

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

Introduction	1
1 Les évolutions du business modèle des Data Centres	3
1.1 Data centres et leurs objectifs	3
1.2 Organisation d'un data centre et difficultés	4
1.3 Virtualisation et partage de ressources	6
1.4 Le besoin d'un modèle plus dynamique	7
1.5 Cloud Computing	8
2 L'aspect réseau	11
2.1 Le rôle du réseau dans les projets de TI	11
2.2 L'architecture réseau d'un data centre typique	13
2.3 Applications business en transformation	14
2.4 Différents usages	14
2.5 Agilité	14
2.6 Sécurité	15
3 Applications SDN	19
3.1 Redéfinition de SDN	19
3.2 Solutions	19
4 Apports de SDN aux data centres	21
4.1 Différents usages	21
4.2 Agilité	21
4.3 Sécurité	21
Conclusion	23
Acronymes	25

Glossaire	27
Bibliographie	31

Liste des tableaux

Table des figures

1.1	Organisation de racks. [5]	5
1.2	Modèle d'infrastructure à ressources partagées. [7]	7
1.3	Capacité fixe de ressources vs charge prévisionnelle. [9]	8
1.4	Vue conceptuelle d'un data centre. [10]	10
2.1	Architecture réseau typique à trois niveaux. [16]	13

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 habilitier 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 les 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 entreprises 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 contraignantes :

- 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 dépasser 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. Enfin, 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 les 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, le management et la distribution de données et d'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 un regroupement 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 éléments 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

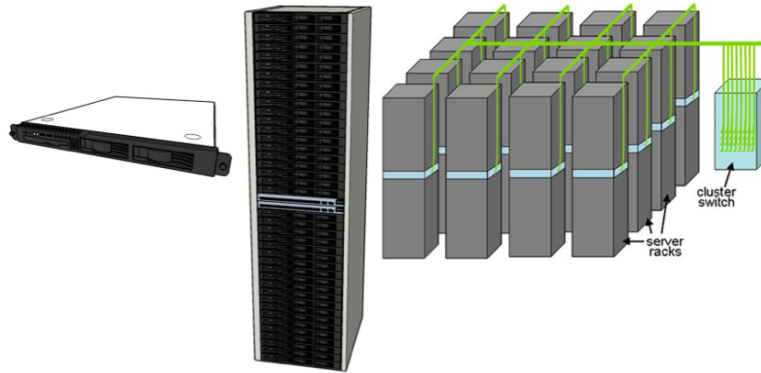


FIGURE 1.1 – Organisation de racks. [5]

Un serveur 1U du rack est montré à gauche. Au milieu on voit un rack et à droite un cluster de racks avec un switch/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 centres 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 10Gbps 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 virtualisation 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.

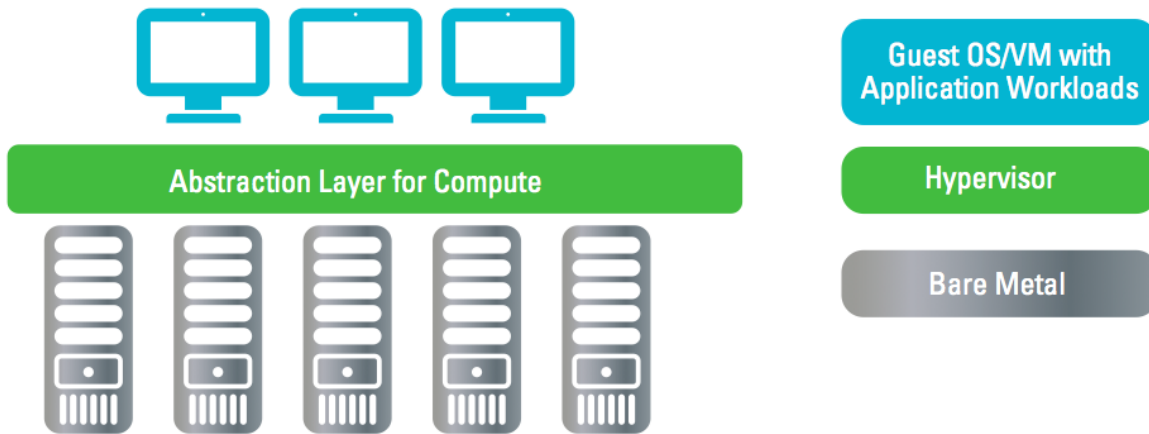


FIGURE 1.2 – Modèle d'infrastructure à ressources partagées. [7]

Cette approche a apporté une maîtrise 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 objectifs déterminés 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 varie 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 charge maximale est déterminée. L'image suivante illustre cette planification et les situations de problèmes de dimensionnement.

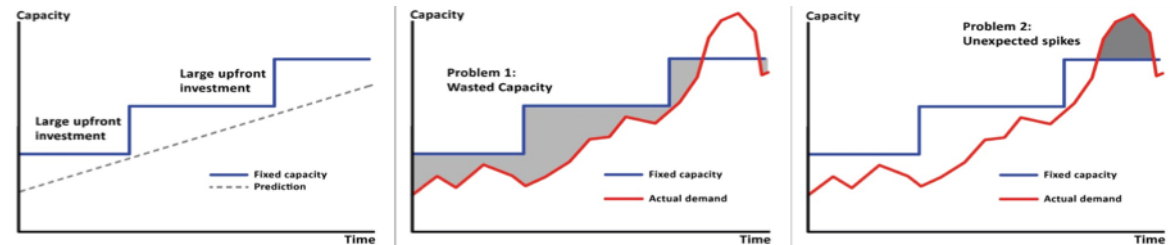


FIGURE 1.3 – Capacité fixe de ressources vs charge prévisionnelle. [9]

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 représenté un premier et important pas pour la viabilité de l'approche Cloud Computing. Toutefois, les autres deux éléments de base de l'infrastructure data centre doivent accompagner ces changements pour autoriser 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, en les activant selon la charge applicative spécifiée à assurer.

L'image suivante illustre une vue conceptuelle d'un data centre basé sur ces trois éléments avec des coches d'abstraction permettant de sécuriser, orchestrer et livrer ses ressources aux consommateurs.

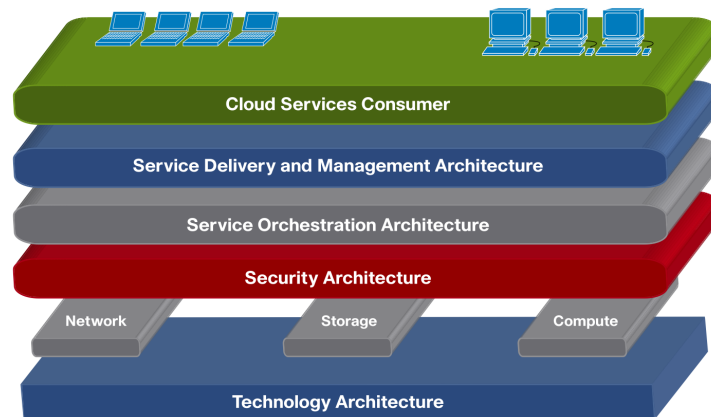


FIGURE 1.4 – Vue conceptuelle d'un data centre. [10]

L'abstraction de ces trois composants matériels est essentielle pour achever le mode de livraison Cloud au sein des data centres. L'adoption de la virtualisation des serveurs a déjà atteint son grand public, en 2009 un sondage avait trouvé que 77% des répondants déployaient au moins un système virtualisé dans leur data centre [11]. On observe 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 virtualisation 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, telles que EMC ViPR, HP StoreVirtual, IBM SmartCloud Virtual Storage Center entre autres.

De manière similaire, il se développe pour les réseaux une technologie fournissant une couche d'abstraction pour divers dispositifs réseau afin de 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 en 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. [12] [13] [7] [10]

Chapitre 2

L'aspect réseau

Dans ce chapitre, les principales problématiques data centre dans un aspect réseau seront présentées et analysées. Seront abordés quelques questionnements sur les réseaux classiques pour tenter de répondre aux nouveaux besoins data centres. Le chapitre présentera comment divers scénarios sont traités aujourd'hui et quels sont les limites.

2.1 Le rôle du réseau dans les projets de TI

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

Les principaux types de modifications dans ces projets incluent l'implémentation d'équipement réseau supplémentaire pour augmenter ou améliorer la redondance, la capacité du réseau, la sécurité réseau et/ou la bande passante. Cependant, plusieurs requis associés à ces changements ne sont pas, en général, identifiés au tout début du projet. Très souvent ils ne sont détectés qu'après les étapes initiales du projet, imposant un supplément de travail et l'ajout de coûts non anticipés.

Les aspects réseau d'un projet peuvent être difficiles à gérer, et des critiques sur le fonctionnement général des réseaux sont fréquemment entendues. Des défis importants incluent la réalisation d'analyses des causes précises et opportunes, la compréhension de

la réactivité au niveau applicatif et la révélation des origines de problèmes de performance. Le simple achat d'équipement réseau n'aborde pas nécessairement ou proprement les requis réels.

Pour supporter la virtualisation complète d'une infrastructure de **TI** et continuer à optimiser le réseau, des décisions sur l'architecture doivent être faites dans le contexte de l'infrastructure existante, de la stratégie et des objectifs larges du business. Sans le développement d'un plan réseau et la conception fonctionnelle associée, les transitions réseau peuvent être risquées et conduire à un contrôle réduit des services livrés, coûts potentiellement élevés contre des résultats insuffisants et des problèmes inattendus de performance ou disponibilité.

Traditionnellement un plan et conception fonctionnelle solides suffisaient pour augmenter le succès des projets avec un réseau réactif, optimisé, moins cher et répondant mieux aux engagements des services applicatifs. Alors que ce plan reste essentiel, il est difficile dans le contexte d'utilisation actuel de maîtriser complètement à l'avance la charge, dimension et tout autre requis qui doivent être assurés par les réseaux.

En face à ses difficultés et aux critiques reçues, il est facile de finir par interpréter les réseaux comme un élément bloquant pour le succès des projets. Même si sa gestion et planification peuvent être complexes, les réseaux représentent un moyen naturel pour le management et renforcement des politiques liées aux risques, performance et coûts. Seulement le réseau voit toutes les données, ressources connectées et interactions des utilisateurs à travers le Cloud. Le réseau est donc positionné de manière unique pour surveiller et mesurer l'usage et la performance des services distribués et de l'infrastructure. Les réseaux ont également un rôle central pour favoriser l'extensibilité et disponibilité. Par exemple avec sa vue unique bout-en-bout, les réseaux peuvent détecter la charge et dynamiquement la rediriger selon les politiques de contrôle.

Afin d'atteindre ce niveau de management et orchestration des ressources, on cherche à concevoir des architectures réseaux qui puissent s'étendre ou se rétracter ainsi que supporter des nouveaux services dynamiquement et rapidement en fonction des besoins immédiats. [14] [15]

2.2 L'architecture réseau d'un data centre typique

La majorité des data centres d'aujourd'hui ont une structure réseau hiérarchique à trois niveaux : couche d'accès, agrégation/distribution et cœur (figure 2.1). Cette architecture a été conçue pour les applications client-serveurs dans des serveurs applicatifs dédiés. Dans cette conception le flux du trafic se fait essentiellement à partir des serveurs en direction le cœur du réseau et ensuite dehors vers internet ou autre (flux Nord/Sud). Les commutateurs composant le cœur du réseau contiennent la grande majorité de l'intelligence du réseau.

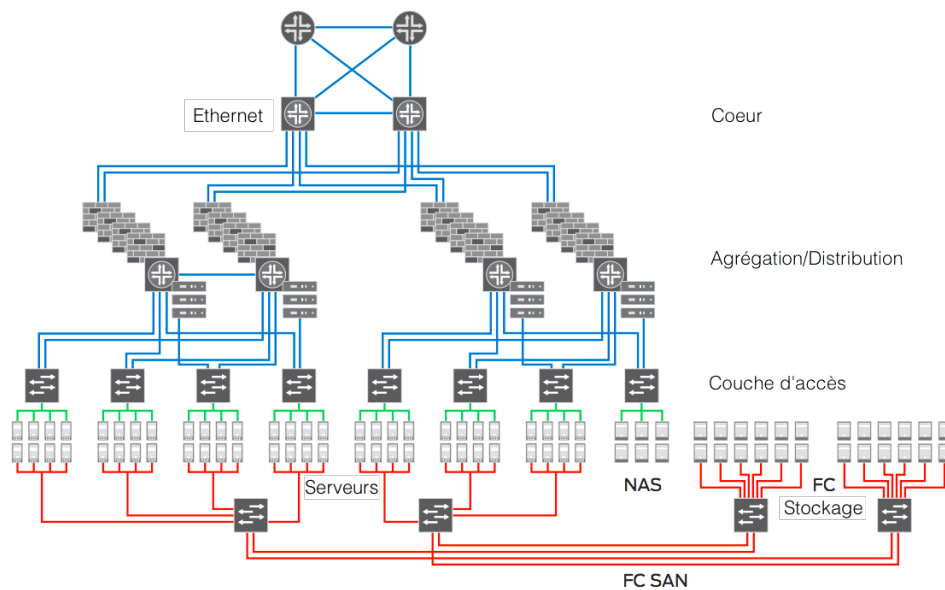


FIGURE 2.1 – Architecture réseau typique à trois niveaux. [16]

Ce modèle d'architecture a été la principale référence de topologie réseau pour les data centres. Cependant, elle commence à devenir compliquée à maintenir dans le contexte du Cloud Computing lors que les applications actuelles commencent à être plus distribuées, avec plusieurs couches et orientées livraison de services. Ces changements des applications ont impacté les réseaux en ce qui concerne le volume et les flux du trafic. Le trafic réseau interne a augmenté avec le déploiement de plus en plus applications et services ; l'utilisation de systèmes de fichiers distribués avec des données stockées séparément a contribué pour l'augmentation de la charge réseau à travers le data centre. De ces faits, on constate une tendance plus grande de communications inter-serveurs ou inter-VMs, impliquant un flux plutôt Est/Ouest que Nord/Sud.

Cette architecture révèle une série d'interfaces de connexions des serveurs à divers type de réseaux tels que réseaux local, de stockage, communication entre processus. Cette disposition ajoute de la complexité et des coûts sous forme de câblage, nombre de ports, extensibilité, énergie, refroidissement etc.

Les data centres d'aujourd'hui exigent des réseau qui sont agile et flexible pour pouvoir réagir rapidement aux changement et garantir une livraison efficace des services. Par exemple, des serveur virtuels peuvent être déplacé d'une part à autre avec une simple commande en fonction de la demande et les réseaux doivent s'adapter rapidement à ces changements pour éviter les perturbation du service. Cela impose que les dispositifs semblent être connectés au même réseau local, indépendamment leur proximité physique. Cette architecture fait défaut de la flexibilité nécessaire pour effectuer ces types de changements, impactant défavorablement l'efficacité opérationnelle de tout le data centre.

2.3 Applications business en transformation

2.4 Différents usages

The growth of server virtualization (virtual machines or VMs), virtualized desktop infrastructures, cloud- computing models, federated or distributed applications, and mobile access devices are all causing shifts in networking traffic patterns toward more E/W traffic flow (Table 1). Industry sources attribute up to 80 percent of network traffic for these next generation applications coming from E/W traffic flows. We expect web applications to deliver integrated, context-specific information and services. And, we expect it right now—low-latency, high performance connections are critical. At the same time, cloud computing and service-oriented applications are introducing more stringent service-level and security demands.

With a physical machine running a network application, that application can have access to the full resources of the network card. Once 10 virtual machines are running together on a single host—sharing a single hardware network card and streaming together through a software switch—that same virtualized application now has fewer networking resources available than it did before. This can lead to overall network performance issues, reduced bandwidth, and increased latency; all issues the application might not

be able to deal with. Even smaller issues such as IP address availability can be impacted by virtualization sprawl.

Virtual infrastructure platforms typically include software that can migrate live virtual machine instances from one physical device to another; VMware Distributed Resource Scheduler (DRS) and VMotion are examples of live migration solutions. Like basic OS virtualization, these migration tools are unaware of the application state, and also have no insight into the Application Delivery Network. For example, VMotion may move a virtual machine running a web shopping cart application from one host server to another without taking into consideration the current persistent state of user's carts, how many connections are coming into the shopping cart, or the network load that this particular virtual machine is currently handling. This migration can cause a lapse in availability; connections to the application and application persistence for the user can be lost during this live migration, resulting in failed transactions, lost shopping cart data, and frustrated users. And while VMotion attempts to move the live image to a host server that is under less load, VMotion doesn't measure the network load of that host device. It might move a live image to a machine with more available CPU cycles but less available network capacity.

2.5 Agilitéé

Moving workloads dynamically requires VMs to stay within a common VLAN in the same Layer 2 (L2) network. If you want to move a VM outside its L2 domain, you have to use manual processes such as assigning and updating the IP addresses for the failed-over services and updating DNS entries correctly. To provide maximum VM flexibility, many enterprises are evaluating ways to enlarge their L2 networks. New capabilities such as Virtual eXtensible LAN (VXLAN) and Network Virtualization using Generic Routing Encapsulation (NVGRE) logically extend an L2 network across L3 networks. However, even with this potential to move VMs across a L3 network, local traffic will still have higher performance and lower latency if it stays within a large L2 network.

2.6 Sécurité

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, other 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 in-activated 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 centres, qui ont été débattues dans le chapitre précédent. Comment SDN approche la problématique ? Qu'est-ce que SDN ?

3.1 Redéfinition de SDN

The definition of network services must be application-centric and simple. The networking requirements of applications should be articulated in an IT-friendly language and used to request desired network behaviors. Today there is limited programmability, resulting in an unfortunate tradeoff. Engineering of cloud applications is either encumbered by detailed network-specific parameters and information, or ignores them and treats the network as a “black box”. Neither is optimal. The first option leads to custom applications for each network type while with the second, applications lack the visibility and control needed to leverage the true capabilities of the network. The proper abstraction of network capabilities, consistent with Software Defined Networking (SDN) principles, drives programmability of network services and increases the consumability of network resources. The instantiation of network services must be instantaneous, aligned with the needs of applications. The network should act reflexively to establish the required connectivity within and across datacenters, and do so in a manner that is consistent with the defined policies of CSPs and their tenants. Today that process is slow, manual and error-prone, relying on work orders to establish a multitude of vendor- dependent configurations.

3.2 Solutions

Nuage Networks™ 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 build 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 centres 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 consommateurs 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 de 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 Protocol, 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. [17]

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. [18]

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. [19]

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. [20]

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. [21]

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. [22] [23]

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. [24]

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. [25]

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. [26]

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. [27] [28]

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. [29] D'après Dosi [30], 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. [31]

Plan de Données Le plan de données 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**. [31]

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. [32]. 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 ». [33]

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. [19]

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: CTSI). 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-AutoScaling-can-reduce-leakage-save-costs.html>. Avr. 2013.

- [10] Kapil BAKSHI. *Cisco Cloud Computing - Data Center Strategy, Architecture, and Solutions*. White Paper. Cisco Systems, Inc. 2009.
- [11] *Virtualization & TCO: Linux vs. Microsoft*. Sondage. Gabriel Consulting Group, Inc. 2009.
- [12] 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>.
- [13] *Cloud-Ready Data Center Reference Architecture, Section : Framework*. White Paper. Juniper Networks, Inc. Mai 2010.
- [14] M. GIROLA et al. *IBM Data Center Networking: Planning for Virtualization and Cloud Computing, chapitre 4 : The new data center design landscape*. IBM redbooks. IBM Redbooks, 2011. ISBN : 9780738435398. URL : <http://books.google.fr/books?id=EKjEAgAAQBAJ>.
- [15] V. JOSYULA, M. ORR et G. PAGE. *Cloud Computing: Automating the Virtualized Data Center, chpaitre 3 : Data Center Architecture and Technologies*. Networking Technology. Pearson Education, 2011. ISBN : 9780132604048.
- [16] *The Cloud-Ready Data Center Network, applying the lessons of cloud computing to vastly improve economics of networking and the user experience*. White Paper. Juniper Networks, Inc. Juin 2012.
- [17] Robert M. KELLER. *Computer Science: Abstraction to Implementation, Section 1.1 The Purpose of Abstraction*. Article. Harvey Mudd College. Sept. 2001.
- [18] *Information Management and Big Data A Reference Architecture*. An Oracle White Paper. Fév. 2013.
- [19] *Intel's Vision of Open Cloud Computing, section Speeding Agility, Reducing Costs, and Accelerating Innovation via Cloud*. White Paper. Intel IT Center. 2013.
- [20] Qingkui CHEN, Haifeng WANG et Wei WANG. « Continuance Parallel Computation Grid Composed of Multi-Clusters. » In : *Journal of Networks* 5.1 (2010).
- [21] William TSCHUDI et al. « High-performance data centers: A research roadmap ». In : (2004).
- [22] Margaret ROUSE. *network fabric*. Web Site. <http://searchsdn.techtarget.com/definition/network-fabric>. Mar. 2014.

- [23] 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>.
- [24] 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.
- [25] *Open Daylight Project*. Web site. <http://www.opendaylight.org/project>. Avr. 2014.
- [26] *Open Source Initiative*. Web site. <http://opensource.org/>. Avr. 2014.
- [27] 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.
- [28] 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>.
- [29] 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.
- [30] G. DOSI. *Technological paradigms and technological trajectories, Research Policy*. Anglais. 1982.
- [31] 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.
- [32] 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>.

- [33] 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 flexible. 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
