Exemple de configuration de multidiffusion UCS L2 avec commutateurs des gammes Nexus 5000 et 1000V

Contenu

Introduction

Ce document décrit comment configurer et dépanner la multidiffusion de couche 2 (L2) pour les machines virtuelles (VM) lors de la configuration de Cisco Unified Computing System (UCS), des commutateurs Cisco Nexus 1000V (N1kV) et des commutateurs Cisco Nexus 5000 (N5k).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Notions de base sur la multidiffusion
- Cisco UCS
- N1kV
- N5k

Components Used

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

- Commutateur de la gamme Cisco Nexus 5020 version 5.0(3)N2(2a)
- Cisco UCS version 2.1(1d)
- Serveur lame Cisco UCS B200 M3 avec carte d'interface virtuelle (VIC) Cisco 1240
- vSphere 5.1 (ESXi et vCenter)
- Cisco N1kV version 4.2(1)SV2(1.1a)

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. Si votre réseau est actif, assurez-vous de bien comprendre l'impact potentiel de toute commande ou configuration de capture de paquets.

Informations générales

La multidiffusion a été initialement conçue pour utiliser la fonctionnalité de couche 3 (L3), dans laquelle plusieurs hôtes d'un réseau s'abonnent à une adresse de multidiffusion. La nouvelle tendance est d'utiliser la fonctionnalité de multidiffusion de couche 2, où le trafic circule entre les machines virtuelles qui participent à une application de multidiffusion sur les hôtes du même VLAN. Ce trafic multicast reste dans le même domaine de couche 2 et n'a pas besoin de routeur.

Lorsqu'aucun routeur de multidiffusion dans le VLAN n'est à l'origine des requêtes, vous devez configurer un interrogateur de surveillance IGMP (Internet Group Management Protocol) afin d'envoyer des requêtes d'appartenance. La surveillance IGMP est activée par défaut sur UCS, N1kV et N5k. Vous pouvez activer l'interrogation IGMP Snooping sur UCS ou N5k, selon l'étendue de la multidiffusion L2. S'il existe des récepteurs de multidiffusion en dehors de l'UCS, configurez le demandeur de surveillance sur le N5k.

Lorsqu'un interrogateur IGMP Snooping est activé, il envoie des requêtes IGMP périodiques qui déclenchent des messages de rapport IGMP des hôtes qui veulent recevoir du trafic de multidiffusion IP. IGMP Snooping écoute ces rapports IGMP afin d'établir un transfert approprié.

Le logiciel IGMP Snooping examine les messages de protocole IGMP dans un VLAN afin de découvrir les interfaces connectées aux hôtes ou autres périphériques intéressés par la réception de ce trafic. Avec les informations d'interface, la surveillance IGMP peut réduire la consommation de bande passante dans un environnement LAN à accès multiple afin d'éviter un flux de VLAN entier. La fonctionnalité IGMP Snooping suit les ports qui sont connectés aux routeurs compatibles multidiffusion afin d'aider à gérer le transfert des rapports d'appartenance IGMP. En outre, le logiciel IGMP Snooping répond aux notifications de modification de topologie.

Configuration

Utilisez cette section afin de configurer la multidiffusion de couche 2 pour les machines virtuelles.

Configuration du réseau

Voici quelques remarques importantes sur la configuration du réseau dans cet exemple :

- L'UCS est connecté à un N5k via un vPC (Virtual Port Channel).
- Le système d'exploitation installé sur les deux hôtes est VMware ESXi 5.1. Chaque hôte possède des machines virtuelles avec des systèmes d'exploitation invité Microsoft Windows 2012.
- La source de la multidiffusion est **MCAST VM** (adresse IP 172.16.16.226) sur l'adresse IP hôte 172.16.16.222 (lame UCS 1/5), qui envoie le trafic à l'adresse IP de multidiffusion 239.14.14.14.
- Les récepteurs de multidiffusion sont **la machine virtuelle AD-1** (adresse IP 172.16.16.224) sur l'adresse IP hôte 172.16.16.220 (serveur lame UCS 1/6), et **TEST de la machine virtuelle (adresse IP 172.16.16.228) sur l'adresse IP hôte 172.16.16.222 (lame UCS 1/5).**
- Le demandeur de surveillance IGMP est configuré sur le N5k avec l'adresse IP 172.16.16.2, ainsi que sur le serveur UCS avec l'adresse IP 172.16.16.233.

Il n'est pas nécessaire de configurer deux interrogateurs dans le même VLAN (16). S'il existe des récepteurs de multidiffusion en dehors de l'UCS, configurez le demandeur de surveillance sur le N5k. Si le trafic de multidiffusion se trouve dans le domaine UCS, créez l'interrogateur de surveillance sur Cisco Unified Computing System Manager (UCSM).

> **Note**: Le demandeur IGMP N5k est élu par **RFC 4605**, ce qui explique le processus de sélection du demandeur.

Configuration de file d'attente IGMP N5k

Voici un exemple de configuration d'un interrogateur IGMP sur un N5k :

```
vlan 16

 ip igmp snooping querier 172.16.16.2

!

int vlan 16

 ip address 172.16.16.2/24

 no shut
```

L'adresse IP du demandeur n'a pas besoin d'être pour une interface virtuelle commutée, et elle peut être une adresse IP différente dans le même sous-réseau du VLAN 16.

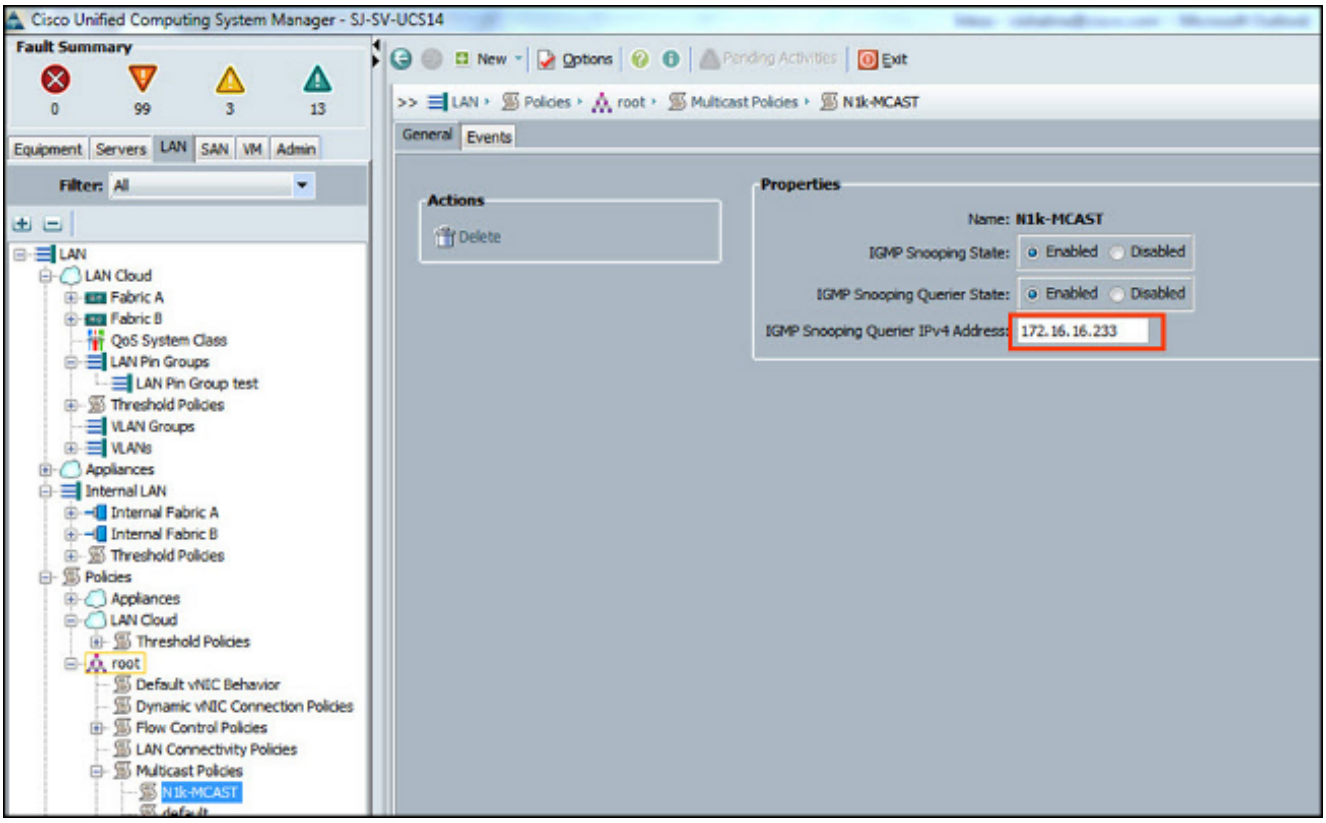
> **Note**: Reportez-vous à la section Configuration de la surveillance IGMP du **Guide de configuration du logiciel NX-OS de la gamme Cisco Nexus 5000** pour plus d'informations sur

la configuration du demandeur IGMP pour votre version spécifique.

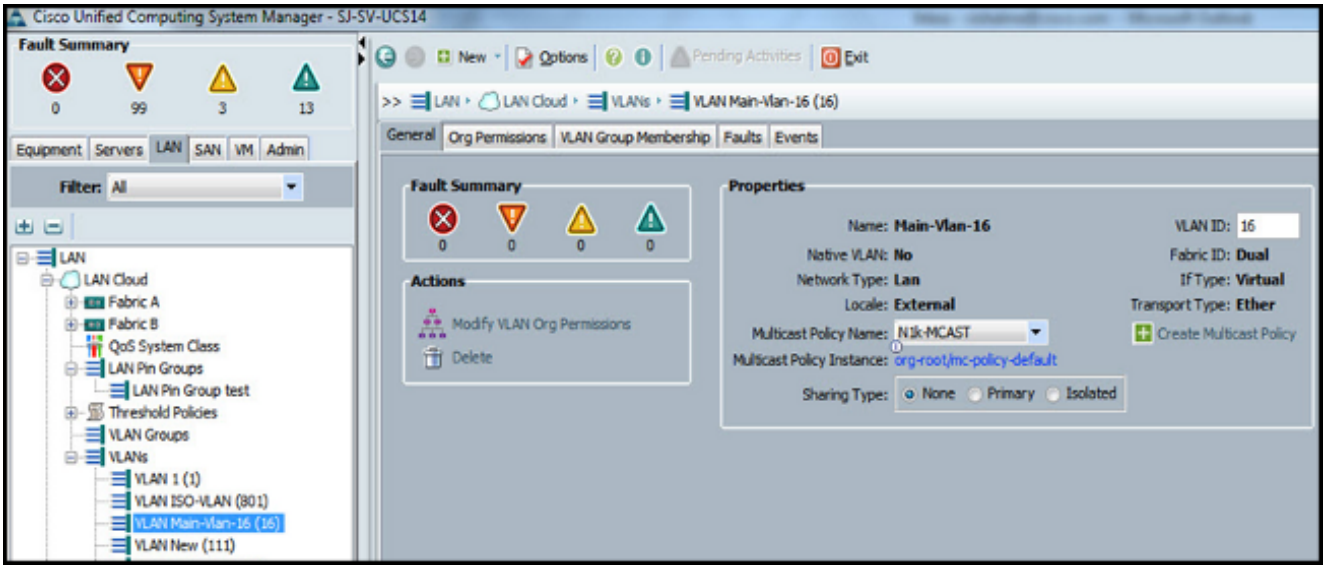
Configuration de la file d'attente UCS IGMP

Complétez ces étapes afin de configurer le demandeur IGMP pour UCS :

1. Créez une nouvelle stratégie de multidiffusion sous l'onglet **LAN** de l'UCSM, comme indiqué ici :



2. Appliquer la stratégie de multidiffusion **N1k-MCAST** au VLAN 16 :



3. Pour le N1kV, vérifiez que la surveillance IGMP est activée sur le VLAN 16 (qui est activé par

défaut). Aucune configuration ne doit être effectuée sur un N1kV afin de prendre en charge la multidiffusion de couche 2 de base.

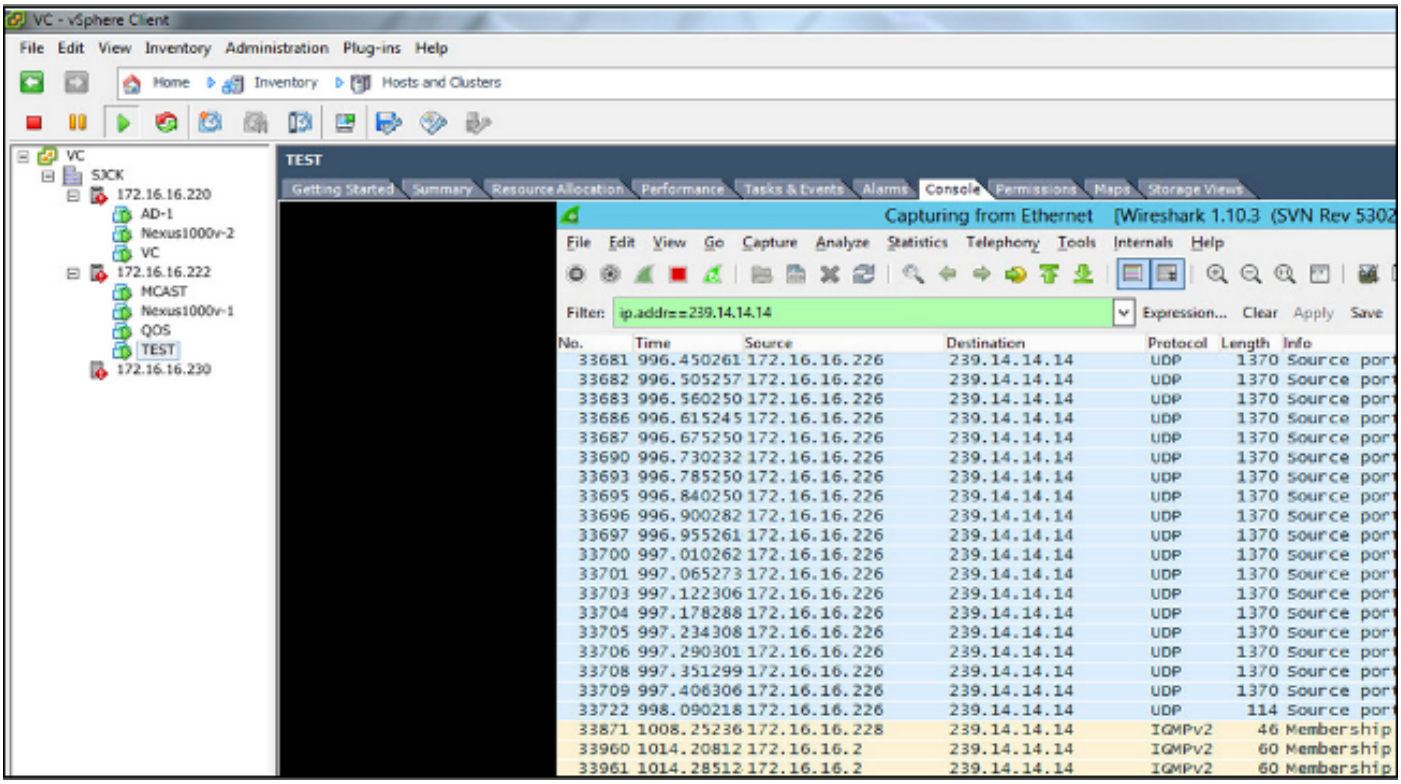
Note: Un lecteur multimédia VideoLAN Client (VLC) est utilisé afin de démontrer la multidiffusion. Pour plus d'informations sur l'utilisation d'un lecteur VLC pour la diffusion multipoint, reportez-vous à l'article Comment utiliser le lecteur multimédia VLC pour diffuser de la vidéo multidiffusion.

Vérification

Utilisez cette section afin de vérifier que votre configuration fonctionne correctement.

Vérification sur N1kV

Vérifiez que les récepteurs de multidiffusion **TEST VM** et **AD-1 VM** ont joint le flux de multidiffusion **239.14.14.14**, à partir duquel **MCAST VM** source le trafic. Cette image montre que la **machine virtuelle TEST** du récepteur de multidiffusion reçoit le flux :



Le résultat de la surveillance N1kV affiche l'adresse de groupe et les voyants du récepteur de multidiffusion, et non le Veth de la machine virtuelle qui génère le trafic de multidiffusion (comme prévu) :

```
Nexus1000v# sh ip igmp snooping groups

Type: S - Static, D - Dynamic, R - Router port

Vlan  Group Address       Ver  Type  Port list
16    */*                 -    R     Eth3/2 Eth4/2
16    239.14.14.14        v2   D     Veth3 Veth6
```

Cette sortie N1kV montre les ports actifs pour la multidiffusion et le demandeur IGMP :

```
Nexus1000v# sh ip igmp snooping groups vlan 16
IGMP Snooping information for vlan 16
  IGMP snooping enabled
  IGMP querier present, address: 172.16.16.2, version: 2, interface Ethernet4/2
  Switch-querier disabled
  IGMPv3 Explicit tracking enabled
  IGMPv2 Fast leave disabled
  IGMPv1/v2 Report suppression disabled
  IGMPv3 Report suppression disabled
  Link Local Groups suppression enabled
  Router port detection using PIM Hellos, IGMP Queries
  Number of router-ports: 2
  Number of groups: 1
  Active ports:
    Veth1       Eth3/2  Veth2   Eth4/2
    Veth3       Veth4   Veth5   Veth6
```

Au niveau de l'hôte, vous pouvez vérifier que le trafic de multidiffusion est reçu par les machines virtuelles qui y participent. Cette sortie montre la machine virtuelle **AD-1**, qui se trouve sur **le module 3** du module superviseur virtuel (VSM) :

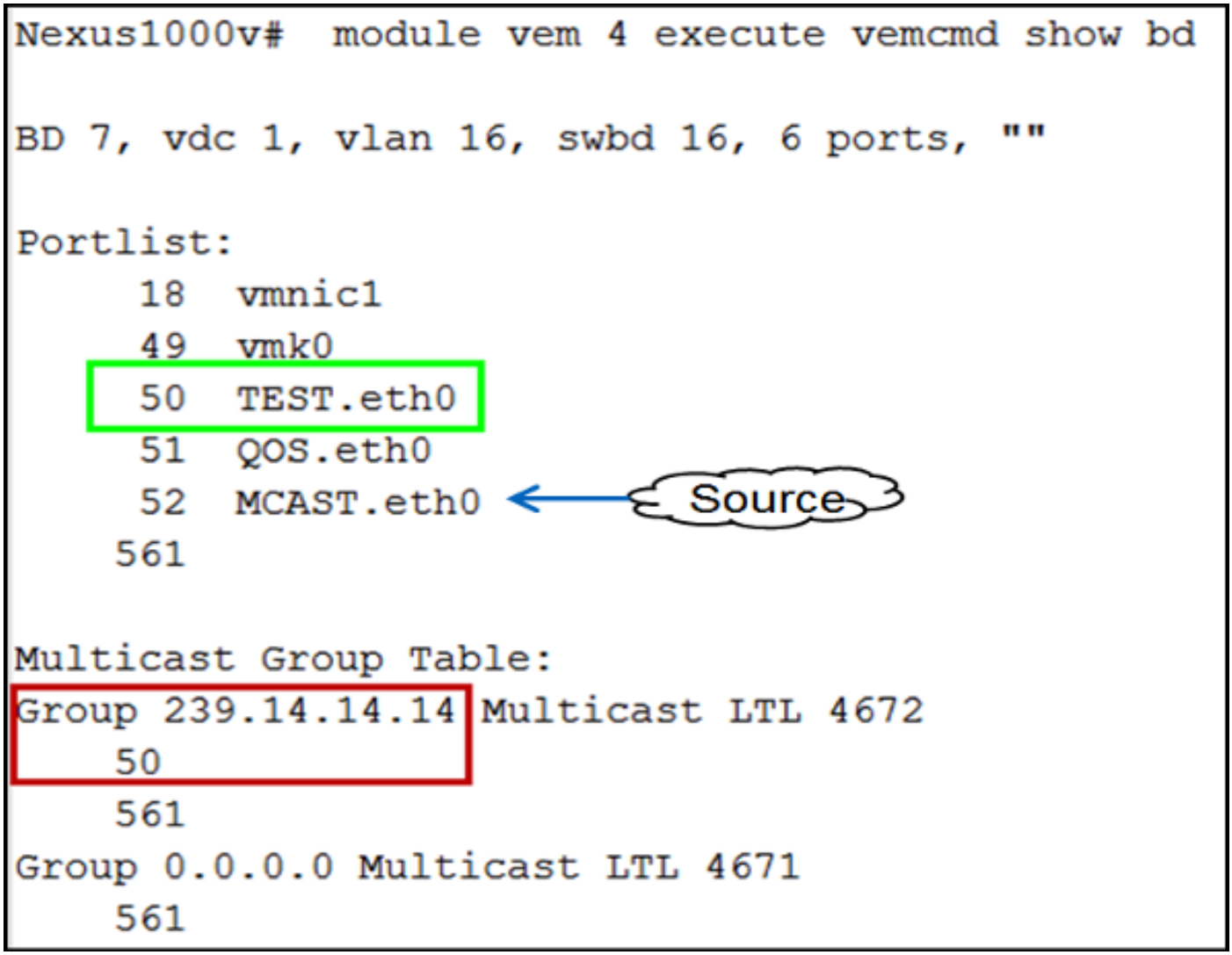
```
Nexus1000v#  module vem 3 execute vemcmd show bd

BD 7, vdc 1, vlan 16, swbd 16, 3 ports, ""

Portlist:
     18  vmnic1
     49  vmk0
     50  AD-1 ethernet0

Multicast Group Table:
Group 239.14.14.14 Multicast LTL 4672
    18
    50
Group 0.0.0.0 Multicast LTL 4671
    18
```

Cette sortie montre le **TEST** de la machine virtuelle, qui se trouve sur **le module 4** du module VSM :



Vérification sur UCS

Cette sortie UCS affiche les ports actifs pour la multidiffusion et l'**adresse de groupe** :

```
SJ-SV-UCS14-B(nxos)# sh ip igmp snooping group
Type: S - Static, D - Dynamic, R - Router port

Vlan  Group Address       Ver  Type  Port list
1     */*                 -    R     Po1
11    */*                 -    R     Po1
15    */*                 -    R     Po1
16    */*                 -    R     Po1
16    239.14.14.14        v2   D     Veth1257 Veth1255
30    */*                 -    R     Po1
111   */*                 -    R     Po1
172   */*                 -    R     Po1
800   */*                 -    R     Po1
```

Cette sortie de surveillance UCS pour VLAN 16 vérifie que le demandeur est configuré sur l'UCSM et le N5k, et montre que seul le demandeur sur le N5k est actuellement actif (comme prévu) :

```
SJ-SV-UCS14-B(nxos)# sh ip igmp snooping vlan 16
IGMP Snooping information for vlan 16
  IGMP snooping enabled
  Optimised Multicast Flood (OMF) disabled
  IGMP querier present, address: 172.16.16.2, version: 2, interface port-channel1
  Switch-querier enabled, address 172.16.16.233, currently not running
  IGMPv3 Explicit tracking enabled
  IGMPv2 Fast leave disabled
  IGMPv1/v2 Report suppression enabled
  IGMPv3 Report suppression disabled
  Link Local Groups suppression enabled
  Router port detection using PIM Hellos, IGMP Queries
  Number of router-ports: 1
  Number of groups: 1
  Active ports:
    Po1 Veth1257        Veth1251        Veth1255
    Veth1279    Veth1281
```

Vérification sur le N5k

Sur le N5k, vérifiez que l'adresse de groupe de multidiffusion **239.14.14.14** et le canal de port actif sont connectés aux interconnexions de fabric UCS :

```
n5k-Rack18-1# sh ip igmp snooping groups
Type: S - Static, D - Dynamic, R - Router port, F - Fabricpath core port

Vlan  Group Address      Ver  Type  Port list
1     */*                -    R     Po40
15    */*                -    R     Po40 Po1110 Po1111
15    239.255.255.253    v2   D     Po10 Po11 Po12
                                     Po13 Po40
16    */*                -    R     Po3 Po40
16    239.14.14.14       v2   D     Po15 Po16
17    */*                -    R     Po40
18    */*                -    R     Po40
```

Dépannage

Cette section fournit des renseignements qui vous permettront de régler les problèmes de configuration.

Voici une liste des mises en garde de base sur la multidiffusion dans le domaine L2 :

- Si la surveillance IGMP n'est pas activée sur le commutateur, le trafic de multidiffusion est diffusé dans le domaine L2.
- Si la surveillance IGMP est activée, un interrogateur doit s'exécuter sur les commutateurs de liaison ascendante sur le VLAN qui contiennent des sources et des récepteurs de multidiffusion.
- S'il n'y a aucun demandeur IGMP dans le VLAN, N1kV et UCS ne transmettent pas la multidiffusion. Il s'agit de la configuration incorrecte la plus courante dans les cas du centre d'assistance technique Cisco (TAC).
- Par défaut, la surveillance IGMP est activée sur N1kV et sur UCS.
- Avec UCS versions 2.1 et ultérieures, la surveillance IGMP peut être activée ou désactivée par VLAN et le demandeur IGMP peut être configuré au niveau UCS.