h e p i a
Haute école du paysage, d'ingénierie
et d'architecture de Genève

Printemps 2016
Session de Bachelor

VMWARE NSX ET VIRTUALISATION RESEAU

Travail de Bachelor réalisé par

Ouafae Ifakren

Pour l'obtention du titre Bachelor of Science HES-SO en Ingénierie des technologies de l'information avec orientation en

Communications, multimédia et réseaux

Suivi par M. Gérald Litzistorf, professeur HES
M. Sylvain Liaudat, Directeur adjoint au SIACG

Et par M. Cédric Good. Directeur de SmartBee

Septembre 2016

h e p i a

Haute école du paysage, d'ingénierie
et d'architecture de Genève

Printemps 2016
Session de Bachelor

ENONCE

h e p i a

Haute école du paysage, d'ingénierie
et d'architecture de Genève

Automne 2016
Session de bachelor

INGÉNIERIE DES TECHNOLOGIES DE L'INFORMATION

ORIENTATION COMMUNICATIONS, MULTIMEDIA ET RESEAUX

VMWARE NSX

Descriptif :

La consolidation des serveurs permet de partager les ressources (CPU, RAM,...) d'un serveur physique à N serveurs logiques (= N machines virtuelles) permettant des gains de surface, de consommation électrique et de productivité.

Certaines grandes entreprises, ayant des centaines de machines virtuelles réparties sur plusieurs serveurs (éventuellement sur plusieurs sites), ont besoin d'une gestion centralisée de leur infrastructure informatique (serveurs logiques - firewall - routeur - commutateur - système de stockage).

La solution NSX créé un réseau logique cohérent au-dessus des dizaines de serveurs physiques hébergeant des centaines de machines virtuelles. Elle offre également des services virtualisés de sécurité tels que VLAN, firewall, VPN et QoS.

Travail demandé :

Ce travail comprend les étapes suivantes :

1) Etude théorique
   - Quelles sont les principales fonctions offertes ?
   - Quels sont les supports disponibles (pdf, livedemo, ...) ?

2a) Analyse du scénario multi-tenants permettant à plusieurs clients d'être parfaitement isolés tout en bénéficiant de services centralisés (monitoring, backup)
   - Quelles sont les options possibles au niveau du design ?
   - Présenter les avantages et inconvénients
   - Définir les tests unitaires

2b) Analyse du scénario firewall et SSL balancer
   - Contrôler le niveau fonctionnel de ces composants en C3 et C4-C7
   - Tableau de maturité

3) Mise en oeuvre des scénarios
   - Documenter toutes les étapes (vSphere, vCenter, ESXi, ...)
   - Effectuer les tests unitaires
   - Mentionner les difficultés rencontrées

4) Guide méthodologique
   - Peut-on conserver les bonnes pratiques du monde physique ?
   - Doit-on réfléchir autrement ?
   - Peut-on se passer d'un firewall physique ?
   - Y a-t-il des limites ?
   - Analyse sur la sécurité (disponibilité, résilience)
   - Avantages et inconvénients par rapport à des composants externes

Sous réserve de modification en cours du travail de Bachelor

Candidate :
Mme Ouafae Ifakren
Filière d'études : ITI

Professeur(s) responsable(s) :
Litzistorf Gérald

En collaboration avec : SIACG & SmartBee
Travail de bachelor soumis à une convention de stage en entreprise : non
Travail de bachelor soumis à un contrat de confidentialité : non

Timbre de la direction

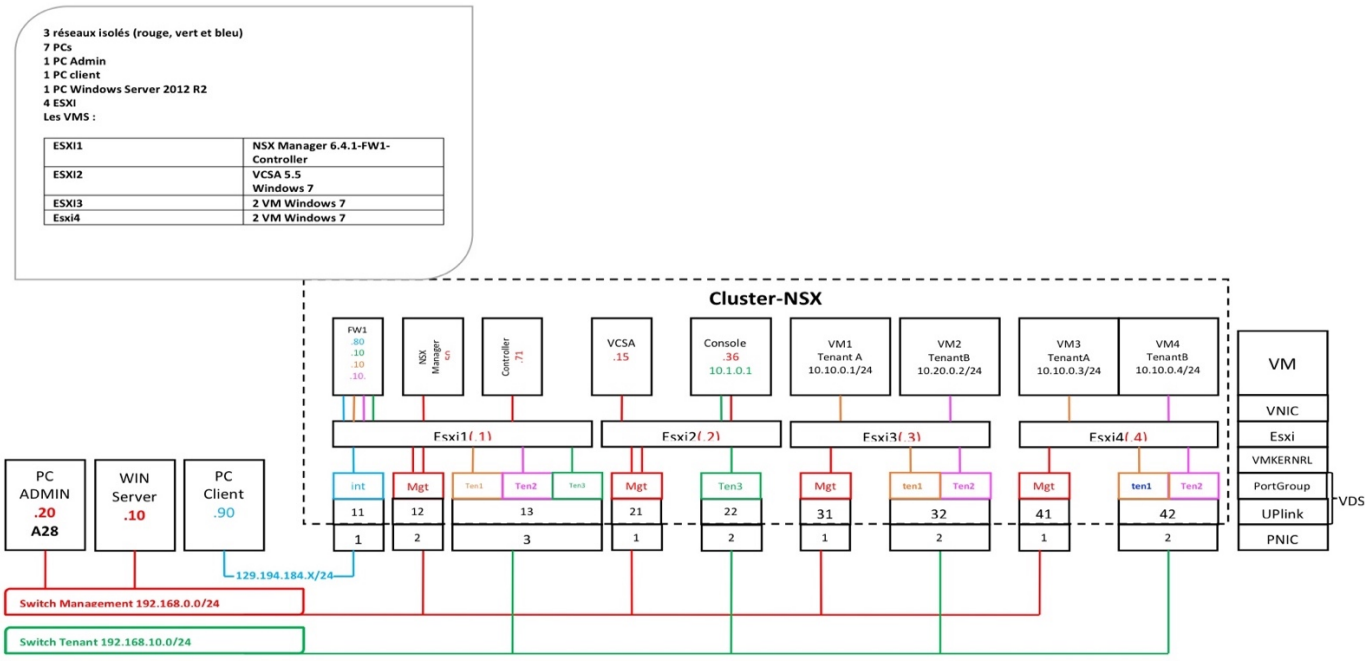
RESUME

VMware NSX est un produit qui sert à produire un réseau virtuel avec toutes les fonctionnalités d'un réseau physique
Ce travail a pour objectif d'étudier et tester les fonctionnalités de VMware NSX pour la mise en place d'une plateforme capable de produire un réseau virtuel.

Tout au long de ce travail, j'ai testé les services proposés par NSX tels que le routing. le firewalling et le Load Balancing en réalisant plusieurs scénarios au sein du laboratoire de réseaux et télécommunications.

Ce travail a été réalisé en plusieurs étapes:

1. La partie documentation consistait à lire tous les documents et livres proposés par Vmware NSX, consulter des blogs, des sites internet dédiés à ce sujet et sélectionner les documents les plus utiles pour réaliser ce travail.
2. Installation et configuration de ESXI 5.5, VCSA (VCenter Server Appliance) et NSX manager
3. Mise en place d'une architecture multi-tenants comportant l'installation de 4 VMS pour deux tenants A et B, la configuration des switches logiques et des routeurs logiques capables de lier les tenants à internet
4. La définition d'une politique de sécurité à l'aide des règles Firewalls distribué et de l'EDGE Firewall capables d'être générées facilement dans une architecture évolutive pour réaliser l'isolation des tenants
5. Mise en place et test du Load Balancing.
6. Comparaison avec une architecture physique



Candidat :

Mme IFAKREN OUAFAE
Filière d'études : ITI

Professeur(s) responsable(s) :

Litzistorf Gérald

En collaboration avec : SIACG & SmartBee
Travail de bachelor soumis à une convention de stage en entreprise : non
Travail de bachelor soumis à un contrat de confidentialité : non

GLOSSAIRE

AD	Active Directory
DFW	Distributed Firewall
DLR	Distributed Logical Router
DNAT	Destination NAT (chez VMware)
ESG	Edge Services Gateway
EDGE FW	Edge Firewall
LS	Logical Switch
SNAT	Source NAT (chez VMware)
VIP	Virtual IP : l'adresse IP du serveur virtuel
VM	Virtual machine
VXLAN	Virtual Extensible LAN

REMERCIEMENT

Je voudrais tout d'abord adresser toute ma gratitude à **M. Litzistrof** , directeur de mon mémoire, dont les conseils,les critiques et la disponibilité ont été d'un grand apport pour la réalisation de ce travail.

J'adresse, en outre, mes remerciements à **M. Cédric Good**, directeur de l'entreprise SmartBee, ainsi qu'à **M. Sylvain Liaudat**, directeur adjoint au Service Intercommunal d'informatique(SIACG), pour leurs conseils et encadrement.

Je remercie tout le personnel administratif de l'HEPIA pour sa collaboration, tout spécialement **Mme Rinckenberger.**

Je voudrais exprimer ma reconnaissance envers toute l'équipe de développeurs de VMware new-yorkais ainsi que toute personne qui m'a soutenue dans la réalisation de ce mémoire.

Enfin, je remercie toute ma famille Ivano et en particulier ma chère maman qui m'a soutenue tout au long de mes études.

LISTE DE FIGURES

TABLE DES MATIERES

INTRODUCTION

La technologie de la virtualisation a évolué rapidement, pour passer de la virtualisation des serveurs à la virtualisation des réseaux.

VMware a lancé ces dernières années son produit NSX après le rachat de la société Nicira
Le principal atout ou caractéristique de ce nouveau produit est sa puissance. En effet, selon VMware,il permet de déployer des réseaux virtuels ayant les mêmes fonctionnalités que les réseaux physiques en quelques clics.
Les questions que l'on se pose de prime abord, et que je vais travailler à répondre tout au long de ce rapport sont les suivantes :

- Comment fonctionne ce produit ?
- Quelles sont les fonctionnalités qu'il propose ?
- Quelle est la bonne pratique pour déployer NSX sans problème ?
- Quelle politique de sécurité suit-il pour assurer un isolement des tenants?
- Est-ce que nous pouvons nous passer des Firewalls physiques ?
- Quels sont les avantages et inconvénients par rapport à un réseau physique ?

Comment ce rapport est-il structuré ?

Ce rapport est constitué de cinq chapitres, à savoir la composants et services, les étapes de l'installation, l'isolation des tenants de NSX et les scénarios utilisés pour tester ses fonctionnalités.
Le rapport s'achève par le bilan.

Chapitre1 : Composants et services
Ce chapitre comprend une vue d'ensemble de l'architecture de VMware NSX, ainsi qu'une description des couches et des services qui le constituent. Enfin, le chapitre présente les définitions des termes techniques.

Chapitre2 : Etapes de l'installation
Dans ce chapitre, j'explique les différentes étapes de l'installation, commençant par la configuration d'Active Directory jusqu'au déploiement des contrôleurs.

Chapitre 3 : Isolation des tenants
Ce chapitre teste l'isolation des tenants en mettant en place différents scénarios multi-tenants
Le chapitre détaille aussi les démarches à suivre pour configurer les VXLANS, les switches logiques, le router distribué et *l'Edge Services Gateway.*
Il explique aussi les différents dispositifs mis en place par VMware pour assurer une sécurité optimale du réseau logique.

Chapitre 4 : Load Balancer – SSL
Vous découvrirez dans ce chapitre les deux scénarios adoptés pour tester les modes *Load Balancing* qui existent dans NSX.
Un autre scénario testera la performance du Load Balancer en activant la haute disponibilité. Et enfin, une conclusion qui le compare avec un *Load Balancer* physique.

Chapitre 5 : Bilan
Dans ce chapitre, j'analyse d'une part les résultats obtenus dans les différents scénarios en mettant en évidence les avantages et les inconvénients par rapport à un réseau physique.
D'autre part, je cite les problèmes rencontrés pour la mise en œuvre de ce projet, et je conclus par les projets futurs que VMware compte mettre en place pour la virtualisation du réseau.

La partie **Annexes** comporte les détails de l'installation, les prérequis matériels et logiciels, le *troubleshooting* des différentes erreurs rencontrées au cours de l'installation ou de la configuration ainsi qu'une liste de prix des modules VMware NSX.

CHAPITRE1 :

COMPOSANTS ET SERVICES

Ce chapitre décrit l'architecture de VMware NSX, présente ses composants et services et ses différents dispositifs utilisés pour assurer la sécurité et l'isolation du réseau logique.

Enfin je donne des définitions des termes techniques utilisés dans ce rapport

.

1.1 PRESENTATION

VMware NSX est une technologie de virtualisation de réseau, appartenant à la famille SDDC (Software Defined Data Center)[1], ce qui lui permet d'être gérée à travers un centre de donnée.

L'architecture de VMware NSX est composée d'un plan de gestion, d'un plan de contrôle et d'un plan de données.
Il est disponible en deux versions :

- **NSX -in** qui dépend de la solution VMware, par conséquent, il ne peut fonctionner qu'avec un hyperviseur Vsphere de VMware.
- **NSX -mh** qui fonctionne avec d'autres hyperviseurs tels que KVM.

Pour VMware NSX, il y a deux points de vue sur le réseau existant, logique et transport.
La vue logique est un ensemble de services de réseau. La machine virtualisée est vue dans le cloud. Elle est donc indépendante de la sous-couche matérielle.
Dans un environnement multi-tenants, à chaque tenant son point de vue logique de son réseau, mais il ne peut pas voir le réseau d'un autre tenant.
Ce réseau se compose de ports virtuels, switch et routeurs virtuels, qui connectent les machines virtuelles (VMS) entre elles ou avec le monde extérieur.
La vue transport réseau représente les dispositifs réels du réseau physique
Ces dispositifs physiques, y compris les serveurs de l'hyperviseur et les périphériques réseau (passerelles), sont considérés comme des nœuds de transport, faisant ainsi une connexion avec le réseau physique.

1.2 ARCHITECTURE[2]

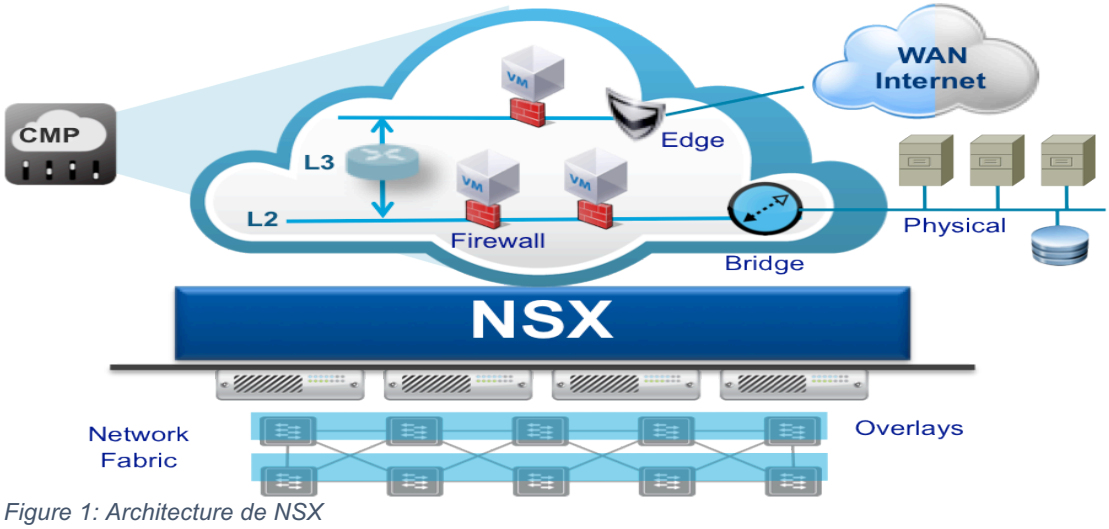


Figure 1: Architecture de NSX

[1] Chapitre 1 paragraphe Définitions
[2] https://blogs.vmware.com/networkvirtualization/2013/08/vmware-nsx.html#.V4voaGNfxAY

L'architecture de VMware NSX comporte plusieurs composants dont certains font partie de la solution VMware NSX, d'autres peuvent appartenir à d'autres solutions comme Openstack ou aussi Cisco.
Les composants appartenant à VMware NSX, sont divisés en plan de données, plan de contrôle et plan de gestion. Le plan de données est le plan qui s'exécute sur l'hyperviseur.
Le plan de contrôle est composé d'un groupe de contrôleurs.
Le plan de gestion, quant à lui, fournit l'API NSX gérée par le NSX manager.

1.2.1 Data plane

Appelé aussi le plan de données. Le Data plane est implémenté au niveau KERNEL et assure le transfert des paquets par les chemins construits par le plan de contrôle.
Il est représenté par le Switch virtuel qui est basé sur le VDS (*Virtual Distributed Switch*), et peut être déployé de deux façons :

- Overlay network : encapsulation implémentée en utilisant STT[3]. GRE[4]. VLXLAN, IPSEC et IPSEC-STT-GRE
- Bridged Network : les données sont envoyées directement, sans encapsulation, au réseau physique. Mais, c'est rarement utilisé.

C'est la première méthode qui va être utilisée dans ce travail.

1.2.2 Control plane

Ou plan de contrôle. Le composant de ce plan est le *controller cluste*r. Via l'API de NSX, le contrôleur gère les instructions du tenant, et communique également avec les hyperviseurs afin de déterminer la position des VMS.
Aucun Trafic du *Data Plane* ne passe par la VM du contrôleur

1.2.3 Management Plane & Consumption Model

Ou le plan de gestion. Il est composé du NSX manager qui fournit une gestion centralisée du réseau logique. Cette gestion est assurée grâce à REST API[5], en utilisant comme outil de gestion CMP (*Cloud Management Platform*) .

1.3 LES COMPOSANTS

1.3.1 NSX manager

Est le centre de l'infrastructure VMware NSX. C'est le premier composant à déployer Il assure le fonctionnement de *management plane* et fournit le point unique pour communiquer avec l'environnement NSX

1.3.2 NSX Controller

Est le composant qui constitue le *control plane*. Il assure le fonctionnement des Switches virtuels (*logical Switches*), et maintient les informations des VMS, des switches logiques, ESXI et des VXLANS.
Il est déployé dans un cluster en nombre impair pour assurer la disponibilité permanente du trafic dans le cas d'une panne de l'un des contrôleurs déployés.

[3] A Stateless Transport Tunneling Protocol for Network Virtualization
[4] Generic Routing Encapsulation
[5] Representational State Transfer : est un style d'architecture pour les systèmes hypermédia distribués, créé par Roy Fielding en 2000 dans le chapitre 5 de sa thèse de doctorat1. Il trouve notamment des applications dans le World Wide Web

1.4 FONCTIONNEMENT DES SERVICES

1.4.1 Les VXLANS

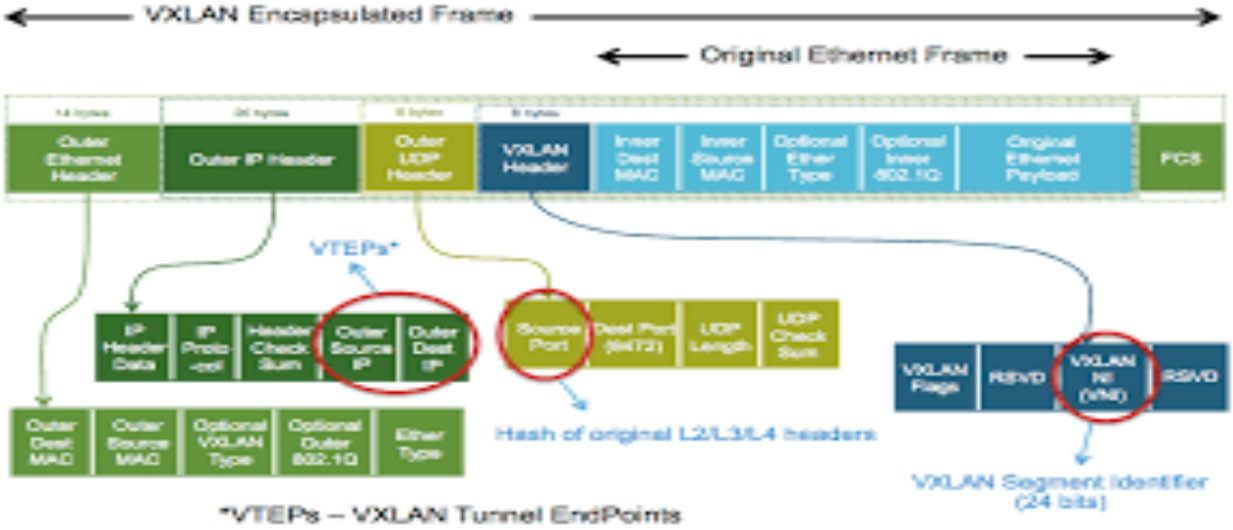


Figure 2: Trame VXLAN [6]

Virtual Extensible LAN est un protocole qui permet de superposer un réseau virtuel L2 sur une couche IP déjà existante.
Ce protocole joue un rôle important dans l'isolation des réseaux virtuels à l'échelle d'un cloud, en offrant les avantages suivants :
Un identifiant sur 24 bits, le *VXLAN Network Identifier* (VNI), permet de numéroter suffisamment de VXLAN pour isoler de très nombreux clients allant jusqu'à 16 millions.
L'encapsulation des trames dans des datagrammes UDP permet au VXLAN d'avoir un champ d'action plus important que le VLAN

Dans le scénario utilisé dans ce travail, le mode adopté dans les VXLANS configurés est le mode unicast parce que les switches physiques utilisés dans ce travail ne supportent pas le mode multicast.

. [6] https://www.vmware.com/files/pdf/products/nsx/vmw-nsx-network-virtualization-design-guide.pdf Page 19

1.4.2 Trafic Unicast

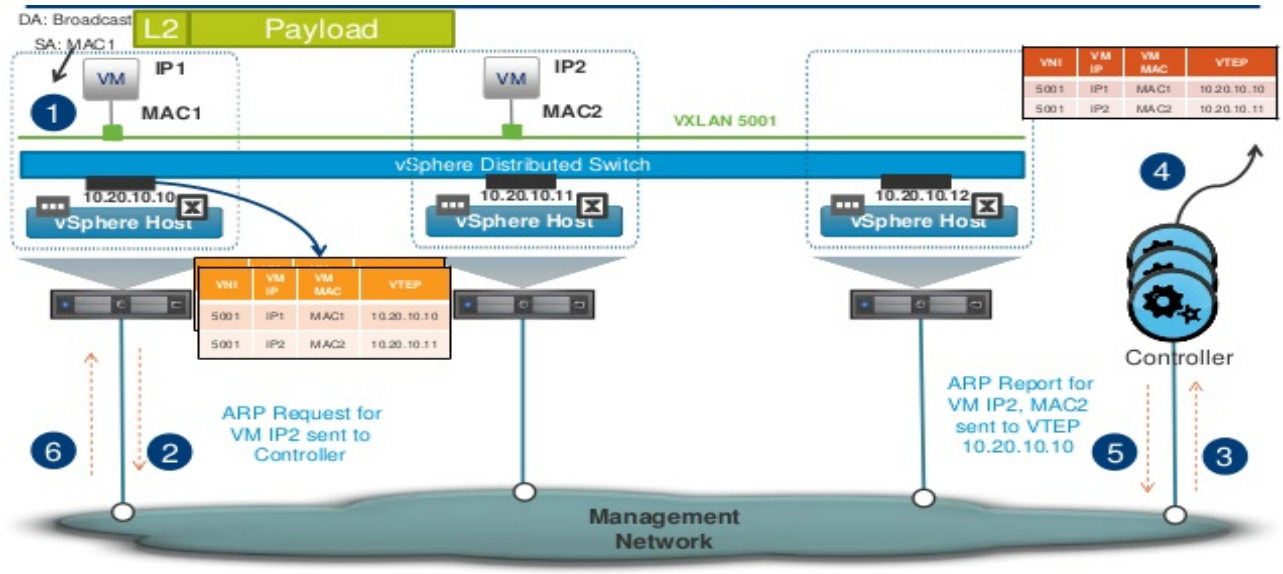


Figure 3 Trafic unicast[7]

- VM1 envoie une requête ARP en broadcast sur le segment 5000 pour déterminer le MAC/IP de VM3.
- Esxi3 intercepte la requête et l'envoie au contrôleur via le plan de contrôle
- Le contrôleur reçoit la requête
- Il vérifie sa table ARP
- Il envoie après l'information à ESXi3
- Esxi3 reçoit l'information du plan de contrôle et met à jour sa table ARP. A ce point le VTEP de VM3 est connu

VNI	VM IP	VM MAC	VTEP
5000	10.1.0.2	MAC1	192.168.10.61
5000	10.1.0.3	MAC2	192.168.10.62

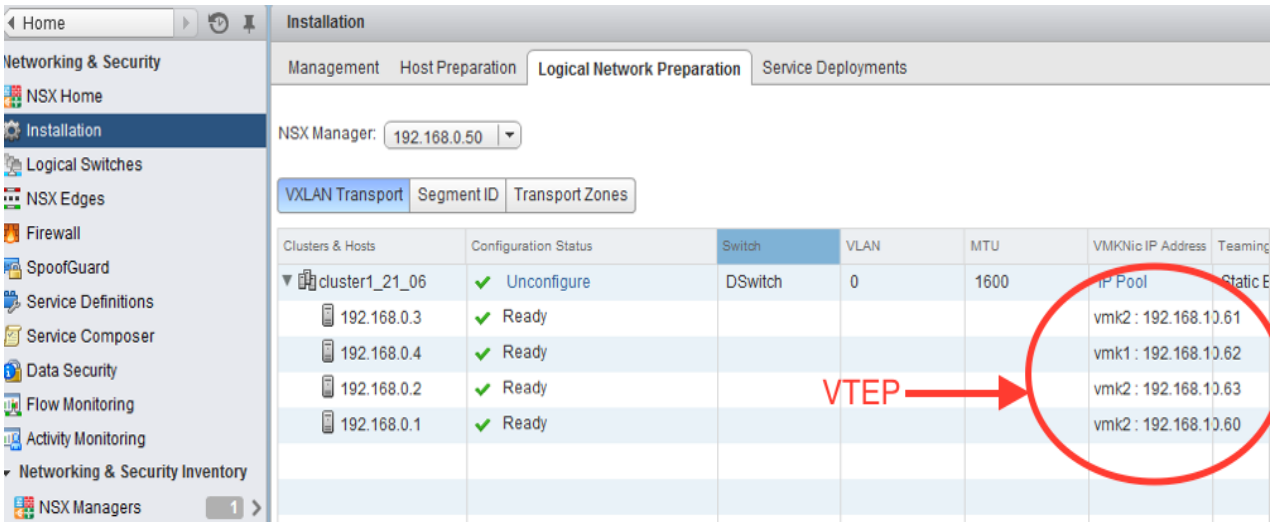
VTEP Table

```
htb-1n-eng-dhcp10 # show control-cluster logical-switches vtep-table  5000
VNI       IP              Segment         MAC               Connection-ID
5000      192.168.10.60   192.168.10.0    00:50:56:65:38:ef 2
5000      192.168.10.61   192.168.10.0    00:50:56:63:6d:1a 9
```

```
htb-1n-eng-dhcp10 # show control-cluster logical-switches vtep-table  5000
VNI       IP              Segment         MAC               Connection-ID
5000      192.168.10.60   192.168.10.0    00:50:56:65:38:ef 2
5000      192.168.10.61   192.168.10.0    00:50:56:63:6d:1a 9
```

[7] http://fr.slideshare.net/VMworld/vmworld-2013-operational-best-practices-for-nsx-in-vmware-environments

1.4.3 Le rôle des VTEP



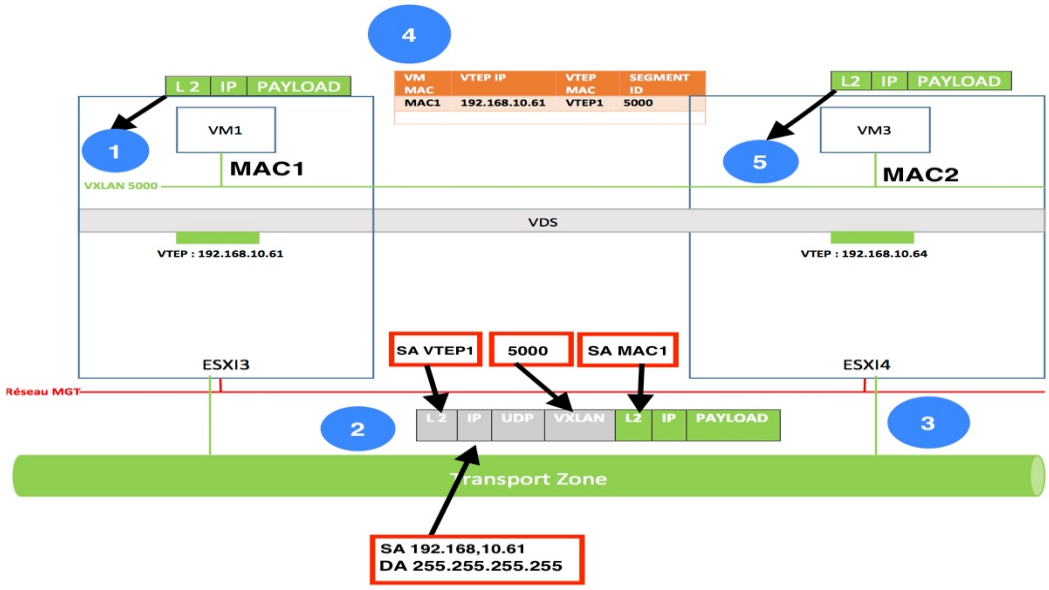


Figure 4:VTEP- envoi de la table

1- VM1 envoie un ARP request à l'adresse broadcast
2- VTEP dans ESXI3 encapsule le paquet dans une entête UDP avec une adresse broadcast et l'adresse VTEP de ESXI3 comme adresse source
3- Le réseau physique transport zone envoie le paquet à tous les ESXI qui sont sur le VXLAN 5000
4- VTEP dans ESXI4 reçoit le paquet encapsulé avec les informations mentionnées dans la figure
5- Il le dés-encapsule et l'envoie à VM3

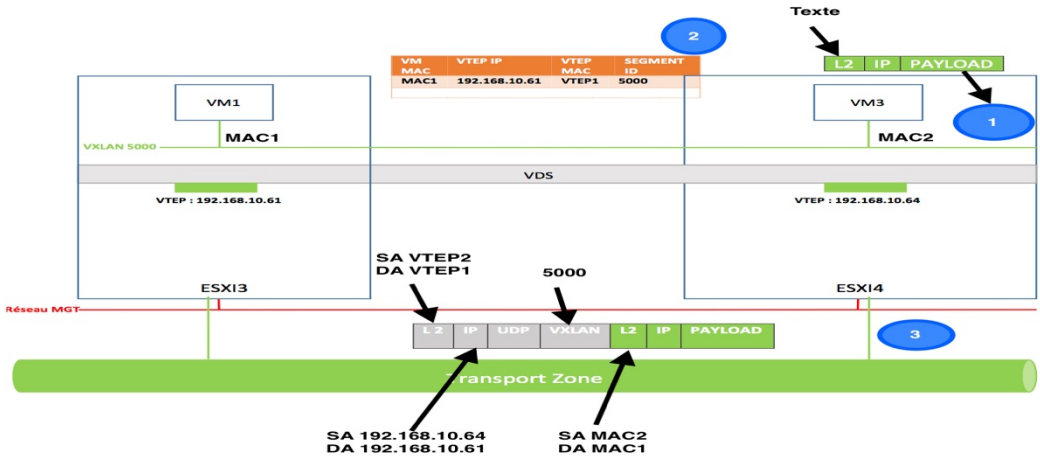


Figure 5:Transfert de la table lookup

1. Vm3 répond au request du VM1 en envoyant un paquet ARP en unicast à MAC1 avec son adresse MAC2
2. VTEP dans ESXI4 fait une recherche dans la table VTEP et obtient l'adresse VETP de ESXI3 et MAC1. ESXI4 sait maintenant que pour envoyer le paquet à VM1, il faut l'envoyer à l'adresse 192.168.10.61
3. VTEP de ESXI4 crée un paquet unicast et l'envoie à l'adresse VTEP de ESXI3

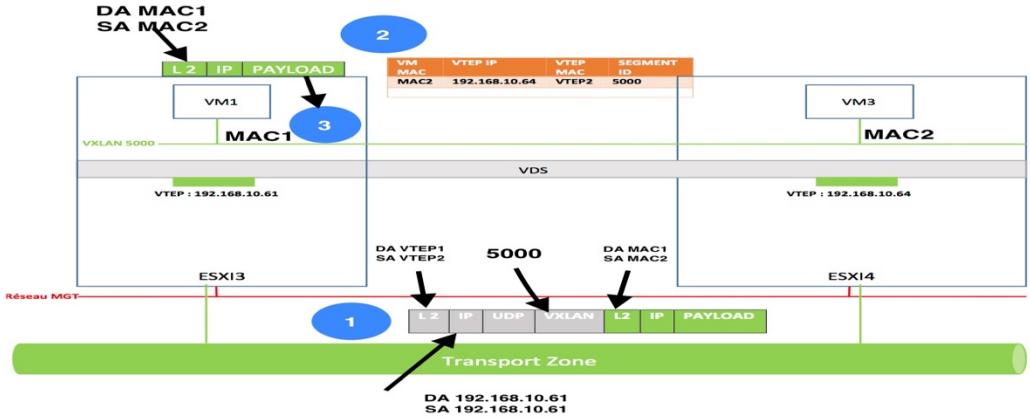


Figure 6:Table entry

1. Le paquet est envoyé à ESXI3
2. VTEP dans ESXI1 reçoit le paquet encapsulé. Grâce à la table VTEP, il apprend que l'adresse VTEP de ESXI4 est192.168.10.64. Il apprend aussi MAC2 de VM3 et vérifie l'ID du VXLAN pour décider ensuite si le paquet devrait être transféré ou non.
3. Le paquet est dés-encapsulé et envoyé à VM1

D'après ces tests, nous constatons une isolation du réseau logique par rapport au réseau physique. La connexion avant la configuration du VXLAN était possible.

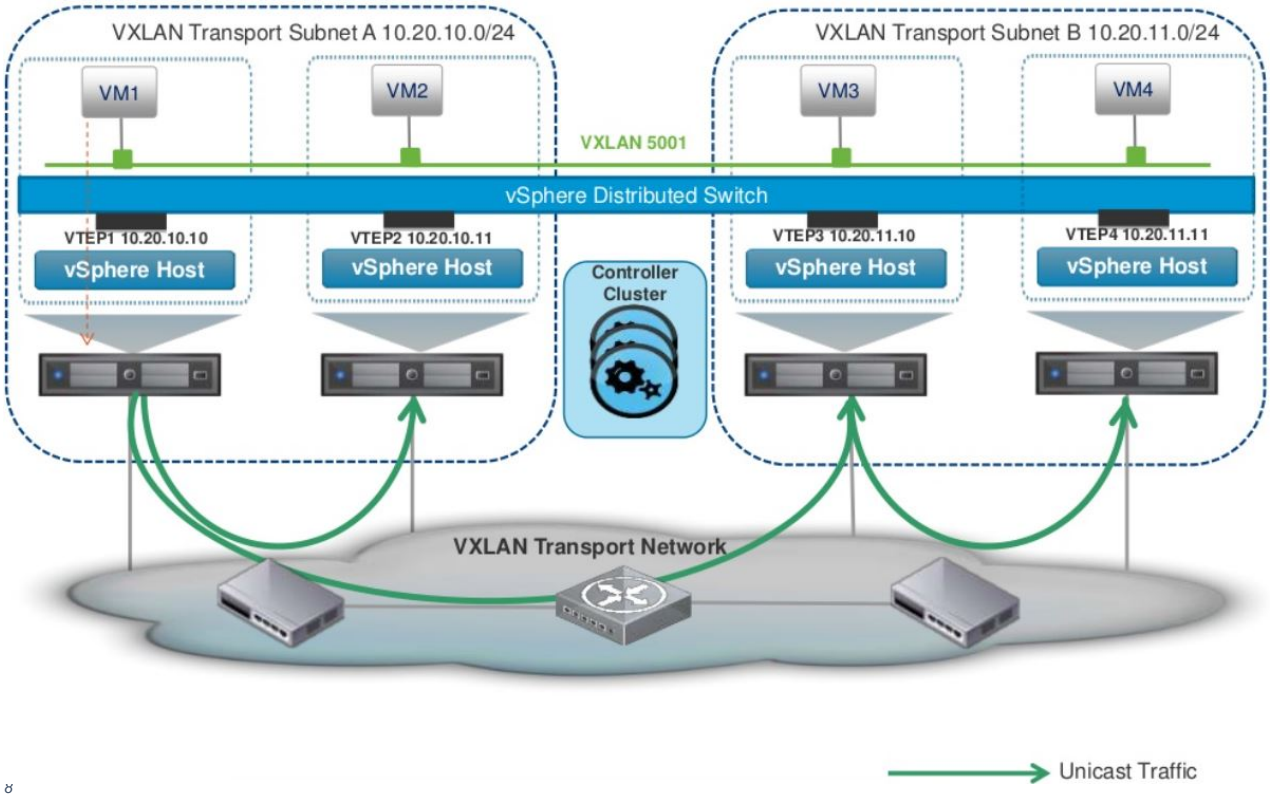
1.4.4 Les Switches logiques (Logical switches)

Il est basé sur le *VSphere Distributed Switches*(VDS) et constitue le *Data Plane*. Il fait l'abstraction de la couche physique et parmi ses avantages :

- Création d'une couche 2 flexible sur la couche physique IP sans ajouter du matériel ou modifier le réseau physique existant

- Communication est-ouest et nord-sud en maintenant une parfaite isolation entre plusieurs tenants.
- Les applications des VMS ne sont pas impactées. Elles voient le réseau virtuel comme un réseau physique
- Facilité d'ajout d'hyperviseurs dans le réseau logique.

Plusieurs fonctionnalités supportées : Port Mirroring, QoS, LACP, Network Health Check, NetFlow, sauvegarde et restauration des configurations, monitoring, management et troubleshooting du réseau logique.



[8]

Figure 7: Switch Logiqiue trafic unicast

1.4.5 La gestion de la sécurité du réseau logique

EDGE Firewall

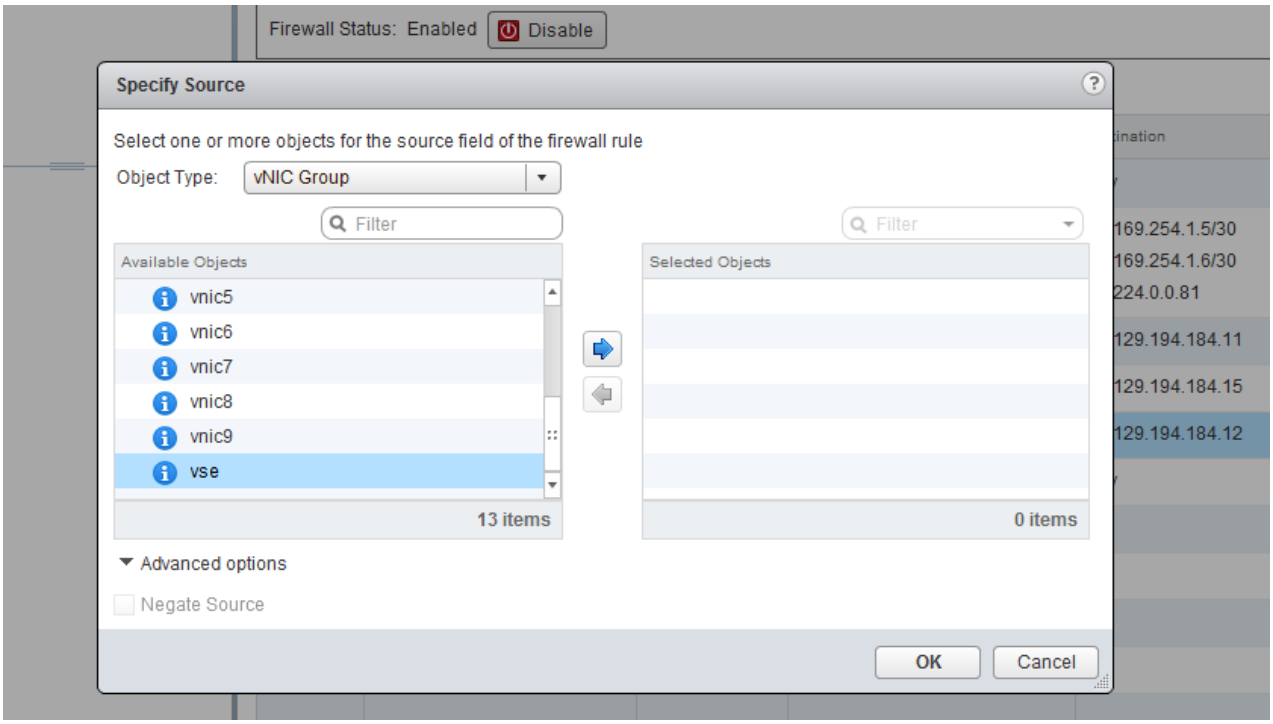
C'est le firewall qui gère le trafic Nord-Sud venant des clients vers les différentes VMS
Il permet de filtrer le flux en appliquant la politique de la liste blanche par des adresses IP statiques.

Le fonctionnement des règles

Ce FW est une VM conçue pour filtrer le trafic nord-sud passant par l'EDGE. Il gère le trafic des couches 3 et 4.
Il supporte les filtres qui se base sur des adresses IP et/ou port pour tous les types de protocoles (ICMP, http…)
Il peut être utilisé comme un FW internet protégeant le réseau logique du trafic venant de l'extérieur.
Tout paquet entrant et évalué avant l'application de la règle NAT.

[8] http://chansblog.com/tag/nsx-logical-switch/

Les trois règles dans la figure 8 sont générées automatiquement.
La règle, nommée firewall qui prend comme source vse, est une règle appliquée au trafic généré par l'EDGE.
Cette source peut être choisie en cliquant sur le plus dans la case source et choisir dans la liste proposée vNIC Group. Les objets de cette liste sont les dix interfaces de l'EDGE.
La lettre i veut dire interface



Hide Generated rules Show Pre rules

No.	Name	Type	Source	Destination
1	routing	Internal	any	any
2	firewall	Internal	vse	any
3	Default Rule	Default	any	any

Figure 8: Edge FW Generated Rules

Le Firewall distribué (DFW)

A la différence de l'EDGE FW, ce dispositif gère surtout le trafic Est-Ouest entre les VMS. Son plus grand avantage est sa capacité d'appliquer la règle au niveau du VNIC de la VM indépendamment du réseau où elle se trouve, ce qui donne la possibilité de la migrer en conservant ses règles FW.

Le fonctionnement des règles DFW

Les règles suivantes sont générées automatiquement :
Règle2 : concerne le protocole *Neighbor Discovery*, le protocole utilisé par IPV6 pour découvrir les autres hôtes.
Règle3 : concerne le trafic du client ou serveur DHCP
Le DFW est installé avec deux *default rules*, une pour la couche 2 et l'autre pour la couche 3.

A la différence du FW EDGE qui est une VM, DFW est installé dans le KERNEl de l'ESXI. Il permet d'inspecter tout le trafic sortant ou entrant dans une VM donnée.

2	Default Rule NDP	any	any	IPv6-ICMP Neighbor Advertise... IPv6-ICMP Neighbor Solicitation	Allow	Distributed Firewall
3	Default Rule DHCP	any	any	DHCP-Client DHCP-Server	Allow	Distributed Firewall
4	Default Rule	any	any	any	Block	Distributed Firewall

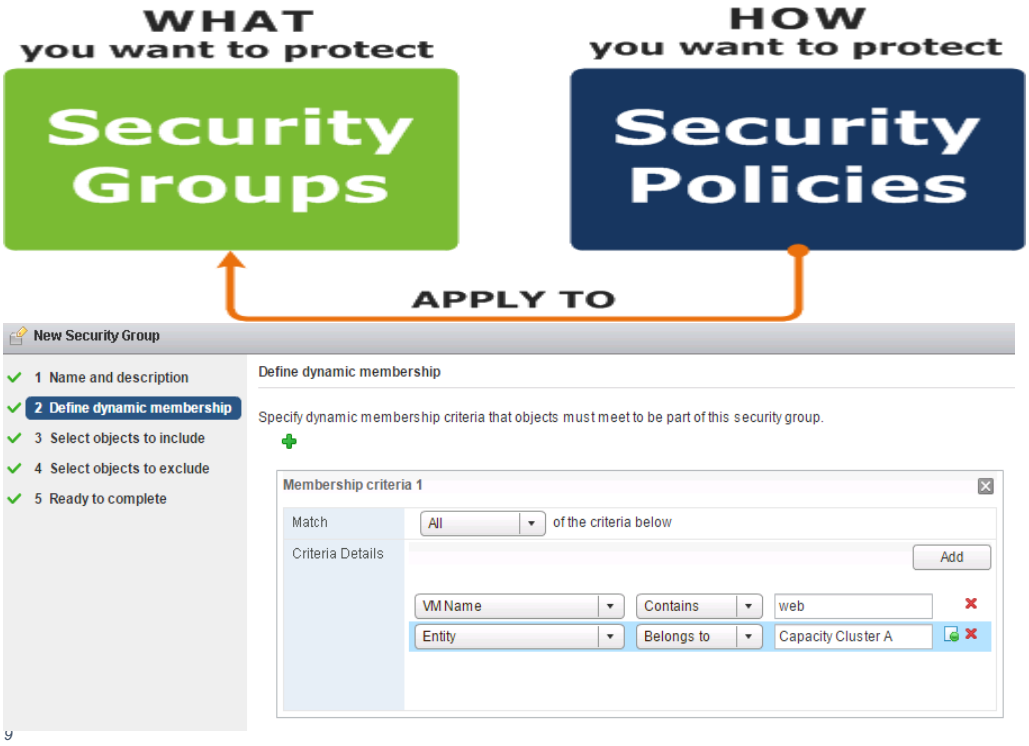
Figure 9: DFW rules

SpoofGuard

Grâce à VMware Tools installé dans les VMS, NSX Manager collecte toutes les adresses IP du réseau logique.
En créant des règles permettant de gérer les adresses IP des VMS, on peut prévenir le *fishing* de sorte que l'adresse IP d'une VM ne peut être autorisée que par l'administrateur.

Service Composer

Ce dispositif permet de créer des politiques de sécurité et/ou des groupes de sécurité sur les VMS se trouvant dans le réseau logique en appliquant les mêmes méthodes utilisées dans un réseau physique.



[9]

Figure 10: Service Composer

NSX offre d'autres services comme le VPN logique, le Load Balancer ou encore NSX extensibility.

[9] http://blogs.vmware.com/consulting/tag/nsx-service-composer

1.5 QUELQUES DEFINITIONS

1.5.1 Les Clusters

Comme dans la définition traditionnelle d'un cluster, il s'agit d'un groupe de machines, appelées nœuds, dont les ressources sont mutualisées et vues comme si nous avions une seule machine.
Outre les fonctions de haute disponibilité, performance ou aussi la répartition des charges, VMware NSX a besoin des clusters parce que c'est le processus par lequel l'instance NSX Manager :

- Installe des modules du noyaux NSX sur les hôtes membres de clusters VCSA
- Construit le control plane et le management plane

Les modules du noyau NSX conditionnées dans des fichiers VIB s'exécutent dans le noyau de l'hyperviseur et fournissent des services tels que le routage distribué et le firewall distribué.

Pour que le NSX puisse fonctionner, il est nécessaire d'installer tous ses composants au niveau des clusters et non pas au niveau des hôtes.
Il existe néanmoins un moyen d'utiliser les hôtes sans clustering. C'est de télécharger manuellement les fichiers VIB sur le site VMware et les inclure dans l'image Esxi.
A la différence des clusters HA[10] ou DRS[11], le cluster ici ne sert que pour déployer quelques composants de VMware NSX comme Controller Cluster ou encore les VXLANS.

1.5.2 Les fichiers VIB

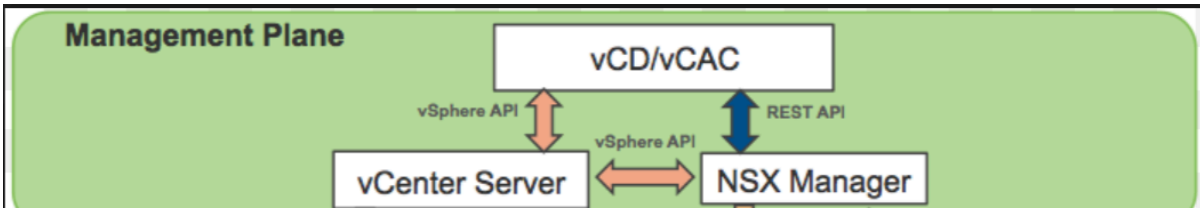
Les lettres VIB signifient *Vsphere Installation Bundle*. Ce fichier et similaire à un fichier zip. C'est une collection de fichiers qui servent à faciliter la distribution.
Un VIB est constitué de trois parties :

1- Une archive de fichiers.
2- Un fichier XML.
3- Un fichier de signature.

La première partie contient les fichiers qui composent les VIB *payload*. Ils sont installés dans l'image ESXI. Quand un VIB est supprimé, les fichiers seront supprimés de l'image aussi.
Le fichier XML décrit le contenu du VIB et les conditions requises pour son installation.
Le fichier de signature contient la signature électronique utilisée pour vérifier le niveau de confiance du VIB et son intégrité. Il contient aussi le nom du créateur ainsi que le nombre de tests et de vérifications qui ont été faites.

1.5.3 VCSA (VCenter Server Appliance)

C'est le composant central de Vsphere sorti avec la version 5. Cet outil permet de centraliser la gestion de l'ensemble des hôtes et des machines virtuelles.
Une seule Appliance peut gérer jusqu'à 100 hôtes et 3000 machines virtuelles.
Elle gère avec le NSX manager le plan de management.



[10] High Availability
[11] Dynamic Ressource Scheduler

Figure 11: Management Plane architecture

1.5.4 Le serveur SSO

Single Sign On ou authentification unique est la fonction qui permet aux utilisateurs de s'authentifier une seule fois pour toute la durée d'une session, indépendamment du nombre d'applications qui nécessitent une authentification. Ils peuvent alors accéder à leurs données en toute transparence, sans contrainte de ressaisir un nouveau couple nom d'utilisateur/mot de passe.

Il a été introduit dans VMware Vsphere avec la version VCenter 5.1. Une nouvelle fonctionnalité, qui ne sert pas seulement à s'authentifier, mais aussi c'est un moyen plus sécurisé pour accéder aux solutions Vsphere.
En effet une authentification par échange de jeton pourrait être configurée pour accéder aux composants Vsphere tels que VCenter server et VCenter Orchestrator.
SSO peut être configuré avec différents moyens d'authentification comme AD ou OpenLDAP.

Pour que Vsphere Web Client soit utilisé, SSO doit avoir le statut ***embeded*** lors de la configuration de VCSA. Et pour cela il faudrait être sûr que le serveur DNS est opérationnel et le serveur NTP est en mode *Running*.

1.5.5 Le Trafic Nord-Sud

C'est le flux de données qui circulent verticalement du client vers le serveur. Il constitue le 80% du Traffic d'une entreprise, contre le trafic circulant entre les serveurs dit Est-Ouest.

1.5.6 Architecture Multi-tenants

L'architecture multi-tenants ou multi-locataires est une architecture où une seule instance peut gérer plusieurs locataires.
Pour un prestataire de service, c'est la solution la plus adaptée parce qu'il suffit de déployer le logiciel une seule fois et de créer par la suite autant d'instances que de clients.
L'administration d'une telle architecture est relativement simple. La complexité reste donc dans le maintien d'une isolation entre les tenants. Cette isolation se fait au niveau logiciel.
[12]

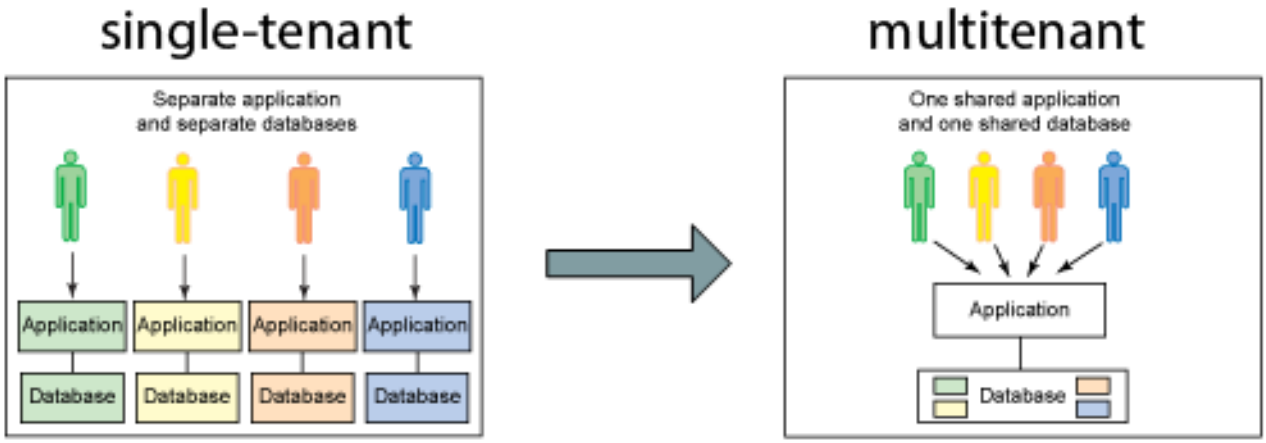


Figure 12: Architecture multi-tenants

[12] http://www.supinfo.com/articles/single/1069-qu-est-ce-que-architecture-multi-tenant

1.5.7 Transport Zone

Pour configurer les switches et les routeurs logiques dans NSX, il est nécessaire de définir d'abord une zone appelée Transport Zone (TZ).
Cette zone contrôle quel cluster, et par conséquent quels hôtes, le switch peut atteindre.
Une TZ peut couvrir plusieurs clusters.
Dans ce travail, j'ai utilisé une seule TZ. Mais dans une architecture multi-tenants, il est préférable d'utiliser plusieurs TZ pour offrir un niveau supplémentaire d'isolation.

1.5.8 Proxy ARP

C'est une fonctionnalité que nous pouvons activer sur les interfaces de l'EDGE dans le cas où nous souhaitons autoriser la passerelle ESG à répondre aux demandes ARP destinées aux autres machines. C'est utile notamment lorsque nous avons deux sous-réseaux qui se chevauche dans des WAN différents.
[13]

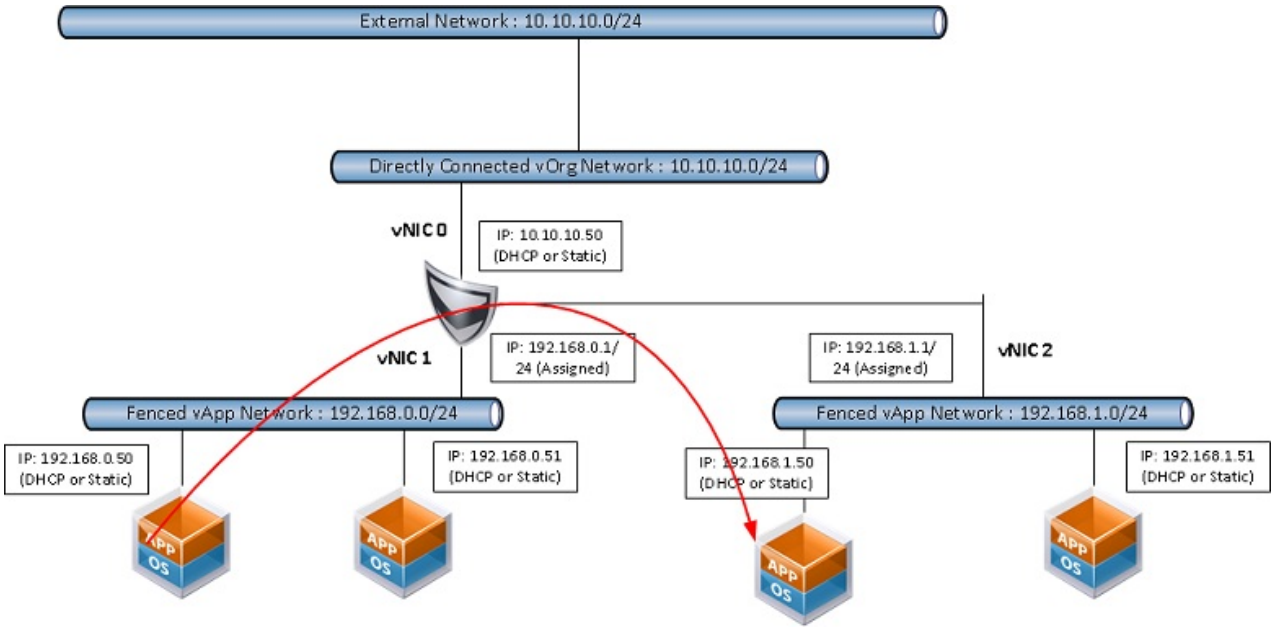


Figure 13: Proxy ARP

1.5.9 Virtual Network Identifier(VNI)

C'est un identificateur que les VXLAN utilise pour numéroter les clients permettant de les isoler.
Le premier numéro est le 5000, puisque les numéros de 0-4999 sont réservés aux VLANS.

1.5.10 SDDC

C'est un modèle d'architecture réseau qui ajoute un niveau d'abstraction aux fonctionnalités des équipements réseau afin de pouvoir les gérer de façon globale. La partie décisionnelle des équipements est séparée de leur partie opérationnelle et déportée vers un unique point de contrôle qui dirige l'ensemble de façon cohérente. Ce découplage permet de déployer le plan de contrôle sur des plateformes dont les capacités sont plus grandes que celles des commutateurs réseaux

[13] http://stretch-cloud.info/2013/01/proxy-arp-icmp-redirect-in-vshield-edge-nic-explained/

classiques. Enfin, cette abstraction à travers une API réseau standard permet un développement de services réseaux à forte valeur ajoutée

Parmi les avantages de ce modèle, on peut citer

- La collecte des données en temps réel
- La capacité de couvrir plusieurs sources de données en même temps

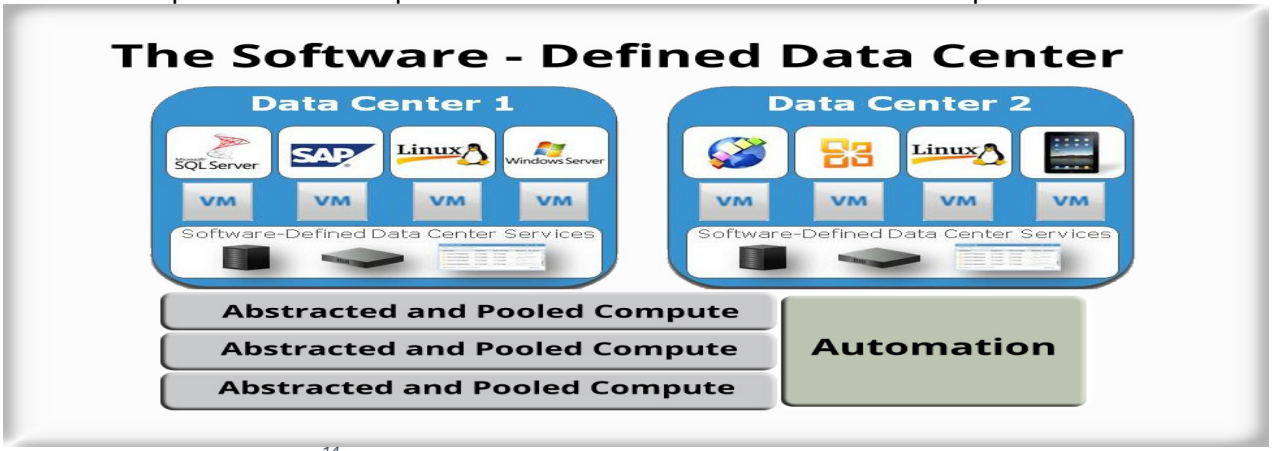


Figure 14:SDDC Architecture [14]

1.5.11 Architecture évolutive

C'est une architecture évolutive (Scalability architecture) en configurant pour chaque tenant son propre ESG avec chacun un sous-réseau public différent.

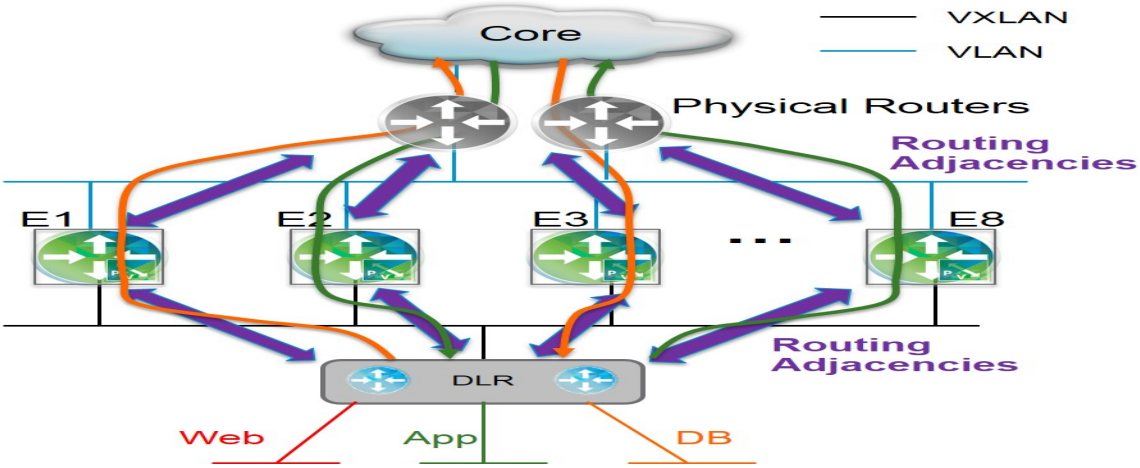
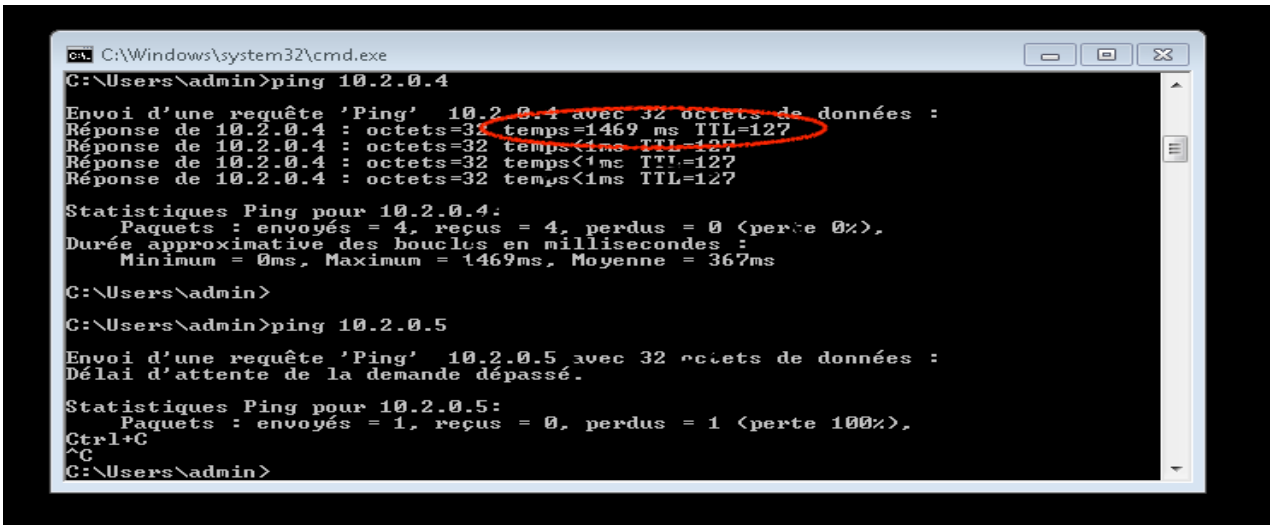


Figure 15: ARCHITECTURE EVOLUTIVE

[14] http://www.costacloud.com/cloud-software-defined-data-center.html

1.6 PERFORMANCE



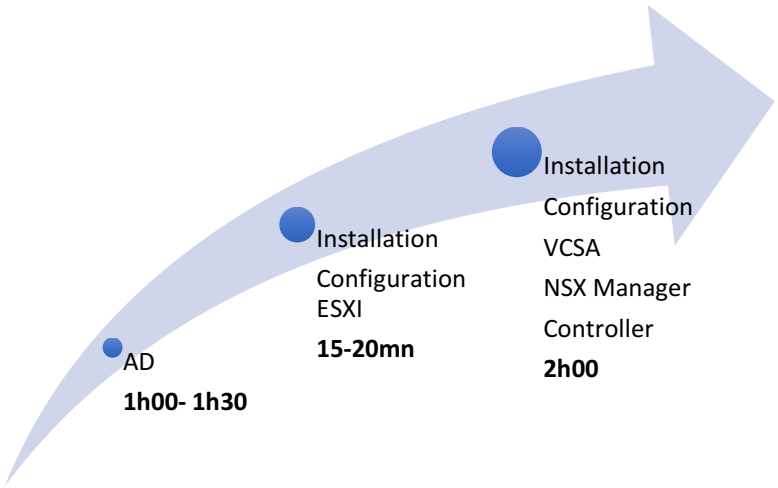
Pour un simple PING de la VM console à VM4 il faudrait 1.5 seconde à peu près pour la première requête. Cela est dû au temps utilisé pour l'échange des informations entre le plan de contrôle qui trouve le chemin de la VM4 (*Control Plane*) et le plan de données (*Data Plane*)

CHAPITRE2 :

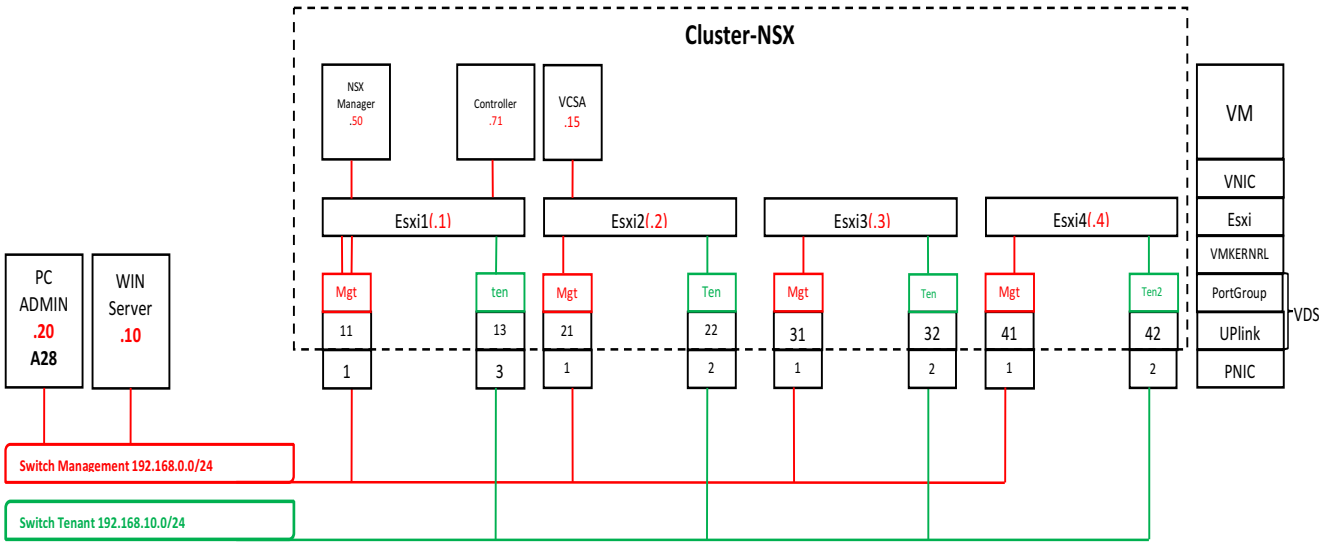
ÉTAPES DE L'INSTALLATION

Ce chapitre consiste à expliquer les différentes étapes de l'installation
Les étapes suivantes doivent être impérativement respectées pour que l'installation et la configuration de VMware NSX se déroulent correctement et sans problème.

1. Installation de Windows Server 2012 R2.
2. Configuration de AD, DNS, Serveur NTP et DHCP.
3. Installation ESXI 5.5
4. Configuration des adresses IP pour les ESXI selon le plan d'adressage adopté
5. Installation de VCenter Client sur le PC d'administration.
6. Installation et configuration de VCSA.
7. Installation des plugins sur Mozilla et ouverture du web client
8. Configuration du cluster et ajout des hôtes.
9. Configuration du VDS
10. Migration des PNICS et des VMKERNEL sur le VDS et suppression des switches standards
11. Installation et configuration de VCenter NSX.
12. Déploiement de NSX controller.



2.1 SCHEMA

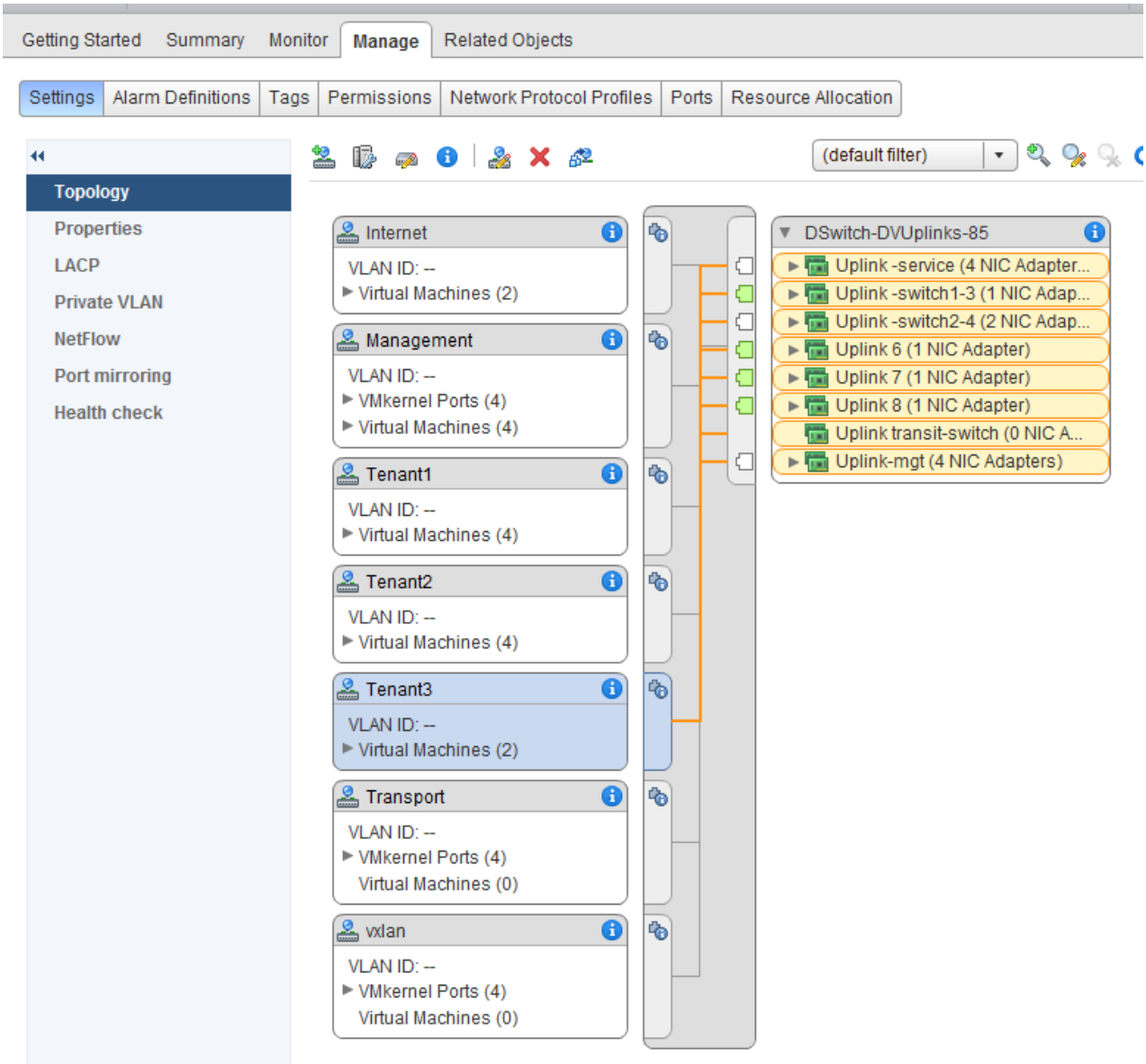


4 ESXIS :
ESX1 et ESXI2 pour les VMS de l'administration
VMS : NSX Manager - Controller - VCSA.
ESXI3 et ESXI4 pour les VMS des tenants A et B

PC Admin :
Pour la gestion du réseau virtuel via l'interface Vsphere web client.

Win Server :
Pour le DNS et AD.

2.2 LA CONFIGURATION DU DISTRIBUTED VIRTUAL SWITCH(VDS)

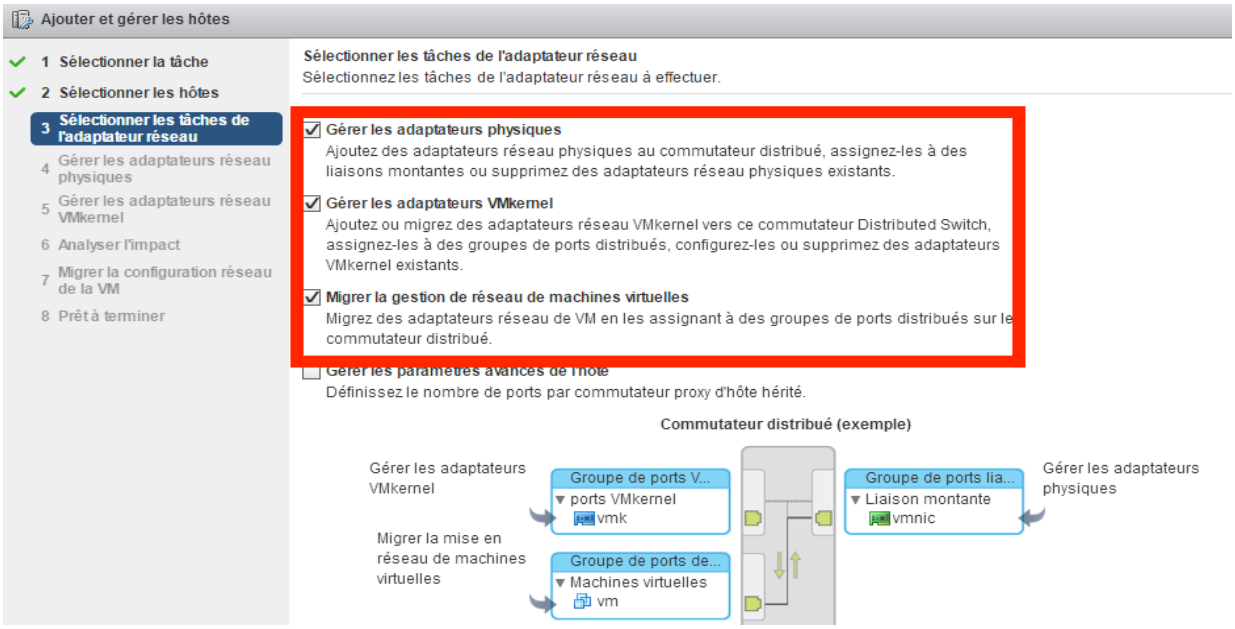


UPLINKS Portgroup : le nombre est défini par l'utilisateur au moment de la création du VDS (8 dans ce cas). Un *UPLINK* sert à configurer les connexions physiques des hôtes.

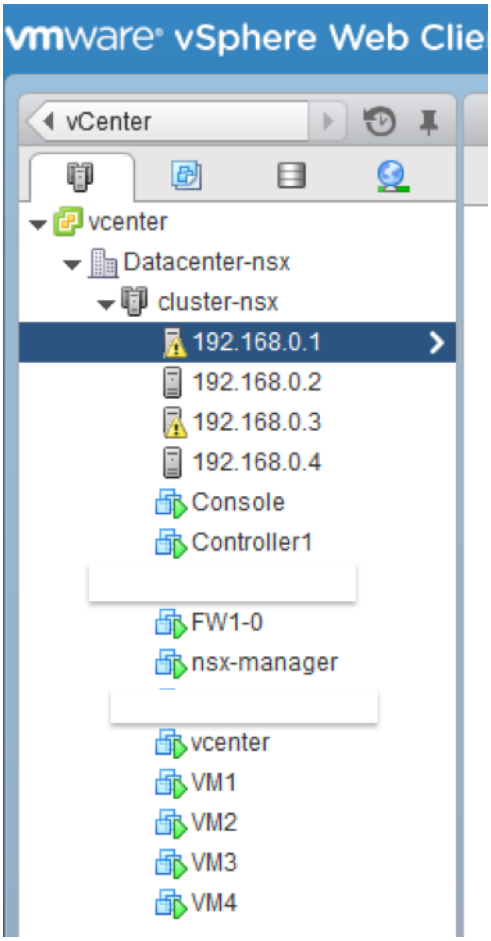
Management PortGroup : est l'équivalent de *management network* dans un switch VMware standard.
C'est le port par lequel passe le trafic du réseau management (rouge dans le schéma) des VMS.

TenatX Portgroup : ces *portgroups* ont été ajoutés par NSX au moment de la création des switches logiques. J'ai changé leurs intitulés pour plus de clarté.

Après la création du VDS, ajouter les hôtes et migrer les adaptateurs physiques (PNIC), les VMKERNELS et les VMS sur celui-ci



2.3 VUE GENERALE



Cette vue est prise sur VSphere Web Client
Acceuil – hôtes et clusters
VCenter et le VCSA qui permet de gérer tous les hôtes et VMS se trouvant dans cluster-nsx

La version VMware NSX 6.2 ne supporte pas la version 5.5 de VMware ESXI. Malgré que VMware confirme sa compatibilité, plusieurs utilisateurs ont remarqué les mêmes bugs dans la version 5.5 que la version ESXI 6 ne produit pas.

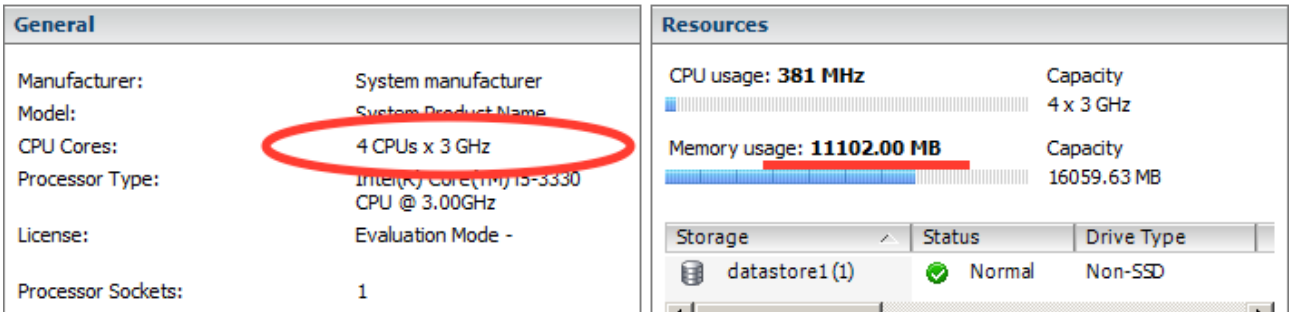
Pourquoi un cluster ?
Le cluster est un prérequis exigé par NSX pour déployer certaines de ses fonctionnalités comme les VXLANS ou aussi le Controller.
Le cluster permet aussi d'installer automatiquement les VIB, les VXLANS et les VTEP sur les hôtes rajoutés ultérieurement.

2.3.1 La configuration logicielle

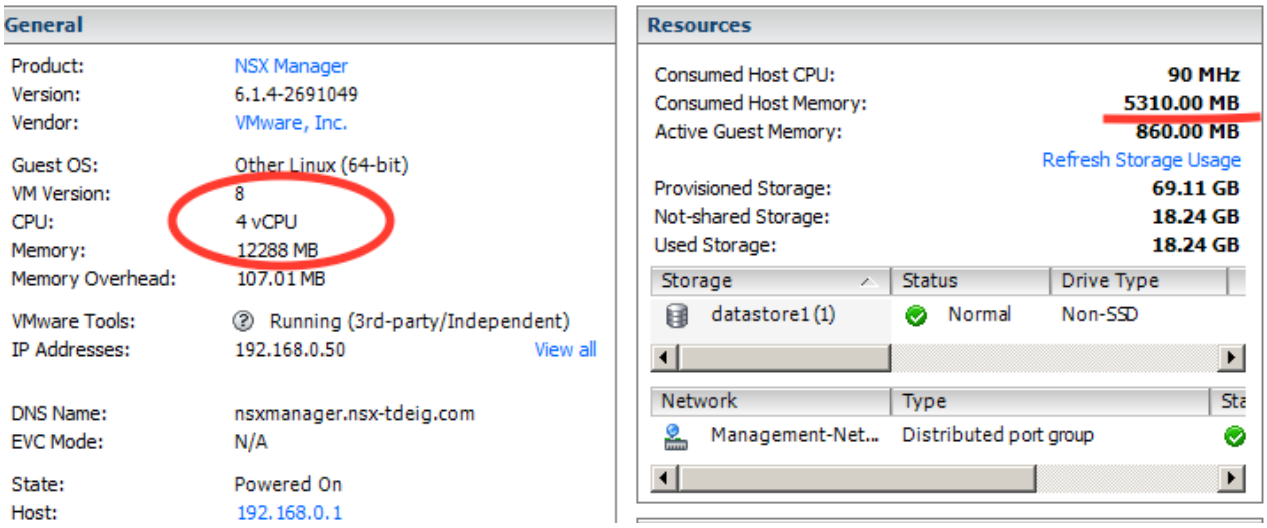
Les logiciels utilisés dans ce travail sont :

- VMware ESXI 5.5.iso
- VMware NSX 6.1.4.ova
- Pour les VMS : Windows7.iso
- Windows Server 2012 R2 pour AD et DNS

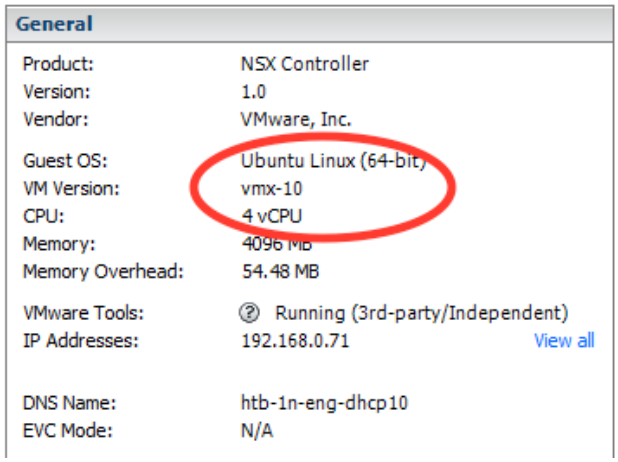
2.3.2 La configuration de ESXI1 :



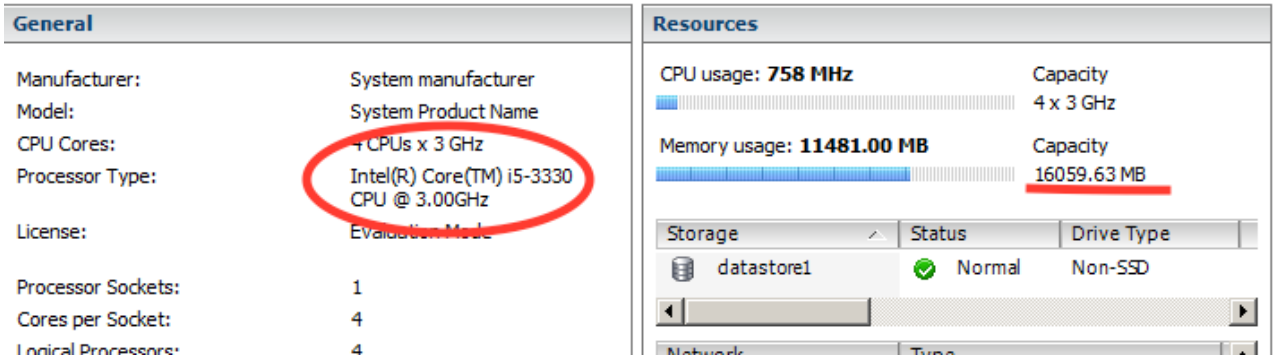
La configuration de NSX Manager



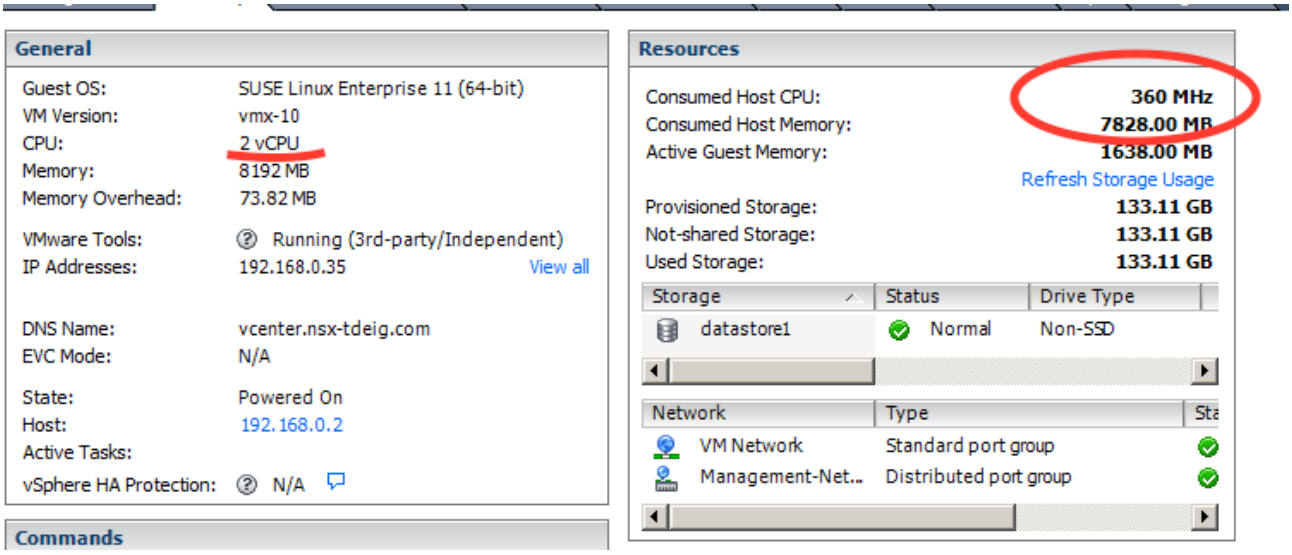
La configuration du Controller



2.3.3 La configuration de ESXI2



La configuration de VCSA



2.4 INSTALLATION

2.4.1 Installation et configuration de Windows Server 2012 R2 :30min

Annexe 2
Après l'installation de Windows Server 2012 R2

1- Changer le nom et l'adresse IP du PC
2- Installer et configurer AD, DNS et DHCP
FQDN = nsx-tdeig.com

2.4.2 Installation et configuration de VMware ESXI [15] :15-20min

L'installation de VMware ESXI5.5 est simple. La version 5 permet de configurer le clavier en Suisse français
Après l'installation, rebooter la machine et appuyer sur F2 pour configurer l'adresse IP et le DNS.

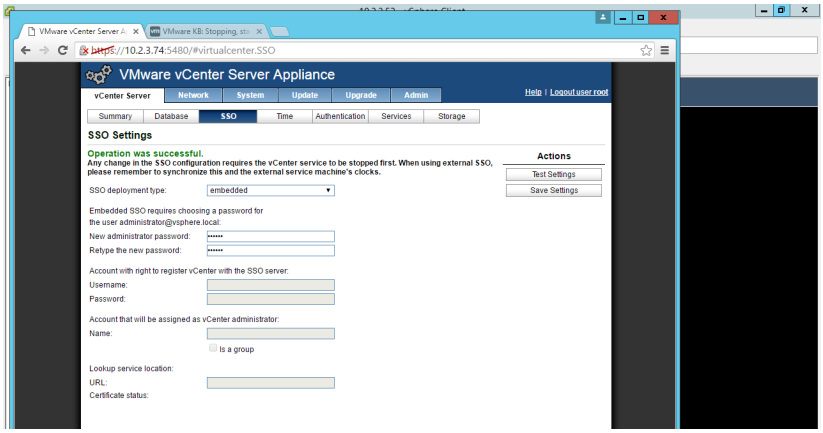
A ce stade. Il faudrait s'assurer que tous les ESXI, le PC Admin et le Windows Server communiquent entre eux, et que le serveur NTP (192.168.0.10) est en mode *Running.*

2.4.3 Installation et configuration de VCSA[16]

Avant de l'installer se connecter à l'hôte ESXI2
en tapant son adresse dans la barre de navigation : https://192.168.0.35 ,et en installant le VCenter client .

Remarques
Avant de configurer le SSO, stopper VXPD par la commande suivante
`~ # service vmware-vpxd stop`
Ne pas oublier de le redémarrer après
`~ # service vmware-vpxd start`

Après la configuration du VCSA, se connecter au VCenter web client par les accès affectés à cette VM.[17]



[15] http://journaldunadminlinux.fr/tutoriel-installer-un-hyperviseur-esxi-5-5/
[16] http://vpourchet.com/2013/11/24/vmware-vsphere-5-5-configuration-de-lappliance-virtuelle-vcenter/
[17] http://www.it-connect.fr/installer-et-configurer-vmware-vsphere-web-client%EF%BB%BF/

2.4.4 Configuration du Cluster

La configuration des clusters se fait dans l'interface Vsphere Web Client.
C'est une opération très simple qui se fait en quelques clics.

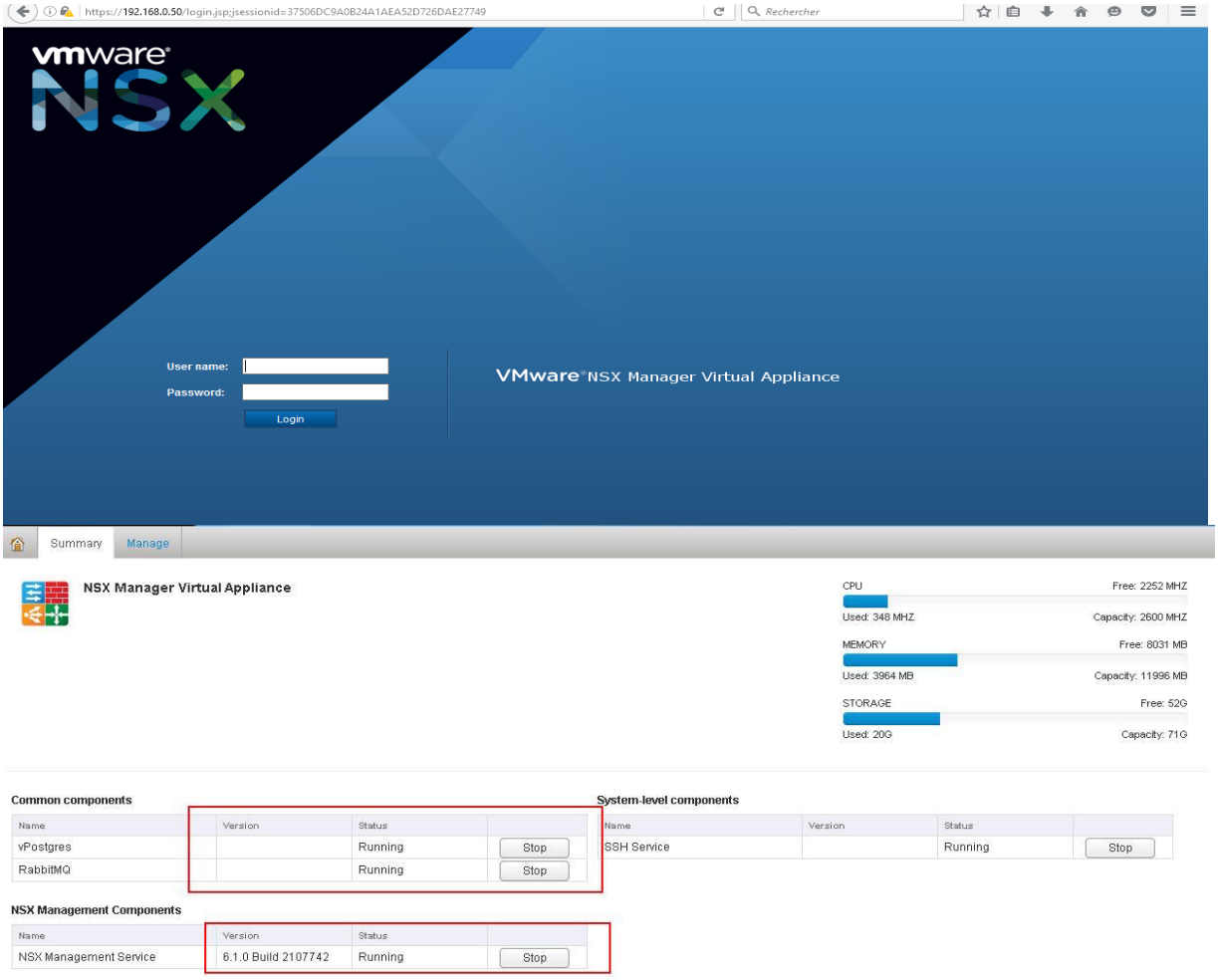
2.4.5 Configuration du VDS

Virtual Distributed Switch sert à simplifier la gestion du réseau de VMS en centralisant la configuration des ports et en donnant des noms aux groupes de ports (PortGroup)
C'est un prérequis pour NSX parce que les VXLANS et les switches logiques se déploient au niveau du VDS en créant des nouveaux *PortGroups*.
Après la création du VDS, il faut :

- Ajouter un autre PortGroup appelé services
- Ajouter les hôtes
- Migrer les PNICS et les VMKERNELS

2.4.6 Installation et configuration de VMware NSX[18]

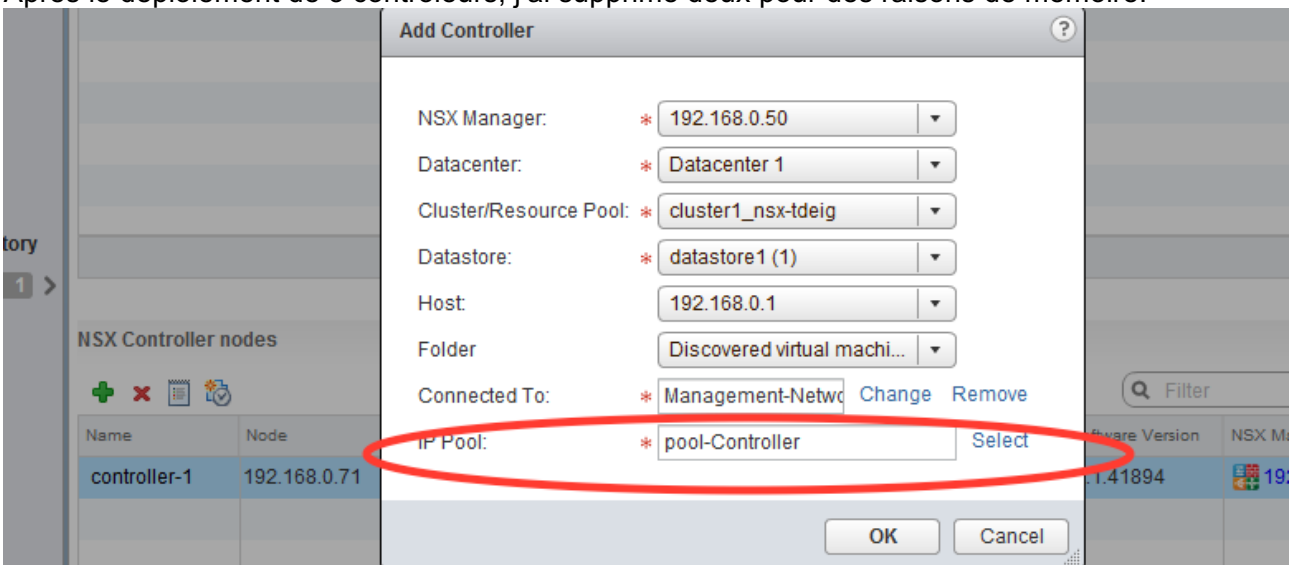
Après le déploiement de la VM NSX Manager (**Annexe4),** il faut ouvrir la plateforme qui gère la configuration du NSX Manager en tapant https://192.168.0.50 dans le navigateur.
Dans la page d'accueil, s'assurer que tous les services sont *en running*.

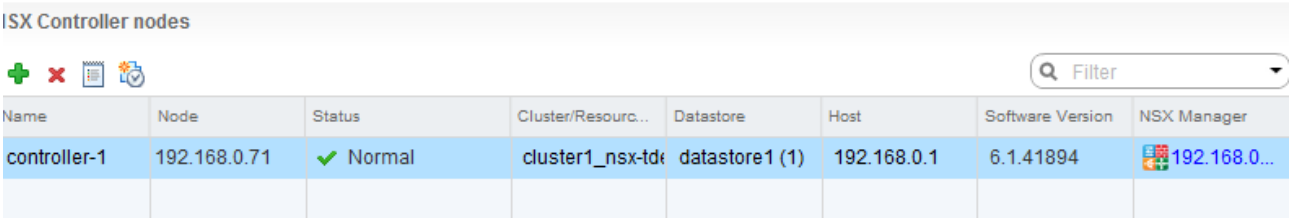


[18] http://dailyhypervisor.com/vmware-nsx-for-vsphere-6-1-step-by-step-installation/

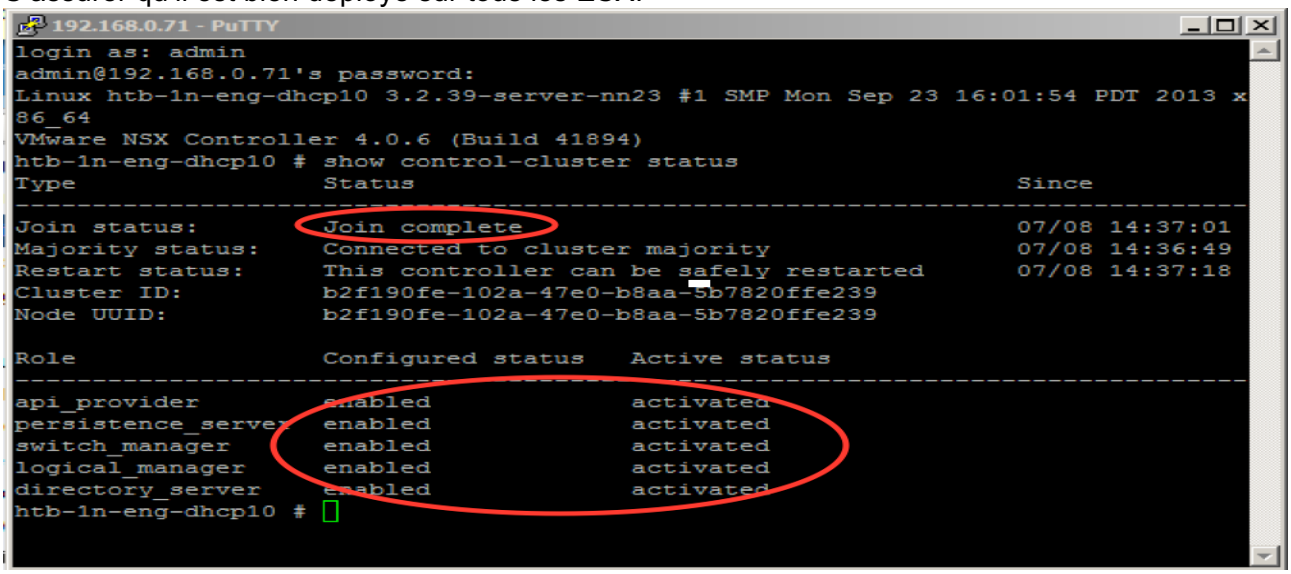
2.4.7 Déploiement du controller cluster[19]

Pour un réseau simple avec peu de ressources et une complexité simple, VMware recommande de déployer 3 Contrôleurs. Un pour le rôle de master, le 2ème pour le rôle de slave et le dernier pour assurer le fonctionnement du réseau dans le cas où un des deux premiers se déconnectent.
J'ai déployé un seul contrôleur pour économiser les ressources RAM
J'ai prévu un pool d'adresses 192.186.0.71-73 par exemple pour le déploiement.
Après le déploiement de 3 contrôleurs, j'ai supprimé deux pour des raisons de mémoire.





S'assurer qu'il est bien déployé sur tous les ESXI



[19] http://wahlnetwork.com/2014/06/02/working-nsx-deploying-nsx-controllers-via-gui-api/

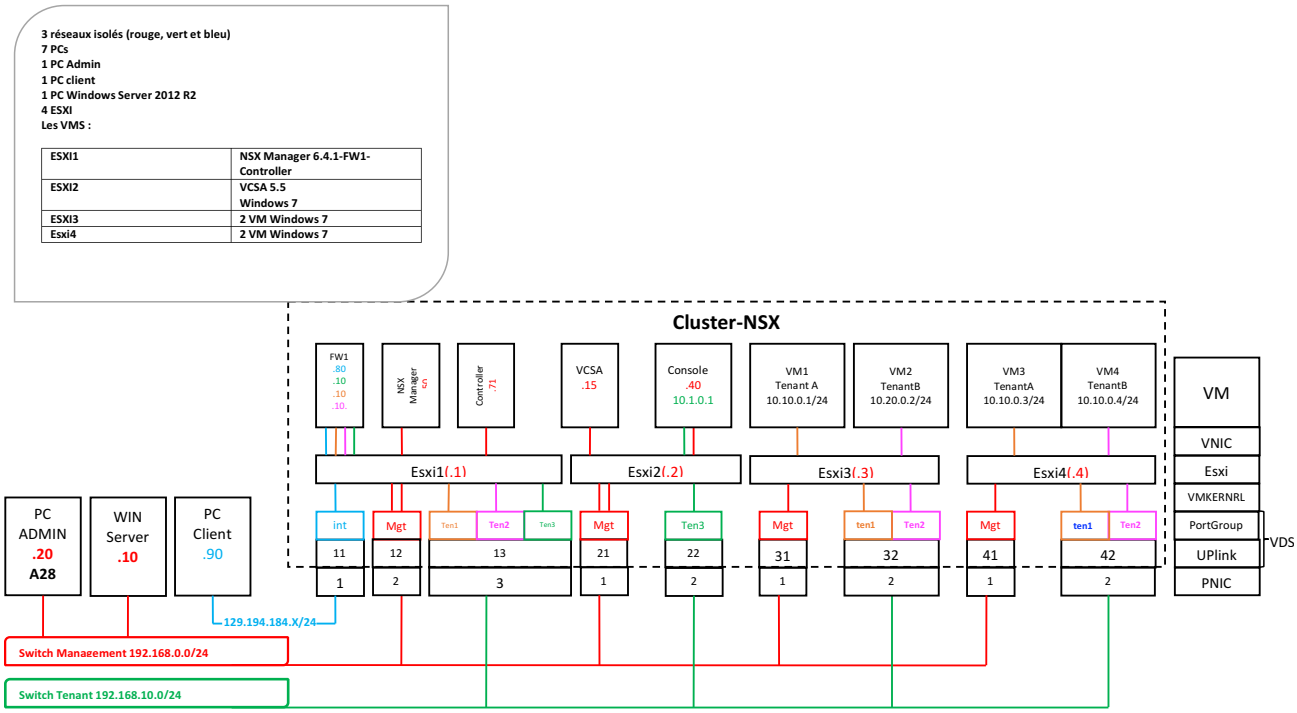
CHAPITRE 3 :

Isolation des Tenants

L'objectif de ce chapitre est de tester l'isolation des tenants. Pour atteindre cet objectif, une architecture multi-tenants sera configurée.
Pour cela, les étapes suivantes vont être réalisées :

1. Configuration des VXLANS
2. Configuration des switches logiques pour 4 VMS
3. Déploiement du DLR
4. Déploiement d'une Edge Gateway Services (EGS)
5. Définition des règles de NAT
6. Définition des règles FW pour isoler les tenants.
7. Tester le FW de l'Edge et le FW distribué et comparer entre eux
8. Comparer entre le FW de NSX et le FW physique

3.1 MISE EN PLACE DE L'ARCHITECTURE MULTI-TENANTS



Le tenant 1 : VM1 et VM3 sont liées par un switch logique et le VNI du leur VXLAN est le 5001
Le tenant 2 : VM2 et VM4 sont liées par un autre switch logique et le VNI de leur VXLAN est le 5002
La VM console est liée au switch logique qui a un VXLAN de VNI 5003
Tous les switches logiques sont connectés à l'EDGE

Comme je n'ai pas un routeur, j'ai utilisé une troisième PNIC sur la machine physique de ESXI1 pour lier entre l'EDGE et le PC client : le réseau bleu.

3.1.1 Démarche à suivre

J'ai élaboré une architecture qui me permet d'avoir :

- Deux tenants. Chaque tenant est identifié par un VNI différent.
- Accéder depuis le réseau physique à tous les tenants.
- Accéder depuis le PC client aux VMS via des adresses publiques.

3.1.2 Problématique

Deux problématiques se posent dans le schéma ci-dessus :

- Le tenant 1 peut accéder au tenant 2 et vice-versa via le l'EDGE.
- Les tenants 1 et 2 accèdent à la VM console

Mon but est d'isoler les tenants par une règle FW qui peut être valable dans une architecture évolutive. La règle doit être valable pour tous les tenants quel que soit leur nombre.
La VM console doit être isolée de sorte que les VMS des tenants ne peuvent pas accéder à elle.

Ainsi donc, quel scénario choisir pour les deux isolations ?

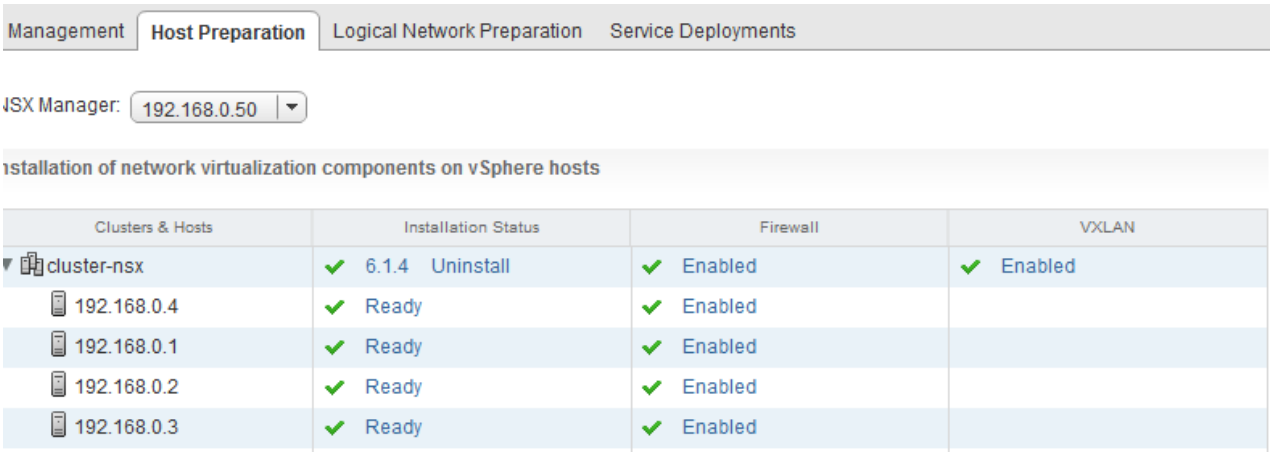
- Isoler les tenants par des règles FW
- Accéder depuis la VM console à toutes les autres VMS
- Accéder depuis le PC Admin à la VM console via RDP
- Bloquer l'accès des VMS à la VM console

3.1.3 Etapes de l'installation

1. Déploiement des VMS : **Annexe 3**
2. Configuration des VXLANS
3. Configuration des switches logiques
4. Déploiement du Routeur logique (DLR)
5. Déploiement de l'EDGE
6. Choisir le dispositif le plus adapté pour assurer une isolation des tenants
7. Se connecter à la VM console depuis le PC Admin via RDP
8. Bloquer l'accès à cette VM depuis les VMS des tenants

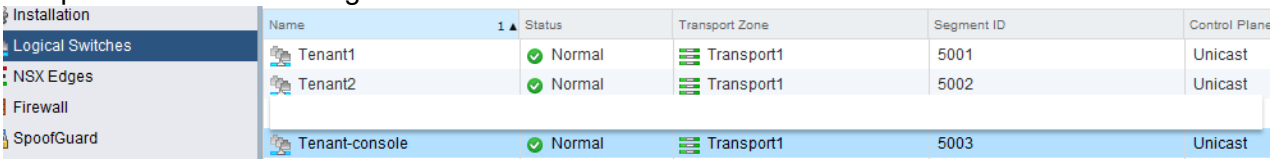
3.1.4 Installation

Configuration des VXLANS [20]



3.1.5 Configuration des switches logiques (LS)[21]

J'ai choisi de lier VM1, VM3 à LS1 et VM2, VM4 à LS2. Cela permet d'avoir un VNI différent pour chaque trafic et faciliter la gestion du flux.



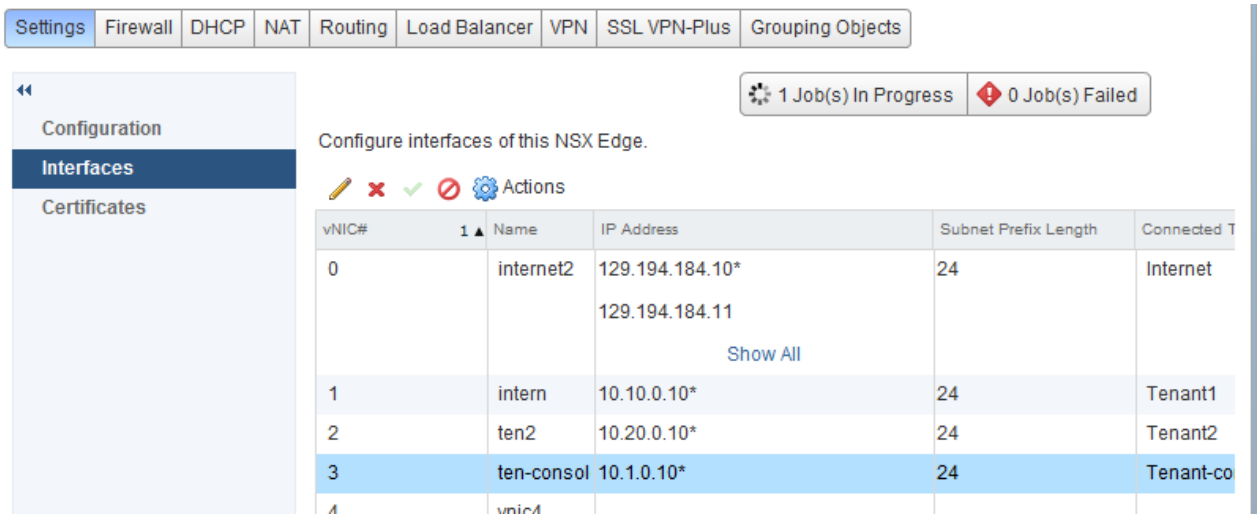
[20] https://pubs.vmware.com/NSX-62/index.jsp?topic=%2Fcom.vmware.nsx-cross-vcenter-install.doc%2FGUID-49BAECC2-B800-4670-AD8C-A5292ED6BC19.html
[21] https://pubs.vmware.com/NSX-6/index.jsp?topic=%2Fcom.vmware.nsx.admin.doc%2FGUID-DF57C441-CE9A-4138-9639-1658DBE65D48.html

3.2 CHOIX DE ESG

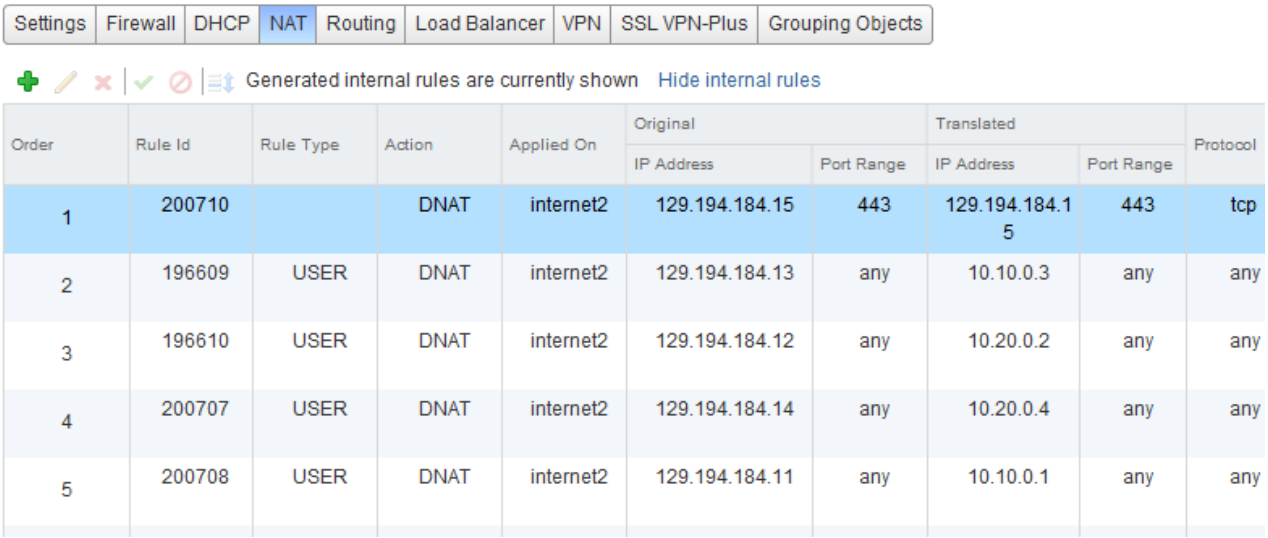
En étudiant les schémas proposés par VMware, j'ai compris que l'ESG n'a pour fonction que de faire le lien entre le réseau logique et le monde externe, et que dans une architecture multi-tenants, il est préférable de déployer le DLR aussi.
Le DLR fait le lien entre les tenants et l'ESG, et rend le trafic plus fluide.
En testant les deux configurations, je me suis rendu compte que l'ESG peut jouer les deux rôles dans un schéma simple à quelques tenants.
Le DLR est utile dans le cas d'une architecture complexe à plusieurs *transport zones*.

3.2.1 L'installation du ESG[22]

Sa configuration est très simple : 4 interfaces sont configurées.
Trois interfaces, de type interne, liées au switches logiques des tenants.
Et la quatrième interface, de type UPLINK, liée au PortGroup internet.



Double-clic sur l'EDGE, dans l'onglet NAT configurer le DNAT comme ci-dessous



Order	Rule Id	Rule Type	Action	Applied On	Original		Translated		Protocol
					IP Address	Port Range	IP Address	Port Range	
1	200710		DNAT	internet2	129.194.184.15	443	129.194.184.15	443	tcp
2	196609	USER	DNAT	internet2	129.194.184.13	any	10.10.0.3	any	any
3	196610	USER	DNAT	internet2	129.194.184.12	any	10.20.0.2	any	any
4	200707	USER	DNAT	internet2	129.194.184.14	any	10.20.0.4	any	any
5	200708	USER	DNAT	internet2	129.194.184.11	any	10.10.0.1	any	any

[22] https://pubs.vmware.com/NSX-6/index.jsp?topic=%2Fcom.vmware.nsx.install.doc%2FGUID-6FB89057-CD13-48AF-82F2-550B89F89FC5.html

3.2.2 Test de connectivité

Avec un test de Ping entre le PC client et l'adresse de translation 129.194.184.12. L'adresse publique de la VM2

```
Pinging 129.194.184.12 with 32 bytes of data:
Reply from 129.194.184.12: bytes=32 time<1ms TTL=127
Reply from 129.194.184.12: bytes=32 time<1ms TTL=127
Reply from 129.194.184.12: bytes=32 time<1ms TTL=127
Reply from 129.194.184.12: bytes=32 time<1ms TTL=127

Ping statistics for 129.194.184.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\albert>ping 129.194.184.15
```

3.3 QUELLE POLITIQUE DE SECURITE CHOISIR ?

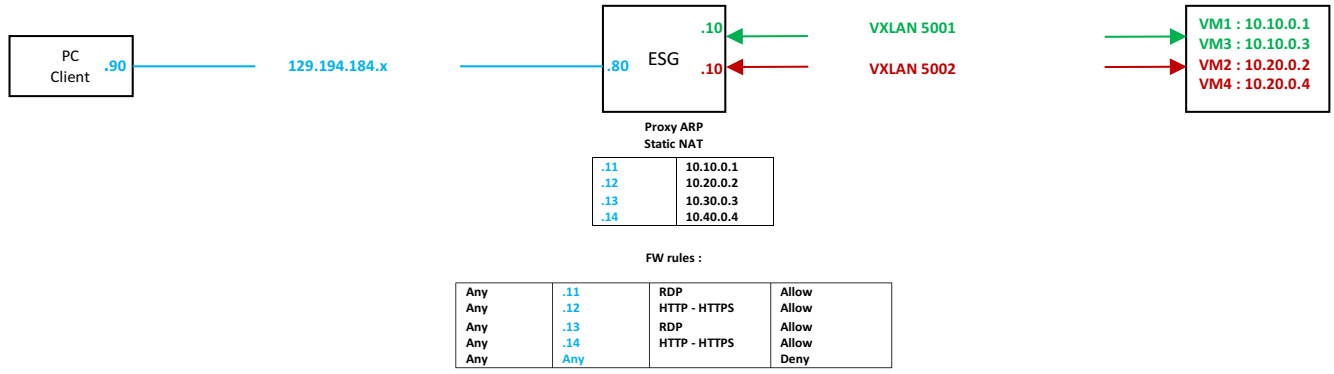
Comme, nous l'avons vu dans le chapitre1, NSX a plusieurs dispositifs qui permettent de filtrer le trafic et le gérer comme le DFW, le FW EDGE, Service Composer ou encore le Guardspoof.

3.3.1 Profil de mon architecture

Pour une question de temps, et pour être dans un contexte d'un réseau de test et non pas de production, l'architecture que j'ai adoptée est une architecture simple avec 4 VMS qui ont le même profil applicatif (Windows 7), un seul ESG qui fait la connexion entre le réseau logique et le réseau physique et qui joue aussi le rôle du DLR en routant le trafic est-ouest.

Ainsi donc, j'ai choisi de gérer le trafic venant du PC client en appliquant des règles FW EDGE et Isoler la VM console, en appliquant des règles DFW.

Schéma 1



Les tenants 1 et 2 appartiennent à des VNI différents pour assurer une couche supplémentaire d'isolation entre les tenants.

Le client peut accéder aux VMS grâce aux règles DNAT (NAT de destination)
Les règles FW permettent aux VMS de ne répondre qu'à une seule adresse publique, l'adresse qui a été définie dans les règles du NAT.

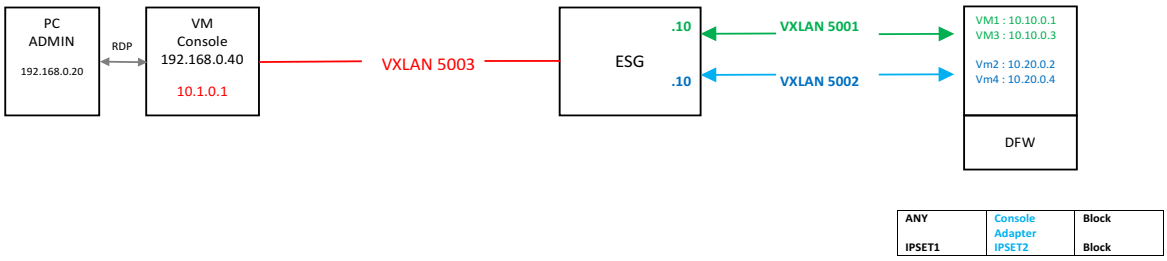
es Hide Pre rules

Search

	Type	Source	Destination	Service	Action
	Internal	vse	any	any	Accept
	User	any	129.194.184.11	RDP	Accept
	User	any	129.194.184.13	RDP	Accept
	User	any	129.194.184.12	HTTP HTTPS	Accept
	User	any	129.194.184.14	HTTP HTTPS	Accept
	Default	any	any	any	Deny

Figure 16:Règles FW

Schéma 2



Le PC Admin communique avec la VM Console via RDP
La règle DFW permet de bloquer le flux des autres VMS en direction de la VM console

3.3.2 Les règles DFW

J'ai utilisé une règle qui prend comme source (any), et comme destination le 2ème VNIC de la VM console, ce qui m'a permis de bloquer le trafic venant des autres VMS vers la console tout en maintenant la connexion entre celle-ci et le PC Admin.

Après le test des règles DFW à plusieurs niveaux dont les switches logiques et le VNIC des VMS, j'ai trouvé que la meilleure façon d'avoir une règle simple et générique et de la définir au niveau de l'IPSET.
L'IPSET permet de définir une plage d'adresses IP ou un sous-réseau, qui est dans ce cas le sous-réseau de chaque tenant.

Figure 17: Règles DFW de la console et tenants

La migration de la VM console vers un autre hôte n'affecte pas les règles DFW déjà définies.

3.4 DEROULEMENT DU TRAVAIL

3.4.1 Isolation des tenants :

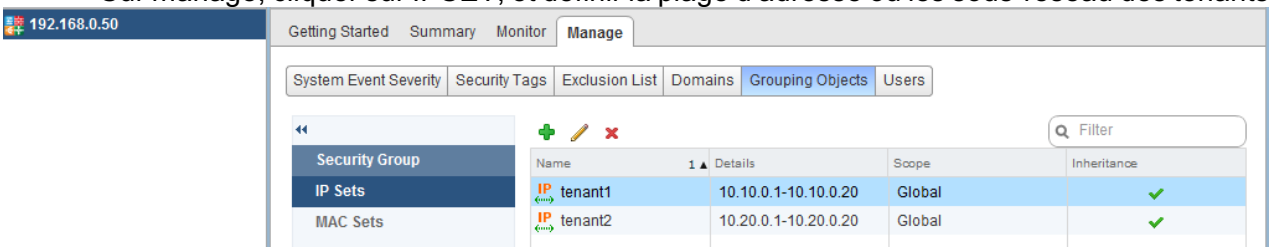
Le but était de trouver une méthode qui me permet d'isoler les tenants d'une manière générique sans devoir à chaque fois qu'un tenant ou une VM sont ajoutés, de configurer une nouvelle règle.

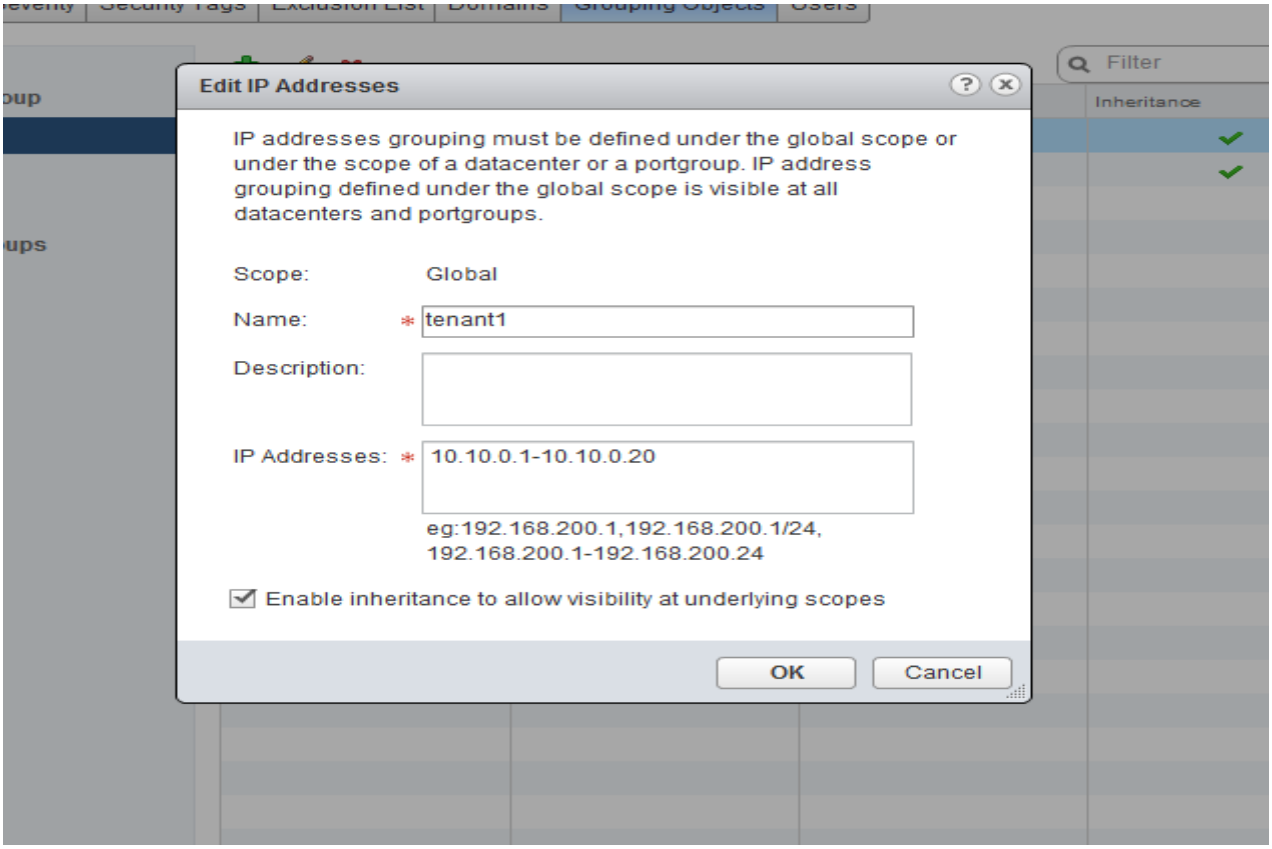
Deux méthodes sont à adopter, la première au niveau des critères des règles DFW, la seconde méthode se fait au niveau de l'architecture, celle d'avoir un ESG dédié pour chaque tenant avec une plage d'adresses publiques différentes.

Cette dernière méthode, je n'ai pas pu la tester, par manque de temps.

Configuration

- Cliquer sur le NSX Manager dans l'onglet Network&Security
- Sur manage, cliquer sur IPSET, et définir la plage d'adresse ou les sous-réseau des tenants





- Revenir à l'onglet DFW
- Choisir any dans source et l'IPSET dans destination pour bloquer le trafic entre les tenants

3.4.2 Isolation de la VM console

Pour isoler la VM console des autres tenants, sans pour autant bloquer le trafic entre elle et le PC Admin, j'ai choisi de définir une règle DFW au niveau du VNIC2 de la console. Le VNIC qui est lié au switch logique. **Figure 15**

Ne pas oublier de donner à la VM console l'accès aux autres tenants en définissant une règle dans l'EDGE FW

	User	Console	any	any	Accept
	Default	any	any	any	Deny

3.4.3 Avantages de l'utilisation de DFW

Le DFW applique les règles définies au niveau du VNIC de la VM. Ceci a plusieurs avantages :

- Seul le trafic qui devrait être le réseau est présent sur celui-ci, le reste est bloqué avant même qu'il ne quitte la VM, ce qui permet une économie du trafic inutile.
- L'inspection de chaque paquet avant qu'il ne soit présent sur le réseau.
- Etendre la capacité du DFW, en ajoutant des hôtes.

3.5 CONCLUSION

Pour ma part, je constate que la différence entre le DFW et le FW EDGE est comme la différence entre un FW physique et une ACL.
La définition de la règle DFW au niveau du VNIC, permet de faire une *stateful inspection* de tout paquet traversant un des objets de notre infrastructure logique (cluster, switch logique, VM…).

Ce que le FW EDGE ne permet pas puisque ses règles ne permettent qu'une *stateless inspection* basée sur des adresses IP statiques. Donc, ce FW joue le même rôle qu'une ACL.

A mon avis, il n'est pas encore temps de remplacer complétement un FW physique.

Une autre solution reste très utile pour gérer le flux venant du réseau externe, c'est d'utiliser le service composer qui nous permet d'établir des politiques de sécurité *(policies Security)* et des groupes de sécurité (Security *groups*) pour l'ensemble des VMS.

Pour une entreprise comme SmartBee, une architecture qui comporte un ESG pour chaque tenant et la méthode la plus adapté à mon avis.
En plus de la facilité de son déploiement, cela nous permet aussi de les isoler en bloquant simplement le routage entre les ESG dans le DFW.

Chapitre 4 :

Load Balancer -SSL

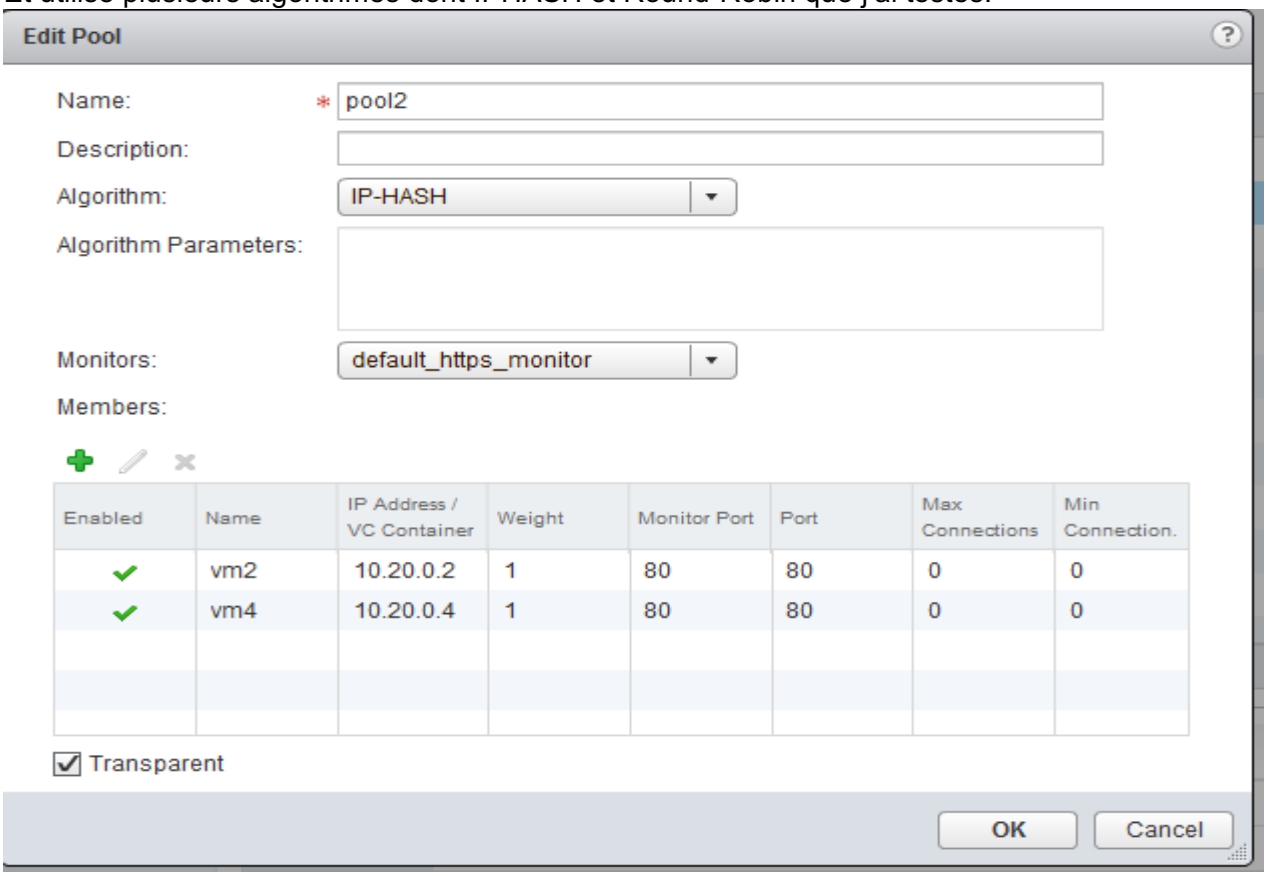
L'objectif de ce chapitre est de

1. Tester les deux modes de Load Balancing proposés par NSX.
2. Le mode transparent et le mode non-transparent et définir la différence entre les deux modes.

3. Faire le parallèle avec un Load Balancer physique

4.1 INTRODUCTION

Parmi les autres fonctionnalités de lESG, le Load balancing,.
Il supporte un éventail important des protocoles comme http, HTTPS. ICMP, FTP…
Et utilise plusieurs algorithmes dont IPHASH et Round-Robin que j'ai testés.

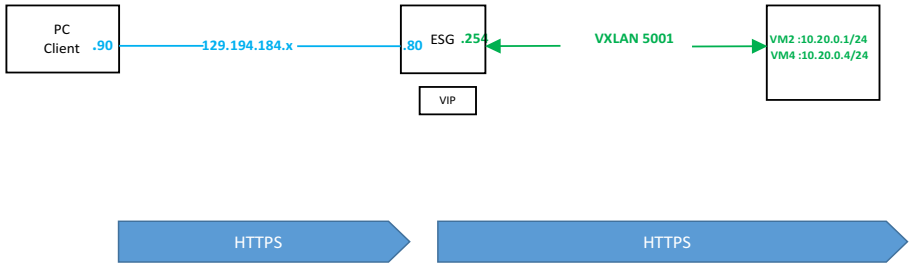


VMware propose deux modes de Load Balancing
1) Le mode transparent, ou inline mode.
2) Le mode non transparent, appelé aussi one-arm ou mode Proxy.

Les deux modes seront étudiés et analysés grâce à des captures Wireshark prises sur les VM2 et le VM4

4.2 MODE NON-TRANSPARENT OU ONE-ARM

4.2.2 Schéma



Client-IP → VIP

Client-IP → VM2 ou VM4 = SERVER IP

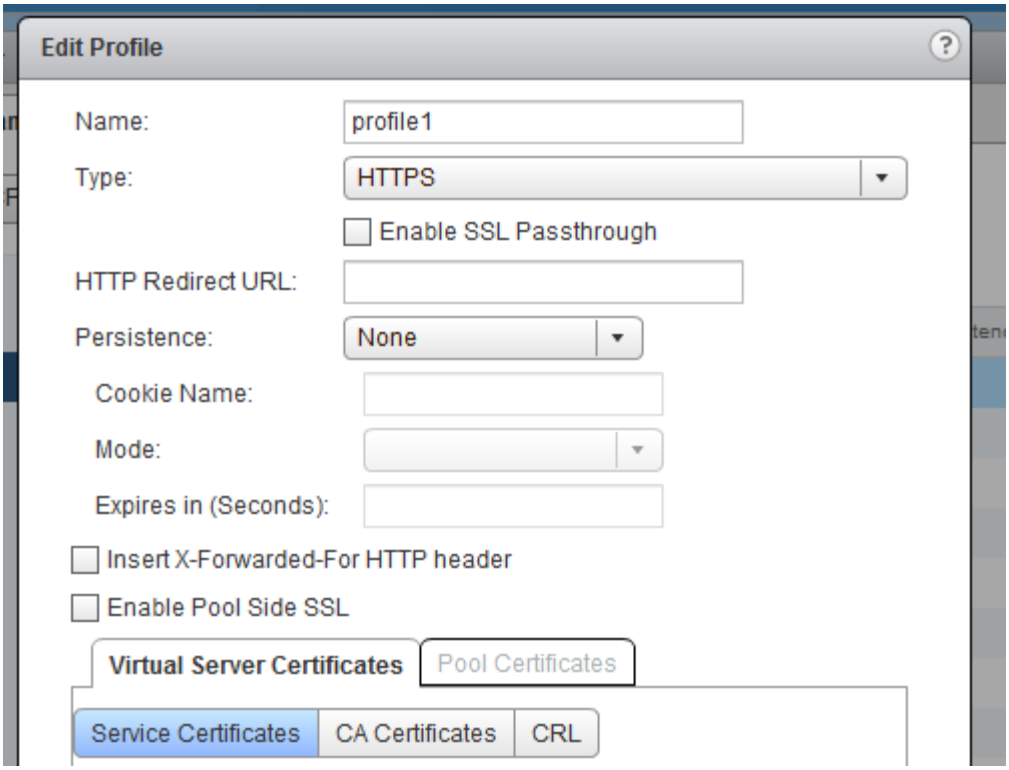
SERVER-IP → Client-IP

VIP → CLIENT-IP

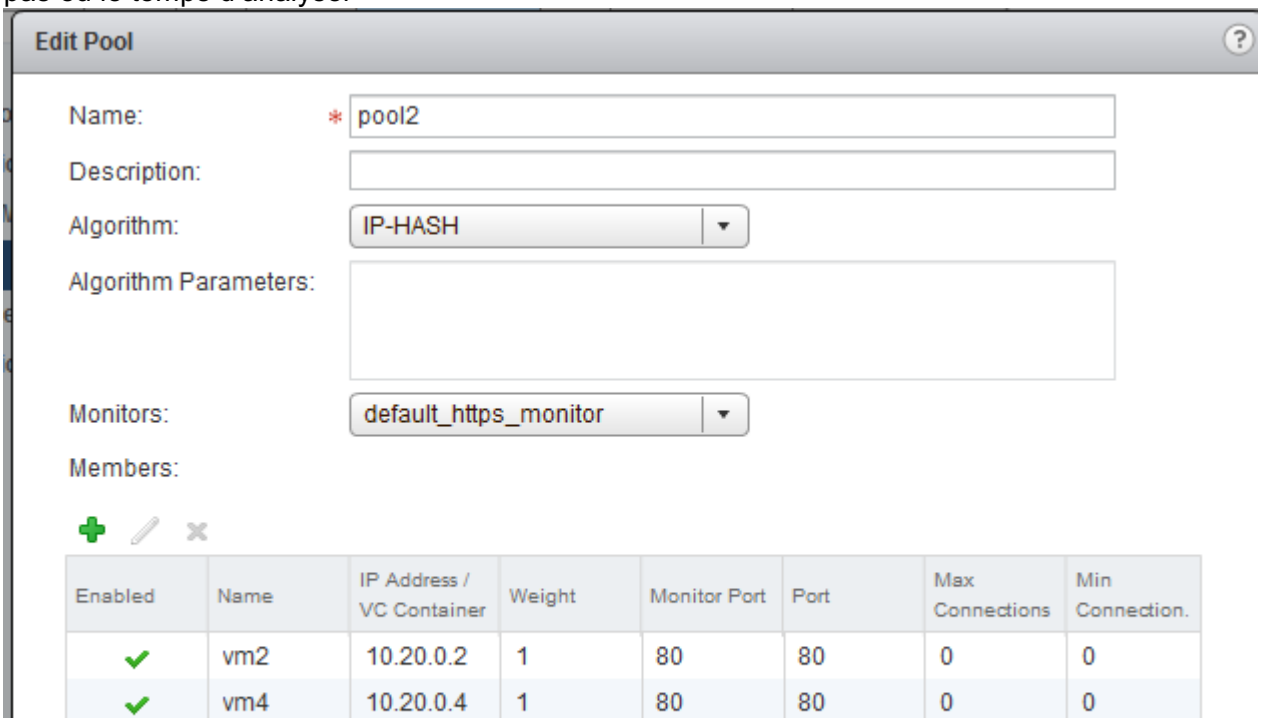
4.2.2 Configuration

Dans l'onglet Load Balancer, Global configurations, activer le Load Balancing

Dans application profiles, définir un profile, en choisissant le HTTPS dans la liste déroulante Type

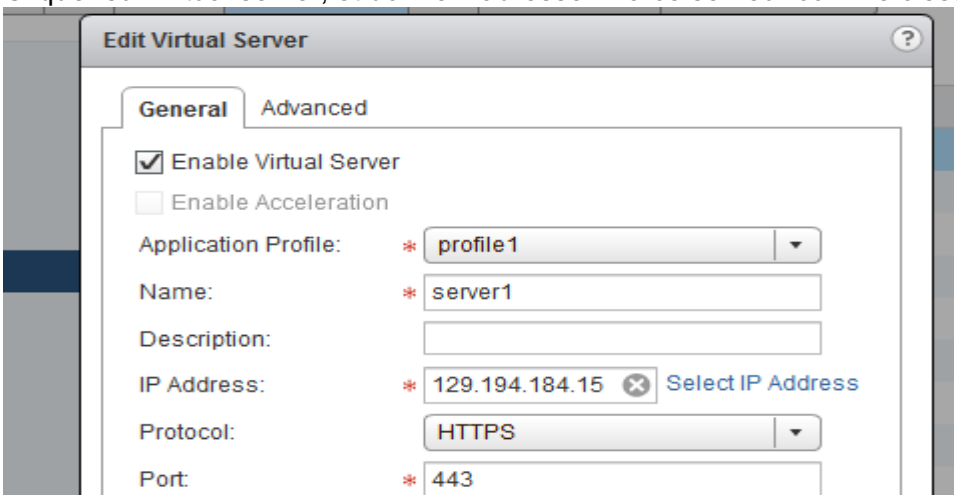


Dans pools, définir l'algorithme. J'ai choisi l'algorithme IPHash dans ma configuration parce Round-Robin est simple, et les autres algorithmes engendrent des erreurs, que malheureusement, je n'ai pas eu le temps d'analyser



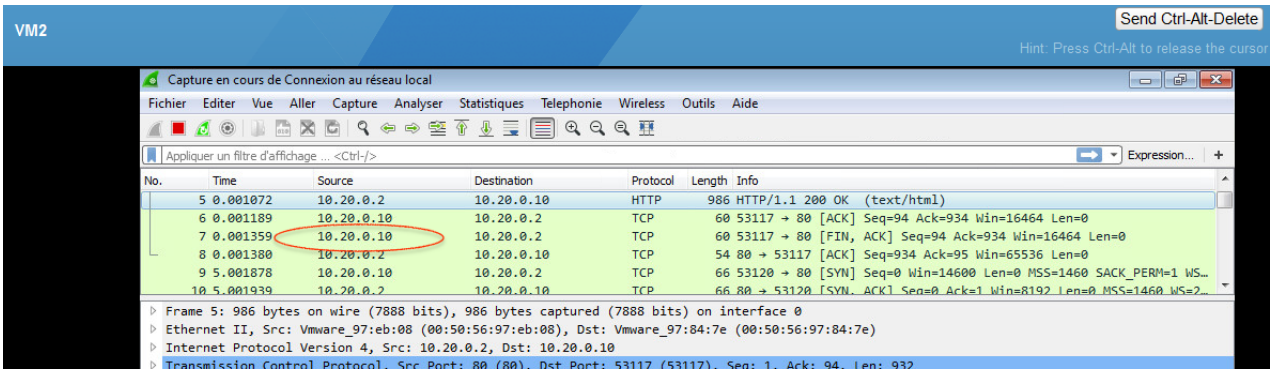
Avant de continuer la configuration, s'assurer que le pool a un statut UP.

Cliquer sur virtual server, et donner l'adresse IP à ce serveur comme c'est indiqué dans la capture



Ne pas oublier d'aller dans l'onglet networking- VDS- PortGroup de ten1. Et modifier la propriété Failover&teaming du port en IPHASH.

4.2.3 Fonctionnement



Le mode non transparent est un mode qui fonctionne comme un proxy, où seulement l'adresse IP de destination est modifiée
Dans cet exemple les VM2 et VM4 ne voient pas l'adresse du client mais seulement l'adresse de l'interface tenant1 de l'ESG qui est le 10.20.0.10.

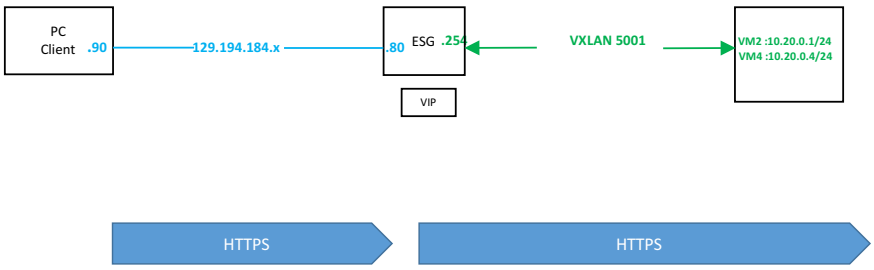
4.2.4 Fonctionnement de l'algorithme IPHASH :

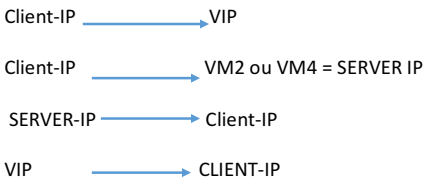
Cet algorithme est basé sur l'adresse IP source et destination, en calculant chaque paquet pour déterminer quel UPLINK utiliser.

Figure 18: Algorithme IPHASH

4.3 MODE TRANSPARENT

4.3.1 Schéma

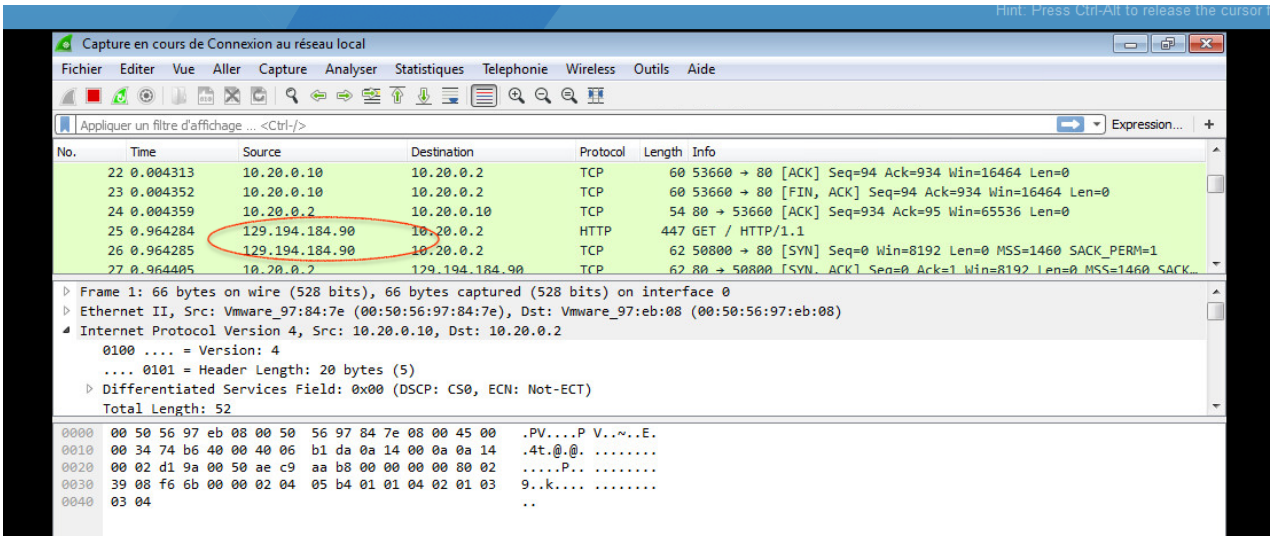




4.3.2 Configuration

Pour configurer le mode transparent, il suffit d'aller sur pools, et cocher la case du mode transparent

4.3.3 Fonctionnement



A la différence du mode-non transparent, ce mode modifie l'adresse IP source et destination. Cette capture qui est prise sur l'interface de VM2 montre que l'adresse du client 129.194.184.90 est affichée.

4.4 LE LOAD BALANCING SSL

4.4.1 Schéma

Client-IP → VIP

Client-IP → VM2 ou VM4 = SERVER IP

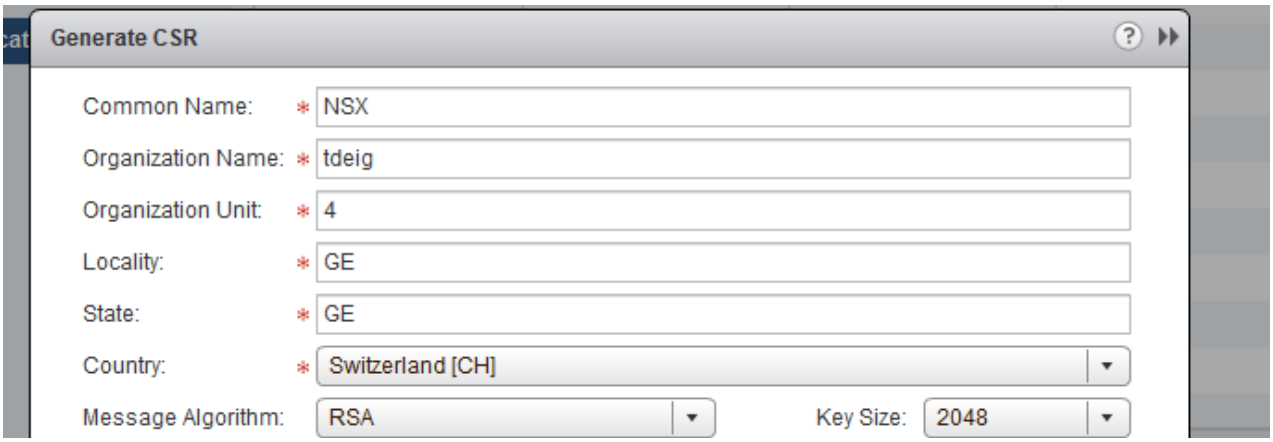
SERVER-IP → Client-IP

VIP → CLIENT-IP

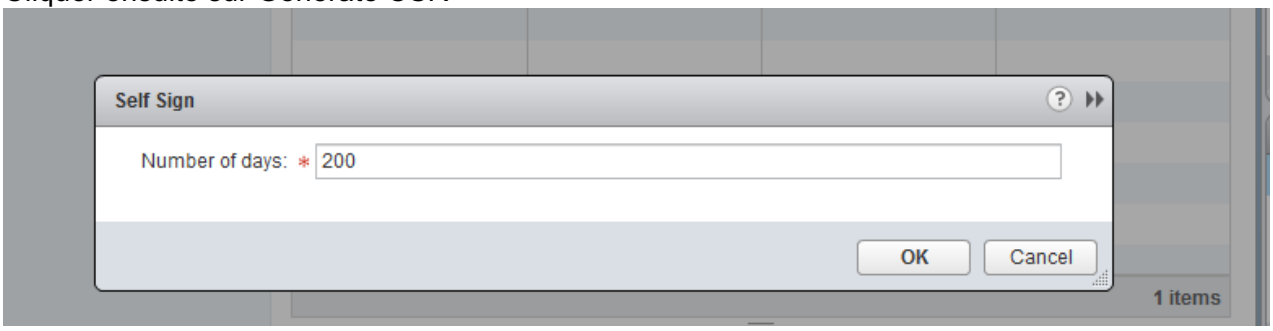
4.4.2 Configuration

NSX permet de configurer le flux chiffré HTTPS sur ESG.
J'ai choisi un certificat auto-signé généré par ESG en allant sur Settings- Certificats

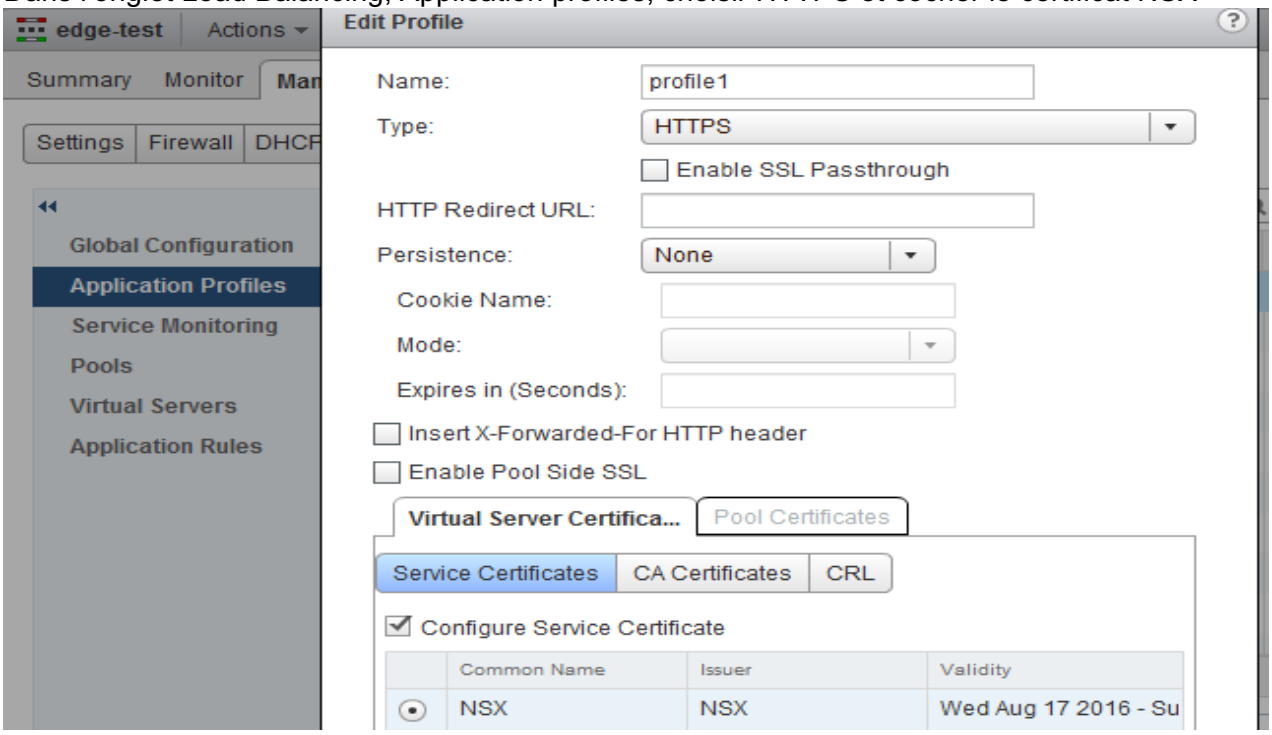
Action Generate CSR



Cliquer ensuite sur Generate CSR

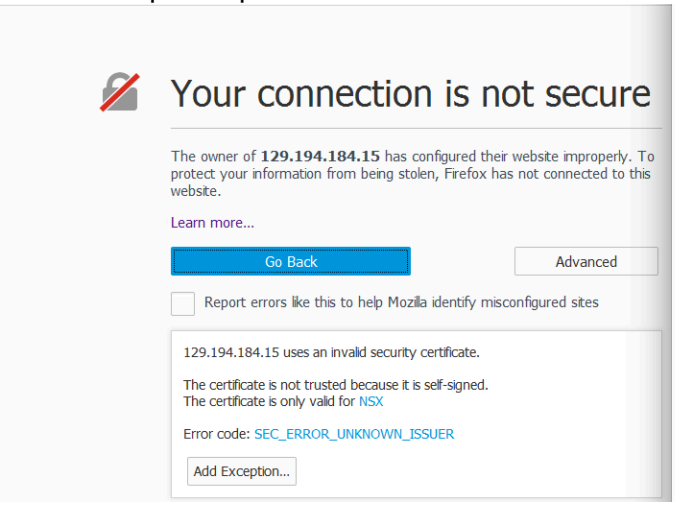


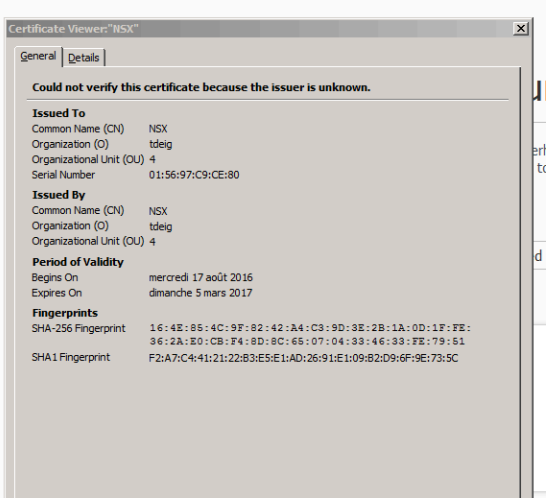
Dans l'onglet Load Balancing, Application profiles, choisir HTTPS et cocher le certificat NSX



Dans Virtual Server, choisir HTTPS au lieu de HTTP

Voici les captures prises sur le PC Client





4.5 ANALYSE

J'ai testé d'abord, le mode transparent et le mode non-transparent. Nous avons vu que la différence réside dans le fait que dans le mode transparent notre VM connaît l'adresse du PC Client.
En fait il n'y a pas de bon ou de mauvais choix, tout se base sur nos propres besoins.
Personnellement, je n'ai jamais vu dans ma vie professionnelle le mode transparent déployé dans un réseau de production.
Néanmoins, il reste un mode à choisir dans le cas où il y'aurait besoin des adresses des clients pour protéger une application.

J'ai sollicité les VM2 et VM4 en envoyant des requêtes enchaînées les unes après les autres.
Au bout de 3 minutes à peu près le pool que j'ai défini a changé son statut en down et le site est devenue indisponible avec l'erreur 503 : Service unavailable.

4.6 CONCLUSION

J'ai activé le HA (High Availibility) pour avoir deux ESG dont 1 est en mode passif.
Normalement, l'ESG passif prend le relais ou cas où la première EDGE est indisponible dans les 15 ms.
Après plusieurs tests, j'ai remarqué que quand j'éteins la VM du premier EDGE, la connexion depuis le PC Client est impossible.
Malheureusement, je n'ai pas eu le temps de faire plus de tests. Mais, je suppose que la synchronisation n'est pas faite correctement.

L'importance du NSX Load Balancing n'est pas visible dans un petit réseau, quand il s'agit d'un seul Load Balancer.

En fait son importance réside dans la simplicité de sa configuration, en choisissant l'algorithme qui nous convient.
Que ce soit un seul Load Balancer ou une centaine, le coût reste fixe, puisque nous pouvons déployer une multitude de Load balancer allant jusqu'à 200 pour un NSX Manager.

Chapitre 5 :

Bilan

Ce chapitre énumère

- Les problèmes que j'ai rencontrés tout au long de la réalisation de ce rapport.
- Un paragraphe qui parle des futurs projets que Vmware compte réaliser dans le domaine de la virtualisation réseau et sa position par rapport aux autres acteurs dans ce marché.
- Donne une conclusion générale évaluant le produit de Vmware NSX et son impact sur le domaine de l'administration réseau
- Je propose quelques sujet qui peuvent compléter mon travail.

Les mêmes pratiques peuvent être conservées dans la virtualisation réseau par NSX.
Le plus important est de bien comprendre le fonctionnement du DFW

Les tests que j'ai réalisés au cours de ce travail ont montré que le DFW reste plus puissant que le FW EDGE et prend la main dans le cas où je bloque la règle par défaut.

Malgré que les tests ont été concluants, et ont montré que le FW EDGE combiné au DFW sont capable de protéger nos tenants, je reste convaincue qu'il n'est pas encore temps de s'en passer d'un FW physique.
Néanmoins, nous pourrions nous passer de limiter notre réseau par des zones de sécurités et se contenter des règles DFW dans notre propre réseau.

5.1 LIMITES

Outre son prix qui reste élevé par rapport à des petites et moyennes entreprises, NSX a d'autres limites notamment :

- Les Bugs qui restent assez fréquents surtout dans la version 6.2.
- La disponibilité du réseau qui reste moyenne.
- Les trames VXLAN demandent un switch qui peut traiter les jumboframes, faute de quoi le traitement des paquets devient plus long
- La multitude de ces composants demande une surveillance très élevée de tous ces composants, sinon on peut passer des heures à faire des troublesootings, alors que le problème pourrait venir d'une simple déconnexion du contrôleur, un service qui a stoppé dans NSX Manager, ou de la mauvaise configuration d'un VXLAN

La méthode la plus simple reste d'avoir un réseau mixte composé de composants virtuels et physiques.

5.2 PROBLEMES RENCONTRES

J'ai rencontré au cours de la réalisation de ce travail, des problèmes d'ordre technique d'autres d'ordre organisationnel. Parmi ces problèmes, je vais souligner les suivantes :

- Vmware NSX est pour moi un nouveau produit que je ne connaissais pas avant. Vu la complexité de ses couches, et les nouveaux termes techniques dont je devais comprendre le fonctionnement, j'ai passé beaucoup de temps dans la partie théorique au détriment de la partie pratique.

- J'ai utilisé au début NSX6.2, une version qui ne fonctionne qu'avec VCSA6.x. Malheureusement, aucune référence VMware ne le signale. Je l'ai abandonné après la consultation de l'équipe de développeurs NSX pour NSX6.1.

- J'ai adopté au début pour la méthode up-down, ce qui ne convient pas à la philosophie VMware, et m'a obligé à changer l'architecture physique plus d'une fois. Heureusement que M.Litzistorf m'a guidé vers la bonne pratique.

- Des problèmes rencontrés dans la configuration du VCSA parce que je n'ai pas compris au début qu'avant de la configurer, il faut avoir d'abord un serveur DNS et NTP fonctionnels.

- L'expiration de la licence VCenter m'a obligée de tout réinstaller.

- La complexité de l'architecture NSX rend la compréhension du trafic du flux difficile.

- La multitude des composants permettant de déployer une politique de sécurité m'a obligé à les tester pratiquement tous pour choisir les plus adaptés à mes scénarios

5.3 CONCLUSION GENERALE

Vmware reste l'entreprise pilote dans la virtualisation réseau. Elle se démarque par le fait que NSX peut fonctionner avec plusieurs hyperviseurs, n'importe quel matériel et ne demande pas une architecture réseau spéciale.
NSX peut être déployé dans un réseau L2 ou L3, et son déploiement reste en général simple et rapide.

Plus besoin d'encombrer le réseau avec des switches et des routeurs physiques, l'architecture NSX reste valable pour petits, moyens ou aussi les grands Clouds

Mais, comme tout se fait au niveau logiciel, une nouvelle couche de complexité s'ajoute à ce niveau.
La virtualisation réseau avec NSX demande d'acquérir un certain nombre des licences. :
Licence VCenter. ESXI. NSX….
Ces licences coutent cher (Annexe7). Selon moi, à proscrire pour les petits réseaux et les infrastructures simples.

Malgré que le déploiement d'un réseau virtuel NSX reste simple, et peut se réaliser en quelques clics, la gestion de tel réseau reste assez complexe, et demande un bagage de connaissances, non seulement en gestion des réseaux comme c'est le cas pour les administrateurs des réseaux physiques, mais des connaissances en virtualisation des serveurs et réseaux, En outre, une connaissance des protocoles de communication et leur fonctionnement (OSPF, BGP, MPLS…) est aussi nécessaire. Par ailleurs, il est indispensable d'avoir des compétences dans le troublesooting, et un savoir en analyse des bugs parce que nous en aurons besoin.
Avec la nouvelle génération du FW distribué que VMware a mis en place, une nouvelle méthode de filtrage de flux a vu le jour.
Le fait que le DFW se base sur le VNIC de la VM pour définir ses règles. Dans ce modèle de FW, chaque VM est protégée par sa propre instance FW, alors que dans les FW classiques, les architectures réseaux se basent sur la disposition des composants dans des zones de sécurité isolées les unes des autres.
La plupart de ces zones sont connectées par des FW. Dans le cas où un serveur est infecté, toute la zone sera infectée.

Donc, dans le cas de DFW, quel est l'intérêt des zones sécurité ?

L'architecture de DFW a plusieurs avantages, notamment :

- Simplification de l'architecture réseau en supprimant les zones sécurité
- Optimisation du flux en favorisant aussi le flux est-ouest et pas seulement nord-sud
- Le FW attaché à la VM peut migrer en même temps que la VM
- Gestion des règles basées sur les attributs de la VM et pas seulement sur son adresse IP

Cependant, quelques questions restent à poser :

- Peut-on faire confiance à cette architecture ?
- Est-il possible de se passer des FW classiques et de les remplacer par cette nouvelle génération des FW, ou peuvent-ils fonctionner ensemble dans un réseau mixte ?
- Ont-ils le même débit, dans les grands réseaux, que les FW physiques ?
- Peuvent-ils inspecter le trafic circulant entre les VMS et Internet avec les mêmes garanties qu'un FW physique ?
- Est-il possible de donner la responsabilité de la sécurité à l'équipe de virtualisation ?
- Est-ce qu'on est en train d'aller vers une structuration des fonctions des administrateurs réseaux ?

Et après-----

Avant que je finisse cette étude, NSX avait déjà sorti la nouvelle version de VMware NSX

NSX Cross VCenter, un produit permettant de gérer un réseau multi-sites avec une seul instance NSX Manager et un seul VCenter.
Une autre génération de FW voit le jour : Le UFW (Universal FW) permettant de protéger un réseau multi-sites.

La virtualisation réseau vise à pratiquer la politique : *one company one team*

Suggestion de sujets

- Etude de VPN et SSl-VPN plus
- Mise en place d'une politique se basant sur Spoof-Guard et simulation d'un fishing attack
- VMware NSX Horizon. Une plateforme pour un labo. Son architecture, ses fonctions.
- Etude approfondie de VMware NSX security : lien entre service composer et DFW, Spoofguard utilité, EDGE FW ou LDR FW lequel choisir ? …..
- Méthodes de gestion des fichiers logs
- Gestion de la sécurité informatique par NSX

Annexes

ANNEXE 1 : PREREQUIS

Prérequis matériel

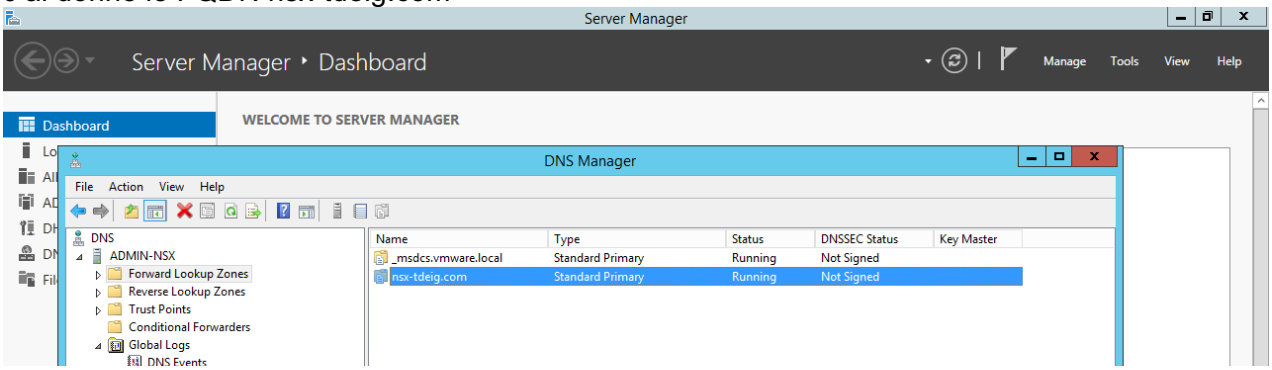
Component	Minimum
Memory	■ NSX Manager: 12 GB ■ NSX Controller: 4 GB ■ NSX Edge Compact: 512 MB, Large: 1 GB, Quad Large: 1 GB, and X-Large: 8 GB ■ Guest Introspection: 1 GB ■ NSX Data Security: 512 MB
Disk Space	■ NSX Manager: 60 GB ■ NSX Controller: 20 GB ■ NSX Edge Compact, Large, and Quad Large: 512 MB, X-Large: 4.5 GB (with 4 GB swap) ■ Guest Introspection: 4GB ■ NSX Data Security: 6 GB per ESX host
vCPU	■ NSX Manager: 4 ■ NSX Controller: 4 ■ NSX Edge Compact: 1, Large: 2, Quad Large: 4, and X-Large: 6 ■ Guest Introspection: 2 ■ NSX Data Security: 1

Les ports requis pour NSX Manager

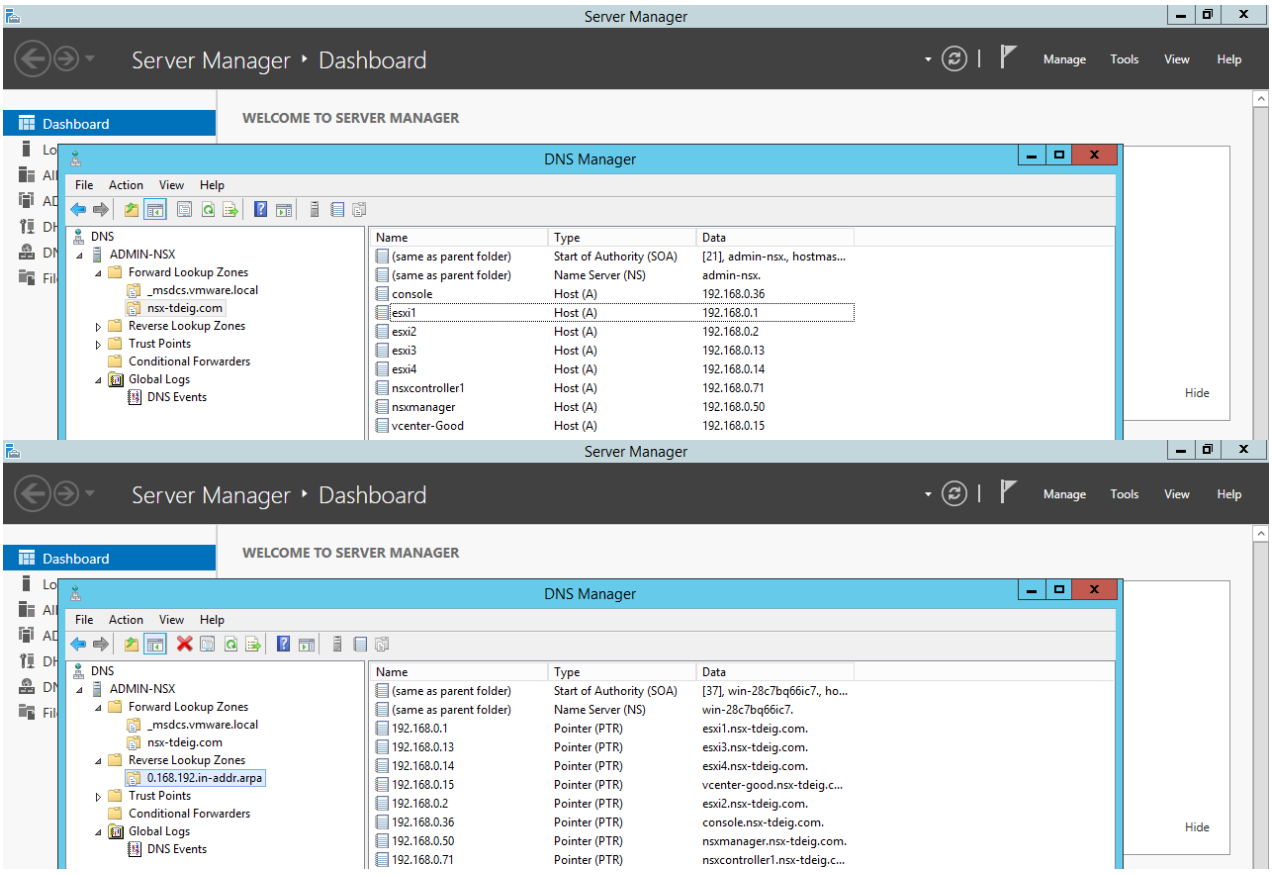
Port	Required for
443/TCP	■ Downloading the OVA file on the ESX host for deployment ■ Using REST APIs ■ Using the NSX Manager user interface
80/TCP	■ Initiating connection to the vSphere SDK ■ Messaging between NSX Manager and NSX host modules
1234/TCP	Communication between ESX Host and NSX Controller Clusters
5671	Rabbit MQ (messaging bus technology)
22/TCP	Console access (SSH) to CLI. By default, this port is closed.

ANNEXE2 : CONFIGURATION DE L'ACTIVE DIRECTORY

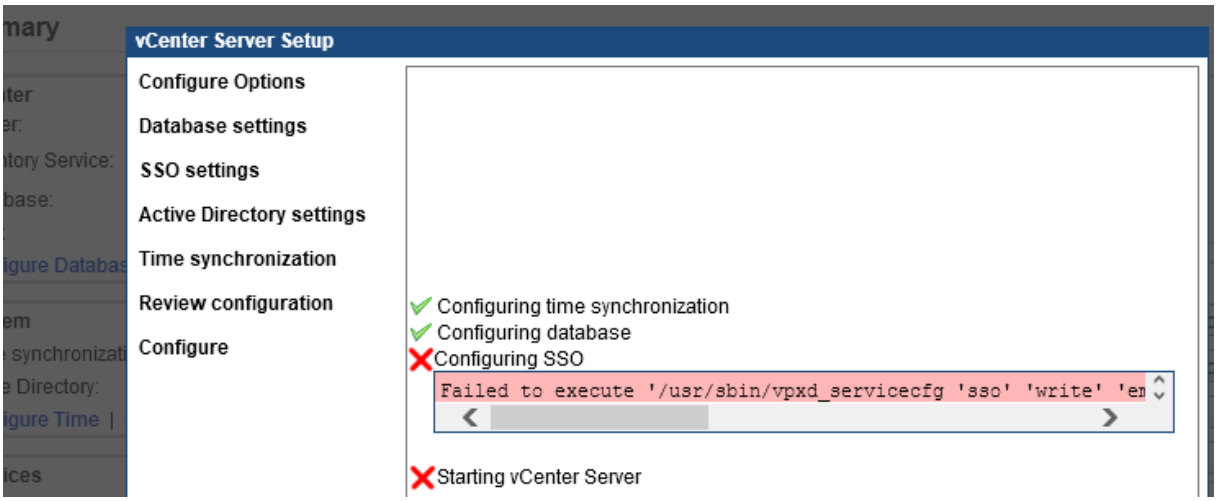
Installer Les services AD et DNS
J'ai donné le FQDN nsx-tdeig.com



Ne pas oublier de configurer une zone de Forwarding, et une autre pour le PTR
Après ajouter tous les ESXIS et les VMS qui appartiennent au réseau management



ANNEXE3 : PROBLEMES DE CONFIGURATION DE VCSA ET SOLUTION



La raison pour laquelle cette erreur est produite est que VCSA ne détecte pas le serveur DNS qui est primordial pour une configuration sans erreur

Dans ce cas, se loguer dans votre VCSA VM en utilisant VCenter client.
Ouvrir le fichier **/etc./hosts**, et rajoute les lignes ci-dessous. Enregistrez et rebooter la VM.

```
192.168.0.35 vcsa_Name
192.168.0.20  Esxi_Name
```

Si 0.0.0.0 est attribué comme adresse IP à VCSA, modifier le fichier
/opt/vmware/share/vami/vami_config_net
En donnant une adresse IP valable pour le DNS et le VCSA

```
vcsa55 login: root
Password:
vcsa55:~ # /opt/vmware/share/vami/vami_config_net

 Main Menu

0)      Show Current Configuration (scroll with Shift-PgUp/PgDown)
1)      Exit this program
2)      Default Gateway
3)      Hostname
4)      DNS
5)      Proxy Server
6)      IP Address Allocation for eth0
Enter a menu number [0]: _
```

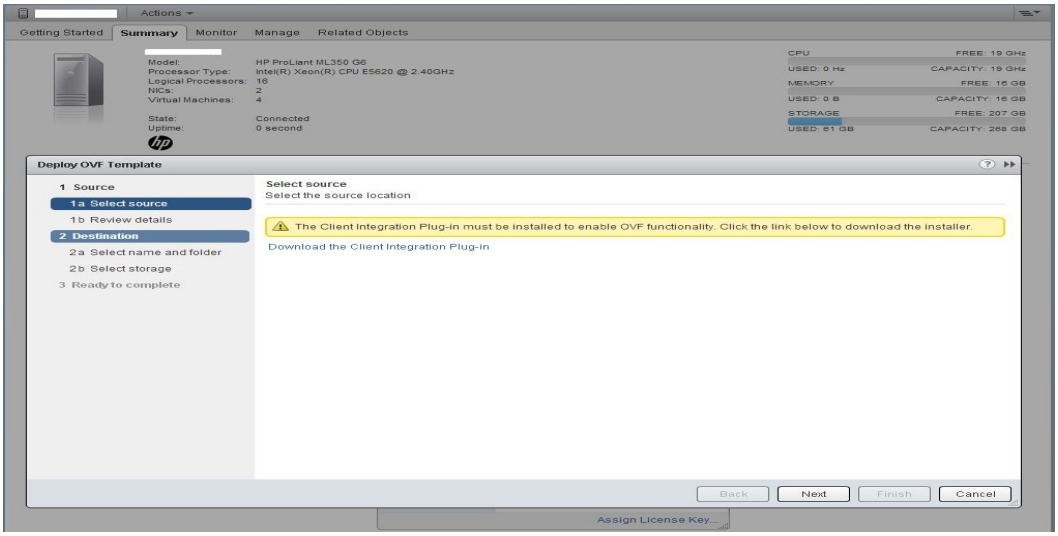
Liste d'exclusion
Avant de mettre le *defaulte rule* du DFW a block, Veuillez à mettre le VCenter dans la liste d'exclusion sinon il est impossible d'accéder à la VM et tous ses services deviennent indisponibles.

Mais pas de panique, vous pouvez supprimer cette action en suivant les étapes suivantes :

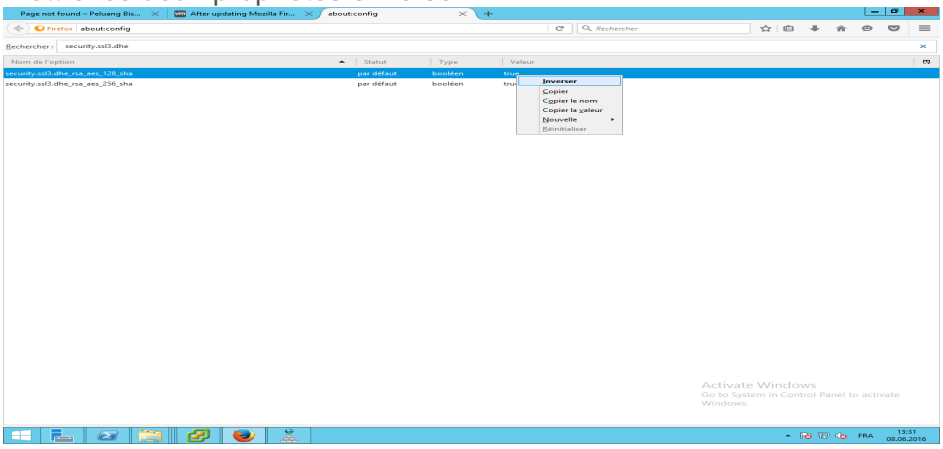
ANNEXE 4 : VSPHERE WEB CLIENT

J'ai essayé Internet Explorer, Chrome et Mozilla Firefox.
Selon moi le meilleur navigateur parmi c'est trois navigateur est Mozilla Firefox. En tout cas, éviter Internet Explorer parce qu'il n'est pas capable de prendre en charge certains plugins du web client.

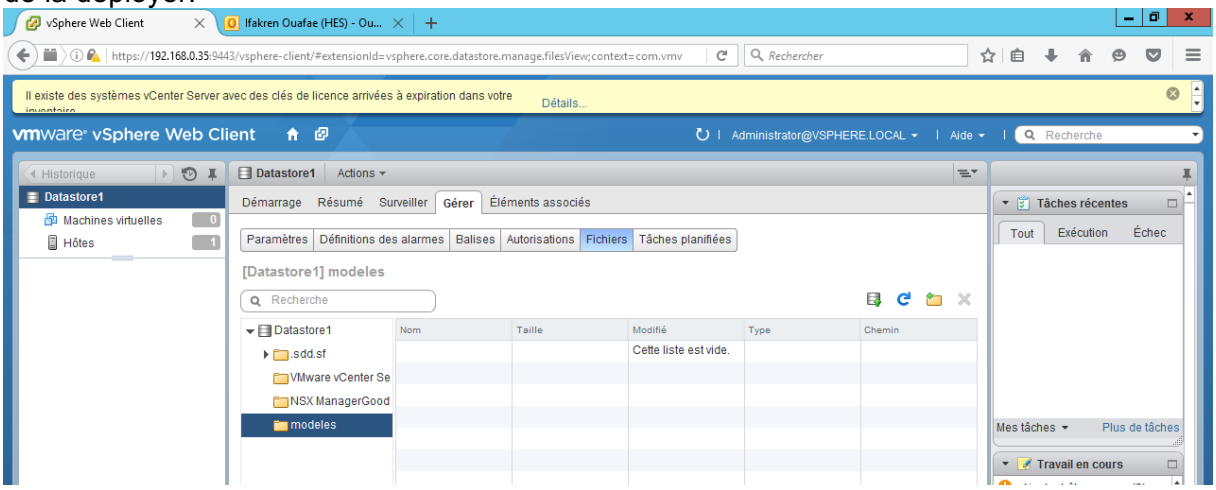
Veillez à ce qu'Adobe Flash Player soit mise à jour.
Pour déployer une VM OVF. Vsphere demande d'installer le client integration plugin



Installer le plugin, et rafraichir la page
Si le message persiste
Ouvrir un nouvel onglet dans Mozilla Firefox, taper : **about:config**
Dans search mettre : **security.ssl3.dhe**
Cliquer entrer.
Mettre les deux propriétés en false.

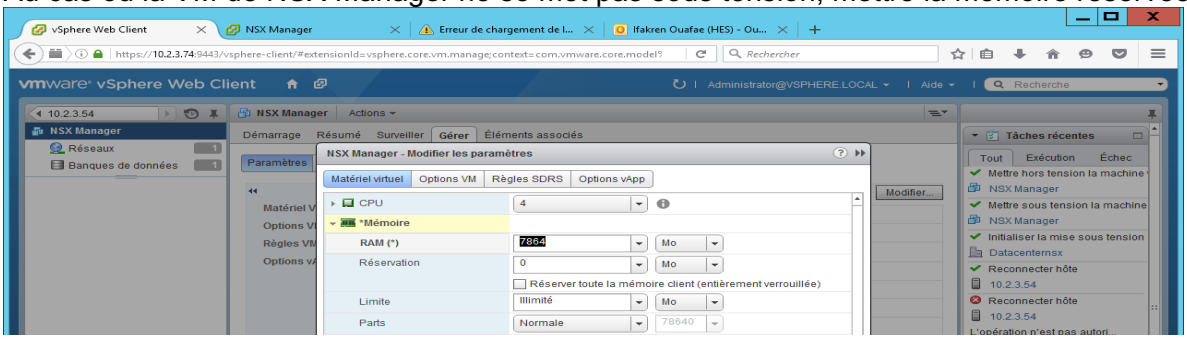


Pour déployer une VM.iso, aller dans banque de données, créer un fichier et rajouter l'mage avant de la déployer.

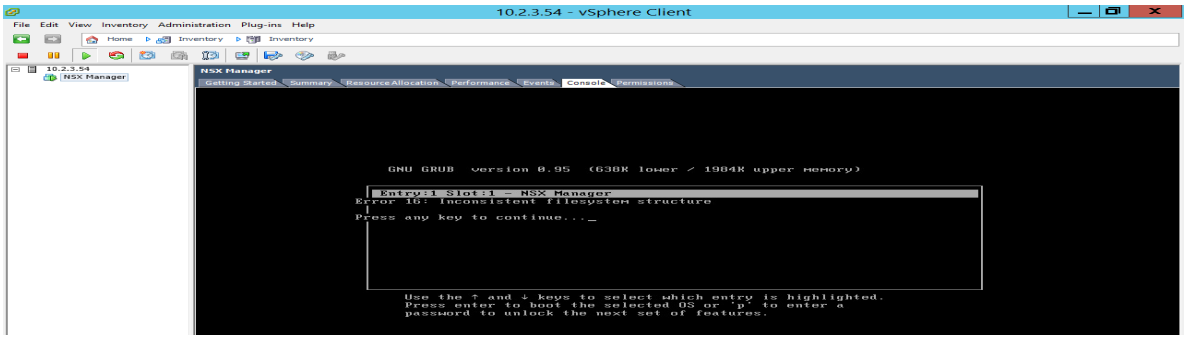


ANNEXE5 : VSPHERE NSX

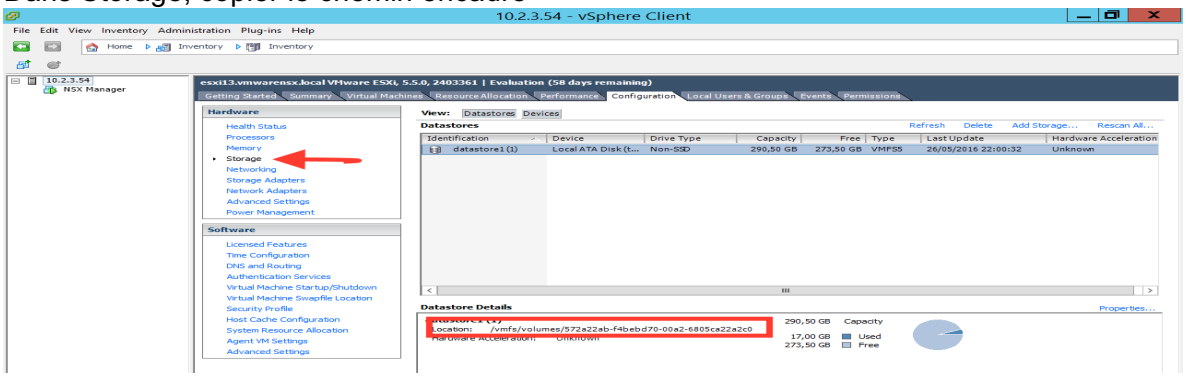
Au cas où la VM de NSX Manager ne se met pas sous tension, mettre la mémoire réservée à 0.



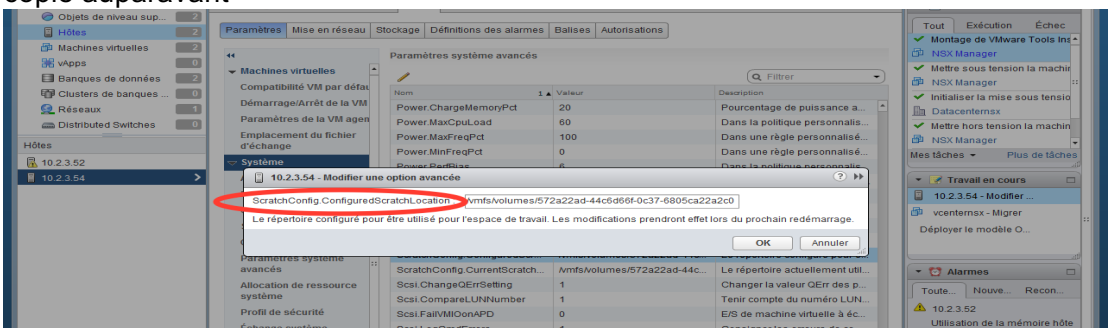
Pour l'erreur ci-dessous



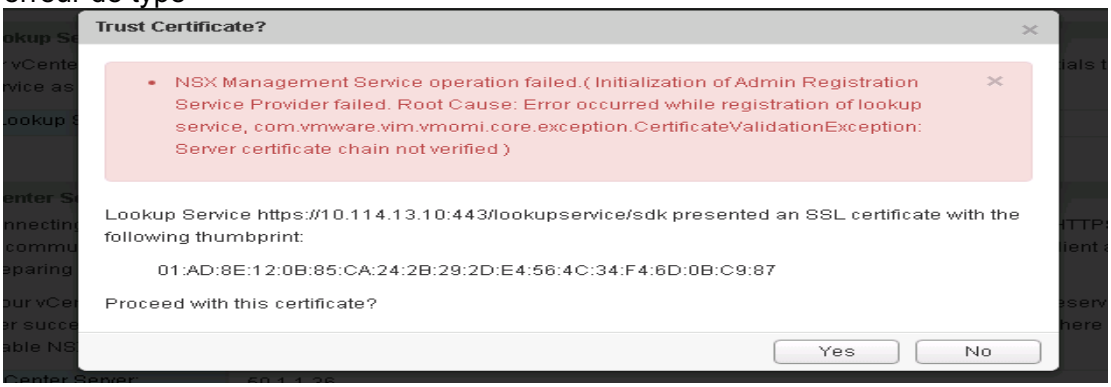
Dans Storage, copier le chemin encadré



Et Dans Système paramètre avancer localiser le fichier entouré ci-dessous, et coller le chemin copié auparavant

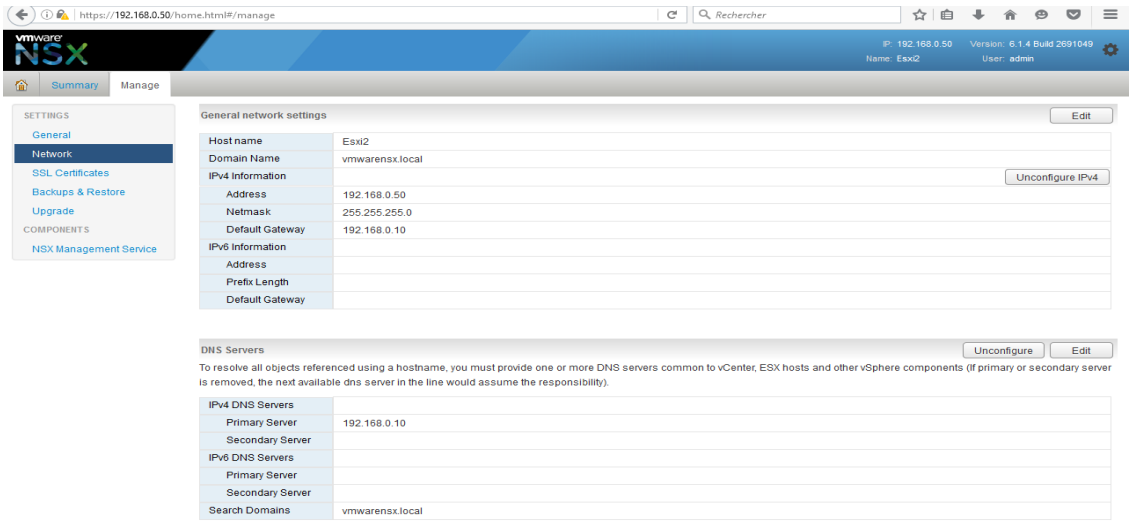


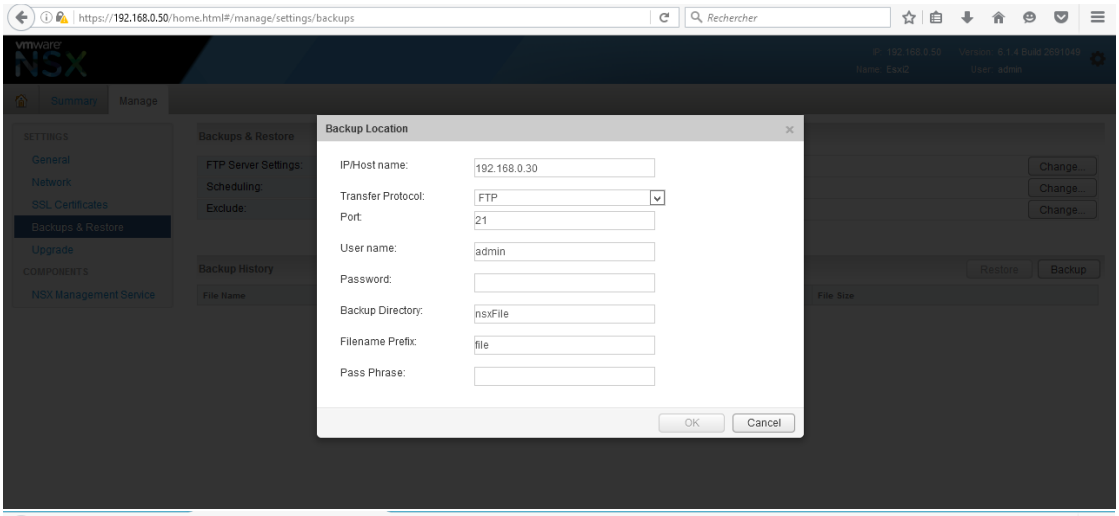
Durant la configuration de NSX Manager, il se peut que la configuration de lookup engendre une erreur de type

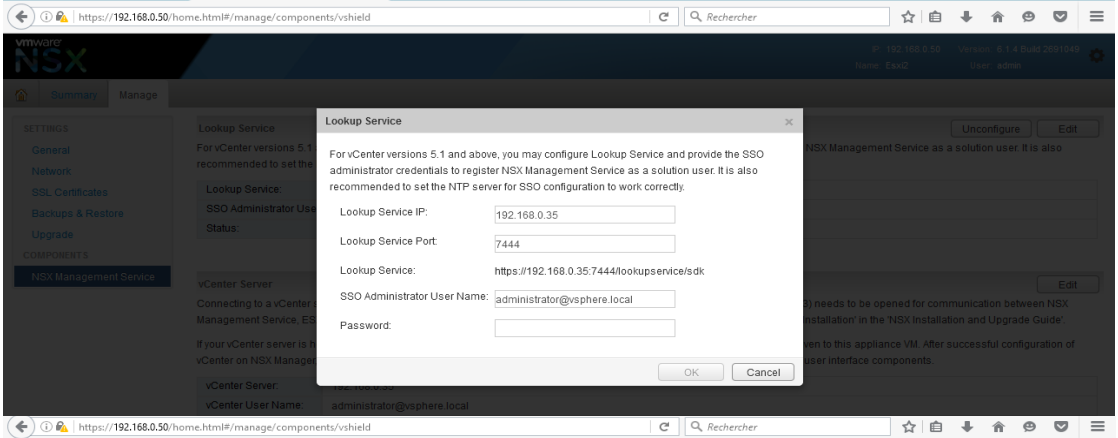


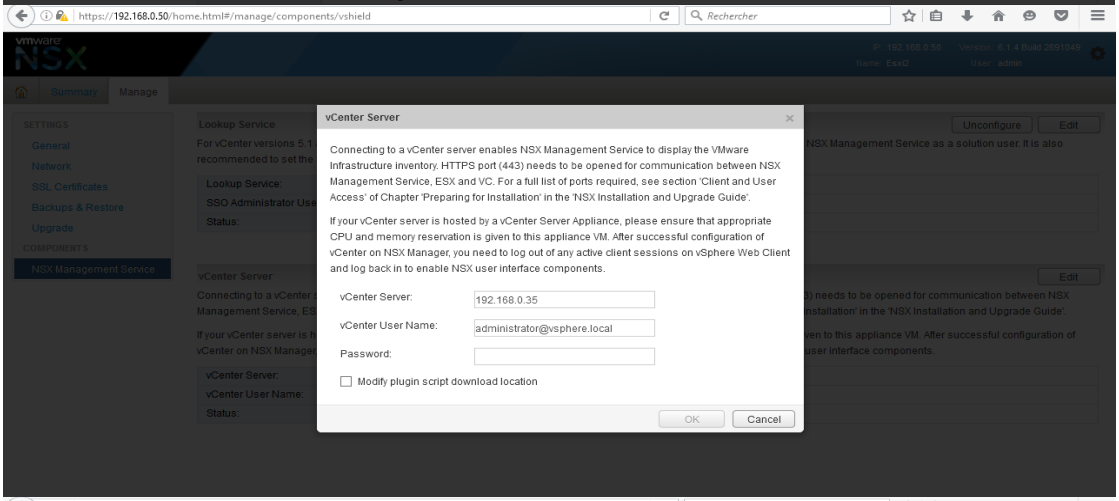
§1-2 Vérifier que le serveur DNS est configuré correctement, et que le NSX manager arrive à le pinger
§1-2 Vérifier la synchronisation de NSX Manager VM avec l'hôte (utiliser le même serveur NTP)
§1-2 Cette erreur peut être générée si l'adresse IP de VCSA a été changé. Dans ce cas, ouvrir l'adresse suivante : *https://[ip_VCSA]:5480*
Aller dans l'onglet Admin et générer un nouveau certificat SSl
Rebooter VCSA VM

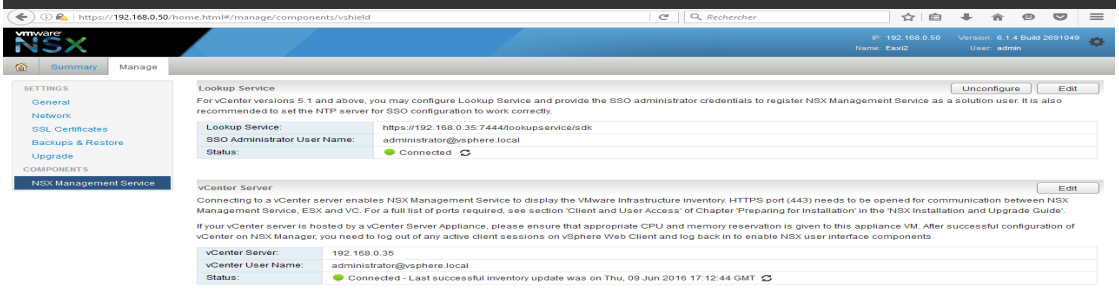
Configuration :



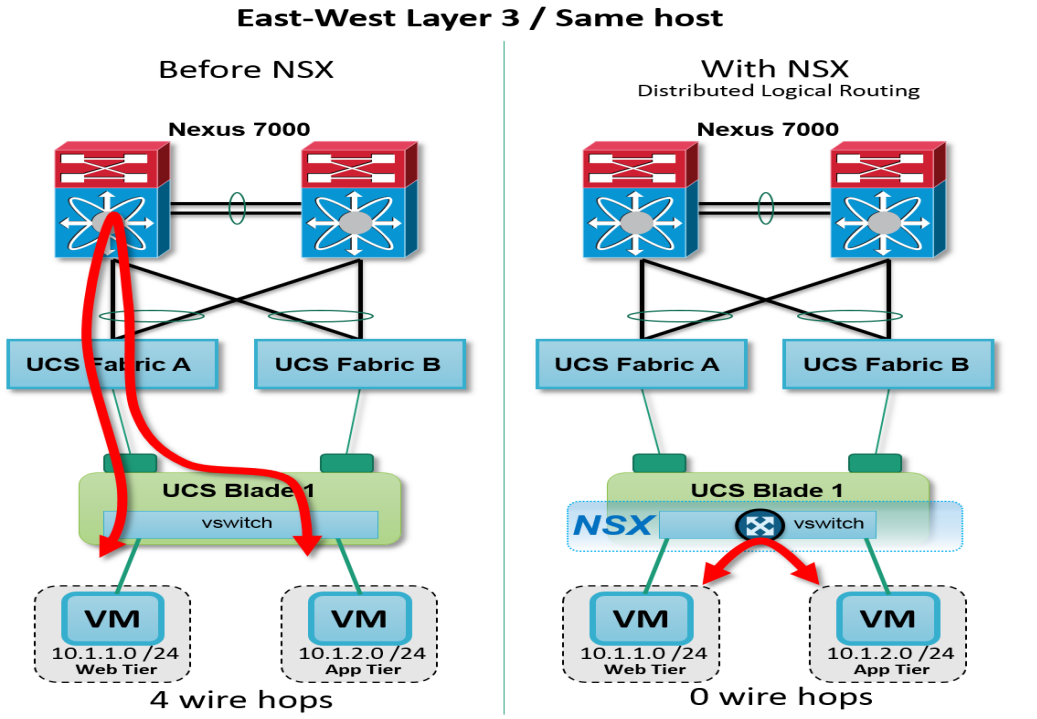

https://192.168.0.50/home.html#/manage/settings/backups
Backup Location
IP/Host name:
192.168.0.30
Transfer Protocol:
FTP
Port:
21
User name:
admin
Password:
Backup Directory:
nsxFile
Filename Prefix:
file
Pass Phrase:
OK
Cancel

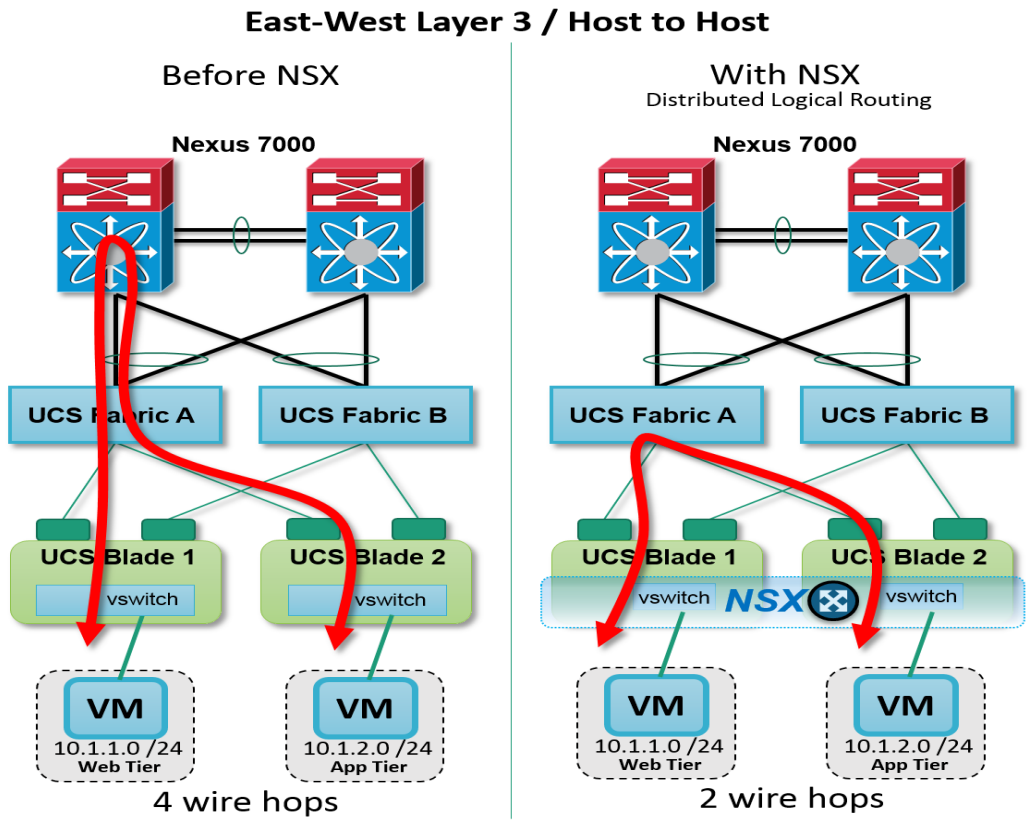

https://192.168.0.50/home.html#/manage/components/vshield
Lookup Service
For vCenter versions 5.1 and above, you may configure Lookup Service and provide the SSO administrator credentials to register NSX Management Service as a solution user. It is also recommended to set the NTP server for SSO configuration to work correctly.
Lookup Service IP:
192.168.0.35
Lookup Service Port:
7444
Lookup Service:
https://192.168.0.35:7444/lookupservice/sdk
SSO Administrator User Name:
administrator@vsphere.local
Password:
OK
Cancel


https://192.168.0.50/home.html#/manage/components/vshield
vCenter Server
Connecting to a vCenter server enables NSX Management Service to display the VMware Infrastructure inventory. HTTPS port (443) needs to be opened for communication between NSX Management Service, ESX and VC. For a full list of ports required, see section 'Client and User Access' of Chapter 'Preparing for Installation' in the 'NSX Installation and Upgrade Guide'.
If your vCenter server is hosted by a vCenter Server Appliance, please ensure that appropriate CPU and memory reservation is given to this appliance VM. After successful configuration of vCenter on NSX Manager, you need to log out of any active client sessions on vSphere Web Client and log back in to enable NSX user interface components.
vCenter Server:
192.168.0.35
vCenter User Name:
administrator@vsphere.local
Password:
Modify plugin script download location
OK
Cancel

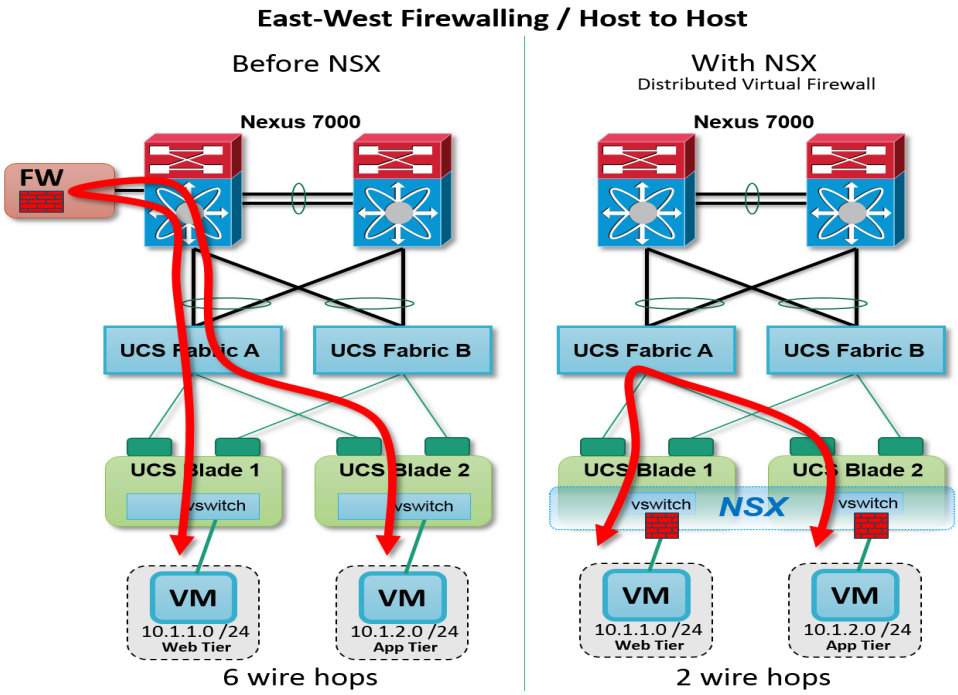

https://192.168.0.50/home.html#/manage/components/vshield
Summary
Manage
Lookup Service
Unconfigure
Edit
Lookup Service:
https://192.168.0.35:7444/lookupservice/sdk
SSO Administrator User Name:
administrator@vsphere.local
Status:
Connected
vCenter Server
Edit
vCenter Server:
192.168.0.35
vCenter User Name:
administrator@vsphere.local
Status:
Connected - Last successful inventory update was on Thu, 09 Jun 2016 17:12:44 GMT

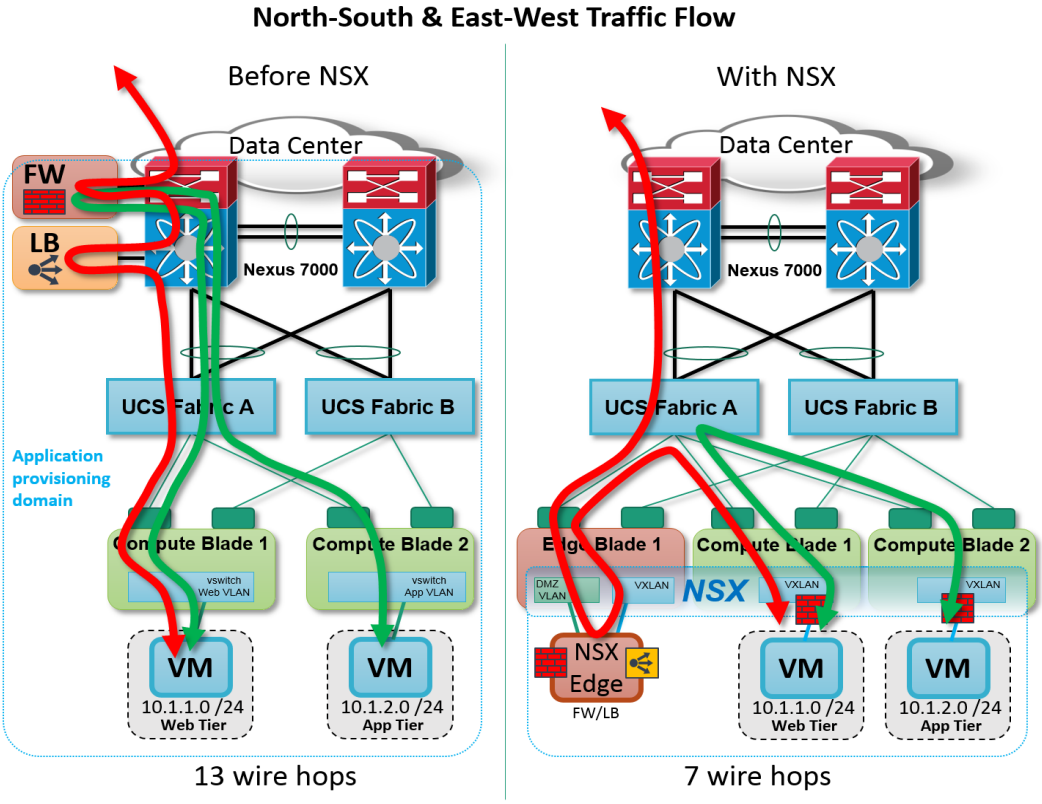
ANNEXE 6 : COMPARAISON ENTRE UNE ARCHITECTURE NSX ET SANS NSX[23]





[23] https://blogs.vmware.com/networkvirtualization/2013/09/vmware_nsx_cisco.html#.V7StEBL82ig


East-West Firewalling / Host to Host
Before NSX
With NSX
Distributed Virtual Firewall
Nexus 7000
FW
UCS Fabric A
UCS Fabric B
UCS Blade 1
UCS Blade 2
vswitch
NSX
VM
10.1.1.0 /24
Web Tier
10.1.2.0 /24
App Tier
6 wire hops
2 wire hops


North-South & East-West Traffic Flow
Before NSX
With NSX
Data Center
FW
LB
Nexus 7000
UCS Fabric A
UCS Fabric B
Application provisioning domain
Compute Blade 1
Compute Blade 2
vswitch Web VLAN
vswitch App VLAN
Edge Blade 1
DMZ VLAN
VXLAN
NSX
NSX Edge
FW/LB
VM
10.1.1.0 /24
Web Tier
10.1.2.0 /24
App Tier
13 wire hops
7 wire hops

ANNEXE7 : PRIX

TITRE DU PRODUIT	Prix de la licence	Support et abonnement pendant 1 an	
VMware vSphere Standard	€ 939.50	Basic	€ 257.79
		Production	€ 305.01
VMware vSphere Enterprise Plus	€ 3,305.00	Basic	€ 693.12
		Production	€ 825.32
VMware vSphere with Operations Management Enterprise Plus	€ 4,155.00	Basic	€ 871.59
		Production	€ 1,037.79

TITRE DU PRODUIT	Prix de la licence	Support et abonnement pendant 1 an		
VMware vSphere Standard Acceleration Kit	€ 10,350.00	Basic	€ 2,374.91	Trouver un revendeur
		Production	€ 2,832.90	Contacter le service commercial
VMware vSphere Enterprise Plus Acceleration Kit	€ 21,750.00	Basic	€ 5,349.46	Trouver un revendeur
		Production	€ 6,369.30	Contacter le service commercial
VMware vSphere with Operations Management Enterprise Plus Acceleration Kit	€ 23,650.00	Basic	€ 6,421.24	Trouver un revendeur
		Production	€ 7,644.11	Contacter le service commercial

Éditions de VMware vCenter Server

Éditions de VMware vCenter Server

TITRE DU PRODUIT	Prix de la licence	Support et abonnement pendant 1 an	
VMware vCenter Server Standard	€ 5,665.00	Basic	€ 1,188.87
		Production	€ 1,415.51

Ce lien donne les prix de Vmware NSX

http://www.virtualizationworks.com/NSX.asp

REFERENCES

http://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmw-nsx-network-virtualization-design-guide.pdf

http://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/whitepaper/products/nsx/vmware-nsx-network-virtualization-platform-white-paper.pdf

https://pubs.vmware.com/NSX-62/topic/com.vmware.ICbase/PDF/nsx_62_admin.pdf

https://pubs.vmware.com/NSX-62/topic/com.vmware.ICbase/PDF/nsx_62_api.pdf

https://pubs.vmware.com/NSX-62/index.jsp?topic=%2Fcom.vmware.nsx.admin.doc%2FGUID-2482B032-F420-432F-A6D0-6CD91506BFCC.html

http://www.routetocloud.com/2015/04/nsx-distributed-firewall-deep-dive/

https://vmwire.com/2011/07/17/vmware-vcenter-server-virtual-appliance-vcsa-features-and-benefits/

http://www.vladan.fr/vcsa-5-5-installation-configuration-part-2/

https://www.vmware.com/support/developer/converter-sdk/conv60_apireference/vim.DistributedVirtualSwitch.html

https://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.networking.doc%2FGUID-B15C6A13-797E-4BCB-B9D9-5CBC5A60C3A6.html