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

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

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 :

- 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
- 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 :	Professeur(s) responsable(s) :	Timbre de
Mme Ouafae Ifakren Filière d'études : ITI	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	

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
- 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

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

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.



Printemps 2016 Session de bachelor

LISTE DE FIGURES

Figure 1: Architecture de NSX	14
Figure 2: Trame VXLAN	16
Figure 3 Trafic unicast	17
Figure 4:VTEP- envoi de la table	18
Figure 5:Transfert de la table lookup	19
Figure 6:Table entry	19
Figure 7: Switch Logiqiue trafic unicast	20
Figure 8: Edge FW Generated Rules	21
Figure 9: DFW rules	22
Figure 10: Service Composer	22
Figure 11: Management Plane architecture	24
Figure 12: Architecture multi-tenants	24
Figure 13: Proxy ARP	25
Figure 14:SDDC Architecture	26
Figure 15: ARCHITECTURE EVOLUTIVE	26
Figure 16:Règles FW	42
Figure 17: Règles DFW de la console et tenants	43
Figure 18: Algorithme IPHASH	50

TABLE DES MATIERES

ENONCE	2
RESUME	3
GLOSSAIRE	4
REMERCIEMENT	5
LISTE DE FIGURES	6
TABLE DES MATIERES	7
INTRODUCTION	11
CHAPITRE1 :	13
COMPOSANTS ET SERVICES	13
1.1 PRESENTATION	14
1.2 ARCHITECTURE	14
1.2.1 DATA PLANE	15
1.2.2 CONTROL PLANE	15
1.2.3 MANAGEMENT PLANE & CONSUMPTION MODEL	15
1.3 LES COMPOSANTS	15
1.3.1 NSX MANAGER	15
1.3.2 NSX CONTROLLER	15
1.4 FONCTIONNEMENT DES SERVICES	16
1.4.1 LES VXLANS	16
1.4.2 TRAFIC UNICAST	17
1.4.3 LE ROLE DES VTEP	18
1.4.4 LES SWITCHES LOGIQUES (LOGICAL SWITCHES)	19
1.4.5 LA GESTION DE LA SECURITE DU RESEAU LOGIQUE	20
	20
LE FONCTIONNEMENT DES REGLES	20
LE FONCTIONNEMENT DES REGLES DFW	21
SPOOFGUARD	22
Service Composer	22
1.5 QUELQUES DEFINITIONS	23
1.5.1 LES CLUSTERS	23
1.5.2 LES FICHIERS VIB	23

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

1.5.3 VCSA (VCENTER SERVER APPLIANCE)	23
1.5.4 LE SERVEUR SSO	24
1.5.5 LE TRAFIC NORD-SUD	24
1.5.6 Architecture Multi-tenants	24
1.5.7 TRANSPORT ZONE	25
1.5.8 PROXY ARP	25
1.5.9 VIRTUAL NETWORK IDENTIFIER(VNI)	25
1.5.10 SDDC	25
1.5.11 ARCHITECTURE EVOLUTIVE	26
<u>1.6</u> <u>PERFORMANCE</u>	27
CHAPITRE2 :	28
ÉTAPES DE L'INSTALLATION	28
2.1 <u>SCHEMA</u>	29
2.2 LA CONFIGURATION DU DISTRIBUTED VIRTUAL SWITCH(VDS)	30
2.3 VUE GENERALE	31
2.3.1 LA CONFIGURATION LOGICIELLE	32
2.3.2 LA CONFIGURATION DE ESXI1 :	32
LA CONFIGURATION DE NSX MANAGER	32
LA CONFIGURATION DU CONTROLLER	33
2.3.3 LA CONFIGURATION DE ESXI2	33
LA CONFIGURATION DE VCSA	33
2.4 INSTALLATION	34
2.4.1 INSTALLATION FT CONFIGURATION DE WINDOWS SERVER 2012 R2 ·30MIN	34
2.4.2 INSTALLATION ET CONFIGURATION DE VMWDOWS SERVER 2012 RE ISONIM	34
2.4.2 INSTALLATION ET CONFIGURATION DE VIEWARE ESAT .13-20Min	34
	25
	33
2.4.5 CONFIGURATION DUVDS	33
2.4.0 INSTALLATION ET CONFIGURATION DE VIVIWARE INSA	55
2.4.7 DEPLOIEMENT DU CONTROLLER CLUSTER	30
CHAPITRE 3 :	37
Isolation des Tenants	37
3.1 MISE EN PLACE DE L'ARCHITECTURE MULTI-TENANTS	38
3.1.1 DEMARCHE A SUIVRE	38
3.1.2 PROBLEMATIQUE	38
3.1.3 ETAPES DE L'INSTALLATION	39
3.1.4 INSTALLATION	39
CONFIGURATION DES VXLANS	39
3.1.5 CONFIGURATION DES SWITCHES LOGIQUES (LS)	39
3.2 CHOIX DE ESG	40
	40
5.2.2 IEST DE CONNECTIVITE	41

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

<u>3.3</u>	QUELLE POLITIQUE DE SECURITE CHOISIR ?	41
3.3.1	PROFIL DE MON ARCHITECTURE	41
SCHEN	MA 1	41
SCHEN	MA 2	42
3.3.2	LES REGLES DFW	42
<u>3.4</u>	DEROULEMENT DU TRAVAIL	43
3.4.1	ISOLATION DES TENANTS :	43
CONF	IGURATION	43
3.4.2	ISOLATION DE LA VM CONSOLE	44
3.4.3	AVANTAGES DE L'UTILISATION DE DFW	44
<u>3.5</u>	CONCLUSION	45
Chap	itre 4 :	46
<u>Load</u>	Balancer -SSL	46
4 1		47
4.1		47
<u>4.2</u>	MODE NON-TRANSPARENT OU ONE-ARM	48
4.2.2	Schema	48
4.2.2	CONFIGURATION	48
4.2.3	FONCTIONNEMENT	50
4.2.4	FONCTIONNEMENT DE L'ALGORITHME IPHASH :	50
<u>4.3</u>	MODE TRANSPARENT	51
4.3.1	Schema	51
4.3.2	CONFIGURATION	51
4.3.3	FONCTIONNEMENT	52
<u>4.4</u>	LE LOAD BALANCING SSL	52
4.4.1	Schema	52
4.4.2	CONFIGURATION	53
<u>4.5</u>	ANALYSE	54
<u>4.6</u>	CONCLUSION	54
<u>Chap</u>	<u>itre 5 :</u>	55
<u>Bilan</u>		55
<u>5.1</u>	LIMITES	56
<u>5.2</u>	PROBLEMES RENCONTRES	56
<u>5.3</u>	CONCLUSION GENERALE	57
_		
Anne	exes	59

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

ANNEXE 1 : PREREQUIS	60
ANNEXE2 : CONFIGURATION DE L'ACTIVE DIRECTORY	61
ANNEXE3 : PROBLEMES DE CONFIGURATION DE VCSA ET SOLUTION	62
ANNEXE 4 : VSPHERE WEB CLIENT	63
ANNEXE5 : VSPHERE NSX	65
ANNEXE 6 : COMPARAISON ENTRE UNE ARCHITECTURE NSX ET SANS NSX	68
ANNEXE7 : PRIX	70
REFERENCES	71

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

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.

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

Printemps 2016 Session de bachelor

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 ARCHITECTURE²

¹ Chapitre 1 paragraphe Définitions

² <u>https://blogs.vmware.com/networkvirtualization/2013/08/vmware-nsx.html#.V4voaGNfxAY</u>

Printemps 2016 Session de bachelor

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 STT³. GRE⁴. 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 cluster*. 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 API⁵, 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 II 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

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

1.4 FONCTIONNEMENT DES SERVICES

1.4.1 Les VXLANS



Figure 2: Trame VXLAN⁶

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.

^{. &}lt;sup>6</sup> 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'

- 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-er	ng-dhcp10 #	show	control-cluster	logical-switche	vtep-table 5000
VNI	IP		Segment	MAC	Connection-1D
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-switche	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

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

Printemps 2016 Session de bachelor

1.4.3 Le rôle des VTEP

🖣 Home 🕞 🐑 🖡	Installation							
Networking & Security	Management Host Pre	Management Host Preparation Logical Network Preparation Service Deployments						
NSX Home								
🔅 Installation	NSX Manager: 192.168.0.50							
💯 Logical Switches								
NSX Edges	VXLAN Transport Segme	ent ID Transport Zones						
📕 Firewall	Clusters & Hosts	Configuration Status	Swite	sh	VLAN	MTU	VMKNic IP Address	Teaming
na SpoofGuard	▼ Blduster1 21 06	✓ Unconfigure	DSv	vitch	0	1600	IP Pool	Static F
Service Definitions	192 168 0 3	 Ready 	20.		* 		vmk2 · 192 168 1	0.61
🔄 Service Composer	102.160.0.4	· Roody					vmk1 : 102.160.1	2.62
🛐 Data Security	9 192.108.0.4	V Ready					VITIKT : 192.108.1	0.62
🕕 Flow Monitoring	192.168.0.2	 Ready 		V	TEP —		vmk2 : 192.168.1	0.63
Activity Monitoring	192.168.0.1	 Ready 					vmk2 : 192.168.1	0.60
 Networking & Security Inventory 								
🚦 NSX Managers 📃 🔰								





- 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



Printemps 2016 Session de bachelor



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
- 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

DA MACI SA MAC2	2				
	VM	VTEP IP	VTEP SEGMENT		
	PAYLOAD MAC	192,168,10,64	MAC ID VTEP2 5000		
VM1				V	из
VXLAN 5000					MAC2
		VDS			
VTEP : 192.168.1	0.61			VTEP : 192.1	.68.10.64
	DA VTEP SA VTEP	¹ ₂ 5000	DA MAC1 SA MAC2		
ESXI3		\ \	1	ESX	14
éseau MGT			XLAN L2 IP	PAYLOAD	
		Transport 2			
	D S	A 192.168.10. A 192.168.10.	61 61		

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



Unicast Traffic

- 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.



Figure 7: Switch Logiqiue trafic unicast

1.4.5 La gestion de la sécurité du réseau logique

EDGE Firewall

ъ

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

Firewall Status: Enabled 🔟 Disable **Specify Source** ? Select one or more objects for the source field of the firewall rule vNIC Group Object Type: Ŧ Q Filter Q Filter -169 254 1 5/30 169.254.1.6/30 Available Objects Selected Objects 2240081 nic5 f) vnic6 129.194.184.11 f) vnic7 129.194.184.15 A vnic8 f) vnic9 29.194.184.12 vse 13 items 0 items Advanced options Negate Source Cancel OK

🔶 📋 🗙 📑 🚉 Hide Generated rules Show Pre rules

No.	Name	Туре	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 KERNEI 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	1 Distributed Firewall
♥3	Default Rule DHCP	* any	* any	DHCP-Client	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.

WH you want to	AT o protect		HOW you want to protect				
Secu Grou	rity ups		Se Po	curit	ty s		
New Security Group	A	PPLY T	0				
 1 Name and description 2 Define dynamic membership 3 Select objects to include 4 Select objects to exclude 5 Ready to complete 	Define dynamic membershi Specify dynamic membershi Membership criteria 1 Match Criteria Details V E	ip ip criteria that objects mus All Of the M Name Intity	t meet to be part of this criteria below Contains Belongs to	s security group.	Add		

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 HA¹⁰ ou DRS¹¹, 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.

single-tenant





multitenant



Figure 12: Architecture multi-tenants

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

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

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.



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.



¹⁴ <u>http://www.costacloud.com/cloud-software-defined-data-center.html</u>



Printemps 2016 Session de bachelor

1.6 PERFORMANCE

C:\Windows\system32\cmd.exe C:\Users\admin>ping 10.2.0.4 ctets de données : TTL=127 voi d'une requête ponse de 10.2.0.4 ponse de 10.2.0.4 ponse de 10.2.0.4 ponse de 10.2.0.4 'Ping nvoi oc tem octet octet octet = 127 tatistiques Ping pour 10.2.0.4: Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%), Durée approximative des bouclos en millisecondes : Minimum = 0ms, Maximum = 1469ms, Moyenne = 367ms :\Users\admin> C:\Users\admin>ping 10.2.0.5 Snvoi d'une requête 'Ping' 10.2.0.5 avec 32 ∘ciets de données : Délai d'attente de la demande dépassé. Statistiques Ping pour 10.2.0.5 Paquets : envoyés = 1, reçus = 0, perdus = 1 (perte 100%), Ctrl+C ^C C:\Users\admin>

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*)

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

Printemps 2016 Session de bachelor

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.



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

Printemps 2016 Session de bachelor

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 *UPLIN*K 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.



Printemps 2016 Session de bachelor

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

🗊 Ajouter et gérer les hôtes



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

Printemps 2016 Session de bachelor

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







Printemps 2016 Session de bachelor

180 MHz

3987.00 MB

368.00 MB Refresh Storage Usage

24.11 GB

24.11 GB

24.11 GB

Þ

Sta

0

Drive Type

Non-SSD

La configuration du Controller



2.3.3 La configuration de ESXI2



La configuration de VCSA

General		Resources			
Guest OS:	SUSE Linux Enterprise 11 (64-bit)	Consumed Host CPU:	(360 MHz	
VM Version:	vmx-10	Consumed Host Memory:		7828.00 M	
CPU:	2 vCPU	Active Guest Memory:		1638.00 M	
Memory:	8192 MB		R	efresh Storage Usag	
Memory Overhead:	73.82 MB	Provisioned Storage:		133.11 G	
VMware Tools:	② Running (3rd-party/Independent)	Not-shared Storage:	133.11		
IP Addresses:	192.168.0.35 View	Used Storage:		133.11 G	
		Storage 🛆	Status	Drive Type	
DNS Name:	vcenter.nsx-tdeig.com	datastore1	📀 Normal	Non-SSD	
EVC Mode:	N/A	•		P	
State:	Powered On	Natural	Trees	-	
Host:	192.168.0.2	Network	туре	2	
Active Tasks:		VM Network	Standard port gro	pup	
vSphere HA Protection:	② N/A [□]	Anagement-Net	Distributed port (group (
				T	

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 VCSA¹⁶

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 NSX¹⁸

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*.

(https://192.168.0.50/lo	gin.jsp;jsessionid=37506DC9A0	B24A1AEA52D726DA	E27749	c	Rechercher	☆ 自	↓ ∩	ø		≡
vmware NS	×									
User Pass	name: word: Logn	-	VMware≊n	ISX Manager Vi	rtual Appliance					
Summary Manage										
NSX Manager Vir	tual Appliance				CPU			Free:	: 2252 Mł	ΗZ
	Contract reserves (1) and a contract restored by the second se Second second s Second second seco				Used: 348 MHZ	1		Capacity:	: 2600 MH	ΗZ
					MEMORY			Fre	e: 8031 M	18
					Lined: 2004 MD			Conneitre	- 4400P k	40
					OSEC. 3864 ME			Capacity.	. 11330 P	20
					STORAGE				1166. 3.	20
					Used: 20G			Cap	pacity: 7′	IG
Common components				System-level compone	mts	192272				
Name	Version	Status	Rtop	Name CCLI Convico	Version	Status	6	Stop	-	
RabbitMQ		Running	Stop	SS.I DEMICE		righting		otop		
			Clob	1						
NSX Management Components	(f)									
Name	Version	Status								
NOV Management Convice	6.1.0 Build 2107742	Running	Stop							

¹⁸ <u>http://dailyhypervisor.com/vmware-nsx-for-vsphere-6-1-step-by-step-installation/</u>

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

2.4.7 Déploiement du controller cluster¹⁹

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 2^{ème} 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.

			Add Controller				?		
			NSX Manager: * Datacenter: * Cluster/Resource Pool: *		192.168.0.50	•			
tory					cluster1_nsx-tdeig				
1 >	NSX Controller no	odes	Host: Folder		192.168.0.1	•			
	🕈 🗙 🗐 🗞		Connected To:	*	Management-Netwo Chang	e R	Remove	Q Filter	
	Name	Node	IP Pool:	*	pool-Controller		Select	flware Version	NSX M
	controller-1	192.168.0.71		_				. 1.41894	19:
					ОК		Cancel		

ISX Controller nodes

🕂 🗶 🧮 🏷									
Name	Node	Status	Cluster/Resourc	Datastore	Host	Software Version	NSX Manager		
controller-1	192.168.0.71	🗸 Normal	cluster1_nsx-tde	datastore1 (1)	192.168.0.1	6.1.41894	192.168.0		

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

🛃 192.168.0.71 - PuTTY										
login as: admin				-						
admin@192.168.0.71's	s password:									
Linux htb-1n-eng-dho	cp10 3.2.39-server-nr	123 #1 SMP Mon Sep 23	16:01:54 H	PDT 2013 x						
86 64										
VMware NSX Controlle	VMware NSX Controller 4.0.6 (Build 41894)									
htb-1n-eng-dhcp10 #	show control-cluster	r status								
Туре	Status		Since							
Join status: 🤇	Join complete		07/08	14:37:01						
Majority status:	Connected to cluster	r majority	07/08	14:36:49						
Restart status:	This controller can	be safely restarted	07/08	14:37:18						
Cluster ID:	b2f190fe-102a-47e0-b	08aa-5b7820ffe239								
Node UUID:	b2f190fe-102a-47e0-b	08aa-5b7820ffe239								
Role	Configured status	Active status								
api_provider	anabled	activated								
persistence_server	enabled	activated								
switch_manager	enabled	activated								
logical_manager	enabled	activated								
directory_server	enabled	activated								
htb-1n-eng-dhcp10 #										
				-						

¹⁹ <u>http://wahlnetwork.com/2014/06/02/working-nsx-deploying-nsx-controllers-via-gui-api/</u>

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

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.

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

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 VXLANS²⁰

Management	Host Preparation	Logical Network Preparation	Service Deployments

JSX Manager: 192.168.0.50 | -

stallation of network virtualization components on vSphere hosts

Clusters & Hosts	Installation Status	Firewall	VXLAN
🛙 🛱 cluster-nsx	✓ 6.1.4 Uninstall	 Enabled 	 Enabled
192.168.0.4	✓ Ready	 Enabled 	
192.168.0.1	✓ Ready	 Enabled 	
192.168.0.2	✓ Ready	 Enabled 	
192.168.0.3	✓ Ready	 Enabled 	

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.

f Installation	Name 1 🛦	Status	Transport Zone	Segment ID	Control Plane
Logical Switches	💁 Tenant1	Normal	Transport1	5001	Unicast
NSX Edges	n Tenant2	Normal	Transport1	5002	Unicast
Firewall					
SpoofGuard	🂁 Tenant-console	🕑 Normal	Transport1	5003	Unicast

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 <u>https://pubs.vmware.com/NSX-6/index.jsp?topic=%2Fcom.vmware.nsx.admin.doc%2FGUID-DF57C441-CE9A-4138-9639-1658DBE65D48.html</u>



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 ESG²²

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.

Settings	Firewall	DHCP	NAT	Routing	Load Baland	cer VPN	SSL VPN-Plus	Grouping Objects			
 Configuration Interfaces Certificates 				Configure	e interfaces o	f this NSX Actions	Edge.	t Job(s) In Progr	ess	\rm 0 Job(s) Failed	
Cerun	Ceruncates		vNIC#	C# 1▲ Name IP Address			Subnet Prefix Length		Connected T		
			0	ir	iternet2	129.194.184.10* 129.194.184.11 S	thow All	24		Internet	
				1	in	itern	10.10.0.10*		24		Tenant1
				2	te	en2	10.20.0.10*		24		Tenant2
		3	te	en-consol	10.1.0.10*		24		Tenant-co		
				4	V	nic/					

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

Settings	Firewall	DHCP	NAT	Routir	ng 🛛 Load Bala	ancer	VPN	SSL VPN-Plus	Grou	ping Objects	J		
+ / :	× ~ e) ≣‡ (Generat	ed inter	rnal rules are	current	tly sho	wn Hide intern	al rule	s	-		
Order	Pula Is	-	Pule Tu		Action	Applia	4.0-	Original			Translated		Protocol
Older	Rule IC		Rule Ty	pe	Action	Applied On		IP Address		Port Range	IP Address	Port Range	FIOLOCOT
1	20	0710			DNAT	inte	ernet2	129.194.18	4.15	443	129.194.184.1 5	443	tcp
2	19	6609	US	ER	DNAT	inte	ernet2	129.194.18	4.13	any	10.10.0.3	any	any
3	19	6610	US	ER	DNAT	inte	ernet2	129.194.18	4.12	any	10.20.0.2	any	any
4	20	0707	US	ER	DNAT	inte	ernet2	129.194.18	4.14	any	10.20.0.4	any	any
5	20	0708	US	ER	DNAT	inte	ernet2	129.194.18	4.11	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

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

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 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:\llsers\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.



Printemps 2016 Session de bachelor

Hide Pre rules			Search	
Туре	Source	Destination	Service	Action
Internal	1 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
igure 16:Règle	es 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 2^{ème} 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 sousréseau de chaque tenant.

Tenant 🔳	P tenant1	tenant2	* any	Block
Console	* any	醒 Console - Networ	* any	Block

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



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

Printemps 2016 Session de bachelor

eventy Securi	ty rags Exclusion List Domains Grouping Objects Osers	
DUD	Edit IP Addresses ? *	Q Filter
	IP addresses grouping must be defined under the global scope or under the scope of a datacenter or a portgroup. IP address grouping defined under the global scope is visible at all datacenters and portgroups.	✓ ✓
ups	Scope: Global	
	Name: * tenant1 Description:	
	IP Addresses: * 10.10.0.1-10.10.0.20	
	eg:192.168.200.1,192.168.200.1/24, 192.168.200.1-192.168.200.24	
	Enable inheritance to allow visibility at underlying scopes	
	OK Cancel	

- 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.

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

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 IESG, 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.

Ec	lit Pool								?
	Name:	*	pool2						
	Description:								
	Algorithm:		IP-HASH		•				
	Algorithm Pa	rameters:							
	Monitors:		default https	monitor	•				
	Members:								
	+ / ×								
	Enabled	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	Min Connection.	
	~	vm2	10.20.0.2	1	80	80	0	0	
	×	vm4	10.20.0.4	1	80	80	0	0	
	✓ Transpare	ent							
							ОК	Cance	<mark>ء ا</mark>

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

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

4.2 MODE NON-TRANSPARENT OU ONE-ARM

4.2.2 Schéma



4.2.2 Configuration

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



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

ſ	Edit Profile		?	
n	Name:	profile1		
	Type:	HTTPS V		
		Enable SSL Passthrough		
	HTTP Redirect URL:			
	Persistence:	None 🔹	t	en
	Cookie Name:			
l	Mode:	•		
l	Expires in (Seconds):			
l	Insert X-Forwarded-F	or HTTP header		
l	Enable Pool Side SS	L		
l	Virtual Server Certif	icates Pool Certificates		
	Service Certificates	CA Certificates CRL		

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

Ed	it Pool									
	Name: *		pool2	pool2						
	Description:									
	Algorithm:		IP-HASH		•					
	Algorithm Pa	arameters:								
	Monitors:		default_https_monitor							
	Members:									
	Kame									
			IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	Min Connection.		
	~	vm2	10.20.0.2	1	80	80	0	0		
	×	vm4	10.20.0.4	1	80	80	0	0		

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



Printemps 2016 Session de bachelor

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

Edit Virtual Server		?
General Advanced		
Enable Virtual Ser	ver	
Enable Acceleration	n	
Application Profile:	* profile1 -	
Name:	* server1	
Description:		
IP Address:	* 129.194.184.15 🔕 Select IP Address	
Protocol:	HTTPS -	
Port:	* 443	

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

1/11/2						Send Ctrl-A	t-Delete
VIVIZ							
	Capture en cours de Co	nnexion au réseau local					×
Fic	nier Editer Vue Al	ler Capture Analyser	Statistiques Telephonie	Wireless	Outils Aide		
<u>"</u>	🔳 🔬 💿 🗎 🛅 🛛	🗙 🛅 🤇 🗢 🗢 😫	🗿 🛓 📃 🔍 Q	् 🎹			
	Appliquer un filtre d'afficha	ge <ctrl-></ctrl->		- X		Expression	+
No.	Time	Source	Destination	Protocol	Length Info		~
	5 0.001072	10.20.0.2	10.20.0.10	HTTP	986 HTTP/1.1 200 OK	(text/html)	
	6 0.001189	10.20.0.10	10.20.0.2	TCP	60 53117 → 80 [ACK]	Seq=94 Ack=934 Win=16464 Len=0	
	7 0.001359	10.20.0.10	10.20.0.2	TCP	60 53117 → 80 [FIN,	ACK] Seq=94 Ack=934 Win=16464 Len=0	
	8 0.001380	10.20.0.2	10.20.0.10	TCP	54 80 → 53117 [ACK]	Seq=934 Ack=95 Win=65536 Len=0	
	9 5.001878	10.20.0.10	10.20.0.2	TCP	66 53120 → 80 [SYN]	Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS	
	10 5.001939	10.20.0.2	10.20.0.10	TCP	66 80 → 53120 [SYN.	ACK1 Sea=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=2	
⊳	Frame 5: 986 bytes	on wire (7888 bits)	, 986 bytes captured	(7888 bits	s) on interface 0		
⊳	Ethernet II, Src: \	/mware_97:eb:08 (00:	50:56:97:eb:08), Dst:	Vmware_97	7:84:7e (00:50:56:97:84:	7e)	
⊳	Internet Protocol	/ersion 4, Src: 10.2	0.0.2, Dst: 10.20.0.1	0			
Þ	Transmission Contro	al Protocol, Src Por	t: 80 (80). Dst Port:	53117 (53	3117). Seg: 1. Ack: 94.	len: 932	

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

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

Printemps 2016 Session de bachelor

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

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

4.3.3 Fonctionnement

🙆 Ca	apture en cours de Co	onnexion au réseau local				×
Fichie	er Editer Vue A	ller Capture Analyser	Statistiques Telepho	nie Wireless	Outils Aide	
<u> </u>	🧕 🕘 🔝 🛅	🕅 🖸 🔍 👄 🔿 🕾	T 🕹 🗐 🔍	ର୍ ବ୍ 🎹		
App	pliquer un filtre d'affich	age <ctrl-></ctrl->			Expression	. +
No.	Time	Source	Destination	Protocol	Length Info	-
	22 0.004313	10.20.0.10	10.20.0.2	TCP	60 53660 → 80 [ACK] Seq=94 Ack=934 Win=16464 Len=0	
	23 0.004352	10.20.0.10	10.20.0.2	TCP	60 53660 → 80 [FIN, ACK] Seq=94 Ack=934 Win=16464 Len=0	
	24 0.004359	10.20.0.2	10.20.0.10	TCP	54 80 → 53660 [ACK] Seq=934 Ack=95 Win=65536 Len=0	
	25 0.964284	129.194.184.90	10.20.0.2	HTTP	447 GET / HTTP/1.1	
	26 0.964285	129.194.184.90	10.20.0.2	TCP	62 50800 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1	
	27 0.964405	10.20.0.2	129.194.184.90	TCP	62 80 → 50800 [SYN. ACK] Sec=0 Ack=1 Win=8192 Len=0 MSS=1460 SA	ск 🔻
▶ Fra	ame 1: 66 bytes	on wire (528 bits),	66 bytes captured	(528 bits) on	interface 0	~
⊳ Etl	hernet II, Src:	Vmware 97:84:7e (00	:50:56:97:84:7e), D	st: Vmware 97	:eb:08 (00:50:56:97:eb:08)	
⊿ In	ternet Protocol	Version 4, Src: 10.3	20.0.10, Dst: 10.20	.0.2		
	0100 = Ver	sion: 4				
	0101 = Hea	der Length: 20 bytes	5 (5)			
\triangleright	Differentiated	Services Field: 0x00	(DSCP: CS0, ECN:	Not-ECT)		
	Total Length: 5	2				-
0000	00 50 56 97 eb	08 00 50 56 97 84	7e 08 00 45 00 .	PVP V~.	.E.	
0010	00 34 74 b6 40	00 40 06 b1 da 0a	14 00 0a 0a 14 .	4t.@.@		
0020	00 02 d1 9a 00	50 ae c9 aa b8 00	00 00 00 80 02 .	P		
0030	39 08 f6 6b 00	00 02 04 05 b4 01	01 04 02 01 03 9	k		
0040	03 04					

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





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

at	Generate CSR			e (*
	Common Name:	*	NSX	
	Organization Name:	*	tdeig]
	Organization Unit:	*	4	
	Locality:	*	GE]
	State:	*	GE	
	Country:	*	Switzerland [CH]	
	Message Algorithm:		RSA ▼ Key Size: 2048 ▼	
Cli	quer ensuite sur Ge	ene	arate CSR	
	Self Sign		(*)	
	Number of days:	*	200	
			OK Cancel	4 itoma
				Titems

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

euge-test Actions •								
Summary Monitor Man	Name:	profile1						
Settings Firewall DHCE	Type:	Type: HTTPS 🔻						
		Enable SSL Passthrou	ıgh					
44	HTTP Redirect URL:							
Global Configuration	Persistence:	None						
Application Profiles	Cookie Name:							
Service Monitoring	Mode:		*					
Pools								
Virtual Servers	Expires in (Seconds):							
Application Rules	Insert X-Forwarded-F	or HTTP header						
	Enable Pool Side SSI	_						
	Virtual Server Certifi	ca Pool Certificates						
	–							
	Service Certificates CA Certificates CRL							
	Configure Service C	Configure Service Certificate						
	Common Name	Issuer	Validity					
	NSX	NSX	Wed Aug 17 2016 - Su					

(?)

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

Printemps 2016 Session de bachelor

Dans Virtual Server, choisir HTTPS au lieu de HTTP

Voici les captures prises sur le PC Client

		Centrificate Viewer:"NSX"
1	Your connection is not secure	Could not verify this certificate because the issuer is unknown.
•	The owner of 129.194.184.15 has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this	Issued To NSX Common Name (CN) NSX Organization (O) tdeig Organizational Unit (OU) 4 Serial Number 01:56:97:C9:CE:80 01:56:97:C9:CE:80
	Learn more	Issued By Common Name (CN) NSX Organization (C) teleig Organizational Unit (CU) 4 Basical of Validity
	Report errors like this to help Mozilla identify misconfigured sites	Begins On mercredi 17 août 2016 Expires On dimanche 5 mars 2017 Fingerprints
	129.194.184.15 uses an invalid security certificate.	SHA-256 Fingerprint 16:4E:85:4C:9F:82:42:A4:C3:9D:8D:3E:2B:1A:0D:1F:FE: 36:2A:ED:CB:F4:8D:8C:65:07:04:33:46:33:FE:79:51 SHA1 Fingerprint F2:A7:C4:41:21:22:83:E5:E1:AD:26:91:E1:09:82:09:6F:9E:73:5C
	The certificate is only valid for NSX Error code: SEC_ERROR_UNKNOWN_ISSUER	
	Add Exception	

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.

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

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.

Peut-on conserver les mêmes pratiques que dans un réseau physique ?

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 SSI-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



Printemps 2016 Session de bachelor

Annexes

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

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

<u>1</u>		<u> </u>	Server Manager						_ 6	X
\mathbf{E}	Server Manager • Dasl	nboard				• @ 🖡	Manage	Tools	View	Help
Da	shboard WELCOME TO SER	VER MANAGER								^
Lo	å		DNS Manager				_ D X			
	File Action View Help ← → 2	5						-		
TU DH	DNS DNS DNS DNS P Forward Lookup Zones P Trust Points Conditional Forwarders Global Logs Fill DNS Events	Name S. msdcs.vmware.local Trsx-tdeig.com	Type Standard Primary Standard Primary	Status Running Running	DNSSEC Status Not Signed Not Signed	Key Master				

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

E Server Manager								J X
Server Manager • Dash	board			• 🕲 I	Manage	Tools	View	Help
Dashboard WELCOME TO SERV	ER MANAGER							^
All File Action View Help		DNS Manager			_ _ ×			
Image: Image	Name (same as parent folder) (same as parent folder) (same as parent folder) (essi1 essi2 essi3 essi4 nsxcontroller1 swranter.Gond	Type Start of Authority (SOA) Name Server (NS) Host (A) Host (A)	Data [21], admin-nsx., hostmas admin-nsx. 192.168.0.36 192.168.0.13 192.168.0.14 192.168.0.14 192.168.0.71 192.168.0.50 192.168.0.15				Hide	2
	-	Server Manager					- 1	J X
Server Manager • Dash	board 7er manager			• ②	Manage	Tools	View	Help
Lo g		DNS Manager			_ D X			- 1
II AI II AI II AL II Action View Help II AL II → → 2 m × 20 G → 2 m II →	6							
DNS D	Name (same as parent folder) (same as parent folder) 12,168.0.1 122,168.0.13 122,168.0.14 122,168.0.2 122,168.0.36	Type Start of Authority (SOA) Name Server (NS) Pointer (PTR) Pointer (PTR) Pointer (PTR) Pointer (PTR) Pointer (PTR)	Data [37], vin-28c7bq66ic7, ho vin-28c7bq66ic7, esxi3.nsx-tdeig.com, esxi3.nsx-tdeig.com, esxi4.nsx-tdeig.com, vcenter-good.nsx-tdeig.c esxi2.nsx-tdeig.com, console.nsx-tdeig.com,				Hide	e
DNS Events	192.168.0.50	Pointer (PTR) Pointer (PTR)	nsxmanager.nsx-tdeig.com. nsxcontroller1.nsx-tdeig.c					

ANNEXE3 : PROBLEMES DE CONFIGURATION DE VCSA ET SOLUTION

nary	vCenter Server Setup	
ter	Configure Options	
er:	Database settings	
tory Service:	SSO settings	
base:	Active Directory settings	
igure Databas	Time synchronization	
om	Review configuration	✓ Configuring time synchronization
synchronizati	Configure	✓ Configuring database ★Configuring SSO
e Directory:		Failed to execute '/usr/sbin/vpxd_servicecfg 'sso' 'write' 'en 🗘
igure Time		< >
ices		★Starting vCenter Server

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							
lont/vmwa	re/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 Me	enu						
0.	Show Compared Configuration (conclusion Shift Palls Property)						
1)	Show current configuration (scroll with Shift-rgop/rgbown)						
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

Actions -			=*
Getting Started Summary Monitor	Manage Related Objects		
Hodel Processor Type: Logical Processors. Virual Machines Unitial Machines Unitial Machines Unitial Machines	HP ProLiant ML350 G6 IntelRJ Xeon(R) CPU E5620 @ 2.40GHz 2 4 Connected 0 second	CPU USED 0 Ha NEMARY USED 0 B STORAGE USED 01 GB	FREE: 19 GHz CAPACITY: 19 GHz FREE: 16 GB CAPACITY: 16 GB FREE: 207 GB CAPACITY: 265 GB
Deploy OVF Template			- 4 (*)
1 Source 10 Review details 2 Destination 2 Beliect name and folder 25 Select storage 3 Ready to complete	Select source Select the source location The Client Integration Plug-in must be installed to enable OVF function Download the Client Integration Plug-in	ctionally. Click the link below to downloa	d the installer.
		Back Next Fin	ish Cancel
	Assign Lines	ase Key	

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.

Bechercher : security.ssl3.dhe				×
Nom de l'option	 Statut 	Туре	Valeur	C9
security.ssl3.dhe_rsa_aes_128_sha	par défaut	booléen	true	
excently set3 after, rue, are, 136, stat	paar did faast	buolden boolden	true en	
				Activate Windows Go to System in Control Panel to activate Windows.
				▲ 13:31 08.05.2016



Printemps 2016 Session de bachelor

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

🚱 vSphere Web Client 🛛 🗙 🛛	🧿 lfakren Ouafae (HES) - Ou	× +								-	٥	x
🗲 🗰 े 🖲 🖗 https://192.168.0.35:944	3/vsphere-client/#extensionId=v	sphere.core.datastore	.manage.filesView;	context=com.vmv C	Q Recherche	r	☆	≜ +	Â	۹	◙	≡
Il existe des systèmes vCenter Server a	vec des clés de licence arrivées	à expiration dans vo	otre Détails								¢	•
vmware [®] vSphere Web Cli	ent 🔒 🗗		7	δIA	dministrator@V	'SPHERE.LOCAL → I Aid	a - - I	Q Re	cherch	Ð		•
🖣 Historique 🕨 🕲 🖡	Datastore1 Actions -					=						Ŧ
Datastore1 Machines virtuelles Hötes	Démarrage Résumé Su Paramètres Définitions de [Datastore1] modeles Q Recherche	urveiller Gérer É s alarmes Balises	léments associés	Fichiers Tâches planifiées		E) C' 🖿 X		🔋 Tâc	hes réc Exécutio	entes on É	⊏ chec	
	Datastore1 Oatastore1 Oatastore1 Odd.sf VMware vCenter Se NSX ManagerGood modeles	Nom	Taille	Modifié Cette liste est vide.	Туре	Chemin	Me	s tâches	▼ vail en c	Plus de ours	tâche □	6 m



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

2 10.2.3.54 - vSphere Client	_ 0 ×					
File Edit View Inventory Administration Plug-ins Help						
🔚 🔄 🏠 Home 🕨 👸 Inventory 🕨 🦉 Inventory						
10.2.5.54 HSX Manager Id List Manager Id Manager						
GNU GRUB version 0,95 (630K lower / 1904K upper memory)						
Entry:1 Slot:1 - NSX Manager						
EFFOR 16: Inconsistent filesystem structure						
Use the 7 and 4 keys to select which entry is highlighted. Press enter to boot the selected (OS or 'p' to enter a password to unlock the next set of features.						
Dans Storage, copier le chemin encadré						
2 10.2.3.54 - vSphere Client						
File Edit View Inventory Administration Plug-ins Help						
🖸 🔯 Inventory > 🕅 Inventory						
af er						
ID.2.5.54 esxil3.vmwarensx.local VMware ESXI, 5.5/b, 2403361 Evaluation (58 days remaining) Getting Ranted, Summary, Virtual Machines, Resource Allocation, Performance, Configuration, Local Users & Groupe, Events, Permissions,						

10.2.3.54 NSX Manager	essill annwarensskisal VHvare ESX 5.50, 2463361 Evaluation (28 days remaining) Fedming Samtay - Variani Hanima, Nanavarahanani, Ferningerich, Ferningerich, Samtay - Samta, Permission,						
	Hardware Health Status Processors Memory Storage Adapters Network Adapters Network Adapters	View: Datastores Refresh Delete Add Storage Rescen Al Datastores Refresh Delete Add Storage Rescen Al Identification Orive Type Capacity Pree Type Losel/Attack Hardware Acceleration iji datastore1(1) Locel/ATA Disk(t Nen-SSD 296,55 GB 273,50 GB VHPSS 26/05/2016 22100:32 Unknown					
	Advanced Settings Power Management Software Licensed Features Time Configuration Authentication Service Withial Machine Service						
	Virtual Machine Swapfie Location Virtual Machine Swapfie Location Security Profile Host Cache Configuration System Resource Allocation Agent VM Settings Advanced Settings	III III III III III III III IIII IIII IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII					

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

🔵 🔘 Objets de niveau sup 📃 🗌					
🗄 Hôtes 📃 🛛	Paramètres Mise en réseau S	Paramètres Mise en réseau Stockage Définitions des alarmes Balises Autorisations			
Machines virtuelles	44	Paramètres système avancés			Montage de VMware Tools Ins A
Banques de données 2	Machines virtuelles	1		Q Filtrer	Mettre sous tension la machir NSX Manager ::
🗊 Clusters de banques 🔲	Compatibilite VM par defat	Nom 1	▲ Valeur	Description	 Initialiser la mise sous tensio
🔍 Réseaux 📃 🚺	Démarrage/Arrêt de la VM	Power.ChargeMemoryPct	20	Pourcentage de puissance a	Datacenternsx
Distributed Switches	Paramètres de la VM agen	Power.MaxCpuLoad	60	Dans la politique personnalis	✓ Mettre hors tension la machin
	Emplacement du fichier	Power.MaxFreqPct	100	Dans une règle personnalisé	🕮 NSX Manager 🚽
Hotes	d'echange	Power.MinFreqPct	0	Dans une règle personnalisé	Mes tâches - Plus de tâches
10.2.3.52	🗢 Systême	Rower RefRise	6	Dane la notitique nereonnatie	() (m
10.2.3.54	/ 📋 10.2.3.54 - Modifier und	e option avancée		4 (S	💌 📝 Travail en cours 👘
	ScratchConfig.ConfiguredS	cratchLocation	72a22ad-44c6d66f-0c37-6805ca2	2a2c0	10.2.3.54 - Modifier
	Le répertoire configuré pou	r être utilisé pour l'espace de trava	il. Les modifications prendront effet	t lors du prochain redémarrage.	🗇 vcenternsx - Migrer
				OK Annuler	Deployer le modele O
	Parametres systeme				
	avances	ScratchConfig.CurrentScratch	. /vmts/volumes/5/2a22ad-44c	Le repertoire actuellement util	🝷 🖸 Alarmes 🛛
	Allocation de ressource	Scsi.ChangeQErrSetting	1	Changer la valeur QErr des p	Toute Nouve Recon
	systeme	Scsi.CompareLUNNumber	1	Tenir compte du numéro LUN	
	Profil de sécurité	Scsi.FailVMIOonAPD	0	E/S de machine virtuelle à éc	4 10.2.3.52
	fahanan aunthura				Utilisation de la mémoire hôte

hepia ____

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 : <u>https://[ip_VCSA]:5480</u>

Aller dans l'onglet Admin et générer un nouveau certificat SSI Rebooter VCSA VM

Configuration :

(https://192.168.0.50/hom	e.html#/manage	C Q Rechercher				
NSX North		P-1192.1680.50 Versom: 6.1.4 Build 2691049 🍎 Name: Eaxi2 User: admin				
Summary Manage						
SETTINGS	General network settings	Edit				
General	Host name	Esxi2				
Network	Domain Name	vmwarensx.local				
SSL Certificates	IPv4 Information	Unconfigure IPv4				
Backups & Restore	Address	192.168.0.50				
Upgrade	Netmask	255.255.255.0				
COMPONENTS	Default Gateway	192.168.0.10				
NSX Management Service	IPv6 Information					
	Address					
	Prefix Length					
	Default Gateway					
	DNS Servers	Unconfigure				
	To resolve all objects referenced using a hoshname, you must provide one or more DNS servers common to vCenter, ESX hosts and other vSphere components (if primary or secondary server is removed, the next available dns server in the line would assume the responsibility).					
	IPv4 DNS Servers					
	Primary Server	192.168.0.10				
	Secondary Server					
	IPv6 DNS Servers					
	Primary Server					
	Secondary Server					
	Search Domains	vmwarensx.local				



Printemps 2016 Session de bachelor

🗲 🛈 🗞 https://192.168.0.50/h	ome.html#/manage/settings/	backups		C ^d Q, Rechercher	☆ 自	↓ ☆ ⊘ ⊇
vmware NSX					IP: 192.168.0.50 Name: Esxi2	Version: 6.1.4 Build 2691049 User: admin
		Backup Location		×		
		ID1 loot nome:		_		
		ir/Host name.	192.168.0.30			
SSL Certificates	Exclude:	Port:	PTP 21	~		
Backups & Restore		liser nome:	21			
		oser name.	admin			
		Password:			File Size	
		Backup Directory:	nsxFile			
		Filename Prefix:	file			
		Pass Phrase:				
				OK Cancel	l .	
() 🖗 https://192.168.0.50/h	ome.html#/manage/compon	ents/vshield		C Q Rechercher	☆自	↓ ☆ ⊕ ♡ ≡
vmware ⁻					IP: 192.168.0.50	Version: 6.1.4 Build 2691049
NSX						User: admin
		Lookup Service		×		Unconfigure Edit
		For vCenter versions 5.1 and	above, you may configure Lookup Ser	vice and provide the SSO		a solution user. It is also
	Lookup Service:	administrator credentials to re recommended to set the NTP	egister NSX Management Service as a server for SSO configuration to work (a solution user. It is also correctly.		
		Lookup Service IP:	192.168.0.35			
		Lookup Service Port	7444			
NSX Management Service		Lookup Service:	https://192.168.0.35:7444/looku	oservice/sdk		
		SSO Administrator User Na	ame: administrator@vsphere.local			munication between NSX
		Password:				ion and Upgrade Guide'.
				OK Concel		successful configuration of
		192.100.0.55		OK Cancel		
() () (https://192.168.0.50/h	vCenter User Name: ome.html#/manage/compon	administrator@vsphere.local ents/vshield		C Q Rechercher	☆自	+ ^ @ V =
vmware [,]				- <u>1</u>	IP: 192.168.0.50	Version: 6.1.4 Build 2691049
NSX						
		vCenter Server		×		
		Connecting to a vCenter serve	er enables NSX Management Service S port (443) needs to be opened for c	to display the VMware	NSX Management Service as	
	Lookup Service:	Management Service, ESX an	nd VC. For a full list of ports required, s	ee section 'Client and User		
		If your vCenter server is hoste	ed by a vCenter Server Appliance, plea	se ensure that appropriate		
		CPU and memory reservation vCenter on NSX Manager, you	n is given to this appliance VM. After su I need to log out of any active client se	iccessful configuration of ssions on vSphere Web Client		
NSX Management Service		and log back in to enable NS	X user interface components.			
		vCenter Server:	192.168.0.35		 needs to be opened for com installation' in the 'NSX Installa 	
		vCenter User Name:	administrator@vsphere.local		ven to this appliance VM. After	
		Password:			user interface components.	
	vCenter User Name:	Modify plugin script dow	vnload location			
				OK Cancel		
🗲 🖲 🖗 https://192.168.0.50/h	ome.html#/manage/compon	ents/vshield		C Rechercher	☆ 白	* * © © =
NSX					IP: 192.168.0.50 Name: Esxi2	Version: 6.1.4 Build 2691049
Summary Manage	Lookup Service					Unconfigure Edit
General Network	For vCenter versions 5.1 recommended to set the	and above, you may configure Lo NTP server for SSO configuration	ookup Service and provide the SSO ad n to work correctly.	ministrator credentials to register	NSX Management Service as	a solution user. It is also
SSL Certificates Backups & Restore	Lookup Service: SSO Administrator Use	https://192.168.0.3 administrator@vs	35:7444/lookupservice/sdk phere.local			
Upgrade COMPONENTS	status:	Connected 2	, 			
NSX Management Service	vCenter Server Connecting to a vCenter (server enables NSX Managemer	nt Service to display the VMware Infras	tructure inventory. HTTPS port (44	3) needs to be opened for com	Edit
	Management Service, ES If your vCenter server is h	x and VC. For a full list of ports n osted by a vCenter Server Applia	equired, see section 'Client and User, ince, please ensure that appropriate C	Access' of Chapter 'Preparing for PU and memory reservation is gi	Installation' in the 'NSX Installa ven to this appliance VM. After	tion and Upgrade Guide'. successful configuration of
	vCenter Server:	192.168.0.35 administrator@webbers !!	availants on vopilere web Cite			
	Status:	Connected - Last succes	sful inventory update was on Thu, 09 J	lun 2016 17:12:44 GMT 🗯		

Printemps 2016 Session de bachelor

ANNEXE 6 : COMPARAISON ENTRE UNE ARCHITECTURE NSX ET SANS NSX²³



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



Printemps 2016 Session de bachelor



East-West Firewalling / Host to Host

UCS Fabric B UCS UCS Fabric A UCS Fabric B Falıc A Application provisioning . domain on pute Blade 1 Compute Blade 2 E Ig Blade 1 Compute L'ade 1 Compute Blade 2 VXLAN App VLAN NSX VI AN NSX VM ŇМ VM VM Edge 10.1.1.0 /24 Web Tier 10.1.1.0 /24 Web Tier 10.1.2.0/24 10.1.2.0/24 FW/LB App Tier App Tier 13 wire hops 7 wire hops

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

Printemps 2016 Session de bachelor

ANNEXE7 : PRIX

TITRE DU PRODUIT	Prix de la licence	Support et abonnement pendant 1 an		
VMware vSphere Standard	£ 020 F0	Basic	€ 257.79	
	€ 939.50	Production	€ 305.01	
VMware vSphere Enterprise Plus	€ 3,305.00	Basic	€ 693.12	
		Production	€ 825.32	
O VMware vSphere with	€ 4,155.00	Basic	€ 871.59	
Operations Management Enterprise Plus		Production	€ 1,037.79	

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



Printemps 2016 Session de bachelor

REFERENCES

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

http://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/whitepaper/products/nsx/v mware-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/convertersdk/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