir les besoins/commentaires.

Résultats concrets : expliquez que l'équipe développe de nouvelles fonctionnalités de manière régulière, ce qui aura pour effet d'augmenter l'engagement client.

La communication des réussites à l'échelle de l'entreprise est la bienvenue

Il est recommandé de promouvoir le projet auprès des membres de l'équipe et des consommateurs du service, mais aussi auprès des branches d'activité ou à l'échelle de l'entreprise tout entière. L'objectif est de susciter l'adhésion du plus grand nombre au projet et de présenter la plate-forme en tant que mode de fonctionnement de facto. Partagez des témoignages intéressants sur les résultats du projet au niveau métier et informatique. Vous pouvez assurer cette promotion en combinant présentations, discussions, articles, billets de blog, réseaux sociaux, e-mails et/ou démonstrations. Tous les membres de l'équipe doivent se considérer comme des ambassadeurs du projet. La célébration des réussites, petites et grandes, est le propre des entreprises performantes. Il s'agit d'une pratique importante qui doit faire partie intégrante de la gestion du changement technologique.

Difficulté du changement : parvenir à une compréhension commune

Nous savons tous à quel point le changement est un processus difficile, particulièrement lent dans des domaines et des disciplines spécifiques, qui peut être perçu par certains comme une menace potentielle à leur carrière ou à leurs moyens de subsistance. Ces facteurs peuvent se traduire par une résistance au progrès. Certaines personnes s'opposent activement à la transformation. La meilleure approche est de parvenir à une compréhension commune des avantages potentiels de la virtualisation du réseau grâce à une communication et à un plaidoyer sincères, et à la promotion des réussites du département technologique. Vous devez être transparent, ouvert et prêt à répondre à la question : « Qu'est-ce que j'y gagne ? Qu'est-ce que nous y gagnons ? ».

Processus

Dans cette section, nous allons voir l'impact de la virtualisation du réseau sur les processus opérationnels, les étapes à suivre pour décortiquer et comprendre vos processus existants, et comment faire évoluer vos processus et outils afin de tirer pleinement parti de la virtualisation et de la sécurité du réseau.

Inventaire et analyse des processus existants

L'un des atouts clés de la virtualisation du réseau est l'automatisation de processus habituellement manuels associés au cycle de vie des applications. C'est l'occasion idéale de procéder à une évaluation globale de vos processus existants afin de déterminer comment les faire évoluer avec la virtualisation du réseau.

Conseil utile : ne vous contentez pas de conserver tous vos processus existants avec la plate-forme de virtualisation et de sécurité du réseau NSX. Vous perdriez les avantages et les économies potentielles dont vous pourriez normalement bénéficier. Identifiez et analysez tous les processus existants en matière de réseau et de sécurité. Déterminez l'impact de la virtualisation du réseau sur les processus suivants :

- provisionnement des applications ;
- gestion des configurations ;
- gestion des modifications ;
- gestion de la capacité ;
- gestion des incidents et des problèmes.

Vous devez comprendre le fonctionnement actuel de ces processus, de bout en bout, et déterminer comment les simplifier et les rationaliser grâce à l'automatisation et à l'orchestration. Vous découvrirez que les processus existants, ou certaines de leurs étapes, peuvent être considérablement rationalisés, voire éliminés.

Après un inventaire approfondi, définissez les priorités d'automatisation de ces processus de sécurité et réseau. Pour des résultats rapides, concentrez-vous sur les aspects à forte valeur ajoutée qui demandent le moins d'efforts. N'essayez pas de rationaliser un trop grand nombre de processus à la fois. Choisissez-en un ou deux pour commencer.

Meilleure pratique en matière de processus : tests de performances

Avant de commencer, il est important de procéder à des tests de performances. Préalablement à tout changement, documentez la durée d'exécution actuelle de vos processus afin d'établir une référence de base. Calculez les efforts et durées de cycle associés à chaque processus. Remesurez-les après l'automatisation des processus. Vous pourrez ainsi comparer les résultats obtenus et les communiquer. L'analyse des performances aidera votre équipe à atteindre ses objectifs (réduire les délais de provisionnement, de détection et d'isolation des problèmes, etc.) ainsi qu'à définir des SLA appropriés pour les utilisateurs.

Automatisation du provisionnement et de la gestion

Une fois les processus actuels inventoriés et évalués, l'étape suivante consiste à automatiser le provisionnement et la gestion de vos applications ou services. Les entreprises utilisent les fonctions d'automatisation inhérentes à la virtualisation du réseau et à NSX pour bénéficier de meilleures performances en termes de vitesse, de normalisation, de cohérence et d'auditabilité. L'automatisation réduit en outre les interruptions de service et les risques de sécurité résultant d'erreurs manuelles. Elle augmente la productivité en matière de développement et de test, accélère la mise sur le marché des nouvelles applications, assure la normalisation et la cohérence des configurations, réduit les erreurs et permet une résolution plus rapide des problèmes.

Bien que NSX n'exige pas d'outils d'automatisation, la plupart des clients utilisent une combinaison d'outils et d'API NSX pour l'automatisation du Cloud. Ces outils et API servent à automatiser le provisionnement et la gestion des services fonctionnels de NSX pour les réseaux virtuels (commutation logique de couche 2, routage de couche 3, équilibrage de charge, protection par pare-feu et services de périmètre). La plupart des entreprises utilisent NSX pour automatiser plusieurs services.

Situation actuelle type : les réseaux physiques et les VLAN continuent d'être provisionnés manuellement, sur du matériel spécialisé, via un clavier et des CLI. La modification du réseau est donc une composante essentielle du déploiement d'applications. Comme vous le savez, satisfaire aux exigences de connectivité réseau, de performances, de disponibilité et de sécurité des applications peut prendre des jours, des semaines, voire plus, ce qui ralentit leur déploiement.

Avec la mise en œuvre de NSX : les entreprises utilisent NSX pour automatiser le provisionnement, la configuration, la gestion et la mise hors-service de la virtualisation et de la sécurité du réseau. NSX dispense les équipes réseau de configurer une multitude de commutateurs physiques avec la réorientation du trafic et les configurations réseau (VLAN, VRF, VDC, QoS, ACL, etc.).

Une fois la configuration initiale du réseau physique en tant que réseau sous-jacent effectuée, plus aucune reconfiguration fréquente et régulière n'est nécessaire lors de nouveaux déploiements d'applications ou en cas d'évolution des besoins applicatifs. Tous ces changements s'effectuent désormais dans l'espace logique du réseau au moyen d'outils d'automatisation.

Meilleure pratique en matière de processus : privilégier l'automatisation de l'informatique

Il est recommandé de commencer par l'automatisation de l'informatique afin de répondre plus rapidement aux demandes de service. Une fois l'informatique automatisée, vous pouvez ajouter un portail en libre-service et un catalogue de services pour permettre aux développeurs d'applications et aux ingénieurs de l'assurance qualité d'accéder à des environnements complets d'un simple clic. Examinons à présent certains des outils d'automatisation utilisés par les clients NSX.

Considérations relatives aux outils

Comme expliqué précédemment, il est important de commencer par identifier, analyser et documenter les tâches et processus que vous souhaitez automatiser. Il s'agit d'une étape clé, car les outils d'automatisation informatique, tels que les orchestrateurs et plates-formes de gestion du Cloud, offrent différentes fonctionnalités. Un minimum d'investissement initial est nécessaire pour se former à tous ces outils et les configurer, mais le jeu en vaut la chandelle.

vRealize Suite et OpenStack permettent de provisionner, de gérer et d'orchestrer l'infrastructure réseau. Commencez par automatiser des tâches distinctes pour apprendre à utiliser l'outil. Une fois familiarisé avec l'outil, vous pourrez passer aux workflows dans lesquels l'application, ses ressources réseau et sa sécurité sont provisionnées et gérées conjointement dans une pile complète. L'opérateur réseau ou l'opérateur réseau Cloud doit participer à l'évaluation et à l'exploitation de n'importe quel outil utilisé pour l'automatisation du réseau.

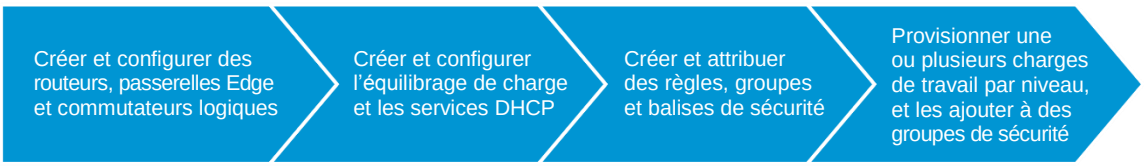
Normalisation et personnalisation des configurations

Les entreprises peuvent normaliser les configurations de calcul, de stockage, de réseau et de sécurité de piles d'applications complètes à l'aide de modèles et de règles. Si elles ont besoin d'apporter un changement, il leur suffit de modifier le modèle et de le lancer en production. Le changement sera automatiquement répercuté sur toutes les charges de travail qui utilisent ce modèle. Un registre de tous les changements est tenu à jour à des fins d'audit et de conformité.

L'équipe d'ingénierie peut publier des configurations statiques et/ou personnalisables. Les environnements statiques sont généralement destinés aux piles certifiées pour une mise en production. Les environnements personnalisables sont quant à eux utilisés en tant que sandbox de test et développement. Ils satisfont à au moins 80 % des exigences de l'utilisateur, mais peuvent être modifiés par le développeur ou l'ingénieur de l'assurance qualité en fonction des besoins. Il est possible de configurer les charges de travail pour qu'elles s'exécutent avec de nouveaux réseaux ou se connectent à des réseaux existants.

Exemple d'automatisation du processus de création de schéma

Examinons les tâches qu'il est possible d'automatiser pour la création d'un schéma d'application normalisée à trois niveaux :



Une fois testé et validé, le schéma est publié dans le catalogue de services et prêt à être consommé par les utilisateurs. L'utilisateur clique sur le service et l'intégralité de la pile d'applications, avec toutes ses exigences de connectivité, de disponibilité et de sécurité associées, est déployée en quelques secondes.

Ce service automatisé est nettement plus rapide qu'un réseau physique traditionnel sans NSX, dont la mise en place peut prendre plusieurs jours ou même semaines. Les entreprises s'épargnent ainsi les longs temps de cycle et retards liés aux workflows complexes de tickets, à l'examen et l'approbation des changements, aux efforts redondants d'identification et de validation des exigences, et à la configuration manuelle.

Meilleure pratique en matière de processus : accès basé sur les rôles

Mettez en œuvre un contrôle d'accès au portail en libre-service basé sur les rôles métiers. Vous devez également définir des règles de réservation et d'allocation des ressources en fonction des groupes métiers, suivre les coûts pour la refacturation, et vous engager sur des niveaux de service (SLA).

Automatisation des règles de sécurité à l'aide de groupes

NSX automatise en natif un grand nombre des tâches qui sont exécutées manuellement dans les infrastructures de sécurité et réseau physiques. Par exemple, il propose de nouvelles méthodes de définition et d'application de règles de sécurité aux VM dans la couche de virtualisation.

Ancienne approche : avec l'ancienne méthode, les équipes de sécurité créent des règles manuellement en fonction des adresses IP, des ports et des protocoles. Le cauchemar de la gestion à « 5-uplet ».

Nouvelle approche : avec la nouvelle méthode, les règles de sécurité sont basées sur des groupes de sécurité. Vous pouvez définir un groupe de sécurité comprenant un ensemble de VM et créer une règle de sécurité pour ces charges de travail. Si vous ajoutez une VM au groupe, la règle de sécurité est automatiquement appliquée aux nouvelles charges de travail sans intervention manuelle. L'appartenance aux groupes peut être définie de manière dynamique en fonction des balises de sécurité et/ou du contexte. Les règles de sécurité NSX peuvent, par exemple, concerner le pare-feu, l'antivirus et le système de prévention d'intrusions.

L'appartenance aux groupes de sécurité est statique ou dynamique. Elle est programmée en fonction de n'importe quelle métadonnée arbitraire relative à la charge de travail, comme l'identité du groupe d'utilisateurs, les caractéristiques du système d'exploitation, les noms et balises de VM, la présence d'un virus, etc. NSX attribue automatiquement le groupe et la règle de sécurité appropriés en fonction du contexte de virtualisation pertinent au lieu de se baser uniquement sur la topologie physique.

Les règles de sécurité préapprouvées sont orchestrées et gérées de manière centralisée, ce qui limite leur prolifération et garantit une application correcte et cohérente de la sécurité. Ce nouveau niveau d'automatisation réduit considérablement la complexité des opérations et les dépenses liées à la gestion des règles de sécurité pour les différentes charges de travail.

Toutes les équipes de sécurité ont recours à une combinaison unique d'appliances de sécurité réseau afin de répondre aux besoins de leur environnement. Outre la protection par pare-feu distribué de NSX, les entreprises doivent également utiliser la plate-forme pour automatiser les solutions de sécurité réseau avancées disponibles auprès des partenaires technologiques VMware.

Les équipes de sécurité réseau ont souvent des difficultés à coordonner les services de sécurité réseau indépendants les uns des autres qui proviennent de plusieurs fournisseurs. NSX facilite la procédure. Il distribue les services réseau au contexte de la carte réseau virtuelle pour former un pipeline logique de services appliqués au trafic du réseau virtuel. Des services réseau tiers peuvent être introduits dans ce pipeline logique, ce qui permet l'utilisation de services physiques ou virtuels. Avec NSX, les entreprises peuvent créer des règles exploitant l'orientation du trafic, le chaînage et l'insertion des services NSX pour piloter l'exécution des services dans le pipeline logique.

Les outils de sécurité intégrés tirent également parti du modèle opérationnel fourni par la plate-forme NSX. Ces intégrations améliorent considérablement la vitesse de provisionnement, la gestion et la qualité de service tout en maintenant la séparation des tâches entre les équipes en charge des serveurs, du réseau et de la sécurité.

Des fonctions de sécurité avancées sont accessibles via les intégrations avec les produits de différents partenaires VMware NSX, tels que Palo Alto Networks, Intel Security, Trend Micro, Symantec et Checkpoint.

Visibilité au niveau des applications à l'aide d'outils modernes

L'hyperviseur est idéalement situé à la frontière entre l'environnement physique et virtuel. Comme il voit tous les paquets qui entrent et sortent d'une VM, le vSwitch NSX offre un très haut niveau de visibilité et de contexte. Il permet en outre de corréler les relations fluides entre les applications, les réseaux virtuels, les réseaux physiques et bien d'autres composants.

Les exemples de scénarios suivants illustrent les fonctions de surveillance et de dépannage uniques de NSX :

Synthèse en temps réel	Surveillance et dépannage	Débogage
Un opérateur peut sélectionner n'importe quelle interface réseau de machine virtuelle, et obtenir une synthèse en temps réel de tous les flux de trafic associés, avec leur état. Il est inutile de configurer des captures complètes de paquets vers un outil distant et de passer au crible les adresses IP à la recherche de la VM.	Chaque aspect d'un réseau virtuel est accessible via la CLI et l'API centrales de NSX. Cela simplifie considérablement les activités de surveillance et de dépannage dans la mesure où vous n'avez plus à rechercher à quel endroit du réseau se situe le problème. En outre, vous n'avez plus besoin de jongler avec plusieurs consoles pour le dépannage.	Le vSwitch gère chaque paquet par voie logicielle, ce qui vous garantit une meilleure visibilité par rapport aux réseaux traditionnels. Vous pouvez créer une transaction synthétique sans même avoir accès aux VM clientes. Il est possible d'injecter des paquets Traceflow dans un pipeline de transfert en vue d'un débogage granulaire des problèmes dans le chemin de données (par exemple, dans le cas de règles ACL excessivement restrictives).

Les opérateurs font déjà appel à un grand nombre d'outils pour la gestion et le support de l'infrastructure du Data Center. Ils utilisent différents outils pour la surveillance, le dépannage et la gestion des changements. Avec la virtualisation du réseau, ces mêmes outils vous offrent toute la visibilité requise sur les réseaux logiques.

Les outils de surveillance en temps réel jouent un rôle important dans les environnements virtualisés en constante évolution où l'infrastructure et les applications sont transférées d'un serveur à l'autre de manière dynamique et où le réseau est automatiquement reconfiguré.

Meilleure pratique en matière de processus : outils

Identifiez les outils VMware ou tiers qui vous offrent toute la visibilité requise sur les relations entre les objets de l'infrastructure virtuelle et physique de calcul, stockage et réseau. La corrélation entre les domaines de l'infrastructure vous aide à restreindre rapidement le périmètre d'un problème à un domaine spécifique et évite le recours à plusieurs outils propres à chaque domaine.

Des outils modernes, tels que vRealize Operations, Arkin, Riverbed, etc., constituent généralement les meilleures options. Il s'agit d'outils spécialement conçus pour les environnements virtuels et physiques. Ils offrent une vue complète de la topologie, de l'intégrité des applications, du taux d'utilisation et de la capacité.

N'oubliez pas qu'une approche mono-fournisseur ne vous garantit pas nécessairement une visibilité optimale. Le recours à plusieurs outils peut optimiser la surveillance, les alertes et le dépannage, comme cela est le cas aujourd'hui pour votre réseau physique. Par exemple, vous utiliserez probablement différents outils pour l'analyse des flux de trafic (SolarWinds, NetQoS, etc.), l'analyse des paquets (Wireshark, SteelCentral, etc.) et les alertes (Netcool, OpenNMS, etc.).

Les réseaux virtuels offrent le même niveau d'instrumentation que les réseaux physiques via des protocoles standard (comme les statistiques au niveau des paquets et des octets via SNMP et les API, SPAN/L3 SPAN, NetFlow/IPFIX, la mise en miroir des ports et Syslog). Les entreprises peuvent ainsi commencer avec leurs outils existants de surveillance, d'alertes et de dépannage, puis passer à un outil moderne, tel que ceux indiqués plus haut.

Un dernier mot à propos des processus

La virtualisation du réseau et NSX sont l'occasion idéale d'évaluer votre mode de fonctionnement actuel et de voir comment aller de l'avant de manière plus efficace. Corriger tous les processus peut sembler une tâche titanesque. Pour éviter la paralysie, optez pour une approche progressive de l'automatisation des processus. Les méthodologies d'amélioration graduelle et continue sont une bonne façon de progresser.

Technologie

Dans cette section, nous aborderons les points à prendre en considération en matière d'architecture et d'infrastructure lors de la planification, du déploiement et de l'exploitation de la virtualisation du réseau et de NSX. Nous examinerons également des cas d'utilisation pratiques de la micro-segmentation et de la reprise d'activité.

Conception simple du réseau physique

Avec NSX, l'architecture du réseau physique est conçue de manière simple pour la connectivité et les performances. Vous pouvez, par exemple, vous appuyer sur un simple fabric de couche 2 que vous utilisez déjà actuellement, ou bien sur un fabric de couche 3 reposant sur une architecture Leaf-Spine. Vous pouvez commencer par la première option et migrer progressivement vers la seconde.

NSX n'impose aucune exigence stricte quant aux limites de la couche 2. Les changements de configuration du réseau physique seront relativement rares dans la mesure où ce dernier sert uniquement à assurer la connectivité entre les hôtes. Cela évite les erreurs de configuration manuelles.

La dissociation des services/topologies réseau et du matériel physique a contribué à l'essor des fabrics Leaf-Spine de couche 3. Cela permet de mettre en place une plate-forme commune reposant sur un même modèle logique de réseau, de sécurité et de gestion.

En séparant la topologie du réseau virtuel, telle que perçue par les VM, de la topologie physique, NSX simplifie la modification de l'architecture réseau. NSX permet aux concepteurs réseau de migrer plus facilement vers des architectures Leaf-Spine utilisant un routage de couche 3 de type ECMP (Equal-Cost Multi-Path) non bloquant entre les commutateurs ToR (Top-of-Rack).

Le réseau physique sous-jacent peut évoluer indépendamment du réseau virtuel, et son architecture est conçue selon des critères d'évolutivité, de débit et de robustesse. La panne d'un périphérique ou d'une liaison n'affecte pas la connectivité des applications.

La conception du fabric ECMP de couche 3 garantit l'uniformité des configurations et renforce l'interopérabilité des périphériques. Les mises à niveau du matériel (comme le déploiement de nouveaux commutateurs) sont indépendantes de NSX, ce qui évite tout impact sur les charges de travail s'exécutant sur vos réseaux virtuels. NSX prend en charge les commutateurs de n'importe quel fournisseur et leur interconnexion.

Combinées aux architectures Leaf-Spine, les superpositions de virtualisation réseau assurent une résilience accrue, une meilleure efficacité opérationnelle, une utilisation plus efficace de la bande passante et une évolutivité optimale pour gérer le volume de communications est-ouest en constante augmentation au sein du Data Center. Les domaines de diffusion L2 plus petits augmentent quant à eux la stabilité du réseau.

Mise en œuvre progressive de la virtualisation du réseau

Avec la virtualisation du réseau NSX, vous n'avez pas à choisir entre tout ou rien. Les réseaux virtuels NSX ne requièrent aucune modification du réseau physique sous-jacent. La virtualisation du réseau peut coexister en toute transparence avec les applications déjà présentes sur le réseau physique.

Les départements technologiques disposent de la flexibilité nécessaire pour virtualiser certaines parties du réseau par simple ajout de nœuds d'hyperviseur à la plate-forme NSX. En outre, des passerelles logicielles NSX, ou des commutateurs ToR physiques proposés par des partenaires VMware, permettent d'interconnecter des réseaux physiques et virtuels de manière transparente. Vous pouvez, par exemple, les utiliser pour prendre en charge l'accès Internet des charges de travail connectées à des réseaux virtuels, ou bien pour connecter directement des VLAN hérités et des charges de travail bare metal à des réseaux virtuels.

Meilleure pratique en matière de technologie : commencer par un seul projet

Déployez la virtualisation et la sécurité du réseau de manière progressive. Nous vous recommandons de commencer par un seul cas d'utilisation et ensemble d'applications. Identifiez les charges de travail présentant un profil de risques/bénéfices intéressant pour tirer parti des nouvelles fonctionnalités. Pour votre première mise en œuvre, choisissez des charges de travail à faible risque, mais suffisamment complexes pour valider les avantages de NSX dans votre environnement.

Le cas d'utilisation sélectionné déterminera, dans une large mesure, les services fonctionnels NSX que vous automatiserez pour vos réseaux virtuels. Par exemple, si vous automatisez le provisionnement réseau, vous pouvez débuter avec la commutation logique de couche 2, le routage de couche 3 et les services de périmètre. Si vous implémentez la micro-segmentation, vous commencerez avec la protection par pare-feu logique.

Définissez une stratégie et une méthode de déploiement continu de nouvelles fonctionnalités NSX pour vos clients. Établissez une cadence régulière sur laquelle l'entreprise sait qu'elle pourra compter pour mener à bien ses projets. Vous vous apercevrez que des versions fréquentes favorisent l'implication des utilisateurs, l'adoption des services et la satisfaction des clients. Au lieu d'imposer artificiellement l'adoption généralisée des services, laissez les choses se faire naturellement.

Meilleure pratique en matière de technologie : ateliers

Maintenir le contact avec les différents collaborateurs métiers et technologiques de votre entreprise est un excellent moyen d'assurer le succès de tout projet, y compris de la virtualisation du réseau. Organisez des ateliers périodiques avec les utilisateurs pour informer les différentes parties prenantes des services de virtualisation et de sécurité du réseau actuellement disponibles, et leur communiquer les plans d'évolution. Encouragez les propriétaires d'application et d'infrastructure à collaborer en vous faisant part de leurs exigences pour les prochaines versions et de leurs commentaires sur les fonctionnalités déjà en production.

Cas d'utilisation : segmentation autour des limites des applications

La micro-segmentation constitue l'un des premiers cas d'utilisation implémentés par la plupart des clients NSX. Elle est depuis longtemps considérée comme une bonne pratique en matière d'architecture de sécurité. Lorsque des pirates s'infiltrent dans le réseau, la segmentation peut en effet limiter leur progression et empêcher toute violation des données. Cette technologie n'a cependant pas connu l'essor escompté en raison des limitations architecturales des réseaux physiques traditionnels qui compliquent sa mise en œuvre.

NSX lève les obstacles opérationnels à l'adoption de la micro-segmentation. La plate-forme assure l'isolation et la segmentation en natif. L'intégration de services avancés permet à des appliances de sécurité tierces de tirer parti du modèle opérationnel de NSX.

L'isolation constitue la base de la plupart des systèmes de sécurité réseau. Elle est utilisée à des fins de conformité ou de confinement, ou encore pour empêcher toute interaction entre les environnements de développement, de test et de production. Les réseaux virtuels sont isolés les uns des autres, mais aussi du réseau physique sous-jacent par défaut, sauf s'ils sont explicitement reliés entre eux. Les opérateurs n'ont pas besoin de définir des sous-réseaux physiques, des VLAN, des listes de contrôle d'accès (ACL) ni des règles de pare-feu.

La segmentation est similaire à l'isolation, mais s'applique aux différents niveaux d'un réseau virtuel n-tier. Traditionnellement, la segmentation réseau est une fonction des pare-feu ou routeurs physiques conçue pour autoriser ou interdire le trafic entre des niveaux ou segments réseau. Par exemple, les routeurs et les pare-feu segmentent le trafic entre un niveau Web, un niveau applicatif et un niveau de base de données.

Problématiques actuelles : les processus classiques de configuration de la segmentation sont manuels, longs et propices aux erreurs, ce qui peut entraîner des violations de sécurité. La mise en œuvre de la segmentation nécessite une expertise spécifique en matière de syntaxe de configuration des périphériques, d'adressage réseau, de ports applicatifs et de protocoles.

Solution de virtualisation du réseau : avec NSX, la règle de sécurité est appliquée dans la couche de virtualisation. Vous pouvez remiser toutes vos astuces de détournement du trafic est-ouest. La sécurité est appliquée de manière transparente avant même que les paquets ne parviennent au premier port réseau virtuel. Comme il est sécurisé en amont, le trafic est-ouest sensible à la latence peut être directement acheminé vers sa destination via le chemin le plus rapide.

La combinaison d'un contrôle centralisé et d'une mise en œuvre distribuée des services rend possible, d'un point de vue opérationnel, l'application de règles extrêmement granulaires au niveau de chaque interface virtuelle. Par exemple, les VM appartenant à un même niveau au sein d'une application à trois niveaux peuvent communiquer avec les autres niveaux, mais pas entre elles. En effet, chaque charge de travail est encapsulée avec ses propres règles de sécurité.

NSX permet de définir des règles de sécurité basées sur des structures métiers de haut niveau (application, utilisateur, groupe, etc.) plutôt que sur des structures d'infrastructure de bas niveau (adresse IP, ports applicatifs, protocoles, etc.). Les règles de sécurité peuvent être appliquées avec davantage de précision, d'exactitude et d'adéquation avec la stratégie d'entreprise, sans interprétation humaine.

Une conception garantissant la mobilité et la récupération des charges de travail

En général, les topologies et l'espace d'adressage des réseaux physiques exigent la modification des adresses IP par le département informatique lors du déplacement des applications. Dans certains cas, les adresses IP sont codées en dur dans les applications, ce qui est encore plus coûteux, car cela nécessite des changements de code et des tests de régression.

NSX libère vos charges de travail des VLAN et de l'adressage IP, et leur assure une mobilité et un placement sans restriction dans le fabric du Data Center. Avec NSX, le placement des charges de travail ne dépend pas de la disponibilité ni de la topologie physique des services de réseau physique à un emplacement donné.

NSX fournit aux VM tout ce dont elles ont besoin en termes de réseau, quel que soit leur emplacement physique. Vous pouvez déplacer librement les charges de travail entre les sous-réseaux, les zones de disponibilité ou les Data Center, sans demander aux équipes opérationnelles de redéfinir leur adresse IP. Lors du déplacement d'une charge de travail, tous ses services de sécurité et réseau la suivent automatiquement, sans aucune intervention humaine.

Les entreprises utilisent les fonctions NSX de placement et de mobilité des charges de travail pour bénéficier des avantages suivants :

- provisionnement plus rapide des applications ;
- migration des charges de travail vers un nouveau Data Center ;
- mise à jour ou actualisation de l'infrastructure physique sous-jacente.

Cas d'utilisation : exploitation plus efficace des ressources serveur à l'aide de la virtualisation du réseau

Les entreprises se servent également de NSX pour accéder à la capacité serveur disponible à d'autres emplacements du Data Center ou dans un autre Data Center. Cela optimise considérablement l'utilisation et la consolidation des ressources serveur. Tous ces cas d'utilisation vous aident à gagner en flexibilité et à réduire vos coûts opérationnels de manière significative, augmentant ainsi la valeur globale de votre investissement dans la virtualisation du réseau et la plate-forme NSX.

Dans les topologies réseau traditionnelles, chaque cluster ou pod dispose de sa propre capacité serveur. La reconfiguration du réseau pour accéder à la capacité disponible dans un autre pod ou cluster est une opération chronophage et source d'erreurs. La capacité serveur disponible reste ainsi inexploitée. Ces ressources inutilisées sont difficilement accessibles. Ceci est dû à la complexité des topologies et équipements réseau traditionnels qui empêche le département technologique de tirer pleinement parti de la capacité serveur disponible.

NSX permet d'étendre le réseau afin d'accéder à la capacité disponible à n'importe quel endroit du Data Center, sans aucune modification de l'infrastructure physique existante. Pour ajouter une autre VM, par exemple sur un serveur situé dans une zone de disponibilité ou dans un sous-réseau différent, il vous suffit de la déployer et de la connecter à votre commutateur logique. Ces deux charges de travail sont désormais adjacentes sur la couche 2, même si elles couvrent plusieurs sous-réseaux et zones de disponibilité sur le réseau physique.

Cas d'utilisation : reprise d'activité

Vous pouvez utiliser NSX en complément de vos solutions de reprise d'activité existantes. Dans l'approche traditionnelle du réseau, l'utilisation d'un site de secours pour la reprise d'activité nécessite de trouver un équilibre entre coût et fonctionnalités. Au lieu de reproduire fidèlement leur topologie et leurs services réseau sur un second site, la plupart des entreprises optent pour une solution « suffisante », où les compromis visant à réduire les coûts se traduisent par une perte de fonctionnalités par rapport à leur Data Center principal.

NSX garantit une reprise d'activité sans concession. NSX ne se contente pas de simples snapshots des machines virtuelles : il effectue un snapshot de l'architecture applicative complète, avec ses caractéristiques de sécurité et réseau. Il vous suffit ensuite d'en envoyer une copie vers un site de reprise où elle restera en attente, sur n'importe quel type de matériel et sans perte de fonctionnalités.

En cas de sinistre, déployez la VM et le tour est joué. Le réseau auquel elle est censée se connecter est déjà opérationnel sur le site de reprise. Vous réduisez ainsi considérablement vos objectifs de délai de reprise, car vous n'avez pas besoin d'attribuer de nouvelles adresses IP aux charges de travail et aux appliances de sécurité.

Dernière réflexion sur la technologie

La virtualisation du réseau et NSX offrent à votre environnement technologique un très haut niveau de flexibilité. Ils couvrent un très large éventail de scénarios d'utilisation. Pour ne pas vous laisser submerger par toutes ces possibilités, concentrez-vous d'abord sur la qualité de service. Élargissez le périmètre de votre cas d'utilisation initial. Choisissez ensuite un deuxième cas d'utilisation à mettre en œuvre. Ne déployez de nouvelles fonctionnalités qu'une fois votre équipe et vos utilisateurs satisfaits des niveaux de qualité.

Étapes suivantes

La mise en œuvre de la virtualisation et de la sécurité du réseau doit être considérée comme une transition au cours de laquelle votre département technologique gagne en maturité et en sophistication et crée davantage de valeur pour l'entreprise à mesure que vous progressez vers le Software-Defined Data Center.

Votre département et les membres d'équipe disposent d'un certain nombre d'options pour apprendre à exploiter tout le potentiel de la virtualisation du réseau et de NSX, et découvrir comment cette approche s'intègre avec le reste de votre structure informatique et la complète.

Étape 1 : formation

Une première étape importante consiste à offrir des opportunités de formation à votre département et aux collaborateurs. Proposez différents types d'apprentissage : formels (ateliers, cours, laboratoires d'essai pratique, programmes) et informels (déjeuners de travail, coaching, mentorat). Pour encourager la formation, vous pouvez envisager d'inclure les objectifs de formation et d'apprentissage dans les objectifs personnels des collaborateurs.

Pour commencer, votre équipe peut participer aux laboratoires d'essai pratique VMware (labs.hol.vmware.com) et aux ateliers et cours avec instructeur proposés par les services de formation VMware (vmware.com/education). VMware propose également des guides d'exploitation de NSX axés sur la surveillance et le dépannage.

Étape 2 : services de transformation

Un point de vue extérieur peut vous aider à mener à bien et à accélérer la transition vers la virtualisation du réseau et NSX. VMware propose à cet effet des services et des ateliers de transformation des opérations (vmware.com/consulting). Par exemple, « Network as a Service (NaaS) Envisioning » vous aide à identifier clairement la vision et les objectifs de votre nouveau modèle opérationnel en matière de réseau et de sécurité. « NaaS Discovery » vous permet de déterminer les fonctions opérationnelles et organisationnelles à améliorer ou à créer pour mettre en œuvre le nouveau modèle opérationnel, et atteindre les objectifs et résultats escomptés.

Étape 3 : projet pilote simple

L'une des meilleures façons de se familiariser avec NSX et de savoir comment le mettre en œuvre est de commencer par un projet pilote de production reposant sur un seul cas d'utilisation et un nombre restreint de charges de travail. Choisissez des charges de travail à faible risque, mais suffisamment complexes pour bien vous familiariser avec le fonctionnement de NSX.

Pour vous aider à démarrer, contactez votre responsable de compte VMware ou partenaire.

Annexe

Objectifs de performances

Le tableau suivant répertorie les objectifs visés par la mise en œuvre de NSX en matière de personnel, de processus et de technologie. Il vous guidera tout au long de votre transition :

Vecteur	État initial/actuel	État final/futur
Structure org.	• Cloisonnée, avec des frontières rigides qui exigent des processus lourds • Procédures de demandes formelles • Absence de collaboration • Renvois de responsabilité : « Ce n'est pas nous, c'est eux » • Objectifs et mesures incitatives hétérogènes et incohérents	• Mixte, avec interactions immédiates • Communication ouverte • Boucles de rétroaction condensées • Hautement collaborative • Objectifs et indicateurs de performances clés communs • Partage des risques et des responsabilités
Personnel	• Spécialisation • Expertise limitée à un domaine • Utilisation de CLI et de scripts • Large accès aux connaissances • Perspectives d'évolution de carrière limitées • Axé sur l'infrastructure matérielle	• Interdomaine et pluridisciplinaire • Expertise multidomaine • Utilisation d'API et d'outils d'automatisation • Apprentissage continu • Retombées positives pour l'entreprise grâce à des projets stratégiques • Orienté services et applications
Processus	• Manuels et sources d'erreurs • Systèmes de tickets fastidieux • Coordination et transferts • Complexité et goulots d'étranglement • Délai d'attente des services • Coûts opérationnels élevés • Orientés infrastructure	• Automatisés, normalisés, cohérents et auditables • Peu de risques d'erreurs manuelles • Traitement rapide/régis par des SLA • Interactions en temps réel • Réduction des coûts d'exploitation • Orientés services ou applications
Outils	• Hérités et spécifiques au domaine • Multiples et cloisonnés • Environnements physiques uniquement • Orientés infrastructure • Problèmes de services difficiles à isoler • CLI distinctes pour les composants	• Outils modernes multidomaines • Environnements physiques et virtuels • Orientés applications • Surveillance intégrée de l'infrastructure et des services • Problèmes de services faciles à isoler • CLI et API centralisées pour l'instrumentation de l'infrastructure

Vecteur	État initial/actuel	État final/futur
Architecture	• Limitations d'une architecture à 3 niveaux classique • Charges de travail entravées • Pare-feu à « point d'étranglement » • Cœur de réseau sursouscrit • Performances des liaisons • Services centralisés liés à l'emplacement	• Fabric Leaf-Spine avec routage ECMP non bloquant • Superposition avec dissociation et abstraction • Mobilité et portabilité des charges de travail • Isolation et segmentation natives • Évolutivité et résilience • Services distribués
Infrastructure	• Physique, avec changements chronophages au niveau de la couche sous-jacente • Sécurité liée à l'infrastructure • Reprise d'activité « suffisante » avec perte de fonctionnalités • Interprétation humaine des règles • Règles axées sur l'infrastructure • Structures d'infrastructure de bas niveau • Gestion fragmentée • Dépendance vis-à-vis du fournisseur de matériel • Chaînage des services complexe	• Virtuelle, avec changements dynamiques au niveau de la superposition • Sécurité orientée applications • Reprise d'activité sans compromis • Règles de sécurité lisibles par machine • Règles orientées métier • Structures métiers de haut niveau • Gestion centralisée • Choix prix/performances • Chaînage des services simple

Rôles en matière de réseau et de sécurité dans le Cloud

Les descriptions suivantes vous aideront à définir les rôles et responsabilités du personnel chargé du réseau et de la sécurité dans le Cloud. Les rôles liés au Cloud sont dévolus à des professionnels du réseau et de la sécurité « traditionnels », c'est-à-dire des personnes qui font déjà partie de vos équipes.

Dans les PME, il est courant qu'une même personne assume au moins deux de ces rôles. Par exemple, un ingénieur réseau pourra être responsable de l'architecture, du développement et/ou de l'exploitation du réseau. Les entreprises n'ont en effet pas toutes besoin d'attribuer ces rôles à des personnes différentes.

Dans les grandes entreprises, en revanche, il n'est pas rare que plusieurs personnes assument un rôle identique ou similaire. Dans un grand nombre de multinationales, par exemple, nous avons vu plusieurs architectes ou ingénieurs réseau Cloud.

Rôles en matière de réseau Cloud

L'*architecte réseau Cloud* est responsable du développement d'architectures et de normes réseau Cloud de bout en bout selon un modèle de consommation basé sur les services (réseau sous forme de service). Ses responsabilités sont les suivantes :

- définir les exigences réseau techniques et opérationnelles ;
- concevoir des réseaux physiques et logiques répondant aux besoins des applications (capacité, performances, etc.) ;
- élaborer et valider des tests destinés à garantir le respect des exigences ;
- guider la planification et l'implémentation des solutions réseau Cloud.

L'*ingénieur réseau Cloud* est responsable de la conception de bas niveau des services et de l'infrastructure réseau, du développement et du test des fonctions réseau, du provisionnement de la capacité, et de la définition de la configuration réseau. Ses responsabilités sont les suivantes :

- s'assurer du respect des exigences clients et des niveaux de service associés ;
- traduire les exigences en schémas logiques et modèles de configuration ;
- concevoir, développer et tester des workflows et scripts personnalisés pour les tâches de routine (intégration, déploiement, surveillance, conformité, etc.) ;
- contribuer à la résolution des problèmes de support de niveaux 2 et 3, proposer des solutions et demander des correctifs.

L'*opérateur réseau Cloud* est responsable de tous les aspects des opérations du Jour 2. Il vérifie que les besoins opérationnels des applications sont satisfaits (performances et capacité, par exemple) et assure la maintenance de l'infrastructure réseau de type Cloud, ainsi que des outils et plates-formes associés. Ses responsabilités sont les suivantes :

- exécuter et contrôler le processus d'automatisation du provisionnement, de la gestion, de la surveillance, des alertes et du dépannage ;
- assurer une surveillance proactive de l'infrastructure réseau de type Cloud et réagir aux problèmes avant qu'ils n'affectent le service ;
- exécuter les opérations de dépannage, procéder à l'analyse des causes profondes des problèmes, et appliquer les solutions et correctifs proposés par l'ingénieur réseau Cloud ;
- assurer le support de niveaux 2 et 3, et gérer les incidents, les problèmes et leur remontée.

Rôles en matière de sécurité du Cloud

L'*architecte de sécurité du Cloud* est responsable de tous les aspects liés à l'architecture, à la conception et au support de l'infrastructure de sécurité du Cloud, notamment la virtualisation, l'automatisation, l'orchestration et la surveillance de la sécurité du réseau. Ses responsabilités sont les suivantes :

- évaluer les risques de sécurité de l'infrastructure et des applications Cloud, et fournir des lignes directrices faisant autorité sur les stratégies et solutions de sécurité ;
- déterminer les règles, processus et audits de sécurité techniques requis pour répondre aux objectifs et besoins en matière de sécurité du Cloud ;
- développer des tests de validation pour vérifier les solutions de sécurité du Cloud, et planifier et accompagner leur implémentation ;
- se tenir informé des menaces et stratégies d'atténuation des risques.

L'*ingénieur sécurité Cloud* est chargé de traduire les règles de sécurité en contrôles de sécurité auditables. Ses responsabilités sont les suivantes :

- concevoir et implémenter des solutions physiques et logiques pour les contrôles de sécurité du Cloud ;
- orchestrer et automatiser les processus de sécurité du Cloud (contrôle, surveillance et audit) ;
- intégrer et implémenter des services et outils de sécurité du Cloud conformes aux exigences et aux niveaux de service requis ;
- faire remonter les problèmes, enquêter sur les atteintes à la sécurité et proposer/implémenter des solutions correctives.

L'*opérateur de sécurité du Cloud* est chargé de comprendre, d'implémenter, d'appliquer, de vérifier et de tenir à jour des contrôles de sécurité spécifiques conformément à la politique de l'entreprise et au processus d'évaluation des risques. Ses responsabilités sont les suivantes :

- surveiller, détecter et analyser les anomalies, vulnérabilités et menaces en matière de sécurité ;
- gérer les journaux de sécurité, assurer la conformité aux normes de journalisation et participer aux audits de sécurité ;
- en cas d'incident, enquêter sur les problèmes de sécurité du Cloud, les diagnostiquer et les résoudre ;
- déployer des solutions et correctifs de sécurité pour remédier aux vulnérabilités.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tél. 877-486-9273 Fax 650-427-5001 www.vmware.com
VMware Global Inc. Tour Franklin 100-101 Terrasse Boieldieu 92042 Paris La Défense 8 Cedex France Tél. +33 1 47 62 79 00 www.vmware.com/fr