Contenu

Introduction

Ce document décrit les étapes pour capturer une circulation qui est complètement en dehors du Système d'informatique unifiée Cisco (UCS) et pour la diriger vers un virtual machine (VM) exécutant un outil de renifleur à l'intérieur de l'UCS.

La source et la destination de trafic étant capturé est en dehors de l'UCS. La capture peut être initiée sur un commutateur physique qui est directement relié à l'UCS ou ce pourrait être quelques sauts loin.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez des connaissances pratiques de ces thèmes :

- Système d'informatique unifiée Cisco (UCS)
- Version 4.1 ou ultérieures de VMware ESX
- Analyseur encapsulé de port de commutateur distant (ERSPAN)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Catalyst 6503 12.2(18)ZYA3c s'exécutants
- Exécution de gamme du Cisco UCS B 2.2(3e)
- Construction 1331820 d'ESXi 5.5 de VMware

Informations générales

L'UCS n'a pas la caractéristique de Remote SPAN (RSPAN) pour recevoir le trafic d'ENVERGURE d'un commutateur connecté et pour le diriger vers un port local. Ainsi la seule manière d'accomplir ceci dans un environnement UCS est à l'aide de la caractéristique encapsulée RSPAN (ERSPAN) sur un commutateur physique et envoyer le trafic capturé à la VM utilisant l'IP.

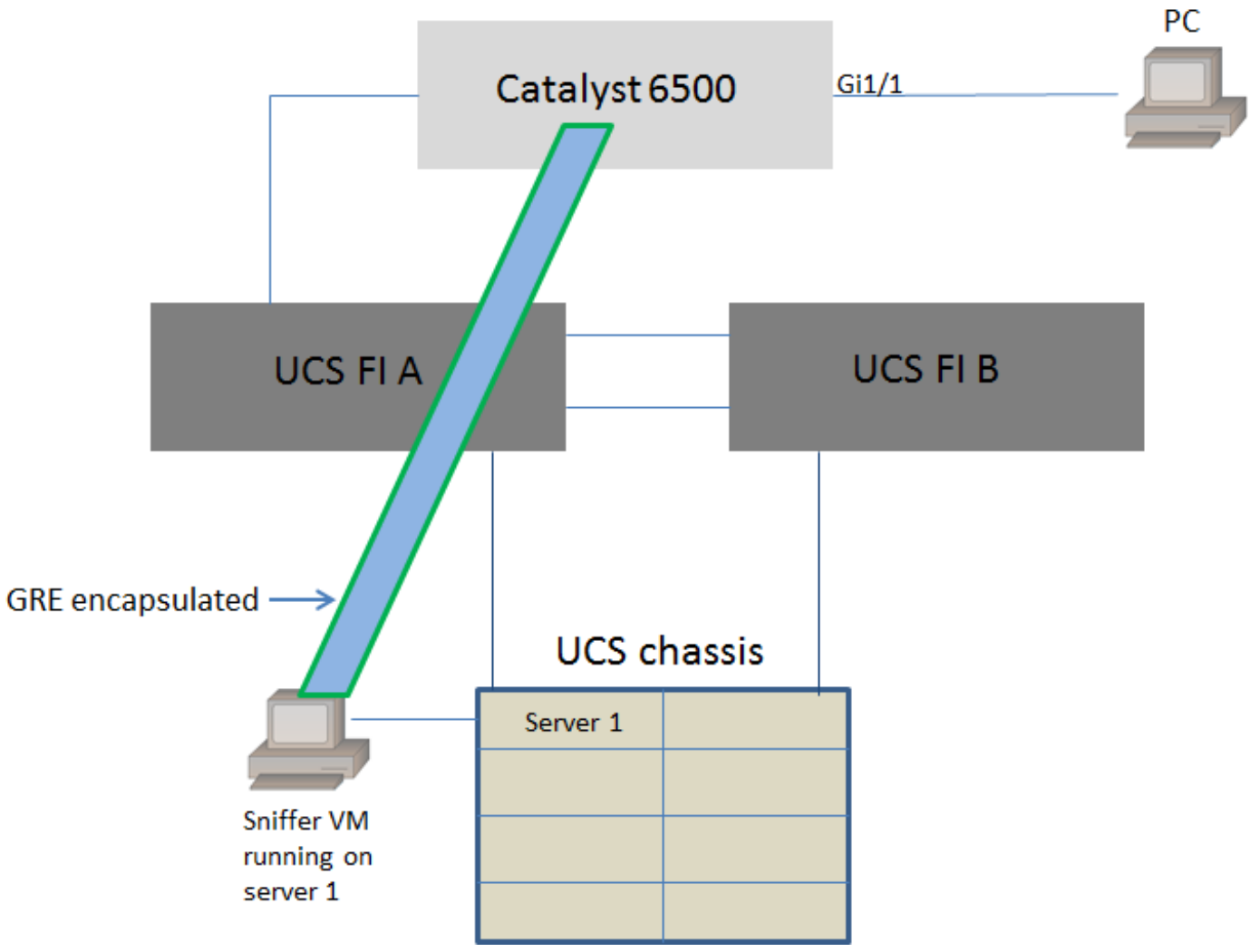
Dans certaines réalisations, la VM exécutant l'outil de renifleur ne peut pas avoir une adresse IP. Ce document explique la configuration exigée quand la VM de renifleur a une adresse IP aussi bien que le scénario sans adresse IP. La limite d'onl ici est que la VM de renifleur doit pouvoir lire l'encapsulation GRE/ERSPAN du trafic qui lui est envoyé.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

Diagramme du réseau

Cette topologie a été considérée dans ce document :



Le PC relié à GigabitEthernet1/1 du Catalyst 6500 est surveillé. Le trafic sur GigabitEthernet1/1 est capturé et envoyé à la VM de renifleur qui fonctionne à l'intérieur du Cisco UCS sur le serveur 1.

La caractéristique ERSPAN sur le commutateur 6500 capture le trafic, l'encapsule utilisant GRE et l'envoie à l'adresse IP de la VM de renifleur.

Configurations

VM de renifleur avec une adresse IP

> Remarque: Les étapes décrites dans cette section peuvent être également utilisées dans le scénario où le renifleur fonctionne dans un serveur de nu-métal sur une lame UCS au lieu de l'exécution sur une VM.

Ces étapes sont exigées quand la VM de renifleur peut avoir une adresse IP :

- Configurez la VM de renifleur à l'intérieur de l'environnement UCS avec une adresse IP qui est accessible des 6500
- Exécutez l'outil de renifleur à l'intérieur de la VM
- Configurez une session de source ERSPAN sur les 6500 et envoyez le trafic capturé directement à l'adresse IP de la VM

Les étapes de configuration sur le commutateur 6500 :

Dans cet exemple, l'adresse IP de la VM de renifleur est 192.0.2.2

VM de renifleur sans adresse IP

Ces étapes sont exigées quand la VM de renifleur ne peut pas avoir une adresse IP :

- Configurez la VM de renifleur à l'intérieur de l'environnement UCS
- Exécutez l'outil de renifleur à l'intérieur de la VM
- Créez une deuxième VM qui peut avoir une adresse IP dans le même hôte et la configurer avec une adresse IP qui est accessible des 6500
- Configurez le port-groupe sur le vSwitch de VMware pour être en mode promiscueux
- Configurez une session de source ERSPAN sur les 6500 et envoyez le trafic capturé à l'adresse IP de la deuxième VM

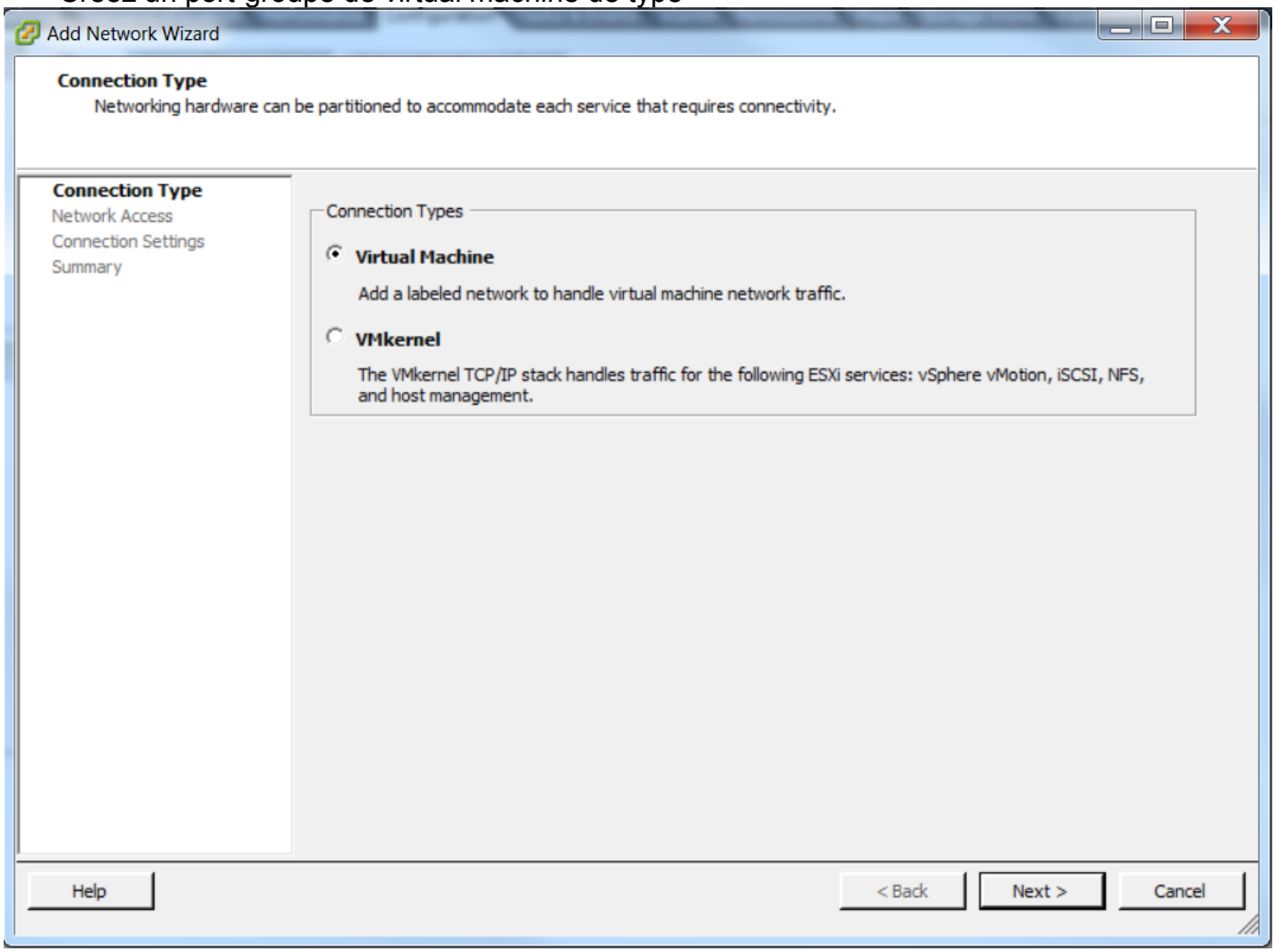
Ces étapes affichent la configuration exigée sur le VMware ESX :

Passez à l'étape 2 directement si vous faites déjà configurer un port-groupe.

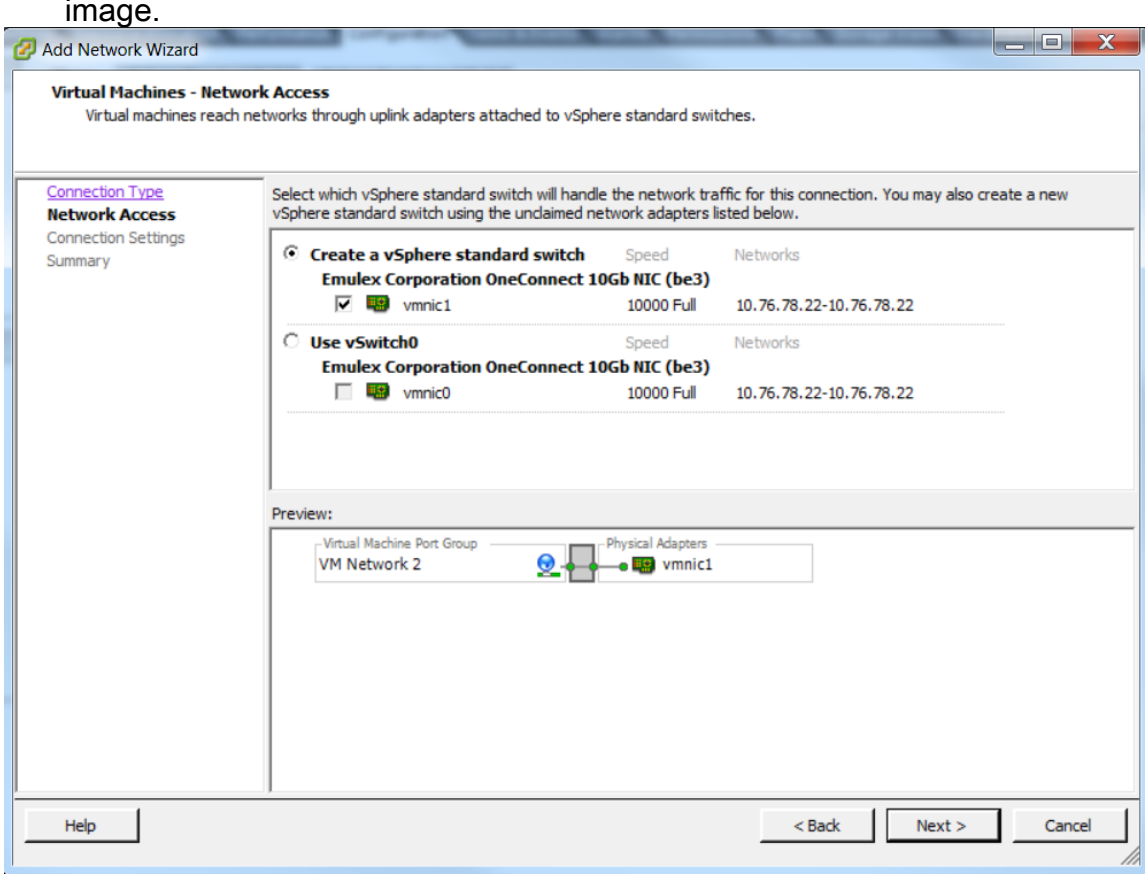
1. Créez un port-groupe de virtual machine et assignez-les deux virtual machine lui

- Naviguez vers l'**onglet Mise en réseau** et cliquez sur Add le **réseau sous le commutateur de norme de vSphere**

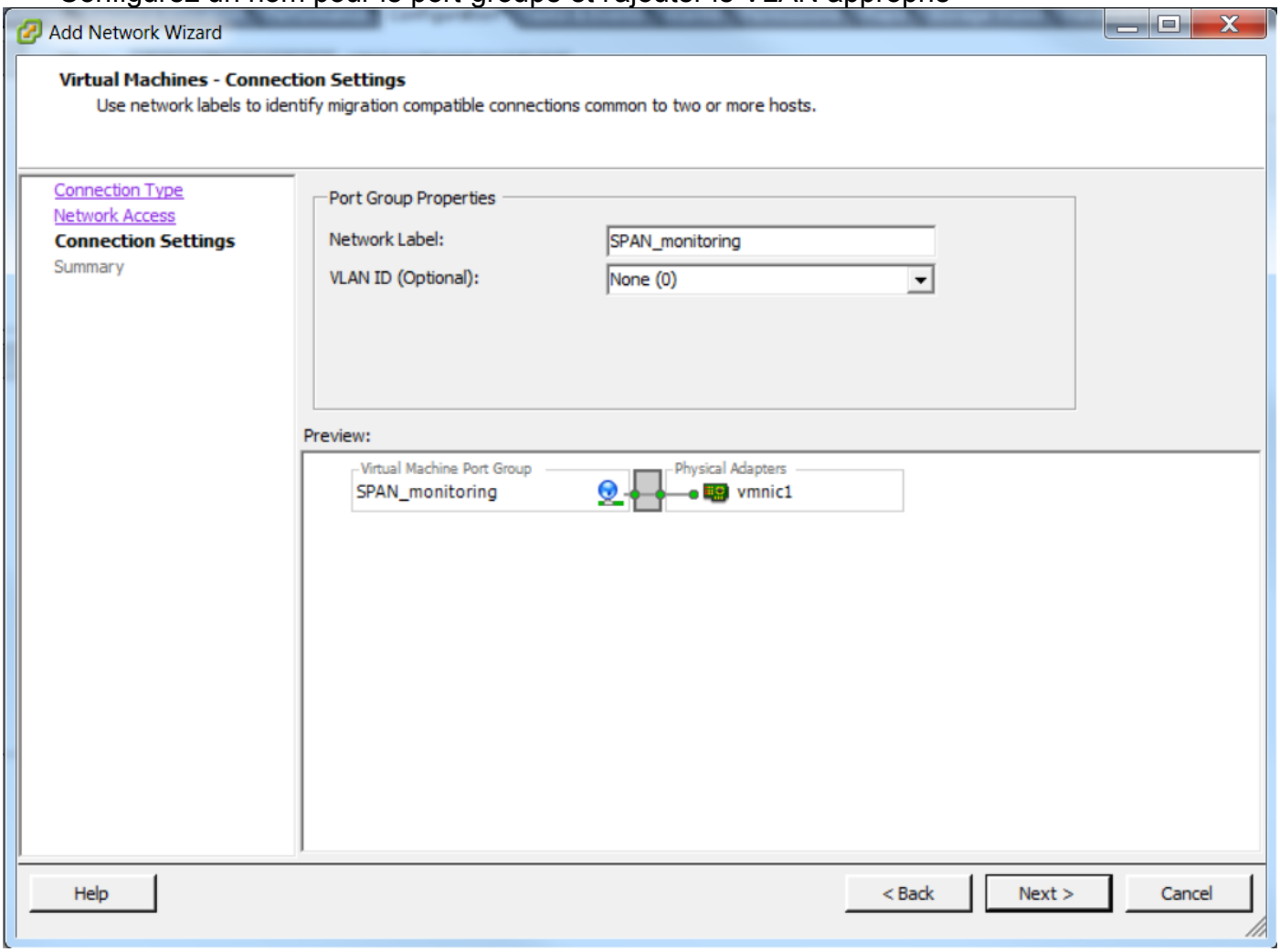
- Créez un port-groupe de virtual machine de type



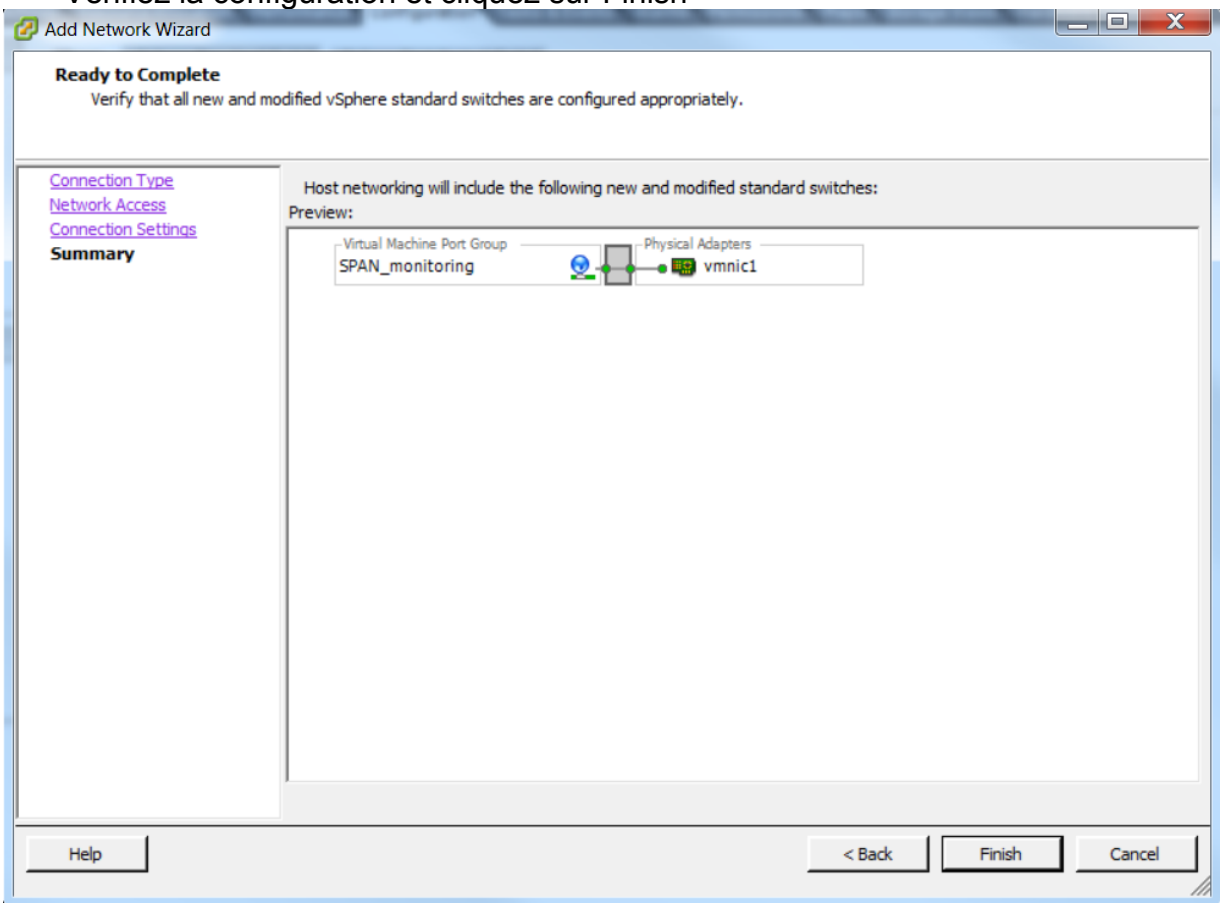
- Assignez une interface physique (vmnic) au port-groupe suivant les indications de cette image.



- Configurez un nom pour le port-groupe et l'ajouter le VLAN approprié



- Vérifiez la configuration et cliquez sur Finish

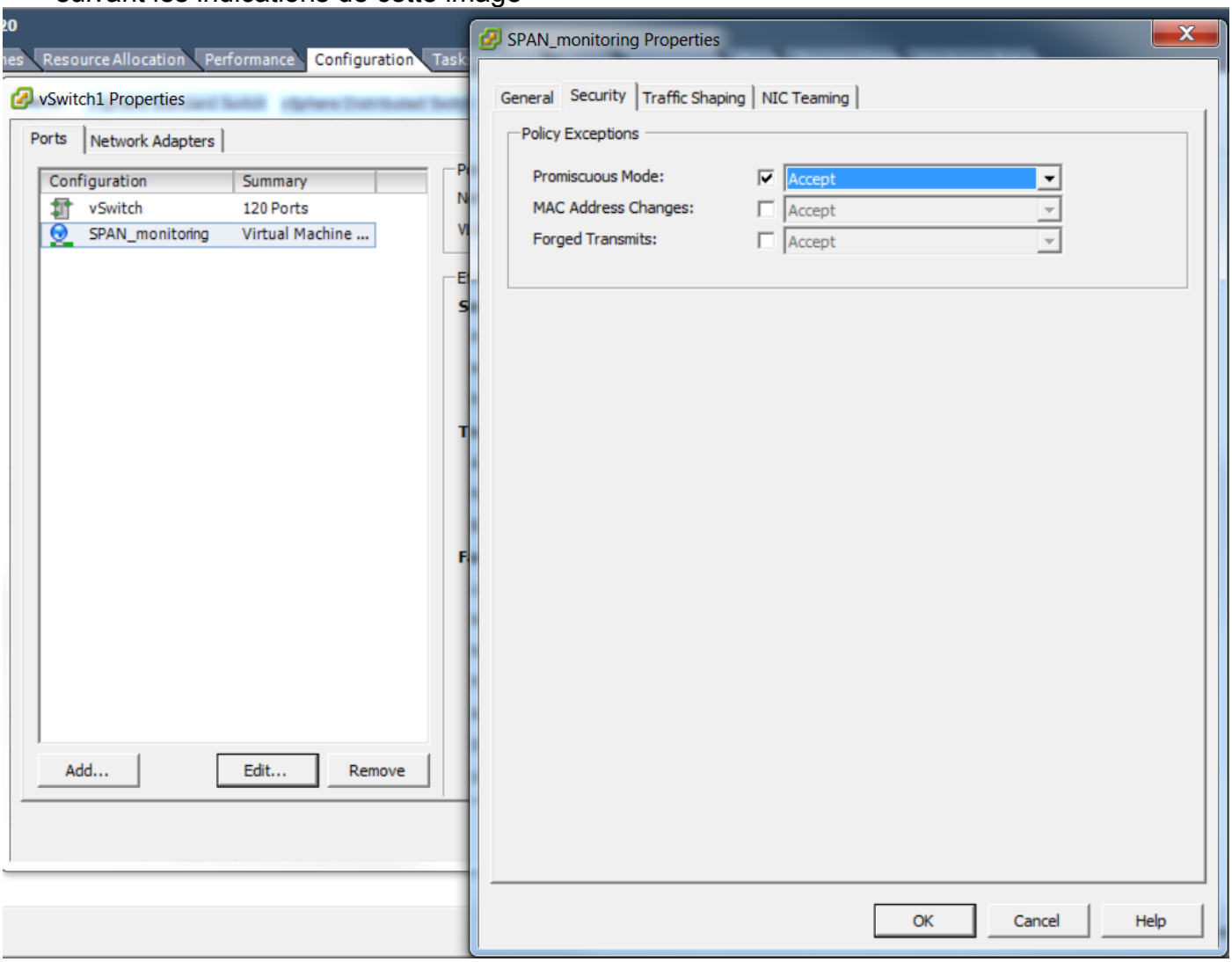


2. Configurez le port-groupe pour être en mode promiscueux.

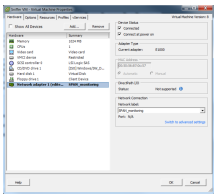
- Le port-groupe doit apparaître sous l'**onglet Mise en réseau** maintenant
- Clic **Properties**

- Sélectionnez le port-groupe et cliquez sur Edit

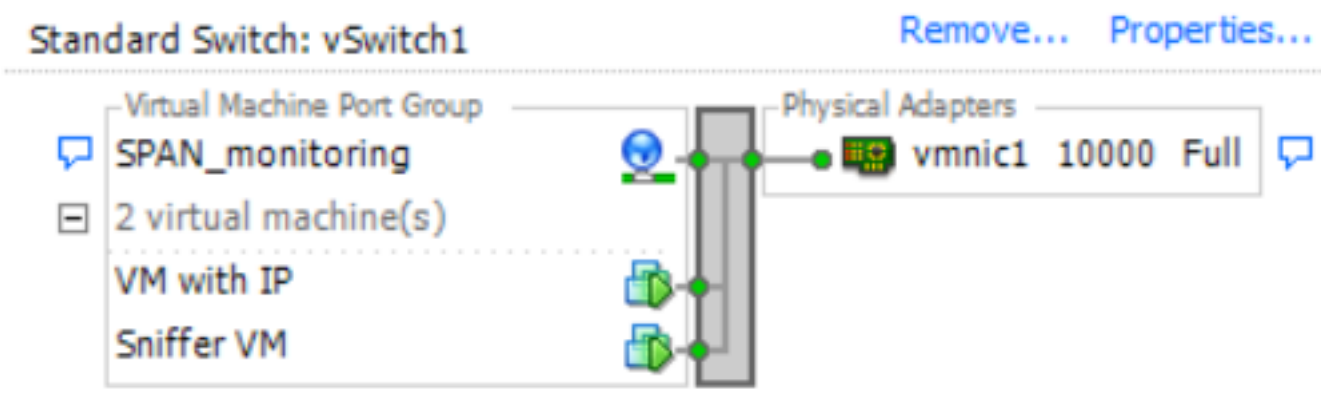
- Allez à l'**onglet Sécurité** et changez la configuration promiscueuse de mode pour recevoir suivant les indications de cette image



3. Assignez les deux virtual machine au port-groupe de la section de configurations de virtual machine.



4. Les deux virtual machine doivent apparaître dans le groupe de port sous l'**onglet Mise en réseau** maintenant.



Dans cet exemple, la VM avec l'IP est la deuxième VM qui a une adresse IP et VM de renifleur est la VM avec l'outil de renifleur sans adresse IP.

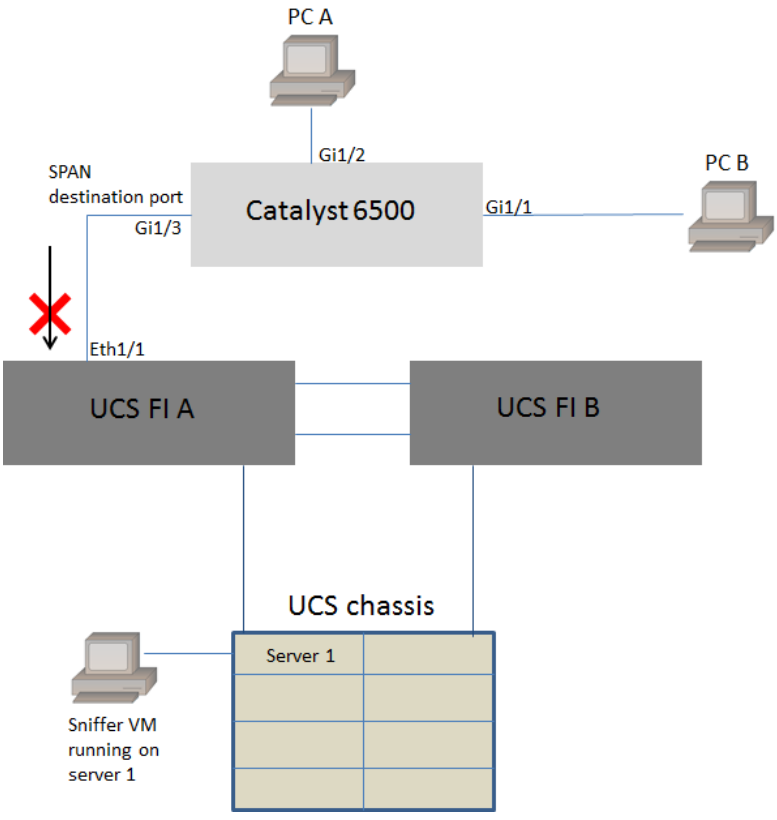
5. Ceci affiche les étapes de configuration sur le commutateur 6500 :

Dans cet exemple, l'adresse IP de la deuxième VM (VM avec l'IP) est 192.0.2.3.

Avec cette configuration, les 6500 encapsule les paquets capturés et les envoie à la VM avec l'adresse IP. Le mode promiscueux sur le vSwitch de VMware permet à la VM de renifleur de voir ces paquets aussi bien.

Scénario de panne

Cette section décrit un scénario de panne commun en utilisant la caractéristique de SPAN local sur un commutateur physique au lieu de la caractéristique ERSPAN. Cette topologie est considérée ici :



Le trafic de PC A à PC B est surveillé utilisant la caractéristique de SPAN local. La destination du trafic d'ENVERGURE est dirigée vers le port connecté à l'UCS Fabric Interconnect (fi).

Le virtual machine avec l'outil de renifleur fonctionne à l'intérieur de l'UCS sur le serveur 1.

C'est la configuration sur le commutateur 6500 :

Tout le trafic circulant sur les ports Gig1/1 et Gig1/2 sera répliqué en fonction pour mettre en communication Gig1/3. L'adresse MAC source et de destination de ces paquets sera inconnue à l'UCS fi.

En mode d'hôte d'extrémité d'Ethernets UCS, le fi relâche ces paquets monodiffusions inconnus.

En mode de commutation Ethernet UCS, le fi apprend l'adresse MAC source sur le port connecté aux 6500 (Eth1/1) et puis inonde les paquets en aval aux serveurs. Cette séquence d'opérations se produisent :

1. Pour la facilité de la compréhension, considérez le trafic allant seulement entre PC A (avec mac-address aaaa.aaaa.aaaa) et PC B (avec mac-address bbbb.bbbb.bbbb) sur les interfaces Gig1/1 et Gig1/2
2. Le premier paquet est de PC A à PC B et ceci est vu sur l'UCS fi Eth1/1
3. Le fi apprend le mac-address aaaa.aaaa.aaaa sur Eth1/1
4. Le fi ne connaît pas le mac-address bbbb.bbbb.bbbb de destination et inonde le paquet à tous les ports dans le même VLAN
5. La VM de renifleur, dans le même VLAN, voient également ce paquet
6. Le paquet suivant est de PC B à PC A
7. Quand ceci frappe Eth1/1, le mac-address bbbb.bbbb.bbbb est appris sur Eth1/1
8. La destination du paquet est pour le mac-address aaaa.aaaa.aaaa
9. Le fi relâche ce paquet pendant que le mac-address aaaa.aaaa.aaaa est appris sur Eth1/1 et le paquet était reçu sur Eth1/1 lui-même
10. Des paquets suivants, destinés pour le mac-address aaaa.aaaa.aaaa ou le mac-address bbbb.bbbb.bbbb sont lâchés pour la même raison

Les informations relatives

- Configurer le mode promiscueux sur un commutateur ou un portgroup virtuel
- ENVERGURE, RSPAN, et ERSPAN sur le Catalyst 6500
- Le trafic du décapsulage ERSPAN avec des outils en source libre
- Support et documentation techniques - Cisco Systems