Guide de dépannage de NSX

Mise à jour 8
Modifié le 21 février 2020
VMware NSX Data Center for vSphere 6.3

vmware®

Vous trouverez la documentation technique la plus récente sur le site Web de VMware, à l'adresse :

https://docs.vmware.com/fr/

Si vous avez des commentaires à propos de cette documentation, envoyez-les à l'adresse suivante :

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware France SAS.
Tour Franklin
100-101 Terrasse Boieldieu
92042 Paris La Défense 8 Cedex
France
www.vmware.com/fr

Table des matières

Guide de dépannage de NSX 1

Le *Guide de dépannage de NSX* décrit comment surveiller et dépanner le système VMware NSX® for vSphere® en utilisant l'interface utilisateur de NSX Manager, vSphere Web Client et d'autres composants de NSX, si nécessaire.

Public visé

Ce guide est destiné à toute personne souhaitant utiliser NSX ou résoudre un problème lié à ce système dans un environnement VMware vCenter. Les informations qu'il contient sont destinées aux administrateurs système expérimentés qui sont familiarisés avec la technologie des machines virtuelles et les opérations de centres de données virtuels. Ce guide suppose que vous connaissez VMware vSphere, notamment VMware ESXi vCenter Server et vSphere Web Client.

Glossaire VMware Technical Publications

VMware Technical Publications fournit un glossaire de termes pouvant ne pas vous être familiers. Pour consulter la définition des termes utilisés dans la documentation technique VMware, visitez le site Web http://www.vmware.com/support/pubs.

Ce chapitre contient les rubriques suivantes :

Directives générales sur le dépannage

Cette rubrique décrit les directives générales que vous pouvez suivre pour résoudre les problèmes liés à NSX pour vSphere.

1. Accédez au Utilisation du tableau de bord de NSX et voyez si des erreurs ou des avertissements sont affichés pour un composant.
2. Accédez à l'onglet **Surveiller (Monitor)** de l'instance principale de NSX Manager et voyez s'il existe des événements système déclenchés. Pour plus d'informations sur les événements système et les alarmes, consultez *Journalisation et événements système dans NSX*.
3. Utilisez l'API `GET api/2.0/services/systemalarms` pour afficher les alarmes sur l'objet NSX. Pour plus d'informations sur l'API, consultez le *Guide de NSX API*.
4. Résolvez le problème comme décrit dans le *Guide de dépannage de NSX*.

5 Si votre problème n'est pas résolu, téléchargez les journaux de support technique et contactez le support VMware. Consultez l'article « How to file a Support Request in My VMware (Comment soumettre une demande de support dans My VMware) ». Pour plus d'informations sur le téléchargement des journaux, consultez *Journalisation et événements système dans NSX*.

Utilisation du tableau de bord de NSX

Le tableau de bord de NSX affiche l'état général des composants NSX dans une vue centralisée. Le tableau de bord de NSX simplifie le dépannage en affichant l'état des différents composants NSX tels que les instances de NSX Manager, les contrôleurs, les commutateurs logiques, la préparation de l'hôte, le déploiement des services, la sauvegarde ainsi que les notifications Edge.

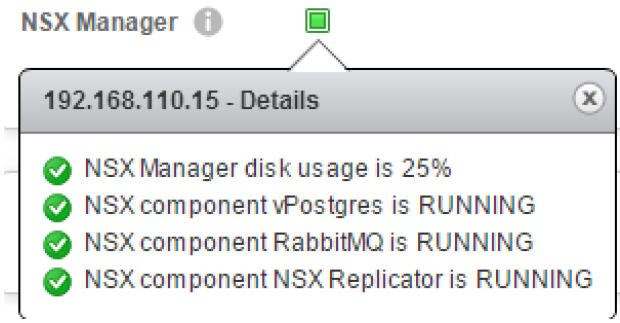
1 Connectez-vous à vSphere Web Client.

2 Cliquez sur **Networking & Security**, puis sur **Tableau de bord (Dashboard)**. La page Tableau de bord s'affiche.

3 Dans un environnement Cross-vCenter NSX, sélectionnez NSX Manager avec le rôle principal ou le rôle secondaire.

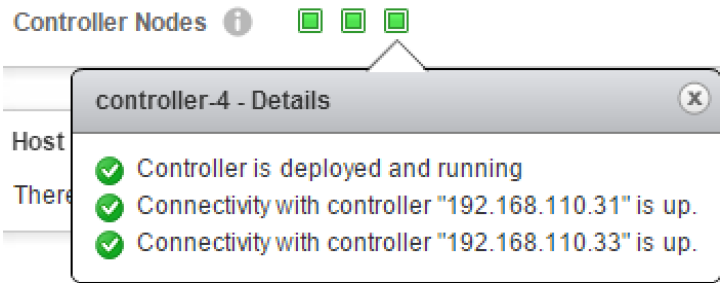
Le tableau de bord fournit les informations suivantes :

- Infrastructure NSX : l'état de composant de NSX Manager des services suivants est surveillé :
  - Service de base de données (vPostgres).
  - Service du bus de messages (RabbitMQ).
  - Service de réplicateur : surveille également les erreurs de réplication (si Cross-vCenter NSX est activé).
  - Utilisation du disque de NSX Manager :
    - Jaune indique une utilisation du disque supérieure à 80 %.
    - Rouge indique une utilisation du disque supérieure à 90 %.

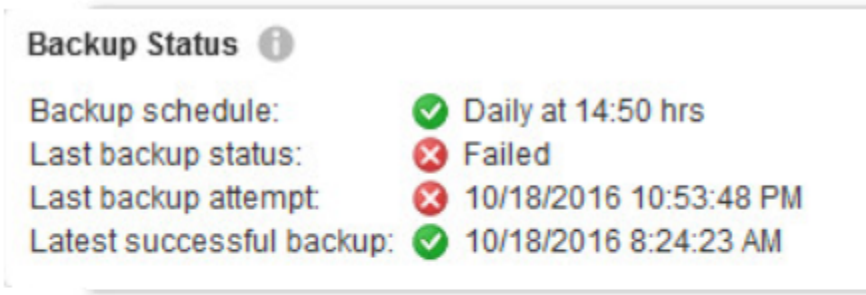


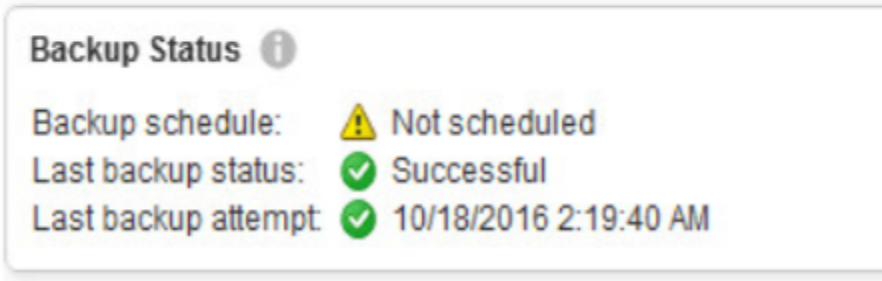
- Infrastructure NSX : état de NSX Controller :
  - État du nœud de contrôleur (actif/inactif/en cours d'exécution/en cours de déploiement/en cours de suppression/échec/inconnu).
  - L'état de connectivité de l'homologue de contrôleur s'affiche. Si le contrôleur est inactif en Rouge, les contrôleurs homologues sont affichés en Jaune.

- État de la VM de contrôleur (désactivée/supprimée).
- Alertes de latence de disque du contrôleur.



- État de la sauvegarde de NSX Manager :
  - Planification des sauvegardes.
  - État de la dernière sauvegarde (Échec/réussite/non planifiée avec date et heure).
  - Dernière tentative de sauvegarde (date et heure avec détails).
  - Dernière sauvegarde réussie (date et heure avec détails).





- Infrastructure NSX : l'état d'hôte des services suivants est surveillé :
  - Déploiement lié :
    - Nombre de clusters avec l'état d'échec de l'installation.
    - Nombre de clusters nécessitant une mise à niveau.
    - Nombre de clusters où l'installation est en cours.

        - Nombre de clusters non préparés.
    - Pare-feu :
        - Nombre de clusters avec le pare-feu désactivé.
        - Nombre de clusters avec l'état de pare-feu jaune/rouge :
            - Jaune indique que le pare-feu distribué est désactivé sur l'un des clusters.
            - Rouge indique que le pare-feu distribué n'a pas pu être installé sur l'un des hôtes/clusters.
    - VXLAN :
        - Nombre de clusters avec VXLAN non configuré.
        - Nombre de clusters avec l'état VXLAN vert/jaune/rouge :
            - Vert indique que la fonctionnalité a été correctement configurée.
            - Jaune signifie occupé lorsque la configuration de VXLAN est en cours.
            - Rouge (erreur) indique l'état lorsque la création de VTEP a échoué, lorsque le VTEP n'a pas pu trouver l'adresse IP, lorsqu'une adresse IP *LinkLocal* a été attribuée au VTEP, etc.
- Infrastructure NSX : État du déploiement des services
    - Échecs de déploiement : état de l'installation pour les déploiements ayant échoué.
    - État de service : pour tous les services en échec.
- Infrastructure NSX : notifications NSX Edge

  Le tableau de bord des notifications Edge met en avant les alarmes actives pour certains services. Elle surveille la liste des événements critiques répertoriés ci-dessous et les suit jusqu'à ce que le problème ne soit pas résolu. Les alarmes sont résolues automatiquement lorsqu'un événement de récupération est signalé ou lorsque la synchronisation, le redéploiement ou la mise à niveau d'Edge est forcée.
    - Équilibrage de charge (état du serveur d'équilibrage de charge Edge) :
        - Le serveur principal de l'équilibrage de charge Edge est inactif.
        - État d'avertissement du serveur principal de l'équilibrage de charge Edge.
    - VPN (tunnel IPSec/état du canal IPSec) :
        - Le canal IPSec Edge est inactif.
        - Le tunnel IPSec Edge est inactif.
    - Dispositif (état des rapports de VM Edge, passerelle Edge, système de fichiers Edge, NSX Manageret Edge Services Gateway) :
        - Pulsation de contrôle d'intégrité manquante pour Edge Services Gateway.
        - La VM Edge a été désactivée.
        - Pulsation de contrôle d'intégrité manquante pour la VM Edge.

- NSX Edge signale un état incorrect.
- NSX Manager signale qu'Edge Services Gateway est défectueux.
- La VM Edge n'est pas présente dans l'inventaire VC.
- Split Brain HA détecté.

Note Les alarmes de l'équilibrage de charge et VPN ne sont pas effacées automatiquement lors de la mise à jour de la configuration. Une fois que le problème est résolu, vous devez effacer manuellement les alarmes avec l'API à l'aide de la commande `alarm-id`. Voici l'exemple d'API que vous pouvez utiliser pour effacer les alarmes. Pour plus de détails, consultez le *Guide de NSX API*.

```
GET https://<<NSX-IP>>/api/2.0/services/alarms/{source-Id}
POST https://<<NSX-IP>>/api/2.0/services/alarms?action=resolve

GET https://<<NSX-IP>>/api/2.0/services/systemalarms/<alarmId>
POST https://<<NSX-IP>>/api/2.0/services/systemalarms/<alarmId>?action=resolve
```

- NSX Services : état de publication du pare-feu :
  - Nombre d'hôtes avec l'état de publication du pare-feu échoué. L'état est Rouge lorsqu'un hôte n'applique pas correctement la configuration du pare-feu distribué publié.
- NSX ServicesNSX : état de la mise en réseau logique :
  - Nombre de commutateurs logiques avec l'état `Erreur` ou `Avertissement`.
  - Signale lorsque le groupe de ports distribué sur lequel il repose est supprimé de vCenter Server.

Référence rapide des lignes de commande de NSX

Vous pouvez utiliser l'interface de ligne de commande de NSXpour résoudre les problèmes.

Tableau 1-1. Vérification de l'installation de NSX sur l'hôte ESXi - Commandes exécutées depuis NSX Manager

Description	Commandes sur NSX Manager	Remarques
Lister tous les clusters pour obtenir les ID de cluster	`show cluster all`	Afficher toutes les informations des clusters
Lister tous les hôtes dans le cluster pour obtenir les ID d'hôte	`show cluster` *clusterID*	Afficher la liste d'hôtes dans le cluster, les ID d'hôte et l'état d'installation de préparation de l'hôte
Lister toutes les VM sur un hôte	`show host` *hostID*	Afficher des informations particulières sur l'hôte, des VM, des ID de VM et l'état de l'alimentation

Tableau 1-2. Noms des VIB et des modules installés sur les hôtes à utiliser dans les commandes

Version de NSX	Version d'ESXi	VIB	Modules
N'importe quelle version 6.3.x	5.5	esx-vxlan et esx-vsip	vdl2, vdrb, vsip, dvfilter-switch-security, bfd, traceflow
6.3.2 et versions antérieures	6.0 et versions ultérieures	esx-vxlan et esx-vsip	vdl2, vdrb, vsip, dvfilter-switch-security, bfd, traceflow
6.3.3 et versions ultérieures	6.0 et versions ultérieures	esx-nsxv	nsx-vdl2, nsx-vdrb, nsx-vsip, nsx-dvfilter-switch-security, nsx-core, nsx-bfd, nsx-traceflow

Tableau 1-3. Vérification de l'installation de NSX sur l'hôte ESXi - Commandes exécutées depuis l'hôte

Description	Commandes sur l'hôte	Remarques
Les VIB présents dépendent des versions de NSX et d'ESXi. Reportez-vous au tableau *Noms des VIB et des modules installés sur les hôtes* pour plus d'informations sur les modules à vérifier dans votre installation.	`esxcli software vib get --vibname <name>`	Vérifier la version/date installée `esxcli software vib list` affiche une liste de tous les VIB sur le système
Lister tous les modules système actuellement chargés dans le système	`esxcli system module list`	Commande équivalente précédente : `vmkload_mod -l | grep -E vdl2|vdrb|vsip|dvfilter-switch-security`
Les modules présents dépendent des versions de NSX et d'ESXi. Reportez-vous au tableau *Noms des VIB et des modules installés sur les hôtes* pour plus d'informations sur les modules à vérifier dans votre installation.	`esxcli system module get -m <name>`	Exécuter la commande pour chaque module
Deux agents UWA : agent du plan de contrôle, agent de pare-feu	`/etc/init.d/vShield-Stateful-Firewall status` `/etc/init.d/netcpad status`	
Vérifier la connexion des agents UWA, le port 1234 vers les contrôleurs et le port 5671 vers NSX Manager	`esxcli network ip connection list | grep 1234` `esxcli network ip connection list | grep 5671`	Connexion TCP du contrôleur Connexion TCP du bus de messages
Vérifier l'état d'EAM	vSphere Web Client, vérifiez **Administration > vSphere ESX Agent Manager**	

Tableau 1-4. Vérification de l'installation de NSX sur un hôte ESXi - Commandes de mise en réseau de l'hôte

Description	Commandes de mise en réseau de l'hôte	Remarques
Lister les cartes réseau physiques/vmnic	`esxcli network nic list`	Vérifier le type de carte réseau, le type de pilote, l'état du lien, MTU
Détails de la carte réseau physique	`esxcli network nic get –n vmnic#`	Vérifier les versions du pilote et du micrologiciel et d'autres détails
Lister les cartes réseau vmk avec des adresses IP/MAC/MTU, etc.	`esxcli network ip interface ipv4 get`	Pour s'assurer que les VTEP sont correctement instanciés
Détails de chaque carte réseau vmk, y compris les informations vDS	`esxcli network ip interface list`	Pour s'assurer que les VTEP sont correctement instanciés
Détails de chaque carte réseau vmk, y compris les infos vDS pour VXLAN vmks	`esxcli network ip interface list ––netstack=vxlan`	Pour s'assurer que les VTEP sont correctement instanciés
Rechercher le nom VDS associé au VTEP de cet hôte	`esxcli network vswitch dvs vmware vxlan list`	Pour s'assurer que les VTEP sont correctement instanciés
Effectuer une commande ping depuis une pile TCP/IP dédiée à VXLAN	`ping ++netstack=vxlan –I vmk1 x.x.x.x`	Pour résoudre les problèmes de communication VTEP : ajouter l'option `–d –s 1572` pour s'assurer que le MTU de réseau de transport est correct pour VXLAN
Afficher une table de routage de la pile TCP/IP dédiée à VXLAN	`esxcli network ip route ipv4 list –N vxlan`	Pour résoudre les problèmes de communication VTEP
Afficher une table ARP de la pile TCP/IP dédiée à VXLAN	`esxcli network ip neighbor list –N vxlan`	Pour résoudre les problèmes de communication VTEP

Tableau 1-5. Vérification de l'installation de NSX sur un hôte ESXi - Fichiers journaux de l'hôte

Description	Fichier journal	Remarques
À partir de NSX Manager	`show manager log follow`	Suit les journaux de NSX Manager Pour un dépannage en temps réel
Des journaux liés à l'installation pour un hôte	`/var/log/esxupdate.log`	

Problèmes liés à l'hôte
Avertissement VMkernel, messages, alertes et rapport de disponibilité
	`/var/log/vmkernel.log`
	`/var/log/vmksummary.log`
	`/var/log/vmkwarning.log`	

L'échec de la charge de module est capturé	`/var/log/syslog`	Échec du pilote IXGBE Les échecs de dépendance des modules NSX sont des indicateurs clés
Sur vCenter, ESX Agent Manager est responsable des mises à jour	Dans les journaux de vCenter, `eam.log`	

Tableau 1-6. Vérification de la commutation logique - Commandes exécutées à partir de NSX Manager

Description	Commande sur NSX Manager	Remarques
Lister tous les commutateurs logiques	`show logical-switch list all`	Lister tous les commutateurs logiques, leurs UUID à utiliser dans API, la zone de transport et vdnscope

Tableau 1-7. Commutation logique - Commandes exécutées à partir de NSX Controller

Description	Commandes sur le contrôleur	Remarques
Rechercher le contrôleur propriétaire du VNI	`show control-cluster logical-switches vni 5000`	Noter l'adresse IP du contrôleur dans la sortie et SSH vers elle
Rechercher tous les hôtes connectés à ce contrôleur pour ce VNI	`show control-cluster logical-switch connection-table 5000`	L'adresse IP source dans la sortie est l'interface de gestion de l'hôte et le numéro de port est le port source de la connexion TCP
Rechercher les VTEP enregistrés pour héberger ce VNI	`show control-cluster logical-switches vtep-table 5002`	
Lister les adresses MAC apprises pour les VM sur ce VNI	`show control-cluster logical-switches mac-table 5002`	Vérifier que l'adresse MAC se trouve en réalité sur le VTEP la signalant
Lister le cache ARP rempli par les mises à jour d'adresses IP de la VM	`show control-cluster logical-switches arp-table 5002`	Le cache ARP expire dans 180 s
Pour une paire hôte/contrôleur spécifique, trouver quels VNI l'hôte a rejoint	`show control-cluster logical-switches joined-vnis <host_mgmt_ip>`	

Tableau 1-8. Commutation logique - Commandes exécutées depuis des hôtes

Description	Commande sur les hôtes	Remarques
Vérifier si VXLAN de l'hôte est synchronisé ou pas	`esxcli network vswitch dvs vmware vxlan get`	Affiche l'état de synchronisation et le port utilisé pour l'encapsulation
Afficher la VM associée et l'ID de port de commutateur local pour les captures de chemin de données	`net-stats -l`	Une meilleure façon d'obtenir le port de commutateur de VM pour une VM spécifique
Vérifier que le module de noyau VXLAN vdl2 est chargé	`esxcli system module get -m vdl2`	Afficher des détails complets du module spécifié. Vérifier la version

Vérifier que la version correcte de VIB VXLAN est installée
Reportez-vous au tableau *Noms des VIB et des modules installés sur les hôtes* pour plus d'informations sur les VIB à vérifier dans votre installation.
	`esxcli software vib get --vibname esx-vxlan`
	ou
	`esxcli software vib get --vibname esx-nsxv`
		Afficher des détails complets du VIB spécifié
		Vérifier la version et la date

Vérifier que l'hôte connaît les autres hôtes dans le commutateur logique	`esxcli network vswitch dvs vmware vxlan network vtep list --vxlan-id=5001 --vds-name=Compute_VDS`	Affiche une liste de tous les VTEP que cet hôte connaît qui hébergent vtep 5001

Tableau 1-8. Commutation logique - Commandes exécutées depuis des hôtes (suite)

Description	Commande sur les hôtes	Remarques
Vérifier que le plan de contrôle est exécuté et actif pour un commutateur logique	`esxcli network vswitch dvs vmware vxlan network list --vds-name Compute_VDS`	S'assurer que la connexion de contrôleur est exécutée et que le nombre de ports/adresses MAC correspond aux VM sur le commutateur logique sur cet hôte
Vérifier que l'hôte a appris les adresses MAC de toutes les VM	`esxcli network vswitch dvs vmware vxlan network mac list --vds-name Compute_VDS --vxlan-id=5000`	Devrait lister toutes les adresses MAC des VM VNI 5000 sur cet hôte
Vérifier que l'hôte dispose en local d'une entrée ARP en cache pour les VM distantes	`esxcli network vswitch dvs vmware vxlan network arp list --vds-name Compute_VDS --vxlan-id=5000`	Vérifier que l'hôte dispose en local d'une entrée ARP en cache pour les VM distantes
Vérifier que la VM est connectée au commutateur logique et mappée vers un VMKnic local Affiche également vers quel ID vmknic un dvPort de VM est mappé	`esxcli network vswitch dvs vmware vxlan network port list --vds-name Compute_VDS --vxlan-id=5000`	Le vdrport sera toujours listé tant que le VNI est associé à un routeur
Afficher les ID de vmknic et vers quel port de commutateur/liaison montante ils sont mappés	`esxcli network vswitch dvs vmware vxlan vmknic list --vds-name=DSwitch-Res01`	

Tableau 1-9. Vérification de la commutation logique - Fichiers journaux

Description	Fichier journal	Remarques
Les hôtes sont toujours connectés à des contrôleurs hébergeant leurs VNI	`/etc/vmware/netcpa/config-by-vsm.xml`	Ce fichier doit toujours avoir tous les contrôleurs dans l'environnement listés. Le fichier `config-by-vsm.xml` est créé par le processus netcpa
Le fichier `config-by-vsm.xml` est transféré par NSX Manager à l'aide de vsfwd Si le fichier `config-by-vsm.xml` n'est pas correct, consulter le journal vsfwd	`/var/log/vsfwd.log`	Analyser ce fichier pour rechercher les erreurs Pour redémarrer le processus : `/etc/init.d/vShield-Stateful-Firewall stop|start`
La connexion au contrôleur est effectuée à l'aide de netcpa	`/var/log/netcpa.log`	Analyser ce fichier pour rechercher les erreurs
Les journaux de module de commutation logique se trouvent dans *vmkernel.log*	`/var/log/vmkernel.log`	Consulter les journaux de module de commutation logique dans */var/log/vmkernel.log* avec le préfixe VXLAN :

Tableau 1-10. Vérification du routage logique - Commandes exécutées à partir de NSX Manager

Description	Commandes sur NSX Manager	Remarques
Commandes pour la passerelle ESG	`show edge`	Les commandes CLI pour la passerelle ESG (Edge Services Gateway) commencent par 'show edge'
Commandes pour la VM de contrôle du DLR	`show edge`	Les commandes CLI pour la VM de contrôle du DLR (routeur logique distribué) commencent par 'show edge'
Commandes pour le DLR	`show logical-router`	Les commandes CLI pour le DLR (routeur logique distribué) commencent par `show logical-router`
Lister tous les dispositifs Edge	`show edge all`	Lister tous les dispositifs Edge qui prennent en charge l'interface de ligne commande centrale
Lister tous les services et les détails de déploiement d'un dispositif Edge	`show edge edgeID`	Afficher les informations de la passerelle ESG
Lister les options de commande d'un dispositif Edge	`show edge edgeID ?`	Afficher des détails, tels que la version, le journal, NAT, la table de routage, le pare-feu, la configuration, l'interface et les services
Afficher les détails du routage	`show edge edgeID ip ?`	Afficher les infos de routage, BGP, OSPF et d'autres détails
Afficher la table de routage	`show edge edgeID ip route`	Afficher la table de routage sur un dispositif Edge
Afficher le voisin de routage	`show edge edgeID ip ospf neighbor`	Afficher la relation de voisin de routage
Afficher les informations de connexion des routeurs logiques	`show logical-router host hostID connection`	Vérifier que le nombre de LIF connectées est correct, que la stratégie d'association est bonne et que le vDS approprié est utilisé
Lister toutes les instances de routeur logique exécutées sur l'hôte	`show logical-router host hostID dlr all`	Vérifier le nombre de LIF et d'itinéraires L'adresse IP du contrôleur doit être la même sur tous les hôtes pour un routeur logique Plan de contrôle actif doit être oui --brief donne une réponse compacte

Tableau 1-10. Vérification du routage logique - Commandes exécutées à partir de NSX Manager (suite)

Description	Commandes sur NSX Manager	Remarques
Consulter la table de routage sur l'hôte	`show logical-router host hostID dlr dlrID route`	Il s'agit de la table de routage transférée par le contrôleur à tous les hôtes dans la zone de transport Elle doit être la même sur tous les hôtes Si des itinéraires sont manquants sur quelques hôtes, essayer la commande sync depuis le contrôleur mentionné précédemment L'indicateur E signifie que des itinéraires sont appris via ECMP
Consulter les LIF pour un DLR sur l'hôte	`show logical-router host hostID dlr dlrID interface (all | intName) verbose`	Les informations de LIF sont transférées à des hôtes à partir du contrôleur Utiliser cette commande pour s'assurer que l'hôte connaît toutes les LIF qu'il devrait

Tableau 1-11. Vérification du routage logique - Commandes exécutées à partir de NSX Controller

Description	Commandes sur NSX Controller	Remarques
Rechercher toutes les instances du routeur logique	`show control-cluster logical-routers instance all`	Devrait lister l'instance du routeur logique et tous les hôtes dans la zone de transport sur lesquels l'instance du routeur logique devrait être installée De plus, affiche le contrôleur qui maintient ce routeur logique
Afficher les détails de chaque routeur logique	`show control-cluster logical-routers instance 0x570d4555`	La colonne IP indique les adresses IP vmk0 de tous les hôtes sur lesquels ce DLR existe
Afficher toutes les interfaces CONNECTÉES au routeur logique	`show control-cluster logical-routers interface-summary 0x570d4555`	La colonne IP indique les adresses IP vmk0 de tous les hôtes sur lesquels ce DLR existe
Afficher tous les itinéraires appris par ce routeur logique	`show control-cluster logical-routers routes 0x570d4555`	Noter que la colonne IP indique les adresses IP vmk0 de tous les hôtes sur lesquels ce DLR existe
Affiche toutes les connexions réseau établies, comme une sortie net stat	`show network connections of-type tcp`	Vérifier si l'hôte que vous dépannez a une connexion netcpa établie vers le contrôleur
Synchroniser des interfaces entre le contrôleur et l'hôte	`sync control-cluster logical-routers interface-to-host <logical-router-id> <host-ip>`	Utile si une nouvelle interface était connectée au routeur logique, mais n'est pas synchronisée avec tous les hôtes
Synchroniser des itinéraires entre le contrôleur et l'hôte	`sync control-cluster logical-routers route-to-host <logical-router-id> <host-ip>`	Utile si des itinéraires sont manquants sur quelques hôtes, mais sont disponibles sur la plupart des hôtes

Tableau 1-12. Vérification du routage logique - Commandes exécutées à partir du dispositif Edge

Description	Commandes sur un dispositif Edge ou une VM de contrôle de routeur logique	Remarques
Afficher la configuration	`show configuration <global | bgp | ospf | …>`	
Afficher les itinéraires appris	`show ip route`	S'assurer que les tables de routage et de transfert sont synchronisées
Afficher la table de transfert	`show ip forwarding`	S'assurer que les tables de routage et de transfert sont synchronisées
Afficher les interfaces du routeur logique distribué	`show interface`	La première carte réseau affichée dans la sortie est l'interface du routeur logique distribué L'interface du routeur logique distribué n'est pas une vNIC réelle sur cette VM Tous les sous-réseaux associés au routeur logique distribué sont de type INTERNE
Afficher les autres interfaces (gestion)	`show interface`	L'interface Gestion/HA est une vNIC réelle sur la VM de contrôle du routeur logique Si HA était activé sans spécifier une adresse IP, 169.254.x.x/ 30 est utilisé Si l'interface de gestion dispose d'une adresse IP, elle s'affiche ici
déboguer le protocole	`debug ip ospf` `debug ip bgp`	Utile pour voir les problèmes avec la configuration (comme des zones OSPF et des minuteurs non concordants et un ASN erroné) Remarque : la sortie n'est visible que sur la console du dispositif Edge (pas via une session SSH)

Tableau 1-12. Vérification du routage logique - Commandes exécutées à partir du dispositif Edge (suite)

Description	Commandes sur un dispositif Edge ou une VM de contrôle de routeur logique	Remarques

Commandes OSPF	`show configuration ospf`
	`show ip ospf interface`
	`show ip ospf neighbor`
	`show ip route ospf`
	`show ip ospf database`
	`show tech-support` (et rechercher les chaînes « EXCEPTION » et « PROBLEM »)	

Commandes BGP	`show configuration bgp`
	`show ip bgp neighbor`
	`show ip bgp`
	`show ip route bgp`
	`show ip forwarding`
	`show tech-support` (rechercher les chaînes « EXCEPTION » et « PROBLEM »)	

Tableau 1-13. Vérification du routage logique - Fichiers journaux des hôtes

Description	Fichier journal	Remarques
Les informations de l'instance du routeur logique distribué sont transférées à des hôtes par vsfwd et enregistrées au format XML	`/etc/vmware/netcpa/config-by-vsm.xml`	Si l'instance du routeur logique distribué est manquante sur l'hôte, regarder d'abord dans ce fichier pour voir si l'instance est listée Si ce n'est pas le cas, redémarrer vsfwd De plus, utiliser ce fichier pour s'assurer que tous les contrôleurs sont connus par l'hôte
Le fichier ci-dessus est transféré par NSX Manager à l'aide de vsfwd Si le fichier `config-by-vsm.xml` n'est pas correct, consulter le journal vsfwd	`/var/log/vsfwd.log`	Analyser ce fichier pour rechercher les erreurs Pour redémarrer le processus : /etc/init.d/vShield-Stateful-Firewall stop|start
La connexion au contrôleur est effectuée à l'aide de netcpa	`/var/log/netcpa.log`	Analyser ce fichier pour rechercher les erreurs
Les journaux de module de commutation logique se trouvent dans vmkernel.log	`/var/log/vmkernel.log`	Consulter les journaux de module de commutation logique dans /var/log/vmkernel.log avec le préfixe vxlan :

Tableau 1-14. Débogage du contrôleur - Commande exécutée depuis NSX Manager

Description	Commande (sur NSX Manager)	Remarques
Lister tous les contrôleurs avec l'état	`show controller list all`	Affiche la liste de tous les contrôleurs et leur état d'exécution

Tableau 1-15. Débogage du contrôleur - Commande exécutée depuis NSX Controller

Description	Commande (sur le contrôleur)	Remarques
Vérifier l'état du cluster de contrôleurs	`show control-cluster status`	Doit toujours afficher « Jonction établie » et « Connecté à la plupart des clusters »
Vérifier les statistiques des connexions flottantes et des messages	`show control-cluster core stats`	Le compteur abandonné ne doit pas changer
Afficher l'activité du nœud liée à la jonction du cluster au départ ou après un redémarrage	`show control-cluster history`	Idéal pour résoudre des problèmes de jonction de cluster
Afficher la liste de nœuds dans le cluster	`show control-cluster startup-nodes`	Noter que la liste ne doit pas forcément contenir QUE des nœuds de cluster actifs Il doit s'agir d'une liste de tous les contrôleurs actuellement déployés Cette liste est utilisée en démarrant le contrôleur pour contacter d'autres contrôleurs dans le cluster
Affiche toutes les connexions réseau établies, comme une sortie net stat	`show network connections of-type tcp`	Vérifier si l'hôte que vous dépannez a une connexion netcpa établie vers le contrôleur
Pour redémarrer le processus de contrôleur	`restart controller`	Ne redémarre que le processus du contrôleur principal Force une reconnexion au cluster
Pour redémarrer le nœud de contrôleur	`restart system`	Redémarre la VM de contrôleur

Tableau 1-16. Débogage du contrôleur - Fichiers journaux sur NSX Controller

Description	Fichier journal	Remarques
Afficher l'historique du contrôleur et les jonctions et redémarrages récents. etc.	`show control-cluster history`	Bon outil de dépannage pour les problèmes de contrôleur, en particulier concernant le clustering
Rechercher un disque lent	`show log cloudnet/cloudnet_java-zookeeper<timestamp>.log filtered-by fsync`	Une manière fiable de rechercher les disques lents consiste à rechercher les messages « fsync » dans le journal cloudnet_java-zookeeper Si la synchronisation dure plus d'une seconde, ZooKeeper imprime ce message, et cela indique qu'un autre élément utilisait le disque à ce moment-là
Rechercher un disque lent/fonctionnant mal	`show log syslog filtered-by collectd`	Les messages comme celui dans la sortie ample sur « collectd » ont tendance à être liés aux disques lents ou fonctionnant mal

Tableau 1-16. Débogage du contrôleur - Fichiers journaux sur NSX Controller (suite)

Description	Fichier journal	Remarques
Vérifier l'utilisation de l'espace disque	`show log syslog filtered-by freespace:`	Il existe une tâche en arrière-plan appelée « freespace » qui nettoie régulièrement les anciens journaux et d'autres fichiers sur le disque lorsque l'utilisation de l'espace atteint un certain seuil. Dans certains cas, si le disque est petit et/ou se remplit très vite, vous verrez de nombreux messages pour libérer l'espace. Cela pourrait indiquer que le disque est rempli complètement
Rechercher des membres du cluster actuellement actifs	`show log syslog filtered-by Active cluster members`	Liste les ID de nœud des membres du cluster actuellement actifs. Peut nécessiter de regarder dans les anciens syslogs, car ce message n'est pas imprimé tout le temps.
Afficher les journaux du contrôleur principal	`show log cloudnet/cloudnet_java-zookeeper.20150703-165223.3702.log`	Il peut y avoir plusieurs journaux zookeeper, regarder le tout dernier fichier horodaté Ce fichier contient des informations sur l'élection maître du cluster de contrôleurs et d'autres informations liées à la nature distribuée des contrôleurs
Afficher les journaux du contrôleur principal	`show log cloudnet/cloudnet.nsx-controller.root.log.INFO.20150703-165223.3668`	Journaux de travail du contrôleur principal, comme création de LIF, écouteur de connexion sur 1234, partitionnement

Tableau 1-17. Vérification du pare-feu distribué - Commandes exécutées à partir de NSX Manager

Description	Commandes sur NSX Manager	Remarques
Afficher des informations de VM	`show vm vmID`	Détails tels que DC, Cluster, Hôte, Nom de VM, vNIC, dvfilters installés
Afficher des informations sur une carte réseau virtuelle particulière	`show vnic icID`	Détails tels que nom de la VNIC, adresse MAC, pg, filtres appliqués
Afficher toutes les informations des clusters	`show dfw cluster all`	Nom de cluster, ID de cluster, Nom de centre de données, Statut du pare-feu
Afficher des informations particulières sur les clusters	`show dfw cluster clusterID`	Nom d'hôte, ID d'hôte, Statut de l'installation
Afficher des informations sur l'hôte liées au DFW	`show dfw host hostID`	Nom de VM, ID de VM, État de l'alimentation
Afficher des détails dans un dvfilter	`show dfw host hostID filter filterID <option>`	Lister les règles, statistiques, ensembles d'adresses etc. pour chaque VNIC
Afficher des informations sur le DFW pour une VM	`show dfw vm vmID`	Afficher le nom de la VM, l'ID de VNIC, des filtres, etc.
Afficher les détails de la VNIC	`show dfw vnic vnicID`	Afficher le nom de la VNIC, l'ID, l'adresse MAC, le groupe de ports, le filtre

Tableau 1-17. Vérification du pare-feu distribué - Commandes exécutées à partir de NSX Manager (suite)

Description	Commandes sur NSX Manager	Remarques
Lister les filtres installés par vNIC	`show dfw host hostID summarize-dvfilter`	Rechercher la VM/vNIC d'intérêt et obtenir le champ de nom à utiliser dans les commandes suivantes comme filtre
Afficher des règles pour un filtre/vNIC spécifique	`show dfw host hostID filter filterID rules` `show dfw vnic nicID`	
Afficher des détails d'un ensemble d'adresses	`show dfw host hostID filter filterID addrsets`	Les règles affichent uniquement des ensembles d'adresses, cette commande peut être utilisée pour développer ce qui fait partie d'un ensemble d'adresses
Détails de Spoofguard par vNIC	`show dfw host hostID filter filterID spoofguard`	Vérifier si SpoofGuard est activé et quelle est l'adresse IP/MAC actuelle
Afficher des détails des enregistrements de flux	`show dfw host hostID filter filterID flows`	Si la surveillance de flux est activée, l'hôte envoie régulièrement des informations sur le flux à NSX Manager Utiliser cette commande pour voir des flux par vNIC
Afficher des statistiques pour chaque règle d'une vNIC	`show dfw host hostID filter filterID stats`	Utile pour voir si des règles sont touchées

Tableau 1-18. Vérification du pare-feu distribué - Commandes exécutées à partir des hôtes

Description	Commandes sur l'hôte	Remarques

Liste des VIB téléchargés sur l'hôte.
Reportez-vous au tableau *Noms des VIB et des modules installés sur les hôtes* pour plus d'informations sur les VIB à vérifier dans votre installation.
	`esxcli software vib list | grep esx-vsip`
	ou
	`esxcli software vib list | grep esx-nsxv`
		Veiller à vérifier que la bonne version du VIB est téléchargée

Détails sur les modules système actuellement chargés
Reportez-vous au tableau *Noms des VIB et des modules installés sur les hôtes* pour plus d'informations sur les modules à vérifier dans votre installation.
	`esxcli system module get -m vsip`
	ou
	`esxcli system module get -m nsx-vsip`
		Veiller à vérifier que le module a été installé/chargé

Liste de processus	`ps | grep vsfwd`	Afficher si le processus vsfwd est exécuté avec plusieurs threads
Commande de démon	`/etc/init.d/vShield-Stateful-Firewall {start|stop|status|restart}`	Vérifier si le démon est en cours d'exécution et redémarrer si nécessaire
Afficher la connexion réseau	`esxcli network ip connection list | grep 5671`	Vérifier si l'hôte dispose d'une connectivité TCP avec NSX Manager

Tableau 1-19. Vérification du pare-feu distribué - Fichiers journaux sur les hôtes

Description	Journal	Remarques
Journal de processus	`/var/log/vsfwd.log`	Journal de démon vsfwd, utile pour le processus vsfwd, connectivité de NSX Manager et dépannage de RabbitMQ
Fichier dédié aux journaux de paquets	`/var/log/dfwpktlogs.log`	Fichier journal dédié pour les journaux de paquets
Capture de paquets au niveau de dvfilter	`pktcap-uw --dvfilter nic-1413082-eth0-vmware-sfw.2 --outfile test.pcap`	

Vérification de l'intégrité de l'hôte NSX

Dans l'interface de ligne de commande centrale de NSX Manager, vous pouvez vérifier l'état de santé de chaque hôte ESXi.

L'état de santé signalé peut être critique, défectueux ou sain.

Par exemple :

```
nsxmgr> show host host-30 health-status
status: HEALTHY

nsxmgr> show host host-29 health-status
UNHEALTHY, Standard Switch vSwitch1 has no uplinks.
UNHEALTHY, Storage volume datastore1 has no enough free spaces: 19.% free.
status: UNHEALTHY

nsxmgr> show host host-28 health-status
CRITICAL, VXLAN VDS vds-site-a VNI 200000 multicast addr is not synchronized with VSM: 0.0.0.0.
CRITICAL, VXLAN VDS vds-site-a VNI 200003 multicast addr is not synchronized with VSM: 0.0.0.0.
CRITICAL, VXLAN VDS vds-site-a VNI 5000 multicast addr is not synchronized with VSM: 0.0.0.0.
Status: CRITICAL
```

La commande host-check peut également être appelée via l'API de NSX Manager.

Dépannage de l'infrastructure NSX

2

La préparation de NSX est un processus en 4 étapes.

1 Connectez NSX Manager à vCenter Server. Il existe une relation un-à-un entre NSX Manager et vCenter Server.

   a Enregistrez-vous avec vCenter Server.

2 Déployez des instances de NSX Controller (requis uniquement pour la commutation logique, le routage distribué ou VXLAN en mode monodiffusion ou hybride. Si vous n'utilisez qu'un pare-feu distribué (DFW), les contrôleurs ne sont pas obligatoires).

3 Préparation de l'hôte : installe des VIB pour VXLAN, DFW et le DLR sur tous les hôtes du cluster. Configure l'infrastructure de messagerie basée sur RabbitMQ. Active le pare-feu. Informe les contrôleurs que les hôtes sont prêts pour NSX.

4 Configurez les paramètres du pool IP et configurez VXLAN : crée un groupe de ports VTEP et des VMKNIC sur tous les hôtes du cluster. Au cours de cette étape, vous pouvez définir l'ID VLAN de transport, la stratégie d'association et le MTU.

Pour plus d'informations sur l'installation et la configuration de chaque étape, consultez le *Guide d'installation de NSX* et le *Guide d'administration de NSX*.

Ce chapitre contient les rubriques suivantes :

Préparation de l'hôte

vSphere ESX Agent Manager déploie des bundles d'installation vSphere (VIB) sur des hôtes ESXi.

Le déploiement sur les hôtes requiert que le DNS soit configuré sur les hôtes, vCenter Server et NSX Manager. Le déploiement ne nécessite pas un redémarrage de l'hôte ESXi, contrairement aux mises à jour ou aux suppressions de VIB.

Les VIB sont hébergés sur NSX Manager et ils sont également disponibles sous forme de fichier compressé.

Le fichier est accessible à l'adresse `https://<NSX-Manager-IP>/bin/vdn/nwfabric.properties`. Le fichier compressé téléchargeable diffère selon la version de NSX et d'ESXi. Par exemple, dans NSX 6.3.0, les hôtes vSphere 6.0 utilisent le fichier `https://<NSX-Manager-IP>/bin/vdn/vibs-6.3.0/6.0-buildNumber/vxlan.zip`.

```
# 5.5 VDN EAM Info
VDN_VIB_PATH.1=/bin/vdn/vibs-6.3.0/5.5-4744075/vxlan.zip
VDN_VIB_VERSION.1=4744075
VDN_HOST_PRODUCT_LINE.1=embeddedEsx
VDN_HOST_VERSION.1=5.5.*

# 6.0 VDN EAM Info
VDN_VIB_PATH.2=/bin/vdn/vibs-6.3.0/6.0-4744062/vxlan.zip
VDN_VIB_VERSION.2=4744062
VDN_HOST_PRODUCT_LINE.2=embeddedEsx
VDN_HOST_VERSION.2=6.0.*

# 6.5 VDN EAM Info
VDN_VIB_PATH.3=/bin/vdn/vibs-6.3.0/6.5-4744074/vxlan.zip
VDN_VIB_VERSION.3=4744074
VDN_HOST_PRODUCT_LINE.3=embeddedEsx
VDN_HOST_VERSION.3=6.5.*

# Single Version associated with all the VIBs pointed by above VDN_VIB_PATH(s)
VDN_VIB_VERSION=6.3.0.4744320

# Legacy vib location. Used by code to discover available legacy vibs.
LEGACY_VDN_VIB_PATH_FS=/common/em/components/vdn/vibs/legacy/
LEGACY_VDN_VIB_PATH_WEB_ROOT=/bin/vdn/vibs/legacy/
```

Les VIB installés sur un hôte dépendent des versions de NSX et d'ESXi :

Version d'ESXi	Version de NSX	VIB installés
5.5	N'importe quelle version 6.3.x	■ esx-vsip ■ esx-vxlan
6.0 ou une version ultérieure	6.3.2 ou une version antérieure	■ esx-vsip ■ esx-vxlan
6.0 ou une version ultérieure	6.3.3 ou une version ultérieure	■ esx-nsxv

Vous pouvez afficher les VIB installés à l'aide de la commande `esxcli software vib list`.

```
[root@esx-01a:~] esxcli software vib list | grep -e vsip -e vxlan
esx-vsip                       6.0.0-0.0.XXXXXXX                    VMware  VMwareCertified
2016-04-20
esx-vxlan                      6.0.0-0.0.XXXXXXX                    VMware  VMwareCertified
2016-04-20
```

ou

```
esxcli software vib list | grep nsxv
esx-nsxv                       6.0.0-0.0.XXXXXXX                  VMware  VMwareCertified
2017-08-11
```

Problèmes courants lors de la préparation de l'hôte

Lors de la préparation d'hôtes, les problèmes typiques que l'on peut rencontrer sont les suivants :

- EAM ne réussit pas à déployer des VIB.
  - Peut être dû à un DNS mal configuré sur des hôtes.
  - Peut être dû à un pare-feu bloquant des ports requis entre ESXi, NSX Manager et vCenter Server.

  La plupart des problèmes sont résolus en cliquant sur l'option **Résoudre (Resolve)**. Consultez la section Le statut de l'installation n'est pas prêt .
- Un VIB précédent d'une version antérieure est déjà installé. Cela nécessite que l'utilisateur redémarre les hôtes.
- NSX Manager et vCenter Server rencontrent des problèmes de communication. L'onglet **Préparation de l'hôte (Host Preparation)** dans le plug-in Networking and Security n'affiche pas tous les hôtes correctement :
  - Vérifiez si vCenter Server peut énumérer tous les hôtes et les clusters.

Si le problème n'est pas résolu avec l'option **Résoudre (Resolve)**, reportez-vous à la section Problème non corrigé avec l'option Résoudre.

Dépannage de la préparation de l'hôte (VIB)

- Vérifiez la santé du canal de communication pour l'hôte. Reportez-vous à la section Vérification de la santé du canal de communication.
- Recherchez des erreurs sur vSphere ESX Agent Manager.

  Accueil de vCenter > Administration > Extensions de vCenter Server > vSphere ESX Agent Manager (vCenter home > Administration > vCenter Server Extensions > vSphere ESX Agent Manager).

  Sur vSphere ESX Agent Manager, vérifiez l'état des agences avec le préfixe « VCNS160 ». Si l'état d'une agence est incorrect, sélectionnez l'agence et affichez ses problèmes.

Agency	State	Status	Optimized Deployment
_VCNS_160_Management & Edge Cl_...	Enabled	Normal	✓
_VCNS_160_Compute Cluster A_VMwa...	Enabled	Alert	✓

Issues for the selected agencies

Trigger Time	Agency	Issue	Host	Agent VM
Thu Apr 28 12:03:12 GMT-0...	_VCNS_160_Compute Clu...	Agent VIB module is not installed	esx-01a.corp.local	

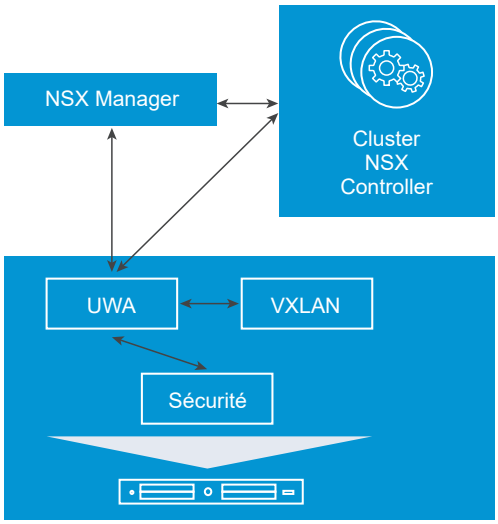
- Sur l'hôte qui a un problème, exécutez la commande `tail /var/log/esxupdate.log`.

```
2016-04-28T19:02:52Z esxupdate: downloader: DEBUG: Downloading https://vcsa-(
o /tmp/tmpKT0wjN...
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR: An esxupdate error exceptic
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR: Traceback (most recent call
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR:   File "/usr/sbin/esxupdate
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR:     cmd.Run()
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR:   File "/build/mts/release/
site-packages/vmware/esx5update/Cmdline.py", line 106, in Run
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR:   File "/build/mts/release/
site-packages/vmware/esximage/Transaction.py", line 73, in DownloadMetadatas
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR: MetadataDownloadError: ('ht
fd3f37ad4c', None, "('https://vcsa-01a.corp.local:443/eam/vib?id=facdb160-21(
rlopen error [Errno -3] Temporary failure in name resolution>')")
2016-04-28T19:03:12Z esxupdate: esxupdate: DEBUG: <<<
```

Dépannage de la préparation de l'hôte (UWA)

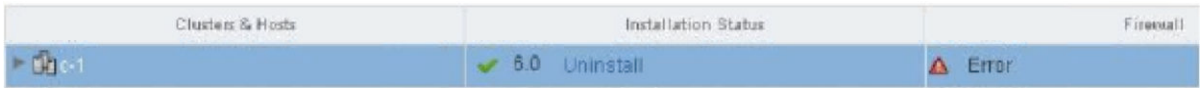
NSX Manager configure deux agents UWA (User World Agent) sur tous les hôtes d'un cluster :

- Agent UWA du bus de messages (vsfwd)
- Agent UWA du plan de contrôle (netcpa)

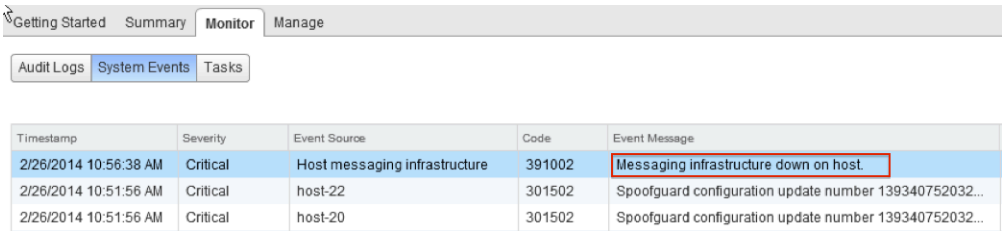


Dans de rares cas, l'installation des VIB réussit, mais, pour une raison quelconque, un agent UWA, ou les deux, ne fonctionne pas correctement. Cela pourrait se traduire par :

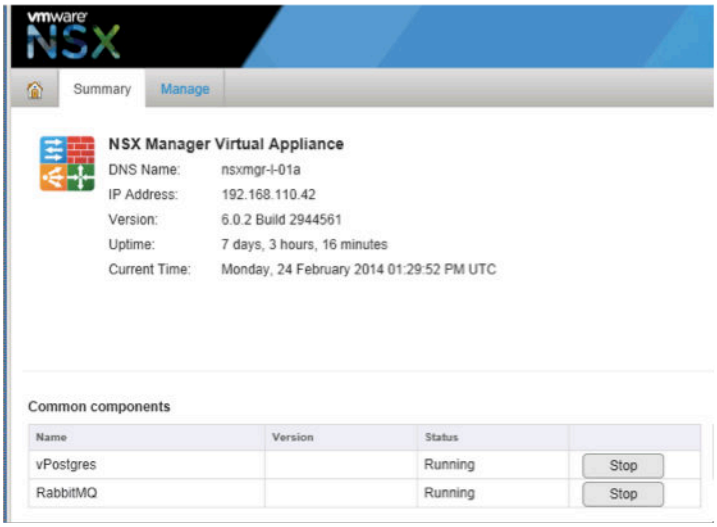
- Le pare-feu indiquant un état incorrect.



- Le plan de contrôle entre les hyperviseurs et les contrôleurs étant inactif. Vérifiez les événements système de NSX Manager. Consultez *Journalisation et événements système dans NSX*.



Si plusieurs hôtes ESXi sont affectés, vérifiez l'état du service de bus de messages sur l'interface utilisateur Web du dispositif NSX Manager dans l'onglet **Résumé (Summary)**. Si RabbitMQ est arrêté, redémarrez-le.



Si le service de bus de messages est actif sur NSX Manager :

- Vérifiez l'état de l'agent UWA du bus de messages sur les hôtes en exécutant la commande `/etc/init.d/vShield-Stateful-Firewall status` sur les hôtes ESXi.

```
[root@esx-01a:~] /etc/init.d/vShield-Stateful-Firewall status
vShield-Stateful-Firewall is running
```

- Consultez les journaux de l'agent UWA du bus de messages sur les hôtes à l'emplacement `/var/log/vsfwd.log`.

- Exécutez la commande `esxcfg-advcfg -l | grep Rmq` sur les hôtes ESXi pour afficher toutes les variables Rmq. Il devrait y avoir 16 variables Rmq.

```
[root@esx-01a:~] esxcfg-advcfg -l | grep Rmq
/UserVars/RmqIpAddress [String] : Connection info for RMQ Broker
/UserVars/RmqUsername [String] : RMQ Broker Username
/UserVars/RmqPassword [String] : RMQ Broker Password
/UserVars/RmqVHost [String] : RMQ Broker VHost
/UserVars/RmqVsmRequestQueue [String] : RMQ Broker VSM Request Queue
/UserVars/RmqPort [String] : RMQ Broker Port
/UserVars/RmqVsmExchange [String] : RMQ Broker VSM Exchange
/UserVars/RmqClientPeerName [String] : RMQ Broker Client Peer Name
/UserVars/RmqHostId [String] : RMQ Broker Client HostId
/UserVars/RmqHostVer [String] : RMQ Broker Client HostVer
/UserVars/RmqClientId [String] : RMQ Broker Client Id
/UserVars/RmqClientToken [String] : RMQ Broker Client Token
/UserVars/RmqClientRequestQueue [String] : RMQ Broker Client Request Queue
/UserVars/RmqClientResponseQueue [String] : RMQ Broker Client Response Queue
/UserVars/RmqClientExchange [String] : RMQ Broker Client Exchange
/UserVars/RmqSslCertSha1ThumbprintBase64 [String] : RMQ Broker Server Certificate base64 Encoded
Sha1 Hash
```

- Exécutez la commande `esxcfg-advcfg -g /UserVars/RmqIpAddress` sur les hôtes ESXi. La sortie doit afficher l'adresse IP de NSX Manager.

```
[root@esx-01a:~] esxcfg-advcfg -g /UserVars/RmqIpAddress
Value of RmqIpAddress is 192.168.110.15
```

- Exécutez la commande `esxcli network ip connection list | grep 5671` sur les hôtes ESXi pour rechercher une connexion du bus de messages active.

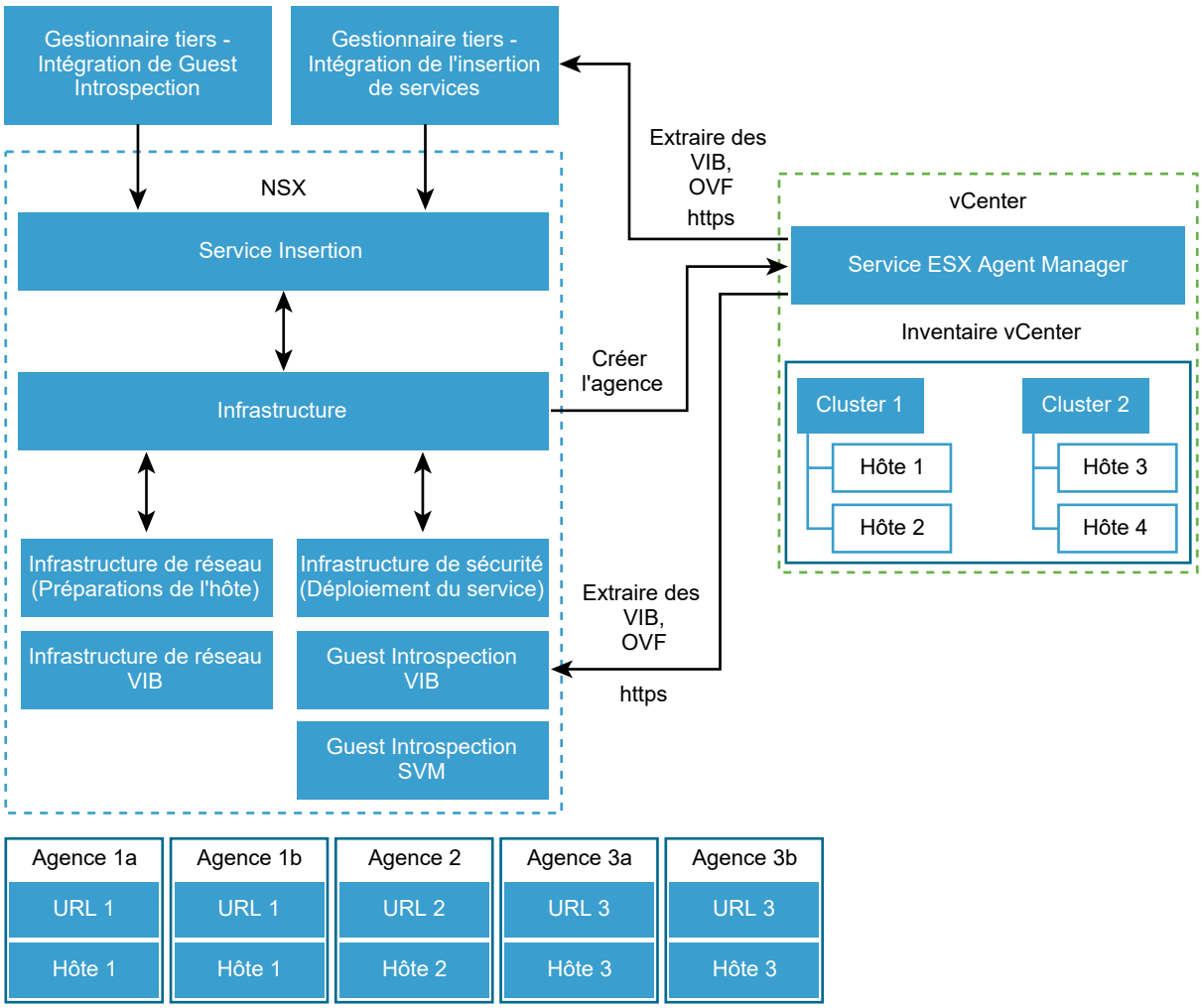
```
[root@esx-01a:~] esxcli network ip connection list | grep 5671
tcp         0       0  192.168.110.51:29969           192.168.110.15:5671   ESTABLISHED
35505  newreno  vsfwd
tcp         0       0  192.168.110.51:29968           192.168.110.15:5671   ESTABLISHED
35505  newreno  vsfwd
```

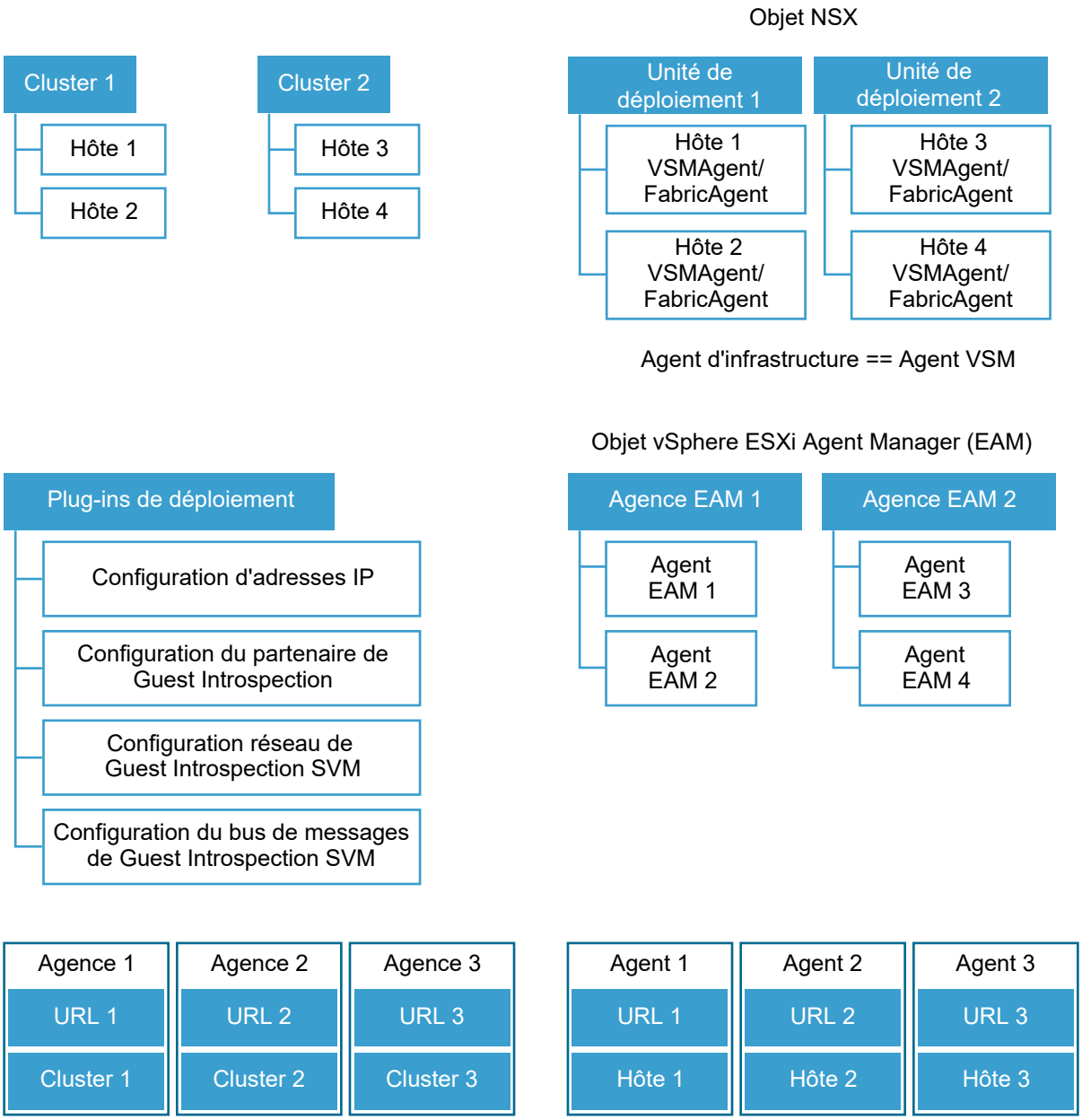
Pour les problèmes liés à l'agent du plan de contrôle, reportez-vous à la section Problèmes de l'agent du plan de contrôle (netcpa).

Comprendre l'architecture de la préparation de l'hôte

Cette rubrique explique l'architecture basique de la préparation de l'hôte.

- Pour déployer l'infrastructure de réseau, accédez à l'onglet **Préparation de l'hôte (Host Preparation)**.
- Pour déployer l'infrastructure de sécurité, accédez à l'onglet **Déploiement du service (Service Deployment)**.


Gestionnaire tiers - Intégration de Guest Introspection
Gestionnaire tiers - Intégration de l'insertion de services
NSX
Service Insertion
Infrastructure
Infrastructure de réseau (Préparations de l'hôte)
Infrastructure de sécurité (Déploiement du service)
Infrastructure de réseau VIB
Guest Introspection VIB
Guest Introspection SVM
Extraire des VIB, OVF
https
Créer l'agence
Extraire des VIB, OVF
https
vCenter
Service ESX Agent Manager
Inventaire vCenter
Cluster 1
Cluster 2
Hôte 1
Hôte 2
Hôte 3
Hôte 4
Agence 1a
URL 1
Hôte 1
Agence 1b
URL 1
Hôte 1
Agence 2
URL 2
Hôte 2
Agence 3a
URL 3
Hôte 3
Agence 3b
URL 3
Hôte 3


Objet NSX
Cluster 1
Hôte 1
Hôte 2
Cluster 2
Hôte 3
Hôte 4
Unité de déploiement 1
Hôte 1 VSMAgent/ FabricAgent
Hôte 2 VSMAgent/ FabricAgent
Unité de déploiement 2
Hôte 3 VSMAgent/ FabricAgent
Hôte 4 VSMAgent/ FabricAgent
Agent d'infrastructure == Agent VSM
Objet vSphere ESXi Agent Manager (EAM)
Plug-ins de déploiement
Configuration d'adresses IP
Configuration du partenaire de Guest Introspection
Configuration réseau de Guest Introspection SVM
Configuration du bus de messages de Guest Introspection SVM
Agence EAM 1
Agent EAM 1
Agent EAM 2
Agence EAM 2
Agent EAM 3
Agent EAM 4
Agence 1
URL 1
Cluster 1
Agence 2
URL 2
Cluster 2
Agence 3
URL 3
Cluster 3
Agent 1
URL 1
Hôte 1
Agent 2
URL 2
Hôte 2
Agent 3
URL 3
Hôte 3

Les termes suivants peuvent vous aider à comprendre l'architecture de la préparation de l'hôte :

Infrastructure	L'infrastructure est une couche logicielle dans NSX Manager qui interagit avec ESX Agent Manager pour installer des services d'infrastructure de réseau et de sécurité sur des hôtes.
Infrastructure de réseau	Des services d'infrastructure de réseau sont déployés sur un cluster. Les services d'infrastructure de réseau incluent la préparation de l'hôte, VXLAN, le routage distribué, le pare-feu distribué et le bus de messages.
Infrastructure de sécurité	Des services d'infrastructure de sécurité sont déployés sur un cluster. Les services d'infrastructure de sécurité incluent Guest Introspection et des solutions de sécurité de partenaire.
Agent d'infrastructure	Un agent d'infrastructure est la combinaison d'un service d'infrastructure et d'un hôte dans la base de données de NSX Manager. Un agent d'infrastructure est créé par hôte pour un cluster sur lequel un service d'infrastructure de réseau ou de sécurité est déployé. Aussi appelé : agent VSM
Unité de déploiement	Combinaison d'un service d'infrastructure et d'un cluster dans la base de données de NSX Manager. Une unité de déploiement doit être créée pour que les services de mise en réseau et de sécurité soient installés.
Agent ESX Agent Manager	Un agent ESX Agent Manager est la combinaison d'une spécification de service et d'un hôte dans la base de données vCenter Server. Un agent ESX Agent Manager est mappé à un agent d'infrastructure NSX.
Agence ESX Agent Manager	Une agence ESX Agent Manager est la combinaison d'une spécification et d'un cluster dans la base de données vCenter Server. La spécification décrit les agents ESX Agent Manager, ainsi que les bundles VIB et OVF et leur configuration (telle que les paramètres de banque de données et réseau) qu'elle gère. NSX Manager crée une agence ESX Agent Manager pour chacun des clusters qui sont en cours de préparation. Une agence ESX Agent Manager est mappée à une unité de déploiement NSX. La base de données de NSX Manager d'unités de déploiement et la base de données de vCenter ESX Agent Manager d'agences ESX Agent Manager doivent être synchronisées. Dans de rares cas, si les deux bases de données ne sont pas synchronisées, NSX déclenche des événements et des alarmes pour vous informer de la condition. NSX Manager crée une unité de déploiement sur sa base de données pour chaque agence ESX Agent Manager.

NSX Manager crée une agence ESX Agent Manager pour chacun des clusters qui sont en cours de préparation. NSX Manager crée une unité de déploiement sur sa base de données pour chaque agence ESX Agent Manager. Une agence ESX Agent Manager = une unité de déploiement.

Vous pouvez afficher des agences des manières suivantes :

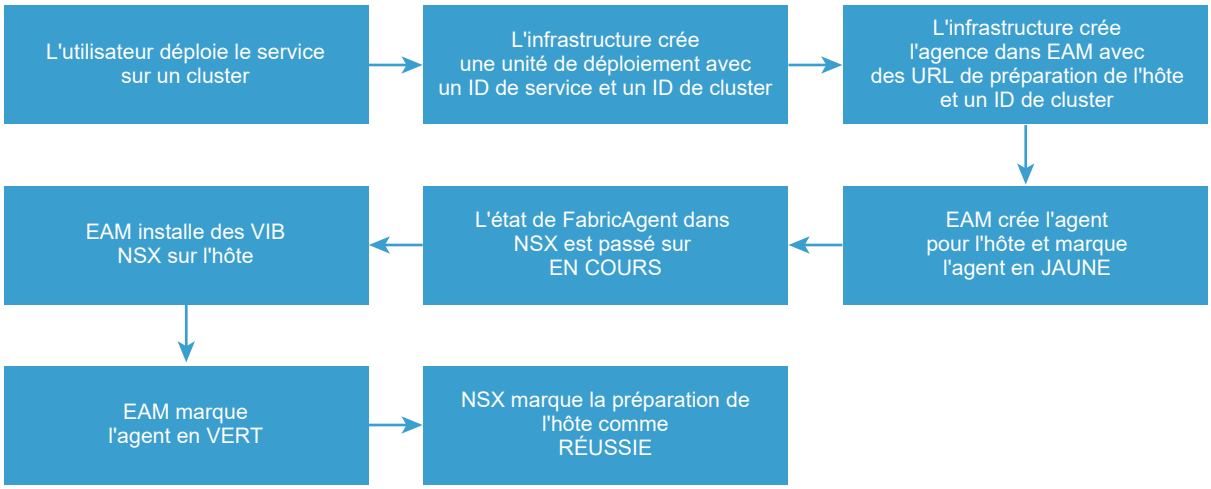
- À partir du MOB d'EAM *https://<VC-hostname/IP>/eam/mob/*.
- À partir de vSphere Web Client :
  - Accédez à **vCenter Solutions Manager > vSphere ESX Agent Manager > Gérer (Manage)**.
  - Sous **Agences ESX (ESX Agencies)**, vous pouvez voir les agences (une par cluster qui a été préparé pour un hôte).

Le cycle de vie d'une unité de déploiement est lié à celui de l'agence et la suppression d'une agence d'ESX Agent Manager entraîne la suppression de l'unité de déploiement correspondante de NSX.

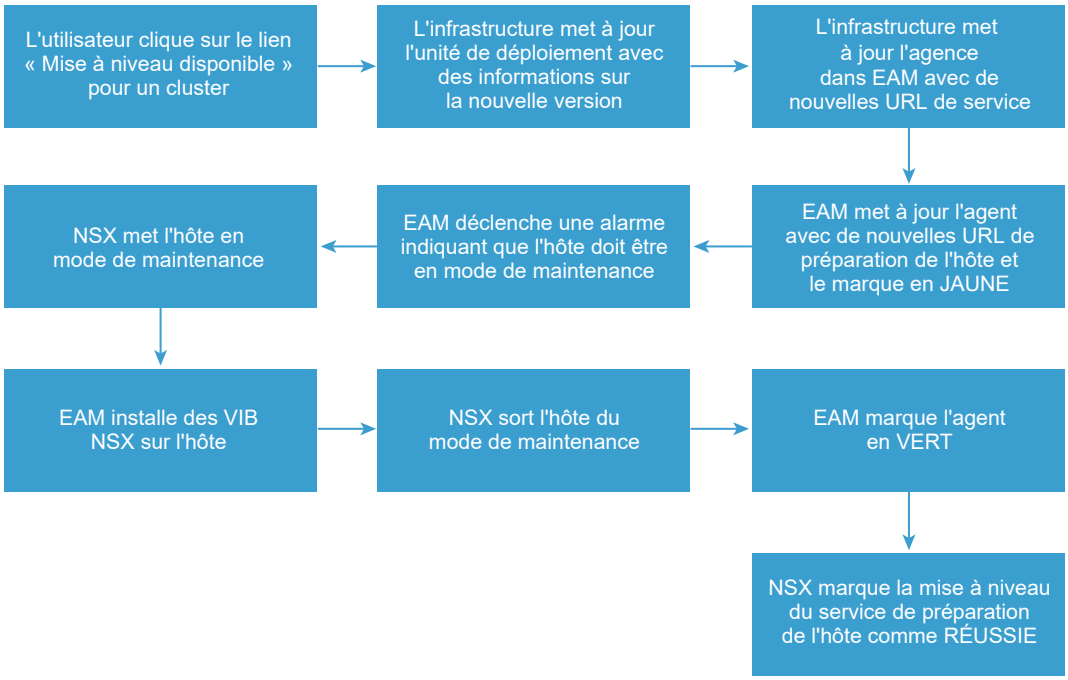
Workflow de déploiement de service pour la préparation de l'hôte

Cette rubrique affiche le workflow de déploiement de service (installation et mise à niveau) pour la préparation de l'hôte.

Workflow d'installation



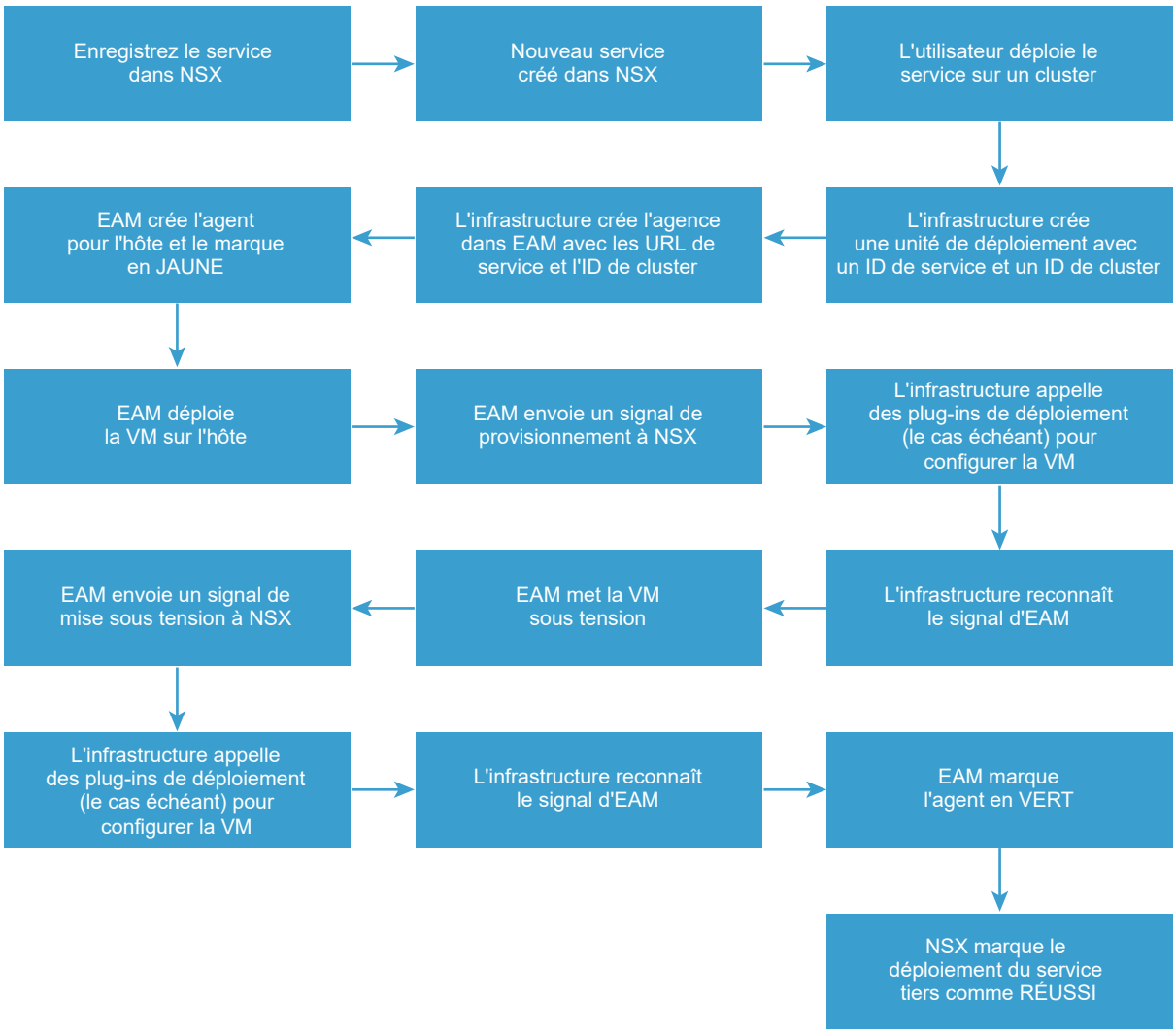
Workflow de mise à niveau



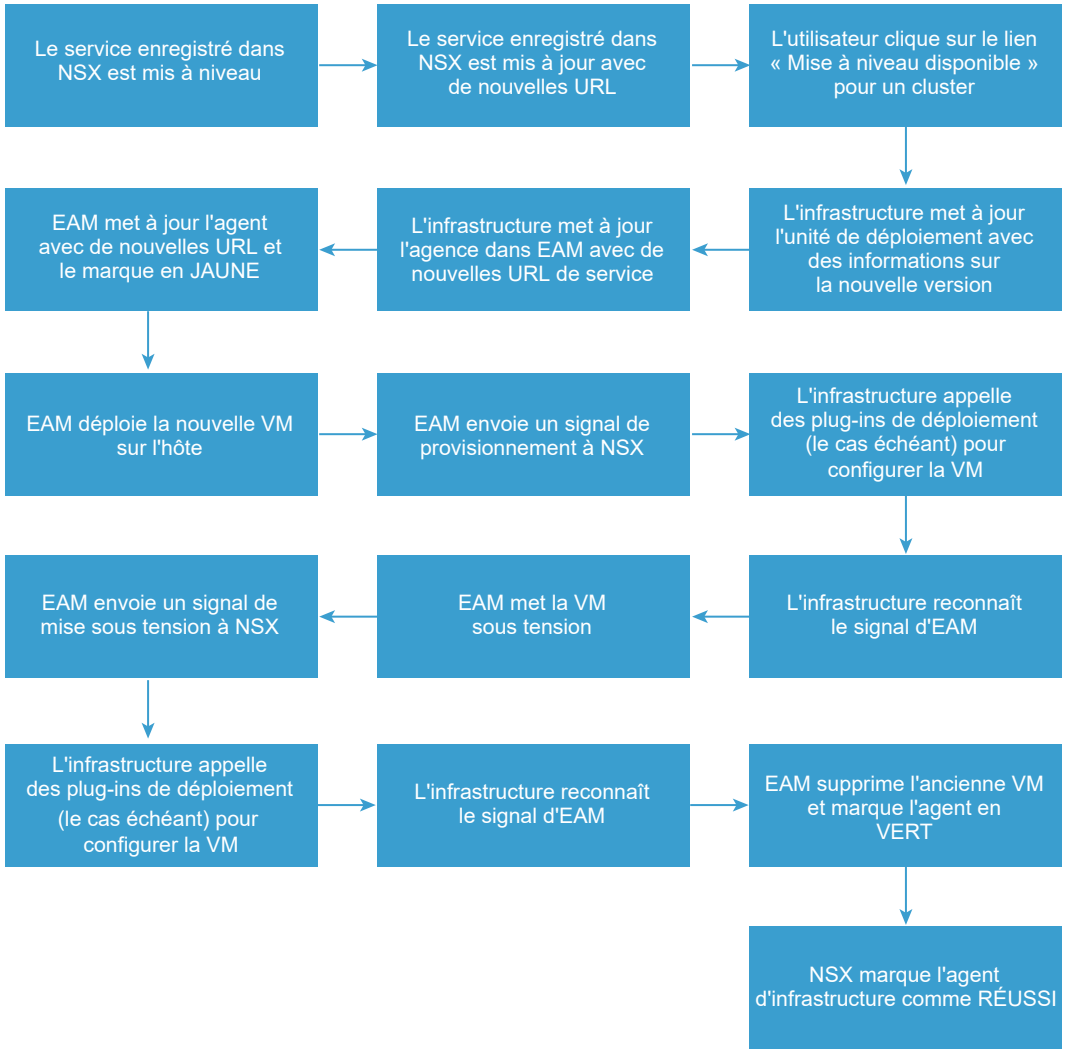
Workflow de déploiement du service pour les services tiers

Cette rubrique affiche le workflow de déploiement de service (installation et mise à niveau) pour les services tiers.

Workflow d'installation



Workflow de mise à niveau



Vérification de la santé du canal de communication

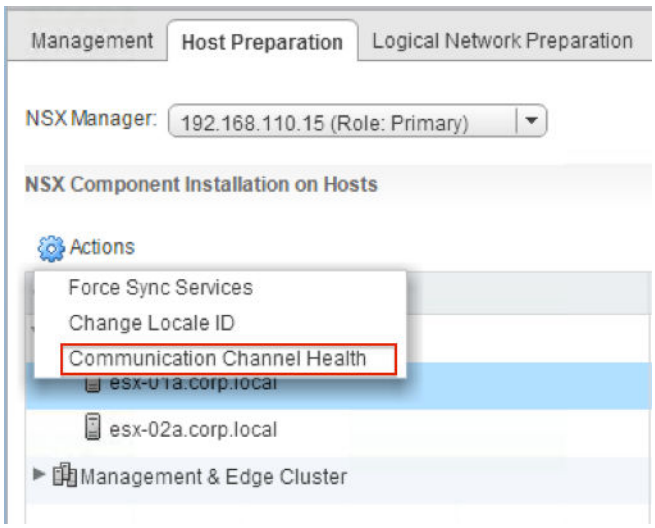
À partir de vSphere Web Client, vous pouvez vérifier l'état de la communication entre divers composants.

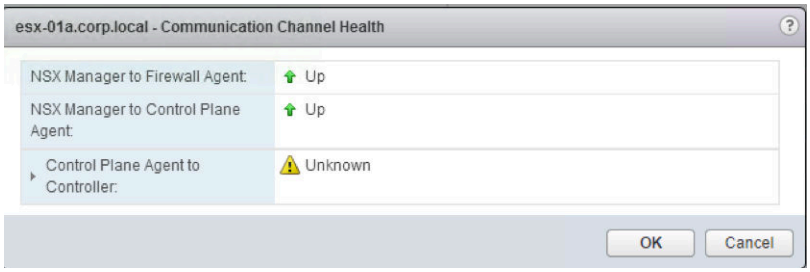
Pour vérifier la santé du canal de communication entre NSX Manager et l'agent de pare-feu, entre NSX Manager et l'agent de plan de contrôle et entre l'agent de plan de contrôle et les contrôleurs, effectuez les étapes suivantes :

1 Dans vSphere Web Client, accédez à **Networking & Security > Installation > Préparation de l'hôte (Host Preparation)**.

2 Sélectionnez un cluster ou développez un cluster et sélectionnez un hôte. Cliquez sur **Actions** ( ), puis sur **Santé du canal de communication (Communication Channel Health)**.

Les informations relatives à la santé du canal de communication s'affichent.





Si l'état de l'une des trois connexions pour un hôte change, un message est inscrit dans le journal NSX Manager. Dans le message du journal, l'état d'une connexion peut être UP (actif), DOWN (inactif) ou NOT_AVAILABLE (non disponible) (apparaît sous la forme Inconnu dans vSphere Web Client). Si l'état passe de UP à DOWN ou NOT_AVAILABLE, un message d'avertissement est généré. Par exemple :

```
2016-05-23 23:36:34.736 GMT+00:00  WARN TaskFrameworkExecutor-25 VdnInventoryFacadeImpl
$HostStatusChangedEventHandler:200 - Host Connection Status Changed: Event Code: 1941, Host:
esx-04a.corp.local (ID: host-46), NSX Manager - Firewall Agent: UP, NSX Manager - Control Plane
Agent: UP, Control Plane Agent - Controllers: DOWN.
```

Si l'état passe de DOWN ou NOT_AVAILABLE à UP, un message INFO semblable au message d'avertissement est généré. Par exemple :

```
2016-05-23 23:55:12.736 GMT+00:00  INFO TaskFrameworkExecutor-25 VdnInventoryFacadeImpl
$HostStatusChangedEventHandler:200 - Host Connection Status Changed: Event Code: 1938, Host:
esx-04a.corp.local (ID: host-46), NSX Manager - Firewall Agent: UP, NSX Manager - Control Plane
Agent: UP, Control Plane Agent - Controllers: UP.
```

Si une erreur de communication survient au niveau du canal du plan de contrôle, un événement système indiquant l'un des motifs de défaillance granulaire suivants est généré :

- 1255601 : Certificat d'hôte incomplet
- 1255602 : Certificat de contrôleur incomplet
- 1255603 : Échec d'établissement d'une liaison SSL

- 1255604 : Connexion refusée
- 1255605 : Expiration de la connexion persistante
- 1255606 : Exception SSL
- 1255607 : Message incorrect
- 1255620 : Erreur inconnue

Par ailleurs, les messages des pulsations sont générés de NSX Manager vers les hôtes. Une synchronisation complète de la configuration est déclenchée, si les pulsations entre le dispositif NSX Manager et netcpa sont perdues.

Pour plus d'informations sur l'affichage des alertes, consultez *Guide d'administration de NSX*.

Le statut de l'installation n'est pas prêt

Lors de préparation de l'hôte, vous pouvez remarquer que l'état du cluster indique qu'il est `Non prêt`.

Problème

Dans l'onglet **Préparation de l'hôte (Host Preparation)** ou **Déploiement du service (Service Deployment)**, le statut de l'installation indique qu'il est `Non prêt`.

Solution

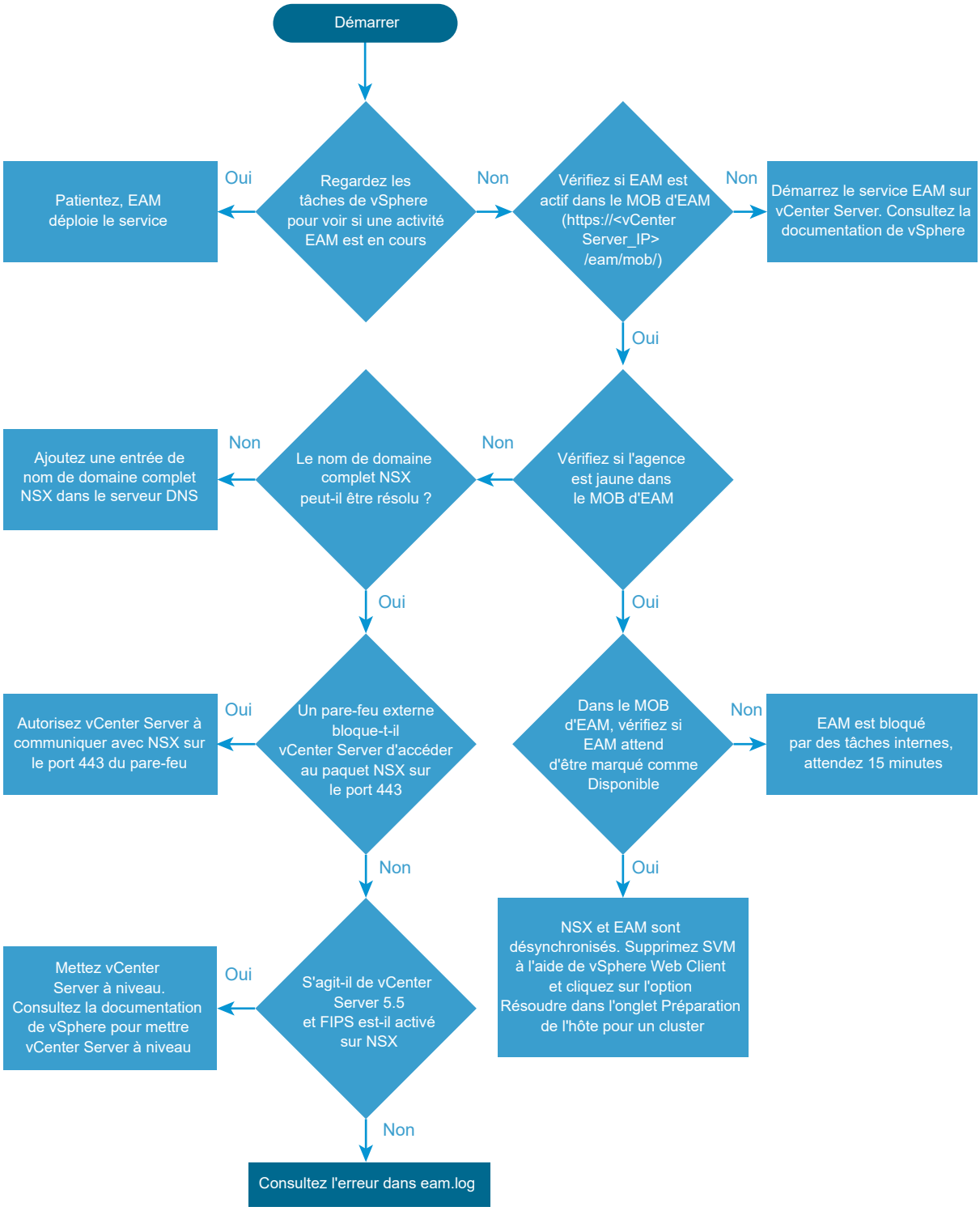
1. Accédez à l'onglet **Mise en réseau et sécurité (Networking & Security) > Installation**> **Préparation de l'hôte (Host Preparation)** ou **Déploiement du service (Service Deployment)**.
2. Sur les clusters et les hôtes, cliquez sur `Non prêt`.

   Vous voyez le message d'erreur suivant.
3. Cliquez sur l'option **Résoudre (Resolve)**.

   Pour afficher la liste des problèmes résolus par l'option **Résoudre (Resolve)**, consultez *Journalisation et événements système dans NSX*.
4. Si vous voyez toujours `Non prêt` et que l'erreur n'est toujours pas résolue, reportez-vous à la section Problème non corrigé avec l'option Résoudre.

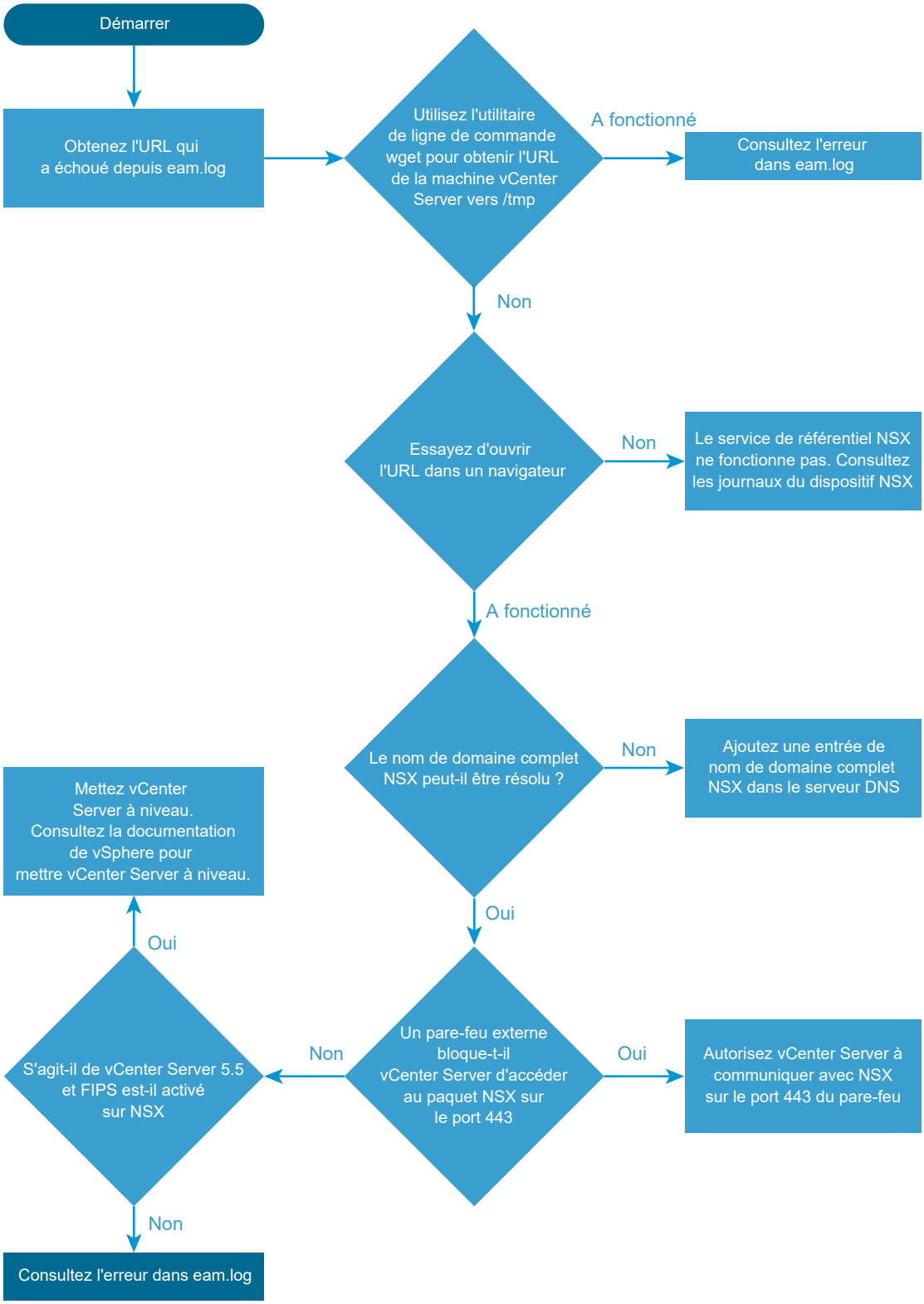
Le service ne répond pas

Le diagramme de flux est une vue d'ensemble du processus de préparation de l'hôte NSX et des actions à suivre lorsque le service ne répond pas pendant une période prolongée ou qu'il indique une icône qui tourne pendant un long moment.


Démarrer
Regardez les tâches de vSphere pour voir si une activité EAM est en cours
Oui
Patientez, EAM déploie le service
Non
Vérifiez si EAM est actif dans le MOB d'EAM (https://<vCenter Server_IP> /eam/mob/)
Non
Démarrez le service EAM sur vCenter Server. Consultez la documentation de vSphere
Oui
Vérifiez si l'agence est jaune dans le MOB d'EAM
Non
Le nom de domaine complet NSX peut-il être résolu ?
Non
Ajoutez une entrée de nom de domaine complet NSX dans le serveur DNS
Oui
Un pare-feu externe bloque-t-il vCenter Server d'accéder au paquet NSX sur le port 443
Oui
Autorisez vCenter Server à communiquer avec NSX sur le port 443 du pare-feu
Non
S'agit-il de vCenter Server 5.5 et FIPS est-il activé sur NSX
Oui
Mettez vCenter Server à niveau. Consultez la documentation de vSphere pour mettre vCenter Server à niveau
Non
Consultez l'erreur dans eam.log
Oui
Dans le MOB d'EAM, vérifiez si EAM attend d'être marqué comme Disponible
Non
EAM est bloqué par des tâches internes, attendez 15 minutes
Oui
NSX et EAM sont désynchronisés. Supprimez SVM à l'aide de vSphere Web Client et cliquez sur l'option Résoudre dans l'onglet Préparation de l'hôte pour un cluster

Le déploiement du service échoue avec l'erreur OVF/VIB non accessible

Le diagramme de flux affiche ce qu'il faut faire lorsque le déploiement du service échoue avec l'erreur `OVF/VIB non accessible`.


Démarrer
Obtenez l'URL qui a échoué depuis eam.log
Utilisez l'utilitaire de ligne de commande wget pour obtenir l'URL de la machine vCenter Server vers /tmp
A fonctionné
Consultez l'erreur dans eam.log
Non
Essayez d'ouvrir l'URL dans un navigateur
Non
Le service de référentiel NSX ne fonctionne pas. Consultez les journaux du dispositif NSX
A fonctionné
Le nom de domaine complet NSX peut-il être résolu ?
Non
Ajoutez une entrée de nom de domaine complet NSX dans le serveur DNS
Oui
Un pare-feu externe bloque-t-il vCenter Server d'accéder au paquet NSX sur le port 443
Oui
Autorisez vCenter Server à communiquer avec NSX sur le port 443 du pare-feu
Non
S'agit-il de vCenter Server 5.5 et FIPS est-il activé sur NSX
Oui
Mettez vCenter Server à niveau. Consultez la documentation de vSphere pour mettre vCenter Server à niveau.
Non
Consultez l'erreur dans eam.log

Problème non corrigé avec l'option Résoudre

Dans l'onglet **Mise en réseau et sécurité (Networking & Security) > Installation** > **Préparation de l'hôte (Host Preparation)** ou **Déploiement du service (Service Deployment)**, le statut de l'installation indique `Non prêt` sur les clusters et les hôtes. Cliquer sur l'option **Résoudre (Resolve)** ne corrige pas le problème.

Problème

- Cliquer sur le lien `Non prêt` indique l'erreur `Le module VIB pour l'agent n'est pas installé sur l'hôte`.
- L'hôte ESXi ne parvient pas à accéder aux VIB à partir de vCenter Server.
- Lors du passage de vShield Endpoint à NSX Manager, vous pouvez voir l'état `Échec`.

Solution

1. Vérifiez que le DNS est correctement configuré sur vCenter Server, les hôtes ESXi et NSX Manager. Assurez-vous que la résolution DNS directe et inverse depuis vCenter Server, les hôtes ESXi, NSX Manager et vSphere Update Manager fonctionne.
2. Pour déterminer si le problème est lié à DNS, consultez les journaux *esxupdate* et recherchez le message “`esxupdate: ERROR: MetadataDownloadError:IOError: <urlopen error [Errno –2] Name= or service not known` dans le fichier *esxupdate.log*.

   Ce message indique que l'hôte ESXi ne peut pas accéder au nom de domaine complet de vCenter Server. Pour plus d'informations, consultez l'article Verifying the VMware vCenter Server Managed IP Address (1008030) (Vérification de l'adresse IP gérée par VMware vCenter Server).
3. Vérifiez que le protocole NTP est correctement configuré. VMware recommande la configuration NTP. Pour déterminer si les problèmes de désynchronisation de NTP ont un impact sur votre environnement, consultez le fichier */etc/ntp.drift* dans les bundles de support de NSX Manager avec les versions 6.2.4 et ultérieures.
4. Vérifiez que tous les ports requis pour NSX for vSphere 6.x ne sont pas bloqués par un pare-feu. Pour plus d'informations liées, consultez :
   - Network Port Requirements for VMware NSX for vSphere (2079386) (Exigences des ports réseau pour VMware NSX for vSphere).
   - TCP and UDP Ports required to access VMware vCenter Server, VMware ESXi and ESX hosts, and other network components (1012382) (Ports TCP et UDP requis pour accéder à VMware vCenter Server, aux hôtes VMware ESXi et ESX et à d'autres composants réseau).

   Note VMware vSphere 6.x prend en charge les téléchargements de VIB sur le port 443 (plutôt que le port 80). Ce port est ouvert et fermé de façon dynamique. Les périphériques intermédiaires entre les hôtes ESXi et vCenter Server doivent autoriser le trafic à l'aide de ce port.
5. Vérifiez que l'adresse IP gérée par vCenter Server est correctement configurée. Pour plus d'informations, consultez l'article Verifying the VMware vCenter Server Managed IP Address (1008030) (Vérification de l'adresse IP gérée par VMware vCenter Server).

6 Vérifiez que vSphere Update Manager fonctionne correctement. À partir de vCenter Server 6.0U3, les procédures d'installation et de mise à niveau de NSX n'exploitent plus vSphere Update Manager avec ESX Agent Manager. VMware vous recommande vivement d'exécuter au moins vCenter Server 6.0U3 ou version ultérieure. Si vous ne pouvez pas effectuer la mise à niveau, assurez-vous que le service vSphere Update Manager est en cours d'exécution. Vous pouvez configurer l'option de contournement de vSphere Update Manager, conformément à l'article 2053782 de la base de connaissances.

7 Si vous spécifiez des ports non par défaut lors du déploiement de vCenter Server, assurez-vous que ces ports ne sont pas bloqués par le pare-feu de l'hôte ESXi.

8 Vérifiez que le processus *vpxd* de vCenter Server écoute sur le port TCP 8089. NSX Manager ne prend en charge que le port 8089 par défaut.

À propos de vSphere ESX Agent Manager (EAM)

vSphere ESX Agent Manager automatise le processus de déploiement et de gestion des services de mise en réseau et de sécurité NSX, tout en développant la fonction d'un hôte ESXi pour fournir des services supplémentaires dont a besoin une solution vSphere.

Journaux et services d'ESX Agent Manager

Des journaux ESX Agent Manager sont inclus dans le cadre du bundle de journaux vCenter.

- Windows : `C:\ProgramData\VMware\vCenterServer\logs\eam\eam.log`
- VCSA : `/var/log/vmware/vpx/eam.log`
- ESXi : `/var/log/esxupdate.log`

Surveillance d'ESX Agent Manager

Important Veillez à passer l'indicateur *bypassVumEnabled* sur **`True`** avant de démarrer l'installation de NSX et à le repasser sur **`False`** après l'installation. Reportez-vous à la section https://kb.vmware.com/kb/2053782.

Pour vérifier l'état d'ESX Agent Manager :

1 Accédez à vSphere Web Client.

2 Cliquez sur **Administration > Extensions de vCenter Server (Administration > vCenter Server Extensions)**, puis cliquez sur vSphere ESX Agent Manager.

   a Cliquez sur l'onglet **Gérer (Manage)**.

   L'onglet **Gérer (Manage)** indique des informations sur l'exécution des agences, liste les agents ESX orphelins et journalise des informations sur les agents ESX gérés par ESX Agent Manager.

   Pour plus d'informations sur les agents et les agences, consultez la documentation de vSphere.

   b Cliquez sur l'onglet **Surveiller (Monitor)**.

L'onglet **Surveiller (Monitor) > Événements (Events)** affiche des informations sur les événements associés à ESX Agent Manager.

Dépannage des problèmes de NSX Manager

Vérifiez que chaque étape du dépannage est correcte pour votre environnement. Chaque étape fournit des instructions afin d'éliminer les causes possibles et de prendre une mesure corrective si nécessaire. Les étapes sont classées dans l'ordre le plus approprié afin d'isoler le problème et d'identifier la bonne résolution. Ne sautez pas une étape.

Problème

- L'installation de VMware NSX Manager échoue.
- La mise à niveau de VMware NSX Manager échoue.
- La connexion à VMware NSX Manager échoue.
- L'accès à VMware NSX Manager échoue.

Solution

1. Consultez les *Notes de mise à jour de NSX* des versions actuelles pour voir si le problème est résolu dans un correctif de bogue.
2. Vérifiez que la configuration système requise minimale est respectée lorsque vous installez VMware NSX Manager.

   Reportez-vous à *Guide d'installation de NSX*.
3. Vérifiez que tous les ports requis sont ouverts dans NSX Manager.

   Reportez-vous à *Guide d'installation de NSX*.
4. Problèmes d'installation :
   - Si la configuration du service de recherche ou de vCenter Server échoue, vérifiez que les dispositifs NSX Manager et du service de recherche sont synchronisés. Utilisez les mêmes configurations de serveur NTP sur NSX Manager et sur le service de recherche. De plus, vérifiez que le DNS est correctement configuré.
   - Vérifiez que le fichier OVA est installé correctement. Si un fichier OVA de NSX ne peut pas être installé, une fenêtre d'erreur dans vSphere Client indique où l'erreur s'est produite. De plus, vérifiez la somme de contrôle MD5 du fichier OVA/OVF téléchargé.
   - Vérifiez que l'heure sur les hôtes ESXi est synchronisée avec NSX Manager.
   - VMware recommande de planifier une sauvegarde des données de NSX Manager immédiatement après l'installation de NSX Manager.
5. Problèmes de mise à niveau :
   - Avant la mise à niveau, consultez les dernières informations sur l'interopérabilité sur la page Matrices d'interopérabilité des produits.

- VMware recommande de sauvegarder la configuration actuelle et de télécharger des journaux de support technique avant la mise à niveau.
- Une resynchronisation forcée avec vCenter Server peut être nécessaire après la mise à niveau de NSX Manager. Pour cela, connectez-vous à l'interface utilisateur graphique Web de NSX Manager. Ensuite, accédez à **Gérer l'enregistrement de vCenter > Service de gestion de NSX > Modifier (Manage vCenter Registration > NSX Management Service > Edit)** et entrez de nouveau le mot de passe de l'administrateur.

6 Problèmes de performances :

- Vérifiez que les exigences de vCPU minimales sont respectées.
- Vérifiez que la partition racine (/) dispose de suffisamment d'espace. Pour cela, connectez-vous à l'hôte ESXi et saisissez cette commande `df –h`.

  Par exemple :

```
[root@esx-01a:~] df -h
Filesystem   Size   Used Available Use% Mounted on
NFS        111.4G  80.8G     30.5G  73% /vmfs/volumes/ds-site-a-nfs01
vfat       249.7M 172.2M     77.5M  69% /vmfs/volumes/68cb5875-d887b9c6-a805-65901f83f3d4
vfat       249.7M 167.7M     82.0M  67% /vmfs/volumes/fe84b77a-b2a8860f-38cf-168d5dfe66a5
vfat       285.8M 206.3M     79.6M  72% /vmfs/volumes/54de790f-05f8a633-2ad8-00505603302a
```

- Utilisez la commande `esxtop` pour vérifier quels processus utilisent de grandes quantités de CPU et de mémoire.
- Si NSX Manager rencontre des erreurs de mémoire insuffisante dans les journaux, vérifiez que le fichier `/common/dumps/java.hprof` existe. Si ce fichier existe, créez une copie du fichier et joignez-la au bundle de journaux de support technique NSX.
- Vérifiez qu'il n'y a pas de problèmes de latence de stockage dans l'environnement.
- Essayez de migrer NSX Manager vers un autre hôte ESXi.

7 Problèmes de connectivité :

- Si NSX Manager rencontre des problèmes de connectivité avec vCenter Server ou avec l'hôte ESXi, connectez-vous à la console d'interface de ligne de commande de NSX Manager, exécutez la commande `debug connection IP_of_ESXi_or_VC` et examinez la sortie.
- Vérifiez que les services de gestion Web de Virtual Center sont démarrés et que le navigateur n'est pas dans un état d'erreur.
- Si l'interface utilisateur Web de NSX Manager n'est pas mise à jour, vous pouvez essayer de résoudre le problème en désactivant et en réactivant les services Web. Reportez-vous à la section https://kb.vmware.com/kb/2126701.
- Vérifiez quel groupe de ports et quelle carte réseau de liaison montante sont utilisés par NSX Manager à l'aide de la commande `esxtop` sur l'hôte ESXi. Pour plus d'informations, consultez https://kb.vmware.com/kb/1003893.

- Essayez de migrer NSX Manager vers un autre hôte ESXi.
- Consultez l'onglet **Tâches et événements (Tasks and Events)** du dispositif de machine virtuelle de NSX Manager de vSphere Web Client sous l'onglet **Surveiller (Monitor)**.
- Si NSX Manager rencontre des problèmes de connectivité avec vCenter Server, essayez de migrer NSX Manager vers le même hôte ESXi sur lequel la machine virtuelle vCenter Server est exécutée pour éliminer les problèmes possibles du réseau physique sous-jacent.

  Notez que cela ne fonctionne que si les deux machines virtuelles se trouvent sur le même VLAN/groupe de ports.

Connexion de NSX Manager à vCenter Server

Une connexion entre NSX Manager et vCenter Server permet à NSX Manager d'utiliser vSphere API pour exécuter des fonctions telles que déployer des machines virtuelles de service, préparer des hôtes et créer des groupes de ports de commutateur logique. Le processus de connexion installe un plug-in de client Web pour NSX sur Web Client Server.

Pour que la connexion fonctionne, DNS et NTP doivent être configurés sur NSX Manager, vCenter Server et les hôtes ESXi. Si vous avez ajouté des hôtes ESXi par nom à l'inventaire vSphere, assurez-vous que des serveurs DNS ont été configurés sur NSX Manager et que la résolution de noms fonctionne correctement. Sinon, NSX Manager ne peut pas résoudre les adresses IP. Le serveur NTP doit être spécifié de sorte que l'heure du serveur SSO et l'heure de NSX Manager soient synchronisées. Sur NSX Manager, le fichier drift dans `/etc/ntp.drift` est inclus dans le bundle de support technique de NSX Manager.

Le compte que vous utilisez pour connecter NSX Manager à vCenter Server doit posséder le rôle vCenter « Administrateur ». Posséder le rôle « Administrateur » permet à NSX Manager de s'enregistrer avec le serveur de service de jeton de sécurité. Lorsqu'un compte d'utilisateur particulier est utilisé pour connecter NSX Manager à vCenter, un rôle « Administrateur d'entreprise » pour l'utilisateur est également créé sur NSX Manager.

Problèmes courants liés à la connexion de NSX Manager à vCenter Server

- DNS mal configuré sur NSX Manager, vCenter Server ou un hôte ESXi.
- NTP mal configuré sur NSX Manager, vCenter Server ou un hôte ESXi.
- Compte d'utilisateur sans rôle vCenter « Administrateur » utilisé pour connecter NSX Manager à vCenter.
- Problèmes de connectivité réseau entre NSX Manager et vCenter Server.
- Utilisateur se connectant à vCenter avec un compte qui n'a pas de rôle sur NSX Manager.

Vous devez commencer par vous connecter à vCenter avec le compte que vous avez utilisé pour lier NSX Manager à vCenter Server. Ensuite, vous pouvez créer des utilisateurs supplémentaires avec des rôles sur NSX Manager à l'aide de **Accueil > Mise en réseau et sécurité > Instances de NSX Manager > {Adresse IP de NSX Manager} > Gérer > Utilisateurs (Home > Networking & Security > NSX Managers > {IP of NSX Manager} > Manage > Users)**.

La première connexion prend jusqu'à 4 minutes pendant que vCenter charge et déploie les bundles d'interface utilisateur de NSX.

Vérifier la connectivité de NSX Manager vers vCenter Server

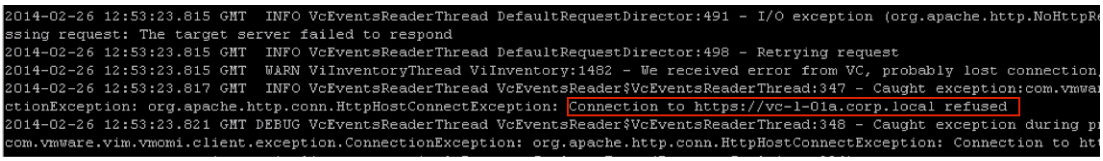
- Connectez-vous à la console d'interface de ligne de commande de NSX Manager.
- Pour vérifier la connectivité, affichez les tables ARP et de routage.

```
nsxmgr# show arp
IP address       HW type     Flags     HW address            Mask     Device
192.168.110.31   0x1         0x2       00:50:56:ae:ab:01     *        mgmt
192.168.110.2    0x1         0x2       00:50:56:01:20:a5     *        mgmt
192.168.110.1    0x1         0x2       00:50:56:01:20:a5     *        mgmt
192.168.110.33   0x1         0x2       00:50:56:ae:4f:7c     *        mgmt
192.168.110.32   0x1         0x2       00:50:56:ae:50:bf     *        mgmt
192.168.110.10   0x1         0x2       00:50:56:03:19:4e     *        mgmt
192.168.110.51   0x1         0x2       00:50:56:03:30:2a     *        mgmt
192.168.110.22   0x1         0x2       00:50:56:01:21:f9     *        mgmt
192.168.110.55   0x1         0x2       00:50:56:01:23:21     *        mgmt
192.168.110.26   0x1         0x2       00:50:56:01:21:ef     *        mgmt
192.168.110.54   0x1         0x2       00:50:56:01:22:ef     *        mgmt
192.168.110.52   0x1         0x2       00:50:56:03:30:16     *        mgmt
```

```
nsxmgr# show ip route
Codes: K – kernel route, C – connected, S – static,
       > – selected route, * – FIB route

S>* 0.0.0.0/0 [1/0] via 192.168.110.1, mgmt
C>* 192.168.110.0/24 is directly connected, mgmt
```

- Recherchez les erreurs dans le journal de NSX Manager qui indiquent la raison de la non-connexion à vCenter Server. La commande qui permet d'afficher le journal est `show log manager follow`.



- Exécutez la commande `debug connection IP_of_ESXi_or_VC` et examinez la sortie.

Exécuter la capture de paquets sur NSX Manager pour afficher les connexions

Utilisez la commande de paquet de débogage : `debug packet [capture|display] interface interface filter`

Le nom d'interface sur NSX Manager est `mgmt`.

La syntaxe de filtre présente le format suivant : « port_80_or_port_443 »

La commande s'exécute uniquement en mode privilégié. Pour passer en mode privilégié, exécutez la commande `enable` et fournissez le mot de passe d'administrateur.

Exemple de capture de paquet :

```
nsxmgr# en
nsxmgr# debug packet display interface mgmt port_80_or_port_443
tcpdump: verbose output suppressed, use –v or –vv for full protocol decode
listening on mgmt, link–type EN10MB (Ethernet), capture size 262144 bytes
23:40:25.321085 IP 192.168.210.15.54688 > 192.168.210.22.443: Flags [P.], seq 2645022162:2645022199,
ack 2668322748, win 244, options [nop,nop,TS val 1447550948 ecr 365097421], length 37
...
```

Vérifier la configuration réseau sur NSX Manager

La commande `show running–config` indique la configuration de base de l'interface de gestion, de NTP et des paramètres d'itinéraire par défaut.

```
nsxmgr# show running–config
Building configuration...

Current configuration:
!
ntp server 192.168.110.1
!
ip name server 192.168.110.10
!
hostname nsxmgr
!
interface mgmt
 ip address 192.168.110.15/24
!
ip route 0.0.0.0/0 192.168.110.1
!
web–manager
```

Certificats de NSX Manager

NSX Manager prend en charge deux manières de générer des certificats.

- CSR générée par NSX Manager : fonctionnalité limitée due à une CSR de base
- PKCS#12 : recommandé pour la production

L'impossibilité du CMS à passer des appels API en mode silencieux est un problème connu.

Cela se produit lorsque l'émetteur du certificat n'est pas connu de l'appelant, car il s'agit d'une autorité de certification racine non approuvée ou car le certificat est auto-signé. Pour résoudre ce problème, utilisez un navigateur pour accéder à l'adresse IP ou au nom d'hôte de NSX Manager et accepter le certificat.

Dispositif NSX Manager secondaire bloqué en mode de transit

Utilisez la solution décrite ci-dessous si votre dispositif NSX Manager secondaire se bloque en mode de transit comme décrit dans le problème. Le problème se produit lorsque vous restaurez la sauvegarde sur le dispositif NSX Manager primaire lorsque le dispositif NSX Managersecondaire est en mode de transit.

Problème

1 Vous avez configuré les dispositifs NSX Manager primaire et secondaire.

2 Vous prenez la sauvegarde du dispositif NSX Manager primaire.

3 Plus tard, vous supprimez le dispositif NSX Manager secondaire. Le dispositif NSX Manager secondaire est en mode de transit.

4 Maintenant, pour certaines raisons, vous restaurez la sauvegarde sur le dispositif NSX Manager primaire.

5 Dans la base de données, le dispositif NSX Manager de transit est mis à jour comme **Secondaire (Secondary)**, mais dans l'interface utilisateur, il s'affiche comme étant en **Transit** et la synchronisation échoue.

6 Il se peut que vous ne puissiez pas supprimer le dispositif NSX Manager secondaire ou le promouvoir à nouveau comme secondaire.

7 Pendant la promotion du dispositif NSX Manager de transit, un message d'erreur indiquant que le `Nœud NSX Manager avec l'adresse IP/nom d'hôte existe déjà` s'affiche.

8 Pendant la suppression du dispositif NSX Manager de transit, un message d'erreur indiquant `Nom d'utilisateur ou mot de passe incorrect` s'affiche.

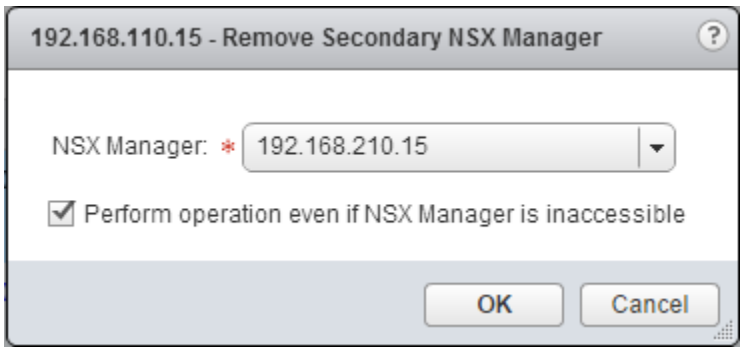
Solution

1 Connectez-vous au vCenter lié à l'instance principale du dispositif NSX Manager à l'aide du vSphere Web Client.

2 Accédez à **Accueil (Home) > Networking & Security**> **Installation**, puis sélectionnez l'onglet **Gestion (Management)**.

3 Sélectionnez le dispositif NSX Manager secondaire que vous souhaitez supprimer, puis cliquez sur **Actions**, puis sur **Supprimer un NSX Manager secondaire (Remove Secondary NSX Manager)**.

Une boîte de dialogue de confirmation s'affiche.



4 Cochez la case **Effectuer l'opération même si NSX Manager est inaccessible (Perform operation even if NSX Manager is inaccessible)**.

5 Cliquez sur **OK**.

Le dispositif NSX Manager secondaire est supprimé de la base de données primaire.

6 Rajoutez le dispositif NSX Manager secondaire.

Étape suivante

Pour plus d'informations sur l'ajout du dispositif NSX Manager secondaire, consultez le *Guide d'installation de NSX*.

Échec de la configuration du service de recherche SSO pour NSX

Problème

- L'enregistrement de NSX Manager sur vCenter Server échoue
- La configuration du service de recherche SSO échoue
- Les erreurs suivantes peuvent apparaître :

```
nested exception is java.net.UnknownHostException: vc.local( vc.corp.local )
```

```
NSX Management Service operation failed.( Initialization of Admin Registration Service Provider failed. Root Cause: Error occurred while registration of lookup service, com.vmware.vim.sso.admin.exception.InternalError: General failure.
```

```
com.vmware.vshield.vsm.security.service.impl.SamlTokenSSOAuthenticator : SSO is not configured or initialized properly so cannot authenticate user.
```

Solution

1 Problèmes de connectivité :

- Si NSX Manager rencontre des problèmes de connectivité avec vCenter Server ou avec l'hôte ESXi, connectez-vous à la console d'interface de ligne de commande de NSX Manager, exécutez la commande `debug connection IP_of_ESXi_or_VC` et examinez la sortie.
- Exécutez une commande ping à partir de NSX Manager vers vCenter Server avec l'adresse IP et le nom de domaine complet pour vérifier le routage ou l'itinéraire par défaut ou statique dans NSX Manager, à l'aide de cette commande :

  ```
  nsxmgr-l-01a# show ip route
  ```

  Codes :

  K : itinéraire du noyau

  C : connecté

  S : statique

  > : itinéraire sélectionné

* : itinéraire FIB

```
S>* 0.0.0.0/0 [1/0] via 192.168.110.2, mgmt

C>* 192.168.110.0/24 is directly connected, mgmt
```

2 Problème de DNS

Exécutez une commande ping à partir de NSX Manager vers vCenter Server avec le nom de domaine complet à l'aide de cette commande :

```
nsx-mgr> ping vc-l-01a.corp.local
```

Un résultat semblable à l'exemple suivant doit apparaître :

```
nsx-mgr> ping vc-l-01a.corp.local
PING vc-1-01a.corp.local (192.168.110.51): 56 data bytes
64 bytes from 192.168.110.51: icmp_seq=0 ttl=64 time=1.749 ms
64 bytes from 192.168.110.51: icmp_seq=1 ttl=64 time=2.111 ms
64 bytes from 192.168.110.51: icmp_seq=2 ttl=64 time=8.082 ms
64 bytes from 192.168.110.51: icmp_seq=3 ttl=64 time=2.010 ms
64 bytes from 192.168.110.51: icmp_seq=4 ttl=64 time=0.857 ms
```

Si cela ne fonctionne pas, accédez à **Gérer > Réseau > Serveurs DNS (Manage > Network > DNS Servers)** dans NSX Manager et vérifiez que DNS est correctement configuré.

3 Problème de pare-feu

S'il existe un pare-feu entre NSX Manager et vCenter Server, vérifiez qu'il autorise SSL sur `TCP/443`. De plus, exécutez une commande ping pour vérifier la connectivité.

4 Vérifiez que tous les ports requis suivants sont ouverts dans NSX Manager.

Tableau 2-1. Ports ouverts de NSX Manager

Port	Requis pour
443/TCP	Le téléchargement du fichier OVA sur l'hôte ESXI pour le déploiement L'utilisation d'API REST L'utilisation de l'interface utilisateur de NSX Manager
80/TCP	Le lancement de la connexion au SDK de vSphere La messagerie entre NSX Manager et les modules d'hôte NSX
1234/TCP	La communication entre NSX Controller et NSX Manager
5671	Rabbit MQ (technologie de bus de messagerie)
22/TCP	Accès de la console (SSH) à l'interface de ligne de commande Remarque : par défaut, ce port est fermé

5 Problèmes de NTP

Vérifiez que l'heure est synchronisée entre vCenter Server et NSX Manager. Pour cela, utilisez les mêmes configurations de serveur NTP sur NSX Manager et sur vCenter Server.

Pour déterminer l'heure sur NSX Manager, exécutez cette commande à partir de l'interface de ligne de commande :

```
nsxmgr-l-01a# show clock

Tue Nov 18 06:51:34 UTC 2014
```

Pour déterminer l'heure sur vCenter Server, exécutez cette commande sur l'interface de ligne de commande :

vc-l-01a:~ # date

Un résultat semblable à l'exemple suivant doit apparaître :

```
Tue Nov 18 06:51:31 UTC 2014
```

Remarque : après la configuration des paramètres d'heure, redémarrez le dispositif.

6 Problèmes d'autorisation utilisateur

Assurez-vous que l'utilisateur dispose des privilèges **admin**.

Pour vous inscrire à vCenter Server ou au service de recherche SSO, vous devez disposer de droits d'administration.

Le compte par défaut est `administrator user: administrator@vsphere.local`

7 Reconnectez-vous à SSO en entrant les informations d'identification.

Préparation du réseau logique : transport VXLAN

NSX prépare le commutateur vSphere Distributed Switch que vous sélectionnez pour VXLAN en créant un groupe de ports virtuels distribué pour les cartes réseau VMkernel de VTEP.

La stratégie d'association, la méthode d'équilibrage de charge, le MTU et l'ID VLAN des VTEP sont choisis lors de la configuration de VXLAN. Les méthodes d'association et d'équilibrage de charge doivent correspondre à la configuration du DVS sélectionné pour le VXLAN.

Le MTU doit être défini pour être au moins égal à 1 600 et supérieur à ce qui est déjà configuré sur le DVS.

Le nombre de VTEP créés dépend de la stratégie d'association sélectionnée et de la configuration du DVS.

Problèmes courants lors de la préparation de VXLAN

La préparation de VXLAN peut échouer pour plusieurs raisons :

- La méthode d'association choisie pour VXLAN ne correspond pas à ce qui peut être pris en charge par le DVS. Pour connaître les méthodes prises en charge, consultez le *Guide de conception de virtualisation réseau de VMware NSX for vSphere* à l'adresse https://communities.vmware.com/docs/DOC-27683.
- Un ID VLAN incorrect est choisi pour les VTEP.
- DHCP sélectionné pour attribuer des adresses IP de VTEP, mais aucun serveur DHCP n'est disponible.
- Il manque une carte réseau VMkernel. Résolvez l'erreur comme décrit dans la section Carte réseau VMkernel de VXLAN désynchronisée.
- Une carte réseau VMkernel dispose d'une adresse IP incorrecte. Résolvez l'erreur comme décrit dans la section https://kb.vmware.com/kb/2137025.
- Un paramètre MTU incorrect est choisi pour les VTEP. Vous devez examiner s'il existe une incompatibilité de MTU, comme décrit plus loin dans cette rubrique.
- Une passerelle VXLAN incorrecte est choisie. Vous devez examiner s'il existe une erreur lors de la configuration de la passerelle VXLAN, comme décrit plus loin dans cette rubrique.

Numéros de port importants

Le port UDP de VXLAN est utilisé pour l'encapsulation UDP. Avant NSX 6.2.3, le numéro de port VXLAN par défaut était 8472. Dans NSX 6.2.3, le numéro de port VXLAN par défaut est devenu le port 4789 pour les nouvelles installations. Dans les installations de NSX 6.2 et versions ultérieures qui utilisent un VTEP matériel, vous devez utiliser le numéro de port VXLAN 4789. Pour plus d'informations sur la modification de la configuration du port VXLAN, reportez-vous à la section « Modifier le port VXLAN » dans le *Guide d'administration de NSX*.

Le plan de contrôle apparaît à l'état *désactivé* si l'hôte ne possède pas de machine virtuelle active qui nécessite une connexion de contrôleur

Utilisez les commandes `show logical-switch` pour afficher les informations relatives à VXLAN sur l'hôte. Pour plus de détails, consultez le *Référence de l'interface de ligne de commandes de NSX*.

La commande `show logical-switch host hostID verbose` affiche l'état du plan de contrôle comme *désactivé* si l'hôte ne possède pas de machine virtuelle qui nécessite une connexion au cluster de contrôleurs pour recueillir les informations de la table de transfert.

```
Network count:  18
VXLAN network:  32003
Multicast IP:   0.0.0.0
Control plane:  Disabled  <<========
MAC entry count:        0
ARP entry count:        0
Port count:     1
```

Erreur lors de la configuration de la passerelle VXLAN

Lors de la configuration de VXLAN à l'aide d'un pool d'adresses IP statiques dans **Mise en réseau et sécurité > Installation > Préparation de l'hôte > Configurer VXLAN (Networking & Security > Installation > Host Preparation > Configure VXLAN)**, lorsque la configuration ne parvient pas à définir une passerelle de pool d'adresses IP sur le VTEP, la configuration de VXLAN passe à l'état Erreur (ROUGE) pour le cluster d'hôtes. Le message d'erreur est « `La passerelle VXLAN ne peut pas être définie sur l'hôte` » et l'état d'erreur est « `VXLAN_GATEWAY_SETUP_FAILURE` ».

Dans l'appel d'API REST, `GET https://<nsxmgr-ip>/api/2.0/nwfabric/status?resource=<cluster-moid>`, l'état de VXLAN est le suivant :

```
<nwFabricFeatureStatus>
<featureId>com.vmware.vshield.nsxmgr.vxlan</featureId>
  <featureVersion>5.5</featureVersion>
  <updateAvailable>false</updateAvailable>
  <status>RED</status>
  <message>VXLAN Gateway cannot be set on host</message>
  <installed>true</installed>
  <enabled>true</enabled>
  <errorStatus>VXLAN_GATEWAY_SETUP_FAILURE</errorStatus>
</nwFabricFeatureStatus>
```

Solution : il existe deux options permettant de corriger l'erreur.

- `Option 1` : supprimez la configuration de VXLAN pour le cluster hôte, corrigez l'installation de la passerelle sous-jacente dans le pool d'adresses IP en vous assurant que la passerelle est correctement configurée et qu'elle est accessible, puis reconfigurez VXLAN pour le cluster hôte.
- `Option 2` : procédez comme suit :
  a. Corrigez l'installation de passerelle sous-jacente dans le pool d'adresses IP en vous assurant que la passerelle est correctement configurée et qu'elle est accessible.
  b. Mettez l'hôte (ou les hôtes) en mode de maintenance pour s'assurer que le trafic de VM est actif sur l'hôte.
  c. Supprimez les VTEP VXLAN de l'hôte.

d Faites sortir l'hôte du mode de maintenance. Lorsque les hôtes quittent le mode de maintenance, le processus de création des VTEP VXLAN se déclenche sur NSX Manager. NSX Manager tentera de recréer les VTEP requis sur l'hôte.

Rechercher une incompatibilité de MTU

- Exécutez la commande suivante pour vérifier si le MTU est configuré sur 1 600 ou plus :

  `ping ++netstack=vxlan –d –s 1572 –I` <vmkx hostname_or_IP>

  où *vmkx* est l'ID de votre port VMkernel et *hostname_or_IP* est l'adresse IP ou le nom d'hôte du port VMkernel.

  Cela vous permet de vérifier la validité de toutes les liaisons montantes. Si vous travaillez dans un environnement à plusieurs VTEP, vous pouvez valider toutes les liaisons montantes en exécutant la commande ping à partir de chaque interface de source/destination de VMkernel de VTEP possible pour valider tous les chemins.

- Vérifiez l'infrastructure physique. Souvent, le problème est résolu par une modification de configuration de l'infrastructure physique.
- Déterminez si le problème se limite à un seul commutateur logique ou si d'autres commutateurs logiques sont également affectés. Vérifiez si le problème concerne tous les commutateurs logiques.

Pour plus d'informations sur la vérification de MTU, reportez-vous à la section « Vérifier l'état de marche de NSX » dans le *Guide de mise à niveau de NSX*.

Carte réseau VMkernel de VXLAN désynchronisée

Lorsque la carte réseau VMkernel est supprimée sur l'hôte, mais que les informations sur la carte réseau VMkernel sont toujours disponibles dans NSX, NSX Manager indique la carte réseau VMkernel supprimée avec une icône **Erreur (Error)**.

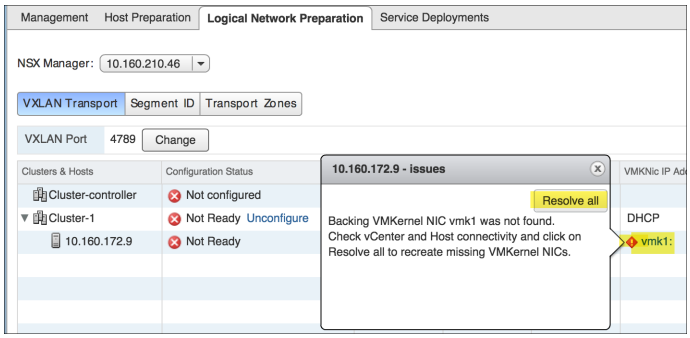
Conditions préalables

La carte réseau VMkernel est supprimée sur l'hôte.

Procédure

1 Dans le vSphere Web Client, accédez à **Networking & Security > Installation** > **Préparation du réseau logique (Logical Network Preparation)**.

2 Dans l'onglet **Transport VXLAN (VXLAN Transport)**, étendez le cluster et les hôtes.



3 Cliquez sur l'icône **Erreur (Error)** pour afficher les informations relatives à la carte réseau VMkernel supprimée sur l'hôte.

4 Cliquez sur le bouton **Tout résoudre (Resolve All)** pour recréer la carte réseau VMkernel supprimée sur l'hôte.

Résultats

La carte réseau VMkernel supprimée est recréée sur l'hôte.

Modification de la stratégie d'association VXLAN et des paramètres MTU

La stratégie d'association VXLAN et les paramètres MTU peuvent être modifiés sur des hôtes et des clusters préparés, mais les modifications s'appliquent uniquement lors de la préparation des nouveaux hôtes et clusters pour VXLAN. Les groupes de ports virtuels existants pour VMkernel de VTEP ne peuvent être modifiés qu'en préparant de nouveau les hôtes et les clusters manuellement. Vous pouvez modifier la stratégie d'association et les paramètres MTU à l'aide d'une API.

Problème

Un paramètre MTU incorrect est choisi pour les VTEP.

Solution

1 Récupérez les informations sur tous les commutateurs préparés pour VXLAN à l'aide de l'API `GET https://<NSX-Manager-IP-Address>/api/2.0/vdn/switches`.

Dans la sortie de l'API, localisez le commutateur que vous voulez modifier, puis notez son nom. Par exemple, *dvs-35*.

2 Recherchez maintenant le commutateur vSphere Distributed Switch spécifique que vous avez noté précédemment.

Par exemple, l'API `GET https://<NSX-Manager-IP-Address>/api/2.0/vdn/switches/dvs-35`.

Un résultat semblable à l'exemple suivant doit apparaître :

```
<vdsContext>
<switch>
 <objectId>dvs-35</objectId>
 <objectTypeName>VmwareDistributedVirtualSwitch</objectTypeName>
 <vsmUuid>423A993F-BEE6-1285-58F1-54E48D508D90</vsmUuid>
 <nodeId>916287b3-761d-430b-8ab2-83878dfe3e7f</nodeId>
 <revision>6</revision>
 <type>
  <typeName>VmwareDistributedVirtualSwitch</typeName>
 </type>
 < name>vds-site-a</name>
 <scope>
  <id>datacenter-21</id>
  <objectTypeName>Datacenter</objectTypeName>
  < name>Datacenter Site A</name>
 </scope>
 <clientHandle/>
 <extendedAttributes/>
 <isUniversal>false</isUniversal>
 <universalRevision>0</universalRevision>
</switch>
<mtu>1600</mtu>
<teaming>FAILOVER_ORDER</teaming>
<uplinkPortName>Uplink 4</uplinkPortName>
<promiscuousMode>false</promiscuousMode
</vdsContext>
```

3 Vous pouvez modifier les paramètres, tels que l'association de stratégie et/ou le MTU, sur un commutateur vSphere Distributed Switch à l'aide de l'appel d'API. L'exemple suivant indique que la stratégie d'association *dvs-35* a été modifiée de *FAILOVER_ORDER* à *LOADBALANCE_SRCMAC* et le paramètre MTU de *1600* à *9000*.

- Pour NSX : `PUT https://<NSX-Manager-IP-Address>/api/2.0/vdn/switches`

Un résultat semblable à l'exemple suivant doit apparaître :

```
<vdsContext>
<switch>
 <objectId>dvs-35</objectId>
 <objectTypeName>VmwareDistributedVirtualSwitch</objectTypeName>
 <vsmUuid>423A993F-BEE6-1285-58F1-54E48D508D90</vsmUuid>
 <nodeId>916287b3-761d-430b-8ab2-83878dfe3e7f</nodeId>
 <revision>6</revision>
 <type>
  <typeName>VmwareDistributedVirtualSwitch</typeName>
 </type>
 <name>vds-site-a</name>
 <scope>
 <id>datacenter-21</id>
 <objectTypeName>Datacenter</objectTypeName>
```

```
 <name>Datacenter Site A</name>
 </scope>
 <clientHandle/>
 <extendedAttributes/>
 <isUniversal>false</isUniversal>
 <universalRevision>0</universalRevision>
</switch>
 <mtu>9000</mtu>
 <teaming>LOADBALANCE_SRCMAC</teaming>
 <uplinkPortName>Uplink 4</uplinkPortName>
 <promiscuousMode>false</promiscuousMode>
</vdsContext>
```

Note Voici une liste des entrées de stratégie d'association valides pour le paramètre *<teaming>* :

- FAILOVER_ORDER
- ETHER_CHANNEL
- LACP_ACTIVE
- LACP_PASSIVE
- LOADBALANCE_LOADBASED
- LOADBALANCE_SRCID
- LOADBALANCE_SRCMAC LACP_V2

4 Vérifiez que la syntaxe utilisée est correcte et que la modification est active pour le commutateur vSphere Distributed Switch que vous utilisez à l'aide de la commande `GET`. Par exemple, `GET https://<NSX-Manager-IP-Address>/api/2.0/vdn/switches/dvs-35`.

5 Ouvrez vSphere Web Client et vérifiez que les modifications de configuration sont prises en compte.

Groupe de ports du commutateur logique désynchronisé

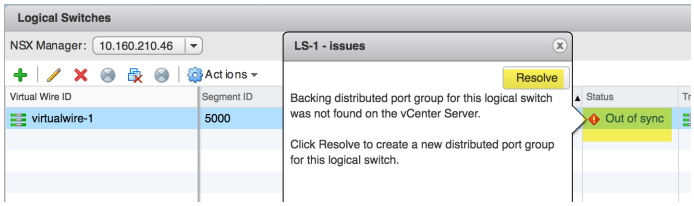
Si le groupe de ports virtuel distribué (DVPG) de sauvegarde du commutateur logique est supprimé sur vCenter Server, la colonne État de la page **Commutateurs logiques (Logical Switches)** affiche l'état **Désynchronisé (Out of sync)**.

Conditions préalables

Le DVPG du commutateur logique est supprimé sur vCenter Server

Procédure

1 Dans vSphere Web Client, accédez à **Page d'accueil (Home) > Mise en réseau et sécurité (Networking & Security)** > **Commutateurs logiques (Logical Switches)**.



2 Dans la colonne État, cliquez sur le lien **Désynchronisé (Out of sync)** pour voir la raison détaillée de cet état désynchronisé.

3 Cliquez sur le bouton **Résoudre (Resolve)** pour résoudre le problème.

Résultats

Cela invoque l'API pour créer le DVPG de sauvegarde.

Dépannage du routage NSX

3

NSX dispose de deux types de sous-système de routage, optimisés pour deux besoins clés.

Les sous-systèmes de routage NSX sont les suivants :

- Routage dans l'espace logique, également appelé routage « Est - Ouest », fourni par le routeur logique distribué (DLR) ;
- Routage entre l'espace physique et l'espace logique, également appelé routage « Nord - Sud », fourni par la passerelle ESG (Edge Services Gateway).

Les deux fournissent des options pour la mise à l'échelle horizontale.

Vous pouvez monter en charge un routage E-O distribué via le DLR.

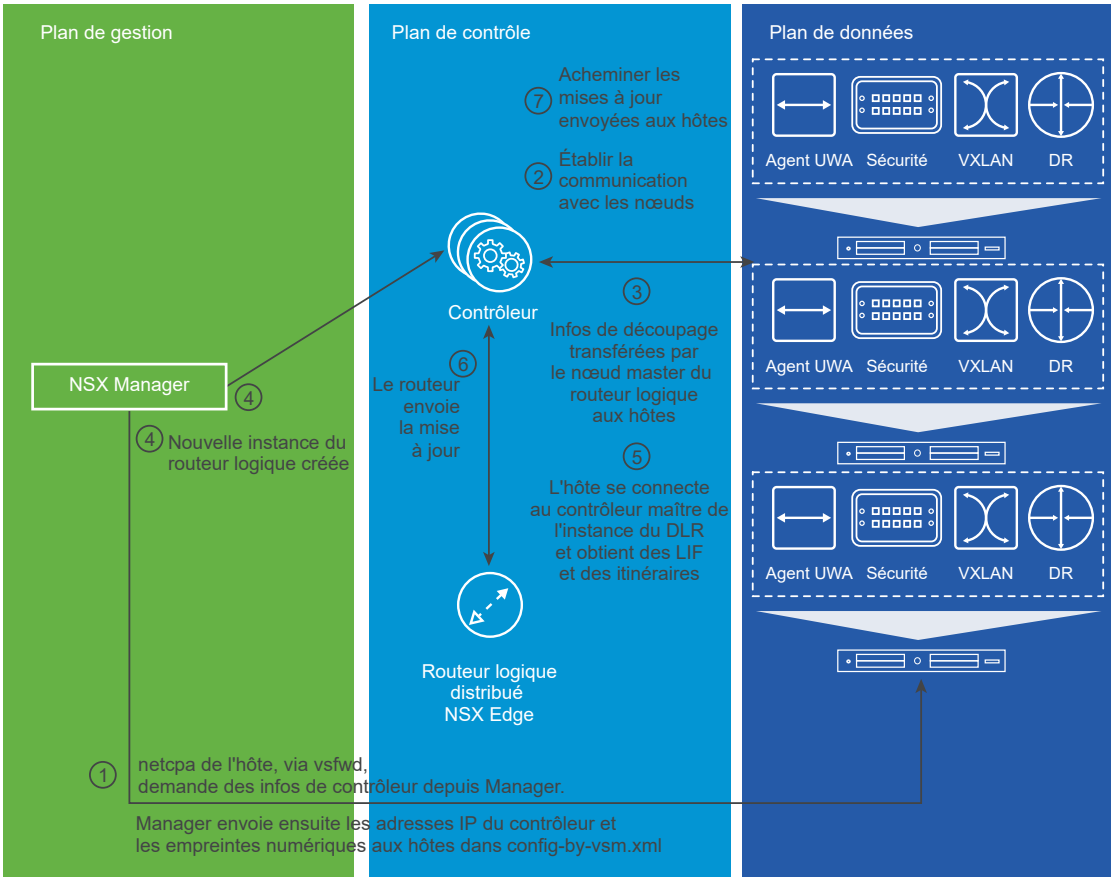
Le DLR prend en charge l'exécution d'un seul protocole de routage dynamique à la fois (OSPF ou BGP) ; la passerelle ESG prend en charge l'exécution des deux protocoles de routage à la fois. Cela s'explique par le fait que le DLR est conçu pour être un routeur « d'extrémité », avec un seul chemin de sortie, ce qui signifie que des configurations de routage plus avancées ne sont en général pas requises.

Le DLR et la passerelle ESG peuvent disposer d'une combinaison d'itinéraires statiques et dynamiques.

Le DLR et la passerelle ESG prennent en charge les itinéraires ECMP.

Les deux fournissent la séparation de domaine L3, ce qui signifie que chaque instance d'un routeur logique distribué ou d'une passerelle ESG possède sa propre configuration L3, semblable à un VRF L3VPN.

Figure 3-1. Création d'un DLR



Ce chapitre contient les rubriques suivantes :

- Comprendre le routeur logique distribué
- Comprendre le routage fourni par la passerelle ESG
- Flux de paquets ECMP
- Routage NSX : conditions requises préalables et considérations
- Interfaces utilisateur du DLR et de la passerelle ESG
- Nouveau dispositif NSX Edge (DLR)
- Opérations d'interface utilisateur classiques de la passerelle ESG et du DLR
- Dépannage du routage NSX

Comprendre le routeur logique distribué

Le DLR est optimisé pour le transfert dans l'espace logique entre des VM, sur des groupes de ports reposant sur VXLAN ou sur VLAN.

Le DLR a les propriétés suivantes :

- Routage de premier saut haute performance et capacité supplémentaire faible :

- Évolue de façon linéaire avec le nombre d'hôtes
- Prend en charge ECMP à 8 voies sur une liaison montante
- Jusqu'à 1 000 instances du DLR par hôte
- Jusqu'à 999 interfaces logiques (LIF) sur chaque DLR (8 x liaison montante + 991 internes) + 1 x gestion
- Jusqu'à 10 000 LIF par hôte distribuées sur toutes les instances du DLR (pas appliqué par NSX Manager)

Gardez les mises en garde suivantes en mémoire :

- Impossible de connecter plusieurs DLR à un VLAN ou VXLAN donné.
- Impossible d'exécuter plusieurs protocoles de routage sur chaque DLR.
- Si OSPF est utilisé, impossible de l'exécuter sur plusieurs liaisons montantes du DLR.
- Pour l'acheminement entre VXLAN et VLAN, la zone de transport doit couvrir un seul DVS.

La conception du DLR à un niveau élevé est comparable à un châssis de routeur modulaire, sur les points suivants :

- Les hôtes ESXi sont comme des cartes de ligne :
  - Ils disposent de ports avec des émetteurs finaux connectés (VM).
  - C'est là que les décisions de transfert sont prises.
- La VM de contrôle du DLR est semblable à un moteur de processeur d'itinéraires :
  - Il exécute des protocoles de routage dynamique afin d'échanger des informations sur le routage avec le reste du réseau.
  - Il calcule des tables de transfert pour des « cartes de ligne » en fonction de la configuration d'interfaces, d'itinéraires statiques et des informations sur le routage dynamique.
  - Il programme ces tables de transfert dans les « cartes de ligne » (via le cluster de contrôleurs, pour permettre la mise à l'échelle et la résilience).
- Le réseau physique connectant des hôtes ESXi entre eux est semblable à un fond de panier :
  - Il transporte les données encapsulées par VLAN ou par VXLAN entre les « cartes de ligne ».

Flux de paquets du DLR de haut niveau

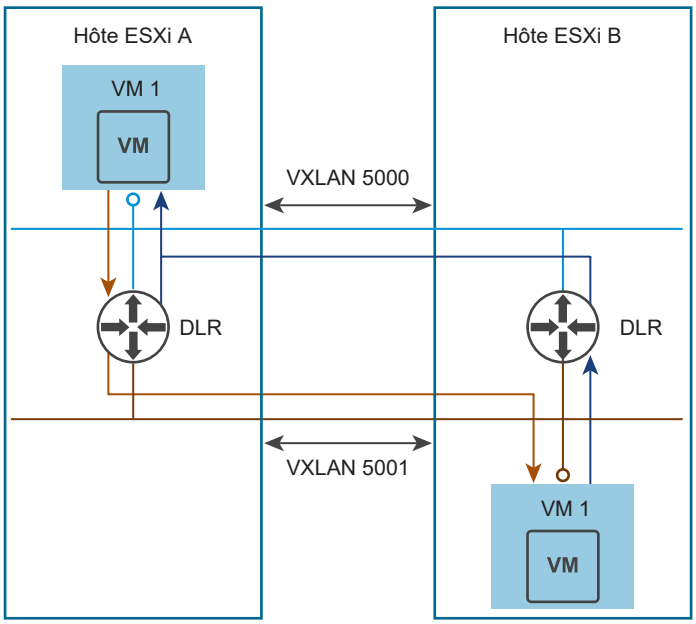
Chaque hôte ESXi dispose de sa propre copie de chaque instance configurée du DLR. Chaque instance du DLR dispose de son propre ensemble unique de tables contenant les informations nécessaires pour transférer des paquets. Ces informations sont synchronisées sur tous les hôtes sur lesquels cette instance du DLR existe. Les instances d'un DLR individuel sur différents hôtes contiennent exactement les mêmes informations.

Le routage est toujours géré par une instance du DLR sur le même hôte sur lequel la machine virtuelle source est exécutée. Cela signifie que lorsque des machines virtuelles source et de destination se trouvent sur des hôtes différents, l'instance du DLR qui fournit le routage entre elles voit des paquets dans une seule direction, de la VM source vers la VM de destination. Le trafic de retour n'est vu que par l'instance correspondante du même DLR sur l'hôte de la VM de destination.

Lorsque que le DLR a terminé le routage, la livraison à la destination finale est de la responsabilité du DVS via L2 – VXLAN ou VLAN si les VM source et de destination se trouvent sur des hôtes différents, ou par le DVS localement si elles se trouvent sur le même hôte.

La Figure 3-2. Flux de paquets du DLR de haut niveau illustre le flux de données entre deux machines virtuelles, VM1 et VM2, exécutées sur des hôtes différents et connectées à deux commutateurs logiques différents, VXLAN 5000 et VXLAN 5001.

Figure 3-2. Flux de paquets du DLR de haut niveau



Flux de paquets (en ignorant la résolution ARP) :

1 VM1 envoie un paquet vers VM2, qui est adressé à la passerelle de VM1 pour le sous-réseau de VM2 (ou celui par défaut). Cette passerelle est une LIF de VXLAN 5000 sur le DLR.

2 Le DVS sur l'Hôte ESXi A fournit le paquet au DLR sur cet hôte, sur lequel la recherche est effectuée, et la LIF de sortie est déterminée (dans ce cas, LIF VXLAN 5001).

3 Le paquet est ensuite envoyé à cette LIF de destination, qui renvoie essentiellement le paquet au DVS, mais sur un commutateur logique différent (5001).

4 Le DVS procède ensuite à la livraison L2 de ce paquet à l'hôte de destination (Hôte ESXi B), où le DVS transférera le paquet à VM2.

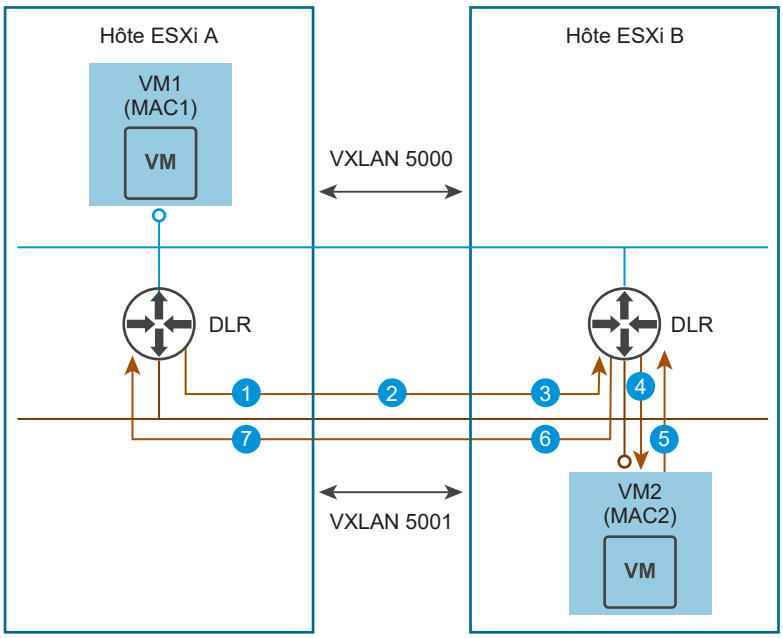
Le trafic de retour suivra dans le même ordre, où le trafic de VM2 est transféré à l'instance du DLR sur l'Hôte ESXi B, puis remis via L2 sur VXLAN 5000.

Processus de résolution d'ARP du DLR

Avant que le trafic de VM1 puisse atteindre VM2, le DLR doit connaître l'adresse MAC de VM2. Une fois qu'il connaît l'adresse MAC de VM2, le DLR peut créer les bons en-têtes L2 pour les paquets sortants.

La Figure 3-3. Processus d'ARP du DLR indique le processus de résolution d'ARP du DLR.

Figure 3-3. Processus d'ARP du DLR



Pour connaître l'adresse MAC, le DLR suit ces étapes :

1 L'instance du DLR sur l'Hôte A génère un paquet de demandes ARP, avec MAC SRC = vMAC et MAC DST = Diffusion. Le module VXLAN sur l'Hôte A trouve tous les VTEP sur le VXLAN 5001 de sortie et envoie à chacun une copie de cette trame de diffusion.

2 Comme la trame quitte l'hôte via le processus d'encapsulation VXLAN, l'adresse MAC SRC passe de vMAC à pMAC A, de sorte que le trafic de retour puisse trouver l'instance du DLR d'origine sur l'Hôte A. La trame est maintenant MAC SRC = pMAC A et MAC DST = Diffusion.

3 Comme la trame est reçue et décapsulée sur l'Hôte B, elle est examinée et on voit qu'elle provient de l'adresse IP qui correspond à la LIF de l'instance du DLR locale sur VXLAN 5001. Cela attribue à la trame l'indicateur abrequest pour exécuter la fonction d'ARP proxy. L'adresse MAC DST passe de Diffusion à vMAC pour que la trame puisse atteindre l'instance du DLR locale.

4 L'instance du DLR locale sur l'Hôte B reçoit la trame Demande d'ARP, MAC SRC = pMAC A, MAC DST = vMAC, et elle voit que l'adresse IP de sa propre LIF la demande. Elle enregistre l'adresse MAC SRC et génère un nouveau paquet de demandes ARP, MAC SRC = vMAC, MAC DST = Diffusion. Cette trame a l'indicateur « DVS Local » pour éviter qu'elle soit saturée via dvUplink. Le DVS fournit la trame à VM2.

5 VM2 envoie une réponse ARP, MAC SRC = MAC2, MAC DST = vMAC. Le DVS la remet à l'instance du DLR locale.

6 L'instance du DLR sur l'Hôte B remplace l'adresse MAC DST par l'adresse pMAC A enregistrée à l'étape 4 et renvoie le paquet au DVS pour remise à l'Hôte A.

7 Une fois que la réponse ARP atteint l'Hôte A, l'adresse MAC DST passe sur vMAC et la trame de réponse ARP avec MAC SRC = MAC2 et MAC DST = vMAC atteint l'instance du DLR sur l'Hôte A.

Le processus de résolution ARP est terminé et l'instance du DLR sur l'Hôte A peut maintenant commencer à envoyer du trafic à VM2.

Suppression ARP du DLR

La suppression ARP (Address Resolution Protocol) est une technique qui permet de réduire la quantité de propagation des diffusions ARP dans des segments VXLAN individuels, c'est-à-dire entre des VM connectées au même commutateur logique.

Lorsque VM1 veut connaître l'adresse MAC de VM2, il envoie une demande ARP. Cette demande ARP est interceptée par le commutateur logique et, si le commutateur logique dispose déjà d'une entrée ARP pour la cible, il envoie la réponse ARP à la machine virtuelle.

Si ce n'est pas le cas, il envoie une requête ARP à NSX Controller. Si le contrôleur connaît la liaison entre adresse IP et adresse MAC de la VM, le contrôleur répond avec la liaison et le commutateur logique envoie la réponse ARP. Si le contrôleur ne dispose pas de l'entrée ARP, la demande ARP est diffusée une nouvelle fois sur le commutateur logique. NSX Controller apprend l'adresse MAC via le module de sécurité de commutateur qui écoute sur les demandes ARP/paquets DHCP.

La suppression ARP a été étendue afin d'inclure également le routeur logique distribué (DLR).

- Les demandes ARP du routeur logique distribué sont traitées de la même façon que les demandes ARP d'autres machines virtuelles et sont soumises à la suppression. Lorsque le routeur logique distribué doit résoudre la demande ARP d'une adresse IP de destination, la demande ARP est supprimée par le commutateur logique, ce qui évite la propagation lorsque la liaison entre adresse IP et adresse MAC est déjà connue par le contrôleur.
- Lorsqu'une LIF est créée, le routeur logique distribué ajoute l'entrée ARP pour l'adresse IP de la LIF dans le commutateur logique, donc les demandes ARP pour l'adresse IP de la LIF sont également supprimées par le commutateur logique.

Comprendre le routage fourni par la passerelle ESG

Le second sous-système du routage NSX est fourni par la passerelle ESG.

La passerelle ESG est essentiellement un routeur dans une machine virtuelle. Elle est livrée dans un facteur de forme semblable à un dispositif avec quatre tailles, et son cycle de vie complet est géré par NSX Manager. La passerelle ESG est utilisée principalement en tant que routeur de périmètre, où elle est déployée entre plusieurs DLR et entre le monde physique et le réseau virtualisé.

La passerelle ESG a les propriétés suivantes :

- Chaque passerelle ESG peut contenir jusqu'à 10 interfaces de vNIC ou 200 sous-interfaces de jonction.

- Chaque passerelle ESG prend en charge ECMP à 8 voies pour la redondance de chemin et l'évolutivité.

Flux de paquets ECMP

Supposons que deux passerelles ESG sont déployées pour fournir une instance du DLR avec des liaisons montantes ECMP bidirectionnelles avec l'environnement physique.

La Figure 3-4. Flux de paquets de la passerelle ESG et du DLR de haut niveau avec ECMP indique le flux de paquets de la passerelle ESG et du DLR lorsque le routage ECMP (Equal-Cost Multipath) est activé entre deux passerelles ESG et l'infrastructure physique.

VM1 a donc accès à deux débits bidirectionnels par rapport à un déploiement avec une seule passerelle ESG.

VM1 est connectée à un commutateur logique avec le VNI 5000.

Le DLR possède deux LIF : Interne sur le VNI 5000 et Liaison montante sur le VNI 5001.

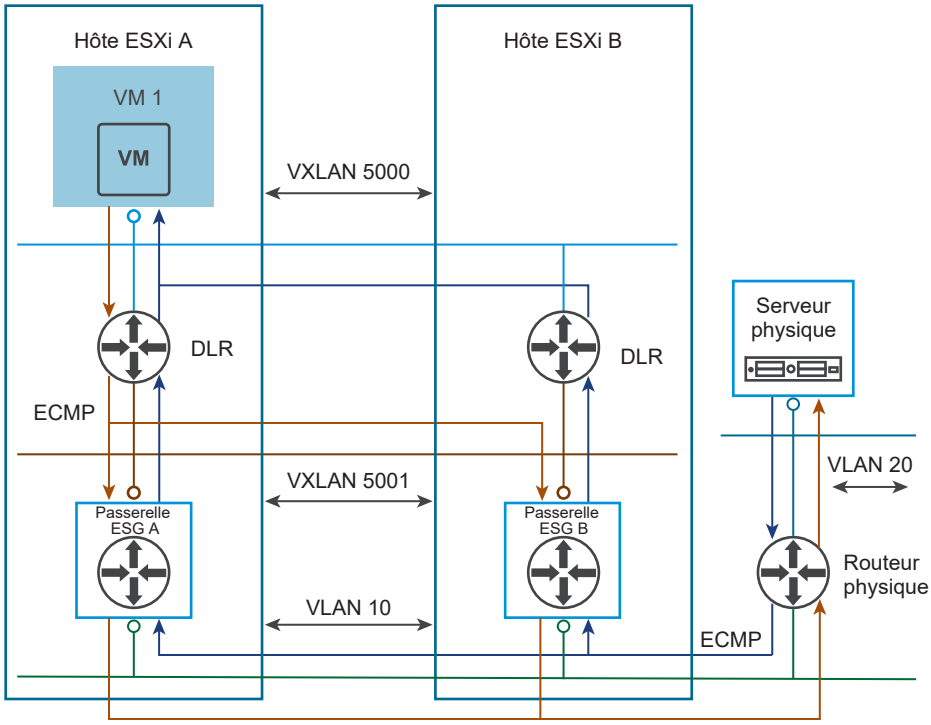
ECMP est activé sur le DLR qui reçoit des itinéraires de même coût vers le sous-réseau IP de VLAN 20 depuis une paire de passerelles ESG, ESG A et ESG B, via un protocole de routage dynamique (BGP ou OSPF).

Les deux passerelles ESG sont connectées à un dvPortgroup reposant sur VLAN associé à VLAN 10, où un routeur physique fournissant la connectivité à VLAN 20 est également connecté.

Les passerelles ESG reçoivent des itinéraires externes pour VLAN 20, via un protocole de routage dynamique depuis le routeur physique.

Le routeur physique en échange prend connaissance du sous-réseau IP associé à VXLAN 5000 depuis les deux passerelles ESG, et effectue l'équilibrage de charge ECMP pour le trafic vers les VM dans ce sous-réseau.

Figure 3-4. Flux de paquets de la passerelle ESG et du DLR de haut niveau avec ECMP



Le DLR peut recevoir jusqu'à huit itinéraires de même coût et équilibrer le trafic entre les itinéraires. ESG A et ESG B dans le schéma fournissent deux itinéraires de même coût.

Les passerelles ESG peuvent procéder au routage ECMP vers le réseau physique, en supposant que plusieurs routeurs physiques sont présents. Pour faire simple, le schéma indique un seul routeur physique.

Il n'est pas nécessaire de configurer ECMP sur les passerelles ESG vers le DLR, car toutes les LIF du DLR sont « locales » sur le même hôte où réside la passerelle ESG. La configuration de plusieurs interfaces de liaison montante sur un DLR n'apporte aucun avantage supplémentaire.

Dans les cas où davantage de bande passante Nord-Sud est requise, plusieurs passerelles ESG peuvent être placées sur différents hôtes ESXi pour passer à environ 80 Gbit/s avec 8 passerelles ESG.

Flux de paquets ECMP (sans la résolution ARP) :

1 VM1 envoie un paquet au serveur physique, qui est envoyé à la passerelle IP de VM1 (qui est une LIF du DLR) sur l'hôte ESXi A.

2 Le DLR effectue une recherche d'itinéraires pour l'adresse IP du serveur physique et il découvre qu'il n'est pas directement connecté, mais il trouve deux itinéraires ECMP reçus de la part des passerelles ESG A et ESG B.

3 Le DLR calcule un hachage ECMP, décide d'un tronçon suivant, qui peut être ESG A ou ESG B, puis envoie le paquet en dehors de la LIF de VXLAN 5001.

4 Le DVS fournit le paquet à la passerelle ESG sélectionnée.

5 La passerelle ESG effectue la recherche de routage et découvre que le sous-réseau du serveur physique est accessible via l'adresse IP du routeur physique sur VLAN 10, qui est directement connecté à l'une des interfaces de la passerelle ESG.

6 Le paquet est envoyé via le DVS, qui le transmet sur le réseau physique après lui avoir attribué l'étiquette 801.Q correcte avec l'ID VLAN 10.

7 Le paquet circule via l'infrastructure de commutation physique pour atteindre le routeur physique, qui effectue une recherche et découvre que le serveur physique est directement connecté à une interface sur VLAN 20.

8 Le routeur physique envoie le paquet au serveur physique.

Sur le chemin du retour :

1 Le serveur physique envoie le paquet à VM1, avec le routeur physique comme tronçon suivant.

2 Le routeur physique effectue une recherche pour le sous-réseau de VM1 et il voit deux chemins de même coût vers ce sous-réseau avec les tronçons suivants, interface VLAN 10 des passerelles ESG A et ESG B, respectivement.

3 Le routeur physique sélectionne l'un des chemins et envoie le paquet à la passerelle ESG correspondante.

4 Le réseau physique fournit le paquet à l'hôte ESXi sur lequel réside la passerelle ESG et la remet au DVS, qui décapsule le paquet et le transfère sur le dvPortgroup associé au VLAN 10 vers la passerelle ESG.

5 La passerelle ESG effectue une recherche d'itinéraires et découvre que le sous-réseau de VM1 est accessible via son interface associée au VXLAN 5001 et le tronçon suivant est l'adresse IP de l'interface de liaison montante du DLR.

6 La passerelle ESG envoie le paquet à l'instance du DLR sur le même hôte que la passerelle ESG.

7 Le DLR effectue une recherche de routage pour découvrir que VM1 est disponible via sa LIF de VXLAN 5000.

8 Le DLR envoie le paquet en dehors de la LIF de VXLAN 5000 au DVS, qui effectue la livraison finale.

Routage NSX : conditions requises préalables et considérations

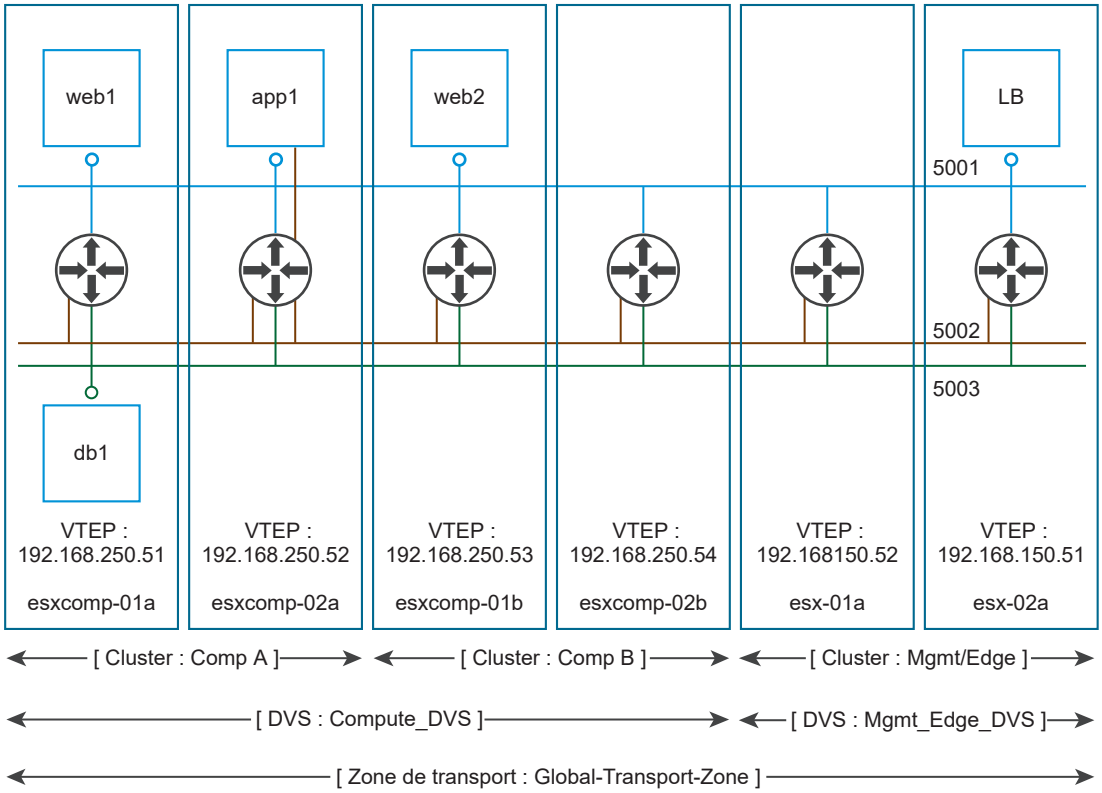
Le DLR et la passerelle ESG reposent sur le DVS pour fournir des services de transfert L2 pour des dvPortgroup (basés sur VXLAN et VLAN) afin que la connectivité de bout en bout fonctionne.

Cela signifie que les services de transfert L2 qui sont connectés au DLR ou à la passerelle ESG doivent être configurés et opérationnels. Dans le processus d'installation de NSX, ces services sont fournis par « Préparation de l'hôte » et « Préparation du réseau logique ».

Lorsque vous créez des zones de transport dans des configurations VDS avec plusieurs clusters, vérifiez que tous les clusters du DVS sélectionné sont inclus sous la zone de transport. Cela permet de s'assurer que le DLR est disponible sur tous les clusters dans lesquels des dvPortgroup du DVS sont disponibles.

Lorsqu'une zone de transport est alignée avec la limite du DVS, l'instance du DLR est créée correctement.

Figure 3-5. Zone de transport correctement alignée avec la limite du DVS



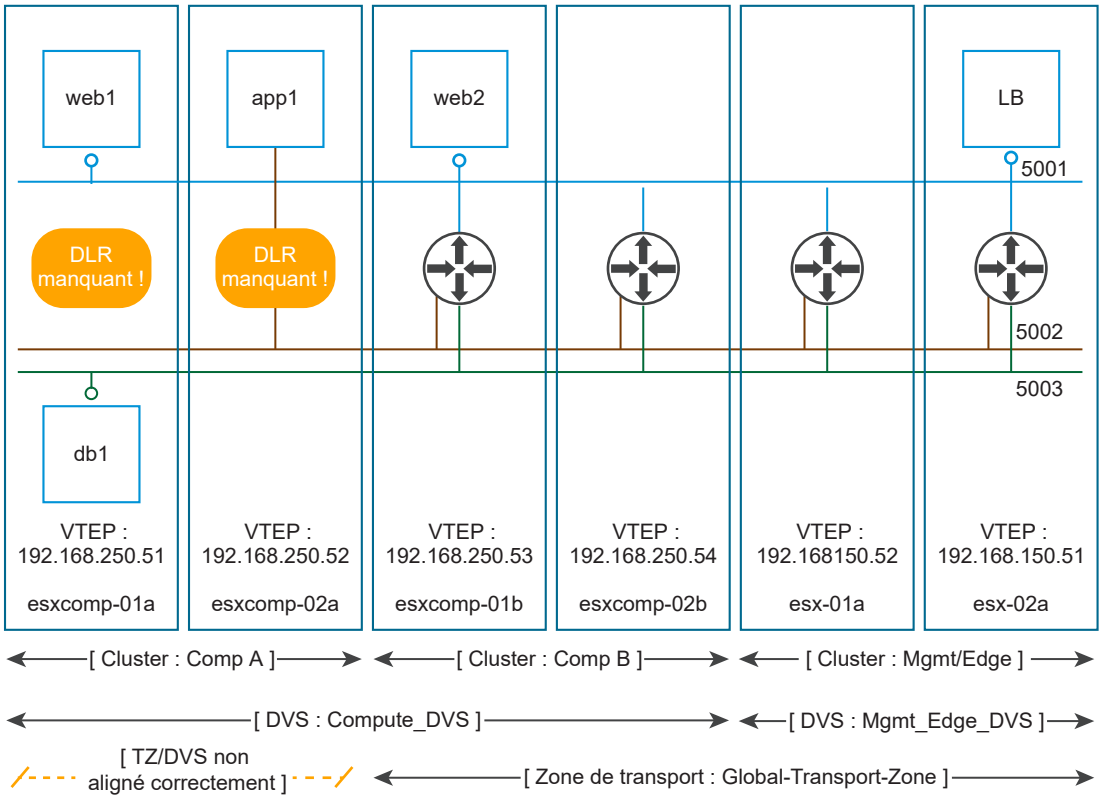
Lorsqu'une zone de transport n'est pas alignée sur la limite du DVS, l'étendue des commutateurs logiques (5001, 5002 et 5003) et des instances du DLR auxquels ces commutateurs logiques sont connectés se retrouve disjointe, ce qui a pour conséquence d'interrompre l'accès des VM du cluster Comp A aux LIF du DLR.

Dans le schéma ci-dessus, le DVS « Compute_DVS » couvre deux clusters, « Comp A » et « Comp B ». « Global-Transport-Zone » inclut « Comp A » et « Comp B ».

Cela se traduit par l'alignement correct entre l'étendue des commutateurs logiques (5001, 5002 et 5003) et l'instance du DLR créée sur tous les hôtes dans tous les clusters sur lesquels ces commutateurs logiques sont présents.

Maintenant, voyons une autre situation, où la zone de transport n'était pas configurée pour inclure le cluster « Comp A » :

Figure 3-6. Zone de transport non alignée avec la limite du DVS



Dans ce cas, les VM exécutées sur le cluster « Comp A » disposent d'un accès complet à tous les commutateurs logiques. Cela s'explique par le fait que les commutateurs logiques sont représentés par des dvPortgoup sur les hôtes, et les dvProtgroup sont une construction au niveau du DVS. Dans notre exemple d'environnement, « Compute_DVS » couvre à la fois « Comp A » et « Comp B ».

Toutefois, les instances du DLR sont créées en alignement strict avec l'étendue de la zone de transport, ce qui signifie qu'aucune instance du DLR ne sera créée sur les hôtes dans « Comp A ».

Par conséquent, la VM « web1 » pourra atteindre les VM « web2 » et « LB », car elles se trouvent sur le même commutateur logique, mais les VM « app1 » et « db1 » ne pourront communiquer avec rien.

Le DLR repose sur le cluster de contrôleurs pour fonctionner, ce qui n'est pas le cas de la passerelle ESG. Avant de créer ou de modifier la configuration d'un DLR, vérifiez que le cluster de contrôleurs est actif et disponible.

Si le DLR doit être connecté à des dvPortgroup de VLAN, vérifiez que les hôtes ESXi avec le DLR configuré peuvent s'atteindre sur UDP/6999 pour que le proxy ARP basé sur VLAN du DLR fonctionne.

Considérations :

- Une instance du DLR donnée ne peut pas être connectée aux commutateurs logiques se trouvant dans des zones de transport distinctes. Cela permet de s'assurer que tous les commutateurs logiques et les instances du DLR sont alignés.

- Le DLR ne peut pas être connecté à des groupes de ports reposant sur VLAN, si ce DLR est connecté à des commutateurs logiques s'étendant sur plusieurs DVS. Comme ci-dessus, cela permet d'assurer un alignement correct des instances du DLR avec les commutateurs logiques et les dvPortgroup sur les hôtes.
- Lorsque vous sélectionnez le placement d'une VM de contrôle du DLR, évitez de la placer sur le même hôte qu'une ou plusieurs de ses passerelles ESG en amont à l'aide de règles d'anti-affinité du DRS si elles se trouvent sur le même cluster. Cela permet de réduire l'impact de l'échec de l'hôte sur le transfert du DLR.
- OSPF ne peut être activé que sur une seule liaison montante (mais il prend en charge plusieurs contiguïtés). BGP, d'un autre côté, peut être activé sur plusieurs interfaces de liaison montante, où cela est nécessaire.

Interfaces utilisateur du DLR et de la passerelle ESG

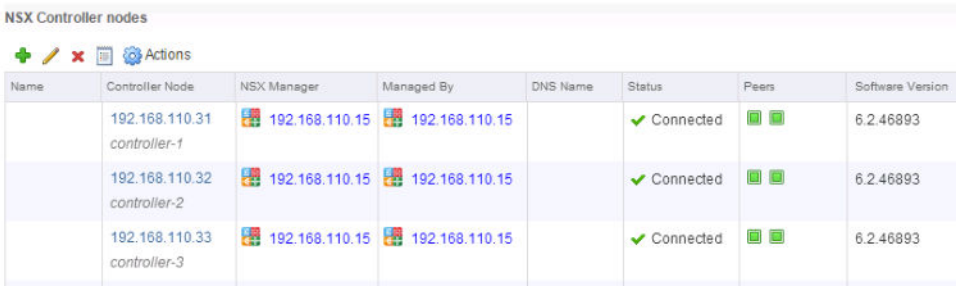
Les interfaces utilisateur du DLR et de la passerelle ESG fournissent des indicateurs de l'état de fonctionnement du système.

Interface utilisateur du routage NSX

L'interface utilisateur de vSphere Web Client fournit deux sections principales applicables au routage NSX.

Elles comportent les dépendances d'infrastructure L2 et de plan de contrôle et la configuration du sous-système de routage.

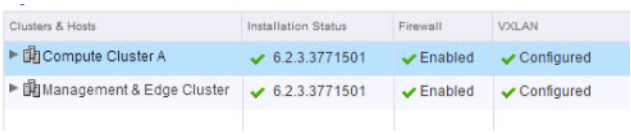
Le routage distribué NSX requiert des fonctions fournies par le cluster de contrôleurs. La capture d'écran suivante montre un cluster de contrôleurs sain.



Points à noter :

- Trois contrôleurs sont déployés.
- L'« État » de tous les contrôleurs est « Connecté ».
- La version logicielle de tous les contrôleurs est la même.
- Chaque nœud de contrôleur contient deux homologues.

Des modules de noyau d'hôte pour le routage distribué sont installés et configurés dans le cadre de la configuration de VXLAN sur l'hôte. Cela signifie que le routage distribué requiert que les hôtes ESXi soient préparés et que VXLAN soit configuré sur eux.

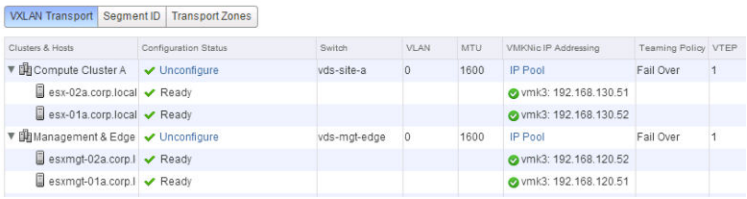


Clusters & Hosts	Installation Status	Firewall	VXLAN
Compute Cluster A	6.2.3.3771501	Enabled	Configured
Management & Edge Cluster	6.2.3.3771501	Enabled	Configured

Points à noter :

- « Statut de l'installation » est en vert.
- « VXLAN » est « Configuré ».

Vérifiez que les composants de transport VXLAN sont bien configurés.



VXLAN Transport | Segment ID | Transport Zones

Clusters & Hosts	Configuration Status	Switch	VLAN	MTU	VMKNic IP Addressing	Teaming Policy	VTEP
Compute Cluster A	Unconfigure	vds-site-a	0	1600	IP Pool	Fail Over	1
esx-02a.corp.local	Ready				vmk3: 192.168.130.51		
esx-01a.corp.local	Ready				vmk3: 192.168.130.52		
Management & Edge	Unconfigure	vds-mgt-edge	0	1600	IP Pool	Fail Over	1
esxmgt-02a.corp.l	Ready				vmk3: 192.168.120.52		
esxmgt-01a.corp.l	Ready				vmk3: 192.168.120.51		

Points à noter :

- L'ID VLAN doit être correct pour le VLAN de transport de VTEP. Notez que dans la capture d'écran ci-dessus, il est égal à « 0 ». Dans la plupart des déploiements réels, ce ne serait pas le cas.
- Le MTU est configuré pour être égal à 1 600 ou plus. Vérifiez que le MTU n'est pas défini sur 9 000 avec l'espoir que le MTU sur les VM soit également défini sur 9 000. Le MTU maximal du DVS est égal à 9 000 et, si des VM sont également définies sur 9 000, il n'y a pas de place pour les en-têtes VXLAN.
- VMKNics doivent contenir les adresses correctes. Vérifiez qu'ils ne sont pas définis sur des adresses 169.254.x.x, ce qui indique que les nœuds n'ont pas pu obtenir les adresses auprès de DHCP.
- La stratégie d'association doit être cohérente pour tous les membres du cluster du même DVS.
- Le nombre de VTEP doit être le même que le nombre de dvUplink. Vérifiez que les adresses IP répertoriées sont valides/attendues.

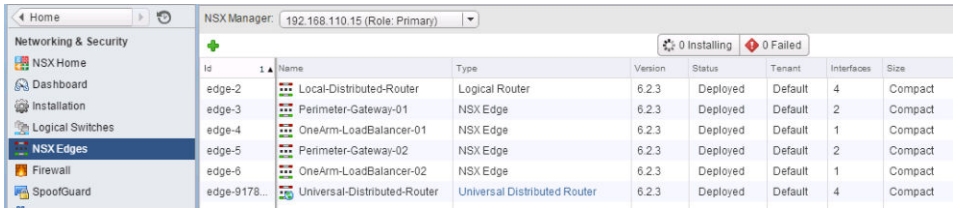
Les zones de transport doivent être correctement alignées sur les limites du DVS pour éviter que le DLR soit manquant sur certains clusters.

Name	NSX vSwitch	Status
Compute Cluster A	vds-site-a	Normal
Management & Edge ...	vds-mgt-edge	Normal

Interface utilisateur de NSX Edge

Le sous-système de routage NSX est configuré et géré dans la section « Dispositifs NSX Edge » de l'interface utilisateur.

Lorsque cette partie de l'interface utilisateur est sélectionnée, la vue suivante s'affiche.



Tous les DLR et les passerelles ESG actuellement déployés sont affichés, avec les informations suivantes :

- « ID » indique l'ID de dispositif Edge de la passerelle ESG ou du DLR, qui peut être utilisé pour des appels API faisant référence à cette passerelle ESG ou à ce DLR
- « Locataire » + « ID » forment le nom de l'instance du DLR. Ce nom est visible et utilisé dans l'interface de ligne de commande de NSX.
- « Taille » est toujours définie sur « Compacte » pour le DLR, et la taille qui était sélectionnée par l'opérateur pour la passerelle ESG.

En plus des informations dans le tableau, il existe un menu contextuel, accessible via des boutons ou via « Actions ».

Tableau 3-1. Menu contextuel de NSX Edge

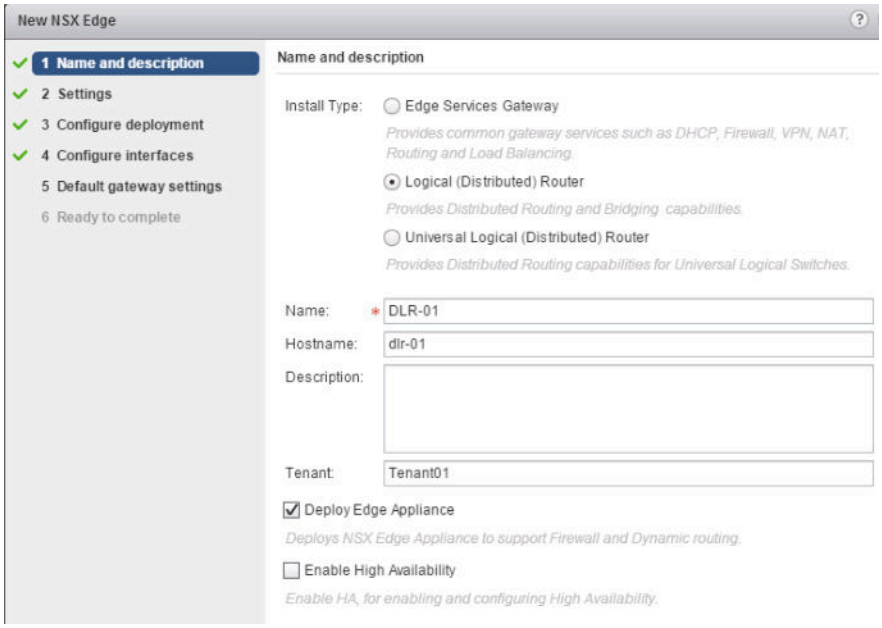
Icône	Action
	L'opération « Forcer la synchronisation » efface la configuration de la VM de contrôle de la passerelle ESG ou du DLR, la redémarre et transfère de nouveau la configuration.
	« Redéployer » détruit la passerelle ESG ou le DLR et en crée une ou un nouveau avec la même configuration. L'ID existant est conservé.
	« Modifier la configuration de la règle automatique » s'applique aux règles du pare-feu intégré de la passerelle ESG, créées lorsque des services sont activés sur la passerelle ESG (par exemple, BGP qui nécessite TCP/179).
	« Télécharger les journaux de support technique » crée un bundle de journaux à partir de la passerelle ESG ou de la VM de contrôle du DLR Pour le DLR, les journaux hôtes ne sont pas inclus dans le bundle de support technique et ils doivent être collectés séparément.
	« Modifier la taille du dispositif » ne s'applique qu'à des passerelles ESG. Cela effectuera un redéploiement avec un nouveau dispositif (les adresses MAC de vNIC changeront).
	« Modifier les informations d'identification CLI » permet à l'opérateur de forcer la mise à jour des informations d'identification CLI. Si la CLI est verrouillée sur une passerelle ESG ou une VM de contrôle du DLR après 5 échecs de connexion, cela ne lèvera pas le verrouillage. Vous devrez attendre 5 minutes ou « Redéployer » votre passerelle ESG/DLR pour vous reconnecter avec les bonnes informations d'identification.
	« Modifier le niveau de journal » change le niveau de détails à envoyer à syslog de la passerelle ESG/du DLR.
	« Configurer le débogage avancé » redéploie la passerelle ESG ou le DLR avec le vidage de mémoire activé et un disque virtuel supplémentaire attaché pour le stockage des fichiers de vidage de mémoire.

Tableau 3-1. Menu contextuel de NSX Edge (suite)

Icône	Action
	« Déployer » devient disponible lorsqu'une passerelle ESG a été créée sans être déployée. Cette option exécute simplement les étapes de déploiement (déploie OVF, configure des interfaces, transfère la configuration au dispositif créé).
	Si la version du DLR/de la passerelle ESG est antérieure à celle de NSX Manager, l'option « Mettre à niveau la version » devient disponible.
	« Filtre » permet de rechercher des passerelles ESG/des DLR par « Nom ».

Nouveau dispositif NSX Edge (DLR)

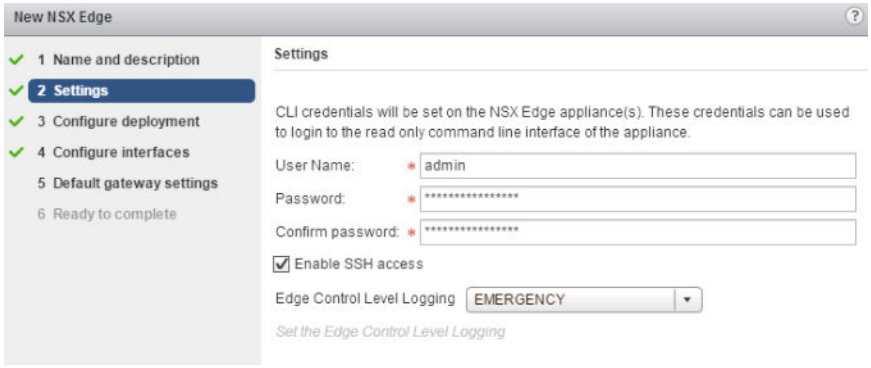
Lorsqu'un opérateur crée un DLR, l'assistant suivant est utilisé pour collecter les informations nécessaires.



Sur l'écran « Nom et description », les informations suivantes sont collectées :

- « Nom » s'affiche dans l'interface utilisateur « Dispositifs NSX Edge ».
- « Nom d'hôte » sera utilisé pour définir le nom DNS de la passerelle ESG ou de la VM de contrôle du DLR, visible sur la session SSH/console, dans les messages syslog et sur la page « Résumé » de vCenter pour la passerelle ESG/VM du DLR sous « Nom DNS ».
- « Description » se trouve dans l'interface utilisateur indiquant la liste de dispositifs NSX Edge.
- « Locataire » sera utilisé pour former le nom de l'instance du DLR, utilisé par l'interface de ligne de commande de NSX. Il peut également être utilisé par une plateforme de gestion de Cloud externe.

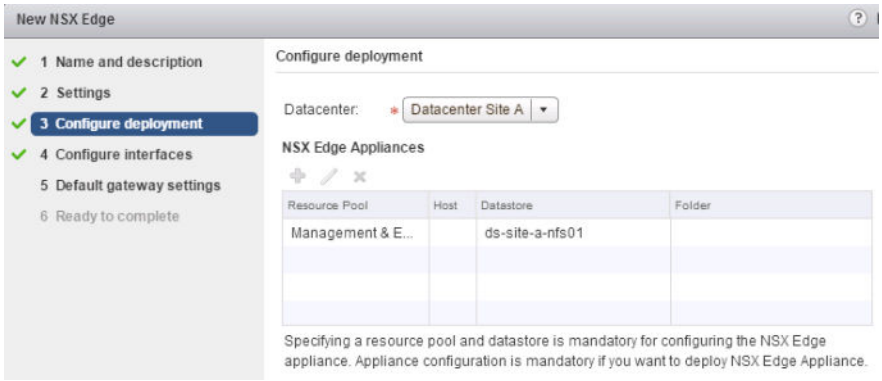
Sur l'écran « Paramètres » :



- « Nom d'utilisateur » et « Mot de passe » définissent les informations d'identification de console de l'interface de ligne de commande/VM pour accéder à la VM de contrôle du DLR. NSX ne prend pas en charge AAA sur la passerelle ESG ou les VM de contrôle du DLR. Ce compte dispose des droits complets vers la passerelle ESG/les VM de contrôle du DLR ; toutefois, la configuration de la passerelle ESG/du DLR ne peut pas être modifiée via la console de l'interface de ligne de commande/VM.
- « Activer l'accès SSH » permet au démon SSH sur la VM de contrôle du DLR de démarrer.
  - Les règles de pare-feu de la VM de contrôle doivent être ajustés pour autoriser l'accès réseau SSH.
  - L'opérateur peut se connecter à la VM de contrôle du DLR depuis un hôte sur le sous-réseau de l'interface de gestion de la VM de contrôle ou sur « Adresse de protocole » OSPF/BGP, si une adresse de protocole est configurée.

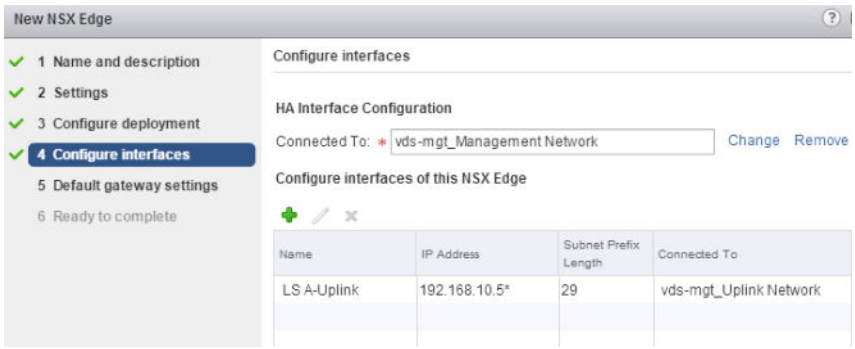
    Note Il n'est pas possible d'avoir une connectivité réseau entre la VM de contrôle du DLR et une adresse IP qui fait partie d'un sous-réseau configuré sur l'une des interfaces « Interne » de ce DLR. Cela est dû au fait que l'interface de sortie de ces sous-réseaux sur la VM de contrôle du DLR pointe vers la pseudo-interface « VDR », qui n'est pas connectée au plan de données.
- « Activer HA » déploie la VM de contrôle en tant que paire HA Active/En veille.
- « Journalisation du niveau de contrôle Edge » définit le niveau de syslog sur le dispositif Edge.

Sur l'écran « Configurer le déploiement » :



- « Centre de données » sélectionne le centre de données vCenter dans lequel il faut déployer la VM de contrôle.
- « Dispositifs NSX Edge Appliance » fait référence à la VM de contrôle du DLR et permet d'en définir exactement une (comme indiqué).
  - Si « HA » est activé, le dispositif Edge en veille sera déployé sur les mêmes cluster, hôte et banque de données. Une règle « Machines virtuelles séparées » de DRS sera créée pour les VM de contrôle du DLR Active et En veille.

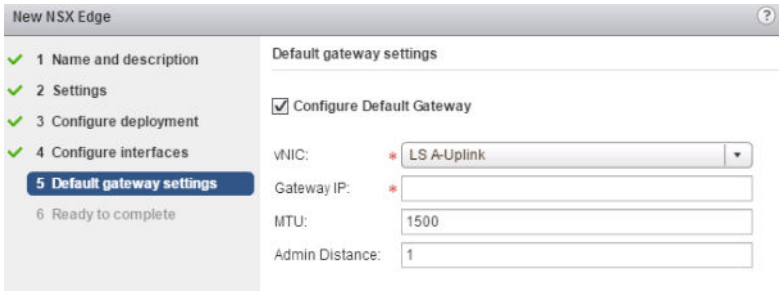
Sur l'écran « Configurer les interfaces » :



- « Interface HA »
  - N'est pas créée en tant qu'interface logique du DLR capable de router. Il ne s'agit que d'une vNIC sur la VM de contrôle.
  - Cette interface ne requiert pas d'adresse IP, car NSX gère la configuration du DLR via VMCI.
  - Cette interface est utilisée pour la pulsation HA si l'option « Activer High Availability » du DLR est cochée sur l'écran « Nom et description ».
- « Interfaces de ce dispositif NSX Edge » fait référence aux interfaces logiques (LIF) du DLR
  - Le DLR fournit des services de passerelle L3 aux VM sur le dvPortgroup ou le commutateur logique « Connecté à » avec des adresses IP provenant des sous-réseaux correspondants.
  - Des LIF de type « Liaison montante » sont créées en tant que vNIC sur la VM de contrôle. Ainsi, jusqu'à huit LIF sont prises en charge. Les deux dernières vNIC disponibles sont allouées à l'interface HA et une vNIC réservée.

- Une LIF de type « Liaison montante » est requise pour que le routage dynamique fonctionne sur le DLR.
- Des LIF de type « Interne » sont créées en tant que pseudo-vNIC sur la VM de contrôle, et il est possible d'en avoir au maximum 991.

Sur l'écran « Paramètres de la passerelle par défaut » :



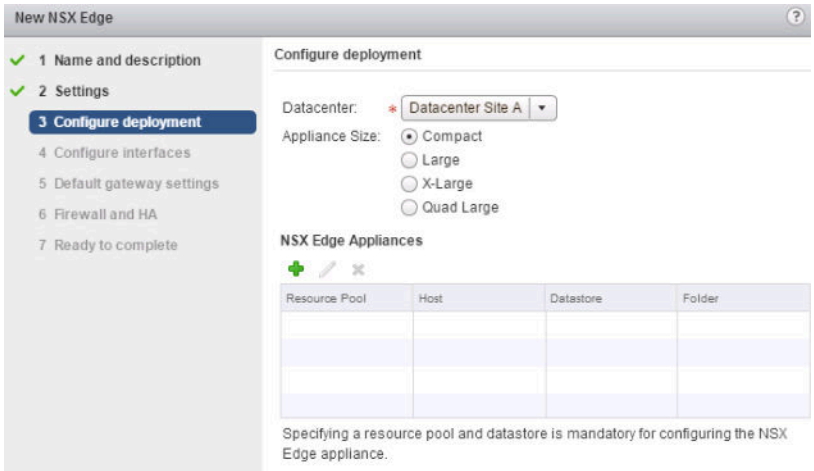
- L'option « Configurer la passerelle par défaut », si elle est sélectionnée, créera un itinéraire par défaut statique sur le DLR. Cette option est disponible si une LIF de type « Liaison montante » est créée sur l'écran précédent.
- Si ECMP est utilisé sur la liaison montante, il est recommandé de laisser cette option désactivée pour empêcher une interruption du plan de données en cas d'échec du tronçon suivant.

Note La double flèche vers la droite en haut à droite permet de « suspendre » l'assistant en cours afin de le reprendre ultérieurement.

Différences entre une passerelle ESG et un DLR

Il existe des différences entre les écrans de l'assistant lorsqu'une passerelle ESG est déployée par rapport à un DLR.

La première différence se trouve sur l'écran « Configurer le déploiement » :



Pour une passerelle ESG, « Configurer le déploiement » permet de sélectionner la taille du dispositif Edge. Si une passerelle ESG est utilisée uniquement pour le routage, « Grande » est une taille par défaut adaptée à plupart des scénarios. La sélection d'une taille plus grande ne fournira pas plus de ressources de CPU aux processus de routage de la passerelle ESG et ne se traduira pas par un débit plus important.

Il est également possible de créer d'une passerelle ESG sans la déployer, ce qui requiert toujours la configuration d'un dispositif Edge.

Un dispositif « Non déployé » peut être déployé ultérieurement via un appel API ou avec l'action d'interface utilisateur « Déployer ».

Si Edge HA est sélectionné, vous devez créer au moins une interface « Interne » ou bien HA échouera en silence, ce qui entraîne le scénario « split-brain ».

L'interface utilisateur de NSX et l'API permettent à un opérateur de supprimer la dernière interface « Interne », ce qui entraîne l'échec en silence de HA.

Opérations d'interface utilisateur classiques de la passerelle ESG et du DLR

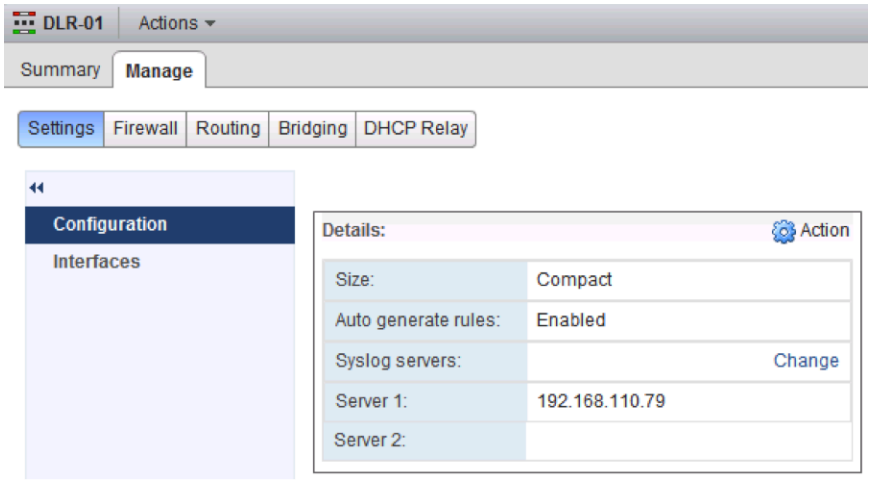
En plus de la création, plusieurs opérations de configuration sont généralement exécutées après le déploiement initial.

Il s'agit des opérations suivantes :

- Configuration Syslog
- Gestion d'itinéraires statiques
- Configuration de protocoles de routage et redistribution d'itinéraire

Configuration Syslog

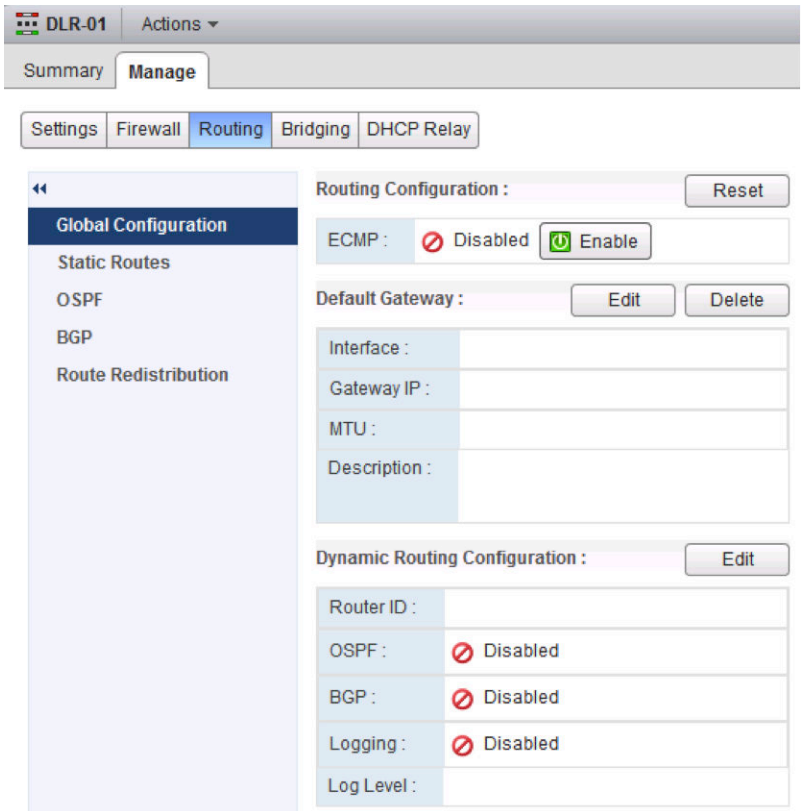
Configurez la passerelle ESG ou la VM de contrôle du DLR pour envoyer des entrées de journal à un serveur Syslog distant.



Remarques :

- Le serveur Syslog doit être configuré en tant qu'adresse IP, car la passerelle ESG/VM de contrôle du DLR n'est pas configurée avec un résolveur DNS.
  - Dans le cas de la passerelle ESG, il est possible d'« Activer le service DNS » (proxy DNS) que la passerelle ESG elle-même pourra utiliser pour résoudre des noms DNS, mais en général en spécifiant un serveur Syslog en tant qu'adresse IP dans une méthode plus fiable avec moins de dépendances.
- Il n'est pas possible de spécifier un port Syslog dans l'interface utilisateur (c'est toujours le port 514), mais le protocole (UDP/TCP) peut être spécifié.
- Des messages Syslog proviennent de l'adresse IP de l'interface d'Edge qui est sélectionnée comme sortie pour l'adresse IP du serveur Syslog par la table de transfert d'Edge.
  - Pour le DLR, l'adresse IP du serveur Syslog ne peut pas se trouver sur des sous-réseaux configurés sur l'une des interfaces « Interne » du DLR. Cela est dû au fait que l'interface de sortie de ces sous-réseaux sur la VM de contrôle du DLR pointe vers la pseudo-interface « VDR », qui n'est pas connectée au plan de données.

Par défaut, la journalisation pour le moteur de routage de la passerelle ESG/du DLR est désactivée. Si nécessaire, activez-la via l'interface utilisateur en cliquant sur « Modifier » pour la « Configuration du routage dynamique ».

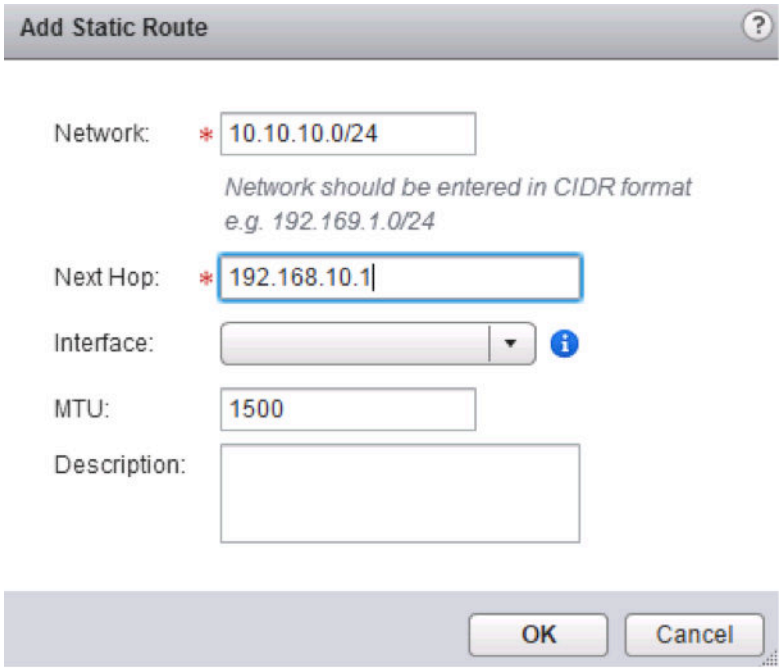


Vous devez également configurer l'ID de routeur, qui sera en général l'adresse IP de l'interface de liaison montante.

Itinéraires statiques

Le tronçon suivant des itinéraires statiques doit être défini sur une adresse IP sur un sous-réseau associé à l'une des LIF du DLR ou à des interfaces de la passerelle ESG. Sinon, la configuration échoue.

« Interface », si non sélectionné, est défini automatiquement en associant le tronçon suivant à l'un des sous-réseaux connectés directement.

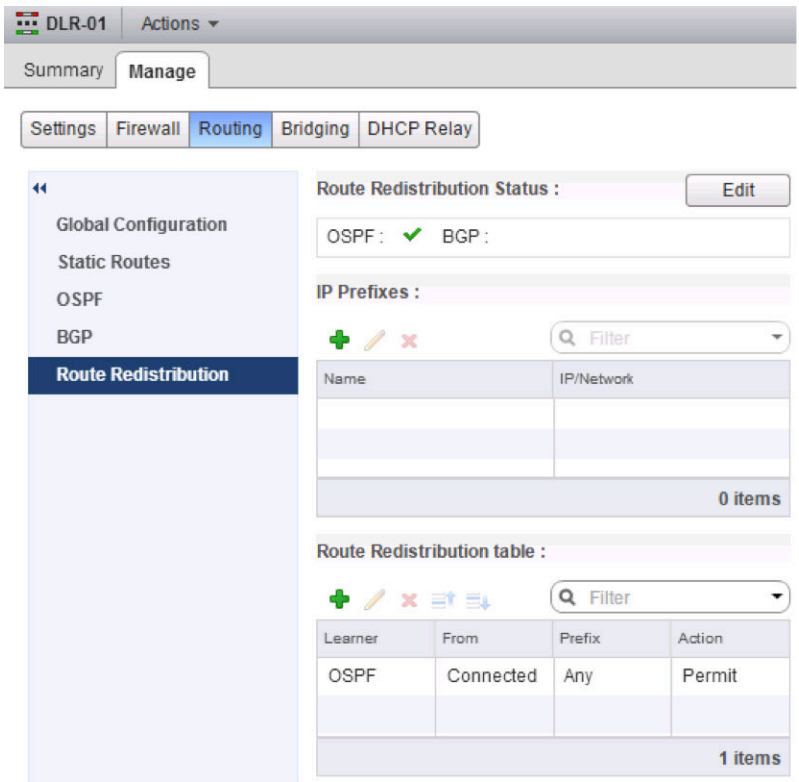


Redistribution d'itinéraire

L'ajout d'une entrée dans le « tableau Redistribution d'itinéraire » n'active pas automatiquement la redistribution pour le « Protocole de l'apprenant » sélectionné. Cela doit être effectué explicitement via « Modifier » pour « État de la redistribution d'itinéraire ».

Le DLR est configuré avec la redistribution d'itinéraires connectés dans OSPF par défaut, mais pas la passerelle ESG.

Le « tableau Redistribution d'itinéraire » est traité de haut en bas. Le traitement est arrêté après la première correspondance. Pour exclure certains préfixes de la redistribution, incluez des entrées plus spécifiques en haut.



Dépannage du routage NSX

NSX fournit plusieurs outils pour s'assurer que le routage fonctionne.

Interface de ligne de commande du routage NSX

Un ensemble de commandes CLI permettent à un opérateur d'examiner l'état d'exécution de diverses parties du sous-système de routage NSX.

En raison de la nature distribuée du sous-système de routage NSX, plusieurs interfaces de ligne de commande (CLI) sont disponibles, accessibles sur divers composants de NSX. À partir de NSX version 6.2, NSX contient également une CLI centralisée qui permet de réduire le « temps de trajet » nécessaire pour accéder et se connecter à divers composants distribués. Il fournit un accès à la plupart des informations depuis un emplacement unique : le shell de NSX Manager.

Vérification des conditions requises préalables

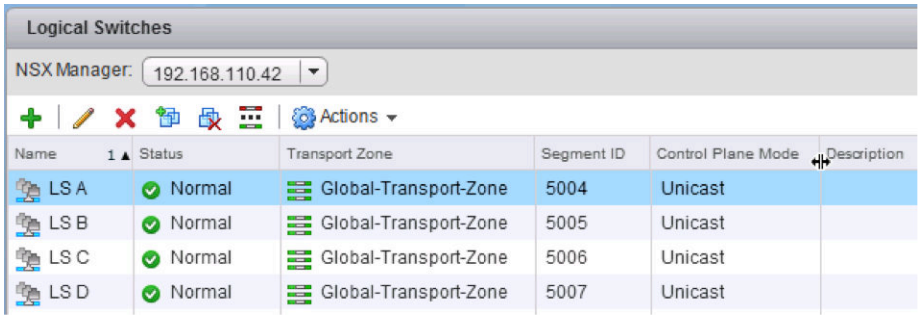
Deux conditions requises préalables majeures doivent être satisfaites pour chaque hôte ESXi :

- Les commutateurs logiques connectés au DLR sont sains.
- L'hôte ESXi a été correctement préparé pour VXLAN.

Vérification de l'intégrité du commutateur logique

Le routage NSX fonctionne avec la commutation logique NSX. Pour vérifier que les commutateurs logiques connectés à un DLR sont sains :

- Recherchez l'ID de segment (VXLAN VNI) pour chaque commutateur logique connecté au DLR en question (par exemple, 5004..5007).



- Sur les hôtes ESXi sur lesquels les VM desservies par ce DLR sont exécutées, vérifiez l'état du plan de contrôle VXLAN pour les commutateurs logiques connectés à ce DLR.

```
# esxcli network vswitch dvs vmware vxlan network list --vds-name=Compute_VDS
VXLAN ID  Multicast IP               Control Plane                       Controller Connection  Port
Count  MAC Entry Count  ARP Entry Count
--------  ------------------------  ----------------------------------  ---------------------
----------  ----------------  ----------------
    5004  N/A (headend replication)  Enabled (multicast proxy,ARP proxy)  192.168.110.201
(up)            2                 2                 0
    5005  N/A (headend replication)  Enabled (multicast proxy,ARP proxy)  192.168.110.202
(up)            1                 0                 0
    5006  N/A (headend replication)  Enabled (multicast proxy,ARP proxy)  192.168.110.203
(up)            1                 1                 0
    5007  N/A (headend replication)  Enabled (multicast proxy,ARP proxy)  192.168.110.202
(up)            1                 0                 0
```

Vérifiez les points suivants pour chaque VXLAN pertinent :

- Pour les commutateurs logiques en mode hybride ou monodiffusion :
  - Le plan de contrôle présente l'état « Enabled » (Activé).
  - « multicast proxy » (Proxy multidiffusion) et « ARP proxy » (Proxy ARP) sont répertoriés ; « ARP proxy » sera répertorié même si vous avez désactivé la découverte d'adresses IP.
  - Une adresse IP de contrôleur valide est répertoriée sous « Controller » (Contrôleur) et « Connection » (Connexion) est « up » (Active).
- « Port Count » (Nombre de ports) semble correct : il y en aura au moins 1, même s'il n'y a aucune VM sur cet hôte connecté au commutateur logique en question. Ce port est le vdrPort, qui est un dvPort spécial connecté au module de noyau du DLR sur l'hôte ESXi.

- Exécutez la commande suivante pour vous assurer que le vdrPort est connecté à chacun des VXLAN applicables.

```
~ # esxcli network vswitch dvs vmware vxlan network port list --vds-name=Compute_VDS --vxlan-id=5004
Switch Port ID  VDS Port ID  VMKNIC ID
--------------  ----------  ---------
      50331656  53                   0
      50331650  vdrPort              0


~ # esxcli network vswitch dvs vmware vxlan network port list --vds-name=Compute_VDS --vxlan-id=5005
Switch Port ID  VDS Port ID  VMKNIC ID
--------------  ----------  ---------
      50331650  vdrPort              0
```

- Dans l'exemple ci-dessous, VXLAN 5004 contient une VM et une connexion de DLR, alors que VXLAN 5005 ne dispose que d'une connexion de DLR.
- Vérifiez que les VM appropriées ont été câblées à leurs VXLAN correspondants, par exemple web-sv-01a sur VXLAN 5004.

```
~ # esxcfg-vswitch -l
DVS Name         Num Ports   Used Ports  Configured Ports  MTU     Uplinks
Compute_VDS      1536        10          512               1600    vmnic0

  DVPort ID           In Use      Client
[..skipped..]
  53                  1           web-sv-01a.eth0
```

Vérification de la préparation de VXLAN

Dans le cadre de la configuration de VXLAN d'un hôte ESXi, le module de noyau du DLR est également installé, configuré et connecté à un dvPort sur un DVS préparé pour VXLAN.

1 Exécutez `show cluster all` pour obtenir l'ID du cluster.

2 Exécutez `show cluster cluster-id` pour obtenir l'ID de l'hôte.

3 Exécutez `show logical-router host hostID connection` pour obtenir les informations sur l'état.

```
nsxmgr-01a# show logical-router host <hostID> connection

Connection Information:
-----------------------

DvsName           VdrPort           NumLifs  VdrVmac
--------          --------          --------  --------
Compute_VDS       vdrPort           4        02:50:56:56:44:52
    Teaming Policy: Default Teaming
    Uplink   : dvUplink1(50331650): 00:50:56:eb:41:d7(Team member)
```

```
    Stats : Pkt Dropped      Pkt Replaced     Pkt Skipped
    Input : 0                0                1968734458
   Output : 303              7799             31891126
```

- Un DVS activé avec VXLAN disposera d'un vdrPort créé, partagé par toutes les instances du DLR sur cet hôte ESXi.
- « NumLifs » fait référence à la somme de LIF de toutes les instances du DLR qui existent sur cet hôte.
- « VdrVmac » est la vMAC que le DLR utilise sur toutes les LIF sur toutes les instances. Cette adresse MAC est la même sur tous les hôtes. Elle n'est jamais vue dans les trames qui se déplacent dans le réseau physique en dehors des hôtes ESXi.
- Pour chaque dvUplink de DVS activé avec VXLAN, il existe un VTEP correspondant ; sauf dans les situations où le mode d'association LACP/Etherchannel est utilisé, lorsqu'un seul VTEP est créé indépendamment du nombre de dvUplink.
  - Le trafic routé par le DLR (MAC SRC = vMAC) lorsque l'on quitte l'hôte verra l'adresse MAC SRC passée sur pMAC d'un dvUplink correspondant.
  - Notez que le port source ou l'adresse MAC source de la VM d'origine est utilisé pour déterminer le dvUplink (il est conservé pour chaque paquet dans les métadonnées de son DVS).
  - Lorsque plusieurs VTEP se trouvent sur l'hôte et que l'un des dvUplink échoue, le VTEP associé au dvUplink échoué sera déplacé sur l'un des dvUplink restants, avec toutes les autres VM qui sont épinglées à ce VTEP. Cela est effectué pour éviter une saturation des changements de plan de contrôle qui seraient associés au déplacement des VM sur un VTEP différent.
- Le nombre entre « () » à côté de chaque « dvUplinkX » est le numéro de dvPort. Il est utile pour la capture de paquets sur la liaison montante individuelle.
- L'adresse MAC affichée pour chaque « dvUplinkX » est une adresse « pMAC » associée à ce dvUplink. Cette adresse MAC est utilisée pour le trafic provenant du DLR, tel que des requêtes ARP générées par le DLR et des paquets qui ont été dirigés par le DLR lorsque ces paquets quittent l'hôte ESXi. Cette adresse MAC est visible sur le réseau physique (directement, si la LIF du DLR est du type VLAN, ou dans des paquets VXLAN pour les LIF VXLAN).
- Paquet abandonné/Remplacé/Ignoré font référence à des compteurs liés à des détails d'implémentation internes du DLR. En général, ils ne sont pas utilisés pour le dépannage ou la surveillance.

Bref récapitulatif du routage

Pour résoudre efficacement les problèmes de routage, il est préférable de revoir le fonctionnement du routage et les tableaux d'informations liés.

1 Recevez un paquet à envoyer à une adresse IP de destination.

2 Consultez la table de routage et déterminez l'adresse IP du tronçon suivant.

3 Déterminez laquelle de vos interfaces réseau peut l'atteindre.

4 Obtenez une adresse MAC de ce tronçon suivant (via ARP).

5 Créez une trame L2.

6 Envoyez la trame en dehors de l'interface.

Pour procéder au routage, vous devez posséder :

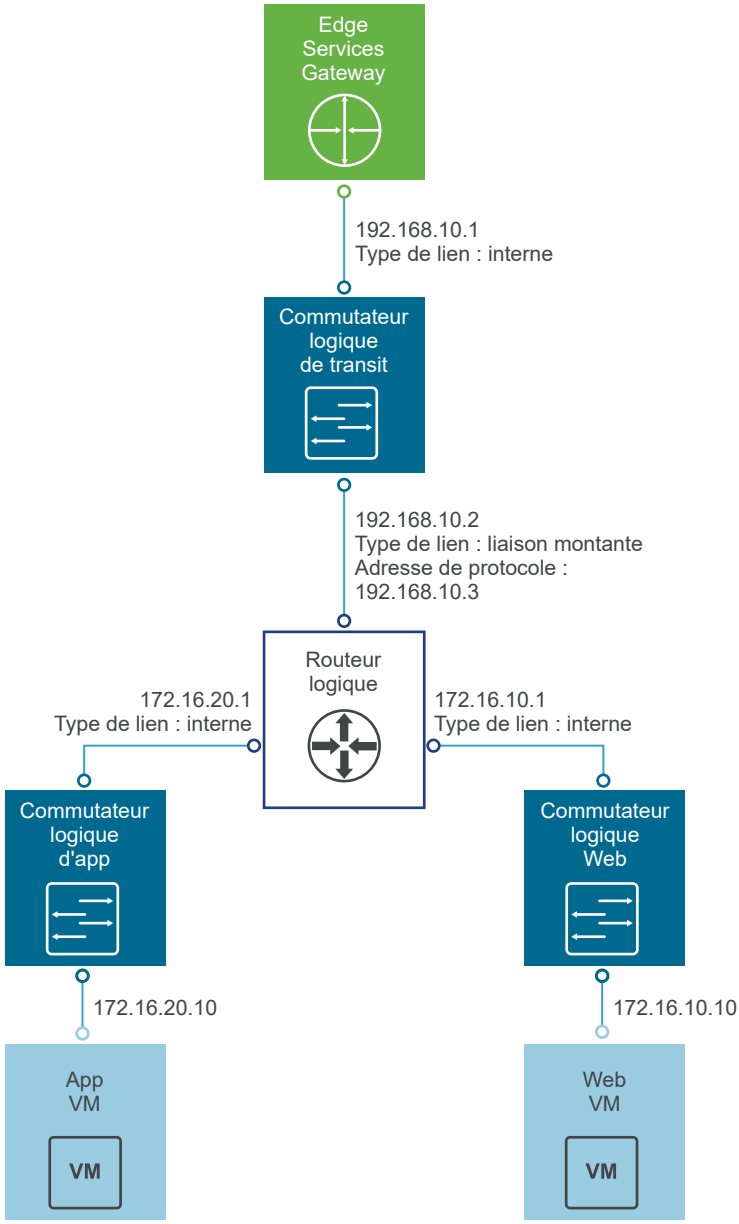
- Une table d'interface (avec les adresses IP et les masques de réseau de l'interface)
- Une table de routage
- Une table ARP

Vérification de l'état du DLR à l'aide d'un exemple de topologie routée

Cette section explique comment vérifier les informations dont le DLR a besoin pour acheminer des paquets.

Prenons un exemple de topologie routée et créons un ensemble de commutateurs logiques et un DLR pour le créer dans NSX.

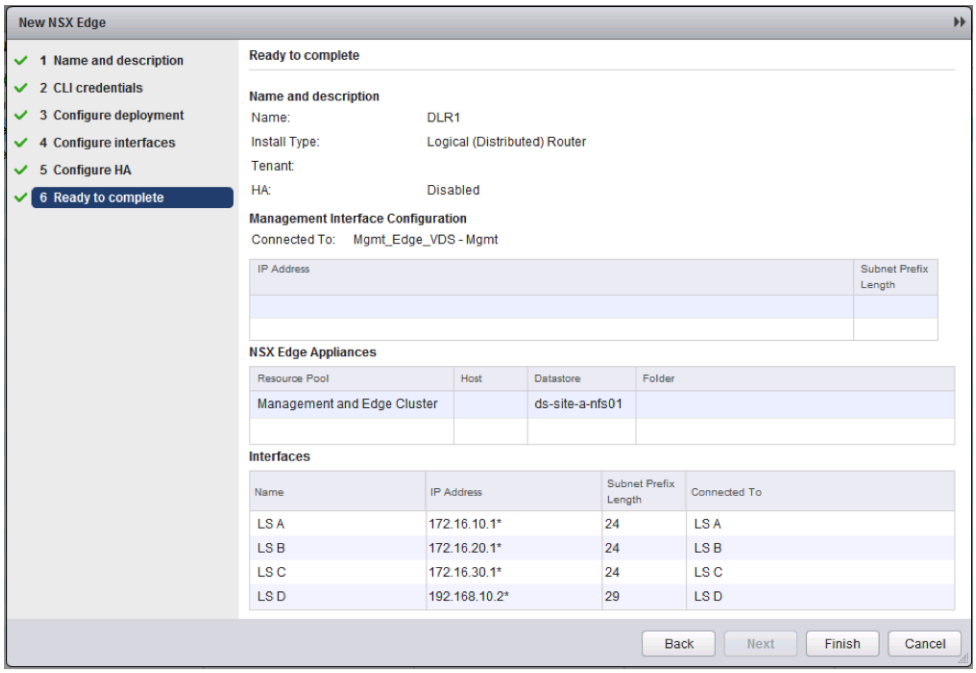
Figure 3-7. Exemple de topologie routée



Le schéma indique :

- 4 x commutateurs logiques, chacun avec son propre sous-réseau
- 3 x VM, connectée par commutateur logique
  - Chacune avec ses propres adresse IP et passerelle IP
  - Chacune avec une adresse MAC (les deux derniers octets sont indiqués)
- Un DLR connecté aux 4 commutateurs logiques ; un commutateur logique est pour la « Liaison montante », le reste est « Interne »
- Une passerelle externe, pouvant être une passerelle ESG, servant de passerelle en amont pour le DLR.

L'écran de l'assistant « Prêt à terminer » apparaît pour le DLR ci-dessus.



Une fois le déploiement du DLR terminé, les commandes de l'interface de ligne de commande d'ESXi peuvent être utilisées pour afficher et valider l'état distribué du DLR en question sur les hôtes participant.

Confirmation des instances du DLR

Vous devez commencer par vérifier si l'instance du DLR a été créée et si son plan de contrôle est actif.

1 À partir du shell de NSX Manager, exécutez `show cluster all` pour obtenir l'ID du cluster.

2 Exécutez `show cluster cluster-id` pour obtenir l'ID de l'hôte.

3 Exécutez `show logical-router host hostID dlr all verbose` pour obtenir les informations sur l'état.

```
nsxmgr# show logical-router host host-id dlr all verbose

VDR Instance Information :
--------------------------

Vdr Name:                   default+edge-1
Vdr Id:                     1460487509
Number of Lifs:             4
Number of Routes:           5
State:                      Enabled
Controller IP:              192.168.110.201
Control Plane Active:       Yes
Control Plane IP:           192.168.210.51
Edge Active:                No
```

Points à noter :

- Cette commande affiche toutes les instances du DLR qui existent sur l'hôte ESXi donné.
- « Vdr Name » (Nom VDR) se compose de « Tenant » (Locataire) et de « Edge Id » (ID de dispositif Edge). Dans l'exemple, « Tenant » (Locataire) n'a pas été spécifié, donc le mot « default » (par défaut) est utilisé. « Edge Id » (ID de dispositif Edge) est « edge-1 », que l'on peut voir dans l'interface utilisateur de NSX.
  - Dans les cas où il existe de nombreuses instances du DLR sur un hôte, une méthode pour trouver la bonne instance consiste à rechercher « Edge ID » affiché dans l'interface utilisateur « NSX Edges » (Dispositifs NSX Edge).
- « Vdr Id » (ID VDR) est utile pour les recherches avancées, notamment dans les journaux.
- « Number of Lifs » (Nombre de LIF) fait référence aux LIF qui existent sur cette instance individuelle du DLR.
- « Number of Routes » (Nombre d'itinéraires) est dans ce cas égal à 5, ce qui représente 4 itinéraires connectés directement (un pour chaque LIF) et un itinéraire par défaut.
- « State » (État), « Controller IP » (Adresse IP du contrôleur) et « Control Plane Active » (Plan de contrôle actif) font référence à l'état du plan de contrôle du DLR. Ils doivent indiquer la bonne adresse IP du contrôleur et « Control Plane Active » (Plan de contrôle actif) doit être égal à « Yes » (Oui). Rappelez-vous que la fonction DLR requiert des contrôleurs qui fonctionnent ; la sortie ci-dessus indique le résultat attendu pour une instance saine du DLR.
- « Control Plane IP » (Adresse IP du plan de contrôle) fait référence à l'adresse IP que l'hôte ESXi utilise pour parler au contrôleur. Cette adresse IP est toujours celle associée au vmknic de gestion de l'hôte ESXi, qui est dans la plupart des cas vmk0.
- « Edge Active » (Dispositif Edge actif) indique si cet hôte est celui sur lequel la VM de contrôle de cette instance du DLR est exécutée et dans un état actif.
  - Le placement de la VM de contrôle active du DLR détermine quel hôte ESXi est utilisé pour exécuter le pontage L2 de NSX, s'il est activé.
- Il existe également une version abrégée de la commande ci-dessus qui produit une sortie comprimée utile pour une présentation rapide. Notez que « Vdr Id » (ID VDR) est affiché au format hexadécimal ici :

```
nsxmgr# show logical-router host host-id dlr all brief

VDR Instance Information :
---------------------------

State Legend: [A: Active], [D: Deleting], [X: Deleted], [I: Init]
State Legend: [SF-R: Soft Flush Route], [SF-L: Soft Flush LIF]

Vdr Name            Vdr Id     #Lifs   #Routes State      Controller Ip    CP Ip
--------            -------    -----   ------- -----      -------------    ------
default+edge-1      0x570d4555 4       5       A          192.168.110.201  192.168.210.51
```

Les états « Soft Flush » (Vidage doux) font référence à des états transitoires de courte durée du cycle de vie de LIF. On ne les voit normalement pas dans un DLR sain.

Interfaces logiques du DLR

Après avoir vérifié que le DLR est créé, assurez-vous que toutes les interfaces logiques du DLR sont présentes et qu'elles sont bien configurées.

1 À partir du shell de NSX Manager, exécutez `show cluster all` pour obtenir l'ID du cluster.

2 Exécutez `show cluster cluster-id` pour obtenir l'ID de l'hôte.

3 Exécutez `show logical-router host hostID dlr all brief` pour obtenir dlrID (Nom VDR).

4 Exécutez `show logical-router host hostID dlr dlrID interface all brief` pour obtenir un résumé des informations d'état de toutes les interfaces.

5 Exécutez `show logical-router host hostID dlr dlrID interface (all | intName) verbose` pour obtenir les informations d'état de toutes les interfaces ou d'une interface spécifique.

```
nsxmgr# show logical-router host hostID dlr dlrID interface all verbose

VDR default+edge-1:1460487509 LIF Information :

Name:                570d45550000000a
Mode:                Routing, Distributed, Internal
Id:                  Vxlan:5000
Ip(Mask):            172.16.10.1(255.255.255.0)
Connected Dvs:       Compute_VDS
VXLAN Control Plane: Enabled
VXLAN Multicast IP:  0.0.0.1
State:               Enabled
Flags:               0x2388
DHCP Relay:          Not enabled

Name:                570d45550000000c
Mode:                Routing, Distributed, Internal
Id:                  Vxlan:5002
Ip(Mask):            172.16.30.1(255.255.255.0)
Connected Dvs:       Compute_VDS
VXLAN Control Plane: Enabled
VXLAN Multicast IP:  0.0.0.1
State:               Enabled
Flags:               0x2288
DHCP Relay:          Not enabled

Name:                570d45550000000b
Mode:                Routing, Distributed, Internal
Id:                  Vxlan:5001
Ip(Mask):            172.16.20.1(255.255.255.0)
Connected Dvs:       Compute_VDS
VXLAN Control Plane: Enabled
VXLAN Multicast IP:  0.0.0.1
State:               Enabled
```

```
Flags:               0x2388
DHCP Relay:          Not enabled

Name:                570d455500000002
Mode:                Routing, Distributed, Uplink
Id:                  Vxlan:5003
Ip(Mask):            192.168.10.2(255.255.255.248)
Connected Dvs:       Compute_VDS
VXLAN Control Plane: Enabled
VXLAN Multicast IP:  0.0.0.1
State:               Enabled
Flags:               0x2208
DHCP Relay:          Not enabled
```

Points à noter :

- Le nom (« Name ») de la LIF est unique sur toutes les instances du DLR sur l'hôte. C'est le même sur les hôtes et sur le nœud de contrôleur maître du DLR.
- Le « Mode » de la LIF indique si la LIF route ou ponte, et si elle est interne ou de liaison montante.
- « Id » indique le type de LIF et l'ID de service correspondant (VXLAN et VNI, ou VLAN et VID).
- « Ip(Mask) » (IP (Masque)) est indiqué pour les LIF « Routing » (Routage).
- Si une LIF est connectée à un VXLAN en mode hybride ou monodiffusion, « VXLAN Control Plane » (Plan de contrôle VXLAN) est « Enabled » (Activé).
- Pour les LIF VXLAN où VXLAN est en mode monodiffusion, « VXLAN Multicast IP » (Adresse IP multidiffusion VXLAN) est indiqué sous la forme « 0.0.0.1 » ; sinon l'adresse IP monodiffusion réelle est affichée.
- « State » (État) doit être « Enabled » (Activé) pour les LIF routées. Pour les LIF de pontage, il est « Enabled » (Activé) sur l'hôte effectuant le pontage et « Init » sur tous les autres hôtes.
- « Flags » (Indicateurs) est une représentation résumée de l'état de la LIF et il indique :
  - Si la LIF est routée ou pontée
  - Si la LIF VLAN est une DI
  - Si le relais DHCP est activé sur la LIF
  - Particulièrement important, l'indicateur 0x0100 est défini lorsqu'une jonction de VNI VXLAN a été causée par le DLR (plutôt qu'un hôte disposant d'une VM sur ce VXLAN)
  - Les indicateurs sont affichés dans un format plus lisible en mode abrégé.

```
nsxmgr# show logical-router host hostID dlr dlrID interface all brief

VDR default+edge-1 LIF Information :

State Legend: [A:Active], [d:Deleting], [X:Deleted], [I:Init],[SF-L:Soft Flush LIF]
Modes Legend: [B:Bridging],[E: Empty], [R:Routing],[S:Sedimented],[D:Distributed]
Modes Legend: [In:Internal],[Up:Uplink]
```

```
Lif Name             Id              Mode     State    Ip(Mask)
--------             --              -----    -----    --------
570d45550000000a     Vxlan:5001      R,D,In   A        172.16.10.1(255.255.255.0)
570d45550000000c     Vxlan:5003      R,D,In   A        172.16.30.1(255.255.255.0)
570d45550000000b     Vxlan:5002      R,D,In   A        172.16.20.1(255.255.255.0)
570d455500000002     Vxlan:5000      R,D,Up   A        192.168.10.5(255.255.255.248)
```

Itinéraires du DLR

Une fois que vous avez vérifié qu'un DLR est présent et sain, et qu'il contient toutes les LIF, l'étape suivante consiste à vérifier la table de routage.

1 À partir du shell de NSX Manager, exécutez `show cluster all` pour obtenir l'ID du cluster.

2 Exécutez `show cluster cluster-id` pour obtenir l'ID de l'hôte.

3 Exécutez `show logical-router host hostID dlr all brief` pour obtenir dlrID (Nom VDR).

4 Exécutez `show logical-router host hostID dlr dlrID route` pour obtenir les informations d'état de toutes les interfaces.

```
nsxmgr# show logical-router host hostID dlr dlrID route

VDR default+edge-1:1460487509 Route Table
Legend: [U: Up], [G: Gateway], [C: Connected], [I: Interface]
Legend: [H: Host], [F: Soft Flush] [!: Reject] [E: ECMP]

Destination      GenMask          Gateway          Flags    Ref Origin   UpTime     Interface
-----------      -------          -------          -----    --- ------   ------     ---------
0.0.0.0          0.0.0.0          192.168.10.1     UG       1   AUTO     10068944   570d455500000002
172.16.10.0      255.255.255.0    0.0.0.0          UCI      1   MANUAL   10068944   570d45550000000a
172.16.20.0      255.255.255.0    0.0.0.0          UCI      1   MANUAL   10068944   570d45550000000b
172.16.30.0      255.255.255.0    0.0.0.0          UCI      1   MANUAL   10068944   570d45550000000c
192.168.10.0     255.255.255.248  0.0.0.0          UCI      1   MANUAL   10068944   570d455500000002
```

Points à noter :

- « Interface » indique la LIF de sortie qui sera sélectionnée pour la « Destination » correspondante. Elle est définie sur le nom de l'une des LIF du DLR (« Lif Name »).
- Pour les itinéraires ECMP, il y aura plusieurs itinéraires avec les mêmes Destination, GenMask et Interface, mais une passerelle différente. Les indicateurs incluront également « E » pour refléter la nature ECMP de ces itinéraires.

Table ARP du DLR

Pour les paquets qu'il transfère, le DLR doit être capable de résoudre les demandes d'ARP pour l'adresse IP du tronçon suivant. Les résultats de ce processus de résolution sont stockés localement sur les instances du DLR des hôtes individuels.

Les contrôleurs ne jouent aucun rôle dans ce processus, et ils ne sont pas utilisés pour distribuer les entrées ARP résultantes aux autres hôtes.

Les entrées en cache inactives sont conservées pendant 600 secondes, puis elles sont supprimées. Pour plus d'informations sur le processus de résolution ARP du DLR, reportez-vous à la section Processus de résolution d'ARP du DLR.

1 À partir du shell de NSX Manager, exécutez `show cluster all` pour obtenir l'ID du cluster.

2 Exécutez `show cluster cluster-id` pour obtenir l'ID de l'hôte.

3 Exécutez `show logical-router host hostID dlr all brief` pour obtenir dlrID (Nom VDR).

4 Exécutez `show logical-router host hostID dlr dlrID arp` pour obtenir les informations d'état de toutes les interfaces.

```
nsxmgr# show logical-router host hostID dlr dlrID arp

VDR default+edge-1:1460487509 ARP Information :
Legend: [S: Static], [V: Valid], [P: Proxy], [I: Interface]
Legend: [N: Nascent], [L: Local], [D: Deleted]

Network           Mac                Flags      Expiry     SrcPort    Interface Refcnt
-------           ---                -----      -------    ---------  --------- ------
172.16.10.1       02:50:56:56:44:52  VI         permanent  0          570d45550000000a 1
172.16.10.11      00:50:56:a6:7a:a2  VL         147        50331657   570d45550000000a 2
172.16.30.1       02:50:56:56:44:52  VI         permanent  0          570d45550000000c 1
172.16.30.11      00:50:56:a6:ba:09  V          583        50331650   570d45550000000c 2
172.16.20.11      00:50:56:a6:84:52  VL         568        50331658   570d45550000000b 2
172.16.20.1       02:50:56:56:44:52  VI         permanent  0          570d45550000000b 1
192.168.10.2      02:50:56:56:44:52  VI         permanent  0          570d455500000002 1
192.168.10.1      00:50:56:8e:ee:ce  V          147        50331650   570d455500000002 1
```

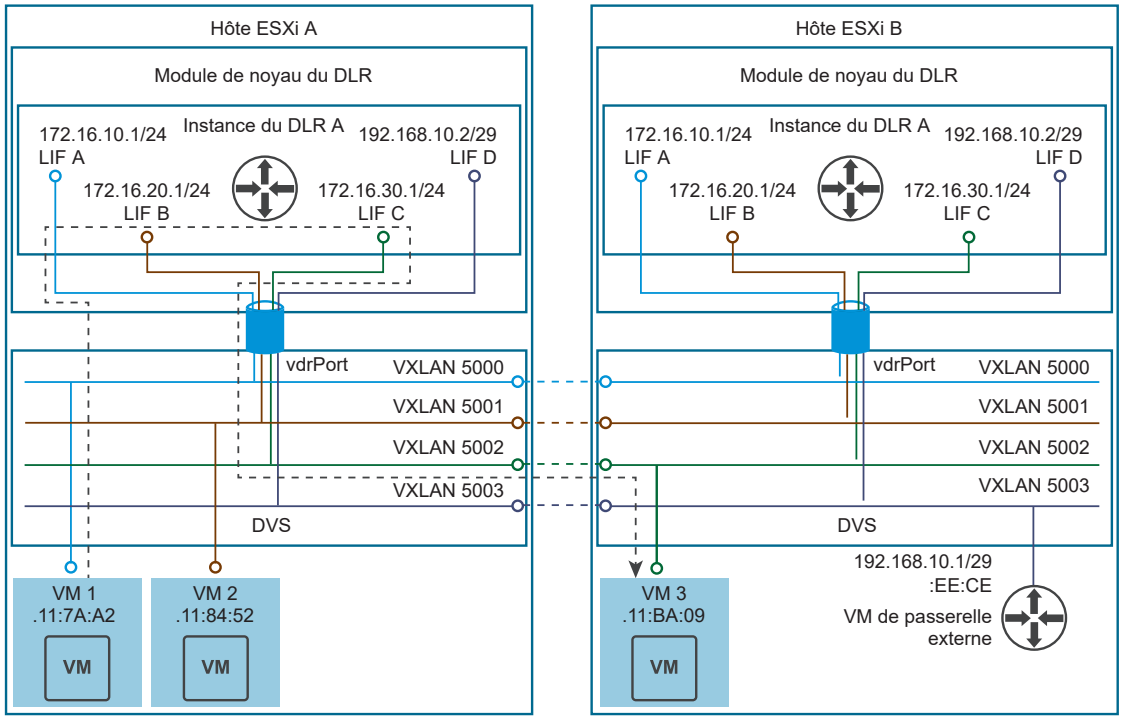
Points à noter :

- Toutes les entrées ARP des LIF du DLR (indicateur « I ») sont les mêmes et elles indiquent la même adresse vMAC que celle mentionnée dans la section Vérification de la préparation de VXLAN.
- Les entrées ARP avec l'indicateur « L » correspondent aux machines virtuelles exécutées sur l'hôte sur lequel la commande CLI est exécutée.
- « SrcPort » indique l'ID de dvPort d'où provient l'entrée ARP. Lorsqu'une entrée ARP provient d'un autre hôte, l'ID de dvPort du dvUplink est indiqué. Cet ID de dvPort peut être croisé avec l'ID de dvPort du dvUplink mentionné à la section Vérification de la préparation de VXLAN.
- Normalement, l'indicateur « Nascent » n'est pas observé. Il est défini lorsque le DLR attend que la réponse ARP arrive. Les entrées avec cet indicateur peuvent indiquer qu'il y a un problème avec la résolution ARP.

Représentation du DLR et de ses composants hôte liés

Le schéma suivant indique deux hôtes, Hôte ESXi A et Hôte ESXi B, où notre « Instance A du DLR » en exemple est configurée et connectée aux quatre LIF VXLAN.

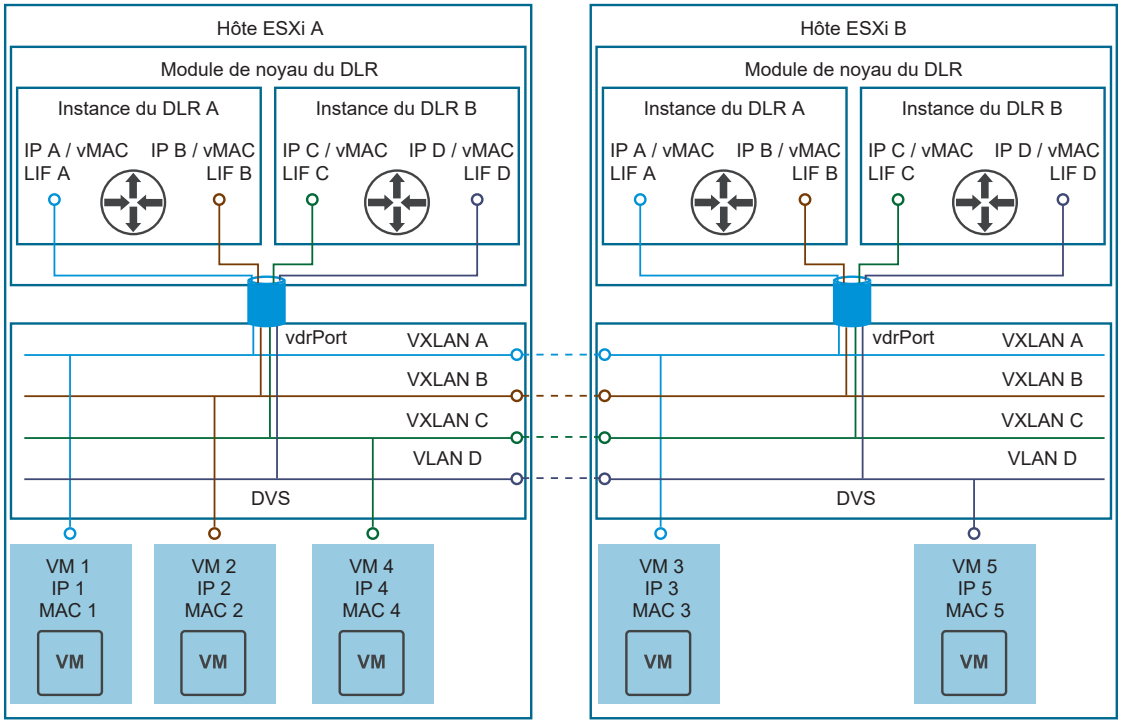
Figure 3-8. Deux hôtes avec une instance du DLR



- Chaque hôte possède un « Commutateur L2 » (DVS) et un « Routeur sur clé » (module de noyau du DLR), connecté à ce « commutateur » via une interface de « jonction » (vdrPort).
  - Notez que cette « jonction » peut transporter à la fois des VLAN et des VXLAN ; toutefois, aucun en-tête 801.Q ou UDP/VXLAN n'est présent dans les paquets qui traversent vdrPort. Au lieu de cela, le DVS utilise une méthode d'étiquetage de métadonnées interne pour communiquer ces informations au module de noyau du DLR.
- Lorsque le DVS voit une trame où l'adresse MAC de destination est vMAC, il sait qu'elle est destinée au DLR et il transfère cette trame à vdrPort.
- Une fois que les paquets arrivent dans le module de noyau du DLR via vdrPort, leurs métadonnées sont examinées pour déterminer le VNI VXLAN ou l'ID VLAN auquel ils appartiennent. Ces informations sont ensuite utilisées pour déterminer à quelle LIF de quelle instance du DLR ce paquet appartient.
  - Ce système présente néanmoins un inconvénient : il n'est pas possible de connecter plusieurs instances du DLR à un VLAN ou un VXLAN donné.

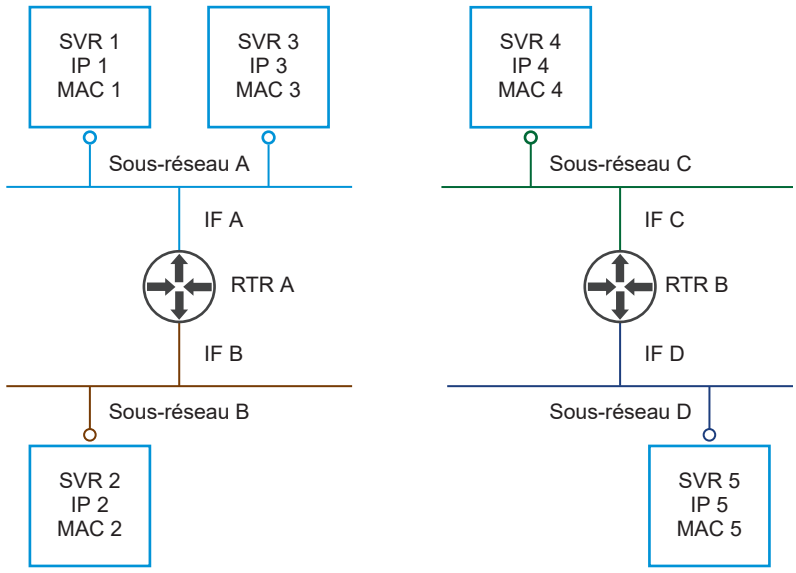
Dans les cas où plusieurs instances du DLR existent, le schéma ci-dessus serait le suivant :

Figure 3-9. Deux hôtes avec deux instances du DLR



Cela correspondrait à une topologie de réseau avec deux domaines de routage indépendants, fonctionnant séparément l'un de l'autre, potentiellement avec des adresses IP se chevauchant.

Figure 3-10. Topologie de réseau correspondant à deux hôtes et à deux instances du DLR



Architecture du sous-système de routage distribué

Des instances du DLR sur des hôtes ESXi ont accès à toutes les informations nécessaires pour exécuter le routage L3.

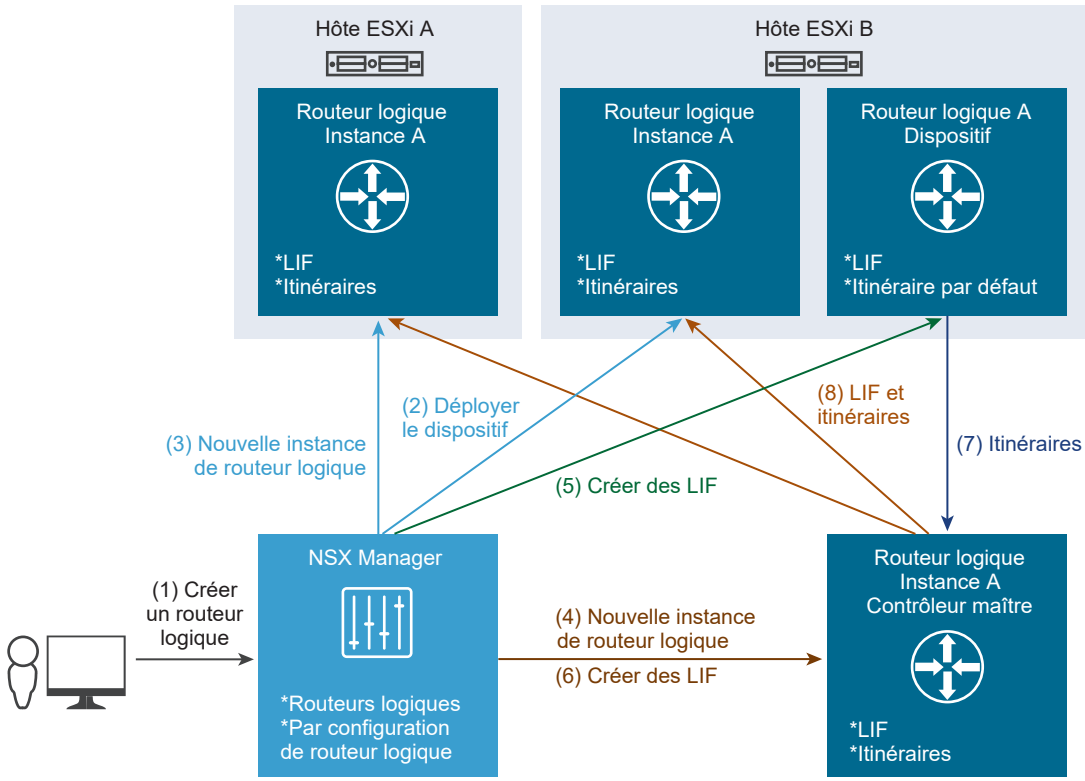
- Des réseaux sont directement connectés (connus depuis la configuration des interfaces)
- Tronçons suivants pour chaque sous-réseau (recherchés dans la table de routage)
- Adresse MAC à insérer dans des trames de sortie pour atteindre les tronçons suivants (table ARP)

Ces informations sont fournies aux instances distribuées sur plusieurs hôtes ESXi.

Processus de création du DLR

Le schéma suivant est une illustration générale du processus utilisé par NSX pour créer un DLR.

Figure 3-11. Processus de création du DLR



Lorsqu'un assistant d'interface utilisateur est envoyé avec le bouton Terminer ou qu'un appel API est passé pour déployer un nouveau DLR, le système réalise les étapes suivantes :

1 NSX Manager reçoit un appel API pour déployer un nouveau DLR (directement ou depuis vSphere Web Client, appelé par l'assistant d'interface utilisateur).

2 NSX Manager appelle son serveur vCenter Server lié pour déployer une VM de contrôle du DLR (ou une paire, si HA a été demandé).

   a La VM de contrôle du DLR est activée et se reconnecte à NSX Manager, prêt à recevoir la configuration.

b Si une paire HA a été déployée, NSX Manager configure une règle d'anti-affinité qui permet à la paire HA de s'exécuter sur différents hôtes. Le DRS agit ensuite pour les éloigner.

3 NSX Manager crée une instance du DLR sur des hôtes :

a NSX Manager recherche les commutateurs logiques qu'il faut connecter au nouveau DLR afin de déterminer à quelle zone de transport ils appartiennent.

b Ensuite, il recherche une liste de clusters qui sont configurés dans cette zone de transport et crée le DLR sur chaque hôte dans ces clusters.

c À ce stade, les hôtes ne connaissent que l'ID du nouveau DLR, mais ils n'ont aucune information correspondante (LIF ou itinéraires).

4 NSX Manager crée une instance du DLR sur le cluster de contrôleurs.

a Le cluster de contrôleurs alloue l'un des nœuds de contrôleur comme maître pour cette instance du DLR.

5 NSX Manager envoie la configuration, notamment les LIF, à la VM de contrôle du DLR.

a Les hôtes ESXi (notamment celui sur lequel est exécutée la VM de contrôle du DLR) reçoivent des informations de découpage de la part du cluster de contrôleurs, déterminent quel nœud de contrôleur est responsable de la nouvelle instance du DLR et se connectent au nœud de contrôleur (s'il n'y avait aucune connexion existante).

6 Une fois la LIF créée sur la VM de contrôle du DLR, NSX Manager crée les LIF du nouveau DLR sur le cluster de contrôleurs.

7 La VM de contrôle du DLR se connecte au nœud de contrôleur de la nouvelle instance du DLR et envoie les itinéraires au nœud de contrôleur :

a Tout d'abord, le DLR traduit sa table de routage en table de transfert (en résolvant les préfixes en LIF).

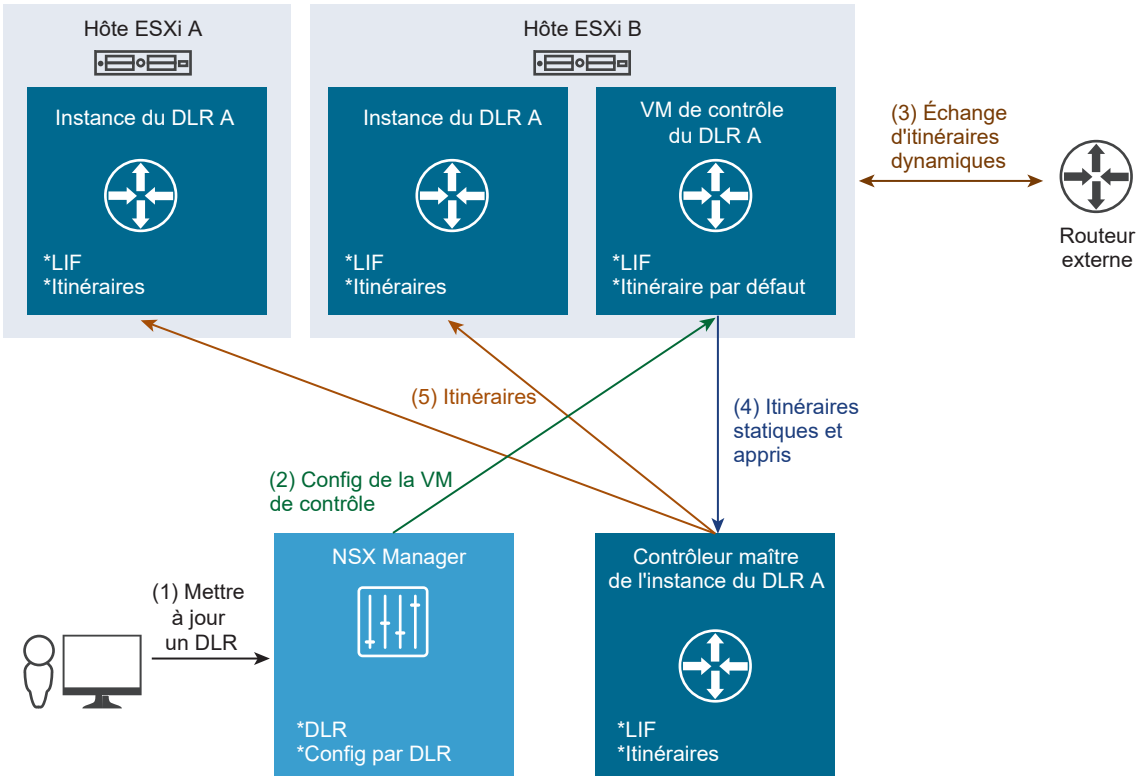
b Ensuite, le DLR envoie la table résultante au nœud de contrôleur.

8 Le nœud de contrôleur transfère les LIF et les itinéraires aux autres hôtes sur lesquels la nouvelle instance du DLR existe, via la connexion établie à l'étape 5.a.

Ajout d'un routage dynamique à un DLR

Lorsque le DLR est créé via un appel API « direct » (au lieu d'utiliser l'interface utilisateur de vSphere Web Client), il est possible de le fournir avec une configuration complète qui inclut un routage dynamique (1).

Figure 3-12. Routage dynamique sur le DLR



1 NSX Manager reçoit un appel API pour modifier la configuration du DLR existant, dans ce cas en ajoutant un routage dynamique.

2 NSX Manager envoie la nouvelle configuration à la VM de contrôle du DLR.

3 La VM de contrôle du DLR applique la configuration et procède à l'établissement de contiguïtés de routage, à l'échange des informations de routage, etc.

4 Après l'échange de routage, la VM de contrôle du DLR calcule la table de transfert et l'envoie au nœud de contrôleur maître du DLR.

5 Le nœud de contrôleur maître du DLR distribue ensuite les itinéraires mis à jour aux hôtes ESXi sur lesquels l'instance du DLR existe.

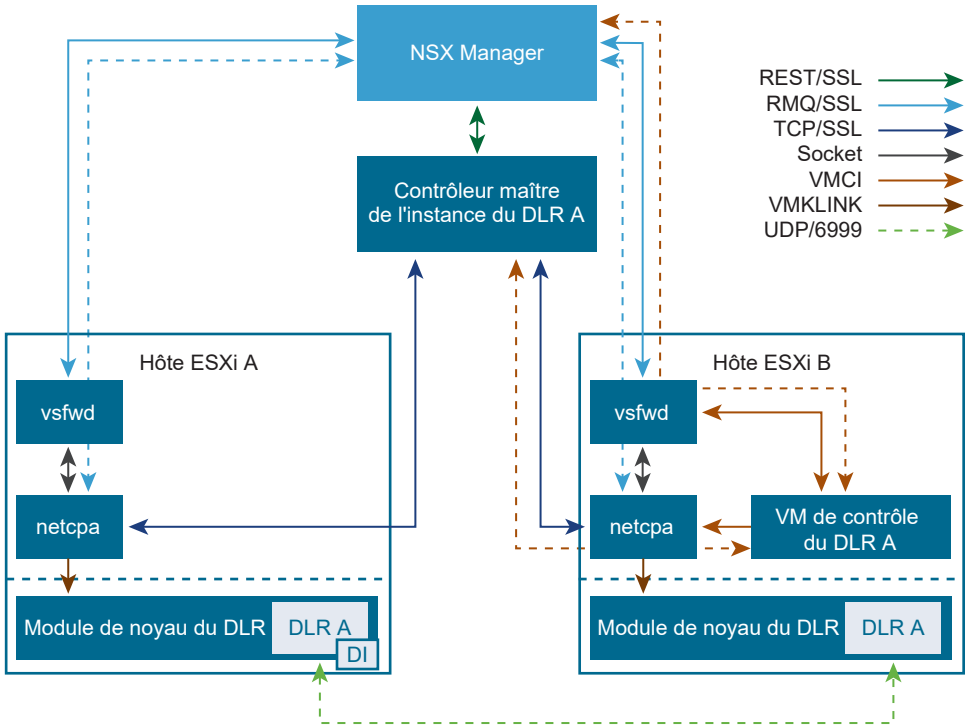
Notez que l'instance du DLR sur l'hôte ESXi sur lequel la VM de contrôle du DLR est exécutée reçoit ses LIF et itinéraires uniquement depuis le nœud de contrôleur maître du DLR, jamais directement depuis la VM de contrôle du DLR ou depuis NSX Manager.

Composants et communications des plans de contrôle et de gestion du DLR

Cette section présente brièvement les composants des plans de contrôle et de gestion du DLR.

La figure indique les composants et les canaux de communication correspondants entre eux.

Figure 3-13. Composants des plans de contrôle et de gestion du DLR



- NSX Manager :
  - Établit des communications directes avec le cluster de contrôleurs
  - Établit une connexion permanente directe avec le processus du client de bus de messages (vsfwd) exécuté sur chaque hôte préparé pour NSX
- Pour chaque instance du DLR, un nœud de contrôleur (en dehors des 3 disponibles) est choisi comme maître
  - La fonction maître peut passer à un nœud de contrôleur différent, si celui d'origine échoue
- Chaque hôte ESXi exécute deux agents UWA (User World Agent) : client de bus de messages (vsfwd) et agent de plan de contrôle (netcpa)
  - netcpa requiert des informations de NSX Manager pour fonctionner (par exemple, où trouver des contrôleurs et comment s'authentifier sur eux) ; ces informations sont accessibles via la connexion de bus de messages fournie par vsfwd
  - netcpa communique également avec le module de noyau du DLR pour le programmer avec les informations pertinentes qu'il reçoit de la part des contrôleurs
- Pour chaque instance du DLR, une VM de contrôle du DLR est exécutée sur l'un des hôtes ESXi ; la VM de contrôle du DLR contient deux canaux de communication :
  - Canal VMCI vers NSX Manager via vsfwd, qui est utilisé pour configurer la VM de contrôle
  - Canal VMCI vers le contrôleur maître du DLR via netcpa, qui est utilisé pour envoyer la table de routage du DLR au contrôleur

- Dans les cas où le DLR possède une LIF VLAN, l'un des hôtes ESXi participants est nommé par le contrôleur comme instance désignée (DI). Le module de noyau du DLR sur les autres hôtes ESXi demande que la DI effectue des requêtes ARP proxy sur le VLAN associé.

Composants de sous-système du routage NSX

Le sous-système du routage NSX est activé par plusieurs composants.

- NSX Manager
- Cluster de contrôleurs
- Modules hôtes ESXi (noyau et UWA)
- VM de contrôle du DLR
- Passerelles ESG

NSX Manager

NSX Manager fournit les fonctions suivantes applicables au routage NSX :

- Agit en tant que plan de gestion centralisé, en fournissant le point d'accès API unifié pour toutes les opérations de gestion de NSX
- Installe le module de noyau de routage distribué et des agents UWA (User World Agent) sur les hôtes afin de les préparer pour les fonctions de NSX
- Crée/détruit des DLR et des LIF du DLR
- Déploie/supprime une VM de contrôle du DLR et une passerelle ESG via vCenter
- Configure le cluster de contrôleurs via une API REST et les hôtes via un bus de messages :
  - Fournit des agents de plan de contrôle d'hôte avec les adresses IP des contrôleurs
  - Génère et distribue aux hôtes et aux contrôleurs les certificats pour des communications de plan de contrôle sécurisées
- Configure des passerelles ESG et des VM de contrôle du DLR via le bus de messages
  - Notez que des passerelles ESG peuvent être déployées sur des hôtes non préparés, auquel cas VIX sera utilisé à la place du bus de messages

Cluster de contrôleurs

Le routage distribué NSX requiert des contrôleurs, mis en cluster pour la mise à l'échelle et la disponibilité, qui fournissent les fonctions suivantes :

- Prennent en charge VXLAN et le plan de contrôle de routage distribué
- Fournissent une interface de ligne de commande pour les statistiques et les états d'exécution
- Choisissent un nœud de contrôleur maître pour chaque instance du DLR
  - Le nœud maître reçoit des informations de routage depuis la VM de contrôle du DLR et les distribue aux hôtes

- Envoie la table des LIF aux hôtes
- Conserve une trace de l'hôte sur lequel réside la VM de contrôle du DLR
- Sélectionne une instance désignée pour les LIF VLAN et communique ces informations aux hôtes ; surveille l'hôte de la DI via des conservations de connexion active du plan de contrôle (la durée d'expiration est de 30 secondes et la durée de détection peut être comprise entre 20 et 40 secondes), envoie aux hôtes une mise à jour si l'hôte de la DI sélectionné disparaît

Modules hôtes ESXi

Le routage NSX utilise directement deux agents UWA (User World Agent) et un module de noyau de routage et repose également sur le module de noyau de VXLAN pour la connectivité VXLAN.

Voici un résumé de ce que chaque composant effectue :

- L'agent de plan de contrôle (netcpa) est un client TCP (SSL) qui communique avec le contrôleur à l'aide du protocole de plan de contrôle. Il peut se connecter à plusieurs contrôleurs. netcpa communique avec le client de bus de messages (vsfwd) pour récupérer les informations liées au plan de contrôle depuis NSX Manager.
- Conditionnement et déploiement de netcpa :
  - L'agent est conditionné dans le VIB de VXLAN (bundle d'installation de vSphere)
  - Installé par NSX Manager via EAM (ESX Agency Manager) lors de la préparation de l'hôte
  - Est exécuté en tant que démon de service sur netcpa ESXi
  - Peut être démarré/arrêté/interrogé via son script de démarrage /etc/init.d/netcpad
  - Peut être redémarré à distance via l'interface utilisateur de Networking and Security Installation -> Préparation de l'hôte -> Statut de l'installation, sur des hôtes individuels ou sur un cluster complet
- Le module de noyau du DLR (vdrb) s'intègre à DVS pour activer le transfert L3
  - Configuré par netcpa
  - Installé dans le cadre du déploiement du VIB de VXLAN
  - Se connecte au DVS via la jonction spéciale appelée « vdrPort », qui prend en charge des VLAN et des VXLAN
  - Conserve des informations sur des instances du DLR, avec par instance :
    - Tables des LIF et des itinéraires
    - Cache ARP de l'hôte local
- Le client de bus de messages (vsfwd) est utilisé par netcpa, des passerelles ESG et des VM de contrôle du DLR pour communiquer avec NSX Manager
  - vsfwd obtient l'adresse IP de NSX Manager depuis /UserVars/RmqIpAddress définie par vCenter via vpxa/hosd et se connecte au serveur de bus de messages à l'aide des informations d'identification par hôte stockées dans d'autres variables /UserVars/Rmq*

- netcpa exécuté sur un hôte ESXi repose sur vsfwd pour réaliser les actions suivantes :
  - Obtenir la clé privée et le certificat SSL du plan de contrôle de l'hôte depuis NSX Manager. Ils sont ensuite stockés dans /etc/vmware/ssl/rui-for-netcpa.*
  - Obtenir des adresses IP et des empreintes numériques SSL de contrôleurs depuis NSX Manager. Elles sont ensuite stockées dans /etc/vmware/netcpa/config-by-vsm.xml.
  - Créer et supprimer des instances du DLR sur son hôte sur ordre de NSX Manager
- Conditionnement et déploiement
  - Comme netcpa, cela fait partie du VIB de VXLAN
  - Est exécuté en tant que démon de service sur vsfwd ESXi
  - Peut être démarré/arrêté/interrogé via son script de démarrage /etc/init.d/ vShield-Stateful-Firewall
- Les passerelles ESG et les VM de contrôle du DLR utilisent le canal VMCI vers vsfwd pour recevoir la configuration de NSX Manager

VM de contrôle du DLR et passerelles ESG

- La VM de contrôle du DLR est un « processeur d'itinéraires » pour son instance du DLR
  - Contient une interface « espace réservé » ou « vNIC réelle » pour chaque LIF du DLR, ainsi qu'une configuration IP
  - Peut exécuter l'un des deux protocoles de routage dynamique disponibles (BGP ou OSPF) et/ou utiliser des itinéraires statiques
  - Requiert au moins une LIF « Liaison montante » pour pouvoir exécuter OSPF ou BGP
  - Calcule la table de transfert à partir des sous-réseaux connectés directement (LIF), des itinéraires statiques et dynamiques, et les envoie via son lien VMCI vers netcpa au contrôleur maître de l'instance du DLR
  - Prend en charge HA dans une configuration de paire de VM Active/En veille
- La passerelle ESG est un routeur indépendant dans une VM
  - Complètement indépendant du sous-système de routage du DLR NSX (aucune intégration du plan de contrôle NSX)
  - En général utilisé en tant que passerelle en amont pour un ou plusieurs DLR
  - Prend en charge plusieurs protocoles de routage dynamique exécutés simultanément

Interface de ligne de commande du plan de contrôle de routage NSX

En plus des composants hôtes, le routage NSX emploie des services du cluster de contrôleurs et des VM de contrôle du DLR, chacun étant une source des informations du plan de contrôle du DLR et possédant sa propre interface de ligne de commande utilisée pour l'examiner.

Contrôleur maître de l'instance du DLR

Chaque instance du DLR est desservie par l'un des nœuds de contrôleur. Les commandes CLI suivantes peuvent être utilisées pour afficher des informations que ce nœud de contrôleur possède pour l'instance du DLR pour laquelle il est le maître :

```
nsx-controller # show control-cluster logical-routers instance 1460487509
LR-Id      LR-Name           Hosts[]         Edge-Connection Service-Controller
1460487509 default+edge-1    192.168.210.57                  192.168.110.201
                             192.168.210.51
                             192.168.210.52
                             192.168.210.56
                             192.168.110.51
                             192.168.110.52

nsx-controller # show control-cluster logical-routers interface-summary 1460487509
Interface                       Type   Id           IP[]
570d455500000002                vxlan  5003         192.168.10.2/29
570d45550000000b                vxlan  5001         172.16.20.1/24
570d45550000000c                vxlan  5002         172.16.30.1/24
570d45550000000a                vxlan  5000         172.16.10.1/24

nsx-controller # show control-cluster logical-routers routes 1460487509
LR-Id       Destination        Next-Hop
1460487509  0.0.0.0/0          192.168.10.1
```

- La sous-commande « instance » de la commande « show control-cluster logical-routers » affiche une liste d'hôtes qui sont connectés à ce contrôleur pour cette instance du DLR. Dans un environnement fonctionnant correctement, cette liste doit inclure tous les hôtes de tous les clusters sur lesquels le DLR existe.
- « interface-summary » (Résumé d'interface) affiche les LIF apprises par le contrôleur auprès de NSX Manager. Ces informations sont envoyées aux hôtes.
- « routes » (Itinéraires) indique la table de routage envoyée à ce contrôleur par la VM de contrôle de ce DLR. Sachez que, contrairement aux hôtes ESXi, cette table n'inclut aucun sous-réseau connecté directement, car ces informations sont fournies par la configuration de LIF.

VM de contrôle du DLR

La VM de contrôle du DLR contient des LIF et des tables de routage/transfert. La principale sortie du cycle de vie de la VM de contrôle du DLR est la table de routage du DLR, qui est un produit d'interfaces et itinéraires.

```
edge-1-0> show ip route

Codes: O - OSPF derived, i - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
Total number of routes: 5

S       0.0.0.0/0            [1/1]         via 192.168.10.1
C       172.16.10.0/24       [0/0]         via 172.16.10.1
C       172.16.20.0/24       [0/0]         via 172.16.20.1
C       172.16.30.0/24       [0/0]         via 172.16.30.1
C       192.168.10.0/29      [0/0]         via 192.168.10.2

edge-1-0> show ip forwarding
Codes: C - connected, R - remote,
       > - selected route, * - FIB route
R>* 0.0.0.0/0 via 192.168.10.1, vNic_2
C>* 172.16.10.0/24 is directly connected, VDR
C>* 172.16.20.0/24 is directly connected, VDR
C>* 172.16.30.0/24 is directly connected, VDR
C>* 192.168.10.0/29 is directly connected, vNic_2
```

- L'objectif de la table de transfert est d'afficher quelle interface du DLR est choisie comme sortie pour un sous-réseau de destination donné.
  - L'interface « VDR » est affichée pour toutes les LIF de type « Internal » (Interne). L'interface « VDR » est une pseudo-interface qui ne correspond pas à une vNIC.

Les interfaces de la VM de contrôle du DLR peuvent être affichées comme suit :

```
edge-1-0> show interface
Interface VDR is up, line protocol is up
  index 2 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,NOARP>
  HWaddr: be:3d:a1:52:90:f4
  inet6 fe80::bc3d:a1ff:fe52:90f4/64
  inet 172.16.10.1/24
  inet 172.16.20.1/24
  inet 172.16.30.1/24
  proxy_arp: disabled
  Auto-duplex (Full), Auto-speed (2460Mb/s)
    input packets 0, bytes 0, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 0, bytes 0, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0

Interface vNic_0 is up, line protocol is up
  index 3 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:50:56:8e:1c:fb
  inet6 fe80::250:56ff:fe8e:1cfb/64
  inet 169.254.1.1/30
  inet 10.10.10.1/24
  proxy_arp: disabled
  Auto-duplex (Full), Auto-speed (2460Mb/s)
    input packets 582249, bytes 37339072, dropped 49, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 4726382, bytes 461202852, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
```

```
Interface vNic_2 is up, line protocol is up
  index 9 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:50:56:8e:ae:08
  inet 192.168.10.2/29
  inet6 fe80::250:56ff:fe8e:ae08/64
  proxy_arp: disabled
  Auto-duplex (Full), Auto-speed (2460Mb/s)
    input packets 361446, bytes 30167226, dropped 0, multicast packets 361168
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 361413, bytes 30287912, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
```

Notes d'intérêt :

- L'interface « VDR » n'est associée à aucune carte réseau de VM (vNIC). Il s'agit d'une simple « pseudo-interface » qui est configurée avec toutes les adresses IP de toutes les LIF « Internal » (Interne) du DLR.
- L'interface vNic_0 dans cet exemple est l'interface HA.
  - La sortie ci-dessus a été prise depuis un DLR déployé avec HA activé, et une adresse IP est attribuée à l'interface HA. Cela s'affiche sous la forme de deux adresses IP, 169.254.1.1/30 (auto-attribuée pour HA) et 10.10.10.1/24, attribuée manuellement à l'interface HA.
  - Sur une passerelle ESG, l'opérateur peut attribuer manuellement l'une de ces vNIC comme HA ou la laisser par défaut pour que le système choisisse automatiquement parmi les interfaces « Internal » (Interne) disponibles. Le type « Internal » (Interne) est obligatoire, sinon HA échouera.
- L'interface vNic_2 est de type liaison montante ; par conséquent, elle est représentée en tant que vNIC « réelle ».
  - Notez que l'adresse IP vue sur cette interface est la même que celle de la LIF du DLR ; toutefois, la VM de contrôle du DLR ne répondra pas aux requêtes ARP pour l'adresse IP de la LIF (dans ce cas, 192.168.10.2/29). Un filtre ARP est appliqué pour l'adresse MAC de cette vNIC qui le rend possible.
  - Le point ci-dessus est vrai tant qu'un protocole de routage dynamique est configuré sur le DLR, lorsque l'adresse IP sera supprimée avec le filtre ARP et remplacée par l'adresse « Protocol IP » (IP de protocole) spécifiée lors de la configuration du protocole de routage dynamique.
  - Cette vNIC est utilisée par le protocole de routage dynamique exécuté sur la VM de contrôle du DLR pour communiquer avec les autres routeurs afin de publier et d'apprendre des itinéraires.
- Une fois le dispositif Edge déconnecté et après le basculement HA, l'adresse IP de l'interface du dispositif Edge déconnecté est supprimée de la base d'informations de routage (RIB)/base d'informations de transfert (FIB) du dispositif Edge actif. Mais le tableau FIB du dispositif Edge en veille ou la commande `show ip forwarding` indique toujours l'adresse IP et elle n'est pas supprimée du tableau FIB. Il s'agit du comportement attendu.

Modes d'échec du sous-système de routage NSX et leurs effets

Ce chapitre décrit les scénarios d'échec classiques pouvant affecter les composants du sous-système de routage NSX et les effets de ces échecs.

NSX Manager

Tableau 3-2. Modes d'échec de NSX Manager et effets

Mode d'échec	Effets de l'échec
Perte de connectivité réseau avec la VM NSX Manager	■ Indisponibilité totale de toutes les fonctions de NSX Manager, notamment les opérations CLMS pour le routage/pontage NSX ■ Aucune perte de données de configuration ■ Aucune indisponibilité des données ou du plan de contrôle
Perte de connectivité réseau entre NSX Manager et les hôtes ESXi ou échec du serveur RabbitMQ	■ Si la VM de contrôle du DLR ou la passerelle ESG est exécutée sur des hôtes affectés, les opérations CLMS sur elles échouent ■ La création et la suppression d'instances du DLR sur des hôtes affectés échouent ■ Aucune perte de données de configuration ■ Aucune indisponibilité des données ou du plan de contrôle ■ Les mises à jour du routage dynamique continuent de fonctionner
Perte de connectivité réseau entre NSX Manager et les contrôleurs	■ Les opérations de création, de mise à jour et de suppression pour le routage distribué et le pontage de NSX échouent ■ Aucune perte de données de configuration ■ Aucune indisponibilité des données ou du plan de contrôle
La VM NSX Manager est détruite (échec de la banque de données)	■ Indisponibilité totale de toutes les fonctions de NSX Manager, notamment les opérations CLMS pour le routage/pontage NSX ■ Risque qu'un sous-ensemble d'instances de routage/pontage devienne orphelin si NSX Manager est restauré vers une ancienne configuration, ce qui requiert un nettoyage et un rapprochement manuels ■ Aucune indisponibilité des données ou du plan de contrôle, sauf si un rapprochement est nécessaire

Cluster de contrôleurs

Tableau 3-3. Modes d'échec de NSX Controller et effets

Mode d'échec	Effets de l'échec
Le cluster de contrôleurs perd la connectivité réseau avec les hôtes ESXi	■ Indisponibilité totale de toutes les fonctions du plan de contrôle du DLR (création, mise à jour et suppression des itinéraires, y compris dynamiques) ■ Indisponibilité des fonctions du plan de gestion du DLR (création, mise à jour et suppression de LIF sur des hôtes) ■ Le transfert de VXLAN est affecté, ce qui peut également entraîner l'échec du processus de transfert de bout en bout (L2+L3) ■ Le plan de données continue de fonctionner selon le dernier état connu
Un ou deux contrôleurs perdent la connectivité avec les hôtes ESXi	■ Si un contrôleur affecté peut toujours atteindre d'autres contrôleurs dans le cluster, les instances du DLR contrôlées par ce contrôleur rencontrent les mêmes effets que ceux décrits ci-dessus. D'autres contrôleurs ne prennent pas le contrôle automatiquement
Un contrôleur perd la connectivité réseau avec les autres contrôleurs (ou complètement)	■ Deux contrôleurs restants prennent le contrôle de VXLAN et de DLR gérés par le contrôleur isolé ■ Le contrôleur affecté passe en mode lecture seule, annule ses sessions sur des hôtes et refuse les nouvelles
Les contrôleurs perdent la connectivité entre eux	■ Tous les contrôleurs passent en mode lecture seule, ferment les connexions aux hôtes et refusent les nouvelles ■ Les opérations de création, de mise à jour et de suppression des LIF et des itinéraires de tous les DLR (y compris dynamiques) échouent ■ La configuration du routage NSX (LIF) peut être désynchronisée entre NSX Manager et le cluster de contrôleurs, ce qui nécessite une intervention manuelle pour la resynchronisation ■ Les hôtes continueront à fonctionner avec le dernier état connu du plan de contrôle
Une VM de contrôleur est perdue	■ Le cluster de contrôleurs perd la redondance ■ Le plan de gestion/contrôle continue à fonctionner normalement
Deux VM de contrôleur sont perdues	■ Le contrôleur restant passera en mode lecture seule ; l'effet est le même que lorsque des contrôleurs perdent la connectivité entre eux (au-dessus). Récupération manuelle du cluster probablement nécessaire

Modules hôtes

netcpa repose sur la clé et le certificat SSL d'hôte, en plus des empreintes numériques SSL, pour établir des communications sécurisées avec les contrôleurs. Ces éléments sont obtenus auprès de NSX Manager via le bus de messages (fourni par vsfwd).

Si le processus d'échange de certificats échoue, netcpa ne pourra pas se connecter correctement aux contrôleurs.

Remarque : cette section n'aborde pas l'échec des modules de noyau, car son effet est grave (PSOD) et cela se produit rarement.

Tableau 3-4. Modes d'échec du module hôte et effets

Mode d'échec	Effets de l'échec
vsfwd utilise l'authentification par nom d'utilisateur/mot de passe pour accéder au serveur de bus de messages, qui peut expirer	■ Si vsfwd sur un hôte ESXi récemment préparé ne peut pas atteindre NSX Manager dans les deux heures, le nom de connexion et le mot de passe temporaires fournis pendant l'installation expirent et le bus de messages sur cet hôte devient inopérable
Les effets de l'échec du client de bus de messages (vsfwd) dépendent du timing.	
S'il échoue avant que d'autres éléments du plan de contrôle de NSX aient pu atteindre un état d'exécution stable	■ Le routage distribué sur l'hôte cesse de fonctionner, car l'hôte ne peut pas communiquer avec les contrôleurs ■ L'hôte n'apprend pas les instances du DLR de NSX Manager
S'il échoue une fois que l'hôte a atteint un état stable	■ Des passerelles ESG et des VM de contrôle du DLR exécutées sur l'hôte ne pourront pas recevoir des mises à jour de configuration ■ L'hôte n'apprend pas les nouveaux DLR et ne peut pas supprimer des DLR existants ■ Le chemin de données de l'hôte continuera de fonctionner selon la configuration de l'hôte au moment de l'échec

Tableau 3-5. Modes d'échec de netcpa et effets

Mode d'échec	Effets de l'échec
Les effets de l'échec de l'agent de plan de contrôle (netcpa) dépendent du timing	
S'il échoue avant que les modules de noyau du chemin de données de NSX aient pu atteindre un état d'exécution stable	■ Le routage distribué sur l'hôte cesse de fonctionner
S'il échoue une fois que l'hôte a atteint un état stable	■ Une ou des VM de contrôle du DLR exécutées sur l'hôte ne pourront pas envoyer les mises à jour de leur table de transfert aux contrôleurs ■ Le chemin de données du routage distribué ne recevra aucune mise à jour de LIF ou d'itinéraire de la part des contrôleurs, mais il continuera à fonctionner selon son état avant l'échec

VM de contrôle du DLR

Tableau 3-6. Modes d'échec de la VM de contrôle du DLR et effets

Mode d'échec	Effets de l'échec
La VM de contrôle du DLR est perdue ou désactivée	■ Les opérations de création, de mise à jour et de suppression des LIF et des itinéraires de ce DLR échouent ■ Aucune mise à jour d'itinéraire dynamique ne sera envoyée aux hôtes (notamment retrait de préfixes reçus via des contiguïtés maintenant rompues)
La VM de contrôle du DLR perd la connectivité avec NSX Manager et les contrôleurs	■ Même effets que ci-dessus, sauf si la VM de contrôle du DLR et ses contiguïtés de routage sont toujours actives, le trafic vers et depuis des préfixes appris précédemment ne sera pas affecté
La VM de contrôle du DLR perd la connexion avec NSX Manager	■ Les opérations de création, de mise à jour et de suppression de NSX Manager pour les LIF et les itinéraires de ce DLR échoueront et ne seront pas retentées ■ Les mises à jour du routage dynamique continuent de se propager
La VM de contrôle du DLR perd la connexion avec les contrôleurs	■ Les modifications apportées au routage (statique ou dynamique) pour ce DLR ne se propagent pas sur les hôtes

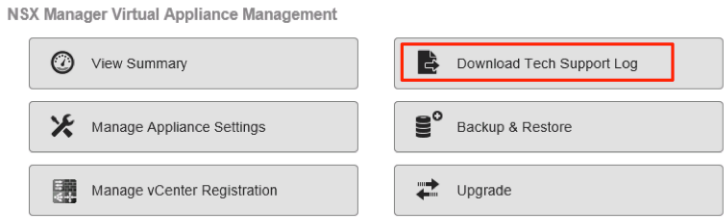
Journaux de NSX applicables au routage

Il est recommandé de configurer tous les composants de NSX pour qu'ils envoient leurs journaux à un collecteur centralisé, où ils peuvent être examinés dans un seul emplacement.

Si nécessaire, vous pouvez modifier le niveau de journal de composants NSX. Pour plus d'informations, reportez-vous à la section « Définition du niveau de journalisation des composants de NSX » dans *Journalisation et événements système dans NSX*.

Journaux de NSX Manager

- `show log` dans l'interface de ligne de commande de NSX Manager
- Bundle de journaux du support technique, collecté via l'interface utilisateur de NSX Manager



Le journal de NSX Manager contient des informations liées au plan de gestion, qui couvre les opérations Créer, Lire, Mettre à jour et Supprimer (CLMS).

Journaux du contrôleur

Les contrôleurs contiennent plusieurs modules, beaucoup disposant de leurs propres fichiers journaux. Les journaux de contrôleur sont accessibles à l'aide de la commande `show log <log file> [ filtered-by <string> ]`. Les fichiers journaux applicables au routage sont les suivants :

- `cloudnet/cloudnet_java-vnet-controller.<start-time-stamp>.log` : ce journal gère la configuration et le serveur API interne.
- `cloudnet/cloudnet.nsx-controller.log` : il s'agit du journal du processus principal du contrôleur.
- `cloudnet/cloudnet_cpp.log.nsx-controller.log` : ce journal gère le clustering et le démarrage.
- `cloudnet/cloudnet_cpp.log.ERROR` : ce fichier est présent si une erreur se produit.

Les journaux de contrôleur sont détaillés et, dans la plupart des cas, ils ne sont requis que lorsque les ingénieurs de VMware sont sollicités pour résoudre des cas plus difficiles.

En plus de l'interface de ligne de commande `show log`, des fichiers journaux individuels peuvent être consultés en temps réel lors de leur mise à jour, à l'aide de la commande `watch log <logfile> [ filtered-by <string> ]`.

Les journaux sont inclus dans le bundle de support du contrôleur qui peut être généré et téléchargé en sélectionnant un nœud de contrôleur dans l'interface utilisateur de NSX et en cliquant sur l'icône **Télécharger les journaux de support technique (Download tech support logs)**.

Journaux de l'hôte ESXi

Les composants de NSX exécutés sur les hôtes ESXi écrivent plusieurs fichiers journaux :

- Journaux VMkernel : `/var/log/vmkernel.log`
- Journaux de l'agent de plan de contrôle : `/var/log/netcpa.log`
- Journaux du client de bus de messages : `/var/log/vsfwd.log`

Les journaux peuvent également être collectés dans le cadre du bundle de support de VM généré depuis vCenter Server. Seuls les utilisateurs ou les groupes d'utilisateurs disposant du privilège *racine* peuvent accéder aux fichiers journaux.

Journaux de la passerelle ESG/VM de contrôle du DLR

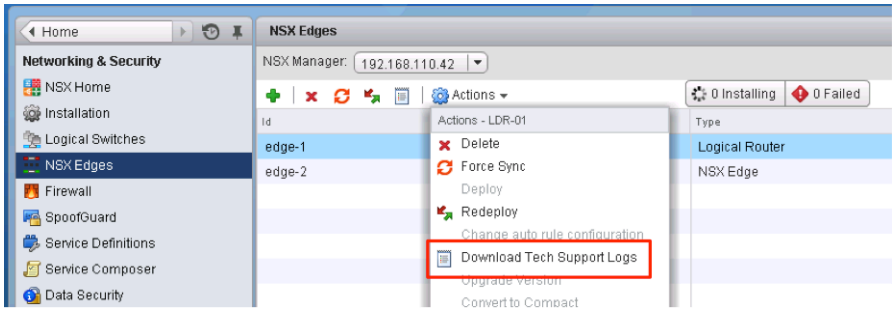
Il existe deux façons d'accéder aux fichiers journaux sur la passerelle ESG et les VM de contrôle du DLR : les afficher à l'aide d'une interface de ligne de commande ou télécharger le bundle de support technique à l'aide de l'interface de ligne de commande ou de l'interface utilisateur.

La commande CLI pour afficher les journaux est `show log [ follow | reverse ]`.

Pour télécharger le bundle de support technique :

- À partir de l'interface de ligne de commande, passez en mode `enable`, puis exécutez la commande `export tech-support <[ scp | ftp ]> <URI>`.

- À partir de vSphere Web Client, sélectionnez l'option **Télécharger les journaux de support technique (Download Tech Support Logs)** dans le menu **Actions**.



Autres fichiers utiles et leurs emplacements

Bien qu'il ne s'agisse pas purement de journaux, plusieurs fichiers peuvent être utiles pour comprendre et résoudre le routage NSX.

- La configuration de l'agent de plan de contrôle `/etc/vmware/netcpa/config-by-vsm.xml` contient les informations sur les composants suivants :
  - Adresses IP des contrôleurs, ports TCP, empreintes numériques de certificat, activer/désactiver SSL
  - dvUplinks sur le DVS activé avec VXLAN (stratégie d'association, noms, UUID)
  - Instances du DLR que l'hôte connaît (ID du DLR, nom)
- La configuration de l'agent de plan de contrôle `/etc/vmware/netcpa/netcpa.xml` contient diverses options de configuration pour netcpa, notamment le niveau de journalisation (qui par défaut est **info**).
- Fichiers de certificat du plan de contrôle : `/etc/vmware/ssl/rui-for-netcpa.*`
  - Deux fichiers : certificat de l'hôte et clé privée de l'hôte
  - Utilisés pour l'authentification des connexions d'hôte aux contrôleurs

Tous ces fichiers sont créés par l'agent du plan de contrôle à l'aide des informations qu'il reçoit de la part de NSX Manager via la connexion du bus de messages fournie par vsfwd.

Scénarios d'échec courants et correctifs

Les scénarios d'échec les plus courants sont classés en deux catégories.

Il s'agit de problèmes de configuration et de plan de contrôle. Les problèmes de plan de gestion, bien que possibles, ne sont pas courants.

Problèmes de configuration et correctifs

Les problèmes courants de configuration et leurs effets sont décrits dans la section Tableau 3-7. Problèmes courants de configuration et leurs effets.

Tableau 3-7. Problèmes courants de configuration et leurs effets

Problèmes	Effets
Le protocole et les adresses IP de transfert sont inversés pour le routage dynamique	La contiguïté de protocole dynamique n'apparaîtra pas
La zone de transport n'est pas alignée avec la limite du DVS	Le routage distribué ne fonctionne pas sur un sous-réseau d'hôtes ESXi (ceux qui manquent dans la zone de transport)
Non-concordance de la configuration du protocole de routage dynamique (minuteurs, MTU, BGP ASN, mots de passe, mappage de zone entre interface et OSPF)	La contiguïté de protocole dynamique n'apparaît pas
Une adresse IP est attribuée à l'interface HA du DLR et la redistribution d'itinéraires connectés est activée	La VM de contrôle du DLR peut attirer le trafic pour le sous-réseau de l'interface HA et faire disparaître le trafic

Pour résoudre ces problèmes, examinez la configuration et corrigez-la si nécessaire.

Lorsque cela est nécessaire, utilisez la commande CLI `debug ip ospf` ou `debug ip bgp` et consultez les journaux sur la VM de contrôle du DLR ou sur la console ESG (pas via la session SSH) pour détecter les problèmes de configuration de protocole.

Problèmes du plan de contrôle et correctifs

Les problèmes du plan de contrôle rencontrés sont souvent causés par les problèmes suivants :

- Agent de plan de contrôle hôte (netcpa) incapable de se connecter à NSX Manager via le canal de bus de messages fourni par vsfwd
- Cluster de contrôleurs ayant des difficultés avec la gestion du rôle maître pour les instances du DLR/VXLAN

Les problèmes de cluster de contrôleurs liés à la gestion de rôles maîtres peuvent souvent être résolus en redémarrant l'une des instances de NSX Controller (`restart controller` sur l'interface de ligne de commande du contrôleur).

Pour plus d'informations sur la résolution des problèmes du plan de contrôle, consultez http://kb.vmware.com/kb/2125767.

Collecte des données de dépannage

Cette section fournit un résumé des commandes CLI couramment utilisées pour le dépannage du routage NSX.

NSX Manager

À partir de NSX 6.2, les commandes qui étaient auparavant exécutées depuis NSX Controller et d'autres composants de NSX pour dépanner le routage NSX sont désormais exécutées directement depuis NSX Manager.

- Liste d'instances du DLR
- Liste de LIF pour chaque instance du DLR
- Liste d'itinéraires pour chaque instance du DLR

- Liste d'adresses MAC pour chaque instance de pontage du DLR
- Interfaces
- Tables de routage et de transfert
- État des protocoles de routage dynamique (OSPF ou BGP)
- Configuration envoyée à la VM de contrôle du DLR ou à la passerelle ESG par NSX Manager

VM de contrôle du DLR et passerelle ESG

La VM de contrôle du DLR et la passerelle ESG fournissent des fonctionnalités pour capturer des paquets sur leurs interfaces. La capture de paquets peut aider à résoudre les problèmes de protocole de routage.

1 Exécutez `show interfaces` pour répertorier les noms d'interface.

2 Exécutez `debug packet [ display | capture ] interface <interface name>`.
   - Si vous utilisez la capture, les paquets sont enregistrés dans un fichier `.pcap`.

3 Exécutez `debug show files` pour répertorier les fichiers de capture enregistrés.

4 Exécutez `debug copy [ scp | ftp ] ...` pour télécharger des captures pour une analyse hors ligne.

```
dlr-01-0> debug packet capture interface vNic_2
tcpdump: listening on vNic_2, link-type EN10MB (Ethernet), capture size 65535 bytes
43 packets captured
48 packets received by filter
0 packets dropped by kernel
```

```
dlr-01-0> debug show files
total 4.0K
-rw------- 1 3.6K Mar 30 23:49 tcpdump_vNic_2.0
```

```
dlr-01-0> debug copy
  scp  use scp to copy
  ftp  use ftp to copy
```

```
dlr-01-0> debug copy scp
  URL  user@<remote-host>:<path-to>
```

La commande `debug packet` utilise tcpdump en arrière-plan et peut accepter des modificateurs de filtrage formatés comme des modificateurs de filtrage tcpdump sur UNIX. La seule exigence est que les espaces dans l'expression de filtre doivent être remplacées par des tirets bas (« _ »).

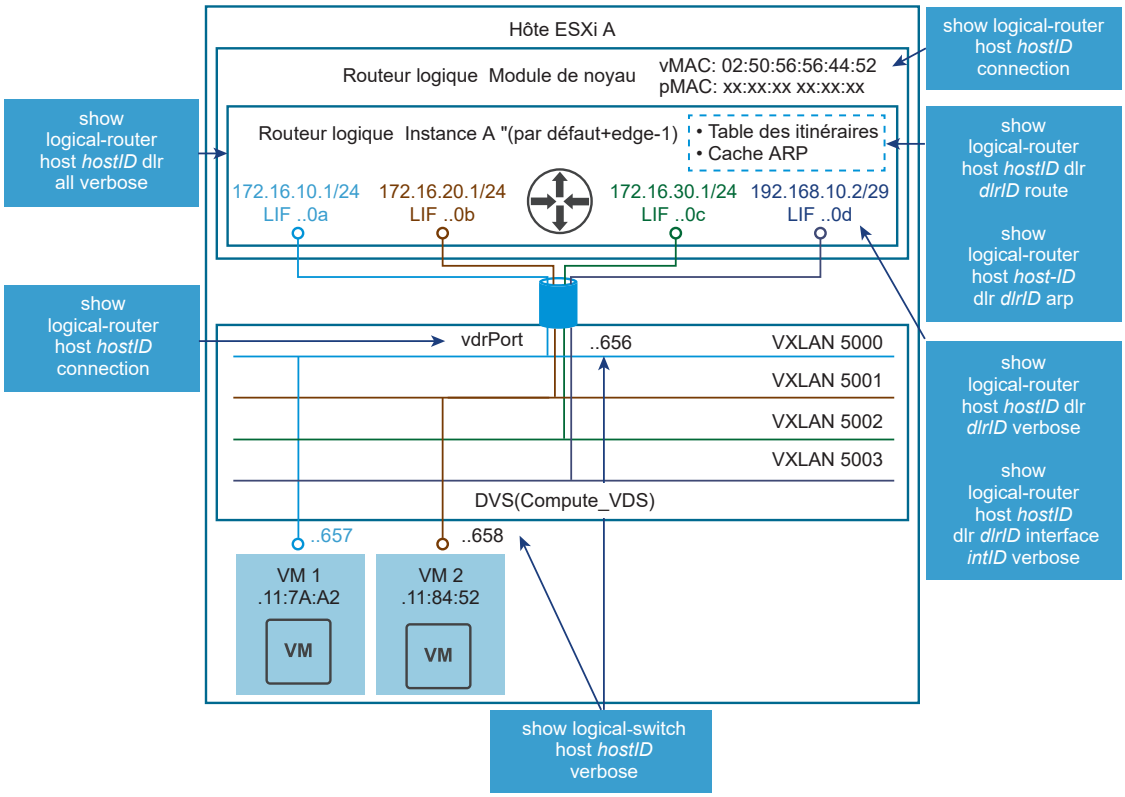
Par exemple, la commande suivante affiche tout le trafic via vNic_0 sauf SSH pour éviter de regarder le trafic appartenant à la session interactive elle-même.

```
plr-02-0> debug packet display interface vNic_0 port_not_22
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on vNic_0, link-type EN10MB (Ethernet), capture size 65535 bytes
04:10:48.197768 IP 192.168.101.3.179 > 192.168.101.2.25698: Flags [P.], seq 4191398894:4191398913,
ack 2824012766, win 913, length 19: BGP, length: 19
04:10:48.199230 IP 192.168.101.2.25698 > 192.168.101.3.179: Flags [.], ack 19, win 2623, length 0
04:10:48.299804 IP 192.168.101.2.25698 > 192.168.101.3.179: Flags [P.], seq 1:20, ack 19, win 2623,
length 19: BGP, length: 19
04:10:48.299849 IP 192.168.101.3.179 > 192.168.101.2.25698: Flags [.], ack 20, win 913, length 0
04:10:49.205347 IP 192.168.101.3.179 > 192.168.101.2.25698: Flags [P.], seq 19:38, ack 20, win 913,
length 19: BGP, length: 19
```

Hôtes ESXi

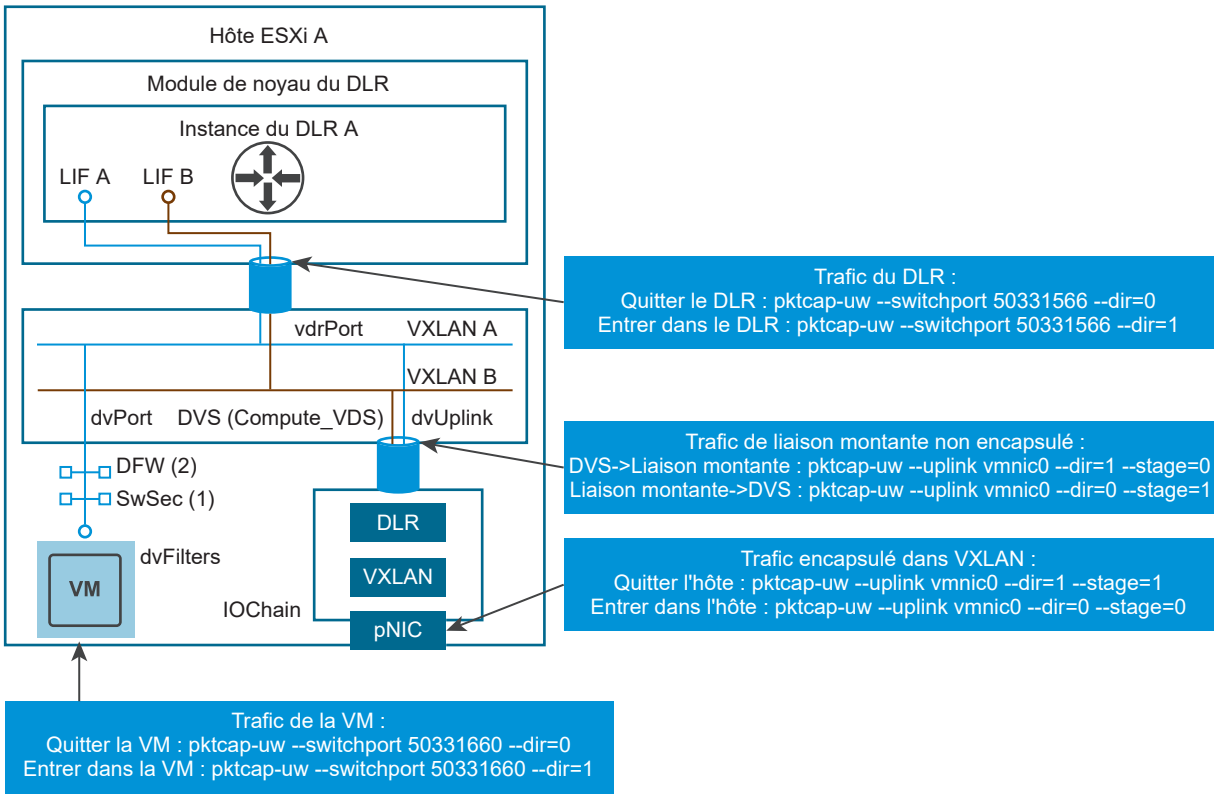
Les hôtes sont étroitement connectés au routage NSX. La Figure 3-14. Composants hôtes liés au dépannage du routage NSX illustre les composants faisant partie du sous-système de routage et les commandes CLI de NSX Manager utilisées pour afficher des informations sur eux :

Figure 3-14. Composants hôtes liés au dépannage du routage NSX



Les paquets capturés dans le chemin de données peuvent aider à identifier les problèmes à diverses étapes du transfert de paquets. La Figure 3-15. Points de capture et commandes CLI liées aborde les points de capture importants et la commande CLI respective à utiliser.

Figure 3-15. Points de capture et commandes CLI liées



Dépannage de NSX Edge 4

Cette rubrique comporte des informations pour comprendre et dépanner VMware NSX Edge.

Pour résoudre des problèmes avec un dispositif NSX Edge, vérifiez que toutes les étapes de dépannage ci-dessous sont avérées pour votre environnement. Chaque étape fournit des instructions ou un lien vers un document afin d'éliminer les causes possibles et de prendre une mesure corrective si nécessaire. Les étapes sont classées dans l'ordre le plus approprié afin d'isoler le problème et d'identifier la bonne résolution. Ne sautez pas une étape.

Consultez les notes de mise à jour des versions actuelles pour voir si le problème est résolu.

Vérifiez que la configuration système requise minimale est respectée lorsque vous installez VMware NSX Edge. Reportez-vous à *Guide d'installation de NSX*.

Problèmes d'installation et de mise à niveau

- Vérifiez que le problème que vous rencontrez n'est pas lié au problème « Would Block ». Pour plus d'informations, reportez-vous à la section https://kb.vmware.com/kb/2107951.
- Si la mise à niveau ou le redéploiement réussit, mais qu'il n'existe aucune connectivité pour l'interface Edge, vérifiez la connectivité sur le commutateur principal de couche 2. Reportez-vous à la section https://kb.vmware.com/kb/2135285.
- Si le déploiement ou la mise à niveau du dispositif Edge échoue avec l'erreur :

  ```
  /sbin/ifconfig vNic_1 up failed : SIOCSIFFLAGS: Invalid argument
  ```

  OU
- Si le déploiement ou la mise à niveau réussit, mais qu'il n'existe aucune connectivité sur les interfaces Edge :

- L'exécution de la commande `show interface` et des journaux de support Edge affiche des entrées semblables à :

```
vNic_0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN qlen 1000
    link/ether 00:50:56:32:05:03 brd ff:ff:ff:ff:ff:ff
    inet 21.12.227.244/23 scope global vNic_0
    inet6 fe80::250:56ff:fe32:503/64 scope link tentative dadfailed
       valid_lft forever preferred_lft forever
```

  Dans les deux cas, le commutateur hôte n'est pas prêt ou il rencontre des problèmes. Pour trouver une solution, examinez le commutateur hôte.

Problèmes de configuration

- Collectez les informations de diagnostic de NSX Edge. Reportez-vous à la section https://kb.vmware.com/kb/2079380.

  Filtrez les journaux NSX Edge en recherchant la chaîne `vse_die`. Les journaux près de cette chaîne peuvent fournir des informations sur l'erreur de configuration.

Utilisation élevée du CPU

Si vous voyez une utilisation élevée du CPU sur le dispositif NSX Edge, vérifiez les performances du dispositif à l'aide de la commande `esxtop` sur l'hôte ESXi. Examinez les articles suivants de la base de connaissances :

- https://kb.vmware.com/kb/1008205
- https://kb.vmware.com/kb/1008014
- https://kb.vmware.com/kb/1010071
- https://kb.vmware.com/kb/2096171

Consultez également https://communities.vmware.com/docs/DOC-9279.

Une valeur élevée pour le processus `ksoftirqd` indique un taux de paquets entrants élevé. Vérifiez si la journalisation est activée sur le chemin de données, comme pour les règles de pare-feu. Exécutez la commande `show log follow` pour déterminer si un grand nombre de résultats de journal a été enregistré.

Affichage des statistiques de rejet de paquets

À partir de NSX for vSphere 6.2.3, vous pouvez utiliser la commande `show packet drops` afin d'afficher des statistiques de rejet de paquets pour les éléments suivants :

- Interface
- Pilote

- L2
- L3
- Pare-feu

Pour exécuter la commande, connectez-vous à l'interface de ligne de commande NSX Edge et passez en mode basique. Pour plus d'informations, consultez la *Référence d'interface de ligne de commande de NSX*. Par exemple :

```
show packet drops

vShield Edge Packet Drop Stats:

Driver Errors
=============
          TX      TX    TX   RX   RX      RX
Interface Dropped Error Ring Full Dropped Error Out Of Buf
vNic_0    0       0     0    0    0       0
vNic_1    0       0     0    0    0       0
vNic_2    0       0     0    0    0       2
vNic_3    0       0     0    0    0       0
vNic_4    0       0     0    0    0       0
vNic_5    0       0     0    0    0       0

Interface Drops
===============
Interface RX Dropped TX Dropped
vNic_0             4          0
vNic_1          2710          0
vNic_2             0          0
vNic_3             2          0
vNic_4             2          0
vNic_5             2          0

L2 RX Errors
============
Interface length crc frame fifo missed
vNic_0         0   0     0    0      0
vNic_1         0   0     0    0      0
vNic_2         0   0     0    0      0
vNic_3         0   0     0    0      0
vNic_4         0   0     0    0      0
vNic_5         0   0     0    0      0

L2 TX Errors
============
Interface aborted fifo window heartbeat
vNic_0          0    0      0         0
vNic_1          0    0      0         0
vNic_2          0    0      0         0
vNic_3          0    0      0         0
vNic_4          0    0      0         0
vNic_5          0    0      0         0
```

```
L3 Errors
=========
IP:
 ReasmFails : 0
 InHdrErrors : 0
 InDiscards : 0
 FragFails : 0
 InAddrErrors : 0
 OutDiscards : 0
 OutNoRoutes : 0
 ReasmTimeout : 0
ICMP:
 InTimeExcds : 0
 InErrors : 227
 OutTimeExcds : 0
 OutDestUnreachs : 152
 OutParmProbs : 0
 InSrcQuenchs : 0
 InRedirects : 0
 OutSrcQuenchs : 0
 InDestUnreachs : 151
 OutErrors : 0
 InParmProbs : 0

Firewall Drop Counters
======================

Ipv4 Rules
==========
Chain – INPUT
rid pkts bytes target prot opt in out source    destination
0    119 30517 DROP   all  --   *   * 0.0.0.0/0 0.0.0.0/0    state INVALID
0      0     0 DROP   all  --   *   * 0.0.0.0/0 0.0.0.0/0
Chain – POSTROUTING
rid pkts bytes target prot opt in out source    destination
0    101 4040  DROP   all   --  *   * 0.0.0.0/0 0.0.0.0/0    state INVALID
0      0    0  DROP   all   --  *   * 0.0.0.0/0 0.0.0.0/0

Ipv6 Rules
==========
Chain – INPUT
rid pkts bytes target prot opt in out source destination
0      0     0   DROP  all      *   * ::/0   ::/0            state INVALID
0      0     0   DROP  all      *   * ::/0   ::/0
Chain – POSTROUTING
rid pkts bytes target prot opt in out source destination
0      0     0   DROP  all       *   * ::/0   ::/0           state INVALID
0      0     0   DROP  all       *   * ::/0   ::/0
```

Comportement normal lors de la gestion de NSX Edge

- Dans vSphere Web Client, lorsque vous configurez VPN L2 sur un dispositif NSX Edge et que vous ajoutez, supprimez ou modifiez **Détails de la configuration du site (Site Configuration Details)**, cette action entraînera la déconnexion et la reconnexion de toutes les connexions existantes. Ce comportement est normal.
- NSX Edge est une machine virtuelle (VM) et il se compose de plusieurs fichiers stockés sur un périphérique de stockage. Les fichiers clés sont le fichier de configuration, le ou les fichiers de disque virtuel, le fichier de configuration NVRAM, le fichier d'échange et le fichier journal. En fonction du placement appliqué ou manuel du profil de stockage de VM, les fichiers de configuration de machine virtuelle, le fichier de disque virtuel, le fichier d'échange peuvent être placés dans le même emplacement, ou dans des emplacements distincts sur différentes banques de données. Si les fichiers de machine virtuelle sont présents dans différents emplacements, NSX Manager affiche et utilise la banque de données comportant le fichier VMX pour le déploiement de machine virtuelle. Lors des opérations de redéploiement ou de mise à niveau, NSX Manager déploie la ou les VM NSX Edge sur la banque de données configurée ou sur la banque de données en direct qui héberge les fichiers VMX. Le *nom de banque de données* et l'*ID de banque de données* (qui héberge le fichier VMX de la VM) sont renvoyés dans le cadre du paramètre `Appliance` et sont affichés sur l'interface utilisateur ou fournis comme réponse à REST API. Vous devez vous reporter à vCenter Server pour plus d'informations sur la disposition exacte de chacun des fichiers de machine virtuelle de NSX Manager et une ou plusieurs banques de données dans lesquelles les fichiers sont placés. Pour plus d'informations, consultez la documentation suivante :
  - *Administrateur de machines virtuelles vSphere*.
  - *Gestion des ressources vSphere*.
  - *Gestion de vCenter Server et des hôtes*.

Ce chapitre contient les rubriques suivantes :

Problèmes de rejet de paquets du pare-feu Edge

Afficher les statistiques de rejet de paquets du pare-feu

À partir de NSX for vSphere 6.2.3, vous pouvez utiliser la commande `show packet drops` afin d'afficher des statistiques de rejet de paquets pour le pare-feu.

Pour exécuter la commande, connectez-vous à l'interface de ligne de commande NSX Edge et passez en mode basique. Pour plus d'informations, consultez la *Référence d'interface de ligne de commande de NSX*. Par exemple :

```
show packet drops

vShield Edge Packet Drop Stats:


Firewall Drop Counters
======================

Ipv4 Rules
==========
Chain – INPUT
rid pkts bytes target prot opt in out source    destination
0    119 30517 DROP   all  --   *   * 0.0.0.0/0 0.0.0.0/0    state INVALID
0      0     0 DROP   all  --   *   * 0.0.0.0/0 0.0.0.0/0
Chain – POSTROUTING
rid pkts bytes target prot opt in out source    destination
0    101 4040  DROP   all   --  *   * 0.0.0.0/0 0.0.0.0/0    state INVALID
0      0    0  DROP   all   --  *   * 0.0.0.0/0 0.0.0.0/0

Ipv6 Rules
==========
Chain – INPUT
rid pkts bytes target prot opt in out source destination
0      0     0   DROP  all      *   * ::/0   ::/0            state INVALID
0      0     0   DROP  all      *   * ::/0   ::/0
Chain – POSTROUTING
rid pkts bytes target prot opt in out source destination
0      0     0   DROP  all       *   * ::/0   ::/0           state INVALID
0      0     0   DROP  all       *   * ::/0   ::/0
```

Problèmes du pare-feu de paquet Edge

Pour exécuter une commande, connectez-vous à l'interface de ligne de commande NSX Edge et passez en mode basique. Pour plus d'informations, consultez la *Référence d'interface de ligne de commande de NSX*.

1 Consultez la table des règles de pare-feu avec la commande `show firewall`. La table `usr_rules` affiche les règles configurées.

```
nsxedge> show firewall
Chain PREROUTING (policy ACCEPT 3146M packets, 4098G bytes)
rid    pkts bytes target     prot opt in     out     source               destination

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
rid    pkts bytes target     prot opt in     out     source               destination
0     78903   16M ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
0         0     0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0
state INVALID
0      140K 9558K block_in   all  --  *      *       0.0.0.0/0            0.0.0.0/0
```

```
0     23789 1184K ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
state RELATED,ESTABLISHED
0      116K 8374K usr_rules  all  --  *      *       0.0.0.0/0            0.0.0.0/0
0         0     0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT 3146M packets, 4098G bytes)
rid    pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 173K packets, 22M bytes)
rid    pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
rid    pkts bytes target     prot opt in     out     source               destination
0     78903   16M ACCEPT     all  --  *      lo      0.0.0.0/0            0.0.0.0/0
0      679K   41M DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0
state INVALID
0     3146M 4098G block_out  all  --  *      *       0.0.0.0/0            0.0.0.0/0
0         0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
PHYSDEV match --physdev-in tap0 --physdev-out vNic_+
0         0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
PHYSDEV match --physdev-in vNic_+ --physdev-out tap0
0         0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
PHYSDEV match --physdev-in na+ --physdev-out vNic_+
0         0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
PHYSDEV match --physdev-in vNic_+ --physdev-out na+
0     3145M 4098G ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
state RELATED,ESTABLISHED
0      221K   13M usr_rules  all  --  *      *       0.0.0.0/0            0.0.0.0/0
0         0     0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain block_in (1 references)
rid    pkts bytes target     prot opt in     out     source               destination

Chain block_out (1 references)
rid    pkts bytes target     prot opt in     out     source               destination

Chain usr_rules (2 references)
rid    pkts bytes target     prot opt in     out     source               destination
131074 70104 5086K ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
match-set 0_131074-os-v4-1 src
131075  116K 8370K ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
match-set 1_131075-ov-v4-1 dst
131073  151K 7844K ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
```

Recherchez une valeur incrémentée d'une règle `DROP invalid` dans la section `POST_ROUTING` de la commande `show firewall`. Cela s'explique en général par :

- Des problèmes de routage asymétrique
- Des applications TCP qui ont été inactives pendant plus d'une heure. S'il existe des problèmes de délai d'expiration d'inactivité et que des applications sont inactives pendant une période anormalement longue, augmentez les paramètres de délai d'expiration d'inactivité à l'aide de REST API. Reportez-vous à la rubrique https://kb.vmware.com/kb/2101275

2 Collectez la sortie de la commande `show ipset`.

```
nsxedge> show ipset
Name: 0_131074-os-v4-1
Type: bitmap:if (Interface Match)
Revision: 3
Header: range 0-64000
Size in memory: 8116
References: 1
Number of entries: 1
Members:
vse (vShield Edge Device)

Name: 0_131074-os-v6-1
Type: bitmap:if (Interface Match)
Revision: 3
Header: range 0-64000
Size in memory: 8116
References: 1
Number of entries: 1
Members:
vse (vShield Edge Device)

Name: 1_131075-ov-v4-1
Type: hash:oservice (Match un-translated Ports)
Revision: 2
Header: family inet hashsize 64 maxelem 65536
Size in memory: 704
References: 1
Number of entries: 2
Members:
Proto=6, DestPort=179, SrcPort=Any    (encoded: 0.6.0.179,0.6.0.0/16)
Proto=89, DestPort=Any, SrcPort=Any    (encoded: 0.89.0.0/16,0.89.0.0/16)

Name: 1_131075-ov-v6-1
Type: hash:oservice (Match un-translated Ports)
Revision: 2
Header: family inet hashsize 64 maxelem 65536
Size in memory: 704
References: 1
Number of entries: 2
Members:
Proto=89, DestPort=Any, SrcPort=Any    (encoded: 0.89.0.0/16,0.89.0.0/16)
Proto=6, DestPort=179, SrcPort=Any    (encoded: 0.6.0.179,0.6.0.0/16)
```

3 Activez la journalisation sur une règle de pare-feu particulière à l'aide de l'API REST ou de l'interface utilisateur Edge, puis surveillez les journaux avec la commande `show log follow`.

Si des journaux ne sont pas visibles, activez la journalisation sur la règle `DROP Invalid` à l'aide de l'API REST suivante.

```
URL : https://NSX_Manager_IP/api/4.0/edges/{edgeId}/firewall/config/global

PUT Method
Input representation
<globalConfig>   <!-- Optional -->
<tcpPickOngoingConnections>false</tcpPickOngoingConnections>   <!-- Optional. Defaults to false --
>
<tcpAllowOutOfWindowPackets>false</tcpAllowOutOfWindowPackets>    <!-- Optional. Defaults to
false -->
<tcpSendResetForClosedVsePorts>true</tcpSendResetForClosedVsePorts>    <!-- Optional. Defaults to
true -->
<dropInvalidTraffic>true</dropInvalidTraffic>    <!-- Optional. Defaults to true -->
<logInvalidTraffic>true</logInvalidTraffic>     <!-- Optional. Defaults to false -->
<tcpTimeoutOpen>30</tcpTimeoutOpen>       <!-- Optional. Defaults to 30 -->
<tcpTimeoutEstablished>3600</tcpTimeoutEstablished>   <!-- Optional. Defaults to 3600 -->
<tcpTimeoutClose>30</tcpTimeoutClose>   <!-- Optional. Defaults to 30 -->
<udpTimeout>60</udpTimeout>             <!-- Optional. Defaults to 60 -->
<icmpTimeout>10</icmpTimeout>           <!-- Optional. Defaults to 10 -->
<icmp6Timeout>10</icmp6Timeout>           <!-- Optional. Defaults to 10 -->
<ipGenericTimeout>120</ipGenericTimeout>    <!-- Optional. Defaults to 120 -->
</globalConfig>
Output representation
No payload
```

Utilisez la commande `show log follow` pour rechercher les journaux semblables à :

```
2016-04-18T20:53:31+00:00 edge-0 kernel: nf_ct_tcp: invalid TCP flag combination IN= OUT=
SRC=172.16.1.4 DST=192.168.1.4 LEN=40 TOS=0x00 PREC=0x00 TTL=64 ID=43343 PROTO=TCP
SPT=5050 DPT=80 SEQ=0 ACK=1572141176 WINDOW=512 RES=0x00 URG PSH FIN URGP=0
2016-04-18T20:53:31+00:00 edge-0 kernel: INVALID IN= OUT=vNic_1 SRC=172.16.1.4
DST=192.168.1.4 LEN=40 TOS=0x00 PREC=0x00 TTL=63 ID=43343 PROTO=TCP SPT=5050 DPT=80
WINDOW=512 RES=0x00 URG PSH FIN URGP=0
```

4 Recherchez les connexions correspondantes dans la table d'état de pare-feu Edge avec la commande `show flowtable rule_id` :

```
nsxedge> show flowtable
1: tcp  6 21554 ESTABLISHED src=192.168.110.10 dst=192.168.5.3 sport=25981
d port=22 pkts=52 bytes=5432 src=192.168.5.3 dst=192.168.110.10 sport=22 dport=259
81 pkts=44 bytes=7201 [ASSURED] mark=0 rid=131073 use=1
2: tcp  6 21595 ESTABLISHED src=127.0.0.1 dst=127.0.0.1 sport=53194
dport=10 001 pkts=33334 bytes=11284650 src=127.0.0.1 dst=127.0.0.1 sport=10001 dport=5319
4 pkts=33324 bytes=1394146 [ASSURED] mark=0 rid=0 use=1
```

Comparez le nombre de connexions actives et le nombre maximal autorisé avec la commande `show flowstats` :

```
nsxedge> show flowstats
Total Flow Capacity: 65536
Current Statistics :
cpu=0 searched=3280373 found=3034890571 new=52678 invalid=659946 ignore=77605
delete=52667 delete_list=49778 insert=49789 insert_failed=0 drop=0 early_drop=0
error=0 search_restart=0
```

5 Consultez les journaux Edge avec la commande `show log follow` et recherchez les rejets d'ALG. Recherchez des chaînes semblables à `tftp_alg`, `msrpc_alg` ou `oracle_tns`. Pour plus d'informations, consultez :

- https://kb.vmware.com/kb/2126674
- https://kb.vmware.com/kb/2137751

Problèmes de connectivité de routage Edge

1 Initiez un trafic contrôlé à partir d'un client à l'aide de la commande `ping <destination_IP_address>`.

2 Capturez le trafic simultanément sur les deux interfaces, écrivez la sortie dans un fichier et exportez-la à l'aide de SCP.

Par exemple :

Capturez le trafic sur l'interface d'entrée avec cette commande :

```
debug packet display interface vNic_0 -n_src_host_1.1.1.1
```

Capturez le trafic sur l'interface de sortie avec cette commande :

```
debug packet display interface vNic_1 -n_src_host_1.1.1.1
```

Pour la capture de paquets simultanée, utilisez l'utilitaire de capture de paquets ESXi `pktcap-uw` dans ESXi. Reportez-vous à la section https://kb.vmware.com/kb/2051814.

Si les rejets de paquets sont cohérents, recherchez les erreurs de configuration liées aux éléments suivants :

- Adresses IP et itinéraires
- Règles de pare-feu ou règles NAT
- Routage asymétrique
- Vérifications de filtre RP

a Vérifiez l'adresse IP et les sous-réseaux de l'interface avec la commande `show interface`.

b Si des itinéraires sont manquants au niveau du plan de données, exécutez ces commandes :

- `show ip route`
- `show ip route static`
- `show ip route bgp`
- `show ip route ospf`

c Consultez la table de routage des itinéraires nécessaires en exécutant la commande `show ip forwarding`.

d Si vous disposez de plusieurs chemins d'accès, exécutez la commande `show rpfilter`.

```
nsxedge> show rpfilter
net.ipv4.conf.VDR.rp_filter = 0
net.ipv4.conf.all.rp_filter = 0
net.ipv4.conf.br-sub.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.lo.rp_filter = 0
net.ipv4.conf.vNic_0.rp_filter = 1
net.ipv4.conf.vNic_1.rp_filter = 1
net.ipv4.conf.vNic_2.rp_filter = 1
net.ipv4.conf.vNic_3.rp_filter = 1
net.ipv4.conf.vNic_4.rp_filter = 1
net.ipv4.conf.vNic_5.rp_filter = 1
net.ipv4.conf.vNic_6.rp_filter = 1
net.ipv4.conf.vNic_7.rp_filter = 1
net.ipv4.conf.vNic_8.rp_filter = 1
net.ipv4.conf.vNic_9.rp_filter = 1

nsxedge> show rpfstats
RPF drop packet count: 484
```

Pour rechercher les statistiques RPF, exécutez la commande `show rpfstats`.

```
nsxedge> show rpfstats
RPF drop packet count: 484
```

Si les rejets de paquets s'affichent de manière aléatoire, recherchez les limites de ressources :

a Pour l'utilisation du CPU ou de la mémoire, exécutez ces commandes :

- `show system cpu`
- `show system memory`
- `show system storage`
- `show process monitor`
- `top`

  Pour ESXi, exécutez la commande `esxtop n`.

```
PCPU USED(%): 2.5 5.0 3.7  77 AVG:  22
PCPU UTIL(%): 0.5 2.7 3.3  92 AVG:  24

      ID      GID NAME             NWLD   %USED    %RUN    %SYS   %WAIT
98255269 98255269 esxtop.11224149     1   67.04   69.86    0.00    6.26
       2        2 system             139    3.03    4.61    0.00 12053.58
   86329    86329 app-01a              6    0.69    0.57    0.00  466.09
   78730    78730 db-01a               6    0.48    0.67    0.00  441.44
   90486    90486 app-02a              6    0.38    0.32    0.00  463.42

 %VMWAIT    %RDY    %IDLE    %OVRLP    %CSTP   %MLMTD    %SWPWT
 11.01       -    0.39    0.00    0.09    0.00    0.00    0.00
 600.00   53.81    0.10   93.13    0.00    0.00    0.00    0.00
 13900.00       -   28.68    0.00    2.69    0.00    0.00    0.00
 600.00   53.81    0.10   93.13    0.00    0.00    0.00    0.00
 600.00    0.00    0.19  151.92    0.00    0.00    0.00    0.00
```

Problèmes de communication entre NSX Manager et Edge

NSX Manager communique avec NSX Edge via VIX ou le bus de messages. Ce choix est fait par NSX Manager lorsque le dispositif Edge est déployé. Il ne change jamais.

Note VIX n'est pas pris en charge dans NSX 6.3.0 et versions ultérieures.

VIX

- VIX est utilisé pour NSX Edge si l'hôte ESXi n'est pas préparé.
- NSX Manager obtient les informations d'identification de l'hôte de la part de vCenter Server pour se connecter à l'hôte ESXi en premier.
- NSX Manager utilise les informations d'identification d'Edge pour se connecter au dispositif Edge.
- Le processus `vmtoolsd` sur le dispositif Edge gère la communication de VIX.

Des échecs de VIX se produisent pour les raisons suivantes :

- NSX Manager ne peut pas communiquer avec vCenter Server.
- NSX Manager ne peut pas communiquer avec les hôtes ESXi.
- Il existe des problèmes internes NSX Manager.
- Il existe des problèmes internes Edge.

Débogage de VIX

Recherchez les erreurs de VIX VIX_E_<error> dans les journaux de NSX Manager pour limiter la cause. Recherchez les erreurs semblables à :

```
Vix Command 1126400 failed, reason com.vmware.vshield.edge.exception.VixException: vShield
Edge:10013:Error code 'VIX_E_FILE_NOT_FOUND' was returned by VIX API.:null

Health check failed for edge  edge-13 VM vm-5025 reason:
com.vmware.vshield.edge.exception.VixException: vShield Edge:10013:Error code
'VIX_E_VM_NOT_RUNNING' was returned by VIX API.:null
```

En général, si le même problème se produit pour plusieurs dispositifs Edge en même temps, il n'est pas du côté du dispositif Edge.

Débogage du bus de messages

Le bus de messages est utilisé pour la communication de NSX Edge lorsque des hôtes ESXi sont préparés.

Lorsque vous rencontrez des problèmes, les journaux de NSX Manager peuvent contenir des entrées semblables à la suivante :

```
GMT ERROR taskScheduler-6 PublishTask:963 - Failed to configure VSE-vm index 0, vm-id vm-117,
edge edge-5. Error: RPC request timed out
```

Ce problème se produit si :

- Le dispositif Edge est défectueux
- La connexion du bus de messages est rompue

Pour diagnostiquer le problème sur le dispositif Edge :

- Pour vérifier la connectivité rmq, exécutez cette commande :

  ```
  nsxedge> show messagebus messages
  ------------------------
  Message bus is enabled
  cmd conn state : listening
  init_req       : 1
  init_resp      : 1
  init_req_err   : 0
  ...
  ```

- Pour vérifier la connectivité vmci, exécutez cette commande :

  ```
  nsxedge> show messagebus forwarder
  ------------------------
  Forwarder Command Channel
  ```

```
vmci_conn          : up
app_client_conn    : up
vmci_rx            : 3649
vmci_tx            : 3648
vmci_rx_err        : 0
vmci_tx_err        : 0
vmci_closed_by_peer: 8
vmci_tx_no_socket  : 0
app_rx             : 3648
app_tx             : 3649
app_rx_err         : 0
app_tx_err         : 0
app_conn_req       : 1
app_closed_by_peer : 0
app_tx_no_socket   : 0
------------------------
Forwarder Event Channel
vmci_conn          : up
app_client_conn    : up
vmci_rx            : 1143
vmci_tx            : 13924
vmci_rx_err        : 0
vmci_tx_err        : 0
vmci_closed_by_peer: 0
vmci_tx_no_socket  : 0
app_rx             : 13924
app_tx             : 1143
app_rx_err         : 0
app_tx_err         : 0
app_conn_req       : 1
app_closed_by_peer : 0
app_tx_no_socket   : 0
------------------------
cli_rx             : 1
cli_tx             : 1
cli_tx_err         : 0
counters_reset     : 0
```

Dans l'exemple, la sortie `vmci_closed_by_peer: 8` indique le nombre de fois que la connexion a été fermée par l'agent hôte. Si ce nombre augmente et que `vmci conn` est inactif, l'agent hôte ne peut pas se connecter au broker RMQ. Dans `show log follow`, recherchez les erreurs répétées dans les journaux Edge : `VmciProxy: [daemon.debug] VMCI Socket is closed by peer`

Pour diagnostiquer le problème sur l'hôte ESXi :

- Pour vérifier si l'hôte ESXi se connecte au broker RMQ, exécutez cette commande :

```
esxcli network ip connection list | grep 5671

tcp   0   0  10.32.43.4:43329  10.32.43.230:5671    ESTABLISHED     35854  newreno
vsfwd
tcp   0   0  10.32.43.4:52667  10.32.43.230:5671    ESTABLISHED     35854  newreno
```

```
vsfwd
tcp   0   0  10.32.43.4:20808  10.32.43.230:5671    ESTABLISHED     35847  newreno
vsfwd
tcp   0   0  10.32.43.4:12486  10.32.43.230:5671    ESTABLISHED     35847  newreno  vsfwd
```

Diagnostic et récupération du dispositif Edge

Diagnostic Edge

- Vérifiez si `vmtoolsd` est exécuté avec cette commande :

```
nsxedge> show process list
Perimeter-Gateway-01-0> show process list
%CPU %MEM    VSZ   RSZ STAT  STARTED     TIME COMMAND
 0.0  0.1   4244   720 Ss     May 16 00:00:15 init [3]
...
 0.0  0.1   4240   640 S      May 16 00:00:00 logger -p daemon debug -t vserrdd
 0.2  0.9  57192  4668 S      May 16 00:23:07 /usr/local/bin/vmtoolsd --plugin-pa
 0.0  0.4   4304  2260 SLs    May 16 00:01:54 /usr/sbin/watchdog
 ...
```

- Vérifiez si Edge est dans un bon état en exécutant cette commande :

```
nsxedge> show eventmgr
------------------------
messagebus     : enabled
debug          : 0
profiling      : 0
cfg_rx         : 1
cfg_rx_msgbus  : 0
...
```

  Utilisez la commande `show eventmgr` pour vérifier que la commande de requête est reçue et traitée.

```
nsxedge> show eventmgr
------------------------
messagebus     : enabled
debug          : 0
profiling      : 0
cfg_rx         : 1
cfg_rx_msgbus  : 0
cfg_rx_err     : 0
cfg_exec_err   : 0
cfg_resp       : 0
cfg_resp_err   : 0
cfg_resp_ln_err: 0
fastquery_rx : 0 fastquery_err : 0
clearcmd_rx    : 0
clearcmd_err   : 0
ha_rx          : 0
```

```
ha_rx_err      : 0
ha_exec_err    : 0
status_rx      : 16
status_rx_err  : 0
status_svr     : 10
status_evt     : 0
status_evt_push: 0
status_ha      : 0
status_ver     : 1
status_sys     : 5
status_cmd     : 0
status_svr_err : 0
status_evt_err : 0
status_sys_err : 0
status_ha_err  : 0
status_ver_err : 0
status_cmd_err : 0
evt_report     : 1
evt_report_err : 0
hc_report      : 10962
hc_report_err  : 0
cli_rx         : 2
cli_resp       : 1
cli_resp_err   : 0
counter_reset  : 0
---------- Health Status -------------
system status  : good
ha state       : active
cfg version    : 7
generation     : 0
server status  : 1
syslog-ng      : 1
haproxy        : 0
ipsec          : 0
sslvpn         : 0
l2vpn          : 0
dns            : 0
dhcp           : 0
heartbeat      : 0
monitor        : 0
gslb           : 0
---------- System Events -------------
```

Récupération du dispositif Edge

Si le processus `vmtoolsd` n'est pas exécuté ou si le dispositif NSX Edge est défectueux, redémarrez le dispositif Edge.

Pour récupérer d'une panne, un redémarrage devrait suffire. Un redéploiement ne devrait pas être nécessaire.

Note Notez toutes les informations de connexion de l'ancien dispositif Edge lorsqu'un redéploiement est terminé.

Pour déboguer une panne du noyau, vous devez obtenir :

- Le fichier vmss (interrompre la VM) ou vmsn (snapshot de VM) de la VM Edge tandis qu'elle est toujours bloquée. S'il existe un fichier vmem, il est également nécessaire. Il peut être utilisé pour extraire un fichier de vidage de mémoire du noyau, que le support VMware peut analyser.
- Le journal de support Edge, généré juste après le redémarrage du dispositif Edge bloqué (mais qui n'est pas redéployé). Vous pouvez également consulter les journaux Edge. Reportez-vous à la section https://kb.vmware.com/kb/2079380.
- Une capture d'écran de la console Edge est également utile, même si en général elle ne contient pas le rapport d'incident complet.

Dépannage du pare-feu 5

Cette section fournit des informations sur le dépannage des problèmes de pare-feu.

Ce chapitre contient les rubriques suivantes :

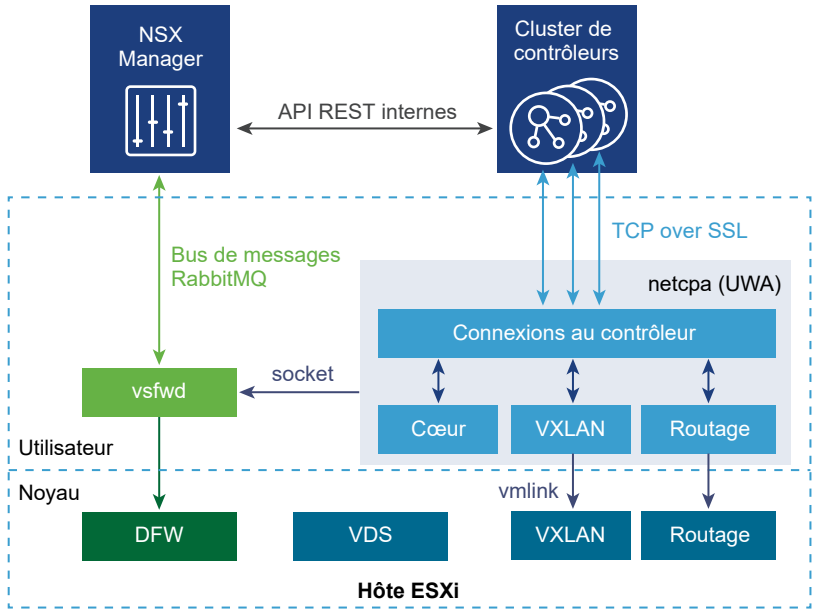
À propos du pare-feu distribué

Un bus de messages RabbitMQ est exploité à des fins de communication entre vsfwd (client RMQ) et le processus serveur RMQ hébergé sur NSX Manager. Le bus de messages est utilisé par NSX Manager pour envoyer diverses informations aux hôtes ESXi, notamment des règles de stratégie devant être programmées sur le pare-feu distribué dans le noyau.

Le pare-feu distribué NSX est un pare-feu hyperviseur à noyau intégré qui fournit une visibilité et un contrôle des charges de travail et des réseaux virtualisés. Vous pouvez créer des stratégies de contrôle d'accès basées sur des objets VMware vCenter, comme des centres de données et des clusters, des noms et des balises de machines virtuelles, des constructions réseau, telles que des adresses IP/VLAN/VXLAN, ainsi que des identités de groupe d'Active Directory. Une stratégie de contrôle d'accès cohérente est maintenant appliquée lorsqu'une machine virtuelle est migrée par vMotion entre des hôtes physiques, sans qu'il soit nécessaire de réécrire les règles de pare-feu. Comme le pare-feu distribué est intégré dans un hyperviseur, il fournit un débit proche de celui de la ligne afin de permettre une consolidation de charge de travail plus importante sur les serveurs physiques. La nature distribuée du pare-feu fournit une architecture évolutive qui étend automatiquement la capacité du pare-feu lorsque des hôtes supplémentaires sont ajoutés à un centre de données.

L'application Web NSX Manager et les composants de NSX sur des hôtes ESXi communiquent entre eux via un processus de broker RabbitMQ qui s'exécute sur la même machine virtuelle que l'application Web NSX Manager. Le protocole de communication utilisé est le protocole AMQP (Advanced Message Queueing Protocol) et le canal est sécurisé par SSL. Sur un hôte ESXi, le processus VSFWD (vShield Firewall Daemon) établit et maintient la connexion SSL avec le broker. Il envoie et reçoit des messages au nom d'autres composants, qui lui parlent via IPC.

Figure 5-1. Schéma de l'utilisateur hôte et de l'espace du noyau ESXi



Commandes de l'interface de ligne de commande pour DFW

Vous pouvez obtenir des informations sur les pare-feu distribués sur l'interface de ligne de commande centrale de NSX Manager.

Utilisation des commandes de l'interface de ligne de commande centrale `Show dfw`

Voici le chemin à suivre pour accéder aux informations souhaitées :

1 Connectez-vous à l'interface de ligne de commande centrale de NSX Manager à l'aide des informations d'identification *admin*.

2 Exécutez les commandes suivantes :

   a Exécutez la commande `show cluster all` pour afficher tous les clusters.

```
nsxmgr>show cluster all
No.  Cluster Name               Cluster Id     Datacenter Name     Firewall Status
1    Compute Cluster A          domain-c33     Datacenter Site A   Enabled
2    Management & Edge Cluster  domain-c41     Datacenter Site A   Enabled
```

b Exécutez la commande `show cluster <clusterID>` pour afficher les hôtes d'un cluster spécifique.

```
nsxmgr> show cluster domain-c33
Datacenter: Datacenter Site A
Cluster: Compute Cluster A
No.  Host Name            Host Id         Installation Status
1    esx-02a.corp.local   host-32          Enabled
2    esx-01a.corp.local   host-28          Enabled
```

c Exécutez la commande `show host <hostID>` pour afficher toutes les machines virtuelles sur un hôte.

```
nsxmgr> show host host-28
Datacenter: Datacenter Site A
Cluster: Compute Cluster A
Host: esx-01a.corp.local
No.  VM Name    VM Id     Power Status
1    web-02a    vm-219    on
2    web-01a    vm-216    on
3    win8-01a   vm-206    off
4    app-02a    vm-264    on
```

d Exécutez la commande `show vm <vmID>` pour afficher les informations d'une machine virtuelle, qui incluent les noms de filtre et les ID de vNIC :

```
nsxmgr> show vm vm-264
Datacenter: Datacenter Site A
Cluster: Compute Cluster A
Host: esx-01a.corp.local
Host-ID: host-28
VM: app-02a
Virtual Nics List:
1.
Vnic Name      app-02a - Network adapter 1
Vnic Id        502ef2fa-62cf-d178-cb1b-c825fb300c84.000
Filters        nic-79396-eth0-vmware-sfw.2
```

e Notez l'ID de vNIC et exécutez d'autres commandes telles que `show dfw vnic <vnicID>` et `show dfw host <hostID> filter <filter ID> rules` :

```
nsxmgr> show dfw vnic 502ef2fa-62cf-d178-cb1b-c825fb300c84.000
Vnic Name      app-02a - Network adapter 1
Vnic Id        502ef2fa-62cf-d178-cb1b-c825fb300c84.000
Mac Address    00:50:56:ae:6c:6b
Port Group Id  dvportgroup-385
Filters        nic-79396-eth0-vmware-sfw.2
```

```
nsxmgr> show dfw host host-28 filter nic-79396-eth0-vmware-sfw.2 rules
ruleset domain-c33 {
  # Filter rules
  rule 1012 at 1 inout protocol any from addrset ip-securitygroup-10 to addrset ip-
securitygroup-10 drop with log;
  rule 1013 at 2 inout protocol any from addrset src1013 to addrset src1013 drop;
  rule 1011 at 3 inout protocol tcp from any to addrset dst1011 port 443 accept;
  rule 1011 at 4 inout protocol icmp icmptype 8 from any to addrset dst1011 accept;
  rule 1010 at 5 inout protocol tcp from addrset ip-securitygroup-10 to addrset ip-
securitygroup-11 port 8443 accept;
  rule 1010 at 6 inout protocol icmp icmptype 8 from addrset ip-securitygroup-10 to addrset
ip-securitygroup-11 accept;
  rule 1009 at 7 inout protocol tcp from addrset ip-securitygroup-11 to addrset ip-
securitygroup-12 port 3306 accept;
  rule 1009 at 8 inout protocol icmp icmptype 8 from addrset ip-securitygroup-11 to addrset
ip-securitygroup-12 accept;
  rule 1003 at 9 inout protocol ipv6-icmp icmptype 136 from any to any accept;
  rule 1003 at 10 inout protocol ipv6-icmp icmptype 135 from any to any accept;
  rule 1002 at 11 inout protocol udp from any to any port 67 accept;
  rule 1002 at 12 inout protocol udp from any to any port 68 accept;
  rule 1001 at 13 inout protocol any from any to any accept;
}

ruleset domain-c33_L2 {
  # Filter rules
  rule 1004 at 1 inout ethertype any from any to any accept;
}
```

Utilisation de la commande de l'interface de ligne de commande centrale `export host-tech-support`

La commande `export host-tech-support` vous permet d'exporter un bundle de support d'un hôte ESXi vers un serveur spécifié. De plus, cette commande collecte des sorties et des fichiers liés à NSX (non limités à ce qui suit) sur des hôtes définis tels que :

- Fichiers journaux de VMKernel et vsfwd
- Liste de filtres
- Liste de règles DFW
- Liste de conteneurs
- Détails de SpoofGuard
- Informations liées à l'hôte
- Informations liées à la découverte d'adresses IP
- Résultats de commande RMQ
- Détails des groupes de sécurité, des profils de services et des instances
- Sorties liées à l'interface de ligne de commande ESX

Cette commande supprime également tous les fichiers temporaires sur NSX Manager.

Pour collecter les sorties et les fichiers liés à NSX :

1 Connectez-vous à l'interface de ligne de commande centrale de NSX Manager à l'aide des informations d'identification *admin*.

2 Exécutez les commandes suivantes :

   a `show cluster all` : pour trouver l'ID d'hôte requis.

   b `export host-tech-support host-id scp uid@ip:/path` : pour générer le bundle de support technique de NSX et pour le copier sur un serveur spécifié.

Pour plus d'informations, consultez :

- Référence rapide des lignes de commande de NSX.
- *Référence de l'interface de ligne de commandes de NSX*.

Dépannage du pare-feu distribué

Cette rubrique contient des informations pour comprendre et dépanner le pare-feu distribué VMware NSX 6.x .

Problème

- La publication de règles du pare-feu distribué échoue.
- La mise à jour de règles pare-feu distribué échoue.

Cause

Vérifiez que chaque étape du dépannage ci-dessous est correcte pour votre environnement. Chaque étape fournit des instructions ou un lien vers un document afin d'éliminer les causes possibles et de prendre une mesure corrective si nécessaire. Les étapes sont classées dans l'ordre le plus approprié afin d'isoler le problème et d'identifier la bonne résolution. Après chaque étape, réessayez de mettre à jour/publier les règles du pare-feu distribué.

Solution

1 Vérifiez que les VIB de NSX sont correctement installées sur chaque hôte ESXi du cluster. Pour ce faire, sur chaque hôte ESXi du cluster, exécutez ces commandes.

```
# esxcli software vib list | grep vsip
esx-vsip                       6.0.0-0.0.4744062  VMware  VMwareCertified   2017-01-04

# esxcli software vib list | grep vxlan
esx-vxlan                      6.0.0-0.0.4744062  VMware  VMwareCertified   2017-01-04
```

Les versions de NSX antérieures à la version 6.2 ont une VIB supplémentaire :

```
# esxcli software vib list | grep dvfilter

esx-dvfilter-switch-security   5.5.0-0.0.2318233  VMware  VMwareCertified   2015-01-24
```

À partir de NSX 6.3.3 avec ESXi 6.0 ou version ultérieure, les VIB esx-vxlan et esx-vsip sont remplacés par esx-nsxv.

```
# esxcli software vib list | grep nsxv
esx-nsxv                       6.0.0-0.0.6216823  VMware  VMwareCertified   2017-08-10
```

2 Sur les hôtes ESXi, vérifiez que le service vShield-Stateful-Firewall est en cours d'exécution.

Par exemple :

```
# /etc/init.d/vShield-Stateful-Firewall status

vShield-Stateful-Firewall is running
```

3 Vérifiez que le bus de messages communique correctement avec NSX Manager.

Le script de surveillance lance automatiquement le processus et le redémarre s'il se termine pour une raison inconnue. Exécutez cette commande sur chaque hôte ESXi du cluster.

Par exemple :

```
# ps | grep vsfwd

107557 107557 vsfwd /usr/lib/vmware/vsfw/vsfwd
```

Au moins 12 processus vsfwd doivent être en cours d'exécution dans la sortie de commande. Si un nombre inférieur de processus (seulement 2 dans le cas le plus probable) est en cours d'exécution, vsfwd ne fonctionne pas correctement.

4 Vérifiez que le port 5671 est ouvert pour les communications dans la configuration de pare-feu.

Cette commande indique la connectivité VSFWD avec le broker RabbitMQ. Exécutez cette commande sur des hôtes ESXi pour voir une liste de connexions depuis le processus vsfwd sur l'hôte ESXi vers NSX Manager. Vérifiez que le port 5671 est ouvert pour les communications sur l'un des pare-feu externes sur l'environnement. De plus, il doit y avoir au moins deux connexions sur le port 5671. Il peut y avoir davantage de connexions sur le port 5671, car des machines virtuelles NSX Edge sont déployées sur l'hôte ESXi et elles établissent également des connexions avec le broker RMQ.

Par exemple :

```
# esxcli network ip connection list |grep 5671

tcp         0       0  192.168.110.51:30133           192.168.110.15:5671   ESTABLISHED
10949155  newreno  vsfwd
tcp         0       0  192.168.110.51:39156           192.168.110.15:5671   ESTABLISHED
10949155  newreno  vsfwd
```

5 Vérifiez que VSFWD est configuré.

Cette commande doit afficher l'adresse IP de NSX Manager.

```
# esxcfg-advcfg -g /UserVars/RmqIpAddress
```

6 Si vous utilisez un profil d'hôte pour cet hôte ESXi, vérifiez que la configuration RabbitMQ n'est pas définie dans le profil d'hôte.

Consultez :

- https://kb.vmware.com/kb/2092871
- https://kb.vmware.com/kb/2125901

7 Vérifiez que les informations d'identification RabbitMQ de l'hôte ESXi sont désynchronisées avec NSX Manager. Téléchargez les journaux de support technique de NSX Manager. Après avoir rassemblé tous les journaux de support technique de NSX Manager, recherchez dans tous les journaux les entrées semblables à ce qui suit :

Remplacez host-420 par l'ID d'hôte de l'hôte suspect.

```
PLAIN login refused: user 'uw-host-420' - invalid credentials.
```

8 Si ce type d'entrée est trouvé dans les journaux de l'hôte ESXi suspect, resynchronisez le bus de messages.

Pour resynchroniser le bus de messages, utilisez l'API REST. Pour mieux comprendre le problème, collectez les journaux immédiatement après la resynchronisation du bus de messages.

```
HTTP Method : POST
Headers ,
Authorization : base64encoded value of username password
Accept : application/xml
Content-Type : application/xml
Request:

POST https://NSX_Manager_IP/api/2.0/nwfabric/configure?action=synchronize

Request Body:

<nwFabricFeatureConfig>
<featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
<resourceConfig>
<resourceId>{HOST/CLUSTER MOID}</resourceId>
</resourceConfig>
</nwFabricFeatureConfig>
```

9 Utilisez la commande `export host-tech-support <host-id> scp <uid@ip:/path>` pour rassembler des journaux de pare-feu spécifiques de l'hôte.

Par exemple :

```
nsxmgr# export host-tech-support host-28 scp Administrator@192.168.110.10
Generating logs for Host: host-28...
```

10 Utilisez la commande `show dfw host host-id summarize-dvfilter` pour vérifier que toutes les règles de pare-feu sont déployées sur un hôte et appliquées aux machines virtuelles.

Dans la sortie, `module: vsip` indique que le module DFW est chargé et en cours d'exécution. `name` indique le pare-feu exécuté sur chaque vNic.

Vous pouvez obtenir les ID d'hôte en exécutant la commande `show dfw cluster all` pour obtenir les ID de domaine du cluster, puis la commande `show dfw cluster domain-id` pour obtenir les ID d'hôte.

Par exemple :

```
# show dfw host host-28 summarize-dvfilter

Fastpaths:
agent: dvfilter-faulter, refCount: 1, rev: 0x1010000, apiRev: 0x1010000, module: dvfilter
agent: ESXi-Firewall, refCount: 5, rev: 0x1010000, apiRev: 0x1010000, module: esxfw
agent: dvfilter-generic-vmware, refCount: 1, rev: 0x1010000, apiRev: 0x1010000, module: dvfilter-
generic-fastpath
agent: dvfilter-generic-vmware-swsec, refCount: 4, rev: 0x1010000, apiRev: 0x1010000, module:
dvfilter-switch-security
agent: bridgelearningfilter, refCount: 1, rev: 0x1010000, apiRev: 0x1010000, module: vdrb
agent: dvfg-igmp, refCount: 1, rev: 0x1010000, apiRev: 0x1010000, module: dvfg-igmp
agent: vmware-sfw, refCount: 4, rev: 0x1010000, apiRev: 0x1010000, module: vsip

Slowpaths:

Filters:
world 342296 vmm0:2-vm_RHEL63_srv_64-shared-846-3f435476-8f54-4e5a-8d01-59654a4e9979 vcUuid:'3f
43 54 76 8f 54 4e 5a-8d 01 59 65 4a 4e 99 79'
 port 50331660 2-vm_RHEL63_srv_64-shared-846-3f435476-8f54-4e5a-8d01-59654a4e9979.eth1
  vNic slot 2
   name: nic-342296-eth1-vmware-sfw.2
   agentName: vmware-sfw
   state: IOChain Attached
   vmState: Detached
   failurePolicy: failClosed
   slowPathID: none
   filter source: Dynamic Filter Creation
  vNic slot 1
   name: nic-342296-eth1-dvfilter-generic-vmware-swsec.1
   agentName: dvfilter-generic-vmware-swsec
   state: IOChain Attached
   vmState: Detached
```

```
   failurePolicy: failClosed
   slowPathID: none
   filter source: Alternate Opaque Channel
 port 50331661 (disconnected)
  vNic slot 2
   name: nic-342296-eth2-vmware-sfw.2 <======= DFW filter
   agentName: vmware-sfw
   state: IOChain Detached
   vmState: Detached
   failurePolicy: failClosed
   slowPathID: none
   filter source: Dynamic Filter Creation
 port 33554441 2-vm_RHEL63_srv_64-shared-846-3f435476-8f54-4e5a-8d01-59654a4e9979
  vNic slot 2
   name: nic-342296-eth0-vmware-sfw.2<========= DFW filter
   agentName: vmware-sfw
   state: IOChain Attached
   vmState: Detached
   failurePolicy: failClosed
   slowPathID: none
   filter source: Dynamic Filter Creation
```

11 Exécutez la commande `show dfw host hostID filter filterID rules`.

Par exemple :

```
# show dfw host host-28 filter nic-79396-eth0-vmware-sfw.2 rules

ruleset domain-c33 {
  # Filter rules
  rule 1012 at 1 inout protocol any from addrset ip-securitygroup-10 to addrset ip-
securitygroup-10 drop with log;
  rule 1013 at 2 inout protocol any from addrset src1013 to addrset src1013 drop;
  rule 1011 at 3 inout protocol tcp from any to addrset dst1011 port 443 accept;
  rule 1011 at 4 inout protocol icmp icmptype 8 from any to addrset dst1011 accept;
  rule 1010 at 5 inout protocol tcp from addrset ip-securitygroup-10 to addrset ip-
securitygroup-11 port 8443 accept;
  rule 1010 at 6 inout protocol icmp icmptype 8 from addrset ip-securitygroup-10 to addrset ip-
securitygroup-11 accept;
  rule 1009 at 7 inout protocol tcp from addrset ip-securitygroup-11 to addrset ip-
securitygroup-12 port 3306 accept;
  rule 1009 at 8 inout protocol icmp icmptype 8 from addrset ip-securitygroup-11 to addrset ip-
securitygroup-12 accept;
  rule 1003 at 9 inout protocol ipv6-icmp icmptype 136 from any to any accept;
  rule 1003 at 10 inout protocol ipv6-icmp icmptype 135 from any to any accept;
  rule 1002 at 11 inout protocol udp from any to any port 67 accept;
  rule 1002 at 12 inout protocol udp from any to any port 68 accept;
  rule 1001 at 13 inout protocol any from any to any accept;
}

ruleset domain-c33_L2 {
  # Filter rules
  rule 1004 at 1 inout ethertype any from any to any accept;
```

12 Exécutez la commande `show dfw host hostID filter filterID addrsets`.

Par exemple :

```
# show dfw host host-28 filter nic-342296-eth2-vmware-sfw.2 addrsets

addrset dst1011 {
ip 172.16.10.10,
ip 172.16.10.11,
ip 172.16.10.12,
ip fe80::250:56ff:feae:3e3d,
ip fe80::250:56ff:feae:f86b,
}
addrset ip-securitygroup-10 {
ip 172.16.10.11,
ip 172.16.10.12,
ip fe80::250:56ff:feae:3e3d,
ip fe80::250:56ff:feae:f86b,
}
addrset ip-securitygroup-11 {
ip 172.16.20.11,
ip fe80::250:56ff:feae:23b9,
}
addrset ip-securitygroup-12 {
ip 172.16.30.11,
ip fe80::250:56ff:feae:d42b,
}
addrset src1013 {
ip 172.16.10.12,
ip 172.17.10.11,
ip fe80::250:56ff:feae:cf88,
ip fe80::250:56ff:feae:f86b,
}
```

13 Si vous avez validé toutes les étapes de dépannage ci-dessus, mais que vous ne pouvez pas publier des règles de pare-feu sur les machines virtuelles hôtes, exécutez une synchronisation forcée de niveau hôte via l'interface utilisateur de NSX Manager ou via l'appel API REST suivant.

```
URL : [https:]https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>
HTTP Method : POST
Headers ,
Authorization : base64encoded value of username password
Accept : application/xml
Content-Type : application/xml
```

Solution

Remarques :

- Vérifiez que VMware Tools est exécuté sur les machines virtuelles si des règles de pare-feu n'utilisent pas d'adresses IP. Pour plus d'informations, consultez https://kb.vmware.com/kb/2084048.

VMware NSX 6.2.0 introduit la possibilité de découvrir l'adresse IP de la machine virtuelle en utilisant l'écoute DHCP ou l'écoute ARP. Ces nouveaux mécanismes de découverte permettent à NSX de mettre en application les règles de sécurité basées sur l'adresse IP pour les machines virtuelles sur lesquelles VMware Tools n'est pas installé. Pour plus d'informations, consultez les notes de mise à jour de NSX 6.2.0.

DFW est activé dès que le processus de préparation de l'hôte est terminé. Si une machine virtuelle n'a pas du tout besoin d'un service DFW, elle peut être ajoutée à la liste d'exclusion (par défaut, NSX Manager, les instances de NSX Controller et les passerelles ESG sont automatiquement exclus de la fonction DFW). Il est possible que l'accès de vCenter Server soit bloqué après la création d'une règle Refuser tout dans DFW. Pour plus d'informations, consultez https://kb.vmware.com/kb/2079620.

- Lors du dépannage du pare-feu distribué VMware NSX 6.x avec le support technique VMware, les éléments suivants sont requis :
  - Sortie de la commande `show dfw host hostID summarize-dvfilter` sur chaque hôte ESXi du cluster.
  - Configuration du pare-feu distribué dans l'onglet **Networking and Security > Pare-feu > Général (Networking and Security > Firewall > General)** et clic sur **Exporter la configuration (Export Configuration)**. Cela exporte la configuration du pare-feu distribué au format XML.
  - Journaux de NSX Manager. Pour plus d'informations, consultez https://kb.vmware.com/kb/2074678.
  - Journaux de vCenter Server. Pour plus d'informations, consultez https://kb.vmware.com/kb/1011641.

Identity Firewall

Problème

La publication ou la mise à jour des règles d'Identity Firewall échoue.

Cause

Identity Firewall (IDFW) autorise les règles du pare-feu distribué basées sur l'utilisateur.

Les règles de Pare-feu distribué (DFW) basées sur l'utilisateur sont déterminées par appartenance dans une appartenance de groupe Active Directory (AD). IDFW surveille où des utilisateurs Active Directory sont connectés et mappe la connexion sur une adresse IP, qui est utilisée par DFW pour appliquer des règles de pare-feu. IDFW requiert une infrastructure Guest Introspection et/ou un analyseur de journaux des événements Active Directory.

Solution

1 Assurez-vous que la synchronisation complète/delta du serveur Active Directory fonctionne sur NSX Manager.

   a Dans vSphere Web Client, connectez-vous au vCenter lié à NSX Manager.

   b Accédez à **Accueil > Networking & Security > Instances de NSX Manager (Home > Networking & Security> NSX Managers)**, puis sélectionnez votre instance de NSX Manager dans la liste.

   c Cliquez sur l'onglet **Gérer (Manage)**, puis sur l'onglet **Domaines (Domains)**. Sélectionnez votre domaine dans la liste. Vérifiez que la colonne **Statut de la dernière synchronisation (Last Synchronization Status)** indique RÉUSSI et que **Heure de la dernière synchronisation (Last Synchronization Time)** est l'heure actuelle.

2 Si votre environnement de pare-feu utilise la méthode de l'analyseur de journaux des événements pour la détection de connexion, suivez ces étapes pour vérifier que vous avez configuré un serveur de journaux des événements pour votre domaine :

   a Dans vSphere Web Client, connectez-vous au vCenter lié à NSX Manager.

   b Accédez à **Accueil > Networking & Security > Instances de NSX Manager (Home > Networking & Security> NSX Managers)**, puis sélectionnez votre instance de NSX Manager dans la liste.

   c Cliquez sur l'onglet **Gérer (Manage)**, puis sur l'onglet **Domaines (Domains)**. Sélectionnez votre domaine dans la liste. Ici, vous pouvez afficher et modifier la configuration détaillée du domaine.

   d Sélectionnez **Serveurs de journaux des événements (Event Log Servers)** dans les détails du domaine et vérifiez que votre serveur de journaux des événements est ajouté.

   e Sélectionnez votre serveur de journaux des événements et vérifiez que la colonne **Statut de la dernière synchronisation (Last Sync Status)** indique RÉUSSI et que **Heure de dernière synchronisation (Last Sync Time)** est l'heure actuelle.

3 Si votre environnement de pare-feu utilise Guest Introspection, l'infrastructure doit être déployée sur les clusters de calcul sur lesquels les VM protégées par IDFW vont résider. L'état d'intégrité de service sur l'interface utilisateur devrait être vert. Vous trouverez des informations de diagnostic de Guest Introspection dans les articles de la base de connaissances suivants : Dépannage de vShield Endpoint/NSX Guest Introspection https://kb.vmware.com/kb/2094261 et Collecte de journaux dans une machine virtuelle de service universel VMware NSX for vSphere 6.x Guest Introspection https://kb.vmware.com/kb/2144624.

4 Après avoir vérifié la configuration correcte de votre méthode de détection de connexion, assurez-vous que l'instance de NSX Manager reçoit les événements de connexion.

   a Connectez-vous en tant qu'utilisateur Active Directory.

   b Exécutez la commande suivante pour rechercher les événements de connexion. Vérifiez que votre utilisateur apparaît dans les résultats. `GET https://<nsxmgr-ip>/1.0/identity/userIpMapping`.

```
Example output:
<UserIpMappings>
    <UserIpMapping>
        <ip>50.1.111.192</ip>
        <userName>user1_group20</userName>
        <displayName>user1_group20</displayName>
        <domainName>cd.ad1.db.com</domainName>
        <startTime class="sql-timestamp">2017-05-11 22:30:51.0</startTime>
        <startType>EVENTLOG</startType>
        <lastSeenTime class="sql-timestamp">2017-05-11 22:30:52.0</lastSeenTime>
        <lastSeenType>EVENTLOG</lastSeenType>
    </UserIpMapping>
</UserIpMappings>
```

5 Vérifiez que votre groupe de sécurité est utilisé dans une règle de pare-feu ou qu'une stratégie de sécurité lui est attribuée. Le traitement de groupe de sécurité dans IDFW n'aura pas lieu, sauf si l'une de ces conditions est vraie.

6 Après avoir vérifié qu'IDFW détecte correctement les connexions, vérifiez que l'hôte ESXi sur lequel réside votre VM de poste de travail reçoit la configuration correcte. Ces étapes utiliseront l'interface de ligne de commande centrale de NSX Manager. Pour vérifier l'adresse IP de la VM de poste de travail renseignée dans la liste **ip-securitygroup** :

   a Reportez-vous à la section Commandes de l'interface de ligne de commande pour DFW pour récupérer le nom de filtre appliqué sur la VM de poste de travail.

   b Exécutez la commande `show dfw host hostID filter filterID rules` pour afficher les éléments de règles DFW.

   c Exécutez la commande `show dfw host hostID filter filterID addrsets` pour afficher l'adresse IP renseignée dans la liste `ip-securitygroup`. Vérifiez que votre adresse IP se trouve dans la liste.

Solution

Remarque : lors du dépannage d'IDFW avec le support technique de VMware, les données suivantes sont utiles :

- Si vous utilisez l'analyseur de journaux des événements, les données de mise à l'échelle Active Directory :
  - Nombre de domaines pour une instance de NSX Manager

    Nombre de forêts

Nombre d'utilisateurs/Forêt

Nombre d'utilisateurs/Domaine

Nombre de groupes Active Directory par domaine

Nombre d'utilisateurs/Groupe Active Directory

Nombre d'Active Directory/Utilisateur

Nombre de contrôleurs de domaine

Nombre de serveurs de journaux Active Directory

- Données de mise à l'échelle de connexion utilisateur :
  - Nombre moyen d'utilisateurs par min
- Détails du déploiement utilisant IDFW avec VDI :
  - Nombre de postes de travail VDI/VC

    Nombre d'hôtes/VC

    Nombre de postes de travail VDI/Hôte
- Si vous utilisez Guest Introspection :
  - Version de VMTools (pilotes Guest Introspection)

    Version du système d'exploitation invité Windows

Dépannage de l'équilibrage de charge

6

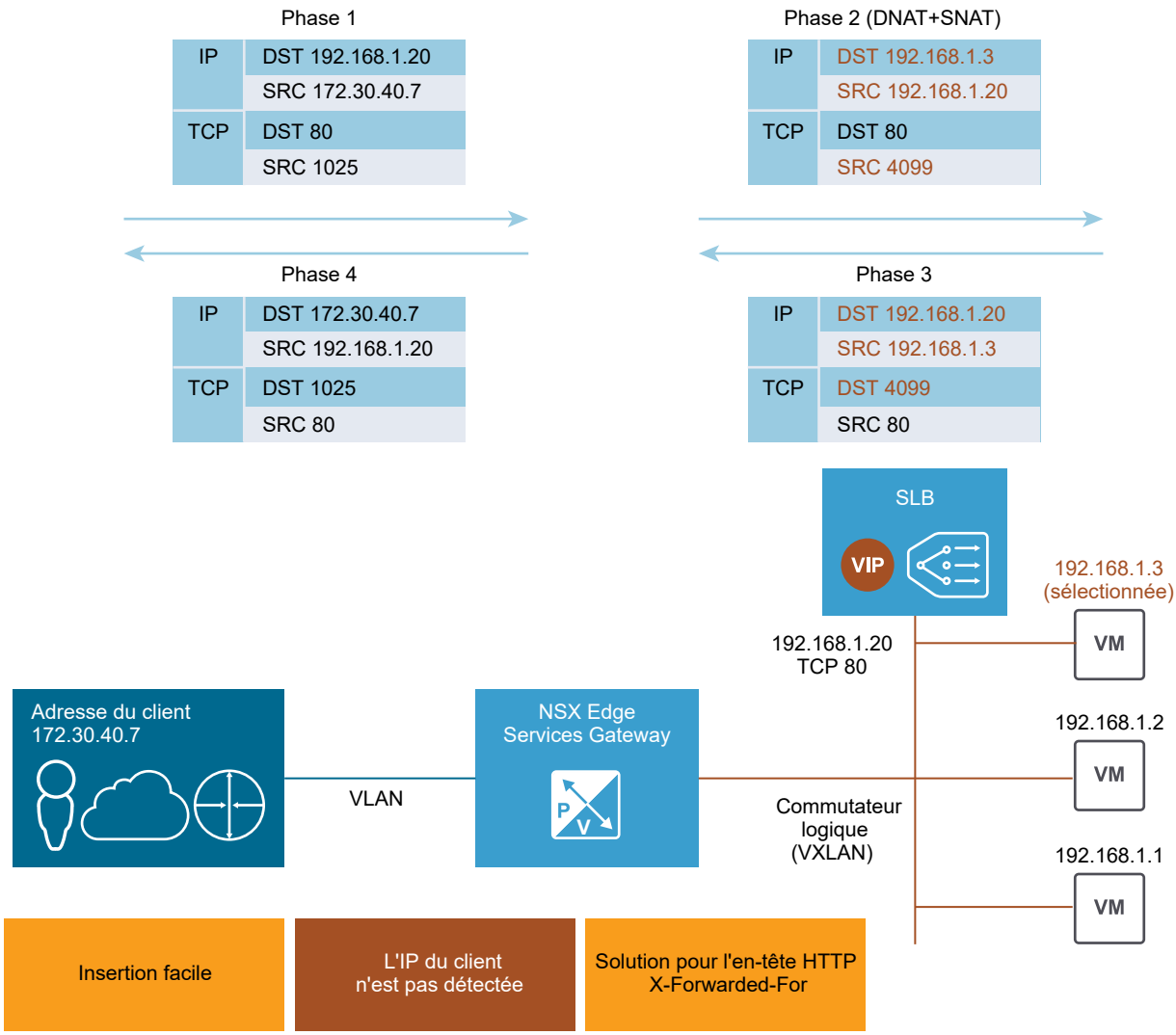
L'équilibrage de charge de NSX Edge permet au trafic réseau d'emprunter plusieurs chemins vers une destination spécifique. Il distribue les demandes de service entrantes uniformément entre plusieurs serveurs de telle sorte que la distribution de la charge est transparente pour les utilisateurs. Deux types de services d'équilibrage de charge doivent être configurés dans NSX : un mode manchot, ou mode proxy, et un mode en ligne, ou mode transparent. Pour plus d'informations, consultez le *Guide d'administration de NSX*.

Avant de commencer le dépannage et la vérification de la configuration, obtenez une description exacte de l'erreur, créez une carte de topologie en rapport avec le client, le serveur virtuel et le serveur principal, puis comprenez les exigences de l'application. Par exemple, un client ne pouvant pas se connecter est différent des erreurs de session aléatoires après la connexion. Pendant le dépannage de l'équilibrage de charge, commencez toujours par la vérification d'erreur de connectivité.

Ce chapitre contient les rubriques suivantes :

Configurer un équilibrage de charge manchot

La passerelle ESG (Edge Services Gateway) peut être considérée comme un proxy pour le trafic client entrant.


Phase 1
IP
DST 192.168.1.20
SRC 172.30.40.7
TCP
DST 80
SRC 1025
Phase 2 (DNAT+SNAT)
IP
DST 192.168.1.3
SRC 192.168.1.20
TCP
DST 80
SRC 4099
Phase 4
IP
DST 172.30.40.7
SRC 192.168.1.20
TCP
DST 1025
SRC 80
Phase 3
IP
DST 192.168.1.20
SRC 192.168.1.3
TCP
DST 4099
SRC 80
SLB
VIP
192.168.1.3
(sélectionnée)
192.168.1.20
TCP 80
VM
192.168.1.2
VM
192.168.1.1
VM
Adresse du client
172.30.40.7
VLAN
NSX Edge
Services Gateway
P
V
Commutateur
logique
(VXLAN)
Insertion facile
L'IP du client
n'est pas détectée
Solution pour l'en-tête HTTP
X-Forwarded-For

En mode proxy, l'équilibrage de charge utilise sa propre adresse IP comme adresse source pour envoyer des demandes à un serveur principal. Le serveur principal affiche tout le trafic provenant de l'équilibrage de charge et répond directement à l'équilibrage de charge. Ce mode est également appelé mode SNAT ou mode non transparent. Pour plus d'informations, consultez le *Guide d'administration de NSX*.

Un équilibrage de charge manchot NSX classique est déployé sur le même sous-réseau avec ses serveurs principaux, excepté le routeur logique. Le serveur virtuel de l'équilibrage de charge NSX écoute sur une adresse IP virtuelle les demandes entrantes du client et les envoie aux serveurs principaux. Pour le trafic de retour, un NAT inverse est requis pour transformer l'adresse IP source du serveur principal en adresse IP virtuelle (VIP), puis pour envoyer l'adresse IP virtuelle au client. Sans cette opération, la connexion au client est interrompue.

Une fois que la passerelle ESG reçoit le trafic, elle effectue deux opérations : DNAT (Destination Network Address Translation, traduction de l'adresse réseau de destination) pour transformer l'adresse IP virtuelle en adresse IP de l'une des machines à équilibrage de charge et SNAT (Source Network Address Translation, traduction de l'adresse réseau source) pour échanger l'adresse IP du client avec celle de la passerelle ESG.

Ensuite, le serveur ESG envoie le trafic au serveur d'équilibrage de charge et ce dernier renvoie la réponse à la passerelle ESG, puis au client. Cette option est beaucoup plus facile à configurer que le mode En ligne, mais elle présente deux mises en garde potentielles. La première est que ce mode requiert un serveur ESG dédié et la seconde est que les serveurs d'équilibrage de charge ne connaissent pas l'adresse IP d'origine du client. Une solution pour les applications HTTP/HTTPS consiste à activer Insérer X-transféré-pour dans le profil d'application HTTP pour que l'adresse IP du client soit transportée dans l'en-tête HTTP X-transféré-pour dans la demande envoyée au serveur principal.

Si l'adresse IP du client doit être visible sur le serveur principal pour des applications autres que HTTP/HTTPS, vous pouvez configurer le pool d'adresses IP pour qu'il soit transparent. Si les clients ne se trouvent pas sur le même sous-réseau que le serveur principal, le mode en ligne est recommandé. Sinon, vous devez utiliser l'adresse IP de l'équilibrage de charge comme passerelle par défaut du serveur principal.

Note En général, il existe trois méthodes pour garantir l'intégrité de la connexion :

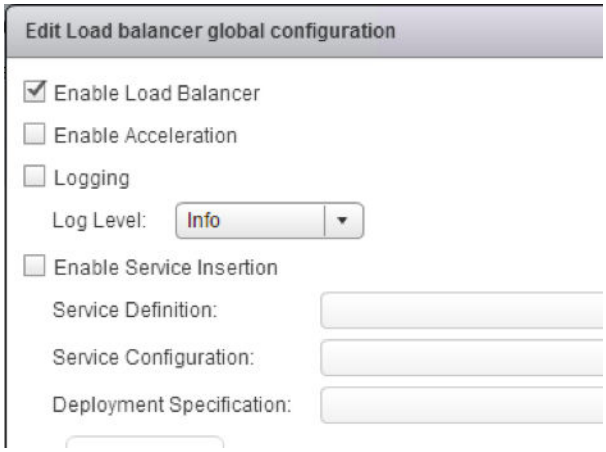
- Mode en ligne/transparent
- Mode SNAT/proxy/non transparent (abordé ci-dessus)
- Retour au serveur direct (DSR) : actuellement non pris en charge

En mode DSR, le serveur principal répond directement au client. Actuellement, l'équilibrage de charge NSX ne prend pas en charge le mode DSR.

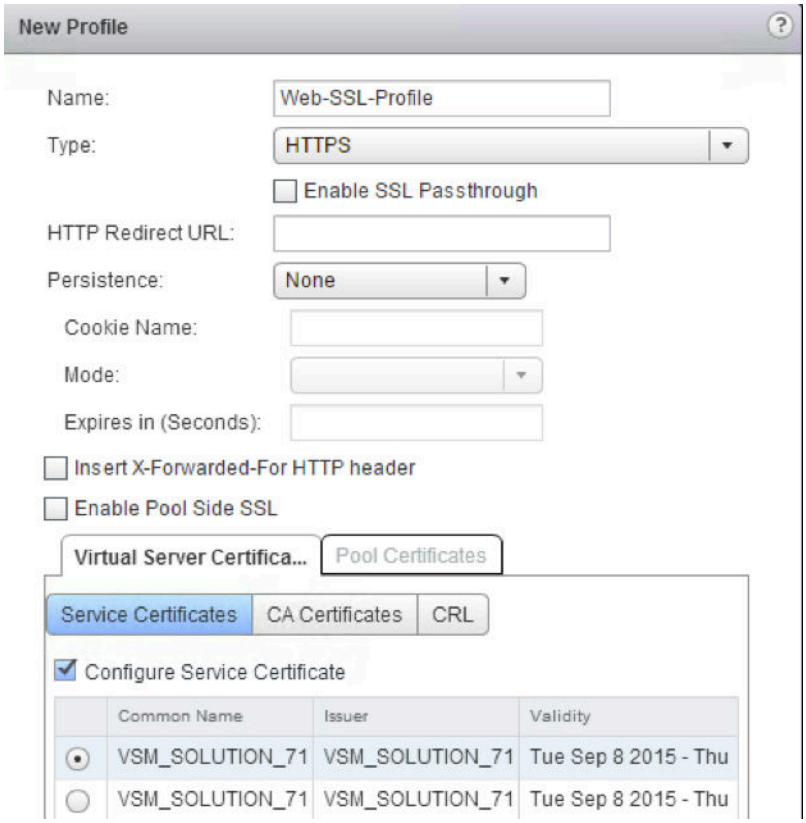
Procédure

1. Par exemple, configurons un serveur virtuel manchot avec le déchargement SSL. Créez un certificat en double-cliquant sur le dispositif Edge et en sélectionnant **Gérer > Paramètres > Certificat (Manage > Settings > Certificate)**.

2 Activez l'équilibrage de charge en sélectionnant **Gérer > Équilibrage de charge > Configuration globale > Modifier (Manage > Load Balancer > Global Configuration > Edit)**.



3 Créez un profil d'application HTTPS en sélectionnant **Gérer > Équilibrage de charge > Profils d'application (Manage > Load Balancer > Application Profiles)**.

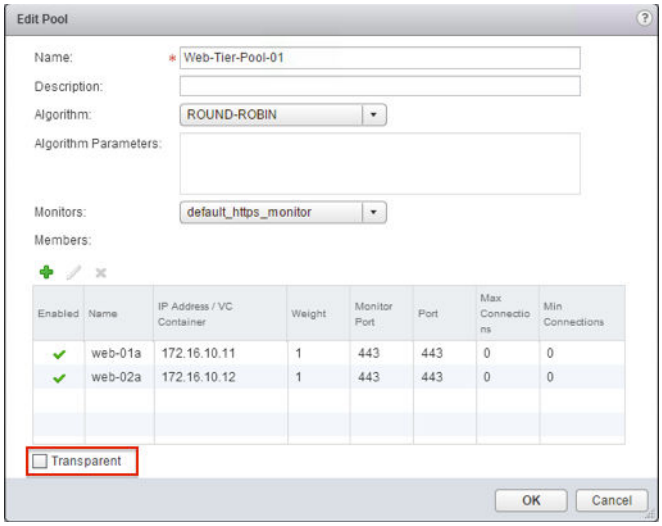


Note La capture d'écran ci-dessus utilise des certificats auto-signés à des fins de documentation uniquement.

4 Facultativement, cliquez sur **Gérer > Équilibrage de charge > Surveillance des services (Manage > Load Balancer > Service Monitoring)** et modifiez la surveillance des services par défaut pour la passer de HTTP/HTTPS de base à des URL/URI spécifiques, selon les besoins.

5 Créez des pools de serveurs en sélectionnant **Gérer > Équilibrage de charge > Pools (Manage > Load Balancer > Pools)**.

Pour utiliser le mode SNAT, ne cochez pas la case **Transparent** dans la configuration de pool.



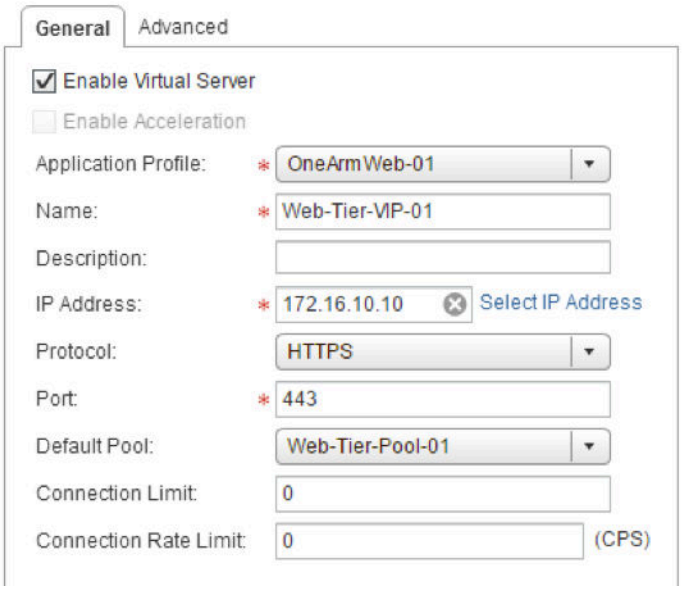
Vérifiez que les VM sont répertoriées et activées.

6 Facultativement, cliquez sur **Gérer > Équilibrage de charge > Pools > Afficher les statistiques du pool (Manage > Load Balancer > Pools > Show Pool Statistics)** pour vérifier l'état.

Vérifiez que l'état du membre est Actif.

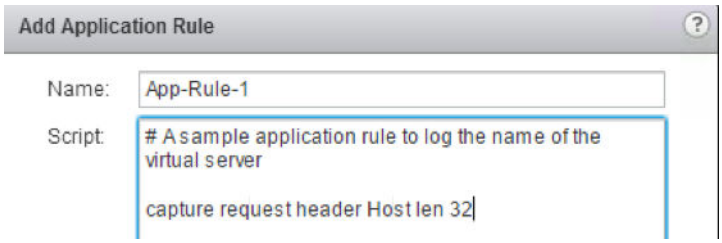
7 Créez un serveur virtuel en sélectionnant **Gérer > Équilibrage de charge > Serveurs virtuels (Manage > Load Balancer > Virtual Servers)**.

Si vous voulez utiliser l'équilibrage de charge de niveau 4 pour UDP ou TCP performances supérieures, cochez **Activer l'accélération (Enable Acceleration)**. Si vous cochez **Activer l'accélération (Enable Acceleration)**, assurez-vous que l'état du pare-feu est **Activé (Enabled)** sur l'équilibrage de charge NSX Edge, car un pare-feu est requis pour SNAT L4.



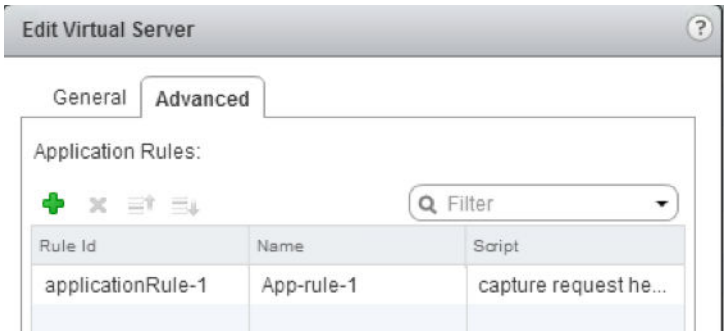
Vérifiez que l'adresse IP est liée au pool de serveurs.

8 Facultativement, si vous utilisez une règle d'application, vérifiez la configuration dans **Gérer > Équilibrage de charge > Règles d'application (Manage > Load Balancer > Application Rules)**.



9 Si vous utilisez une règle d'application, vérifiez qu'elle est associée au serveur virtuel dans **Gérer > Équilibrage de charge > Serveurs virtuels > Avancé (Manage > Load Balancer > Virtual Servers > Advanced)**.

Pour voir des exemples pris en charge, consultez : https://communities.vmware.com/docs/DOC-31772.



En mode non transparent, le serveur principal ne peut pas voir l'adresse IP du client, mais il peut voir l'adresse IP interne de l'équilibrage de charge. Comme solution pour le trafic HTTP/HTTPS, cochez **Insérer l'en-tête HTTP X-transféré-pour (Insert X-Forwarded-For HTTP header)**. Avec cette option cochée, l'équilibrage de charge Edge ajoute l'en-tête « X-transféré-pour » avec la valeur de l'adresse IP source du client.

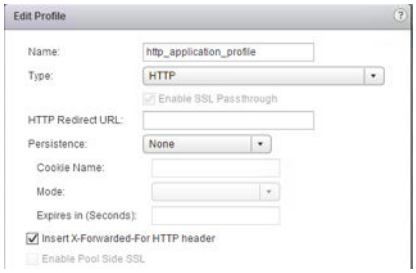
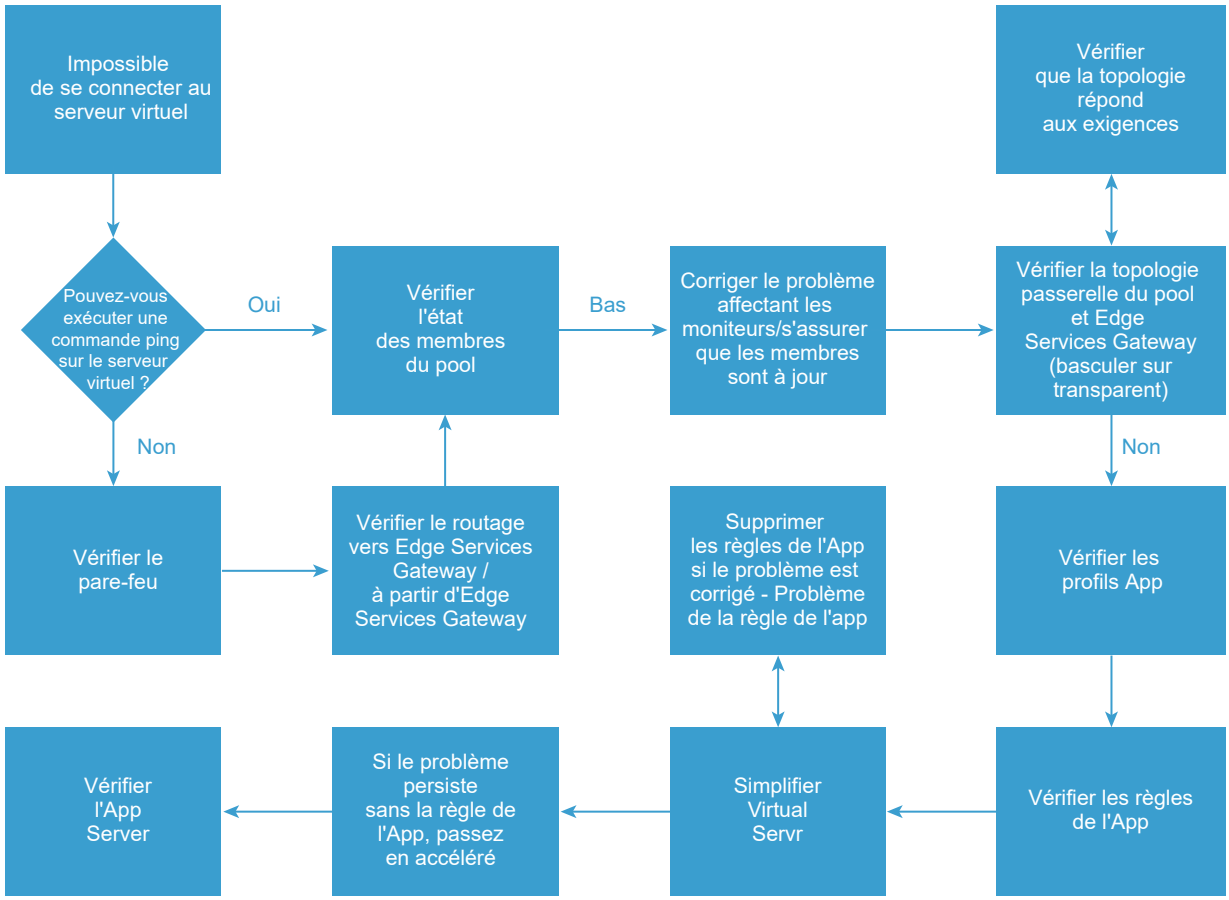


Diagramme de flux de dépannage pour l'équilibrage de charge

Le diagramme de flux suivant représente une vue d'ensemble du dépannage des problèmes d'équilibrage de charge.



Dépannage et vérification de la configuration de l'équilibrage de charge à l'aide de l'interface utilisateur

Vous pouvez vérifier la configuration de l'équilibrage de charge via vSphere Web Client. Vous pouvez utiliser l'interface utilisateur pour dépanner l'équilibrage de charge.

Après avoir compris ce qui devrait fonctionner et après avoir défini un problème, vérifiez la configuration via l'interface utilisateur comme suit.

Conditions préalables

Notez les informations suivantes :

- L'IP, le protocole et le port du serveur virtuel.
- L'IP et le port des serveurs d'applications principaux.
- La topologie qui était prévue, en ligne ou manchot. Pour plus de détails, consultez la rubrique Équilibrage de charge logique dans le *Guide d'administration de NSX*.
- Vérifiez l'itinéraire de la trace et utilisez les outils de connectivité réseau pour voir que les paquets se déplacent vers l'emplacement qui convient (Edge Services Gateway).
- Vérifiez que les pare-feux en amont autorisent le trafic correctement.
- Définissez le problème que vous rencontrez. Par exemple, les enregistrements DNS du serveur virtuel sont corrects, mais vous ne récupérez aucun contenu ou contenu incorrect, etc.

Problème

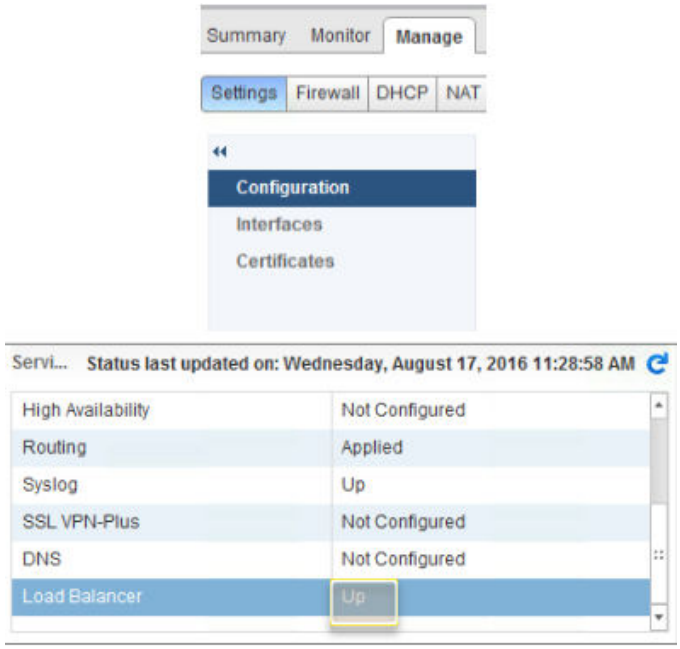
L'équilibrage de charge ne fonctionne pas comme prévu.

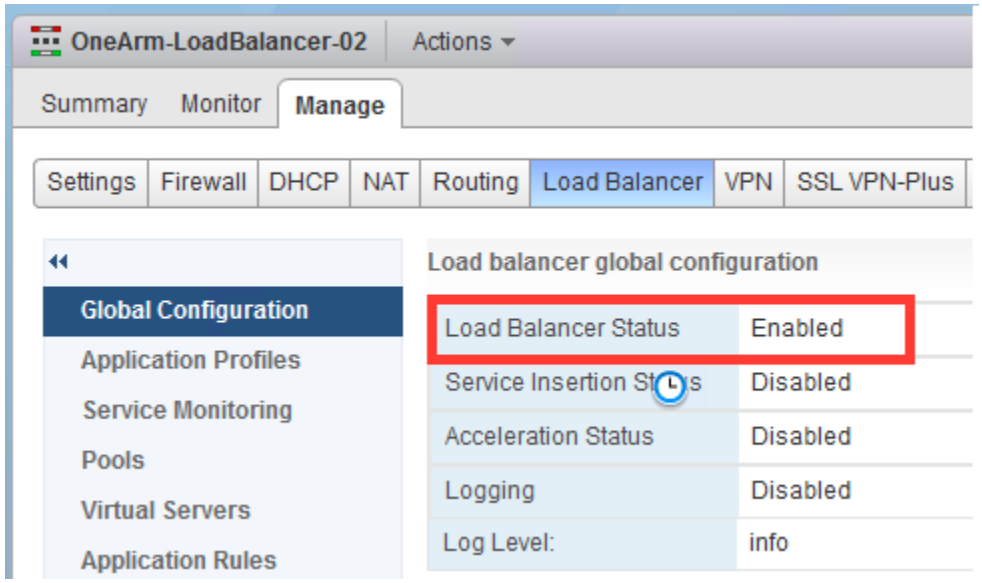
Solution

1. Vérifiez les exigences d'application suivantes : protocoles requis pour être pris en charge sur l'équilibrage de charge (TCP, UDP, HTTP, HTTPs), ports, exigences de persistance et membres du pool.
    - L'équilibrage de charge et le pare-feu sont-ils activés ? Edge Services Gateway dispose-t-il des itinéraires appropriés ?
    - Quels adresse IP, port et protocole le serveur virtuel doit-il écouter ?
    - Le déchargement SSL est-il utilisé ? Avez-vous besoin d'utiliser SSL lors de la communication avec les serveurs principaux ?
    - Utilisez-vous des règles d'applications ?
    - Quelle est la topologie ? L'équilibrage de charge NSX doit analyser tout le trafic du client et du serveur.
    - L'équilibrage de charge NSX est-il en ligne ou l'adresse source du client est-elle traduite pour s'assurer que le trafic de retour revient vers l'équilibrage de charge ?

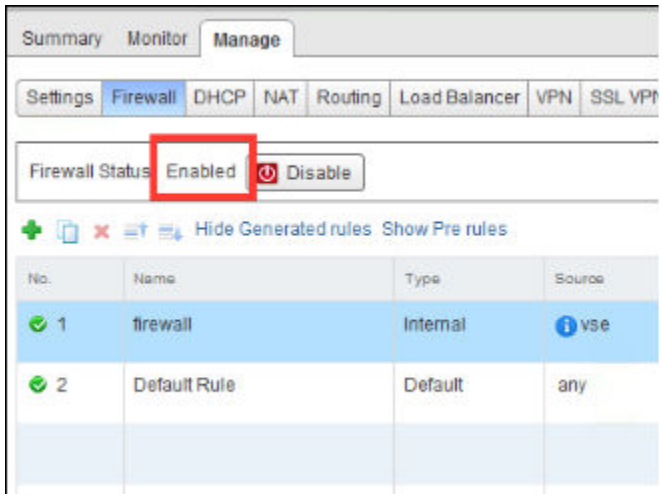
2 Accédez au dispositif NSX Edge, puis vérifiez les configurations qui sont requises pour activer l'équilibrage de charge et autoriser la circulation du trafic comme suit :

a Vérifiez que l'équilibrage de charge est répertorié comme **Actif (Up)**.





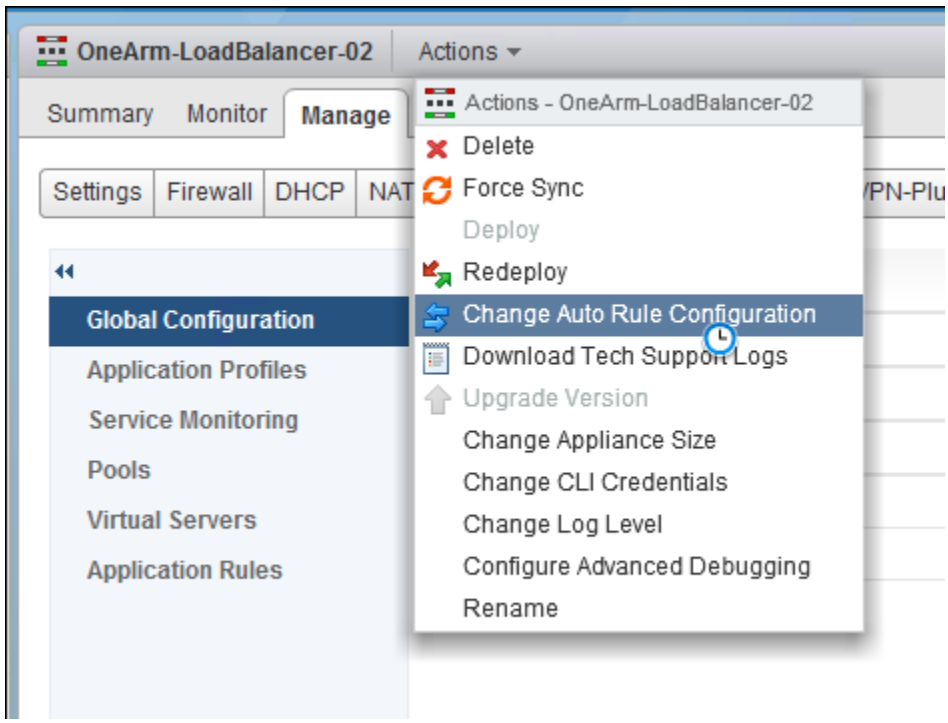
b Vérifiez que le pare-feu est **Activé (Enabled)**. Le pare-feu DOIT être activé pour les serveurs virtuels accélérés. Les VIP TCP et L7 HTTP/HTTPS non accélérées doivent présenter une politique qui autorise le trafic. Remarquez que les filtres de pare-feu n'auront pas d'impact sur les serveurs virtuels accélérés.



c Vérifiez que les règles NAT sont créées pour le serveur virtuel. Dans l'onglet **NAT**, cliquez sur le lien **Masquer les règles internes (Hide internal rules)** ou **Afficher les règles internes (Unhide internal rules)** pour vérifier.

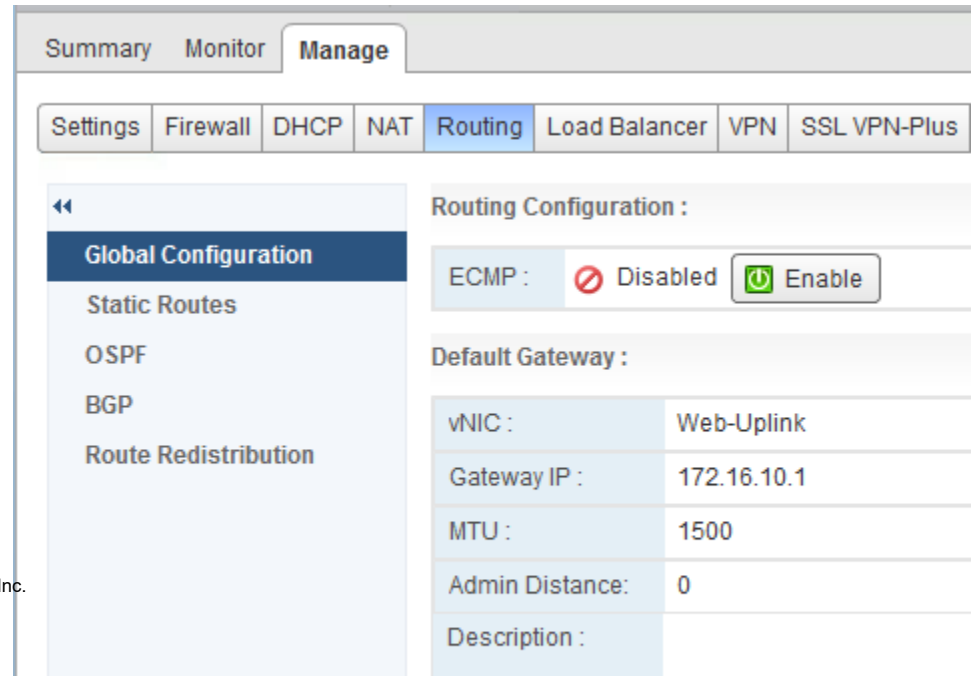
Note Si l'équilibrage de charge est activé et que les services sont configurés, mais que vous n'avez pas configuré de règles NAT, cela signifie que la configuration de la règle automatique n'a pas été activée.

d Vous pouvez modifier les configurations de la règle automatique. Pour plus de détails, consultez la rubrique Modifier la configuration de la règle automatique dans le *Guide d'administration de NSX*. Lorsque NSX Edge Services Gateway est déployé, vous avez la possibilité de configurer la configuration de la règle automatique. Si cette option n'a pas été sélectionnée lors du déploiement d'Edge Services Gateway, vous devez l'activer pour que l'équilibrage de charge fonctionne correctement. Vérifiez l'état de membre du pool avec l'interface utilisateur.

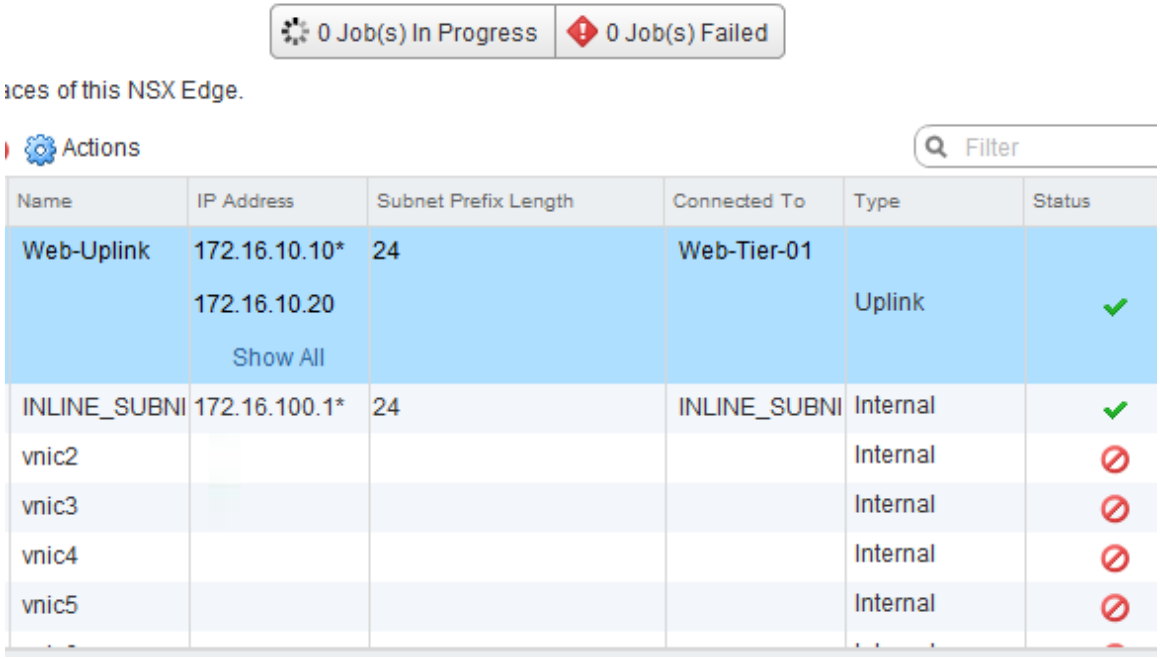


e Vérifiez le routage et vérifiez que Edge Services Gateway a un itinéraire par défaut ou un itinéraire statique vers vos systèmes clients et les serveurs principaux. S'il n'existe aucun itinéraire vers les serveurs, la vérification de l'intégrité échouera. Si vous utilisez un protocole de routage dynamique, il se peut que vous deviez utiliser l'interface de ligne de commande. Pour plus d'informations, consultez la section Interface de ligne de commande du routage NSX.

a Vérifiez l'itinéraire par défaut.



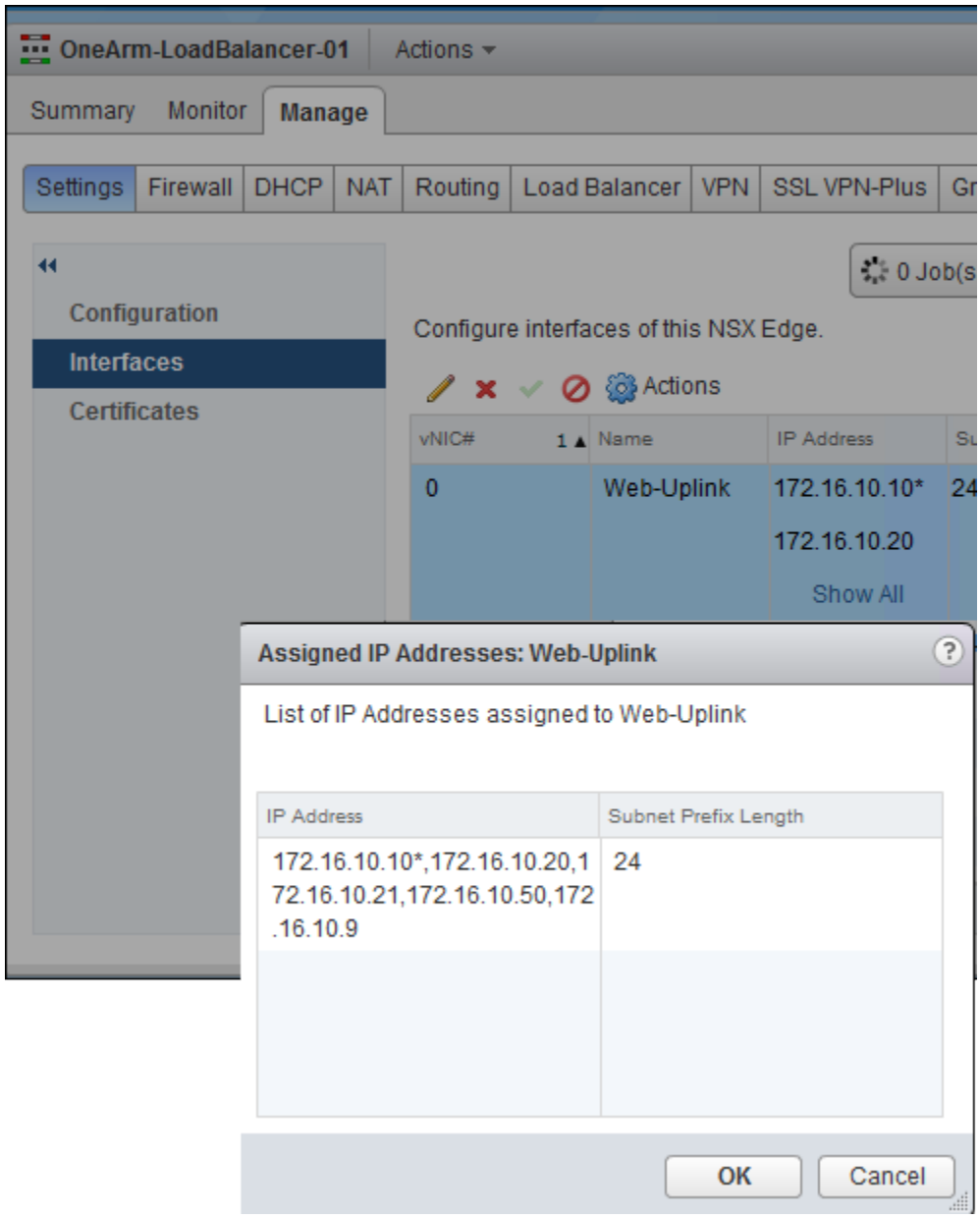
dispose d'une interface dans le sous-réseau. À plusieurs reprises, les serveurs d'application sont connectés à ces serveurs.



c Vérifiez les itinéraires statiques dans l'onglet **Routage (Routing)** > **Itinéraires statiques (Static Routes)**.

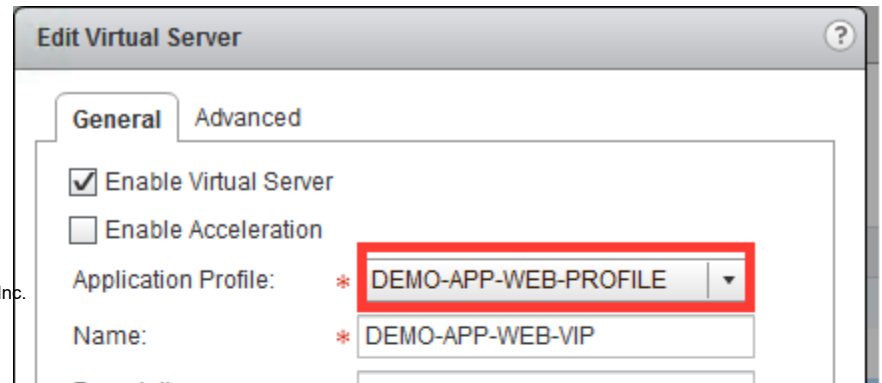
3 Vérifiez l'adresse IP, le port et le protocole du serveur virtuel.

a Double-cliquez sur un dispositif NSX Edge et accédez à **Gérer (Manage) > Paramètres (Settings)**> **Interfaces**. Vérifiez que l'adresse IP du serveur virtuel est ajoutée à une interface.

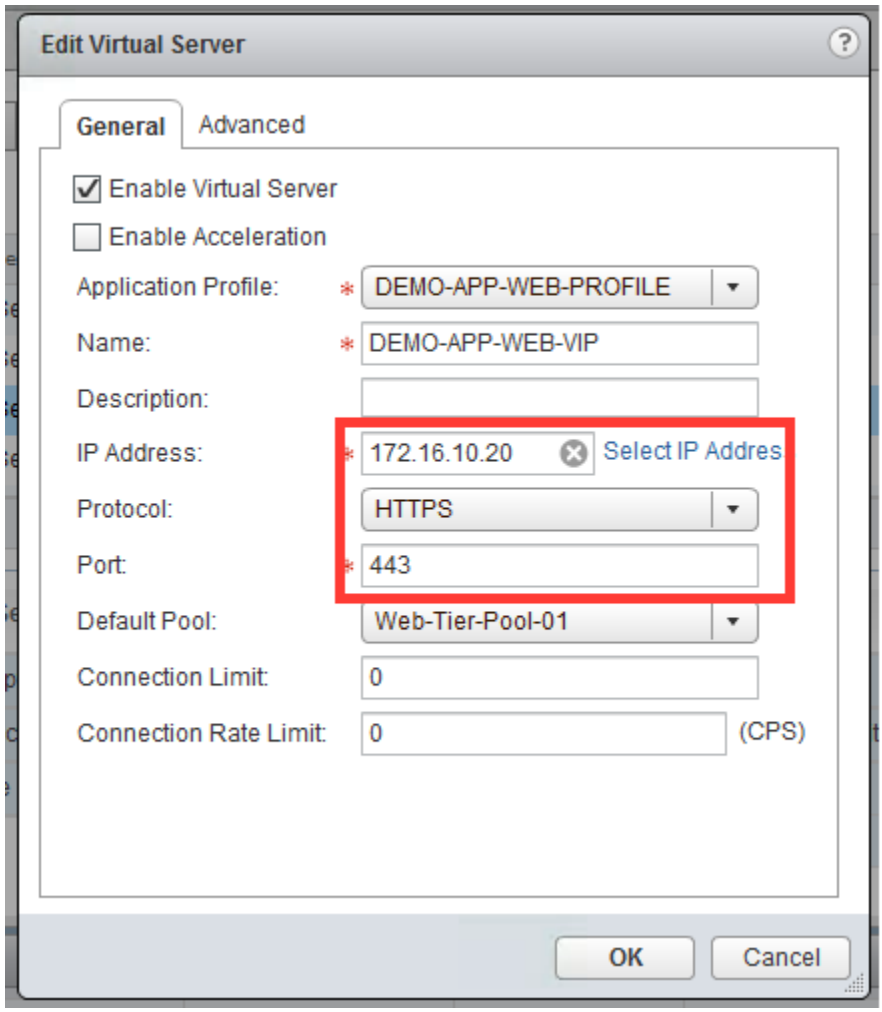


b Vérifiez que le serveur virtuel dispose de la bonne adresse IP, de port(s) et de protocoles configurés pour prendre en charge l'application.

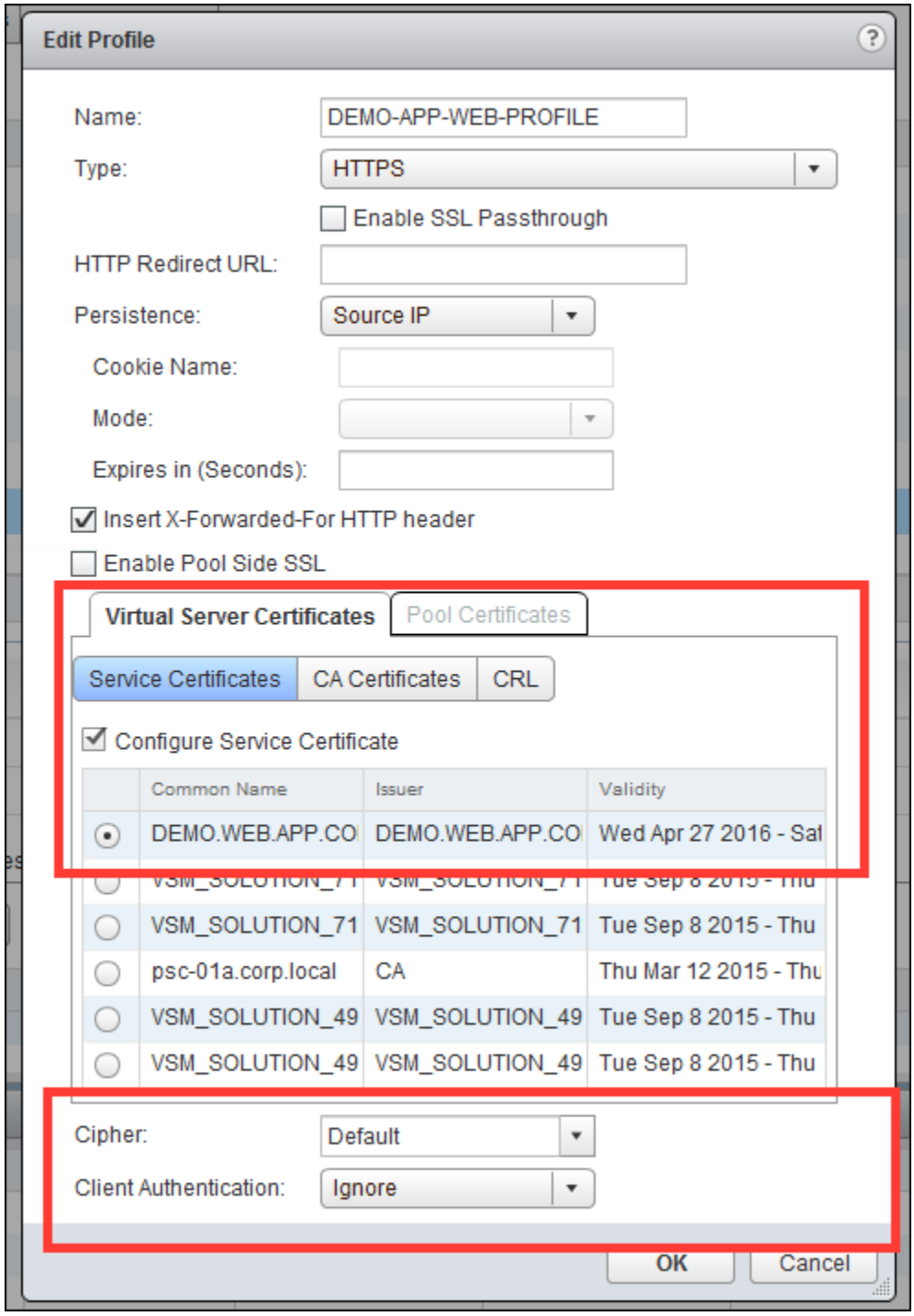
a Vérifiez le profil d'application utilisé par le serveur virtuel.



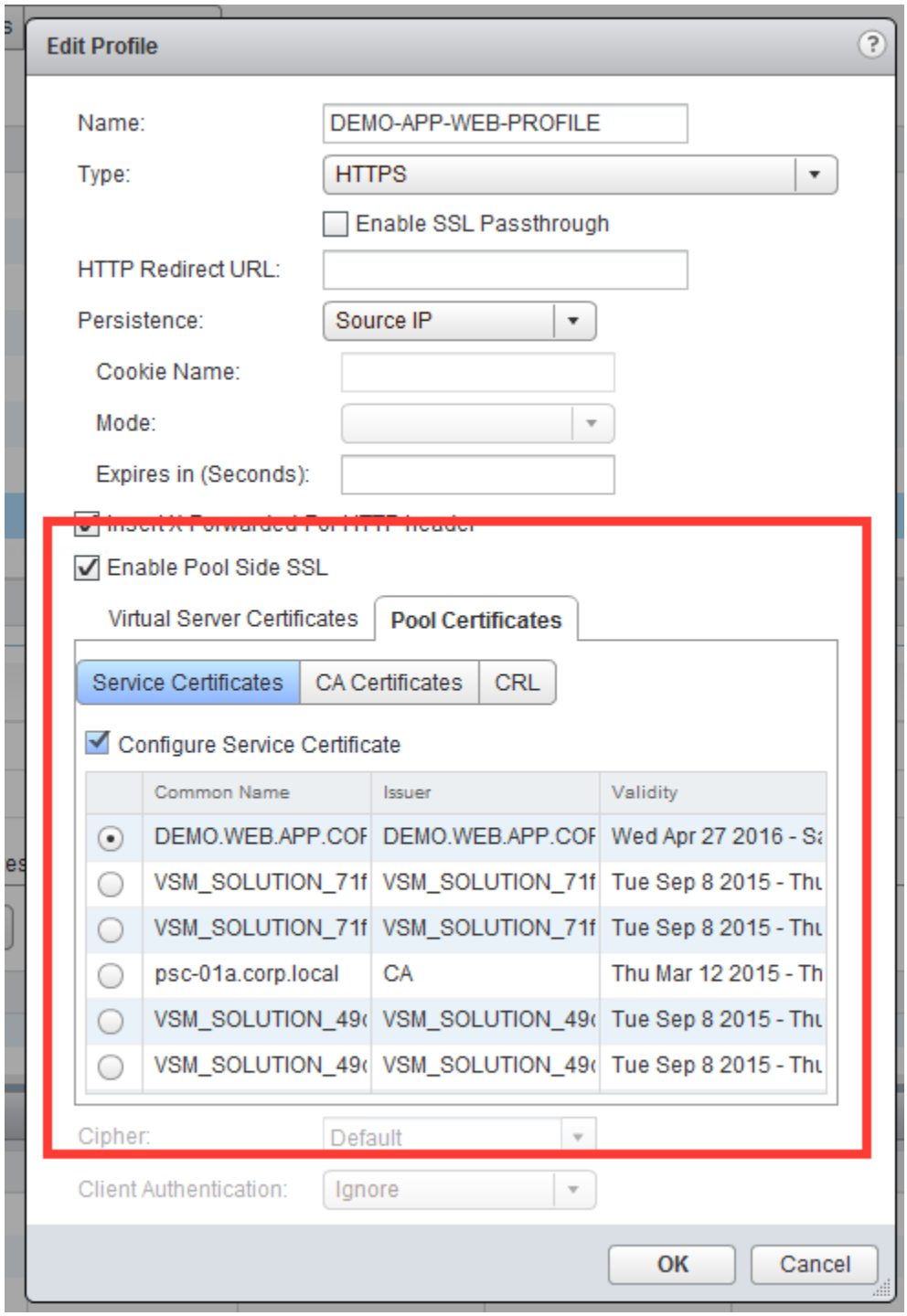
HTTPS) sur le serveur virtuel.



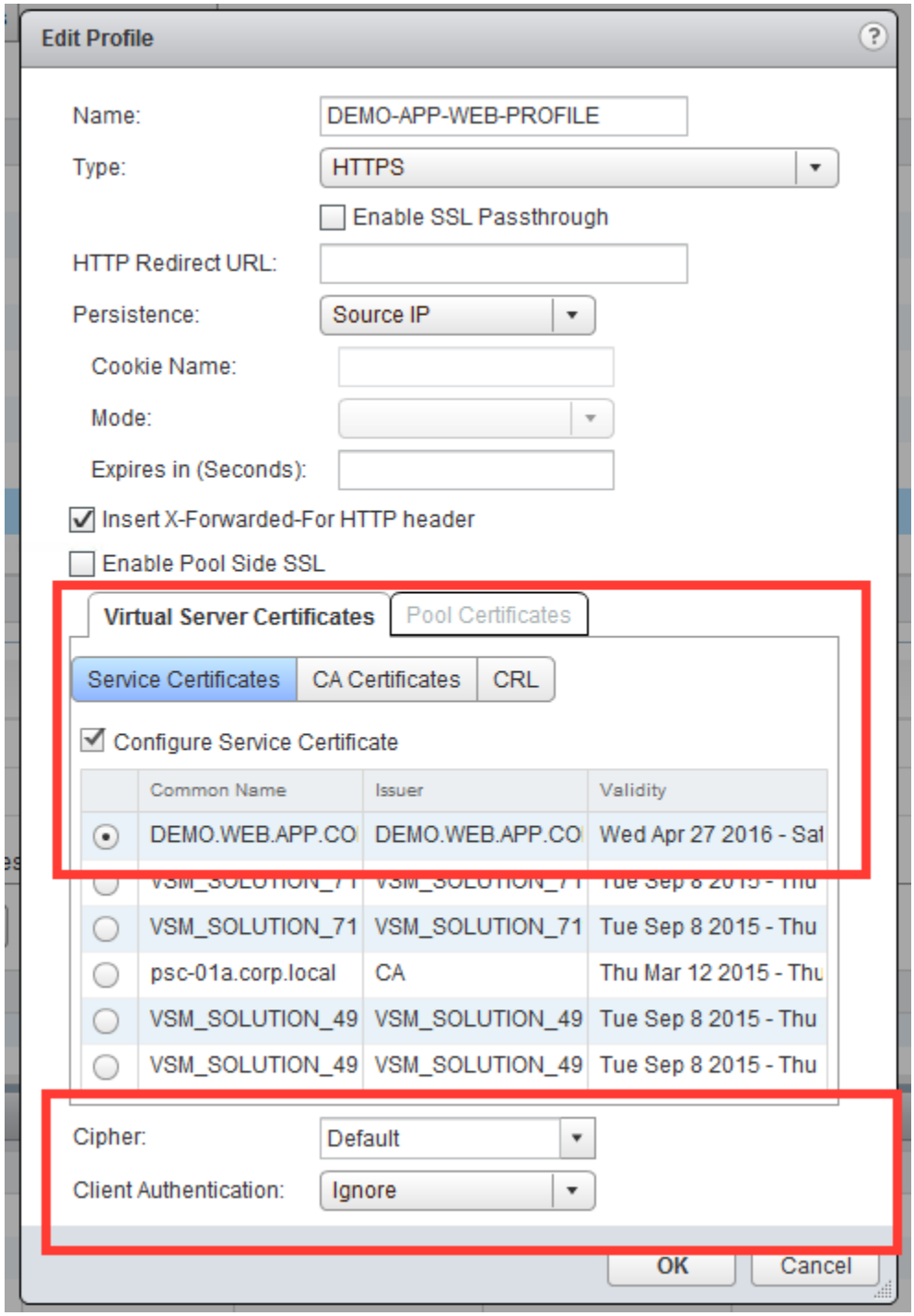
c Vérifiez que le profil d'application respecte la méthode persistante prise en charge, le type (protocole) et SSL (si nécessaire). Si vous utilisez SSL, vérifiez que vous utilisez un certificat avec le nom et la date d'expiration qui conviennent.



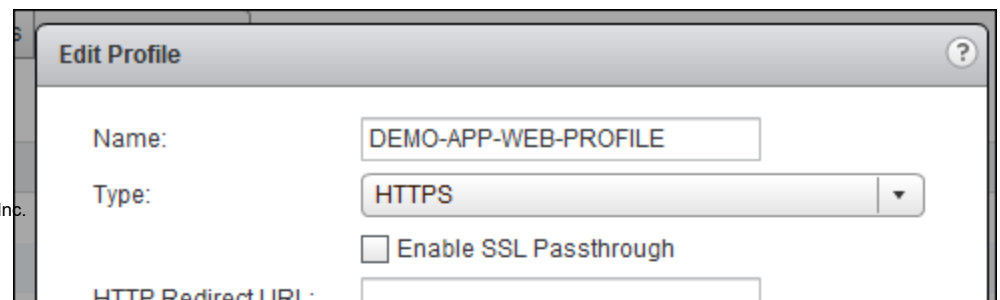
d Vérifiez si le bon certificat est utilisé pour que les clients se connectent.



e Vérifiez si vous avez besoin d'un certificat client, alors que les clients ne sont pas configurés. Vérifiez aussi si vous avez sélectionné une liste de chiffrement étroite qui est trop étroite (par exemple, les clients qui utilisent d'anciens navigateurs).

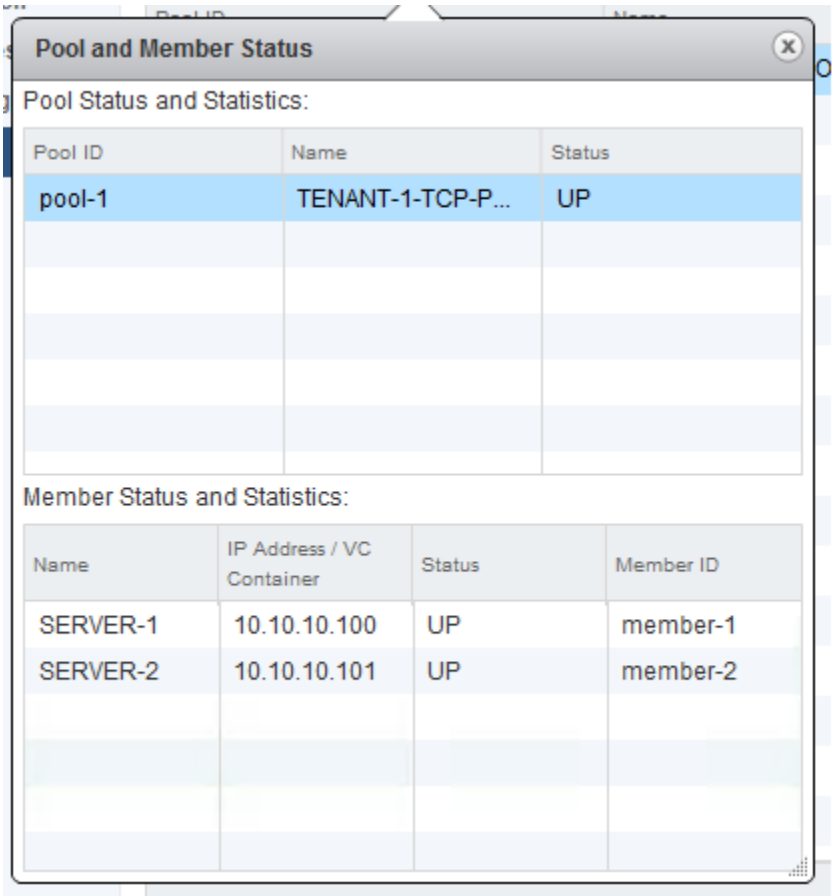


f Vérifiez si vous avez besoin de SSL vers les serveurs principaux.

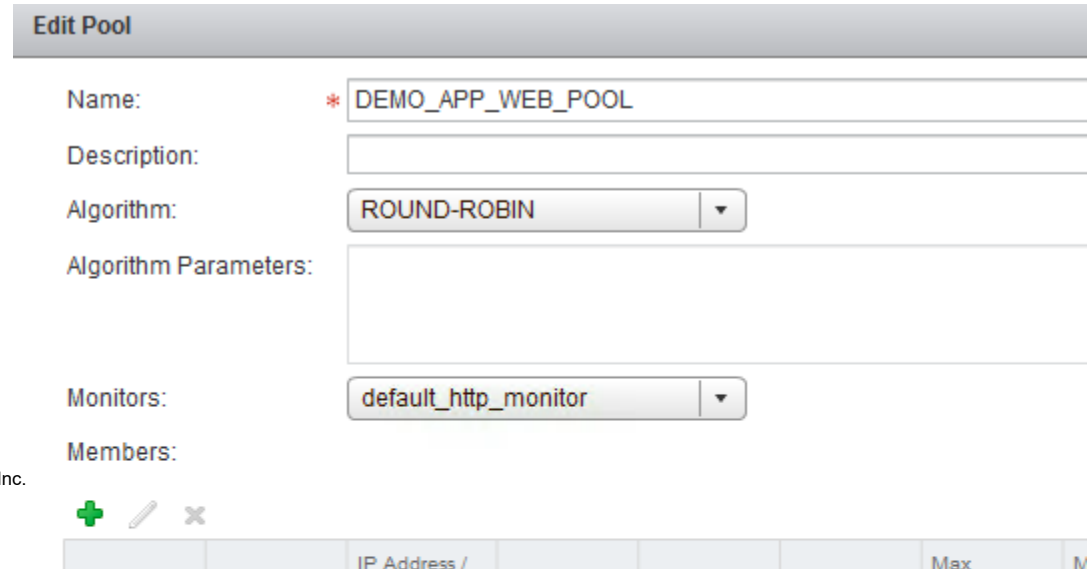


4 Vérifiez la configuration et l'état du pool comme suit :

a Vérifiez l'état du pool. Au moins un membre doit pouvoir assurer le trafic, mais il se peut qu'un seul membre ne soit pas suffisant pour assurer tout le trafic. Si aucun membre ou si un nombre limité de membres du pool sont actifs, essayez de rectifier le problème comme décrit dans les étapes suivantes.

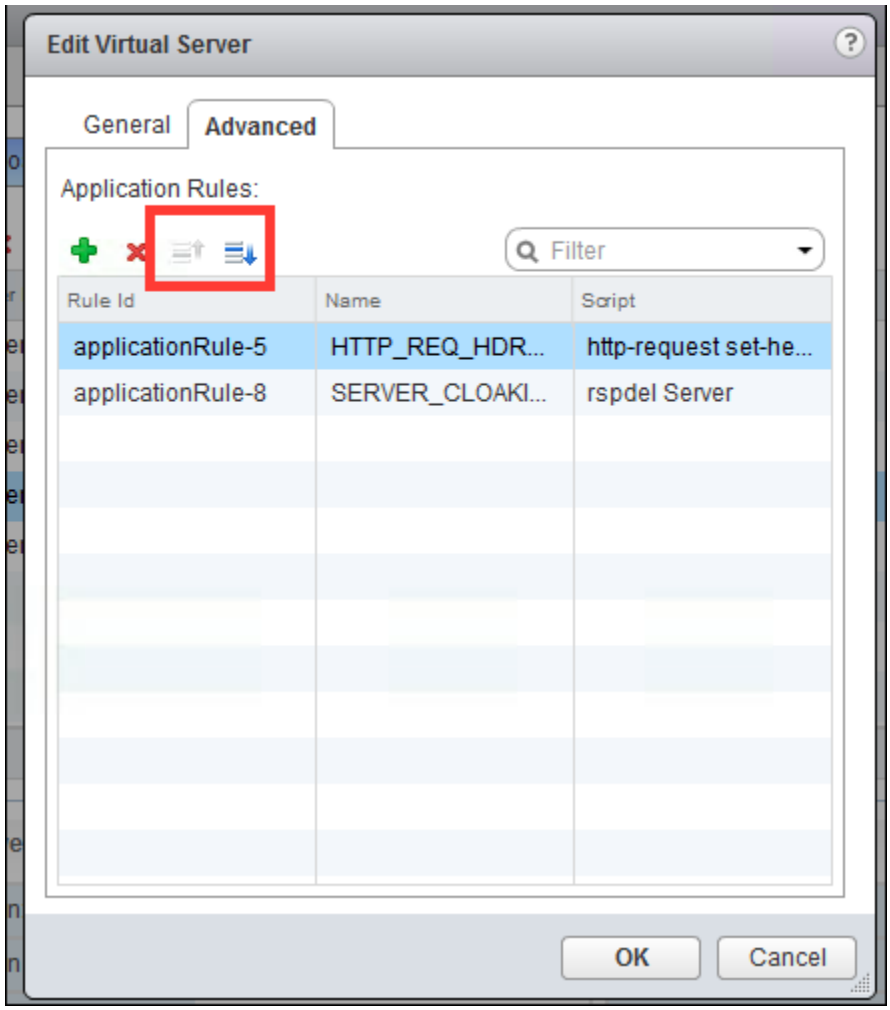


b Vérifiez que la topologie est correcte. Le trafic client SNAT est contrôlé dans la configuration du pool. Si Edge Services Gateway hébergeant la fonction d'équilibrage de charge n'est pas en ligne pour voir tout le trafic, un échec va se produire. Pour conserver l'adresse IP de l'adresse source du client, sélectionnez le mode **Transparent**. Pour plus d'informations, consultez le *Guide d'administration de NSX*.



5 Si vous utilisez des règles d'application, vérifiez les règles. Si nécessaire, supprimez les règles pour voir si le trafic circule.

   a Réorganisez les règles pour voir si leur ordre entraîne l'interruption du trafic par la logique. Pour plus d'informations sur l'ajout d'une règle d'application et pour voir des exemples de règle d'application, consultez la rubrique Ajouter une règle d'application dans le *Guide d'administration de NSX*.



Étape suivante

Si vous n'avez pas trouvé le problème, il se peut que vous deviez utiliser l'interface de ligne de commande (CLI) pour découvrir ce qu'il se passe. Pour plus d'informations, consultez Dépannage de l'équilibrage de charge à l'aide de l'interface de ligne de commande.

Dépannage de l'équilibrage de charge à l'aide de l'interface de ligne de commande

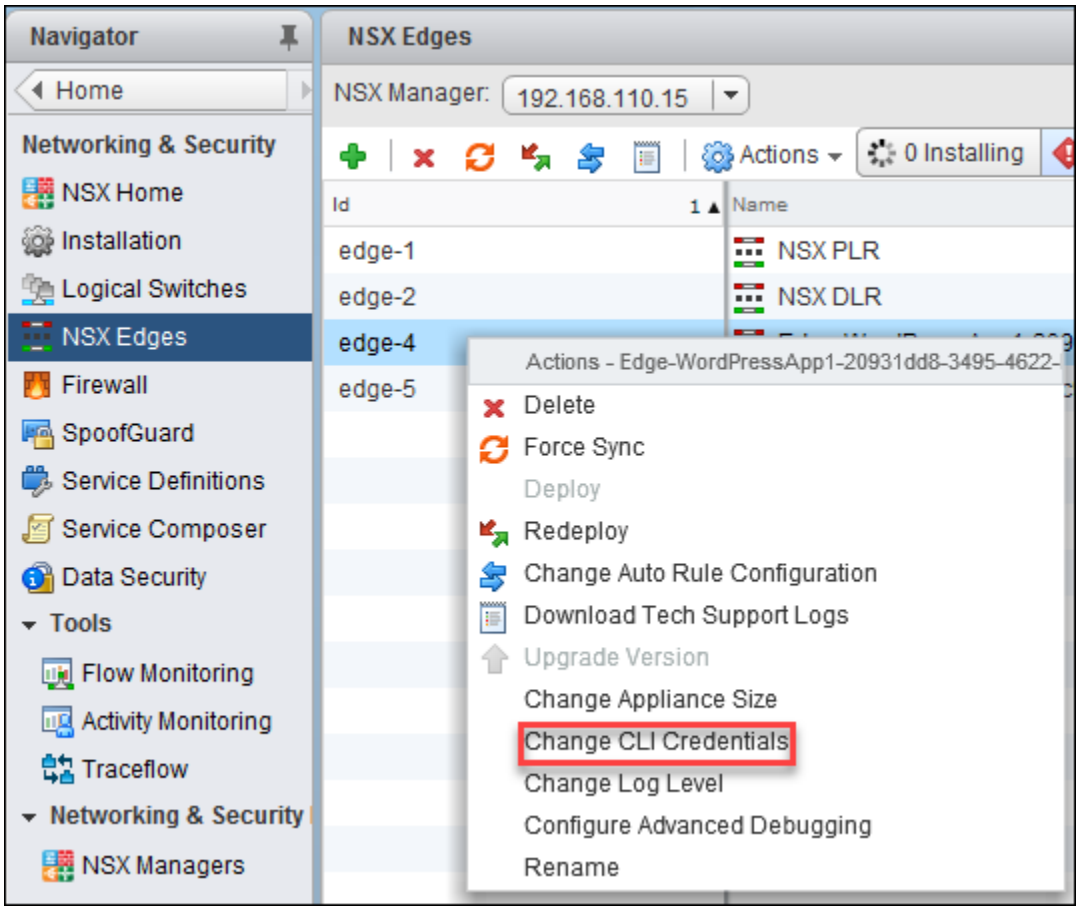
L'interface de ligne de commande de NSX peut servir à récupérer les journaux de suivi détaillés, à utiliser les captures de paquets et à examiner les mesures dans le cadre du dépannage de l'équilibrage de charge.

Problème

L'équilibrage de charge ne fonctionne pas comme prévu.

Solution

1 Activez la connexion SSH ou vérifiez que vous pouvez vous connecter via SSH au dispositif virtuel. Edge Services Gateway est un dispositif virtuel qui a la possibilité d'activer SSH pendant le déploiement. Si vous devez activer SSH, sélectionnez le dispositif requis, puis dans le menu **Actions**, cliquez sur **Modifier les informations d'identification CLI (Change CLI Credentials)**.



2 Edge Services Gateway présente plusieurs commandes d'affichage qui étudient l'état de l'exécution et l'état de la configuration. Utilisez les commandes pour afficher les informations relatives à la configuration et aux statistiques.

```
nsxedge> show configuration loadbalancer
nsxedge> show configuration loadbalancer virtual [virtual-server-name]
nsxedge> show configuration loadbalancer pool [pool-name]
nsxedge> show configuration loadbalancer monitor [monitor-name]
nsxedge> show configuration loadbalancer profile [profile-name]
nsxedge> show configuration loadbalancer rule [rule-name]
```

3 Pour que l'équilibrage de charge et NAT fonctionnent correctement, le pare-feu doit être activé. Utilisez la commande `#show firewall`. Si vous ne voyez pas de sortie logique à l'aide de la commande, consultez la section Dépannage et vérification de la configuration de l'équilibrage de charge à l'aide de l'interface utilisateur.

```
NSX-edge-8-0> show firewall
Chain PREROUTING (policy ACCEPT 21947 packets, 7809K bytes)
rid    pkts bytes target     prot opt in     out     source               destination

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
rid    pkts bytes target     prot opt in     out     source               destination
)       348 67915 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
)       134  5360 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0           state INVALID
)     21482 7736K block_in   all  --  *      *       0.0.0.0/0            0.0.0.0/0
)     20545 7671K ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED
)       937 65139 usr_rules  all  --  *      *       0.0.0.0/0            0.0.0.0/0
)         0     0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
rid    pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 20673 packets, 1248K bytes)
rid    pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
rid    pkts bytes target     prot opt in     out     source               destination
)       348 67915 ACCEPT     all  --  *      lo      0.0.0.0/0            0.0.0.0/0
)        34  1360 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0           state INVALID
)     20295 1179K block_out  all  --  *      *       0.0.0.0/0            0.0.0.0/0
)         0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           PHYSDEV match
)         0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           PHYSDEV match
)         0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           PHYSDEV match
)         0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           PHYSDEV match
)     14599  802K ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED
)      5696  377K usr_rules  all  --  *      *       0.0.0.0/0            0.0.0.0/0
)         0     0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain block_in (1 references)
rid    pkts bytes target     prot opt in     out     source               destination

Chain block_out (1 references)
rid    pkts bytes target     prot opt in     out     source               destination

Chain usr_rules (2 references)
rid    pkts bytes target     prot opt in     out     source               destination
133137  4861  333K ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           match-set 0_
133138     0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           match-set 1_
133139   936 65099 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           match-set 2_
133141   835 43459 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           match-set 3_
133131     1    40 LOG        all  --  *      *       0.0.0.0/0            0.0.0.0/0           LOG flags 0
133131     1    40 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
```

4 L'équilibrage de charge requiert le bon fonctionnement du NAT. Utilisez la commande `show nat`. Si vous ne voyez pas de sortie logique à l'aide de la commande, consultez la section Dépannage et vérification de la configuration de l'équilibrage de charge à l'aide de l'interface utilisateur.

```
NSX-edge-8-0> show nat
Chain PREROUTING (policy ACCEPT 568 packets, 40044 bytes)
rid    pkts bytes target     prot opt in     out     source               destination
0       568 40044 int_dnat   all  --  *      *       0.0.0.0/0            0.0.0.0/0
0       568 40044 usr_dnat   all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain INPUT (policy ACCEPT 568 packets, 40044 bytes)
rid    pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 896 packets, 46706 bytes)
rid    pkts bytes target     prot opt in     out     source               destination
0       896 46706 int_dnat   all  --  *      *       0.0.0.0/0            0.0.0.0/0
0       896 46706 usr_dnat   all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain POSTROUTING (policy ACCEPT 896 packets, 46706 bytes)
rid    pkts bytes target     prot opt in     out     source               destination
0       896 46706 int_snat   all  --  *      *       0.0.0.0/0            0.0.0.0/0
0       896 46706 usr_snat   all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain int_dnat (2 references)
rid    pkts bytes target     prot opt in     out     source               destination

Chain int_snat (1 references)
rid    pkts bytes target     prot opt in     out     source               destination
0          0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain usr_dnat (2 references)
rid    pkts bytes target     prot opt in     out     source               destination
0          0     0 DNAT       tcp  --  vNic_2 *       0.0.0.0/0            192.168.8.20
0          0     0 LOG        all  --  vNic_2 *       0.0.0.0/0            192.168.8.11
0          0     0 DNAT       all  --  vNic_2 *       0.0.0.0/0            192.168.8.11

Chain usr_snat (1 references)
rid    pkts bytes target     prot opt in     out     source               destination
0          0     0 LOG        all  --  *      vNic_2  10.10.10.101         0.0.0.0/0
0          0     0 SNAT       all  --  *      vNic_2  10.10.10.101         0.0.0.0/0
0          0     0 LOG        all  --  *      vNic_2  10.10.10.0/24         0.0.0.0/0
0          0     0 SNAT       all  --  *      vNic_2  10.10.10.0/24         0.0.0.0/0
NSX-edge-8-0>
```

5 En plus du pare-feu qui est activé et de l'équilibrage de charge qui possède des règles NAT, vous devez aussi vous assurer que le processus d'équilibrage de charge est activé. Utilisez la commande `show service loadbalancer` pour vérifier l'état du moteur de l'équilibrage de charge (L4/L7).

```
nsxedge> show service loadbalancer
haIndex:              0
------------------------------------------------------------------------
Loadbalancer Services Status:

L7 Loadbalancer     : running
------------------------------------------------------------------------
L7 Loadbalancer Statistics:
STATUS     PID        MAX_MEM_MB MAX_SOCK   MAX_CONN   MAX_PIPE   CUR_CONN   CONN_RATE
CONN_RATE_LIMIT MAX_CONN_RATE
running    1580       0          2081       1024       0          0          0
```

```
0               0
------------------------------------------------------------------------
L4 Loadbalancer Statistics:
MAX_CONN   ACT_CONN   INACT_CONN TOTAL_CONN
0          0          0          0

Prot LocalAddress:Port Scheduler Flags
  -> RemoteAddress:Port           Forward Weight ActiveConn InActConn
```

a Utilisez la commande `show service loadbalancer session` pour afficher la table de session de l'équilibrage de charge. Vous verrez des sessions s'il y a du trafic sur le système.

```
nsxedge> show service loadbalancer session
------------------------------------------------------------------------
L7 Loadbalancer Statistics:
STATUS     PID        MAX_MEM_MB MAX_SOCK   MAX_CONN   MAX_PIPE   CUR_CONN   CONN_RATE
CONN_RATE_LIMIT MAX_CONN_RATE
running    1580       0          2081       1024       0          0          0
0               0

------------------L7 Loadbalancer Current Sessions:

0x2192df1f300: proto=unix_stream src=unix:1 fe=GLOBAL be=<NONE> srv=<none> ts=09 age=0s
calls=2 rq[f=c08200h,
i=0,an=00h,rx=20s,wx=,ax=] rp[f=008000h,i=0,an=00h,rx=,wx=,ax=] s0=[7,8h,fd=1,ex=]
s1=[7,0h,fd=-1,ex=] exp=19s


------------------------------------------------------------------------
L4 Loadbalancer Statistics:
MAX_CONN   ACT_CONN   INACT_CONN TOTAL_CONN
0          0          0          0

L4 Loadbalancer Current Sessions:

pro expire state       source       virtual    destination
```

b Vérifiez la commande `show service loadbalancer` pour afficher l'état de table rémanente de couche 7 de l'équilibrage de charge. Remarquez que ce tableau n'affiche pas d'informations sur les serveurs virtuels accélérés.

```
nsxedge> show service loadbalancer table
------------------------------------------------------------------------
L7 Loadbalancer Sticky Table Status:

TABLE    TYPE    SIZE(BYTE)   USED(BYTE)
```

6 Si tous les services requis s'exécutent correctement, étudiez la table de routage : vous devez avoir un itinéraire vers le client et vers les serveurs. Utilisez les commandes `show ip route` et `show ip forwarding` qui mappent des itinéraires avec les interfaces.

```
NSX-edge-8-0> sh ip route

Codes: O - OSPF derived, i - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2,
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

Total number of routes: 4

S       0.0.0.0/0             [1/1]         via 192.168.8.2
C       10.10.10.0/24         [0/0]         via 10.10.10.1
C       169.254.1.4/30        [0/0]         via 169.254.1.5
C       192.168.8.0/24        [0/0]         via 192.168.8.3
NSX-edge-8-0> sh ip forwarding
Codes: C - connected, R - remote,
       > - selected route, * - FIB route

R>* 0.0.0.0/0 via 192.168.8.2, vNic_2
C>* 10.10.10.0/24 is directly connected, vNic_0
C>* 169.254.1.4/30 is directly connected, vNic_0
C>* 192.168.8.0/24 is directly connected, vNic_2
NSX-edge-8-0>
```

7 Assurez-vous d'avoir une entrée ARP pour les systèmes, comme la passerelle ou le tronçon suivant, et les serveurs principaux à l'aide de la commande `show arp`.

```
OneArm-LoadBalancer-01-0>   show arp
------------------------------------------------------------------------
vShield Edge ARP Cache:
IP Address                              Interface  MAC Address        State
fe80::250:56ff:feae:f86b                vNic_0     00:50:56:ae:f8:6b  STALE
fe80::250:56ff:feae:5066                vNic_1     00:50:56:ae:50:66  STALE
fe80::250:56ff:feae:3e3d                vNic_0     00:50:56:ae:3e:3d  STALE
172.16.100.11                           vNic_1     00:50:56:ae:50:66  REACHABLE
172.16.10.1                             vNic_0     02:50:56:56:44:52  REACHABLE
172.16.10.11                            vNic_0     00:50:56:ae:3e:3d  REACHABLE
OneArm-LoadBalancer-01-0>
```

8 Les journaux donnent des informations pour aider à trouver le trafic qui pourrait aider au diagnostic des problèmes. Utilisez les commandes `show log` ou `show log follow` pour suivre le journal qui aidera à détecter le trafic. Remarquez que vous devez exécuter l'équilibrage de charge avec **Journalisation (Logging)** activé, et défini sur **Info** ou **Débogage (Debug)**.

```
nsxedge> show log
2016-04-20T20:15:36+00:00 vShieldEdge kernel: Initializing cgroup subsys cpuset
2016-04-20T20:15:36+00:00 vShieldEdge kernel: Initializing cgroup subsys cpu
2016-04-20T20:15:36+00:00 vShieldEdge kernel: Initializing cgroup subsys cpuacct
...
```

9 Après avoir vérifié que les services de base s'exécutent avec les bons chemins vers les clients, regardons ce qui se passe dans la couche d'application. Utilisez la commande `show service loadbalancer pool` pour afficher l'état du pool de l'équilibrage de charge (L4/L7). Un membre du pool doit être en mesure du servir du contenu ; en général, plusieurs membres sont nécessaires car le volume des requêtes dépasse la capacité d'une seule charge de travail. Si la surveillance de santé est fournie par un contrôle de santé intégré, la sortie affiche `heure de modification du dernier état` et `raison de l'échec` lorsque le contrôle de santé échoue. Si la surveillance de santé est fournie par un service de surveillance, outre les deux sorties citées précédemment, l'`heure du dernier contrôle` s'affiche aussi.

```
nsxedge> show service loadbalancer pool
------------------------------------------------------------------------
Loadbalancer Pool Statistics:

POOL Web-Tier-Pool-01
|  LB METHOD round-robin
|  LB PROTOCOL L7
|  Transparent disabled
|  SESSION (cur, max, total) = (0, 0, 0)
|  BYTES in = (0), out = (0)
   +->POOL MEMBER: Web-Tier-Pool-01/web-01a, STATUS: UP
   |  |  HEALTH MONITOR = BUILT-IN, default_https_monitor:L7OK
   |  |  |  LAST STATE CHANGE: 2016-05-16 07:02:00
   |  |  SESSION (cur, max, total) = (0, 0, 0)
   |  |  BYTES in = (0), out = (0)
   +->POOL MEMBER: Web-Tier-Pool-01/web-02a, STATUS: UP
   |  |  HEALTH MONITOR = BUILT-IN, default_https_monitor:L7OK
   |  |  |  LAST STATE CHANGE: 2016-05-16 07:02:01
   |  |  SESSION (cur, max, total) = (0, 0, 0)
   |  |  BYTES in = (0), out = (0)
```

10 Vérifiez l'état de la surveillance des services (OK, WARNING, CRITICAL) pour voir la santé de tous les serveurs principaux configurés.

```
nsxedge> show service loadbalancer monitor
------------------------------------------------------------------------
Loadbalancer Health Check Statistics:

MONITOR PROVIDER   POOL               MEMBER     HEALTH STATUS
built-in           Web-Tier-Pool-01   web-01a    default_https_monitor:L7OK
built-in           Web-Tier-Pool-01   web-02a    default_https_monitor:L7OK
```

Pour la commande `show service load balancer monitor`, trois types de valeurs de surveillance de santé sont affichés dans la sortie de l'interface de ligne de commande :

- Intégré : la surveillance de santé est activée et est réalisée par le moteur L7 (proxy HA).

- Service de surveillance : la surveillance de santé est activée et est réalisée par le moteur du service de surveillance (NAGIOS). L'état d'exécution du service de surveillance peut être vérifié avec les commandes de l'interface de ligne de commande `show service monitor` et `show service monitor service`. Le champ **État (Status)** doit être `OK`, `AVERTISSEMENT` ou `CRITIQUE`.
- Non défini : la surveillance de santé est désactivée.

La dernière colonne de la sortie est l'état de santé du membre du pool. Les états suivants s'affichent :

Tableau 6-1. État de santé avec une description

État de santé	Description

Intégré	■ UNK : inconnu
	■ INI : initialisation
	■ SOCKERR : erreur de socket
	■ L4OK : vérification effectuée sur la couche 4, aucun test de couche supérieure activé
	■ L4TOUT : expiration de la couche 1 à 4
	■ L4CON : problème de connexion de la couche 1 à 4. Par exemple, « Connexion refusée » (tcp rst) ou « Aucun itinéraire vers l'hôte » (icmp)
	■ L6OK : vérification effectuée sur la couche 6
	■ L6TOUT : expiration de la couche 6 (SSL)
	■ L6RSP : réponse incorrecte de la couche 6 - erreur de protocole. Peut survenir parce que :
	  ■ le serveur principal prend uniquement en charge « SSLv3 » ou « TLSv1.0 », ou
	  ■ le certificat du serveur principal n'est pas valide, ou
	  ■ la négociation du chiffrement a échoué, etc
	■ L7OK : vérification effectuée sur la couche 7
	■ L7OKC : vérification effectuée sous condition sur la couche 7. Par exemple, 404 avec disable-on-404
	■ L7TOUT : expiration de la couche 7 (HTTP/SMTP)
	■ L7RSP : réponse incorrecte de la couche 7 - erreur de protocole
	■ L7STS : erreur de réponse de la couche 7. Par exemple, HTTP 5xx

CRITIQUE	■ La version 2 du protocole SSL n'est pas prise en charge par votre bibliothèque SSL ■ Version du protocole SSL non prise en charge ■ Impossible de créer le contexte SSL ■ Impossible d'établir une connexion SSL ■ Impossible d'initier la négociation SSL ■ Impossible de récupérer le certificat de serveur ■ Impossible de récupérer le sujet du certificat ■ Format d'heure incorrect dans le certificat ■ Le certificat « <cn> » a expiré le <expire time of certificate> ■ Le certificat « <cn> » a expiré aujourd'hui <expire time of certificate>
AVERTISSEMENT/ CRITIQUE	Le certificat « <cn> » expire dans <days_left/expire time of certificate> jour(s)

Tableau 6-1. État de santé avec une description (suite)

État de santé	Description
ICMP	■ Réseau inaccessible ■ Hôte inaccessible ■ Protocole inaccessible ■ Port inaccessible ■ Échec de l'itinéraire source ■ Hôte source isolé ■ Réseau inconnu ■ Hôte inconnu ■ Réseau refusé ■ Hôte refusé ■ Type de service (ToS) incorrect pour le réseau ■ Type de service (ToS) incorrect pour l'hôte ■ Interdit par le filtre ■ Violation de la priorité d'hôte ■ Limite de priorité. Niveau minimal de priorité requis pour l'opération ■ Code non valide
UDP/TCP	■ Échec de la création du socket ■ Connexion à l'adresse xxxx et au port xxx : [consultez Code d'erreur Linux] ■ Aucune donnée reçue de l'hôte ■ Réponse inattendue de la part de l'hôte/socket
HTTP/HTTPS	■ HTTP INCONNU : erreur d'allocation de mémoire ■ HTTP CRITIQUE : impossible d'ouvrir le socket TCP (échec de la création du socket ou de la connexion au serveur) ■ HTTP CRITIQUE : erreur lors de la réception des données ■ HTTP CRITIQUE : aucune donnée reçue de l'hôte ■ HTTP CRITIQUE : réponse HTTP non valide reçue de la part de l'hôte : <status line> (format de ligne de format attendu incorrect) ■ HTTP CRITIQUE : ligne d'état non valide <status line> (le code d'état ne contient pas 3 chiffres : XXX) ■ HTTP CRITIQUE : état non valide <status line> (code d'état >= 600 ou < 100) ■ HTTP CRITIQUE : chaîne introuvable ■ HTTP CRITIQUE : modèle introuvable ■ HTTP AVERTISSEMENT : taille de page <page_length> trop grande ■ HTTP AVERTISSEMENT : taille de page <page_length> trop petite

11 Lorsque le code d'erreur est L4TOUT/L4CON, c'est qu'il y a généralement des problèmes de connectivité sur la mise en réseau sous-jacente. `Duplicate IP` se produit souvent comme cause première avec ce type de raison. Lorsque cette erreur se produit, le dépannage se présente comme suit :

   a Vérifiez l'état de Haute disponibilité (HA) des Edge, lorsque la haute disponibilité est activée à l'aide de la commande `show service highavailability` sur les deux Edge. Vérifiez si le lien Haute disponibilité est DÉSACTIVÉ et si tous les Edges sont `Active`, pour qu'il n'y ait plus d'IP Edge en doublon sur le réseau.

   b Vérifiez la table ARP Edge par la commande `show arp` et vérifiez si l'entrée ARP du serveur principal est modifiée entre les deux adresses MAC.

   c Vérifiez la table ARP du serveur principal ou utilisez la commande `arp-ping`, puis vérifiez si une autre machine à la même IP que l'IP Edge.

12 Vérifiez les statistiques de l'objet d'équilibrage de charge (VIP, pools, membres). Regardez le pool spécifique et vérifiez que les membres sont prêts et exécutés. Vérifiez si le mode transparent est activé. Si oui, Edge Services Gateway doit être en ligne entre le client et le serveur. Vérifiez si les serveurs affichent les incréments de compteur de sessions.

```
nsxedge> show service loadbalancer pool Web-Tier-VIP-01
TIMESTAMP                SESSIONS       BYTESIN        BYTESOUT       SESSIONRATE    HTTPREQS
2016-04-27 19:56:40      00             00             00             00             00
2016-04-27 19:55:00      00             32             100            00             00
```

```
nsxedge> show service loadbalancer pool Web-Tier-VIP-01 | MEMBER
+-> POOL MEMBER: TENANT-1-TCP-POOL-80/SERVER-1, STATUS:  UP
+-> POOL MEMBER: TENANT-1-TCP-POOL-80/SERVER-2, STATUS:  UP
```

13 Étudiez à présent le serveur virtuel et vérifiez s'il y a un pool par défaut et voyez si le pool y est lié aussi. Si vous utilisez des pools via des règles d'application, vous devez étudier de plus près des pools spécifiques comme illustré dans la commande `#show service loadbalancer pool`. Spécifiez le nom du serveur virtuel.

```
nsxedge> show service loadbalancer virtual Web-Tier-VIP-01

------------------------------------------------------------------------
Loadbalancer VirtualServer Statistics:

VIRTUAL Web-Tier-VIP-01
|  ADDRESS [172.16.10.10]:443
|  SESSION (cur, max, total) = (0, 0, 0)
|  RATE (cur, max, limit) = (0, 0, 0)
|  BYTES in = (0), out = (0)
   +->POOL Web-Tier-Pool-01
   |  LB METHOD round-robin
   |  LB PROTOCOL L7
   |  Transparent disabled
```

```
|  SESSION (cur, max, total) = (0, 0, 0)
|  BYTES in = (0), out = (0)
   +->POOL MEMBER: Web-Tier-Pool-01/web-01a, STATUS: UP
   |  |  HEALTH MONITOR = BUILT-IN, default_https_monitor:L7OK
   |  |  |  LAST STATE CHANGE: 2016-05-16 07:02:00
   |  |  SESSION (cur, max, total) = (0, 0, 0)
   |  |  BYTES in = (0), out = (0)
   +->POOL MEMBER: Web-Tier-Pool-01/web-02a, STATUS: UP
   |  |  HEALTH MONITOR = BUILT-IN, default_https_monitor:L7OK
   |  |  |  LAST STATE CHANGE: 2016-05-16 07:02:01
   |  |  SESSION (cur, max, total) = (0, 0, 0)
   |  |  BYTES in = (0), out = (0)
```

14 Si tout a l'air d'être configuré correctement et que vous avez encore une erreur, vous devez capturer le trafic pour comprendre ce qu'il se passe. Il y a deux connexions : entre client et serveur virtuel, et entre Edge Services Gateway et le pool principal (avec ou sans la configuration transparente au niveau du pool). La commande `#show ip forwarding` a indiqué les interfaces vNIc et vous pouvez utiliser ces données.

Par exemple, supposez que l'ordinateur client est sur *vNic_0* et que le serveur est sur *vNic_1*. Vous utilisez l'adresse IP cliente *192.168.1.2* et l'adresse IP VIP *192.168.2.2* exécutées sur le port 80. IP de l'interface de l'équilibrage de charge et un serveur principal IP de *192.168.3.3*. Il existe deux commandes de capture de paquets différentes : une qui affiche les paquets alors que l'autre capture les paquets dans le fichier à télécharger. Capturez les paquets pour détecter l'échec anormal de l'équilibrage de charge. Vous pouvez capturer les paquets à partir de deux directions :

- Capturer les paquets du client.
- Capturer les paquets envoyés au serveur principal.

```
#debug packet capture interface interface-name [filter using _ for space]- creates a packet
capture file that you can download
#debug packet display interface interface-name [filter using _ for space]- outputs packet data to
the console
#debug show files - to see a list of packet capture
#debug copy scp user@url:path file-name/all - to download the packet capture
```

Par exemple :

- Capture sur vNIC_0 : `debug packet display interface vNic_0`
- Capture sur toutes les interfaces : `debug packet display interface any`
- Capture sur vNIC_0 avec un filtre :`debug packet display interface vNic_0 host_192.168.11.3_and_host_192.168.11.41`
- Une capture de paquet du client vers le trafic du serveur virtuel : `#debug packet display|capture interface vNic_0 host_192.168.1.2_and_host_192.168.2.2_and_port_80`
- Une capture de paquet entre Edge Services Gateway et le serveur où le pool est en mode transparent : `#debug packet display|capture interface vNic_1 host 192.168.1.2_and_host_192.168.3.3_and_port_80`

- Une capture de paquet entre Edge Services Gateway et le serveur n'est pas en mode transparent : `#debug packet display|capture interface vNic_1 host 192.168.3.1_and_host_192.168.3.3_and_port_80`

Problèmes courants d'équilibrage de charge

Cette rubrique aborde plusieurs problèmes et leur résolution.

Les problèmes suivants sont courants lorsque l'équilibrage de charge NSX est utilisé :

- L'équilibrage de charge sur le port TCP (par exemple, le port 443) ne fonctionne pas.
  - Vérifiez la topologie. Pour plus de détails, consultez le *Guide d'administration de NSX*.
  - Vérifiez que l'adresse IP du serveur virtuel est accessible avec une commande ping ou vérifiez le routeur en amont pour vous assurer que la table ARP est renseignée.
  - Dépannage et vérification de la configuration de l'équilibrage de charge à l'aide de l'interface utilisateur.
  - Dépannage de l'équilibrage de charge à l'aide de l'interface de ligne de commande.
  - Capturez des paquets.
- Un membre du pool d'équilibrage de charge n'est pas utilisé.
  - Vérifiez que le serveur se trouve dans le pool, qu'il est activé et surveillez son état de santé.
- Le trafic Edge n'est pas à équilibrage de charge.
  - Vérifiez le pool et la configuration de persistance. Si la persistance est configurée et que vous utilisez un petit nombre de clients, il se peut que vous ne voyiez pas une distribution uniforme des connexions aux membres du pool principal.
- Le moteur d'équilibrage de charge de couche 7 est arrêté.
- Le moteur du moniteur de santé est arrêté.
  - Activez le service d'équilibrage de charge. Consultez le *Guide d'administration de NSX*.
- L'état du moniteur du membre du pool est AVERTISSEMENT/CRITIQUE.
  - Vérifiez que le serveur d'applications est accessible à partir de l'équilibrage de charge.
  - Vérifiez que le pare-feu du serveur d'applications ou DFW autorise le trafic.
  - Assurez-vous que le serveur d'applications peut répondre à la sonde d'intégrité spécifiée.
- Le membre du pool présente l'état INACTIF.
  - Vérifiez que le membre du pool est activé dans la configuration du pool.
- La table rémanente de couche 7 n'est pas synchronisée avec le dispositif Edge en veille.
  - Vérifiez que la haute disponibilité (HA) est configurée.

- Connexions client, mais impossible d'effectuer une transaction d'application.
  - Vérifiez que la persistance adéquate est configurée dans le profil d'application.
  - Si l'application fonctionne avec un seul serveur dans le pool (et non deux), il s'agit très probablement d'un problème de persistance.

Dépannage de base

1 Vérifiez l'état de la configuration de l'équilibrage de charge dans vSphere Web Client :

   a Cliquez sur **Mise en réseau et sécurité > Dispositifs NSX Edge (Networking & Security > NSX Edges)**.

   b Double-cliquez sur une instance de NSX Edge.

   c Cliquez sur **Gérer (Manage)**, puis sur l'onglet **Équilibrage de charge (Load Balancer)**.

   d Vérifiez l'état de l'équilibrage de charge et le niveau de journalisation configuré.

2 Avant de dépanner le service d'équilibrage de charge, exécutez la commande suivante sur le dispositif NSX Manager pour vous assurer que le service est actif et en cours d'exécution :

```
nsxmgr> show edge edge-4 service loadbalancer
haIndex:              0
------------------------------------------------------------------------
Loadbalancer Services Status:

L7 Loadbalancer     : running
------------------------------------------------------------------------
L7 Loadbalancer Statistics:
STATUS     PID        MAX_MEM_MB MAX_SOCK   MAX_CONN   MAX_PIPE   CUR_CONN   CONN_RATE
CONN_RATE_LIMIT MAX_CONN_RATE
running    1580       0          2081       1024       0          0          0
0               0
------------------------------------------------------------------------
L4 Loadbalancer Statistics:
MAX_CONN   ACT_CONN   INACT_CONN TOTAL_CONN
0          0          0          0

Prot LocalAddress:Port Scheduler Flags
  -> RemoteAddress:Port           Forward Weight ActiveConn InActConn
```

Note Vous pouvez exécuter `show edge all` pour rechercher les noms des dispositifs NSX Edge.

Dépannage des problèmes de configuration

Lorsque l'opération de configuration de l'équilibrage de charge est refusée par l'interface utilisateur de NSX ou l'appel API REST, elle est classée comme problème de configuration.

Dépannage des problèmes du plan de données

La configuration de l'équilibrage de charge est acceptée par NSX Manager, mais il existe des problèmes de connectivité ou de performance entre le dispositif Edge client et le serveur d'équilibrage de charge. Les problèmes de plan de données incluent également des problèmes de CLI d'exécution de l'équilibrage de charge et des problèmes d'événement système de l'équilibrage de charge.

1 Passez le niveau de journalisation du dispositif Edge dans NSX Manager de INFO à TRACE ou DÉBOGAGE à l'aide de l'appel API REST.

```
URL: https://NSX_Manager_IP/api/1.0/services/debug/loglevel/com.vmware.vshield.edge?level=TRACE
Method: POST
```

2 Vérifiez l'état de membre du pool dans vSphere Web Client.

   a Cliquez sur **Mise en réseau et sécurité > Dispositifs NSX Edge (Networking & Security > NSX Edges)**.

   b Double-cliquez sur une instance de NSX Edge.

   c Cliquez sur **Gérer (Manage)**, puis sur l'onglet **Équilibrage de charge (Load Balancer)**.

   d Cliquez sur **Pools** pour voir un résumé des pools d'équilibrages de charge configurés.

   e Sélectionnez votre pool d'équilibrages de charge. Cliquez sur **Afficher les statistiques du pool (Show Pool Statistics)** et vérifiez que l'état du pool est ACTIF.

3 Vous pouvez obtenir des statistiques de configuration du pool d'équilibrages de charge plus détaillées à partir du dispositif NSX Manager à l'aide de l'appel API REST suivant :

```
URL: https://NSX_Manager_IP/api/4.0/edges/{edgeId}/loadbalancer/statistics
Method: GET

<?xml version="1.0" encoding="UTF-8"?>
<loadBalancerStatusAndStats>
    <timeStamp>1463507779</timeStamp>
    <pool>
        <poolId>pool-1</poolId>
        <name>Web-Tier-Pool-01</name>
        <member>
            <memberId>member-1</memberId>
            <name>web-01a</name>
            <ipAddress>172.16.10.11</ipAddress>
            <status>UP</status>
            <lastStateChangeTime>2016-05-16 07:02:00</lastStateChangeTime>
            <bytesIn>0</bytesIn>
            <bytesOut>0</bytesOut>
            <curSessions>0</curSessions>
            <httpReqTotal>0</httpReqTotal>
            <httpReqRate>0</httpReqRate>
            <httpReqRateMax>0</httpReqRateMax>
            <maxSessions>0</maxSessions>
            <rate>0</rate>
```

```
            <rateLimit>0</rateLimit>
            <rateMax>0</rateMax>
            <totalSessions>0</totalSessions>
        </member>
        <member>
            <memberId>member-2</memberId>
            <name>web-02a</name>
            <ipAddress>172.16.10.12</ipAddress>
            <status>UP</status>
            <lastStateChangeTime>2016-05-16 07:02:01</lastStateChangeTime>
            <bytesIn>0</bytesIn>
            <bytesOut>0</bytesOut>
            <curSessions>0</curSessions>
            <httpReqTotal>0</httpReqTotal>
            <httpReqRate>0</httpReqRate>
            <httpReqRateMax>0</httpReqRateMax>
            <maxSessions>0</maxSessions>
            <rate>0</rate>
            <rateLimit>0</rateLimit>
            <rateMax>0</rateMax>
            <totalSessions>0</totalSessions>
        </member>
        <status>UP</status>
        <bytesIn>0</bytesIn>
        <bytesOut>0</bytesOut>
        <curSessions>0</curSessions>
        <httpReqTotal>0</httpReqTotal>
        <httpReqRate>0</httpReqRate>
        <httpReqRateMax>0</httpReqRateMax>
        <maxSessions>0</maxSessions>
        <rate>0</rate>
        <rateLimit>0</rateLimit>
        <rateMax>0</rateMax>
        <totalSessions>0</totalSessions>
    </pool>
    <virtualServer>
        <virtualServerId>virtualServer-1</virtualServerId>
        <name>Web-Tier-VIP-01</name>
        <ipAddress>172.16.10.10</ipAddress>
        <status>OPEN</status>
        <bytesIn>0</bytesIn>
        <bytesOut>0</bytesOut>
        <curSessions>0</curSessions>
        <httpReqTotal>0</httpReqTotal>
        <httpReqRate>0</httpReqRate>
        <httpReqRateMax>0</httpReqRateMax>
        <maxSessions>0</maxSessions>
        <rate>0</rate>
        <rateLimit>0</rateLimit>
        <rateMax>0</rateMax>
        <totalSessions>0</totalSessions>
    </virtualServer>
</loadBalancerStatusAndStats>
```

4 Pour vérifier les statistiques d'équilibrage de charge à partir de la ligne de commande, exécutez les commandes suivantes sur le dispositif NSX Edge.

   Pour un serveur virtuel particulier : exécutez d'abord `show service loadbalancer virtual` pour obtenir le nom du serveur virtuel. Exécutez ensuite `show statistics loadbalancer virtual <virtual-server-name>`.

   Pour un pool TCP particulier : exécutez d'abord `show service loadbalancer pool` pour obtenir le nom du pool. Exécutez ensuite `show statistics loadbalancer pool <pool-name>`.

5 Examinez les statistiques de l'équilibrage de charge pour rechercher des signes d'échec.

Dépannage de VPN (Virtual Private Network) 7

NSX Edge prend en charge plusieurs types de VPN. Cette section de dépannage décrit comment dépanner les problèmes VPN L2 et VPN SSL.

Ce chapitre contient les rubriques suivantes :

VPN L2

Avec VPN L2, vous pouvez étendre plusieurs réseaux logiques L2 (VLAN et VXLAN) sur des limites L3, connectés par tunnel dans un VPN SSL. Il est en outre possible de configurer plusieurs sites sur un serveur VPN de niveau 2 (L2). Les machines virtuelles demeurent sur le même sous-réseau lorsqu'elles sont déplacées entre des sites et leurs adresses IP ne changent pas. Vous pouvez également déployer un dispositif Edge autonome sur un site distant sans que NSX soit « activé » sur ce site. L'optimisation côté sortie permet à Edge de router n'importe quel paquet envoyé localement vers l'adresse IP d'optimisation côté sortie et de ponter tout le reste.

VPN L2 permet donc aux entreprises de migrer de façon transparente des charges de travail reposant sur VXLAN ou VLAN entre des emplacements physiques distincts. Pour les fournisseurs de cloud, VPN L2 fournit un mécanisme aux locataires intégrés sans modifier les adresses IP existantes des charges de travail et des applications.

Problèmes de configuration courants VPN L2

Cette rubrique décrit les problèmes courants de configuration liés à VPN L2.

Problème

Voici quelques problèmes de configuration courants :

- Le client VPN L2 est configuré, mais le pare-feu Internet n'autorise pas la circulation du trafic dans le tunnel via le port de destination 443.

- Le client VPN L2 est configuré pour valider le certificat du serveur, mais il n'est pas configuré avec le certificat d'autorité de certification ou le nom de domaine complet qui convient.
- Le serveur VPN L2 est configuré, mais la règle du NAT/pare-feu n'est pas créée sur un pare-feu Internet.
- L'interface de carte réseau virtuelle n'est pas soutenue par un groupe de ports distribué ou un groupe de ports standard.

Note Le serveur VPN L2 écoute sur le port 443 par défaut. Ce port est configurable à partir des paramètres du serveur VPN L2.

Le client VPN L2 lance une connexion sortante vers le port 443 par défaut. Ce port est configurable à partir des paramètres du client VPN L2.

Solution

1 Vérifiez si le processus du serveur VPN L2 est exécuté.
   a Connectez-vous à la machine virtuelle NSX Edge.
   b Exécutez la commande `show process monitor` et vérifiez si vous pouvez trouver un processus portant le nom *l2vpn*.
   c Exécutez la commande `show service network-connections` et vérifiez si le processus *l2vpn* écoute sur le port 443.
2 Vérifiez si le processus du client VPN L2 est exécuté.
   a Connectez-vous à la machine virtuelle NSX Edge.
   b Exécutez la commande `show process monitor`, puis vérifiez si vous pouvez trouver un processus portant le nom *nacliendt*.
   c Exécutez la commande `show service network-connections`, puis vérifiez si le processus *nacliendt* écoute sur le port 443.
3 Vérifiez si le serveur VPN L2 est accessible depuis Internet.
   a Ouvrez le navigateur, puis rendez-vous sur **`https://<l2vpn-public-ip>`**.
   b Une page de connexion au portail devrait s'afficher. Si la page du portail s'affiche, cela signifie que le serveur VPN L2 est accessible par Internet.
4 Vérifiez si l'interface de carte réseau virtuelle est soutenue par un groupe de ports distribué ou par un groupe de ports standard.
   a Si l'interface de carte réseau virtuelle est soutenue par un groupe de ports distribué, un port de réception est défini automatiquement.
   b Si l'interface de carte réseau virtuelle est soutenue par un groupe de ports standard, vous devez configurer manuellement le commutateur distribué vSphere comme suit :
      - Donnez au port le mode de **promiscuité (promiscuous)**.
      - Donnez à l'option **Transmissions forcées (Forged Transmits)** la valeur **Accepter (Accept)**.

5 Limitez le problème de bouclage VPN L2.

a Deux grands problèmes sont observés si l'association NIC n'est pas configurée correctement : MAC flapping et paquets en doublons. Vérifiez la configuration comme décrit dans Options L2VPN pour limiter le bouclage

6 Vérifiez si les VM du VPN L2 peuvent communiquer entre elles.

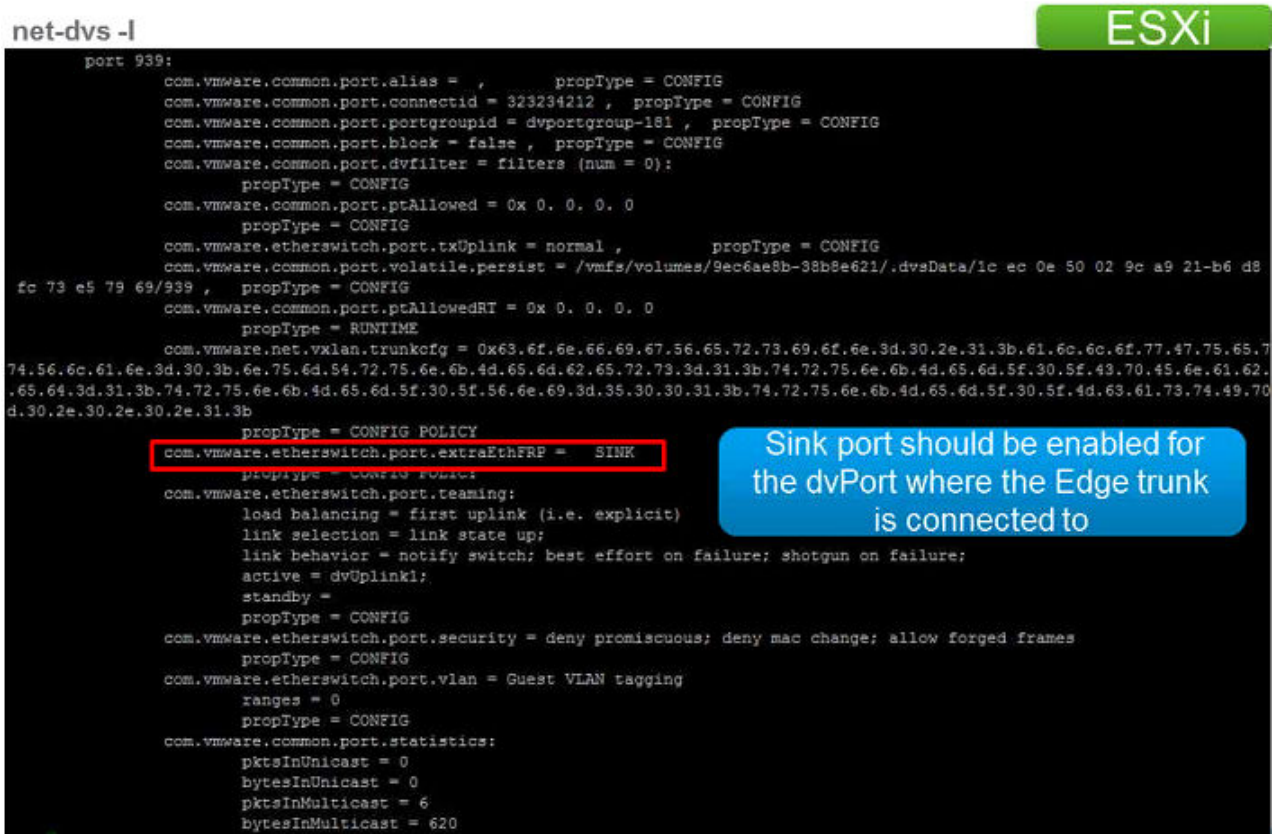
a Connectez-vous à la CLI du serveur VPN L2, puis capturez le paquet sur l'interface tactile correspondante `debug packet capture interface name`.

b Connectez-vous au client VPN L2, puis capturez la capture de paquet sur l'interface tactile correspondante `debug packet capture interface name`.

c Analysez ces captures pour vérifier si l'ARP est en cours de résolution et la circulation du trafic des données.

d Vérifiez si la propriété `Allow Forged Transmits: dvSwitch` est définie sur le port de carte réseau virtuelle *VPN L2*.

e Vérifiez si le port de réception est défini sur *port de carte réseau virtuelle du VPN*. Pour ce faire, connectez-vous à l'hôte et émettez la commande `net-dvs -l`. Vérifiez que la propriété de réception est bien définie pour le port interne Edge VPN L2 (`com.vmware.etherswitch.port.extraEthFRP = SINK`). Le port interne renvoie au *dvPort* à laquelle la carte réseau virtuelle NSX Edge est connectée.

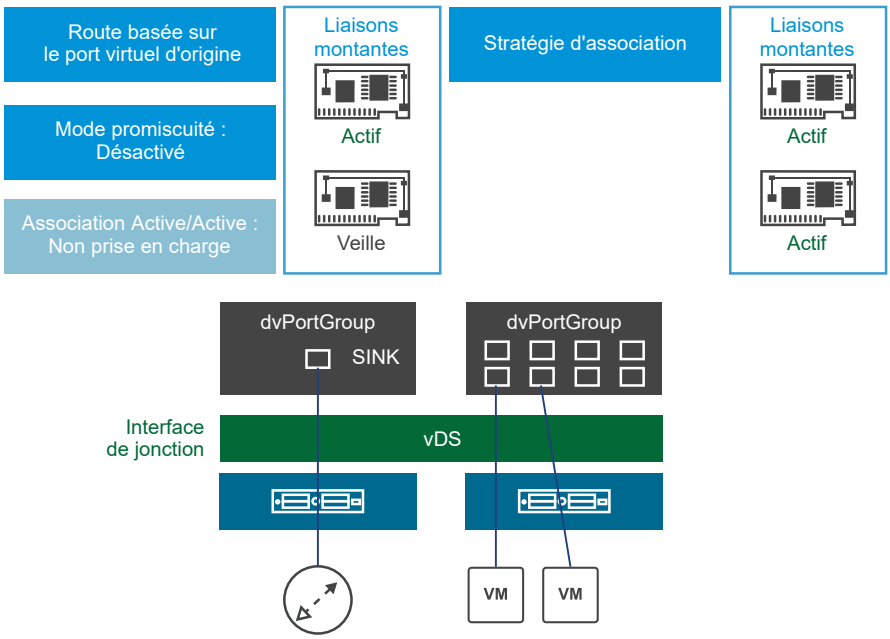


Options L2VPN pour limiter le bouclage

Deux options permettent de limiter le bouclage. Les dispositifs NSX Edge et les machines virtuelles peuvent résider sur un seul ou sur plusieurs hôtes ESXi différents.

Option 1 : Dispositifs Edge L2VPN et machines virtuelles sur des hôtes ESXi différents

1. Déployer les machines virtuelles et les dispositifs Edges L2VPN sur des hôtes ESXi distincts



1 Déployez les dispositifs Edge et les machines virtuelles sur des hôtes ESXi distincts.

2 Configurez comme suit la règle d'association et de basculement pour le groupe de ports distribués associé à la carte réseau virtuelle du dispositif Edge :

   a Définissez l'équilibrage de charge sur Itinéraire basé sur le port virtuel d'origine.

   b Configurez une liaison montante comme active et mettez l'autre en veille.

3 Configurez comme suit la règle d'association et de basculement pour le groupe de ports distribués associé aux machines virtuelles :

   a Toutes les règles d'association conviennent.

   b Plusieurs liaisons montantes actives peuvent être configurées.

4 Configurez les dispositifs Edge pour qu'ils utilisent le mode de port de réception et désactivez le mode de promiscuité sur la carte réseau virtuelle.

Note

- Désactiver le mode Proximité : si vous utilisez vSphere Distributed Switch.
- Activer le mode Proximité : si vous utilisez un commutateur virtuel pour configurer l'interface de jonction.

Si le mode Proximité est activé sur un commutateur virtuel, certains des paquets provenant des liaisons montantes qui ne sont pas actuellement utilisées par le port de proximité ne sont pas ignorés. Vous devez activer et désactiver `ReversePathFwdCheckPromisc` qui va ignorer explicitement tous les paquets provenant des liaisons montantes actuellement inutilisées, pour le port de proximité.

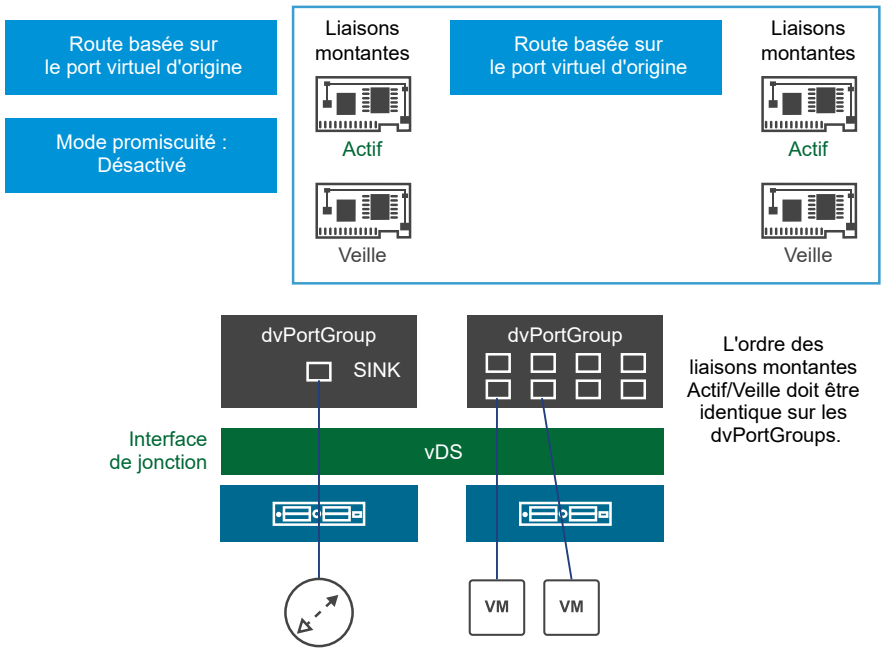
Pour bloquer les paquets en double, activez la vérification RPF pour le mode Proximité à partir de l'interface de ligne de commande ESXi sur laquelle NSX Edge est présent :

```
esxcli system settings advanced set –o /Net/ReversePathFwdCheckPromisc –i 1
esxcli system settings advanced list –o /Net/ReversePathFwdCheckPromisc
Path: /Net/ReversePathFwdCheckPromisc
Type: integer
Int Value: 1
Default Int Value: 0
Max Value: 1
Min Value: 0
String Value:
Default String Value:
Valid Characters:
Description: Block duplicate packet in a teamed environment when the virtual switch is set to
Promiscuous mode.
```

Dans la stratégie de sécurité **Groupe de ports (PortGroup)**, passez l'option **Mode de proximité (PromiscousMode)** de **Accepter (Accept)** à **Refuser (Reject)**, puis définissez-la de nouveau sur **Accepter (Accept)** pour activer la modification configurée.

- Option 2 : Dispositifs Edge et machines virtuelles sur le même hôte ESXi

2. Déployer les machines virtuelles et les dispositifs Edges L2VPN sur le même hôte



a Configurez comme suit la stratégie d'association et de basculement du groupe de ports distribués associé à la carte réseau virtuelle de jonction du dispositif Edge :

   1 Définissez l'équilibrage de charge sur Itinéraire basé sur le port virtuel d'origine.

   2 Configurez une liaison montante comme active et mettez l'autre en veille.

b Configurez comme suit la règle d'association et de basculement pour le groupe de ports distribués associé aux machines virtuelles :

   1 Toutes les règles d'association conviennent.

   2 Une seule liaison montante peut être active.

   3 L'ordre des liaisons montantes actives/en veille doit être identique pour le groupe de ports distribués des machines virtuelles et celui de la carte réseau virtuelle du dispositif Edge.

c Configurez le dispositif Edge autonome côté client pour qu'il utilise le mode de port de réception et désactivez le mode de promiscuité sur la carte réseau virtuelle.

Dépannage à l'aide de la CLI

Vous pouvez utiliser l'interface de ligne de commande 'CLI) NSX pour réaliser quelques tâches de dépannage du VPN L2.

Problème

Le VPN L2 ne fonctionne pas comme prévu.

Solution

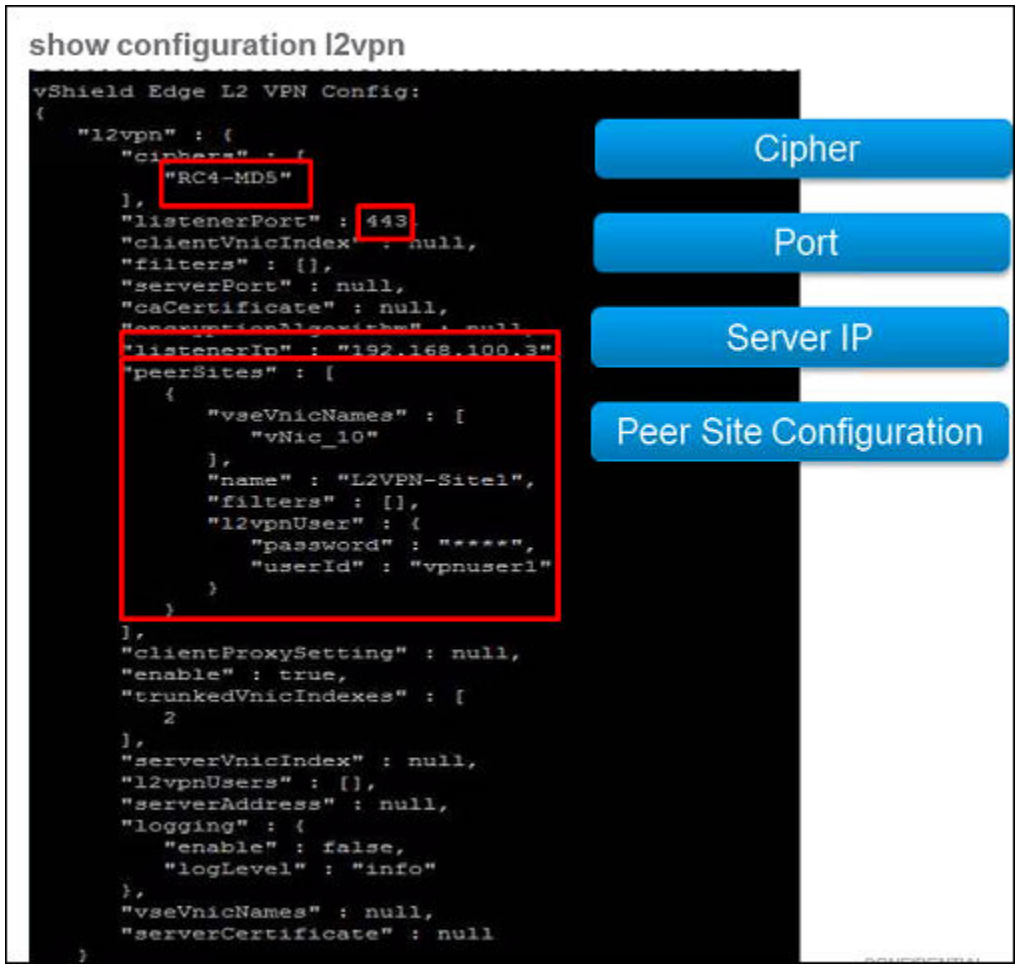
1 Utilisez la commande CLI centrale suivante pour voir les problèmes de configuration :

`show edge <edgeID> configuration l2vpn.`

Par exemple, `show edge edge-1 configuration l2vpn.`

2 Utilisez les commandes suivantes sur le client et le serveur Edge :

- `show configuration l2vpn` : vérifiez les quatre valeurs clés suivantes pour vérifier le serveur.



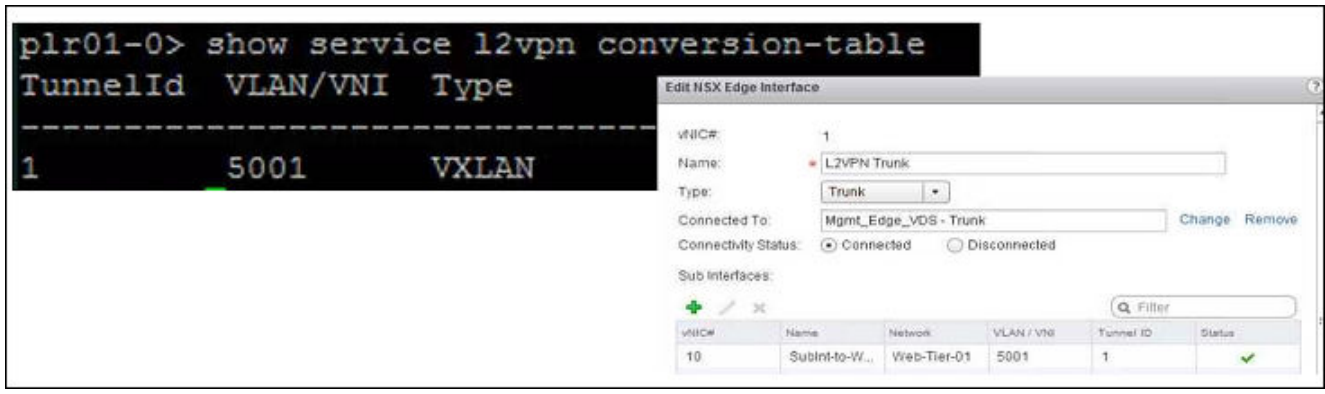
- `show service l2vpn bridge` : le nombre d'interfaces dépend du nombre de clinets VPN L2. Dans la sortie ci-dessous, un seul client VPN L2 (na1) est configuré. Port1 renvoie à *vNic_2*. L'adresse MAC de 02:50:56:56:44:52 a été apprise sur l'interface *vNic_2* et n'est pas locale à Edge (serveur VPN L2). La ligne 3 de l'exemple suivant renvoie à l'interface *na1*.

```
plr01-0> show service l2vpn bridge

bridge name     bridge id              STP enabled     interfaces
br-sub          8000.0050568e19fb      no              vNic_2
                                                       na1

List of learned MAC addresses for L2 VPN bridge br-sub
-----------------------------------------------------------------
port no mac addr                is local?       vlanid          ageing timer
  1     00:50:56:8e:19:fb       yes             0                 0.00
  1     02:50:56:56:44:52       no              1                 0.87
  2     2a:56:30:31:7e:3b       yes             0                 0.00
```

- `show service l2vpn trunk table`
- `show service l2vpn conversion table` : dans l'exemple suivant, une trame Ethernet qui arrive sur le tunnel n° 1 présentera un ID VLAN n°1 converti en VXLAN avec un numéro VLAN de 5001 avant que le paquet soit transmis au VDS.



- `show process monitor` : identifiez si les processus l2vpn (serveur) et naclientd (client) sont en cours d'exécution.
- `show service network-connections` : identifiez si les processus l2vpn (serveur) et naclientd (client) écoutent sur le port 443.

VPN SSL

Vous pouvez utiliser ces informations pour résoudre les problèmes liés à votre configuration.

Le portail Web VPN SSL ne s'ouvre pas

Les utilisateurs de VPN SSL ne peuvent pas ouvrir la page de connexion au portail Web VPN SSL pour télécharger et installer le module d'installation du client VPN-Plus SSL.

Problème

La page de connexion au portail Web VPN SSL ne s'ouvre pas ou la page s'affiche de manière incorrecte dans votre navigateur système.

Cause

L'une des raisons suivantes peut provoquer ce problème :

- Votre système utilise une version de navigateur non prise en charge.
- Les cookies et JavaScript ne sont pas activés dans votre navigateur.

Solution

1 Assurez-vous que vous ouvrez la page de connexion au portail Web VPN SSL dans l'un des navigateurs pris en charge suivants.

Navigateur	Versions prises en charge minimales
Internet Explorer	9.0.8112.16421
Chrome	67.03396
Safari	10.x

2 Ouvrez les paramètres de votre navigateur et vérifiez que les cookies et JavaScript sont activés.

3 Si la langue du navigateur n'est pas définie sur Anglais, définissez la langue sur Anglais et voyez si le problème persiste.

4 Vérifiez que vous avez sélectionné le chiffrement AES sur le serveur VPN SSL. Certains navigateurs ne prennent pas en charge le chiffrement AES.

VPN-Plus SSL : échecs d'installation

Utilisez cette rubrique pour comprendre les probables problèmes d'installation spécifiques du client VPN-Plus SSL et la manière de les résoudre.

Problème

Les problèmes courants liés à l'installation du client VPN-Plus SSL sont les suivants :

- Le client VPN-Plus SSL est installé correctement, mais il ne fonctionne pas.
- Sur les machines Mac, des messages d'avertissement d'extension du noyau s'affichent.
- Sous Mac OS High Sierra, les messages d'erreur d'installation suivants s'affichent :

```
/opt/sslvpn-plus/naclient/signed_kext/tap.kext failed to load - (libkern/kext)system policy
prevents
loading; check the system/kernel logs for errors or try kextutil(8).
Error: Could not load /opt/sslvpn-plus/naclient/signed_kext/tap.kext
```

```
installer[4571] <Debug>: install:didFailWithError:Error Domain=
PKInstallErrorDomain Code=112 "An error occurred while running scripts from the package
“naclient.pkg”.
" UserInfo={NSFilePath=./postinstall,NSURL=file://<pathtofile>/
naclient.pkg,PKInstallPackageIdentifier=
com.vmware.sslvpn,NSLocalizedDescription=An error occurred while running scripts from the
package “naclient.pkg”.}
```

```
installer[4571] <Error>: Install failed: The Installer encountered an error that caused the
installation to fail. Contact the software manufacturer for assistance.
installer: The install failed (The Installer encountered an error that caused the installation to
fail.
Contact the software manufacturer for assistance.)
```

- Sur les machines Windows, le message d'erreur suivant s'affiche : `Échec de l'installation avec le motif E000024B : essayez de redémarrer la machine.`

Cause

L'une des raisons suivantes peut provoquer l'échec du client VPN-Plus SSL même s'il a été installé correctement sur votre ordinateur :

- Le fichier de configuration (naclient.cfg) est manquant ou le fichier de configuration n'est pas valide.
- Les autorisations de répertoire ou les autorisations de l'utilisateur sont incorrectes.
- Le serveur VPN SSL n'est pas accessible.
- Sur les machines Linux et Mac, le pilote tap n'est pas chargé.

Sur les machines Mac, des messages d'avertissement d'extension du noyau s'affichent, car votre système bloque le chargement de l'extension du noyau.

Sous Mac OS High Sierra, des erreurs d'installation s'affichent lorsque votre machine Mac n'autorise pas l'extension de noyau (kext) et il ne vous invite pas non plus à charger la kext.

Sur les machines Windows, le message d'échec d'installation du pilote (E000024B) s'affiche, car vous avez activé l'option **Masquer l'adaptateur réseau SSL du client (Hide SSL client network adapter)** dans l'installateur du client VPN-Plus SSL Edge.

Solution

1. Vérifiez que vous installez le client VPN-Plus SSL sur des systèmes d'exploitation pris en charge. Pour plus d'informations sur les systèmes d'exploitation pris en charge, consultez la rubrique Présentation de VPN-Plus SSL dans le *Guide d'administration de NSX*.
2. Sur les machines Windows, vérifiez que les utilisateurs qui installent le client VPN-Plus SSL disposent des privilèges **d'administrateur**. Sur les machines Linux et Mac, les utilisateurs doivent disposer des privilèges **racine** pour installer le client VPN-Plus SSL. De plus, pour que le client VPN-Plus SSL démarre et s'exécute correctement sur les machines Mac, les utilisateurs doivent disposer des autorisations **d'exécution** sur le répertoire `/usr/local/lib`.
3. Sur les machines Linux, vérifiez que les bibliothèques suivantes sont installées. Ces bibliothèques sont requises pour que l'interface utilisateur fonctionne.
   - TCL
   - TK
   - NSS

4 Si le pilote tap n'est pas chargé sur les machines Mac et Linux, exécutez le script shell pour charger le pilote.

Système d'exploitation	Description
Mac	Exécutez le script shell `Naclient.sh` du répertoire `/opt/sslvpn-plus/naclient/` avec des privilèges **sudo**.
Linux	Exécutez le script shell `naclient.sh` avec des privilèges **sudo**. Vous trouverez ce script dans le répertoire `linux_phat_client/linux_phat_client`.

5 Pour résoudre les messages d'avertissement d'extension de noyau sur des machines avec macOS High Sierra ou version ultérieure, vous devez fournir l'approbation d'utilisateur explicite pour le chargement d'une extension de noyau (kext). Procédez comme suit :

a Sur votre machine Mac, ouvrez la fenêtre **Préférences système (System Preferences) > Sécurité et confidentialité (Security & Privacy)**.

b En bas de la fenêtre, vous pouvez voir un message semblable à « `Le chargement de certains logiciels système a été bloqué.` » `Cliquez sur le bouton « Autoriser ».`

c Pour effectuer l'installation, cliquez sur **Autoriser (Allow)**.

Pour obtenir des informations détaillées sur la fourniture d'approbation d'utilisateur pour le chargement d'une extension de noyau, consultez la note technique à l'adresse suivante https://developer.apple.com/library/content/technotes/tn2459/_index.html.

d Pendant le chargement de l'extension de noyau, le processus d'installation du client VPN-Plus SSL continue en arrière-plan. Le client VPN-Plus SSL est installé, mais vous obtenez le message d'erreur suivant : `L'installation a échoué. Le programme d'installation a rencontré une erreur qui provoque l'échec de l'installation. Contactez le fabricant du logiciel.`

e Pour résoudre cette erreur, désinstallez le client VPN-Plus SSL et réinstallez-le.

6 Pour résoudre les messages d'erreur d'installation sur Mac OS High Sierra, procédez comme suit.

a Vérifiez que les notifications sont activées. Accédez à **Préférences système (System Preferences) > Sécurité et confidentialité (Security & Privacy) > Autoriser les notifications (Allow Notifications)**.

Note La première fois que vous installez le client VPN-Plus SSL sur Mac OS High Sierra, une fenêtre de notification vous invite à autoriser l'installation. Cette notification dure généralement 30 minutes. Si la notification disparaît avant que vous ayez cliqué sur **Autoriser (Allow)**, redémarrez votre ordinateur et réinstallez le client VPN-Plus SSL.

Si l'installation échoue toujours, cela implique que votre système n'autorise pas l'extension de noyau (kext) et il ne vous invite pas non plus à charger la kext. Effectuez les sous-étapes restantes pour ajouter `tuntap kext team id` à la liste de kext préapprouvées.

b Redémarrez la machine Mac en mode de récupération.

1 Cliquez sur le logo Apple en haut à gauche de votre écran.

2 Cliquez sur **Redémarrer (Restart)**.

3 Appuyez immédiatement sur les touches de commande et R jusqu'à ce que vous voyiez un logo Apple ou un globe en rotation. Un globe en rotation s'affiche lorsque votre machine Mac tente de démarrer la récupération de macOS en se connectant à Internet, car elle ne parvient pas à démarrer par l'intermédiaire du système de récupération intégré. Mac est maintenant démarré en mode de récupération.

c Dans la barre supérieure, cliquez sur **Utilitaires (Utlities) > Terminal**.

d Pour ajouter `tuntap kext team id` à la liste des kext préapprouvées, exécutez la commande – `spctl kext–consent add KS8XL6T9FZ`.

e Redémarrez votre machine Mac en mode normal.

f Pour vérifier si team-id est visible dans la liste des kext préapprouvées, exécutez la commande – `spctl kext–consent list`.

g Installez le module du client VPN-Plus SSL.

7 Sur les machines Windows, si vous voyez l'erreur d'échec d'installation du pilote (E00024B), désactivez l'option **Masquer l'adaptateur réseau SSL du client (Hide SSL client network adapter)** dans l'installateur du client VPN-Plus SSL Edge. Pour des instructions sur la désactivation de cette option, consultez l'article de la base de connaissances de VMware à l'adresse https://kb.vmware.com/s/article/2108766.

VPN-Plus SSL : problèmes de communication

Utilisez cette rubrique pour comprendre les probables problèmes de connectivité de VPN SSL et de chemin de données et la manière de les résoudre.

Problème

Les problèmes courants liés à la connectivité de VPN SSL et aux chemins de données sont les suivants :

- Le client VPN-Plus SSL ne peut pas se connecter au serveur VPN SSL.
- Le client VPN-Plus SSL est installé, mais les services VPN-Plus SSL ne sont pas en cours d'exécution.
- Le nombre maximal d'utilisateurs connectés est atteint. Le portail Web VPN SSL ou le client VPN-Plus SSL affiche le message suivant :

  `Nombre maximal d'utilisateurs atteint/Nombre maximal d'utilisateurs connectés atteint selon la licence VPN SSL. Réessayez un peu plus tard` ou `La lecture de SSL a échoué`.
- Les services VPN SSL sont en cours d'exécution, mais le chemin de données ne fonctionne pas.
- La connexion VPN SSL est établie, mais les applications dans le réseau privé ne sont pas accessibles.

Solution

1. Si le client VPN-Plus SSL ne peut pas se connecter au serveur VPN SSL, procédez comme suit :
   - Vérifiez que l'utilisateur VPN SSL se connecte avec le nom d'utilisateur et le mot de passe corrects.
   - Vérifiez si l'utilisateur VPN SSL est valide.
   - Vérifiez si l'utilisateur VPN SSL peut atteindre le serveur VPN SSL à l'aide du portail Web.
2. Sur le dispositif NSX Edge, procédez comme suit pour vérifier si le processus de VPN SSL est en cours d'exécution.
   a. Connectez-vous au dispositif NSX Edge à partir de l'interface de ligne de commande. Pour plus d'informations sur la connexion à l'interface de ligne de commande Edge, reportez-vous à la section *Référence de l'interface de ligne de commandes de NSX*.
   b. Exécutez la commande `show process monitor` et localisez le processus *sslvpn*.
   c. Exécutez la commande `show service network-connections` et vérifiez si le processus *sslvpn* est répertorié sur le port 443.

   Note Par défaut, votre système utilise le port 443 pour le trafic SSL. Toutefois, si vous avez configuré un autre port TCP pour le trafic SSL, assurez-vous que le processus *sslvpn* est répertorié sur ce numéro de port TCP.

3 Sur le client VPN-Plus SSL, vérifiez si les services VPN-Plus SSL sont en cours d'exécution.

Système d'exploitation	Description
Windows	Ouvrez le **Gestionnaire des tâches**, puis vérifiez si le service du client VPN-Plus SSL est démarré.
Mac	■ Vérifiez que le processus `naclientd` est démarré pour le démon. ■ Vérifiez que le processus `naclient` est démarré pour l'interface utilisateur. Pour vérifier si les processus sont en cours d'exécution, exécutez la commande `ps –ef | grep "naclient"`.
Linux	■ Vérifiez que les processus `naclientd` et `naclient_poll` sont démarrés. ■ Pour vérifier si les processus sont en cours d'exécution, exécutez la commande `ps –ef | grep "naclient"`.

Si les services ne sont pas en cours d'exécution, exécutez les commandes suivantes pour démarrer les services.

Système d'exploitation	Commande
Mac	Exécutez la commande `sudo launchctl load –w /Library/LaunchDaemons/com.vmware.naclientd.plist`.
Linux	Exécutez la commande `sudo service naclient start`.

4 Si le nombre maximal d'utilisateurs VPN SSL connectés est atteint, augmentez le nombre d'utilisateurs simultanés (CCU) en augmentant le format de NSX Edge.

Pour plus d'informations, reportez-vous au *Guide d'administration de NSX*. Notez que les utilisateurs connectés sont déconnectés du VPN lorsque vous effectuez cette opération.

5 Si les services VPN SSL sont en cours d'exécution, mais que le chemin de données ne fonctionne pas, procédez comme suit :

a Vérifiez si une adresse IP virtuelle est attribuée après une connexion réussie.

b Vérifiez si les itinéraires sont ajoutés.

6 Lorsque des applications dans le réseau privé (principal) ne sont pas accessibles, procédez comme suit pour résoudre le problème :

a Vérifiez que le réseau privé et le pool IP ne sont pas dans le même sous-réseau.

b Si l'administrateur n'a pas défini de pool IP, ou si le pool IP est épuisé, procédez comme suit.

1 Connectez-vous à vSphere Web Client.

2 Cliquez sur **Networking & Security**, puis sur **Dispositifs NSX Edge (NSX Edges)**.

3 Double-cliquez sur un dispositif NSX Edge, puis cliquez sur l'onglet **VPN-Plus SSL (SSL VPN-Plus)**.

4 Ajoutez un pool IP statique comme expliqué dans la rubrique Ajouter un pool IP dans le *Guide d'administration de NSX*. Assurez-vous que vous ajoutez l'adresse IP dans la zone de texte **Passerelle (Gateway)**. L'adresse IP de la passerelle est attribuée à l'interface *na0*. Tout le trafic non-TCP traverse la carte virtuelle nommée interface *na0*. Vous pouvez créer plusieurs pools IP avec des adresses IP de passerelle différentes, mais attribuées à la même interface *na0*.

5 Utilisez la commande `show interface na0` pour vérifier les adresses IP fournies et vérifiez si tous les pools IP sont attribués à la même interface *na0*.

6 Connectez-vous à la machine cliente, accédez à l'écran **Client VPN-Plus SSL - Statistiques (SSL VPN-Plus Client - Statistics)** et vérifiez l'adresse IP virtuelle attribuée.

c Connectez-vous à l'interface de ligne de commande NSX Edge et prenez une capture de paquets sur l'interface na0 en exécutant la commande `debug packet capture interface na0`. Vous pouvez également capturer des paquets à l'aide de l'outil **Capture de paquets (Packet Capture)**. Pour plus de détails, reportez-vous à la section *Guide d'administration de NSX*.

Note La capture de paquets continue à s'exécuter en arrière-plan jusqu'à ce que vous l'arrêtiez en exécutant la commande `no debug packet capture interface na0` .

d Si l'optimisation TCP n'est pas activée, vérifiez les règles de pare-feu.

e Pour le trafic non-TCP, veillez à ce que la passerelle par défaut soit définie en tant qu'interface interne du dispositif Edge sur le réseau principal.

f Pour les clients Mac et Linux, connectez-vous au système sur lequel le client VPN SSL est installé et prenez une capture de paquets sur l'interface tap0 ou sur l'adaptateur virtuel en exécutant la commande `tcpdump –i tap0 –s 1500 –w filepath`. Sur les clients Windows, utilisez un analyseur de paquets, comme Wireshark, et capturez des paquets sur l'adaptateur du client VPN-Plus SSL.

7 Si les étapes ci-dessus ne résolvent pas le problème, utilisez les commandes CLI NSX Edge suivantes pour résoudre le problème.

Objectif	Commande
Vérifier l'état du VPN SSL.	`show service sslvpn-plus`
Vérifier les statistiques de VPN SSL.	`show service sslvpn-plus stats`
Vérifier les clients VPN qui sont connectés.	`show service sslvpn-plus tunnels`
Vérifier les sessions de VPN-Plus SSL.	`show service sslvpn-plus sessions`

VPN-Plus SSL : problèmes d'authentification

Vous rencontrez des problèmes avec l'authentification de VPN-Plus SSL.

Problème

L'authentification de VPN-Plus SSL échoue.

Solution

- Pour les problèmes d'authentification, vérifiez les paramètres suivants :
  a Assurez-vous que le serveur d'authentification externe est accessible à partir de NSX Edge. À partir de NSX Edge, exécutez une commande ping sur le serveur d'authentification et vérifiez si le serveur est accessible.
  b Vérifiez la configuration du serveur d'authentification externe à l'aide d'outils, tels que le navigateur LDAP, et vérifiez si la configuration fonctionne. Seuls les serveurs d'authentification LDAP et Active Directory peuvent être vérifiés à l'aide du navigateur LDAP.
  c Assurez-vous que le serveur d'authentification local est défini sur la priorité la plus faible s'il est configuré dans le processus d'authentification.
  d Si vous utilisez Active Directory (AD), définissez-le sur le mode `no-ssl` et effectuez une capture de paquets sur l'interface à partir de laquelle le serveur AD est accessible.
  e Si l'authentification est réussie sur le serveur Syslog, vous voyez un message semblable à : `Log Output - SVP_LOG_NOTICE, 10-28-2013,09:28:39,Authentication,a,-,-,10.112.243.61,-,PHAT,,SUCCESS,,,10-28-2013,09:28:39,-,-,,,,,,,,,-,,-,`
  f Si l'authentification échoue sur le serveur Syslog, vous voyez un message semblable à : `Log Output - SVP_LOG_NOTICE, 10-28-2013,09:28:39,Authentication,a,-,-,10.112.243.61,-,PHAT,,FAILURE,,,10-28-2013,09:28:39,-,-,,,,,,,,,-,,-,`

Le client VPN-Plus SSL cesse de répondre

Le client VPN-Plus SSL cesse de répondre lorsque l'optimisation TCP est activée.

Problème

Vous avez configuré l'exécution du service VPN-Plus SSL sur NSX Edge et activé l'optimisation TCP pour l'envoi du trafic via le tunnel. Le client VPN-Plus SSL cesse de répondre lorsque vous exécutez n'importe quel outil de mesure et d'optimisation des performances réseau (par exemple, iperf3) sur le client VPN-Plus SSL.

Cause

L'un des deux scénarios suivants peut provoquer une erreur de lecture du tunnel lors de l'envoi de données depuis le client VPN-Plus SSL :

- Le serveur principal ferme la connexion TCP à l'aide du serveur VPN SSL en envoyant une séquence FIN TCP.
- L'opération d'écriture des tunnels échoue lors du transfert de données vers le serveur principal.

L'erreur de lecture du tunnel est `unknown protocol ID`. Cette erreur efface le tunnel entre le serveur VPN SSL et le client VPN-Plus SSL, qui à son tour provoque l'échec des opérations de lecture/d'écriture SSL sur le client. Ainsi, le client VPN-Plus SSL cesse de répondre.

Solution

- Pour résoudre ce problème, procédez comme suit dans vSphere Web Client pour désactiver l'optimisation TCP du trafic réseau privé via le tunnel VPN SSL.
  a. Double-cliquez sur la VM NSX Edge dans laquelle vous avez configuré le service VPN-Plus SSL.
  b. Cliquez sur l'onglet **VPN-Plus SSL (SSL VPN-Plus)**, puis sélectionnez le réseau privé.
  c. Décochez la case **Activer l'optimisation TCP (Enable TCP Optimization)**.

Analyse de base des journaux

Les journaux de la passerelle VPN-Plus SSL sont envoyés au serveur syslog configuré sur le dispositif NSX Edge. Les journaux du client VPN-Plus SSL sont stockés dans le répertoire suivant sur l'ordinateur de l'utilisateur distant : `C:\Users\`*`nom d'utilisateur`*`\AppData\Local\VMware\vpn\svp_client.log`.

Analyse de base des journaux - Authentification

Réussite de l'authentification

- La sortie de journal suivante indique que l'utilisateur *a* s'est correctement authentifié avec Network Access Client le *28 octobre 2016* à *09h28*.

```
SVP_LOG_NOTICE,10-28-2016,09:28:39,Authentication,a,-,-,10.112.243.61,-,PHAT,,SUCCESS,,,10-28-2016,09:28:39,-,-,,,,,,,,,,,-,,-,-
```

Échec de l'authentification

- La sortie de journal suivante indique que l'utilisateur *a* n'a pas pu s'authentifier avec Network Access Client le *28 octobre 2016* à *09h28*.

```
SVP_LOG_NOTICE,10-28-2016,09:28:39,Authentication,a,-,-,10.112.243.61,-,PHAT,,FAILURE,,,10-28-2016,09:28:39,-,-,,,,,,,,,,,-,,-,-
```

Pour résoudre les problèmes d'authentification, reportez-vous à la section VPN-Plus SSL : échecs d'installation.

Analyse de base des journaux - Chemin de données

Réussite du chemin de données

- La sortie de journal suivante indique que l'utilisateur *a* s'est correctement connecté avec Network Access Client sur TCP le *28 octobre 2016* à *09h41* au serveur Web principal *192.168.10.8*.

```
SVP_LOG_INFO,10-28-2016,09:41:03,TCP Connect,a,-,-,10.112.243.61,-,PHAT,,SUCCESS,,,10-28-2013,09:41:03,-,-,192.168.10.8,80,,,,,,,,,-,,-,-
```

Échec du chemin de données

- La sortie de journal suivante indique que l'utilisateur *a* n'a pas pu se connecter avec Network Access Client sur TCP le *28 octobre 2016* à *09h41* au serveur Web principal *192.168.10.8*.

```
SVP_LOG_INFO,10-28-2016,09:41:03,TCP Connect,a,-,-,10.112.243.61,-,PHAT,,FAILURE,,,10-28-2013,09:41:03,-,-,192.168.10.8,80,,,,,,,,,-,,-,-
```

VPN IPSec

Utilisez ces informations pour vous aider à dépanner les problèmes de négociation rencontrés avec votre configuration.

Négociation réussie (en phases 1 et 2)

Les exemples suivants montrent le résultat d'une négociation réussie entre NSX Edge et un périphérique Cisco.

NSX Edge

Dans l'interface de ligne de commande NSX Edge (ipsec auto -status, partie de la commande show service ipsec) :

```
000 #2: "s1-c1":500 STATE_QUICK_I2 (sent QI2, IPsec SA established);
      EVENT_SA_REPLACE in 2430s; newest IPSEC; eroute owner; isakmp#1; idle;
      import:admin initiate
000 #2: "s1-c1" esp.f5f6877d@10.20.131.62 esp.7aaf335f@10.20.129.80
      tun.0@10.20.131.62 tun.0@10.20.129.80 ref=0 refhim=4294901761
000 #1: "s1-c1":500 STATE_MAIN_I4 (ISAKMP SA established); EVENT_SA_REPLACE in
      27623s; newest ISAKMP; lastdpd=0s(seq in:0 out:0); idle;
      import:admin initiate
```

Cisco

```
ciscoasa# show crypto isakmp sa detail

    Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

    IKE Peer: 10.20.129.80
    Type : L2L        Role    : responder
    Rekey : no        State   : MM_ACTIVE
    Encrypt : 3des    Hash    : SHA
    Auth : preshared  Lifetime: 28800
    Lifetime Remaining: 28379
```

Règle de phase 1 non correspondante

Ce qui suit énumère les journaux d'erreur de Règle de phase 1 non correspondante.

NSX Edge

NSX Edge se bloque à l'état STATE_MAIN_I1. Recherchez des informations dans /var/log/messages indiquant que l'entité homologue a renvoyé un message d'IKE avec l'option NO_PROPOSAL_CHOSEN définie.

```
000 #1: "s1-c1":500 STATE_MAIN_I1 (sent MI1,
      expecting MR1); EVENT_RETRANSMIT in 7s; nodpd; idle;
      import:admin initiate
000 #1: pending Phase 2 for "s1-c1" replacing #0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      | got payload 0x800(ISAKMP_NEXT_N) needed: 0x0 opt: 0x0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      | ***parse ISAKMP Notification Payload:
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      |    next payload type: ISAKMP_NEXT_NONE
Aug 26 12:31:25 weiqing-desktop ipsec[6569]: |    length: 96
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      |    DOI: ISAKMP_DOI_IPSEC
Aug 26 12:31:25 weiqing-desktop ipsec[6569]: |    protocol ID: 0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]: |    SPI size: 0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      |    Notify Message Type: NO_PROPOSAL_CHOSEN
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      "s1-c1" #1: ignoring informational payload,
       type NO_PROPOSAL_CHOSEN msgid=00000000
```

Cisco

Si la commande debug crypto est activée, un message d'erreur est imprimé pour indiquer qu'aucune proposition n'a été acceptée.

```
ciscoasa# Aug 26 18:17:27 [IKEv1]:
      IP = 10.20.129.80, IKE_DECODE RECEIVED
```

```
      Message (msgid=0) with payloads : HDR + SA (1)
      + VENDOR (13) + VENDOR (13) + NONE (0) total length : 148
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80,
      processing SA payload
Aug 26 18:17:27 [IKEv1]: Phase 1 failure:  Mismatched attribute
      types for class Group Description:  Rcv'd: Group 5
      Cfg'd: Group 2
Aug 26 18:17:27 [IKEv1]: Phase 1 failure:  Mismatched attribute
      types for class Group Description:  Rcv'd: Group 5
      Cfg'd: Group 2
Aug 26 18:17:27 [IKEv1]: IP = 10.20.129.80, IKE_DECODE SENDING
      Message (msgid=0) with payloads : HDR + NOTIFY (11)
      + NONE (0) total length : 124
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80,
      All SA proposals found unacceptable
Aug 26 18:17:27 [IKEv1]: IP = 10.20.129.80, Error processing
      payload: Payload ID: 1
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, IKE MM Responder
      FSM error history (struct &0xd8355a60)  <state>, <event>:
      MM_DONE, EV_ERROR-->MM_START, EV_RCV_MSG-->MM_START,
      EV_START_MM-->MM_START, EV_START_MM-->MM_START,
      EV_START_MM-->MM_START, EV_START_MM-->MM_START,
      EV_START_MM-->MM_START, EV_START_MM
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, IKE SA
      MM:9e0e4511 terminating:  flags 0x01000002, refcnt 0,
      tuncnt 0
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, sending
      delete/delete with reason message
```

Phase 2 non correspondante

Ce qui suit énumère les journaux d'erreur de Phase 2 Stratégie non correspondante.

NSX Edge

NSX Edge se bloque à STATE_QUICK_I1. Un message du journal indique que l'homologue a envoyé un message NO_PROPOSAL_CHOSEN.

```
000 #2: "s1-c1":500 STATE_QUICK_I1 (sent QI1, expecting
      QR1); EVENT_RETRANSMIT in 11s; lastdpd=-1s(seq in:0 out:0);
      idle; import:admin initiate
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: | got payload
      0x800(ISAKMP_NEXT_N) needed: 0x0 opt: 0x0
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: | ***parse
      ISAKMP Notification Payload:
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |    next payload
      type: ISAKMP_NEXT_NONE
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |    length: 32
Aug 26 12:33:54 weiqing-desktop ipsec[6933]:
      |    DOI: ISAKMP_DOI_IPSEC
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |    protocol ID: 3
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |    SPI size: 16
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |    Notify Message
      Type: NO_PROPOSAL_CHOSEN
```

```
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: "s1-c1" #3:
      ignoring informational payload, type NO_PROPOSAL_CHOSEN
      msgid=00000000
```

Cisco

Le message de débogage indique que la phase 1 est terminée, mais la phase 2 a échoué en raison d'une erreur de négociation de la stratégie.

```
Aug 26 16:03:49 [IKEv1]: Group = 10.20.129.80,
      IP = 10.20.129.80, PHASE 1 COMPLETED
Aug 26 16:03:49 [IKEv1]: IP = 10.20.129.80, Keep-alive type
      for this connection: DPD
Aug 26 16:03:49 [IKEv1 DEBUG]: Group = 10.20.129.80,
      IP = 10.20.129.80, Starting P1 rekey timer: 21600 seconds
Aug 26 16:03:49 [IKEv1]: IP = 10.20.129.80, IKE_DECODE RECEIVED
      Message (msgid=b2cdcb13) with payloads : HDR + HASH (8)
      + SA (1) + NONCE (10) + KE (4) + ID (5) + ID (5) + NONE (0)
      total length : 288
.
.
.
Aug 26 16:03:49 [IKEv1]: Group = 10.20.129.80, IP = 10.20.129.80,
      Session is being torn down. Reason: Phase 2 Mismatch
```

Incompatibilité de PFS

Les journaux d'erreurs d'incompatibilité de PFS sont présentés ci-dessous.

NSX Edge

PFS est négocié dans le cadre de la phase 2. Si PFS ne correspond pas, le comportement est semblable au cas d'erreur décrit dans Phase 2 non correspondante.

```
000 #4: "s1-c1":500 STATE_QUICK_I1 (sent QI1, expecting
      QR1); EVENT_RETRANSMIT in 8s; lastdpd=-1s(seq in:0 out:0);
      idle; import:admin initiate
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | got payload 0x800
      (ISAKMP_NEXT_N) needed: 0x0 opt: 0x0
Aug 26 12:35:52 weiqing-desktop ipsec[7312]:
      | ***parse ISAKMP Notification Payload:
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |    next payload
      type: ISAKMP_NEXT_NONE
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |    length: 32
Aug 26 12:35:52 weiqing-desktop ipsec[7312]:
      |    DOI: ISAKMP_DOI_IPSEC
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |    protocol ID: 3
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |    SPI size: 16
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |    Notify Message
      Type: NO_PROPOSAL_CHOSEN
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: "s1-c1" #1: ignoring
      informational payload, type NO_PROPOSAL_CHOSEN
      msgid=00000000
```

```
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | info:  fa 16 b3 e5
      91 a9 b0 02  a3 30 e1 d9  6e 5a 13 d4
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | info:  93 e5 e4 d7
Aug 26 12:35:52 weiqing-desktop ipsec[7312]:
      | processing informational NO_PROPOSAL_CHOSEN (14)
```

Cisco

```
<BS>Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
      IP = 10.20.129.80, sending delete/delete with
      reason message
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
      IP = 10.20.129.80, constructing blank hash payload
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
      IP = 10.20.129.80, constructing blank hash payload
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
      IP = 10.20.129.80, constructing IKE delete payload
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
      IP = 10.20.129.80, constructing qm hash payload
Aug 26 19:00:26 [IKEv1]: IP = 10.20.129.80, IKE_DECODE SENDING
      Message (msgid=19eb1e59) with payloads : HDR + HASH (8)
      + DELETE (12) + NONE (0) total length : 80
Aug 26 19:00:26 [IKEv1]: Group = 10.20.129.80, IP = 10.20.129.80,
      Session is being torn down. Reason: Phase 2 Mismatch
```

PSK non correspondant

Ce qui suit énumère les journaux d'erreur d'incompatibilité de PSK.

NSX Edge

PSK est négocié lors de la dernière étape de la Phase 1. Si la négociation de PSK échoue, l'état de NSX Edge est STATE_MAIN_I4. L'homologue envoie un message contenant INVALID_ID_INFORMATION.

```
Aug 26 11:55:55 weiqing-desktop ipsec[3855]:
      "s1-c1" #1: transition from state STATE_MAIN_I3 to
      state STATE_MAIN_I4
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #1:
      STATE_MAIN_I4: ISAKMP SA established
      {auth=OAKLEY_PRESHARED_KEY
      cipher=oakley_3des_cbc_192 prf=oakley_sha group=modp1024}
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #1: Dead Peer
      Detection (RFC 3706): enabled
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #2:
      initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS+UP+SAREFTRACK
      {using isakmp#1 msgid:e8add10e proposal=3DES(3)_192-SHA1(2)_160
      pfsgroup=OAKLEY_GROUP_MODP1024}
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #1:
      ignoring informational payload, type INVALID_ID_INFORMATION
      msgid=00000000
```

Cisco

```
Aug 26 15:27:07 [IKEv1]: IP = 10.115.199.191,
      IKE_DECODE SENDING Message (msgid=0) with payloads : HDR
      + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13)
      + VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130)
      + NONE (0) total length : 304
Aug 26 15:27:07 [IKEv1]: Group = 10.115.199.191,
      IP = 10.115.199.191, Received encrypted Oakley Main Mode
      packet with invalid payloads, MessID = 0
Aug 26 15:27:07 [IKEv1]: IP = 10.115.199.191, IKE_DECODE SENDING
      Message (msgid=0) with payloads : HDR + NOTIFY (11)
      + NONE (0) total length : 80
Aug 26 15:27:07 [IKEv1]: Group = 10.115.199.191,
      IP = 10.115.199.191, ERROR, had problems decrypting
      packet, probably due to mismatched pre-shared key.
      Aborting
```

Capture de paquets pour une négociation réussie

La liste suivante énumère une session de capture de paquets pour une négociation réussie entre NSX Edge et un périphérique Cisco.

```
No.     Time        Source        Destination   Protocol Info
9203    768.394800  10.20.129.80  10.20.131.62  ISAKMP  Identity Protection
                                                        (Main Mode)
Frame 9203 (190 bytes on wire, 190 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
      Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
      Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 0000000000000000
  Next payload: Security Association (1)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000
  Length: 148
  Security Association payload
    Next payload: Vendor ID (13)
    Payload length: 84
    Domain of interpretation: IPSEC (1)
    Situation: IDENTITY (1)
    Proposal payload # 0
      Next payload: NONE (0)
      Payload length: 72
      Proposal number: 0
      Protocol ID: ISAKMP (1)
      SPI Size: 0
      Proposal transforms: 2
      Transform payload # 0
```

```
         Next payload: Transform (3)
         Payload length: 32
         Transform number: 0
         Transform ID: KEY_IKE (1)
         Life-Type (11): Seconds (1)
         Life-Duration (12): Duration-Value (28800)
         Encryption-Algorithm (1): 3DES-CBC (5)
         Hash-Algorithm (2): SHA (2)
         Authentication-Method (3): PSK (1)
         Group-Description (4): 1536 bit MODP group (5)
      Transform payload # 1
         Next payload: NONE (0)
         Payload length: 32
         Transform number: 1
         Transform ID: KEY_IKE (1)
         Life-Type (11): Seconds (1)
         Life-Duration (12): Duration-Value (28800)
         Encryption-Algorithm (1): 3DES-CBC (5)
         Hash-Algorithm (2): SHA (2)
         Authentication-Method (3): PSK (1)
         Group-Description (4): Alternate 1024-bit MODP group (2)
  Vendor ID: 4F456C6A405D72544D42754D
    Next payload: Vendor ID (13)
    Payload length: 16
    Vendor ID: 4F456C6A405D72544D42754D
  Vendor ID: RFC 3706 Detecting Dead IKE Peers (DPD)
    Next payload: NONE (0)
    Payload length: 20
    Vendor ID: RFC 3706 Detecting Dead IKE Peers (DPD)

No.     Time        Source        Destination   Protocol Info
9204    768.395550  10.20.131.62  10.20.129.80  ISAKMP Identity Protection
                                                          (Main Mode)

Frame 9204 (146 bytes on wire, 146 bytes captured)
Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
      Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
      Dst: 10.20.129.80 (10.20.129.80)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Security Association (1)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000
  Length: 104
  Security Association payload
    Next payload: Vendor ID (13)
    Payload length: 52
    Domain of interpretation: IPSEC (1)
    Situation: IDENTITY (1)
    Proposal payload # 1
```

```
      Next payload: NONE (0)
      Payload length: 40
      Proposal number: 1
      Protocol ID: ISAKMP (1)
      SPI Size: 0
      Proposal transforms: 1
      Transform payload # 1
         Next payload: NONE (0)
         Payload length: 32
         Transform number: 1
         Transform ID: KEY_IKE (1)
         Encryption-Algorithm (1): 3DES-CBC (5)
         Hash-Algorithm (2): SHA (2)
         Group-Description (4): Alternate 1024-bit MODP group (2)
         Authentication-Method (3): PSK (1)
         Life-Type (11): Seconds (1)
         Life-Duration (12): Duration-Value (28800)
  Vendor ID: Microsoft L2TP/IPSec VPN Client
    Next payload: NONE (0)
    Payload length: 24
    Vendor ID: Microsoft L2TP/IPSec VPN Client

No.     Time        Source        Destination   Protocol Info
9205    768.399599  10.20.129.80  10.20.131.62  ISAKMP Identity Protection
                                                          (Main Mode)

Frame 9205 (222 bytes on wire, 222 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
      Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
      Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Key Exchange (4)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000
  Length: 180
  Key Exchange payload
    Next payload: Nonce (10)
    Payload length: 132
    Key Exchange Data (128 bytes / 1024 bits)
  Nonce payload
    Next payload: NONE (0)
    Payload length: 20
    Nonce Data


No.     Time        Source        Destination   Protocol Info
9206    768.401192  10.20.131.62  10.20.129.80  ISAKMP Identity Protection
                                                          (Main Mode)
Frame 9206 (298 bytes on wire, 298 bytes captured)
```

```
Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
      Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
      Dst: 10.20.129.80 (10.20.129.80)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Key Exchange (4)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000
  Length: 256
  Key Exchange payload
    Next payload: Nonce (10)
    Payload length: 132
    Key Exchange Data (128 bytes / 1024 bits)
  Nonce payload
    Next payload: Vendor ID (13)
    Payload length: 24
    Nonce Data
  Vendor ID: CISCO-UNITY-1.0
    Next payload: Vendor ID (13)
    Payload length: 20
    Vendor ID: CISCO-UNITY-1.0
  Vendor ID: draft-beaulieu-ike-xauth-02.txt
    Next payload: Vendor ID (13)
    Payload length: 12
    Vendor ID: draft-beaulieu-ike-xauth-02.txt
  Vendor ID: C1B7EBE18C8CBD099E89695E2CB16A4A
    Next payload: Vendor ID (13)
    Payload length: 20
    Vendor ID: C1B7EBE18C8CBD099E89695E2CB16A4A
  Vendor ID: CISCO-CONCENTRATOR
    Next payload: NONE (0)
    Payload length: 20
    Vendor ID: CISCO-CONCENTRATOR

No.     Time        Source        Destination   Protocol Info
9207    768.404990  10.20.129.80  10.20.131.62  ISAKMP Identity Protection
                                                          (Main Mode)

Frame 9207 (110 bytes on wire, 110 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
      Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
      Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Identification (5)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
```

```
  Flags: 0x01
  Message ID: 0x00000000
  Length: 68
  Encrypted payload (40 bytes)

No.     Time        Source        Destination   Protocol Info
9208    768.405921  10.20.131.62  10.20.129.80  ISAKMP   Identity Protection
                                                          (Main Mode)
Frame 9208 (126 bytes on wire, 126 bytes captured)
Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
      Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
      Dst: 10.20.129.80 (10.20.129.80)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Identification (5)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x01
  Message ID: 0x00000000
  Length: 84
  Encrypted payload (56 bytes)

No.     Time        Source        Destination   Protocol Info
9209    768.409799  10.20.129.80  10.20.131.62  ISAKMP   Quick Mode

Frame 9209 (334 bytes on wire, 334 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
      Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
      Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Hash (8)
  Version: 1.0
  Exchange type: Quick Mode (32)
  Flags: 0x01
  Message ID: 0x79a63fb1
  Length: 292
  Encrypted payload (264 bytes)

No.     Time        Source        Destination   Protocol Info
9210    768.411797  10.20.131.62  10.20.129.80  ISAKMP   Quick Mode

Frame 9210 (334 bytes on wire, 334 bytes captured)
Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
      Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
      Dst: 10.20.129.80 (10.20.129.80)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
```

```
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Hash (8)
  Version: 1.0
  Exchange type: Quick Mode (32)
  Flags: 0x01
  Message ID: 0x79a63fb1
  Length: 292
  Encrypted payload (264 bytes)

No.     Time        Source        Destination   Protocol Info
9211    768.437057  10.20.129.80  10.20.131.62  ISAKMP   Quick Mode

Frame 9211 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
      Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
      Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Hash (8)
  Version: 1.0
  Exchange type: Quick Mode (32)
  Flags: 0x01
  Message ID: 0x79a63fb1
  Length: 52
  Encrypted payload (24 bytes)
```

Dépannage de NSX Controller

8

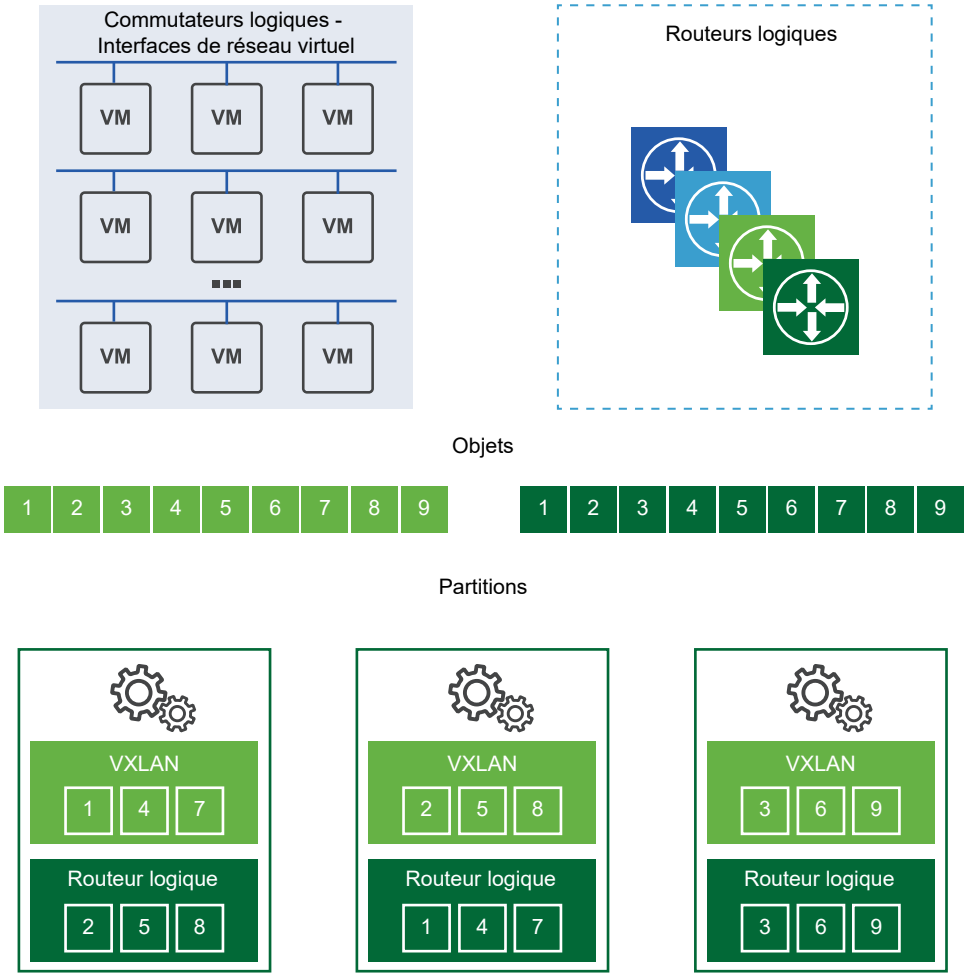
Cette section comporte des informations sur l'identification des causes de défaillance de NSX Controller et de dépannage des contrôleurs.

Ce chapitre contient les rubriques suivantes :

Comprendre l'architecture du cluster de contrôleurs

Le cluster NSX Controller représente un système distribué évolutif, dans lequel un ensemble de rôles est attribué à chaque nœud de contrôleur pour définir le type de tâches que le nœud peut implémenter. Pour des raisons de résilience et de performance, les déploiements de VM de contrôleur doivent se faire sur trois hôtes distincts.

Le partitionnement est utilisé pour répartir les charges de travail entre les nœuds du cluster NSX Controller. Le partitionnement est l'action de diviser les charges de travail de NSX Controller en différentes partitions pour que chaque instance de NSX Controller possède une portion égale de travail.



Cela démontre comment des nœuds de contrôleur distincts agissent en tant que maître pour des entités données comme la commutation logique, le routage logique et d'autres services. Après qu'une instance maître du dispositif NSX Controller soit choisie pour un rôle, ce dispositif NSX Controller divise les différents routeurs et commutateurs logiques sur toutes les instances de NSX Controller disponibles dans un cluster.

Chaque case numérotée sur une partition représente des partitions que le maître utilise pour diviser les charges de travail. Le commutateur logique maître divise les commutateurs logiques en partitions et attribue ces partitions aux différentes instances du dispositif NSX Controller. Le maître des routeurs logiques divise aussi les routeurs logiques en partitions et attribue ces partitions aux différentes instances du dispositif NSX Controller.

Ces partitions sont attribuées aux différentes instances du dispositif NSX Controllerdans ce cluster. Le maître pour un rôle décide quelles instances du dispositif NSX Controller sont attribuées à quelle partition. Si une requête arrive sur la partition du routeur 3, il est indiqué à la partition de se connecter à la troisième instance du dispositif NSX Controller. Si une requête arrive sur la partition du commutateur logique 2, cette requête est traitée par la deuxième instance du dispositif NSX Controller.

Lorsqu'une des instances du dispositif NSX Controller dans un cluster échoue, les maîtres pour les rôles redistribuent les partitions aux clusters disponibles restants. Un des nœuds de contrôleur est choisi comme maître pour chaque rôle. Le maître est responsable d'allouer les partitions aux nœuds de contrôleur individuels, de déterminer lorsqu'un nœud échoue et de réattribuer les partitions aux autres nœuds. Le maître informe aussi les hôtes ESXi de l'échec du nœud du cluster.

L'élection du maître pour chaque rôle requiert un vote majoritaire de tous les nœuds actifs et inactifs dans le cluster. C'est la raison principale pour laquelle un cluster de contrôleurs doit toujours être déployé avec un nombre impair de nœuds.

ZooKeeper

ZooKeeper est une architecture client/serveur qui est responsable du mécanisme de cluster NSX Controller. Le cluster de contrôleur est découvert et créé à l'aide de Zookeeper. Lorsque le cluster se présente, cela signifie littéralement que ZooKeeper arrive entre tous les nœuds. Les nœuds de ZooKeeper passent par un processus d'élection pour former le cluster de contrôle. Le cluster doit comporter un nœud maître ZooKeeper. Pour ce faire, il faut procéder à une élection inter-nœud.

Lorsqu'un nouveau nœud de contrôleur est créé, le dispositif NSX Manager propage les informations sur le nœud au cluster actif, avec l'IP et l'ID du nœud. En tant que tel, chaque nœud connaît le nombre total de nœuds disponibles pour la mise en cluster. Pendant l'élection maître ZooKeeper, chaque nœud diffuse un vote pour choisir un nœud maître. L'élection est redéclenchée jusqu'à ce qu'un nœud obtienne la majorité des votes. Par exemple, dans un cluster à trois nœuds, le maître doit avoir reçu au moins deux des votes.

Note Pour éviter le scénario dans lequel un maître ZooKeeper ne peut pas être élu, le nombre de nœuds dans le cluster DOIT être trois.

- Lorsque le premier contrôleur est déployé, c'est un cas spécial et le premier contrôleur devient le maître. À ce titre, lors du déploiement des contrôleurs, le premier nœud doit achever son déploiement avant que d'autres nœuds soient ajoutés.
- Lors de l'ajout du deuxième contrôleur, c'est aussi un cas spécial, car le nombre de nœuds est pair à ce moment.
- Lorsque le troisième nœud est ajouté, le cluster atteint un état stable pris en charge.

ZooKeeper peut supporter une seule défaillance à la fois. Cela signifie que si un nœud de contrôleur tombe en panne, cela doit être récupéré avant tout autre échec. Sinon, il peut y avoir des problèmes avec le fractionnement du cluster.

Gestionnaire de domaine du plan de contrôle central (CCP)

C'est la couche au-dessus de ZooKeeper qui fournit la configuration pour ZooKeeper sur tous les nœuds pour démarrer. Le gestionnaire de domaine met à jour la configuration entre tous les nœuds dans le cluster, puis lance un appel de procédure à distance pour démarrer le processus ZooKeeper.

Le gestionnaire de domaine est responsable du démarrage de tous les domaines. Pour rejoindre le cluster, le domaine CCP communique avec le domaine CCP sur d'autres machines. Le composant du domaine CCP qui aide à l'initialisation du cluster est *zk-cluster-bootstrap*.

Relation du contrôleur avec les autres composants

Le cluster de contrôleurs est chargé d'entretenir et de fournir des informations sur les commutateurs logiques, les routeurs logiques et les VTEP aux hôtes ESXi.

Lorsqu'un commutateur logique est créé, les nœuds du contrôleur à l'intérieur du cluster déterminent quel nœud sera *maître* ou *propriétaire* pour ce commutateur logique. Il en est de même lorsqu'un routeur logique est ajouté.

Une fois que la propriété est définie pour un commutateur logique ou un routeur logique, le nœud envoie cette propriété aux hôtes ESXi qui appartiennent à cette zone de transport du commutateur ou du routeur. L'intégralité de l'élection de la propriété et la propagation des informations sur la propriété aux hôtes s'appellent le « partitionnement ». Remarquez que la propriété implique que le nœud est responsable de toutes les opérations liées à NSX pour ce commutateur logique ou ce routeur logique. Les autres nœuds n'effectueront pas d'opération pour ce commutateur logique.

Comme seul un propriétaire doit être la source de vérité pour un commutateur et un routeur logiques, à chaque fois que le cluster de contrôleurs est fractionné de sorte qu'au moins deux nœuds sont élus comme propriétaires pour un commutateur ou un routeur logiques, chaque hôte du réseau peut avoir des informations différentes concernant la source de vérité de ce commutateur ou routeur logique. Si cela se produit, il y aura une indisponibilité du réseau car les opérations de contrôle réseau et de plan de données peuvent avoir uniquement qu'une source de vérité.

Si un nœud de contrôleur est défaillant, les nœuds restants dans le cluster réexécuteront le partitionnement pour déterminer la propriété du commutateur logique et du routage logique.

Problèmes de déploiement de NSX Controller

Des instances de NSX Controller sont déployées par NSX Manager au format OVA. Posséder un cluster de contrôleurs offre une haute disponibilité. Le déploiement de contrôleurs requiert que DNS et NTP soient configurés sur NSX Manager, vCenter Server et des hôtes ESXi. Un pool d'adresses IP statiques doit être utilisé pour attribuer des adresses IP à chaque contrôleur.

Il vous est recommandé d'implémenter des règles d'anti-affinité du DRS pour conserver des instances de NSX Controller sur des hôtes séparés. Vous devez déployer trois instances de NSX Controller.

Problèmes courants liés aux contrôleurs

Lors du déploiement d'instances de NSX Controller, les problèmes typiques que l'on peut rencontrer sont les suivants :

- Échec du déploiement d'instance(s) de NSX Controller.
- NSX Controller n'a pas réussi à rejoindre le cluster.

- L'exécution de la commande `show control-cluster status` montre que l'`État de la majorité` bascule entre `Connecté à la majorité du cluster` et `Connexion interrompue à la majorité du cluster`.
- NSX Dashboard affichant un problème concernant l'état de la connectivité.
  - La commande `show control-cluster status` est la commande recommandée pour voir si un contrôleur a rejoint un cluster de contrôle. Vous devez exécuter cette commande sur chaque contrôleur pour connaître l'état général du cluster.

```
controller # show control-cluster status
Type                Status                                          Since
--------------------------------------------------------------------------------
Join status:        Join complete                                   10/17 18:16:58
Majority status:    Connected to cluster majority                   10/17 18:16:46
Restart status:     This controller can be safely restarted         10/17 18:16:51
Cluster ID:         af2e9dec-19b9-4530-8e68-944188584268
Node UUID:          af2e9dec-19b9-4530-8e68-944188584268
Role                Configured status   Active status
--------------------------------------------------------------------------------
api_provider        enabled             activated
persistence_server  enabled             activated
switch_manager      enabled             activated
logical_manager     enabled             activated
dht_node            enabled             activated
```

Note Lorsque vous voyez qu'un nœud de contrôleur est déconnecté, n'utilisez pas la commande `join cluster` ou `force join`. Cette commande est conçue pour joindre un nœud au cluster. Ce faisant, le cluster pourrait entrer dans un état totalement incertain.

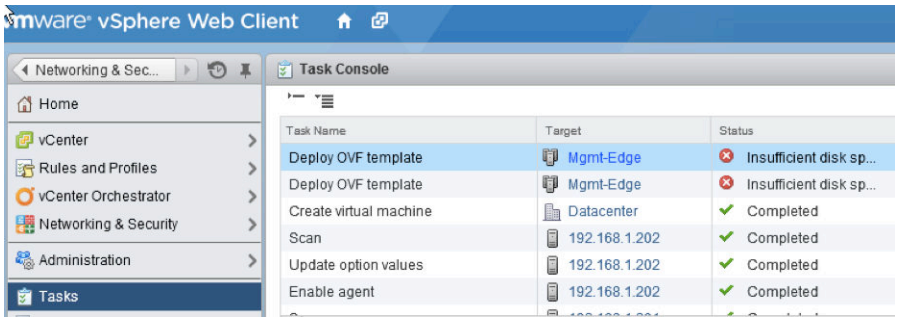
Les nœuds de démarrage du cluster ne sont qu'un indice donné aux membres du cluster pour savoir où regarder lorsque les membres démarrent. Ne vous inquiétez pas si cette liste contient des membres du cluster qui ne sont plus en service. Le fonctionnement du cluster n'est pas impacté.

Tous les membres du cluster doivent avoir le même ID de cluster. Si ce n'est pas le cas, le cluster passe en état rompu et vous devez collaborer avec le support technique de VMware pour le réparer.

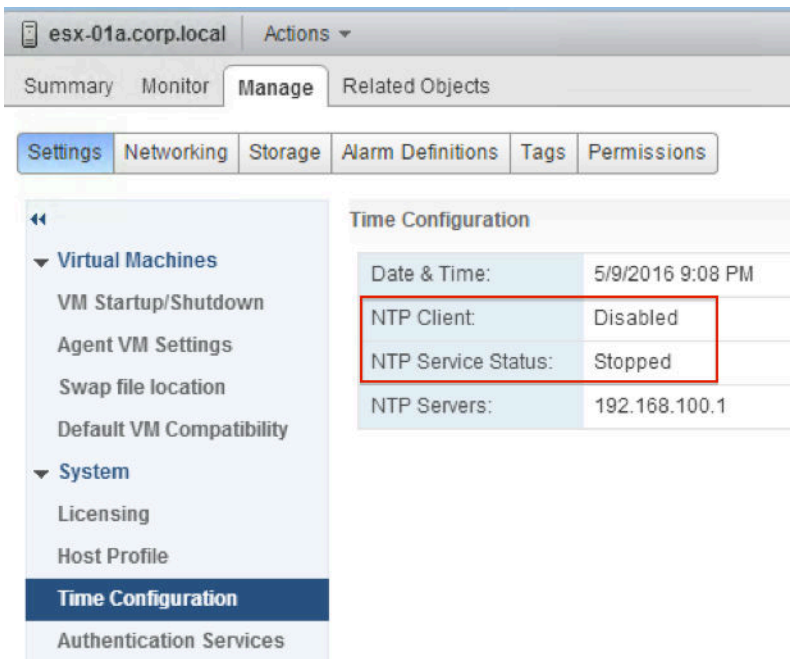
  - La commande `show control-cluster startup-nodes` n'a pas été conçue pour afficher tous les nœuds actuellement dans le cluster. À la place, elle affiche quels autres nœuds de contrôleur sont utilisés par ce nœud pour démarrer l'adhésion au cluster lors du redémarrage du processus du contrôleur. En conséquence, la sortie de la commande peut afficher certains nœuds qui sont fermés ou qui ont été autrement nettoyés du cluster.
  - De plus, la commande `show control-cluster network ipsec status` permet de contrôler l'état IPsec (Internet Protocol Security). Si vous voyez que les contrôleurs ne peuvent pas communiquer entre eux pendant une durée allant de quelques minutes à quelques heures, exécutez la commande `cat /var/log/syslog | egrep "sending DPD request|IKE_SA"` et regardez si les messages des journaux indiquent une absence de trafic. Vous pouvez aussi

exécuter la commande `ipsec statusall | egrep "bytes_i|bytes_o"` et vérifier qu'il n'y a pas deux tunnels IPsec qui sont définis. Fournissez la sortie de ces commandes et les journaux du contrôleur lorsque vous signalez un soupçon de problème de contrôle à votre représentant du support technique VMware.

- Problèmes de connectivité IP entre NSX Manager et les instances de NSX Controller. Cela est en général causé par des problèmes de connectivité du réseau physique ou par un pare-feu bloquant la communication.
- Ressources insuffisantes, telles qu'un stockage disponible sur vSphere pour héberger les contrôleurs. L'affichage du journal des événements et des tâches de vCenter lors du déploiement de contrôleurs peut identifier ce genre de problèmes.

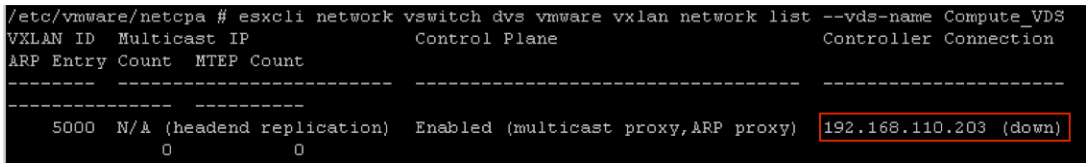


- Un contrôleur indésirable avec un comportement anormal ou des contrôleurs mis à niveau avec l'état **Déconnecté (Disconnected)**.
- DNS sur des hôtes ESXi et NSX Manager n'ont pas été configurés correctement.
- NTP sur des hôtes ESXi et NSX Manager sont désynchronisés.

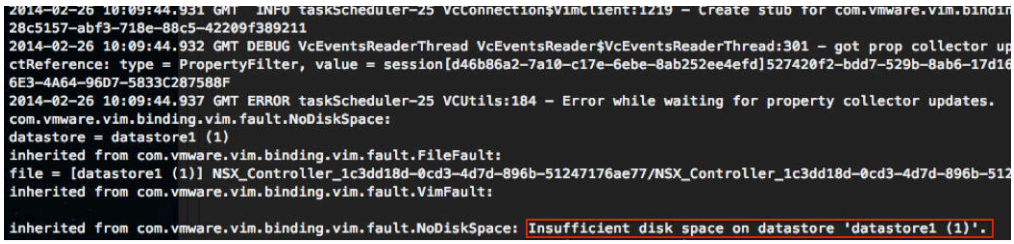


- Lorsque des machines virtuelles récemment connectées ne disposent pas d'un accès réseau, cela provient probablement d'un problème de plan de contrôle. Vérifiez l'état du contrôleur.

Essayez également d'exécuter la commande `esxcli network vswitch dvs vmware vxlan network list --vds-name <name>` sur des hôtes ESXi pour vérifier l'état du plan de contrôle. Notez que la connexion au contrôleur est inactive.



- L'exécution de la commande de l'interface de ligne de commande `show log manager follow` de NSX Manager peut identifier d'autres raisons d'un échec du déploiement des contrôleurs.



Problèmes de connectivité des hôtes

Vérifiez les erreurs de connectivité des hôtes à l'aide des commandes suivantes : Exécutez ces commandes sur chacun des nœuds de contrôleur.

- Vérifiez les statistiques d'erreurs anormales à l'aide de la commande `show log cloudnet/cloudnet_java-vnet-controller*.log filtered-by host_IP`.
- Vérifiez les statistiques de message de commutateur logique/routeur ou de taux de message élevé à l'aide des commandes suivantes :
  - `show control-cluster core stats` : statistiques globales
  - `show control-cluster core stats-sample` : derniers échantillons de statistiques
  - `show control-cluster core connection-stats ip` : statistiques par connexion
  - `show control-cluster logical-switches stats`
  - `show control-cluster logical-routers stats`
  - `show control-cluster logical-switches stats-sample`
  - `show control-cluster logical-routers stats-sample`
  - `show control-cluster logical-switches vni-stats vni`
  - `show control-cluster logical-switches vni-stats-sample vni`
  - `show control-cluster logical-switches connection-stats ip`
  - `show control-cluster logical-routers connection-stats ip`

- Vous pouvez utiliser la commande `show host hostID health-status` pour vérifier l'état de santé des hôtes dans vos clusters préparés. Pour le dépannage des contrôleurs, les vérifications de santé suivantes sont prises en charge :
  - Vérifiez si le fichier `net-config-by-vsm.xml` est synchronisé avec la liste de contrôleurs.
  - Vérifiez s'il existe une connexion de socket avec le contrôleur.
  - Vérifiez si le VNI (VXLAN Network Identifier) est créé et si la configuration est correcte.
  - Vérifiez si le VNI se connecte pour maîtriser les contrôleurs (si le plan de contrôle est activé).

Problèmes d'installation et de déploiement

- Vérifiez qu'au moins trois nœuds de contrôleur sont déployés dans un cluster : VMware recommande d'exploiter les règles anti-affinité vSphere natives pour éviter de déployer plusieurs nœuds de contrôleur sur le même hôte ESXi.
- Vérifiez que tous les dispositifs NSX Controller affichent un état `Connecté`. Si un ou plusieurs nœuds de contrôleur affichent un état `Déconnecté`, vérifiez que les informations suivantes sont cohérentes en exécutant la commande `show control-cluster status` sur tous les nœuds de contrôleur :

Type	Statut
État d'association	Association terminée
État de la majorité	Connecté à la majorité du cluster
ID de cluster	Même information sur tous les nœuds de contrôleur

- Assurez-vous que tous les nœuds sont cohérents sur tous les nœuds de contrôleur.

Rôle	État configuré	État actif
`api_provider`	activé	activé
`persistence_server`	activé	activé
`switch_manager`	activé	activé
`logical_manager`	activé	activé
`directory_server`	activé	activé

- Vérifiez que le processus `vnet-controller` est exécuté. Exécutez la commande `show process` sur tous les nœuds de contrôleur et assurez-vous que le service `java-dir-server` est exécuté.
- Vérifiez l'historique du cluster et assurez-vous qu'il n'y a aucun signe d'instabilité de la connexion de l'hôte ou d'échecs d'association CNI et de modification d'adhésion du cluster. Pour vérifier cela, exécutez la commande `show control-cluster history`. La commande montre aussi si le nœud est souvent redémarré. Vérifiez qu'il n'existe pas de nombreux fichiers journaux présentant une taille nulle (0) et différents ID de processus.
- Vérifiez que l'identificateur réseau VXLAN (VNI) est configuré. Pour plus d'informations, consultez la section Étapes de préparation du VXLAN dans le VMware VXLAN Deployment Guide.

- Vérifiez que SSL est activé sur le cluster de contrôleur. Exécutez la commande `show log cloudnet/cloudnet_java-vnet-controller*.log filtered-by sslEnabled` sur chacun des nœuds de contrôleur.

Dépannage de la latence de disque

Vous pouvez afficher les alertes de latence de disque dans l'onglet **Gestion (Management)**. Les instances de NSX Controller doivent fonctionner sur des disques à latence faible.

Afficher les alertes de latence du disque

Les alertes de latence du disque surveillent et signalent les problèmes de disponibilité ou de latence du disque. Vous pouvez afficher les informations relatives à la latence pour chaque NSX Controller. Les calculs de latence en lecture et en écriture sont ajoutés à une moyenne de déplacement de 5 secondes (par défaut), qui est à son tour utilisée pour déclencher une alerte lors de la violation de la limite de la latence. L'alerte est désactivée une fois que la moyenne revient à la limite inférieure. Par défaut, la limite supérieure est définie sur 200 ms et la limite inférieure sur 100 ms. Les latences élevées ont un impact sur le fonctionnement des applications mises en cluster distribué sur chaque nœud de contrôleur.

Pour afficher les alertes de latence du disque pour NSX Controller, procédez comme suit :

Conditions préalables

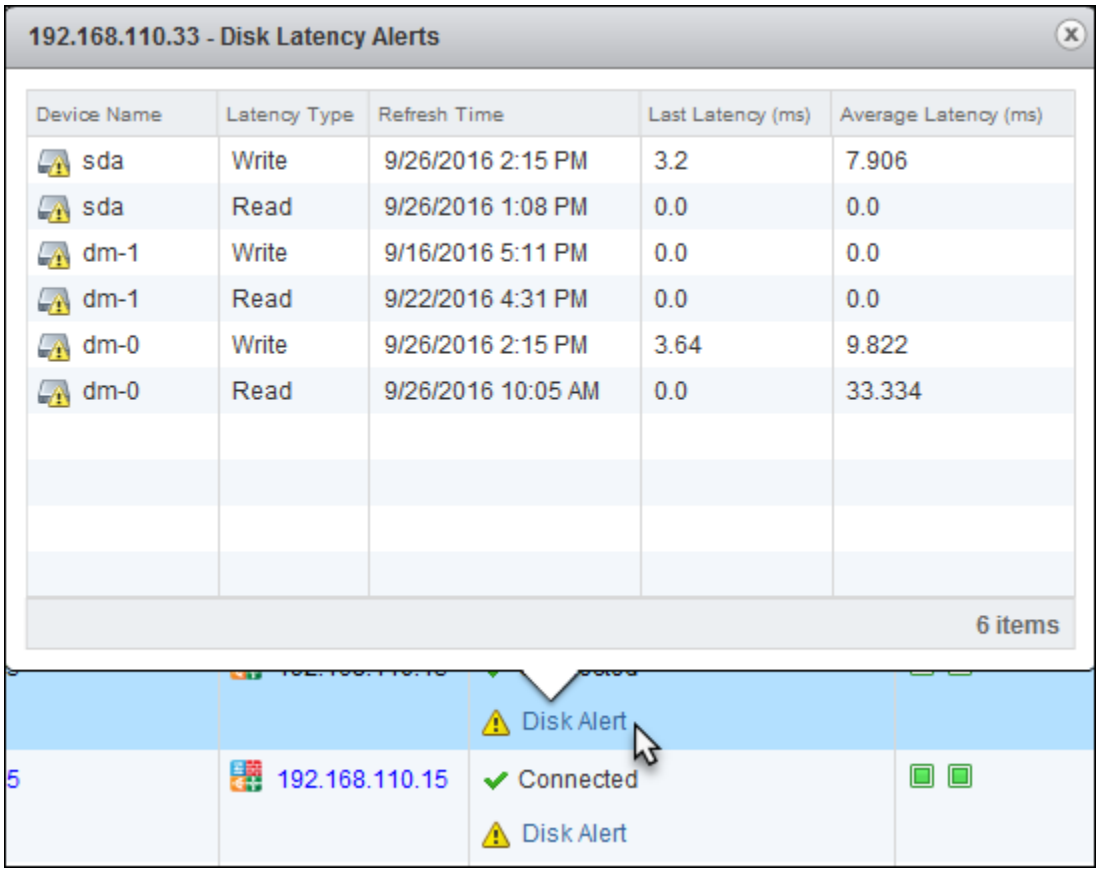
La limite de la latence est atteinte.

Procédure

1. Connectez-vous à vSphere Web Client.
2. Cliquez sur **Networking & Security**, puis sur **Installation**.

3 Sous **Gestion (Management)**, allez dans le contrôleur requis, puis cliquez sur le lien **Alerte de disque (Disk Alert)**.

La fenêtre Alertes de latence du disque apparaît.



Résultats

Vous pouvez afficher les informations sur la latence pour le contrôleur sélectionné. Les journaux des alertes sont stockés pendant sept jours dans le fichier `cloudnet/run/iostat/iostat_alert.log`. Vous pouvez utiliser la commande `show log cloudnet/run/iostat/iostat_alert.log` pour afficher le fichier journal.

Étape suivante

Pour plus d'informations de dépannage concernant les problèmes de latence du disque, consultez la section Problèmes de latence du disque.

Pour plus d'informations sur les messages de journal, consultez le document *Journalisation et événements système dans NSX*.

Problèmes de latence du disque

Les contrôleurs doivent fonctionner sur des disques à latence faible. Le cluster requiert un système de stockage de disque pour chaque nœud afin d'avoir une latence d'écriture maximale inférieure à 300 ms et une latence d'écriture moyenne inférieure à 100 ms.

Problème

- Un dispositif NSX Controller déployé est déconnecté d'un cluster de contrôleurs.
- Impossible de recueillir des journaux de contrôleur car la partition de disque est pleine.
- Si le système de stockage ne respecte pas ces exigences, le cluster risque de devenir instable et d'entraîner l'interruption du système.
- Les écouteurs TCP applicables à un dispositif NSX Controller en fonctionnement n'apparaissent plus dans la sortie de la commande `show network connections of-type tcp`.
- Le contrôleur déconnecté tente de rejoindre le cluster à l'aide d'une UUID composée de zéros uniquement, ce qui n'est pas valide.
- La commande de l'historique des clusters de contrôle d'affichage affiche un message ressemblant à :

  ```
  INFO.20150530-000550.1774:D0530 13:25:29.452639 1983 zookeeper_client.cc:774] Zookeeper
  client disconnected!
  ```

- L'exécution de la commande `show log cloudnet/cloudnet_java-zookeeper*.log` dans la console NSX Controller contient des entrées similaires à :

  ```
  cloudnet_java-zookeeper.20150530-000550.1806.log-2015-05-30
       13:25:07,382 47956539 [SyncThread:1] WARN
       org.apache.zookeeper.server.persistence.FileTxnLog - fsync-ing the write ahead
       log in SyncThread:1 took 3219ms which will adversely effect operation latency.
       See the ZooKeeper troubleshooting guide
  ```

- Les journaux NSX Controller contiennent des entrées similaires à :

  ```
  D0525 13:46:07.185200 31975
       rpc-broker.cc:369] Registering address resolution for: 20.5.1.11:7777
  D0525 13:46:07.185246 31975
       rpc-tcp.cc:548] Handshake complete, both peers support the same
       protocol
  D0525 13:46:07.197654 31975
       rpc-tcp.cc:1048] Rejecting a connection from peer
       20.5.1.11:42195/ef447643-f05d-4862-be2c-35630df39060, cluster
       9f7ea8ff-ab80-4c0c-825e-628e834aa8a5, which doesn't match our cluster
       (00000000-0000-0000-0000-000000000000)
  D0525 13:46:07.222869 31975
       rpc-tcp.cc:1048] Rejecting a connection from peer
       20.5.1.11:42195/ef447643-f05d-4862-be2c-35630df39060, cluster
       9f7ea8ff-ab80-4c0c-825e-628e834aa8a5, which doesn't match our cluster
       (00000000-0000-0000-0000-000000000000)
  ```

Cause

Ce problème survient en raison de lentes performances du disque, ce qui impacte négativement le cluster NSX Controller.

- Vérifiez la présence de disques lents en recherchant les messages *fsync* dans le fichier `/var/log/cloudnet/cloudnet_java-zookeeper log`. Si *fsync* prend plus d'une seconde, ZooKeeper affiche

un message d'avertissement *fsync*, qui est une bonne indication mettant en valeur la trop grande lenteur du disque. VMware recommande de consacrer un numéro d'unité logique spécifiquement pour le cluster de contrôles et/ou de déplacer la baie de stockage plus près du cluster de contrôles en termes de latences.

- Vous pouvez afficher les calculs de latence en lecture et en écriture qui sont ajoutés à une moyenne de déplacement de 5 secondes (par défaut), qui est à son tour utilisée pour déclencher une alerte lors de la violation de la limite de la latence. L'alerte est désactivée une fois que la moyenne revient à la limite inférieure. Par défaut, la limite supérieure est définie sur 200 ms et la limite inférieure sur 100 ms. Vous pouvez utiliser la commande `show disk-latency-alert config`. La sortie s'affiche comme suit :

```
enabled=True   low-wm=51      high-wm=150
nsx-controller # set disk-latency-alert enabled yes
nsx-controller # set disk-latency-alert low-wm 100
nsx-controller # set disk-latency-alert high-wm 200
```

- Utilisez l'API REST `GET /api/2.0/vdn/controller/<controller-id>/systemStats` pour récupérer l'état d'alerte de latence des nœuds du contrôleur.
- Utilisez l'API REST `GET /api/2.0/vdn/controller` pour indiquer si une alerte de latence du disque est détectée sur un nœud de contrôleur.

Solution

1. Déployez NSX Controller sur des disques à faible latence.
2. Chaque contrôleur doit utiliser son propre serveur de stockage de disque. Ne partagez pas le même serveur de stockage de disque entre deux contrôleurs.

Étape suivante

Pour plus d'informations sur l'affichage des alertes, consultez la section Afficher les alertes de latence du disque

Défaillances du cluster NSX Controller

Lorsque l'un des nœuds NSX Controller du cluster échoue, deux contrôleurs fonctionnent toujours. La majorité du cluster est conservée et le plan de contrôle continue de fonctionner.

Problème

Le cluster NSX Controller a échoué.

Solution

1. Connectez-vous à vSphere Web Client.
2. Dans **Networking & Security**, cliquez sur **Installation > Gestion (Installation > Management)**.

3 Dans la section de nœuds NSX Controller, observez la colonne Homologues. Si la colonne Homologues affiche des cases vertes, cela signifie que la connectivité des contrôleurs homologues ne présente pas d'erreur dans le cluster. Une case rouge indique une erreur avec un homologue. Cliquez sur la case pour afficher les détails.

4 Si la colonne Homologues affiche un problème avec le cluster de contrôleurs, connectez-vous à chaque CLI NSX Controller pour effectuer un diagnostic détaillé. Exécutez la commande `control-cluster status` d'affichage pour diagnostiquer l'état de chaque contrôleur. Tous les contrôleurs du cluster doivent avoir la même UUID de cluster. Toutefois, il est possible que l'UUID de cluster soit différente de l'UUID du contrôleur maître. Vous pouvez trouver des informations sur les problèmes de déploiement comme décrits dans Problèmes de déploiement de NSX Controller .

5 Vous pouvez essayer les étapes suivantes pour résoudre le problème avant de redéployer le nœud de contrôleur ou le cluster de contrôleur :

   a Vérifiez que le contrôleur est activé.

   b Tentez d'exécuter une commande ping du contrôleur affecté vers d'autres nœuds et le gestionnaire pour vérifier les chemins d'accès réseau. Si vous trouvez des problèmes réseau, traitez-les comme décrit dans Problèmes de déploiement de NSX Controller .

   c Vérifiez l'état IPSec (Internet Protocol Security) à l'aide des commandes CLI suivantes.

      - Vérifiez si IPSec est activé à l'aide de la commande `show control-cluster network ipsec status`.
      - Vérifiez l'état des tunnels IPSec à l'aide de la commande `show control-cluster network ipsec tunnels`.

      Vous pouvez aussi utiliser les informations de l'état IPSec pour ouvrir un ticket avec le support technique VMware.

   d Si le problème n'est pas un problème réseau, vous pouvez choisir de redémarrer ou de redéployer.

   Si vous souhaitez redémarrer un nœud, assurez-vous qu'un seul contrôleur est redémarré à la fois. Toutefois, si le cluster de contrôleur est dans un état où plusieurs nœuds de contrôleur ont échoué, redémarrez-les tous en même temps. Lors du redémarrage d'un nœud à partir d'un cluster sain, confirmez toujours que le cluster est reformé correctement ensuite, puis confirmez que le partitionnement du cluster est fait correctement.

6 Si vous décidez de redéployer des contrôleurs, utilisez l'une des deux approches suivantes :

   - Approche 1 : supprimez le nœud de contrôleur interrompu et redéployez un nouveau nœud de contrôleur.
   - Approche 2 : supprimez le cluster de contrôleurs et redéployez un nouveau cluster de contrôleurs.

     VMware recommande la deuxième approche.

Étape suivante

Choisissez une approche :

- Approche 1 : supprimer le contrôleur interrompu et redéployer un nouveau contrôleur
- Approche 2 : redéployer le cluster NSX Controller

Approche 1 : supprimer le contrôleur interrompu et redéployer un nouveau contrôleur

Vous pouvez d'abord essayer de résoudre le problème sans redéployer un nouveau cluster NSX Controller. Dans cette approche, vous devez d'abord supprimer le nœud NSX Controller interrompu, puis déployer un nouveau nœud NSX Controller.

Procédure

1 Supprimer un NSX Controller

Vous pouvez supprimer un NSX Controller de force ou normalement. La procédure de suppression normale vérifie les conditions suivantes avant de supprimer le nœud :

2 Redéployer un NSX Controller

Après la suppression du nœud de contrôleur interrompu, déployez un nouveau nœud de contrôleur.

Supprimer un NSX Controller

Vous pouvez supprimer un NSX Controller de force ou normalement. La procédure de suppression normale vérifie les conditions suivantes avant de supprimer le nœud :

- Actuellement, il n'existe aucune opération de mise à niveau de nœud NSX Controller.
- Le cluster de contrôleurs est sain et une demande API du cluster de contrôleurs peut être traitée.
- L'état de l'hôte, comme obtenu à partir de l'inventairevCenter Server, se montre comme étant connecté et activé.
- Ce n'est pas le dernier nœud de contrôleur.

La procédure de suppression forcée ne vérifie pas les conditions susmentionnées avant de supprimer le nœud de contrôleur.

- À retenir lors de la suppression de contrôleurs :
  - Ne tentez pas de supprimer la VM de contrôleur avant de la supprimer via l'interface utilisateur ou l'API vSphere Web Client. Lorsque l'interface utilisateur n'est pas disponible, supprimez le contrôleur via l'API `DELETE /2.0/vdn/controller/{controllerId}`.
  - Après la suppression d'un nœud, assurez-vous que le cluster existant reste stable.
  - Lors de la suppression de tous les nœuds d'un cluster, le dernier nœud restant doit être supprimé à l'aide de l'option **Forcer la suppression du contrôleur (Forcefully remove the controller)**. Vérifiez systématiquement que la VM du contrôleur est bien supprimée. Si ce n'est pas le cas, mettez la machine virtuelle hors tension manuellement et supprimez la VM du contrôleur via l'interface utilisateur.

- Si l'opération de suppression échoue, cela signifie que la VM n'a pas pu être supprimée. Dans ce cas, appelez la suppression du contrôleur via l'interface utilisateur à l'aide de l'option **Forcer la suppression du contrôleur (Forcefully remove the controller)**. Pour l'API, définissez le paramètre `forceRemoval` sur *true*. Après une suppression forcée, mettez la machine virtuelle hors tension manuellement et supprimez la VM du contrôleur via l'interface utilisateur.
- Dans la mesure où un cluster multi-nœud peut uniquement supporter un échec, une suppression est considérée comme un échec. Le nœud supprimé doit être redéployé avant qu'un autre échec se produise.

- Pour l'environnement Cross-vCenter NSX :
  - La suppression de la VM du contrôleur ou sa désactivation directe dans vCenter Server n'est pas une opération prise en charge. La colonne **État (Status)** affiche l'état **Désynchronisé (Out of sync)**.
  - Si la suppression du contrôleur n'est que partielle et qu'une entrée est oubliée dans la base de données NSX Manager dans un environnement Cross-vCenter NSX, utilisez l'API `DELETE api/2.0/vdn/controller/external`.
  - Si le contrôleur a été importé via l'API NSX Manager, utilisez l'API `removeExternalControllerReference` avec l'option `forceRemoval`.
  - Lorsque vous supprimez un contrôleur, NSX demande la suppression d'une VM de contrôleur via vCenter Server à l'aide de l'ID d'objet géré (MOID) de la VM. Si vCenter Server ne trouve pas la VM avec son MOID, NSX signale l'échec de la demande de suppression du contrôleur et abandonne l'opération.

    Si l'option **Supprimer de force (Forcefully Delete)** est sélectionnée, NSX n'arrête pas l'opération de suppression du contrôleur et efface les informations du contrôleur. NSX met également à jour tous les hôtes afin qu'ils ne fassent plus confiance au contrôleur supprimé. Toutefois, si la VM de contrôleur est toujours active et en cours d'exécution avec un MOID différent, elle dispose toujours d'informations d'identification pour participer comme membre du cluster de contrôleurs. Dans ce scénario, n'importe quel commutateur logique ou routeur attribué à ce nœud de contrôleur ne fonctionne pas correctement, car les hôtes ESXi ne font plus confiance au contrôleur supprimé.

Pour supprimer le dispositif NSX Controller, procédez comme suit :

Procédure

1. Connectez-vous à vSphere Web Client.
2. Cliquez sur **Networking & Security**, puis sur **Installation**.
3. Sous **Gestion (Management)**, sélectionnez le contrôleur que vous souhaitez supprimer.
4. Cliquez sur l'icône **Supprimer (x) (Delete (x))**.

5 Sélectionnez **Supprimer (Delete)** ou **Supprimer de force (Forcefully Delete)**.

- Lorsque vous sélectionnez l'option **Supprimer de force (Forcefully Delete)**, le contrôleur est supprimé de force, et non normalement. Cette option ignore les échecs et efface les données de la base de données. Vous devez vérifier que les échecs possibles sont traités manuellement. Vous devez confirmer que la VM de contrôleur est correctement supprimée. Si ce n'est pas le cas, vous devez la supprimer via le vCenter Server

Note Si vous supprimez le dernier contrôleur du cluster, vous devez sélectionner l'option **Supprimer de force (Forcefully Delete)** pour supprimer le dernier nœud de contrôleur. Si le système ne comporte aucun contrôleur, les hôtes fonctionnent en mode « administration à distance ». Les nouvelles machines virtuelles ou les machines virtuelles faisant l'objet d'une opération vMotion rencontreront des problèmes de mise en réseau tant que le déploiement des nouveaux contrôleurs et la synchronisation n'auront pas été effectués.

- Si vous ne sélectionnez pas cette option, le contrôleur est supprimé normalement.

6 Cliquez sur **Oui (Yes)**. La suppression normale du contrôleur utilise la séquence suivante :

a Désactivez le nœud.

b Vérifiez la santé du cluster.

c Si le cluster n'est pas sain, activez le contrôleur et faites échouer la demande de suppression.

d Si le cluster est sain, supprimez la VM du contrôleur, puis libérez l'adresse IP du nœud.

e Supprimez l'identité de la VM du contrôleur du cluster.

Le contrôleur sélectionné est supprimé.

7 Resynchronisez l'état du contrôleur en cliquant sur **Actions > Mettre à jour l'état du contrôleur (Actions > Update Controller State)**.

Redéployer un NSX Controller

Après la suppression du nœud de contrôleur interrompu, déployez un nouveau nœud de contrôleur.

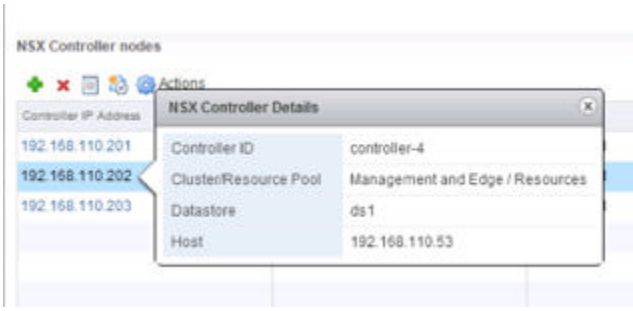
Procédure

1 Connectez-vous à vSphere Web Client.

2 Dans **Networking & Security**, cliquez sur **Installation > Gestion (Installation > Management)**.

3 Dans la section **Nœuds NSX Controller**, cliquez sur le contrôleur concerné. Prenez des captures d'écran ou notez les informations de configuration dans l'écran **Détails de NSX Controller** pour référence ultérieure.

Par exemple :



4 Déployez un nouveau nœud NSX Controller en cliquant sur l'icône **Ajouter un nœud (+) (Add Node (+))**.

5 Dans la boîte de dialogue Ajouter un contrôleur, sélectionnez le centre de données sur lequel vous souhaitez ajouter les nœuds, puis configurez les paramètres du contrôleur.

   a Sélectionnez le cluster approprié.

   b Sélectionnez un hôte dans le cluster, puis un stockage.

   c Sélectionnez le groupe de ports distribué.

   d Sélectionnez le pool d'adresses IP à partir duquel les adresses IP doivent être assignées au nœud.

   e Cliquez sur **OK**, attendez la fin de l'installation et assurez-vous que le nœud dispose d'un état **Normal**.

   Pour obtenir des informations détaillées sur l'ajout d'un nœud de contrôleur, reportez-vous à la section « Déployer un cluster NSX Controller » dans le *Guide d'installation de NSX*.

6 Resynchronisez l'état du contrôleur en cliquant sur **Actions > Mettre à jour l'état du contrôleur**.

   Mettre à jour l'état du contrôleur transfère la configuration actuelle de VXLAN et du routeur logique distribué (y compris les objets universels dans un déploiement de Cross-vCenter NSX) depuis NSX Manager vers le cluster de contrôleurs.

Approche 2 : redéployer le cluster NSX Controller

Dans cette approche, supprimez les trois nœuds de contrôleur et ajoutez de nouveaux nœuds de contrôleur pour maintenir un cluster à trois nœuds entièrement fonctionnel.

VMware recommande de supprimer le cluster NSX Controller lorsque l'une des conditions suivantes est remplie :

- Un ou plusieurs nœuds de contrôleur sont confrontés à des erreurs catastrophiques ou irrécupérables.
- Les machines virtuelles de contrôleur sont inaccessibles et ne peuvent pas être réparées.

Dans de tels cas, supprimez de préférence tous les nœuds du contrôleur, même lorsque certains nœuds de contrôleur semblent sains.

Redéployez un nouveau cluster de contrôleurs, puis mettez à jour le mécanisme d'état du contrôleur sur NSX Manager. La mise à jour de l'état du contrôleur entraîne la resynchronisation de VXLAN et le redéploiement des routeurs logiques distribués.

Procédure

1. Connectez-vous à vSphere Web Client.
2. Accédez à **Mise en réseau et sécurité > Installation > Gestion**.
3. Dans la section **Nœuds de NSX Controller**, supprimez les trois nœuds de contrôleur. Supprimez un nœud à la fois et cliquez sur **Supprimer** (✖).

   Lorsqu'il n'existe aucun contrôleur dans le système, les hôtes fonctionnent en mode « headless ». Les nouvelles machines virtuelles ou les machines virtuelles migrées rencontreront des problèmes de mise en réseau tant que le déploiement des nouveaux contrôleurs et la synchronisation n'auront pas été effectués.
4. Déployez trois nouveaux nœuds de contrôleur pour créer un cluster NSX Controller entièrement fonctionnel.

   Pour obtenir des informations détaillées sur l'ajout d'un cluster de contrôleurs, reportez-vous à la section « Déployer un cluster NSX Controller » dans le *Guide d'installation de NSX*.
5. Resynchronisez l'état du contrôleur en cliquant sur **Actions > Mettre à jour l'état du contrôleur**.

Contrôleur fantôme

Un contrôleur fantôme peut être une machine virtuelle (VM) de contrôleur dynamique ou une VM inexistante faisant partie ou non du cluster. NSX Manager synchronise la liste de toutes les VM de l'inventaire vCenter Server. Un contrôleur fantôme est créé lorsque le serveur vCenter Server ou l'hôte supprime une VM de contrôleur sans demande de la part de NSX Manager ou lorsque l'inventaire vCenter Server modifie le MOID de référence des VM de contrôleur.

Lorsque le contrôleur est créé à partir de NSX, les informations de configuration sont stockées dans NSX Manager. NSX Manager déploie la nouvelle VM de contrôleur via le serveur vCenter Server.

L'administrateur NSX fournit la configuration, y compris le pool d'adresses IP, à NSX Manager pour créer un contrôleur. NSX Manager supprime une adresse IP du pool et envoie cette adresse IP avec le reste de la configuration du contrôleur sous forme de demande de création de VM au serveur vCenter Server. NSX Manager attend que le serveur vCenter Server confirme l'état de la demande.

- `The controller creation process was successful` : si la VM de contrôleur est créée correctement, vCenter Server la démarre. NSX Manager stocke le MOID de la VM avec le reste des informations de configuration du contrôleur. Le MOID (ou MO-REF) est un identifiant unique que vCenter attribue à chaque objet dans son inventaire. vCenter Server utilise également ce MOID pour effectuer le suivi de la VM si elle fait toujours partie de l'inventaire vCenter Server.
- `The controller creation process was not successful` : si les configurations d'adresse IP et de connexion réseau étaient incorrectes, NSX Manager pourrait ne pas être en mesure de contacter

vCenter Server. NSX Manager attend un intervalle de temps prédéfini pour créer un cluster de contrôleurs à un seul nœud (pour le premier) ou un nouveau contrôleur à joindre au cluster actif. Lorsque le temps est écoulé, NSX Manager demande à vCenter Server de supprimer la VM. L'adresse IP est renvoyée au pool et NSX déclare l'échec de la création du contrôleur.

Processus de création du contrôleur fantôme

Lorsque NSX Manager demande de supprimer un contrôleur, vCenter Server recherche la VM de contrôleur à supprimer à l'aide du MOID.

Toutefois, si des activités de vCenter entraînent la suppression de la VM de contrôleur de l'inventaire vCenter Server, vCenter supprime le MOID de sa base de données. Notez que la VM de contrôleur peut toujours être active sur NSX Manager, même après sa suppression de l'inventaire vCenter. Mais, pour vCenter Server, la VM de contrôleur n'existe plus. Même si vCenter Server a supprimé la VM de son inventaire, la VM n'est peut-être pas supprimée. Si la VM est toujours active, elle participe toujours ou tente toujours de participer au cluster de contrôleurs NSX.

Voici les exemples les plus courants des processus de création du contrôleur fantôme :

- L'administrateur de vCenter Server supprime l'hôte qui contient la VM de contrôleur de l'inventaire. Il rajoute ensuite l'hôte. Lorsque l'hôte est supprimé, vCenter Server supprime tous les MOID associés à l'hôte et les VM qu'il contient. Lorsque l'hôte est rajouté ultérieurement, vCenter Server attribue un nouveau MOID à l'hôte et aux VM. Pour les utilisateurs de NSX, l'hôte et la VM sont toujours identiques, mais du point de vue de vCenter Server, les hôtes et les VM sont de nouveaux objets. Toutefois, pour des raisons pratiques, les hôtes et les VM sont toujours identiques. Les applications qui s'exécutent dans l'hôte et les VM ne changent pas.
- L'administrateur de vCenter Server supprime la VM de contrôleur via vCenter Server ou à l'aide de la gestion de l'hôte. La suppression n'a pas été lancée par NSX Manager.
- *Supprimer*, dans ce cas, comprend également tous les échecs d'hôte/de stockage qui entraînent la perte de la VM. Dans ce cas, la VM est perdue pour vCenter Server, ainsi que pour le cluster et NSX Manager. Mais, comme la suppression n'a pas été lancée par NSX Manager, NSX Manager et le cluster de contrôleurs pensent que le contrôleur est toujours valide. L'état du contrôleur renvoyé à NSX Manager indique que ce nœud de contrôleur est inactif, qu'il ne fait pas partie du cluster et qu'il est affiché sur l'interface utilisateur. NSX Manager possède également des journaux indiquant que le contrôleur n'est plus accessible.

Actions à suivre lorsque vous voyez un contrôleur fantôme

1 Synchronisez les contrôleurs comme décrit dans la section NSX Controller est déconnecté.

2 Consultez les entrées du journal. Si la VM de contrôleur a été supprimée par accident ou si elle était endommagée, vous devez utiliser l'option **Supprimer de force (Forcefully Delete)** pour effacer l'entrée de la base de données NSX Manager. Pour plus de détails, voir Supprimer un NSX Controller.

3 Après la suppression du contrôleur, vérifiez que :

- La VM de contrôleur est bien supprimée.

- La commande `show controller-cluster startup-nodes` n'affiche que les contrôleurs valides.
- Les entrées Syslog de NSX Manager n'affichent plus de contrôleur supplémentaire.

À partir de NSX 6.2.7 ou version ultérieure, NSX Manager vérifie l'inventaire vCenter pour s'assurer que la VM de contrôleur existe toujours dans l'inventaire en fonction du MOID d'origine. Si NSX Manager ne peut pas trouver la VM de contrôleur dans l'inventaire, NSX Manager recherche la VM à l'aide de l'UUID d'instance de la VM. L'UUID d'instance est stocké dans la VM, donc il ne change pas même lorsque la VM est rajoutée à l'inventaire vCenter. Si NSX Manager peut trouver la VM avec l'UUID d'instance, NSX Manager met à jour sa base de données avec le nouveau MOID.

Toutefois, si vous clonez la VM de contrôleur, la VM clonée possède les mêmes propriétés que la VM d'origine, ainsi qu'un nouvel UUID d'instance. NSX Manager ne peut pas détecter le MOID de la VM clonée.

Entrées de journal du contrôleur fantôme

L'entrée de journal de niveau d'erreur suivante se produit lorsqu'un contrôleur fantôme est détecté :

- `2017-07-31 22:15:05.844 UTC ERROR NVPStatusCheck ControllerServiceImpl:2146 : le contrôleur <#> n'existe pas, il est peut-être déjà supprimé. Ignorer tout en enregistrant ses informations de connectivité.`
- `2017-07-31 22:15:05.769 UTC ERROR NVPStatusCheck ControllerServiceImpl:2580 : le nœud est créé par cette instance de NSX Manager <#>, mais la base de données ne contient aucun enregistrement et la suppression est peut-être en cours.`

NSX Controller est déconnecté

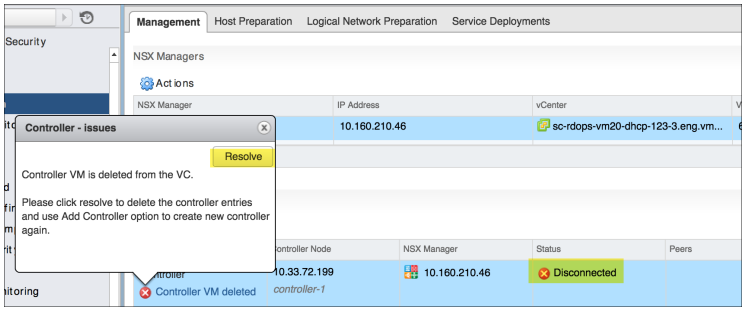
Si la VM NSX Controller a été désactivée à partir de vCenter Server ou qu'une VM de contrôleur a été supprimée du dispositif vCenter Server, la colonne **État (Status)** de la page **Installation** > **Gestion (Management)** affiche l'état **Désynchronisé (Out of sync)**.

Conditions préalables

VM de contrôleur hors tension ou VM de contrôleur supprimée du serveur vCenter Server.

Procédure

1 Dans vSphere Web Client, accédez à **Networking & Security > Installation** > **Gestion (Management)**.



2 Cliquez sur le lien **Erreur (Error)** pour consulter la raison détaillée de cet état désynchronisé.

3 Cliquez sur le bouton **Résoudre (Resolve)** pour résoudre le problème.

Résultats

Si la VM du contrôleur est désactivée, Management Plane déclenche une commande `power on` pour le contrôleur.

Si la VM du contrôleur est supprimée, les entrées de ce dernier sont supprimées du Management Plane et Management Plane communique la suppression du contrôleur au plan de contrôle central.

Étape suivante

Créez un nouveau contrôleur à l'aide de l'option **Ajouter un nœud (Add Node)**. Pour plus de détails, consultez le *Guide d'administration de NSX*.

Problèmes de l'agent du plan de contrôle (netcpa)

Sur NSX pour vSphere, le plan de contrôle (netcpa) fonctionne comme daemon d'agent local, en communiquant avec NSX Manager et le cluster de contrôleurs. La fonctionnalité **Santé du canal de communication (Communication Channel Health)** est une vérification de santé proactive qui signale périodiquement l'état du plan de contrôle central au plan de contrôle local à NSX Manager et s'affiche dans l'interface utilisateur NSX Manager. Ce rapport sert aussi de pulsation pour détecter l'état opérationnel du dispositif NSX Manager pour le canal netcpa de l'hôte ESXi. Il fournit les détails des erreurs pendant les erreurs de communication, génère un événement lorsqu'un canal passe à un état incorrect et génère aussi des messages de pulsation du dispositif NSX Manager vers les hôtes.

Problème

Problèmes de connectivité entre l'agent du plan de contrôle et le contrôleur.

Cause

Il se peut que l'agent du plan de contrôle ne fonctionne pas correctement en cas de connexion manquante.

Solution

1 Validez l'état de connexion lorsque le canal passe dans un état incorrect à l'aide de la commande suivante :

```
GET https://<NSX_Manager_IP>/api/2.0/vdn/inventory/host/{hostId}/connection/status
```

Exemple de valeur renvoyée :

```
<?xml version="1.0" encoding="UTF-8"?>
<hostConnStatus>
<hostName>10.161.246.20</hostName>
<hostId>host-21</hostId>
<nsxMgrToFirewallAgentConn>UP</nsxMgrToFirewallAgentConn>
<nsxMgrToControlPlaneAgentConn>UP</nsxMgrToControlPlaneAgentConn>
<hostToControllerConn>DOWN</hostToControllerConn>
```

```
<fullSyncCount>-1</fullSyncCount>
<hostToControllerConnectionErrors>
<hostToControllerConnectionError>
<controllerIp>10.160.203.236</controllerIp>
<errorCode>1255604</errorCode>
<errorMessage>Connection Refused</errorMessage>
</hostToControllerConnectionError>
<hostToControllerConnectionError>
<controllerIp>10.160.203.237</controllerIp>
<errorCode>1255603</errorCode>
<errorMessage>SSL Handshake Failure</errorMessage>
</hostToControllerConnectionError>
</hostToControllerConnectionErrors>
</hostConnStatus>
```

Les codes d'erreur suivants sont pris en charge :

```
1255602 : Certificat de contrôleur incomplet 1255603 : Échec d'établissement d'une liaison SSL
1255604 : Connexion refusée 1255605 : Expiration de la connexion persistante 1255606 : Exception
SSL 1255607 : Message incorrect 1255620 : Erreur inconnue
```

2 Déterminez la raison pour laquelle l'agent du plan de contrôle est inactif de la manière suivante :

a Vérifiez l'état de l'agent du plan de contrôle sur les hôtes en exécutant la commande `/etc/init.d/netcpad status` sur les hôtes ESXi.

```
[root@esx-01a:~] /etc/init.d/netcpad status
netCP agent service is running
```

b Vérifiez les configurations de l'agent du plan de contrôle à l'aide de la commande `more /etc/vmware/netcpa/config-by-vsm.xml`. Les adresses IP des instances de NSX Controller devraient apparaître.

```
[root@esx-01a:~] more /etc/vmware/netcpa/config-by-vsm.xml
<config>
  <connectionList>
    <connection id="0000">
      <port>1234</port>
      <server>192.168.110.31</server>
      <sslEnabled>true</sslEnabled>
      <thumbprint>A5:C6:A2:B2:57:97:36:F0:7C:13:DB:64:9B:86:E6:EF:1A:7E:5C:36</thumbprint>
    </connection>
    <connection id="0001">
      <port>1234</port>
      <server>192.168.110.32</server>
      <sslEnabled>true</sslEnabled>
      <thumbprint>12:E0:25:B2:E0:35:D7:84:90:71:CF:C7:53:97:FD:96:EE:ED:7C:DD</thumbprint>
    </connection>
    <connection id="0002">
      <port>1234</port>
      <server>192.168.110.33</server>
      <sslEnabled>true</sslEnabled>
```

```
      <thumbprint>BD:DB:BA:B0:DC:61:AD:94:C6:0F:7E:F5:80:19:44:51:BA:90:2C:8D</thumbprint>
    </connection>
  </connectionList>
...
```

3 Validez les connexions aux contrôleurs depuis l'agent du plan de contrôle à l'aide de la commande suivante. La sortie est une connexion pour chaque contrôleur.

```
>[root@esx-01a:~] esxcli network ip connection list | grep 1234
tcp     0   0  192.168.110.51:16594     192.168.110.31:1234   ESTABLISHED     36754  newreno
netcpa-worker
tcp     0   0  192.168.110.51:46917     192.168.110.33:1234   ESTABLISHED     36754  newreno
netcpa-worker
tcp     0   0  192.168.110.51:47891     192.168.110.32:1234   ESTABLISHED     36752  newreno
netcpa-worker
```

4 Validez les connexions aux contrôleurs depuis l'agent du plan de contrôle pour afficher l'état `CLOSED` ou `CLOSE_WAIT` en exécutant la commande suivante :

```
esxcli network ip
        connection list |grep "1234.*netcpa*" | egrep "CLOSED|CLOSE_WAIT"
```

5 Si l'agent du plan de contrôle est inactif depuis un temps important, il se peut que les connexions ne soient pas présentes du tout. Pour valider cela, exécutez la commande suivante : La sortie est une connexion pour chaque contrôleur.

```
esxcli network ip
        connection list |grep "1234.*netcpa*" |grep ESTABLISHED
```

6 Mécanisme de récupération automatique de l'agent du plan de contrôle (netcpa) : le processus de surveillance de l'agent du plan de contrôle automatique détecte que l'agent du plan de contrôle est dans un état incorrect. Lorsque l'agent du plan de contrôle est dans un état incorrect, il ne répond plus et essaie automatiquement de récupérer.

   a Lorsque l'agent du plan de contrôle ne répond plus, un fichier de base dynamique est généré. Vous pouvez trouver le fichier de base comme suit :

```
ls /var/core
 netcpa-worker-zdump.000
```

   b Une erreur de Syslog est signalée dans le fichier *vmkwarning.log*.

```
cat /var/run/log/vmkwarning.log | grep NETCPA
2017-08-11T06:32:17.994Z cpu1:1000044539)ALERT: Critical - NETCPA is hanged
Taking live-dump & restarting netcpa process!
```

Note Si le moniteur de l'agent du plan de contrôle connaît une défaillance temporaire en raison d'une réponse différée à la vérification de l'état, un message d'avertissement semblable au suivant peut être signalé dans les journaux VMKernel.

```
Avertissement - NETCPA n'a pas pu obtenir l'état de netcpa !
```

Vous pouvez ignorer cet avertissement.

7 Si le problème n'est pas récupéré automatiquement, redémarrez l'agent du plan de contrôle comme suit :

   a Connectez-vous en tant que racine à l'hôte ESXi via SSH ou via la console.

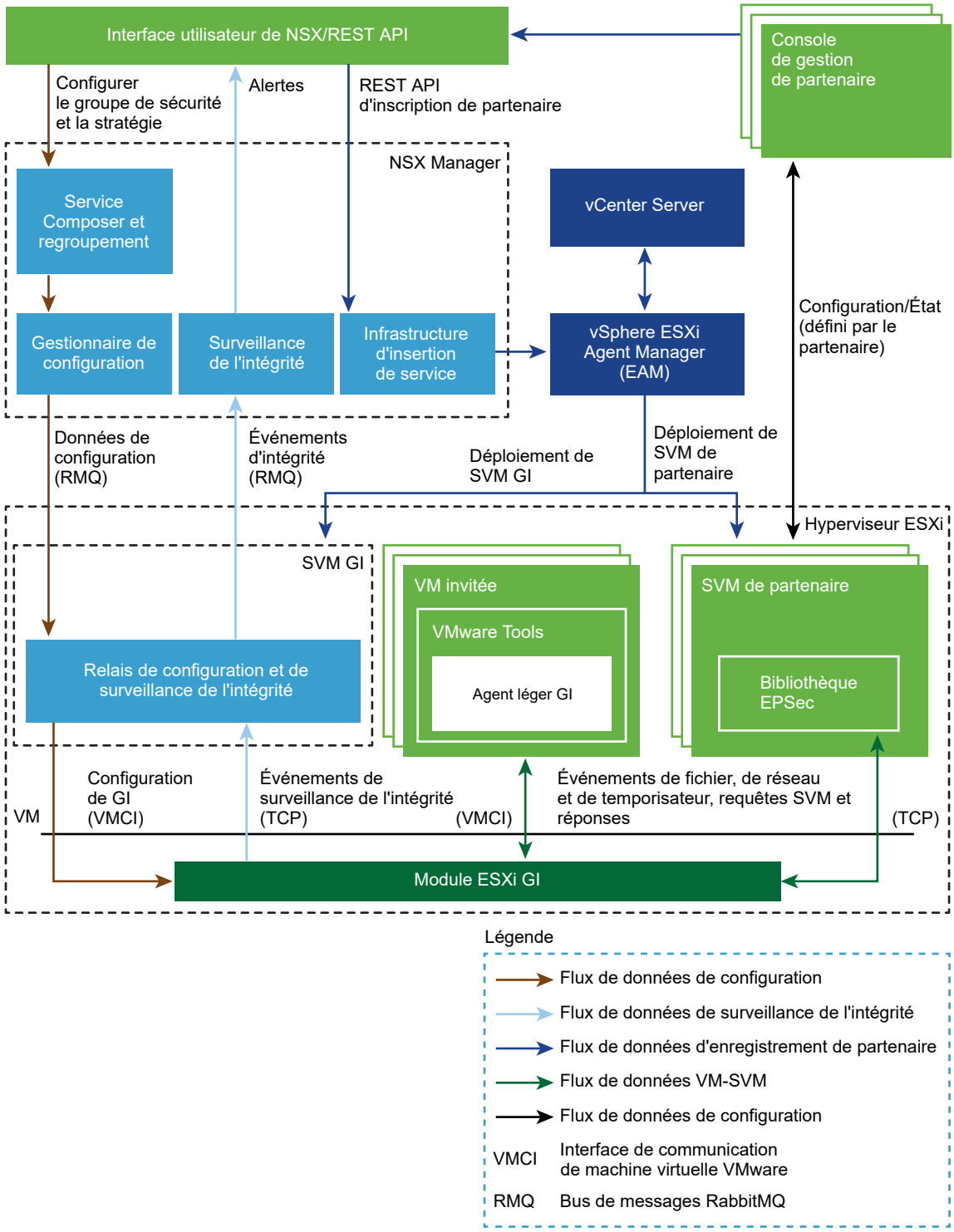
   b Exécutez la commande `/etc/init.d/netcpad restart` pour redémarrer l'agent du plan de contrôle sur l'hôte ESXi.

Dépannage de Guest Introspection

9

Ce chapitre contient les rubriques suivantes :

Architecture de Guest Introspection



Journaux de Guest Introspection

Il existe plusieurs journaux différents que vous pouvez capturer afin de les utiliser lors du dépannage de Guest Introspection.

Journaux de module ESX GI (MUX)

Si des machines virtuelles sur un hôte ESXi ne fonctionnent pas avec Guest Introspection, ou s'il existe des alarmes sur un hôte concernant la communication avec le SVA, il peut y avoir un problème avec le module ESX GI sur l'hôte ESXi.

Chemin du journal et exemple de message

Chemin du journal MUX
/var/log/syslog
var/run/syslog.log

Les messages du module ESX GI (MUX) suivent le format <timestamp>EPSecMUX<[ThreadID]>: <message>

Par exemple :

```
2017-07-16T05:44:49Z EPSecMux[38340669]: [ERROR] (EPSEC) [38340669]
Attempted to recv 4 bytes from sd 49, errno = 104 (Connection reset by peer)
```

Dans l'exemple ci-dessus :

- [ERROR] est le type de message. Les autres types peuvent être [DEBUG], [INFO]
- (EPSEC) indique que les messages sont relatifs à Endpoint Security

Activation et affichage des fichiers journaux

Pour afficher la version du VIB du module ESX GI installé sur l'hôte, exécutez la commande `#esxcli software vib list | grep epsec-mux`.

Pour activer la journalisation complète, effectuez ces étapes sur le shell de commande d'hôte ESXi :

1 Exécutez la commande ps -c |grep Mux pour rechercher les processus du module ESX GI en cours d'exécution.

   Par exemple :

   ```
   ~ # ps -c | grep Mux
   192223 192223 sh  /bin/sh /sbin/watchdog.sh -s vShield-Endpoint-Mux -q 100 -t 1000000 /usr/lib/
   vmware/vShield-Endpoint-Mux 900 -c 910
   192233 192233 vShield-Endpoint-Mux /usr/lib/vmware/vShield-Endpoint-Mux 900 -c 910
   192236 192233 vShield-Endpoint-Mux /usr/lib/vmware/vShield-Endpoint-Mux 900 -c 910
   ```

2 Si le service n'est pas en cours d'exécution, vous pouvez le redémarrer avec la commande `/etc/init.d/vShield-Endpoint-Mux start` ou `/etc//init.d/vShield-Endpoint-Mux restart`.

3 Pour arrêter les processus en cours d'exécution du module ESX GI, notamment le processus watchdog.sh, exécutez la commande `~ # kill -9 192223 192233 192236 .`

   Notez que deux processus du module ESX GI sont générés.

4 Démarrez un module ESX GI avec une nouvelle option –d. Notez que l'option -d n'existe pas pour les builds epsec-mux 5.1.0-01255202 et 5.1.0-01814505 ~ # /usr/lib/vmware/vShield–Endpoint–Mux –d 900 –c 910

5 Affichez les messages de journaux du module ESX GI dans le fichier /var/log/syslog.log sur l'hôte ESXi. Vérifiez que les entrées correspondant aux solutions globales, à l'ID de solution et au numéro de port sont correctement spécifiés.

Exemple : Exemple de fichier muxconfig.xml

```
<?xml version="1.0" encoding="UTF–8"?>

<EndpointConfig>

  <InstalledSolutions>

    <Solution>

      <id>100</id>

      <ipAddress>xxx.xxx.xxx.xxx</ipAddress>

      <listenOn>ip</listenOn>

      <port>48655</port>

      <uuid>42383371–3630–47b0–8796–f1d9c52ab1d0</uuid>

      <vmxPath>/vmfs/volumes/7adf9e00–609186d9/EndpointService (216)/EndpointService (216).vmx</
vmxPath>

    </Solution>

    <Solution>

      <id>102</id>

      <ipAddress>xxx.xxx.xxx.xxx</ipAddress>

      <listenOn>ip</listenOn>

      <port>48651</port>

      <uuid>423839c4–c7d6–e92e–b552–79870da05291</uuid>

      <vmxPath>/vmfs/volumes/7adf9e00–609186d9/apoon/EndpointSVM–alpha–01/EndpointSVM–alpha–01.vmx</
vmxPath>

    </Solution>

    <Solution>

      <id>6341068275337723904</id>
```

```
      <ipAddress>xxx.xxx.xxx.xxx</ipAddress>
      <listenOn>ip</listenOn>
      <port>48655</port>
      <uuid>42388025-314f-829f-2770-a143b9cbd1ee</uuid>
      <vmxPath>/vmfs/volumes/7adf9e00-609186d9/DlpService (1)/DlpService (1).vmx</vmxPath>
    </Solution>
  </InstalledSolutions>
  <DefaultSolutions/>
  <GlobalSolutions>
    <solution>
      <id>100</id>
      <tag></tag>
      <order>0</order>
    </solution>
    <solution>
      <id>102</id>
      <tag></tag>
      <order>10000</order>
    </solution>
    <solution>
      <id>6341068275337723904</id>
      <tag></tag>
      <order>10001</order>
    </solution>
  </GlobalSolutions>
</EndpointConfig>
```

Journaux de l'agent léger GI

L'agent léger est installé sur le système d'exploitation invité de machine virtuelle et détecte les détails de l'ouverture de session utilisateur.

Chemin du journal et exemple de message

L'agent léger se compose de pilotes GI : vsepflt.sys, vnetflt.sys, vnetwfp.sys (Windows 10 et versions ultérieures).

Les journaux de l'agent léger se trouvent sur l'hôte ESXi, dans le cadre du bundle de journaux vCenter. Le chemin du journal est `/vmfs/volumes/<datastore>/<vmname>/vmware.log`. Par exemple : `/vmfs/volumes/5978d759-56c31014-53b6-1866abaace386/Windows10-(64-bit)/vmware.log`

Les messages de l'agent léger suivent le format <timestamp> <VM Name><Process Name><[PID]>: <message>.

Dans l'exemple de journal ci-dessous, `Guest: vnet or Guest:vsep` indique les messages de journal liés aux pilotes GI respectifs, suivis de messages de débogage.

Par exemple :

```
2017-10-17T14:25:19.877Z| vcpu-0| I125: Guest: vnet: AUDIT: DriverEntry :
 vnetFilter build-4325502 loaded
2017-10-17T14:25:20.282Z| vcpu-0| I125: Guest: vsep:
AUDIT: VFileSocketMgrConnectHelper : Mux is connected
2017-10-17T14:25:20.375Z| vcpu-0| I125:
Guest: vsep: AUDIT: DriverEntry : vfileFilter build-4286645 loaded

2017-10-17T18:22:35.924Z| vcpu-0| I125: Guest: vsep: AUDIT:
VFileSocketMgrConnectHelper : Mux is connected
2017-10-17T18:24:05.258Z| vcpu-0| I125: Guest: vsep: AUDIT:
VFileFltPostOpCreate : File (\Windows\System32\Tasks\Microsoft\Windows\
SoftwareProtectionPlatform\SvcRestartTask) in a transaction, ignore
```

Exemple : Activation de la journalisation du pilote d'agent léger vShield Guest Introspection

Comme le paramètre de débogage peut saturer le fichier vmware.log jusqu'à la limite, nous vous recommandons de désactiver le mode de débogage dès que vous avez collecté toutes les informations requises.

Cette procédure vous oblige à modifier le Registre Windows. Avant de modifier le Registre, veillez à en faire une sauvegarde. Pour plus d'informations sur la sauvegarde et la restauration du Registre, consultez l'article 136393 de la base de connaissances de Microsoft.

Pour activer la journalisation de débogage pour le pilote d'agent léger :

1 Cliquez sur **Démarrer > Exécuter (Start > Run)**. Entrez regedit et cliquez sur **OK**. La fenêtre Éditeur du Registre s'ouvre. Pour plus d'informations, consultez l'article 256986 de la base de connaissances de Microsoft.

2 Créez cette clé à l'aide de l'éditeur du Registre : `HKEY_LOCAL_Machine\SYSTEM \CurrentControlSet\services\vsepflt\parameters`.

3 Sous la clé de paramètre qui vient d'être créée, créez ces valeurs de type DWORD. Assurez-vous que hexadécimal est sélectionné lorsque vous entrez ces valeurs :

```
Name: log_dest
Type: DWORD
Value: 0x2

Name: log_level
Type: DWORD
Value: 0x10
```

Autres valeurs pour la clé de paramètre `log level` :

```
Audit 0x1
Error 0x2
Warn 0x4
Info 0x8
Debug 0x10
```

4 Ouvrez une invite de commande en tant qu'administrateur. Exécutez ces commandes pour décharger et recharger le mini-pilote du système de fichiers vShield Endpoint :

- `fltmc unload vsepflt`
- `fltmc load vsepflt`

Les entrées de journal se trouvent dans le fichier vmware.log situé dans la machine virtuelle.

Activation de la journalisation du pilote d'introspection réseau vShield GI

Comme le paramètre de débogage peut saturer le fichier vmware.log jusqu'à la limite, nous vous recommandons de désactiver le mode de débogage dès que vous avez collecté toutes les informations requises.

Cette procédure vous oblige à modifier le Registre Windows. Avant de modifier le Registre, veillez à en faire une sauvegarde. Pour plus d'informations sur la sauvegarde et la restauration du Registre, consultez l'article 136393 de la base de connaissances de Microsoft.

1 Cliquez sur **Démarrer > Exécuter (Start > Run)**. Entrez regedit et cliquez sur **OK**. La fenêtre Éditeur du Registre s'ouvre. Pour plus d'informations, consultez l'article 256986 de la base de connaissances de Microsoft.

2 Modifiez le Registre :

```
Windows Registry Editor Version 5.0
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vnetflt\Parameters]
"log_level" = DWORD: 0x0000001F
"log_dest"  = DWORD: 0x00000001
```

3 Redémarrez la machine virtuelle.

Emplacement des fichiers journaux vsepflt.sys et vnetflt.sys

Avec les paramètres de Registre log_dest DWORD:0x00000001, le pilote de l'agent léger de point de terminaison se connecte au débogueur. Exécutez le débogueur (DbgView depuis SysInternals ou windbg) pour capturer la sortie de débogage.

Vous pouvez également définir le paramètre de Registre log_dest sur DWORD:0x000000002. Dans ce cas, les journaux de pilote seront imprimés dans le fichier vmware.log, qui se trouve dans le dossier de machine virtuelle correspondant sur l'hôte ESXi.

Activation de la journalisation d'UMC

Le composant en mode utilisateur (UMC) Guest Introspection s'exécute dans le service VMware Tools sur la machine virtuelle protégée.

1 Sous Windows XP et Windows Server 2003, créez un fichier `tools config`, s'il n'existe pas dans le chemin suivant :`C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\tools.conf`.

2 Sous Windows Vista, Windows 7 et Windows Server 2008, créez un fichier `tools config`, s'il n'existe pas dans le chemin suivant : `C:\ProgramData\VMWare\VMware Tools\tools.conf`

3 Ajoutez ces lignes dans le fichier `tools.conf` pour activer la journalisation de composant UMC.

```
[logging]
log = true
vsep.level = debug
vsep.handler = vmx
```

Avec le paramètre `vsep.handler = vmx` , le composant UMC se connecte au fichier `vmware.log` , qui se trouve dans le dossier de machine virtuelle correspondant sur l'hôte ESXi.

Avec les journaux de paramètre suivants, les journaux de composant UMC sont imprimés dans le fichier journal spécifié.

```
vsep.handler = file
vsep.data = c:/path/to/vsep.log
```

Journaux EPSecLib et SVM GI

EPSecLib reçoit des événements du module ESX GI (MUX) de l'hôte ESXi.

Chemin du journal et exemple de message

Chemin du journal EPSecLib
/var/log/syslog
var/run/syslog

Les messages EPSecLib suivent le format <timestamp> <VM Name><Process Name><[PID]>: <message>

Dans l'exemple ci-dessous, [ERROR] est le type de message et (EPSEC) indique que les messages sont relatifs à Guest Introspection.

Par exemple :

```
Oct 17 14:26:00 endpoint-virtual-machine EPSecTester[7203]: [NOTICE] (EPSEC)
 [7203] Initializing EPSec library build: build-00000

Oct 17 14:37:41 endpoint-virtual-machine EPSecSample: [ERROR] (EPSEC) [7533] Event
terminated reading file. Ex: VFileGuestEventTerminated@tid=7533: Event id: 3554.
```

Collecte des journaux

Pour activer la journalisation de débogage de la bibliothèque EPSec, qui est un composant de la SVM GI :

1 Connectez-vous à la SVM GI en obtenant le mot de passe de console auprès de NSX Manager.

2 Créez le fichier `/etc/epseclib.conf` et ajoutez :

```
ENABLE_DEBUG=TRUE

ENABLE_SUPPORT=TRUE
```

3 Modifiez les autorisations en exécutant la commande `chmod 644 /etc/epseclib.conf`.

4 Redémarrez le processus GI-SVM en exécutant la commande `/usr/local/sbin/rcusvm restart`.

Cela active la journalisation de débogage pour EPSecLib sur la SVM GI et les journaux de débogage sont disponibles dans les messages /var/log/messages applicables à NSX for vSphere 6.2.x et 6.3.x. Comme le paramètre de débogage peut saturer le fichier vmware.log jusqu'à la limite, nous vous recommandons de désactiver le mode de débogage dès que vous avez collecté toutes les informations requises.

Journaux de SVM GI

Avant de capturer les journaux, déterminez l'ID de l'hôte ou le MOID de l'hôte :

- Exécutez les commandes `show cluster all` et `show cluster <cluster ID>` dans NSX Manager.

  Par exemple :

```
nsxmgr-01a> show cluster all

No.  Cluster Name       Cluster Id              Datacenter Name   Firewall Status
1    RegionA01-COMP01   domain-c26              RegionA01         Enabled
2    RegionA01-MGMT01   domain-c71              RegionA01         Enabled

nsxmgr-01a> show cluster  domain-c26

Datacenter: RegionA01
```

```
Cluster: RegionA01-COMP01
No.  Host Name            Host Id                 Installation Status
1    esx-01a.corp.local   host-29                 Ready
2    esx-02a.corp.local   host-31                 Ready
```

1 Pour déterminer l'état actuel de journalisation, exécutez cette commande :

   `GET https://nsxmanager/api/1.0/usvmlogging/host-##/com.vmware.vshield.usvm`

   `GET https://nsxmanager/api/1.0/usvmlogging/host-##/root`

2 Pour modifier l'état actuel de journalisation, exécutez cette commande :

   `POST https://nsxmanager/api/1.0/usvmlogging/host-##/changelevel`

```
## Example to change root logger ##

<?xml version="1.0" encoding="UTF-8" ?>
<logginglevel>
<loggerName>root</loggerName>
<level>DEBUG</level>
</logginglevel>

## Example to change com.vmware.vshield.usvm ##

<?xml version="1.0" encoding="UTF-8" ?>
<logginglevel>
<loggerName>com.vmware.vshield.usvm</loggerName>
<level>DEBUG</level>
</logginglevel>
```

3 Pour générer des journaux, exécutez cette commande :

   `GET https://NSXMGR_IP/api/1.0/hosts/host.###/techsupportlogs`

   Sélectionnez `Send` et `Download`.

   Notez que cette commande génère des journaux de SVM GI et enregistre le fichier sous `techsupportlogs.log.gz`. Comme le paramètre de débogage peut saturer le fichier vmware.log jusqu'à la limite, nous vous recommandons de désactiver le mode de débogage dès que vous avez collecté toutes les informations requises.

Collecte des détails de l'environnement et de la charge de travail de Guest Introspection

La collecte des détails de l'environnement est utile lors de la vérification de la compatibilité des composants.

1 Déterminez si NSX Guest Introspection est utilisé dans l'environnement du client. Si ce n'est pas le cas, supprimez le service Guest Introspection pour la machine virtuelle et vérifiez que le problème est résolu.

2 Collectez les détails de l'environnement :

   a Version du build ESXi : exécutez la commande `uname -a` sur l'hôte ESXi ou cliquez sur un hôte dans vSphere Web Client et recherchez le numéro de build en haut du volet de droite.

   b Version et numéro de build du produit Linux

   c `/usr/sbin/vsep – v` indique la version de production

```
Build number
------------------
Ubuntu
dpkg -l | grep vmware-nsx-gi-file
SLES12 and RHEL7
rpm -qa | grep vmware-nsx-gi-file
```

3 Version de VMware NSX ® for vSphere ® et les éléments suivants :

   - Nom et numéro de version de la solution de partenaire
   - Numéro de version de la bibliothèque EPSec utilisée par la solution de partenaire : connectez-vous à la SVM GI et exécutez le chemin d'accès `#strings` à `EPSec library/libEPSec.so | grep BUILD`
   - Système d'exploitation invité dans la machine virtuelle
   - Autres applications ou pilotes de système de fichiers tiers

4 Version du module ESX GI (MUX) : exécutez le logiciel esxcli de commande `vib list | grep epsec-mux`.

5 Collectez les détails de la charge de travail, tels que le type de serveur.

6 Collectez des journaux de l'hôte ESXi. Pour plus d'informations, consultez l'article Collecting diagnostic information for VMware ESX/ESXi (653) (Collecte d'informations de diagnostic pour VMware ESX/ESXi).

7 Collectez des journaux de machine virtuelle de service (SVM GI) à partir de la solution de partenaire. Contactez votre partenaire pour en savoir plus sur la collecte des journaux de SVM GI.

8 Collectez un fichier d'état interrompu lorsque le problème se produit. Consultez l'article Suspending a virtual machine on ESX/ESXi to collect diagnostic information (2005831) (Interruption d'une machine virtuelle sur ESX/ESXi pour collecter des informations de diagnostic).

9 Après la collecte des données, comparez la compatibilité des composants vSphere. Pour plus d'informations, consultez les Matrices d'interopérabilité des produits VMware.

Dépannage de l'agent léger sur Linux ou Windows

L'agent léger Guest introspection est installé avec VMware Tools ™ sur chaque machine virtuelle invitée.

Dépannage de l'agent léger sur Linux

Si une machine virtuelle est lente lors des opérations de lecture, d'écriture, de décompression ou d'enregistrement des fichiers, l'agent léger peut présenter des problèmes.

1 Vérifiez la compatibilité de tous les composants concernés. La compatibilité est l'un des principaux problèmes avec le point de terminaison. Vous avez besoin des numéros de build d'ESXi, de vCenter Server, de NSX Manager, ainsi que de la solution de sécurité que vous avez choisie (Trend Micro, McAfee, Kaspersky, Symantec etc.). Une fois ces données collectées, comparez la compatibilité des composants vSphere. Pour plus d'informations, consultez les Matrices d'interopérabilité des produits VMware.

2 Vérifiez que l'introspection de fichier est installée sur le système.

3 Vérifiez que l'agent léger est en cours d'exécution avec la commande *service vsepd status*. Une fois que cette commande est exécutée, vous devez voir le service vsep en état d'exécution.

4 Si vous pensez que l'agent léger pose un problème de performances avec le système, arrêtez le service en exécutant la commande *service vsepd stop*.

5 Puis effectuez un test pour obtenir une ligne de base. Vous pouvez ensuite démarrer le service vsep et effectuer un autre test en exécutant la commande *service vsepd start*.

6 Activez le débogage pour l'agent léger Linux :

   a Ouvrez le fichier `/etc/vsep/vsep.conf`

   b Passez DEBUG_LEVEL=4 sur DEBUG_LEVEL=7 pour tous les journaux

   c Vous pouvez définir cette option sur DEBUG_LEVEL=6 pour les journaux modérés

   d La destination du journal par défaut (DEBUG_DEST=2) est vmware.log (sur l'hôte). Pour la modifier sur invité (c'est-à-dire /var/log/message ou /var/log/syslog), définissez DEBUG_DEST=1

   Note L'activation de la journalisation complète peut provoquer une activité de journalisation importante qui entraîne la saturation du fichier `vmware.log`, qui peut devenir potentiellement très volumineux. Désactivez la journalisation complète dès que possible.

Dépannage de l'agent léger sur Windows

1 Vérifiez la compatibilité de tous les composants concernés. Vous avez besoin des numéros de build d'ESXi, de vCenter Server, de NSX Manager, ainsi que de la solution de sécurité que vous avez choisie (Trend Micro, McAfee, Kaspersky, Symantec etc.). Une fois toutes ces données collectées, vous pouvez comparer la compatibilité des composants vSphere. Pour plus d'informations, consultez les Matrices d'interopérabilité des produits VMware.

2 Vérifiez que VMware Tools ™ est à jour. Si vous voyez qu'une seule machine virtuelle en particulier est affectée, consultez l'article Installing and upgrading VMware Tools in vSphere (2004754) (Installation et mise à niveau de VMware Tools dans vSphere).

3 Vérifiez que l'agent léger est chargé en exécutant la commande Powershell `fltmc`.

Une fois que cette commande est exécutée, vous devez voir le nom vsepflt dans la liste des pilotes. Si le pilote n'est pas chargé, vous devriez être en mesure de charger le pilote avec la commande `fltmc load vsepflt`.

4 Si l'agent léger pose un problème de performances avec le système, déchargez le pilote avec cette commande : `fltmc unload vsepflt`.

   Puis effectuez un test pour obtenir une ligne de base. Vous pouvez ensuite charger le pilote et effectuer un autre test en exécutant cette commande :

   `fltmc load vsepflt`.

   Si vous constatez qu'il existe un problème de performances avec l'agent léger, consultez l'article Slow VMs after upgrading VMware Tools in NSX and vCloud Networking and Security (2144236) (Lenteur des VM après la mise à niveau de VMware Tools dans NSX et vCloud Networking and Security).

5 Si vous n'utilisez pas l'introspection réseau, supprimez ou désactivez ce pilote.

   L'introspection réseau peut également être supprimée par le biais du programme d'installation Modifier VMware Tools :

   a Montez le programme d'installation de VMware Tools.

   b Accédez à **Panneau de configuration > Programmes et fonctionnalités (Control Panel > Programs and Features)**.

   c Cliquez avec le bouton droit sur **VMware Tools > Modifier (VMware Tools > Modify)**.

   d Sélectionnez **Installation complète (Complete install)**.

   e Recherchez l'introspection de fichier NSX. Il doit y avoir un sous-dossier juste pour l'introspection réseau.

   f Désactivez **Introspection réseau (Network Introspection)**.

   g Redémarrez la VM pour terminer la désinstallation du pilote.

6 Activez la journalisation de débogage pour l'agent léger. Pour plus d'informations, consultez Journaux de Guest Introspection. Toutes les informations de débogage sont configurées pour s'enregistrer dans le fichier vmware.log pour cette machine virtuelle.

7 Consultez les analyses de fichier de l'agent léger en consultant les journaux procmon. Pour plus d'informations, consultez l'article Troubleshooting vShield Endpoint performance issues with anti-virus software (2094239) (Dépannage des problèmes de performances de vShield Endpoint avec un logiciel antivirus).

Collecter les détails de l'environnement et de la charge de travail

1 Déterminez si NSX Guest Introspection est utilisé dans l'environnement du client. Si ce n'est pas le cas, supprimez le service Guest Introspection pour la machine virtuelle et vérifiez que le problème est résolu. Résolvez un problème de Guest Introspection uniquement si Guest Introspection est requis.

2 Collectez les détails de l'environnement :

   a Version du build ESXi : exécutez la commande `uname -a` sur l'hôte ESXi ou cliquez sur un hôte dans vSphere Web Client et recherchez le numéro de build en haut du volet de droite.

   b Version et numéro de build du produit Linux

   c */usr/sbin/vsep - v* indique la version de production

```
Build number
------------------
Ubuntu
dpkg -l | grep vmware-nsx-gi-file
SLES12 and RHEL7
rpm -qa | grep vmware-nsx-gi-file
```

3 Version de VMware NSX ® for vSphere ® et les éléments suivants :

   - Nom et numéro de version de la solution de partenaire
   - Numéro de version de bibliothèque EPSec utilisé par la solution de partenaire : connectez-vous à la SVM et exécutez le chemin d'accès `#strings` à `EPSec library/libEPSec.so | grep BUILD`
   - Système d'exploitation invité dans la machine virtuelle
   - Autres applications ou pilotes de système de fichiers tiers

4 Version du module ESX GI (MUX) : exécutez la commande *esxcli software vib list | grep epsec-mux*.

5 Collectez les détails de la charge de travail, tels que le type de serveur.

6 Collectez des journaux de l'hôte ESXi. Pour plus d'informations, consultez l'article Collecting diagnostic information for VMware ESX/ESXi (653) (Collecte d'informations de diagnostic pour VMware ESX/ESXi).

7 Collectez des journaux de machine virtuelle de service (SVM) à partir de la solution de partenaire. Contactez votre partenaire pour en savoir plus sur la collecte de journaux de SVM.

8 Collectez un fichier d'état interrompu lorsque le problème se produit. Consultez l'article Suspending a virtual machine on ESX/ESXi to collect diagnostic information (2005831) (Interruption d'une machine virtuelle sur ESX/ESXi pour collecter des informations de diagnostic).

Dépannage du blocage de l'agent léger

Si l'agent léger se bloque, le fichier de base est généré dans `/directory`. Collectez le fichier de vidage de mémoire (de base) à partir de `location / directory`. Utilisez la commande `file` pour vérifier si le fichier de base est généré par vsep. Par exemple :

```
# file core
core: ELF 64-bit LSB  core file x86-64, version 1 (SYSV), SVR4-style, from '/usr/sbin/vsep'
```

La machine virtuelle se bloque ou se fige

Collectez le fichier vmss VMware de la machine virtuelle dans un état interrompu, consultez l'article Suspending a virtual machine on ESX/ESXi to collect diagnostic information (2005831) (Interruption d'une machine virtuelle sur ESX/ESXi pour collecter des informations de diagnostic) ou bloquez la machine virtuelle et collectez le fichier de vidage de mémoire complet. VMware offre un utilitaire pour convertir un fichier vmss ESXi en fichier de vidage de mémoire. Pour plus d'informations, consultez le site Vmss2core fling.

Dépannage du module ESX GI (MUX)

Module ESX GI (MUX)

Si toutes les machines virtuelles sur un hôte ESXi ne fonctionnent pas avec Guest Introspection, ou s'il existe des alarmes sur un hôte particulier concernant la communication avec le SVA GI, il peut y avoir un problème avec le module ESX GI sur l'hôte ESXi.

1 Vérifiez si le service est en cours d'exécution sur l'hôte ESXi en exécutant la commande *# /etc/init.d/vShield-Endpoint-Mux status* :

   Par exemple :

   ```
   # /etc/init.d/vShield-Endpoint-Mux status
            vShield-Endpoint-Mux is running
   ```

2 Si vous voyez que le service n'est pas en cours d'exécution, redémarrez-le ou démarrez-le avec cette commande :

   `/etc/init.d/vShield-Endpoint-Mux start`

   ou

   `/etc/init.d/vShield-Endpoint-Mux restart`

   Notez qu'il n'est pas risqué de redémarrer ce service pendant les heures de production, car il ne présente pas un impact important, et il redémarre en quelques secondes.

3 Pour vous faire une meilleure idée de ce que fait le module ESX GI ou pour vérifier l'état de communication, vous pouvez consulter les journaux sur l'hôte ESXi. Les journaux du module ESX GI sont écrits dans le fichier `syslog` de l'hôte. Ils sont également inclus dans les journaux de support de l'hôte ESXi.

   Pour plus d'informations, consultez l'article Collecting diagnostic information for ESX/ESXi hosts and vCenter Server using the vSphere Web Client (2032892) (Collecte des informations de diagnostic des hôtes ESX/ESXi et vCenter Server à l'aide de vSphere Web Client).

4 L'option de journalisation par défaut du module ESX GI est info et elle peut être déclenchée pour débogage afin de recueillir plus d'informations :

   Pour plus d'informations, consultez Journaux de Guest Introspection.

5 Le fait de réinstaller le module ESX GI peut également résoudre de nombreux problèmes, en particulier si la mauvaise version est installée ou si l'hôte ESXi a été introduit dans l'environnement dans lequel le point de terminaison était précédemment installé. Le module doit être supprimé et réinstallé.

   Pour supprimer le VIB, exécutez cette commande : *esxcli software vib remove -n epsec-mux*

6 Si vous rencontrez des problèmes avec l'installation du VIB, consultez le fichier /var/log/esxupdate.log sur l'hôte ESXi. Ce journal contient des informations très claires sur la raison pour laquelle le pilote n'a pas été installé correctement. Il s'agit d'un problème courant lors de l'installation du module ESX GI. Pour plus d'informations, consultez l'article Installing NSX Guest Introspection services (ESX GI Module VIB) on the ESXi host fails in VMware NSX for vSphere 6.x (2135278) (L'installation des services NSX Guest Introspection (VIB du module ESX GI) sur l'hôte ESXi échoue dans VMware NSX for vSphere 6.x).

7 Pour rechercher une image ESXi endommagée, recherchez un message semblable à celui-ci :

```
esxupdate: esxupdate: ERROR: Installation Error:
 (None, 'No image profile is found on the host or image profile is empty.
 An image profile is required to install or remove VIBs. To install an image profile,
 use the esxcli image profile install command.')
```

8 Pour confirmer que l'image est endommagée, exécutez la commande *cd /vmfs/volumes* sur l'hôte ESXi.

   a Recherchez le fichier imgdb.tgz en exécutant cette commande : *find * | grep imgdb.tgz*.

      En général, cette commande provoque deux correspondances. Par exemple :

      0ca01e7f-cc1ea1af-bda0-1fe646c5ceea/imgdb.tgz ou *edbf587b-da2add08-3185-3113649d5262/imgdb.tgz*

   b Sur chaque correspondance, exécutez cette commande : *ls-l match_result*

      Par exemple :

```
> ls -l 0ca01e7f-cc1ea1af-bda0-1fe646c5ceea/imgdb.tgz -rwx------
 1 root root  26393 Jul 20 19:28 0ca01e7f-cc1ea1af-bda0-1fe646c5ceea/imgdb.tgz
   > ls -l edbf587b-da2add08-3185-3113649d5262/imgdb.tgz -rwx------
  1 root root   93 Jul 19 17:32 edbf587b-da2add08-3185-3113649d5262/imgdb.tgz
```

      La taille par défaut du fichier imgdb.tgz est bien supérieure à celle de l'autre fichier ou si l'un des fichiers n'est que de quelques octets, elle indique que le fichier est endommagé. Le seul moyen pris en charge pour résoudre ce problème consiste à réinstaller ESXi pour cet hôte ESXi en particulier.

Dépannage d'EPSecLib

NSX Manager gère le déploiement de cette machine virtuelle.

EPSecLib

Dans le passé (avec vShield), la solution SVA tierce gérait le déploiement. Désormais, cette solution se connecte à NSX Manager. NSX Manager gère le déploiement de ce SVA. S'il existe des alarmes sur les SVA dans l'environnement, redéployez-les via NSX Manager.

- Toute configuration est perdue, car elle est stockée complètement dans NSX Manager.
- Il est préférable de redéployer les machines virtuelles SVA, au lieu de les redémarrer.
- NSX s'appuie sur EAM pour déployer et surveiller les VIB et les SVM sur l'hôte, tels que le SVA.
- EAM est la source de vérité pour déterminer le statut d'installation.
- Le statut d'installation de l'interface utilisateur de NSX peut uniquement indiquer si les VIB sont installés, ou si la SVM est sous tension.
- Le statut du service dans l'interface utilisateur de NSX indique si la fonctionnalité dans la machine virtuelle fonctionne.

Déploiement de SVA et relation entre NSX et le processus de vCenter Server

1. Lorsque le cluster est sélectionné pour être préparé pour le point de terminaison, une agence est créée sur EAM pour déployer le SVA.
2. EAM déploie ensuite le fichier ovf sur l'hôte ESXi avec les informations de l'agence qu'il a créées.
3. NSX Manager vérifie si ovf a été déployé par EAM.
4. NSX Manager vérifie si la machine virtuelle a été mise sous tension par EAM.
5. NSX Manager communique au gestionnaire de solutions SVA de partenaire que la machine virtuelle a été mise sous tension et enregistrée.
6. EAM envoie un événement à NSX pour indiquer que l'installation est terminée.
7. Le gestionnaire de solutions SVA de partenaire envoie un événement à NSX pour indiquer que le service dans la machine virtuelle SVA est actif et en cours d'exécution.
8. Si vous rencontrez un problème avec le SVA, vous pouvez consulter les journaux qui se trouvent dans deux emplacements. Vous pouvez consulter les journaux EAM, car EAM gère le déploiement de ces machines virtuelles. Pour plus d'informations, consultez l'article Collecting diagnostic information for VMware vCenter Server 4.x, 5.x and 6.0 (1011641) (Collecte d'informations de diagnostic pour VMware vCenter Server 4.x, 5.x et 6.0). Vous pouvez également consulter les journaux SVA.

   Pour plus d'informations, consultez Journaux de Guest Introspection.
9. S'il existe un problème avec le déploiement de SVA, il est probable qu'EAM et la communication avec NSX Manager présentent un problème. Vous pouvez consulter les journaux EAM, et la chose la plus simple consiste à redémarrer le service EAM. Pour plus d'informations, consultez Préparation de l'hôte.
10. Si toutes les mesures ci-dessus semblent fonctionner, mais que vous voulez tester la fonctionnalité du point de terminaison, vous pouvez tester cela avec un fichier Eicar Test :
    - Créez un fichier texte avec n'importe quelle étiquette. Par exemple : eicar.test.

- Le fichier ne doit contenir que la chaîne suivante :

  ```
  X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
  ```

- Enregistrez le fichier. Lors de l'enregistrement, vous devez constater que le fichier est supprimé. Cela prouve que la solution de point de terminaison fonctionne.