le cnam

Master Réseaux Informatiques d'Entreprise
RIE07 2012 – 2014

Grenoble INP FORMATION CONTINUE

Mémoire

présenté et soutenu le 10 avril 2014 par
Cynthia Lopes do Sacramento

Applications SDN

du data centre au Cloud

Jury :	Romain Kobylanski
	François Miller
	Véronique Panne
Tuteur :	Claude Casery
Entreprise :	Bull

Table des matières

Liste des tableaux

Table des figures

Introduction

Les centres de traitement de données évoluent aujourd'hui à un rythme intense pour accompagner l'explosion constatée dans l'utilisation des données. L'accélération de l'innovation dans l'informatique impose une rénovation constante du business. La virtualisation a permis aux centres de données d'améliorer la productivité de ses serveurs, mais pour arriver à l'agilité souhaitée, les data centres doivent faire évoluer leurs réseaux et débloquer le Cloud Computing. Cette étude analyse les applications **Software-Defined Networking : Réseau Informatique Défini par Logiciel (SDN)** pour distinguer ses apports dans le contexte des data centres et habiliter le passage au Cloud Computing.

La plupart des infrastructures de **Technologie de l'Information (TI)** n'ont pas été construites pour supporter la croissance explosive de la capacité de traitement de l'information observé aujourd'hui. Plusieurs centres de données sont devenus hautement distribués et relativement fragmentés. Ils se trouvent donc limités dans leur capacité à évoluer rapidement et à supporter l'intégration des nouveaux types de technologies ou se mettre à l'échelle pour monter le business en puissance selon les besoins de ses consommateurs.

Lors qu'ils sont équipés d'infrastructures performantes, partagées et dynamiques ainsi qu'avec des outils nécessaires pour libérer les ressources de la demande traditionnelle, les **Système d'Information (SI)** peuvent alors répondre plus efficacement aux besoins métiers. Par conséquent, les structures pourraient se focaliser dans l'innovation et ajuster des ressources à leurs priorités stratégiques. Cela soulagerait la prise de décisions, qui pourrait se concentrer sur l'information en temps-réel.

Alors que le coût du réseau dans un data centre est estimé à 15% [1] du total sans être un des plus élevés, il est largement établi qu'il représente un élément clé pour la réduction des coûts et l'augmentation du retour sur investissement. Les coûts d'investissement dans le serveurs ont été évalués à 45% des coûts des data centres. Malheureusement la charge utile des serveurs est remarquablement basse, arrivant à seulement 10% d'utilisation

dans certains exemples.

La technique de la virtualisation a permis le déplacement des processus entre machines, mais des contraintes réseau continuent à limiter l'agilité dans les data centres. L'agilité est définie par la capacité d'affecter tout service n'importe où dans le data centre, tout en assurant la sécurité, la performance et l'isolation entre tous les services. Les designs des réseaux conventionnels dans un data centre empêchent cette agilité ; par nature ils fragmentent à la fois les réseaux et la capacité des serveurs, limitant et réduisant la croissance dynamique des pools de serveur. [2]

L'agilité est donc un élément clé ; certaines entreprises s'évertuent à déployer des nouvelles applications ou faire évoluer les existantes au rythme de la croissance de leur business. Selon le sondage mené par AlgoSec avec 240 professionnels de l'informatique, 25% des organisations participantes doivent attendre plus de 11 semaines pour qu'une nouvelle application soit mise en ligne (et dans 14%, ce temps dépasse 5 mois). Les résultats révèlent également que 59% des organisations nécessitent plus de huit heures pour réaliser un changement de connectivité dans une application. [3]

Cependant, lors du passage au Cloud, les entreprises réalisent que la virtualisation des serveurs est considérablement limitée par les designs Ethernet classiques et les contrôles de sécurité réseau traditionnels. Avec l'augmentation de la virtualisation au sein des data centres, quatre tâches critiques deviennent pénibles :

— Prévention de la congestion du trafic ;
— Réduction de la complexité des politiques réseau et maintien du niveau de service ;
— Élimination des points aveugles qui conduisent à des pannes ;
— Scellage des failles de sécurité pour protéger les données.

Cette étude a pour but de démontrer comment SDN peut être appliqué aux data centres pour débloquer le Cloud Computing et élargir ses limites. Dans le premier chapitre, le contexte des data centres sera défini. Ensuite, les enjeux dans l'aspect réseau seront exposés. Le chapitre suivant présentera les applications SDN qui répondent à ses enjeux. En fin, le quatrième et dernier chapitre démontrera les apports de SDN dans ce cadre.

Chapitre 1

Les évolutions du business modèle des Data Centres

Ce chapitre a pour but de définir un data centre afin de pouvoir analyser ses problématiques, enjeux et solutions possibles, en vue de comprendre son état actuel et ses limites par rapport aux nouveaux besoins et défis business. Les éléments plus importants de la conception et de l'architecture du data centre seront présentés ainsi que les difficultés qui l'ont amené faire à évoluer son modèle de livraison vers l'approche Cloud Computing.

1.1 Data centres et leurs objectifs

Un data centre (aussi nommé « ferme de serveurs ») est un répertoire centralisé pour le stockage, management et distribution de données et informations. Typiquement, un data centre est une installation utilisée pour loger des systèmes informatiques et ses composants associés, tels que systèmes de télécommunication et stockage.

Les data centres traditionnels hébergent historiquement de nombreuses applications relativement petites ou moyennes, chacune s'exécutant dans une infrastructure matérielle dédiée qui est isolée et protégée des autres systèmes dans la même installation. Ces data centres accueillent du matériel et du logiciel pour multiples unités organisationnelles ou même diverses entreprises. Différents systèmes informatiques au sein d'un tel data centre ont souvent très peu d'éléments en commun en termes de matériel, logiciel ou infrastructure de maintenance, et en général ne communiquent pas entre eux.

Les tendances de l'informatique vers une approche côté serveur et l'explosion en popularité des services sur internet ont changé ce scénario. Des infrastructures data centre entières ont été dédiées à un seul acteur pour faire fonctionner ses services offerts. Dans ce cadre, un data centre appartient à une seule organisation et utilise des matériels et plateformes logicielles relativement homogènes qui partagent une couche commune de systèmes de management. Ces data centres dédiés exécutent un nombre réduit d'applications (ou services internet) beaucoup plus importants en taille ; l'infrastructure commune de management permet alors une meilleure flexibilité de déploiement.

Ces infrastructures sont montées pour gérer la taille des applications déployées et la haute disponibilité exigée pour ces services, visant en général 99,99% de durée de fonctionnement (une heure au maximum de temps d'arrêt par an). Il est difficile d'atteindre un fonctionnement libre des failles dans une collection de systèmes matériel et cela devient encore plus complexe avec le grand nombre de serveurs impliqués

Les infrastructures de ces data centres doivent être dimensionnées précisément en fonction de la charge des applications supportées. Par conséquent, des nouvelles approches ont été proposées pour la construction et l'opération de ces systèmes qui doivent être conçus pour tolérer un nombre important de failles avec très peu ou aucun impact sur la performance et disponibilité des services offerts. [4] [5]

1.2 Organisation d'un data centre et difficultés

Un data centre est en général organisé en lignes de racks où chaque rack contient des dispositifs modulaires tels que serveurs, switches, briques de stockages ou instruments spécialisés. Des composants essentiels de l'infrastructure, branchés aux racks des data centres d'entreprises tels que compute, stockage et réseau, sont la base sur laquelle les applications business sont construites. Un châssis se présente avec ses propres ventilateurs, source d'alimentation, panier d'interconnexion et module de management. Pour réduire l'espace occupé, des serveurs peuvent être compartimentés dans un châssis qui est glissé dans le rack. Un châssis fournit des slots de taille standard où il est possible d'insérer des élément actifs modulaires (aussi connus en tant que « blades »). Un seul châssis peut contenir 16 serveurs 1 U ; étant donné que les racks supportent 6 châssis, ils ont une capacité théorique de 96 éléments modulaires.

La figure 1.1 montre l'organisation des racks dans un data centre. Un serveur occupe 1

FIGURE 1.1 – Organisation de racks. [5]

U du rack est montré à gauche. Au milieu on voit un rack et à droite un cluster de racks avec un swtich/routeur de niveau cluster. En général un ensemble de serveurs 1U sont montés dans un rack et inter-connectés avec commutateur Ethernet local. Ces switches au niveau des racks, qui peuvent utiliser des liens de 1 à 10 Gbps, ont un nombre de connexions montantes vers un ou plus switches de niveau cluster (data centre).

Le stockage dans les data centre peut être proposé de diverses manières. Souvent le stockage de haute performance est logé dans des « tours de stockage » qui permettent un accès distant transparent au stockage, indépendamment du nombre et des types des dispositifs de stockage physiques installés. Le stockage peut également être fourni dans une « brique de stockage » plus petite, localisée dans le rack ou slot de châssis ainsi que directement intégrée aux serveurs. Dans tous les cas, un accès réseau efficace au stockage est crucial.

Le problème le plus important dans cette structure est la potentielle insuffisance de bande passante. En général, les connexions montantes sont conçues pour supporter un certain taux de demandes excédentaires puisque la fourniture d'une bande passante entière n'est pas toujours possible. Par exemple, 20 serveurs à 1Gbps chacun doit partager un lien Ethernet montant unique de 10Gps à un taux de demande excédentaire de 2. Cette situation peut être problématique si la charge réseau non locale monte considérablement. Comme le stockage est traditionnellement fourni dans une tour séparée, tout le trafic de stockage traverse le lien montant dans le réseau stockage. Par exemple, l'archivage d'un gros volume peut consommer une importante bande passante. À mesure que les data centres augmentent en taille, une architecture réseau plus extensible devient

essentielle.

La consommation d'énergie est également une des préoccupations de la conception des data centres, car les coûts liés sont devenus une part importante de la totalité des coûts pour cette classe de systèmes. Actuellement les CPUs ne sont plus le seul élément cible d'amélioration de l'efficacité énergétique, car ils ne dominent plus la majorité de la consommation. Des problématiques de ventilation et surconsommation d'énergie sont des facteurs de plus en plus critiques dans la conception de data centres.[5] [6]

1.3 Virtualisation et partage de ressources

Le besoin d'augmenter l'efficacité dans l'utilisation des ressources a conduit à une conception d'infrastructures avec partage de ressources et virtualisation. La virtualisation fait référence à l'abstraction des ressources logiques de leurs couches physiques pour améliorer l'agilité, la flexibilité et la réduction des coûts et ainsi privilégier le business. La virtualisatoin permet de consolider un ensemble de composants d'infrastructures sous-utilisés en un nombre de dispositifs plus petits et mieux utilisés, contribuant à l'économie des coûts.

La virtualisation de serveurs est une méthode pour abstraire le système d'exploitation de la plateforme matérielle. Cela permet aux multiples systèmes d'exploitation ou multiples instances du même système d'exploitation de coexister dans un ou plusieurs processeurs. L'image 1.2 illustre le partage de ressources par l'intermédiaire de la virtualisation.

Un hyperviseur ou moniteur de machines virtuelles est inséré entre le système d'exploitation et le matériel pour réaliser la séparation entre le logique et le physique. Les instances de systèmes d'exploitation lancées sont appelées invités, ou systèmes d'exploitation invités. L'hyperviseur fournit l'émulation matérielle aux systèmes invités et gèrent l'allocation de ressources matérielles.

Ce modèle apporte des avantages pour l'efficacité dans l'utilisation de ressources avec des charges applicatives idéales. Cependant, quand une application commence à consommer plus de ressources que l'estimé, il peut arriver des scénarios où les systèmes d'exploitation invités n'ont pas assez de ressources, impactant ainsi la qualité du service business offert.

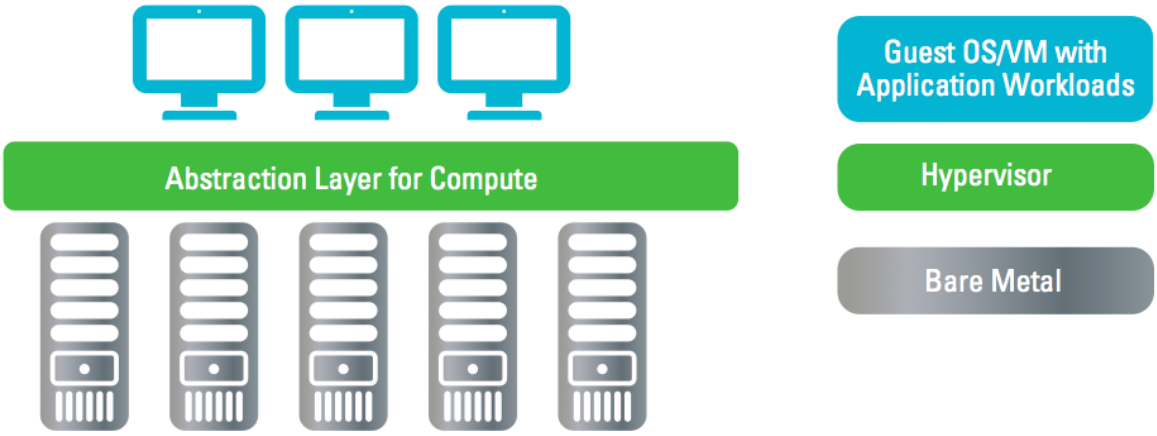

FIGURE 1.2 – Modèle d'infrastructure à ressources partagées. [7]

Cette approche a apporté une maitrise globale de management, monitoring et outillage. Elle a aussi mis en évidence que le composant « compute » de l'infrastructure améliore clairement l'utilisation et automatisation des ressources serveurs. Cette amélioration a été possible grâce à la programmation du contrôle de ressources fournies aux instances invitées. Toutefois, le développement de nouvelles solutions pour gérer la charge dynamique de certaines application faisait toujours défaut. [8][7]

1.4 Le besoin d'un modèle plus dynamique

Traditionnellement, les data centres d'entreprises sont conçus pour durer pour toujours et atteindre les objectives visibles de l'économie. Cela veut dire que les éléments sous-jacents sont dimensionnés et construits pour supporter le pic de charge projeté en termes de performance, disponibilité et sécurité. Quand la croissance volumétrique projetée ne correspond pas à la réalité, cette méthode de dimensionnement peut conduire à une situation de sous-dimensionnement ou sur-dimensionnement. Ce qui apporte un effet négatif pour les investissements et les effort de réduction de coûts.

En général, pour atteindre une meilleure disponibilité, les infrastructures sont amenées à une sous-utilisation des ressources. Comme la charge des applications varient continuellement dans les applications sur internet, il reste deux choix : soit sous-dimensionner la provision et perdre des clients ou alors sur-dimensionner et gaspiller les ressources.

Dans tous les cas, un plan détaillé de capacité est fait pour spécifier une série d'investissements importants en matériel et logiciel, dont la capacité est déterminée. L'image suivante illustre cette planification et les situations de problèmes de dimensionnement.

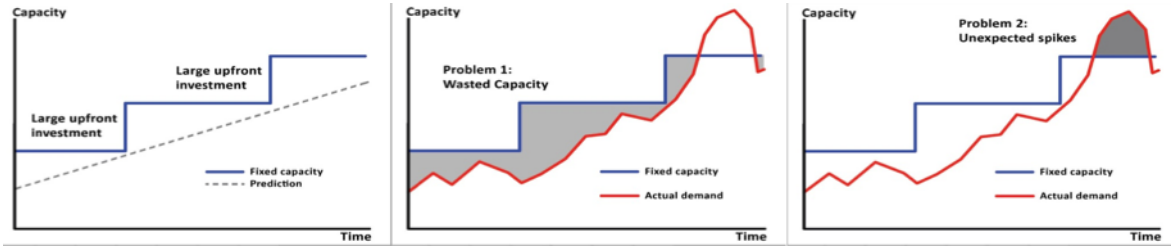

FIGURE 1.3 – Capacité fixe de ressources vs charge prévisionnelle. [9]

Face à cette problématique, un nouveau mode de livraison a été proposé pour aborder les défis du traitement des demandes pour la variation dynamique des charges applicatives. Avec la nouvelle tendance du Cloud Computing et l'infrastructure en tant que service (IaaS), la conception de clusters hautement disponibles et des solutions extensibles peut être architecturée avec des requis non-fonctionnels comme base.

Avec sa nature extensible, le modèle de livraison cloud permet aux ressources d'être étendues et réduites dynamiquement en fonction de la consommation. Une couche logicielle d'abstraction, implémentée par les hyperviseurs, virtualise le traitement des ressources physiques, permettant ainsi au processeur, à la mémoire et aux disques durs de s'accommoder aux variations des demandes. [9] [7]

1.5 Cloud Computing

En termes très simples, le Cloud Computing peut être défini comme un nouveau modèle de consommation et livraison de ressources de **TI** et de services métiers, et est principalement caractérisé par :

- Libre service à la demande ;
- Service réseau très accessible ;
- Location indépendante de services en commun ;
- Extensibilité et approvisionnement rapides ;
- Paiement à la consommation.

Les avancements importants dans la virtualisation, réseau, approvisionnement et architectures multi-tenantes ont permis de faire évoluer radicalement les infrastructures de data centres. Le plus grand impact du Cloud Computing vient de l'instauration de nouveaux modèles de consommation et de livraison de services qui supportent l'innovation du business.

L'évolution des data centres a permis de rendre service à une plus grande variété de besoins dans le monde du travail, ce qui implique la prise en compte de plusieurs facteurs lors de la conception face à différents objectifs. Le Cloud Computing est donc né en tant que nouveau paradigme pour les architectures data centre.

Le Cloud Computing livre dynamiquement des services sur des réseaux à partir d'un ensemble abstrait de ressources. Ces ressources se retrouvent quelque part dans le « nuage » (symbole qui fait allusion à la représentation d'internet dans les topologies réseau) disponibles immédiatement à la demande. Les types de ressources ainsi que leur localisation sont transparents aux utilisateurs finaux. Ces utilisateurs se soucient principalement que leurs applications, données et contenus soient sécurisés et disponibles, avec un niveau de qualité spécifié.

Du point de vue de l'infrastructure, le Cloud Computing fait des fortes demandes aux ressources mutualisées dans une variété de technologies (de compute, de stockage, de réseau) pour leur allocation dynamique. Tout ceci dans un environnement automatisé, orchestré et logiquement diversifié, en conciliant une variété d'applications. L'orchestration permet de mutualiser les ressources à travers multiples data centres pour une réponse dynamique aux besoins clients.

La virtualisation de serveurs a représentée un premier et important pas à la viabilisation de l'approche Cloud Computing. Toutefois, les autres deux éléments de base de l'infrastructure data centre doivent accompagner ces changements pour qu'on puisse avoir un accès complet aux services offerts par le Cloud. Plus spécifiquement la couche d'abstraction assurée par les hyperviseurs qui ont permis la séparation des systèmes logiques des serveurs physiques dans le cas de la virtualisation de serveurs doit être également appliquée aux matériels réseaux et de stockage. Cela permettra la définition d'un data centre entièrement piloté par du logiciel qui gère les ressources physiques les activant selon la charge applicative spécifiée à assurer.

L'abstraction de ces trois composants matériels est essentielle pour achever le mode de livraison cloud au sein des data centres. La virtualisation des serveurs a déjà atteint son

adoption grand public, en 2009 un sondage avait trouvé que 77% répondant déployait au moins un système virtualisé dans leur data centre [10]. Il se déroule actuellement beaucoup de travail en recherche et développement pour acquérir un niveau équivalent de maturité pour les dispositifs réseau et stockage.

L'abstraction du stockage signifie la capacité à mutualiser les dispositifs physiques de stockage pour pouvoir les utiliser en tant que volumes de stockage logiques. Cela caractérise la virtulisation du stockage ou le **Software Defined-Storage, Stockage Défini par Logiciel (SDS)**. Pour l'aspect stockage, il est connu que des solutions **SDS** se trouvent disponibles dans le marché, tels que EMC ViPR, HP StoreVirtual, IBM SmartCloud Virtual Storage Center entre autres.

De manière similaire, pour les réseaux il se développe une technologie fournissant une couche d'abstraction pour divers dispositifs réseau pour permettre l'isolation logique et indépendances du matériel. Il se trouve que **SDN** est une des approches proposées pour traiter la problématique de l'abstraction réseau et fait donc l'objet de cette étude. Le chapitre suivant démontrera pour quoi les réseaux traditionnels ne sont pas adaptés aux exigences du Cloud Computing et analysera des exemples sur divers problèmes rencontrés. L'approche SDN et ses apports seront détaillés par la suite. [11] [12] [7]

I

Chapitre 2

L'aspect réseau

Dans ce chapitre, les principales problématiques data centre dans un aspect réseau seront présentées et analysées. Comment on fait aujourd'hui ? Quels sont les limites ?

2.1 Le réseau dans un data centre

Lors du développement de projets pour l'optimisation de **TI** tels que la consolidation de data centre et la virtualisation de serveur, une attention spéciale doit être prise au rôle critique des réseaux dans la planification, exécution et succès en général du projet. Il est souvent admet que des planifications supplémentaire par rapport aux réseaux auraient pu contribuer pour le succès de plusieurs projets.

Les principaux types de changements réseau dans les projets d'optimisation TI incluent l'implémentation d'équipement réseau supplémentaire pour augmenter la redondance, l'augmentation de la capacité du réseau avec la modernisation de switchs, l'amélioration de la sécurité réseau et l'augmentation de la bande passante. Cependant, plusieurs requis associés à ces changement l'initiative en général sont pas identifiés tout de suite au début du projet. Très souvent ils ne sont pas détectés qu'après les étapes initales du projet, imposant un supplément de travail et l'ajout des coûts non anticipés.

The networking aspects of projects can be challenging and user complaints about the network are frequently heard. Important challenges include the inability to perform accurate and timely root-cause analysis, understand application level responsiveness,

and address network performance issues. Simply buying more network equipment does not necessarily or appropriately address the real requirements.

Looking ahead, many expect that the network will become more important to their companies' overall success. To address this, networking investments related to support of server and storage virtualization are currently at the top of the list for consideration, followed by overall enhancement and optimization of the networking environment. To support virtualization of the entire IT infrastructure and to continue to optimize the network, IT organizations need to make architectural decisions in the context of the existing infrastructure, IT strategy, and overall business goals.

Developing a plan for the network and associated functional design is critical. Without a strong plan and a solid functional design, networking transitions can be risky, leading to reduced control of IT services delivered over the network, the potential for high costs with insufficient results, and unexpected performance or availability issues for critical business processes.

With a plan and a solid functional design, the probability of success is raised : a more responsive network with optimized delivery, lower costs, increased ability to meet application service level commitments, and a network that supports and fully contributes to a responsive IT environment.

2.2 Challenges réseau

Unified Fabric

If one studies a typical data center server infrastructure, it is easy to notice that servers have a series of network interfaces connected to multiple types of networks (LAN, SAN, IPC). This arrangement adds complexity in the form of cost, cabling, port count, scalability, power, and cooling. If we follow the same tradition in a cloud data center, this architecture will not scale to the density that is typically expected. Hence, to continue to reduce the total cost of ownership (TCO) and to deploy virtual machines, all servers must have a consistent and ubiquitous set of network and storage capabilities. One of the simplest and most efficient ways to deliver these capabilities is to deploy a unified fabric. The shift to a unified fabric gives all servers (physical and virtual) access to the LAN, SAN, and IPC networks, allowing more to be consolidated in the customer's network for

greater efficiency and costs savings.

Cisco is offering not only 10 Gigabit Ethernet, but also lossless 10 Gigabit Ethernet, currently called Data Center Ethernet or Enhanced Ethernet. This becomes the foundation to consolidate fabrics like Fiber Channel (for SAN), which require the stringent lossless nature of a network. Fibre Channel over Ethernet (FCoE), which is a standard accepted by standard bodies and industry, is leading the way to unify fabric on a cloud data center. Hence, to consolidate server I/O, the server access layer must be adapted to support a unified fabric. Additionally, a new breed of adapters, called converged network adapters (CNAs), would be implemented in the server platform, which will act at the consolidation and virtualization point in the compute layer.

Cisco believes that the network platform is a foundational component of a utility service platform as it is critical to providing intelligent connectivity within and beyond the data center. With the right built-in and external tools, the network is ideally placed to provide a secure, trusted, and robust services platform.

The network is the natural home for management and enforcement of policies relating to risk, performance, and cost. Only the network sees all data, connected resources, and user interactions within and between clouds. The network is thus uniquely positioned to monitor and meter usage and performance of distributed services and infrastructure. An analogy for the network in this context would be the human body's autonomic nervous system (ANS) that acts as a system (functioning largely below the level of consciousness) that controls visceral (inner organ) functions. ANS is usually divided into sensory (afferent) and motor (efferent) subsystems that is analogous to visibility and control capabilities we need from a services platform to derive a desired outcome. Indeed, at the time of this writing, there is a lot of academic research into managing complex network systems, might they be biological, social, or traditional IT networking. Management tools for the data center and wider networks have moved from a user-centric focus (for example, GUI design) to today's process-centric programmatic capabilities. In the future, the focus will most likely shift toward behavioral- and then cognitive-based capabilities.

The network also has a pivotal role to play in promoting resilience and reliability. For example, the network, with its unique end-to-end visibility, helps support dynamic orchestration and redirection of workloads through embedded policy-based control capabilities. The network is inherently aware of the physical location of resources and users. Context-aware services can anticipate the needs of users and deploy resources appropriately, balancing end-user experience, risk management, and the cost of service.

2.3 Différents usages

2.4 Agilité

2.5 Sécurité

introduction Some security risks unique to a virtualization infrastructure include communication blind spots, inter-VM attacks, and mixed trust level VMs. Instant-on gaps and resource contention are also important considerations. This section addresses each of these threats and issues.

communication Blind Spots

In virtualized environments, traditional network security appliances are blind to the communication between VMs on the same host unless all communications are routed outside the host machine to this separate appliance. But this security configuration introduces significant time lags. One way to eliminate blind spots while reducing time lags is to place a dedicated scanning security VM on the host that coordinates communication between VMs. This solution works well in a virtualized environment. However, a dedicated security VM is not ideal for a cloud environment. The dedicated security VM integrates with the hypervisor to communicate with other guest VMs. In some cloud environments, such as in a multi-tenant public cloud, users do not have access to the hypervisor. In the cloud, protection is best provided as self-defending VMs. Protection is self contained on each VM and does not require communication outside of the VM to remain secure.

inter-Vm attacks and hypervisor compromises

Virtualized servers use the same operating systems, enterprise applications, and web applications as physical servers. Hence, the ability of an attacker to remotely exploit vulnerabilities in these systems and applications is a significant threat to virtualized environments as well. And once an attacker compromises one element of a virtual environment, oather elements may also be compromised if virtualization-aware security is not implemented. In one scenario, an attacker can compromise one guest VM, which can then pass the infection to other guest VMs on the same host. Co-location of multiple VMs increases the attack surface and risk of VM-to-VM compromise. A firewall and an

intrusion detection and prevention system need to be able to detect malicious activity at the VM level, regardless of the location of the VM within the virtualized environment.

Another attack mode involves the hypervisor, which is the software that enables multiple VMs to run within a single computer. While central to all virtualization methods, hypervisors bring both new capabilities and computing risks. A hypervisor can control all aspects of all VMs that run on the hardware, so it is a natural security target. Therefore, securing a hypervisor is vital, yet more complex than it seems.

In an attack known as "hyperjacking," malware that has penetrated one VM may attack the hypervisor. When a guest VM attempts this attack, it is often called a "guest VM escape" because the guest VM breaks out of, or escapes, its isolated environment and attacks the host hypervisor. Once compromised, a hypervisor can then attack other guest VMs on that host.

VMs make requests to the hypervisor through several different methods, usually involving a specific application programming interface (API) call. An API is the interface created to manage VMs from the host machine. These APIs are prime targets for malicious code, so virtualization vendors attempt to ensure that APIs are secure and that VMs make only authentic (i.e. authenticated and authorized) requests. Because this is a critical path function, speed is a significant requirement in all hypervisors to ensure that overall performance is not impeded. When attackers targeted a zero-day vulnerability in a virtualization application called HyperVM made by LXLabs, as many as 100,000 web sites were destroyed [1]. In addition, certain virtualization vendors like Amazon Web Services have made their APIs public. These will undoubtedly become interesting targets for cybercriminals. Vendors that have not made their APIs public like vSphere, while not usually externally exposed, can also become potential targets for attacks within their perimeters. There is a risk that, owing to the rapid change in the API space and the current race to market, virtualization management systems will not be secure in the future.

mixed trust level Vms

VMs with mission-critical data may reside on the same host as VMs with less critical data – resulting in mixed trust level VMs. Enterprises can attempt to segregate these different levels of secure information on separate host machines, but in some cases, this can defeat the purpose of a virtualized environment – to make the most efficient use of resources. Enterprises need to ensure that mission-critical information is protected while

still realizing the benefits of virtualization. With self-defending VM security, VMs can remain safe even in mixed trust level environments, with protection such as intrusion detection and prevention, a firewall, integrity monitoring, log inspection, and antivirus capabilities.

instant-on gaps

Virtualized environments are not necessarily inherently less secure than their physical counterparts. However, in some cases, the practical uses of virtualization can introduce vulnerabilities, unless administrators are aware of these vulnerabilities and take steps to eliminate them. Instant-on gaps are an example of such a vulnerability. Beyond server consolidation, enterprises take advantage of the dynamic nature of VMs by quickly provisioning, cloning, migrating, and decommissioning VMs as needed, for test environments, scheduled maintenance, and disaster recovery, and to support task workers who need computational resources on-demand. As a result, when VMs are activated and inactivated in rapid cycles, rapidly and consistently provisioning security to those VMs and keeping them up-to-date can be challenging.

After a period of time, dormant VMs can eventually deviate so far from the baseline security state that simply powering them on introduces significant security vulnerabilities. And even if VMs are dormant, attackers may still be able to access them. Also, new VMs may be cloned from VM templates with out-of-date security. Even when VMs are built from a template with virus protection and other security applications, the VMs need the security agent to have the latest security configurations and pattern file updates.

When dormant, reactivated, or cloned VMs have out-of-date security, attackers may be able to leverage an exploit for a longer period of time – the attack may have more longevity. Generally, if a guest VM is not online during the deployment or updating of antivirus software, it will lie dormant in an unprotected state and be instantly vulnerable when it does come online. One solution is a dedicated security VM on each host that automatically updates VMs with the latest security when activated or cloned, and safely allows enterprises to realize the benefits of virtualization.

resource contention

The legacy security architecture also results in linear growth of memory allocation as the number of VMs on a single host grows. In physical environments, antivirus software

must be installed on each operating system. Applying this architecture to virtual systems means that each VM requires additional significant memory footprint an unwanted drain on server consolidation efforts. Products that are not virtualization-aware suggest the use of randomization or grouping to avoid resource contention.

However, randomization does not help to avoid times of high system usage and requires that a long period of time be reserved for the full scan cycle. Grouping does not allow for the mobile nature of virtualization, requiring reconfiguration when VMs are migrated or cloned.

Chapitre 3

Applications SDN

Ce chapitre redéfinira SDN et présentera ses réponses aux problématiques réseau rencontrées en général dans les data centre, discutées dans le chapitre précédent. Comment SDN approche la problématique ? Qu'est-ce que SDN ?

3.1 Redéfinition de SDN

3.2 Solutions

Nuage NetworksTM removes the constraints of the datacenter network through an innovative Virtualized Services Platform (VSP) that abstracts network capabilities and automates service instantiation. With the Nuage Networks Software Defined Networking solution, cloud service providers, web-scale operators and large tech enterprises can b uild a robust and scalable multi-tenant networking infrastructure that delivers secure virtual slices of readily consumable compute, storage and networking instantaneously across thousands of tenants and user groups.

Chapitre 4

Apports de SDN aux data centres

Ce chapitre démontre les apports de SDN au sein des data centre par rapports aux problématiques présentées précédemment.

4.1 Différents usages

4.2 Agilité

4.3 Sécurité

Conclusion

Même avec le succès incontestable de l'architecture d'internet, l'état de l'industrie réseau et l'essence de son infrastructure se trouvent en phase critique. Il est généralement admis que les réseaux courants sont excessivement chers, compliqués à gérer, sujets aux blocages des fournisseurs et difficiles à faire évoluer.

On constate donc un réel besoin de faire évoluer cette architecture mais des résistances s'opposent à cette évolution en raison de la complexité et la possible saturation du système. En réponse, les réseaux programmables ont été un objet intensif de recherche par la communauté. Les travaux dans ce domaine s'orientent vers l'offre SDN, un nouveau paradigme transformant cette architecture.

L'approche SDN sépare le plan de contrôle et le plan de données, offrant un contrôle et une vision centralisés du réseau. Cela peut apporter certains bénéfices comme le contrôle directement programmable, la simplification du hardware réseau et la simplification de l'ingénierie du trafic. En revanche, des défis d'implémentation sont à surmonter tels que la concentration des risques dans un contrôle physiquement centralisé, l'équilibre entre flexibilité et performance et les conditions d'interopérabilité.

La flexibilité apportée par SDN est telle que de nombreuses possibilités d'applications sont à imaginer. Essentiellement pour l'administration de data centers, le contrôle d'accès et de la mobilité pour les réseaux campus ainsi que l'ingénierie du trafic pour les réseaux WAN.

Le marché suit de près les nouveautés dans le domaine et investit sur les technologies implémentant SDN. Les stratégies ne sont pas encore assez matures et les consommateurs potentiels attendent des offres plus consolidées. Cependant, des solutions innovantes commencent à surgir et certaines sociétés assument le rôle de tête dans le marché.

On s'aperçoit que l'ampleur des possibilités SDN, même si elle présente un avantage en théorie, freine son adoption. En raison de la grande variété de concepts et produits,

les consommateur hésitent toujours à prendre une décision. En même temps, les grands fournisseurs cherchent à la fois à exploiter le nouveau marché et à protéger leurs solutions consolidées. Ces obstacles même s'ils sont confirmés, ne semblent pas être assez forts pour empêcher les échanges à long terme.

Au vu cette étude, il semblerait que dans un futur proche, les clients les plus informés et les plus disposés à innover vont commencer à déployer SDN. Leurs expériences et les résultats obtenus vont fortement impacter le choix des prochains consommateurs. Il est possible que ceux qui dessineront le futur de la technologie des réseaux informatiques pour les prochaines années seront ceux qui auront osé se lancer les premiers. Cette démarche peut éventuellement représenter un risque, mais aussi l'opportunité de tirer des bénéfices plus durables et de prendre de plus larges parts du marché.

Acronymes

ACI Application Centric Infrastructure, Infrastructure centrée sur les applications

API Application Programming Interface, Interface de Programmation

ASIC Application Specific Integrated Circuit, Circuit intégré pour application spécifique

DHCP Dynamic Host Control Protocol, Protocole pour la configuration automatique d'hôte

DNS Domain Name System, Système de noms de domaine

HTTP HyperText Transfer Protcol, Protocole de transfert de hypertexte

IaaS Infrastructure as a Service, Infrastructure en tant que service

IDS Intrusion Detection System, Système de Détection d'Intrusion

IETF Internet Engineering Task Force, Détachement d'ingénierie d'internet

IP Internet Protocol, Protocole d'Internet

IPS Intrusion Prevention System, Système de Prévention d'Intrusion

IRTF Internet Research Task Force, Détachement de recherche d'internet

LAN Local Area Network, Réseau local

MPLS MultiProtocol Label Switching, Commutation multi-protocoles par étiquettes

NAT Network Address Translation, Traduction d'adresse réseau

NFV Network Functions Virtualization, Virtualisation des fonctions réseau

NOS Network Operating System, Système d'exploitation réseau

ONE Open Network Environment, Environnement Réseau Ouvert

ONF Open Networking Foundation

QoS Quality of Service, Qualité de service

SDN Software-Defined Networking : Réseau Informatique Défini par Logiciel

SI Système d'Information

TI Technologie de l'Information

VLAN Virtual Local Area Network, Virtual LAN

VM Virtual Machine, Machine Virtuelle

WAN Wide Area Network, Réseau étendu

Glossaire

Abstraction En informatique, l'abstraction est un terme souvent employé pour désigner le mécanisme et la pratique qui réduisent et factorisent les détails négligeables de l'idée exprimée afin de se focaliser sur moins de concepts à la fois. C'est aussi la notion de couches d'abstraction utilisée comme moyen pour gérer la complexité des systèmes informatiques où les couches correspondent à des niveaux de détails appliqués. [13]

Big Data Big Data est un terme appliqué aux ensembles de données dont la taille (ou le format) est au-delà de la capacité des outils logiciels communs, qui ne peuvent plus les capturer, les gérer et les traiter. Une nouvelle classe de technologies et outils a été développée pour attribuer une valeur commerciale à ces données grâce à une analyse complexe. Le terme est employé en référence à ce type de données ainsi qu'aux technologies utilisées pour les stocker et les traiter. [14]

Cloud Computing Cloud Computing, ou informatique dans les nuages, est une évolution de la fourniture de services **TI** qui offre un moyen d'optimiser l'usage et le déploiement rapide de ressources. Cela se fait par des systèmes et solutions plus efficaces et **scalables**, fournissant un niveau plus haut d'automatisation. Diverses entreprises ont adopté le cloud computing et réalisent des avantages significatifs en agilité, réduction de coûts et soutien de la croissance du business. [15]

Cluster En réseaux informatiques, un cluster désigne un groupe des machines reliées entre elles à l'aide d'un réseau de communication. Cette configuration est souvent utilisée pour réaliser des calculs à haute performance. [16]

Data Center Centre de traitement de données. Il s'agit d'une installation utilisée pour héberger des systèmes informatiques et les composants associés, comme les systèmes de télécommunication et de stockage. En général, un data center inclut alimentation et connexions des données redondantes, contrôles d'environnements comme la climatisation ainsi que divers dispositifs de sécurité. [17]

Fabric En informatique, fabric (qui signifie tissu en anglais) est un synonyme de plateforme ou structure. En général, le terme fabric décrit la façon dont différents composants travaillent ensemble pour former une entité unique. Dans ces systèmes la liaison entre les composants est tellement dense qu'un schéma représentant leurs relations rassemblerait à une pièce de tissu tricotée. Sous ce terme généralement admis par l'industrie réseau, un fabric est une topologie réseau dans laquelle les composants transmettent des données l'un à l'autre à travers les switches d'interconnexion. [18] [19]

Middlebox Boîtier intermédiaire. Un middlebox est un serveur conservant des états de la communication entre deux hôtes. Ils se différencient des hôtes qui représentent les extrémités de la communication. Ils sont encore différents des routeurs qui ne gardent pas d'états concernant les sessions de communications. [20]

Open Daylight Association initiée par Linux Foundation pour l'union des géants du marché réseau dans le but de développer un contrôleur SDN open source, pour l'innover, l'encourager et pour permettre son adoption accélérée. [21]

Open Source Logiciel avec code source ouvert, qui peut donc être utilisé librement, modifié et partagé par quelqu'un. Un logiciel open source est développé par plusieurs personnes et distribué sous des licences qui se conforment à la définition d'open source. [22]

OpenFlow Le protocole OpenFlow vise à standardiser l'interface entre les applications et le contrôleur ainsi que l'interface entre le contrôleur et les éléments de commutation. [23] [24]

Paradigme Un paradigme consiste en une collection de règles, standards et exemples de pratiques scientifiques, partagés par un groupe de scientifiques. Sa genèse et poursuite en tant que tradition de recherche sont conditionnées à un fort engagement et consensus des personnes impliquées. [25] D'après Dosi [26], quand un nouveau paradigme technologique apparaît, il représente une discontinuité ou un changement dans la manière de penser. Ce changement apporté par le paradigme est souvent lié à une sorte d'innovation radicale qui implique une nouvelle technologie. Dans ce document, le terme paradigme sera employé dans ce sens d'innovation et application de nouvelle technologie.

Plan de Contrôle Intelligence du réseau, ensemble des données locales utilisées pour établir les entrées des tableaux de commutation, qui sont utilisés par le plan de données pour effectuer la transmission du trafic entre les ports d'entrée et de sortie du dispositif. [27]

Plan de Données Le plan de donnés traite les data-grammes entrants dans le média à travers une série d'opérations au niveau des liens qui collectent ces data-grammes et réalisent divers tests de cohérence basiques. Ensuite les data-grammes sont transférés en accord avec des tableaux pré-remplis par le **plan de contrôle**. [27]

Scalabilité Terme provenant de l'anglicisme *scalability* qui exprime la capacité d'être mis à échelle. En informatique cela désigne la capacité d'un système, d'un réseau ou un processus de gérer l'augmentation ou la réduction de la charge de manière à pouvoir la gérer. [28]. Le terme est souvent employé pour exprimer une extensibilité, évolutivité ou passage à l'échelle, mais il n'y «a pas d'équivalent communément admis en français ». [29]

Virtualisation Pour diverses entreprises, l'infrastructure serveur virtualisée est la base sur laquelle le **cloud** est construit. Initialement, les technologies de virtualisation ont permis aux data centers de consolider leurs infrastructures pour réduire les coûts. Avec le temps, l'intégration des technologies pour le management flexible de ressources a facilité une allocation plus dynamique. Cela a aidé à réduire les coûts et a également augmenté la flexibilité et la performance. [15]

Bibliographie

[1] Albert Greenberg et al. « The cost of a cloud: research problems in data center networks ». In : *ACM SIGCOMM Computer Communication Review* 39.1 (2008), p. 68–73.

[2] Albert Greenberg et al. « The cost of a cloud: research problems in data center networks, section 3. Agility ». In : *ACM SIGCOMM Computer Communication Review* 39.1 (2008), p. 68–73.

[3] *Examining the Impact of Security Management on the Business*. Executive Summary. An AlgoSec Survey. 2013.

[4] *Understanding Data Centers and Cloud Computing, Section What Is a Data Center?* White Paper. Global Knowledge Training LLC. 2010.

[5] Luiz André Barroso et Urs Hölzle. « The datacenter as a computer: An introduction to the design of warehouse-scale machines, Chapitre 1 : Introduction ». In : *Synthesis lectures on computer architecture* 4.1 (2009), p. 1–108.

[6] Krishna Kant. « Data center evolution: A tutorial on state of the art, issues, and challenges, section 2. Data center organization and issues ». In : *Computer Networks* 53.17 (2009), p. 2939–2965.

[7] Sandeep Raghuraman. *The Journey Toward the Software-Defined Data Center*. White Paper. Cognizant (NASDAQ: CTSH). Sept. 2013.

[8] M. Girola et al. *IBM Data Center Networking: Planning for Virtualization and Cloud Computing, chapitre 2 : Servers, storage, and software components*. IBM redbooks. IBM Redbooks, 2011. isbn : 9780738435398. url : `http://books.google.fr/books?id=EKjEAgAAQBAJ`.

[9] Harish Ganesan. *AWS Cost Saving Tip 5: How Amazon Auto Scaling can save costs*. Web Site. http://harish11g.blogspot.fr/2013/04/Amazon-Web-Services-AWS-Cost-Saving-Tips-how-Amazon-AutoScaling-can-reduce-leakage-save-costs.html. Avr. 2013.

[10] *Virtualization & TCO: Linux vs. Microsoft*. Sondage. Gabriel Consulting Group, Inc. 2009.

[11] M. Girola et al. *IBM Data Center Networking: Planning for Virtualization and Cloud Computing, chapitre 1 : Drivers for a dynamic infrastructure*. IBM redbooks. IBM Redbooks, 2011. ISBN : 9780738435398. URL : `http://books.google.fr/books?id=EKjEAgAAQBAJ`.

[12] *Cloud-Ready Data Center Reference Architecture, Section : Framework*. White Paper. Juniper Networks, Inc. Mai 2010.

[13] Robert M. Keller. *Computer Science: Abstraction to Implementation, Section 1.1 The Purpose of Abstraction*. Article. Harvey Mudd College. Sept. 2001.

[14] *Information Management and Big Data A Reference Architecture*. An Oracle White Paper. Fév. 2013.

[15] *Intel's Vision of Open Cloud Computing, section Speeding Agility, Reducing Costs, and Accelerating Innovation via Cloud*. White Paper. Intel IT Center. 2013.

[16] Qingkui Chen, Haifeng Wang et Wei Wang. « Continuance Parallel Computation Grid Composed of Multi-Clusters. » In : *Journal of Networks* 5.1 (2010).

[17] William Tschudi et al. « High-performance data centers: A research roadmap ». In : (2004).

[18] Margaret Rouse. *network fabric*. Web Site. http://searchsdn.techtarget.com/definition/netw fabric. Mar. 2014.

[19] Martin Casado et al. « Fabric: A Retrospective on Evolving SDN, section 3 Extending SDN ». In : *Proceedings of the First Workshop on Hot Topics in Software Defined Networks*. HotSDN '12. Helsinki, Finland : ACM, 2012, p. 85–90. ISBN : 978-1-4503-1477-0. DOI : `10.1145/2342441.2342459`. URL : `http://doi.acm.org/10.1145/2342441.2342459`.

[20] Pamela Zave. « Internet Evolution and the Role of Software Engineering ». English. In : *The Future of Software Engineering*. Sous la dir. de Sebastian Nanz. Section 3 The Real Internet et 4 Internet trends and evolution. Springer Berlin Heidelberg, 2011, p. 152–172. ISBN : 978-3-642-15186-6. DOI : `10.1007/978-3-642-15187-3_12`. URL : `http://dx.doi.org/10.1007/978-3-642-15187-3_12`.

[21] *Open Daylight Project*. Web site. http://www.opendaylight.org/project. Avr. 2014.

[22] *Open Source Initiative*. Web site. http://opensource.org/. Avr. 2014.

[23] Bruno Nunes Astuto et al. *A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks*. Anglais. Section 3. SOFTWARE-DEFINED NETWORKING ARCHITECTURE. Jan. 2014.

[24] Nick McKeown et al. « OpenFlow: Enabling Innovation in Campus Networks ». In : *SIGCOMM Comput. Commun. Rev.* 38.2 (mar. 2008). Section 2. THE OPENFLOW SWITCH, p. 69–74. issn : 0146-4833. doi : 10.1145/1355734.1355746. url : http://doi.acm.org/10.1145/1355734.1355746.

[25] D. Despotovi S. Cvetanovi et I. Mladenovi. « The concept of technological paradigm and the cyclical movements of the economy ». Anglais. In : *Facta universitatis - series: Economics and Organization* 9.2 (2012), p. 149–159. issn : 330.342.143.

[26] G. Dosi. *Technological paradigms and technological trajectories, Research Policy*. Anglais. 1982.

[27] Thomas Nadeau D. et Ken Gray. *SDN: Software Defined Networks*. 1st. Chapitre 2 - Centralized and Distributed Control and Data Planes. O'Reilly Media, Inc., 2013. isbn : 1449342302, 9781449342302.

[28] André B. Bondi. « Characteristics of Scalability and Their Impact on Performance ». In : *Proceedings of the 2Nd International Workshop on Software and Performance*. WOSP '00. Ottawa, Ontario, Canada : ACM, 2000, p. 195–203. isbn : 1-58113-195-X. doi : 10.1145/350391.350432. url : http://doi.acm.org/10.1145/350391.350432.

[29] René J CHEVANCE. « Serveurs multiprocesseurs et SGBD parallélisés ». In : *Techniques de l'ingénieur. Informatique* H2068 (2001), H2068–1.

SDN : Software-Defined Networking

rédigé par Cynthia Lopes do Sacramento

Résumé

De récentes technologies et concepts émergent pour répondre aux nouvelles utilisations des réseaux et internet. Comme par le passé pour le Big Data, conçu pour le traitement des énormes quantités de données ou le Cloud Computing pour le management de l'hébergement de ressources. Une évolution similaire est attendue dans le domaine des réseaux informatiques. Ce qui a mobilisé la communauté dans les projets de recherche sur les réseaux programmables, dont un des sujets est l'objet de cette étude : SDN - Réseaux Informatiques Définis par Logiciel. SDN est un nouveau paradigme créé pour adapter les infrastructures courantes aux enjeux de la communication actuelle : une plus haute bande passante et les exigences des applications modernes. SDN propose une nouvelle architecture plus dynamique, facile à gérer, rentable et flexible. Cette architecture sépare le plan de contrôle (intelligence et état du réseau) du plan de données (fonctions de transmission). L'approche permet de rendre le contrôle directement programmable avec l'infrastructure sous-jacente abstraite aux applications réseaux et services.

Mots clés : SDN, Réseaux Programmables, Plan de Contrôle, Plan de Données

Abstract

New technologies and concepts appear in response to new network and internet usage requirements. Such as Big Data for massive data processing and Cloud Computing for resources hosting management. Similar evolution is expected for the computer networks. As result the research community has produced many works on programmable networks. Among them, the subject of this study : SDN - Software Defined Networking. SDN is a new paradigm designed to adapt current infrastructures to the issues of the recent communication : increasingly need for high speed and the exigences of modern applications. SDN proposes a new architecture plus dynamic, ease to manage, profitable and flexibile. This architecture decouples the control plane (network intelligence and state) from the data plane (transmission functions). This approach makes de the control directly programmable and causes the underlying infrastructure to be abstracted to network applications and services.

Keywords : SDN, Programmable Networks, Control Plane, Data Plane