

Exemple de configuration du Nexus 1000v VXLAN

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Informations générales](#)

[Au sujet de VXLAN](#)

[Conditions requises VXLAN](#)

[Modes VXLAN](#)

[Mode Multicast](#)

[Mode Unicast](#)

[Configurez](#)

[Activez la caractéristique VXLAN](#)

[Vérifiez que la caractéristique est activée](#)

[Configurez le mode par défaut](#)

[Configurez le Port-profil VTEP](#)

[Créez les interfaces VTEP VMKernel](#)

[Créez le domaine de passerelle](#)

[Créez le Port-profil VXLAN pour des VMs](#)

[Vérifiez le domaine de passerelle](#)

[Vérifiez la Connectivité](#)

[Commutez au mode d'Unicast](#)

[Vérifiez le domaine de passerelle d'Unicast](#)

[Vérifiez la Connectivité en mode d'Unicast](#)

[Déployez la passerelle VXLAN](#)

[Au sujet de la passerelle VXLAN](#)

[Activez la caractéristique](#)

[Préparez le VSM pour la passerelle VXLAN](#)

[Installez la passerelle VXLAN sur l'appliance 1x10](#)

[Vérifiez les modules dans le VSM](#)

[Formez une Haute disponibilité](#)

[Vérifiez](#)

[VSM CLI](#)

[Commandes VEM](#)

[Dépannez](#)

Introduction

Ce document décrit comment configurer le RÉSEAU LOCAL extensible virtuel (VXLAN) sur la gamme de Cisco Nexus un 1000V (N1kV) commutent.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

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.

Informations générales

Cette section décrit la caractéristique VXLAN et comment est peut être mise en application afin d'adresser des limites d'évolutivité dans des centres de traitement des données.

Au sujet de VXLAN

Puisque le champ d'ID DE VLAN dans une trame est seulement 12 bits, il limite le nombre de VLAN à 4,096 avec certains réservés. La caractéristique VXLAN introduit un champ de l'ID 24-bit, qui mesure les possibilités pour inclure un potentiel de 16 millions de segments différents de RÉSEAU LOCAL. C'est semblable à la transition de l'ipv4 à l'IPv6.

Pour la comparaison, c'est l'affichage de trame standard :

C'est l'affichage de trame encapsulée VXLAN :

Avec le transport VXLAN, la trame initiale de la couche 2 (L2) est encapsulée dans un paquet de la couche 3 (L3). La destination alors De-encapsule le paquet et envoie la trame en fonction sur

l'adresse de Contrôle d'accès au support (MAC) de destination qui est contenue en dedans. Ceci permet le trafic segmenté sur une infrastructure en cours et permet à des réseaux pour refléter les domaines L2 à travers des centres de traitement des données. En outre, il active des améliorations telles que des vMotions croisés de centre de traitement des données.

L'utilisation de la technologie VXLAN est pratique dans les environnements qui exigent de vous de mesurer et fournir des infrastructures pour des clients. Un bon exemple de ceci est le directeur de vCloud de VMware, où les fournisseurs déploient des ressources pour leurs clients. Ceci inclut des ressources informatiques des serveurs, des ressources en réseau qui utilisent le réseau de VMware, ou du Cisco Networking actionné par le N1kV. Un fournisseur utilise des VLAN comme mécanisme de transport pour le locataire VXLANs. Sans VXLAN, des locataires sont donnés leur propre VLAN, qui peut mesurer jusqu'à la limite 4,096 rapidement. Chaque locataire peut maintenant être assigné un VXLAN et peut utiliser l'infrastructure VLAN pour le transport. C'est extensible et toujours segmenté.

Conditions requises VXLAN

Pour que VXLAN fonctionne, ces conditions doivent être remplies :

- La taille maximum d'unité de transition (MTU) dans tout le transport doit être grimpée jusqu'à 50 octets ou la taille de MTU doit être diminuée sur les virtual machine (VMs).
- Le Protocole ARP (Address Resolution Protocol) de proxy doit être configuré sur les passerelles pour le transport VLAN (en-tête Ethernet (14) + en-tête d'UDP (8) + en-tête IP (20) + en-tête VXLAN (8) = 50 octets).
- Le routage de Multidiffusion doit être configuré (pour le mode de Multidiffusion). Remarque: C'est seulement pour VXLANs avant la version 1.5 et la version 1.5 avec le mode de Multidiffusion. La version 1.5 a été empaquetée avec la version 4.2.1.SV2(2.1) N1kV. Cette version prend en charge une méthode d'Unicast de transport aussi bien.
- Piller de Protocole IGMP (Internet Group Management Protocol) querier ou Protocol Independent Multicast (PIM) doit être configuré.
- On doit permettre le port 8472 de Protocole UDP (User Datagram Protocol) par tous les Pare-feu. Remarque: C'est le port qui est utilisé pour le trafic encapsulé.
- Des interfaces de VMkernel doivent être configurées sur chaque hôte. Remarque: Ceux-ci s'appellent les périphériques du tunnel VXLAN (VTEP). Ils encapsulent et De-encapsulent le trafic VXLAN dans l'environnement. Vous pouvez utiliser le même VMkernel que vous utilisez pour **I3control**.

Modes VXLAN

Dans la version 1.5 VXLAN, emballée dans la version 4.2.1.SV2(2.1) N1kV, VXLAN peut fonctionner en mode de Multidiffusion ou mode d'Unicast. Chacun des deux modes sont décrits dans cette section.

[Mode Multicast](#)

Chaque VXLAN a un groupe-IP assigné de Multidiffusion. Quand une VM joint le VXLAN, le module virtuel d'Ethernets (VEM) envoie IGMP-joignent des demandes au groupe assigné. L'émission, la Multidiffusion, et le trafic de propagation est envoyée à tout le VTEPs ; le trafic unicast est envoyé à la destination VTEP.

Mode Unicast

Pour l'émission, la Multidiffusion, et les trames de monodiffusion inconnues, chaque VXLAN envoie le trafic à l'adresse IP de destination de chaque VTEP qui loge une VM dans le même VXLAN. Si plus d'un VTEP existe, seulement un du VTEPs est choisi pour recevoir le trafic de propagation, qui est semblable à un récepteur indiqué d'émission sur le Système d'informatique unifiée Cisco (UCS). Le VEMs utilisent alors l'adresse IP comme destination VTEP pour l'encapsulation.

Avec le mode d'Unicast, il y a également une caractéristique de distribution de MAC. Avec cette configuration, le VSM apprend toutes les adresses MAC de tout les VEMs et les trace au VTEP indiqué. L'inondation et la réplication est éliminée parce que le VEM connaît toujours la destination VTEP pour la VM spécifique de destination.

Remarque: Ceci est seulement pris en charge pour VEMs qui sont gérés par le même VSM.

Configurez

Employez cette section afin de configurer VXLAN sur la gamme N1kV commutent.

Activez la caractéristique VXLAN

Sélectionnez ces commandes afin d'activer la caractéristique VXLAN :

```
Nexus1000v# conf t Enter configuration commands, one per line. End with CNTL/Z.  
Nexus1000v(config)# feature segmentation
```

Vérifiez que la caractéristique est activée

Écrivez la **caractéristique d'exposition** | commande de **segmentation de grep** afin de vérifier que la caractéristique est activée :

```
Nexus1000v(config)# show feature | grep segmentation  
network-segmentation 1 enabled  
segmentation 1 enabled
```

Configurez le mode par défaut

Remarque: Le mode par défaut est réservé unicast, sans distribution de MAC. Cet exemple dans ce document configure le mode de Multidiffusion comme par défaut et les transitions au mode d'Unicast plus tard.

Ne sélectionnez l'**aucune** commande **réservée unicast de mode de segment** afin de configurer le mode par défaut :

```
Nexus1000v(config)# no segment mode unicast-only
```

Configurez le Port-profil VTEP

Maintenant vous devez configurer le port-profil qui l'utilisation de VTEPs. La configuration de port-profil est semblable à d'autres port-profil d'accès, avec la configuration VXLAN ajoutée. Une fois que la **capacité vxlan** est configurée, le VEM utilise le VMkernel indiqué pour l'encapsulation et la De-encapsulation. Il inclut également les informations en tant qu'élément de l'élection indiquée de récepteur.

```
Nexus1000v# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Nexus1000v(config)# port-profile type vethernet VTEP
Nexus1000v(config-port-prof)# vmware port-group
Nexus1000v(config-port-prof)# switchport mode access
Nexus1000v(config-port-prof)# switchport access vlan 168
Nexus1000v(config-port-prof)# capability vxlan
Nexus1000v(config-port-prof)# no shutdown
Nexus1000v(config-port-prof)# state enabled
```

Créez les interfaces VTEP VMKernel

Terminez-vous ces étapes afin de créer l'interface VTEP VMkernel :

1. Créez un VMkernel et déplacez-le au port-profil VXLAN-activé :
2. Choisissez le port-profil VTEP qui a le **vxlan de capacité** configuré :
3. Assignez au VTEP une adresse IP dans votre VLAN externe :
4. Terminez l'assistant.

Créez le domaine de passerelle

Le domaine de passerelle définit l'ID de segment (ID VXLAN) et le groupe de multidiffusion (adresse IP).

Sélectionnez ces commandes afin de créer le domaine de passerelle :

```
Nexus1000v# conf t
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Nexus1000v(config)# bridge-domain 192.168.1.x
Nexus1000v(config-bd)# segment id 5000
Nexus1000v(config-bd)# group 239.1.1.1
```

Créez le Port-profil VXLAN pour des VMs

Pour que les VMs utilisent le VXLAN, vous devez créer un port-profil pour eux. La configuration de port-profil est identique mais elle accède à un domaine de passerelle au lieu d'un VLAN.

Sélectionnez ces commandes afin de créer le port-profil VXLAN pour les VMs :

```
Nexus1000v# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Nexus1000v(config)# port-profile type vethernet vxlan-192.168.1.x
Nexus1000v(config-port-prof)# vmware port-group
Nexus1000v(config-port-prof)# switchport mode access
Nexus1000v(config-port-prof)# switchport access bridge-domain 192.168.1.x
Nexus1000v(config-port-prof)# no shutdown
Nexus1000v(config-port-prof)# state enabled
```

Vérifiez le domaine de passerelle

Une fois que vous placez les VMs dans le port-profil, vous devez vérifier que les configurations du domaine de passerelle sont correctes et que les VMs sont incluses.

Sélectionnez la commande de **show bridge-domain** afin de vérifier le domaine de passerelle :

```
Nexus1000v# show bridge-domain 192.168.1.x

Bridge-domain 192.168.1.x (2 ports in all)
Segment ID: 5000 (Manual/Active)
Mode: Multicast (override)
MAC Distribution: DisableGroup IP: 239.1.1.1
State: UP Mac learning: Enabled
Veth18, Veth19
```

Vérifiez la Connectivité

Cette image illustre comment vérifier que vos VMs ont la Connectivité sur le VXLAN interne :

Commutez au mode d'Unicast

Maintenant vous devez commuter au mode réservé Unicast et vérifier que vous avez toujours la Connectivité.

Sélectionnez ces commandes afin de commuter au mode d'Unicast :

```
Nexus1000v# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Nexus1000v(config)# bridge-domain 192.168.1.x
Nexus1000v(config-bd)# segment mode unicast-only
```

Vérifiez le domaine de passerelle d'Unicast

Sélectionnez la commande de **show bridge-domain** afin de vérifier le domaine de passerelle d'unicast :

```
Nexus1000v# show bridge-domain 192.168.1.x
```

```
Bridge-domain 192.168.1.x (2 ports in all)
Segment ID: 5000 (Manual/Active)
Mode: Unicast-only (override)
MAC Distribution: DisableGroup IP: 239.1.1.1
State: UP Mac learning: Enabled
Veth18, Veth19
```

Vérifiez la Connectivité en mode d'Unicast

Cette image illustre comment vérifier la Connectivité en mode d'Unicast :

Déployez la passerelle VXLAN

Cette section donne un aperçu de la passerelle VXLAN et décrit le processus qui est utilisé afin de la déployer.

Au sujet de la passerelle VXLAN

La passerelle VXLAN a été créée afin de fournir une manière pour que des segments VXLAN communiquent avec des segments réguliers VLAN. Il permet à des VMs sur VXLANs pour communiquer avec les serveurs physiques sur des VLAN externes. C'est comparable à l'appliance de vShield de VMware, qui permet à des VMs sur des réseaux internes pour communiquer avec d'autres ordinateurs sur les réseaux du fournisseur.

Cette passerelle est une lame virtuelle de service (VSB) qui est installée sur les appliances de gamme 1x10 de Cisco Nexus. Quand vous installez la passerelle VXLAN sur une appliance de gamme 1x10 de Nexus, vous devez exécuter l'appliance avec le type de réseau **flexible** (type 5).

Remarque: La passerelle VXLAN exige l'autorisation avancée sur le N1kV, ainsi vous devez s'assurer que vous avez les permis suffisants avant que vous commutiez à l'édition avancée avec la commande **avancée par édition de commutateur SVS** dans le mode de configuration.

Activez la caractéristique

Afin d'activer la passerelle VXLAN, vous devez activer la caractéristique sur le N1kV. Sélectionnez ces commandes afin d'activer la caractéristique :

```
Nexus1000v(config)# feature vxlan-gateway
Nexus1000v(config)# 2013 Aug 1 18:34:20 Nexus1000v %SEG_BD-2-VXLAN_GATEWAY_ENABLED:
  Feature vxlan-gateway enabled
Nexus1000v(config)# show feature | grep gateway
vxlan-gateway 1 enabled
```

Préparez le VSM pour la passerelle VXLAN

des Port-profil pour la passerelle VXLAN doivent être provisionnés sur le VSM avant l'installation. Ces profils incluent un port-profil de liaison ascendante et un port-profil de vEthernet pour les VTEP, qui sont configurés avec ces commandes :

```
Nexus1000v(config)# feature vxlan-gateway
Nexus1000v(config)# 2013 Aug 1 18:34:20 Nexus1000v %SEG_BD-2-VXLAN_GATEWAY_ENABLED:
  Feature vxlan-gateway enabled
```

```
Nexus1000v(config)# show feature | grep gateway
vxlan-gateway 1 enabled
```

Maintenant vous devez configurer le port-profil de la passerelle VTEP VXLAN, qui inclut la caractéristique **vxlan de capacité** aussi bien que l'adresse IP de transport que la passerelle VXLAN emploie afin de transporter le trafic. Sélectionnez ces commandes afin de le configurer :

```
Nexus1000v(config)# port-profile vxgw-vtep <---No vmware port-group cmd;
  Not published to vCenter
Nexus1000v(config-port-prof)# switchport mode access
Nexus1000v(config-port-prof)# switchport access vlan 168
Nexus1000v(config-port-prof)# capability vxlan
Nexus1000v(config-port-prof)# no shutdown
Nexus1000v(config-port-prof)# state enabled
Nexus1000v(config-port-prof)# transport ip address 10.10.168.25 255.255.255.0
  gateway 10.10.168.254
```

La passerelle VXLAN exige un port-profil pour les deux interfaces physiques de fonction émulation. Ces liens doivent être configurés dans un joncteur réseau de Port canalisé. Le Control Protocol d'agrégation de liaisons (LACP) et les Ports canalisés statiques sont pris en charge.

La passerelle prend un segment VXLAN et le trace à un 802.1Q VLAN. Ceci est configuré dans un *service instance*.

Remarque: Vous pouvez également configurer le service instance après que la passerelle soit enregistrée.

Sélectionnez ces commandes afin de configurer le joncteur réseau de Port canalisé :

```
Nexus1000v(config)#port-profile type ethernet vxlan-gw-uplink <---No vmware
  port-group cmd.
Nexus1000v(config-port-prof)# switchport mode trunk
Nexus1000v(config-port-prof)# switchport trunk allowed vlan 119,219,319
Nexus1000v(config-port-prof)# mtu 9000
Nexus1000v(config-port-prof)# channel-group auto mode active
Nexus1000v(config-port-prof)# no shutdown
Nexus1000v(config-port-prof)# description Virtual PP push in opaque data to vxgw
Nexus1000v(config-port-prof)# state enabled
Nexus1000v(config-port-prof)# service instance 168
Nexus1000v(config-port-prof-srv)# encapsulation dot1q 168 bridge-domain 192.168.1.x
Nexus1000v(config-port-prof-srv)#
```

Afin d'enregistrer la passerelle VXLAN avec le VSM, vous devez noter les adresses MAC primaires et secondaires à partir du VSMs. Sélectionnez la commande **interne de l'information VMs d'exposition du VSM** :

```
Nexus1000v# show vms internal info Global svcs connection mode: ipv4
Cached IP address: 10.10.168.2
DVS INFO:
```



```
-----
DVS name: [Nexus1000v]
UUID: [ee 63 3c 50 04 b1 6d d6-58 61 ff ba 56 05 14 fd]
Description: [(null)]
Config version: [91]
Max ports: [8192]
DC name: [jristain]
OPQ data&colon; size [723], data&colon; [data-version 1.0]
```

```
switch-domain 27
switch-name Nexus1000v
cp-version 4.2(1)SV2(2.1)
control-vlan 1
system-primary-mac 00:50:56:bc:6a:3d
active-vsm packet mac 00:50:56:bc:2a:5f
active-vsm mgmt mac 00:50:56:bc:57:4e
standby-vsm ctrl mac 0050-56bc-74f1
inband-vlan 1
svs-mode L3
l3control-ipaddr 10.10.168.2
```

Vous pouvez maintenant installer la passerelle VXLAN sur l'appliance de gamme 1x10 de Nexus.

Installez la passerelle VXLAN sur l'appliance 1x10

Une fois que vous copiez le logiciel de passerelle VXLAN sur le **bootflash** : répertoire de **référentiel de l'appliance** de gamme 1x10 de Nexus, vous pouvez créer un VSB. Sélectionnez ces commandes afin de le créer :

```
1010(config)# virtual-service-blade VXGW
1010(config-vs-b-config)# virtual-service-blade-type
new vxgw.4.2.1.SV2.2.1.iso
```

Sélectionnez la commande de **virtuel-service-lame d'exposition** afin de vérifier les interfaces que vous avez créées dans le VSB :

```
1010(config-vs-b-config)# show virtual-service-blade name VXGW
virtual-service-blade VXGW
Description:
Slot id: 1
Host Name:
Management IP:
VSB Type Name : vx-gw-1.5
Configured vCPU: 3
Operational vCPU: 3
Configured Ramsize: 2048
Operational Ramsize: 2048
Disksize: 3
Heartbeat: 0
```

Legends: P - Passthrough

```
-----
Interface Type MAC VLAN State Uplink-Int
Pri Sec Oper Adm
-----
```

```
VsbEthernet1/1 gw-uplink1 up up
VsbEthernet1/2 management 168 up up
VsbEthernet1/3 gw-uplink2 up up
internal NA NA NA up up
HA Role: Primary
HA Status: NONE
```

```
Status: VSB NOT PRESENT
Location: PRIMARY
SW version:
HA Role: Secondary
HA Status: NONE
Status: VSB NOT PRESENT
Location: SECONDARY
SW version:
VSB Info:
```

Vérifiez le résumé de réseau afin de visualiser les liaisons ascendantes disponibles. Les interfaces de passerelle VXLAN doivent être placées dans un mode de fonction émulation et être goupillées à une liaison ascendante d'appareils de gamme 1x10 de Nexus. Sélectionnez la commande de **show network summary** afin de visualiser le résumé de réseau :

```
1010(config-vsbs-config)# show network summary
```

```
Legends: P - Passthrough
```

```
-----
Port State Uplink-Interface Speed RefCnt MTU Nat-Vlan
Oper Admin Oper Admin Oper Admin
-----
```

```
Gi1 up up 1000 1 9000
Gi2 up up 1000 1 9000
Gi3 up up 1000 0 9000
Gi4 up up 1000 0 9000
Gi5 up up 1000 0 9000
Gi6 up up 1000 0 9000
control0 up up Gi1 Gi1 1000 9000
mgmt0 up up Gi2 Gi2 1000 9000
```

Pin que le VSB relie aux liaisons ascendantes d'appareils de gamme 1x10 de Nexus et les a placées au mode de fonction émulation. Vous devez également configurer un ID DE VLAN pour l'interface de la Gestion VSB.

Remarque: Assurez-vous que vous avez le LACP activé sur les interfaces en amont. Quand vous configurez ces sections, les interfaces avec liaison ascendante exécutent le LACP.

Sélectionnez ces commandes afin de goupiller les interfaces VSB aux liaisons ascendantes :

```
1010(config-vsbs-config)# interface gw-uplink1 uplink GigabitEthernet3
1010(config-vsbs-config)# interface gw-uplink2 uplink GigabitEthernet4
1010(config-vsbs-config)# interface gw-uplink1 mode passthrough
1010(config-vsbs-config)# interface gw-uplink2 mode passthrough
1010(config-vsbs-config)# interface management uplink GigabitEthernet2
1010(config-vsbs-config)# interface management vlan 168
```

Une fois que les liaisons ascendantes de réseau sont configurées, activez le VSB et le vérifiez que le déploiement est réussi. Il y a de nombreux champs que vous devez écrire les informations dans quand vous déployez le VSB ; vous devez ajouter les adresses MAC primaires et de réserve du VSM qui a été précédemment décrit. **Le module de service** est la passerelle VXLAN. En outre, deux adresses IP sont nécessaires afin de se terminer l'installation.

```
1010(config-vsbs-config)# enable
Enter vsb image: [vxgw.4.2.1.SV2.2.1.iso]
Enter the VSM domain id[1-4095]: 27
Enter Management IP version [V4]: [V4]
Enter Management IP address of service module on primary: 10.10.168.101
Enter Management subnet mask of service module on primary: 255.255.255.0
Enter default gateway IP address of service module on primary: 10.10.168.254
Enter management IP address of service module on secondary: 10.10.168.102
Enter management subnet mask of service module on secondary: 255.255.255.0
```

```
Enter default gateway IP address of service module on secondary: 10.10.168.254
Enter HostName: VXLANGW
Enter the password for 'admin': S0lT3st1ng
VSM L3 Ctrl IPv4 address : 10.10.168.2
VSM Primary MAC Address: 0050.56bc.6a3d
VSM Standby MAC Address: 0050.56bc.74f1
Enter VSM uplink port-profile name: vxgw-pc
Enter VTEP port-profile name: vxgw-vtep
----Details entered----
```

DomainId : 27

IPV4V6 : V4PriMgmtIPv4 : 10.10.168.101

PriMgmtIPv4Subnet : 255.255.255.0

PriGatewayIPv4 : 10.10.168.254

SecMgmtIPv4 : 10.10.168.102

SecMgmtIPv4Subnet : 255.255.255.0

SecGatewayIPv4 : 10.10.168.254

HostName : VXLANGW

Password : S0lT3st1ng

VSMIPv4 : 10.10.168.2

VSMPriMac : 0050.56bc.6a3d

VSMStdbyMac : 0050.56bc.74f1

UplinkPPName : vxgw-pcVSMEncapPPName : vxgw-vtep

Do you want to continue installation with entered details (Y/N)? [Y]

Note: VSB installation is in progress, please use show virtual-service-blade commands to check the installation status.

Note: VSB installation may take up to 5 minutes.

Sélectionnez la commande **récapitulative de virtuel-service-lame d'exposition** sur l'appliance de gamme 1x10 de Nexus afin de vérifier que le VSB est déployé et mis sous tension :

```
1010(config-vsbs-config)# show virtual-service-blade summary
```

```
-----
Name HA-Role HA-Status Status Location
-----
```

```
VXGW PRIMARY ACTIVE VSB POWERED ON PRIMARY
```

```
VXGW SECONDARY NONE VSB DEPLOY IN PROGRESS SECONDARY
```

Vérifiez les modules dans le VSM

Les passerelles VXLAN sont maintenant ajoutées comme modules dans la configuration VSM. Sélectionnez la commande de **show module** sur le VSM afin de vérifier :

```
Nexus1000v# show module
```

```
Mod Ports Module-Type Model Status
```

```
-----
1 0 Virtual Supervisor Module Nexus1000V ha-standby
```

```
2 0 Virtual Supervisor Module Nexus1000V active *
```

```
3 248 Virtual Ethernet Module NA ok
```

```
4 248 Virtual Ethernet Module NA ok
```

```
5 332 Virtual Ethernet Module NA ok
```

```
6 332 Virtual Ethernet Module NA ok
```

```
7 4 Virtual Service Module VXLAN Gateway ok
```

```
8 4 Virtual Service Module VXLAN Gateway ok
```

```
Mod Sw Hw
```

```
-----
1 4.2(1)SV2(2.1) 0.0
```

```
2 4.2(1)SV2(2.1) 0.0
```

```
3 4.2(1)SV2(2.1) VMware ESXi 5.1.0 Releasebuild-799733 (3.1)
```

```
4 4.2(1)SV2(2.1) VMware ESXi 5.1.0 Releasebuild-799733 (3.1)
```

```

5 4.2(1)SV2(2.1) VMware ESXi 5.1.0 Releasebuild-799733 (3.1)
6 4.2(1)SV2(2.1) VMware ESXi 5.1.0 Releasebuild-799733 (3.1)
7 4.2(1)SV2(2.1) Linux 2.6.27.10
8 4.2(1)SV2(2.1) Linux 2.6.27.10

```

```
Mod Server-IP Server-UUID Server-Name
```

```

-----
1 10.10.168.2 NA NA
2 10.10.168.2 NA NA
3 10.10.168.1 24266920-d498-11e0-0000-00000000000f 10.10.168.1
4 10.10.168.4 24266920-d498-11e0-0000-00000000000e 10.10.168.4
5 10.10.168.5 d54be571-831f-11df-aaa7-d0d0fd095a08 10.10.168.5
6 10.10.168.3 24266920-d498-11e0-0000-00000000000c 10.10.168.3
7 10.10.168.101 e6b86534-5d0c-4cde-a48e-2b555f929d2b VXLANGW
8 10.10.168.102 06cc2f30-bc2b-4b6f-a7d2-4e712c530761 VXLANGW

```

Formez une Haute disponibilité

Maintenant vous pouvez configurer les modules dans une paire (ha) facilement disponible.

Sélectionnez la **commande service-module de show module** sur le VSM afin de vérifier le statut des modules :

```
Nexus1000v# show module service-module
```

```
Mod Cluster-id Role HA Mode Status
```

```

-----
7 0 Unconfigured Standalone Init
8 0 Unconfigured Standalone Init

```

Afin de configurer l'ha, assurez-vous que le nombre de batterie apparie le service instance dans le port-profil de liaison ascendante de passerelle VXLAN :

```
Nexus1000v# configure t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Nexus1000v(config)# service 7 role primary ha-cluster 1
```

```
Nexus1000v(config)# service 8 role secondary ha-cluster 1
```

Vérifiez que la passerelle VXLAN forme une paire ha. En outre, vérifiez que les Ports canalisés sont configurés pour le LACP et qu'ils sont **en activité** :

```
Nexus1000v# show module service-module
```

```
Mod Cluster-id Role HA Mode Status
```

```

-----
7 1 Primary HA Active
8 1 Secondary HA StandbyNexus1000v# show port-channel summary

```

```
Flags: D - Down P - Up in port-channel (members)
```

```
I - Individual H - Hot-standby (LACP only)
```

```
s - Suspended r - Module-removed
```

```
S - Switched R - Routed
```

```
U - Up (port-channel)
```

```

-----
Group Port- Type Protocol Member Ports
Channel
-----

```

```
1 Po1(SU) Eth NONE Eth4/1(P) Eth4/2(P)
```

```
2 Po2(SU) Eth NONE Eth3/1(P) Eth3/2(P)
```

```
3 Po3(SU) Eth NONE Eth6/1(P) Eth6/2(P)
```

```
4 Po4(SU) Eth NONE Eth5/2(P)
```

```
5 Po5(SD) Eth NONE --
6 Po6(SU) Eth LACP Eth7/1(P) Eth7/3(P)
7 Po7(SU) Eth LACP Eth8/1(P) Eth8/3(P)
```

Sélectionnez la commande de **ha-batterie de service** si vous voulez au basculement la passerelle VXLAN :

```
Nexus1000v# service ha-cluster 1 switchover
```

Remarque: Cette commande de basculement est différente qu'une commande du système d'exploitation de basculement de Nexus traditionnel (NXOS) parce que vous devez basculement la batterie ha que vous avez créée.

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

[L'Output Interpreter Tool](#) (clients [enregistrés](#) seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

VSM CLI

Vérifiez que le VTEPs sont programmés correctement sur le VSM :

```
Nexus1000v# show bridge-domain 192.168.2.x vteps

D: Designated VTEP I:Forwarding Publish Incapable VTEP

Bridge-domain: 192.168.2.xVTEP Table Version: 9

Port Module VTEP-IP Address VTEP-Flags
-----
Veth11 3 10.17.168.20 (D)
Veth28 4 10.17.168.22 (D)
Veth21 7 10.17.124.70 (DI*) <---- VXLAN GW
Veth22 8 10.17.124.70 (DI) <---- VXLAN GW (Standby)
```

Commandes VEM

Il y a beaucoup de VEM commande (VEMCMDs) que vous pouvez utiliser afin de vérifier la configuration, visualiser les statistiques, et valider l'installation de votre VXLAN. Afin de visualiser les commandes disponibles, recherchez la base de données avec le **vemcmd | commande vxlan de grep** :

```
~ # vemcmd | grep vxlan
```

```
show vxlan interfaces Show the VXLAN Encap Interfaces
show vxlan-encap ltl <ltl> Show VXLAN Encap Information
show vxlan-encap mac <MAC.MAC.MAC>
show vxlan-stats Show VXLAN port stats for all ports
show vxlan-stats bd-all Show VXLAN port stats for all BDs
show vxlan-stats ltl <ltl> Show VXLAN port stats detail
show vxlan-stats ltl-detail Show all VXLAN ports stats detail
```

```
show vxlan-stats ltl <ltl> bd-all cookie <number>
show vxlan-stats ltl <ltl> bd-name <bd-name>
show vxlan-vteps Show VXLAN VTEPs
show vxlan-vteps bd-name <bd-name>
show vxlan threads Show the VXLAN thread stats
clear vxlan threads Clear the VXLAN thread stats
show vlan-vxlan mapping Show VXLAN VLAN mappings
```

Écrivez l'**exposition de vemcmd les interfaces que vxlan** commandent afin de vérifier que le VEM est programmé avec le VTEP correct :

```
~ # vemcmd show vxlan interfaces
LTL VSM Port IP Seconds since Last Vem Port
IGMP Query Received
(* = IGMP Join Interface/Designated VTEP)
-----
51 Veth6 10.10.168.22 33 vmk2*
```

Remarque: * dans la sortie affiche le VTEP qui est le récepteur indiqué sur l'hôte.

Vous devriez également vérifier que les **secondes** puisque la dernière requête IGMP a reçu des transitions de nombre à 0 après une certaine heure. Le moment de requête du par défaut IGMP pour NXOS est de 125 secondes. Ceci montre que des requêtes IGMP sont reçues sur le VTEP et que le transport de Multidiffusion est fonctionnel.

Remarque: Vous ne pouvez pas voir les ports de vEthernet VTEP dans la sortie du **show ip igmp snooping groups** commander sur un N1kV. Par défaut, tout les trafic de multidiffusion pour les groupes de domaine de passerelle est inondé sur le transport VLAN ; ainsi, la surveillance IGMP n'est pas utilisée sur le N1kV.

Sélectionnez la commande de **<x> LTL de vxlan-encap d'exposition de vemcmd** afin de visualiser les informations d'encapsulation pour une VM de particularité :

```
~ # vemcmd show vxlan-encap ltl 53

Encapsulation details for LTL 53 in BD "192.168.1.x":
Source MAC: 00:50:56:bc:77:25
Segment ID: 5000
Multicast Group IP: 239.1.1.1

Encapsulating VXLAN Interface LTL: 51
Encapsulating Source IP: 10.10.168.22
Encapsulating Source MAC: 00:50:56:6d:7a:25

Pinning of VXLAN Interface to the Uplink:
LTL IfIndex PC_LTL VSM_SGID Eff_SGID iSCSI_LTL* Name
51 1c000050 561 32 0 0 vmk2= IGMP Join
```

Écrivez les **vxlan-stats d'exposition de vemcmd** commandent sur l'hôte afin de vérifier les statistiques pour VXLAN. Cette commande montre le nombre d'encapsulations et De-encapsulations qui se produisent pour chaque logique locale de cible VM (LTL).

Remarque: Tous les émission et trafic de multidiffusion est classifiée en tant qu'**encaps Mcast/Repl**. C'est parce que le trafic doit être envoyé à tout le VTEPs. Le trafic unicast est classifié comme **encaps d'Ucast**. Si vous tentez de dépanner une question où l'ARP ne se termine pas, alors vérifiez que la colonne d'**encaps Mcast/Repl** incrémente avec chaque demande d'ARP.

```
~ # vemcmd show vxlan-stats
LTL Ucast Mcast/Repl Ucast Mcast Total
Encaps Encaps Decaps Decaps Drops
51 7557 507 8012 0 0
53 7137 431 7512 0 0
```

Sélectionnez la commande du **segment 5001 de l'exposition 12 de vemcmd** afin de vérifier que l'hôte de source apprend l'adresse MAC de la destination dynamiquement :

```
~ # vemcmd show l2 segment 5001
Bridge domain 14 brtmax 4096, brtcnt 2, timeout 300
Segment ID 5001, swbd 4097, "192.168.2.x"
Flags: P - PVLAN S - Secure D - Drop
Type MAC Address LTL timeout Flags PVLAN Remote IP DSN
Static 00:50:56:bc:77:25 55 0 0.0.0.0 0
Dynamic 00:50:56:bc:19:5b 561 0 10.17.168.22 0
```

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.