MÉMOIRE

ASR – Administrateurs Systèmes et Réseaux

Philippe COMBOT
Formation ASR20 - CESI Strasbourg
2022-2023

Conception d'une offre de service de virtualisation réseau avec NSX de VMware

Responsable de formation : Laurence ROLIN

Tuteur : Daniel DAHLEN

CESI ÉCOLE D'INGÉNIEURS

Stordata vos données, notre engagement

vmware NSX-T

Philippe combot

Table des matières

REMERCIEMENTS 9

INTRODUCTION 10

1 PRESENTATION DU PROJET D'ETUDES 10

1.1 Les besoins des entreprises modernes 11

1.2 Historique de la virtualisation en datacenter 12

PRESENTATION DE L'ENTREPRISE 13

1 PRESENTATION DE STORDATA 13

2 LES CLIENTS DE STORDATA 14

3 CHIFFRES D'AFFAIRES DE STORDATA 16

4 LES CONCURRENTS DE STORDATA 16

5 AGENCE STORDATA ENTZHEIM 17

5.1 Organigramme « Professional service » 17

6 MES INTERVENTIONS 18

6.1 Les actions effectuées 18

AVANT-PROJET 19

1 ANALYSE DES BESOINS DU MARCHE 19

1.1 Etudes d'opportunité pour les entreprises 20

ETUDE DES TECHNOLOGIES 21

1 VIRTUALISATION DU RESEAU 21

1.1 Introduction 21

1.2 Pourquoi faut-il s'intéresser à la virtualisation du réseau ? 21

1.3 Principes de base de la virtualisation du réseau 22

1.4 Avantages de la virtualisation du réseau 22

1.5 Inconvénients de la virtualisation du réseau 22

1.6 Applications pratiques de la virtualisation du réseau 23

1.7 Conclusion 23

1.8 Schéma virtualisation réseau 24

2 LA MICRO-SEGMENTATION 26

2.1 Introduction 26
2.2 Définition de la micro-segmentation 26
2.3 Architecture firewall 27
2.4 Les avantages de la micro-segmentation 28
2.5 Les inconvénients de la micro-segmentation 29
2.6 Applications de la micro-segmentation 29
2.7 Schéma Micro-segmentation 30
3 COMPARAISON ACI CISCO ET NSX VMWARE 32
3.1 Fonctionnalités 32
3.2 Architecture 32
3.3 Interopérabilité 32
3.4 Fonctionnalités de sécurité 33
3.5 Facilité de déploiement 33
3.6 Tableau comparatif technique ACI Cisco et NSX VMware 34
4 COMPARAISON VXLAN ET GENEVE 35
4.1 Fonctionnalités 35
4.2 Interopérabilité 35
4.3 Performance 35
4.4 Schéma d'encapsulation de paquets 36
4.5 Comparatif des entêtes GENEVE VxLAN 37
4.6 Tableau de comparaison technique : VxLAN et GENEVE 40
4.7 Conclusion 41
5 PRESENTATION NSX 42
5.1 Introduction 42
5.2 La virtualisation du réseau avec NSX 42
5.3 Schéma Data Center 43
5.4 Principes fondamentaux de la virtualisation de réseau VMware 44
5.5 Fonctionnalités de NSX 44
5.6 Présentation des fonctionnalités principale de NSX 46
6 PRESENTATION DE PHOTON 47
6.1 Conteneurisation sous NSX 47

DEMARRAGE DU PROJET 48
1 CHARTE DE PROJET 48
2 PLANNING PREVISIONNEL DU PROJET 49
3 MATRICE DE RISQUES DU PROJET 50
4 WBS STRUCTURE DE DECOUPAGE DES ACTIVITES 53
5 PBS ORGANIGRAMME TECHNIQUE DU PROJET 54
6 OBS STRUCTURE ORGANISATIONNELLE DU PROJET 55
COUTS DES LICENCES NSX 56
1 LICENCE MAQUETTE NSX 56
2 LICENCE ENTREPRISE NSX 56
3 MAINTENANCE NSX 57
4 COUT DES EQUIPEMENTS 57
4.1 Architecture de l'infrastructure du lab 58
CONCEPTION DE LA MAQUETTE 59
1 INTRODUCTION 59
2 DESCRIPTIONS DE L'INTERFACE GRAPHIQUE (UI) DE NSX 60
3 SERVICES DE RESEAU ET DE SECURITE NSX 67
4 DISTRIBUTED VSWITCH 69
4.1 La commutation logique NSX 69
5 LE ROUTAGE LOGIQUE 71
6 DISTRIBUTED FIREWALL 72
7 EDGE NODE 73
8 LE PROTOCOLE GENEVE 74
8.1 Interface TEP (Terminal End Points) 75
8.2 Segments 75
SCHEMA ET VUE DE LA MAQUETTE 76
1 VUE PHYSIQUE 76
2 VUE LOGIQUE 77
3 VUE RESEAU 78
4 VUE RESEAU ESXI-01 78

5 VUE RESEAU ESXI-02 79
TESTS 81
1 MICRO-SEGMENTATIONS ET ROUTAGE TIER-1 /EST-OUEST 81
1.2 Création d'un segment VLAN 84
1.3 Connexion d'un segment VLAN à la Gateway TIER-1 84
2 ROUTAGE TIER-0/NORD-SUD 88
3 LA SAUVEGARDE SOUS NSX 91
4 DESINSTALLATION NSX DES HOSTS ESXI 95
5 CONCLUSION 101
BILAN 102
1 BILAN DU PROJET NSX 102
2 BILAN EN ENTREPRISE 102
3 BILAN PERSONNEL 103
4 MES PROJETS FUTURS 104
4.1 Formation et certification 104
4.2 Projet de certification NSX 105
CONCLUSION DU PROJET NSX 106
GLOSSAIRE 107
1 DEFINITIONS 107
TABLE D'ILLUSTRATIONS 110
BIBLIOGRAPHIE 111
ANNEXE TECHNIQUE DU PROJET NSX 113
1 SOCLE DE VIRTUALISATION VMWARE NSX-T 113
1.1 Cluster NSX Manager 113
1.2 Création du dvs management 113
1.3 Configuration des dvs 117
1.4 Configuration d'un distributed port group 121
2 CONFIGURATION NSX 123
2.1 vSphere Client 123
2.2 Serveurs 124

2.3 VMs 124
2.4 Virtual switches ESX01 125
2.5 Virtual switches ESX02 126
2.6 Enregistrement DNS des VM 126
2.7 Enregistrement DNS 126
2.8 Déploiement NSX Manager 127
3 VISUEL DE L'INTERFACE GRAPHIQUE NSX 133
3.1 Accueil 133
3.2 Mise en reseau 133
3.3 Sécurité 134
3.4 Inventaire 134
3.5 Planifier et dépanner 134
3.6 Systéme 135
4 ENREGISTREMENT DU VCENTER DANS NSX 135
4.1 Aller dans System / Infrastructure / Gestionnaire de calcul 135
4.2 Ajouter un gestionnaire de calcul 136
4.3 Remarque importante 136
5 CREATION DU CLUSTER NSX MANAGER 136
5.1 Aller dans System / Dispositifs / Ajouter un dispositif NSX 136
5.2 Configuration « VIP » du cluster Manager 139
5.3 Connection 140
6 CONFIGURATION TRANSPORT ZONES NSX 141
6.1 Transport Zones 141
6.2 Ajouter une zone 142
6.3 IP Pool 143
7 HOST TRANSPORT NODES 145
7.1 Ajout d'un profil de nœud de transport 145
8 CREATION DES PROFILES 150
9 CONFIGURATION SEGMENT 151
9.1 Schéma segments et gateway 154
10 CONFIGURATION DES VM 154

10.1 Vm1 155
10.2 Vm2 155
11 DEPLOIEMENT EDGE NODE 155
11.1 Création du segment pour les deux nœud edges 155
11.2 Création des nœuds edges 156
11.3 Création du cluster Edge 159
12 ROUTAGE TIER-1 / EST-OUEST 161
12.1 Gateway TIER-1 161
12.2 Connexion des segments 162
12.3 Tests 163
13 ROUTAGE TIER-0 / NORD-SUD 164
13.1 Segments d'uplink 164
13.2 Gateway TIER-0 165
14 CONFIGURATION SAUVEGARDE NSX 170
14.1 Configuration 170
14.2 Utilisation 171
14.3 Verification de la sauvegarde sur le serveur 171
15 DESINSTALLER NSX DES HOSTS 172
15.1 Conditions préalables 172
15.2 Procédure 173
15.3 Vérifiez que NSX-T Data Center est supprimé de l'hôte. 174
16 TROUBLESHOOTING NSX 177
16.1 Error 503 177
16.2 Tester la connectivité entre deux VM 177
16.3 Probleme de MTU 178
17 MOB MANAGEMENT OBJECT REFERENCE 179
17.1 Présentation 179

CESI
ÉCOLE D'INGÉNIEURS

FICHE DE CONFIDENTIALITE
DES RAPPORTS, MEMOIRES, THESES ET SOUTENANCES PROFESSIONNELS

Formation/qualification préparée : Bachelor

Nom-Prénom du stagiaire : COMBOT Philippe

Titre du dossier professionnel : Conception d'une offre de service de virtualisation réseau avec NSX de VMWARE

Date de la soutenance : 04/10/23

Nom de l'entreprise : STORDATA

Nom et qualité du représentant de l'entreprise : DAHLEN Daniel - Chef de projets

Noms, entreprises et fonctions des membres de jury :

Nom-Prénom	Entreprise	Fonction

Mode de diffusion autorisé
(Cocher la case correspondante)

☒ **Diffusion libre**
Le dossier est conservé en archives au CESI, il peut être librement consulté et reproduit. Il peut être utilisé par les destinataires, les études peuvent faire l'objet de publication....

☐ **Diffusion limitée au CESI**
Les membres du jury rendent leur exemplaire au stagiaire à la fin de la soutenance. Le stagiaire est responsable de cette restitution. Un exemplaire est conservé en archives au CESI. Le dossier peut être consulté pour exemple ou illustration par les stagiaires des promotions suivantes mais il ne peut être ni sorti du CESI, ni reproduit, sauf autorisation expresse de l'auteur et de son entreprise. La mention « Diffusion limitée au CESI, reproduction interdite » doit figurer sur la page de garde.

☐ **Diffusion interdite**
Les membres du jury rendent leur exemplaire au stagiaire à la fin de la soutenance. Le stagiaire est responsable de cette restitution. Un exemplaire est conservé au CESI, à titre de preuve dans le dossier pédagogique du stagiaire. Le dossier ne peut être ni consulté, ni sorti du CESI, ni reproduit, sauf autorisation expresse de l'auteur et de son entreprise. La mention « Diffusion et reproduction interdites » doit figurer sur la page de garde.

Signatures :

Pour l'entreprise | **Le stagiaire** | **Le CESI**

Remerciements

Je tiens à exprimer ma profonde gratitude envers les personnes qui ont marqué mon parcours de manière inoubliable :

D'abord, je remercie chaleureusement **Daniel DAHLEN** pour sa grande humanité et sa bienveillance à mon égard.

Ensuite, je suis infiniment reconnaissant envers **Marc PEREIRA**, pour son altruisme et sa gentillesse.

Stéphane HEIMLICH mérite également toute ma reconnaissance pour son aide précieuse et son écoute attentive.

David MALAURE a joué un rôle clé dans mon parcours grâce à ses conseils avisés et son expertise technique.

Gaelle CUENOT m'a prodigué une écoute sincère et une aide précieuse, je lui en suis très reconnaissant.

Jérôme COUSIN mérite une mention spéciale pour la confiance qu'il m'a accordée et pour m'avoir confié un projet stimulant et enrichissant.

Cristelle BOURNET a fait preuve d'une disponibilité exemplaire, d'une écoute attentive et d'une bienveillance qui m'ont profondément touché.

Je tiens à exprimer ma gratitude envers le **SERVICE RH**, qui s'est toujours montré aux petits soins à mon égard.

Un merci particulier au PDG, Monsieur **Olivier TEICHMAN**.

Enfin, je souhaite exprimer ma reconnaissance envers la société **STORDATA** dans son ensemble, ainsi qu'à toutes les personnes qui m'ont accompagné tout au long de mon projet d'étude.

En terminant, mes remerciements vont au CESI, et tout particulièrement à **Laurence ROLLIN**, **Sophie METZ** et **Boris MALLICK** pour leur soutien permanent durant ma recherche d'entreprise et mon année scolaire.

Votre aide a été inestimable dans mon parcours et je vous en remercie.

Introduction

1 Présentation du projet d'études

La virtualisation du réseau est devenue un élément clé dans la conception et la gestion des infrastructures informatiques modernes.
Elle permet de créer des environnements virtuels flexibles, évolutifs et hautement sécurisés, répondant aux exigences croissantes des entreprises.

Dans ce contexte, NSX de VMware émerge comme une solution de virtualisation du réseau à la pointe de la technologie, offrant une gamme complète de fonctionnalités avancées pour la création et la gestion de réseaux virtuels.

Ce mémoire se concentre sur l'étude et l'implémentation d'une maquette NSX dans le but de comprendre les avantages et les possibilités qu'elle offre aux entreprises.
NSX permet de virtualiser le réseau, en séparant la gestion du réseau de son infrastructure physique sous-jacente.

Il offre une approche basée sur les logiciels pour créer et gérer des réseaux virtuels, ce qui simplifie la configuration, l'administration et la sécurité du réseau.
Mon objectif principal est d'explorer les différentes fonctionnalités de NSX et d'évaluer son impact sur les performances, la sécurité et la flexibilité des infrastructures réseau.

Nous étudierons également les cas d'utilisation courants de NSX, tels que la micro-segmentation, la mise en place de réseaux étendus virtuels (GENEVE), la gestion centralisée du réseau, ainsi que son intégration avec d'autres solutions logicielles et matérielles.

Je vise à fournir une analyse approfondie des fonctionnalités de NSX, ainsi que des bonnes pratiques pour sa mise en œuvre.
Nous examinerons les avantages et les défis associés à l'adoption de NSX, en mettant l'accent sur son impact sur la sécurité, la flexibilité et l'efficacité opérationnelle des infrastructures réseau.

1.1 Les besoins des entreprises modernes

Les défis de l'industrie se sont accrus brutalement en raison de la nécessité pour l'utilisateur, de passer d'un environnement rigide axé sur le matériel à un environnement agile et axé sur le logiciel.

Ce qui permet une automatisation des règles, une indépendance vis-à-vis du cloud, des plateformes logicielles uniques, et une sécurité distribuée.
Le réseau cloud virtuel est la vision du futur pour l'ère numérique.

L'impératif est de faire en sorte que l'expérience du data center soit similaire à celle d'un cloud public, avec une architecture permettant aux utilisateurs de se connecter en réseau de n'importe où.
Les réseaux et les modèles de sécurité traditionnels se sont avérés trop rigides et bloque les changements rapides.

Les réseaux et la sécurité doivent s'adapter à ce nouveau monde.
Les entreprises ont commencé à s'adapter à ce besoin de rapidité et de changement en utilisant des cloud publics qui offrent de l'agilité et des opérations simplifiées.
La nature du travail a changé et la frontière entre le bureau et le domicile tend à s'estomper.

Le réseau et la sécurité doivent fusionner pour offrir aux utilisateurs un accès transparent, sécurisé et fiable.
L'un des moyens de répondre à cette demande croissante d'agilité, est le réseau cloud virtuel, qui offre une architecture de réseau et de sécurité adaptée à l'ère numérique.

1.2 Historique de la virtualisation en datacenter

Pour apprécier pleinement la nature transformatrice de NSX, il est important de comprendre les changements qui ont eu lieu dans les data centers au cours des dernières décennies.
Avant la virtualisation le déploiement d'un serveur (Workload) était physique, statique et manuelles.

Un administrateur installé un système d'exploitation et une application sur un serveur physique dans un rack de data center.
Les nouveaux serveurs nécessitaient que l'administrateur contacte les équipes réseaux et sécurité, pour créer une nouvelle infrastructure réseau et définir des règles de sécurité.

Comme ces processus étaient en grande partie manuelle, ils prenaient généralement des jours, voir des semaines.
Ceux qui augmentaient le temps nécessaire pour fournir les services à l'entreprise.
La nature des serveurs traditionnelles et leur schéma de trafic réseau sont différents de ceux des applications modernes.

La grande majorité du trafic réseau transité par le cœur de réseau vers le réseau étendu.
Ce modèle de flux de trafic est appelé trafic Nord-Sud.
Dans ces environnements, il était pratique de fournir des services réseaux tels que le routage de couches 3, et la surveillance de la qualité de service (QoS).

Les changements apportés en partie par la virtualisation ont considérablement modifié ce modèle nécessitant une réévaluation de la façon dont le réseau et la sécurité du data center pourrait être amélioré.

Présentation de l'entreprise

1 Présentation de Stordata

Stordata est une entreprise française spécialisée dans les solutions de stockage de données pour les entreprises.
Créée en 2004, elle a rapidement grimpé les échelons pour devenir l'un des leaders du marché grâce à son expertise en matière de stockage de données, de sécurité informatique et de gestion de projets complexes.

En 2023, l'entreprise compte plus de 170 employés et a généré un chiffre d'affaires de plus de 90 millions d'euros.
Stordata propose une gamme de produits et de services variée, allant de la conception de centres de données clé en main à la mise en place de solutions de stockage de données pour les entreprises de toutes tailles.

L'entreprise travaille avec une grande variété de clients, des start-ups aux grandes entreprises, en passant par les organisations gouvernementales et les institutions financières.
Les solutions proposées par Stordata sont personnalisables pour répondre aux besoins spécifiques de chaque client, grâce à sa capacité à offrir des solutions innovantes qui tirent parti des dernières avancées technologiques.
En termes de sécurité et de conformité, Stordata s'engage à garantir la protection des données de ses clients.

Ses solutions de sécurité informatique sont conçues pour protéger les données contre les cyberattaques et les menaces internes.
L'entreprise travaille également en étroite collaboration avec ses clients pour s'assurer que leurs données respectent les réglementations en vigueur.
Stordata à la capacité de gérer des projets complexes.
Ses solutions sont évolutives, ce qui leur permet de s'adapter aux besoins en constante évolution des entreprises.

L'entreprise s'appuie sur une équipe de professionnels hautement qualifiés qui sont continuellement formés pour offrir des solutions de pointe.
Les employés de Stordata sont passionnés par leur travail et sont engagés à fournir un service client exceptionnel.

En tant qu'entreprise responsable, Stordata est également engagée dans des initiatives environnementales et sociales.
Elle adopte des pratiques durables pour réduire son empreinte carbone et minimise son impact sur l'environnement.

L'entreprise travaille en partenariat avec des organisations à but non lucratif pour soutenir les communautés locales et les initiatives de développement durable.

2 Les clients de Stordata

Les clients de Stordata sont issus de divers secteurs tels que la finance, la santé, l'éducation, l'automobile et les services publics.
Elle travaille avec de grands groupes internationaux, mais également avec des PME et des entreprises locales.

Dans le secteur financier, Stordata propose des solutions de stockage sur mesure pour les banques, les compagnies d'assurance et les fonds d'investissement.
Ces clients ont besoin d'une solution rapide et sûre pour stocker des quantités massives de données transactionnelles, tout en respectant les règlementations en vigueur.

Dans le secteur de la santé, Stordata fournit des solutions de stockage pour les hôpitaux, les cliniques et les laboratoires de recherche.
Les clients ont besoin d'une solution pour stocker des données volumineuses telles que des images médicales, des dossiers de patients et des résultats d'analyse de laboratoire, tout en garantissant la sécurité et la facilité d'accès par les professionnels de santé autorisés.

Les solutions de Stordata pour le secteur de l'éducation permettent aux universités, aux écoles et aux établissements d'enseignement supérieur de stocker des quantités massives de données en toute sécurité, telles que les données de recherche, les dossiers étudiants et les ressources pédagogiques en ligne.

Dans le secteur automobile, Stordata fournit des solutions de stockage pour les données de conception et de fabrication, ainsi que pour les données de diagnostic des véhicules.

Les clients du secteur des services publics, tels que les fournisseurs d'énergie, les services de transport et les services de communication, ont besoin de solutions de stockage pour stocker des quantités massives de données de manière fiable et sécurisée.

Tableau 1.Clients Stordata

3 Chiffres d'affaires de Stordata

Pour l'année 2021/2022, le chiffre d'affaires de Stordata s'élevé à 90 millions d'euros. C'est une performance qui témoigne de la qualité de ses produits et services.

De plus, l'entreprise compte sur une équipe de 170 personnes, ce qui prouve son dynamisme et sa capacité à faire face aux défis du marché.

Stordata est un acteur majeur dans son domaine et ses résultats financiers en sont la preuve.

4 Les concurrents de Stordata

La société Stordata, dont les bureaux sont répartis à Versailles, Strasbourg, ainsi que dans plusieurs autres villes de France, évolue dans le secteur de l'informatique de stockage et de la sécurité des données.
Dans son environnement concurrentiel, plusieurs acteurs de renom se démarquent également en proposant des services et des produits similaires.

Econocom, un acteur majeur de l'informatique et des services numériques, se positionne également comme un concurrent sérieux à Strasbourg.

Leurs solutions couvrent l'infrastructure IT, les services cloud, la gestion de la mobilité et la transformation digitale.

De plus, nous pouvons citer des acteurs régionaux plus spécialisés tels que :

- Atheo
- OCI
- SCC

Qui offrent des solutions de gestion IT, de cybersécurité et d'assistance aux utilisateurs.

5 Agence STORDATA Entzheim

5.1 Organigramme « Professional service »

Au sein de notre agence située à Strasbourg/Entzheim, nous formons une équipe de neuf.

Parmi eux figurent :

- Marc PEREIRA, notre ingénieur système.
- Daniel DAHLEN, notre chef de projet.
- Stéphane HEIMLICH, autre ingénieur système.

Pour garantir une expertise complète en matière de réseau et de sécurité, nous avons deux ingénieurs spécialisés :

- Gael CUENOT.
- David MALAURE.

Notre assistante commerciale :

- Canan BAKIR

Support technique :

- Emmanuel GRETH.

Notre commercial :

- Thierry SCHAAL

Pour finir en tant qu'administrateur système et réseau, je m'appelle Philippe COMBOT.

6 Mes interventions

6.1 Les actions effectuées

Pendant mon parcours professionnel, j'ai participé à des interventions diverses et enrichissantes qui ont renforcé mes compétences et approfondi mon expertise dans le domaine informatique.

Voici un résumé détaillé de mes réalisations :

Élaboration de scripts Ansible : J'ai activement contribué à la conception et à l'écriture de scripts Ansible. Ces outils d'automatisation ont été déployés pour simplifier et accélérer les tâches récurrentes au sein de l'infrastructure. Grâce à ces scripts, j'ai pu automatiser des processus tels que la configuration des serveurs, le déploiement d'applications et les mises à jour système. Cette approche a non seulement amélioré l'efficacité opérationnelle, mais a également réduit les risques d'erreurs humaines, renforçant ainsi la stabilité et la sécurité du système.

Maintenance en Datacenter : Mon implication dans des activités de maintenance en Datacenter m'a permis d'acquérir une expérience précieuse dans la gestion et la surveillance des équipements informatiques critiques. J'ai participé à des tâches telles que la vérification régulière des composants, le remplacement des pièces défectueuses, la mise à jour des firmwares et la gestion des sauvegardes. Cette approche préventive et corrective a joué un rôle essentiel dans la garantie de la disponibilité et de la fiabilité des infrastructures, en minimisant les temps d'arrêt et en assurant une continuité de service optimale.

Déploiement de solutions réseau : J'ai pris part activement à des projets de déploiement de solutions réseau, qui ont impliqué la mise en place d'architectures innovantes et la configuration minutieuse des équipements réseau. Lors de ces déploiements, j'ai également joué un rôle clé dans la résolution des problèmes liés à la connectivité et j'ai participé au remplacement d'équipements obsolètes par des solutions plus modernes et performantes. Mon objectif était de garantir la mise en œuvre efficace des nouvelles infrastructures réseau tout en minimisant les interruptions pour les utilisateurs, assurant ainsi une transition fluide et transparente.

Ces diverses interventions ont été des opportunités pour appliquer mes connaissances théoriques à des situations réelles, développant ainsi une expertise pratique et concrète.
Elles m'ont permis de réaliser l'importance cruciale de la collaboration, de la planification méticuleuse et de la résolution proactive des problèmes dans le domaine de l'informatique.
J'ai été témoin des retombées concrètes de ces actions, tant en termes d'efficacité opérationnelle que de satisfaction des utilisateurs, et cela m'a encouragé à poursuivre mon engagement envers l'excellence dans tous les aspects de mon travail.

Avant-Projet

1 Analyse des besoins du marché

L'analyse des besoins du marché révèle que de nombreuses entreprises sont à la recherche d'une solution de virtualisation du réseau qui leur permette de simplifier et d'automatiser la gestion de leur infrastructure tout en garantissant la sécurité de leurs données.

NSX répond à ces besoins en offrant une plateforme de virtualisation complète et évolutive qui permet de créer et de gérer des réseaux virtuels à grande échelle, en toute simplicité et en toute sécurité.

Dans ce marché en évolution rapide, les fournisseurs de solutions de virtualisation doivent être en mesure de proposer des solutions qui répondent aux besoins spécifiques des clients de toutes tailles.

NSX est une solution de virtualisation de réseau flexible et adaptative qui répond à ces exigences.
NSX permet de créer des réseaux virtuels complexes pour les grandes entreprises.
De plus, NSX offre des fonctionnalités de sécurité avancées, telles que le pare-feu distribué et le chiffrement du trafic réseau, pour répondre aux exigences de sécurité des clients.

Les entreprises recherchent également des solutions de virtualisation de réseaux qui peuvent s'intégrer avec les technologies existantes, telles que les infrastructures de cloud computing.

NSX offre une intégration transparente avec les plateformes de cloud computing telles que AWS, Azure et Google Cloud, ainsi qu'avec les plateformes de conteneurisation telles que Kubernetes.

1.1 Etudes d'opportunité pour les entreprises

L'étude d'opportunité effectuer sur la solution NSX de VMware pour la France révèle un potentiel de marché important pour cette technologie.
Les avantages de la solution NSX de VMware sont multiples :

une sécurité renforcée grâce à la segmentation du réseau,
une gestion centralisée facilitant la configuration et la mise à jour des équipements, ainsi qu'une réduction des coûts grâce à la virtualisation des fonctions réseau.

Une analyse du marché français a montré que de nombreuses entreprises sont déjà engagées dans une démarche de virtualisation de leur infrastructure.
Les résultats montrent que la solution NSX de VMware est bien positionnée sur le marché en termes de fonctionnalités et de coût.

La concurrence est forte avec la solution ACI de Cisco qui offre une automatisation plus poussée et une orchestration avancée
Cette étude d'opportunité pour la France montre un marché porteur pour cette technologie.
La solution NSX est compétitive en termes de fonctionnalités et de coût par rapport à la concurrence, bien que la solution ACI de Cisco soit un concurrent de taille.

Etude des technologies

Au moyen de cette analyse approfondie des technologies, mon objectif est de vous fournir les connaissances essentielles pour une meilleure appréhension des concepts liés à la virtualisation, aux réseaux et aux protocoles réseau.

1 Virtualisation du réseau

1.1 Introduction

La virtualisation du réseau est une technologie qui transforme la manière dont les réseaux sont conçus, gérés et utilisés.
Elle permet de créer des réseaux virtuels qui sont indépendants de l'infrastructure physique sous-jacente, ce qui offre de nombreux avantages en termes de flexibilité, d'agilité et d'efficacité.
Nous allons explorer la virtualisation du réseau en détail, en examinant ses principes de base, ses avantages et ses inconvénients, ainsi que ses applications pratiques.

1.2 Pourquoi faut-il s'intéresser à la virtualisation du réseau ?

La virtualisation du réseau est une technique qui permet de créer des réseaux virtuels sur un même matériel physique, offrant ainsi de nombreux avantages pour les entreprises.

Économies de coûts : Diminution des dépenses liées à l'acquisition et à la maintenance opérationnelle.

Flexibilité et agilité accrues : La virtualisation du réseau permet de créer et de modifier rapidement des réseaux virtuels pour répondre aux évolutions des besoins de l'entreprise.

Amélioration de la sécurité : La virtualisation permet de mettre en place de la micro-segmentation rendu possible et facilité par la notion de pare-feu distribué réseau pour améliorer la sécurité de l'infrastructure.

Meilleure utilisation des ressources : La virtualisation du réseau permet de mieux utiliser la couche physique sous-jacente du réseau.

Simplification de la gestion du réseau : La virtualisation du réseau simplifie la gestion du réseau en centralisant la configuration et le suivi des différents éléments du réseau.
Avec un SDDC (Software Defined Data Center) qui désigne un datacenter dans lequel l'infrastructure est virtualisée par abstraction et mise en commun des ressources.

L’infrastructure software-defined permet aux administrateurs informatiques de provisionner et de gérer facilement l’infrastructure physique à l’aide de modèles software-defined et d’API servant à définir et automatiser la configuration de l’infrastructure et les opérations de gestion de cycle de vie.
Il est maintenant possible d’installer et d’exploiter une application en quelques minutes.
Cette approche de la virtualisation est en fait un cadre indispensable pour améliorer l’agilité et la réactivité des services informatiques, le tout à un cout réduit.

1.3 Principes de base de la virtualisation du réseau

La virtualisation du réseau est basée sur la séparation de la couche de management et de la couche control plane.
La couche de management est responsable de la gestion et de la configuration du réseau, tandis que la couche control plane transporte les données entre les différents nœuds du réseau.

En virtualisant ces deux couches, il est possible de créer des réseaux virtuels qui peuvent être configurés, gérés et utilisés de manière indépendante de l'infrastructure physique sous-jacente.

Cela offre une grande flexibilité et une grande agilité dans la gestion des réseaux, car les différents réseaux virtuels peuvent être configurés et gérés de manière indépendante, sans perturber les autres réseaux qui partagent la même infrastructure physique.

1.4 Avantages de la virtualisation du réseau

La virtualisation du réseau offre de nombreux avantages par rapport aux réseaux traditionnels.
Tout d'abord, elle permet une meilleure utilisation des ressources, car plusieurs réseaux virtuels peuvent être créés sur une même infrastructure physique, ce qui permet d'économiser de l'espace et des coûts.

De plus, elle offre une plus grande flexibilité dans la gestion des réseaux, car les réseaux virtuels peuvent être configurés et gérés de manière indépendante, sans perturber les autres réseaux.

La virtualisation du réseau offre également une grande agilité dans la gestion des réseaux, car elle permet de déployer des réseaux virtuels rapidement et facilement, sans avoir à ajouter de nouveaux équipements physiques.
Elle offre également une meilleure sécurité, car les réseaux virtuels peuvent être isolés les uns-des-autres, ce qui empêche la propagation des attaques.

1.5 Inconvénients de la virtualisation du réseau

La virtualisation du réseau présente également quelques inconvénients.
Elle peut être complexe à gérer, en particulier dans les environnements de grande envergure.

La gestion de plusieurs réseaux virtuels peut être compliquée et nécessiter des compétences spécifiques, ce qui peut augmenter les coûts de gestion.

1.6 Applications pratiques de la virtualisation du réseau

La virtualisation du réseau a de nombreuses applications pratiques dans les environnements informatiques modernes.

Elle est couramment utilisée dans les centres de données pour créer des réseaux virtuels pour les différentes applications et services qui y sont hébergés.
Elle est également utilisée dans les réseaux d'entreprise pour créer des réseaux isolés pour les différents départements ou équipes de l'entreprise.

La virtualisation du réseau est également utilisée dans les réseaux de télécommunications pour créer des réseaux virtuels qui permettent de segmenter le trafic et d'optimiser les performances.

Elle est également utilisée dans les réseaux de fournisseurs de services pour offrir des services de réseaux privés virtuels aux clients.

1.7 Conclusion

La virtualisation du réseau est une technologie qui offre de nombreux avantages en termes de flexibilité, d'agilité et d'efficacité dans la gestion des réseaux.

Elle permet de créer des réseaux virtuels qui sont indépendants de l'infrastructure physique sous-jacente, ce qui permet de mieux utiliser les ressources et de simplifier la gestion des réseaux.

La virtualisation du réseau est utilisée dans les environnements informatiques modernes, en particulier dans les centres de données, les réseaux d'entreprise et les réseaux de fournisseurs de services.

1.8 Schéma virtualisation réseau

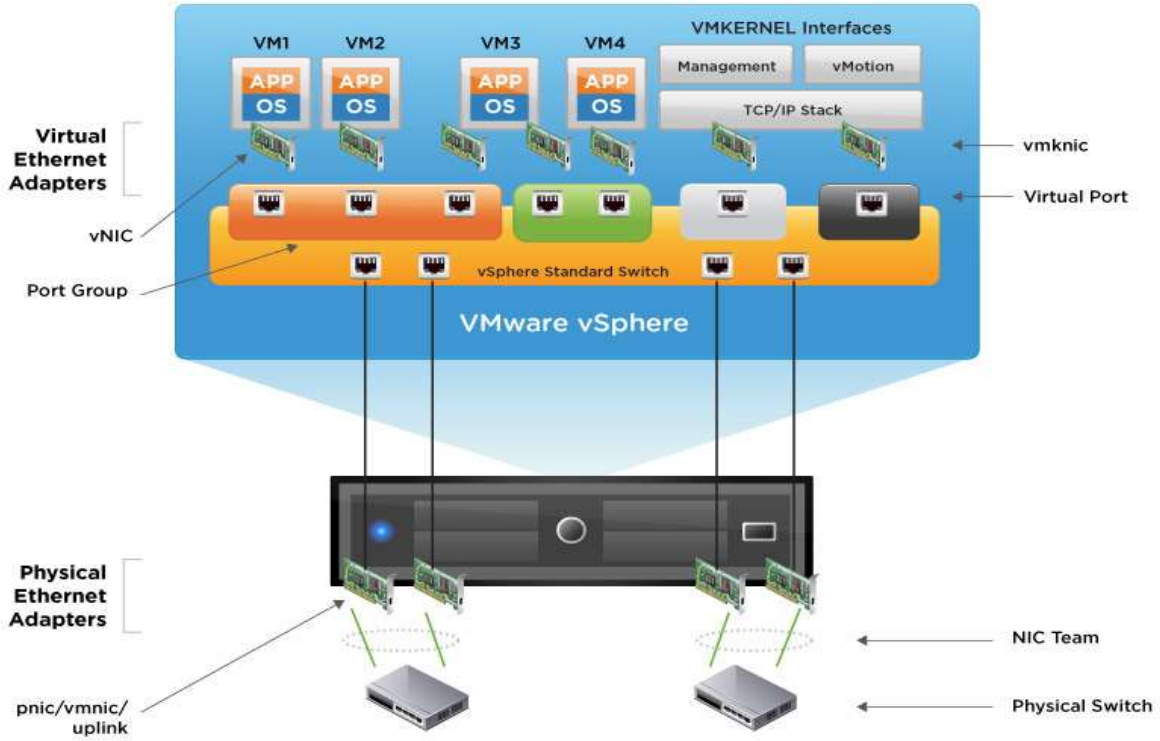


Figure 1.Virtualisation du réseau

Cette perspective dévoile un panorama complet des éléments qui contribuent à la virtualisation du réseau.
Elle englobe d'abord la composante du réseau physique du serveur, les uplinks (Adaptateurs Ethernet Physiques) qui connectent le monde réel au monde virtuel.

Elle englobe également la dimension virtualisée, comprenant les vNICs (cartes réseau virtuelles associées aux machines virtuelles), les groupes de ports (Virtual Port Groups) qui permettent de gérer le trafic au niveau virtuel, les vmknics utilisés pour les services de gestion, et les interfaces VMKERNEL qui facilitent la communication entre le système d'exploitation et l'hyperviseur.

En bas de la hiérarchie, nous trouvons la composante physique représentée par les commutateurs (Physical Switches) qui gèrent le trafic au niveau matériel, assurant ainsi une connectivité transparente entre les ressources virtuelles et le monde extérieur.

Explications technique des thermes de virtualisation abordé :

VMknic (Virtual Machine Kernel Network Interface Card)
Une VMknic, est une interface réseau virtuelle qui est utilisée dans l'environnement de virtualisation.
Elle permet la communication entre les machines virtuelles et les composants du noyau de l'hyperviseur.
Les VMknic sont associées à des services tels que la gestion du stockage, la gestion de la migration, et d'autres fonctions essentielles pour les machines virtuelles.

VMkernel
VMkernel est la couche logicielle de l'hyperviseur qui fonctionne directement sur le matériel physique de l'ordinateur hôte.
Elle est responsable de la gestion des ressources matérielles et des opérations de bas niveau nécessaires pour exécuter les machines virtuelles.
Elle gère également les connexions réseau, le stockage, et d'autres fonctionnalités de la virtualisation.
Elle agit comme une interface entre les machines virtuelles et le matériel physique, garantissant ainsi une exécution efficace et isolée des machines virtuelles sur un même hôte.

Uplink
Un uplink, également appelé lien montant, désigne une connexion réseau qui relie un périphérique ou un composant à un réseau ou à un système plus large.
Il s'agit généralement d'une liaison de données sortante, permettant au périphérique de transmettre des informations vers un réseau central ou vers un autre périphérique.

Switch réseau
Un switch réseau, également appelé commutateur réseau, est un équipement informatique essentiel dans les réseaux de communication.
Il fonctionne au niveau de la couche de liaison de données (couche 2) du modèle OSI (Open Systems Interconnection).
Son rôle principal est de relier et de diriger le trafic réseau entre les différents périphériques, tels que les ordinateurs, les imprimantes, les serveurs, et d'autres appareils au sein d'un réseau local (LAN).

2 La Micro-segmentation

2.1 Introduction

Le monde de la sécurité informatique est en constante évolution et les cybercriminels deviennent de plus en plus sophistiqués dans leurs attaques.
Les entreprises doivent donc trouver des moyens de protéger leur environnement informatique contre les menaces émergentes.

Dans ce contexte, la micro-segmentation est une technologie de sécurité qui est devenue de plus en plus populaire ces dernières années.
Nous allons étudier la micro-segmentation et son rôle dans la sécurité informatique, ses avantages et ses inconvénients, ainsi que les meilleures pratiques pour mettre en œuvre cette technologie de manière efficace.

2.2 Définition de la micro-segmentation

La micro-segmentation est une technique de sécurité qui permet de diviser un réseau en segments logiques.
Cette technique consiste à isoler chaque segment de manière à restreindre l'accès aux ressources critiques et à protéger les applications et les données contre les attaques malveillantes.

En d'autres termes, la micro-segmentation permet de créer une couche de sécurité supplémentaire en limitant le trafic entre les segments du réseau.
Cette technique est différente de la segmentation traditionnelle, qui se contente de diviser les réseaux en sous-réseaux. La micro-segmentation est plus fine et permet de segmenter les réseaux à un niveau plus granulaire.

La micro-segmentation est une technique de pointe qui permet de diviser un réseau en segments plus petits et plus gérables, appelés micro-segments.
Cette technique permet d'isoler et de protéger les machines virtuelles sur un réseau en utilisant des politiques de sécurité granulaires pour protéger les ressources

2.3 Architecture firewall

2.3.1 Architecture firewall classique

Un pare-feu constitue un dispositif de sécurité du réseau, exerçant une surveillance tant sur les données entrantes que sortantes.

Un pare-feu analyse le flux et en fonction des critères défini par les règles de sécurité, bloque ce flux ou le laisse passer.

À partir d'un ensemble prédéterminé de règles de sécurité, il prend la décision de consentir ou d'entraver une fraction spécifique de ce flux de données.

Cette composante revêt une importance substantielle au sein d'une infrastructure informatique, assurant la sécurité aussi bien du réseau que des informations qui le parcourent.

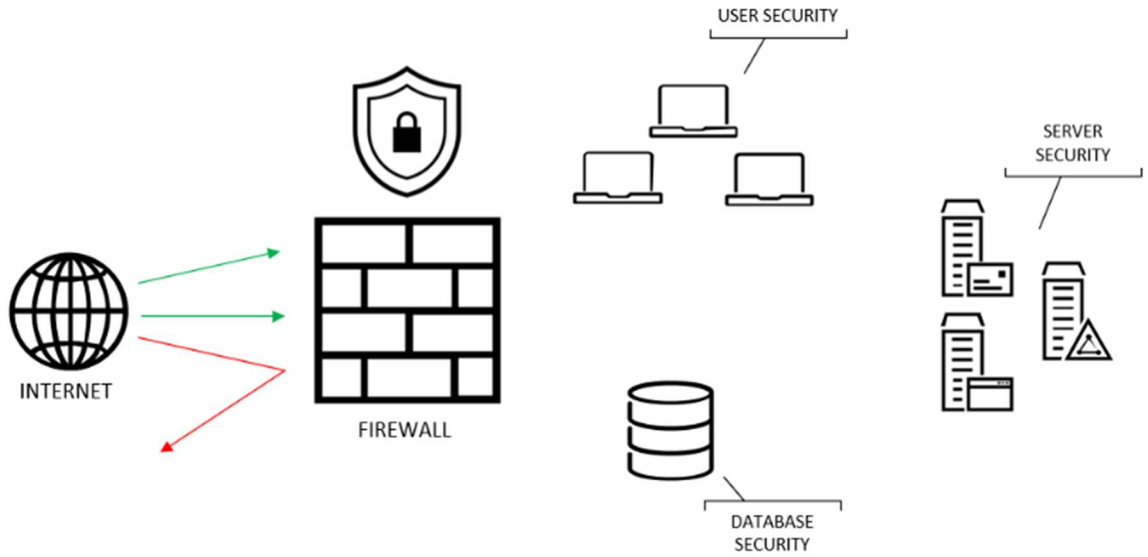


Figure 2.Firewall classique

2.3.2 Architecture firewall distribué

Dans cet exemple, à la différence du premier schéma on retrouve des pares-feux distribue en plus du pare-feu principale.

On retrouve une méthode plus granulaire de filtrage grâce à la micro-segmentation (segment) et au pare-feu distribué(DFW).

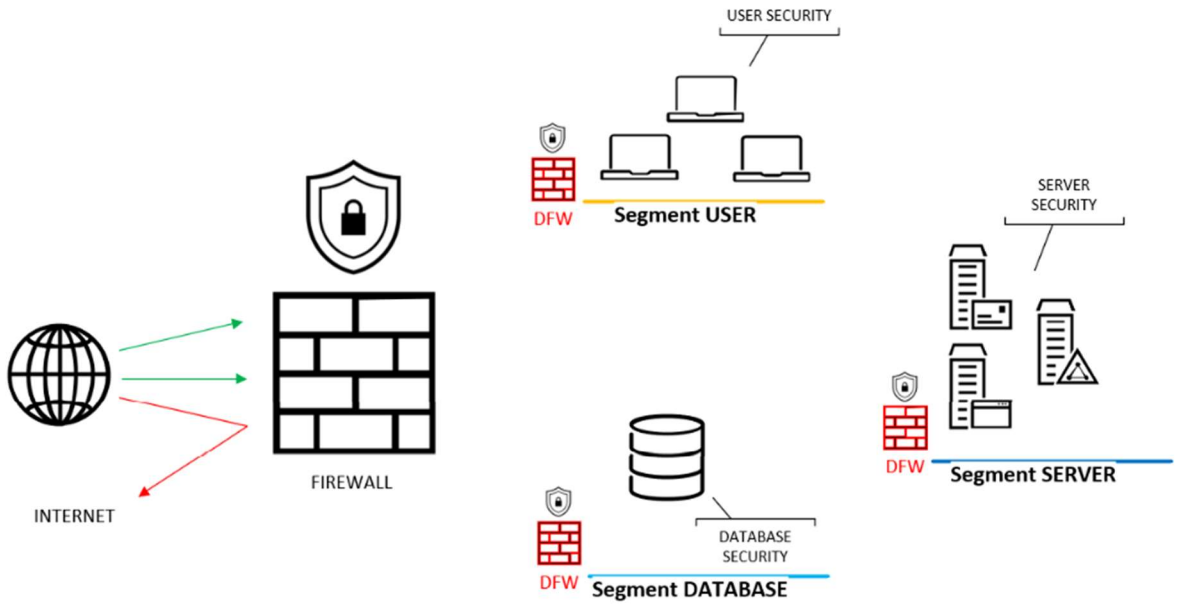


Figure 3.Firewall distribué

2.4 Les avantages de la micro-segmentation

La micro-segmentation présente de nombreux avantages en matière de sécurité informatique. Tout d'abord, elle permet de réduire considérablement la surface d'attaque du réseau.
En effet, en segmentant le réseau, il est possible de restreindre l'accès aux ressources critiques et de limiter le trafic entre les segments.

De cette manière, les cybercriminels ont moins de chances de pénétrer dans le réseau.
De plus, la micro-segmentation permet de mieux contrôler le trafic entre les segments du réseau.
Les administrateurs peuvent définir des règles de sécurité pour chaque segment et chaque workload individuellement au sein du même segment.

Elle permet de faciliter la conformité réglementaire en matière de sécurité informatique.
Les entreprises doivent se conformer à des normes de sécurité strictes, telles que la directive NIS2 voté le 10 novembre 2022.
https://www.ssi.gouv.fr/directive-nis-2-ce-qui-va-changer-pour-les-entreprises-et-ladministration-francaises/

La micro-segmentation peut aider les entreprises à se conformer à ces normes en isolant les données sensibles et en restreignant l'accès aux ressources critiques.

2.5 Les inconvénients de la micro-segmentation

Bien que la micro-segmentation offre de nombreux avantages en matière de sécurité et de gestion de réseau, elle présente également des inconvénients potentiels.
La configuration et la gestion de la micro-segmentation peuvent être complexes, ce qui peut nécessiter des compétences techniques avancées.

Il est donc important de prendre en compte ce facteur lors de la planification et de la mise en œuvre de la micro-segmentation.

2.6 Applications de la micro-segmentation

La micro-segmentation est largement utilisée dans les environnements de cloud computing, où elle est utilisée pour isoler les machines virtuelles et pour améliorer la sécurité des données et des applications.

Elle est aussi utilisée dans les environnements de conteneurs, où elle permet d'isoler les conteneurs les uns des-autres et de protéger les applications contre les menaces externes et internes.
Elle est également utilisée dans les environnements de réseau défini par logiciel (SDN), où elle permet une gestion centralisée des politiques de sécurité et une isolation granulaire des machines virtuelle.

La micro-segmentation est une technique de pointe qui permet de diviser un réseau en segments plus petits et plus gérables, appelés micro-segments.
Cette technique permet d'isoler et de protéger les machines virtuelles sur un réseau en utilisant des politiques de sécurité granulaires pour protéger les ressources critiques contre les menaces externes et internes.

2.7 Schéma Micro-segmentation

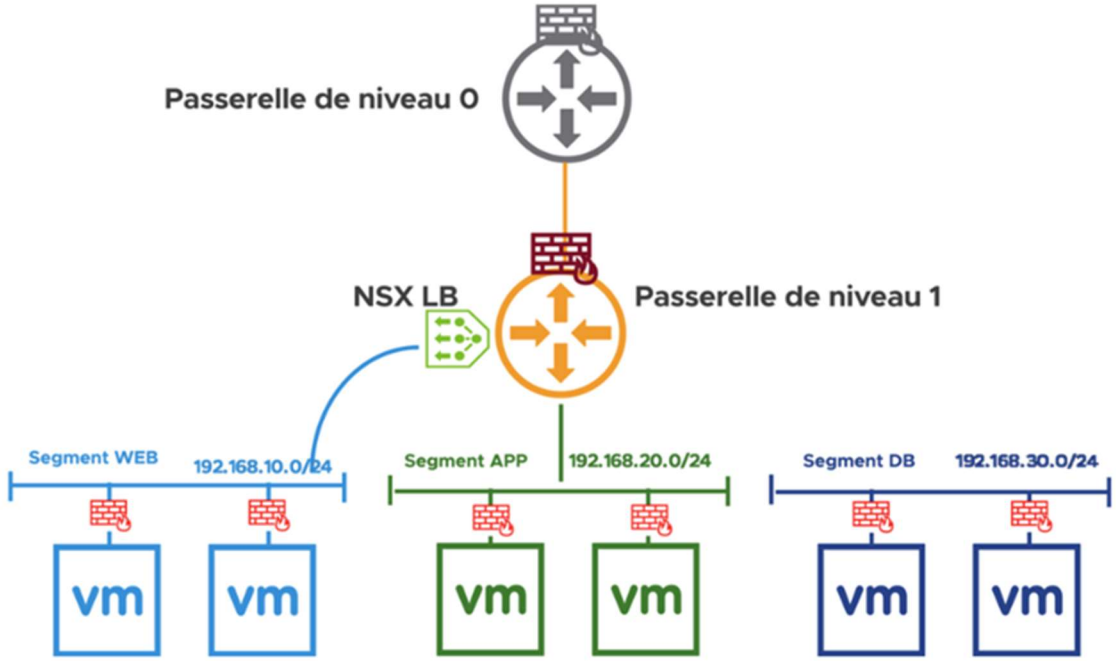


Figure 4.Micro-segmentation

Voici un exemple concret illustrant les possibilités offertes par la technologie de micro-segmentation en entreprise, destinée à la protection d'un accès WEB(internet, site internet), d'applications et de bases de données :

L'architecture comprend trois segments distincts :

- **Segment WEB** : Ce segment est spécifiquement dédié au site web. Il abrite un service web associé à des machines virtuelles. Chacune de ces machines virtuelles est équipée d'un pare-feu distribué pour renforcer la sécurité.
- **Segment APP** : Le segment APP est réservé aux applications. Il comporte des services applicatifs hébergés sur des machines virtuelles, chacune étant également munie d'un pare-feu distribué.
- **Segment DB** (Database) : Ce segment est conçu pour héberger les bases de données. Il abrite les bases de données nécessaires au fonctionnement du système. Comme les autres segments, il est équipé de pares-feux distribués sur les machines virtuelles.

Pour garantir des performances optimales, le segment WEB est doté d'un équilibrage de charge (load balancing) qui répartit efficacement la charge du trafic entrant.

La connectivité entre ces segments est assurée par deux passerelles :

- Une passerelle de niveau **TIER/1** permet un acheminement bidirectionnel des paquets entre les segments, c’est le trafic Est-Ouest
- Une passerelle de niveau **TIER/0** permet l'acheminement des paquets, c’est le trafic Nord-Sud.

De plus, pour renforcer encore davantage la sécurité du réseau, des pare-feu distribués sont déployés au niveau des passerelles.

Cette configuration de micro-segmentation offre une sécurité accrue, une isolation des ressources, une gestion optimisée du trafic, et des performances améliorées pour les applications et les services hébergés.

Elle constitue une approche robuste pour protéger un environnement d'entreprise sensible.

3 Comparaison ACI Cisco et NSX VMware

Cisco ACI et VMware NSX sont deux solutions de virtualisation du réseau.
ACI est une solution de réseau centrée sur l'application qui utilise le concept de politique pour gérer le réseau.
NSX, quant à lui, est une solution de réseau centrée sur la sécurité qui utilise la segmentation pour isoler le trafic.

3.1 Fonctionnalités

Cisco ACI offre des fonctionnalités telles que la gestion des politiques, la segmentation, la visibilité et le contrôle centralisés, ainsi que la gestion unifiée des réseaux physiques et virtuels.

Il utilise des politiques pour définir les règles de trafic pour les applications.
Les politiques sont appliquées de manière cohérente dans l'ensemble du réseau, ce qui garantit une cohérence dans la gestion du réseau.
Cisco ACI prend également en charge la segmentation, ce qui permet d'isoler le trafic entre les différents groupes d'utilisateurs.

VMware NSX, quant à lui, offre des fonctionnalités telles que la segmentation, la gestion centralisée, la virtualisation des fonctions réseau et la sécurité.
Il utilise la segmentation pour isoler le trafic entre les différentes applications et les différents groupes d'utilisateurs.

Il prend également en charge la virtualisation des fonctions réseau, ce qui permet de déployer des services réseau tels que des pares-feux et des équilibrages de charge de manière virtuelle.

3.2 Architecture

Cisco ACI utilise une architecture basée sur des contrôleurs pour gérer le réseau.
Il utilise des commutateurs de couche 2 et de couche 3 pour le transport du trafic.
Le contrôleur APIC d'ACI est responsable de la gestion des politiques et de la segmentation.
VMware NSX utilise une architecture basée sur des micro-segments pour la gestion du réseau.
Il utilise également des commutateurs de couche 2 et de couche 3 pour le transport du trafic.
NSX Manager est le composant responsable de la gestion centralisée du réseau.

3.3 Interopérabilité

Cisco ACI est conçu pour être utilisé avec les équipements de commutation et de routage de Cisco.
Il prend également en charge les protocoles de routage standard tels que OSPF et BGP.

ACI utilise des normes ouvertes telles que OpenFlow pour permettre l'interopérabilité avec d'autres équipements.
VMware NSX prend en charge une large gamme d'équipements de commutation et de routage.
Il prend également en charge les protocoles de routage standard tels que OSPF et BGP.
NSX utilise également des normes ouvertes telles que OpenFlow pour permettre l'interopérabilité avec d'autres équipements.

3.4 Fonctionnalités de sécurité

En termes de sécurité, les deux solutions offrent des fonctionnalités similaires, mais avec des approches différentes.
ACI offre une sécurité centrée sur l'application qui utilise les politiques pour contrôler l'accès au réseau.

Il utilise également des fonctionnalités de micro-segmentation pour isoler le trafic entre les différents groupes d'utilisateurs.
ACI prend en charge la surveillance des menaces et la gestion des politiques de sécurité.

NSX, quant à lui, offre une sécurité centrée sur la segmentation.
Il utilise la segmentation pour isoler le trafic entre les différentes applications et les différents groupes d'utilisateurs.
Il prend également en charge la surveillance des menaces et la gestion des politiques de sécurité.
NSX permet de déployer des pares-feux virtuels pour renforcer la sécurité du réseau.

3.5 Facilité de déploiement

En termes de facilité de déploiement, les deux solutions offrent des outils de déploiement et de configuration pour faciliter le processus de déploiement.
ACI utilise Cisco Application Policy Infrastructure Controller (APIC) pour la gestion centralisée et la configuration du réseau.

Il prend également en charge les outils de déploiement automatisés tels que Ansible.
NSX utilise VMware NSX Manager pour la gestion centralisée et la configuration du réseau.
Il prend également en charge les outils de déploiement automatisés tels que Ansible et Terraform.

3.6 Tableau comparatif ACI Cisco et NSX VMware

Critère	ACI Cisco	NSX VMware
Architecture	- Basée sur un modèle centré sur l'application. - Utilise des commutateurs ACI et le contrôleur APIC (Application Policy Infrastructure Controller).	- Orientée sur la virtualisation réseau. - Comprend NSX Manager, les hyperviseurs et les commutateurs virtuels NSX.
Définition des politiques réseau	- Utilise des politiques d'application pour définir le comportement du réseau.- Approche basée sur les applications.	- Définit les politiques de manière granulaire, basées sur des règles. - Les règles peuvent être définies en fonction de groupes d'objets.
Virtualisation	- Fournit une segmentation réseau native (VRF-like) pour isoler les applications. - Virtualisation réseau à l'échelle du data center.	- Offre une virtualisation réseau complète, y compris la segmentation et le micro-segmentation des charges de travail.
Gestion du trafic	- Permet le contrôle automatisé du trafic avec des politiques applicatives.	- Offre une gestion avancée du trafic grâce à des règles de sécurité et de routage. - Peut être intégré avec des services tiers.
Sécurité	- Fournit une sécurité avancée grâce à l'isolation des applications et à la segmentation. - Offre une visibilité avancée et des politiques de sécurité basées sur l'application.	- Propose une micro-segmentation pour une isolation fine des charges de travail. - Intégration avec des pares-feux tiers.
Interopérabilité	- Conçu pour fonctionner avec un large éventail d'équipements réseau Cisco. - Peut interagir avec des solutions tierces via des API ouvertes.	- Peut fonctionner avec une variété de fournisseurs de matériel réseau. - Prise en charge d'intégrations tierces via des API ouvertes.
Coût	- Investissement initial élevé en matériel Cisco.	- Offre une variété de licences en fonction des fonctionnalités requises. - Peut réduire les coûts opérationnels grâce à l'automatisation.

4 Comparaison VxLAN et GENEVE

VxLAN et GENEVE sont deux protocoles d'encapsulation utilisés pour la virtualisation du réseau.
Ils permettent de créer des réseaux virtuels qui sont indépendants du réseau physique.
Ils ont tous les deux des approches différentes de la virtualisation du réseau.

4.1 Fonctionnalités

VxLAN offre des fonctionnalités telles que la virtualisation du réseau, la segmentation, la gestion centralisée et l'interopérabilité.
Il utilise un identificateur de réseau virtuel (VNI) pour identifier les différents réseaux virtuels.

VxLAN prend également en charge la segmentation, ce qui permet d'isoler le trafic entre les différents groupes d'utilisateurs.
GENEVE offre des fonctionnalités similaires à VxLAN, mais avec des améliorations.
Il utilise également un identificateur de réseau virtuel pour identifier les différents réseaux virtuels.

GENEVE prend en charge la segmentation, la gestion centralisée et l'interopérabilité.
Il offre également des améliorations telles que la prise en charge de l'encapsulation de paquets de taille variable et la prise en charge des données de contrôle du réseau.

4.2 Interopérabilité

VxLAN est un protocole standard qui est pris en charge par plusieurs fournisseurs de réseau.
Il est également pris en charge par des équipements de commutation et de routage de différents fournisseurs.
Cependant, l'interopérabilité peut être un défi en raison des différences dans les implémentations du protocole.

GENEVE est également un protocole standard qui est pris en charge par plusieurs fournisseurs de réseau.
Il est également pris en charge par des équipements de commutation et de routage de différents fournisseurs.
GENEVE est conçu pour être plus flexible et plus évolutif que VxLAN.

4.3 Performance

GENEVE est conçu pour être plus flexible et plus évolutif que VxLAN.
Il offre également des performances élevées, avec une surcharge minimale liée à l'encapsulation et au désencapsulassions des paquets.

GENEVE peut prendre en charge des paquets de taille variable, ce qui permet une meilleure utilisation de la bande passante.

4.4 Schéma d'encapsulation de paquets

4.4.1 VxLAN

On retrouve sur ce schéma nos deux serveurs, connecter par un switch physique et un tunnel VXLAN.
Les deux VTP(Virtual Tunnel Endpoint).
L'encapsulation entre les deux serveurs est possible sur internet grâce au tunnel.

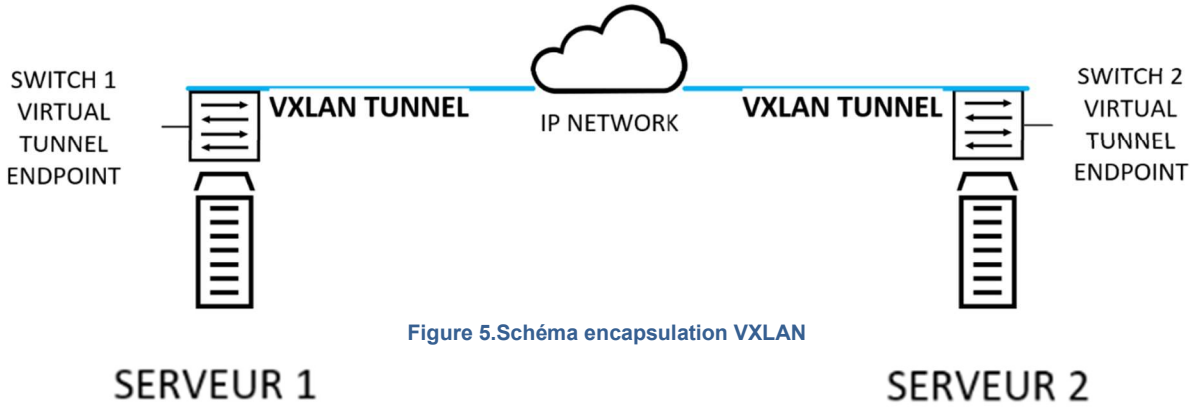


Figure 5.Schéma encapsulation VXLAN

4.4.2 GENEVE

Sur ce schéma une approche différente de l'encapsulation de paquets.
Le switch est virtualisé(VDS Virtual Distributed Switch) les paquets transite par un nœud de transport et les TEP(Terminal End Point).

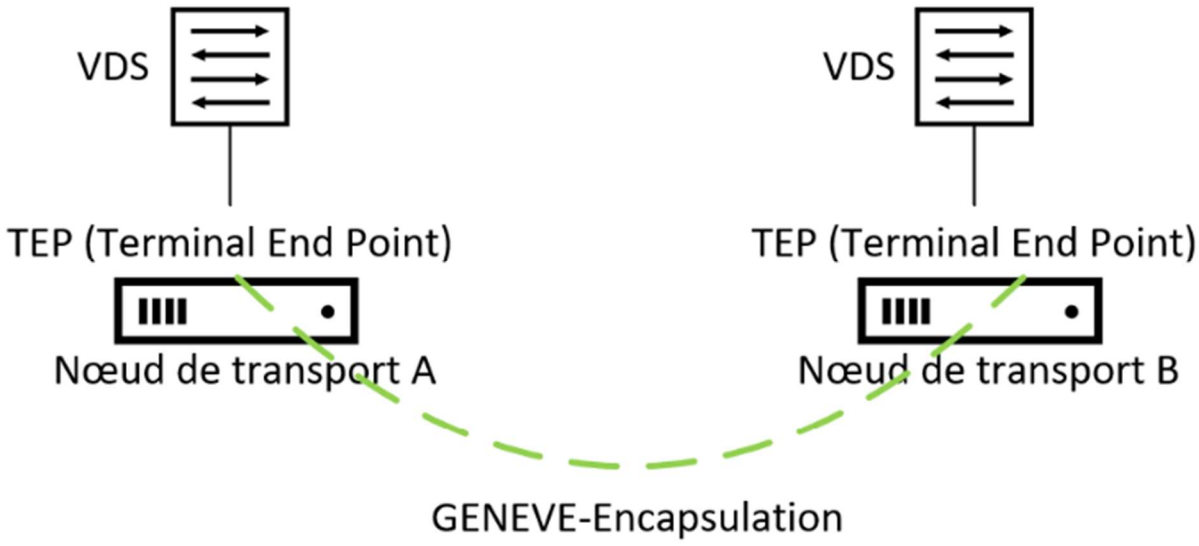


Figure 6.Schéma encapsulation GENEVE

4.5 Comparatif des entêtes GENEVE VxLAN

4.5.1 GENEVE

Figure 7.Entête GENEVE

GENEVE signifie Generic Network Virtualization Encapsulation (encapsulation générique de virtualisation du réseau).
Comme VxLAN, GENEVE encapsule également les paquets avec un en-tête unique et utilise UDP comme mécanisme de transport.

Geneve prend en charge l'unicast, le multicast et le broadcast.
Geneve définit uniquement un format de données d'encapsulation.
GENEVE est développé pour être flexible et extensible de la meilleure façon possible.

Ce qui rend GENEVE puissant et à l'épreuve du temps, c'est son extensibilité grâce à un ensemble proposé d'options TLV qui peuvent être définies.
Le format d'option flexible de GENEVE ainsi que l'utilisation de l'IANA (Internet Assigned Numbers Authority) pour désigner les classes d'options sont des avantages clés par rapport aux méthodes d'encapsulation VxLAN.

Concernant les entêtes on retrouve le **VNI** pour Virtual Network identifier, le Protocol Type (UDP ou TCP) par exemple ou encore la partie **Reserved** pour les données encapsulées.

4.5.2 Explications des entêtes

Champ V (Variable Length Field) :
Le champ V, également connu sous le nom de champ Variable Length Field, est une partie dynamique de l'en-tête Geneve.
Son rôle principal est de permettre la transmission d'informations variables ou d'options spécifiques pour la virtualisation réseau.
Ce champ peut varier en longueur en fonction des besoins de l'encapsulation, ce qui le rend flexible pour l'inclusion d'informations supplémentaires, telles que des métadonnées, des paramètres de qualité de service (QoS) ou d'autres données personnalisées.

Champ O (OAM Flags) :
Le champ O, qui signifie OAM (Operations, Administration, and Maintenance) Flags, est utilisé pour la gestion et la maintenance des réseaux virtuels. Ce champ contient des indicateurs ou des drapeaux qui signalent des informations importantes pour la surveillance et la gestion du trafic.

Champ C (Critical Option Bit) :
Le champ C, abréviation de Critical Option Bit, joue un rôle crucial dans la détermination de la manière dont le paquet Geneve doit être traité par les équipements réseau.
Il indique si les informations contenues dans le champ V sont essentielles au traitement du paquet.
Si le bit C est défini à 1, cela signifie que les données dans le champ V sont critiques et que le paquet doit être traité en conséquence.
Si le bit C est à 0, les informations dans le champ V peuvent être considérées comme facultatives, et le traitement peut être simplifié en fonction de cette indication.

4.5.3 VxLAN

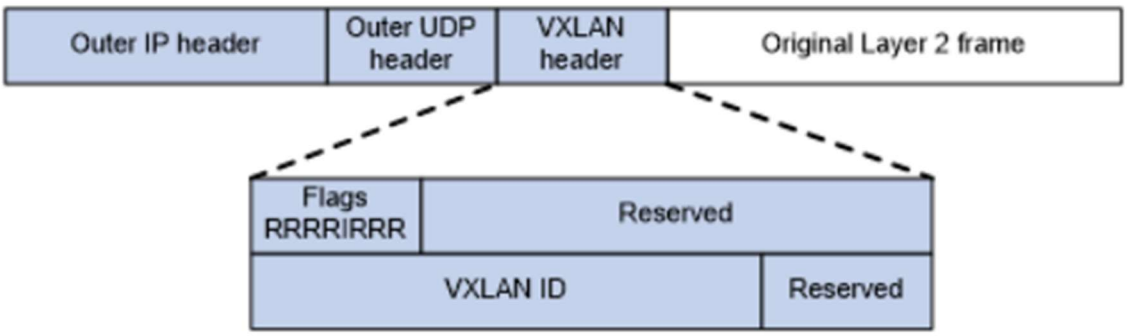


Figure 8.Entête VxLAN

VxLAN pour Virtual Extensible LAN.
Il permet la formation d'un segment LAN de couche 2 à travers le réseau de couche 3.
En tirant parti de la technologie VxLAN sur le réseau de couche 3 routé sous-jacent, les problèmes de spanning-tree(protocole réseaux) et de trunking(lien qui permet de faire transiter plusieurs VLANs) des VLANs(Virtual local network) sont atténués.

VxLAN est officiellement documenté dans la RFC 7348, ce qui en fait une norme. Chaque segment VxLAN possède un identifiant appelé VNI, qui est de 24 bits et permet d'étendre les valeurs VxLAN à environ 16 millions de segments VxLAN.

Concernant les entêtes on retrouve également un **VXLAN ID** (VNI coté GENEVE) et les partis **Reserved** pour l'encapsulation des données.

On retrouve ici les mêmes notions de flags et de protocole ou du IP header qu'avec le protocole GENEVE.

4.6 Tableau de comparaison VxLAN et GENEVE

PARAMÈTRE	VxLAN	GENEVE
Abréviation de	VxLAN (réseau local extensible virtuel)	GENEVE (Encapsulation générique de virtualisation de réseau)
Développé par	VMware, Arista Networks et Cisco	VMware, Microsoft, Red Hat et Intel
Protocole	UDP	UDP
Port	4789	6081
Longueur d'en-tête	8 octets	16 octets
Sécurité des transports, chaînage de services, télémétrie intra-bande	Non supporté	Supporter en charge
RFC	RFC 7348	RFC 8926
Protocol Identifier	Non	Oui
Indication de charge utile non-client	Non	Oui
Extensibilité.	Non. Tous les champs de l'en-tête VxLAN ont des valeurs prédéfinies	Oui
Mécanisme d'extensibilité des fournisseurs compatible avec le matériel	Limité	Oui
Terme utilisé pour les points de terminaison de tunnel	VTEP	TEP

Tableau 2.Comparaison VxLAN VS GENEVE

4.7 Conclusion

D'un point de vue général, VxLAN et Geneve fournissent le même résultat fonctionnel, c'est-à-dire l'encapsulation et le transport de trames L2 à l'intérieur d'un paquet IP de couche 3.

Les deux utilisent le protocole UDP pour remplir leur fonction.
Cependant, certains aspects différencient les deux protocoles de tunnellisation.
Alors que la longueur de l'en-tête de la trame VxLAN est de 8 octets, Geneve a doublé la taille de l'en-tête, qui est de 16 octets.

Il y a trois aspects qui ne sont pas disponibles avec VxLAN, la sécurité du transport, le chaînage de services et la télémétrie en bande.
les principales lacunes de VxLAN auxquelles Geneve a remédié sont les suivantes :

VxLAN ne dispose pas du champ d'identification du protocole

- Cependant, un multiplexage/démultiplexage plus poussé nécessite un identifiant de protocole dans l'adresse de la charge utile, ce qui fait défaut au VXLAN.

- Aucune possibilité d'envoyer une trame de paquet qui n'appartient pas au client, c'est-à-dire que l'autre extrémité ne peut pas distinguer s'il s'agit d'un paquet client ou non.

- Tous les champs de VXLAN sont fixes et il n'y a pas d'option d'interopérabilité à l'aide de champs extensibles.

Une dernière distinction entre les deux protocoles est que VxLAN appelle les points d'extrémité du tunnel "VTEP" alors que "TEP" est la terminologie utilisée dans le cas de Geneve.

5 Présentation NSX

5.1 Introduction

Le monde de la virtualisation du réseau est en constante évolution et VMware est un leader dans ce domaine depuis de nombreuses années.

NSX est la dernière génération de la solution de virtualisation du réseau de VMware, offrant une plateforme de gestion de réseau moderne et évolutive qui offre des fonctionnalités avancées de virtualisation de réseau, de sécurité et de conteneurisation.

5.2 La virtualisation du réseau avec NSX

NSX est une plate-forme de virtualisation de réseau définie par logiciel (SDN) qui permet de créer, gérer et sécuriser des réseaux virtuels.
Cette solution offre une approche moderne de la virtualisation de réseau, permettant de créer des réseaux virtuels multiclouds de haute performance, en utilisant des technologies telles que la virtualisation des fonctions réseau et les micro-segments de sécurité.

NSX est une solution très flexible et évolutive, qui permet une gestion centralisée des réseaux virtuels, quel que soit l'environnement dans lequel ils sont déployés.
Elle prend en charge les environnements multiclouds, les centres de données locaux et distants, offrant des performances accrues pour les applications et les machines virtuelle, peu importe où elles se trouvent.

NSX offre une sécurité avancée grâce à la segmentation de réseau et à la protection des machines virtuels, en utilisant des techniques telles que l'isolation des réseaux virtuels et la segmentation basée sur les politiques.
Cela permet aux entreprises de garantir la sécurité de leurs données et de leurs applications, tout en facilitant la conformité réglementaire.

Cette solution est conçue pour répondre aux besoins des environnements de cloud computing modernes, en permettant aux entreprises de créer des réseaux virtuels privés qui sont indépendants du matériel physique sous-jacent.

NSX offre une plateforme de gestion de réseau évolutive qui prend en charge la virtualisation de réseaux, la sécurité et la conteneurisation.
C’est une plate-forme complète de mise en réseau et de sécurité de couche 2 à couche 7 qui vous permet de gérer un réseau depuis une console unique.

5.3 Schéma Data Center

Voici une représentation comparative entre un Data Center traditionnel, caractérisé par une architecture physique, et un Data Center orienté vers la virtualisation, avec l'utilisation de NSX.

Cette illustration met en évidence les concepts que j'ai précédemment abordés :

- Dans le Data Center traditionnel, l'accent est mis sur l'infrastructure matérielle physique, avec des serveurs physiques, des commutateurs physiques, et des câbles physiques interconnectant les composants.

- En revanche, dans le Data Center centré sur la virtualisation avec NSX, les éléments matériels sont toujours présents, mais une couche de virtualisation, orchestrée par NSX, est interposée entre les ressources physiques et les applications. Cela permet de créer des réseaux virtuels, d'isoler les charges de travail, d'appliquer des politiques de sécurité avancées, et de simplifier la gestion du réseau.

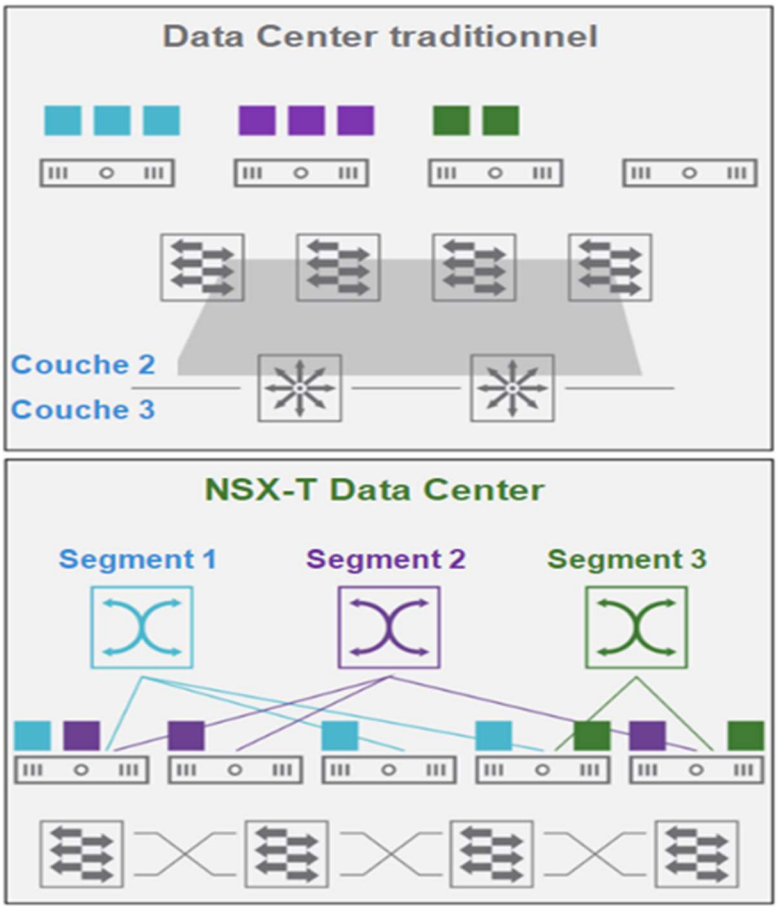


Figure 9.NSX Datacenter

5.4 Principes fondamentaux de la virtualisation de réseau VMware

Cette solution utilise des commutateurs virtuels pour agréger et gérer les connexions entre les machines virtuelles, permettant ainsi de configurer les réseaux virtuels de manière dynamique et souple, sans avoir à modifier la configuration physique du réseau.

Les principes fondamentaux de la virtualisation de réseau VMware reposent sur deux concepts clés :

- **La création de réseaux virtuels.**
- **La segmentation du réseau.**

La création de réseaux virtuels permet de regrouper les machines virtuelles en réseaux logiques, offrant ainsi une isolation et une gestion indépendante des machines virtuelles.

La segmentation du réseau permet de diviser un réseau en sous-réseaux logiques, appelés segments, qui peuvent être configurés indépendamment les uns-des-autres.

La gestion centralisée des réseaux virtuels, permet de simplifier la configuration et la gestion des réseaux virtuels.

Les principes fondamentaux reposent sur la création de réseaux virtuels et la segmentation du réseau, offrant une gestion centralisée des réseaux virtuels et une sécurité avancée du réseau pour la protection des machines virtuel.

5.5 Fonctionnalités de NSX

NSX offre une variété de fonctionnalités avancées qui permettent aux entreprises de créer des réseaux virtuels privés avec une sécurité améliorée et une gestion simplifiée.

Parmi ces fonctionnalités, on peut citer :

Virtualisation de réseau : permet de créer des réseaux virtuels qui sont isolés du réseau physique sous-jacent.

Sécurité avancée : fonctionnalités de sécurité avancées, telles que la micro-segmentation, qui permet de diviser les réseaux virtuels en segments plus petits pour une sécurité renforcée.
NSX prend également en charge les pares-feux distribués, les réseaux privés virtuels (VPN) et l'inspection de paquets, ce qui permet de renforcer la sécurité du réseau.

Conteneurisation : permet de prendre en charge les environnements de conteneurs, tels que Kubernetes.
Cela permet aux entreprises de déployer des applications en conteneurs sur un réseau virtuel sécurisé, ce qui facilite la gestion et l'orchestration des conteneurs.

Évolutivité : NSX est conçu pour être évolutif et prend en charge les environnements de cloud computing modernes.

Voici quelques cas d'utilisation de la solution NSX :

- **Virtualisation en Data Centers** : NSX permet la création de réseaux virtuels qui peuvent être gérés à partir d'une plate-forme centralisée.

- **Micro-segmentation et sécurité** : comme mentionné précédemment, NSX offre une fonctionnalité de micro-segmentation qui permet aux entreprises de segmenter leur réseau en zones plus petites et plus gérables.
  Cela permet de limiter la surface d'attaque et d'isoler les machines virtuelles sensibles.
  NSX permet également d'appliquer des politiques de sécurité granulaires à chaque segment.

- **Cloud hybride et multicloud** : NSX est conçu pour fonctionner avec des environnements cloud hybrides et multicloud.
  Les entreprises peuvent utiliser NSX pour créer des réseaux privés virtuels entre leurs centres de données locaux et les clouds publics tels que Microsoft Azure, AWS ou Google Cloud.
  Cela permet aux entreprises de bénéficier des avantages de la flexibilité et de l'évolutivité des clouds publics tout en conservant le contrôle et la sécurité de leur infrastructure privée.

- **Automatisation du réseau** : NSX est prévus pour fonctionner avec des outils d'automatisation tels que Ansible et Terraform, Cela permet aux entreprises de déployer des réseaux virtuels et des politiques de sécurité de manière automatisée.

- **Virtualisation des fonctions réseau** : permet la virtualisation des fonctions réseau telles que le pare-feu, le routage, la commutation et la gestion des adresses IP.
  Cela permet aux entreprises de déployer des fonctions réseau plus rapidement et plus efficacement, sans avoir à se soucier de la configuration matérielle.

5.6 Présentation des fonctionnalités principale de NSX

NSX est la prochaine étape logique en matière de réseau et de sécurité, NSX répond à des préoccupations et des points faibles spécifiques.
En voici les détails :

- **Segmentation du réseau** : La segmentation du réseau sous NSX permet de déployer créer et de configurer rapidement des segments, ainsi que de créer des zones de sécurité virtuelles en les définissant entièrement sous forme logicielle.

- **Mesures VMware NSX** : La fonctionnalité « Mesures » de NSX collecte des données qui lui permettent de surveiller des statistiques clés dans les entités de votre NSX et les environnements NSX Application Platform.

.

- **VMware NSX Intelligence** : La fonctionnalité « Intelligence » de NSX agrège les flux de trafic réseau dans votre environnement NSX pour fournir une visibilité approfondie des flux, des recommandations de stratégie de pare-feu et une détection du trafic suspecte.

- **VMware NSX Network Detection and Response** : La fonctionnalité « NSX Network Detection and Response » envoie des données d'alerte de menace aux services de cloud VMware NSX « Advanced Threat Prevention », qui effectue ensuite une corrélation et une visualisation sur ces données à l'aide de l'interface utilisateur NSX.

- **Protection contre les programmes malveillants NSX** : Cette fonctionnalité détecte et empêche les Malwares (programmes malveillants) d'entrer dans votre environnement.
  Il utilise les services de cloud NSX « Advanced Threat Prevention » pour extraire des mises à jour de détection.

- **NSX Advanced Load balancer** : NSX « Advanced Load Balancer » fournit un équilibrage de charge multi-cloud, un pare-feu d'application Web, des analyses d'application et des services de conteneur du centre de données vers le cloud.

- **VMware SD-WAN** : Permet de mettre en œuvre des stratégies cloud à l'échelle de l'entreprise.
  Les utilisateurs peuvent accéder de manière sécurisée aux machines virtuelle multi cloud et aux applications SaaS(Software as a service) via le SD-WAN(Software-defined Wide Area Network).

6 Présentation de Photon

La distribution Photon de VMware est une solution puissante pour la conteneurisation, offrant une plateforme légère, sécurisée et flexible pour exécuter des applications dans des conteneurs.

Grâce à son système d'exploitation minimaliste, à ses fonctionnalités avancées de gestion des conteneurs et à son intégration avec l'écosystème VMware, Photon permet aux entreprises de tirer pleinement parti des avantages des conteneurs tout en simplifiant la gestion et en renforçant la sécurité.

6.1 Conteneurisation sous NSX

6.1.1 Kubernetes

Kubernetes est une plateforme puissante pour la gestion d'orchestration de conteneurs, offrant des fonctionnalités avancées, une haute disponibilité, une flexibilité de déploiement et un écosystème riche.

Son adoption croissante dans l'industrie témoigne de son efficacité et de son importance pour la gestion des applications conteneurisées à grande échelle.

Que ce soit pour les entreprises cherchant à moderniser leurs infrastructures ou pour les développeurs souhaitant simplifier le déploiement et la gestion de leurs applications, Kubernetes reste un choix incontournable.

Démarrage du projet

1 Charte de projet

Objectifs du projet :

- Déployer la solution de virtualisation NSX sur une infrastructure UCS Cisco.
- Assurer la qualité et la sécurité de l'application tout au long du processus de déploiement.

Portée du projet :

- Déploiement de la solution de virtualisation réseau NSX.
- Tests et validation de la solution (cas d'usage).
- Edition d'un DAT (document d'architecture technique)

Ressources du projet :

- Administrateur système et réseaux.
- Accès aux systèmes et aux données nécessaires pour le déploiement de la solution.
- Appui de la direction et du service PS de l'entreprise pour la réussite du projet.

Calendrier du projet :

- Phase de planification : du 1er novembre 2022 au 1er février 2023.
- Phase de déploiement : du 2 février 2023 au 30 juin 2023.
- Phase de tests et de validation : du 1er juillet 2023 au 30 septembre 2023.

Risques et contraintes du projet :

- Risques liés aux délais de déploiement et d'apprentissage de la solution.
- Risques liés à la sécurité et à la qualité de l'application.
- Contraintes liées à l'intégration de l'application avec les systèmes existants du lab de l'entreprise.

Responsabilités des membres de l'équipe :

- L'administrateur est responsable de la conception et du déploiement de la solution. (Philippe COMBOT)

Approbation : La présente charte de projet est approuvée par les parties prenantes suivantes :

- Le chef de projet. (Daniel DAHLEN)
- Le représentant de la direction de l'entreprise. (Jérôme COUSIN)

2 Planning prévisionnel du projet

Conception d'une maquette NSX (10 mois)

1. Phase de planification (2 mois)

    - Réunion de démarrage du projet
    - Définition des objectifs de la maquette
    - Identification des ressources nécessaires (équipement matériel, etc.)
    - Collecte des exigences techniques

2. Conception (2 mois)

    - Conception de l'architecture de la maquette
    - Définition des composants NSX à inclure (définition des clusters, des réseaux, des pares-feux virtuels, etc.)
    - Élaboration du plan de déploiement pour la maquette
    - Création d'un schéma de la configuration réseau virtuel

3. Configuration et déploiement de la maquette (5 mois)

    - Mise en place de l'environnement matériel et des serveurs nécessaires
    - Installation et configuration de VMware vSphere (plateforme de virtualisation)
    - Déploiement des composants NSX (NSX Manager, contrôleur, hôtes ESXi, etc.)
    - Configuration des réseaux virtuels, des règles de pare-feu, des services de sécurité

4. Tests et validation (2 mois)

    - Tests fonctionnels de la maquette (connectivité, isolation, performances)
    - Vérification de la configuration NSX (virtualisation du réseau, routage, commutation, pare-feu, micro-segmentation)
    - Validation des cas d'utilisation
    - Correction des problèmes identifiés

5. Documentation et présentation (1 mois)

    - Rédaction de la documentation technique (configuration, procédures d'exploitation, etc.)
    - Préparation d'une présentation pour l'équipe ou les parties prenantes
    - Présentation de la maquette, de son architecture, et des résultats des tests

6. Conclusion et recommandations (1 semaine)

    - Analyse des retours d'expérience
    - Présentation des avantages et des inconvénients de l'approche NSX
    - Recommandations pour une utilisation future de NSX dans des projets réels

3 Matrice de risques du projet

La gestion des risques d'un projet informatique repose sur l'analyse continue des risques éventuels du projet afin de pouvoir l'accommoder aux résultats de cette analyse.

Voici les différents risques de mon projet que j'ai analyse et autour desquelles j'ai eu une réflexion.

Cause	Effet
Erreur de configuration - bug système	Perte de temps pour le deploiment de la maquette
Crash système - Pas de back-up	Impact sur le bon déroulement de deploiment maquette
Formation NSX	Retard sur le deploiement de la maquette
Mauvaise organisation	Retard sur le deploiement de la maquette
Mauvaise gestion des délais	Retard sur le projet

Figure 10.Cause et Effet matrice de risques

Matrice de risque						Plan de réponse	Risque résiduel					
Probabilité							Probabilité					
VH						Prévoir back-up des VM	VH					
H							H					
M							M					
L							L					
VL					X		VL					X
Gravité	VL	L	M	H	VH		Gravité	VL	L	M	H	VH
VH						Prévoir back-up des données	VH					
H							H					
M					X		M					
L							L					
VL							VL				X	
Gravité	VL	L	M	H	VH		Gravité	VL	L	M	H	VH
VH						Formation et certification NSX	VH					
H							H					
M					X		M					
L							L					
VL							VL				X	
Gravité	VL	L	M	H	VH		Gravité	VL	L	M	H	VH
VH						Création d'un DAT du projet NSX	VH					
H							H					
M					X		M					
L							L					
VL							VL				X	
Gravité	VL	L	M	H	VH		Gravité	VL	L	M	H	VH
VH						Prévoir des délais larges	VH					
H							H					
M					X		M					
L							L					
VL							VL				X	
Gravité	VL	L	M	H	VH		Gravité	VL	L	M	H	VH

Figure 11.Plan de réponse matrice de risques

Je présente ici des solutions à mes questions, accompagnées d'une évaluation de la probabilité, échelonnée de "VH" (Très Haute) à "VL" (Très Basse).

Cette démarche systématique permet de hiérarchiser les options en fonction de leur fiabilité ou de leur probabilité d'aboutir, offrant ainsi une méthode structurée pour orienter les choix et prendre des décisions éclairées.

Légende :

- VH = very high
- H = high
- M = medium
- L = low
- VL = very low

Cause	Effet	Matrice de risque					Plan de réponse	Risque résiduel					
		Probabilité						Probabilité					
Erreur de configuration - bug système	Perte de temps pour le deploiment de la maquette	VH					Prévoir back-up des VM	VH					
		H						H					
		M						M					
		L						L					
		VL						VL					
		Gravité	VL	L	M	H	VH	Gravité	VL	L	M	H	VH
Crash système - Pas de back-up	Impact sur le bon déroulement de deploiment maquette	VH					Prévoir back-up des données	VH					
		H						H					
		M						M					
		L						L					
		VL						VL					
		Gravité	VL	L	M	H	VH	Gravité	VL	L	M	H	VH
Formation NSX	Retard sur le deploiement de la maquette	VH					Formation et certification NSX	VH					
		H						H					
		M						M					
		L						L					
		VL						VL					
		Gravité	VL	L	M	H	VH	Gravité	VL	L	M	H	VH
Mauvaise organisation	Retard sur le deploiement de la maquette	VH					Création d'un DAT du projet NSX	VH					
		H						H					
		M						M					
		L						L					
		VL						VL					
		Gravité	VL	L	M	H	VH	Gravité	VL	L	M	H	VH
Mauvaise gestion des délais	Retard sur le projet	VH					Prévoir des délais larges	VH					
		H						H					
		M						M					
		L						L					
		VL						VL					
		Gravité	VL	L	M	H	VH	Gravité	VL	L	M	H	VH

Figure 12.Matrice de risques

Grâce à cette matrice de risque, j'ai pu anticiper les éventualités et élaborer des solutions pour faire face aux défis qui se présentent dans le cadre de mon projet.

Cette approche proactive permet d'atténuer les risques et de garantir une gestion efficace des problèmes, contribuant ainsi à la réussite globale du projet.

4 WBS Structure de Découpage des Activités

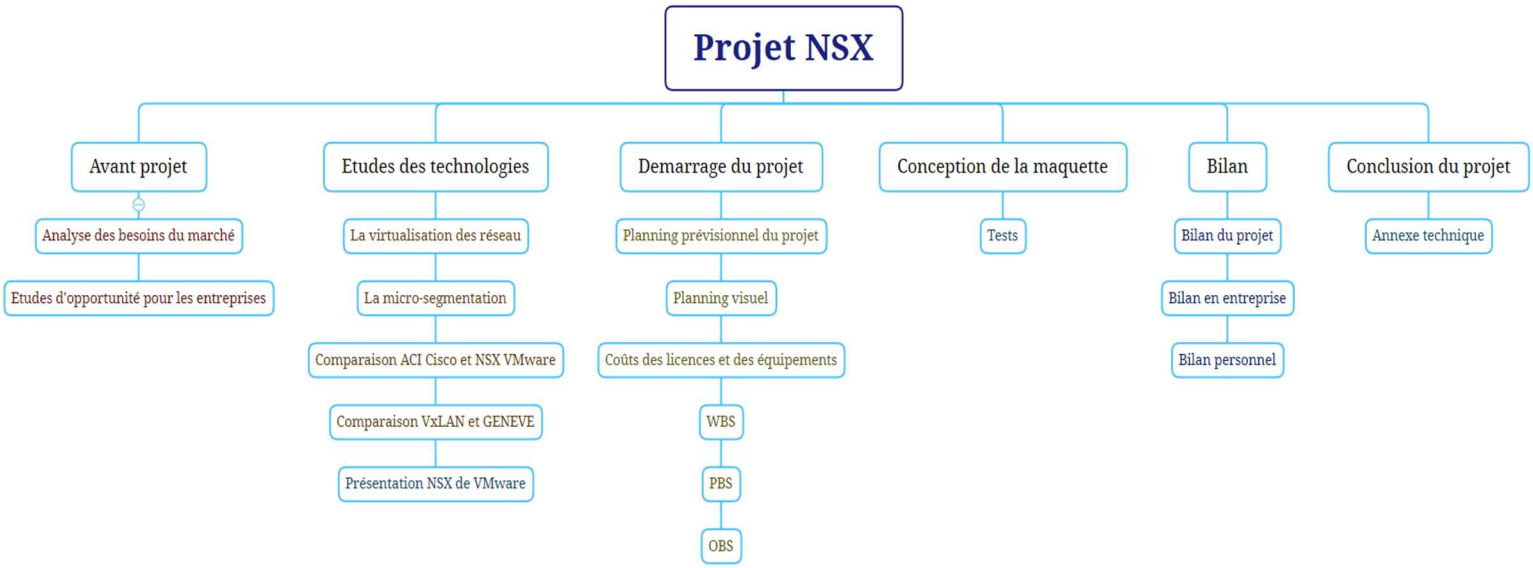


Figure 13.WBS

La méthode WBS (Work Breakdown Structure) représente une technique de gestion de projet qui se caractérise par la décomposition progressive d'un projet principal en tâches filles, celles-ci étant ensuite subdivisées en sous-tâches.

Cette approche structurée permet d'obtenir une vue détaillée de l'ensemble du projet, tout en facilitant la planification, l'attribution des responsabilités, et le suivi de l'avancement des travaux.

Elle favorise également une meilleure compréhension de la complexité d'un projet en le divisant en éléments plus gérables et plus spécifiques.

5 PBS Organigramme technique du projet

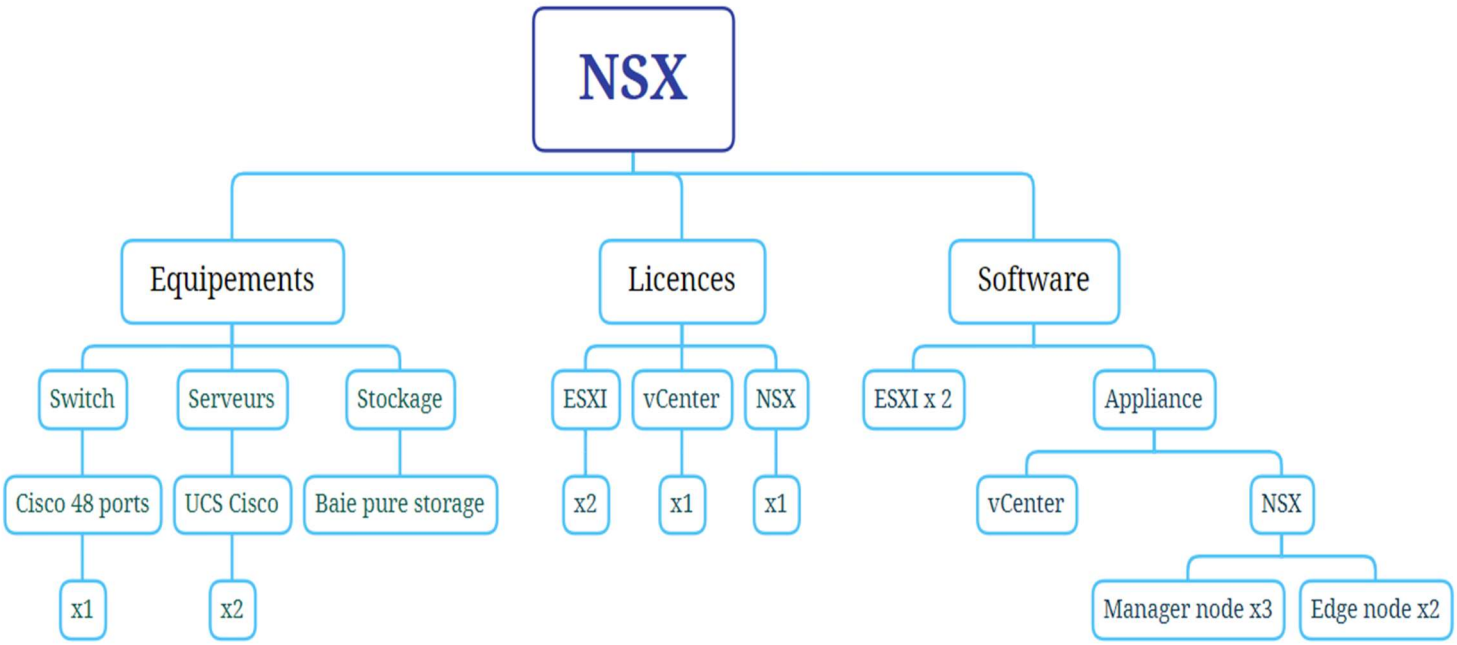


Figure 14.PBS

Le PBS (Product Breakdown Structure) revêt le rôle central dans la représentation technique de mon projet.

Il offre une vue structurée et méthodique de mon projet de maquette NSX, exposant de manière claire et organisée mes exigences en matière d'équipements, de licences et de logiciels.

Cette présentation précise permet de rationaliser la gestion des ressources et la planification, tout en facilitant une compréhension globale des besoins inhérents à mon projet.

6 OBS Structure organisationnelle du projet

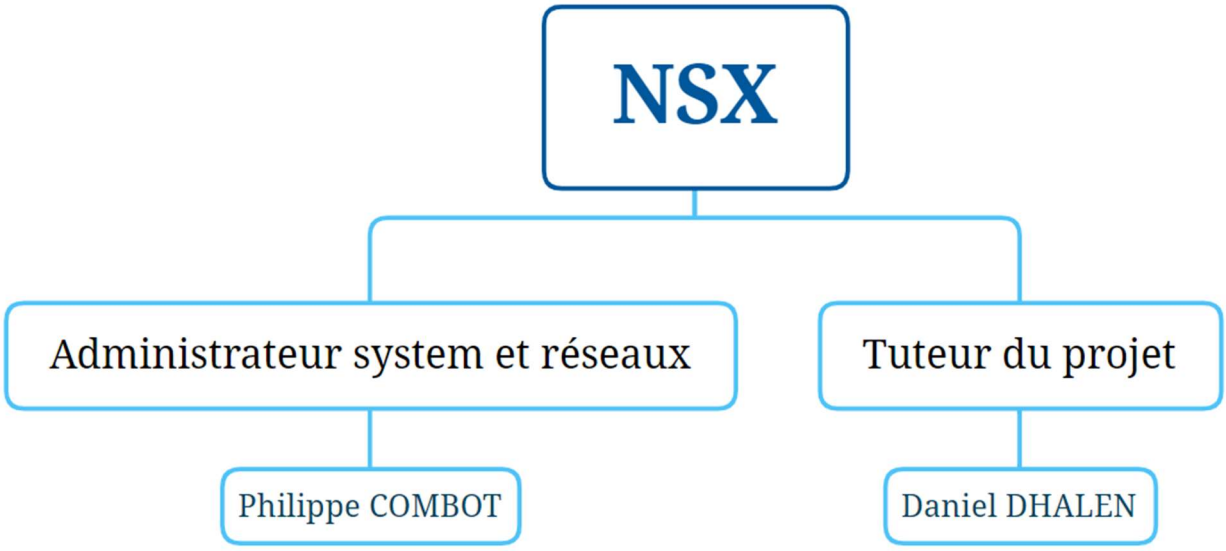


Figure 15.OBS

L'acronyme OBS, qui signifie "Organigramme de la Structure Organisationnelle du Projet" en français, est une représentation graphique qui illustre les ressources requises pour la réalisation du projet

Coûts des licences NSX

1 Licence maquette NSX

Grâce à la collaboration établie avec VMware et Stordata, une licence d'une année a été accordée, ouvrant la voie au déploiement opérationnel de la solution NSX.

Cette licence permet la mise en place concrète et en conditions réelles de NSX, offrant ainsi une opportunité d'évaluation, de test et d'intégration dans l'environnement existant.

2 Licence entreprise NSX

Voici un exemple de de prix facturé pour une infrastructure en entreprise, composé de deux serveurs avec 20 cœurs, 4 CPU soit 80 cœurs.

Price Lst

Référence Constructeur	Réf. TD SYNNEX	Description	Prix public unit. HT EUR	Total List Price EUR	Remise	Prix d'achat unit. HT EUR	Qté	Prix Total HT EUR	Date de début	Date de fin	Durée (Mois)	Contract No.	Commentaire
VCS8-STD-C	7766681	VMware vCenter Server 8 Standard for vSphere 8 (Per Instance)	6 145,00	6 145,00	8,00	5 653,40	1	5 653,40					
VCS8-STD-G-SSS-C	7766682	Basic Support/Subscription VMware vCenter Server 8 Standard for vSphere 8 (Per Instance) for 1 year	1 290,52	1 290,52	5,00	1 225,99	1	1 225,99					
NX-T-ADV-C-TLSS-C	8662954	VMware NSX Advanced per Core for 1-year term	258,00	20 640,00	10,00	232,20	80	18 576,00					
NX-TPAD-DF-AVEPC-TLSS-C	8232188	VMware NSX Threat Prevention Add-on to NSX Distributed Firewall, NSX ADV, or NSX ENT Plus per Core for 1-year term.	83,58	6 686,40	10,00	75,22	80	6 017,60					

20 cores * 4 CPU soit 80 cores

Figure 17.Devis NSX

Total List Price	34 761,92
Total LP Discount %	9,46
Total Customer Price	31 472,99
Frais de port	0,00
Total Customer price incl. freight charges	31 472,99

TOTAL CUSTOMER PRICE incl. freight charges.	**31 472,99**

Figure 16.Devis NSX prix

3 Maintenance NSX

Assurer la maintenance interne de la solution NSX requiert la certification du personnel compétent.
En cas de problèmes complexes, l'ouverture d'un ticket auprès de VMware est une démarche essentielle.

Cette approche garantit que des experts se penchent sur les défis rencontrés, offrant ainsi des solutions spécialisées et une résolution efficace.

Cette combinaison de compétences internes et d'assistance externe contribue à maintenir la fiabilité et la performance de NSX tout en réduisant les perturbations potentielles dans l'infrastructure.

Une gestion proactive et une collaboration étroite avec VMware permettent de préserver la stabilité opérationnelle de l'environnement NSX.

4 Cout des équipements

Avec une mise en place réalisée au sein d'une infrastructure préexistante, il convient de noter que cette démarche présente l'avantage indéniable de réduire considérablement les coûts.

En l'occurrence, Stordata a judicieusement exploité ses ressources internes en mettant à profit son environnement de test dédié aux Preuves de Concept (PoC).
Cela a permis d'éviter tout déboursement supplémentaire.

Pour cette mise en œuvre, j'ai utilisé une infrastructure Cisco UCS, et une baie de stockage NetApp, reconnue pour sa fiabilité et sa capacité à répondre aux besoins de stockage de données complexes.

L'utilisation de ces ressources existantes nous a permis de réaliser ce projet de manière efficace, en capitalisant sur notre propre infrastructure de test, ce qui a représenté un avantage significatif en termes de coûts et de ressources.

4.1 Architecture de l'infrastructure du lab

L'architecture s'appuie sur des baies de stockage NetApp installées en Cluster-Mode 9.5 et des serveurs installés avec vSphere 6.7 pour la virtualisation.

Elle est composée de :

- 1 paire HA FAS2554A en CDOT 9.5 pour le stockage de tous les environnements
- 5 serveurs DELL R820 pour l'infrastructure VMware pour le PS, le Conseil et les Avant-vente.
- Deux switches 10 Gbit/s CN1610 pour la connexion entre les ESX et le Cluster NetApp.
- Deux switches FC Brocade pour la connexion entre les ESX et le Cluster NetApp.

Le Cluster VMware créé dispose de 1.250 To de mémoire et de 30 To de disques SAS connecté en Fibre-Channel.

Les Datastores sont montés sur des agrégats hybrides.

Conception de la maquette

1 Introduction

L'objectif principal de cette maquette est donc de mener une exploration approfondie des multiples fonctionnalités de NSX, tout en évaluant son impact significatif sur les performances, la sécurité et la flexibilité des infrastructures réseau.

L'implémentation de cette maquette NSX offre ainsi une opportunité pour appréhender pleinement les avantages et les opportunités qu'elle confère aux entreprises.

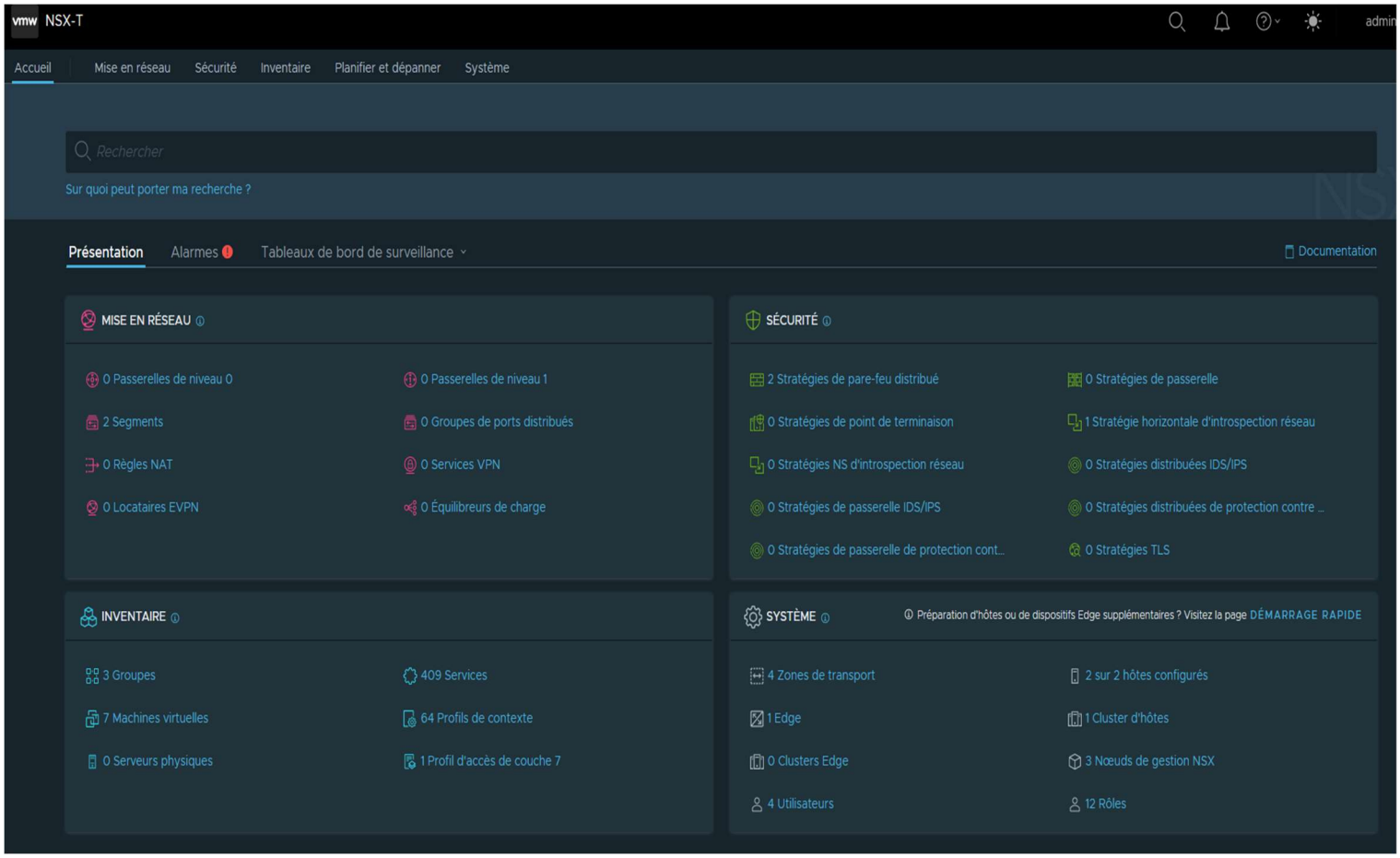
Une attention particulière sera également accordée à l'étude des cas d'utilisation les plus courants de NSX, notamment la micro-segmentation, la création de réseaux virtuels étendus (GENEVE) et la gestion centralisée du réseau.

Cette approche holistique nous permettra d'acquérir une vision globale des applications pratiques de NSX dans différents contextes et scénarios.
Le souhait est de fournir une analyse en profondeur des fonctionnalités de NSX, mettant en exergue les meilleures pratiques pour une implémentation réussie.

2 Descriptions de l'interface graphique (UI) de NSX

2.1.1 Dashboard NSX

Le tableau de bord au sein de l'interface NSX de VMware est un panorama informatif essentiel, dévoilant une multitude de renseignements capitaux pour la gestion et la surveillance du réseau virtualisé.



2.1.2 Mise en réseau

La partie dédiée au réseau au sein du tableau de bord se présente comme un sanctuaire d'informations essentielles, soigneusement organisées pour fournir une vision approfondie des éléments interconnectés du réseau virtuel.

Ce segment distinctif englobe divers panneaux, chacun offrant une perspective aiguisée des fondations réseau :

- **Topologie virtuelle étendue** : Le tableau de bord propose une représentation graphique étendue de la topologie virtuelle. Cette cartographie visuelle présente les machines virtuelles, les segments, les commutateurs et les routeurs, créant ainsi une vue holistique des interactions.

- **Visualisation des flux de données** : Affichage graphique des trajectoires empruntées par les paquets de données entre les segments, offrant une compréhension visuelle du cheminement du trafic.

- **Configuration des segments** : Il permet de contrôler les paramètres de ces dispositifs cruciaux, incluant les VLAN, les politiques de sécurité, et les fonctions de commutation avancées.

- **Gestion des adresses IP et services associer** : Une section distincte dédiée à la gestion des adresses IP. Elle offre un moyen pour gérer et surveiller les allocations d'adresses IP, garantissant une utilisation efficace des ressources d'adressage.

- **Routage intégré** : Le tableau de bord présente une fenêtre dédiée au routage. Elle permet de concevoir, surveiller et ajuster les routes entre les différents segments, participant ainsi à l'orchestration de la connectivité fluide.

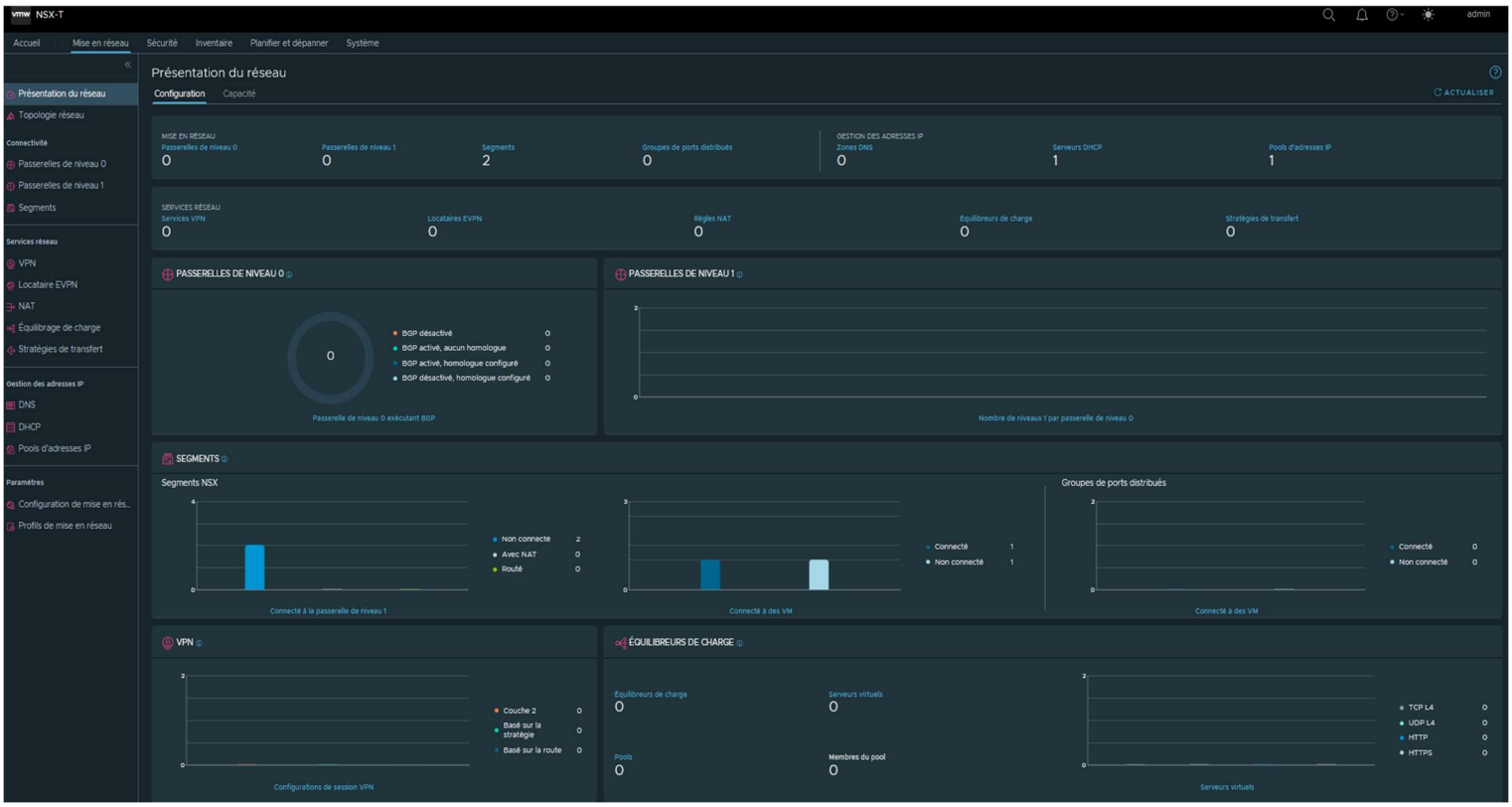
- **Visualisation de la bande passante** : Cette visualisation dynamique met en lumière l'utilisation actuelle et historique de la bande passante, offrant une base pour l'optimisation de la performance.

- **Analyse de latence** : Ceci permet aux administrateurs de repérer rapidement les éventuels problèmes de performance liés aux délais de transmission.

- **Répartition des charges** : Le tableau de bord intègre une vue de la répartition des charges. Cela révèle comment les charges de travail sont distribuées entre les hôtes physiques, contribuant à un équilibrage optimal.
- **VPN** : Permet de crée un réseau privé virtuel.

- **NAT** : Permet de faire correspondre des adresses IP à d’autres adresse IP.

- **DNS** : Permet de configurer son propre serveur DNS.


NSX-T
admin
Accueil
Mise en réseau
Sécurité
Inventaire
Planifier et dépanner
Système
Présentation du réseau
Topologie réseau
Connectivité
Passerelles de niveau 0
Passerelles de niveau 1
Segments
Services réseau
VPN
Locataire EVPN
NAT
Équilibrage de charge
Stratégies de transfert
Gestion des adresses IP
DNS
DHCP
Pools d'adresses IP
Paramètres
Configuration de mise en rés...
Profils de mise en réseau
Présentation du réseau
Configuration
Capacité
ACTUALISER
MISE EN RÉSEAU
Passerelles de niveau 0 0
Passerelles de niveau 1 0
Segments 2
Groupes de ports distribués 0
GESTION DES ADRESSES IP
Zones DNS 0
Serveurs DHCP 1
Pools d'adresses IP 1
SERVICES RÉSEAU
Services VPN 0
Locataires EVPN 0
Règles NAT 0
Équilibreurs de charge 0
Stratégies de transfert 0
PASSERELLES DE NIVEAU 0
BGP désactivé 0
BGP activé, aucun homologue 0
BGP activé, homologue configuré 0
BGP désactivé, homologue configuré 0
Passerelle de niveau 0 exécutant BGP
PASSERELLES DE NIVEAU 1
Nombre de niveaux 1 par passerelle de niveau 0
SEGMENTS
Segments NSX
Non connecté 2
Avec NAT 0
Routé 0
Connecté à la passerelle de niveau 1
Connecté 1
Non connecté 1
Connecté à des VM
Groupes de ports distribués
Connecté 0
Non connecté 0
Connecté à des VM
VPN
Couche 2 0
Basé sur la stratégie 0
Basé sur la route 0
Configurations de session VPN
ÉQUILIBREURS DE CHARGE
Équilibreurs de charge 0
Serveurs virtuels 0
Pools 0
Membres du pool 0
TCP L4 0
UDP L4 0
HTTP 0
HTTPS 0
Serveurs virtuels

2.1.3 Sécurité

La portion réservée à la sécurité se manifeste en tant qu'espace renfermant des informations cruciales, habilement agencées dans le but de fournir une perspective éclairée sur les éléments fondamentaux de la posture sécuritaire du réseau virtuel.

Cette division emboîte le pas à une pluralité de panneaux, chacun doté d'une vision unique des composantes axées sur la sécurité :

- **Vue globale des menaces** : D'emblée, le tableau de bord dévoile une vue panoramique des menaces. Cette représentation graphique des activités suspectes ou des tentatives d'intrusion aide à saisir rapidement l'état de sécurité et à identifier les sources potentielles de risques.

- **Gestion des pares-feux** : Une section primordiale du tableau de bord est réservée à la gestion des pares-feux. Cette plateforme centralisée permet la création, la modification et la suppression de règles de sécurité, offrant ainsi un contrôle sur les flux de données entrants et sortants.

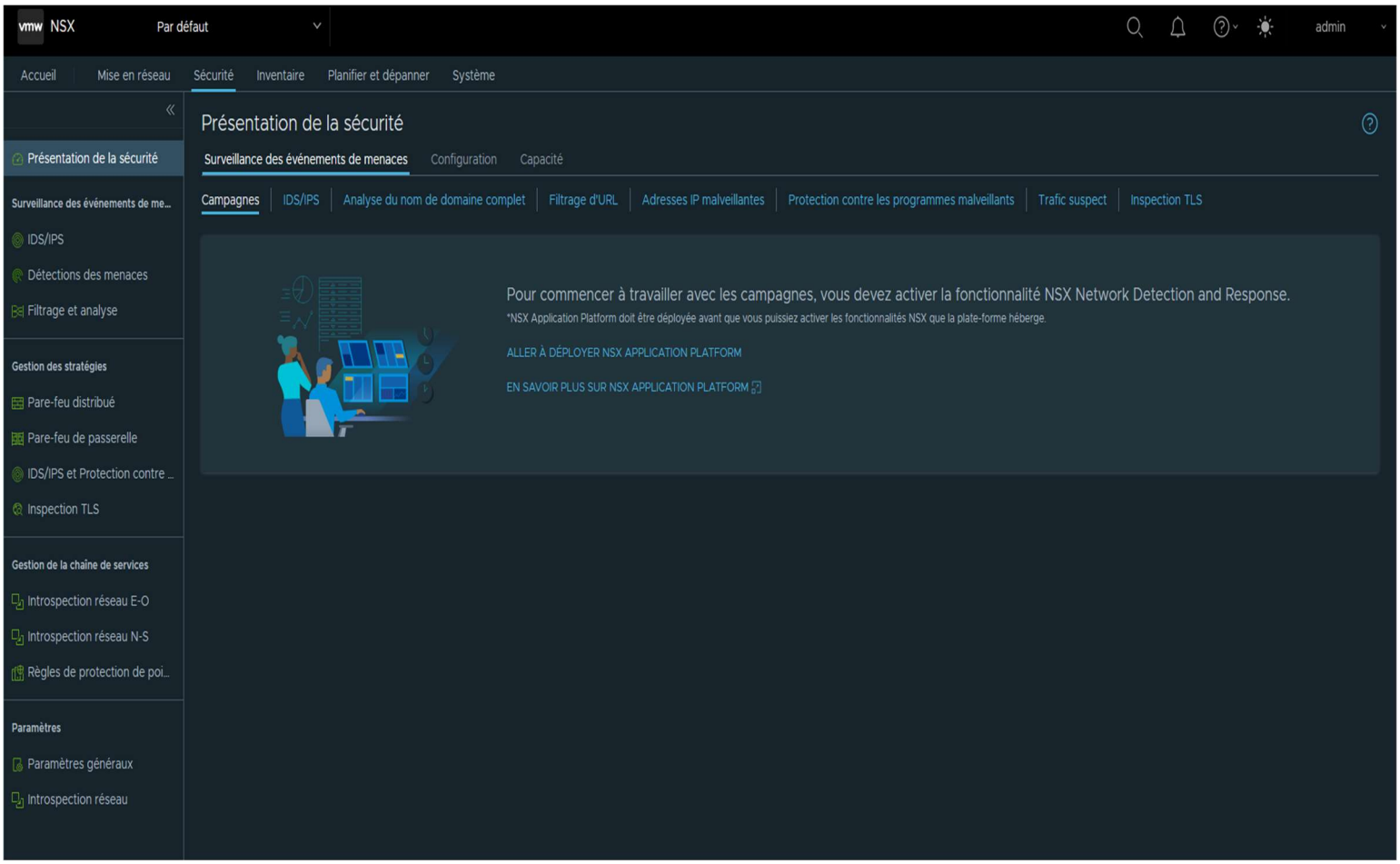
- **Détection d'anomalies** : Une partie du tableau de bord se penche sur la détection d'anomalies. Elle s'appuie sur l'analyse comportementale pour identifier les activités inhabituelles, permettant une réaction précoce face à d'éventuelles menaces.

- **Analyse des vulnérabilités** : Une fenêtre dédiée à l'analyse des vulnérabilités est intégrée. Cela permet aux administrateurs d'identifier les failles potentielles dans le réseau et de prendre des mesures correctives.

- **Intégration des services de sécurité** : Le tableau de bord comporte une section visant à intégrer des services de sécurité externes. Cela offre une approche intégrée pour gérer les mécanismes de défense additionnels, tels que les solutions de détection et de prévention des intrusions.

- **Journalisation des Activités** : Une perspective qui concerne la journalisation des activités. Cette section offre une visibilité sur les événements passés, facilitant la recherche de traces en cas d'incident.

- **Statistiques de Conformité** : Enfin, le tableau de bord des statistiques de conformité, signalant l'adhérence aux politiques de sécurité et aux normes réglementaires.

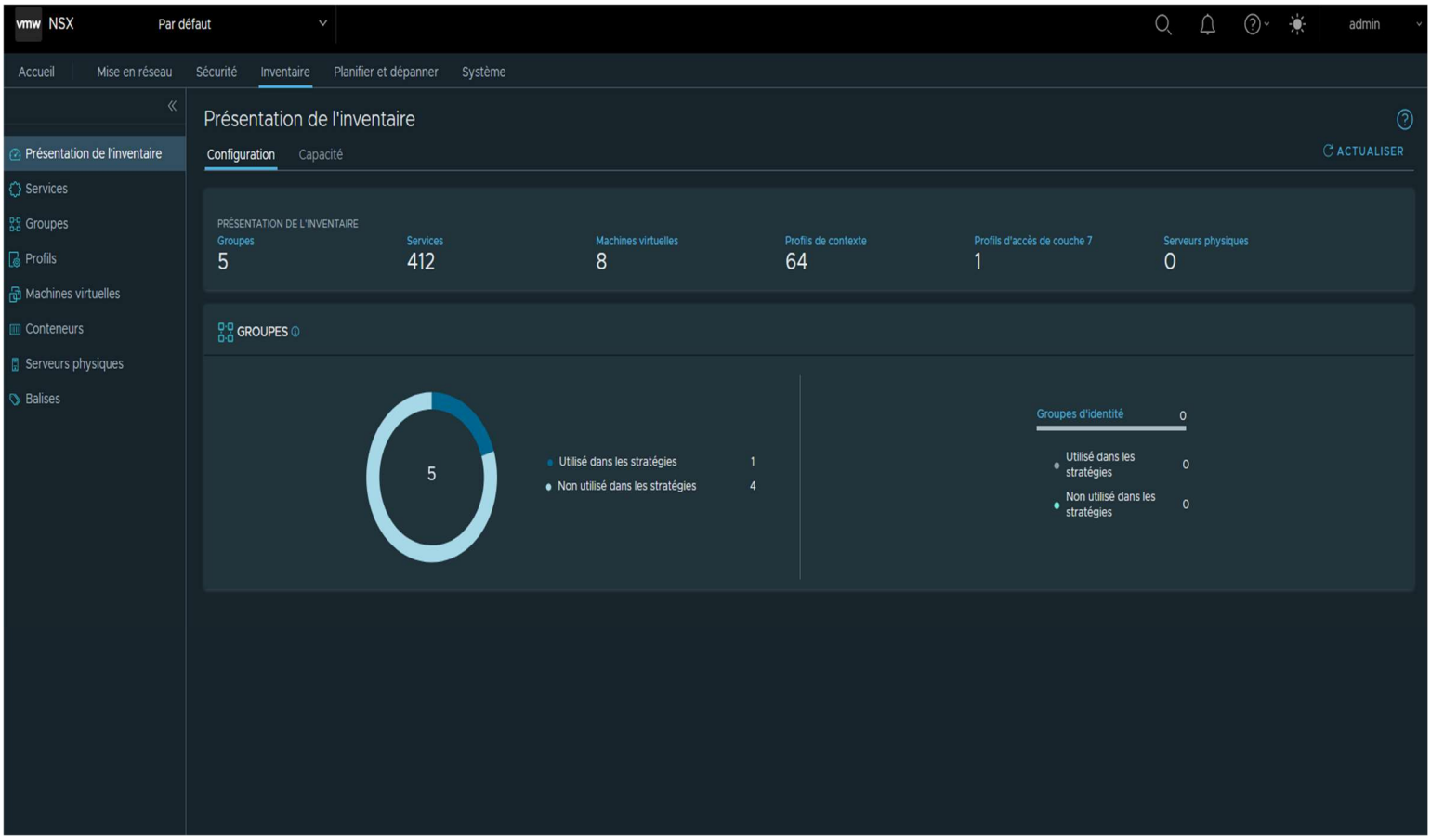

vmw NSX
Par défaut
admin
Accueil
Mise en réseau
Sécurité
Inventaire
Planifier et dépanner
Système
Présentation de la sécurité
Présentation de la sécurité
Surveillance des événements de menaces
Configuration
Capacité
Surveillance des événements de me...
IDS/IPS
Détections des menaces
Filtrage et analyse
Campagnes
IDS/IPS
Analyse du nom de domaine complet
Filtrage d'URL
Adresses IP malveillantes
Protection contre les programmes malveillants
Trafic suspect
Inspection TLS
Gestion des stratégies
Pare-feu distribué
Pare-feu de passerelle
IDS/IPS et Protection contre ...
Inspection TLS
Pour commencer à travailler avec les campagnes, vous devez activer la fonctionnalité NSX Network Detection and Response.
*NSX Application Platform doit être déployée avant que vous puissiez activer les fonctionnalités NSX que la plate-forme héberge.
ALLER À DÉPLOYER NSX APPLICATION PLATFORM
EN SAVOIR PLUS SUR NSX APPLICATION PLATFORM
Gestion de la chaîne de services
Introspection réseau E-O
Introspection réseau N-S
Règles de protection de poi...
Paramètres
Paramètres généraux
Introspection réseau

2.1.4 Inventaire

La partie dédiée à l'inventaire offre une vision détaillée des actifs présents au sein de l'écosystème virtuel.

Cette séparation comporte plusieurs modules, chacun contribuant à un panorama précis de l'inventaire :

- **Liste des machines virtuelles** : Cet affichage fournit un aperçu détaillé des machines virtuelles actives, de leurs attributs et de leurs emplacements.
- **Liste des serveurs physiques**: Cette partie fournit une vue d'ensemble des serveurs physiques et de leurs configurations.
- **Liste des services** : Cela permet de visualiser les services exécutés en temps réel et leurs comportements.



2.1.5 Système

La subdivision consacrée au système, propose une vision précise des aspects essentiels du fonctionnement du réseau virtuel.
Cette division divers modules, chacun contribuant à une vue analytique de l'état systémique :

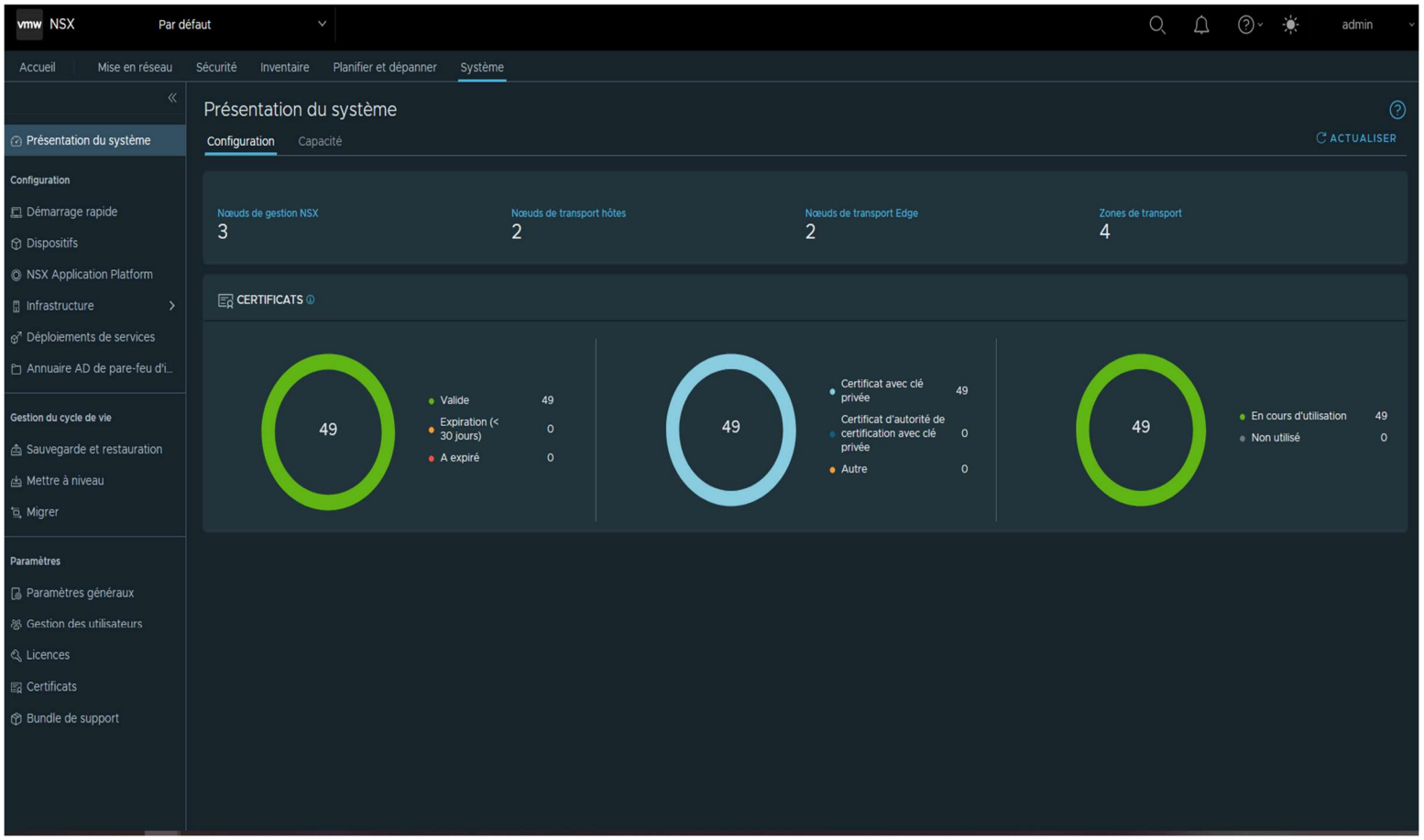
- **Événements Système** : Une portion cruciale du tableau de bord est allouée aux événements système. Elle dresse une liste des événements, des alertes et des incidents récents, assurant ainsi une visibilité sur les activités et les anomalies.

- **Ressources Virtuelles** : Un panneau notable s'attarde sur les ressources virtuelles. Il offre une vue synthétique de l'utilisation des ressources au niveau des machines virtuelles, y compris la consommation de CPU, de mémoire et de stockage.

- **Tendances de la Performance** : Une perspective dynamique est celle des tendances de la performance. Elle permet de suivre l'évolution des métriques clés au fil du temps, aidant ainsi à anticiper les besoins en ressources.

- **Gestion des certificats** : Permet la gestion des certificats de sécurité.

- **Gestion des licences** : Propose une vue d'ensemble des licences applicables aux différentes machines virtuelles et aux composants NSX.



3 Services de réseau et de sécurité NSX

3.1.1 Les services

Commutation :La commutation de paquets, ou commutation par paquets, ou encore transmission par paquets, est une technique utilisée pour le transfert de données informatiques dans des réseaux spécialisés.

Routage :Le routage est le mécanisme par lequel des chemins sont sélectionnés dans un réseau pour acheminer les données d'un expéditeur jusqu'à un ou plusieurs destinataires.

VPN :Les VPN servent à transmettre des données de manière sûre et anonyme sur des réseaux publics.

Equilibrage de charge : L'équilibrage de la charge est la pratique consistant à répartir les charges de travail informatiques entre deux ou plusieurs ordinateurs.

Protection par pare-feu : Un pare-feu est un logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau.

Détection et prévention des intrusions : La détection d'intrusion est le processus de surveillance de votre trafic réseau et d'analyse de celui-ci pour détecter des signes d'éventuelles intrusions.

Connectivités aux réseaux physiques :Interopérabilité avec les toutes les technologies existantes.

NAT :NAT (Network Address Translation) est un processus de modification des adresses IP et des ports source et de destination

DHCP : Dynamic Host Configuration Protocol est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station ou d'une machine, notamment en lui attribuant automatiquement une adresse IP et un masque de sous-réseau.


Commutation
Routage
VPN
Équilibrage de charge
Protection par pare-feu
Détection et prévention des intrusions
Connectivité aux réseaux physiques
NAT
DHCP
MetaData Proxy

4 Distributed vSwitch

NSX repose sur un commutateur virtuel, ou vSwitch, exécuté sur les hôtes ESXi.
Un vSwitch est un composant en mode noyau exécuté sur l'hôtes de virtualisation qui effectue le transfert de trame Ethernet pour les VM.

Chaque VM se connecte au vSwitch via un ou plusieurs adaptateurs réseau virtuels(vNIC).
Une vNIC remplit les mêmes fonctions qu'une carte d'interface réseau physique : elle encapsule et désencapsule les trames Ethernet, puis les envoie et les reçoit vers et depuis le port de commutateur auquel il est connecté.

Dans un hôte ESXi, la vNIC de la VM se connecte à un port virtuel sur le vSwitch.
Sans NSX, le vSwitch peut uniquement transférer le trafic entre les VM locales et les liaisons montantes physiques.

L'infrastructure physique est alors responsable du transfert approprié du trafic entre les hôtes.
Avec NSX, le vSwitch peut atteindre les hôtes distants directement via des tunnels de superpositions : NSX peut ainsi contrôler le transfert du trafic sans s'appuyer sur les décisions de l'infrastructure physique.

4.1 La commutation logique NSX

La commutation logique, revêt la capacité de rediriger intelligemment le flux de données entre les machines virtuelles (VM) au sein d'un environnement virtualisé.

4.1.1 Défis liés à la commutation des Data Centers traditionnels

- Segmentation mutualisée ou applicative.
- Exigence de mobilité des VM de la couche 2.
- Besoin de grands réseaux de couche 2, ce qui entraîne des domaines de broadcast.

4.1.2 Avantages de la commutation logique

- Gestion scalable de la mutualisation à l'échelle du Data Center.
- Possibilité d'utiliser la topologie physique existante.
- Activation de réseaux de couche 2, appelés segments sur l'infrastructure de couche 3 à l'aide de réseaux de superposition.
- Segments qui s'étendent sur des hôtes physiques et des commutateurs de réseau

4.1.3 Schéma commutation logique

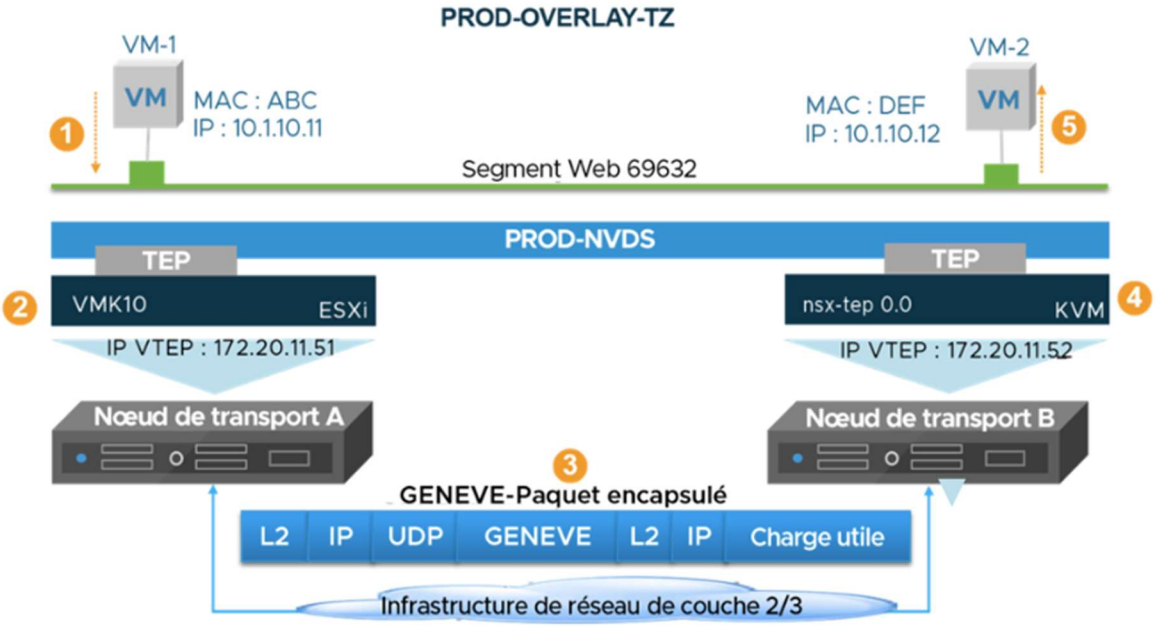


Figure 18.Schéma commutation logique

Explication du schéma :

- 1 La VM envois un paquet
- 2 le paquet transite par la TEP(encapsulation
- 3 le paquet est encapsulé avec les informations de destination(VNI etc…)
- 4 le paquet a rejoint la TEP de destination (désencapsulassions)
- 5 le paquet est arrivé à destination

5 Le routage logique

5.1.1 Routeur distribué(DR)

Le routeur distribué, dans son essence, agit comme une entité de routage hautement adaptable, orchestrée pour diriger les paquets de données entre les segments virtuels en employant des itinéraires optimisés

- Exécuté localement dans les nœuds de transport qui participent au fabric NSX.
- Généralement exécuté en tant que module de noyau dans l'hyperviseur.
- Fournit un routage distribué dans l'environnement réseau logique.
- Le traffic entre différents sous-réseaux d'un même hyperviseur ne quitte pas l'hyperviseur.

5.1.2 Routeur de services(SR)

L'essence même d'un routeur de services repose sur sa capacité à offrir un routage défini par logiciel, orchestré pour diriger les paquets de données entre diverses destinations virtuelles.

- Responsable de la fourniture de services de passerelle on/off, y compris le routage N/S.
- Fournit des services centralisés tels que NAT,BGP,LB et Edge, la connectivité au réseau physique.
- Le SR est instancié sous forme de service sur une appliance nommée le nœud Edge

6 Distributed Firewall

Le pare-feu distribué sert à exercer un contrôle granulaire sur les flux de données au sein des réseaux virtuels.

Voici quelques-unes de ses fonctions clés :

- **Micro-segmentation Sécurisée** : Le pare-feu distribué divise le réseau virtuel en segments plus restreints, permettant de contrôler précisément le trafic entre les machines virtuelles. Cela élève la sécurité en limitant la surface d'attaque et en empêchant la propagation latérale des menaces.

- **Gestion Centrale des Politiques** : Grâce à une gestion centralisée des politiques de sécurité, le pare-feu distribué offre une vision holistique sur l'ensemble de l'infrastructure. Cela garantit la cohérence des règles de sécurité à travers différents segments.

- **Filtrage de Paquets Avancé** : Ce pare-feu exerce un filtrage de paquets précis à l'échelle des machines virtuelles. Il peut s'appuyer sur des critères variés tels que les adresses IP, les ports, les protocoles et même les attributs spécifiques des charges de travail.

- **Détection des Menaces** : Grâce à l'inspection approfondie des paquets, le pare-feu distribué peut identifier les signes de comportements malveillants ou d'anomalies dans le trafic réseau. Ceci contribue à prévenir les attaques.

- **Intégration avec les Flux de Travail** : En s'intégrant étroitement avec les processus de déploiement et d'évolutivité des machines virtuelles, le pare-feu distribué garantit que la sécurité n'est pas un obstacle aux initiatives de développement.

- **Réduction de la Complexité** : La distribution de la sécurité à l'intérieur de l'infrastructure élimine le besoin d'une concentration unique de contrôle, ce qui allège la complexité et améliore la résilience.

- **Évolutivité Agile** : Le pare-feu distribué est en mesure de s'étendre en parallèle avec l'expansion de l'environnement virtuel, maintenant ainsi une protection constante au fil de la croissance.

7 Edge node

Le nœud agit comme une passerelle entre le réseau virtuel et le réseau physique externe (encapsule et désencapsule avec le protocole Geneve).

Il remplit plusieurs rôles cruciaux :

- **Routage et commutation avancés** : Le nœud périphérique est capable de prendre des décisions de routage complexes, ce qui permet de diriger le trafic entre les différents segments virtuels et les réseaux physiques. Il peut également effectuer des opérations de commutation de paquets pour optimiser le flux de trafic.

- **Services de sécurité** : Le nœud périphérique joue un rôle vital dans la sécurité du réseau. Il peut mettre en œuvre des pares-feux, des services de détection et de prévention d'intrusion, ainsi que des services de répartition de charge pour assurer la disponibilité et la sécurité des applications.

- **VPN (Virtual Private Network)** : Les nœuds périphériques peuvent fournir des fonctionnalités VPN pour établir des connexions sécurisées entre les réseaux virtuels et les sites distants, permettant ainsi une connectivité sécurisée sur des réseaux non confiants, comme Internet.

- **Optimisation de la performance** : Grâce à la gestion avancée du trafic, les nœuds périphériques peuvent optimiser la performance du réseau en appliquant des politiques de qualité de service (QoS) pour garantir la bande passante aux applications critiques.

- **Gestion et visibilité** : Les nœuds périphériques fournissent des outils de gestion et de surveillance pour le réseau virtuel. Cela inclut la collecte de statistiques de trafic, la génération de journaux, et la capacité de dépannage pour identifier et résoudre rapidement les problèmes réseau.

Figure 19.Edge Node

8 Le protocole Geneve

NSX utilise une encapsulation appelée GENEVE pour ses tunnels.
GENEVE ressemble fortement à VxLAN, avec une fonctionnalité supplémentaire : la prise en charge de champs TLV (Type, Lenght, Value) dans son en-tête.

Cela permet de transporter des métadonnées qui ne sont pas strictement définies dans la norme et rend GENEVE très flexible, ce qui permet à NSX de s'adapter au développement futur du réseau.

Comme VxLAN, GENEVE contient également des champs de longueur fixe, comme l'identifiant de réseau virtuel (VNI) 24 bits.
Grâce au VNI, plusieurs segments (overlay) peuvent être transportés par le même GENEVE entre deux TEP.

L'encapsulation générique de virtualisation du réseau (GENEVE) est un mécanisme de tunnelisation de superposition IETF assurant l'encapsulation de la couche 2(L2) sur la couche 3(L3) des paquets de données.

Les paquets encapsulés dans GENEVE sont communiqués de la manière suivante :

- Le terminal de tunnel(TEP) sur le nœud de transport source(TN) encapsule la trame Ethernet(couche2) de la VM dans un paquet GENEVE/UDP/IP/ETH.

- Le paquet encapsulé est transmis au terminal TEP de destination sur le port UDP/6081.

- Le TEP de destination désencapsule le paquet et fournit la trame source à la VM de destination.

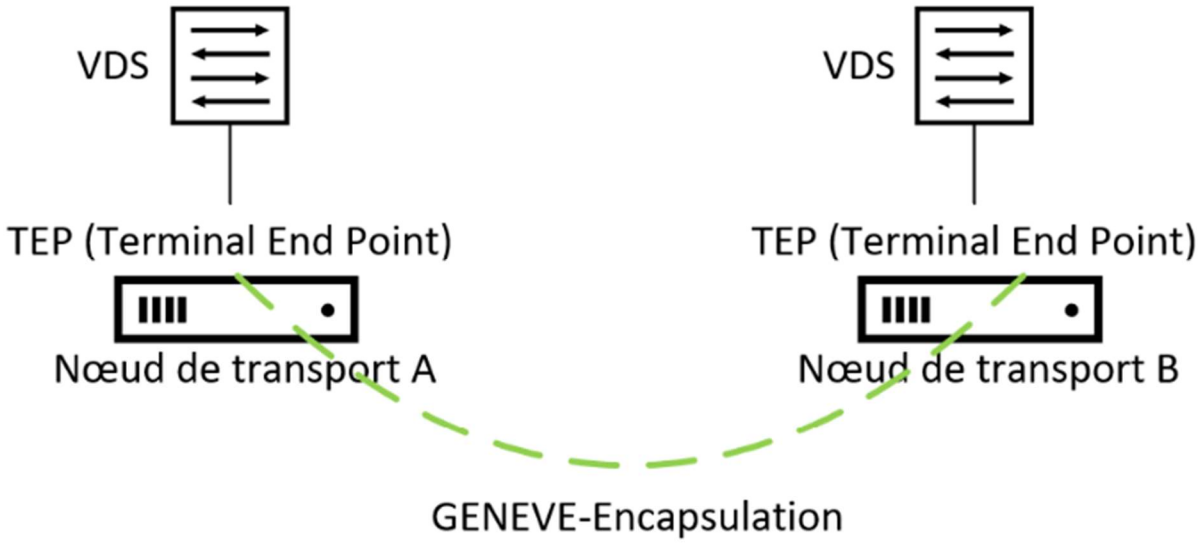


Figure 20.Encapsulation des données

8.1 Interface TEP (Terminal End Points)

Le tunnel terminal (TEP) est le composant qui termine un tunnel sur un nœud de transport.
Il a une adresse IP routable dans l'infrastructure physique (les TEP sont représentées par des vmks sur les hôtes ESXi).

Le trafic tunnelisé entre les nœuds de transport est uniquement considéré par l'infrastructure physique comme un trafic IP entre des TEP, quel que soit le type de trafic de couche 2 transporté par le tunnel.

8.2 Segments

Les segments (overlay) NSX sont regroupés sous une structure logique appelée zone de transport.

Les hôtes associés à une zone de transport donnée ont accès à tous les segments définis dans la zone de transport.

La zone de transport définit ainsi l'étendue du segment dans le réseau(c'est-à-dire les hôtes sur lesquels les segments sont disponibles).

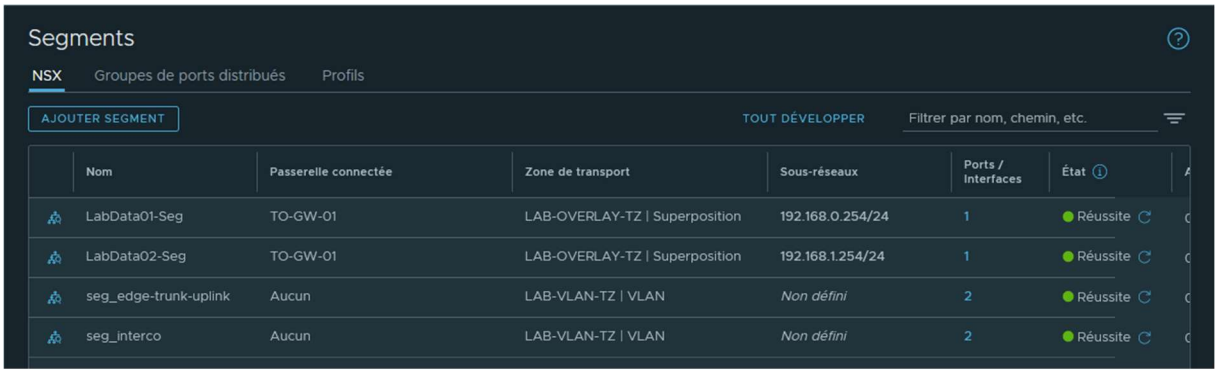


Figure 21.Segments

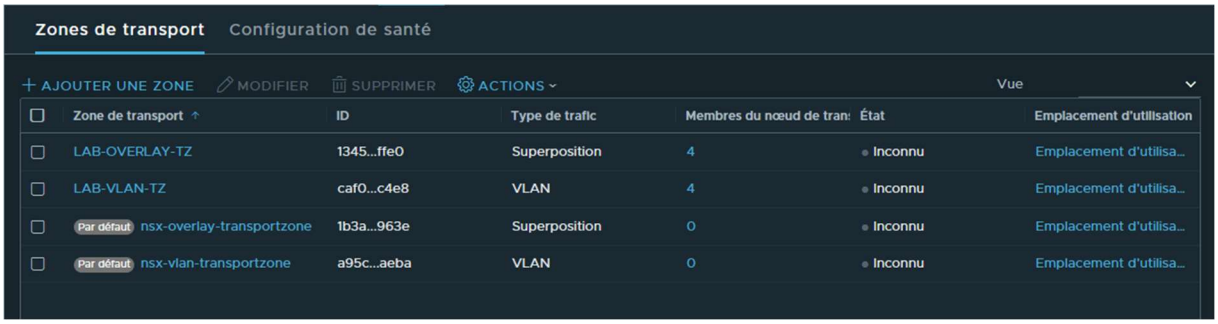


Figure 22.Zones de transport

Schéma et vue de la maquette

1 Vue physique

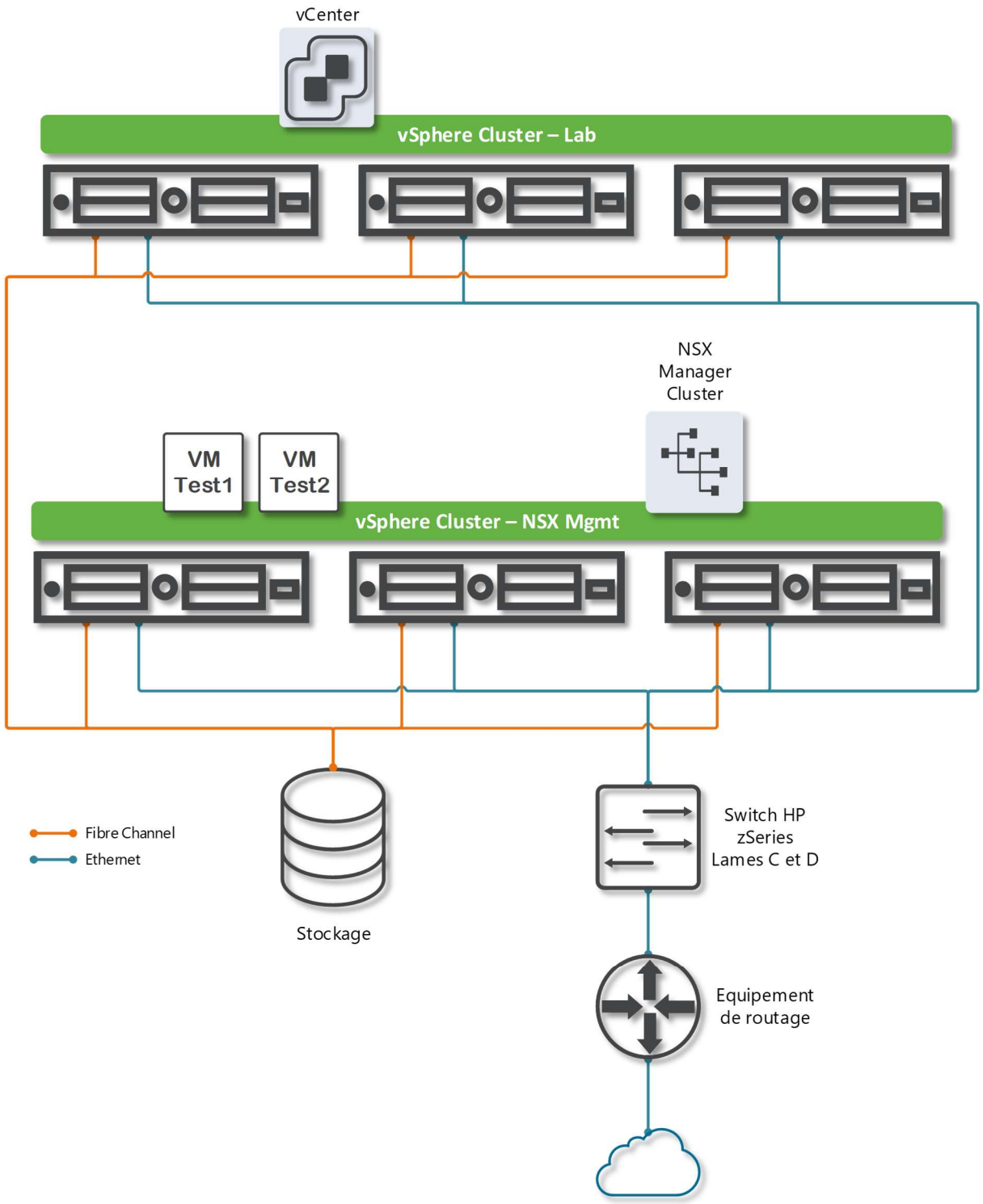


Figure 23.Vue physique

Sur ce schéma, j'ai dépeint les composants qui composent ma maquette, à savoir les éléments serveurs, le routeur, le système de stockage, le commutateur réseau, ainsi que l'infrastructure de connectivité, incluant les fibres optiques et les câbles.

2 Vue logique

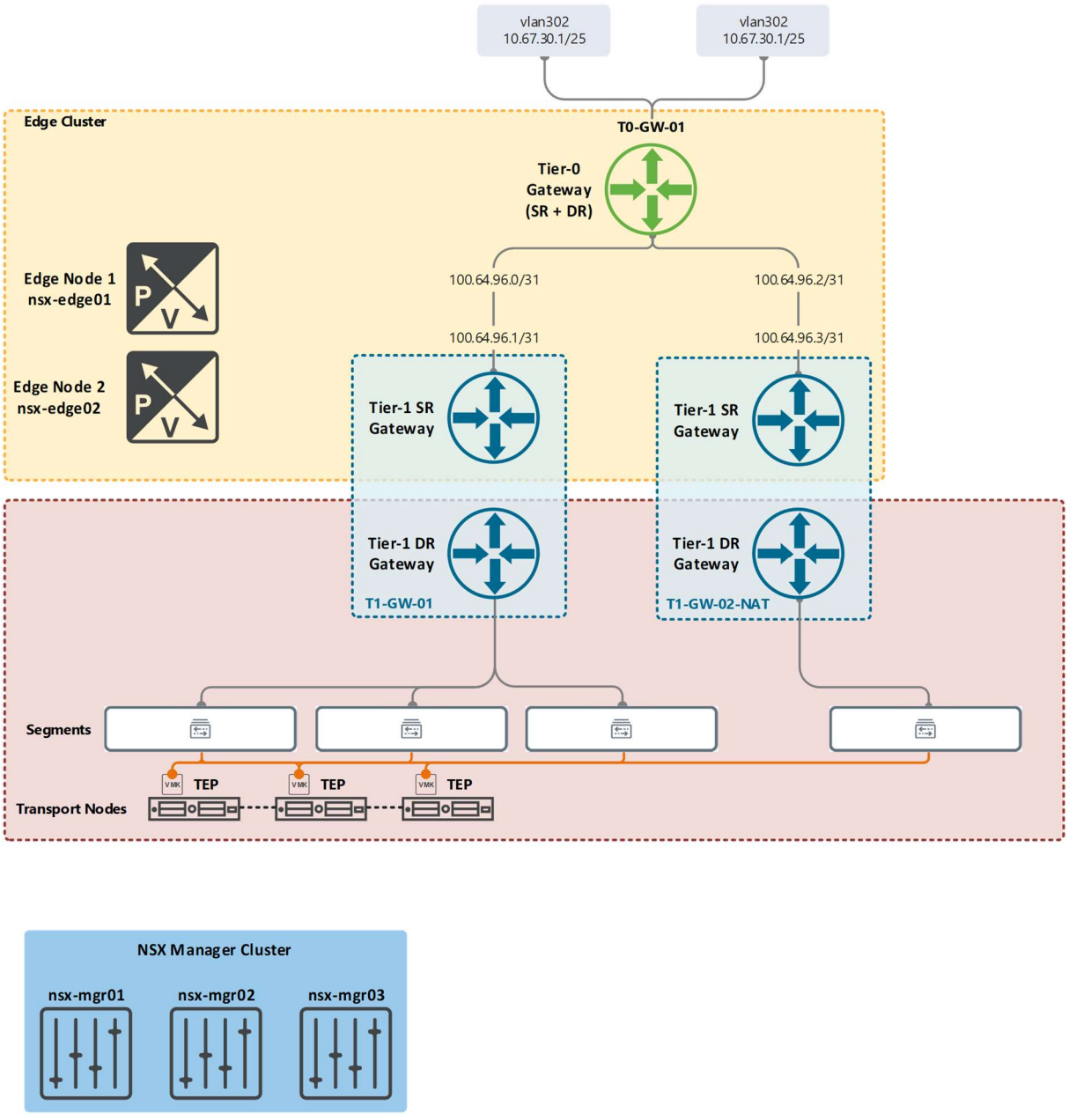


Figure 24.Vue logique

La vue logique reprend de manière exhaustive les segments, les TEP (Terminating End Points) de mes serveurs, les nœuds de transport et les passerelles (Gateway).

3 Vue réseau

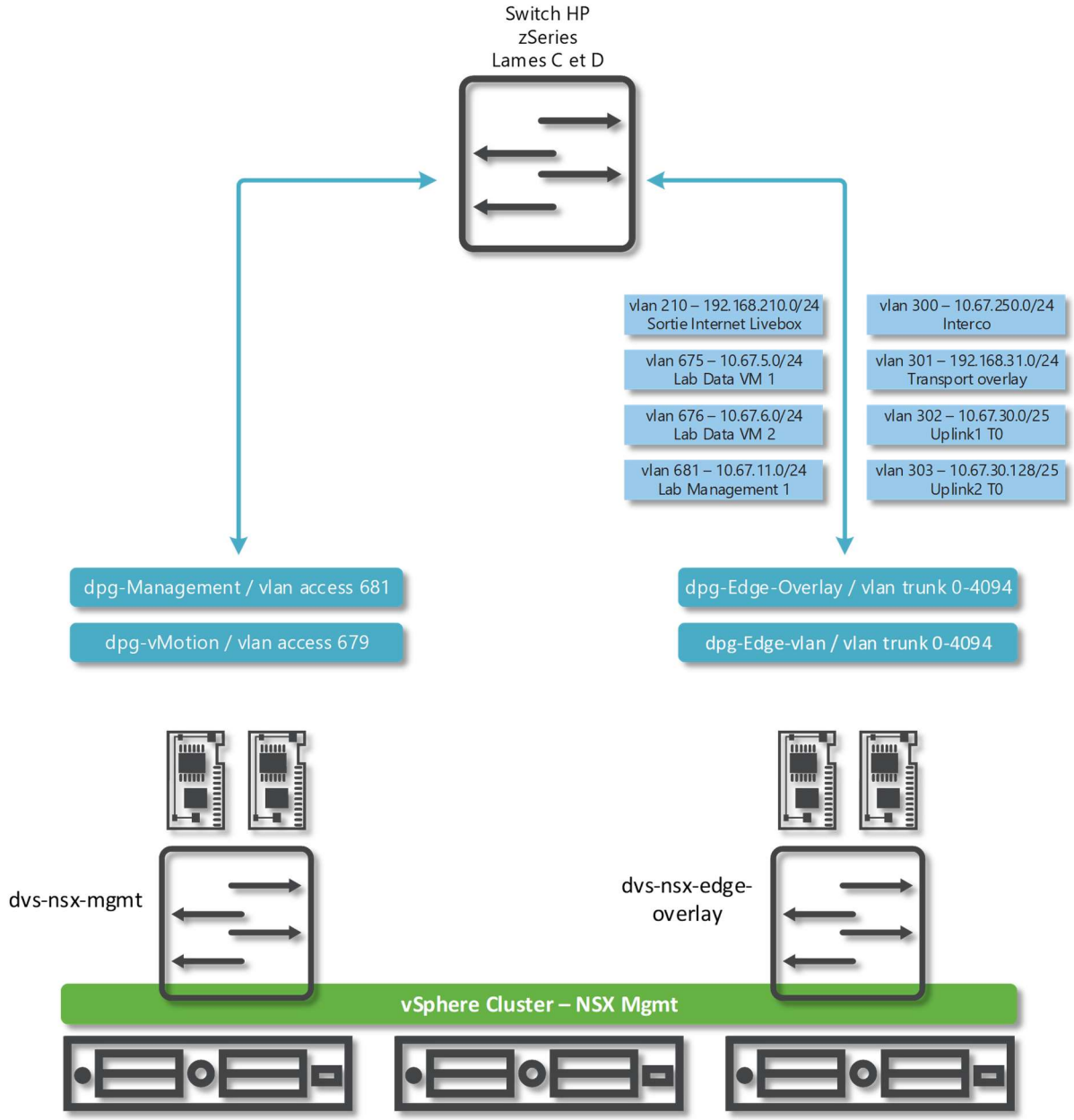


Figure 25.Vue réseau

Cette vue englobe les VLAN (Virtual LANs) ainsi que mon schéma d'adressage IP. Elle offre une vision globale de la manière dont les adresses IP sont attribuées aux différents VLANs.

Cette organisation permet de garantir une segmentation logique claire et de favoriser une utilisation optimale de l'espace d'adressage IP.

4 Vue réseau ESXI-01

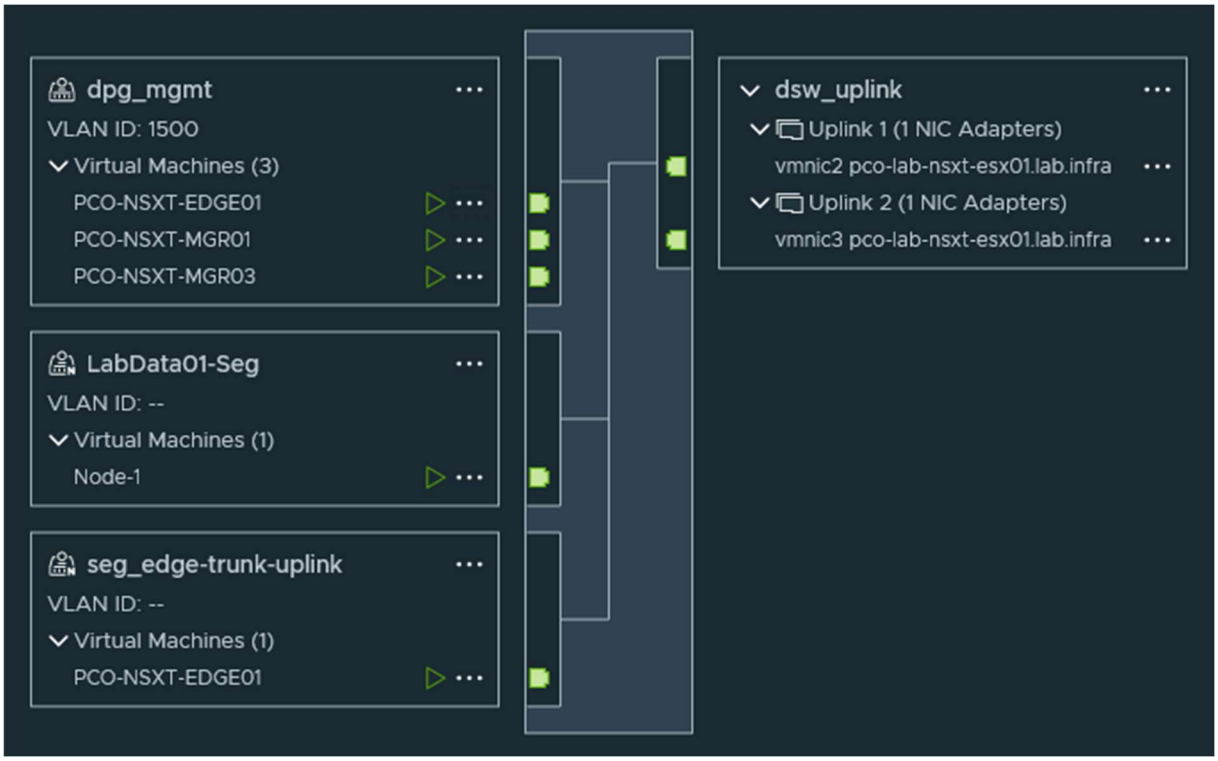


Figure 26.Vue réseau ESXI-01

5 Vue réseau ESXI-02

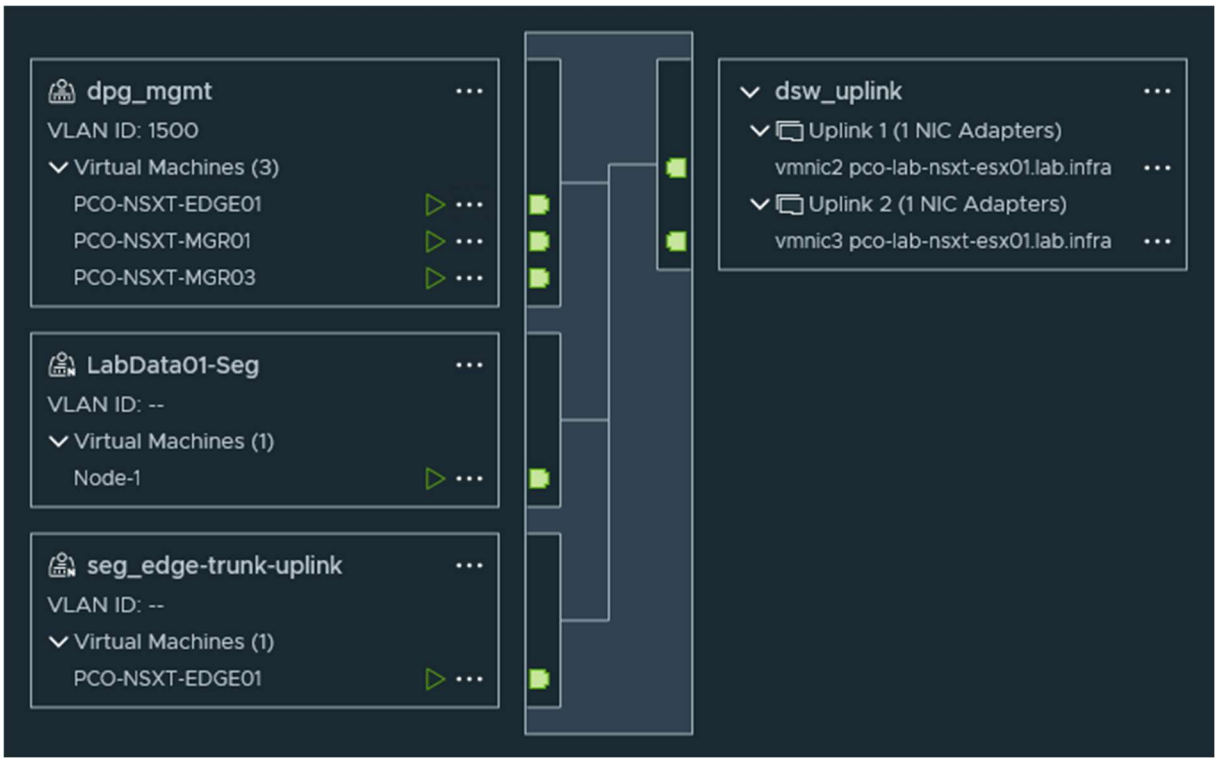


Figure 27.Vue réseau ESXI-02

5.1.1 Résumé des vues ESXI-01 et ESXI-02

Les deux vues illustrées ci-dessus (ESXI-01, ESXI-02) présentent divers éléments que je vais décrire en détail.
Du côté droit de la vue réseau, on peut observer les Up Links, correspondant aux cartes réseau des serveurs physiques.

Ces liens établissent la connexion entre la couche virtualisée et la couche physique de l'infrastructure.

À gauche de l'image capturée, les composants virtualisés par la solution NSX sont identifiés :

- DPG pour Distributed Port Group, représentant un groupe de ports distribués.
- Mon premier segment, marquant la création d'un segment spécifique.
- Un segment Trunk, favorisant le passage des VLANs entre les deux environnements ESXI.

Cette configuration démontre la manière dont les éléments virtualisés et physiques s'intègrent pour assurer la connectivité et la gestion au sein de l'architecture.

Tests

1 Micro-segmentations et Routage TIER-1 /Est-Ouest

L'objectif de ce test consiste à élaborer deux segments distincts et à établir deux machines virtualisées sous Debian, tout en instaurant une interaction mutuelle entre elles.
Une machine virtualisée est assignée à chaque segment, chacun possédant un sous-réseau distinct.

Un segment Trunk, assurant la transmission des VLANs, est conçu pour les deux environnements ESXI.
Je prévois également de mettre en place une Gateway TIER-1 pour faciliter un routage logique bidirectionnel (Est-Ouest) entre les segments.

La communication entre les hôtes et les machines virtuelles s'exécute via l'usage de VLANs et l'entremise d'un commutateur de couche 2 conformément au modèle OSI.

Afin de permettre auxdits segments d'échanger des données avec les éléments au sein de NSX (tels qu'Internet et les autres segments), il devient impératif d'ajouter une interface aux passerelles TIER-1.

1.1.1 Création Gateway TIER-1

En premier lieu, il est essentiel de mettre en place une passerelle de sortie (Gateway) afin de permettre la communication entre les différents segments.
Cette passerelle permet l'échange d'informations entre les segments concernés.

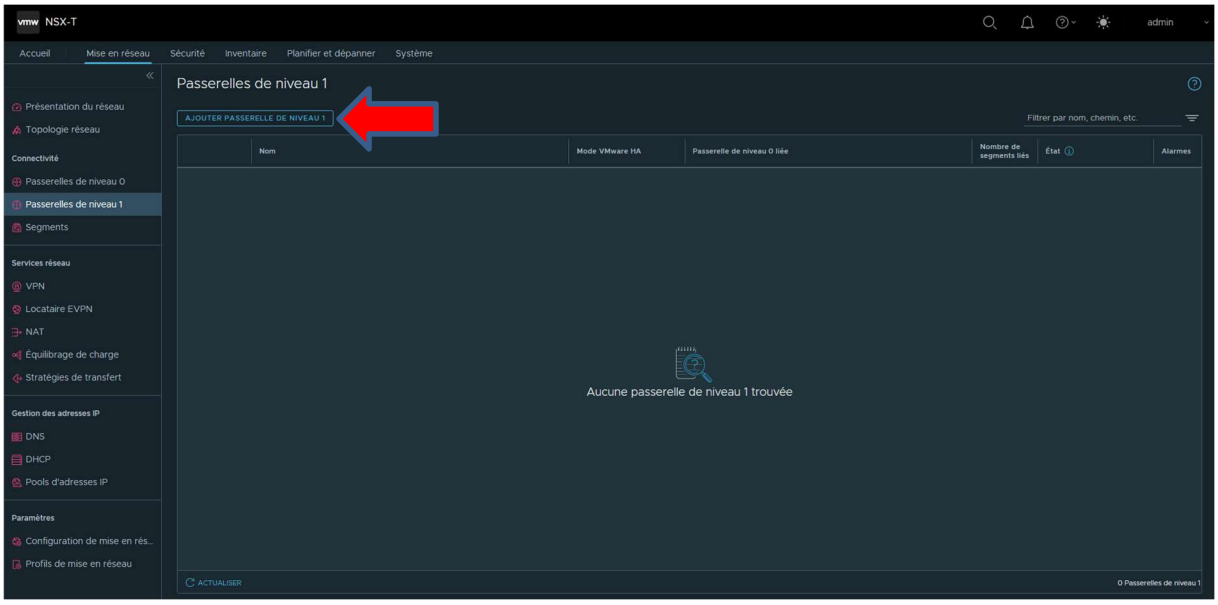


Figure 28.Gateway TIER-1

Je configure la passerelle de manière à établir la connexion entre les segments à venir.

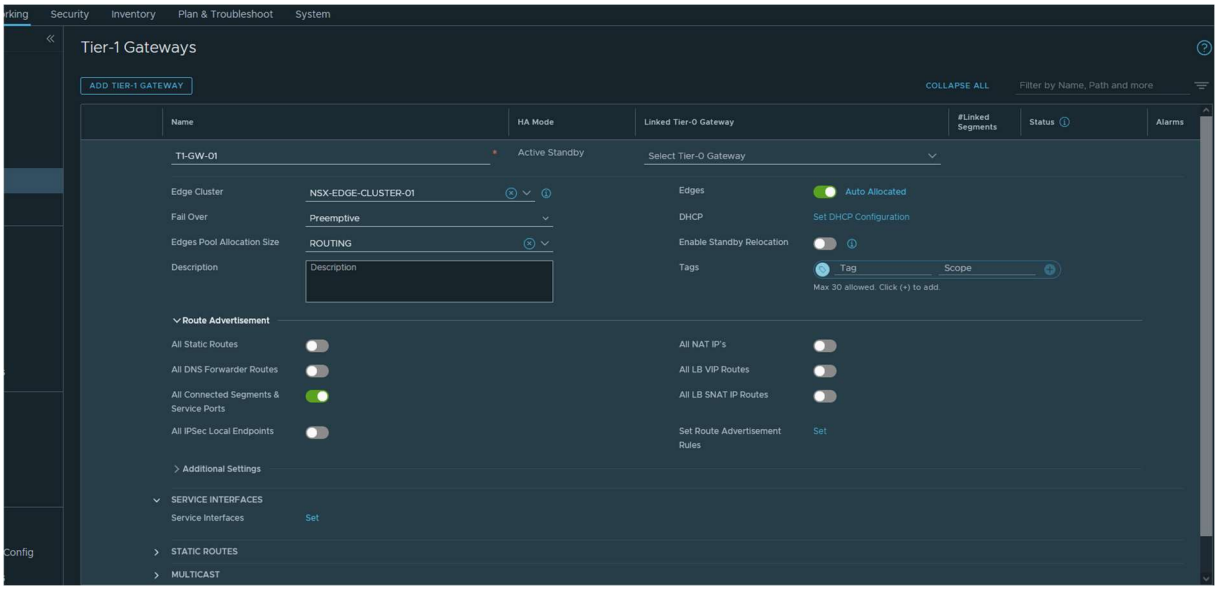


Figure 29Gateway TIER-1

Une fois la passerelle créée, je passe à l'étape de création de mes segments.

1.1.2 Segments 01

Je débute en créant un segment de type overlay dans l'interface NSX.
Mon premier objectif est de concevoir un segment overlay qui sera associé à notre Gateway TIER-1. Pour ce faire, je saisis les renseignements suivants :

- Nom : le nom choisi pour le segment.
- Gateway Connectée : la passerelle préalablement établie.
- Zone de Transport : la zone déjà définie.
- Sous-réseau : l'adresse de la passerelle du segment, au format requis.

Il est à noter que ces segments constituent des domaines virtuels de niveau 2.
Ils sont intrinsèquement liés à des zones de transport, préconfigurées en amont.
À cette étape, je procède à la connexion de ma machine virtuelle au segment nouvellement créé.

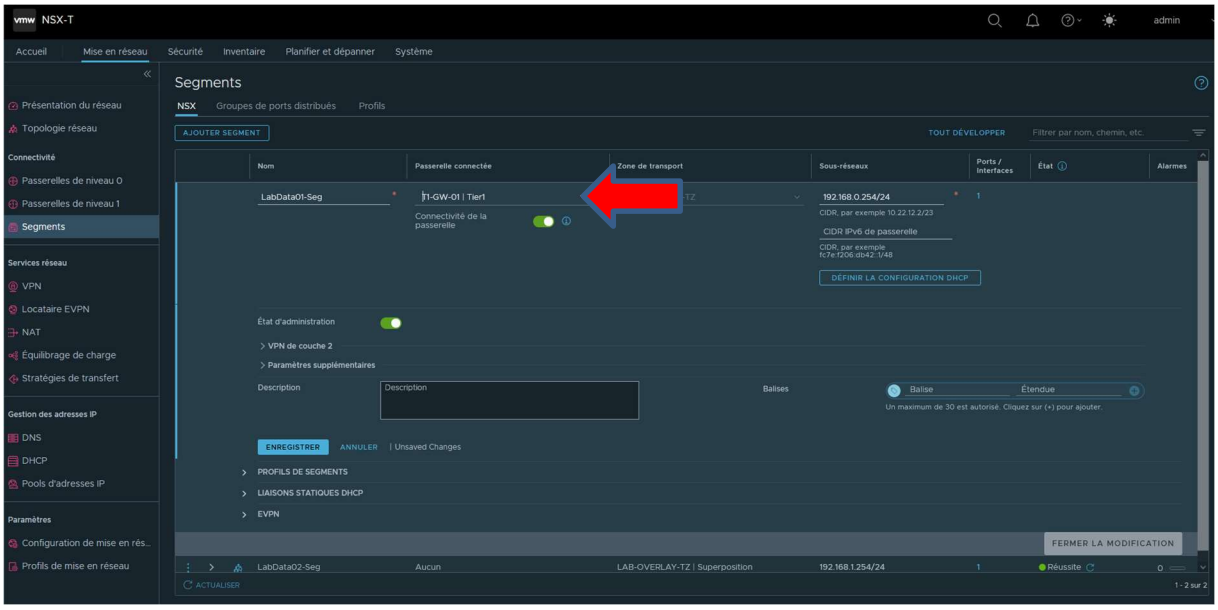


Figure 30.Segments 01

1.1.3 Segments 02

À présent, je génère mon deuxième segment.

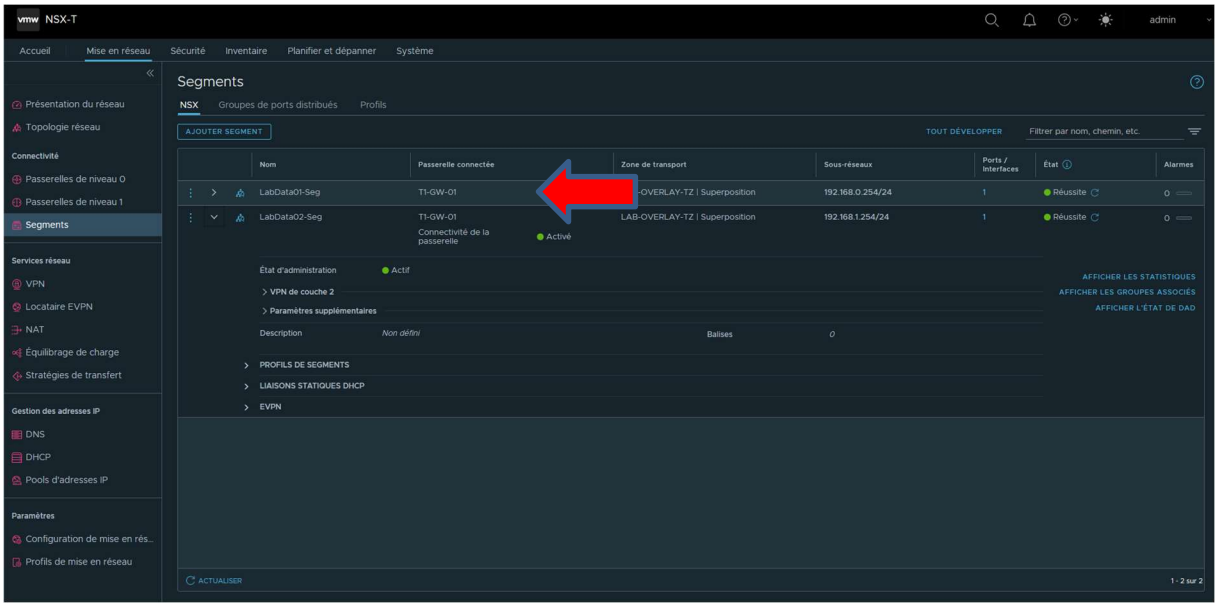


Figure 31.Segments 02

Ensuite, je procède à la configuration de la passerelle que j'ai préalablement créée pour les deux segments.

1.2 Création d'un segment VLAN

De plus, j'ai mis en place un segment VLAN en fournissant les détails suivants :

- Nom : le nom désigné pour le segment VLAN.
- Zone de Transport : sélection de la zone de transport appropriée.
- VLAN : saisie du numéro de VLAN requis.
- Sous-réseaux : spécification de l'adresse et de l'étendue de la passerelle du segment.

1.3 Connexion d'un segment VLAN à la Gateway TIER-1

Il existe la possibilité d'acheminer le trafic issu d'un segment de type VLAN vers Internet et les autres segments en établissant une interface sur la passerelle TIER-1. Au moment de concevoir cette interface, il est impératif d'utiliser l'adresse IP identique à celle spécifiée dans le sous-réseau du segment concerné.

1.3.1 Ajout d'une interface

Je fournis les informations suivantes :

- Nom : nom à attribuer au VLAN ainsi qu'à l'interface.
- Adresse IP / Masque : l'adresse IP de l'interface, en adéquation avec la passerelle.
- Connecté À (Segment) : je sélectionne le segment VLAN que j'ai créé.

1.3.2 Installation des machines de tests

Je déploie deux machines virtuelles sous Debian 12 Bookworm, en mode non graphique.
Par la suite, j'établis la connexion entre les segments et les machines virtuelles. Je procède à la configuration des cartes réseau des machines en attribuant des adresses IP statiques.

1.3.3 Test de connectivité « ping »

Je me connecte en SSH aux deux machines et je vérifie initialement que les adresses IP concordent en exécutant la commande suivante :

ip a

Par la suite, j'effectue un test de connectivité en utilisant la commande :

ping AdresseIPDeLaMachine

Les spécifications des machines de test sous Debian 12 "Bookworm" sont les suivantes :

- Pour Segment01 : Adresse IP 192.168.0.1
- Pour Segment02 : Adresse IP 192.168.1.1

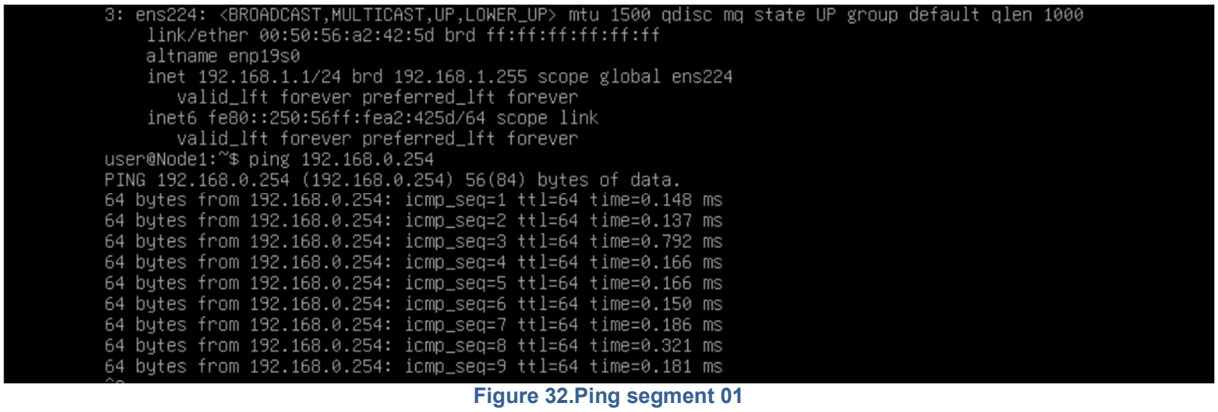


Figure 32.Ping segment 01

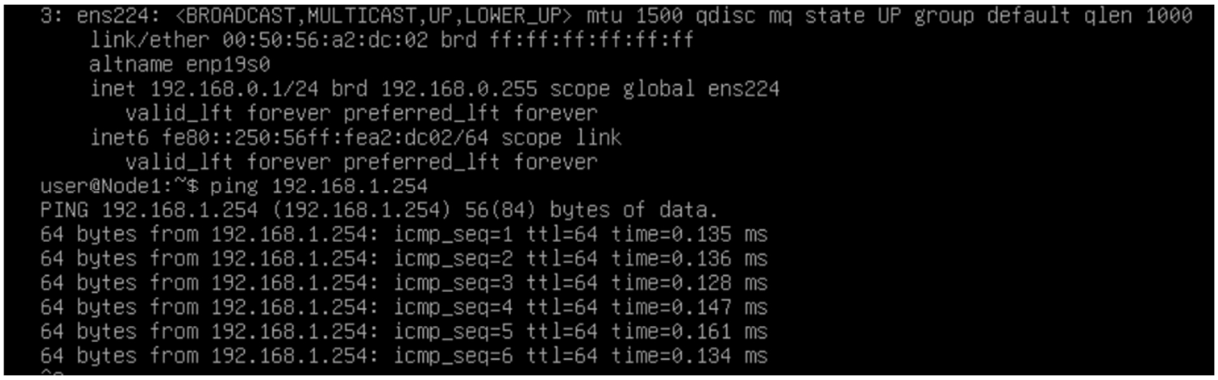


Figure 33.Ping segment 02

Les deux machines sont capables de se pinguer mutuellement malgré leur présence sur deux segments distincts.
La passerelle, l'interface et les segments remplissent efficacement leurs fonctions assignées, facilitant ainsi la communication entre les segments.

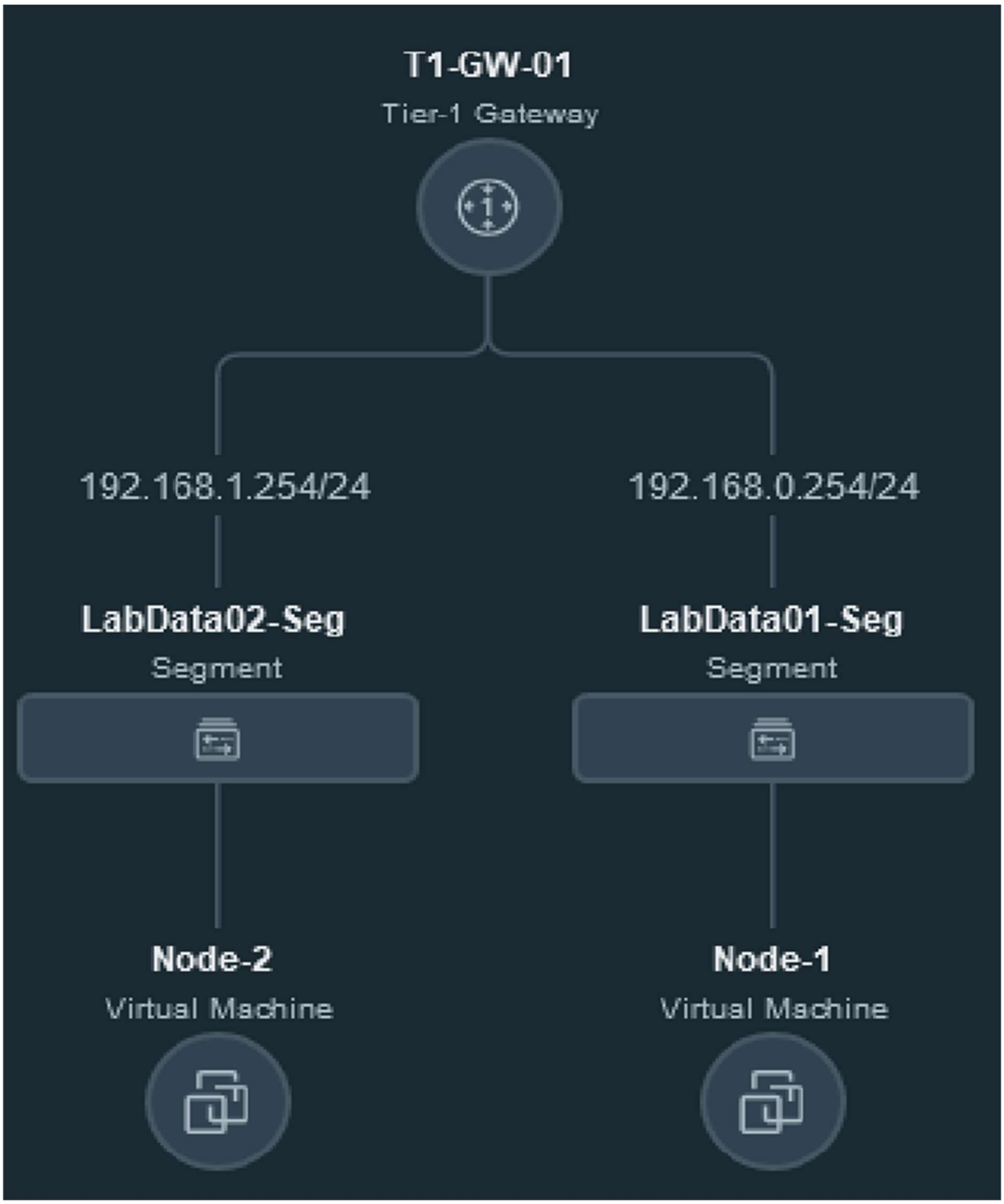


Figure 34Segment 1 et 2 + Gateway

1.3.4 Routage entre deux segment avec le même subnet

L'un des avantages majeurs offerts par NSX, la micro-segmentation et le protocole GENEVE réside dans leur capacité à permettre la communication de plusieurs segments partageant le même sous-réseau.

En effet, le protocole GENEVE, en exploitant le VNI (Virtual Network Identifier) et le TEP (Terminal End Point), résout efficacement divers problèmes de ce genre grâce à son mode opératoire.

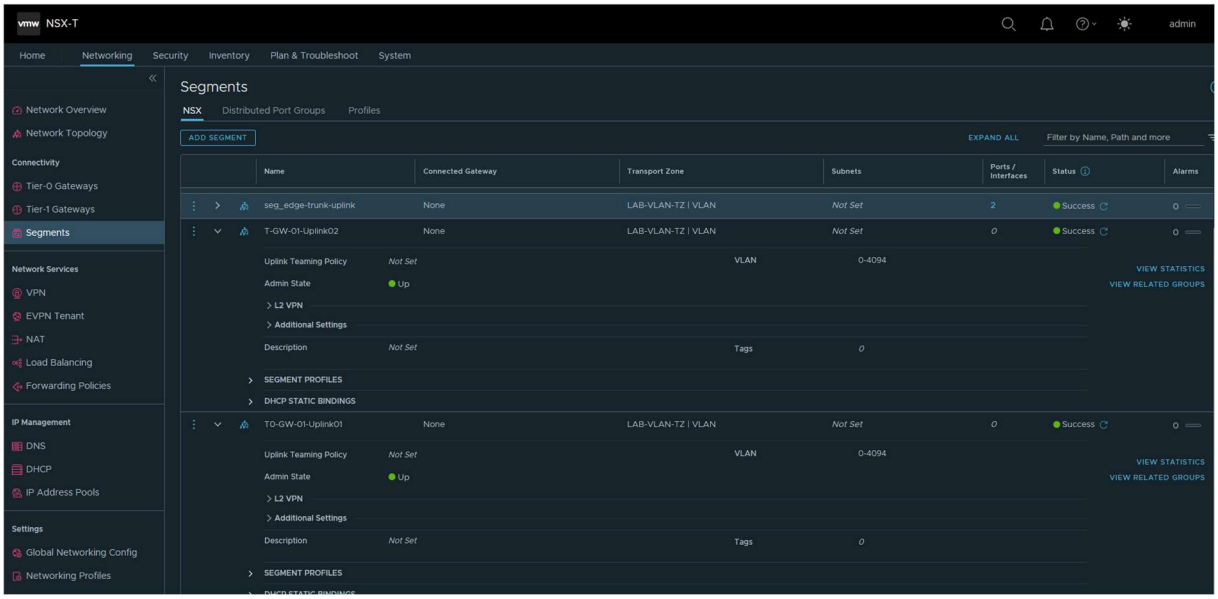
1.3.5 Règles de filtrage entre VM du même segment

La configuration de règle de pare-feu entre deux machines virtuelles sur le même segment est possible.
On peut alors décider de laisse passer ou non certains flux entre les deux VM du même segment.

2 Routage TIER-0/Nord-Sud

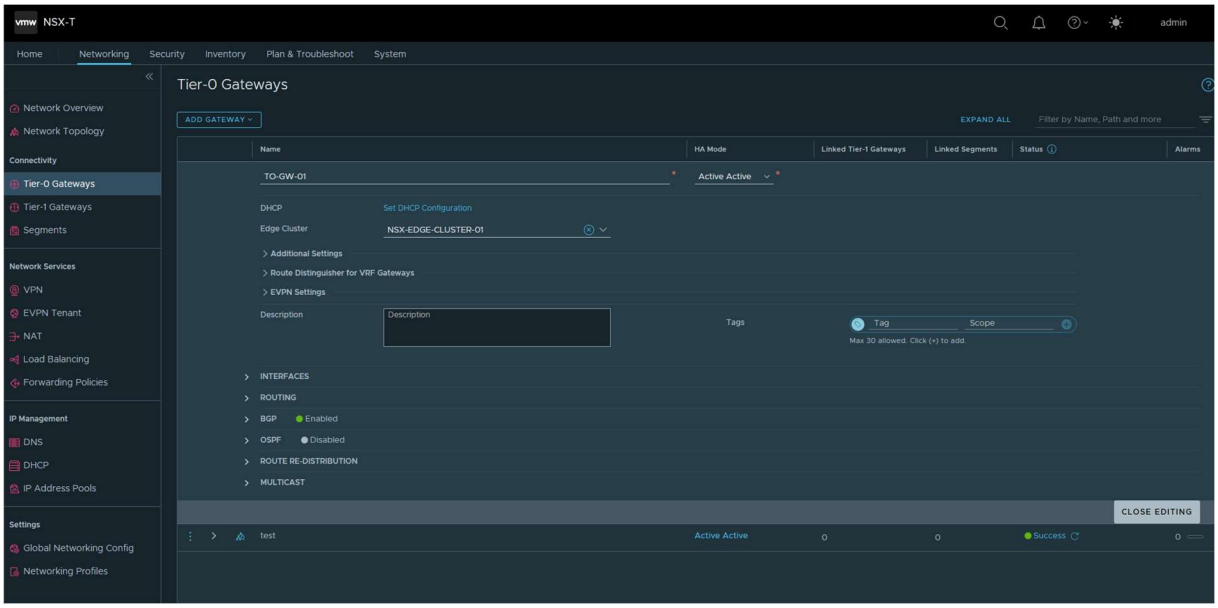
2.1.1 Segments d'uplink

Je configure deux segments d'uplink pour mon cluster de nœuds de périphérie (edge nodes).



2.1.2 Gateway TIER-0

Je suis la même procédure que lors de la création de ma passerelle de niveau TIER-1.



2.1.3 Configuration OSPF

Le protocole OSPF est un protocole de routage opérant selon le principe d'état de liens.
Grâce à OSPF, lorsqu'un routeur détecte une modification au sein de sa table de routage ou une transformation dans la topologie du réseau, il propage instantanément cette information en mode multidiffusion à tous les autres hôtes utilisant également OSPF au sein du réseau.

En conséquence, ces hôtes se voient dotés d'une table de routage renfermant les mêmes données actualisées.

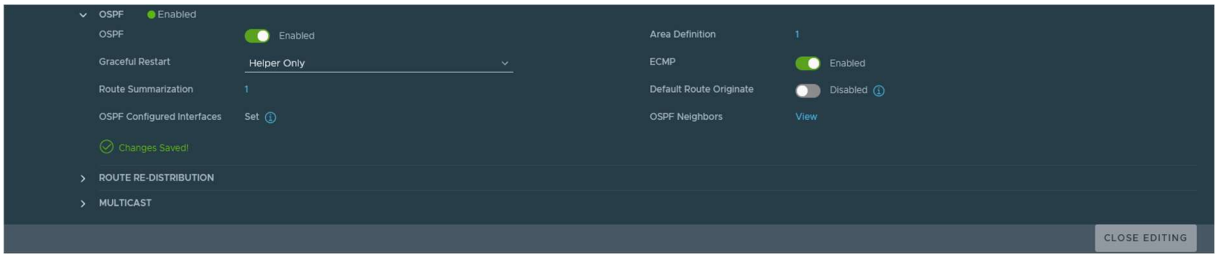


Figure 35.OSPF configuration

Je procède désormais à la configuration des routes OSPF.
Je sélectionne un sous-réseau ainsi qu'un CIDR approprié pour cette étape.

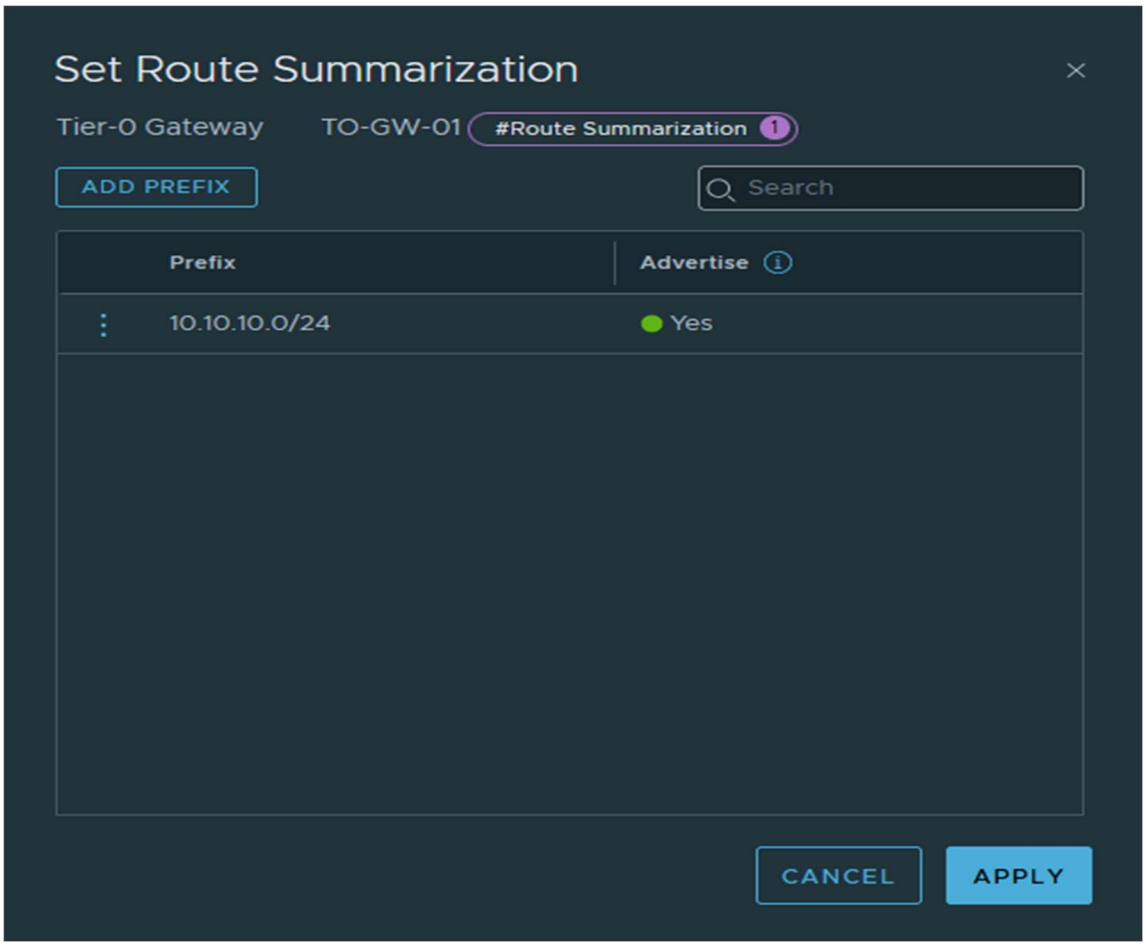


Figure 36.OSPF Summarization

Il existe des outils comme :

https://www.calcip.com/route-summarization/

Pour faire du calcul de route OSPF.

3 La sauvegarde sous NSX

La solution NSX offre la possibilité d'établir des sauvegardes quotidiennes ou périodiques de manière intrinsèque pour vos serveurs et configurations.
Cette fonction de sauvegarde peut être configurée aisément et peut être restaurée en cas d'incidents.

3.1.1 Configuration

Dans la section dédiée à la sauvegarde, je débute en complétant les détails du serveur distant :

- Adresse IP
- Port
- Chemin de l'arborescence où la sauvegarde sera stockée sur le serveur distant
- Identifiant de connexion (login) et mot de passe

Une empreinte SSH est générée la sécurité de la connexion SSH vers le serveur distant.

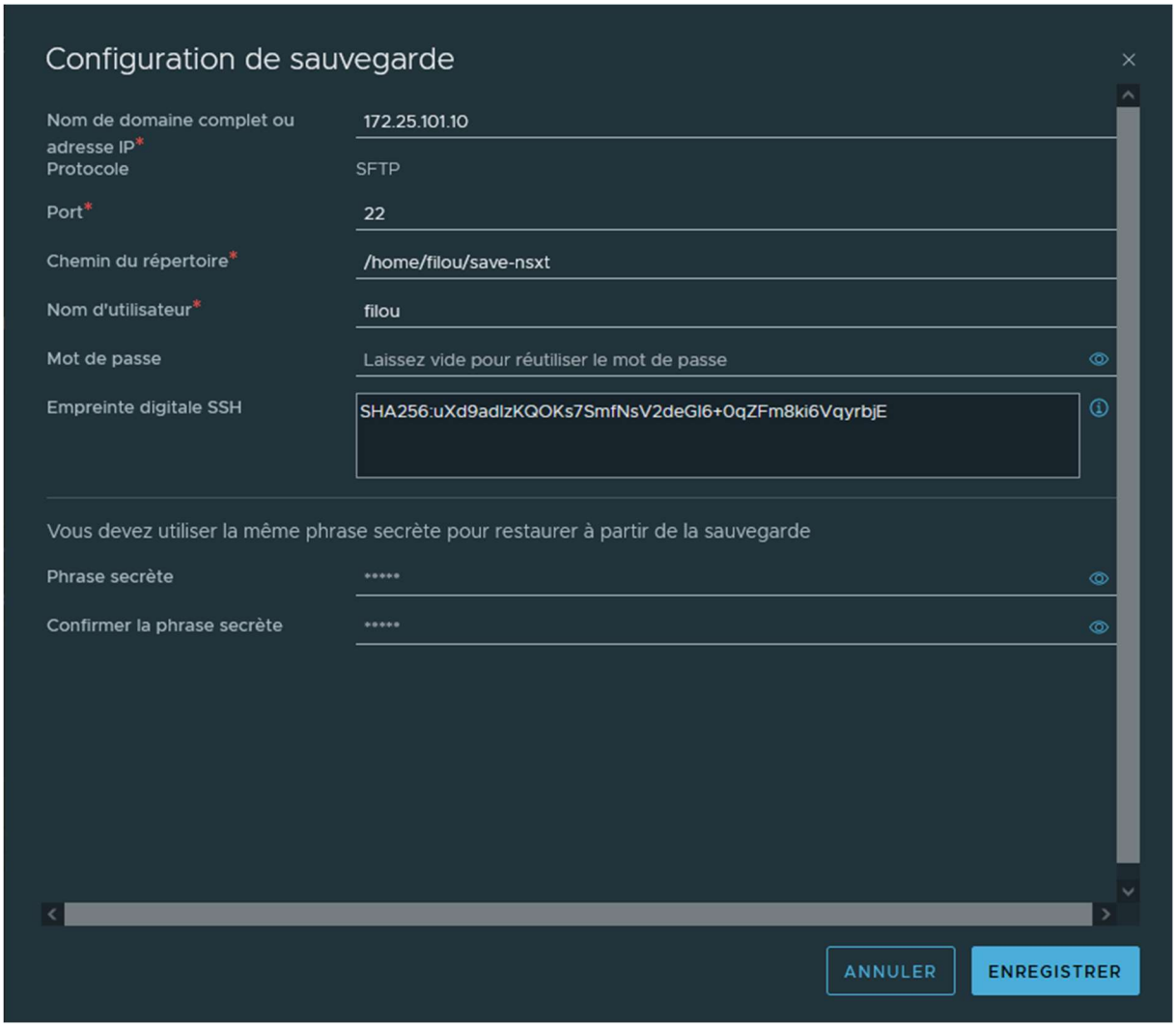


Figure 37.Sauvegarde NSX configuration

Un message vous assure que l'empreinte a été correctement ajouté.

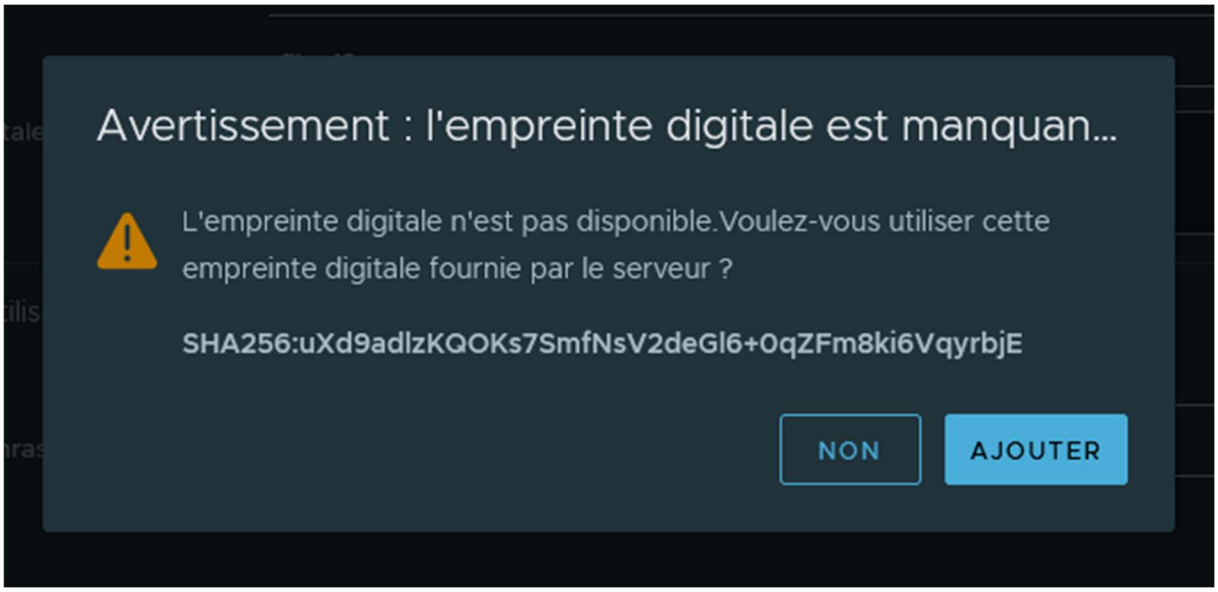


Figure 38.Empreinte SSH NSX

3.1.2 Utilisation

Après avoir finalisé la configuration, il est désormais possible de personnaliser la manière dont les sauvegardes seront réalisées.
Il vous est possible de définir une période ou une fréquence pour l'exécution des sauvegardes des fichiers de configuration NSX.

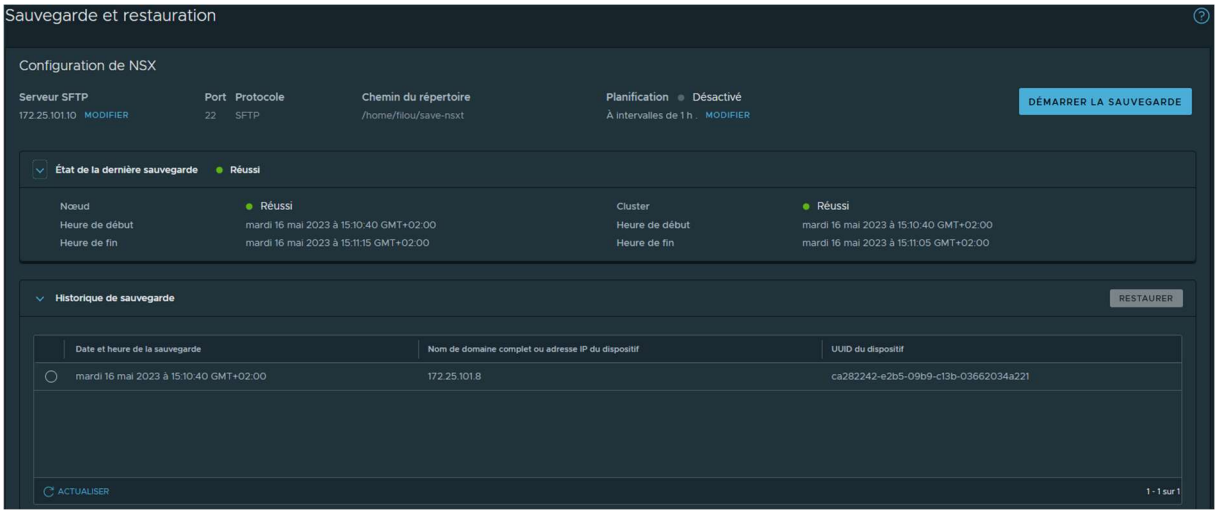


Figure 39.Restauration et sauvegarde

Je déclenche la sauvegarde afin de vérifier que la configuration s'effectue correctement sur le serveur distant.
Enfin, c'est également à cet endroit que la restauration du système peut être réalisée en utilisant les sauvegardes.

3.1.3 Verification de la sauvegarde sur le serveur

J’observe que les sauvegardes effectuées pour le test sont bel et bien présentes sur le serveur distant.

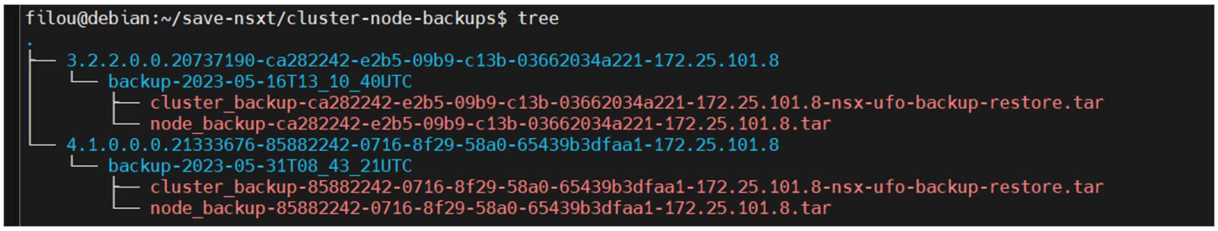


Figure 40.Serveur distant sauvegarde

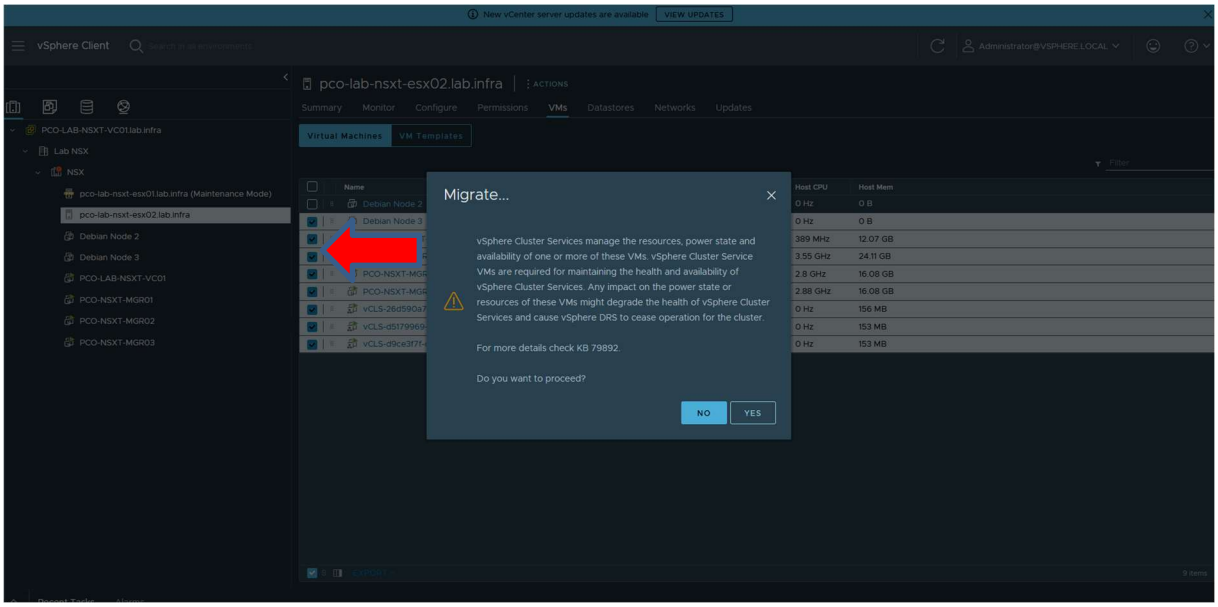
4 Désinstallation NSX des hosts ESXI

Dans certaines situations, la désinstallation de NSX à partir des hôtes peut être requise.
C'est pourquoi j'ai consacré du temps à étudier cette problématique et à mener une série de tests afin de comprendre comment procéder de la manière la plus optimale et efficace possible.

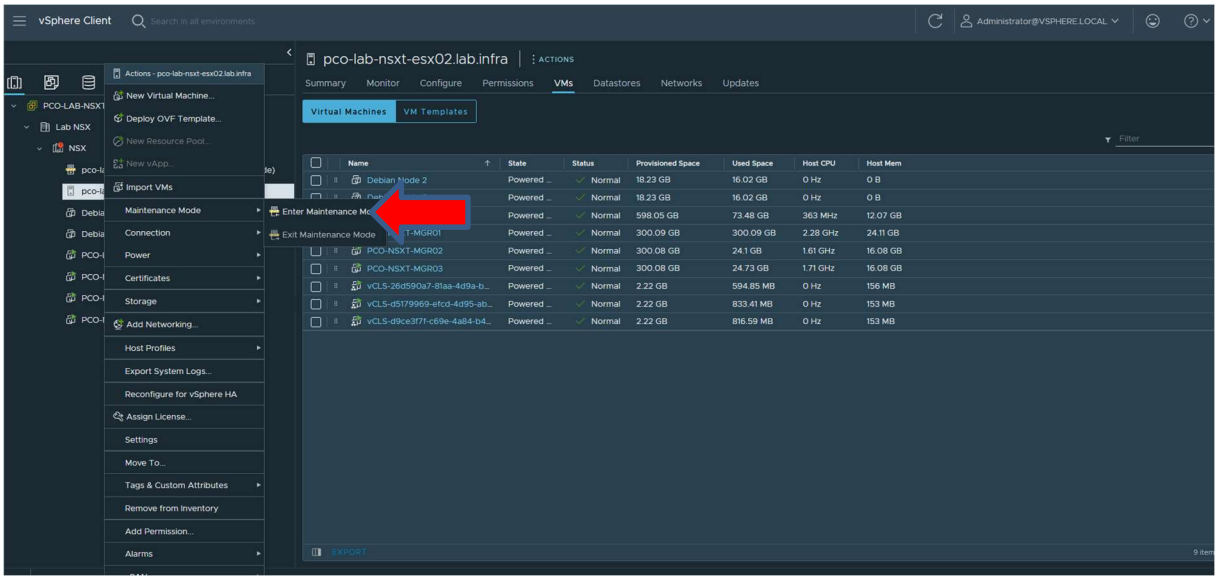
4.1.1 Conditions préalables

Nous débutons en :

- Transférant les machines virtuelles vers le deuxième hôte ESX.
- Transférant les machines virtuelles en fonction de leur état (allumées ou éteintes).



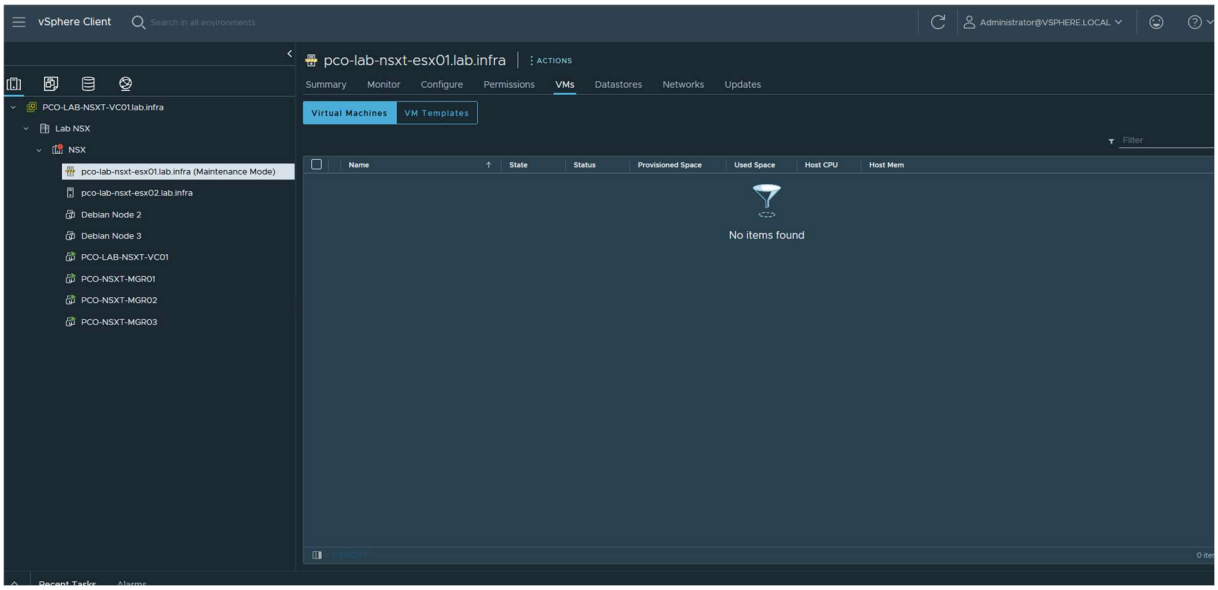
Au sein de vCenter Server, je place les hôtes en mode de maintenance.
Un mode qui permet d’effectuer des actions spécifiques sur les hosts.



Un point crucial à noter :

- Lorsqu'un hôte ESXi est en mode verrouillé, assurez-vous d'ajouter l'utilisateur root à la liste des exceptions. Ceci permettra d'établir une session SSH avec l'hôte.

Les machines virtuelles ont été déplacées vers le second hôte avec succès.



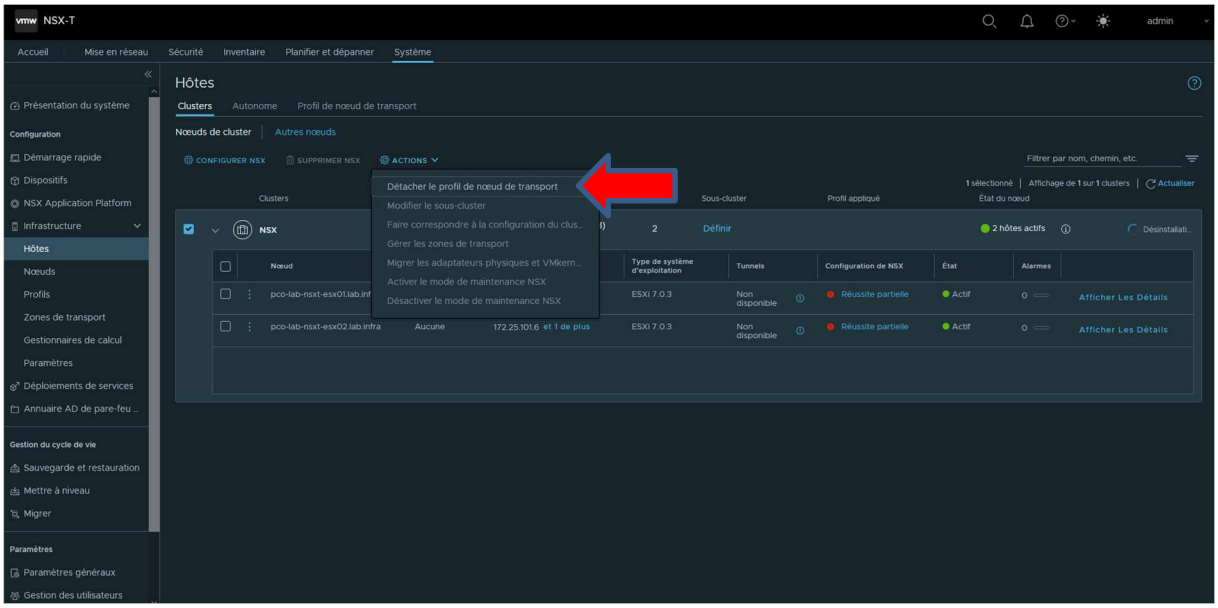
4.1.2 Procédure

En utilisant un navigateur, je me connecte à l'interface d'administration d'un gestionnaire NSX en tant qu'administrateur à l'adresse :

- https://<adresse-IP-du-getionnaire-nsx>

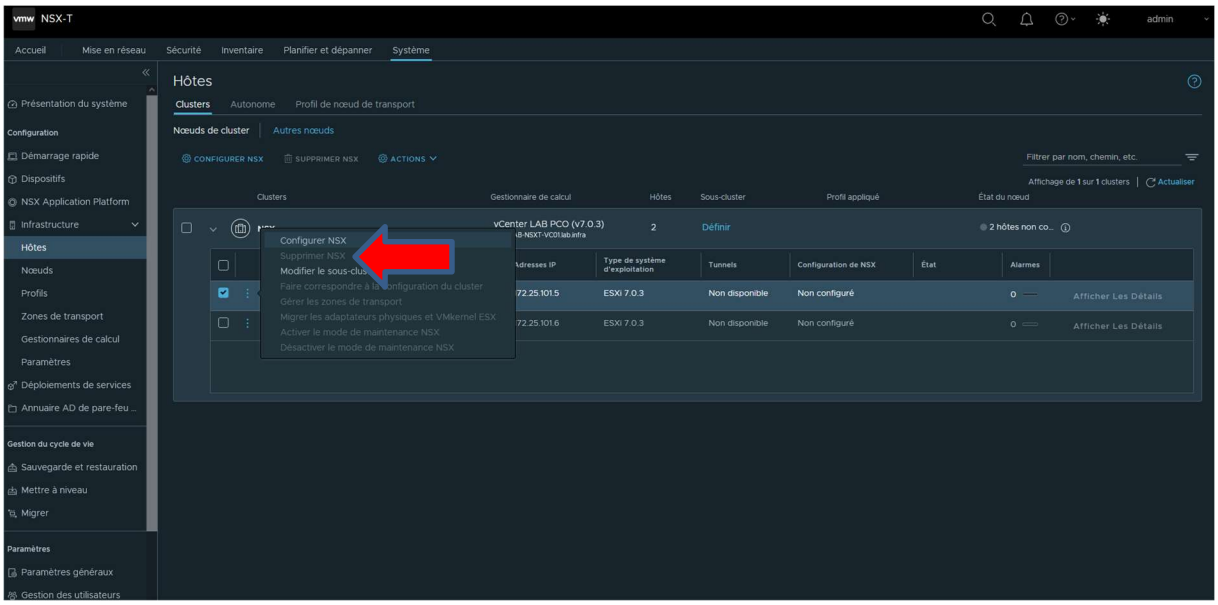
Naviguez dans l'interface utilisateur et choisissez un hôte.
Si le cluster dispose d'un profil de nœud de transport appliqué, sélectionnez le cluster et accédez à :

– Actions > Détacher le profil TN.



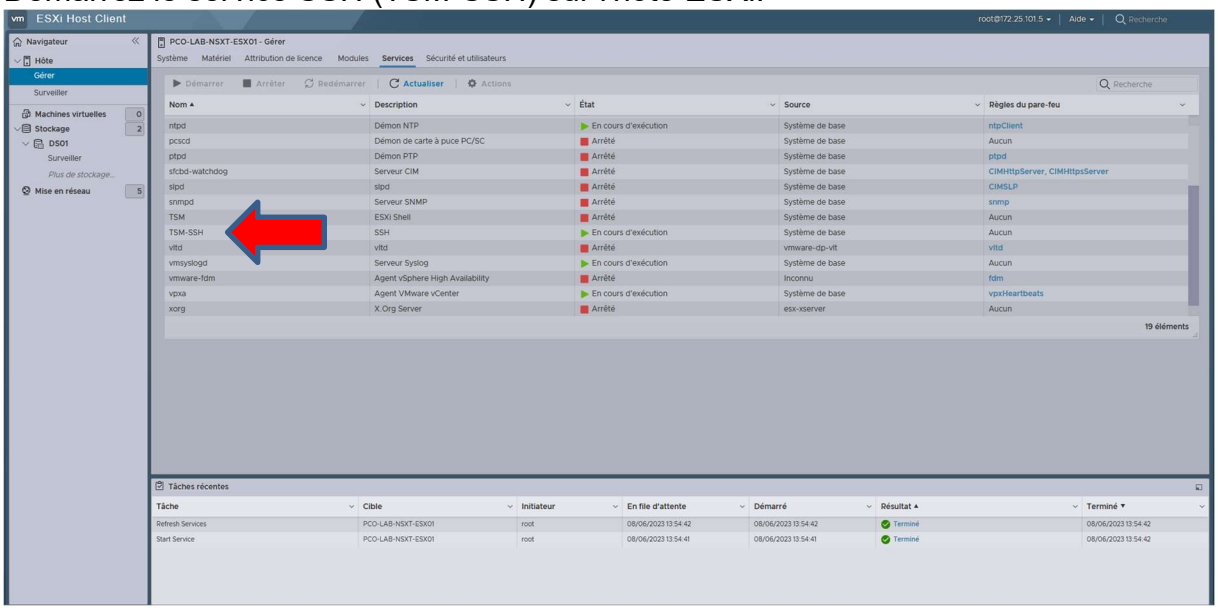
Si le cluster a un profil de nœud de transport appliqué, dans la colonne "Configuration NSX pour le cluster", vous verrez le nom du profil qui y est associé.

Choisissez l'hôte et cliquez sur l'option "Supprimer NSX".



4.1.3 Vérifiez que NSX-T Data Center est supprimé de l'hôte

Démarrez le service SSH (TSM-SSH) sur l'hôte ESXi.



Connectez-vous à l'interface de ligne de commande de l'hôte en tant que super utilisateur (root).
Exécutez la commande suivante pour vérifier les VIB (un VIB est un module logiciel ESXi) du centre de données NSX-T :

- esxcli software vib list | grep -E 'nsx|vsipfwlib'

```
[root@PCO-LAB-NSXT-ESX01:~] esxcli software vib list | grep -E 'nsx|vsipfwlib'
nsx-adf                        3.2.2.0.0-7.0.20737187              VMware  VMwareCertified   2023-06-08
nsx-cfgagent                   3.2.2.0.0-7.0.20737187              VMware  VMwareCertified   2023-06-08
nsx-context-mux                3.2.2.0.0-7.0.20737187              VMware  VMwareCertified   2023-06-08
nsx-cpp-libs                   3.2.2.0.0-7.0.20737187              VMware  VMwareCertified   2023-06-08
nsx-esx-datapath               3.2.2.0.0-7.0.20737187              VMware  VMwareCertified   2023-06-08
nsx-exporter                   3.2.2.0.0-7.0.20737187              VMware  VMwareCertified   2023-06-08
nsx-host                       3.2.2.0.0-7.0.20737187              VMware  VMwareCertified   2023-06-08
nsx-ids                        3.2.2.0.0-7.0.20737187              VMware  VMwareCertified   2023-06-08
nsx-monitoring                 3.2.2.0.0-7.0.20737187              VMware  VMwareCertified   2023-06-08
nsx-mpa                        3.2.2.0.0-7.0.20737187              VMware  VMwareCertified   2023-06-08
nsx-nestdb                     3.2.2.0.0-7.0.20737187              VMware  VMwareCertified   2023-06-08
nsx-netopa                     3.2.2.0.0-7.0.20737187              VMware  VMwareCertified   2023-06-08
nsx-opsagent                   3.2.2.0.0-7.0.20737187              VMware  VMwareCertified   2023-06-08
nsx-platform-client            3.2.2.0.0-7.0.20737187              VMware  VMwareCertified   2023-06-08
nsx-proto2-libs                3.2.2.0.0-7.0.20737187              VMware  VMwareCertified   2023-06-08
nsx-proxy                      3.2.2.0.0-7.0.20737187              VMware  VMwareCertified   2023-06-08
nsx-python-gevent              1.1.0-18242523                      VMware  VMwareCertified   2023-06-08
nsx-python-greenlet            0.4.14-18242315                     VMware  VMwareCertified   2023-06-08
nsx-python-logging             3.2.2.0.0-7.0.20737187              VMware  VMwareCertified   2023-06-08
nsx-python-protobuf            2.6.1-18242311                      VMware  VMwareCertified   2023-06-08
nsx-python-utils               3.2.2.0.0-7.0.20737187              VMware  VMwareCertified   2023-06-08
nsx-sfhc                       3.2.2.0.0-7.0.20737187              VMware  VMwareCertified   2023-06-08
nsx-shared-libs                3.2.2.0.0-7.0.20737187              VMware  VMwareCertified   2023-06-08
nsx-vdpi                       3.2.2.0.0-7.0.20737187              VMware  VMwareCertified   2023-06-08
nsxcli                         3.2.2.0.0-7.0.20737187              VMware  VMwareCertified   2023-06-08
vsipfwlib                      3.2.2.0.0-7.0.20737187              VMware  VMwareCertified   2023-06-08
[root@PCO-LAB-NSXT-ESX01:~]
```

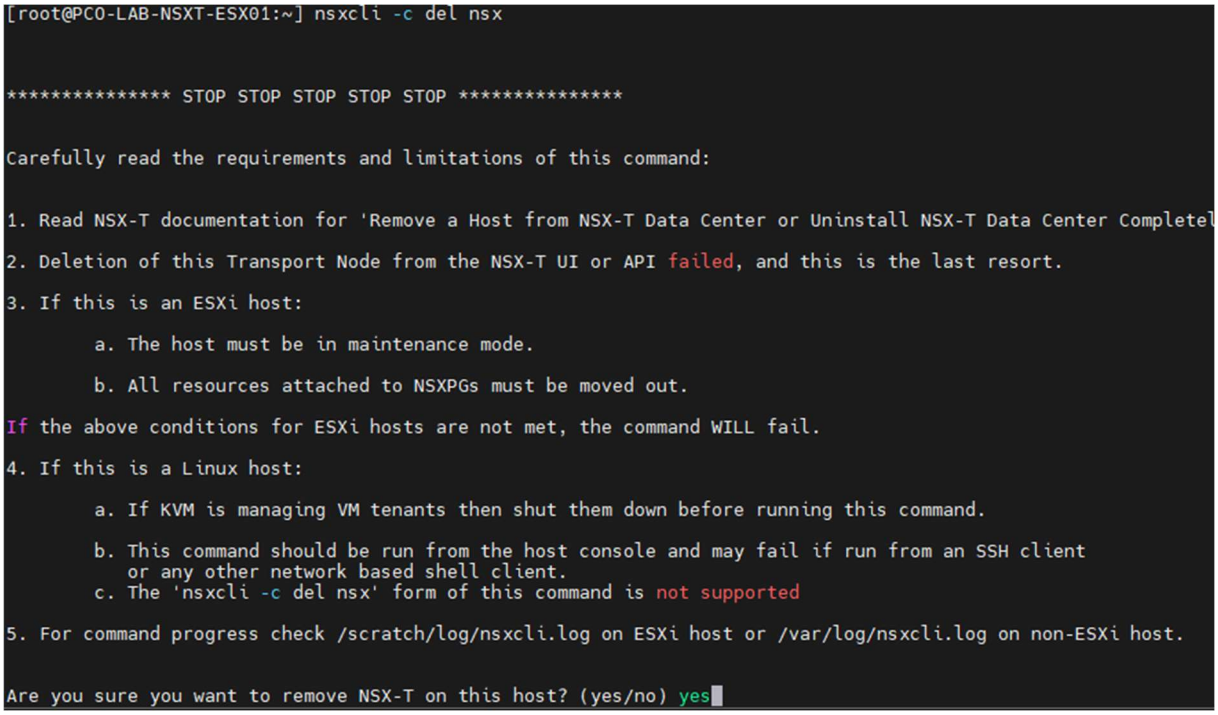
Pour désactiver le protocole SNMP sur l'hôte ESXi, exécutez la commande suivante :

- esxcli system snmp set --enable false

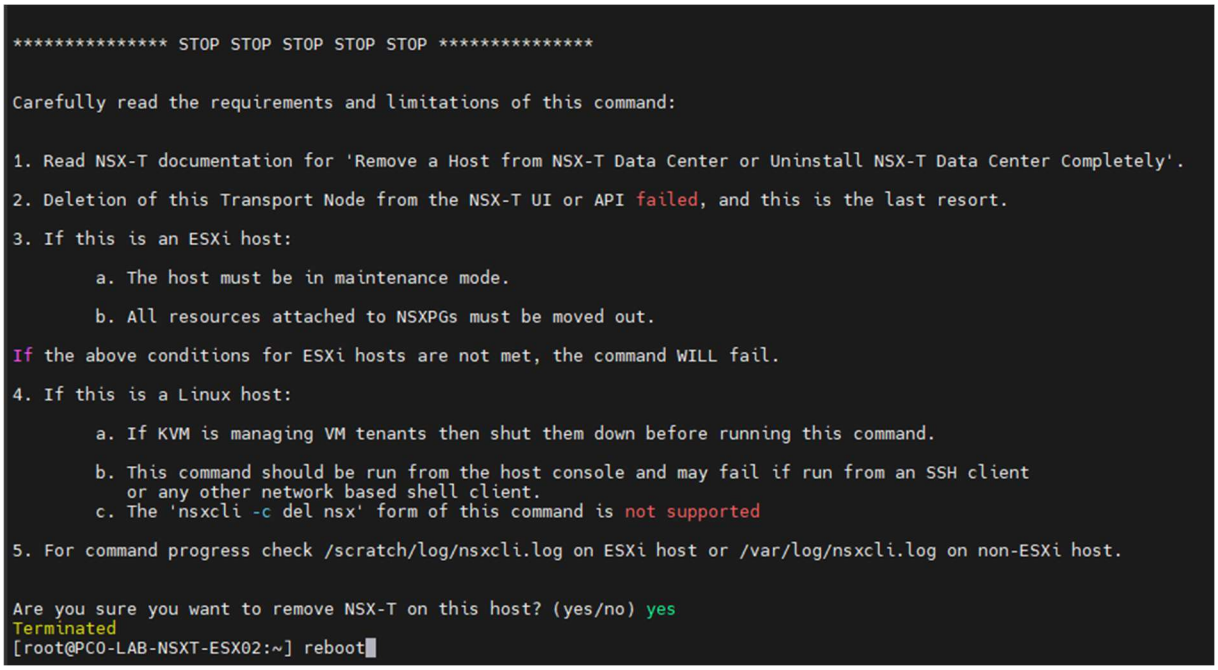
Ensuite, pour exécuter la commande :

- nsxcli -c del nsx

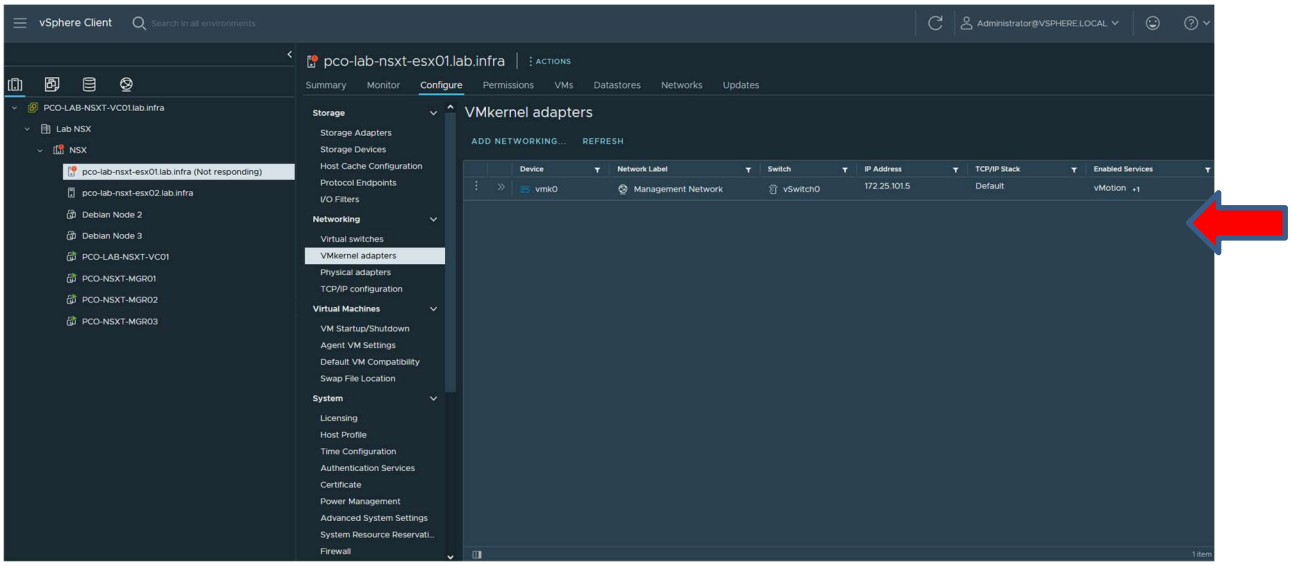
Assurez-vous d'exécuter ces commandes avec prudence et en respectant les directives spécifiques pour votre environnement.



Après avoir effectué les étapes nécessaires, il est recommandé de redémarrer l'hôte ESXi.
Cela permettra de finaliser les modifications et de garantir que les configurations soient correctement prises en compte.



Les VMkernel TEP spécifique aux flux GENEVE ont été supprimés sur les deux hôtes ESXi, ce qui indique que les hôtes ont été complètement débarrassés des fichiers NSX.
Cela témoigne du succès de la désinstallation de NSX.



Ces diverses étapes et actions sont essentielles pour garantir que les hôtes soient complètement dépourvus de fichiers associés à NSX.
Cette approche rigoureuse est recommandée pour garantir la fiabilité du processus de désinstallation de NSX.

5 Conclusion

Je tiens à souligner que j'ai exposé en profondeur les tests que j'ai menés sur la maquette NSX.
Les actions variées ainsi que les essais rigoureux que j'ai entrepris sont méticuleusement répertoriés dans les annexes techniques de ce mémoire.
Pour faciliter la compréhension des aspects techniques abordés dans ce document, un glossaire exhaustif a été élaboré.

Cette ressource permet aux lecteurs de se familiariser avec les termes spécifiques employés et d'appréhender pleinement les concepts présentés.
Chaque étape de cette démarche a été entreprise avec précaution et avec l'objectif de garantir la validité des résultats obtenus.

Mon engagement dans la réalisation de ces tests repose sur la nécessité de démontrer la fiabilité et l'efficacité des procédures explorées dans l'environnement de la maquette NSX.

L'intégralité des détails concernant les manipulations effectuées, les résultats obtenus et les conclusions tirées sont minutieusement documentés dans ce mémoire.
Cette approche rigoureuse renforce la crédibilité de l'étude et la valeur des résultats obtenus au sein de ce contexte technique complexe.

Bilan

1 Bilan du projet NSX

Cette étude a montré que la virtualisation du réseau avec NSX offre de nombreux avantages par rapport aux approches traditionnelles.

Tout d'abord, NSX permet une plus grande automatisation et une meilleure orchestration des tâches de réseautage, ce qui permet de réduire les temps de déploiement et de minimiser les erreurs humaines.

De plus, NSX offre une plus grande évolutivité et une meilleure gestion des politiques de sécurité, permettant une sécurité plus fine et adaptée aux besoins de l'entreprise.
NSX est une solution interopérable avec les environnements multicloud, ce qui permet une utilisation plus flexible des ressources réseau.

2 Bilan en entreprise

Au sein de l'entreprise, mon parcours a été synonyme d'un épanouissement général remarquable.
Dès les premiers jours, j'ai été immergé dans un environnement dynamique et stimulant, propice au développement de mes compétences professionnelles.

La société m'a offert des opportunités d'apprentissage concrètes et m'a permis de m'impliquer activement dans des projets liés aux réseaux et à la virtualisation.
Au fil du temps, j'ai pu constater une réelle montée en compétences dans ces domaines clés de l'informatique.

Les responsables et les équipes m'ont soutenu et guidé avec bienveillance tout au long de mon accompagnement.
J'ai pu bénéficier de formations et de sessions de coaching personnalisées, ce qui m'a permis d'acquérir une expertise pointue dans la configuration et la gestion des réseaux ainsi que des environnements virtuels.

La confiance accordée par l'entreprise m'a également donné l'opportunité de prendre des initiatives et de participer activement à des projets d'envergure.
Cette expérience a été enrichissante et m'a permis de développer ma capacité à travailler en équipe, à communiquer efficacement et à résoudre des problèmes complexes.

Je suis reconnaissant envers l'entreprise pour sa bienveillance et son soutien continu, qui ont été des piliers essentiels dans mon épanouissement professionnel.

Cette expérience a non seulement renforcé ma passion pour les réseaux et la virtualisation, mais elle m'a également permis de découvrir le monde de l'entreprise d'une manière positive et inspirante.
Ces compétences acquises et cette expérience me serviront de solides fondations pour ma future carrière en tant qu'ingénieur informatique.

3 Bilan personnel

Cette formation m'a permis de découvrir ma passion pour l'informatique sous un nouvel angle, nourrissant ma curiosité et mon désir constant d'apprendre.
Au fil des projets et des enseignements, j'ai pu développer mes compétences techniques dans des domaines variés tels que la programmation, le réseau, la sécurité informatique et la gestion de projets.

Sur le plan personnel, j'ai acquis une confiance en moi renforcée grâce aux défis que j'ai relevés avec succès.
La collaboration au sein d'équipes multiculturelles et la communication ont été des aspects clés de mon épanouissement personnel.
J'ai également développé ma capacité à résoudre des problèmes de manière créative et à prendre des initiatives.

Ces réalisations m'ont conforté dans mon choix d'ambitionner un master en informatique.
Je souhaite poursuivre mon cheminement académique pour approfondir mes connaissances dans des domaines spécifiques qui suscitent mon intérêt, tels que l'intelligence artificielle, la cybersécurité ou l'informatique distribuée.

Un master me permettra d'acquérir une expertise approfondie, de m'engager dans des projets de recherche novateurs et de travailler avec des spécialistes reconnus.

4 Mes projets futurs

Mon aspiration professionnelle se dessine vers le projet d'intégrer un Master en cybersécurité (MICSI) au sein du CESI.
Mon objectif est de devenir ingénieur réseau, en me spécialisant particulièrement dans la virtualisation du réseau et la cybersécurité.

Pour y parvenir, j'ai le ferme désir d'obtenir les certifications CCNA, témoignant ainsi de ma maîtrise des fondements cruciaux du réseau, tandis que je m'attelle à renforcer inlassablement mes compétences en cybersécurité pour faire face aux défis toujours plus complexes de notre ère numérique.

Convaincu de la pertinence du Master MICSI au CESI, je perçois cette opportunité comme une véritable pépinière d'apprentissage, propice au développement de mes connaissances et compétences, et ainsi de mener à bien mes aspirations professionnelles.

4.1 Formation et certification

Depuis mon intégration au sein de l'entreprise, j'ai saisi chaque occasion pour me perfectionner en réussissant divers examens en ligne.
J’ai obtenu plusieurs certifications VMware, notamment en NSX (Networking & Security - Network virtualisation) et en Multicloud.

En plus des certifications VMware, j'ai également obtenu la certification Sophos Firewall (Technique).
Mon parcours de formation ne s'arrête pas là, car j'ai suivi avec succès deux formations Cisco, à savoir Cisco ENCOR (Implementing and Operating Cisco Enterprise Network Core Technologies) et ENSLD (Designing Cisco Enterprise Networks), en collaboration avec Stordata.

Ces formations m'ont permis d'approfondir mes connaissances dans le domaine des réseaux Cisco, renforçant ainsi mes compétences en matière de conception, de déploiement et de gestion d'infrastructures réseau sophistiquées.

4.2 Projet de certification NSX

Animé d'une véritable passion pour les technologies de virtualisation réseau, je me suis lancé dans un projet de certification portant sur NSX de VMware, dans sa version implémentation technique.

Ce projet vise à approfondir de manière substantielle mes connaissances et compétences dans la mise en œuvre et la gestion de cette solution.
Au cœur de ce projet réside mon objectif principal, à savoir explorer les fonctionnalités et les avantages offerts par NSX dans le domaine spécifique de la virtualisation réseau.

Cette démarche vise à saisir pleinement les subtilités et les atouts de cette technologie. Je mets un point d'honneur à plonger en profondeur dans les concepts clés qui sous-tendent NSX, tels que la micro-segmentation, stratégie essentielle pour subdiviser le réseau en segments plus restreints et renforcer ainsi la sécurité.

De même, je désire explorer en détail les réseaux virtuels étendus (GENEVE) qui favorisent une connectivité fluide et transparente, adaptée aux environnements complexes et distribués.

Conclusion du projet NSX

La virtualisation du réseau est devenue une tendance majeure dans le monde de l'informatique ces dernières années, offrant une plus grande flexibilité, une évolutivité plus importante et une meilleure utilisation des ressources réseau.

L'un des acteurs majeurs dans ce domaine est VMware, avec sa solution NSX.
Dans ce mémoire, nous avons étudié l'opportunité d'utiliser cette solution dans un contexte bien précis et de ses avantages par rapport aux solutions traditionnelles de réseautage.

La solution NSX de VMware est une plateforme de virtualisation de réseau évolutive et flexible, qui permet de créer et de gérer des réseaux virtuels à partir d'une interface unique et centralisée.

Nous avons examiné en détail les fonctionnalités de NSX, ainsi que ses avantages et ses limitations.
Nous avons également étudié les différentes utilisations possibles de cette solution, ainsi que son impact sur l'architecture et la sécurité du réseau.

Il est apparu que la solution NSX offre de nombreux avantages pour les entreprises, notamment une meilleure gestion de la sécurité des réseaux, une réduction des coûts liés à l'infrastructure physique et une augmentation de la flexibilité des réseaux.

Son implémentation peut être complexe, nécessitant des compétences et une expertise importantes.

Philippe combot

Glossaire

Un glossaire est un outil essentiel qui permet de clarifier et de définir les termes techniques, les acronymes et les concepts spécifiques utilisés dans le contenu de ce mémoire.
Il clarifie les termes techniques et assure une référence cohérente.

1 Définitions

Cloud : Hébergement en ligne (Ex OVH, Ionos)

Multicloud : Plusieurs hébergement en ligne

Firewall : Pare-feu (est un logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau)

SDN : Software defined Networking (mise en réseau définie par logiciel)

Switch : Commutateur en français, permet l'acheminement des paquets entre les équipements.

TEP : Terminal end point (Point d'arrivé)

DPG : Distributed port group (ports distribués)

DSW : Distributed switch (commutateur distribué)

VLAN : Réseau virtuel

Appliance : Application

SDDC : Software defined data center

Lan : Local area network (Réseau local)

Wan : Wide area network (Réseau étendu)

Troubleshooting : Diagnostique

Interopérable : Capacité de matériels, de logiciels ou de protocoles différents à fonctionner ensemble et à partager des informations

Virtualisation : La virtualisation consiste, en informatique, à exécuter sur une machine hôte, dans un environnement isolé, des systèmes d'exploitation — on parle alors de virtualisation système — ou des applications — on parle alors de virtualisation applicative.

Serveur : Un serveur informatique offre des services accessibles via un réseau. Il peut être matériel ou logiciel, c'est un ordinateur qui exécute des opérations suivant les requêtes effectuées par un autre ordinateur appelé « client ». C'est pourquoi on entend souvent parler de relation « client/serveur ».

Software : Logiciel est un ensemble des programmes, procédés et règles, et éventuellement de la documentation, relatifs au fonctionnement d'un ensemble de traitement de données.

Orchestration : L'orchestration correspond à la configuration, gestion et coordination automatisées des systèmes informatiques, applications et services. L'orchestration facilite la gestion des tâches et workflows complexes pour le service informatique.

Micro-segmentation : La micro-segmentation est une approche de sécurité réseau qui permet aux architectes de sécurité de construire des limites de zones de sécurité réseau par machine dans les centres de données et les déploiements cloud afin de séparer et de sécuriser les machines virtuelles de manière indépendante.

MCO : Maintien en condition opérationnelle

API : application programming interface ou « interface de programmation d'application ») est une interface logicielle qui permet de « connecter » un logiciel ou un service à un autre logiciel ou service afin d'échanger des données et des fonctionnalités.

VPN : un réseau privé virtuel, plus communément abrégé en VPN, est un système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics.

Conteneurisation : La conteneurisation est un processus de déploiement logiciel qui regroupe le code d'une application avec tous les fichiers et bibliothèques dont elle a besoin pour s'exécuter sur n'importe quelle infrastructure.

Centre de données : Un centre de données, ou centre informatique est un lieu où sont regroupés les équipements constitutifs d'un système d'information.

QoS : La qualité de service ou quality of service est la capacité à véhiculer dans de bonnes conditions un type de trafic donné, en termes de disponibilité, débit, délais de transmission, gigue, taux de perte de paquets.

Malware : Un logiciel malveillant ou maliciel, aussi dénommé logiciel nuisible ou programme malveillant ou pourriciel, est un programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur dont l'ordinateur est infecté.

VxLAN : Le VxLAN est une technologie de virtualisation réseau qui vise à résoudre des problèmes d'évolutivité associés au déploiement du cloud computing. Il utilise une technique d'encapsulation proche du VLAN et permet d’encapsuler des trames Ethernet de couche 2 OSI dans des datagrammes UDP de couche 4.

GENEVE : Protocole de virtualisation réseau VMware (encapsulation).

VNI : Virtual network identifier.

UDP : Le User Datagram Protocol est un des principaux protocoles de télécommunication utilisés par Internet. Il fait partie de la couche transport du modèle OSI, quatrième couche de ce modèle, comme TCP. Il a été défini en 1980 par David P. Reed et est détaillé dans la RFC 768.

vNIC : Carte d'interface réseau virtuelles.

VM : Virtual machines (machines virtuelles).

ESXi : VMware ESXi est un hyperviseur de type 1 de classe entreprise développé par VMware pour déployer et servir des ordinateurs virtuels.

vSwitch : Commutateur vituel

vCenter : vCenter Server est l'utilitaire de gestion centralisée pour VMware et est utilisé pour gérer les machines virtuelles, plusieurs hôtes ESXi et tous les composants dépendants à partir d'un seul emplacement centralisé.

MTU : Lors d'une transmission de données informatiques, la maximum transmission unit est la taille maximale d'un paquet pouvant être transmis en une seule fois sur une interface.

Firmwares : Dans un système informatique, un firmware est un programme intégré dans un matériel informatique pour qu'il puisse fonctionner.

SaaS : Software as a service.

SD-WAN : Software-defined Wide Area Network.

Trame : Les paquets IP ne peuvent pas transiter sur un réseau tel quel, ils vont eux aussi être encapsulés avant de pouvoir « voyager» sur le réseau. L'encapsulation des paquets IP produit ce que l'on appelle une trame.

Ping : Ping est le nom d'une commande informatique permettant de tester l'accessibilité d'une autre machine à travers un réseau IP

Subnet : Un sous-réseau est une subdivision logique d'un réseau de taille plus importante.

SSH : Secure Shell est à la fois un programme informatique et un protocole de communication sécurisé.

Trunk : Un trunk est un lien physique permettant le transit de plusieurs VLANs.

Table d'illustrations

Figure 1.Virtualisation du réseau 24
Figure 2.Firewall classique 27
Figure 3.Firewall distribué 28
Figure 4.Micro-segmentation 30
Figure 5.Schéma encapsulation VXLAN 36
Figure 6.Schéma encapsulation GENEVE 36
Figure 7.Entête GENEVE 37
Figure 8.Entête VxLAN 39
Figure 9.NSX Datacenter 43
Figure 10.Cause et Effet matrice de risques 50
Figure 11.Plan de réponse matrice de risques 51
Figure 12.Matrice de risques 52
Figure 13.WBS 53
Figure 14.PBS 54
Figure 15.OBS 55
Figure 16.Devis NSX prix 56
Figure 17.Devis NSX 56
Figure 18.Schéma commutation logique 70
Figure 19.Edge Node 73
Figure 20.Encapsulation des données 74
Figure 21.Segments 75
Figure 22.Zones de transport 75
Figure 23.Vue physique 76
Figure 24.Vue logique 77
Figure 25.Vue réseau 78
Figure 26.Vue réseau ESXI-01 79
Figure 27.Vue réseau ESXI-02 79
Figure 28.Gateway TIER-1 81
Figure 29Gateway TIER-1 82
Figure 30.Segments 01 83
Figure 31.Segments 02 83
Figure 32.Ping segment 01 85
Figure 33.Ping segment 02 85
Figure 34Segment 1 et 2 + Gateway 86
Figure 35.OSPF configuration 89
Figure 36.OSPF Summarization 90
Figure 37.Sauvegarde NSX configuration 92
Figure 38.Empreinte SSH NSX 93
Figure 39.Restauration et sauvegarde 93
Figure 40.Serveur distant sauvegarde 94

Bibliographie

Mishchenko, D. (s.d.). *VMware ESXi: Planning, Implementation, and Security*.

Sivaraman, M. R. (s.d.). *VMware ESXi Cookbook*.

Thakurratan, R. S. (2017). *Learning VMware NSX : next-generation network administration skills unveiled*. Consulté le 6 12, 2023, sur http://babordplus.u-bordeaux.fr/notice.php?q=id:2864616

Virtualization for dummies, AMD Special Edition. (s.d.). Consulté le 6 12, 2023

VMware. (2022). *WMware NSX*.

(Thakurratan, 2017)
(Virtualization for dummies, AMD Special Edition)
(VMware, 2022)


Stordata
vos données, notre engagement


vmware
NSX-T


CESI
ÉCOLE D'INGÉNIEURS

Annexe technique du projet NSX

1 Socle de virtualisation VMware NSX-T

1.1 Cluster NSX Manager

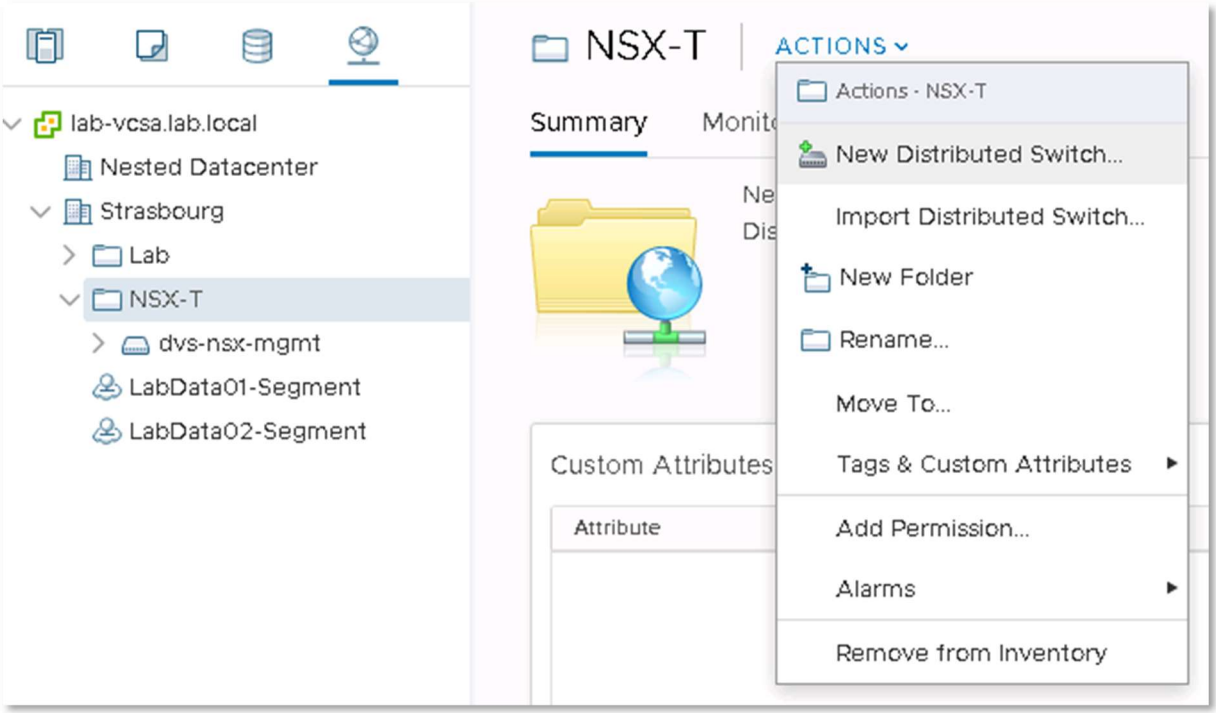
1.1.1 Pré-requis

Ci-dessous les prérequis nécessaires au déploiement du cluster NSX Manager :

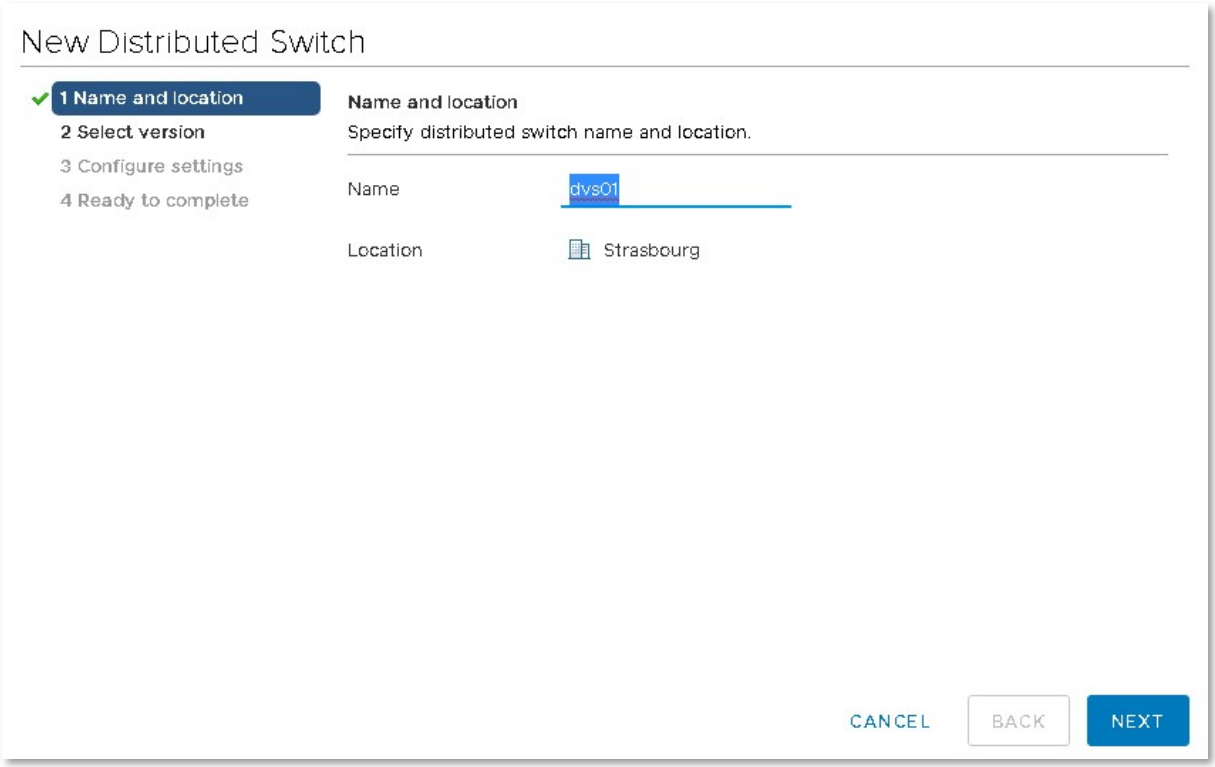
- **Configurer une MTU à 1600 minimum sur le réseau physique où transiteront les flux overlay.**
- Avoir au moins un distributed vSwitch avec des uplinks dans le VLAN d'administration
    - On utilisera un dvs d'administration existant (management + vMotion) ou on en déploie un et on migre les vmKernel existant.
    - Bien s'assurer avec l'équipe réseau que les VLANs soient bien déclarés côté switch.
- Idéalement, avoir un second dvs pour les flux edge overlay.
    - Créer un distributed port group sur le VLAN overlay.
    - Soit sur le dvs d'administration soit sur un dvs dédié (recommandé).
- Créer les entrées DNS pour les NSX Manager et de la VIP.
- Ne pas mettre DRS en automatique dans le cluster hébergeant les Appliance NSX-T Manager.
    - Les opérations DRS peuvent perturber le déploiement des « Appliance ».
- Implicite mais NSX requiert à minima une licence vSphere Enterprise Plus à cause des dvs.

1.2 Création du dvs management

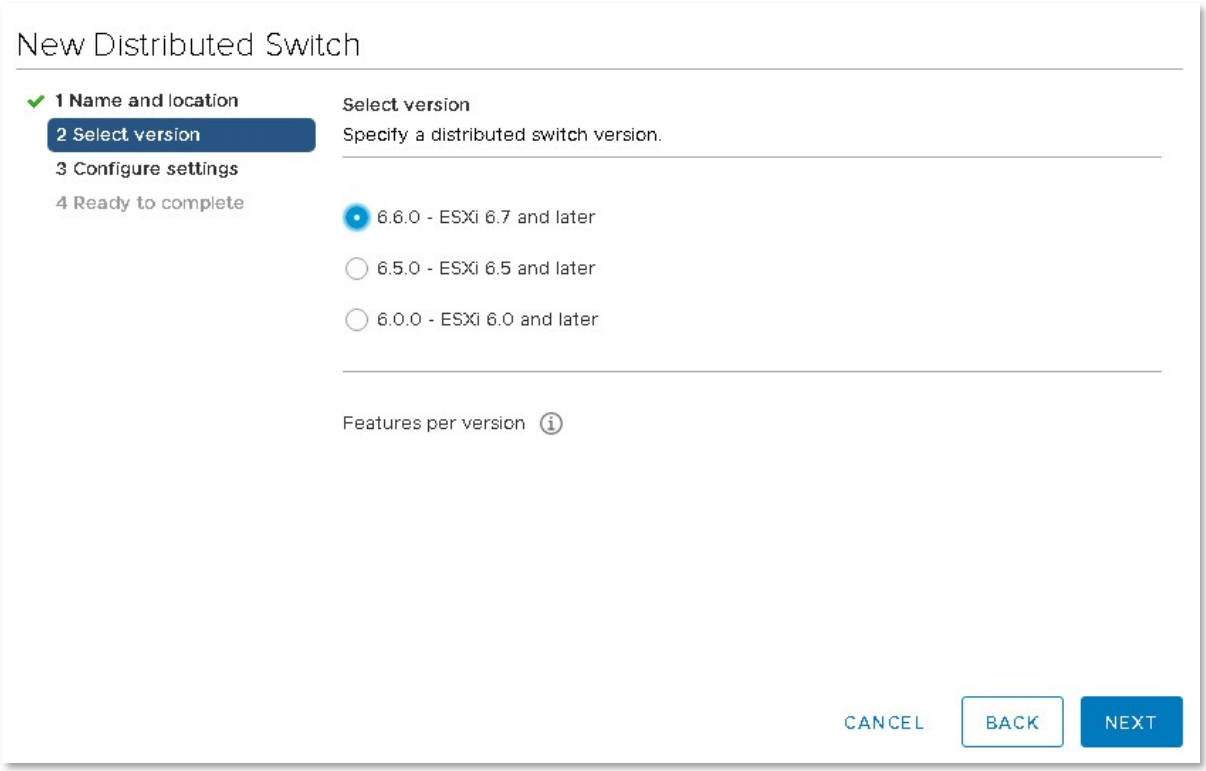
Dans l'interface de management du vCenter, aller dans la vue Network puis action et Create new distributed switch



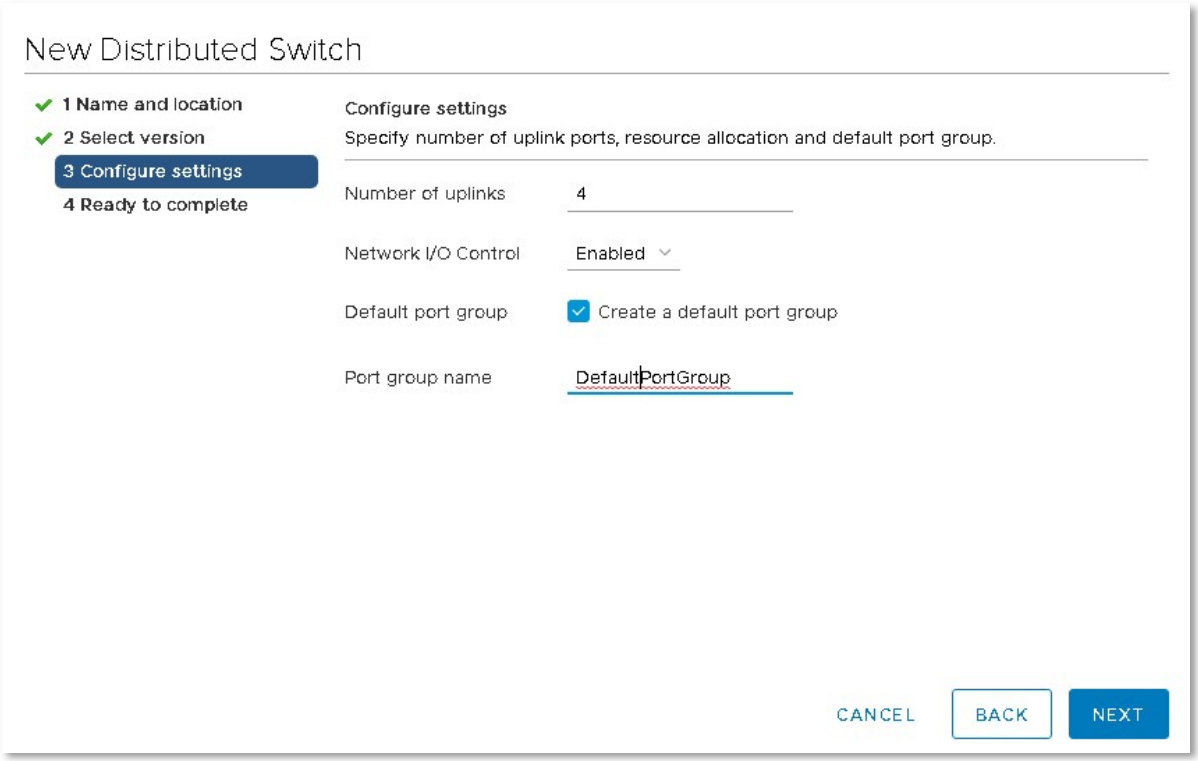
Dérouler l'assisant de création du dvs en renseignant les différentes informations demandées.



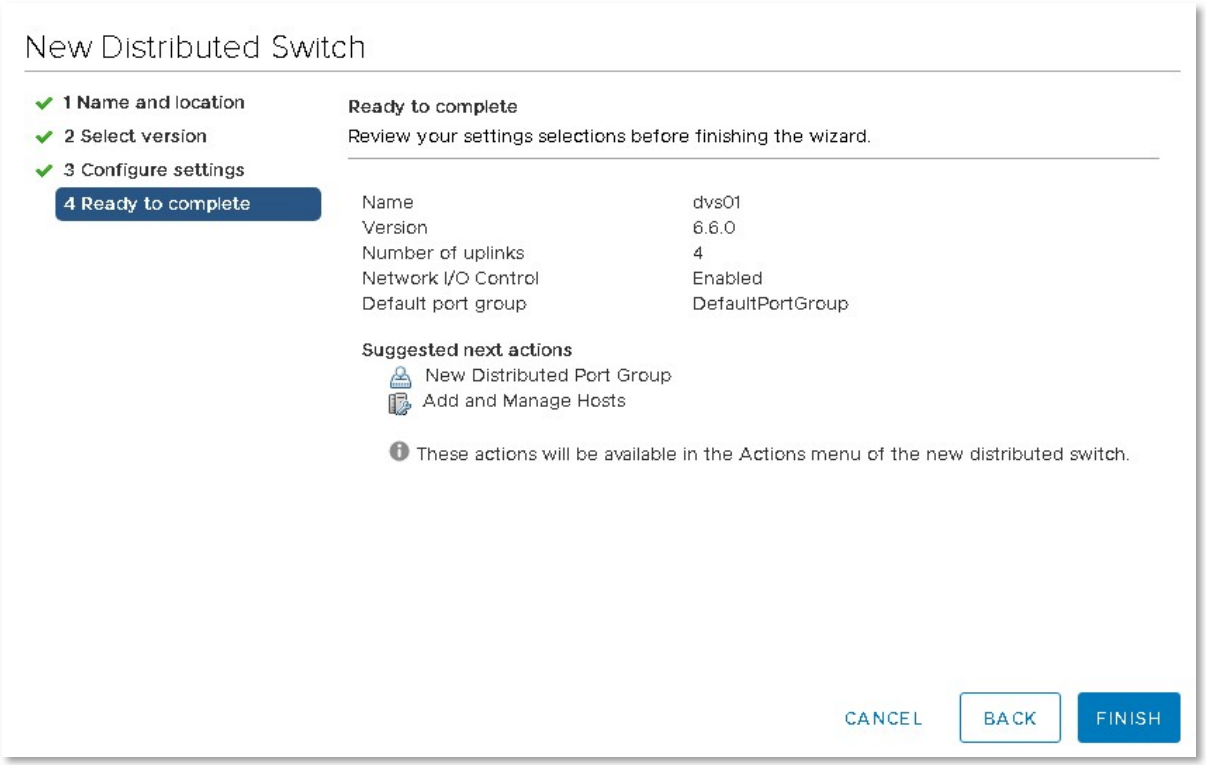
On nomme le dvs.



On sélectionne la version du dvs en fonction de la version des ESXi du cluster sur lequel il sera déployé.



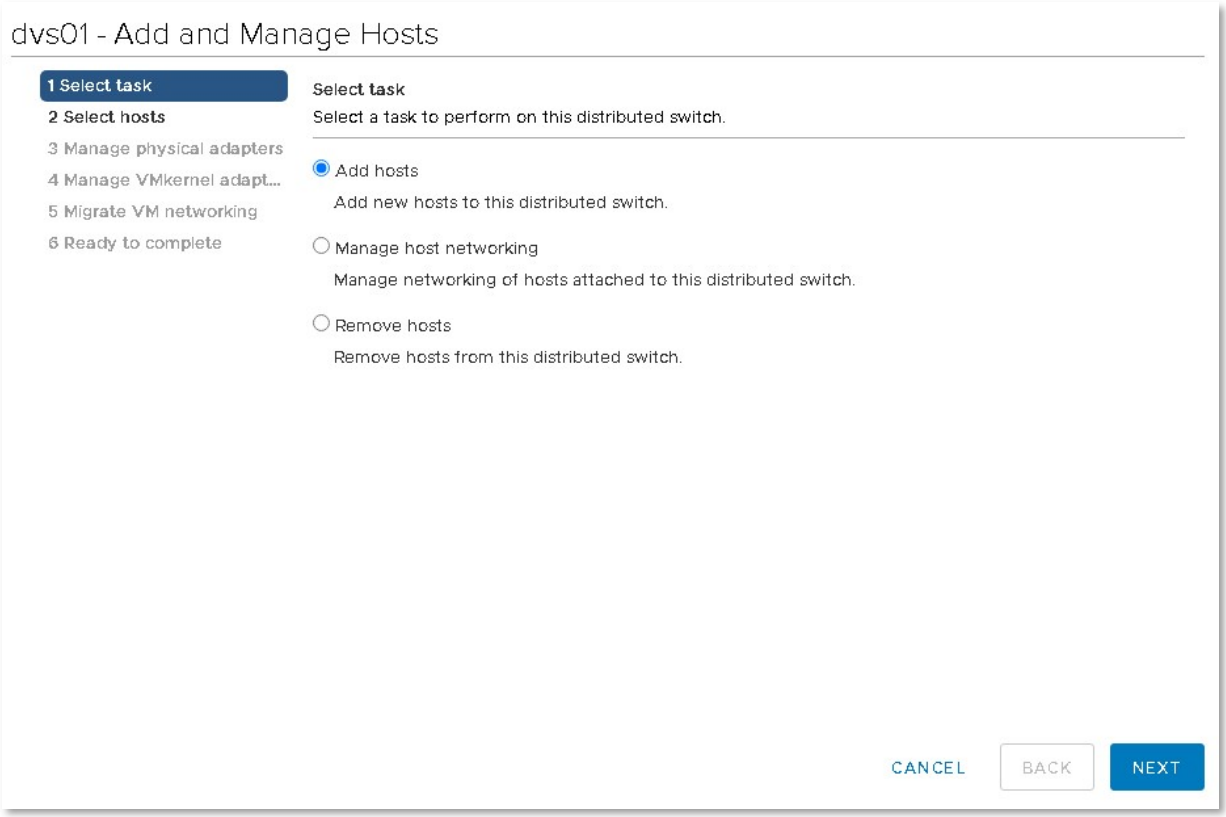
On indique le nombre d'uplink (interface physique) qui seront utilisé par le dvs.
La création d'un « Default port group » n'est pas obligatoire.



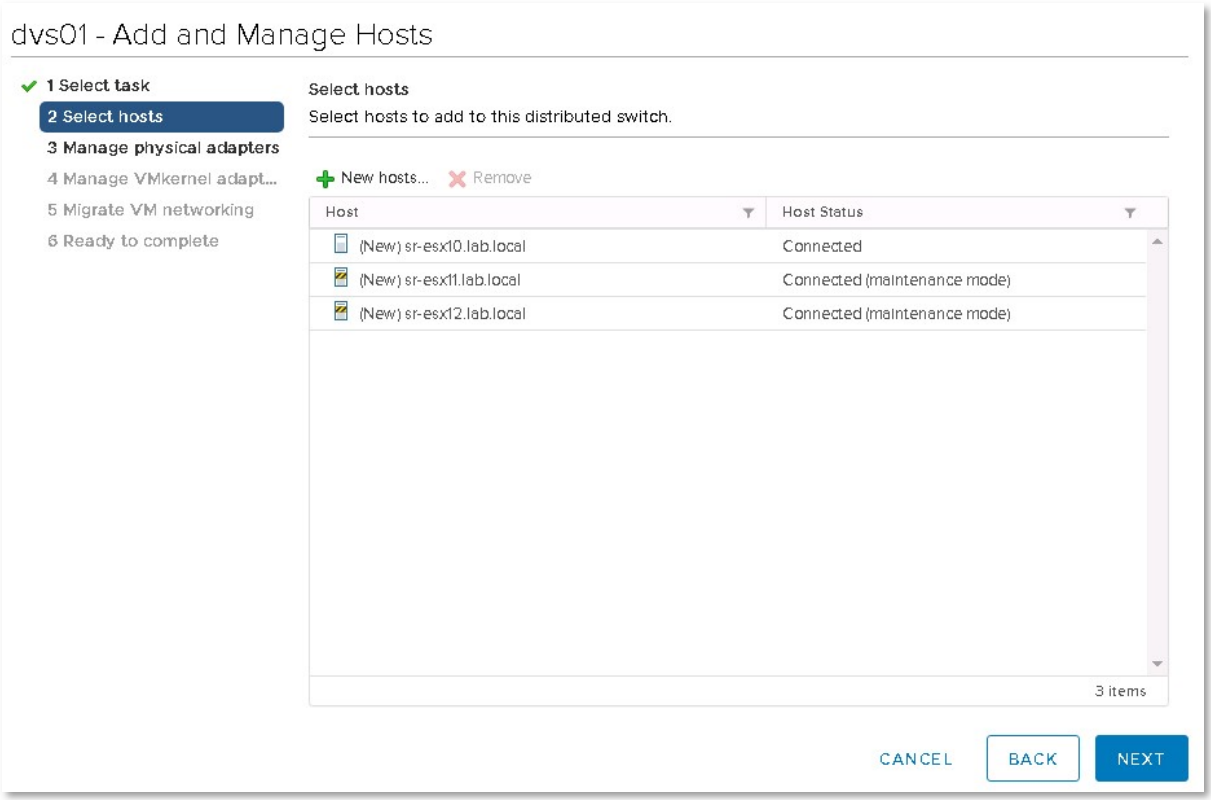
On clique sur finish pour terminer la création du dvs.

1.3 Configuration des dvs

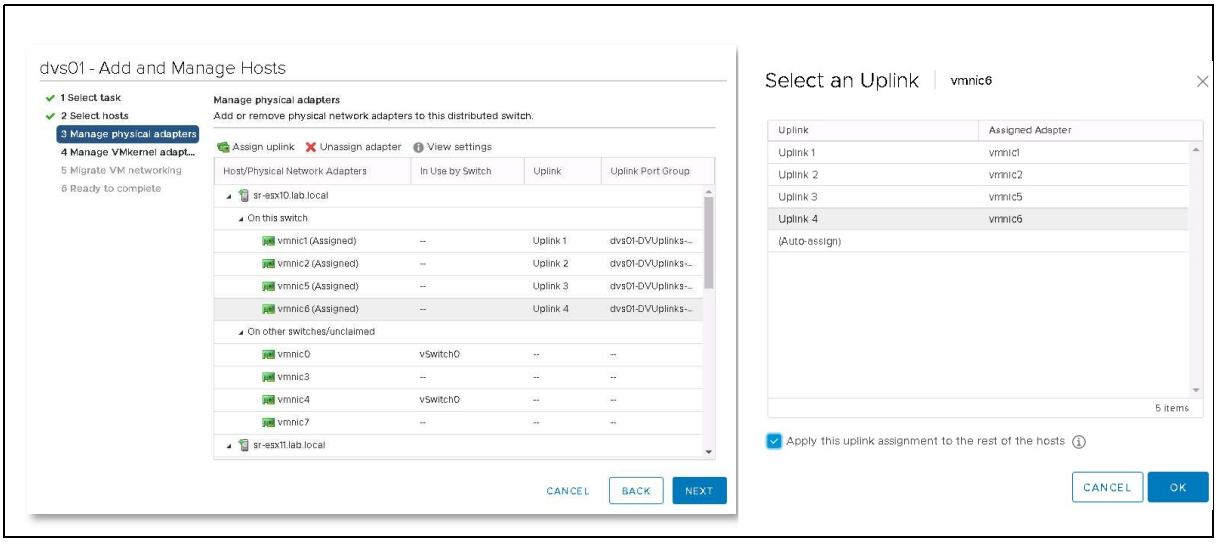
Aller dans Network / <dvs_name> / Hosts puis action et Add and Manage hosts



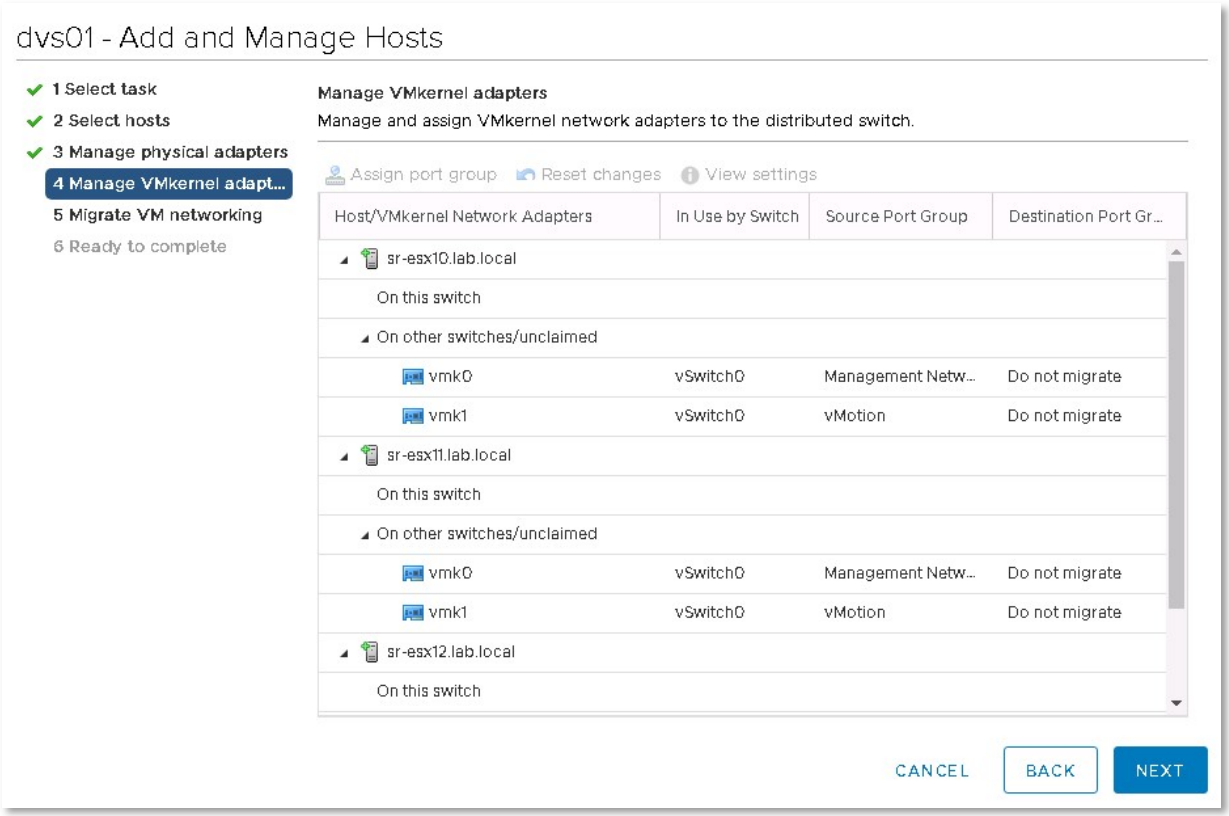
Pour ajouter des hôtes, on sélectionne « Add host ».



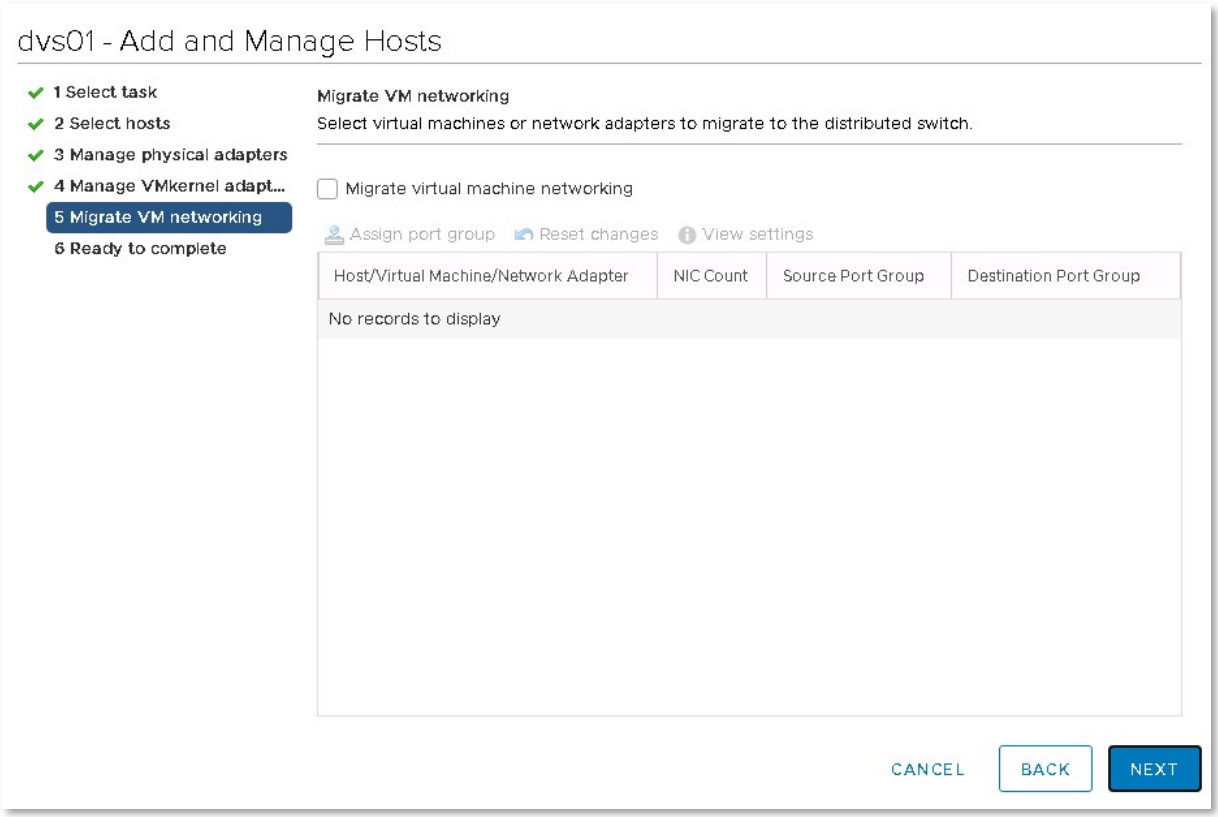
On clique sur « new host » puis on sélectionne les hôtes où sera déployé le dvs.



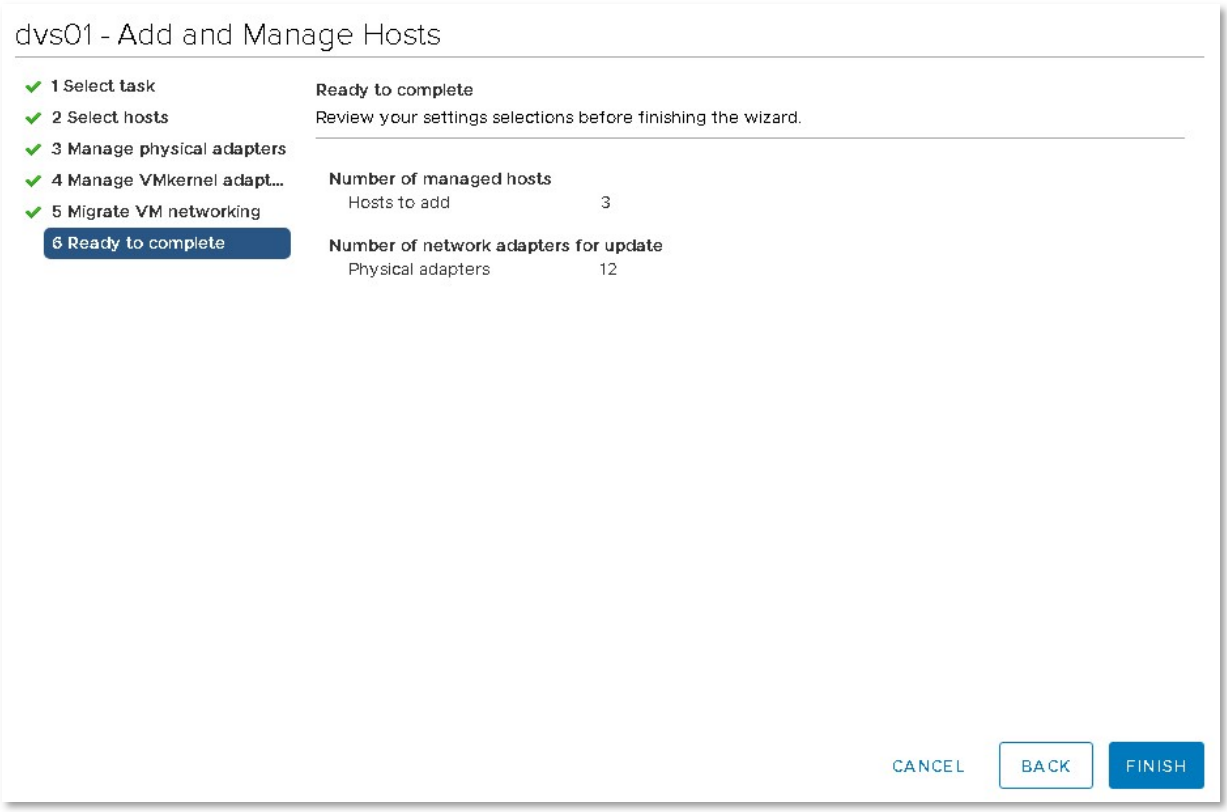
On associe les interfaces physiques aux uplink dvs en cochant la pour appliquer la même configuration à tous les hôtes.



Dans le cas d'une migration d'un vSwitch standard vers dvs, on pourra migrer à chaud les vmKernel existant sur le nouveau dvs.
Il y a un rollback automatique en cas de coupure de la liaison avec le vCenter. Notamment dans le cas d'un VLAN non configuré côté switch par exemple.



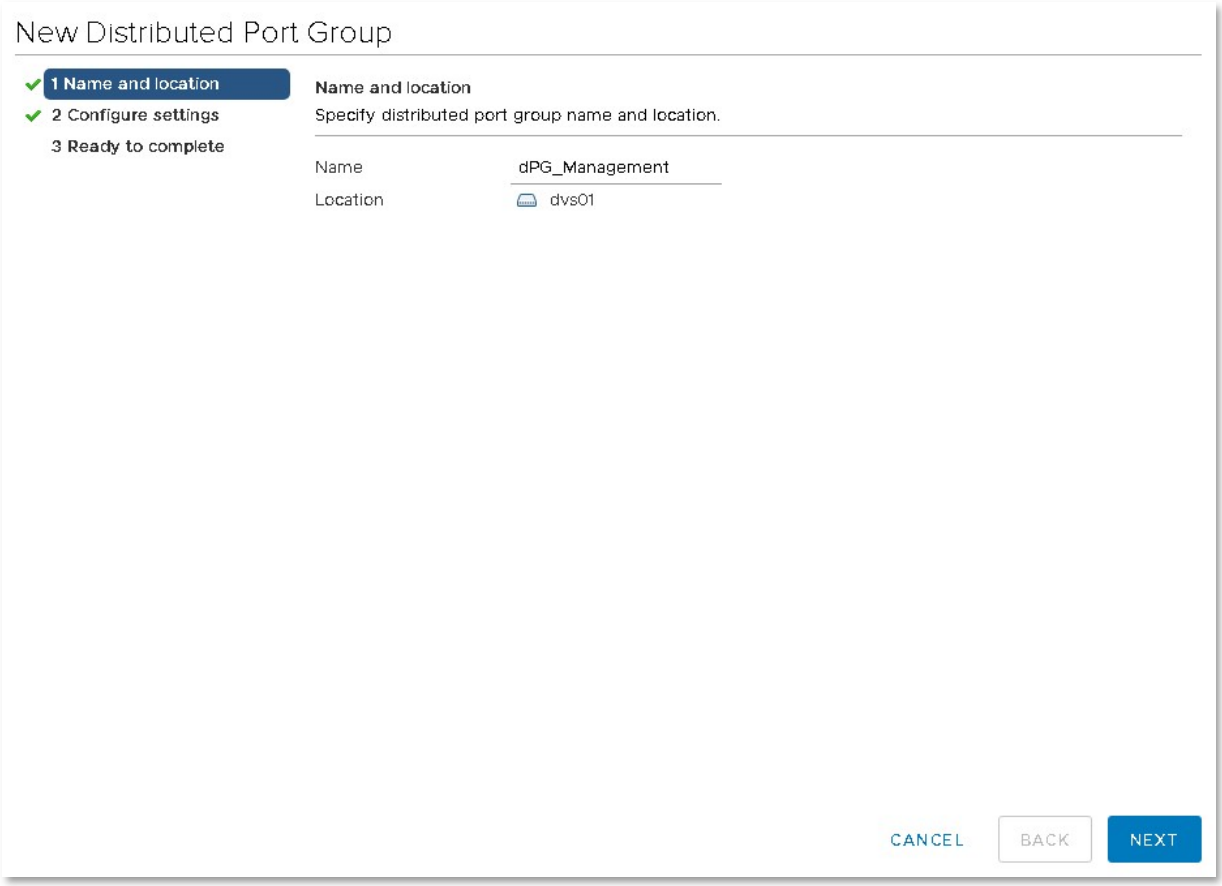
De la même manière, on migrer des VM existantes sur le nouveau dvs.



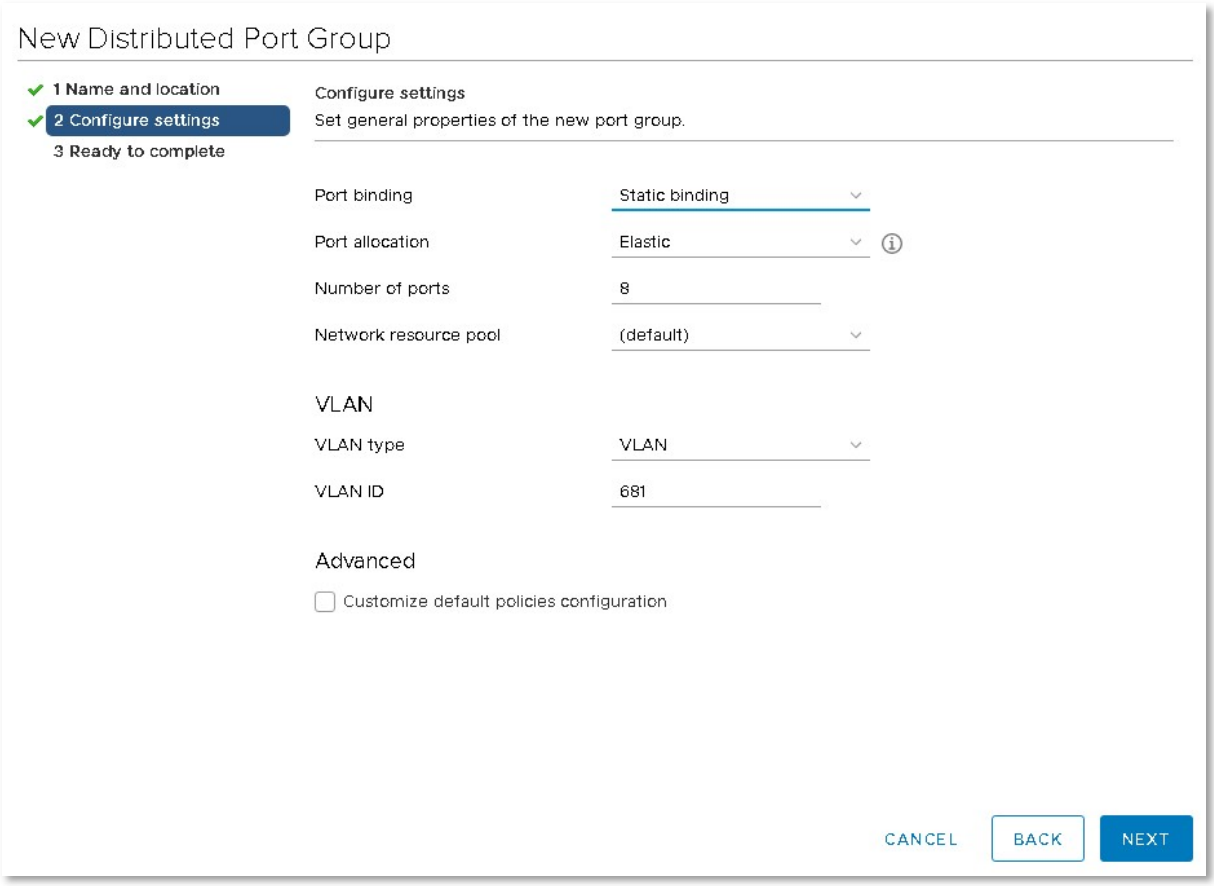
Enfin, on clique sur « Finish » pour terminer l'ajout des hôtes ESXi au dvs.

1.4 Configuration d’un distributed port group

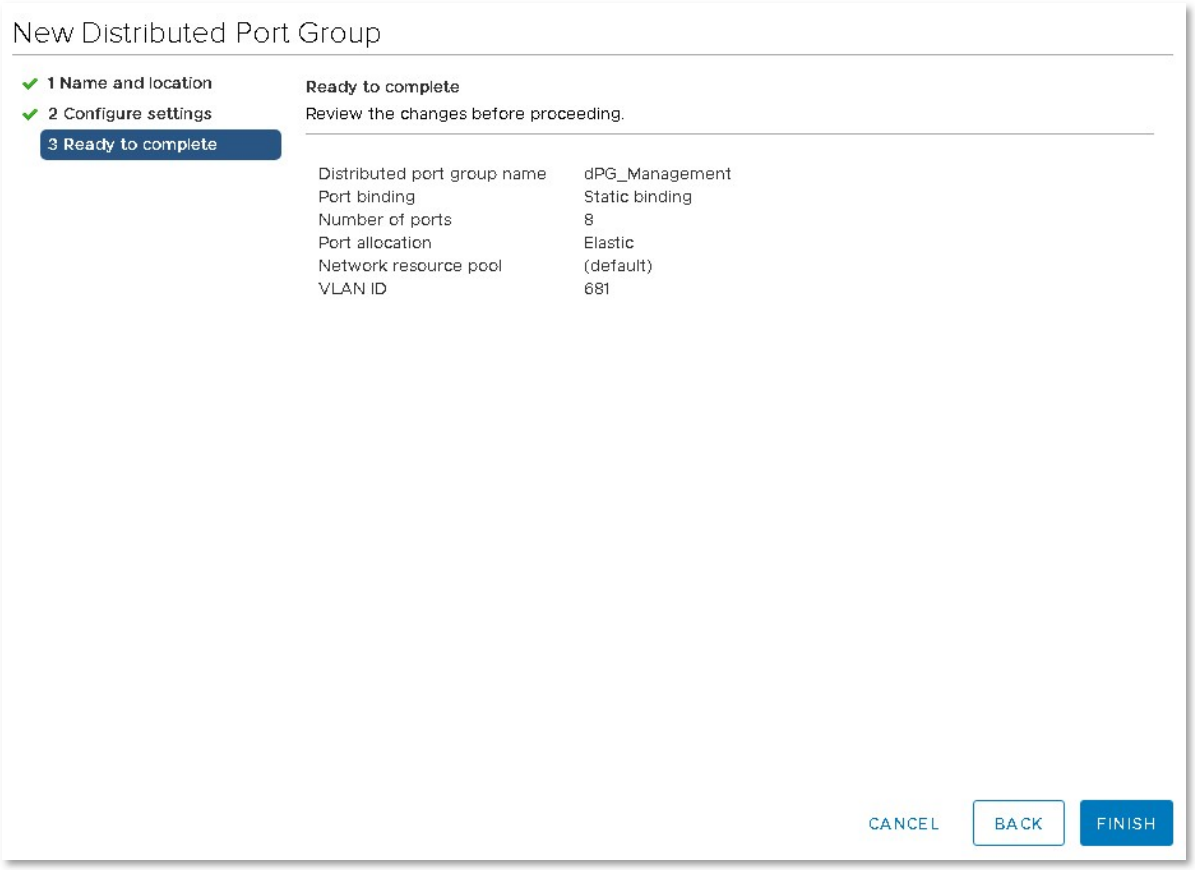
Aller dans Network / <dvs_name> / Hosts puis action et Add distributed port group



On nomme le distributed port group. Choisir un nom explicite et si besoin, indiquer l’id de VLAN, ça peut faciliter l’exploitation pour sur les réseaux complexe.
Exemple de nomenclature : dPG_<portGroupName> ou dPG_<VLANID>_<portGroupName>



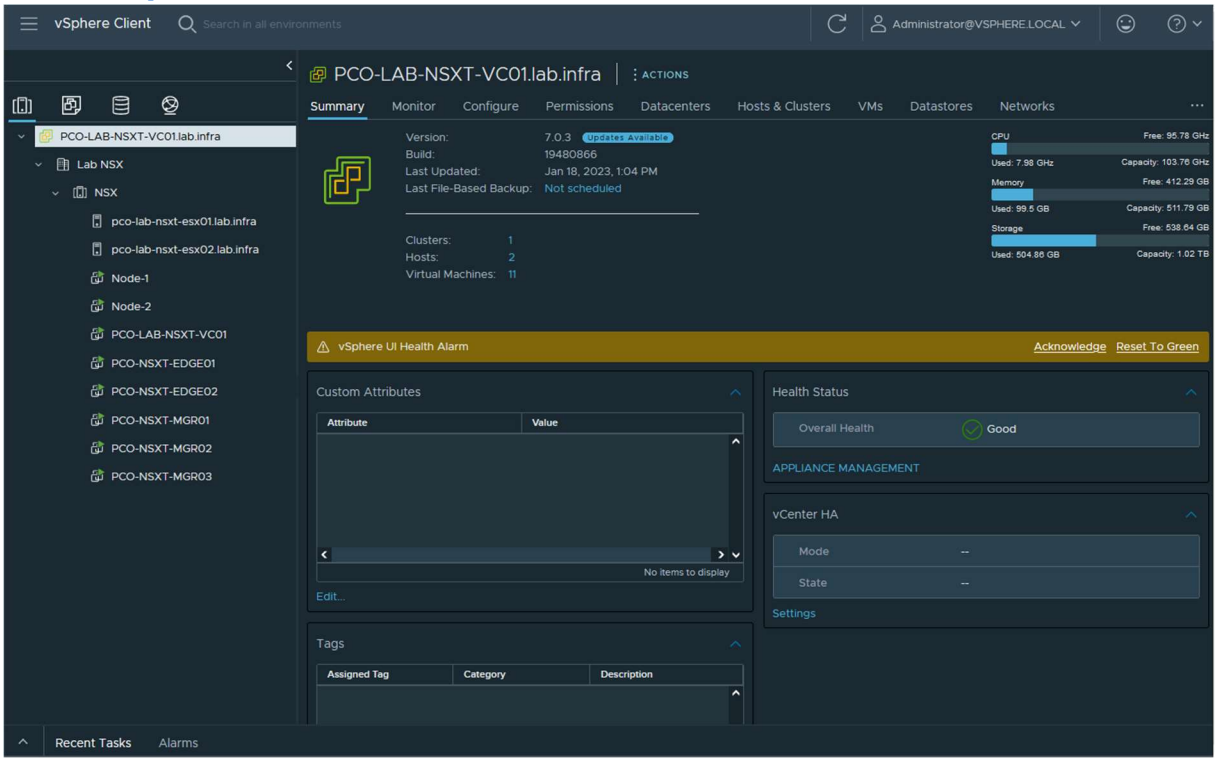
On laissera le port binding en static et l'allocation de port en elastic.
En fonction du besoin, on tag le VLAN.
Sauf exception, on laissera les paramètres avancés dans leur configuration par défaut.



On clique sur « Finish » pour terminer la configuration du distributed port group.

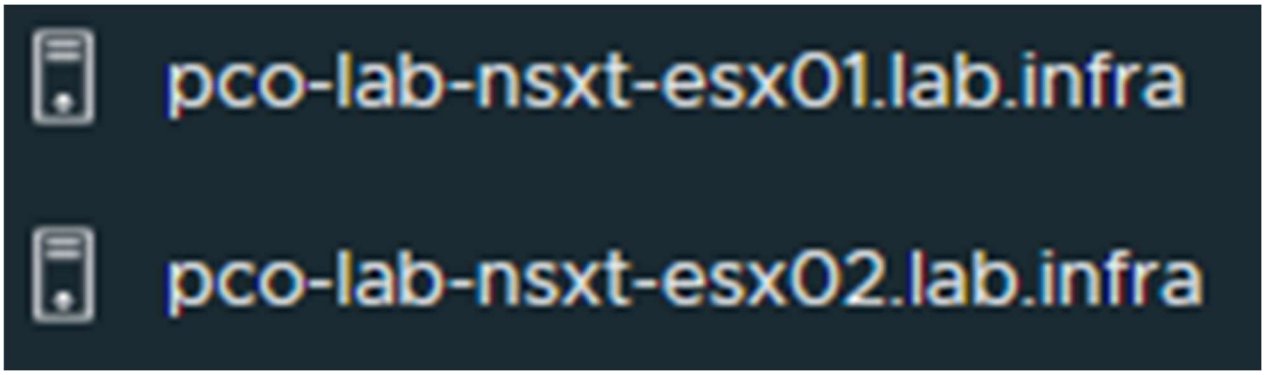
2 Configuration NSX

2.1 vSphere Client



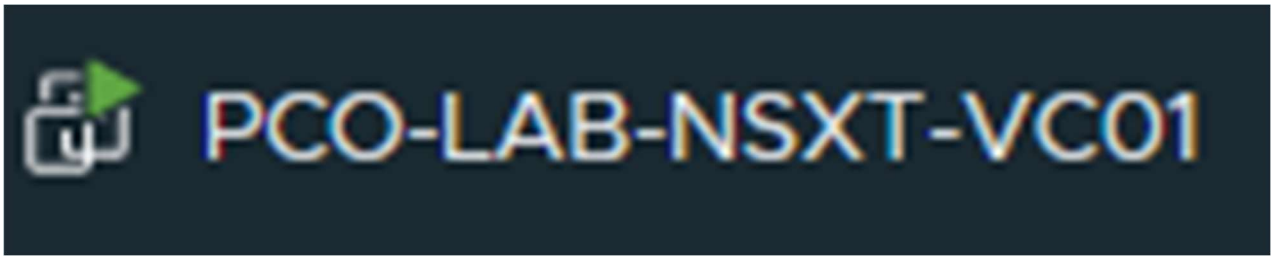
2.2 Serveurs

Deux ESXI sur UCS Cisco

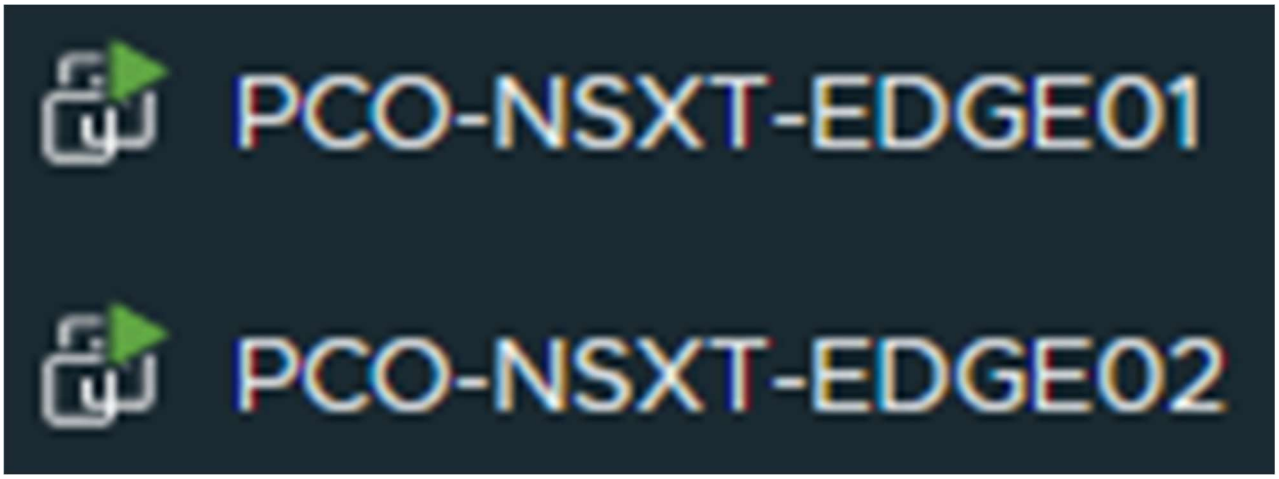


2.3 VMs

vCenter

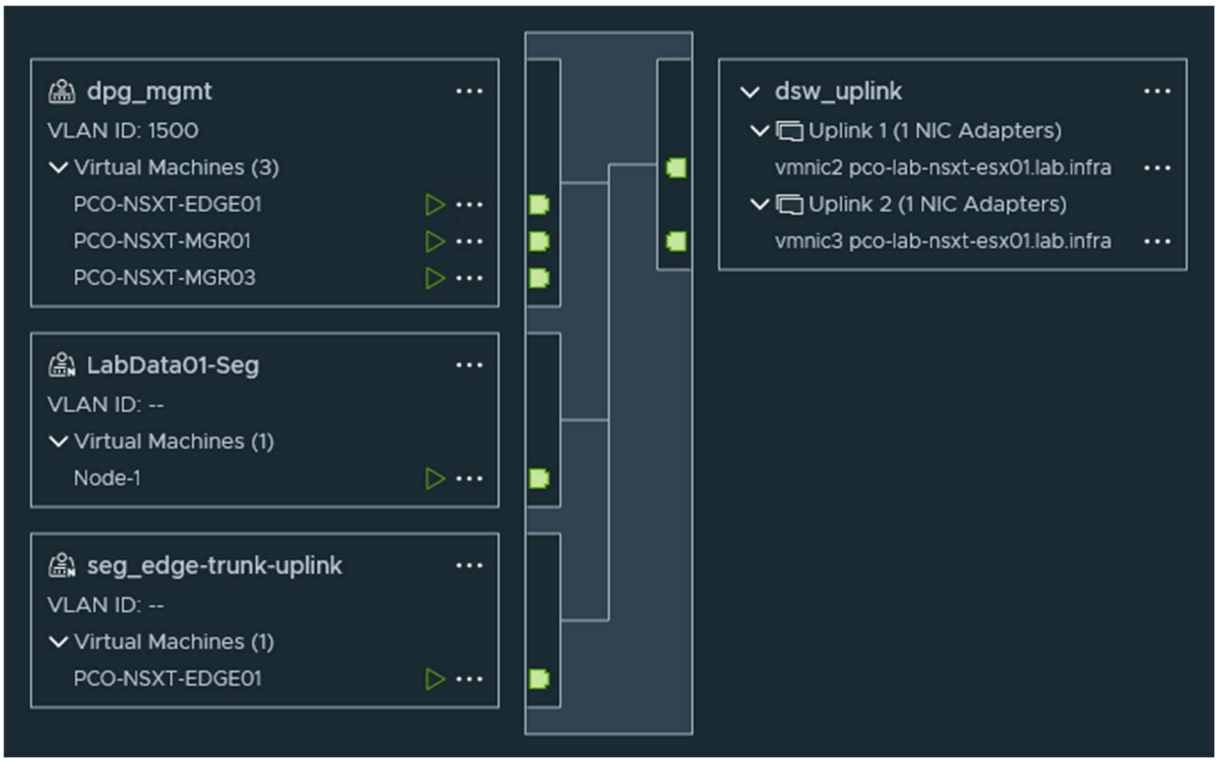


Edge node

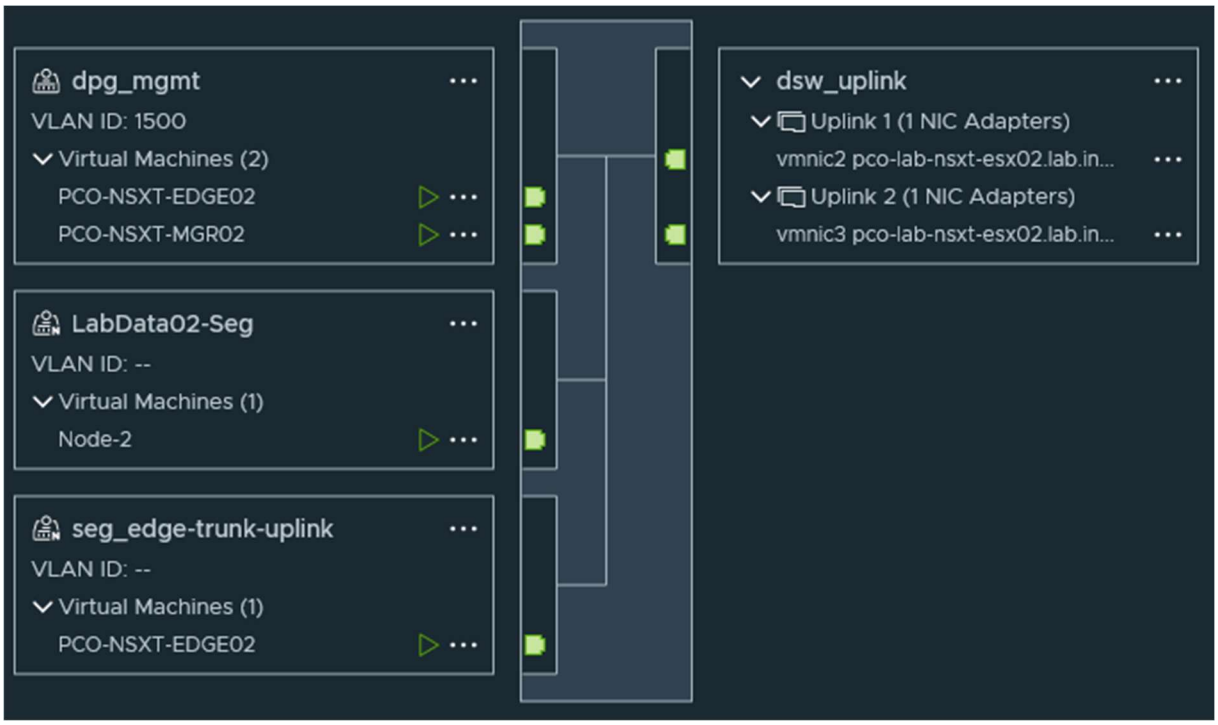


Management

2.4 Virtual switches ESX01



2.5 Virtual switches ESX02



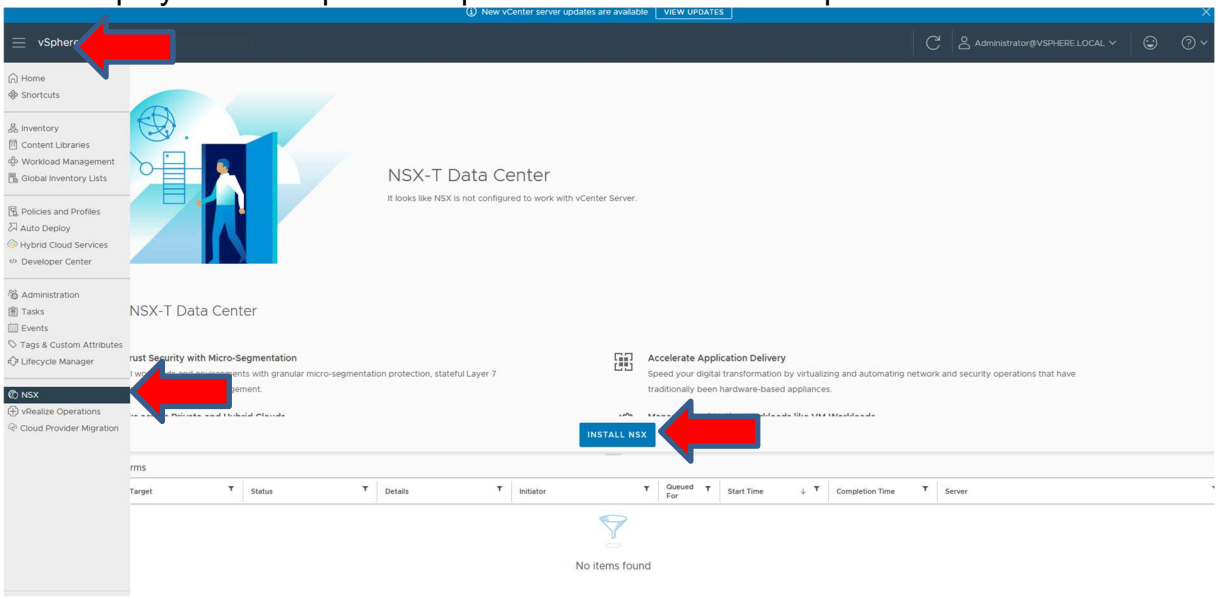
2.6 Enregistrement DNS des VM

2.7 Enregistrement DNS

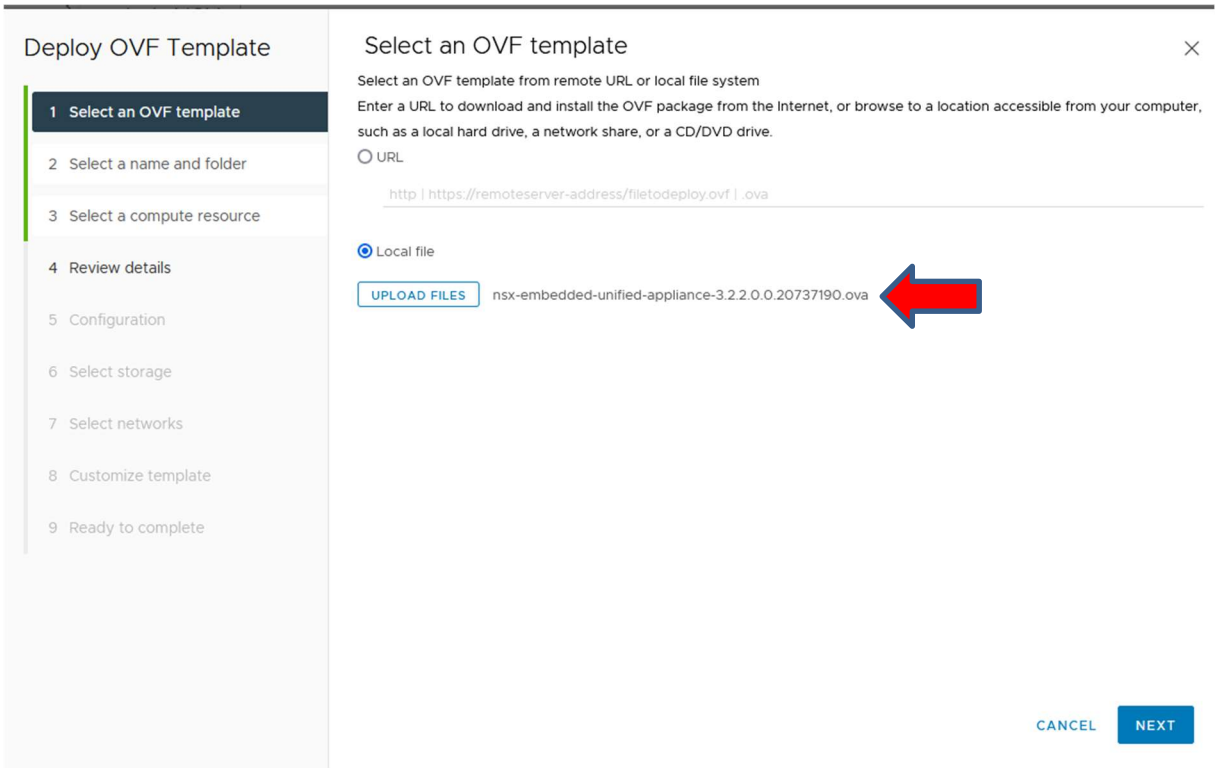
PCO-LAB-NSXT-ESX01	Host (A)	172.25.101.5	static
pco-lab-nsxt-esx02	Host (A)	172.25.101.6	static
PCO-LAB-NSXT-VC01	Host (A)	172.25.101.7	static
PCO-Node-Manager	Host (A)	172.25.101.10	static
PCO-NSXT-EDGE01	Host (A)	172.25.101.9	static
PCO-NSXT-IP-VIRTU	Host (A)	172.25.101.15	static
PCO-NSXT-MGR01	Host (A)	172.25.101.8	static
PCO-NSXT-MGR02	Host (A)	172.25.101.13	static
PCO-Win-2016	Host (A)	172.25.101.1	static

2.8 Déploiement NSX Manager

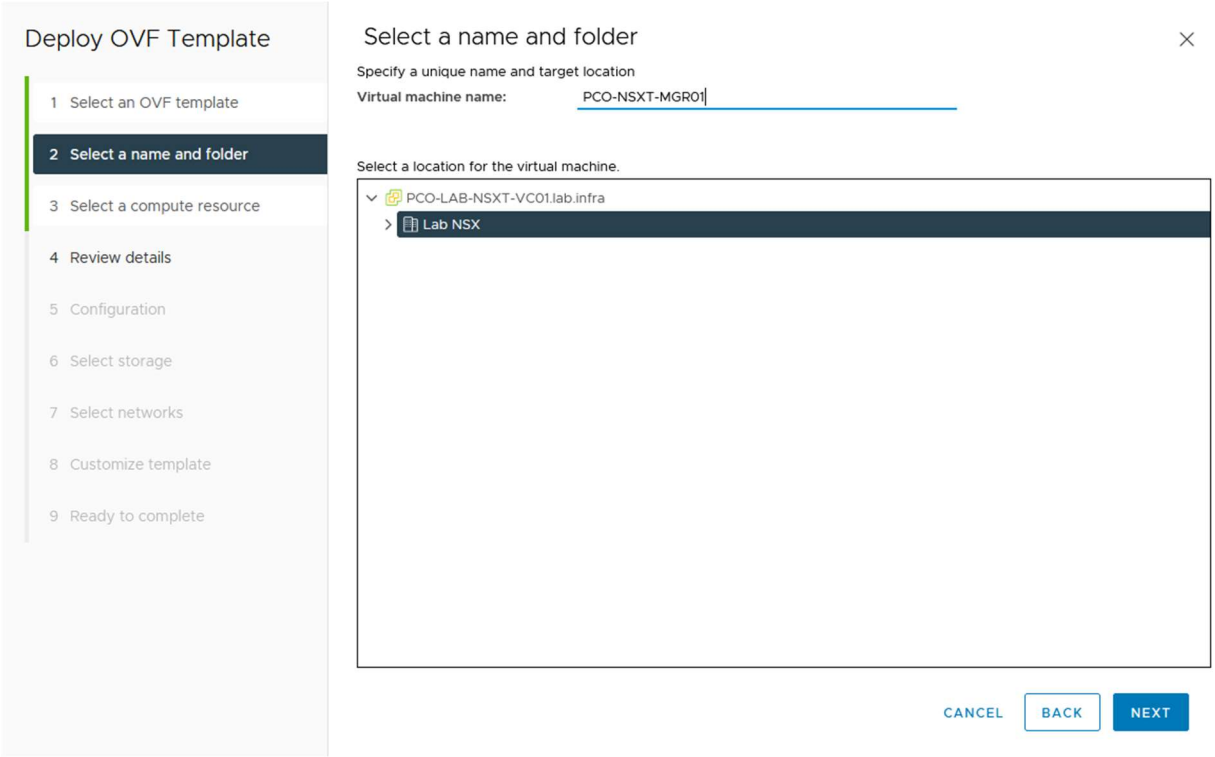
Pour déployer NSX depuis le vSphere client suivre les étapes suivantes



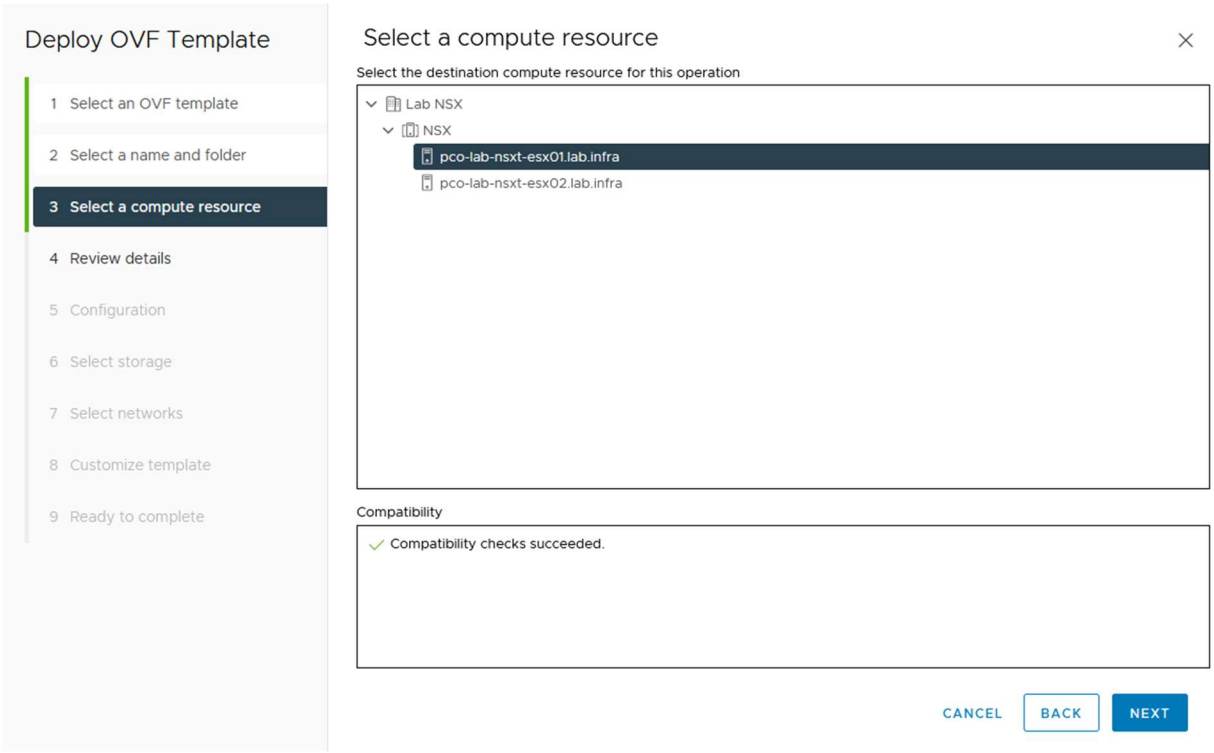
On selectionne le fichier



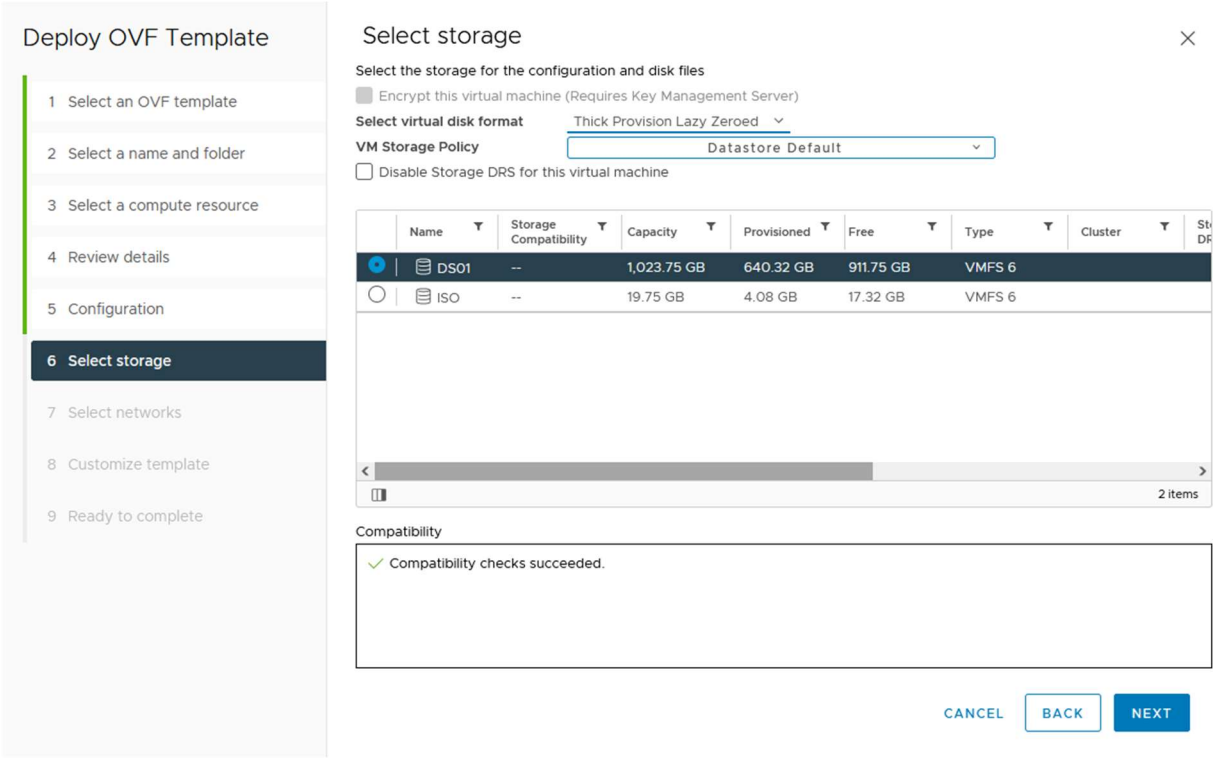
Vous nommez votre VM



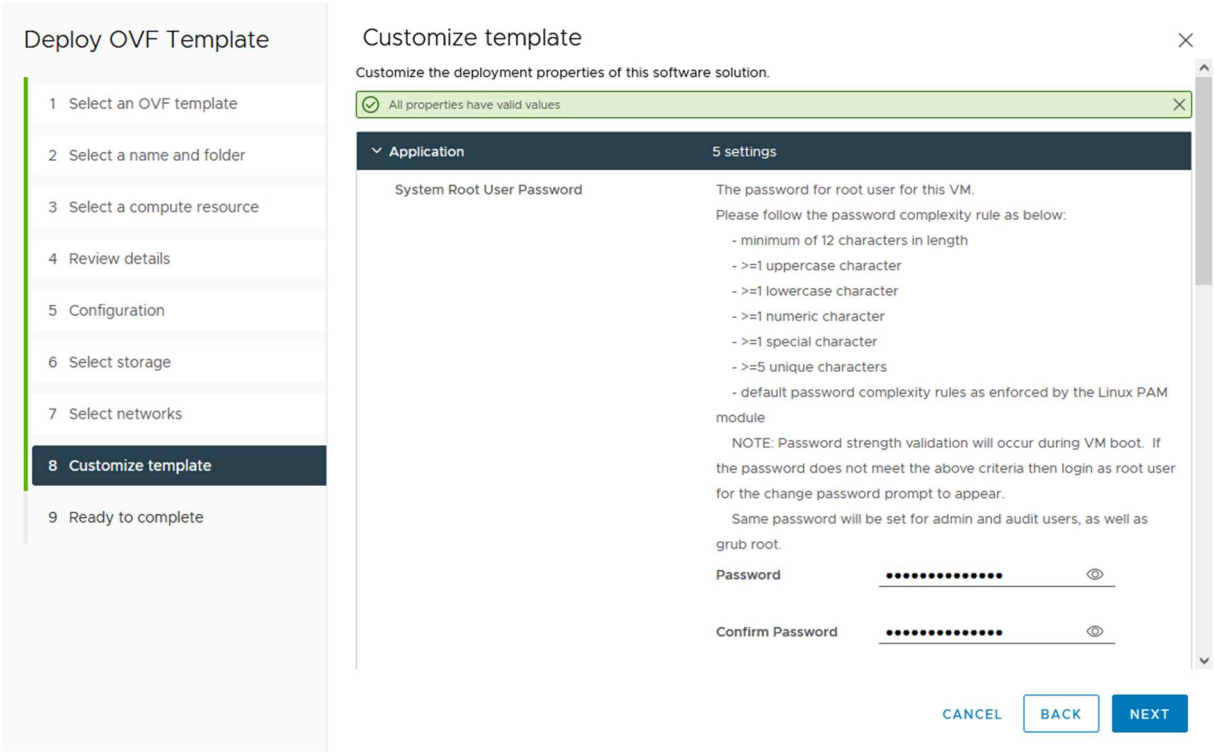
Vous sélectionner l'hyperviseur qui va héberger « l'Appliance »



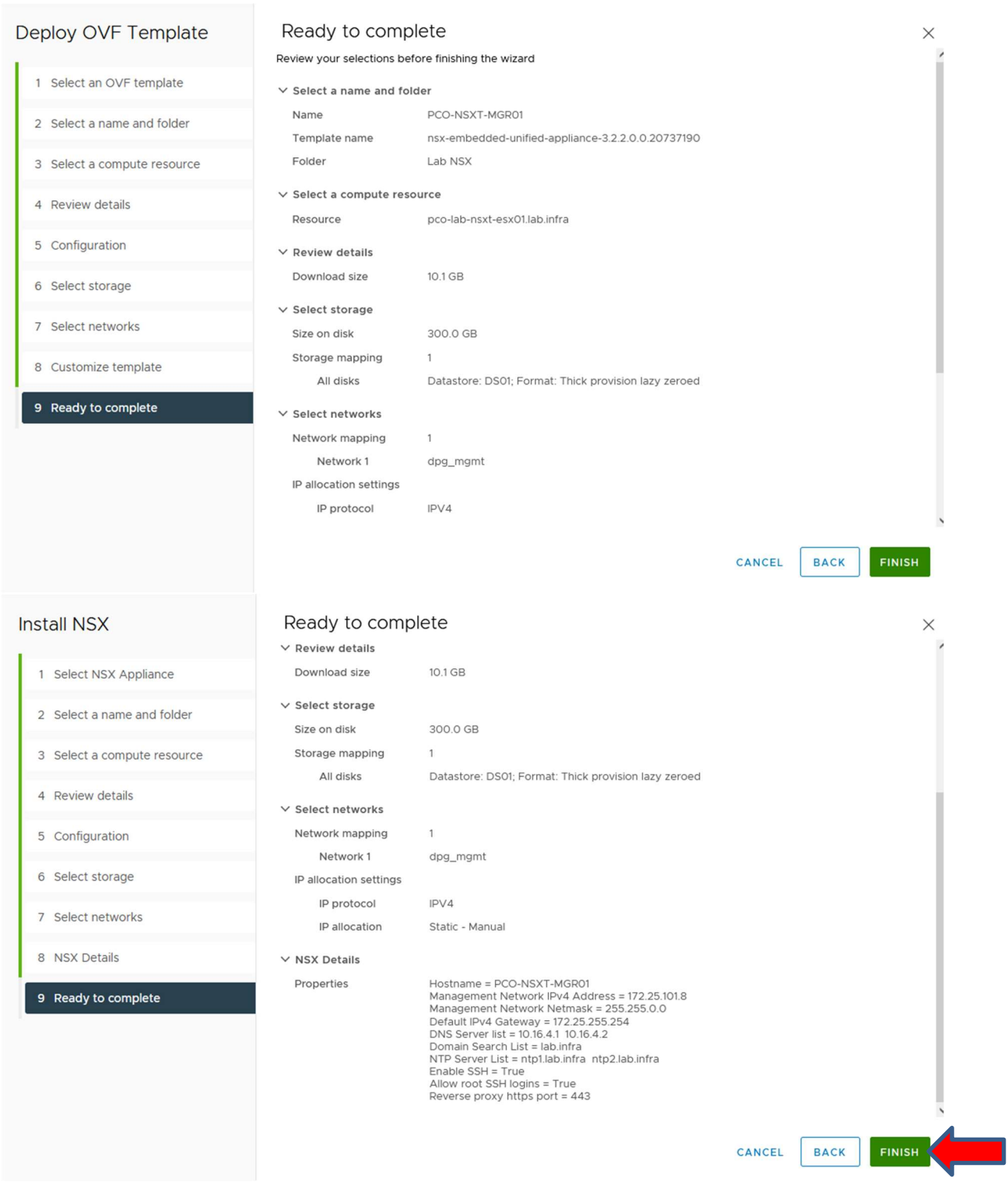
Vous sélectionner le stockage



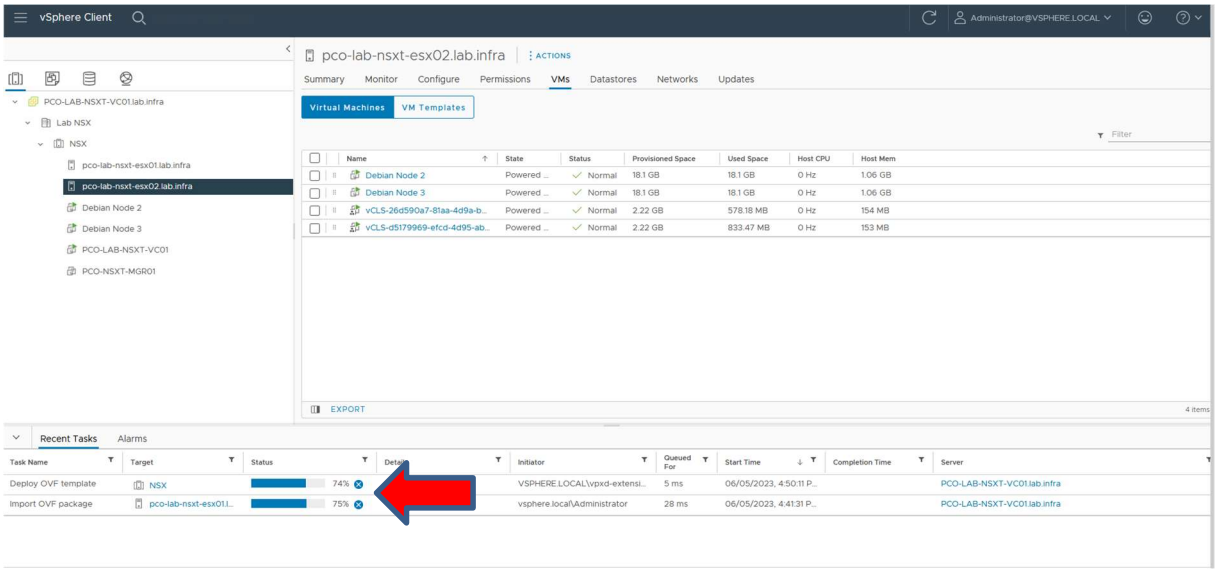
Configuration password et réseaux (IP/CIDR/DNS/DNS)



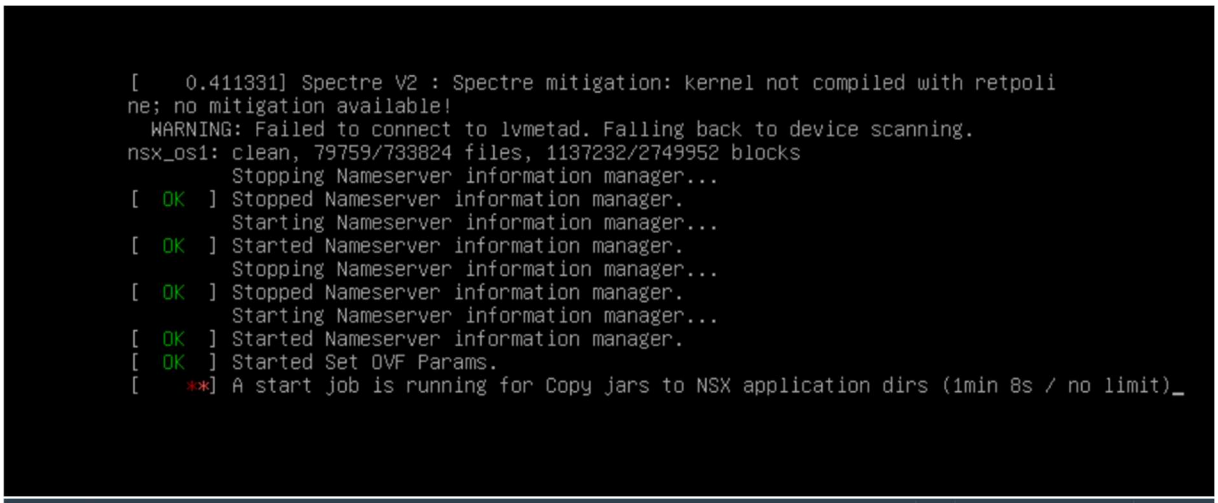
Résumé de la configuration effectué

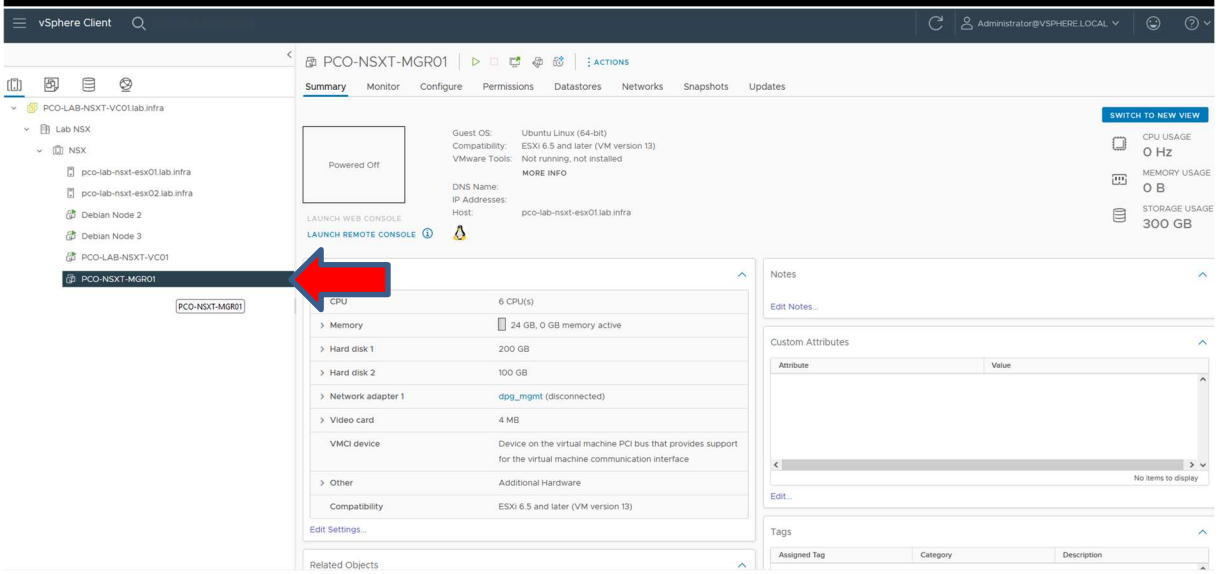


Dans vCenter vous devez avoir deux taches en cours dans les « tasks »

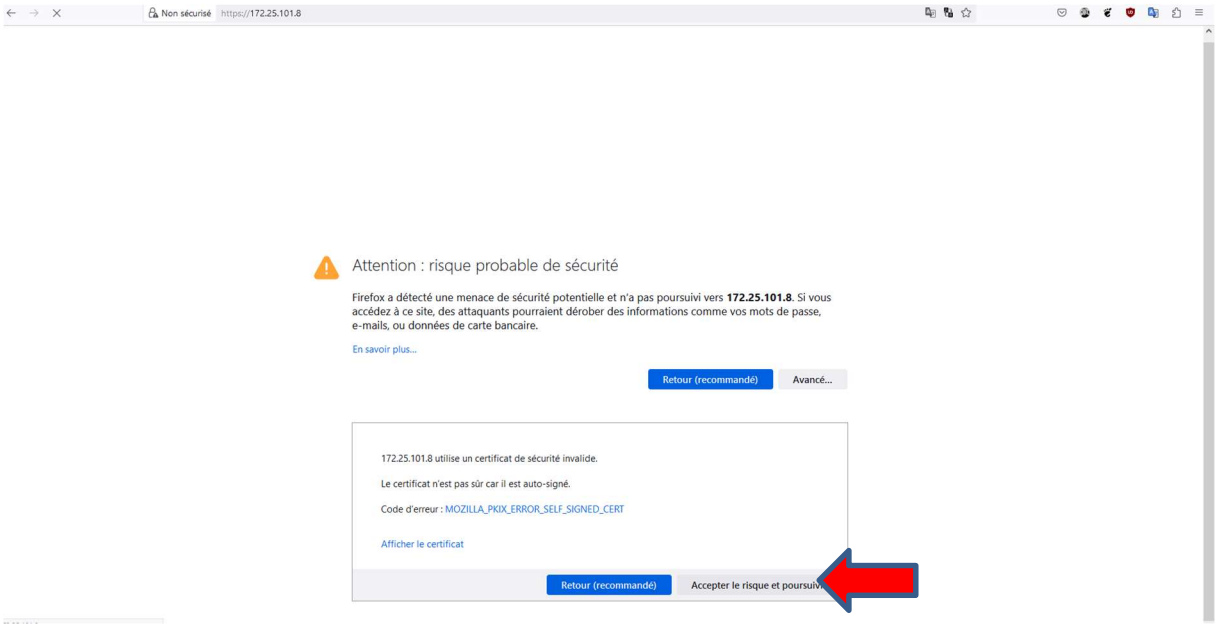


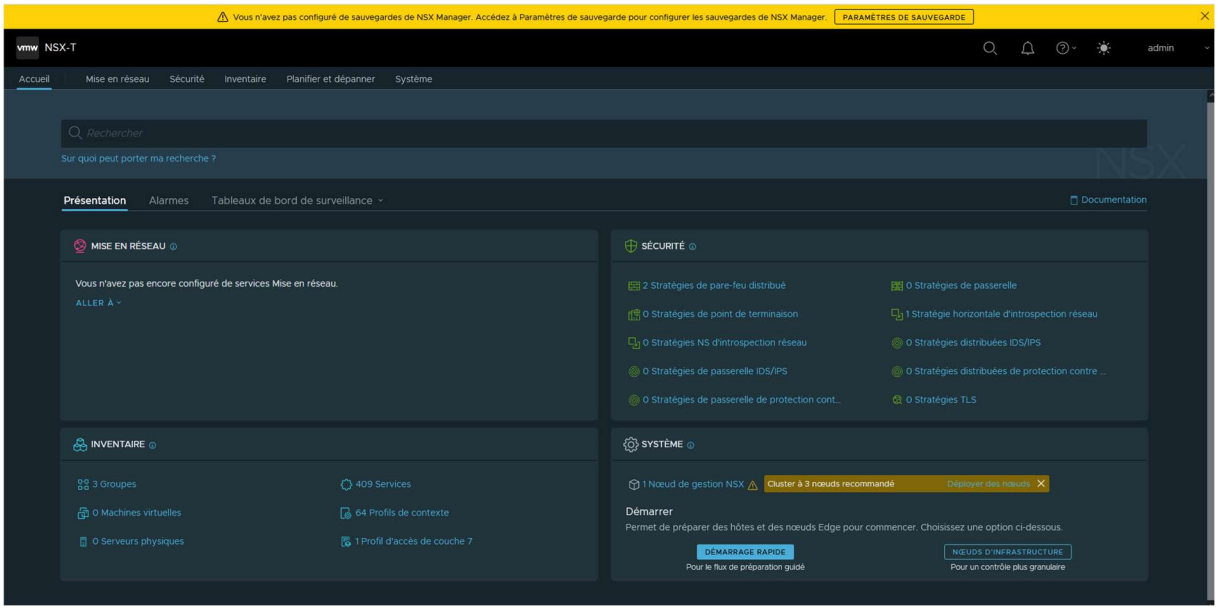
Une fois les taches terminer démarrer la VM





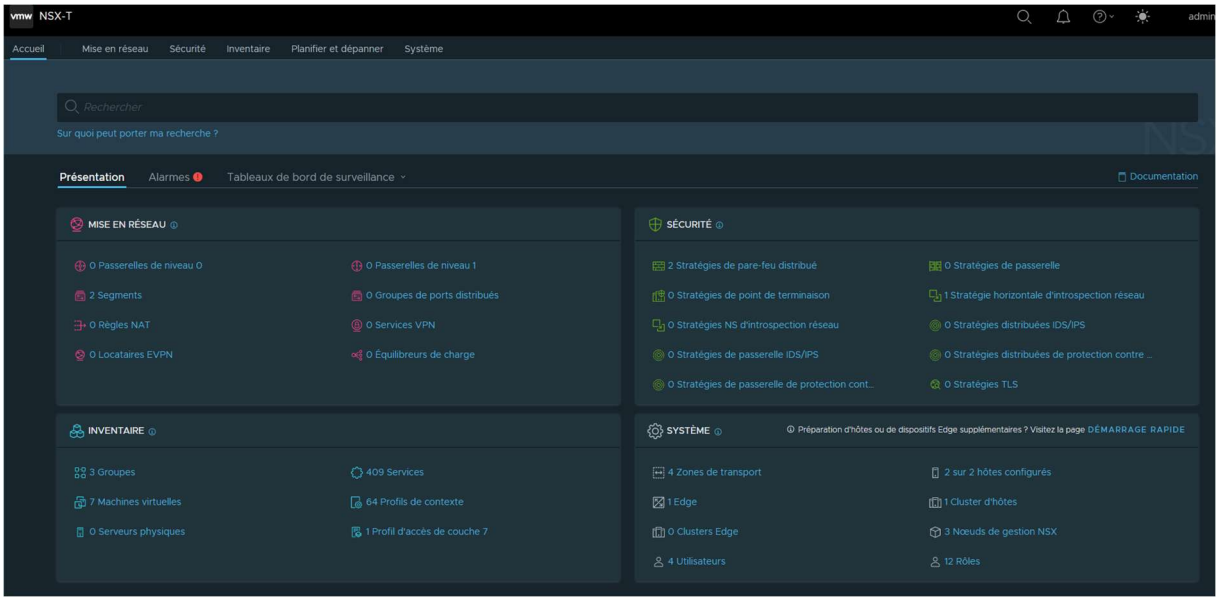
Se connecter à l’IP de la VM manager


Non sécurisé
https://172.25.101.8
Attention : risque probable de sécurité
Firefox a détecté une menace de sécurité potentielle et n'a pas poursuivi vers 172.25.101.8. Si vous accédez à ce site, des attaquants pourraient dérober des informations comme vos mots de passe, e-mails, ou données de carte bancaire.
En savoir plus...
Retour (recommandé)
Avancé...
172.25.101.8 utilise un certificat de sécurité invalide.
Le certificat n'est pas sûr car il est auto-signé.
Code d'erreur : MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT
Afficher le certificat
Retour (recommandé)
Accepter le risque et poursuivre

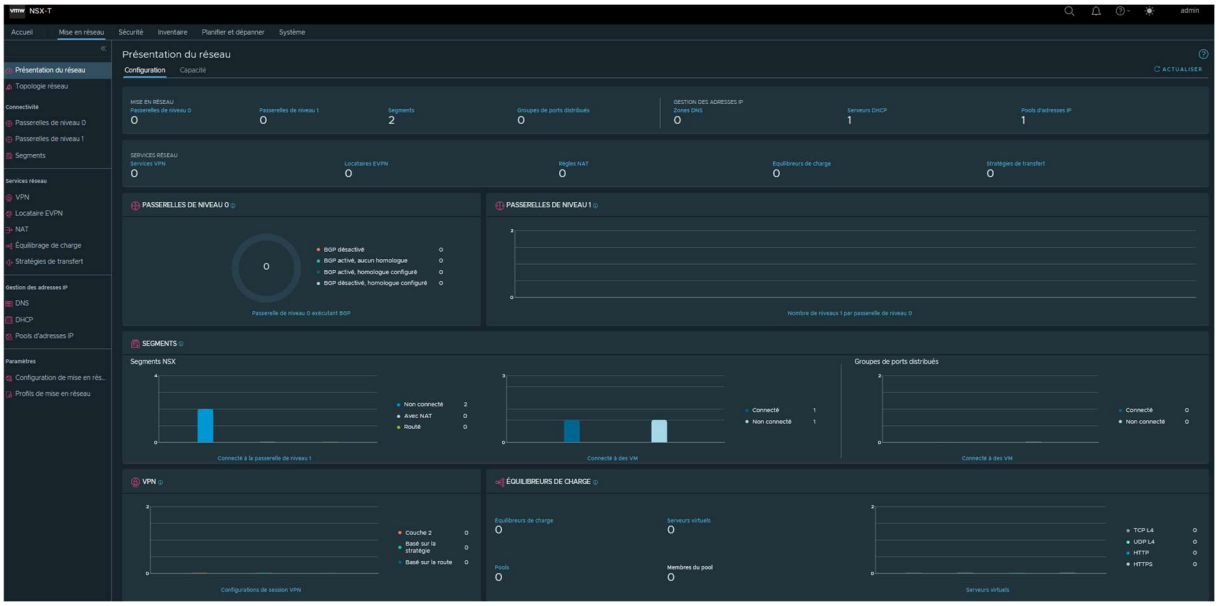

Vous n'avez pas configuré de sauvegardes de NSX Manager. Accédez à Paramètres de sauvegarde pour configurer les sauvegardes de NSX Manager.
PARAMÈTRES DE SAUVEGARDE
vmw NSX-T
admin
Accueil
Mise en réseau
Sécurité
Inventaire
Planifier et dépanner
Système
Rechercher
Sur quoi peut porter ma recherche ?
Présentation
Alarmes
Tableaux de bord de surveillance
Documentation
MISE EN RÉSEAU
Vous n'avez pas encore configuré de services Mise en réseau.
ALLER À
SÉCURITÉ
2 Stratégies de pare-feu distribué
0 Stratégies de passerelle
0 Stratégies de point de terminaison
1 Stratégie horizontale d'introspection réseau
0 Stratégies NS d'introspection réseau
0 Stratégies distribuées IDS/IPS
0 Stratégies de passerelle IDS/IPS
0 Stratégies distribuées de protection contre ...
0 Stratégies de passerelle de protection cont...
0 Stratégies TLS
INVENTAIRE
3 Groupes
409 Services
0 Machines virtuelles
64 Profils de contexte
0 Serveurs physiques
1 Profil d'accès de couche 7
SYSTÈME
1 Nœud de gestion NSX
Cluster à 3 nœuds recommandé
Déployer des nœuds
Démarrer
Permet de préparer des hôtes et des nœuds Edge pour commencer. Choisissez une option ci-dessous.
DÉMARRAGE RAPIDE
Pour le flux de préparation guidé
NŒUDS D'INFRASTRUCTURE
Pour un contrôle plus granulaire

3 Visuel de l'interface graphique NSX

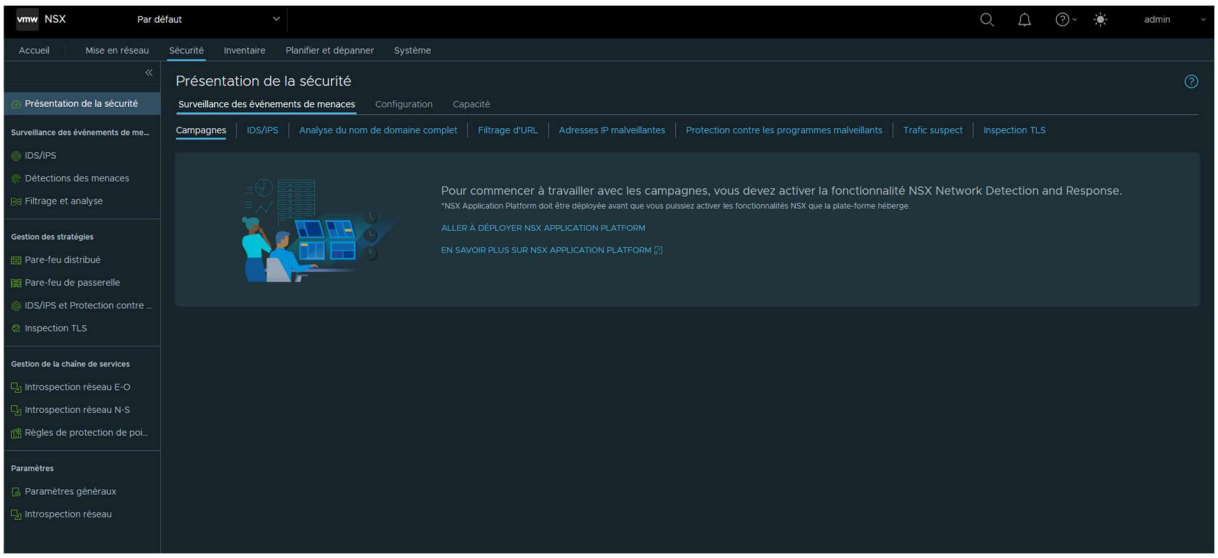
3.1 Accueil



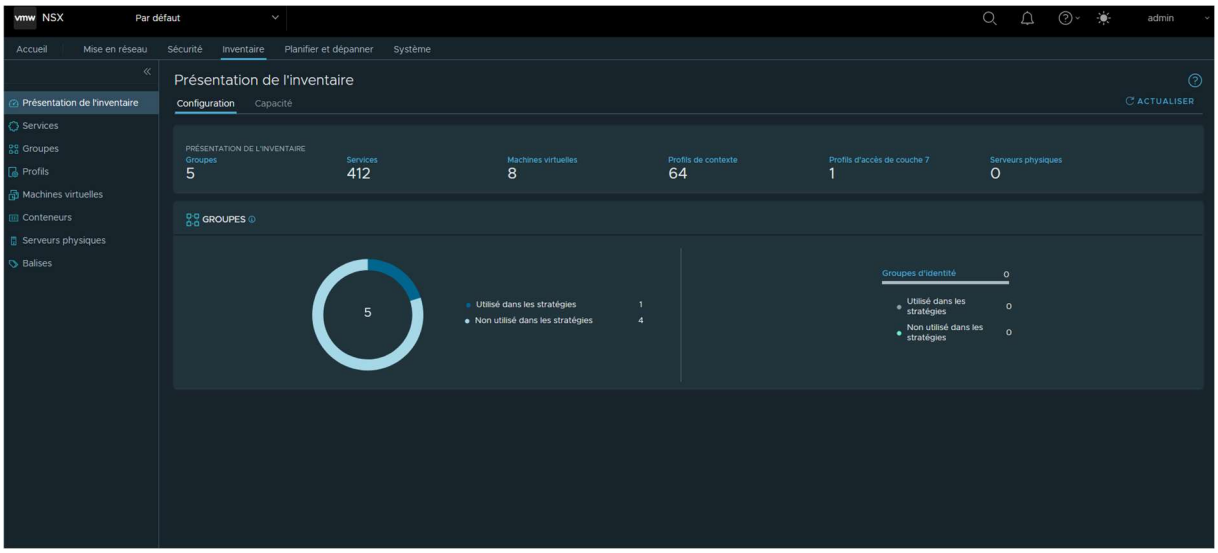
3.2 Mise en reseau



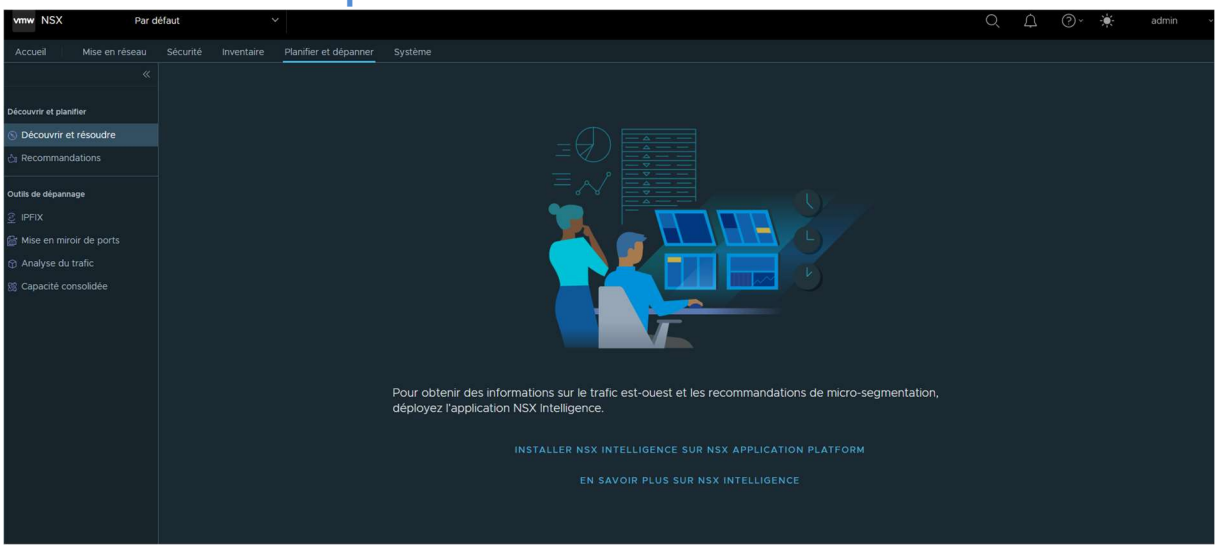
3.3 Sécurité



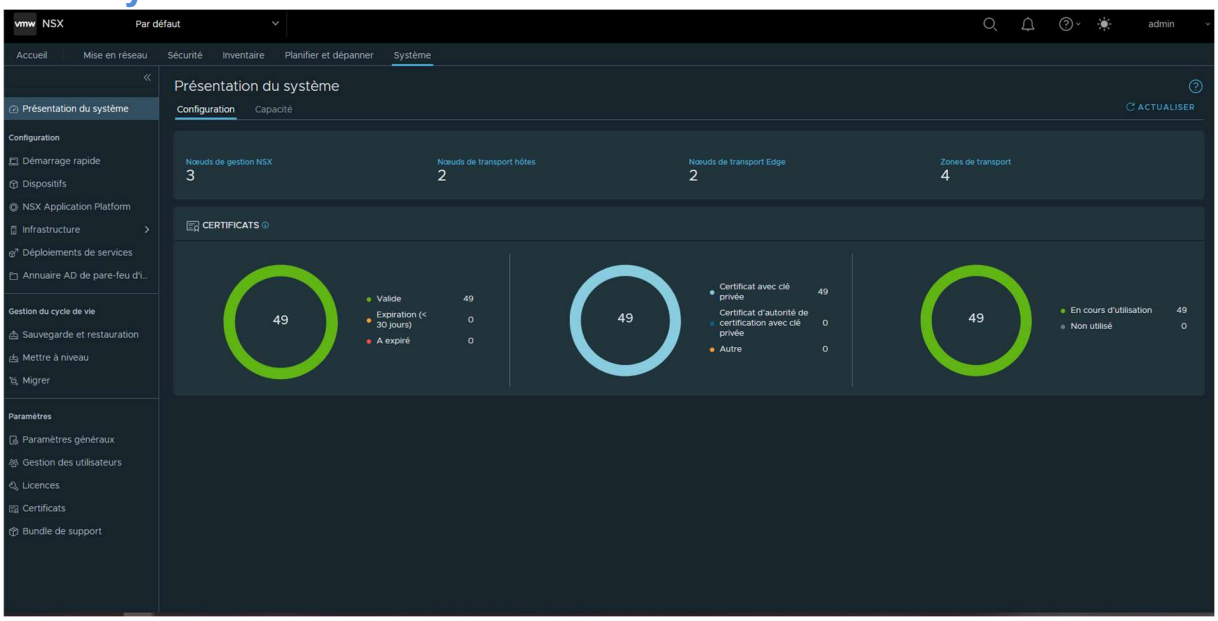
3.4 Inventaire



3.5 Planifier et dépanner

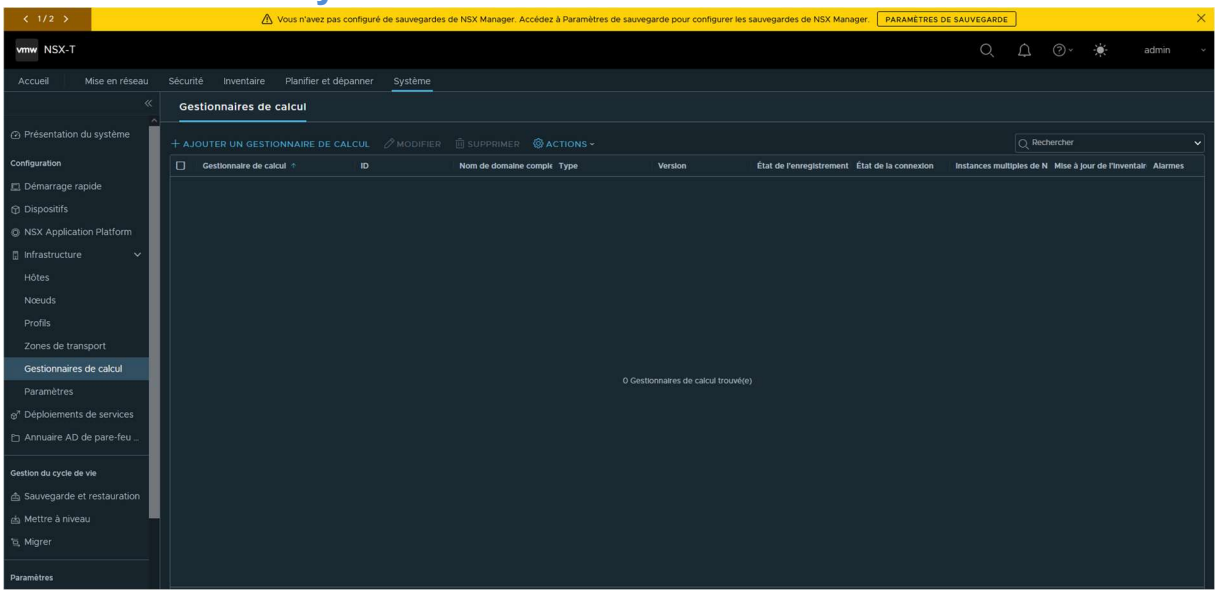


3.6 Systéme

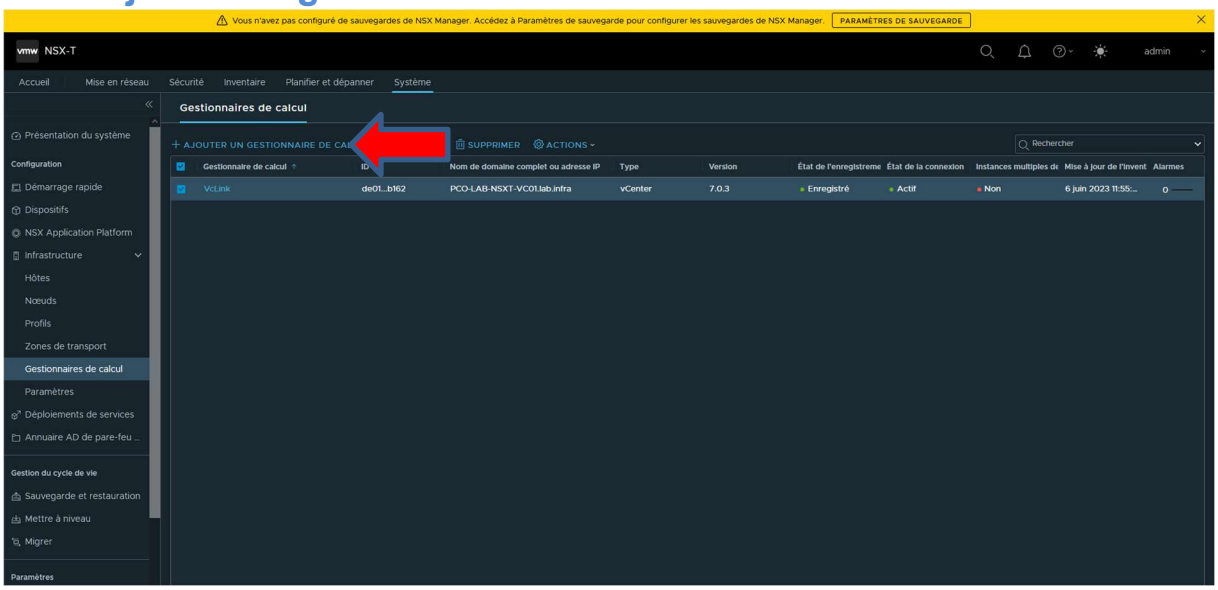


4 Enregistrement du vCenter dans NSX

4.1 Aller dans System / Infrastructure / Gestionnaire de calcul



4.2 Ajouter un gestionnaire de calcul



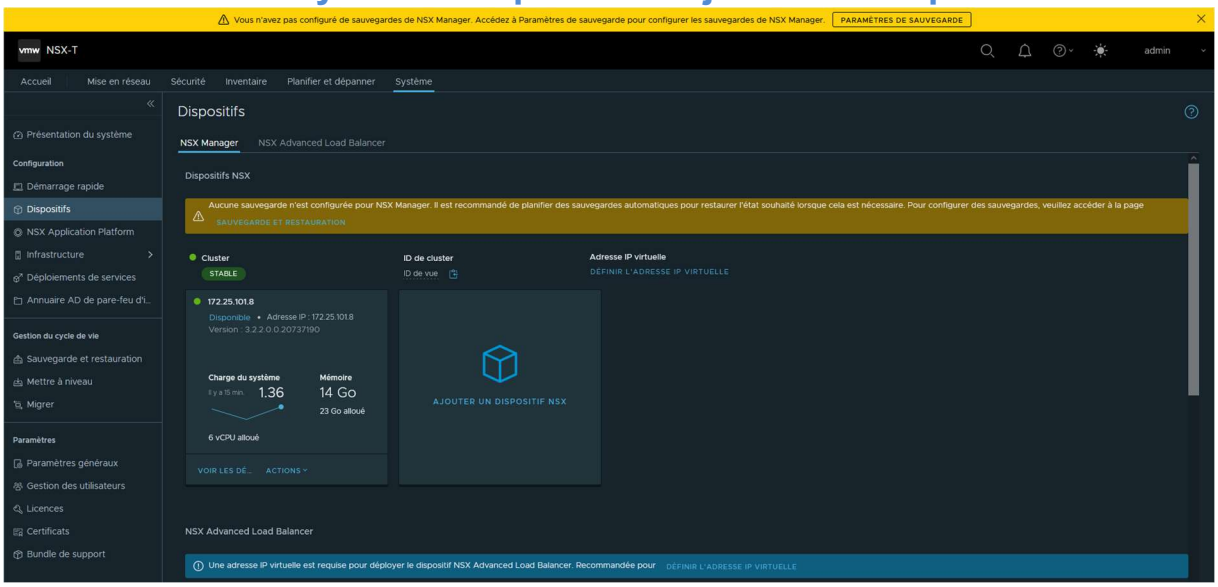
Le vCenter apparait et s'active.

4.3 Remarque importante

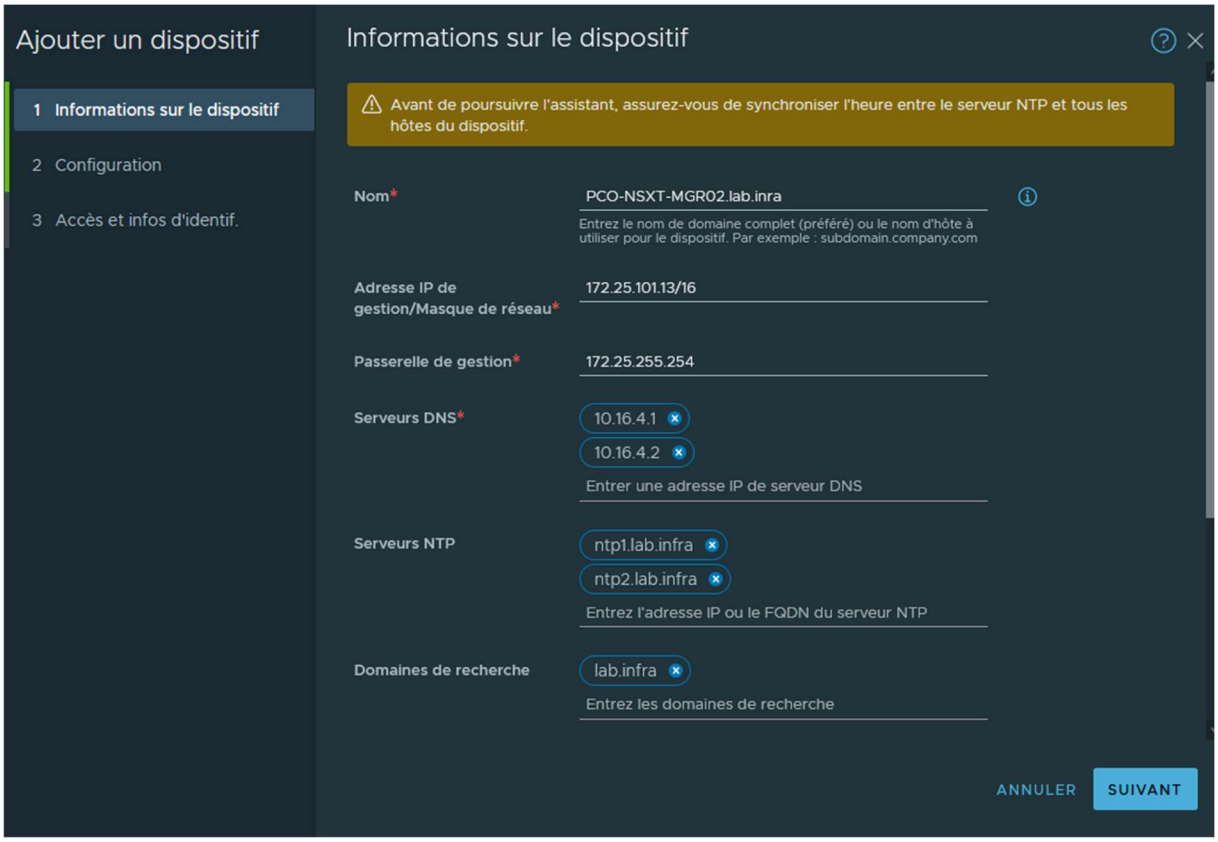
Si vous installez l'Appliance NSX manager depuis le menu NSX de vCenter pas besoin d'effectuer les actions ci-dessus.

5 Création du cluster NSX Manager

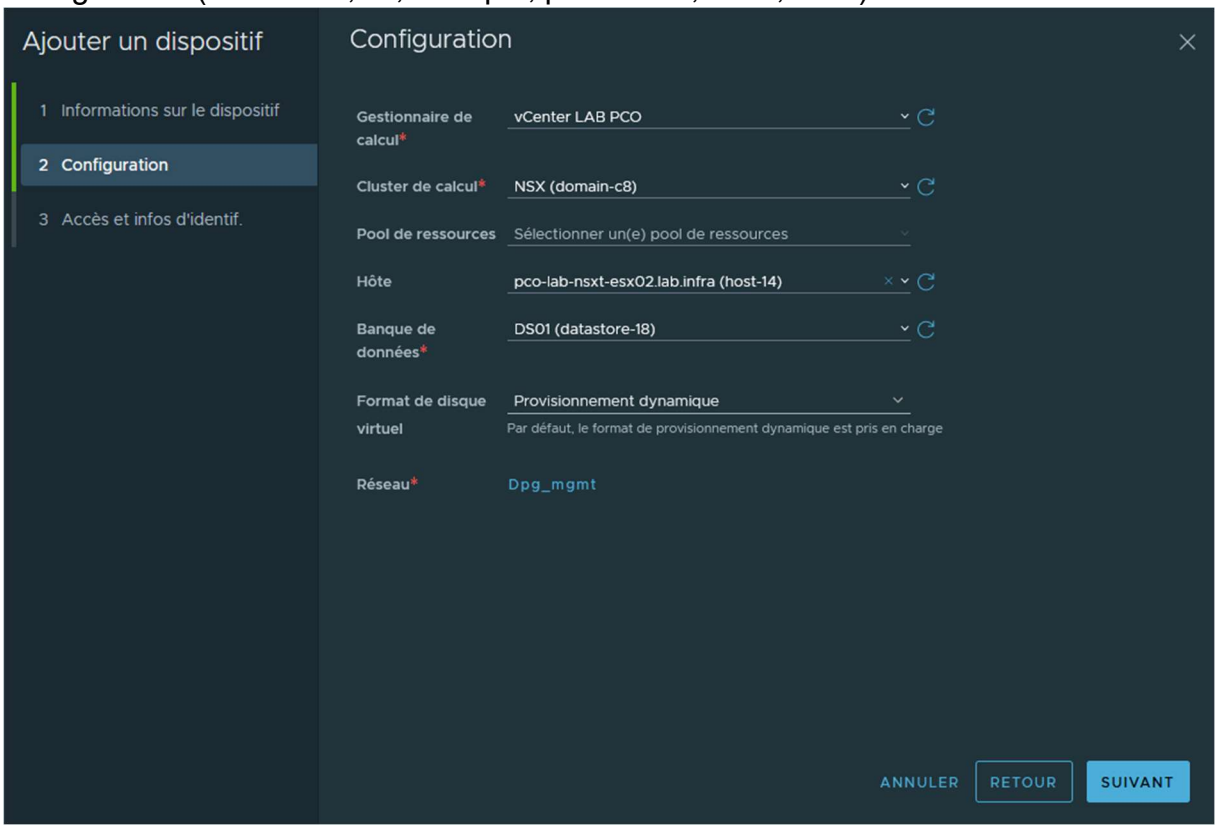
5.1 Aller dans System / Dispositifs / Ajouter un dispositif NSX



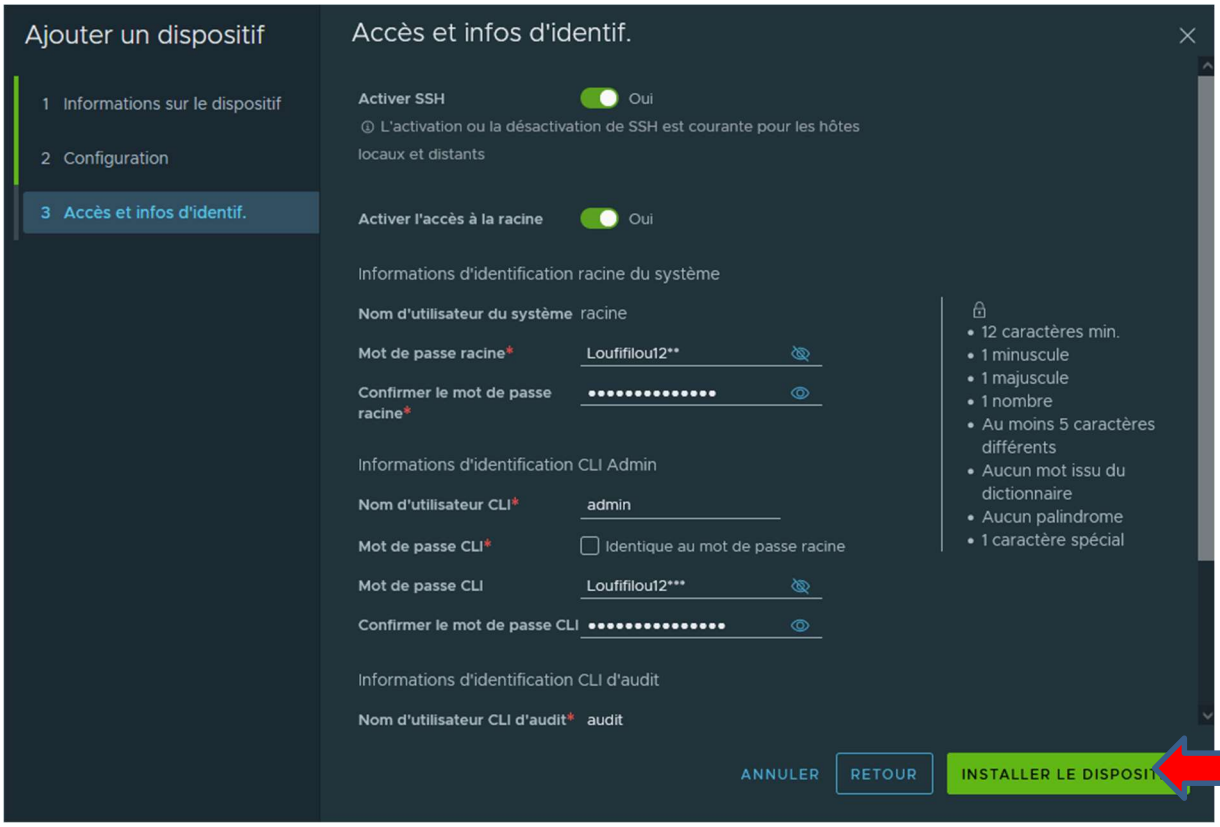
Il est recommandé de déployer 3 NSX Manager Node pour un environnement de production.



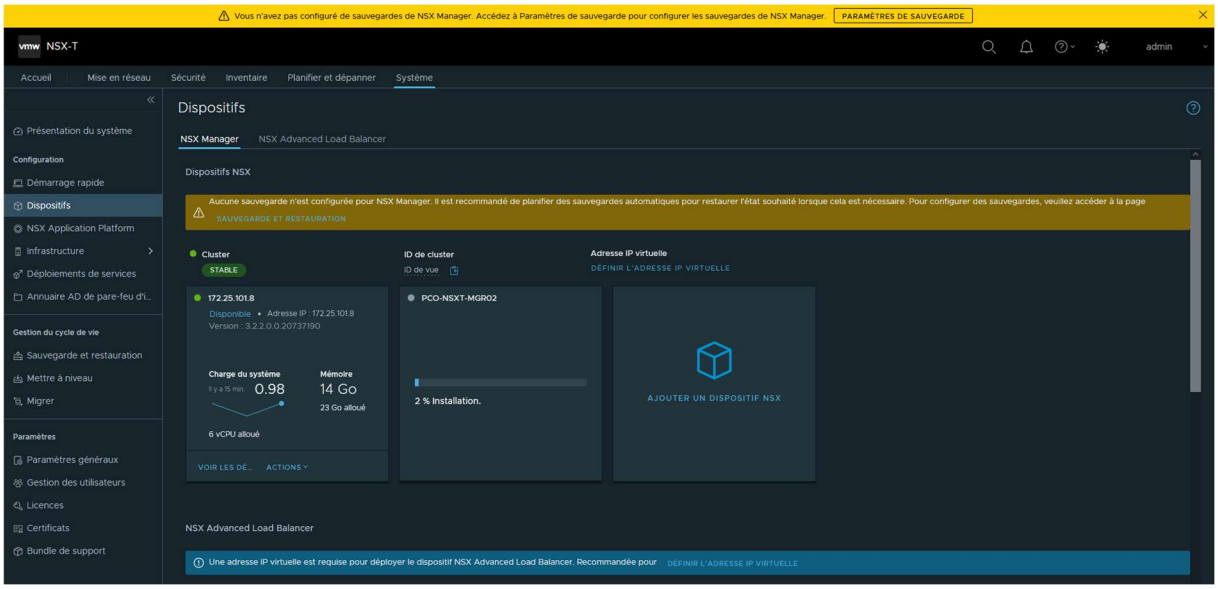
On déploie une seconde Appliance NSX Manager en renseignant les informations de configuration (hostname, IP, masque, passerelle, DNS, NTP).



On sélectionne le vCenter (compute manager), le cluster et l'hôte sur lequel déployer l'Appliance, un datastore et un port group (pour l'interface de management).

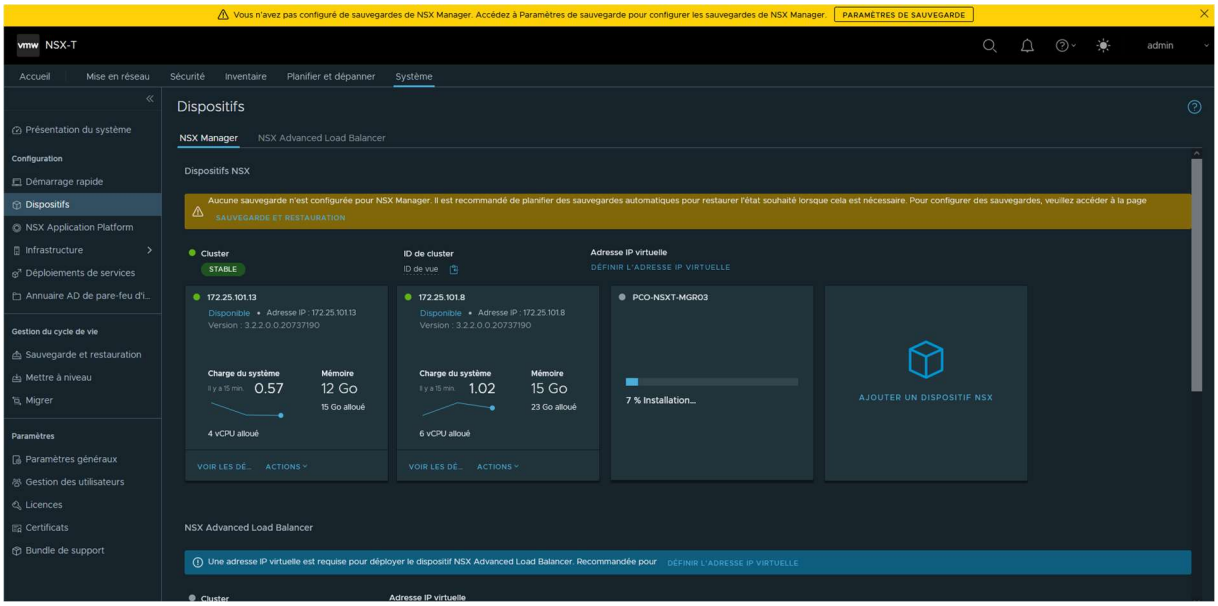


On renseigne les credentials des différents comptes natif (root, admin et audit). Enfin, on clique sur « Install Appliance » pour démarrer le déploiement.

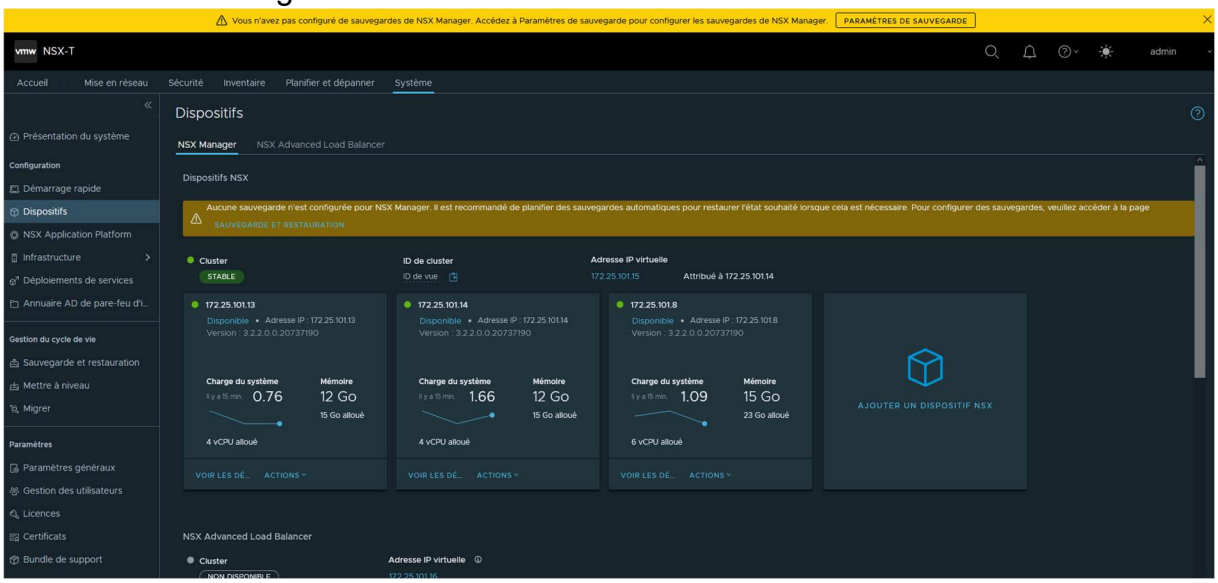


Avant de déployer le 3ème node, il faut attendre que le second ait terminer son déploiement et qu'il remonte correctement dans la console NSX Manager.

On répète ces opérations pour le 3ème NSX Manager Node.

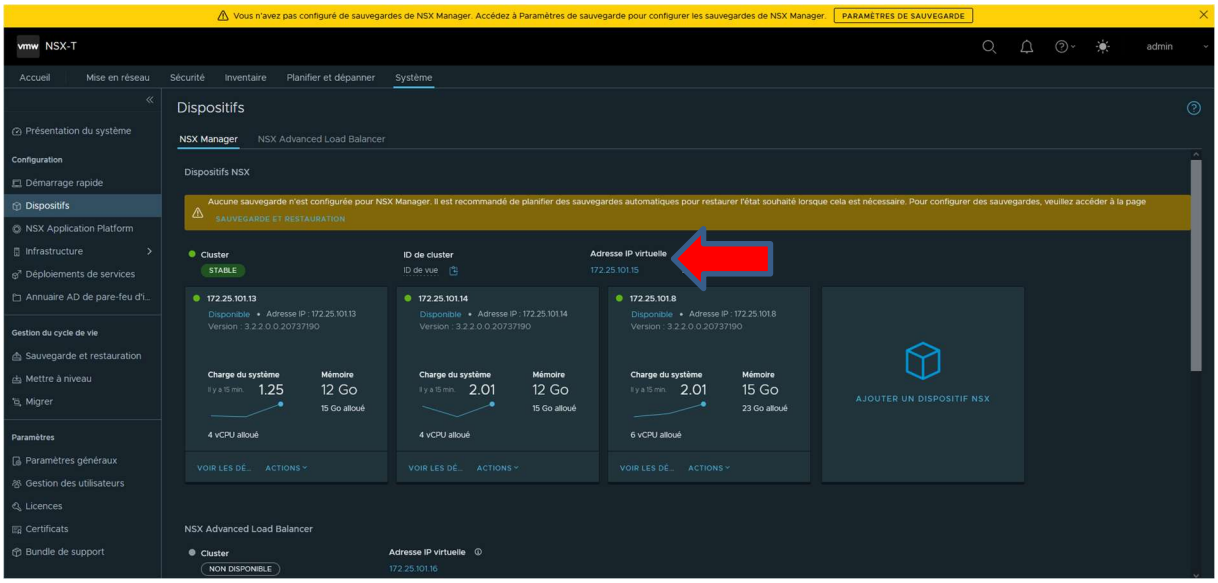


Le cluster de manager est installé et stable



5.2 Configuration « VIP » du cluster Manager

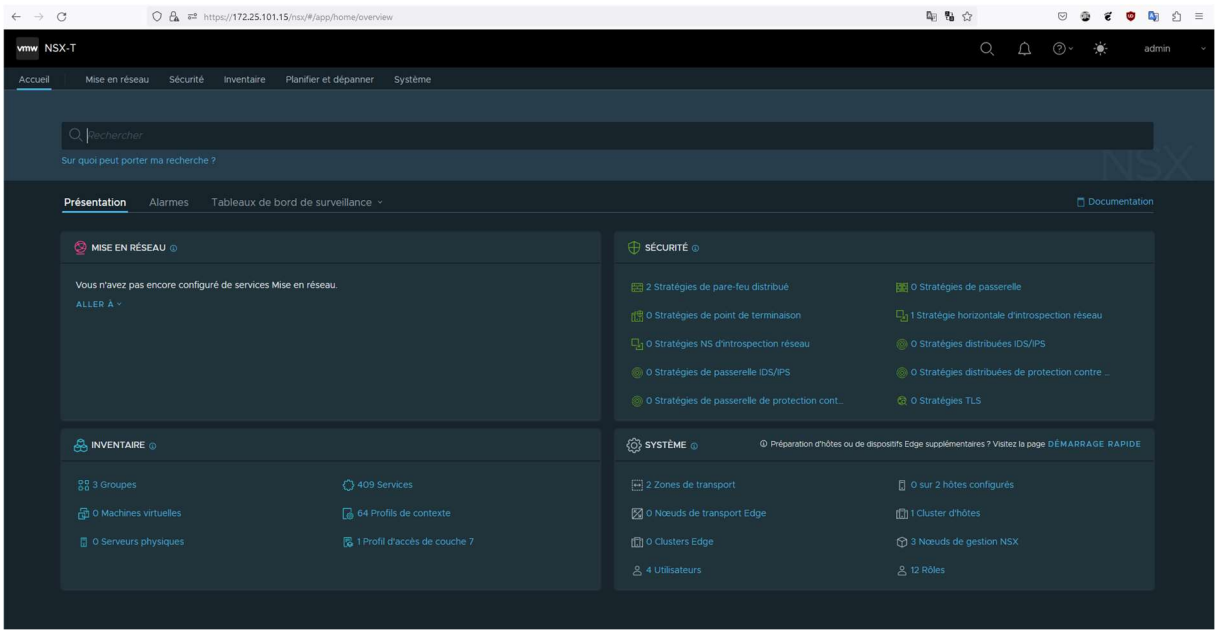
Cliquer sur « Définir l'adresse IP virtuelle »



L’ip virtuelle est configuré pour le cluster de manager

5.3 Connection

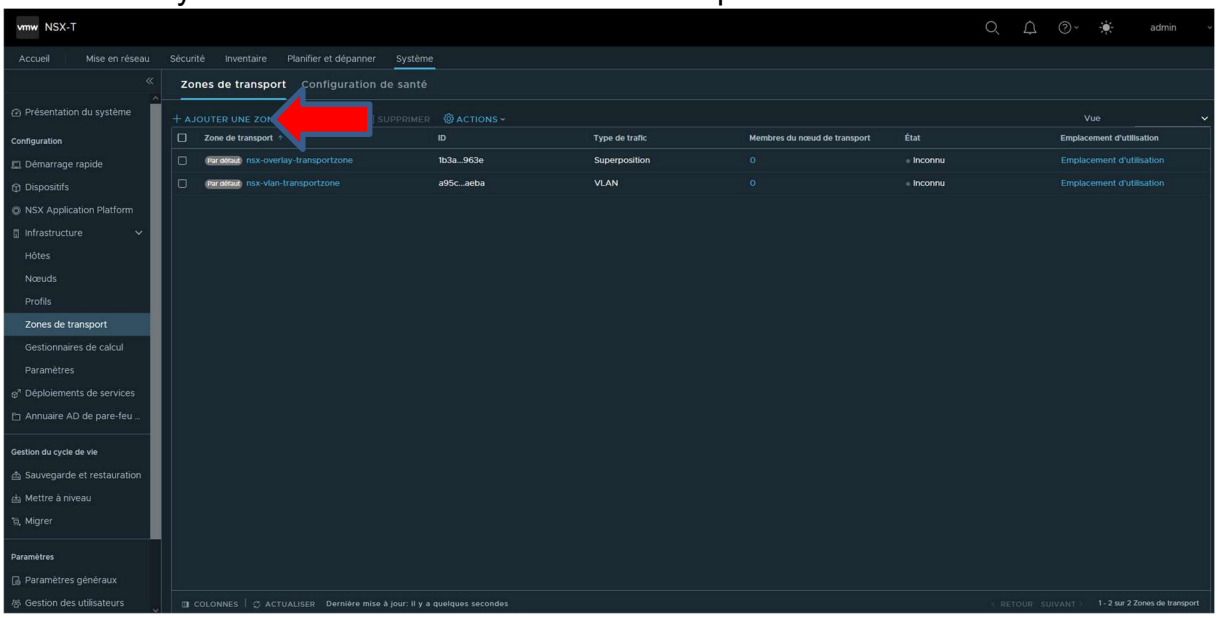
Je peux maintenant me connecter depuis l’adresse IP virtuelle du manager



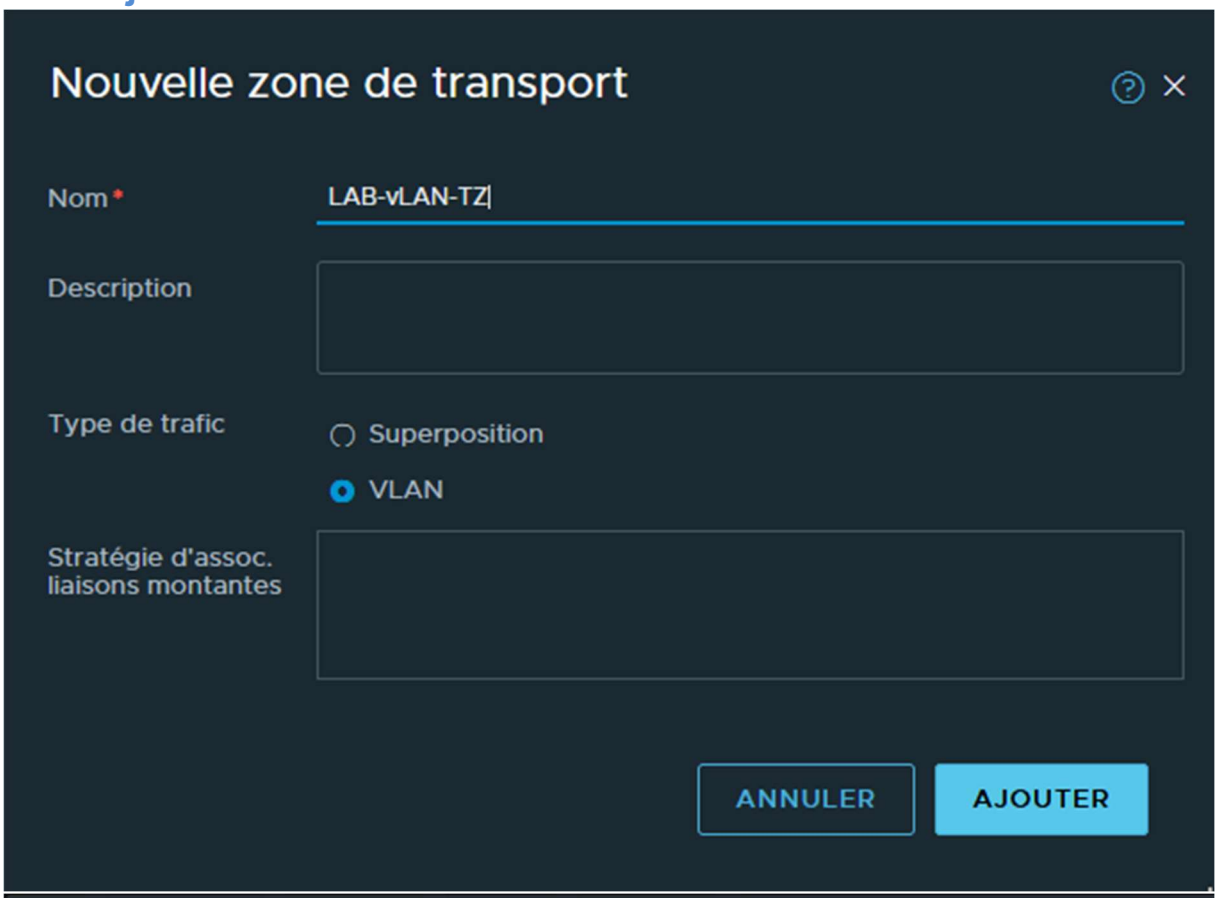
6 Configuration Transport Zones NSX

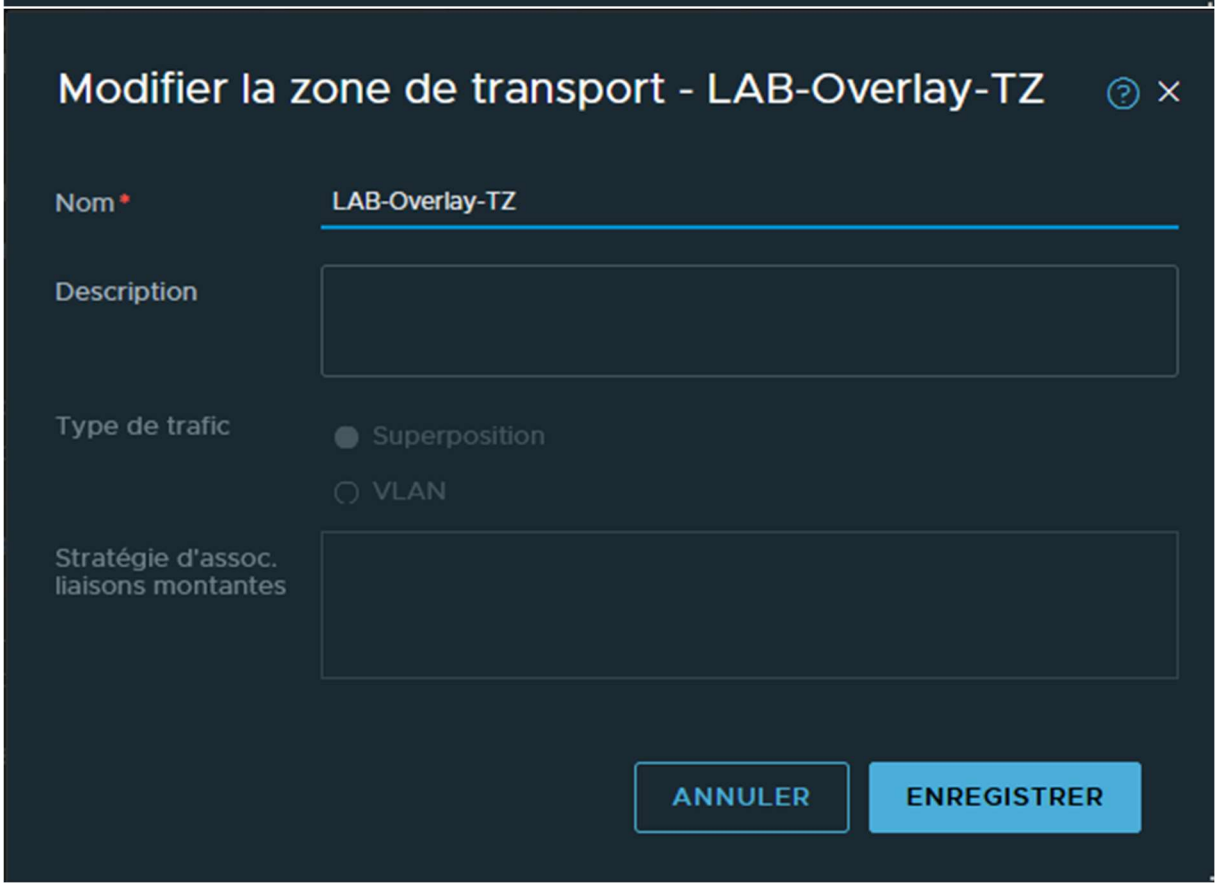
6.1 Transport Zones

Aller dans System / Infrastructure / Zones de transport



6.2 Ajouter une zone

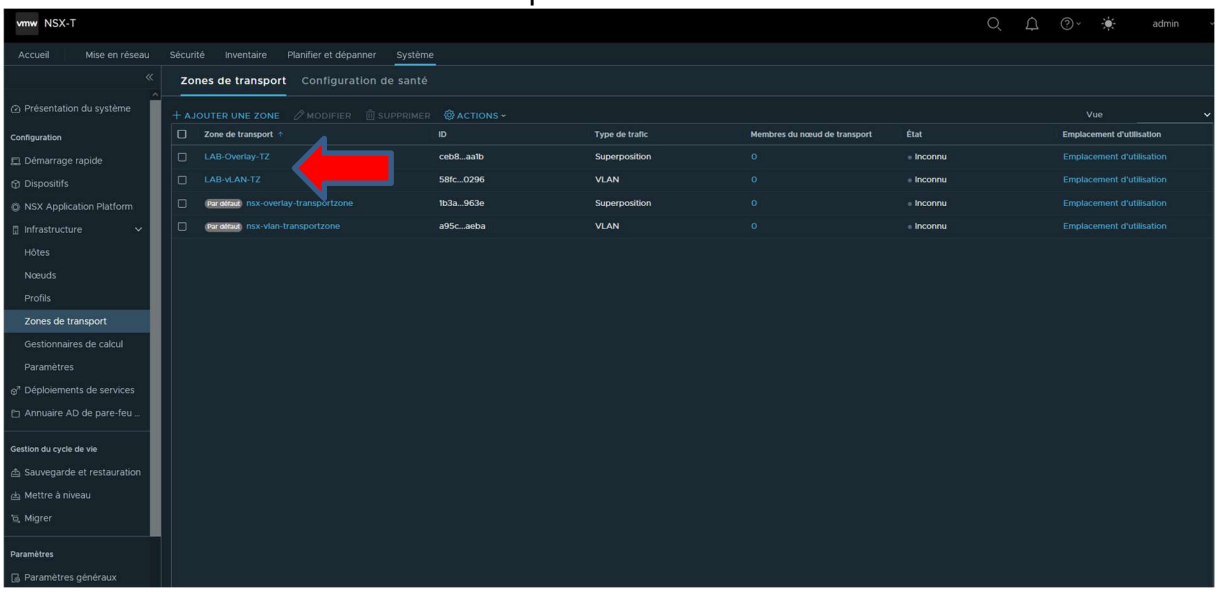




On nomme la transport zone pour le flux overlay puis on clique sur « Add ».

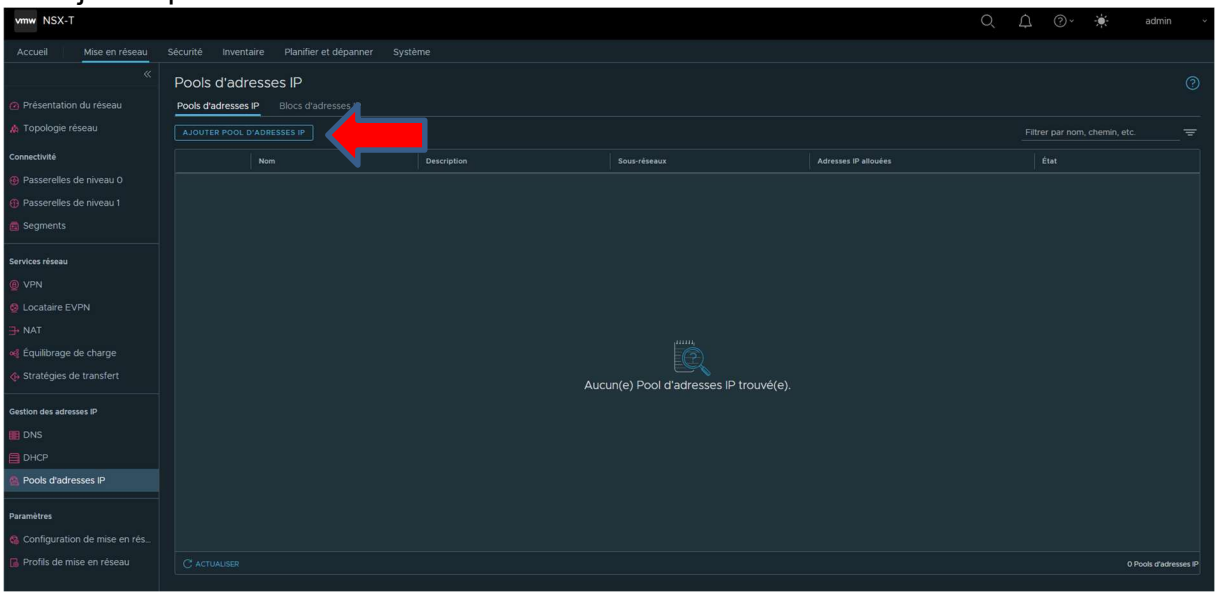
Idem pour le transport zone VLAN.

Vous avez maintenant les deux transport zone de crée

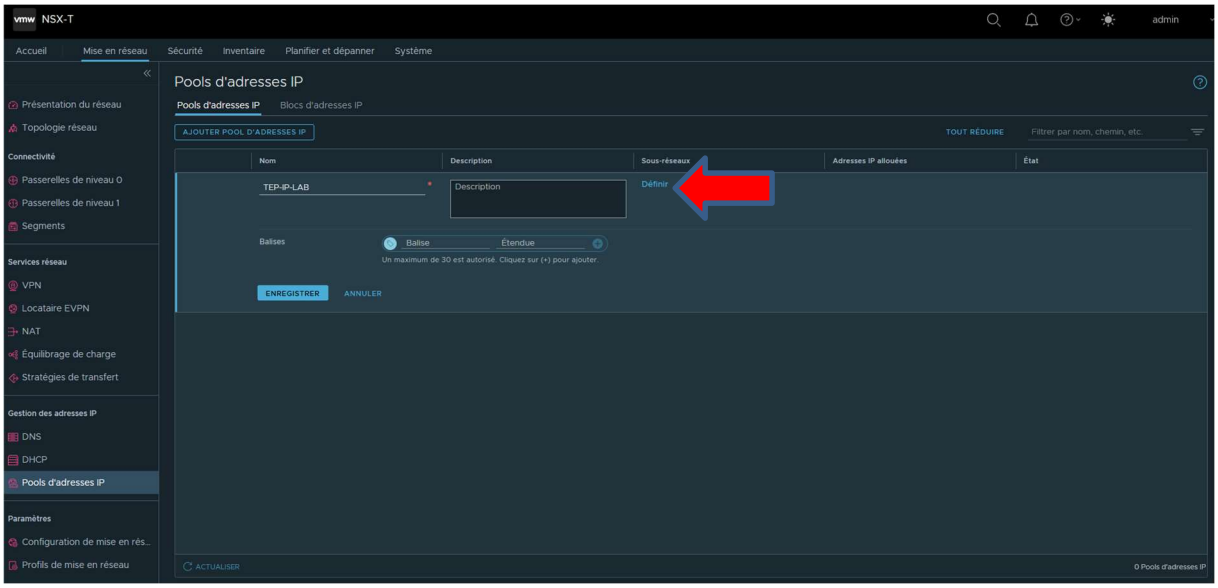


6.3 IP Pool

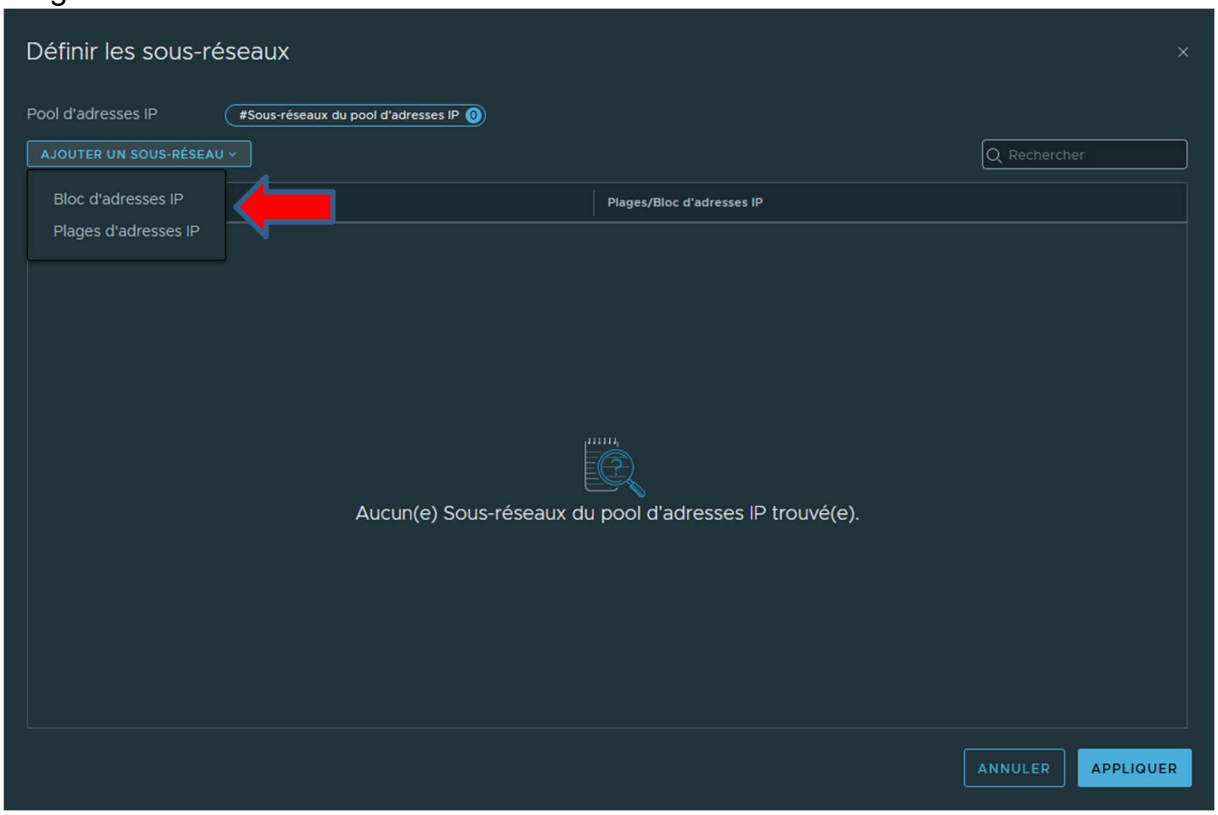
Aller dans Mise en réseau / Gestion des addresses IP / Pools d’adresses IP et cliquer sur Ajouter pool d’adresses IP



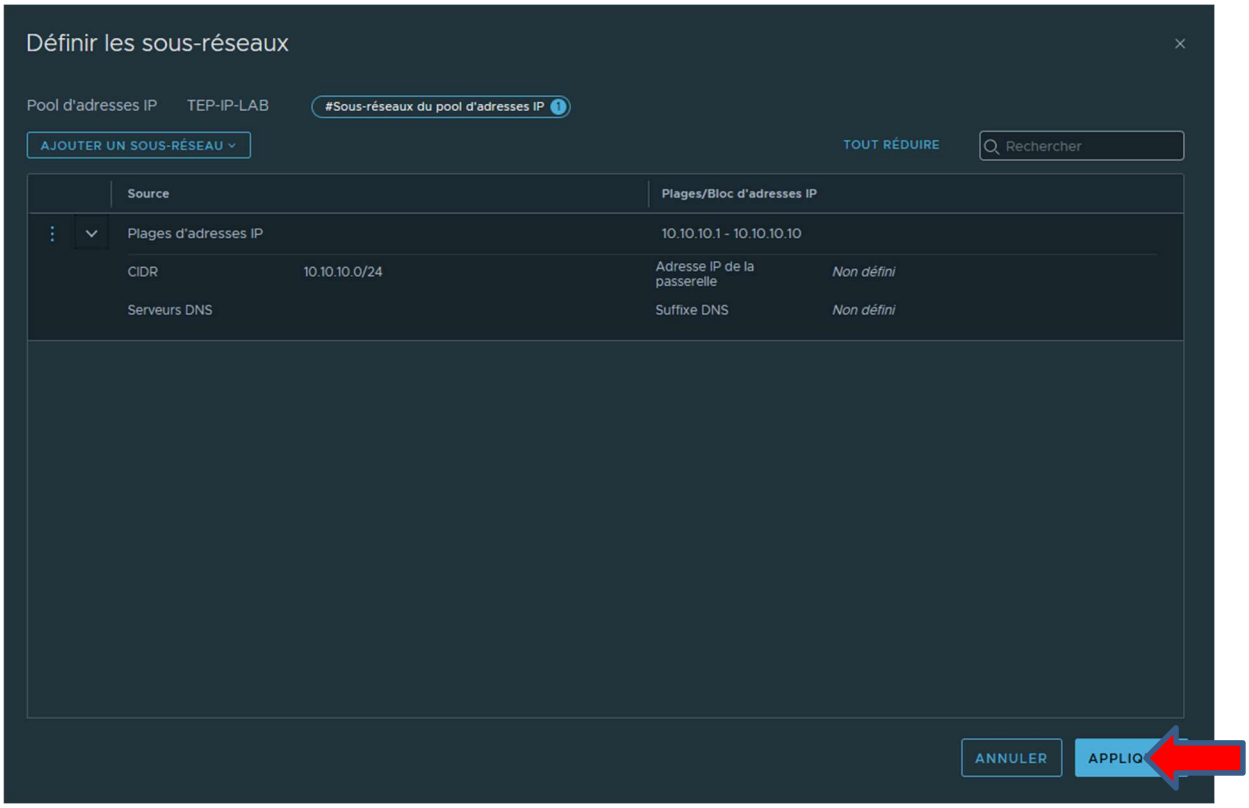
Cliquer sur Définir



En fonction du besoin et de l'environnement, on ajoutera un subnet complet ou un range d'IP.



Nous allons opter pour une plage d'adresse IP

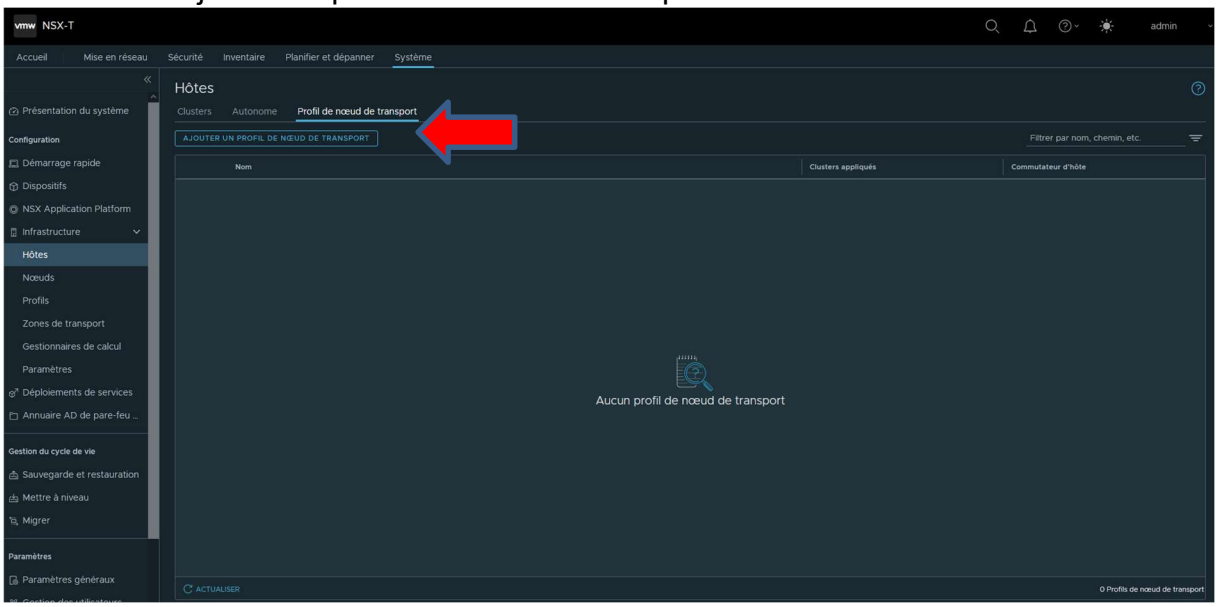


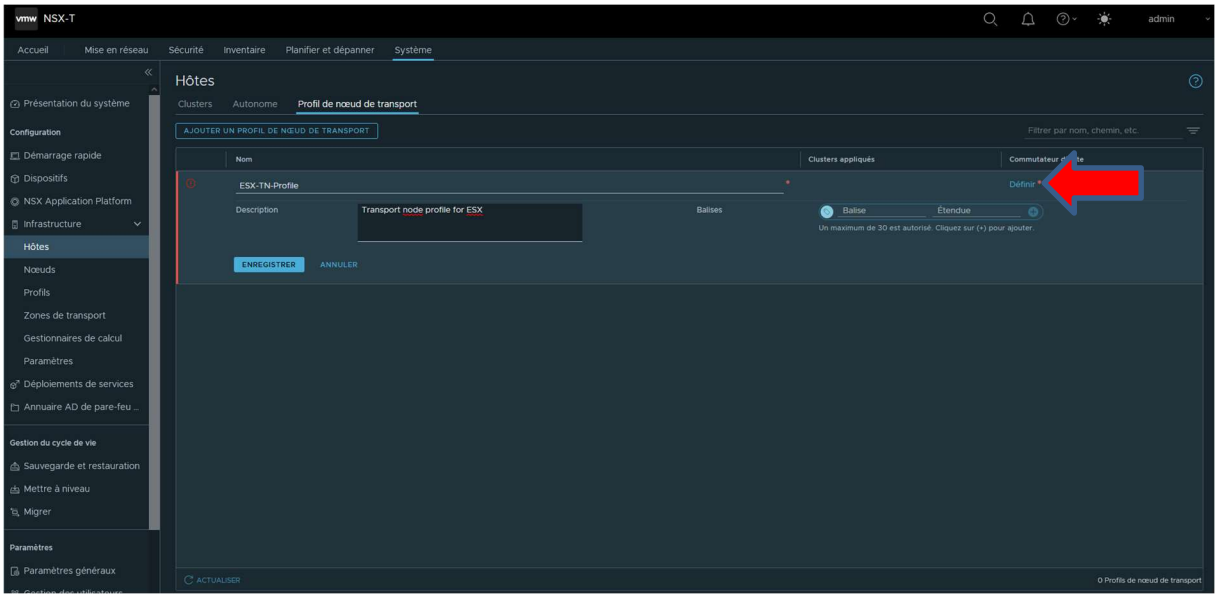
Dans le cadre de ma maquette, j'ai un VLAN de transport pour mes trames TEP sur mes UCS.

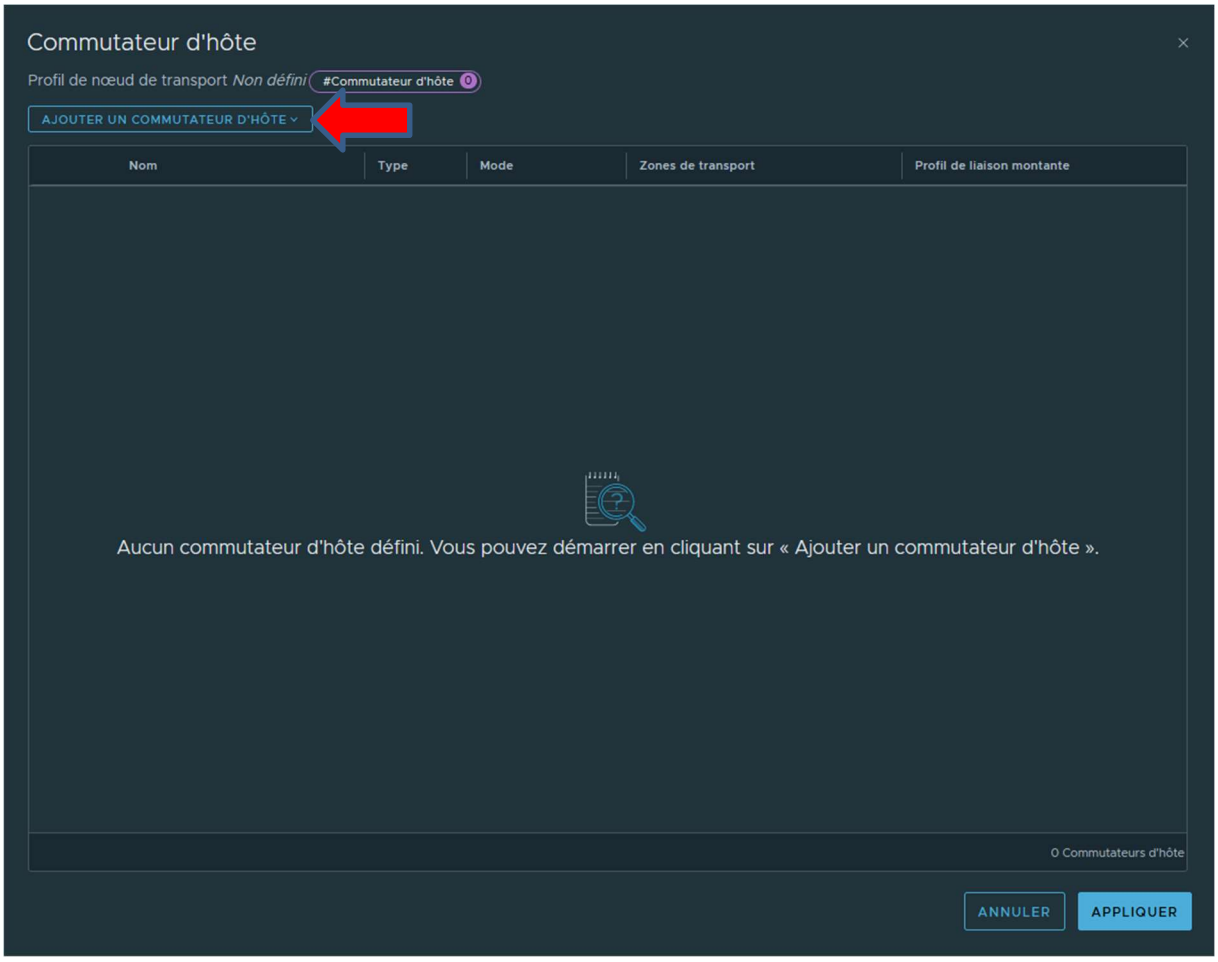
7 Host Transport Nodes

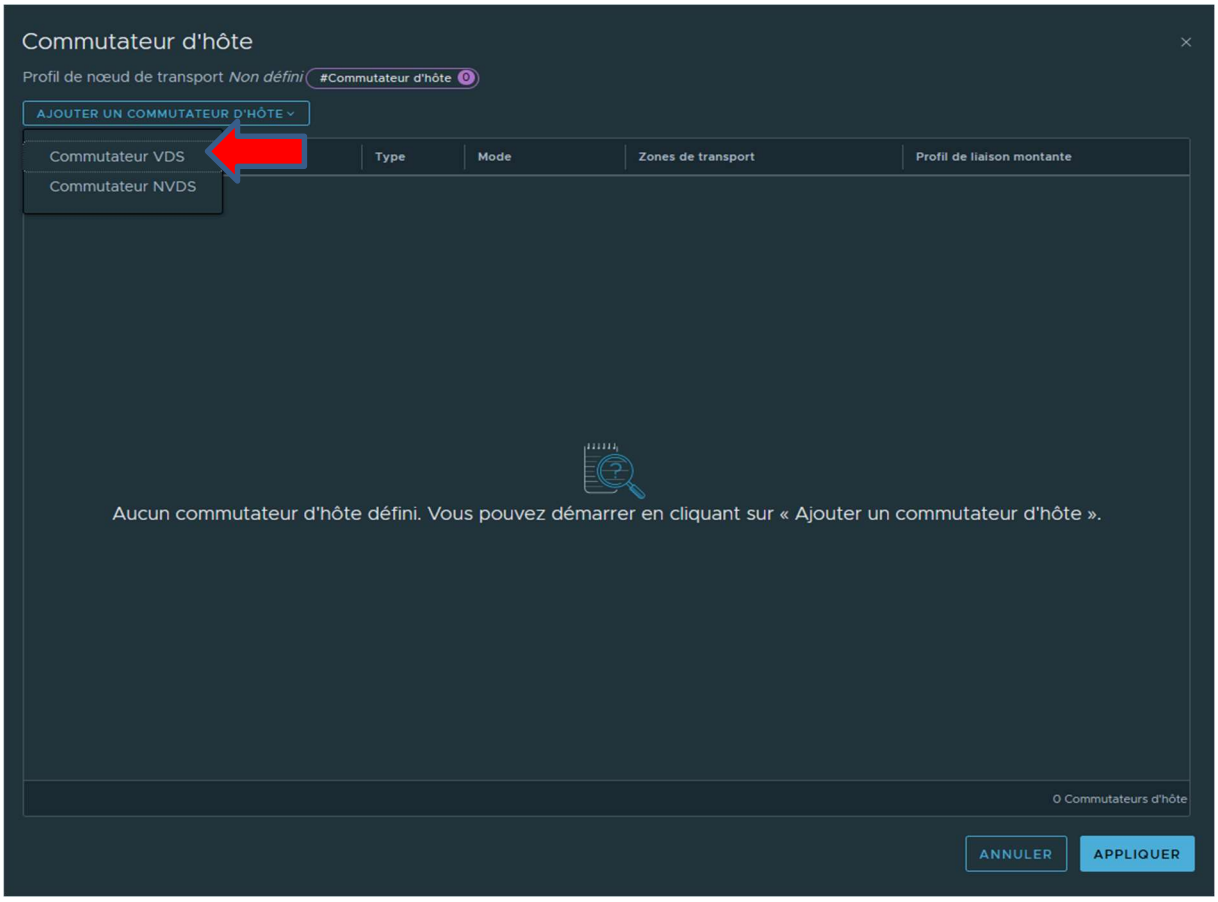
7.1 Ajout d'un profil de nœud de transport

Nous allons ajouter un profil de nœud de transport

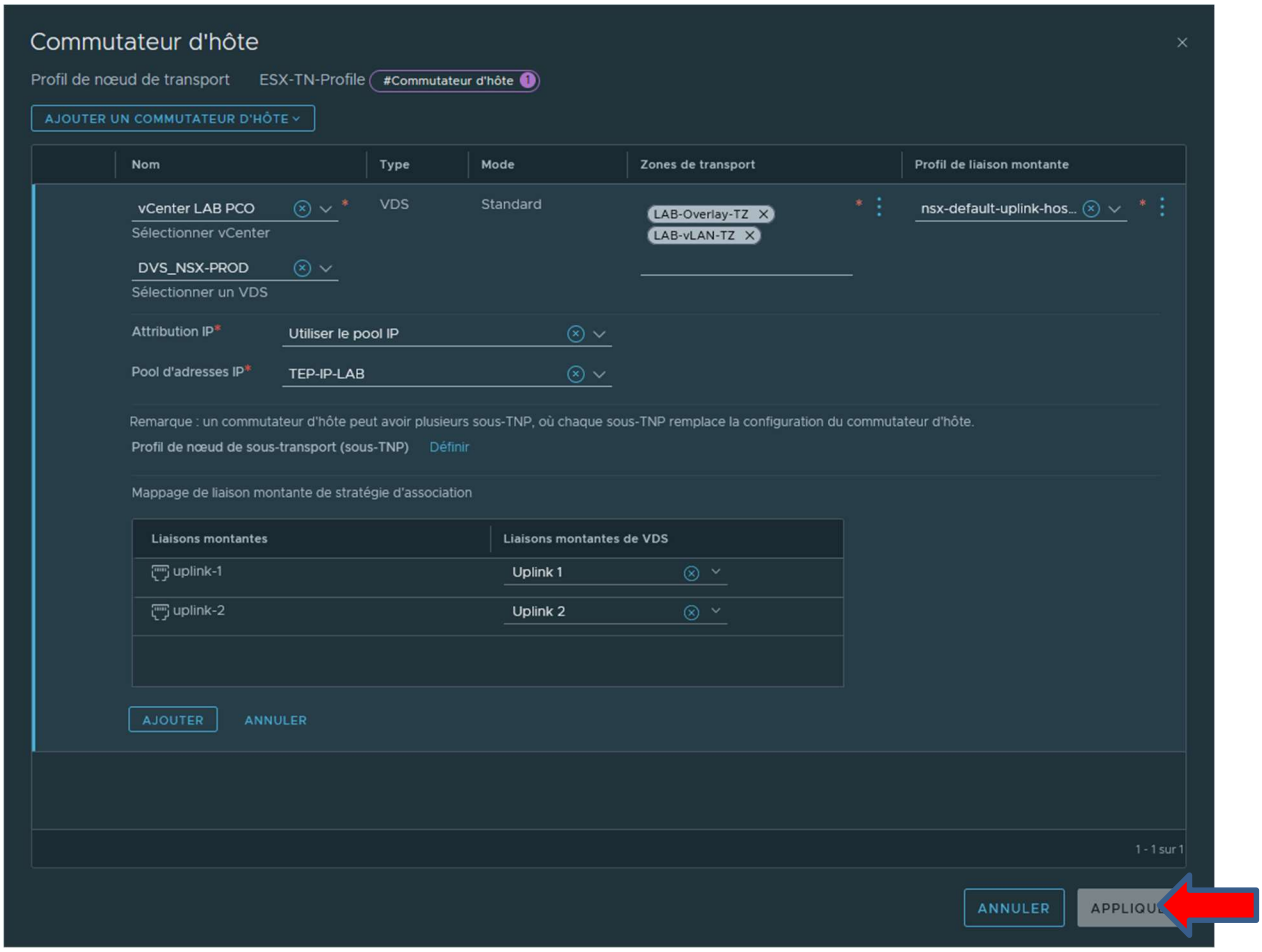



NSX-T
admin
Accueil
Mise en réseau
Sécurité
Inventaire
Planifier et dépanner
Système
Présentation du système
Configuration
Démarrage rapide
Dispositifs
NSX Application Platform
Infrastructure
Hôtes
Nœuds
Profils
Zones de transport
Gestionnaires de calcul
Paramètres
Déploiements de services
Annuaire AD de pare-feu ...
Gestion du cycle de vie
Sauvegarde et restauration
Mettre à niveau
Migrer
Paramètres
Paramètres généraux
Hôtes
Clusters
Autonome
Profil de nœud de transport
AJOUTER UN PROFIL DE NŒUD DE TRANSPORT
Filtrer par nom, chemin, etc.
Nom
Clusters appliqués
ESX-TN-Profile
Définir
Description
Transport node profile for ESX
Balises
Balise
Étendue
Un maximum de 30 est autorisé. Cliquez sur (+) pour ajouter.
ENREGISTRER
ANNULER
ACTUALISER
0 Profils de nœud de transport

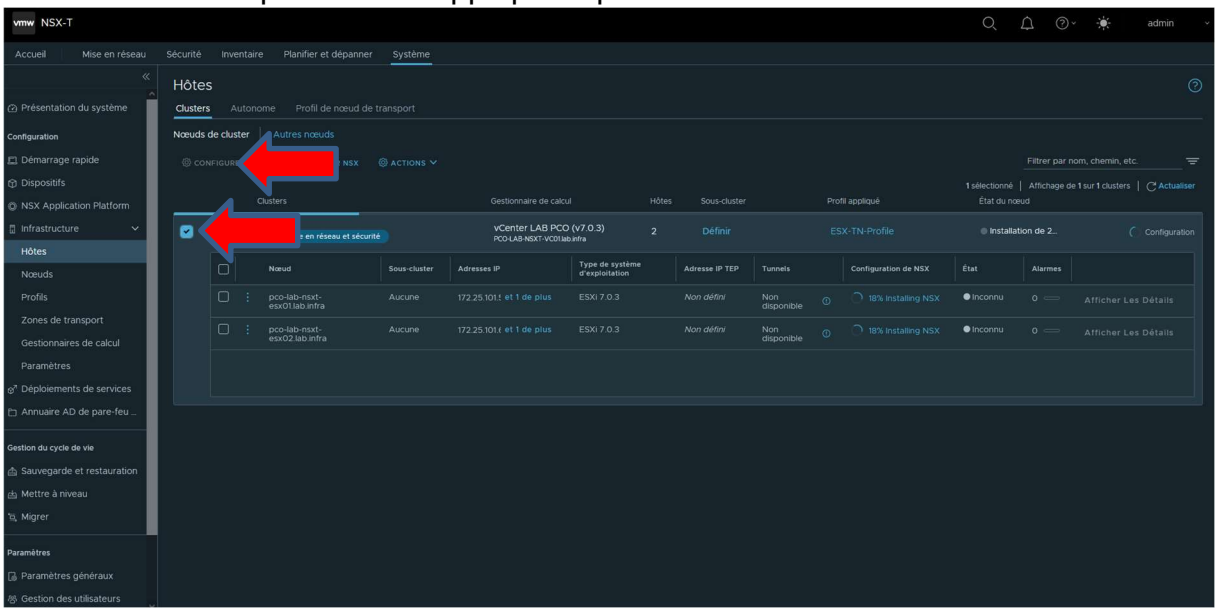

Commutateur d'hôte
Profil de nœud de transport Non défini
#Commutateur d'hôte 0
AJOUTER UN COMMUTATEUR D'HÔTE
Nom
Type
Mode
Zones de transport
Profil de liaison montante
Aucun commutateur d'hôte défini. Vous pouvez démarrer en cliquant sur « Ajouter un commutateur d'hôte ».
0 Commutateurs d'hôte
ANNULER
APPLIQUER

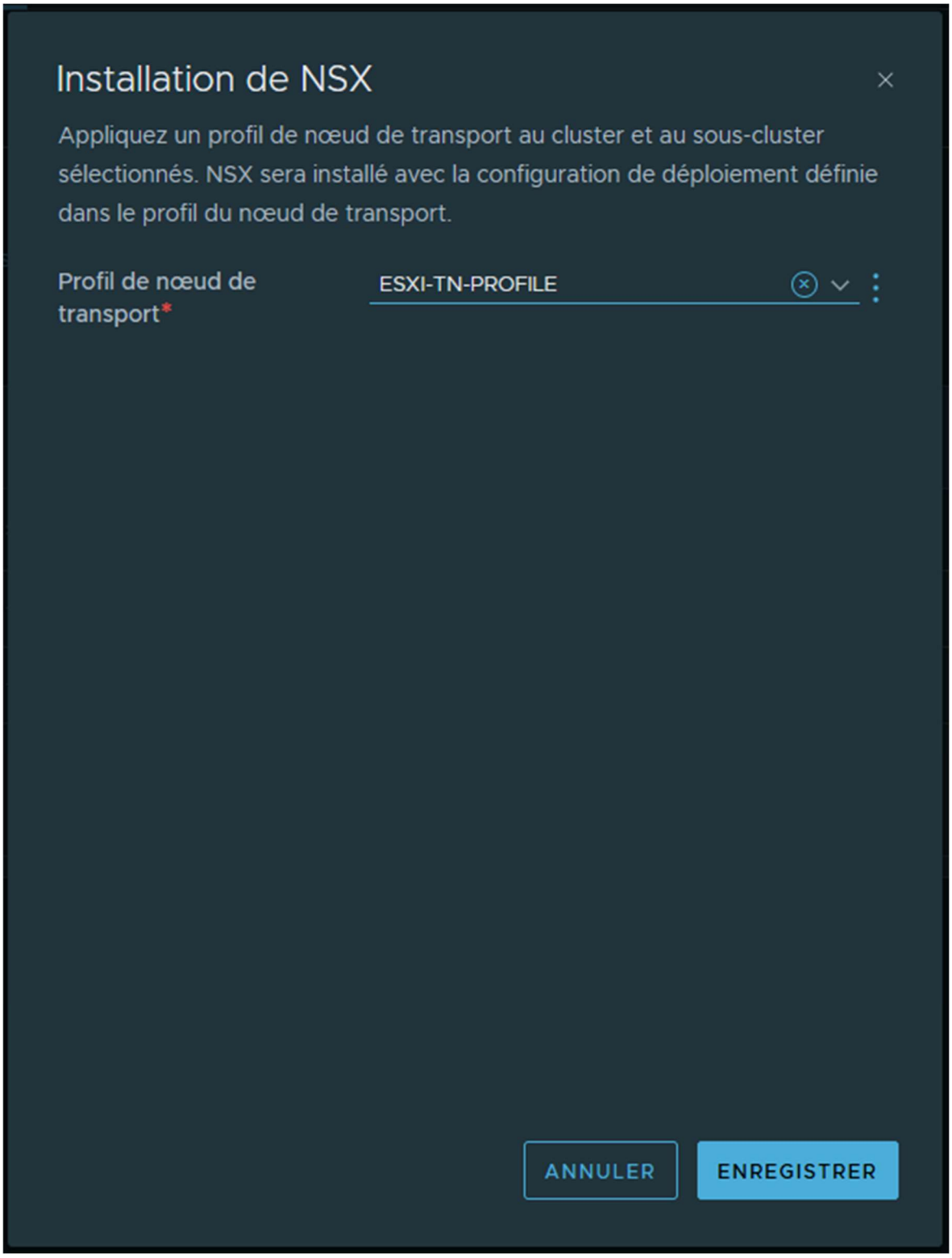


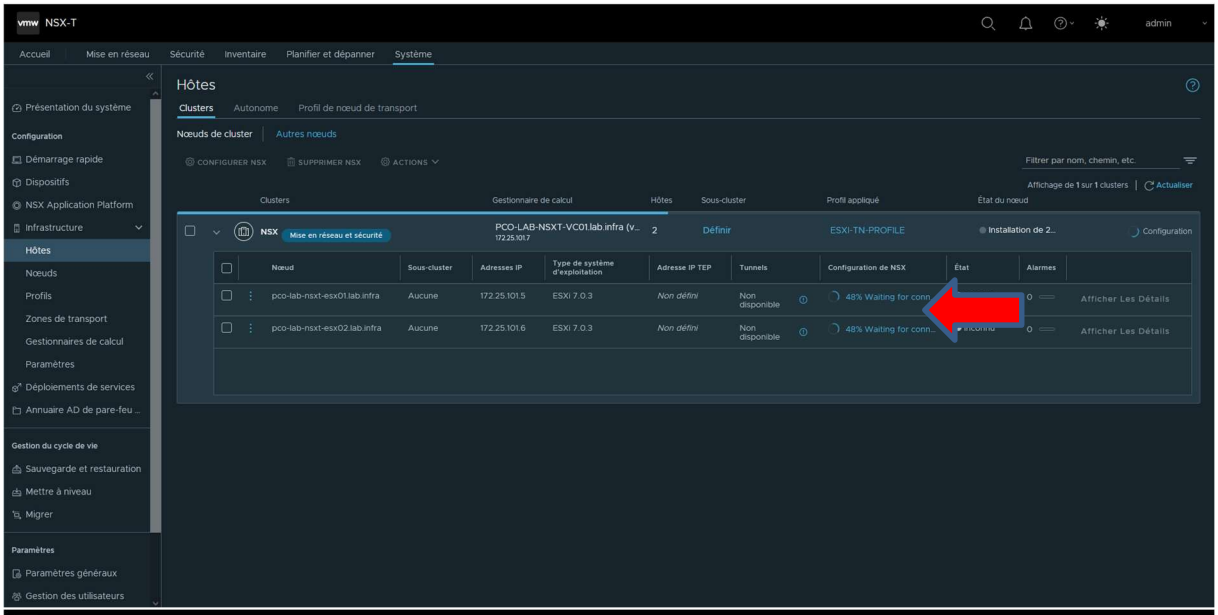
On ajoute les transports zones et les informations demander

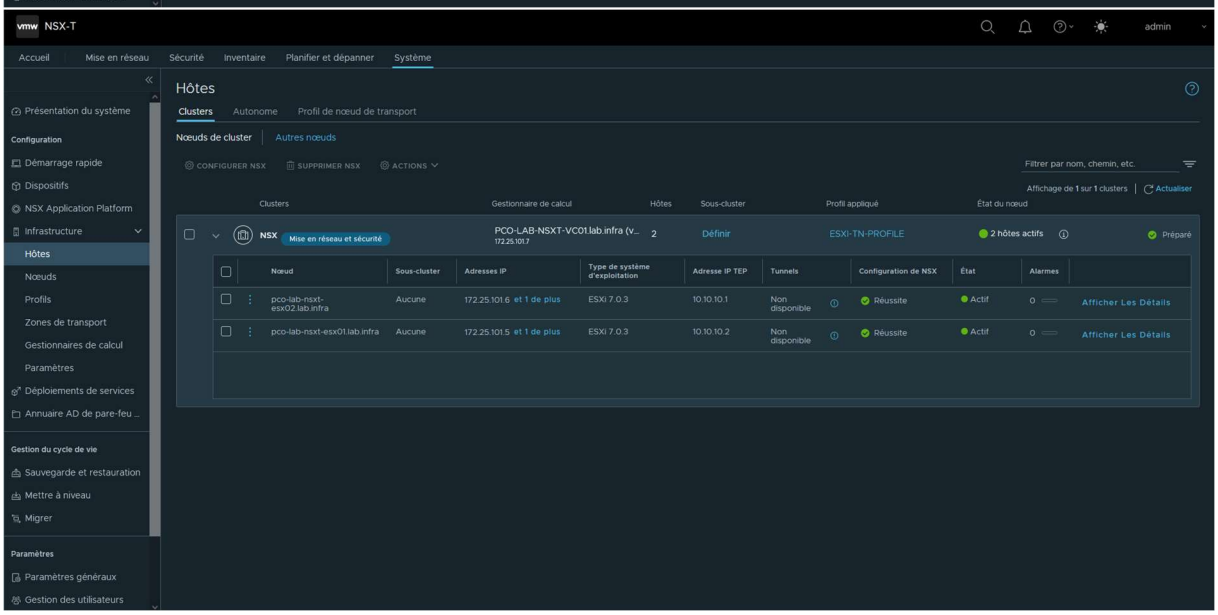


On sélectionne le profil et on l'applique le profil sur le cluster d'ESX



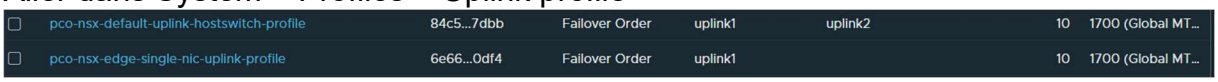

Installation de NSX
Appliquez un profil de nœud de transport au cluster et au sous-cluster sélectionnés. NSX sera installé avec la configuration de déploiement définie dans le profil du nœud de transport.
Profil de nœud de transport*
ESXI-TN-PROFILE
ANNULER
ENREGISTRER



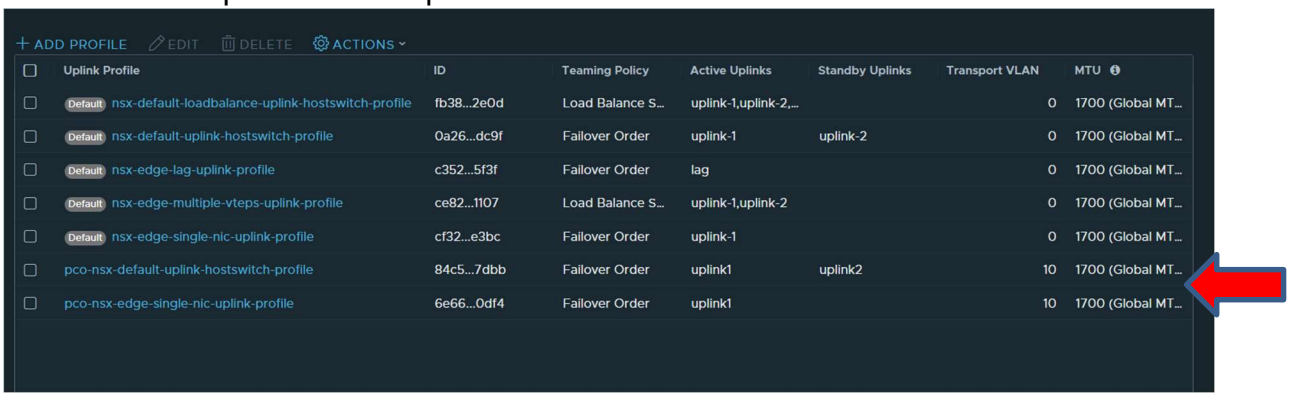


8 Création des Profiles

Aller dans System > Profiles > Uplink profile

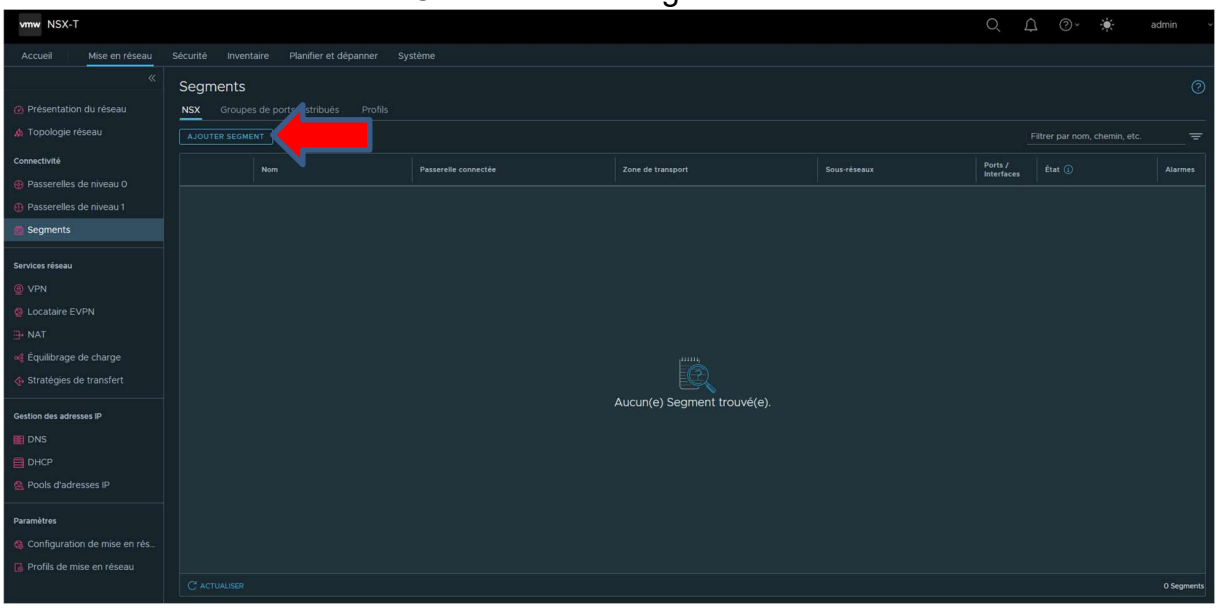


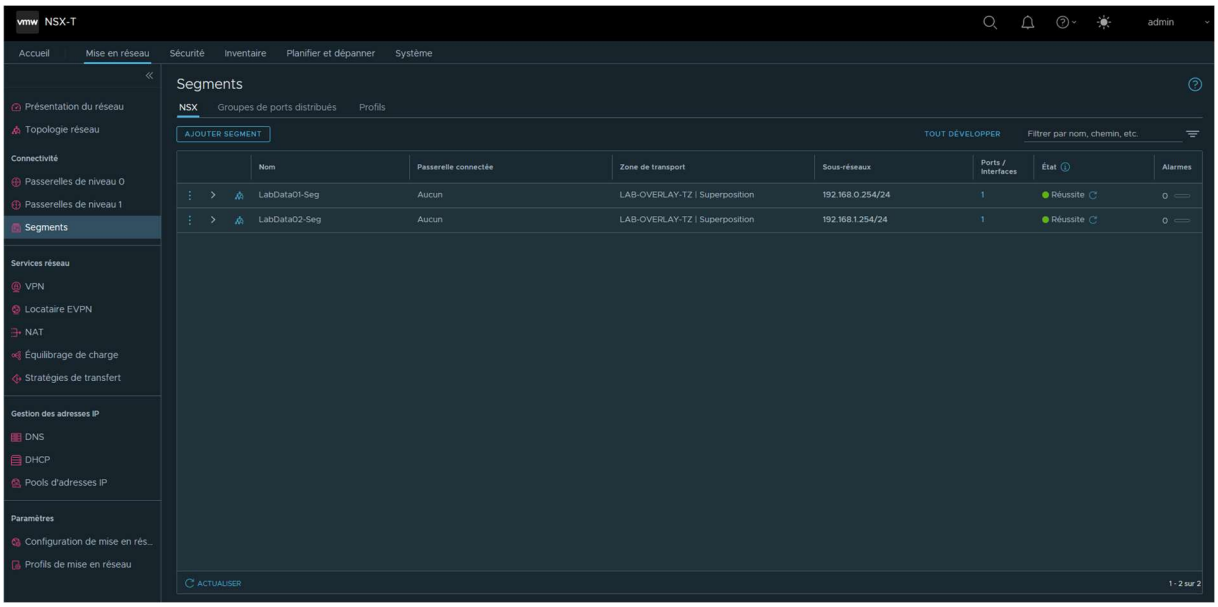
Vous crées les profils avec l'uplink souhaitez et le VLAN necessaire



9 Configuration Segment

Aller dans Mise en réseau > Connectivité > Segments.



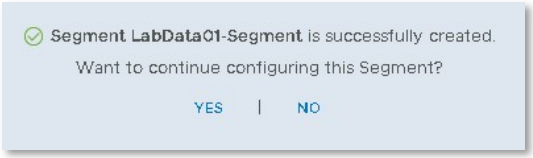


Cliquer sur « Ajouter Segment ».
Renseigner les champs suivants :

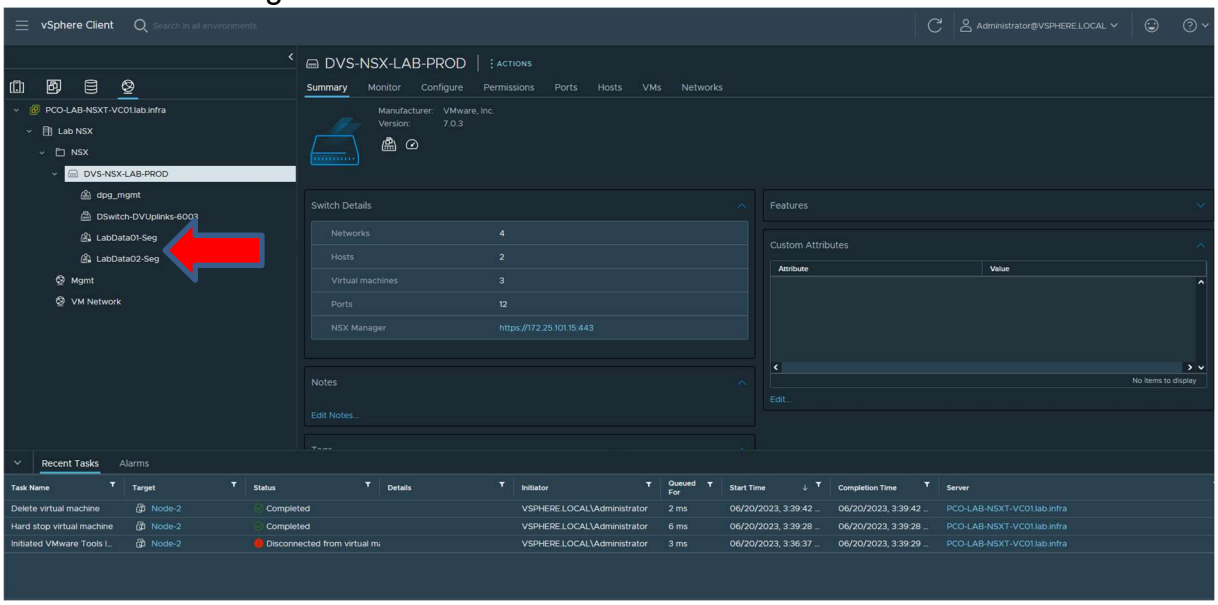
- Segment Name
- Transport zone
- Subnet

Pour le moment, on ne connecte pas de Gateway.

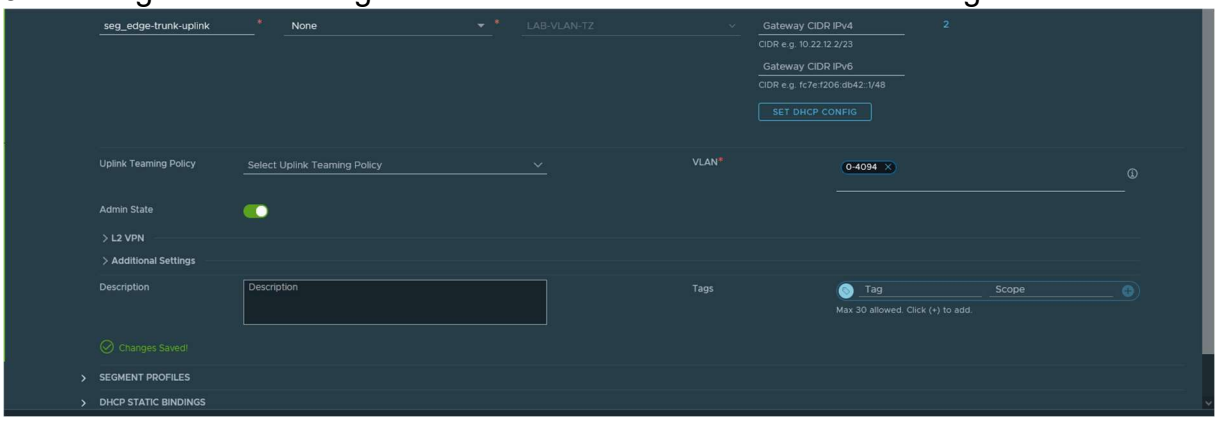
Cliquer sur Save un peu plus bas et répondre « non ».

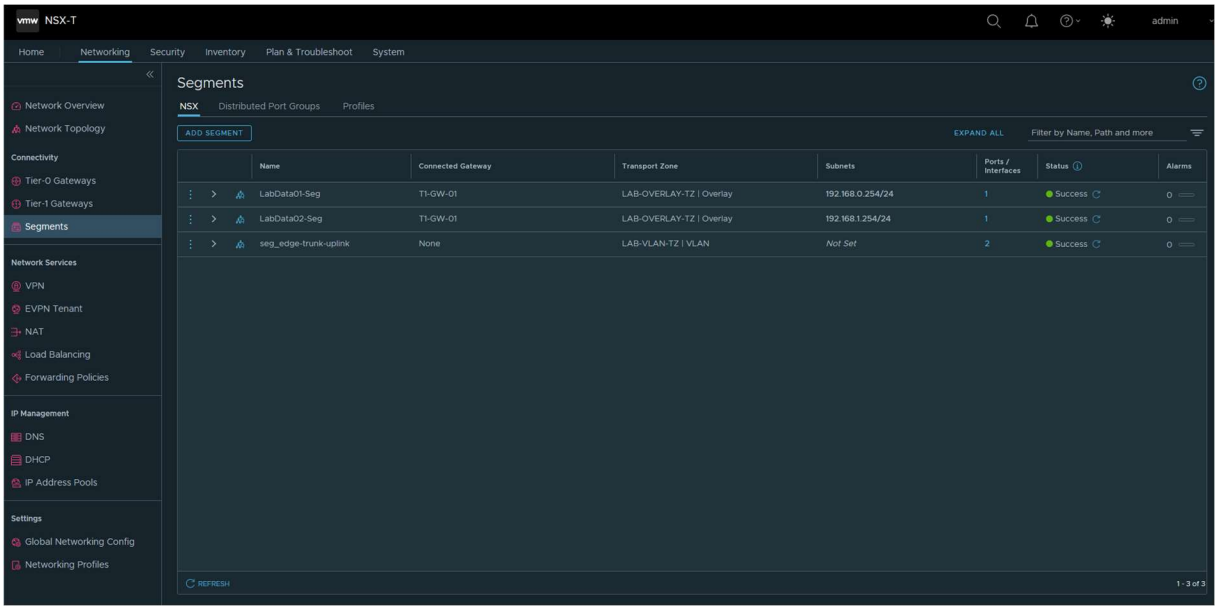


On retrouve les segments dans la vue Network du vCenter

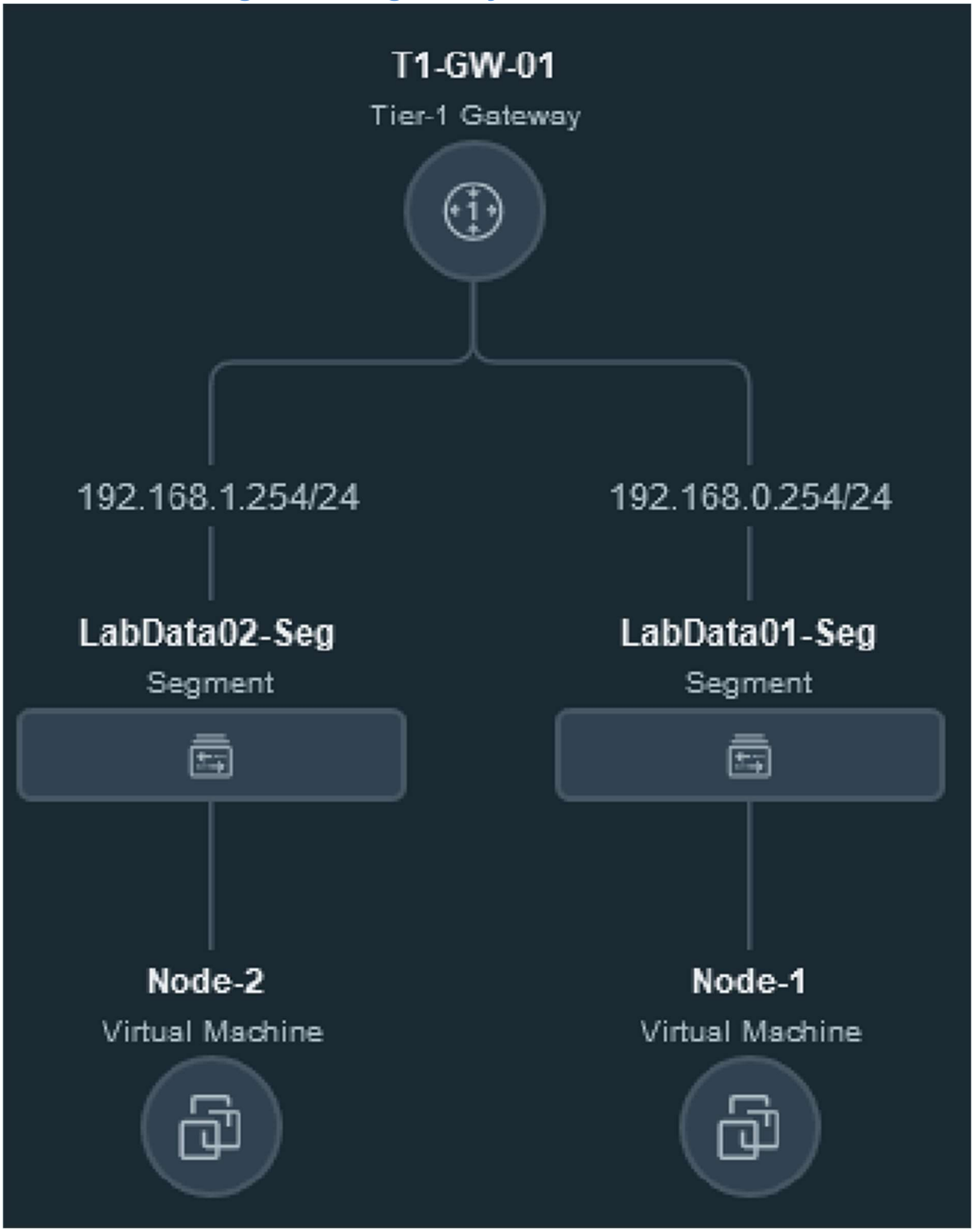


Je crée également un segment VLAN trunk entre les deux nœud edges




NSX-T
admin
Home
Networking
Security
Inventory
Plan & Troubleshoot
System
Network Overview
Network Topology
Connectivity
Tier-0 Gateways
Tier-1 Gateways
Segments
Network Services
VPN
EVPN Tenant
NAT
Load Balancing
Forwarding Policies
IP Management
DNS
DHCP
IP Address Pools
Settings
Global Networking Config
Networking Profiles
Segments
NSX
Distributed Port Groups
Profiles
ADD SEGMENT
EXPAND ALL
Filter by Name, Path and more
Name
Connected Gateway
Transport Zone
Subnets
Ports / Interfaces
Status
Alarms
LabData01-Seg
T1-GW-01
LAB-OVERLAY-TZ | Overlay
192.168.0.254/24
1
Success
0
LabData02-Seg
T1-GW-01
LAB-OVERLAY-TZ | Overlay
192.168.1.254/24
1
Success
0
seg_edge-trunk-uplink
None
LAB-VLAN-TZ | VLAN
Not Set
2
Success
0
REFRESH
1 - 3 of 3

9.1 Schéma segments et gateway



10 Configuration des VM

On configure avec une IP de chaque range des segments configurés auparavant

	Nom	Passerelle connectée	Zone de transport	Sous-réseaux	Ports / Interfaces	État	Alarmes
⋮ ›	LabData01-Seg	Aucun	LAB-OVERLAY-TZ | Superposition	192.168.0.254/24	1	Réussite	0
⋮ ›	LabData02-Seg	Aucun	LAB-OVERLAY-TZ | Superposition	192.168.1.254/24	1	Réussite	0

10.1 Vm1

```
  GNU nano 7.2                                    interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens192
iface ens192 inet dhcp

# The secondary network interface
allow-hotplug ens224
iface ens224 inet static
  address 192.168.0.1/24
  gateway 192.168.0.254
  dns-nameservers 10.16.4.1 10.16.4.2
  dns-domain lab.infra
```

10.2 Vm2

```
  GNU nano 7.2                            /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens192
iface ens192 inet dhcp

# The seconday network interface
allow-hotplug ens224
iface ens224 inet static
  address 192.168.1.1/24
  gateway 192.168.1.254
  dns-nameservers 10.16.4.1 10.16.4.2
  dns-domains lab.infra
```

Désactiver les interfaces primary des deux VMs avec la commande :
sudo ifdown ens192

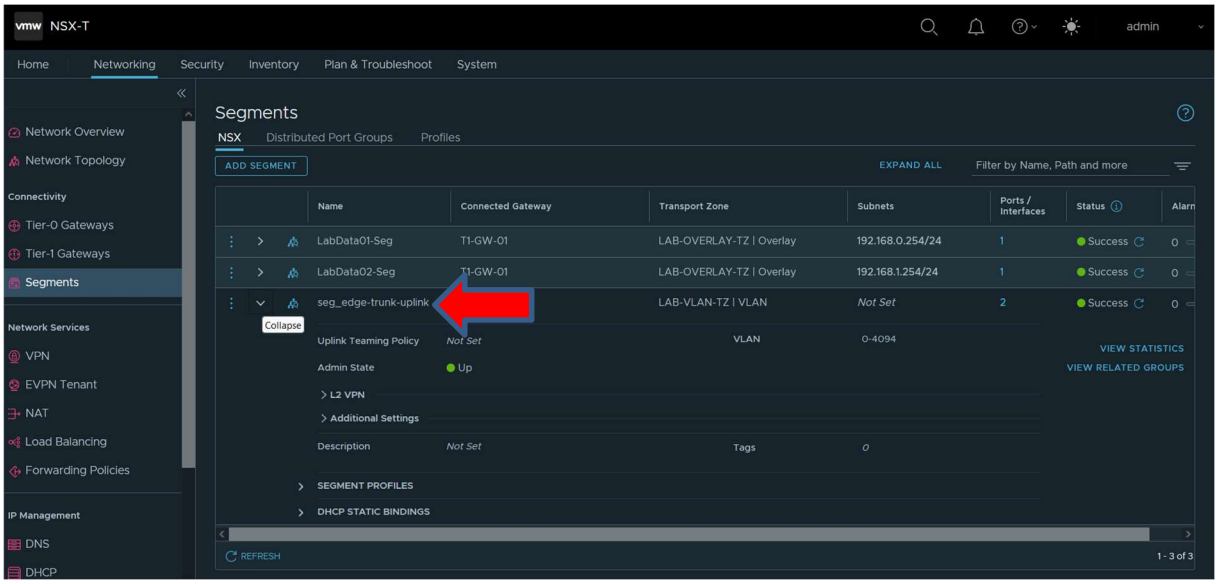
```
2: ens192: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether 00:50:56:a2:2e:aa brd ff:ff:ff:ff:ff:ff
```

Il faut reboot les VM’s

11 Déploiement Edge node

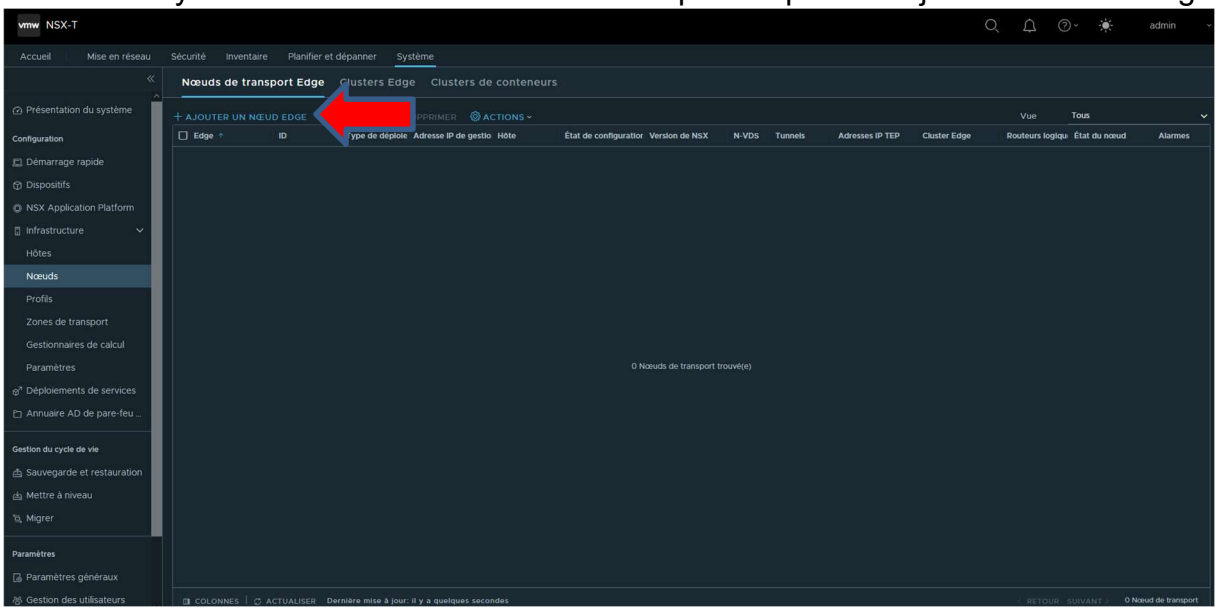
11.1 Création du segment pour les deux nœud edges

Je crée un segment edge trunk sur NSX pour les deux nœud edges

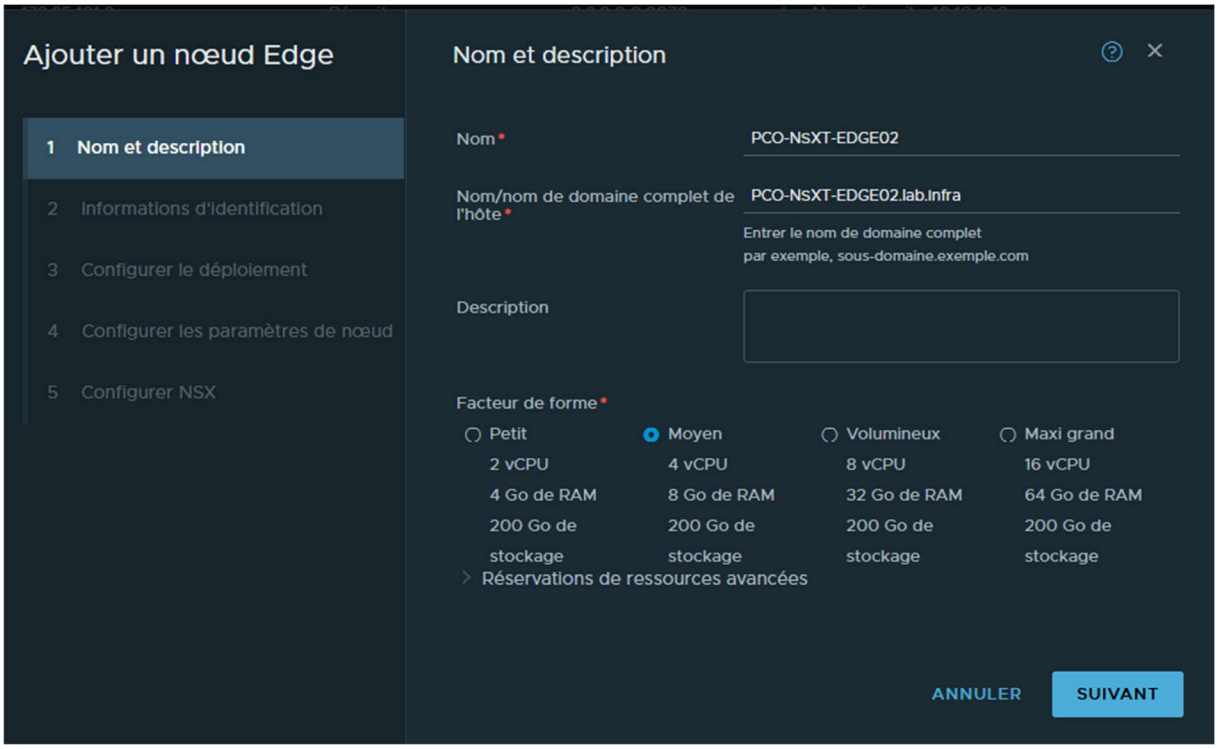


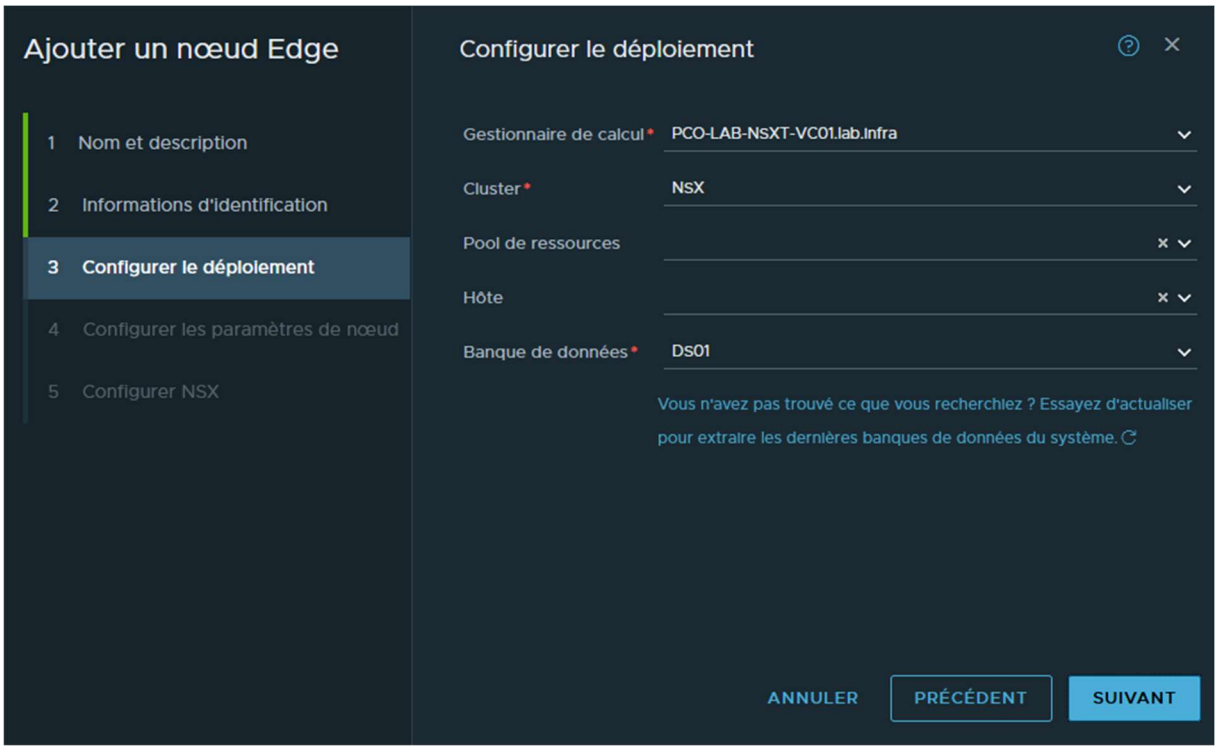
11.2 Création des nœuds edges

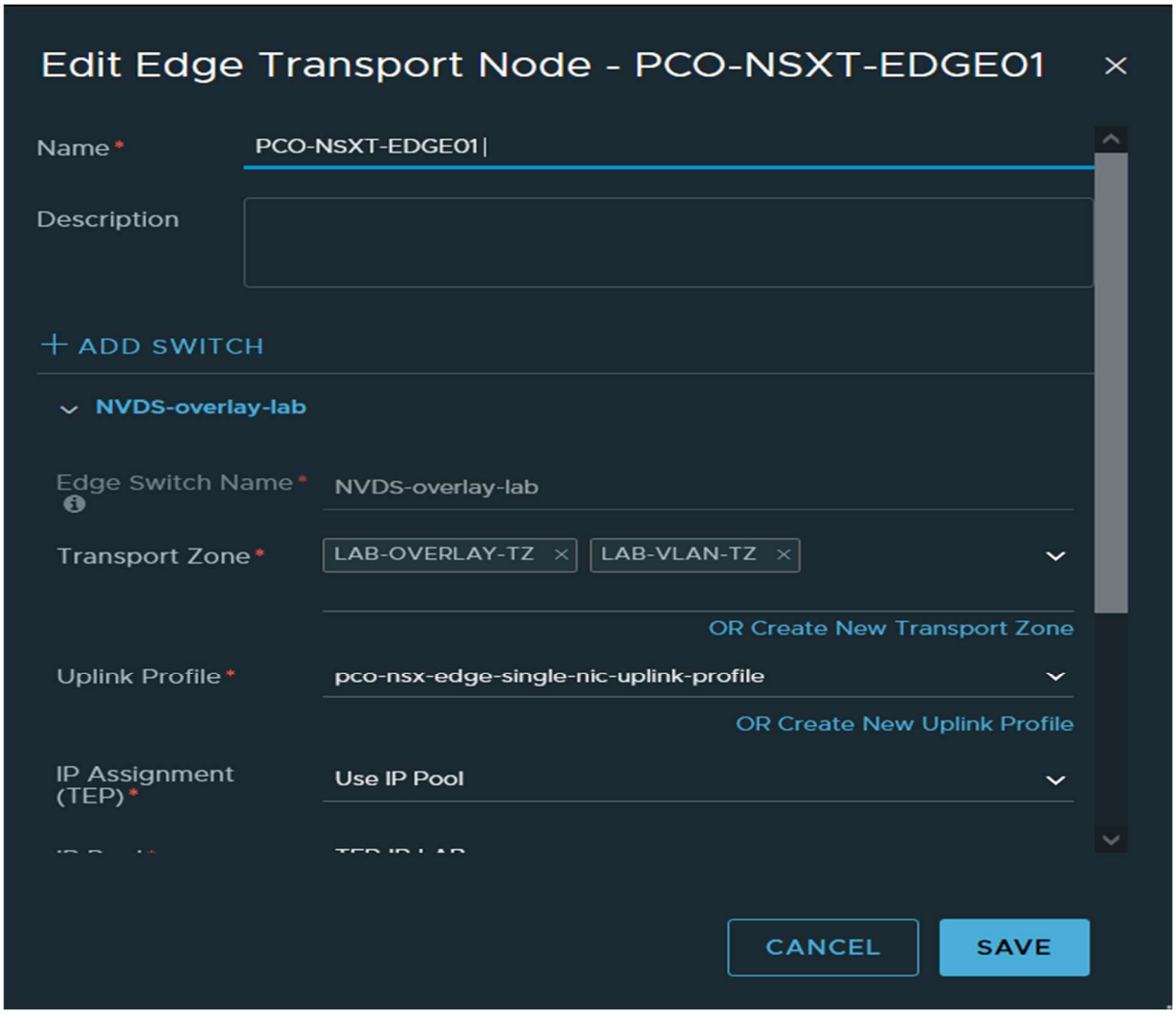
Aller dans Système > Infrastructure > Noeuds > puis cliquer sur Ajouter un nœud edge

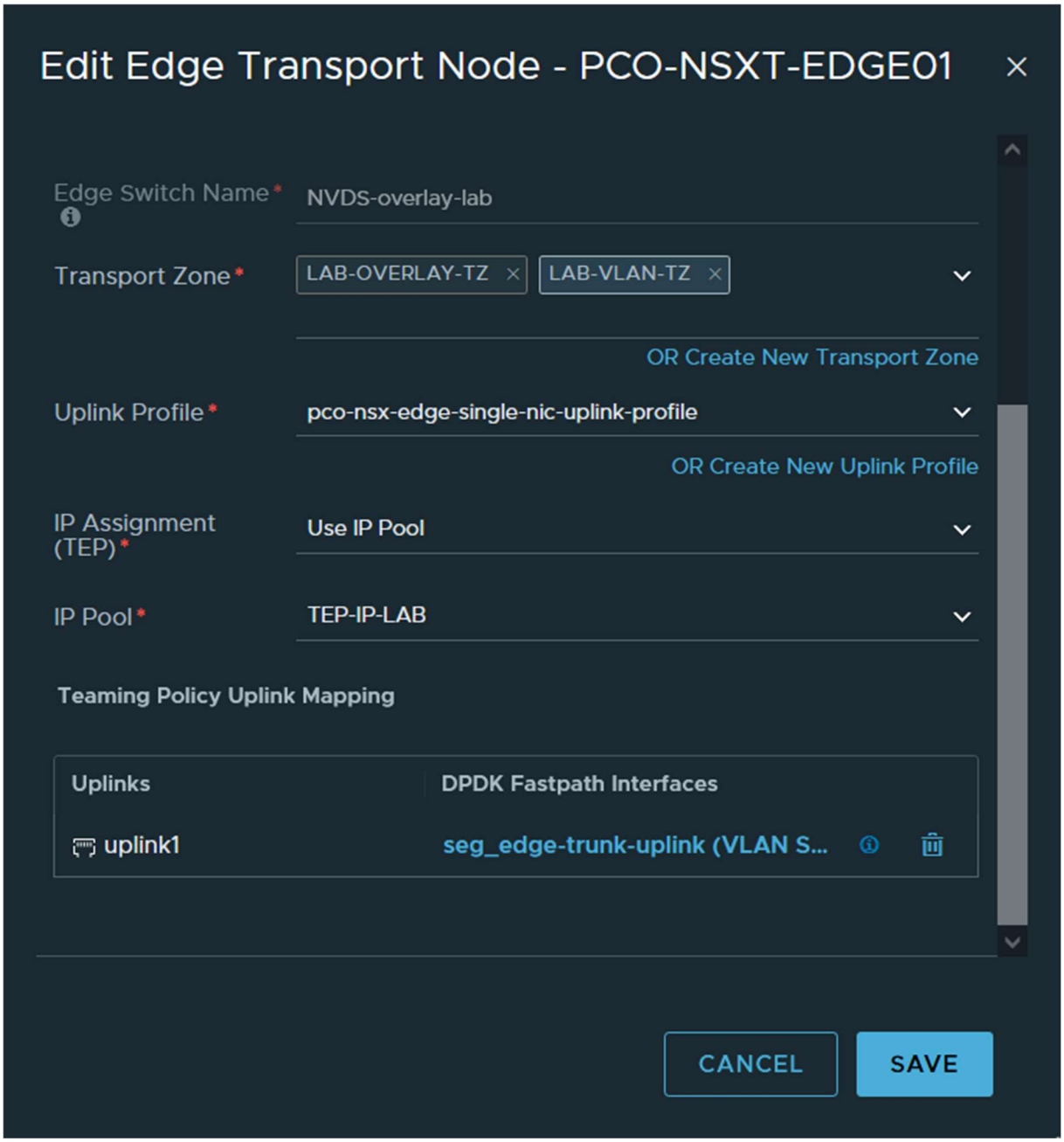


Configuration du Edge


Ajouter un nœud Edge
1 Nom et description
2 Informations d'identification
3 Configurer le déploiement
4 Configurer les paramètres de nœud
5 Configurer NSX
Nom et description
Nom *
PCO-NSXT-EDGE02
Nom/nom de domaine complet de l'hôte *
PCO-NSXT-EDGE02.lab.infra
Entrer le nom de domaine complet
par exemple, sous-domaine.exemple.com
Description
Facteur de forme *
Petit
2 vCPU
4 Go de RAM
200 Go de stockage
Moyen
4 vCPU
8 Go de RAM
200 Go de stockage
Volumineux
8 vCPU
32 Go de RAM
200 Go de stockage
Maxi grand
16 vCPU
64 Go de RAM
200 Go de stockage
Réservations de ressources avancées
ANNULER
SUIVANT


Ajouter un nœud Edge
1 Nom et description
2 Informations d'identification
3 Configurer le déploiement
4 Configurer les paramètres de nœud
5 Configurer NSX
Configurer le déploiement
Gestionnaire de calcul *
PCO-LAB-NSXT-VC01.lab.infra
Cluster *
NSX
Pool de ressources
Hôte
Banque de données *
DS01
Vous n'avez pas trouvé ce que vous recherchiez ? Essayez d'actualiser pour extraire les dernières banques de données du système.
ANNULER
PRÉCÉDENT
SUIVANT

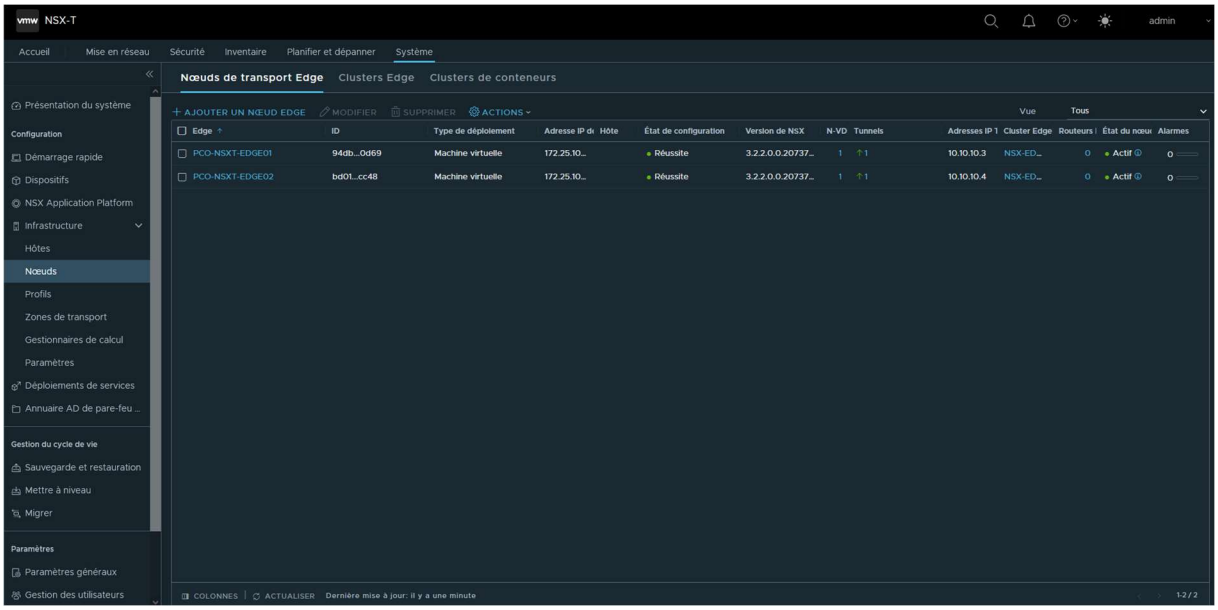

Edit Edge Transport Node - PCO-NSXT-EDGE01
Name *
PCO-NSXT-EDGE01
Description
+ ADD SWITCH
NVDS-overlay-lab
Edge Switch Name *
NVDS-overlay-lab
Transport Zone *
LAB-OVERLAY-TZ
LAB-VLAN-TZ
OR Create New Transport Zone
Uplink Profile *
pco-nsx-edge-single-nic-uplink-profile
OR Create New Uplink Profile
IP Assignment (TEP) *
Use IP Pool
CANCEL
SAVE



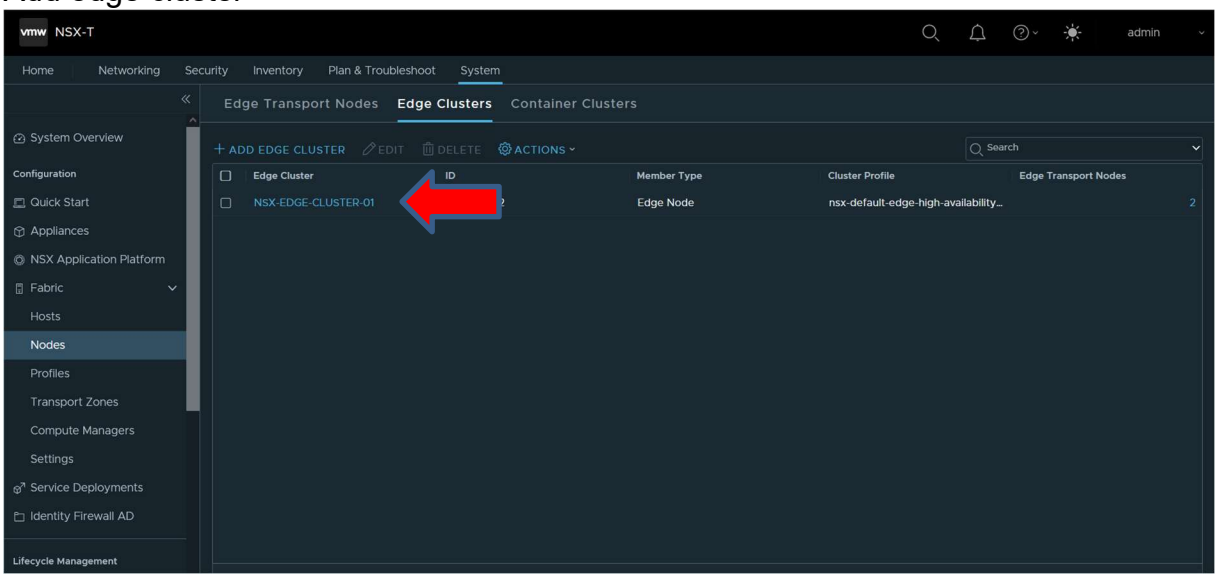
Remarque :
La procédure détaille la création d'un Edge Node, elle est à répéter pour le 2ème Edge Node afin de pouvoir créer un cluster.

11.3 Création du cluster Edge

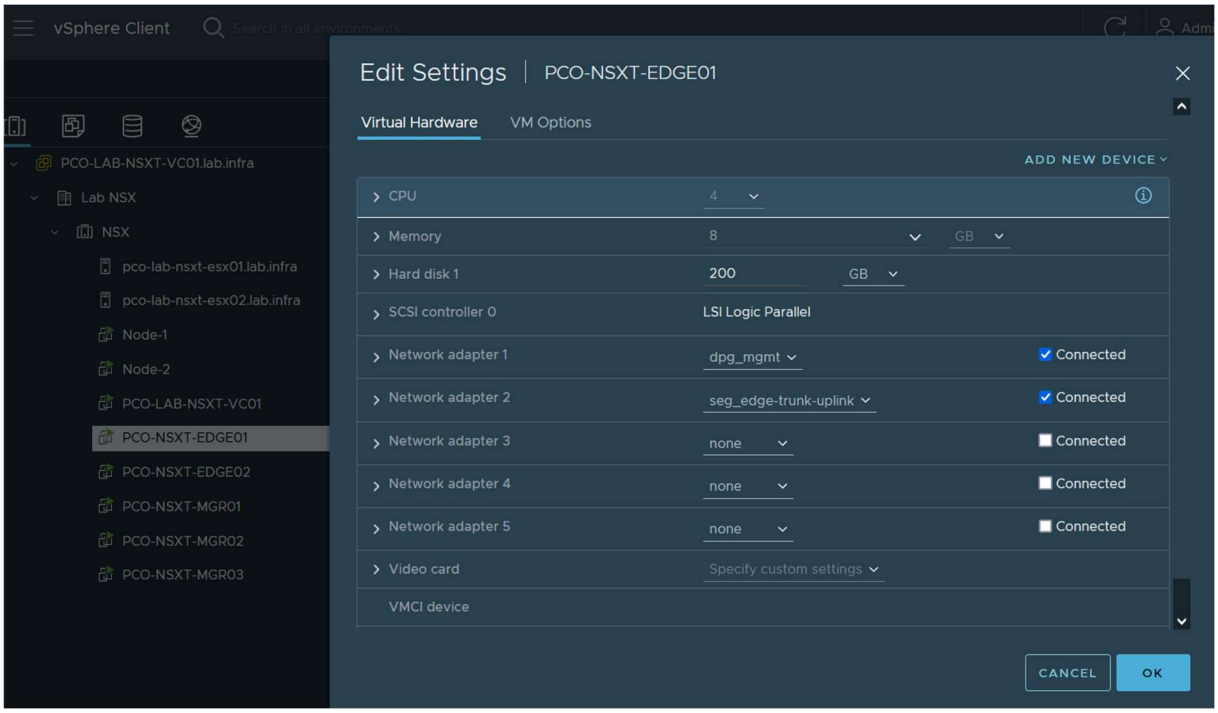
Aller dans System > Configuration > Fabric > Nodes > Edge Clusters.



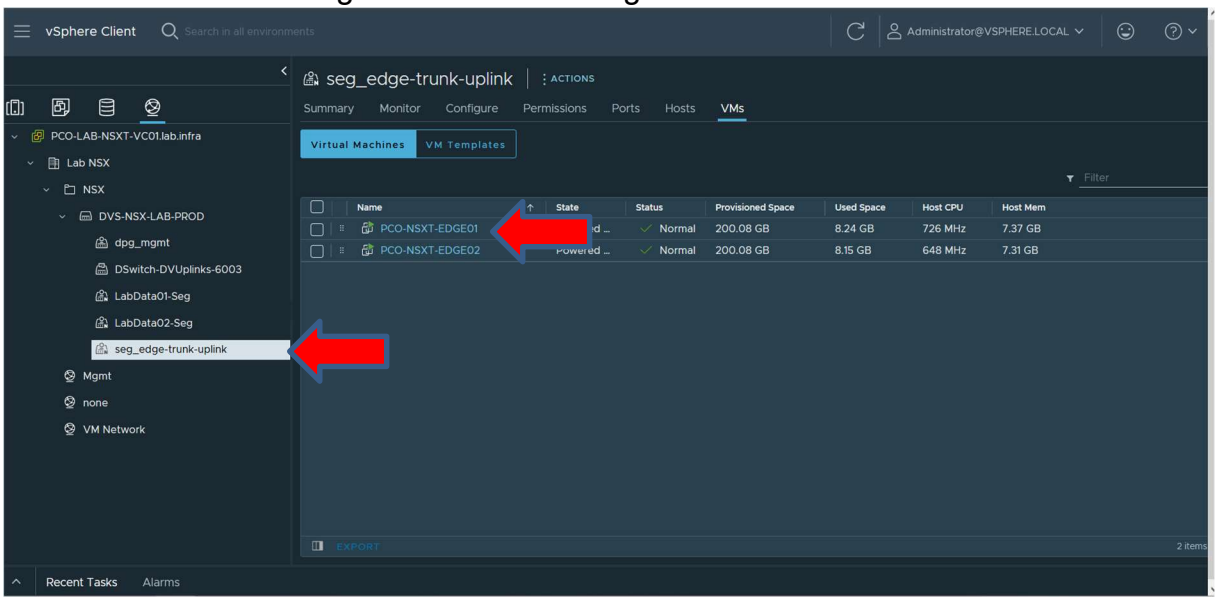
Add edge cluster



Edit settings des deux nœuds dans vCenter et rajouter le segment



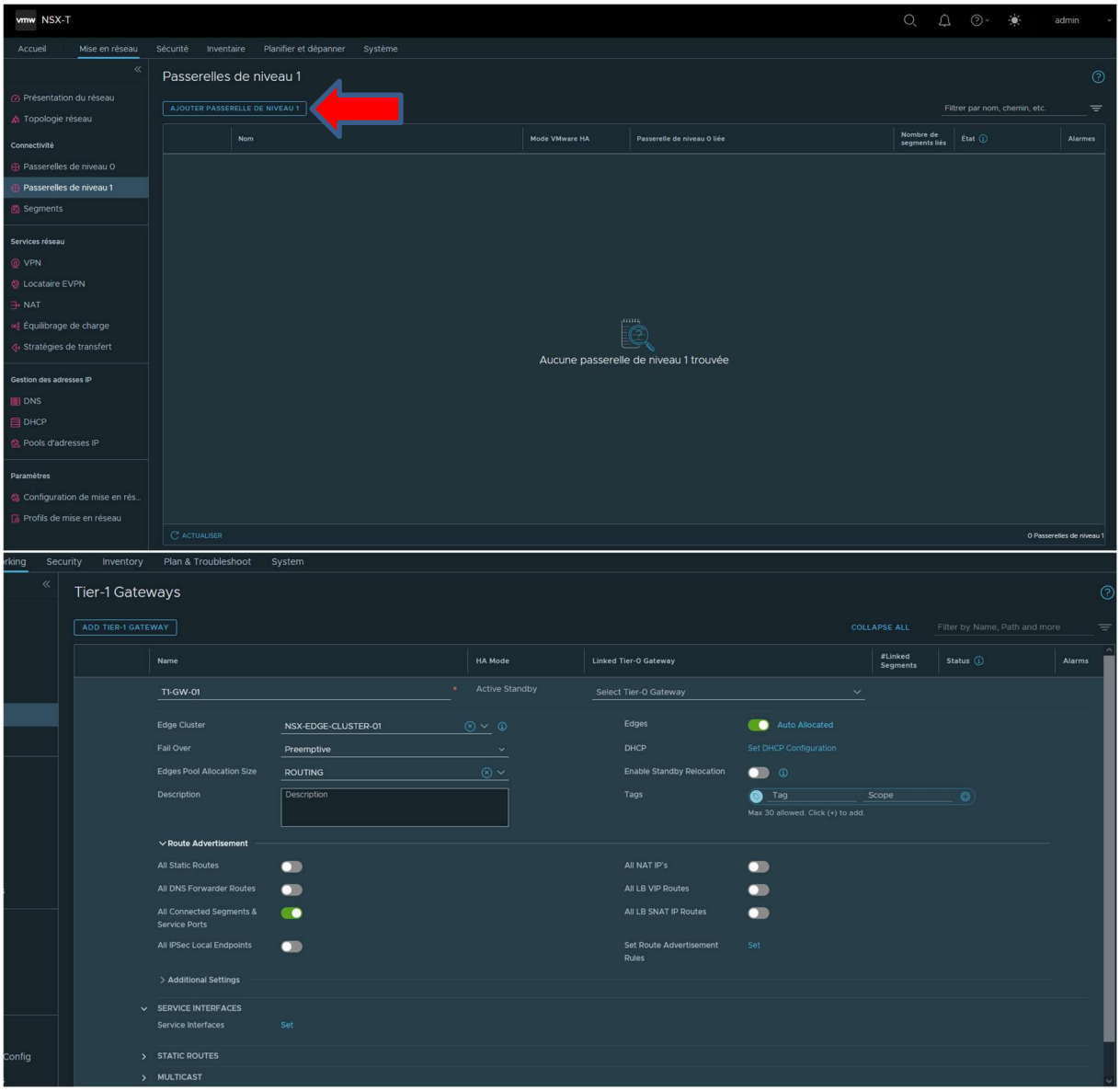
Vérifiez et afficher le segment des nœud edge dans vCenter



12 Routage TIER-1 / Est-Ouest

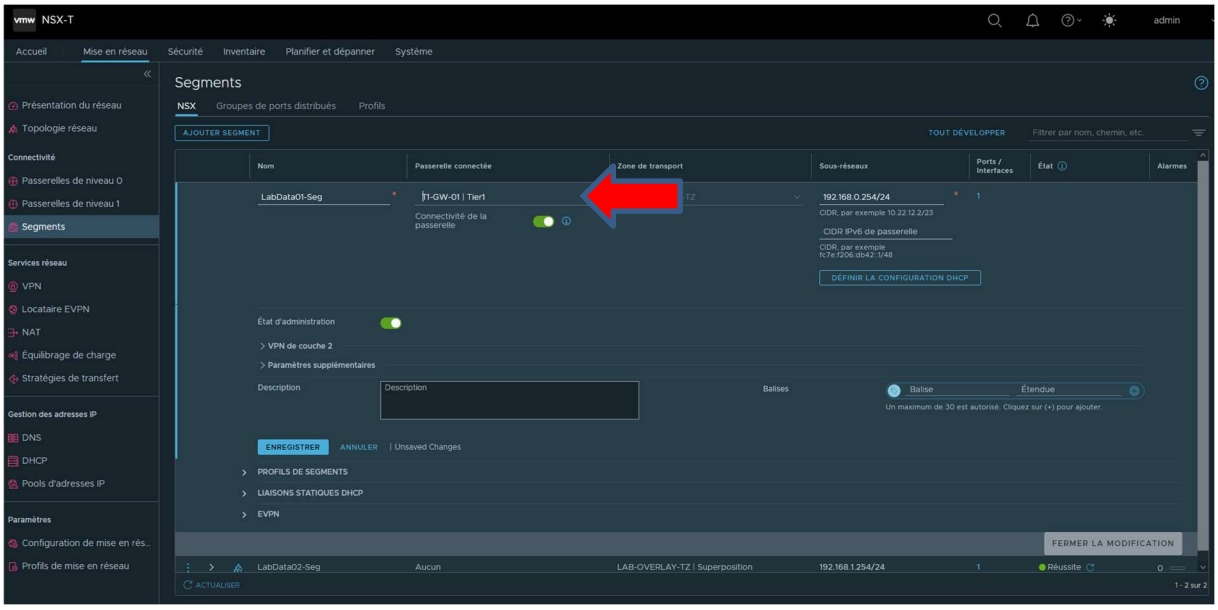
12.1 Gateway TIER-1

Aller dans Mise en réseau > Connectivité > Passerelles de niveau 1 puis cliquer sur Ajouter passerelle de niveau 1

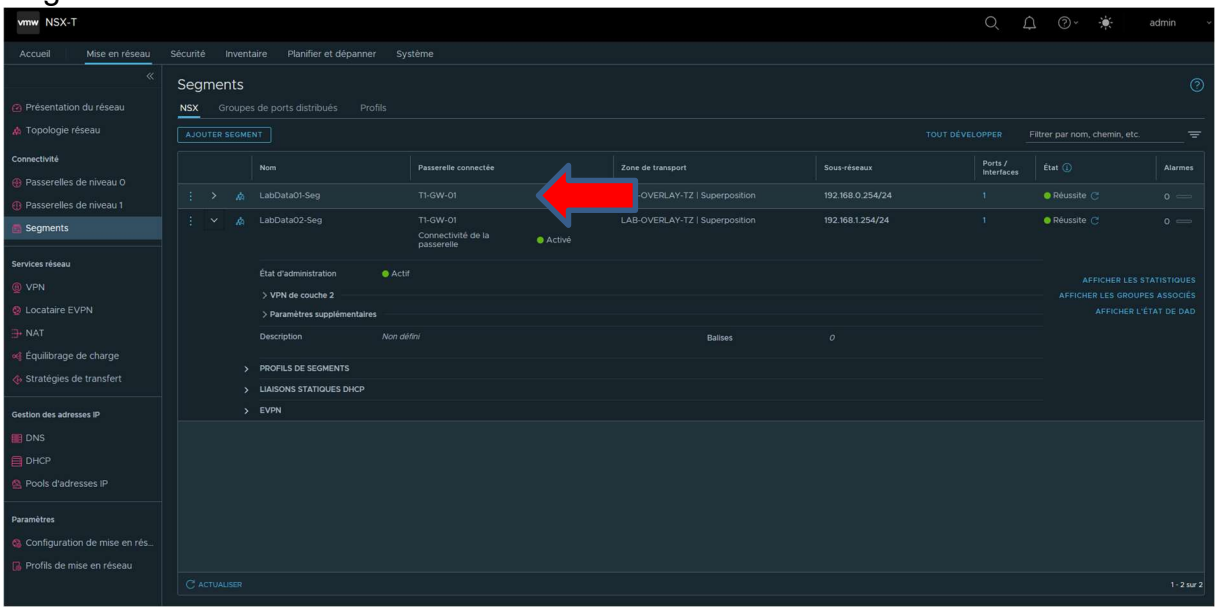


12.2 Connexion des segments

Aller dans Networking > Connectivité > Segments
Editer un segment pour y ajouter une gateway :
Segments 01



Segments 02



12.3 Tests

Machines de test :

- Segment01 : 192.168.0.1
- Segment02 : 192.168.1.1

```
3: ens224: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:a2:42:5d brd ff:ff:ff:ff:ff:ff
    altname enp19s0
    inet 192.168.1.1/24 brd 192.168.1.255 scope global ens224
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fea2:425d/64 scope link
       valid_lft forever preferred_lft forever
user@Node1:~$ ping 192.168.0.254
PING 192.168.0.254 (192.168.0.254) 56(84) bytes of data.
64 bytes from 192.168.0.254: icmp_seq=1 ttl=64 time=0.148 ms
64 bytes from 192.168.0.254: icmp_seq=2 ttl=64 time=0.137 ms
64 bytes from 192.168.0.254: icmp_seq=3 ttl=64 time=0.792 ms
64 bytes from 192.168.0.254: icmp_seq=4 ttl=64 time=0.166 ms
64 bytes from 192.168.0.254: icmp_seq=5 ttl=64 time=0.166 ms
64 bytes from 192.168.0.254: icmp_seq=6 ttl=64 time=0.150 ms
64 bytes from 192.168.0.254: icmp_seq=7 ttl=64 time=0.186 ms
64 bytes from 192.168.0.254: icmp_seq=8 ttl=64 time=0.321 ms
64 bytes from 192.168.0.254: icmp_seq=9 ttl=64 time=0.181 ms
```

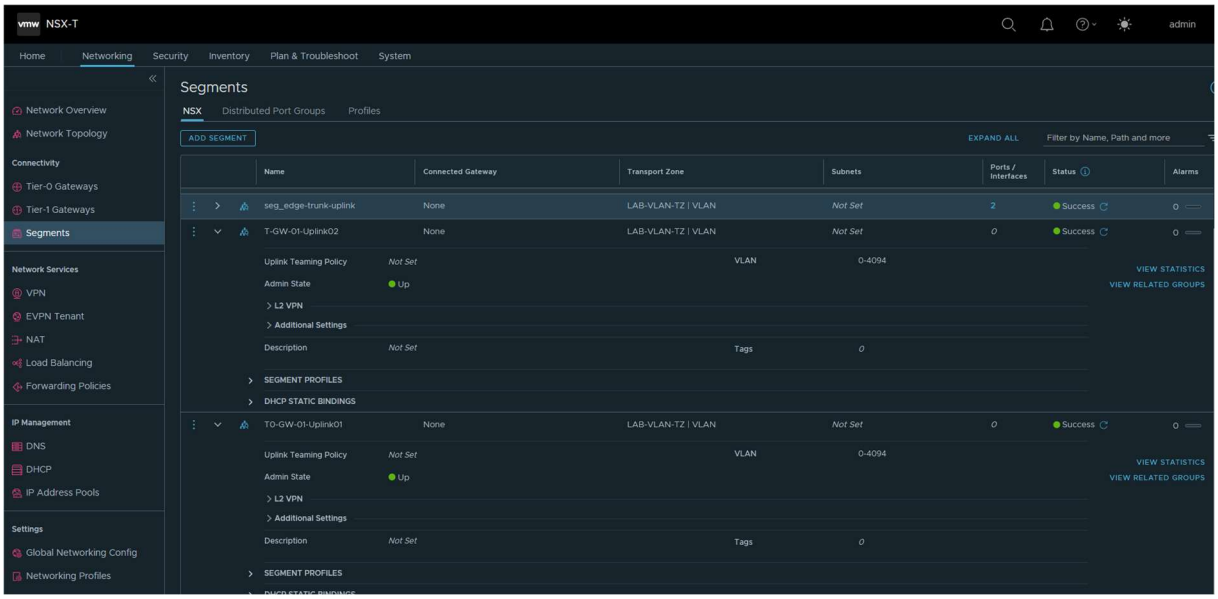
```
3: ens224: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:a2:dc:02 brd ff:ff:ff:ff:ff:ff
    altname enp19s0
    inet 192.168.0.1/24 brd 192.168.0.255 scope global ens224
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fea2:dc02/64 scope link
       valid_lft forever preferred_lft forever
user@Node1:~$ ping 192.168.1.254
PING 192.168.1.254 (192.168.1.254) 56(84) bytes of data.
64 bytes from 192.168.1.254: icmp_seq=1 ttl=64 time=0.135 ms
64 bytes from 192.168.1.254: icmp_seq=2 ttl=64 time=0.136 ms
64 bytes from 192.168.1.254: icmp_seq=3 ttl=64 time=0.128 ms
64 bytes from 192.168.1.254: icmp_seq=4 ttl=64 time=0.147 ms
64 bytes from 192.168.1.254: icmp_seq=5 ttl=64 time=0.161 ms
64 bytes from 192.168.1.254: icmp_seq=6 ttl=64 time=0.134 ms
```

Les deux machines ce ping entre elle sur deux segments différents.

13 Routage TIER-0 / Nord-Sud

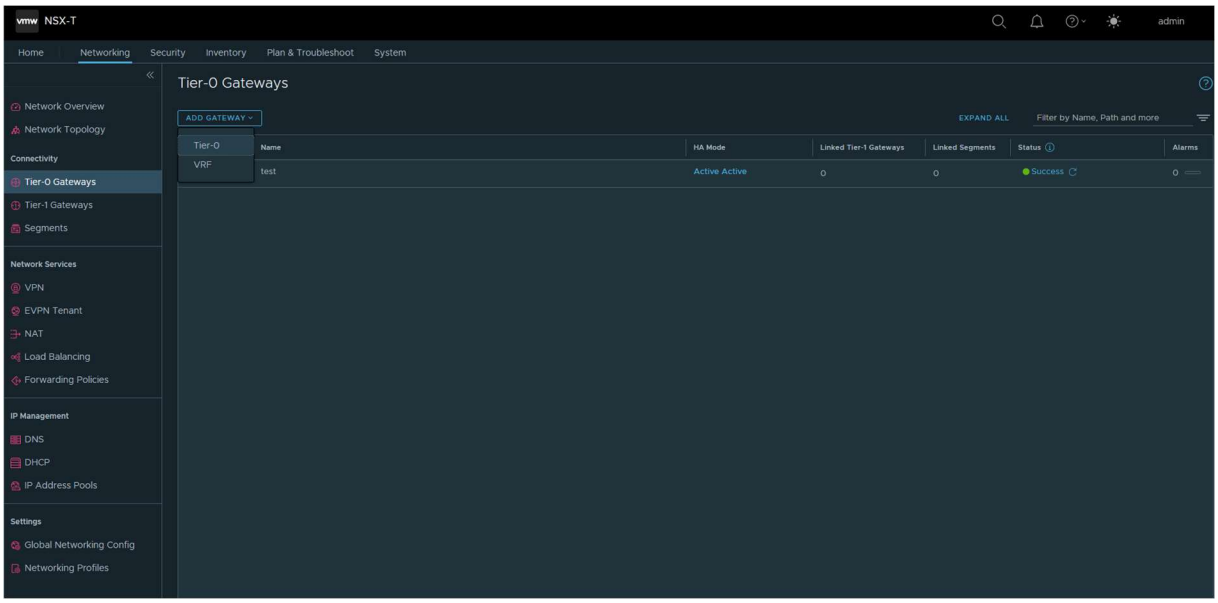
13.1 Segments d'uplink

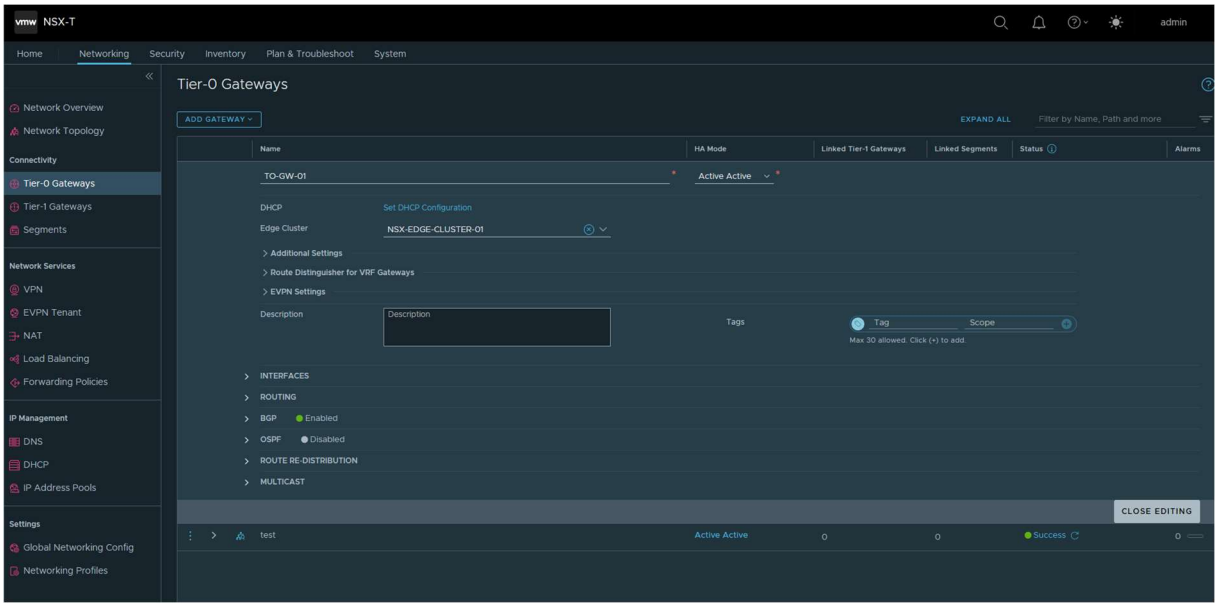
Je crée deux segments d'uplink pour mon cluster de edge node



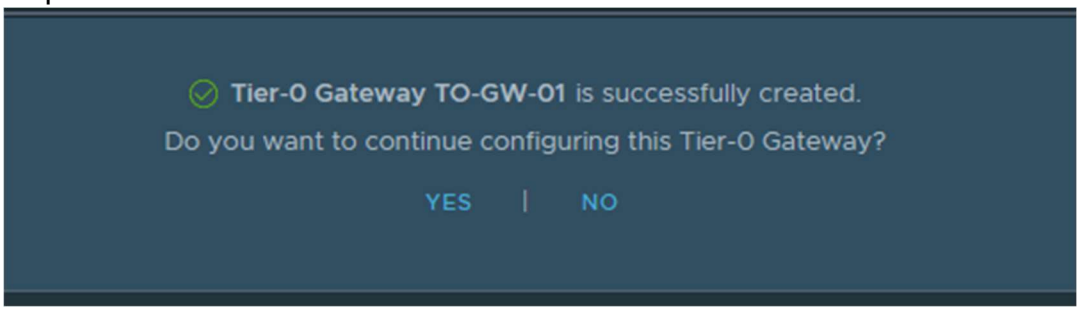
13.2 Gateway TIER-0

Aller dans Networking > Connectivity > Tier-0 Gateways puis cliquer sur Add Gateway > TIER-0.

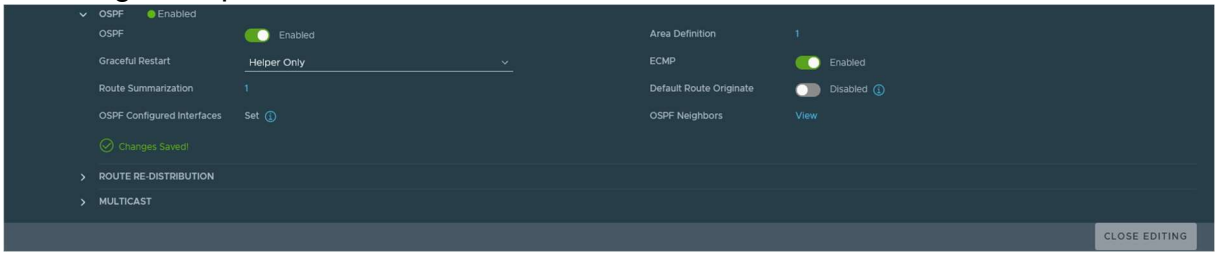


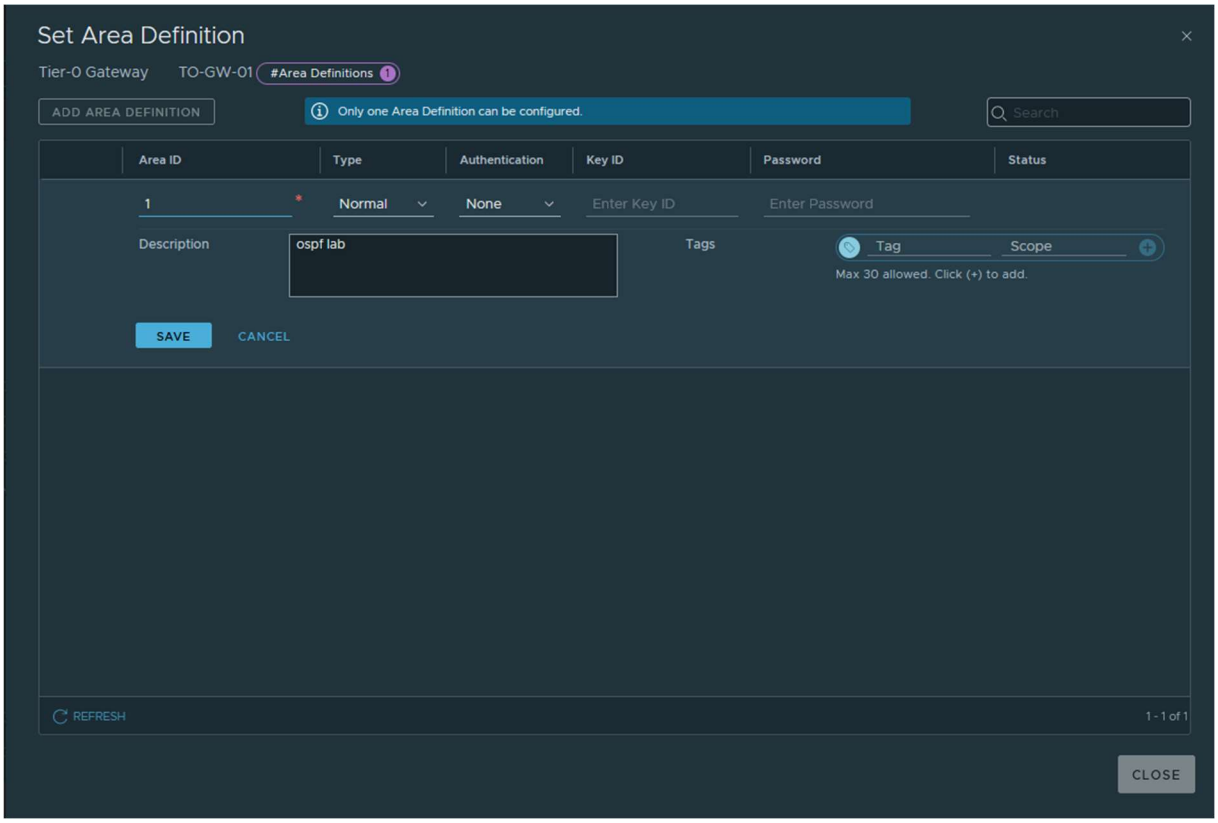


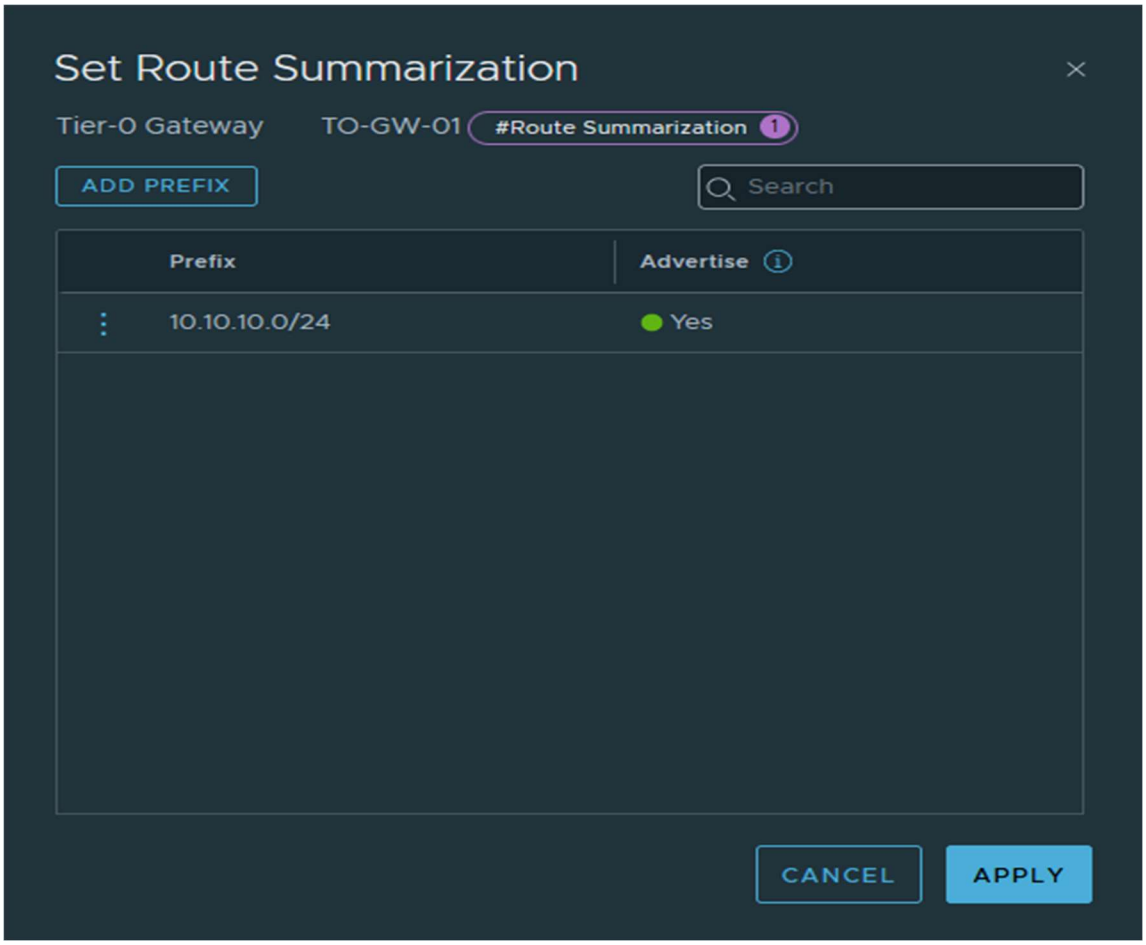
Répondre « Yes »



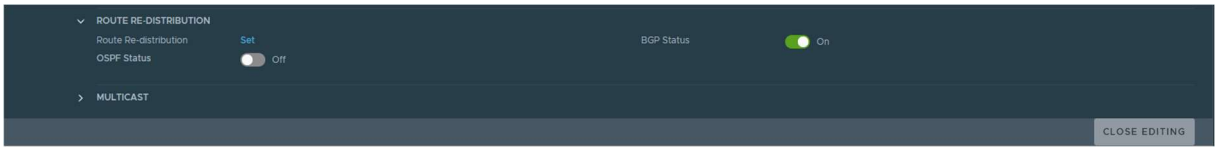
Je configure le protocole OSPF





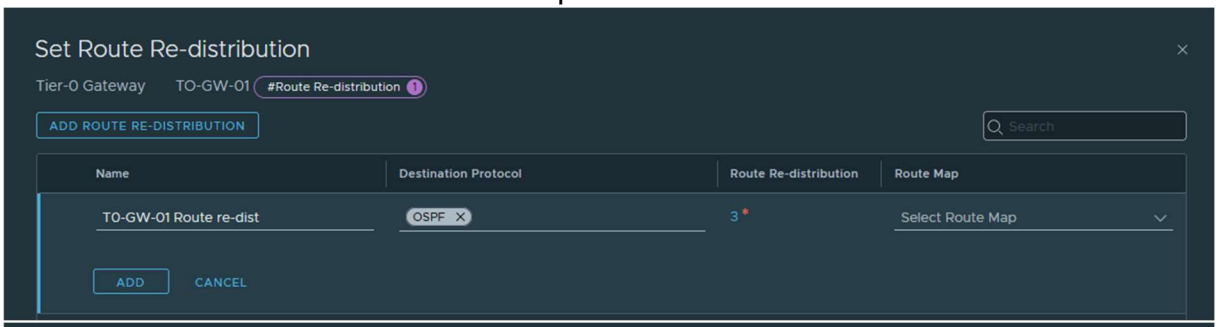


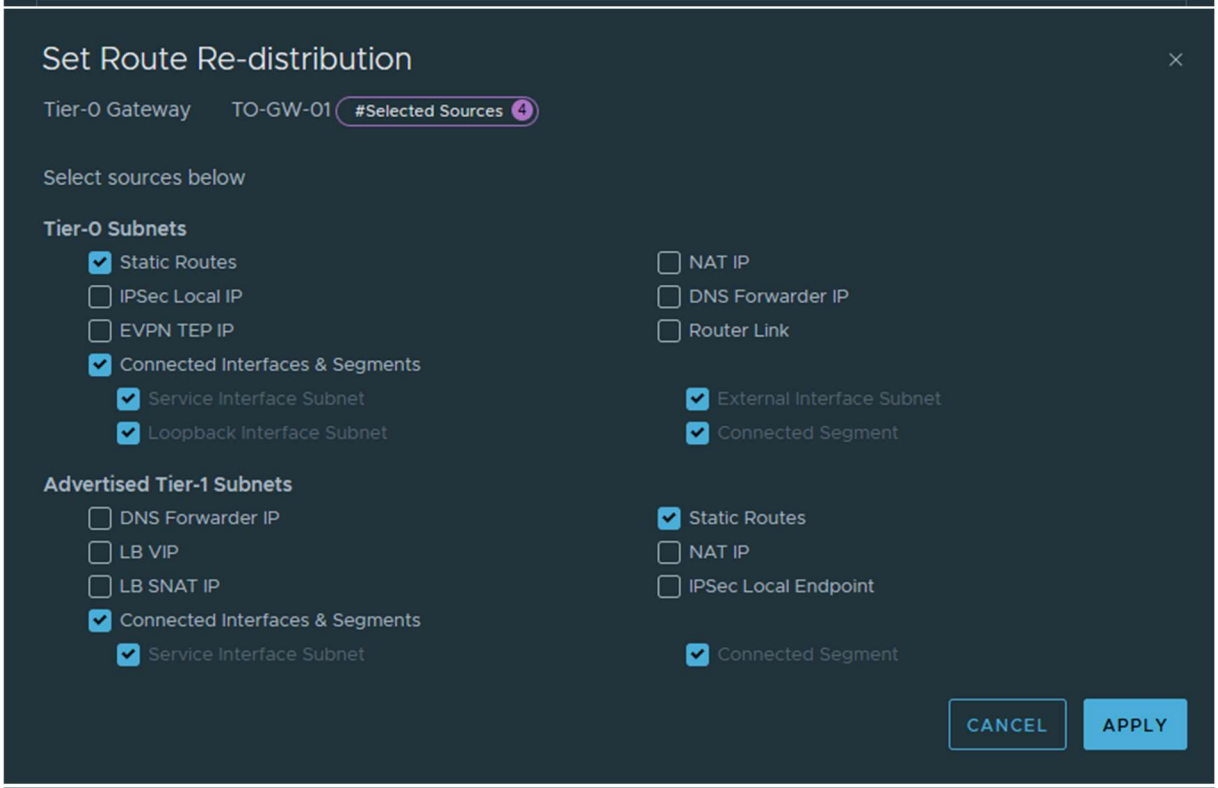
Développer la section ROUTE RE-DISTRIBUTION

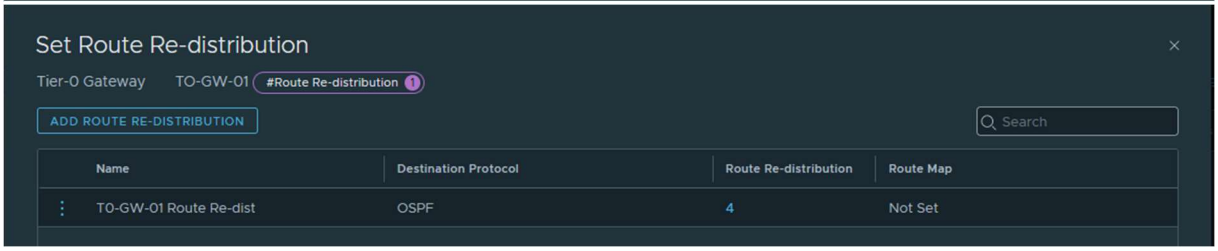


Cliquer sur « Set » puis « ADD ROUTE REDISTRIBUTION »

Définir le nom de la redistribution et cliquer sur « Set »



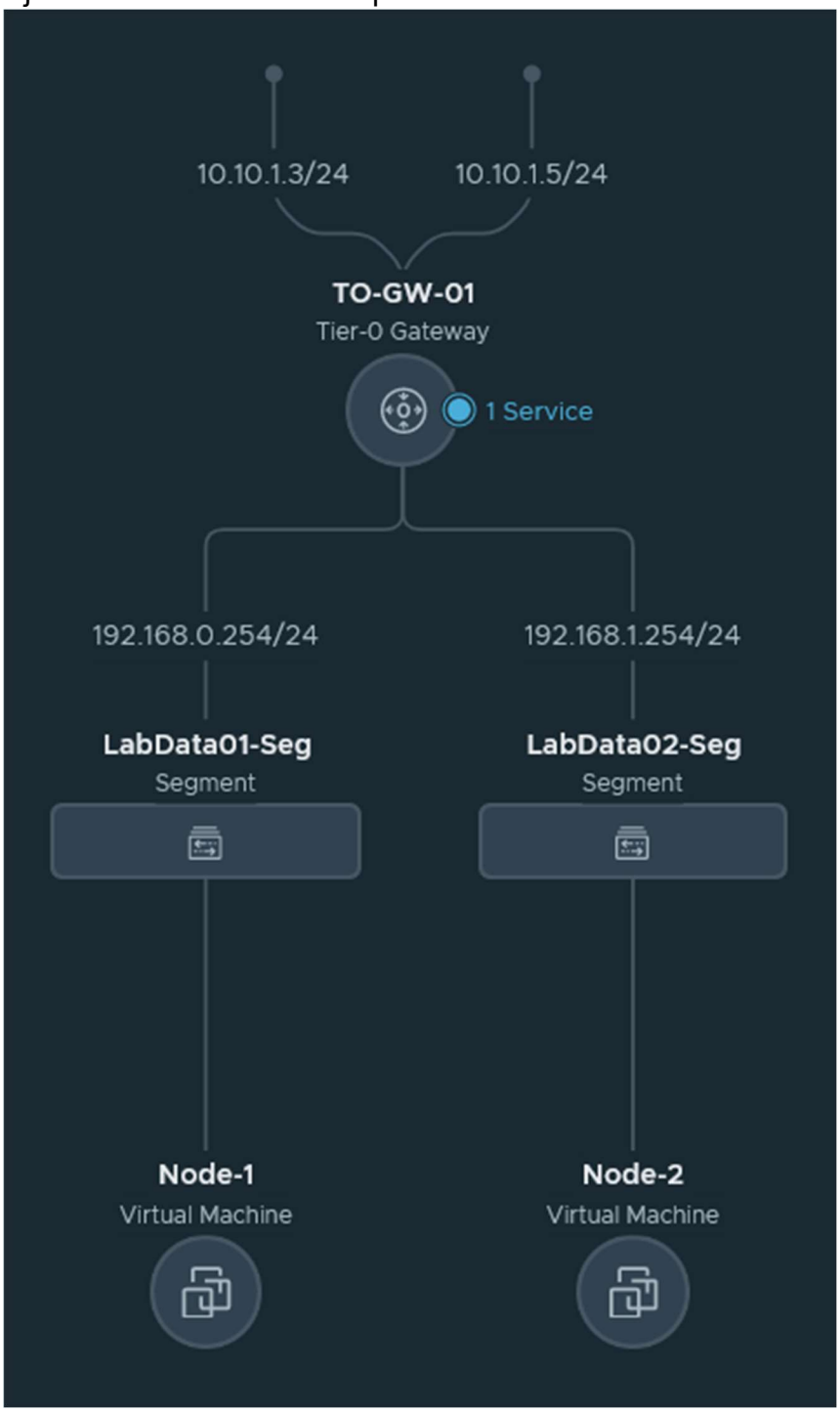




Tout valider et vérifier que la redistribution des routes est bien activée

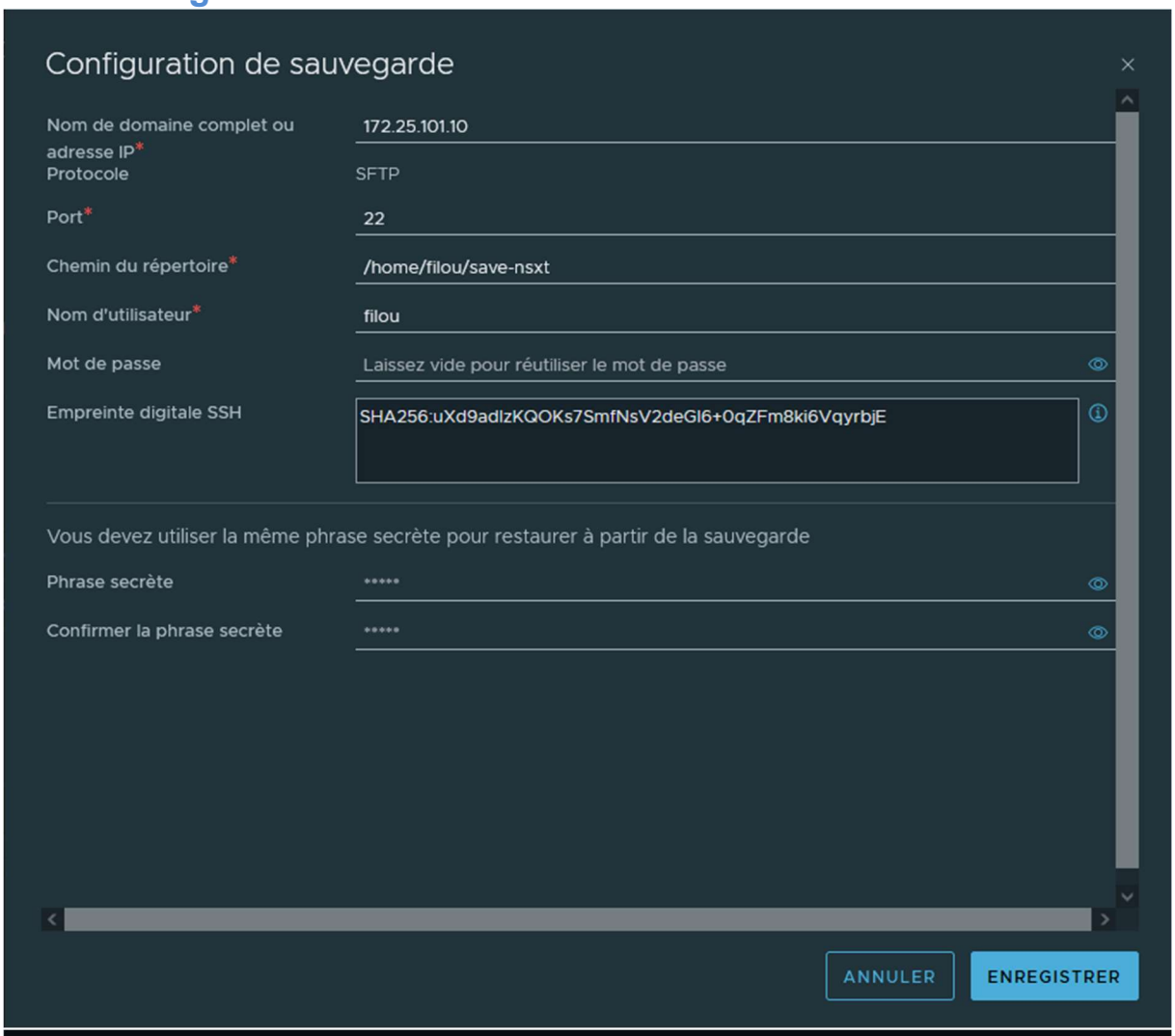
Développer la section INTERFACES et cliquer sur « Set »

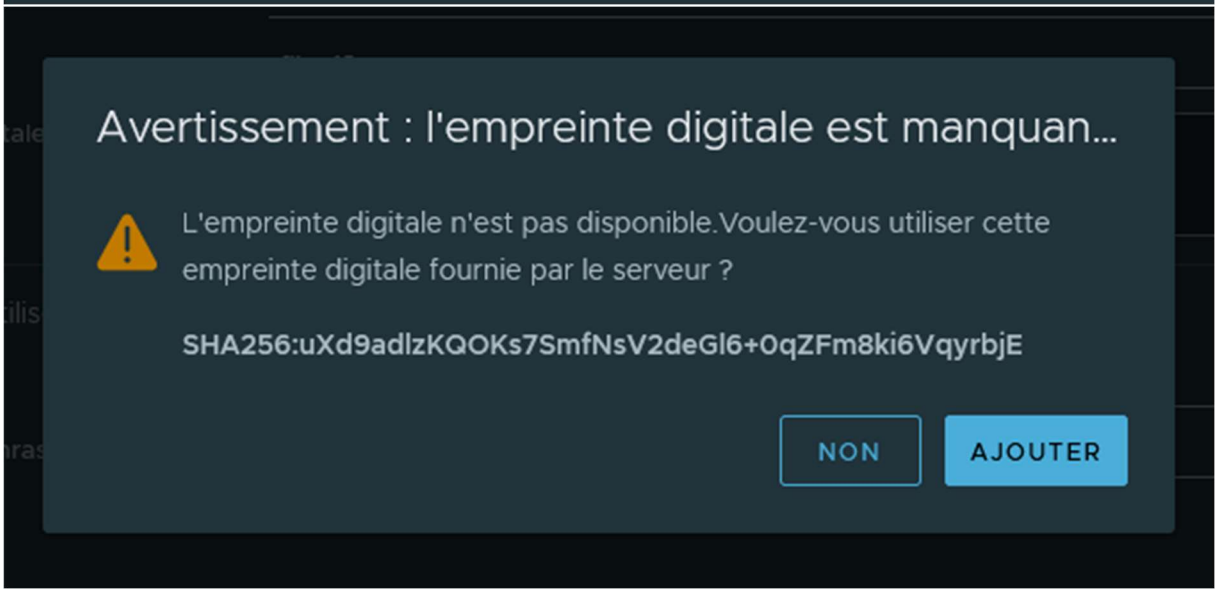
Ajouter les 2 interfaces d'uplink



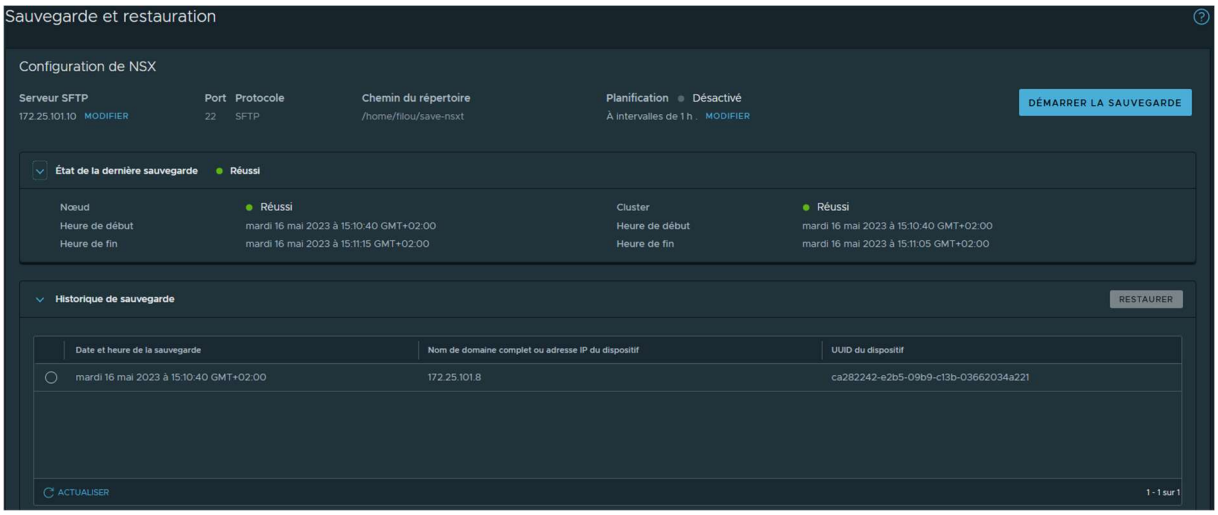
14 Configuration sauvegarde NSX

14.1 Configuration





14.2 Utilisation



14.3 Verification de la sauvegarde sur le serveur

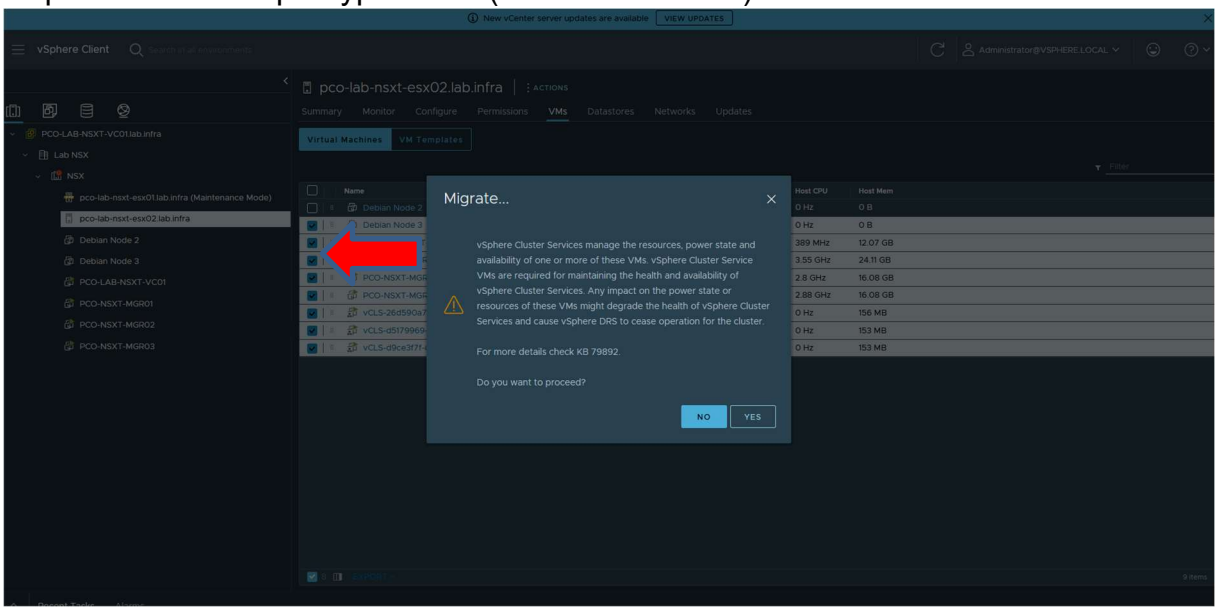
```
filou@debian:~/save-nsxt/cluster-node-backups$ tree
.
├── 3.2.2.0.0.20737190-ca282242-e2b5-09b9-c13b-03662034a221-172.25.101.8
│   └── backup-2023-05-16T13_10_40UTC
│       ├── cluster_backup-ca282242-e2b5-09b9-c13b-03662034a221-172.25.101.8-nsx-ufo-backup-restore.tar
│       └── node_backup-ca282242-e2b5-09b9-c13b-03662034a221-172.25.101.8.tar
└── 4.1.0.0.0.21333676-85882242-0716-8f29-58a0-65439b3dfaa1-172.25.101.8
    └── backup-2023-05-31T08_43_21UTC
        ├── cluster_backup-85882242-0716-8f29-58a0-65439b3dfaa1-172.25.101.8-nsx-ufo-backup-restore.tar
        └── node_backup-85882242-0716-8f29-58a0-65439b3dfaa1-172.25.101.8.tar
```

15 Désinstaller NSX des hosts

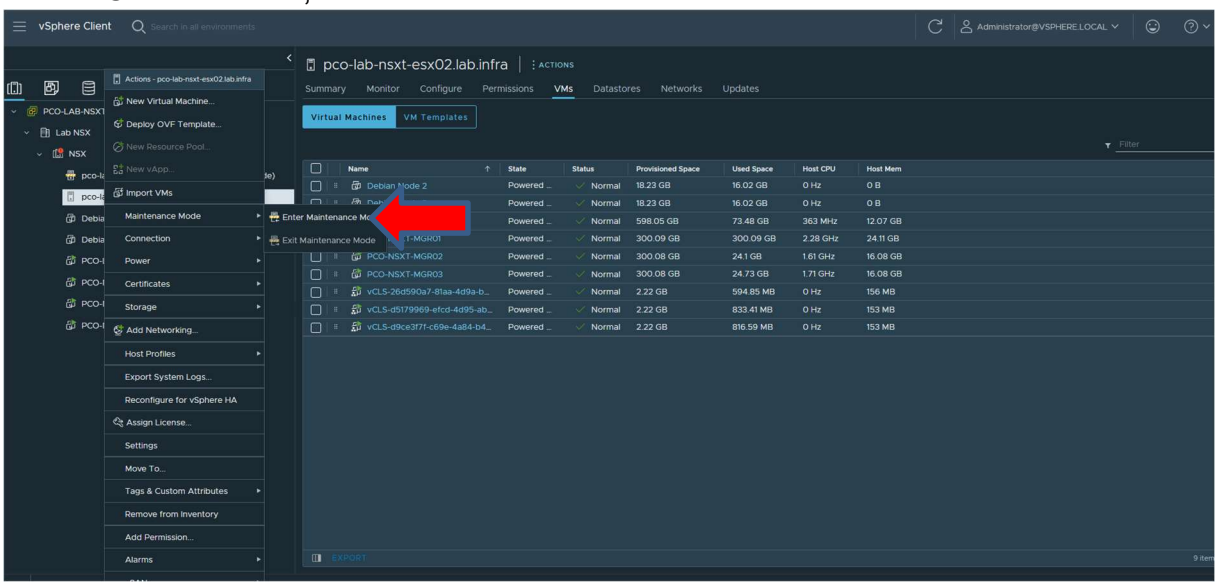
15.1 Conditions préalables

Déplacez les VM’s vers le second host ESX

Déplacez les VM’s par type d’état (allumé ou éteinte)

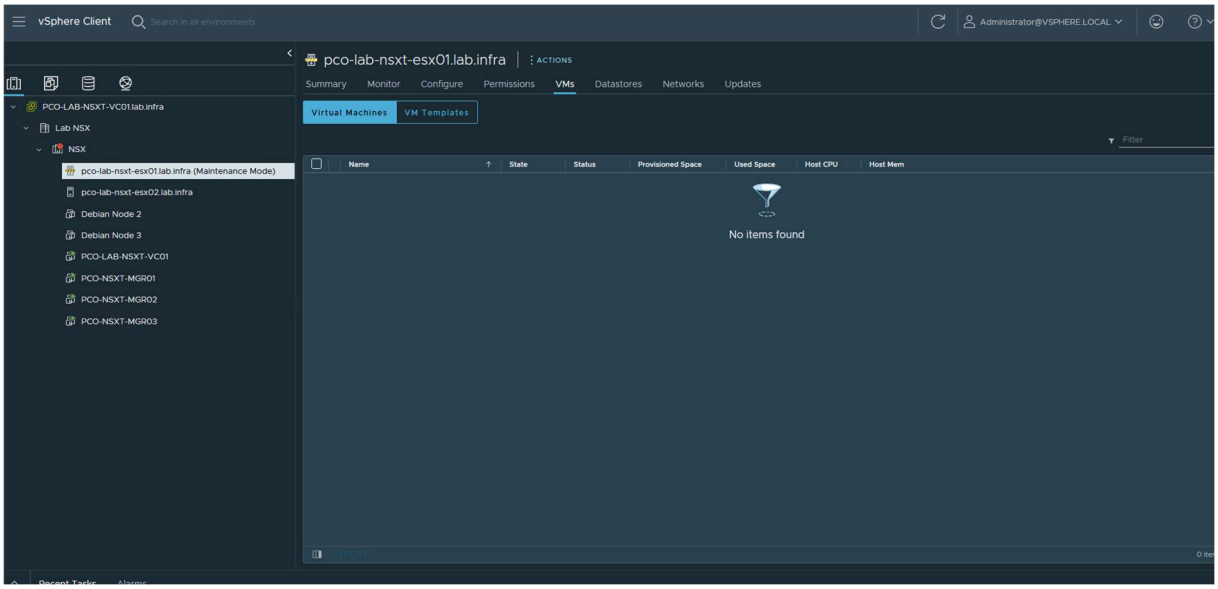


Dans vCenter Server, mettez les hôtes en mode maintenance



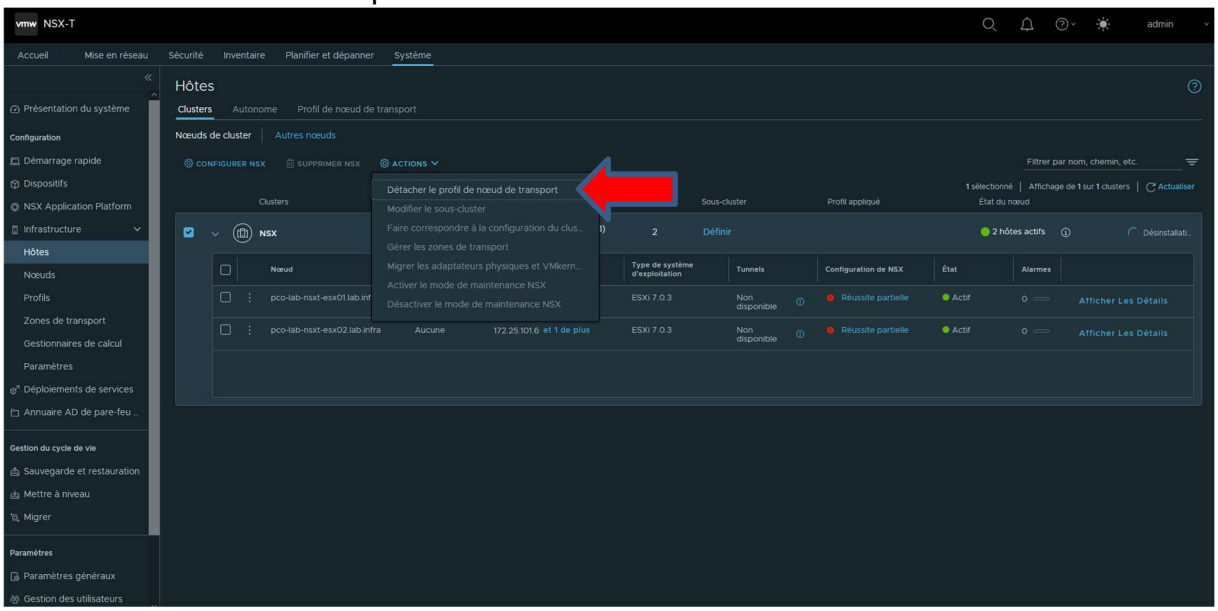
Sur un hôte ESXi placé en état verrouillé, assurez-vous que l'utilisateur root est ajouté à la liste d'exceptions, afin qu'une session SSH puisse être établie avec l'hôte.

Les VM’s ont été migré vers le second hosts



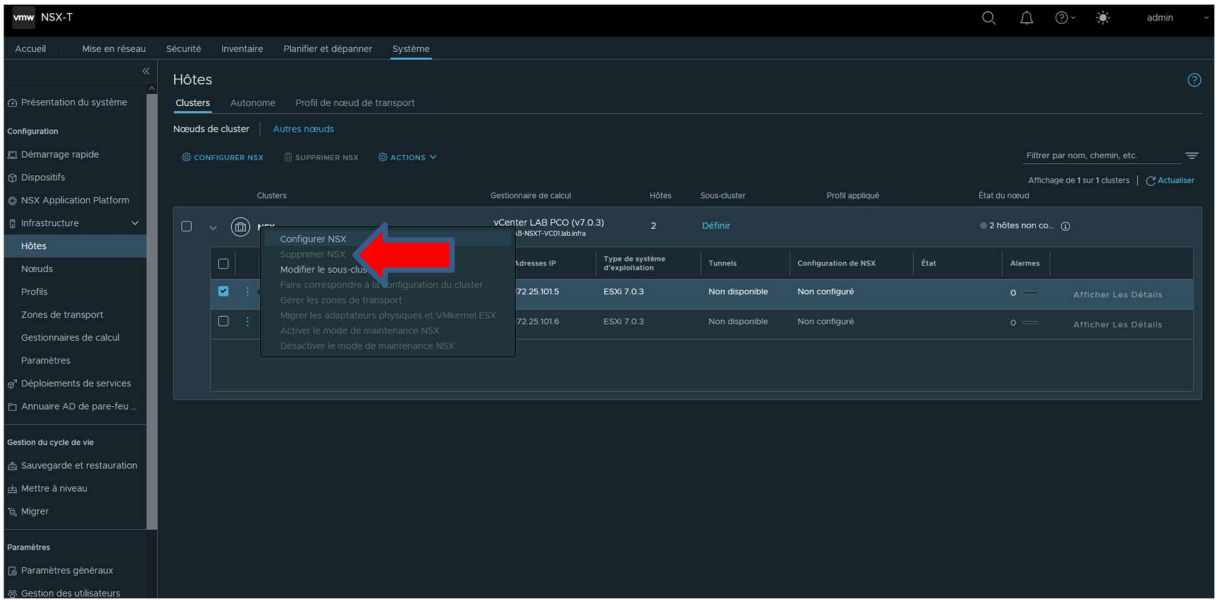
15.2 Procédure

Depuis un navigateur, connectez-vous avec des privilèges d'administrateur à un gestionnaire NSX à l'adresse https://<nsx-manager-ip-address>.
Naviguez dans l'interface utilisateur en fonction de la version du centre de données NSX-T et sélectionnez un hôte :
Si le cluster a un profil de nœud de transport appliqué, sélectionnez le cluster et cliquez sur Actions > Détacher le profil TN.



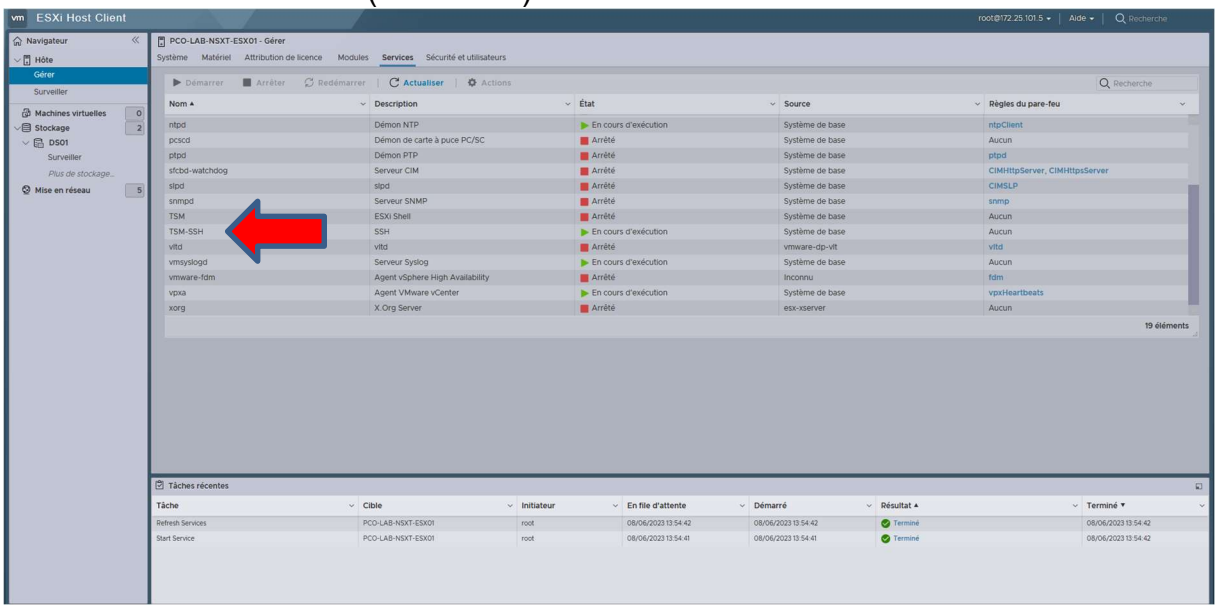
Si le cluster a un profil de nœud de transport appliqué, la colonne Configuration NSX pour le cluster affiche le nom du profil.

Sélectionnez l'hôte et cliquez sur Supprimer NSX.



15.3 Vérifiez que NSX-T Data Center est supprimé de l'hôte.

Démarrer le service SSH (TSM-SSH) sur l'ESX



Connectez-vous à l'interface de ligne de commande de l'hôte en tant que root.

Exécutez cette commande pour vérifier les VIB du centre de données NSX-T

```
esxcli software vib list | grep -E 'nsx|vsipfwlib'
```

```
[root@PCO-LAB-NSXT-ESX01:~] esxcli software vib list | grep -E 'nsx|vsipfwlib'
nsx-adf                        3.2.2.0.0-7.0.20737187               VMware  VMwareCertified   2023-06-08
nsx-cfgagent                   3.2.2.0.0-7.0.20737187               VMware  VMwareCertified   2023-06-08
nsx-context-mux                3.2.2.0.0-7.0.20737187               VMware  VMwareCertified   2023-06-08
nsx-cpp-libs                   3.2.2.0.0-7.0.20737187               VMware  VMwareCertified   2023-06-08
nsx-esx-datapath               3.2.2.0.0-7.0.20737187               VMware  VMwareCertified   2023-06-08
nsx-exporter                   3.2.2.0.0-7.0.20737187               VMware  VMwareCertified   2023-06-08
nsx-host                       3.2.2.0.0-7.0.20737187               VMware  VMwareCertified   2023-06-08
nsx-ids                        3.2.2.0.0-7.0.20737187               VMware  VMwareCertified   2023-06-08
nsx-monitoring                 3.2.2.0.0-7.0.20737187               VMware  VMwareCertified   2023-06-08
nsx-mpa                        3.2.2.0.0-7.0.20737187               VMware  VMwareCertified   2023-06-08
nsx-nestdb                     3.2.2.0.0-7.0.20737187               VMware  VMwareCertified   2023-06-08
nsx-netopa                     3.2.2.0.0-7.0.20737187               VMware  VMwareCertified   2023-06-08
nsx-opsagent                   3.2.2.0.0-7.0.20737187               VMware  VMwareCertified   2023-06-08
nsx-platform-client            3.2.2.0.0-7.0.20737187               VMware  VMwareCertified   2023-06-08
nsx-proto2-libs                3.2.2.0.0-7.0.20737187               VMware  VMwareCertified   2023-06-08
nsx-proxy                      3.2.2.0.0-7.0.20737187               VMware  VMwareCertified   2023-06-08
nsx-python-gevent              1.1.0-18242523                       VMware  VMwareCertified   2023-06-08
nsx-python-greenlet            0.4.14-18242315                      VMware  VMwareCertified   2023-06-08
nsx-python-logging             3.2.2.0.0-7.0.20737187               VMware  VMwareCertified   2023-06-08
nsx-python-protobuf            2.6.1-18242311                       VMware  VMwareCertified   2023-06-08
nsx-python-utils               3.2.2.0.0-7.0.20737187               VMware  VMwareCertified   2023-06-08
nsx-sfhc                       3.2.2.0.0-7.0.20737187               VMware  VMwareCertified   2023-06-08
nsx-shared-libs                3.2.2.0.0-7.0.20737187               VMware  VMwareCertified   2023-06-08
nsx-vdpi                       3.2.2.0.0-7.0.20737187               VMware  VMwareCertified   2023-06-08
nsxcli                         3.2.2.0.0-7.0.20737187               VMware  VMwareCertified   2023-06-08
vsipfwlib                      3.2.2.0.0-7.0.20737187               VMware  VMwareCertified   2023-06-08
[root@PCO-LAB-NSXT-ESX01:~]
```

Désactivation du protocole SNMP sur l'host ESXI
esxcli system snmp set --enable false

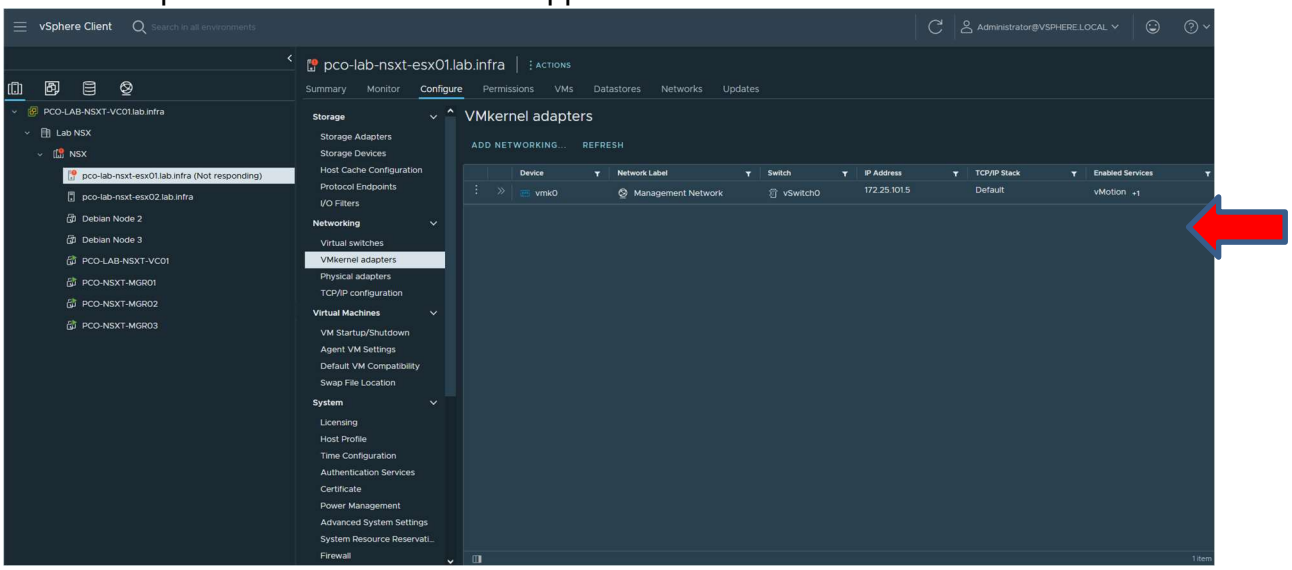
On tape la commande
nsxcli -c del nsx

```
[root@PCO-LAB-NSXT-ESX01:~] nsxcli -c del nsx


*************** STOP STOP STOP STOP STOP ***************

Carefully read the requirements and limitations of this command:

1. Read NSX-T documentation for 'Remove a Host from NSX-T Data Center or Uninstall NSX-T Data Center Completel

2. Deletion of this Transport Node from the NSX-T UI or API failed, and this is the last resort.

3. If this is an ESXi host:

        a. The host must be in maintenance mode.

        b. All resources attached to NSXPGs must be moved out.

If the above conditions for ESXi hosts are not met, the command WILL fail.

4. If this is a Linux host:

        a. If KVM is managing VM tenants then shut them down before running this command.

        b. This command should be run from the host console and may fail if run from an SSH client
           or any other network based shell client.
        c. The 'nsxcli -c del nsx' form of this command is not supported

5. For command progress check /scratch/log/nsxcli.log on ESXi host or /var/log/nsxcli.log on non-ESXi host.


Are you sure you want to remove NSX-T on this host? (yes/no) yes
```

On reboot l'ESXI

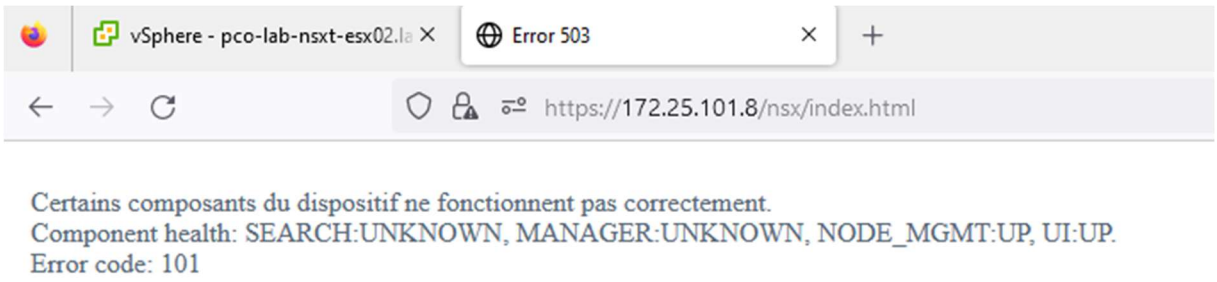
```
*************** STOP STOP STOP STOP STOP ***************

Carefully read the requirements and limitations of this command:

1. Read NSX-T documentation for 'Remove a Host from NSX-T Data Center or Uninstall NSX-T Data Center Completely'.

2. Deletion of this Transport Node from the NSX-T UI or API failed, and this is the last resort.

3. If this is an ESXi host:

       a. The host must be in maintenance mode.

       b. All resources attached to NSXPGs must be moved out.

If the above conditions for ESXi hosts are not met, the command WILL fail.

4. If this is a Linux host:

       a. If KVM is managing VM tenants then shut them down before running this command.

       b. This command should be run from the host console and may fail if run from an SSH client
          or any other network based shell client.
       c. The 'nsxcli -c del nsx' form of this command is not supported

5. For command progress check /scratch/log/nsxcli.log on ESXi host or /var/log/nsxcli.log on non-ESXi host.


Are you sure you want to remove NSX-T on this host? (yes/no) yes
Terminated
[root@PCO-LAB-NSXT-ESX02:~] reboot
```

On vérifie que les VMkernel ont été supprimé sur les deux ESXI



16 Troubleshooting NSX

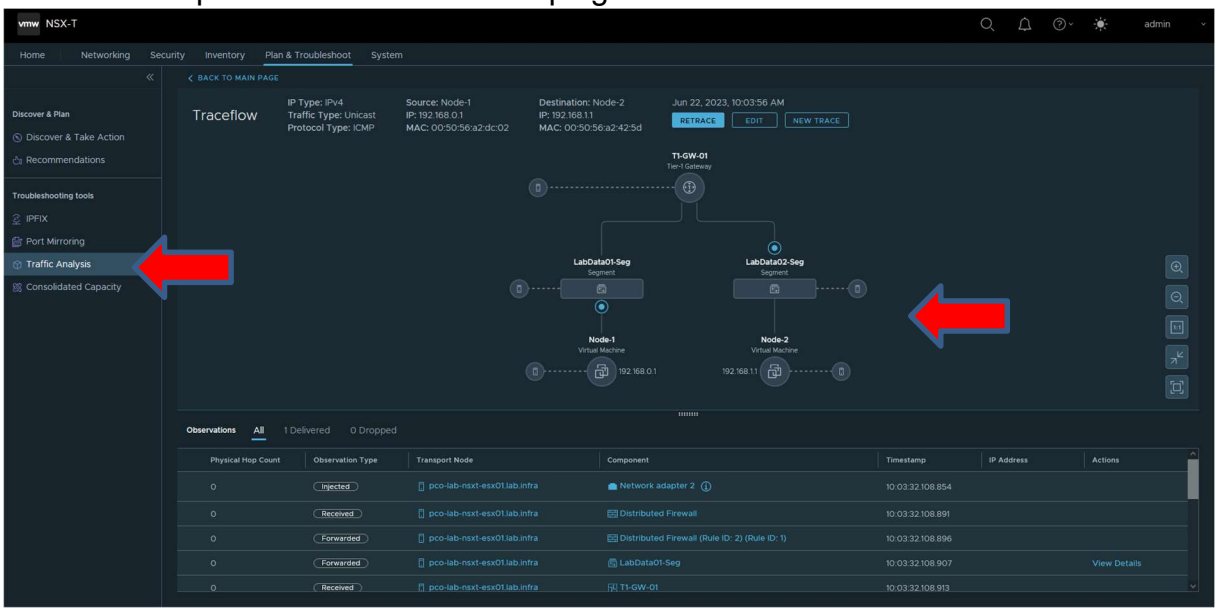
16.1 Error 503



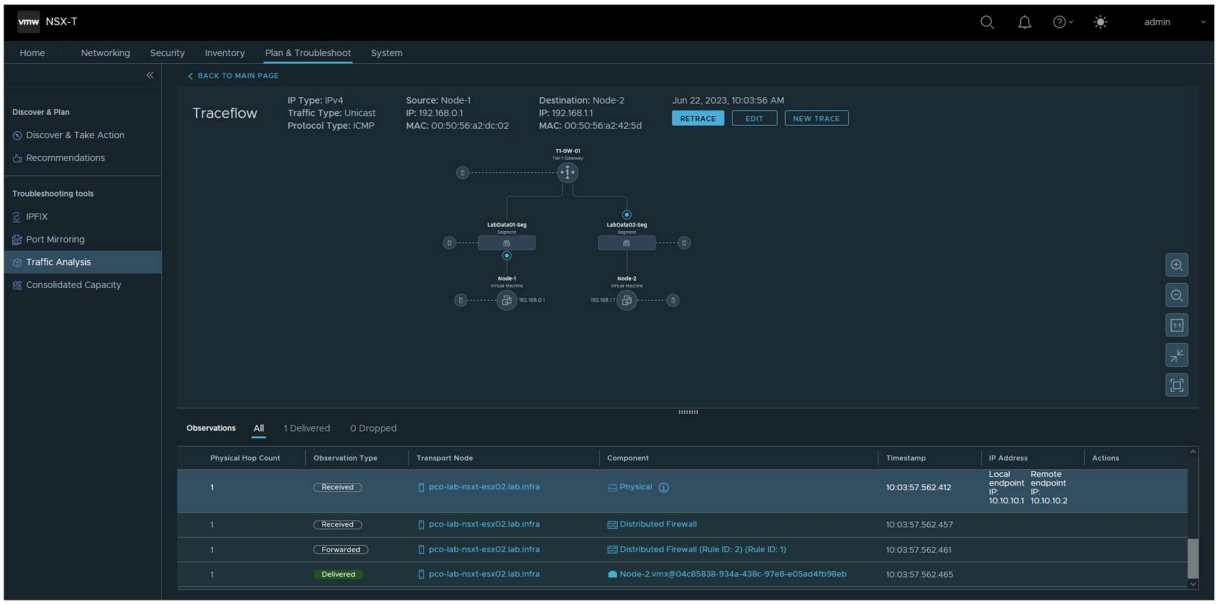
Ce probleme arrive de temps en temps quand NSX effectue des actions interne independement du fonctionnement de la solution.

16.2 Tester la connectivité entre deux VM

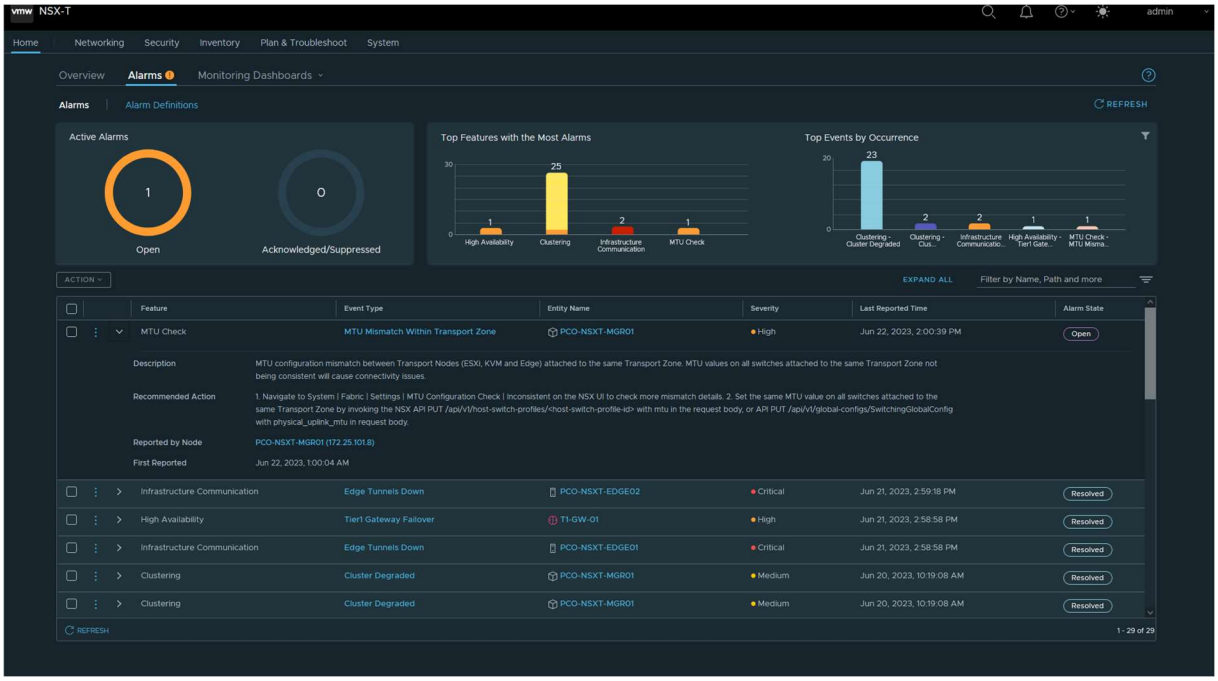
Aller dans Plan & Troubleshoot > Traffic Analysis
Vous avez la possibilité d'effectuer un ping



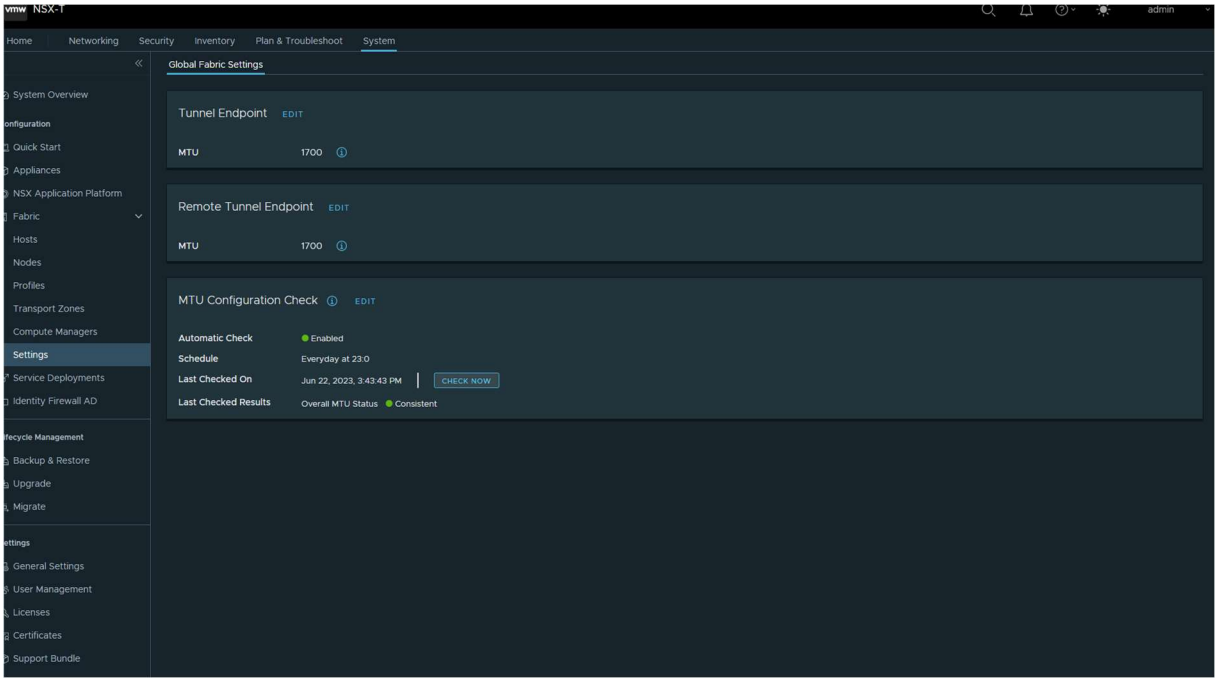
Le packet a bien été delivré



16.3 Probleme de MTU



Aller dans System > Fabric > Settings pour checker la MTU



17 MOB Management Object Reference

17.1 Présentation

Accessible depuis l'adresse du vCenter avec l'extension suivante /mob.
Permet d'avoir accès à la base de données de NSX.
https://172.25.101.7/mob