Nexus 7000 Virtual Device Context Scenarios de déploiements & « Best Practices »

Introduction

L'objectif de ce document est de fournir aux lecteurs des informations sur les domaines d'application, les cas d'usage, les meilleures pratiques de la fonctionnalité Cisco Virtual Device Context, et ceci tout en respectant les principes de virtualisation logiques d'un même équipement physique.

Ce document est donc à destination des architectes réseaux, des ingénieurs, et des personnes opérationnelles ayant un intérêt pour le design, le déploiement, ainsi que les cas d'usage possibles de la fonctionnalité Virtual Device Context (VDC) disponible dans le système d'exploitation NX-OS qui équipe le commutateur « Datacenter class » Cisco Nexus 7000.

Virtual Device Context (VDC)

La fonctionnalité Cisco Virtual Device Context (VDC) permet de virtualiser un équipement physique en un ou plusieurs équipements logiques. Chacune de ces instances logiques est configurée et managée exactement de la même manière qu'un équipement physique dédié.

Ce partitionnement logique de l'équipement est effectivement total dans le sens ou un VDC assure la même segmentation du plan de control, du plan de données, et du plan de management que sur un environnement physique. Ceci permet également d'atteindre une séparation du « domaine de faute » équivalent à une implémentation multi équipements.

Scénario de déploiement

La section suivante présente les différents scénarii de déploiement dans lesquels l'utilisation des VDC peut répondre aux besoins opérationnels tout en minimisant les équipements physiques. Les architectures présentées sont volontairement très génériques de manière à pouvoir être appliquées à un maximum d'environnement, mais il est évident qu'elles peuvent être facilement adaptées afin de s'intégrer précisément à un cas d'usage précis.

Virtual Device Contexts dans le cadre d'insertion de services tels que les environnements de sécurité.

Les VDC peuvent être utilisés de manière très efficace dans presque toutes les situations ou il est nécessaire de rediriger et d'isoler des flux à direction d'un équipement fournissant des services IP. Ceci est particulièrement vrai dans le cadre de services de sécurités tels que les Firewalls.

Les bénéfices apportés par la segmentation logique du plan de contrôle, de données, et de management, facilitent en effet l'insertion de service réseau et l'exécution des politiques de manière plus déterministe et sécuritaire dans les environnements sensibles.

En créant par exemple des VDCs séparés pour chaque domaines adjacent à un pare-feu, l'administrateur réseau peut ainsi créer différentes « aréas » logiques parfaitement isolées, qui ne pourront être ni contournées ni fusionnées à l'intérieur de l'équipement physique. En d'autres termes, même une erreur de configuration ne pourra permettre une communication entre VDC. La seule et uniquement possibilité de contourner un pare-feu connecté à plusieurs VDCs, est le rajout d'une connexion physique entre deux VDCs. **Ce qui représente exactement le même niveau de risque par rapport à un environnement totalement physique.**

Un exemple de déploiement de ce type à base de VDC est illustré ci-dessous. Dans cet exemple, deux VDC's supplémentaires ont été crée pour réaliser l'architecture, il y a donc un total de trois VDC utilisés. Le VDC par défaut, lequel existe initialement dès le premier boot de l'équipement physique, est utilisé pour la création des deux VDC supplémentaires. Une fois ces VDC supplémentaires créés, le VDC par défaut aura le rôle de master VDC vis-à-vis des autres VDC. Etant donné les droits associés au VDC master, ce dernier doit être strictement réservé à l'administration des VDCs dans les environnements hautement sécurisés. Les deux autres VDC sont utilisés pour constituer l'infrastructure des domaines de sécurités « inside » et « outside » du pare-feu dans cet exemple.

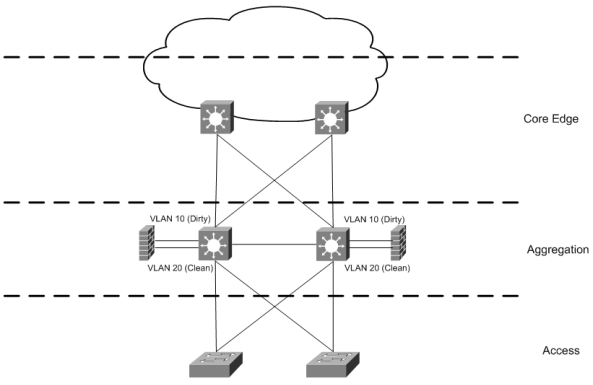

Figure 1 - Séparation de domaines avec VLANs

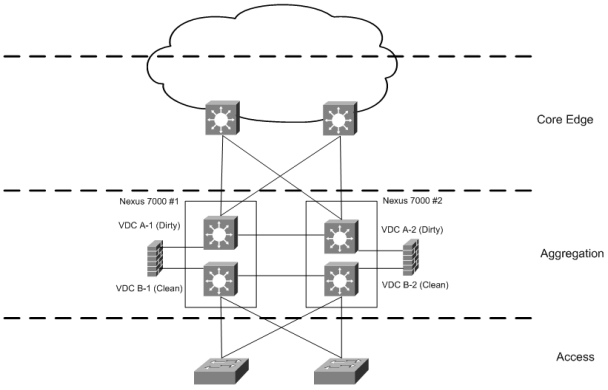

Figure 2 - Séparation des domaines avec VDCs

Virtual Device Contexts dans une consolidation horizontale

Les VDCs peuvent être également utilisés dans des approches de consolidation d'équipements physiques « parallèles », partageant un même rôle fonctionnel à travers un ou plusieurs domaines administratifs ou zones de services. Ce type de consolidation, « horizontale », peut s'appliquer par exemple à des équipements constituant une couche d'agrégation dans un Datacenter fournissant des services à différent groupes, tel que des départements ou business unit dans une entreprise ou, dans le cas d'un environnement service provider à différents clients.

Dans un déploiement traditionnel les blocs d'accès d'un Datacenter partageant un même niveau de service, sont connectés sur des équipements d'agrégation communs, eux-mêmes constitués d'équipements physiques dédiés. Ceci peut être réalisé dans un but d'offrir un niveau de disponibilité, de sécurité, ou un niveau de service (SLA) différents par groupe, département, client ….Une alternative à ce modèle est l'utilisation de VDC afin de créer des équipements d'agrégations virtuels. Ceci représente un avantage en termes d'optimisation des ressources, de l'espace, consommation électrique, refroidissement tout en offrant le même niveau d'isolation entre les couches d'agrégations.

Alors qu'une architecture physique est d'avantage évolutive par nature, en rajoutant des équipements, on ajoute en effet de manière linéaire les ressources associées à ces équipements, il est souvent plus difficile de contrôler les coûts associés à ce type d'évolution. Avec l'usage de VDC, les ressources peuvent être d'avantage contrôlées et affectées, et ceci de manière plus granulaire. Enfin, il est important de noter que dans le cas ou il serait nécessaire de faire évoluer une architecture logique vers une architecture physique, cette migration sera particulièrement simple grâce à la structure des VDCs. Un VDC est en effet très simplement remplaçable par un équipement physique. Sa configuration est indépendante, et ses liens physiques d'attachement avec le reste de l'architecture dédiée.

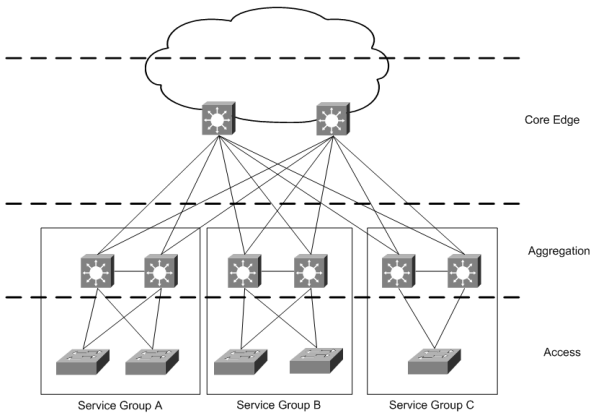

Figure 3 - Typical physical topology

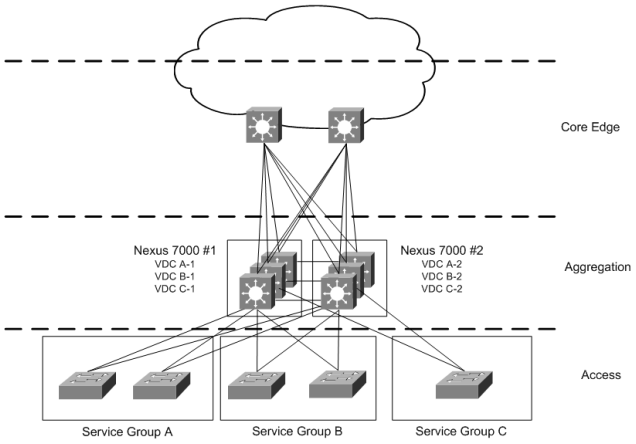

Figure 4 - Horizontal Consolidation w/VDCs

L'exemple précédent illustre la consolidation horizontale de plusieurs couches d'agrégations en utilisant des VDCs tous connectés à une couche de cœur commune. Le VDC fournissant une virtualisation complète, plan de contrôle, données et management, les designs les utilisant sont plus flexibles que d'autres solutions utilisant d'autres solutions de virtualisation tel que les VRF ou les VLANs.

Avec l'usage des VDCs, les équipements d'agrégation virtuels peuvent être contrôlés et opérés de manière classique depuis un domaine administratif unique, mais peuvent aussi être contrôlées et maintenus séparément depuis des domaines administratifs différents.

Cas typique d'usage : Consolidation des blocs d'agrégation, environnement Datacenter Multi-tenant, fusion & acquisition, service hébergés, équipements en co-location.

Virtual Device Contexts dans une consolidation verticale

Les VDC peuvent également être utilisés afin de consolider des équipements physiques qui fournissent des caractéristiques fonctionnelles différentes dans une topologie donnée. Ce type de consolidation verticale peut être illustré par exemple dans le cas ou un architecte réseau décide de réaliser une consolidation verticale entre une couche cœur et une couche d'agrégation. Ce type de modèle « collapsed » entre cœur et agrégation fournit les mêmes bénéfices que le modèle précédent de consolidation horizontale, optimisation de l'utilisation des interfaces physiques de l'équipement, des ressources, de l'espace, puissance….

La consolidation verticale ne perturbe pas non plus les modèles opérationnels en place. Les possibilités de découpages des responsabilités d'un point de vue opérationnel en un groupe unique ou plusieurs groupes restent exactement similaires et consistant par rapport à une architecture utilisant une séparation physique des équipements.

Encore une fois, cela est possible grâce à une totale séparation par VDC du plan de management mais aussi de l'ensemble de l'instrumentation comme AAA, le monitoring, SNMP, Syslog, XML,…

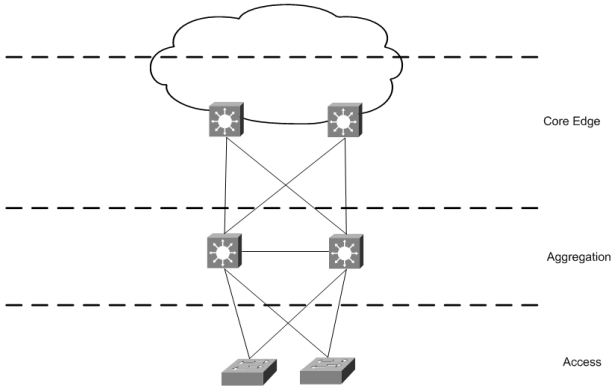

Figure 6 – Topologie physique

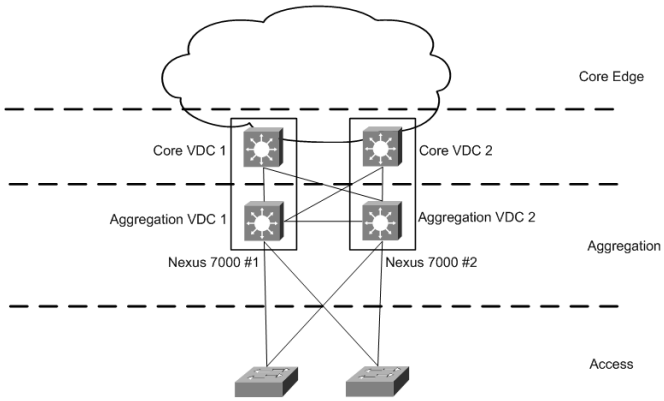

Figure 5 – Consolidation verticale avec l'usage de VDCs

Cas typique d'usage : Consolidation cœur & agrégation pour les architectures de taille moyenne, environnement de tests ou développement, sites secondaires ou distants.

Virtual Device Contexts pour une consolidation combinée horizontale et verticale.

Dans le cas ou le niveau de consolidation et la densité sont des critères importants, il y a alors une troisième option combinant les stratégies de consolidation horizontale et verticale avec les VDCs. Il est en effet possible d'utiliser les VDCs pour fournir les services normalement délivrés par plusieurs types d'équipements physiques, et ainsi pousser au maximum l'optimisation des ressources comme l'espace, la consommation et le refroidissement. Ce type de consolidation mixte, horizontale et verticale apporte également une diminution des couts très significatifs comparativement à une architecture physique similaire.

Comme nous l'avons vu dans les exemples précédents, et comme son nom l'indique, une consolidation combinée horizontale et verticale permet de consolider des équipements partageant un même rôle fonctionnel avec d'autres équipements ayant un rôle différent.

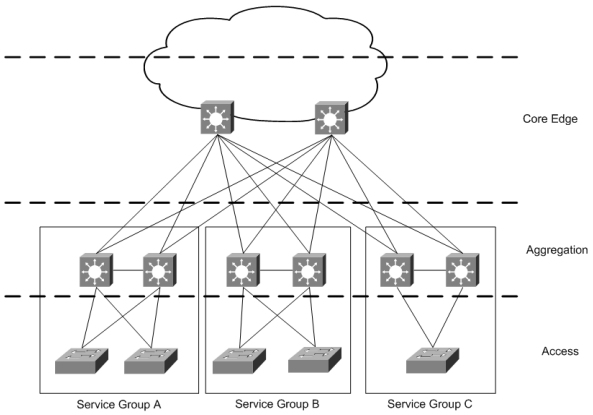

Figure 7- Topologie physique classique

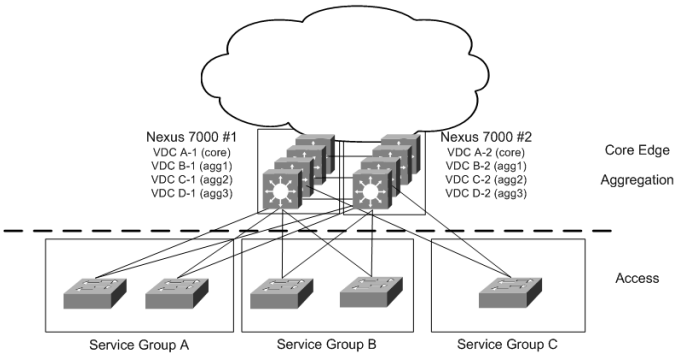

Figure 8 – Consolidation combine verticale et horizontale avec VDCs.

Cas typique d'usage : Consolidation cœur & agrégation pour les architectures de taille moyenne, environnement de tests ou développement, sites secondaires ou distants.

Virtual Device Contexts bonnes pratiques

- Dans les déploiements très sensibles d'un vue de vue sécurité, il est recommandé que le VDC par défaut soit réservé au rôle de master VDC, et soit strictement utilisé pour l'administration des autres VDCs. Ceci implique qu'il n'y ait pas de données commutées par ce VDC sans que cela soit absolument nécessaire.

- Dans tous les environnements utilisant des VDC, il est recommandé que l'accès au VDC par défaut soit restreint aux personnes ayant besoin de réaliser des tâches opérationnelles sur les VDCs. Ainsi, uniquement ces personnes posséderont un compte avec le rôle « vdc-admin » en plus d'un potentiel droit de type « network-admin »

- Dans le cas ou le VDC master doit absolument traiter des paquets de données, il faut alors faire en sorte que ce dernier ait la charge d'assurer le rôle le plus critique, nécessitant le plus haut niveau de disponibilité. Cela permet de minimiser la probabilité que des tâches opérationnelles sur un VDC de priorités inférieure (réaffectation de ressources, redémarrage du VDC, …) puisse impacter le VDC le plus critique.

- Dans le cas ou les VDCs ont des domaines administratifs séparés (différents administrateur par VDC), l'utilisation des fonctionnalités AAA pour l'authentification et les autorisations doit être considérée de manière maitrisée. En effet, l'authentification des administrateurs de plusieurs VDCs sur le même serveur AAA revient implicitement à considérer que l'ensemble des VDCs sont administrés dans un même domaine d'administration. De manière à correctement séparer les responsabilités entre les VDCs, et prévenir le fait d'un compte « admin » d'un VDC puisse avoir accès à un autre VDC, les options suivantes sont possibles :

    - Créer différent comptes utilisateur sur le serveur AAA et limiter l'accès à ces utilisateurs en utilisant des fonctionnalités comme Network Access Restrictions (Disponible sur CiscoSecure ACS), afin de spécifier l'adresse IP du client AAA. Comme chaque VDC utilise son adresse IP d'administration pour forger les paquets AAA, il est en effet possible de faire la distinction entre les VDCs, et ainsi octroyer des droits spécifiques à un administrateur sur un VDC donné.

    - Il est également possible d'utiliser un serveur AAA différent par VDC. Il faut dans ce cas que le compte de l'administrateur d'un VDC donné n'existe pas dans la base de données des utilisateurs des autres serveurs AAA.

- Il est recommandé de configurer explicitement la politique de HA dans les nouveaux VDC créés afin de minimiser l'impact d'un redémarrage ou l'arrêt d'un VDC dans un

environnement « dual sup ». En effet, la politique de HA par défaut dans les environnements dual sup est « switchover », ce qui déclenche une « bascule » des cartes de supervision dans le cas d'un problème dans un VDC.

- Revoir la politique du plan de contrôle, Control Plane Policing (CoPP), et les limites configurées afin de s'assurer qu'elles soient appropriées pour l'environnement. Le système applique CoPP de manière collectif pour tous les VDCs du fait qu'il y ait une seule interface logique in-bande pour le plan de contrôle.

Conclusion

À partir des différents scénarii explorés, il devient évident que les VDCs offrent une grande quantité de possibilités et d'options de conception permettant de maximiser l'espace dans les nouveaux Datacenter, mais également dans des centres existants, tout en optimisant l'usage des ressources.

La limitation de ressources étant l'un des facteurs principaux limitant l'évolution des architectures globales des Datacenters, ces outils supplémentaires apportés par les VDCs permettant leur optimisation tout en préservant les modèles opérationnels, sont particulièrement intéressants.

Le Virtual Device Context est juste l'un des nombreux outils disponibles sur les Cisco Nexus 7000 qui offre ce type de bénéfice et d'optimisation tout est restant totalement transparent pour les opérations.