

# Configuration VLAN privé et Cisco UCS antérieure à 2.2(2C)

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Théorie](#)

[Implémentation PVLAN dans UCS](#)

[Objectif](#)

[Configuration](#)

[Diagrammes du réseau](#)

[PVLAN sur vSwitch : PVLAN isolé avec port fiable sur un périphérique en amont](#)

[Configuration dans UCS](#)

[Configuration des périphériques en amont](#)

[Dépannage](#)

[PVLAN isolé sur N1K avec port discret sur un périphérique en amont](#)

[Configuration dans UCS](#)

[Configuration des périphériques en amont](#)

[Configuration de N1K](#)

[Dépannage](#)

[PVLAN isolé sur N1K avec port de promiscuité sur le profil de port de liaison ascendante N1K](#)

[Configuration dans UCS](#)

[Configuration des périphériques en amont](#)

[Configuration de N1K](#)

[Dépannage](#)

[PVLAN de communauté sur N1K avec port de promiscuité sur le profil de port de liaison ascendante N1K](#)

[Dépannage](#)

[PVLAN isolé et PVLAN de communauté sur le port promotionnel DVS VMware sur le DVS](#)

[Vérification](#)

[Dépannage](#)

## Introduction

Ce document décrit la prise en charge des VLAN privés (PVLAN) dans Cisco Unified Computing System (UCS), une fonctionnalité introduite dans la version 1.4 de Cisco UCS Manager (UCSM). Il détaille également les fonctionnalités, les mises en garde et la configuration lorsque des PVLAN sont utilisés dans un environnement UCS.

**CE DOCUMENT EST À UTILISER AVEC UCSM VERSION 2.2(2C) ET LES VERSIONS**

**ANTÉRIEURES.** Dans les versions ultérieures à la version 2.2(2C), des modifications ont été apportées à UCSM et ESXi DVS est pris en charge. Il y a également des changements dans le fonctionnement du marquage pour la carte réseau PVLAN.

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- UCS
- Cisco Nexus 1000 V (N1K)
- VMware
- Commutation de couche 2 (L2)

### Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Informations générales

### Théorie

Un VLAN privé est un VLAN configuré pour l'isolation de couche 2 par rapport aux autres ports du même VLAN privé. Les ports qui appartiennent à un PVLAN sont associés à un ensemble commun de VLAN de support, qui sont utilisés pour créer la structure PVLAN.

Il y a trois types de ports PVLAN :

- Un **port proche** communique avec tous les autres ports PVLAN et est le port utilisé afin de communiquer avec des périphériques en dehors du PVLAN.
- Un **port isolé** a une séparation L2 complète (y compris les diffusions) des autres ports du même PVLAN, à l'exception du port proche.
- Un **port de communauté** peut communiquer avec d'autres ports du même PVLAN ainsi qu'avec le port proche. Les ports communautaires sont isolés au niveau de L2 à partir de ports d'autres communautés ou de ports PVLAN isolés. Les diffusions ne sont propagées qu'à d'autres ports de la communauté et du port proche.

Référez-vous à [RFC 5517, VLAN privés de Cisco Systems : Sécurité évolutive dans un environnement multiclient](#) afin de comprendre la théorie, le fonctionnement et les concepts des PVLAN.

### Implémentation PVLAN dans UCS

UCS ressemble de près à l'architecture Nexus 5000/2000, où le Nexus 5000 est analogue à l'UCS 6100 et le Nexus 2000 aux extenseurs de fabric UCS 2104.

De nombreuses limitations de la fonctionnalité PVLAN dans UCS sont causées par les limitations trouvées dans l'implémentation Nexus 5000/2000.

Points importants à retenir :

- Seuls les ports isolés sont pris en charge dans UCS. Avec N1K incorporé, vous pouvez utiliser des VLAN de communauté, mais le port de promiscuité doit également se trouver sur N1K.
- Il n'existe aucune prise en charge pour les ports/agrégations proches, les ports/agrégations communautaires ou les agrégations isolées.
- Les ports fiables doivent se trouver en dehors du domaine UCS, par exemple un commutateur/routeur en amont ou un N1K en aval.

## Objectif

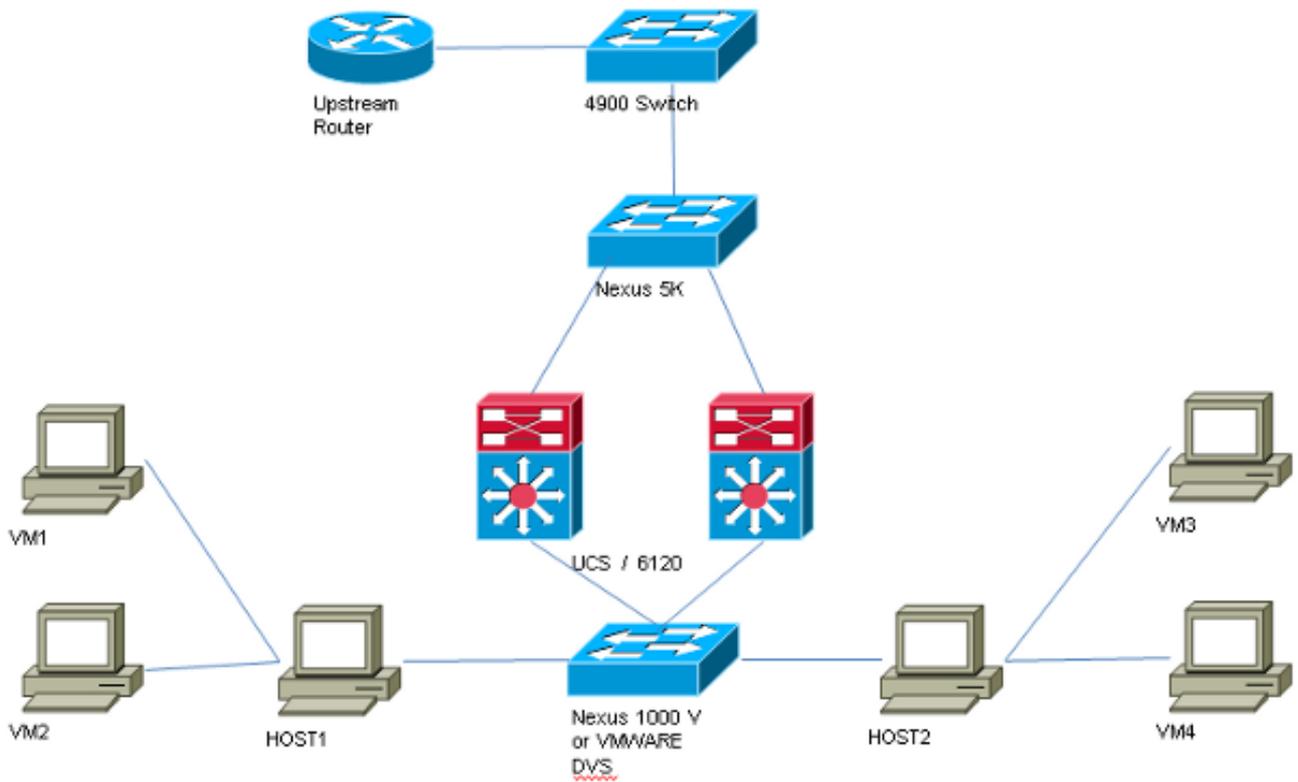
Ce document couvre plusieurs configurations différentes disponibles pour PVLAN avec UCS :

1. PVLAN isolé avec port proche sur un périphérique en amont.
2. PVLAN isolé sur N1K avec port proche sur un périphérique en amont.
3. PVLAN isolé sur N1K avec port proche sur le profil de port de liaison ascendante N1K
4. PVLAN de communauté sur N1K avec port proche sur le profil de port de liaison ascendante N1K.
5. PVLAN isolé sur le port de promiscuité du commutateur virtuel distribué (DVS) VMware sur le DVS.
6. PVLAN de communauté sur le port de promiscuité du commutateur DVS VMware sur le DVS.

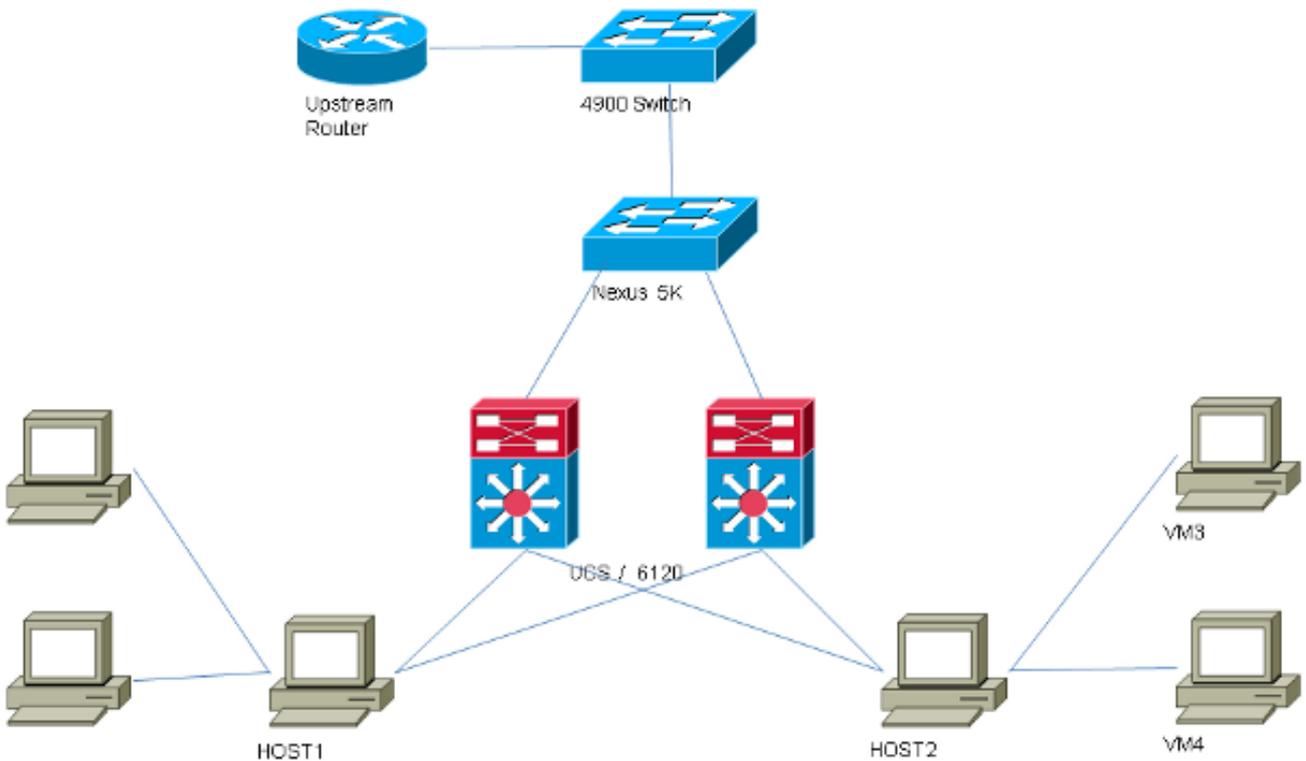
## Configuration

### Diagrammes du réseau

La topologie de tous les exemples avec un commutateur distribué est la suivante :



La topologie de tous les exemples sans commutateur distribué est la suivante :



### PVLAN sur vSwitch : PVLAN isolé avec port fiable sur un périphérique en amont

Dans cette configuration, vous transmettez le trafic PVLAN via UCS à un port proche qui est en amont. Étant donné que vous ne pouvez pas envoyer à la fois les VLAN principal et secondaire

sur la même vNIC, vous avez besoin d'une vNIC pour chaque lame pour chaque PVLAN, afin de transporter le trafic PVLAN.

## Configuration dans UCS

Cette procédure décrit comment créer les VLAN principaux et les VLAN isolés.

**Note:** Cet exemple utilise 266 comme principal et 166 comme isolé ; les ID de VLAN seront déterminés par le site.

1. Afin de créer le VLAN principal, cliquez sur **Principal** comme Type de partage, et entrez un ID de VLAN de 266 :

The screenshot shows the configuration interface for a VLAN. The 'Properties' section is at the top, and the 'Secondary VLANs' section is below it.

**Properties**

Name: **266**      VLAN ID:

Native VLAN: **No**      Fabric ID: **Dual**

Network Type: **Lan**      If Type: **Virtual**

Locale: **External**      Transport Type: **Ether**

Multicast Policy Name:      

Multicast Policy Instance: [org-root/mc-policy-default](#)

Sharing Type:  None  Primary  Isolated

**Secondary VLANs**

Filter | Export | Print

Name	ID	Type	Transport	Native	VLAN Sharing
166	166	Lan	Ether	No	Isolated

2. Afin de créer le VLAN isolé, cliquez sur **Isolé** comme Type de partage, entrez un ID de VLAN de 166, et choisissez **VLAN 266 (266)** comme VLAN principal :



Seul le VLAN isolé est ajouté, il doit être défini comme principal et il ne peut y en avoir qu'un pour chaque vNIC. Comme le VLAN natif est défini ici, ne configurez pas l'étiquetage VLAN sur les groupes de ports VMware.

## Configuration des périphériques en amont

Ces procédures décrivent comment configurer un Nexus 5K pour passer le PVLAN à un commutateur 4900 en amont où se trouve le port proche. Bien que cela ne soit pas nécessaire dans tous les environnements, utilisez cette configuration au cas où vous deviez passer le PVLAN par un autre commutateur.

Sur le Nexus 5K, entrez ces commandes et vérifiez la configuration de la liaison ascendante :

1. Activer la fonctionnalité PVLAN :

```
Nexus5000-5(config)# feature private-vlan
```

2. Ajoutez les VLAN comme principaux et isolés :

```
Nexus5000-5(config)# vlan 166
Nexus5000-5(config-vlan)# private-vlan isolated
Nexus5000-5(config-vlan)# vlan 266
Nexus5000-5(config-vlan)# private-vlan primary
```

3. Associez le VLAN 266 au VLAN 166 isolé :

```
Nexus5000-5(config-vlan)# private-vlan association 166
```

4. Assurez-vous que toutes les liaisons ascendantes sont configurées afin d'agrégier les VLAN :

```
interface Ethernet1/1description Connexion au 4900switchport mode trunkvitesse
1000interface Ethernet1/3description Connexion au port FIB 5switchport mode trunkvitesse
1000interface Ethernet1/4description Connexion au port FIA 5switchport mode trunkvitesse
1000
```

Sur le commutateur 4900, procédez comme suit et configurez le port de promiscuité. Le PVLAN se termine par le port proche.

1. Activez la fonction PVLAN si nécessaire.
2. Créez et associez les VLAN comme sur le Nexus 5K.
3. Créez le port proche sur le port de sortie du commutateur 4900. À partir de ce point, les paquets du VLAN 166 sont vus sur le VLAN 266 dans ce cas.

```
Switch(config-if)#switchport mode trunk
switchport private-vlan mapping 266 166
switchport mode private-vlan promiscuous
```

Sur le routeur en amont, créez une sous-interface pour le VLAN 266 uniquement. À ce niveau, les exigences dépendent de la configuration réseau que vous utilisez :

1. interface GigabitEthernet0/1.1

2. encapsulation dot1Q 266
3. Adresse IP 209.165.200.225 255.255.255.224

## Dépannage

Cette procédure décrit comment tester la configuration.

1. Configurez l'interface virtuelle du commutateur (SVI) sur chaque commutateur, ce qui vous permet d'envoyer une requête ping à l'interface SVI à partir du PVLAN :

```
(config)# interface vlan 266
(config-if)# ip address 209.165.200.225 255.255.255.224
(config-if)# private-vlan mapping 166
(config-if)# no shut
```

2. Vérifiez les tables d'adresses MAC afin de voir où votre adresse MAC est apprise. Sur tous les commutateurs, l'adresse MAC doit se trouver dans le VLAN isolé, sauf sur le commutateur avec le port proche. Sur le commutateur proche, notez que l'adresse MAC se trouve dans le VLAN principal.

Sur l'interconnexion de fabric, l'adresse MAC 0050.56bd.7bef est apprise sur Veth1491 :

```
14.17.154.200 - PuTTY
F340-31-9-1-B(nxos)# show mac address-table
Legend:
  * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
  age - seconds since last seen,+ - primary entry using vPC Peer-Link
  VLAN      MAC Address      Type      age      Secure  NTFY      Ports
-----+-----+-----+-----+-----+-----+-----
* 166      000c.29d2.495a    dynamic   80       F       F       Veth1491
* 166      0025.b581.991e    static    0        F       F       Veth1491
* 166      0050.56bd.7bef    dynamic   20       F       F       Veth1491
* 266      0025.b581.9a9d    static    0        F       F       Veth1475
* 266      0050.56bd.53b6    dynamic   170      F       F       Veth1475
* 177      000c.29d2.4950    dynamic   10       F       F       Veth1480
* 177      0025.b581.9a3f    dynamic   10       F       F       Veth1402
* 177      0025.b581.9a4d    dynamic   10       F       F       Veth1480
* 177      0025.b585.100a    dynamic   980     F       F       Veth1424
* 177      0050.566b.01ad    dynamic   980     F       F       Veth1402
* 177      0050.566c.d835    dynamic   10       F       F       Veth1472
* 126      0025.b581.999e    static    0        F       F       Veth1392
* 124      0023.04c6.dbe2    dynamic   10       F       F       Veth1404
* 124      0023.04c6.dbe3    static    0        F       F       Veth1404
* 4044     0024.971f.6bc2    dynamic   0        F       F       Eth2/1/9
* 4044     0026.5108.0b2c    dynamic   0        F       F       Eth1/1/9
* 4044     0026.5108.cac2    dynamic   0        F       F       Eth1/1/9
--More--
```

Sur le Nexus 5K, l'adresse MAC 0050.56bd.7bef est apprise sur Eth1/4 :

```

F340-11-12-COMM.cisco.com - PuTTY
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
F340.11.13-Nexus5000-5# show mac
mac          mac-list
F340.11.13-Nexus5000-5# show mac
mac          mac-list
F340.11.13-Nexus5000-5# show mac address-table
Legend:
      * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
      age - seconds since last seen,+ - primary entry using vPC Peer-Link
-----+-----+-----+-----+-----+-----+-----+
VLAN    MAC Address          Type         age      Secure NTFY   Ports
-----+-----+-----+-----+-----+-----+
* 266   0050.56aa.0a63       dynamic      260      F      F      Eth1/3
* 266   0050.56bd.53b6       dynamic      10       F      F      Eth1/4
* 166   000c.29d2.495a       dynamic      160      F      F      Eth1/4
* 166   0050.56bd.6fd2       dynamic      100      F      F      Eth1/3
* 166   0050.56bd.7bef       dynamic      60       F      F      Eth1/4
F340.11.13-Nexus5000-5#

```

Sur le commutateur 4900, l'adresse MAC 0050.56bd.7bef est apprise sur GigabitEthernet1/1 :

```

F340-11-05-COMM.cisco.com - PuTTY
Unicast Entries
vlan  mac address          type         protocols          port
-----+-----+-----+-----+-----+
266   000c.29d2.495a       dynamic      ip,ipx,assigned,other  GigabitEthernet1/1
266   0050.56bd.53b6       dynamic      ip,ipx,assigned,other  GigabitEthernet1/1
266   0050.56bd.6fd2       dynamic      ip,ipx,assigned,other  GigabitEthernet1/1
266   0050.56bd.7bef       dynamic      ip,ipx,assigned,other  GigabitEthernet1/1
266   c84c.75f6.013f       static       ip,ipx,assigned,other  Switch

Multicast Entries
vlan  mac address          type         ports
-----+-----+-----+-----+
1     0100.0ccc.ccce       system      Gi1/1
1     ffff.ffff.ffff       system      Gi1/1
2     ffff.ffff.ffff       system      Gi1/1
11    ffff.ffff.ffff       system      Gi1/1
12    ffff.ffff.ffff       system      Gi1/1
13    ffff.ffff.ffff       system      Gi1/1
14    ffff.ffff.ffff       system      Gi1/1
15    ffff.ffff.ffff       system      Gi1/1
16    ffff.ffff.ffff       system      Gi1/1
17    ffff.ffff.ffff       system      Gi1/1
18    ffff.ffff.ffff       system      Gi1/1
--More--

```

Dans cette configuration, les systèmes de ce VLAN isolé ne peuvent pas communiquer entre eux, mais peuvent communiquer avec d'autres systèmes via le port proche du commutateur 4900. L'un des problèmes est de configurer les périphériques à vapeur descendante. Dans ce cas, vous utilisez VMware et deux hôtes.

N'oubliez pas que vous devez utiliser une vNIC pour chaque PVLAN. Ces vNIC sont présentées à

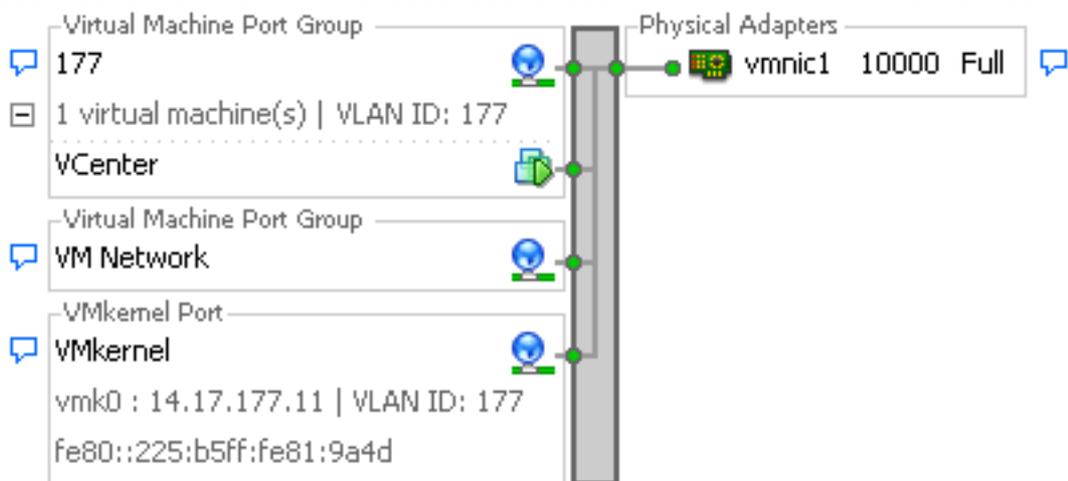
VMware vSphere ESXi. Vous pouvez ensuite créer des groupes de ports et inviter des invités à ces groupes de ports.

Si deux systèmes sont ajoutés au même groupe de ports sur le même commutateur, ils peuvent communiquer entre eux car leurs communications sont commutées localement sur le commutateur virtuel. Dans ce système, il y a deux lames avec deux hôtes chacune.

Sur le premier système, deux groupes de ports différents ont été créés : un appelé 166 et un appelé 166A. Chacune est connectée à une seule carte réseau, qui est configurée dans le VLAN isolé sur UCS. Il n'y a actuellement qu'un seul invité pour chaque groupe de ports. Dans ce cas, comme ils sont séparés sur ESXi, ils ne peuvent pas se parler.

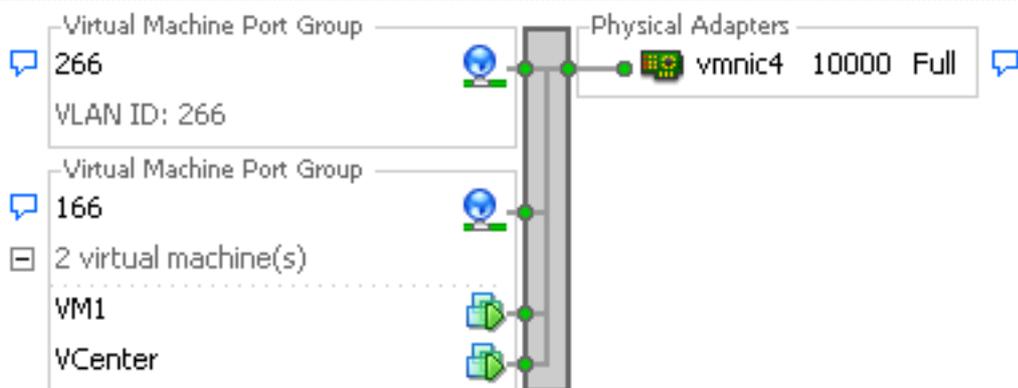
### Standard Switch: vSwitch0

[Remove...](#) [Properties...](#)



### Standard Switch: vSwitch1

[Remove...](#) [Properties...](#)



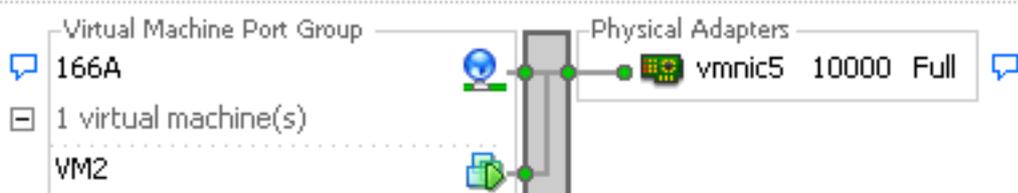
### Standard Switch: vSwitch2

[Remove...](#) [Properties...](#)



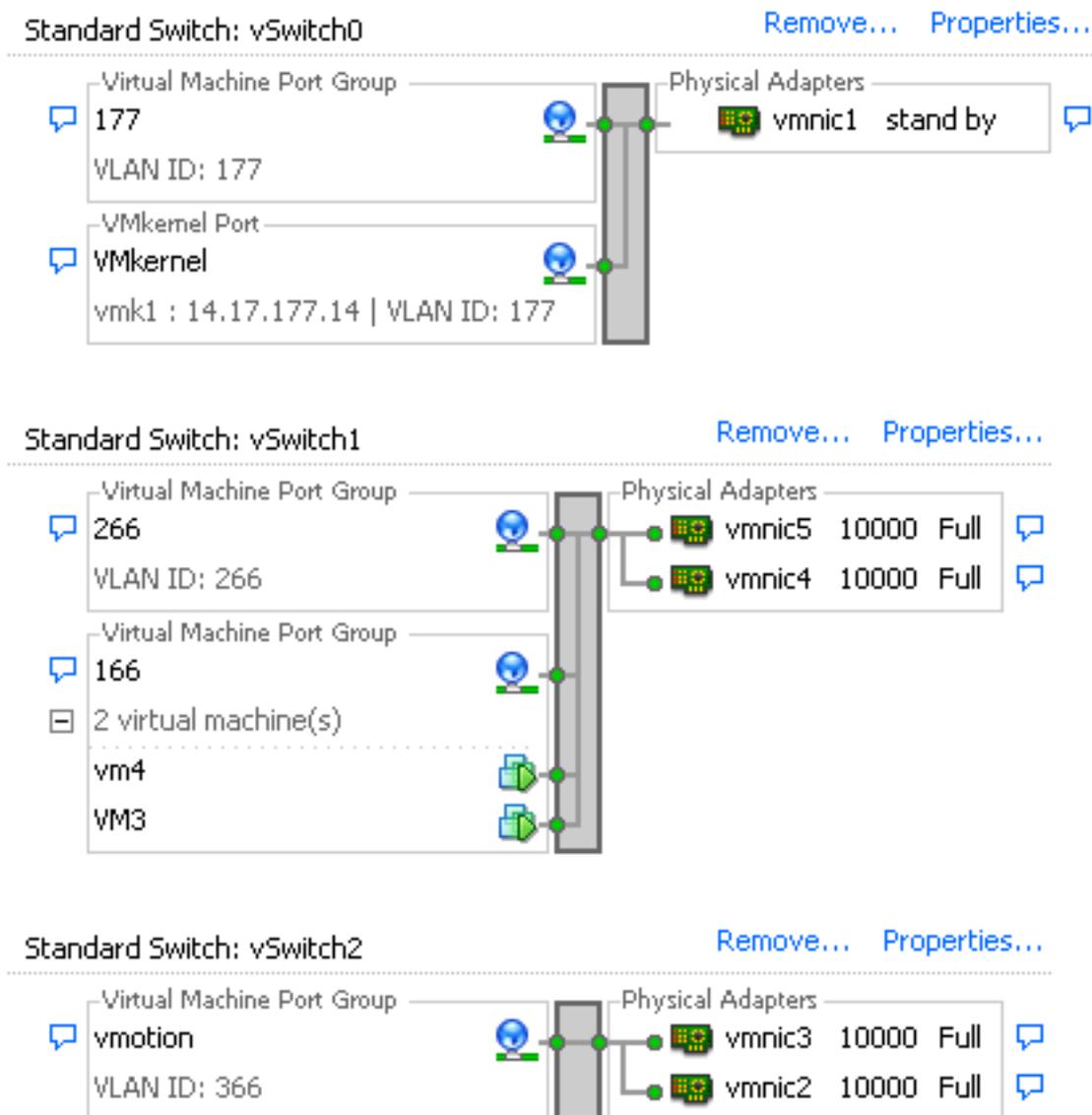
### Standard Switch: vSwitch3

[Remove...](#) [Properties...](#)



Sur le deuxième système, il n'y a qu'un seul groupe de ports appelé 166. Ce groupe de ports compte deux invités. Dans cette configuration, VM3 et VM4 peuvent communiquer entre eux même si vous ne voulez pas que cela se produise. Pour corriger cela, vous devez configurer une seule carte réseau pour chaque machine virtuelle (VM) qui se trouve dans le VLAN isolé, puis créer un groupe de ports attaché à cette vNIC. Une fois configuré, placez un seul invité dans le

groupe de ports. Ce n'est pas un problème avec une installation Windows sans système d'exploitation, car vous n'avez pas ces commutateurs virtuels sous-jacents.



## PVLAN isolé sur N1K avec port discret sur un périphérique en amont

Dans cette configuration, vous transmettez le trafic PVLAN via un N1K, puis l'UCS vers un port proche qui est en amont. Étant donné que vous ne pouvez pas envoyer à la fois les VLAN principal et secondaire sur la même vNIC, vous avez besoin d'une vNIC pour chaque liaison ascendante PVLAN afin de transporter le trafic PVLAN.

### Configuration dans UCS

Cette procédure décrit comment créer les VLAN principaux et les VLAN isolés.

**Note:** Cet exemple utilise 266 comme principal et 166 comme isolé ; les ID de VLAN seront déterminés par le site.



**Properties**

Name: <b>166</b>	VLAN ID: <input type="text" value="166"/>
Native VLAN: <b>No</b>	Fabric ID: <b>Dual</b>
Network Type: <b>Lan</b>	If Type: <b>Virtual</b>
Locale: <b>External</b>	Transport Type: <b>Ether</b>

Sharing Type:  None  Primary  Isolated Primary VLAN:

---

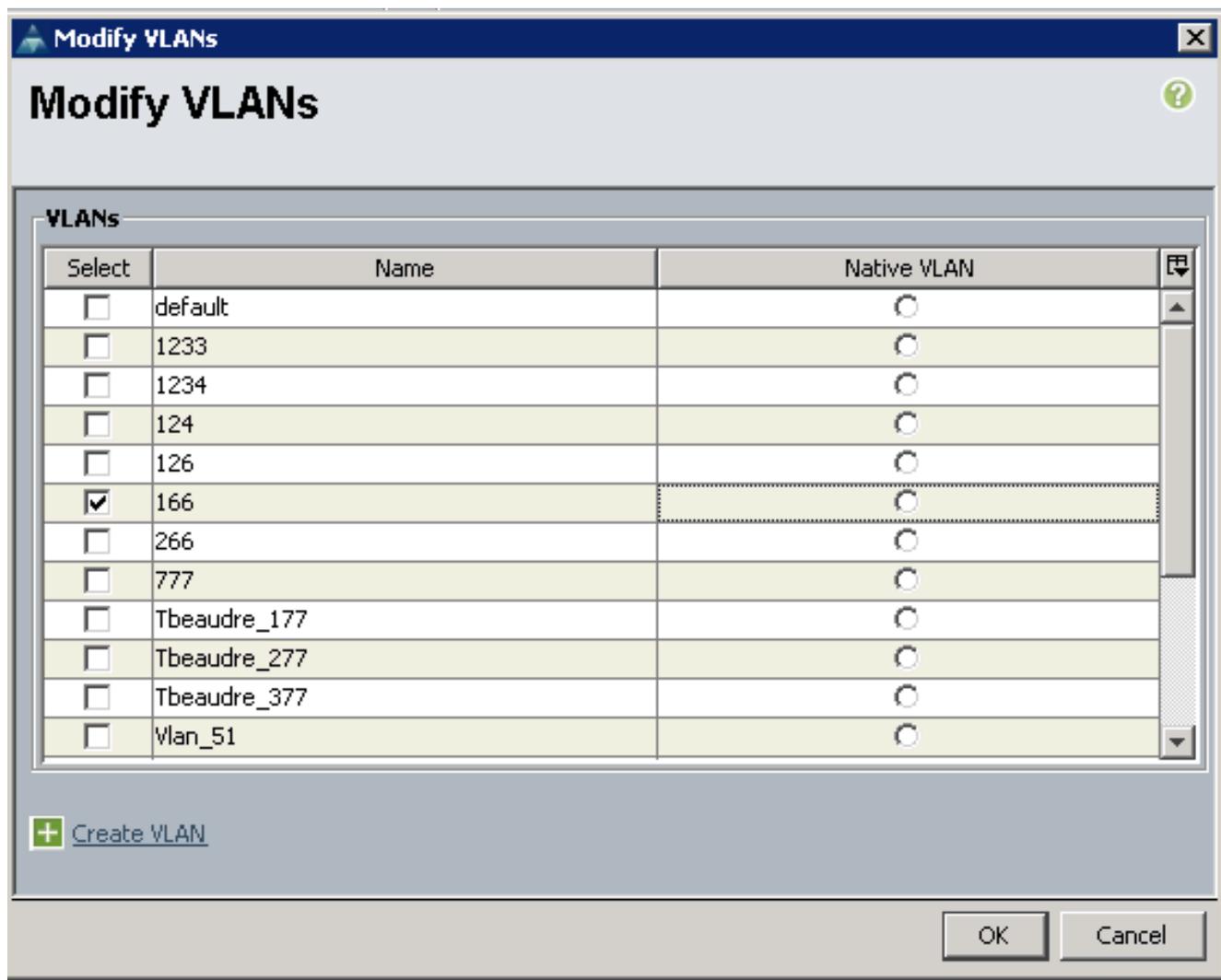
**Primary VLAN Properties**

Name: <b>266</b>	VLAN ID: <b>266</b>
Native VLAN: <b>No</b>	Fabric ID: <b>Dual</b>
Network Type: <b>Lan</b>	If Type: <b>Virtual</b>
Locale: <b>External</b>	Transport Type: <b>Ether</b>

Multicast Policy Name:

Multicast Policy Instance: [org-root/mc-policy-default](#)

- Afin d'ajouter le VLAN à la vNIC, cochez la case **Sélectionner** pour VLAN 166. VLAN 166 n'a pas de VLAN natif sélectionné.



Seul le VLAN isolé est ajouté, il ne doit pas être défini comme natif et il ne peut y en avoir qu'un pour chaque vNIC. Comme le VLAN natif n'est pas défini ici, marquez le VLAN natif sur le N1K. L'option de marquage d'un VLAN natif n'est pas disponible dans le DVS VMware, donc ceci n'est pas pris en charge sur le DVS.

## Configuration des périphériques en amont

Ces procédures décrivent comment configurer un Nexus 5K afin de passer le PVLAN à un commutateur 4900 en amont où se trouve le port proche. Bien que cela ne soit pas nécessaire dans tous les environnements, utilisez cette configuration au cas où vous deviez passer le PVLAN par un autre commutateur.

Sur le Nexus 5K, entrez ces commandes et vérifiez la configuration de la liaison ascendante :

1. Activer la fonctionnalité PVLAN :

```
Nexus5000-5(config)# feature private-vlan
```

2. Ajoutez les VLAN comme principaux et isolés :

```
Nexus5000-5(config)# vlan 166
```

```
Nexus5000-5(config-vlan)# private-vlan isolated
```

```
Nexus5000-5(config-vlan)# vlan 266
Nexus5000-5(config-vlan)# private-vlan primary
```

### 3. Associez le VLAN 266 au VLAN 166 isolé :

```
Nexus5000-5(config-vlan)# private-vlan association 166
```

### 4. Assurez-vous que toutes les liaisons ascendantes sont configurées afin d'agrégier les VLAN :

```
interface Ethernet1/1description Connexion au 4900switchport mode trunkvitesse
1000interface Ethernet1/3description Connexion au port FIB 5switchport mode trunkvitesse
1000interface Ethernet1/4description Connexion au port FIA 5switchport mode trunkvitesse
1000
```

Sur le commutateur 4900, procédez comme suit et configurez le port de promiscuité. Le PVLAN se termine par le port proche.

1. Activez la fonction PVLAN si nécessaire.
2. Créez et associez les VLAN comme sur le Nexus 5K.
3. Créez le port proche sur le port de sortie du commutateur 4900. À partir de ce point, les paquets du VLAN 166 sont vus sur le VLAN 266 dans ce cas.

```
Switch(config-if)#switchport mode trunk
switchport private-vlan mapping 266 166
switchport mode private-vlan promiscuous
```

Sur le routeur en amont, créez une sous-interface pour le VLAN 266 uniquement. À ce niveau, les exigences dépendent de la configuration réseau que vous utilisez :

1. interface GigabitEthernet0/1.1
2. encapsulation dot1Q 266
3. Adresse IP 209.165.200.225 255.255.255.224

## Configuration de N1K

Cette procédure décrit comment configurer la N1K en tant que trunk standard et non en tant que trunk PVLAN.

1. Créez et associez les VLAN comme sur le Nexus 5K. Référez-vous à la section [Configuration des périphériques en amont](#) pour plus d'informations.
2. Créez un profil de port de liaison ascendante pour le trafic PVLAN :

```
Switch(config)#port-profile type ethernet pvlan_uplink
Switch(config-port-prof)# vmware port-group
Switch(config-port-prof)# switchport mode trunk
Switch(config-port-prof)# switchport trunk allowed vlan 166,266
Switch(config-port-prof)# switchport trunk native vlan 266 <-- This is necessary to handle
traffic coming back from the promiscuous port.
Switch(config-port-prof)# channel-group auto mode on mac-pinning
Switch(config-port-prof)# no shut
Switch(config-port-prof)# state enabled
```

3. Créez le groupe de ports pour le VLAN isolé ; créez un port hôte PVLAN avec l'association d'hôte pour les VLAN principaux et isolés :

```

Switch(config)# port-profile type vethernet pvlan_guest
Switch(config-port-prof)# vmware port-group
Switch(config-port-prof)# switchport mode private-vlan host
Switch(config-port-prof)# switchport private-vlan host-association 266 166
Switch(config-port-prof)# no shut
Switch(config-port-prof)# state enabled

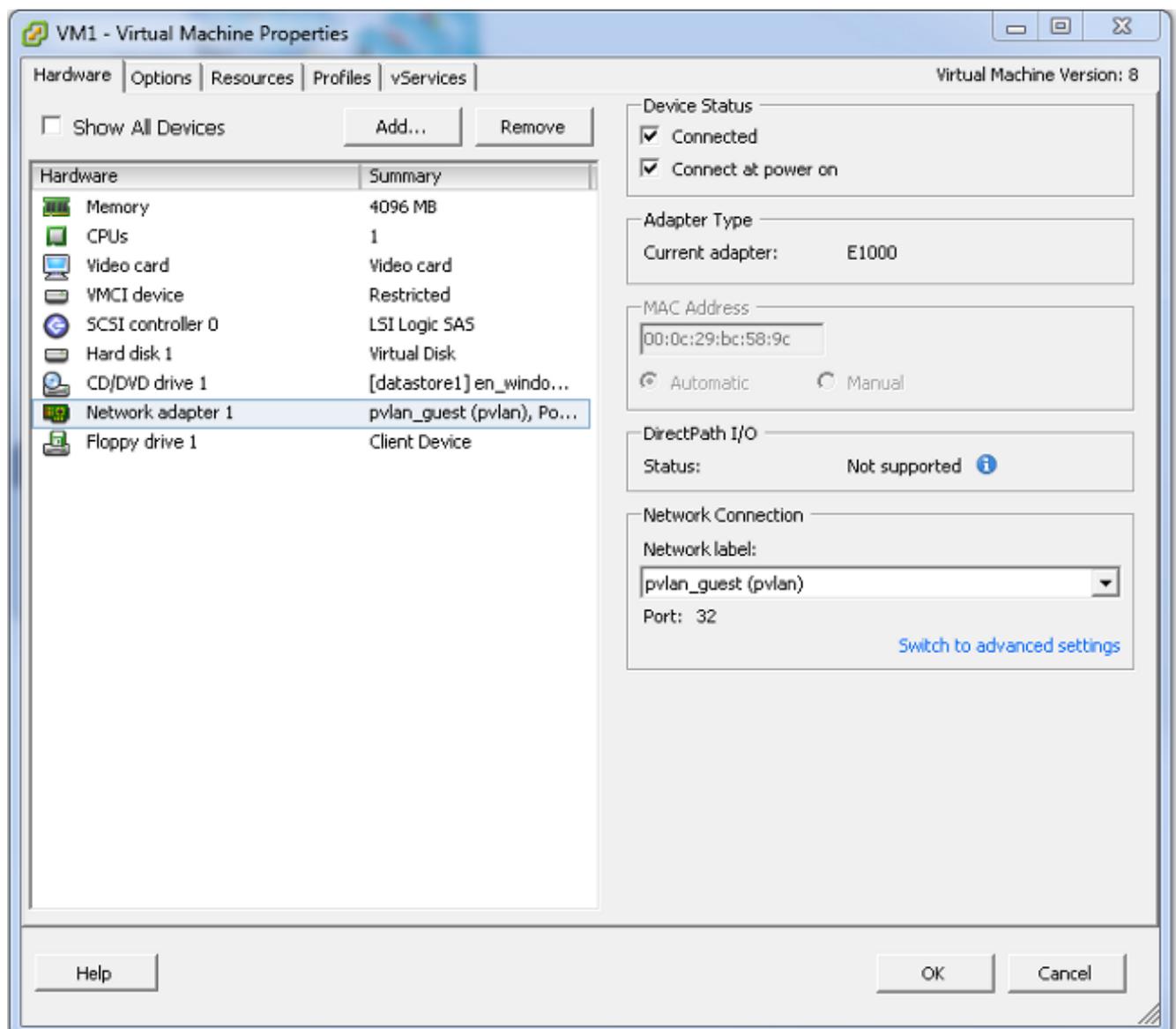
```

4. Dans vCenter, ajoutez la vNIC appropriée à la liaison ascendante PVLAN. Il s'agit de la vNIC à laquelle vous avez ajouté le VLAN isolé sous Configuration dans les paramètres UCS.

<input type="checkbox"/>		vmnic3	--	<a href="#">View Details...</a>	Select an uplink port gr...
<input checked="" type="checkbox"/>		vmnic4	pvlan	<a href="#">View Details...</a>	pvlan_uplink
<input type="checkbox"/>		vmnic5	--	<a href="#">View Details...</a>	Select an uplink port gr...

5. Ajoutez la machine virtuelle au groupe de ports approprié :

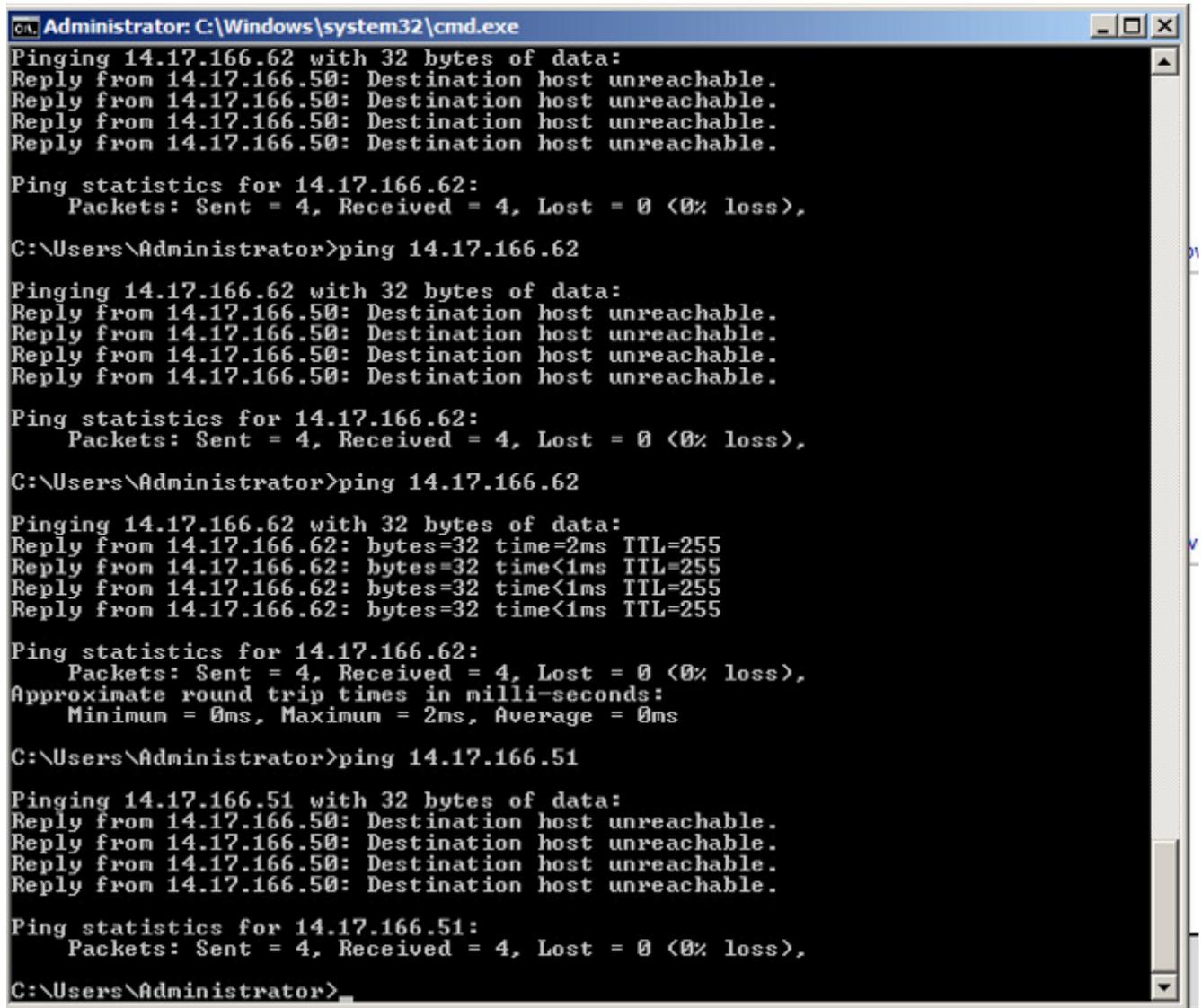
Dans l'onglet Matériel, cliquez sur **Carte réseau 1**. Choisissez **pvlan\_guest (pvlan)** pour l'étiquette Réseau sous Connexion réseau :



## Dépannage

Cette procédure décrit comment tester la configuration.

1. Exécutez des requêtes ping vers d'autres systèmes configurés dans le groupe de ports, ainsi que vers le routeur ou un autre périphérique au niveau du port proche. Les requêtes ping envoyées au périphérique au-delà du port proche doivent fonctionner, tandis que celles envoyées aux autres périphériques du VLAN isolé doivent échouer.



```
C:\Windows\system32\cmd.exe
Pinging 14.17.166.62 with 32 bytes of data:
Reply from 14.17.166.50: Destination host unreachable.

Ping statistics for 14.17.166.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\Administrator>ping 14.17.166.62

Pinging 14.17.166.62 with 32 bytes of data:
Reply from 14.17.166.50: Destination host unreachable.

Ping statistics for 14.17.166.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\Administrator>ping 14.17.166.62

Pinging 14.17.166.62 with 32 bytes of data:
Reply from 14.17.166.62: bytes=32 time=2ms TTL=255
Reply from 14.17.166.62: bytes=32 time<1ms TTL=255
Reply from 14.17.166.62: bytes=32 time<1ms TTL=255
Reply from 14.17.166.62: bytes=32 time<1ms TTL=255

Ping statistics for 14.17.166.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Users\Administrator>ping 14.17.166.51

Pinging 14.17.166.51 with 32 bytes of data:
Reply from 14.17.166.50: Destination host unreachable.

Ping statistics for 14.17.166.51:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\Administrator>
```

2. Sur la N1K, les machines virtuelles sont répertoriées sur le VLAN principal ; cela se produit parce que vous êtes dans des ports hôtes PVLAN qui sont associés au PVLAN. En raison de la manière dont les machines virtuelles sont apprises, assurez-vous de ne pas définir le PVLAN comme natif sur le système UCS. Notez également que vous apprenez le périphérique en amont à partir du canal de port et que le périphérique en amont est également appris sur le VLAN principal. Vous devez l'apprendre dans cette méthode, c'est pourquoi vous avez le VLAN principal comme VLAN natif sur la liaison ascendante PVLAN.

Dans cette capture d'écran, les deux périphériques sur Veth3 et Veth4 sont les machines virtuelles. Le périphérique sur Po1 est le routeur en amont qui dépasse le port proche.

```

pvlan# show mac address-table
VLAN      MAC Address      Type      Age      Port
-----+-----+-----+-----+-----+-----
1         0002.3d10.b102   static    0        N1KV Internal Port      3
1         0002.3d20.b100   static    0        N1KV Internal Port      3
1         0002.3d30.b102   static    0        N1KV Internal Port      3
1         0002.3d40.0002   static    0        N1KV Internal Port      3
1         0002.3d60.b100   static    0        N1KV Internal Port      3
177       0002.3d20.b102   static    0        N1KV Internal Port      3
177       0002.3d40.b102   static    0        N1KV Internal Port      3
177       0050.5686.4fe8   static    0        Veth2                    3
177       0050.5686.7787   static    0        Veth1                    3
177       0002.3d40.2100   dynamic   3        Po3                      3
177       000c.29c2.d1ba   dynamic   15       Po3                      3
177       0050.5686.3bc0   dynamic   56       Po3                      3
177       0050.56bc.5eea   dynamic   1        Po3                      3
177       0050.56bc.761d   dynamic   1        Po3                      3
266       000c.2996.9a1d   static    0        Veth4                    3
266       000c.29bc.589c   static    0        Veth3                    3
266       0012.8032.86a9   dynamic   214     Po1                      3
Total MAC Addresses: 17
pvlan#

```

3. Sur le système UCS, vous devez apprendre tous les MAC, pour cette communication, dans le VLAN isolé. Vous ne devez pas voir le amont ici :

```

F340-31-9-1-B(nxos)# show mac address-table
Legend:
      * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
      age - seconds since last seen,+ - primary entry using vPC Peer-Link
      VLAN      MAC Address      Type      age      Secure NTFY      Ports
-----+-----+-----+-----+-----+-----
* 166         000c.2996.9a1d   dynamic   10       F      F      Veth1491
* 166         000c.29bc.589c   dynamic   270     F      F      Veth1491
* 166         0025.b581.991e   static    0        F      F      Veth1491

```

4. Sur le Nexus 5K, les deux machines virtuelles se trouvent sur le VLAN isolé, tandis que le périphérique en amont se trouve sur le VLAN principal :

```

F340.11.13-Nexus5000-5# show mac address-table
Legend:
      * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
      age - seconds since last seen,+ - primary entry using vPC Peer-Link
      VLAN      MAC Address      Type      age      Secure NTFY      Ports
-----+-----+-----+-----+-----+-----
* 266         0012.8032.86a9   dynamic    0        F      F      Eth1/1
* 166         000c.2996.9a1d   dynamic   40       F      F      Eth1/4
* 166         000c.29bc.589c   dynamic   60       F      F      Eth1/4

```

5. Sur le commutateur 4900, où se trouve le port proche, tout se trouve sur le VLAN principal :

```

Unicast Entries
vlan      mac address      type      protocols      port
-----+-----+-----+-----+-----
266      000c.2996.9a1d   dynamic  ip,ipx,assigned,other  GigabitEthernet1/1
266      000c.29bc.589c   dynamic  ip,ipx,assigned,other  GigabitEthernet1/1
266      0012.8032.86a9   dynamic  ip,ipx,assigned,other  GigabitEthernet1/2

Multicast Entries
vlan      mac address      type      ports
-----+-----+-----+-----
1         0100.0ccc.cccc   system   Gi1/1
1         ffff.ffff.ffff   system   Gi1/1
266      ffff.ffff.ffff   system   Gi1/1,Gi1/2

```

## PVLAN isolé sur N1K avec port de promiscuité sur le profil de port de liaison ascendante N1K

Dans cette configuration, vous contenez le trafic PVLAN vers N1K avec uniquement le VLAN principal utilisé en amont.

### Configuration dans UCS

Cette procédure décrit comment ajouter le VLAN principal à la vNIC. Il n'est pas nécessaire de configurer PVLAN car vous n'avez besoin que du VLAN principal.

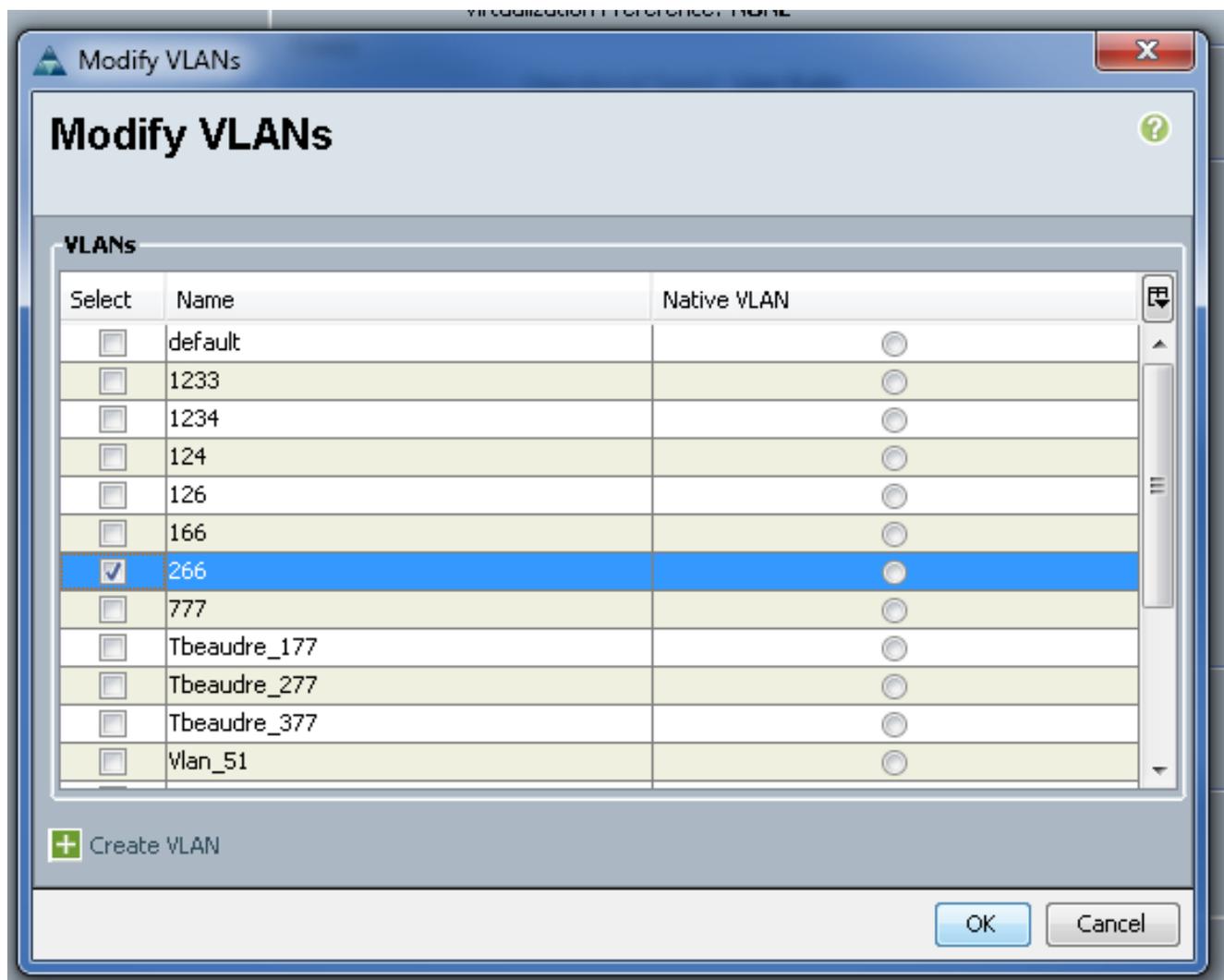
**Note:** Cet exemple utilise 266 comme principal et 166 comme isolé ; les ID de VLAN seront déterminés par le site.

1. Notez que le type de partage est **Aucun**.

The screenshot shows the configuration page for VLAN 266 in the UCS management interface. The 'Properties' section is expanded, showing the following settings:

- Name: 266
- VLAN ID: 266
- Native VLAN: No
- Fabric ID: Dual
- Network Type: Lan
- If Type: Virtual
- Locale: External
- Transport Type: Ether
- Multicast Policy Name: <not set>
- Multicast Policy Instance: org-root/mc-policy-default
- Sharing Type:  None  Primary  Isolated

2. Cochez la case **Sélectionner** pour VLAN 266 afin d'ajouter le VLAN principal à la vNIC. Ne le définissez pas en tant que Native.



## Configuration des périphériques en amont

Ces procédures décrivent comment configurer les périphériques en amont. Dans ce cas, les commutateurs en amont n'ont besoin que de ports agrégés et ils n'ont besoin que de trunk VLAN 266, car il s'agit du seul VLAN que les commutateurs en amont voient.

Sur le Nexus 5K, entrez ces commandes et vérifiez la configuration de la liaison ascendante :

1. Ajoutez le VLAN en tant que VLAN principal :

```
Nexus5000-5(config-vlan)# vlan 266
```

2. Assurez-vous que toutes les liaisons ascendantes sont configurées afin d'agréger les VLAN :

```
interface Ethernet1/1description Connexion au 4900switchport mode trunkvitesse
1000interface Ethernet1/3description Connexion au port FIB 5switchport mode trunkvitesse
1000interface Ethernet1/4description Connexion au port FIA 5switchport mode trunkvitesse
1000
```

Sur le commutateur 4900, procédez comme suit :

1. Créez les VLAN utilisés comme VLAN principaux sur N1K.
2. Agrégation de toutes les interfaces vers et depuis le commutateur 4900 afin que le VLAN soit transmis.

Sur le routeur en amont, créez une sous-interface pour le VLAN 266 uniquement. À ce niveau, les exigences dépendent de la configuration réseau que vous utilisez.

1. interface GigabitEthernet0/1.1
2. encapsulation dot1Q 266
3. Adresse IP 209.165.200.225 255.255.255.224

## Configuration de N1K

Cette procédure décrit comment configurer le N1K.

1. Créer et associer les VLAN :

```
Switch(config)# vlan 166
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# vlan 266
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# private-vlan association 166
```

2. Créez un profil de port de liaison ascendante pour le trafic PVLAN avec le port proche noté :

```
Switch(config)#port-profile type ethernet pvlan_uplink
Switch(config-port-prof)# vmware port-group
Switch(config-port-prof)# switchport mode private-vlan trunk promiscuous
Switch(config-port-prof)# switchport private-vlan trunk allowed vlan 266 <-- Only need to
allow the primary VLAN
Switch(config-port-prof)# switchport private-vlan mapping trunk 266 166 <-- The VLANs must
be mapped at this point
Switch(config-port-prof)# channel-group auto mode on mac-pinning
Switch(config-port-prof)# no shut
Switch(config-port-prof)# state enabled
```

3. Créez le groupe de ports pour le VLAN isolé ; créez un port hôte PVLAN avec l'association d'hôte pour les VLAN principaux et isolés :

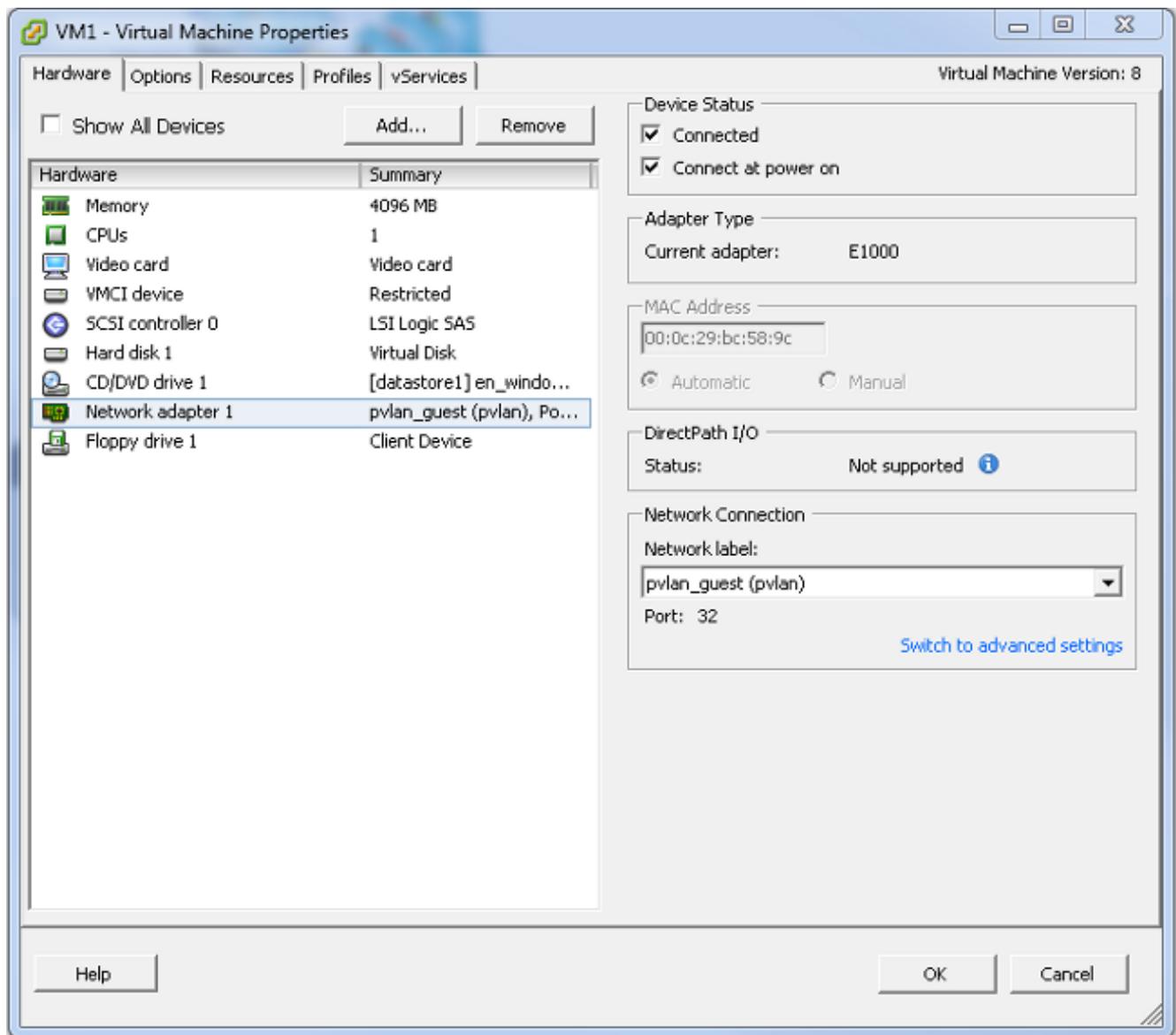
```
Switch(config)# port-profile type vethernet pvlan_guest
Switch(config-port-prof)# vmware port-group
Switch(config-port-prof)# switchport mode private-vlan host
Switch(config-port-prof)# switchport private-vlan host-association 266 166
Switch(config-port-prof)# no shut
Switch(config-port-prof)# state enabled
```

4. Dans vCenter, ajoutez la vNIC appropriée à la liaison ascendante PVLAN. Il s'agit de la vNIC à laquelle vous avez ajouté le VLAN isolé sous Configuration dans les paramètres UCS.

<input type="checkbox"/>	 vmnic3	--	<a href="#">View Details...</a>	Select an uplink port gr...
<input checked="" type="checkbox"/>	 vmnic4	pvlan	<a href="#">View Details...</a>	pvlan_uplink
<input type="checkbox"/>	 vmnic5	--	<a href="#">View Details...</a>	Select an uplink port gr...

5. Ajoutez la machine virtuelle au groupe de ports approprié.

Dans l'onglet Matériel, cliquez sur **Carte réseau 1**. Choisissez **pvlan\_guest (pvlan)** pour l'étiquette Réseau sous Connexion réseau.



## Dépannage

Cette procédure décrit comment tester la configuration.

1. Exécutez des requêtes ping vers d'autres systèmes configurés dans le groupe de ports, ainsi que vers le routeur ou un autre périphérique au niveau du port proche. Les requêtes ping envoyées au périphérique au-delà du port proche doivent fonctionner, tandis que celles envoyées aux autres périphériques du VLAN isolé doivent échouer.

```

Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ping 14.17.166.61
Pinging 14.17.166.61 with 32 bytes of data:
Reply from 14.17.166.61: bytes=32 time<1ms TTL=255
Reply from 14.17.166.61: bytes=32 time<1ms TTL=255

Ping statistics for 14.17.166.61:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\Administrator>ping 14.17.166.51
Pinging 14.17.166.51 with 32 bytes of data:
Reply from 14.17.166.50: Destination host unreachable.

Ping statistics for 14.17.166.51:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
C:\Users\Administrator>_

```

- Sur la N1K, les machines virtuelles sont répertoriées sur le VLAN principal ; cela se produit parce que vous êtes dans des ports hôtes PVLAN qui sont associés au PVLAN. Notez également que vous apprenez le périphérique en amont à partir du canal de port et que le périphérique en amont est également appris sur le VLAN principal.

Dans cette capture d'écran, les deux périphériques sur Veth3 et Veth4 sont les machines virtuelles. Le périphérique sur Po1 est le périphérique en amont qui dépasse le port proche.

```

pvlan(config-port-prof)# show mac address-table
VLAN      MAC Address      Type      Age      Port      Mod
-----+-----+-----+-----+-----+-----
1         0002.3d10.b102   static    0        N1KV Internal Port  3
1         0002.3d20.b100   static    0        N1KV Internal Port  3
1         0002.3d30.b102   static    0        N1KV Internal Port  3
1         0002.3d40.0002   static    0        N1KV Internal Port  3
1         0002.3d60.b100   static    0        N1KV Internal Port  3
177       0002.3d20.b102   static    0        N1KV Internal Port  3
177       0002.3d40.b102   static    0        N1KV Internal Port  3
177       0050.5686.4fe8   static    0        Veth2       3
177       0050.5686.7787   static    0        Veth1       3
177       0002.3d40.2100   dynamic   1        Po3         3
177       000c.29c2.d1ba   dynamic   55       Po3         3
177       0050.5686.3bc0   dynamic   45       Po3         3
177       0050.56bc.5eea   dynamic   1        Po3         3
177       0050.56bc.761d   dynamic   1        Po3         3
266       000c.2996.9a1d   static    0        Veth4       3
266       000c.29bc.589c   static    0        Veth3       3
266       c84c.75f6.013f   dynamic  104     Po1         3
Total MAC Addresses: 17
pvlan(config-port-prof)#

```

- Sur le système UCS, vous devez apprendre tous les MAC, pour cette communication, dans le VLAN principal que vous utilisez sur le N1K. Vous ne devez pas apprendre l'amont ici :

```
F340-31-9-1-B(nxos)# show mac address-table
Legend:
    * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
    age - seconds since last seen,+ - primary entry using vPC Peer-Link
```

VLAN	MAC Address	Type	age	Secure	NTFY	Ports
* 266	000c.2996.9a1d	dynamic	100	F	F	Veth1491
* 266	000c.29bc.589c	dynamic	180	F	F	Veth1491
* 177	0025.b581.9a3f	dynamic	0	F	F	Veth1402
* 177	0025.b585.100a	dynamic	350	F	F	Veth1424
* 177	0050.566b.01ad	dynamic	380	F	F	Veth1402
* 126	0025.b581.999e	static	0	F	F	Veth1392
* 124	0023.04c6.dbe2	dynamic	0	F	F	Veth1404

4. Sur le Nexus 5K, tous les MAC se trouvent dans le VLAN principal que vous avez sélectionné :

```
F340.11.13-Nexus5000-5# show mac address-table
Legend:
    * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
    age - seconds since last seen,+ - primary entry using vPC Peer-Link
```

VLAN	MAC Address	Type	age	Secure	NTFY	Ports
* 266	000c.2996.9a1d	dynamic	90	F	F	Eth1/4
* 266	000c.29bc.589c	dynamic	20	F	F	Eth1/4
* 266	c84c.75f6.013f	dynamic	100	F	F	Eth1/1

5. Sur le commutateur 4900, tout se trouve sur le VLAN principal que vous avez sélectionné :

```
Switch#show mac address-table
Unicast Entries
```

vlan	mac address	type	protocols	port
266	000c.2996.9a1d	dynamic	ip,ipx,assigned,other	GigabitEthernet1/1
266	000c.29bc.589c	dynamic	ip,ipx,assigned,other	GigabitEthernet1/1
266	c84c.75f6.013f	static	ip,ipx,assigned,other	Switch

```
Multicast Entries
```

vlan	mac address	type	ports
1	0100.0ccc.ccce	system	Gi1/1
1	ffff.ffff.ffff	system	Gi1/1
166	ffff.ffff.ffff	system	Gi1/1
266	ffff.ffff.ffff	system	Gi1/1,Gi1/2,Switch

## PVLAN de communauté sur N1K avec port de promiscuité sur le profil de port de liaison ascendante N1K

Il s'agit de la seule configuration prise en charge pour le VLAN de communauté avec UCS.

Cette configuration est identique à celle configurée dans le [PVLAN isolé sur N1K avec un port Promiscuité sur la section du profil de port de liaison ascendante N1K](#). La seule différence entre la communauté et l'isolement est la configuration du PVLAN.

Afin de configurer le N1K, créez et associez les VLAN comme vous l'avez fait sur le Nexus 5K :

```
Switch(config)# vlan 166
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# vlan 266
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# private-vlan association 16
```

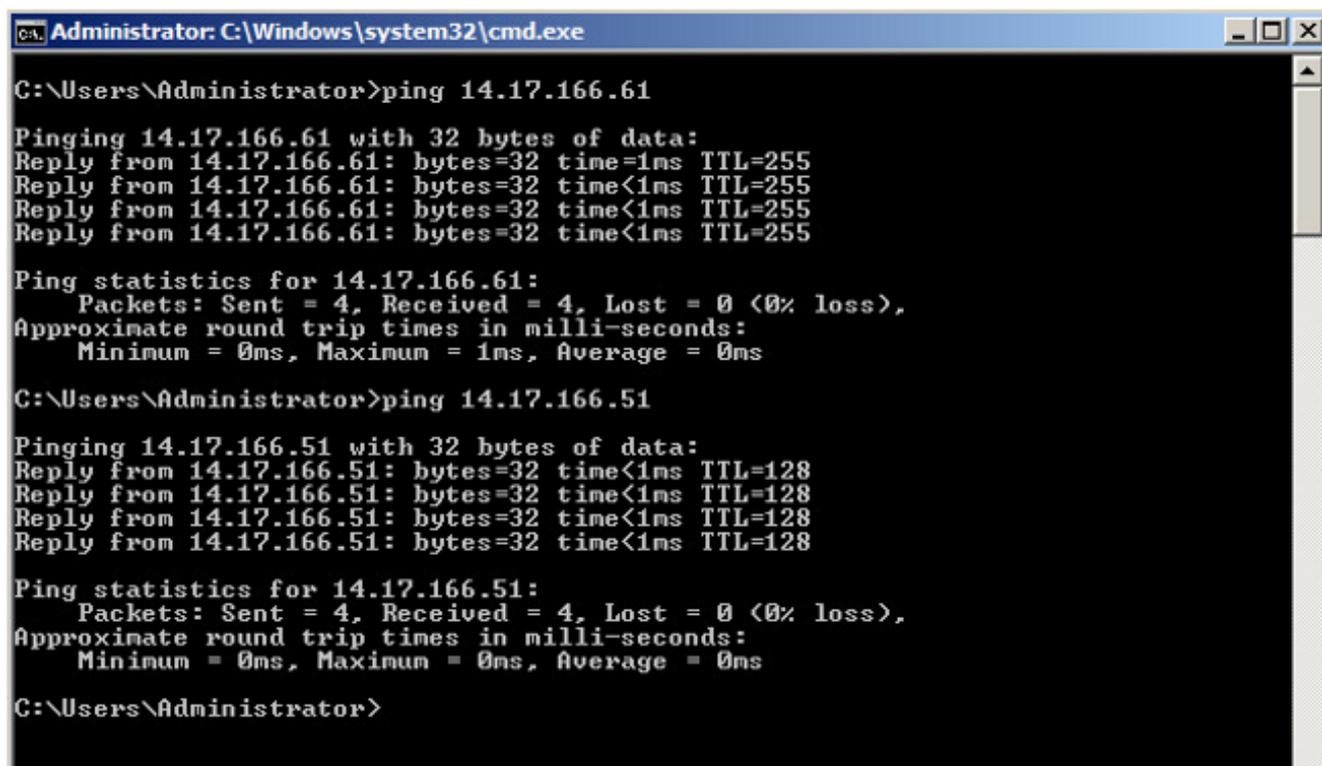
Toutes les autres configurations sont identiques au PVLAN isolé sur N1K avec un port proche sur le profil de port de liaison ascendante N1K.

Une fois configuré, vous pouvez communiquer avec toutes les machines virtuelles connectées au profil de port vEthernet utilisé pour votre PVLAN.

## Dépannage

Cette procédure décrit comment tester la configuration.

1. Exécutez des requêtes ping vers d'autres systèmes configurés dans le groupe de ports, ainsi que vers le routeur ou un autre périphérique au niveau du port proche. Les requêtes ping au-delà du port de promiscuité et vers d'autres systèmes de la communauté doivent fonctionner.



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ping 14.17.166.61

Pinging 14.17.166.61 with 32 bytes of data:
Reply from 14.17.166.61: bytes=32 time=1ms TTL=255
Reply from 14.17.166.61: bytes=32 time<1ms TTL=255
Reply from 14.17.166.61: bytes=32 time<1ms TTL=255
Reply from 14.17.166.61: bytes=32 time<1ms TTL=255

Ping statistics for 14.17.166.61:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Administrator>ping 14.17.166.51

Pinging 14.17.166.51 with 32 bytes of data:
Reply from 14.17.166.51: bytes=32 time<1ms TTL=128

Ping statistics for 14.17.166.51:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>
```

2. Tous les autres dépannages sont identiques au [PVLAN isolé](#).

## PVLAN isolé et PVLAN de communauté sur le port promotionnel DVS VMware sur le DVS

En raison des problèmes de configuration sur le système DVS et UCS, les PVLAN avec DVS et UCS ne sont pas pris en charge avant la version 2.2(2c).

## Vérification

Aucune procédure de vérification n'est actuellement disponible pour ces configurations.

## Dépannage

Les sections précédentes contiennent des informations que vous pouvez utiliser pour dépanner vos configurations.

L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .