SDN 101 : Introduction à la mise en réseau logicielle

CITRIX®

Durant toute l'année écoulée, les sujets les plus chauds en matière de réseau auront été la mise en réseau logicielle (ou SDN) et la virtualisation de réseau. Il règne toutefois une grande confusion au sein des directions informatiques d'entreprise à propos de ces deux sujets. Cette confusion a de multiples origines, dont notamment le nombre élevé de fournisseurs proposant des solutions résolvant différents problèmes à l'aide de différentes architectures et technologies, mais prétendant toutes intégrer la mise en réseau logicielle et la virtualisation de réseau.

Le principal objectif de ce livre blanc est de mettre fin à cette confusion. Pour y parvenir, ce document commencera par présenter la technologie SDN dans le contexte plus large d'une tendance générale, pour ensuite détailler les solutions logicielles et identifier les principaux scénarios les plus adaptés au SDN. Ce livre blanc comparera également le SDN et la virtualisation de réseau et décrira les relations existant entre ces deux approches émergentes en matière de mise en réseau.

Contexte

Le réseau de données traditionnel

Dans l'approche réseau traditionnelle, la quasi totalité de la fonctionnalité de mise en réseau est mise en œuvre au sein d'une appliance dédiée (commutateur, routeur ou contrôleur de mise à disposition d'applications). En outre, dans cette appliance dédiée, la quasi totalité de la fonctionnalité est elle-même mise en œuvre sur un matériel dédié, de type ASIC (circuit intégré propre à une application) par exemple.

Les principales caractéristiques de cette approche de mise en œuvre d'appliances réseau sont :

- Les ASIC qui fournissent la fonctionnalité réseau évoluent lentement,
- L'évolution de la fonctionnalité ASIC est contrôlée par le fournisseur de l'appliance,
- Les appliances sont propriétaires,
- Chaque appliance est configurée individuellement,
- Les tâches telles que le provisioning, la gestion des modifications et le déprovisioning sont particulièrement longues et sources d'erreurs.

Les structures de mise en réseau font l'objet d'une pression croissante afin d'offrir une plus grande efficacité et une plus grande agilité que ne le permet pour l'instant l'approche traditionnelle. L'une des causes de cette pression accrue est l'adoption massive de la virtualisation de serveurs. Dans la virtualisation de serveurs, des machines virtuelles sont transférées de façon dynamique d'un serveur à un autre en quelques secondes ou quelques minutes seulement. Cependant, si le déplacement d'une machine virtuelle aboutit à la traversée d'une limite de couche 3, la reconfiguration du réseau indispensable à la prise en charge de la machine virtuelle dans son nouvel emplacement peut prendre plusieurs jours, voire plusieurs semaines. Il peut être parfois délicat de définir de façon précise ce que l'on entend par réseau agile. Ceci étant dit, s'il faut plusieurs semaines pour reconfigurer un réseau du fait du déplacement d'une machine virtuelle, une chose est sûre, ce réseau ne pourra pas être qualifié d'agile.

Le résultat : un réseau traditionnel évolue lentement, voit sa fonctionnalité limitée à ce qui est proposé par les fournisseurs d'ASIC et d'appliances réseau, génère des frais d'exploitation élevés et demeure par nature relativement statique. Le SDN a la capacité à surmonter tous ces inconvénients.

Le passage au logiciel

Comme nous l'avons vu précédemment, le réseau de données traditionnel a toujours été fortement orienté vers le matériel. Toutefois, ces dernières années, l'adoption d'appliances réseau virtualisées et l'intérêt grandissant en faveur des datacenters logiciels (ou SDDC) ont donné naissance à une nouvelle tendance : le recours accru à une fonctionnalité réseau logicielle. Ainsi, par exemple, dans la seconde moitié des années 2000, les appliances réseau de type contrôleurs d'optimisation WAN (WOC) ou contrôleurs de mise à disposition d'applications (ADC) se présentaient sous la forme d'appliances matérielles spécialisées. En clair, les fonctionnalités de type chiffrement/déchiffrement ou traitement des flux TCP étaient effectuées au sein d'un matériel spécifiquement conçu pour elles. Principalement du fait de la demande en faveur d'une agilité accrue, il est désormais courant de voir cette fonctionnalité WOC ou ADC fournie par un logiciel s'exécutant sur un serveur standard ou sur une machine virtuelle.

Le SDDC peut être considéré comme le parfait contraire du réseau de données traditionnel précédemment décrit. Par exemple, l'une des principales caractéristiques du datacenter logiciel réside dans le fait que l'infrastructure du datacenter est virtualisée dans son intégralité et délivrée sous forme de service. Une autre de ses caractéristiques est que le contrôle automatisé des applications et services du datacenter est assuré par un système de gestion basé sur des stratégies.

Les scénarios les plus adaptés

Ce qui caractérise souvent toute approche technologique fondamentalement nouvelle, c'est la grande confusion qui règne autour des scénarios susceptibles d'être pris en charge par cette nouvelle approche. Pour pouvoir évaluer et adopter avec succès une nouvelle approche technologique comme le SDN, les directions informatiques doivent identifier le ou les scénarios importants pour l'entreprise et les mieux adaptés à cette nouvelle approche.

Suite à tout ce qui a été dit au sujet du SDN ces deux dernières années, l'éventail suivant de scénarios est apparu comme le plus adapté à cette nouvelle technologie.

- Prendre en charge le transfert, la réplication et l'allocation dynamiques de ressources virtuelles,
- Alléger la charge de travail administrative associée à la configuration et au provisioning de fonctionnalités comme la qualité de service ou la sécurité,

- Déployer et faire évoluer plus facilement la fonctionnalité réseau,
- Effectuer le suivi du trafic en bénéficiant d'une visibilité de bout en bout sur le réseau,
- Optimiser l'utilisation des ressources réseau,
- Réduire les frais d'exploitation,
- Faire évoluer plus rapidement la fonctionnalité réseau en se basant sur un cycle de vie de développement des logiciels,
- Permettre aux applications de demander de façon dynamique des services à partir du réseau,
- Mettre en œuvre une fonctionnalité de sécurité plus efficace,
- Réduire la complexité.

La mise en réseau logicielle

La fondation ONF (Open Networking Foundation) est le groupe principalement associé au développement et à la standardisation du SDN. D'après l'ONF[1], « la mise en réseau logicielle (ou SDN) est une architecture émergente à la fois dynamique, facilement gérable, rentable et évolutive, idéalement adaptée à la nature dynamique et aux bandes passantes élevées associées aux applications modernes. Cette architecture dissocie le contrôle du réseau des fonctionnalités de redirection, ce qui permet au contrôle du réseau de devenir directement programmable et à l'infrastructure sous-jacente d'être extraite au profit des services réseau et applicatifs. Le protocole OpenFlow™ constitue un élément fondamental, indispensable à la conception de solutions SDN. »

Selon l'ONF, l'architecture SDN est :

- **Directement programmable :** le contrôle du réseau est directement programmable car il est dissocié des fonctionnalités de redirection.
- **Agile :** La séparation du contrôle et des fonctionnalités de redirection permet aux administrateurs d'ajuster le trafic de façon dynamique à l'échelle du réseau afin de répondre à l'évolution des besoins.
- **Gérée centralement :** L'intelligence (logique) du réseau est centralisée au sein de contrôleurs SDN logiciels qui fournissent une vision d'ensemble du réseau et sont perçus par les applications et les moteurs de stratégies comme un commutateur logique unique.
- **Configurée par programmation :** Le SDN permet aux gestionnaires de réseaux de configurer, de gérer, de sécuriser et d'optimiser très rapidement des ressources réseau par l'intermédiaire de programmes SDN automatisés et dynamiques qu'ils peuvent écrire eux-mêmes, ces programmes ne dépendant pas d'un quelconque logiciel propriétaire.
- **Basée sur des standards ouverts et non liée à un quelconque fournisseur :** Lorsqu'il est mis en œuvre via des standards ouverts, le SDN simplifie la conception et l'exploitation des réseaux, les instructions étant alors fournies par des contrôleurs SDN et non plus par une multitude de protocoles et de périphériques propriétaires.

[1] https://www.opennetworking.org/sdn-resources/sdn-definition

La Figure 1 est une représentation graphique de l'architecture SDN telle qu'envisagée par l'ONF.

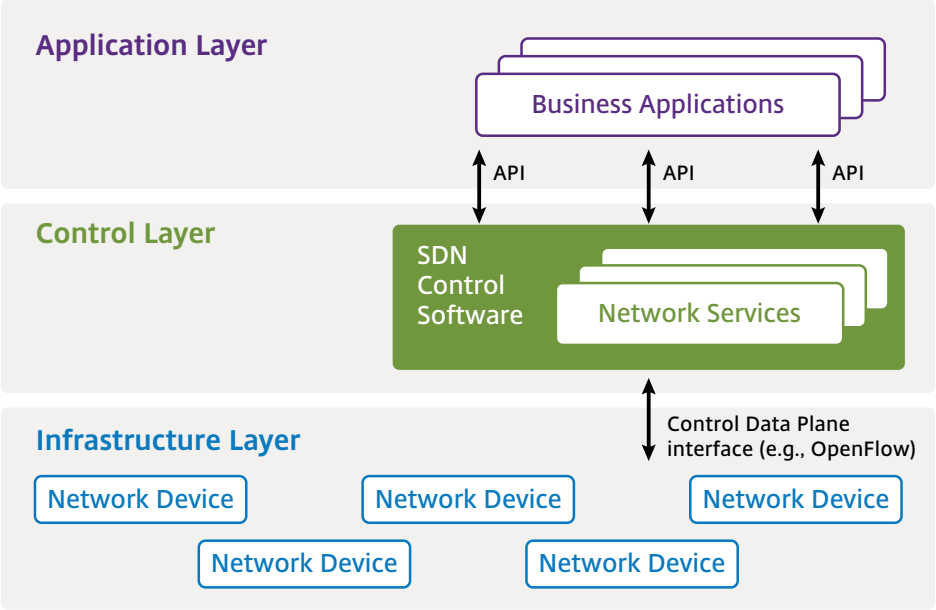

Figure 1 : L'architecture SDN
Source : ONF

Une description des principaux concepts composant l'architecture SDN illustrée à la Figure 1 est fournie ci-dessous.

Applications d'entreprise

Fait référence aux applications directement consommables par les utilisateurs. Par exemple, applications de vidéoconférence, de gestion de la chaîne d'approvisionnement ou de gestion de la relation client.

Services réseau et de sécurité

Fait référence à la fonctionnalité qui permet aux applications d'entreprise de fonctionner de façon efficace et sécurisée. Par exemple, un large éventail de fonctionnalités des couches 4 à 7, comme les ADC, les WOC et les fonctionnalités de sécurité de type pare-feu, dispositifs IDS/IPS ou de protection contre le déni de service distribué.

Commutateur SDN pur

Dans un commutateur SDN pur, toutes les fonctionnalités de contrôle d'un commutateur traditionnel (c'est-à-dire les protocoles de routage qui sont utilisés pour concevoir les bases d'information de retransmission) s'exécutent au sein du contrôleur central. La fonctionnalité à l'intérieur du commutateur se limite exclusivement au panneau de données.

Commutateur hybride

Dans un commutateur hybride, les technologies SDN et les protocoles de commutation traditionnels s'exécutent simultanément. Le gestionnaire du réseau peut ainsi configurer le contrôleur SDN pour détecter et contrôler certains flux de trafic bien précis, tandis que les protocoles réseau distribués traditionnels continueront à assurer le routage du reste du trafic sur le réseau.

Réseau hybride
Un réseau hybride est un réseau au sein duquel les commutateurs traditionnels et les commutateurs SDN, qu'il s'agisse de commutateurs SDN purs ou de commutateurs hybrides, opèrent dans le même environnement.

API orientée vers le Nord
Dans la Figure 1, l'API orientée vers le Nord est l'API qui permet les communications entre la couche de contrôle et la couche des applications d'entreprise. Il n'existe actuellement aucune norme en matière d'API orientée vers le Nord.

API orientée vers le Sud
Dans la Figure 1, l'API orientée vers le Sud est l'API qui permet les communications entre la couche de contrôle et la couche d'infrastructure. Parmi les protocoles permettant ces communications figurent notamment OpenFlow, XMPP (protocole extensible de présence et de messagerie) et le protocole de configuration réseau.

Une part non négligeable de la confusion qui entoure le SDN vient du fait que de nombreux fournisseurs n'adhèrent pas totalement à la définition du SDN adoptée par l'ONF. Ainsi, si certains fournisseurs considèrent OpenFlow comme un élément fondamental de leurs solutions SDN, d'autres adoptent une attitude attentiste à l'égard de ce protocole. Les différentes interprétations relatives à ce qui constitue précisément la couche d'infrastructure représentent une autre source de confusion. Pour l'ONF, la couche d'infrastructure est constituée d'un large éventail de commutateurs et de routeurs physiques et virtuels. Comme indiqué ci-dessous, l'une des approches actuellement adoptée en matière de virtualisation de réseau s'appuie sur une architecture très similaire à celle illustrée à la Figure 1, mais composée uniquement des commutateurs et routeurs virtuels.

La virtualisation de réseau

La virtualisation de réseau n'est pas un sujet nouveau, les directions informatiques mettant en œuvre depuis longtemps des technologies comme le VLAN (LAN virtuel), le VRF (routage et retransmission virtuels) ou le VPN (réseau privé virtuel). Cependant, dans le cadre du présent livre blanc, le terme *virtualisation de réseau* se réfèrera à la fonctionnalité illustrée dans la moitié droite de la Figure 2. En clair, le terme virtualisation de réseau se réfèrera à la capacité à fournir une mise en réseau de bout en bout clairement dissociée du réseau physique sous-jacent, d'une manière similaire à celle avec laquelle la virtualisation de serveurs fournit des ressources de traitement clairement dissociées des serveurs x86 sous-jacents.

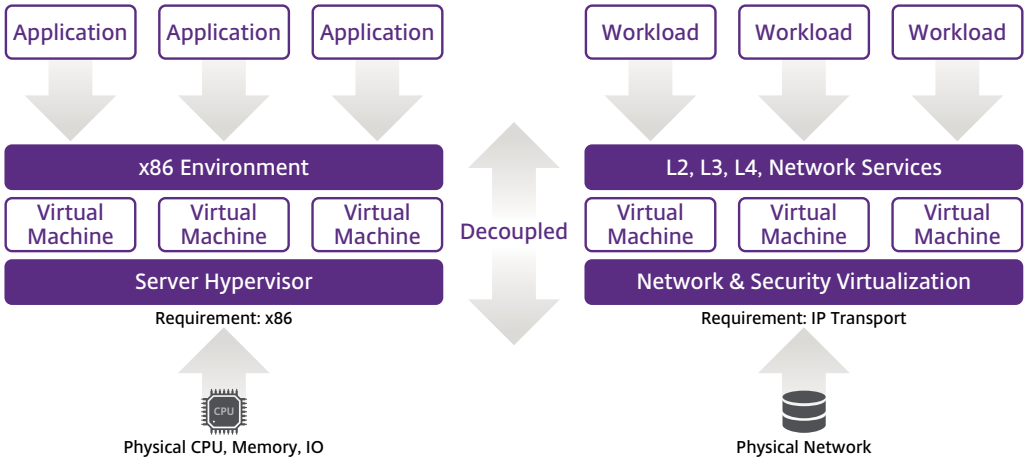

Figure 2 : La virtualisation de réseau
Source : VMware

Il existe une première façon de mettre en œuvre la virtualisation de réseau : une application s'exécute sur un contrôleur SDN, s'appuie sur le protocole OpenFlow et définit des réseaux virtuels basés sur des stratégies faisant correspondre les flux au réseau virtuel approprié à l'aide des parties L1-L4 de l'en-tête. Cette approche est souvent désignée sous le terme de virtualisation de réseau infrastructurelle (« fabric-based »).

Une autre façon de mettre en œuvre la virtualisation de réseau consiste à s'appuyer sur l'encapsulation et le tunneling pour construire de multiples topologies de réseaux virtuels se superposant sur un réseau physique commun. Cette approche est souvent désignée sous le terme de virtualisation de réseau par superposition (« overlay-based »). Depuis quelques années, les directions informatiques mettent en œuvre la virtualisation de réseau via cette dernière méthode en s'appuyant sur des protocoles comme VXLAN. Toutefois, la première génération de solutions de ce type n'intégrait pas de contrôleur. Ces solutions sans contrôleur utilisant en général le « flooding » pour diffuser les informations relatives aux systèmes terminaux, elles n'étaient pas très évolutives.

La Figure 3 illustre une approche plus récente de mise en œuvre de la virtualisation de réseau. Cette approche intègre un contrôleur et s'appuie sur une architecture similaire à celle illustrée à la Figure 1, à l'exception des éléments du réseau, qui sont soit des commutateurs virtuels (vSwitches), soit des routeurs virtuels (vRouters). L'un des rôles principaux du contrôleur de la Figure 3 est de fournir la fonctionnalité de panneau de contrôle du tunnel. Cette fonctionnalité permet au périphérique entrant d'effectuer une opération de mappage qui détermine où le paquet encapsulé doit être envoyé pour atteindre sa machine virtuelle de destination prévue.

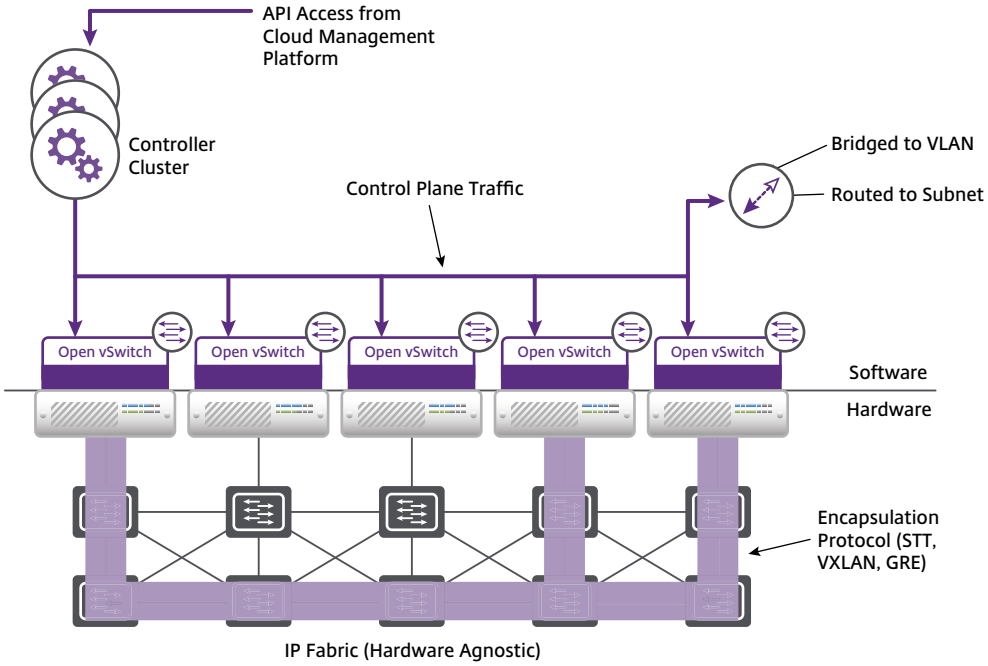

Figure 3 : La virtualisation de réseau par superposition (overlay)
Source : VMware

Dans l'approche illustrée à la Figure 3, un réseau virtuel peut être un réseau de couche 2 ou de couche 3, alors que le réseau physique peut être de couche 2, de couche 3 ou d'une combinaison dépendant de la technologie de superposition utilisée. Avec les couches de superposition, l'en-tête extérieur comprend généralement un champ d'une longueur de 24 bits, ces 24 bits pouvant servir à identifier environ 16 millions de réseaux virtuels. En pratique, la limite se situe plutôt entre 16 000 et 32 000 réseaux virtuels. Dans l'approche illustrée à la Figure 3, la virtualisation est effectuée en périphérie du réseau, le reste du réseau physique de couche 2/3 demeurant inchangé et ne nécessitant aucune modification de configuration pour la prise en charge de la virtualisation du réseau.

Le principal avantage d'une solution de virtualisation de réseau par superposition est qu'elle permet une prise en charge de la mobilité des machines virtuelles totalement indépendante du réseau physique. Si une machine virtuelle change d'endroit, même pour un nouveau sous-réseau, les commutateurs placés à la périphérie de la couche de superposition se contentent de mettre à jour leurs tables de mappage afin de refléter la nouvelle localisation de la machine virtuelle.

Résumé

S'il est vrai que le SDN s'appuie sur de nombreuses technologies habilitantes, il ne constitue pas en soi une technologie à proprement parler, mais bien une architecture. Qu'elle adopte une approche infrastructurelle ou par superposition, la virtualisation de réseau peut être considérée comme une application SDN. Le principal avantage d'une solution de virtualisation de réseau est qu'elle permet une prise en charge de la mobilité des machines virtuelles totalement indépendante du réseau physique. Mais le SDN présente de nombreux autres avantages potentiels, comme la simplification des tâches de provisioning (qualité de service, sécurité, etc.).

Si certaines caractéristiques du SDN, telles que le recours accru au logiciel, sont déjà largement adoptées sur le marché, ce n'est que très récemment que les fournisseurs ont commencé à proposer de véritables solutions SDN, dont l'adoption ne fait que commencer. Etant donnés tous les avantages susceptibles d'être offerts par le SDN, les directions informatiques se doivent de concevoir un plan d'évolution de leurs réseaux intégrant cette architecture. Le chapitre 4 du Guide 2013 de la virtualisation de réseau et de la mise en réseau logicielle dresse les grandes lignes de ce type de plan[2].

Pour en savoir plus, consultez le site citrix.fr/sdn

[2] http://www.webtorials.com/content/2014/01/2013-guide-to-network-virtualization-sdn-3.html

Siège social
Fort Lauderdale, Floride, États-Unis

Siège Silicon Valley
Santa Clara, Californie, États-Unis

Siège Europe, Moyen-Orient, Afrique
Schaffhausen, Suisse

Centre de développement Inde
Bangalore, Inde

Siège Division en ligne
Santa Barbara, Californie, États-Unis

Siège Pacifique
Hong Kong, Chine

Siège Amérique latine
Coral Gables, Floride, États-Unis

Centre de développement Royaume-Uni
Chalfont, Royaume-Uni