

Guide de dépannage de NSX-T Data Center

Modifié le 19 septembre 2018

VMware NSX-T Data Center 2.3



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

Copyright © 2017, 2018 VMware, Inc. Tous droits réservés. [Informations relatives aux copyrights et marques commerciales.](#)

Table des matières

Guide de dépannage de NSX-T Data Center 5

1 Journaux et services 6

- Messages de journal 6
 - Configurer la journalisation à distance 7
 - ID de messages de journal 9
- Résolution des problèmes de Syslog 10
- Vérification des services 11
- Collecte des bundles de support 13

2 Dépannage de problèmes de connectivité de couche 2 15

- Vérifier l'état des clusters NSX Manager et NSX Controller 15
- Vérifier les ports logiques 16
- Consulter l'état des nœuds de transport 17
- Vérifier l'état du commutateur logique 17
- Vérifier le CCP pour le commutateur logique 18
- Vérifier l'état du plan de contrôle local 18
- Dépannage de problèmes de session de configuration 19
- Dépannage de problèmes de session L2 20
- Dépannage de problèmes de plan de données pour un commutateur logique de superposition 21
- Dépannage de problèmes de plan de données pour un commutateur logique VLAN 23
- Dépannage de problèmes d'ARP pour un commutateur logique de superposition 23
- Dépannage de problèmes de perte de paquets pour un commutateur logique VLAN ou lorsque l'ARP est résolue 24

3 Dépannage lors de l'installation 26

4 Dépannage lors du routage 30

5 Dépannage du pare-feu 32

- Détermination des règles de pare-feu qui s'appliquent à un hôte ESXi 32
- Détermination des règles de pare-feu qui s'appliquent à un hôte KVM 35
- Journaux de paquet de pare-feu 36

6 Autres scénarios de dépannage 38

- Échec d'ajout ou de suppression d'un nœud de transport 38
- Un nœud de transport prend environ 5 minutes pour se connecter à un autre contrôleur 39
- Machine virtuelle NSX Manager dégradée 40

| | |
|--|----|
| Expiration de l'agent NSX lors de la communication avec NSX Manager | 41 |
| Échec d'ajout d'un hôte ESXi | 42 |
| État incorrect de NSX Controller | 43 |
| Adresses IP de gestion de machines virtuelles KVM non accessibles lorsque IPFIX est activé | 43 |

Guide de dépannage de NSX-T Data Center

Le *Guide de dépannage de NSX-T Data Center* fournit des informations sur le dépannage des problèmes pouvant survenir dans un environnement NSX-T Data Center.

Public visé

Ce guide est destiné aux administrateurs système de NSX-T Data Center. Il est impératif de maîtriser la virtualisation, la mise en réseau et des opérations de centre de données.

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>.

Journaux et services

1

Les journaux peuvent être utiles dans de nombreux scénarios de dépannage. Il est également important de vérifier l'état des services.

Ce chapitre contient les rubriques suivantes :

- [Messages de journal](#)
- [Résolution des problèmes de Syslog](#)
- [Vérification des services](#)
- [Collecte des bundles de support](#)

Messages de journal

Messages de journal de tous les composants de NSX-T Data Center, y compris ceux qui s'exécutent sur les hôtes ESXi, conformes au format syslog, comme spécifié dans RFC 5424. Les messages de journal des hôtes KVM sont au format RFC 3164. Les fichiers journaux se trouvent dans le répertoire `/var/log`.

Sur les dispositifs NSX-T Data Center, vous pouvez exécuter la commande CLI NSX-T Data Center suivante pour afficher les journaux :

```
get log-file <auth.log | http.log | kern.log | manager.log | node-mgmt.log | syslog> [follow]
```

Sur les hyperviseurs, vous pouvez utiliser des commandes Linux telles que `tail`, `grep` et `more` pour afficher les journaux. Vous pouvez également utiliser ces commandes sur des dispositifs NSX-T Data Center.

Pour plus d'informations sur la norme RFC 5424, reportez-vous à <https://tools.ietf.org/html/rfc5424>. Pour plus d'informations sur la norme RFC 3164, reportez-vous à <https://tools.ietf.org/html/rfc3164>.

La norme RFC 5424 définit le format suivant pour les messages de journal :

```
<facility * 8 + severity> version UTC-TZ hostname APP-NAME procid MSGID [structured-data] msg
```

Exemple de message de journal :

```
<187>1 2016-03-15T22:53:00.114Z nsx-manager NSX - SYSTEM [nsx@6876 comp="nsx-manager"
errorCode="MP4039" subcomp="manager"] Connection verification failed for broker '10.160.108.196'.
Marking broker unhealthy.
```

Chaque message comporte des informations sur le composant (comp) et le sous-composant (subcomp) pour faciliter l'identification de la source du message.

NSX-T Data Center produit des journaux normaux (installation local6, avec la valeur numérique 22) et des journaux d'audit (installation local7, avec la valeur numérique 23). Tous les appels API déclenchent un journal d'audit.

Un journal d'audit qui est associé à un appel d'API comporte les informations suivantes :

- Un paramètre d'identifiant d'entité entId pour identifier l'objet de l'API.
- Un paramètre d'identifiant de demande req-id pour identifier un appel d'API spécifique.
- Un paramètre d'identifiant de demande externe ereqId si l'appel d'API contient l'en-tête X-NSX-EREQID:<string>.
- Un paramètre d'utilisateur externe euser si l'appel d'API contient l'en-tête X-NSX-EUSER:<string>.

La norme RFC 5424 définit les niveaux de gravité suivants :

| Niveau de gravité | Description |
|-------------------|---|
| 0 | Urgence : le système est inutilisable |
| 1 | Alerte : une mesure doit être prise immédiatement |
| 2 | Critique : conditions critiques |
| 3 | Erreur : conditions d'erreur |
| 4 | Avertissement : conditions d'avertissement |
| 5 | Avis : condition normale mais significative |
| 6 | Informatif : messages informatifs |
| 7 | Débogage : messages de niveau de débogage |

Tous les journaux avec la gravité urgence, alerte, critique ou erreur contiennent un code d'erreur unique dans la partie de données structurée du message de journal. Le code d'erreur se compose d'une chaîne et d'un nombre décimal. La chaîne représente un module spécifique.

Le champ MSGID identifie le type de message. Pour obtenir une liste des ID de messages, consultez [ID de messages de journal](#).

Configurer la journalisation à distance

Vous pouvez configurer des dispositifs NSX-T Data Center et des hyperviseurs pour envoyer des messages de journal à un serveur de journalisation distant.

La journalisation à distance est prise en charge sur NSX Manager, NSX Controller, NSX Edge et les hyperviseurs. Vous devez configurer la journalisation à distance sur chaque nœud individuellement.

Sur un hôte KVM, le module d'installation de NSX-T Data Center configure automatiquement le démon rsyslog en plaçant les fichiers de configuration dans le répertoire /etc/rsyslog.d.

Conditions préalables

- Configurez un serveur de journalisation pour recevoir les journaux.

Procédure

1 Pour configurer la journalisation à distance sur un dispositif NSX-T Data Center :

- a Exécutez la commande suivante pour configurer un serveur de journalisation et les types de messages à envoyer au serveur de journalisation. Plusieurs installations ou ID de message peuvent être spécifiés sous forme d'une liste séparée par des virgules, sans espace.

```
set logging-server <hostname-or-ip-address[:port]> proto <proto> level <level> [facility <facility>] [messageid <messageid>] [certificate <filename>] [structured-data <structured-data>]
```

Pour plus d'informations sur cette commande, reportez-vous à la *Référence CLI de NSX-T*. Vous pouvez exécuter la commande plusieurs fois pour ajouter plusieurs configurations de serveur de journalisation. Par exemple :

```
nsx> set logging-server 192.168.110.60 proto udp level info facility syslog messageid SYSTEM,FABRIC
nsx> set logging-server 192.168.110.60 proto udp level info facility auth,user
```

- b vous pouvez afficher la configuration de la journalisation à l'aide de la commande `get logging-server`. Par exemple,

```
nsx> get logging-servers
192.168.110.60 proto udp level info facility syslog messageid SYSTEM,FABRIC
192.168.110.60 proto udp level info facility auth,user
```

2 Pour configurer la journalisation à distance sur un hôte ESXi :

- a Exécutez les commandes suivantes pour configurer syslog et envoyer un message de test :

```
esxcli network firewall ruleset set -r syslog -e true
esxcli system syslog config set --loghost=udp://<log server IP>:<port>
esxcli system syslog reload
esxcli system syslog mark -s "This is a test message"
```

- b Vous pouvez exécuter la commande suivante pour afficher la configuration :

```
esxcli system syslog config get
```


3 Pour configurer la journalisation à distance sur un hôte KVM :

- a Modifiez le fichier `/etc/rsyslog.d/10-vmware-remote-logging.conf` pour votre environnement.
- b Ajoutez la ligne suivante au fichier :

```
*.* @<ip>:514;RFC5424fmt
```

- c Exécutez la commande suivante :

```
service rsyslog restart
```

ID de messages de journal

Dans un message de journal, le champ ID de message identifie le type de message. Vous pouvez utiliser le paramètre `messageid` dans la commande `set logging-server` pour filtrer les messages de journal envoyés à un serveur de journalisation.

Tableau 1-1. ID de messages de journal

| ID de message | Exemples |
|-----------------|---|
| FABRIC | Nœud hôte Préparation de l'hôte Nœud Edge Zone de transport Nœud de transport Profils de liaison montante Profils de cluster Cluster Edge Clusters et points de terminaison de pont |
| SWITCHING | Commutateur logique Ports de commutateur logique Profils de commutation Fonctionnalités de sécurité de commutateur |
| ROUTING | Routeur logique Ports de routeur logique Routage statique Routage dynamique NAT |
| FIREWALL | Règles de pare-feu Sections de règles de pare-feu |
| FIREWALL-PKTLOG | Journaux de connexion de pare-feu Journaux de paquet de pare-feu |

Tableau 1-1. ID de messages de journal (suite)

| ID de message | Exemples |
|---------------|---|
| GROUPING | Ensembles d'adresses IP Ensembles MAC NSGroups NSServices Groupes NSService Pool VNI Pool IP |
| DHCP | relais DHCP |
| SYSTEM | Gestion des dispositifs (Syslog distant, NTP, etc.) Gestion des clusters Gestion de l'approbation Attribution de licences Utilisateur et rôles Gestion des tâches Installation (NSX Manager, NSX Controller) Mise à niveau (NSX Manager, NSX Controller, NSX Edge et mises à niveau des packages d'hôte) Réalisation Balises |
| MONITORING | SNMP Connexion au port Traceflow |
| - | Tous les autres messages de journal. |

Résolution des problèmes de Syslog

Si le serveur de journaux distant ne reçoit pas les journaux, procédez comme suit.

- Vérifiez l'adresse IP du serveur de journaux distant.
- Vérifiez que le paramètre `level` est correctement configuré.
- Vérifiez que le paramètre `facility` est correctement configuré.
- Si le protocole est TLS, définissez le protocole sur UDP pour vérifier qu'il n'existe pas une incompatibilité avec le certificat.
- Si le protocole est TLS, vérifiez que le port 6514 est ouvert sur les deux extrémités.
- Supprimez le filtre d'ID du message et vérifiez que le serveur reçoit bien les journaux.
- Redémarrez le service `rsyslog` avec la commande `restart service rsyslogd`.

Un exemple de rsyslog fichier de configuration (/etc/rsyslog.conf) :

```
### rsyslog config file. Customized by VMware.
### Do not edit this file by hand. Use the API to make changes.
$PreserveFQDN on
$ModLoad imklog
$ModLoad immark
module(load="imuxsock" sysSock.useSpecialParser="off")
$RepeatedMsgReduction on
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$ActionFileDefaultTemplate RSYSLG_SyslogProtocol23Format
$IncludeConfig /etc/rsyslog.d/*.conf
$template RFC5424fmt,"<%PRI%>1 %TIMESTAMP:::date-rfc3339% %HOSTNAME% %APP-NAME% %PROCID% %MSGID%
%STRUCTURED-DATA% %msg%\n"
$WorkDirectory /var/spool/rsyslog
$ModLoad imudp
$UDPServerAddress 127.0.0.1
$UDPServerRun 514
$PrivDropToUser syslog
$ActionQueueType LinkedList # nsx exporter: e7347687-8be7-4519-a8e1-73c5192c9b43
*.info @1.2.3.4:514;RFC5424fmt # nsx exporter: e7347687-8be7-4519-a8e1-73c5192c9b43
```

Vérification des services

Les services qui interrompent leur exécution ou qui ne démarrent pas peuvent causer des problèmes. Il est important de s'assurer que tous les services fonctionnent normalement.

Pour vérifier l'état du service NSX Manager :

```
nsxmgr> get services
Service name:      cm-inventory
Service state:     stopped

Service name:      http
Service state:     stopped
Session timeout:   1800
Connection timeout: 30
Redirect host:     (not configured)

Service name:      install-upgrade
Service state:     stopped
Enabled:           True

Service name:      liagent
Service state:     stopped

Service name:      manager
Service state:     stopped
Logging level:     info
```

```

Service name:      mgmt-plane-bus
Service state:     running

Service name:      node-mgmt
Service state:     running

Service name:      nsx-message-bus
Service state:     running

Service name:      nsx-upgrade-agent
Service state:     running

Service name:      ntp
Service state:     running

Service name:      search
Service state:     stopped

Service name:      snmp
Service state:     stopped

Start on boot:     False
Service name:      ssh

Service state:     running
Start on boot:     True

Service name:      syslog
Service state:     running

```

Dans l'exemple ci-dessus, le service http est arrêté. Vous pouvez démarrer le service http à l'aide de la commande suivante :

```
nsxmgr> start service http
```

Service SSH

Si le service SSH n'était pas activé lors du déploiement du dispositif, vous pouvez vous connecter au dispositif en tant qu'administrateur et l'activer avec la commande suivante :

```
start service ssh
```

Vous pouvez configurer le service SSH de manière à ce qu'il démarre lorsque l'hôte démarre lui-même avec la commande suivante :

```
set service ssh start-on-boot
```

Pour activer la connexion racine SSH, vous pouvez vous connecter au dispositif en tant que racine, modifier le fichier `/etc/ssh/sshd_config` et remplacer la ligne

```
PermitRootLogin prohibit-password
```

Vous pouvez également activer le service SSH et activer l'accès SSH racine en mettant le dispositif hors tension et en modifiant ses propriétés vApp

par

```
PermitRootLogin yes
```

avant de redémarrer le serveur sshd avec la commande suivante :

```
/etc/init.d/ssh restart
```

Collecte des bundles de support

Vous pouvez collecter des bundles de support sur des nœuds de cluster et d'infrastructure enregistrés et télécharger les bundles sur votre machine ou sur un serveur de fichiers.

Si vous choisissez de télécharger les bundles sur votre machine, vous obtenez un fichier d'archive composé d'un fichier manifeste et de bundles de support pour chaque nœud. Si vous choisissez de télécharger les bundles sur un serveur de fichiers, le fichier manifeste et les bundles individuels sont téléchargés sur le serveur de fichiers séparément.

Remarque concernant NSX Cloud Si vous souhaitez collecter le bundle de support pour CSM, connectez-vous à CSM, accédez à **Système > Utilitaires > Bundle de support**, puis cliquez sur **Télécharger**. Le bundle de support pour PCG est disponible à partir de NSX Manager en suivant les instructions suivantes. Le bundle de support pour PCG contient également des journaux de toutes les machines virtuelles de charge de travail.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à NSX Manager sur *https://nsx-manager-ip-address*.
- 2 Sélectionnez **Système > Utilitaires** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **Bundle de support**.
- 4 Sélectionnez les nœuds cibles.

Les types de nœuds disponibles sont les nœuds de gestion, les nœuds de contrôleur, les dispositifs Edge, les hôtes et les passerelles PCG.

- 5 (Facultatif) Spécifiez l'âge de journal en jours pour exclure les journaux antérieurs au nombre de jours spécifié.
- 6 (Facultatif) Basculez le commutateur qui indique s'il faut inclure ou exclure les fichiers noyaux et les journaux d'audit.

Note Les fichiers noyaux et les journaux d'audit peuvent contenir des informations sensibles, telles que des mots de passe ou des clés de chiffrement.

- 7 (Facultatif) Cochez une case pour télécharger les bundles sur un serveur de fichiers.

- 8 Cliquez sur **Démarrer la collecte des bundles** pour démarrer la collecte des bundles de support.
En fonction du nombre de fichiers journaux existants, chaque nœud peut prendre plusieurs minutes.
- 9 Surveillez l'état du processus de collecte.
Le champ d'état indique le pourcentage de nœuds ayant terminé la collecte des bundles de support.
- 10 Cliquez sur **Télécharger** pour télécharger le bundle si l'option pour envoyer le bundle à un serveur de fichiers n'a pas été définie.

Dépannage de problèmes de connectivité de couche 2

2

S'il y a un problème de communication entre deux interfaces virtuelles (VIF) qui sont connectées au même commutateur logique, par exemple, vous ne pouvez pas effectuer un test ping d'une machine virtuelle vers une autre, vous pouvez suivre les étapes de cette section pour résoudre ce problème.

Avant de commencer, assurez-vous qu'aucune règle de pare-feu ne bloque le trafic entre les deux ports logiques. Il est recommandé de suivre l'ordre des rubriques de cette section pour résoudre les problèmes de connectivité.

Ce chapitre contient les rubriques suivantes :

- [Vérifier l'état des clusters NSX Manager et NSX Controller](#)
- [Vérifier les ports logiques](#)
- [Consulter l'état des nœuds de transport](#)
- [Vérifier l'état du commutateur logique](#)
- [Vérifier le CCP pour le commutateur logique](#)
- [Vérifier l'état du plan de contrôle local](#)
- [Dépannage de problèmes de session de configuration](#)
- [Dépannage de problèmes de session L2](#)
- [Dépannage de problèmes de plan de données pour un commutateur logique de superposition](#)
- [Dépannage de problèmes de plan de données pour un commutateur logique VLAN](#)
- [Dépannage de problèmes d'ARP pour un commutateur logique de superposition](#)
- [Dépannage de problèmes de perte de paquets pour un commutateur logique VLAN ou lorsque l'ARP est résolue](#)

Vérifier l'état des clusters NSX Manager et NSX Controller

Vérifiez que l'état des clusters NSX Manager et NSX Controller est normal et que les contrôleurs sont connectés à NSX Manager.

Procédure

- 1 Exécutez la commande d'interface de ligne de commande suivante sur un NSX Manager pour vous assurer que l'état est stable.

```
NSX-Manager> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.47 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.201 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086)
- 192.168.110.202 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086)
- 192.168.110.203 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086)
```

- 2 Exécutez la commande d'interface de ligne de commande suivante sur un NSX Controller pour vous assurer que l'état est actif.

```
NSX-Controller1> get control-cluster status
uuid: db4aa77a-4397-4d65-ad33-9fde79ac3c5c
is master: true
in majority: true

  uuid                                address                status
  ---                                -
0cfe232e-6c28-4fea-8aa4-b3518baef00d 192.168.110.201        active
bd257108-b94e-4e6d-8b19-7fa6c012961d 192.168.110.202        active
538be554-1240-40e4-8e94-1497e963a2aa 192.168.110.203        active
```

- 3 Exécutez la commande de ligne de commande suivante sur un NSX Controller pour vous assurer qu'il est connecté à NSX Manager.

```
NSX-Controller1> get managers
- 192.168.110.47 Connected
```

Vérifier les ports logiques

Vérifiez que les ports logiques sont configurés sur le même commutateur logique et que leur état est actif.

Procédure

- 1 Dans l'interface utilisateur graphique de NSX Manager, obtenez les UUID des ports logiques.
- 2 Effectuez l'appel d'API suivant pour chaque port logique afin de vous assurer que les ports logiques sont sur le même commutateur logique.

```
GET https://<nsx-mgr>/api/v1/logical-ports/<logical-port-uuid>
```

- 3 Effectuez l'appel d'API suivant pour chaque port logique afin de vous assurer que son état est actif.

```
GET https://<nsx-mgr>/api/v1/logical-ports/<logical-port-uuid>/status
```


Consulter l'état des nœuds de transport

Consultez l'état du nœud de transport.

Procédure

- ◆ Effectuez l'appel d'API suivant pour obtenir l'état du nœud de transport.

```
GET https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-ID>/state
```

Si l'appel renvoie l'erreur de délai d'expiration du RPC, effectuez les étapes de dépannage suivantes :

- Exécutez `/etc/init.d/nsx-opsAgent status` pour voir si `opsAgent` est en cours d'exécution.
- Exécutez `/etc/init.d/nsx-mpa status` pour voir si `nsx-mpa` est en cours d'exécution.
- Pour voir si `nsx-mpa` est connecté à NSX Manager, consultez les journaux du signal de pulsation de `nsx-mpa`.
- Pour voir si `opsAgent` est connecté à NSX Manager, vérifiez le journal de `nsx-opsAgent`. Le message suivant s'affiche si `opsAgent` est connecté à NSX Manager.

```
Connected to mpa, cookie: ...
```

- Pour voir si `opsAgent` se bloque lors du traitement de `HostConfigMsg`, vérifiez le journal de `nsx-opsAgent`. Si c'est le cas, vous verrez un message de demande RMQ, mais la réponse n'est pas envoyée ou a été envoyée après un délai important.
- Vérifiez que `opsAgent` ne s'est pas bloqué lors de l'exécution de `HostConfigMsg`.
- Pour voir si la transmission des messages RMQ à l'hôte prend un long moment, comparez les horodatages des messages du journal sur NSX Manager et sur l'hôte.

Si l'appel renvoie l'erreur `partial_success`, il existe plusieurs causes possibles. Commencez par consulter les journaux de `nsx-opsAgent`. Sur l'hôte ESXi, consultez les fichiers `hostd.log` et `vmkernel.log`. Sur KVM, le `syslog` contient tous les journaux.

Vérifier l'état du commutateur logique

Vérifiez l'état du commutateur logique.

Procédure

- ◆ Effectuez l'appel d'API suivant pour obtenir l'état du commutateur logique.

```
GET https://<nsx-mgr>/api/v1/logical-switches/<logical-switch-ID>/state
```

Si l'appel renvoie l'erreur `partial_success`, la réponse contient une liste de nœuds de transport pour lesquels NSX Manager n'a pas pu transférer la configuration du commutateur logique ou n'a pas obtenu de réponse. Les étapes de dépannage sont semblables à celles pour le nœud de transport. Vérifiez les éléments suivants :

- Tous les composants requis sont installés et en cours d'exécution.
- `nsx-mpa` est connecté à NSX Manager.
- `nsxa` est connecté à la verticale de commutation.
- Exécutez la commande `grep` pour rechercher l'ID du commutateur logique dans `nsxa.log` et `nsxaVim.log` pour voir si la configuration du commutateur logique a été reçue par le nœud de transport.
- Vérifiez le temps d'activité de `nsxa` et `nsx-mpa`. Recherchez l'heure de démarrage et d'arrêt de `nsxa` en exécutant la commande `grep` pour les messages de journal `nsxa` dans le fichier `syslog`.
- Découvrez l'heure de connexion de `nsxa` à la verticale de commutation. Si la configuration du commutateur logique est envoyée à l'hôte alors que `nsxa` n'est pas connecté à la verticale de commutation, la configuration peut ne pas être transmise à l'hôte.

Sur KVM, aucune configuration du commutateur logique n'est transférée à l'hôte. Par conséquent, la plupart des problèmes de commutateur logique sont susceptibles de se trouver dans le plan de gestion.

Sur ESXi, un réseau opaque est mappé au commutateur logique. Pour utiliser le commutateur logique, les utilisateurs doivent connecter les machines virtuelles au réseau opaque à l'aide de vCenter Server ou de vSphere API.

Vérifier le CCP pour le commutateur logique

Vérifiez que le commutateur logique est dans le plan de contrôle central (CCP).

Procédure

- ◆ Exécutez la commande d'interface de ligne de commande suivante sur un NSX Controller pour vous assurer que le commutateur logique est présent.

```
NSX-Controller1> get logical switches
VNI    UUID                                Name
52104  feab22ec-94b2-46f4-88f8-f9d44a416272  ls1
```

Note Cette commande d'interface de ligne de commande ne répertorie pas les commutateurs logiques reposant sur VLAN.

Vérifier l'état du plan de contrôle local

Pour un commutateur logique de superposition, vérifiez que le `netcpa` présent sur l'hôte est connecté au plan de contrôle central.

Conditions préalables

Recherchez le contrôleur sur lequel se trouve le commutateur logique. Reportez-vous à la section [Vérifier le CCP pour le commutateur logique](#).

Procédure

- 1 Utilisez SSH avec le contrôleur se trouvant sur le commutateur logique.
- 2 Exécutez la commande suivante et vérifiez que le contrôleur affiche les hyperviseurs qui sont connectés à ce VNI.

```
get logical-switch 5000 connection-table
```

- 3 Sur les hyperviseurs, exécutez la commande `/bin/nsxcli` pour démarrer l'interface de ligne de commande de NSX.
- 4 Exécutez la commande suivante pour obtenir les sessions CCP.

```
host1> get ccp-session
Session Index State Controller
Config 0      UP    10.33.74.163
L2      5000   UP    10.33.74.163
```

Vous devez voir une session de configuration sur l'un des nœuds CCP du cluster CCP. Pour chaque commutateur logique de superposition, vous devez voir une session L2 vers un des nœuds CCP du cluster CCP. Pour les commutateurs logiques VLAN, il n'existe pas de connexion CCP.

Dépannage de problèmes de session de configuration

Si la session de configuration CCP n'est pas activée, vérifiez l'état de l'agent MPA et de netcpa.

Procédure

- 1 Effectuez l'appel d'API suivant pour voir si l'agent MPA est connecté à NSX Manager.

```
GET https://<nsx-mgr>/api/v1/logical-ports/<logical-port-uuid>
```

- 2 Sur l'hyperviseur, exécutez la commande `/bin/nsxcli` pour démarrer l'interface de ligne de commande de NSX.
- 3 Exécutez la commande suivante pour obtenir l'UUID de nœud.

```
host1> get node-uuid
0c123dd4-8199-11e5-95e2-73cc1cd9b614
```

- 4 Exécutez la commande suivante pour voir si NSX Manager a transféré les informations CCP à l'hôte.

```
cat /etc/vmware/nsx/config-by-vsm.xml
```

- 5 Si config-by-vsm.xml dispose d'informations CCP, vérifiez qu'un nœud de transport est configuré sur l'hyperviseur.

NSX Manager envoie le certificat d'hôte de l'hyperviseur à l'étape de création du nœud de transport. Le CCP doit posséder le certificat d'hôte avant de pouvoir accepter les connexions à partir de l'hôte.

- 6 Vérifiez la validité du certificat d'hôte dans /etc/vmware/nsx/host-cert.pem.

Le certificat doit être le même que celui que NSX Manager possède pour l'hôte.

- 7 Exécutez la commande suivante pour vérifier si l'état de netcpa.

Sur ESXi :

```
/etc/init.d/netcpad status
```

Sur KVM :

```
/etc/init.d/nsx-agent status
```

- 8 Démarrez ou redémarrez netcpa.

Sur ESXi, démarrez netcpa s'il n'est pas en cours d'exécution ou redémarrez-le s'il est en cours d'exécution.

```
/etc/init.d/netcpad start
```

```
/etc/init.d/netcpad restart
```

Sur KVM, démarrez netcpa s'il n'est pas en cours d'exécution ou redémarrez-le s'il est en cours d'exécution.

```
/etc/init.d/nsx-agent start
```

```
/etc/init.d/nsx-agent restart
```

- 9 Si la session de configuration n'est pas encore activée, collectez des bundles de support technique et contactez le support VMware.

Dépannage de problèmes de session L2

Cela s'applique uniquement aux commutateurs logiques de superposition.

Procédure

- 1 Sur l'hyperviseur, exécutez la commande /bin/nsxcli pour démarrer l'interface de ligne de commande de NSX.
- 2 Exécutez la commande suivante pour voir si le commutateur logique est présent sur l'hôte.

```
host1> get logical-switches
```

3 Vérifiez que l'état du port n'est pas Administration désactivée.

Sur ESXi, exécutez `net-dvs` et examinez la réponse. Par exemple,

```
port 63eadf53-ff92-4a0e-9496-4200e99709ff:
com.vmware.port.extraConfig.opaqueNetwork.id = ... <- this should match the logical switch UUID
com.vmware.port.opaque.network.id = ... <- this should match the logical switch UUID
com.vmware.port.opaque.network.type = nsx.LogicalSwitch , propType = RUNTIME
com.vmware.common.port.block = false, ... <- Make sure the value is false.
com.vmware.vswitch.port.vxlan = ...
com.vmware.common.port.volatile.status = inUse ... <- make sure the value is inUse.
```

Si le port logique se retrouve à l'état bloqué, collectez des bundles de support technique et contactez le support VMware. En attendant, exécutez la commande suivante pour obtenir le nom DVS :

```
[root@host1:~] net-dvs | grep nsx-switch
com.vmware.common.alias = nsx-switch , propType = CONFIG
```

Exécutez la commande suivante pour débloquent le port :

```
[root@host1:~] net-dvs -s com.vmware.common.port.block=false <DVS-NAME> -p <logical-port-ID>
```

Sur KVM, exécutez `ovs-vsctl list interface` et vérifiez que l'interface avec l'UUID de VIF correspondant est présente et que l'état `admin_state` est actif. Vous pouvez voir l'UUID de VIF dans OVSDb avec `external-ids:iface-id`.

Dépannage de problèmes de plan de données pour un commutateur logique de superposition

Les étapes décrites dans cette section abordent le dépannage des problèmes de connectivité entre des machines virtuelles situées sur différents hyperviseurs via le commutateur de superposition lorsque les états de configuration et d'exécution sont normaux.

Si les machines virtuelles se trouvent sur le même hyperviseur, accédez à [Dépannage de problèmes d'ARP pour un commutateur logique de superposition](#).

Procédure

- 1 Exécutez la commande suivante sur le contrôleur qui possède le commutateur logique pour voir si le CCP dispose de la liste VTEP correcte :

```
controller1> get logical-switch 5000 vtep
```

- 2 Sur chaque hyperviseur, exécutez la commande suivante dans l'interface de ligne de commande de NSX pour voir s'il dispose de la liste VTEP correcte :

Sur ESXi :

```
host1> get logical-switch <logical-switch-UUID> tep-table
```

Sinon, vous pouvez exécuter la commande shell suivante pour obtenir les informations VTEP :

```
[root@host1:~] net-vd12 -M vtep -s vds -n VNI
```

Sur KVM :

```
host1> get logical-switch <logical-switch-UUID or VNI> tep-table
```

- 3 Vérifiez si les VTEP présentes sur l'hyperviseur peuvent effectuer un test ping les unes sur les autres.

À l'invite du shell ESXi :

```
host1> ping ++netstack=vxlan <remote-VTEP-IP>
```

À l'invite du shell KVM :

```
host1> ping <remote-VTEP-IP>
```

Si les VTEP ne peuvent pas effectuer de test ping les unes sur les autres,

- a Assurez-vous que le VLAN de transport spécifié lors de la création du nœud de transport correspond à celui attendu par la sous-couche. Si vous utilisez des ports d'accès dans la sous-couche, le VLAN de transport doit être défini sur 0. Si vous spécifiez un VLAN de transport, les ports de commutateur sous-jacents auxquels les hyperviseurs se connectent doivent être configurés pour accepter ce VLAN en mode trunk.
 - b Vérifiez la connectivité sous-jacente.
- 4 Vérifiez que les sessions BFD entre les VTEP sont actives.

Sur ESXi, exécutez `net-vd12 -M bfd` et examinez la réponse. Par exemple,

```
BFD count: 1
=====
Local IP: 192.168.48.35, Remote IP: 192.168.197.243, Local State: up, Remote State: up, Local
Diag: No Diagnostic, Remote Diag: No Diagnostic, minRx: 1000000, isDisabled: 0
```

Sur KVM, trouvez l'interface GENEVE à l'adresse IP distante.

```
ovs-vsctl list interface <GENEVE-interface-name>
```

Si vous ne connaissez pas le nom de l'interface, exécutez `ovs-vsctl find Interface type=geneve` pour renvoyer toutes les interfaces de tunnel. Recherchez des informations BFD.

Si vous ne trouvez pas d'interface GENEVE sur le VTEP distant, vérifiez que nsx-agent est en cours d'exécution et que le pont d'intégration OVS est connecté à nsx-agent.

```
[root@host1 ~]# ovs-vsctl show
96c9e543-fc68-448a-9882-6e161c313a5b
  Manager "tcp:127.0.0.1:6632"
    is_connected: true
  Bridge nsx-managed
    Controller "tcp:127.0.0.1:6633"
```

```
is_connected: true
Controller "unix:ovs-l3d.mgmt"
is_connected: true
fail_mode: secure
```

Dépannage de problèmes de plan de données pour un commutateur logique VLAN

Les étapes décrites dans cette section abordent le dépannage des problèmes de connectivité entre des machines virtuelles situées sur différents hyperviseurs via le VLAN configuré sur la sous-couche lorsque les états de configuration et d'exécution sont normaux.

Si les machines virtuelles sont sur le même hyperviseur et que tous les états de configuration et d'exécution sont normaux, accédez à [Dépannage de problèmes d'ARP pour un commutateur logique de superposition](#).

Procédure

- ◆ Vérifiez que la sous-couche est configurée pour le VLAN pour le commutateur logique en mode trunk.

Sur ESXi, vérifiez que le VLAN est configuré sur le port logique en exécutant `net-dvs` et en recherchant le port logique. Par exemple :

```
port 63eadf53-ff92-4a0e-9496-4200e99709ff:
  com.vmware.common.port.volatile.vlan = VLAN 1000 propType = RUNTIME VOLATILE
```

Sur KVM, le commutateur logique VLAN est configuré comme une règle openflow sur un pont d'intégration. En d'autres termes, pour le trafic reçu à partir d'un VIF, marquez-le avec VLAN X et acheminez-le sur le port de correctif vers le pont PIF. Exécutez `ovs-vsctl list interface` et vérifiez la présence du port de correctif entre la passerelle gérée par NSX et le pont NSX-switch.

Dépannage de problèmes d'ARP pour un commutateur logique de superposition

Les étapes décrites dans cette section abordent le dépannage d'un commutateur de superposition lorsque des paquets sont perdus.

Pour un commutateur logique reposant sur VLAN, accédez à [Dépannage de problèmes de perte de paquets pour un commutateur logique VLAN ou lorsque l'ARP est résolue](#).

Avant d'effectuer les étapes de dépannage suivantes, exécutez la commande `arp -n` sur chaque machine virtuelle. Si l'ARP est résolue sur les deux machines virtuelles, il est inutile d'effectuer les étapes de cette section. Au lieu de cela, accédez à la section suivante [Dépannage de problèmes de perte de paquets pour un commutateur logique VLAN ou lorsque l'ARP est résolue](#).

Procédure

- ◆ Si les deux points de terminaison sont ESXi et qu'un proxy ARP est activé sur le commutateur logique (pris en charge uniquement pour les commutateurs logiques de superposition), vérifiez la table ARP sur le CCP et l'hyperviseur.

Sur le CCP :

```
controller1> get logical-switch 5000 arp-table
```

Sur l'hyperviseur, démarrez l'interface de ligne de commande de NSX et exécutez la commande suivante :

```
host1> get logical-switch <logical-switch-UUID> arp-table
```

L'extraction de la table ARP indique uniquement si l'état du proxy ARP est correct. Si la réponse ARP n'est pas reçue via le proxy ou si l'hôte est de type KVM et qu'il ne prend pas en charge le proxy ARP, le chemin de données doit diffuser la demande ARP. Il peut y avoir un problème au niveau de l'acheminement du trafic BUM. Essayez les étapes décrites ci-dessous :

- Si le mode de réplication du commutateur logique est MTEP, modifiez le mode de réplication sur SOURCE pour le commutateur logique à partir de l'interface utilisateur graphique de NSX Manager. Cela peut résoudre le problème et le test ping commencera à fonctionner.
- Ajoutez des entrées ARP statiques et vérifiez que le reste du chemin de données est fonctionnel.

Dépannage de problèmes de perte de paquets pour un commutateur logique VLAN ou lorsque l'ARP est résolue

Vous pouvez utiliser l'outil Traceflow automatisé ou suivre manuellement les paquets pour dépanner les problèmes de perte de paquets.

Pour exécuter l'outil Traceflow, dans l'interface utilisateur graphique de NSX Manager, accédez à **Outils > Traceflow**. Pour plus d'informations, consultez le *Guide d'administration de NSX-T*.

Procédure

- ◆ Pour effectuer manuellement le suivi des paquets de données,

Sur ESXi, exécutez `net-stats -l` pour obtenir l'ID du port de commutateur des VIF. Si les VIF source et de destination se trouvent sur le même hyperviseur, exécutez les commandes suivantes :

```
pktcap-uw --switchport <src-switch-port-ID> --dir=0
pktcap-uw --switchport <dst-switch-port-ID> --dir=1
```

Si les VIF source et de destination se trouvent sur des hyperviseurs différents, exécutez les commandes suivantes sur l'hyperviseur qui héberge la VIF source :

```
pktcap-uw --switchport <src-switch-port-ID> --dir=0
pktcap-uw --uplink <uplink-name> --dir=1
```


Exécutez les commandes suivantes sur l'hyperviseur qui héberge la VIF de destination :

```
pktcap-uw --uplink <uplink-name> --dir=0  
pktcap-uw --switchport <dest-switch-port-ID> --dir=1
```

Sur KVM, si les VIF source et de destination se trouvent sur le même hyperviseur, exécutez la commande suivante :

```
ovs-dpctl dump-flows
```

Dépannage lors de l'installation

3

Cette section fournit des informations sur le dépannage des problèmes d'installation.

Services d'Infrastructure de base

Les services suivants doivent s'exécuter sur les dispositifs et les hyperviseurs, également sur vCenter Server si ce dernier est utilisé comme gestionnaire de calcul.

- NTP
- DNS

Assurez-vous que le pare-feu ne bloque pas le trafic entre les composants NSX-T et les hyperviseurs. Assurez-vous que les ports requis sont ouverts entre les composants.

Pour vider le cache DNS sur NSX Manager, utilisez SSH pour vous connecter en tant qu'utilisateur racine au gestionnaire et exécutez la commande suivante :

```
root@nsx-mgr-01:~# /etc/init.d/resolvconf restart
[ ok ] Restarting resolvconf (via systemctl): resolvconf.service.
```

Vous pouvez ensuite vérifier le fichier de configuration DNS.

```
root@nsx-mgr-01:~# cat /etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 192.168.253.1
search mgt.sg.lab
```

Vérification de la communication d'un hôte à un contrôleur et à un gestionnaire

Sur un hôte ESXi à l'aide des commandes d'interface de ligne de commande NSX-T :

```
esxi-01.corp.local> get managers
- 192.168.110.19    Connected

esxi-01.corp.local> get controllers
Controller IP      Port      SSL      Status      Is Physical Master  Session State  Controller
FQDN
192.168.110.16    1235     enabled  connected                    true            up             NA
```

Sur un hôte KVM à l'aide des commandes d'interface de ligne de commande NSX-T :

```
kvm-01> get managers
- 192.168.110.19    Connected

kvm-01> get controllers
Controller IP      Port      SSL      Status      Is Physical Master  Session State  Controller
FQDN
192.168.110.16    1235     enabled  connected                    true            up             NA
```

Sur un hôte ESXi à l'aide des commandes d'interface de ligne de commande d'hôte :

```
[root@esxi-01:~] esxcli network ip connection list | grep 1235
tcp          0          0 192.168.110.53:42271          192.168.110.16:1235
ESTABLISHED  67702     newreno  netcpa
[root@esxi-01:~]
[root@esxi-01:~] esxcli network ip connection list | grep 5671
tcp          0          0 192.168.110.253:11721        192.168.110.19:5671  ESTABLISHED  2103688
newreno     mpa
tcp          0          0 192.168.110.253:30977        192.168.110.19:5671  ESTABLISHED  2103688
newreno     mpa
```

Sur un hôte KVM à l'aide des commandes d'interface de ligne de commande d'hôte :

```
root@kvm-01:/home/vmware# netstat -nap | grep 1235
tcp          0          0 192.168.110.55:53686        192.168.110.16:1235  ESTABLISHED  2554/netcpa
root@kvm-01:/home/vmware#
root@kvm-01:/home/vmware#
root@kvm-01:/home/vmware# netstat -nap | grep 5671
tcp          0          0 192.168.110.55:50108        192.168.110.19:5671  ESTABLISHED  2870/mpa
tcp          0          0 192.168.110.55:50110        192.168.110.19:5671  ESTABLISHED  2870/mpa

root@kvm-01:/home/vmware# tcpdump -i ens32 port 1235 | grep kvm-01
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens32, link-type EN10MB (Ethernet), capture size 262144 bytes
<truncated output>
03:46:27.040461 IP nsxcontroller01.corp.local.1235 > kvm-01.corp.local.38754: Flags [P.], seq
3315301231:3315301275, ack 2671171555, win 323, length 44
03:46:27.040509 IP kvm-01.corp.local.38754 > nsxcontroller01.corp.local.1235: Flags [.], ack 44, win
1002, length 0
```

```

^C
<truncated output>
root@kvm-01:/home/vmware#

root@kvm-01:/home/vmware# tcpdump -i ens32 port 5671 | grep kvm-01
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens32, link-type EN10MB (Ethernet), capture size 262144 bytes
03:51:16.802934 IP kvm-01.corp.local.58954 > nsxmgr01.corp.local.amqps: Flags [P.], seq 1153:1222,
ack 1790, win 259, length 69
03:51:16.823328 IP nsxmgr01.corp.local.amqps > kvm-01.corp.local.58954: Flags [P.], seq 1790:1891,
ack 1222, win 254, length 101
^C
<truncated output>

```

Échec d'enregistrement de l'hôte

Si NSX-T utilise l'adresse IP incorrecte, l'enregistrement de l'hôte échoue. Cela peut se produire lorsqu'un hôte possède plusieurs adresses IP. Une tentative de suppression du nœud de transport laisse ce dernier à l'état Orphelin. Pour résoudre le problème :

- Accédez à **Infrastructure > Nœuds > Hôtes**, modifiez l'hôte et supprimez toutes les adresses IP à l'exception de celle de gestion.
- Cliquez sur les erreurs et sélectionnez **Résoudre**.

Problèmes de l'hôte KVM

Les problèmes de l'hôte KVM sont parfois induits par une insuffisance d'espace disque. Le répertoire / boot peut se remplir rapidement et provoquer des erreurs comme :

- Échec de l'installation du logiciel sur l'hôte
- Aucun espace restant sur le périphérique

Vous pouvez exécuter la commande **df-h** pour vérifier l'espace de stockage disponible. Si le répertoire / boot est à 100 %, vous pouvez procéder comme suit :

- Exécutez `sudo dpkg --get-architecture | grep ^i` pour voir tous les noyaux installés.
- Exécutez `uname -r` pour voir le noyau en cours d'exécution. Ne supprimez pas ce noyau (linux-image).
- Utilisez `apt-get purge` pour supprimer les images dont vous n'avez plus besoin. Par exemple, exécutez `sudo apt-get purge linux-image-3.13.0-32-generic linux-image-3.13.0-33-generic`.
- Redémarrez l'hôte.
- Dans NSX Manager, vérifiez les erreurs et sélectionnez **Résoudre**.
- Assurez-vous que les machines virtuelles sont sous tension.

Erreur de configuration lors du déploiement d'une machine virtuelle Edge

Après le déploiement d'une machine virtuelle Edge, NSX Manager affiche l'état de la machine virtuelle sous la forme d'une **erreur de configuration**. Le journal du gestionnaire dispose d'un message similaire au suivant :

```
nsx-manager NSX - FABRIC [nsx@6876 comp="nsx-manager" errorCode="MP16027" subcomp="manager"] Edge
758ad396-0754-11e8-877e-005056abf715 is not ready for configuration error occurred, error detail is
NSX Edge configuration has failed. The host does not support required cpu features: ['aes'].
```

Redémarrer le service de chemin de données du dispositif Edge, puis la machine virtuelle doit résoudre le problème.

Forcer la suppression d'un nœud de transport

Vous pouvez supprimer un nœud de transport bloqué à l'état Orphelin en effectuant l'appel API suivant :

```
DELETE https://<NSX Manager>/api/v1/transport-nodes/<TN ID>?force=true
```

NSX Manager ne procède à aucune validation quant à l'exécution éventuelle de machines virtuelles actives sur l'hôte. Vous êtes responsable de la suppression de N-VDS et des fichiers VIB. Si vous avez ajouté le nœud via le gestionnaire de calcul, supprimez d'abord le gestionnaire de calcul, puis supprimez le nœud. Le nœud de transport est également supprimé.

Dépannage lors du routage

4

NSX-T comprend des outils de dépannage des problèmes de routage.

Traceflow

Vous pouvez utiliser Traceflow pour inspecter le flux de paquets. Vous pouvez voir les paquets livrés, abandonnés, reçus et transférés. Si un paquet est abandonné, un motif s'affiche. Par exemple, un paquet peut être abandonné en raison d'une règle de pare-feu.

Vérification des tables de routage

Pour afficher la table de routage sur un routeur de service, exécutez les commandes suivantes :

```
edge01> get logical-router
Logical Route
UUID                                VRF    LR-ID  Name                                Type
Ports
736a80e3-23f6-5a2d-81d6-bbefb2786666 0       0      SR-t0-router                        TUNNEL                                3
c9393d0c-1fcf-4c34-889d-2da1eeee25b8 1       10     SR-t0-router                        SERVICE_ROUTER_TIER0                 5
9333c94e-5938-46b4-8c7d-5e6ac2c8b7b5 2       8      DR-t1-router01                     DISTRIBUTED_ROUTER_TIER1              6
c91eb7c5-0297-4fed-9c22-b96df1c9b80f 3       9      DR-t0-router                        DISTRIBUTED_ROUTER_TIER0              4

edge01> vrf 1
edge01(tier0_sr)> get route

Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT
t1l: Tier1-LB VIP, t1s: Tier1-LB SNAT

Total number of routes: 25

b   10.10.20.0/24      [20/0]      via 192.168.140.1
b   10.10.30.0/24      [20/0]      via 192.168.140.1
b   10.20.20.0/24      [20/0]      via 192.168.140.1
b   10.20.30.0/24      [20/0]      via 192.168.140.1
b   30.0.0.0/8         [20/0]      via 192.168.140.1
rl  100.64.80.0/31      [0/0]       via 169.254.0.1
rl  100.64.80.2/31      [0/0]       via 169.254.0.1
rl  100.64.80.4/31      [0/0]       via 169.254.0.1
<TRUNCATED OUTPUT>
b   192.168.200.0/24   [20/0]      via 192.168.140.1
```

| | | | |
|---|------------------|--------|-------------------|
| b | 192.168.210.0/24 | [20/0] | via 192.168.140.1 |
| b | 192.168.220.0/24 | [20/0] | via 192.168.140.1 |
| b | 192.168.230.0/24 | [20/0] | via 192.168.140.1 |
| b | 192.168.240.0/24 | [20/0] | via 192.168.140.1 |

Pour obtenir l'adresse IP des interfaces, exécutez la commande suivante :

```
edge01(tier0_sr)> get interfaces
Logical Router
UUID                                VRF  LR-ID  Name                Type
c9393d0c-1fcf-4c34-889d-2da1eeee25b8  1    10    SR-t0-router       SERVICE_ROUTER_TIER0
interfaces
  interface    : 977ac2eb-8ab7-40e9-8abe-782a438c749a
  ifuid        : 285
  name         : uplink01
  mode         : lif
  IP/Mask      : 192.168.140.3/24
  MAC          : 00:50:56:b5:d5:64
  LS port      : 14391f86-efef-4e3d-98c3-f291c17d13f8
  urpf-mode    : STRICT_MODE
  admin        : up
  MTU          : 1600

  interface    : 6af81d72-4d32-5f66-b7ae-403e617290e5
  ifuid        : 270
  mode         : blackhole

  interface    : 015e709d-6079-5c19-9556-8be2e956f775
  ifuid        : 269
  mode         : cpu

  interface    : 3f40f838-eb8a-4f35-854c-ea8bb872dc47
  ifuid        : 272
  name         : bp-sr0-port
  mode         : lif
  IP/Mask      : 169.254.0.2/28
  MAC          : 02:50:56:56:53:00
  VNI          : 25489
  LS port      : 770a208d-27fa-4f8d-afad-a9c41ca6295b
  urpf-mode    : NONE
  admin        : up
  MTU          : 1500

  interface    : 00003300-0000-0000-0000-00000000000a
  ifuid        : 263
  mode         : loopback
  IP/Mask      : 127.0.0.1/8
```

Annonce des routes T1

Vous devez annoncer les routes T1 afin qu'elles soient visibles sur le routeur T0 et les routeurs supérieurs. Vous pouvez annoncer différents types de routes : NSX connecté, NAT, Statique, VIP d'équilibrage de charge et SNAT d'équilibrage de charge.

Dépannage du pare-feu

5

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

Ce chapitre contient les rubriques suivantes :

- [Détermination des règles de pare-feu qui s'appliquent à un hôte ESXi](#)
- [Détermination des règles de pare-feu qui s'appliquent à un hôte KVM](#)
- [Journaux de paquet de pare-feu](#)

Détermination des règles de pare-feu qui s'appliquent à un hôte ESXi

Pour résoudre les problèmes de pare-feu avec un hôte ESXi, vous pouvez consulter les règles de pare-feu qui s'appliquent à l'hôte.

Pour obtenir la liste des dvFilters sur l'hôte ESXi :

```
[root@esxi-01:~] summarize-dvfilter
<TRUNCATED OUTPUT>
world 70181 vmm0:app-01a vcUuid:'50 35 9c 70 18 8e 99 1d-3c f9 8e cc 6b 27 4c 6f'
port 50331655 app-01a.eth0
vNic slot 2
name: nic-70181-eth0-vmware-sfw.2
agentName: vmware-sfw
state: IOChain Attached
vmState: Detached
failurePolicy: failClosed
slowPathID: none
filter source: Dynamic Filter Creation
world 70179 vmm0:web-02a vcUuid:'50 35 2b f3 4a 4b 10 83-54 72 50 f7 25 10 d8 64'
port 50331656 web-02a.eth0
vNic slot 2
name: nic-70179-eth0-vmware-sfw.2
agentName: vmware-sfw
state: IOChain Attached
vmState: Detached
failurePolicy: failClosed
slowPathID: none
filter source: Dynamic Filter Creation
```


Pour trouver un dvFilter pour une machine virtuelle spécifique :

```
[root@esxi-01:~] summarize-dvfilter | less -p web

world 70179 vmm0:web-02a vcUuid:'50 35 2b f3 4a 4b 10 83-54 72 50 f7 25 10 d8 64'
port 50331656 web-02a.eth0
  vNic slot 2
    name: nic-70179-eth0-vmware-sfw.2
  agentName: vmware-sfw
    state: IOChain Attached
    vmState: Detached
    failurePolicy: failClosed
    slowPathID: none
    filter source: Dynamic Filter Creation
.
.
.
```

Pour déterminer les règles de pare-feu qui s'appliquent à un dvFilter spécifique (dans cet exemple, nic-70227-eth0-vmware-sfw.2 est le nom du dvFilter) :

```
[root@esxi-02:~] vsipioctl getrules -f nic-70227-eth0-vmware-sfw.2
ruleset mainrs {
rule 3072 at 1 inout protocol tcp from any to addrset 48822ec3-2670-497b-82f9-524618c16877 port 443
accept with log;
rule 3072 at 2 inout protocol tcp from any to addrset 48822ec3-2670-497b-82f9-524618c16877 port 80
accept with log;
rule 3074 at 3 inout protocol tcp from addrset 48822ec3-2670-497b-82f9-524618c16877 to addrset
8b9e75e7-bc62-4d7f-9a58-a872f393448e port 8443 accept with log;
rule 3074 at 4 inout protocol tcp from addrset 48822ec3-2670-497b-82f9-524618c16877 to addrset
8b9e75e7-bc62-4d7f-9a58-a872f393448e port 22 accept with log;
rule 3075 at 5 inout protocol tcp from addrset 8b9e75e7-bc62-4d7f-9a58-a872f393448e to addrset
b695c8df-9894-4068-a5e7-5504fe48d459 port 3306 accept with log;
rule 3076 at 6 inout protocol tcp from ip 192.168.110.10 to addrset rdst3076 port 443 accept with log;
rule 3076 at 7 inout protocol icmp typecode 8:0 from ip 192.168.110.10 to addrset rdst3076 accept
with log;
rule 3076 at 8 inout protocol tcp from ip 192.168.110.10 to addrset rdst3076 port 22 accept with log;
rule 3076 at 9 inout protocol tcp from ip 192.168.110.10 to addrset rdst3076 port 80 accept with log;
rule 2 at 10 inout protocol any from any to any accept with log;
}

ruleset mainrs_L2 {
rule 1 at 1 inout ethertype any stateless from any to any accept;
}
}
```

Pour obtenir la liste des ensembles d'adresses utilisées dans un dvFilter spécifique :

```
[root@esxi-02:~] vsipioctl getaddrsets -f nic-70227-eth0-vmware-sfw.2
addrset 48822ec3-2670-497b-82f9-524618c16877 {
ip 172.16.10.13,
mac 52:54:00:42:4d:38,
}
addrset 8b9e75e7-bc62-4d7f-9a58-a872f393448e {
}
```

```

addrset b695c8df-9894-4068-a5e7-5504fe48d459 {
ip 172.16.30.11,
mac 52:54:00:64:0e:4f,
}
addrset rdst3076 {
ip 172.16.10.13,
ip 172.16.30.11,
mac 52:54:00:42:4d:38,
mac 52:54:00:64:0e:4f,
}

```

Pour vérifier les flux via un dvFilter spécifique :

```

[root@esxi-02:~] vsipioctl getflows -f nic-75360-eth0-vmware-sfw.2
Count retrieved from kernel active(L3,L4)=20, active(L2)+inactive(L3,L4)=0, drop(L2,L3,L4)=0
a5d914f7a5b85fe5 Active tcp 0800 IN 3076 0 0 192.168.110.10:Unknown(51281) -> 172.16.10.11:ssh(22)
513 FINWAIT2:FINWAIT2 4304 5177 34 33
a5d914f7a5b86001 Active tcp 0800 OUT 2 0 0 172.16.10.11:http(80) -> 100.64.80.1:Unknown(60006) 457
SYNSENT:CLOSED 56 819 1 1
a5d914f7a5b86006 Active igmp 0800 IN 2 0 0 0.0.0.0 -> 224.0.0.1 36 0 1 0
a5d914f7a5b86011 Active tcp 0800 IN 3072 0 0 100.64.80.1:Unknown(60098) -> 172.16.10.11:http(80) 320
FINWAIT2:FINWAIT2 413 5411 9 6
a5d914f7a5b86012 Active tcp 0800 OUT 3074 0 0 172.16.10.11:Unknown(46001) ->
172.16.20.11:Unknown(8443) 815 FINWAIT2:FINWAIT2 7418 1230 10 9
a5d914f7a5b86013 Active udp 0800 OUT 2 0 0 172.16.10.11:Unknown(40080) -> 192.168.110.10:domain(53)
268 140 2 2
a5d914f7a5b86014 Active udp 0800 OUT 2 0 0 172.16.10.11:Unknown(59251) -> 192.168.110.10:domain(53)
268 140 2 2
a5d914f7a5b86015 Active ipv6-icmp 86dd OUT 2 0 0 fe80::250:56ff:feb5:a60e -> ff02::1:ff62:5ed4 135 0
0 72 0 1
a5d914f7a5b86016 Active ipv6-icmp 86dd OUT 2 0 0 fe80::250:56ff:feb5:a60e -> ff02::1:ff62:5ed4 135 0
0 72 0 1
a5d914f7a5b86017 Active tcp 0800 IN 3072 0 0 100.64.80.1:Unknown(60104) -> 172.16.10.11:http(80) 320
FINWAIT2:FINWAIT2 413 5451 9 7
a5d914f7a5b86018 Active tcp 0800 OUT 3074 0 0 172.16.10.11:Unknown(46002) ->
172.16.20.11:Unknown(8443) 815 TIMEWAIT:TIMEWAIT 7314 1230 8 9
a5d914f7a5b86019 Active tcp 0800 IN 3072 0 0 100.64.80.1:Unknown(60110) -> 172.16.10.11:http(80) 320
FINWAIT2:FINWAIT2 373 5451 8 7
a5d914f7a5b8601a Active tcp 0800 OUT 3074 0 0 172.16.10.11:Unknown(46003) ->
172.16.20.11:Unknown(8443) 815 FINWAIT2:FINWAIT2 7418 1230 10 9
a5d914f7a5b8601b Active tcp 0800 IN 3072 0 0 100.64.80.1:Unknown(60114) -> 172.16.10.11:http(80) 328
TIMEWAIT:TIMEWAIT 413 5451 9 7
a5d914f7a5b8601c Active tcp 0800 OUT 3074 0 0 172.16.10.11:Unknown(46004) ->
172.16.20.11:Unknown(8443) 815 TIMEWAIT:TIMEWAIT 7262 1218 7 9
a5d914f7a5b8601d Active tcp 0800 OUT 2 0 0 172.16.10.11:http(80) -> 100.64.80.1:Unknown(60060) 457
SYNSENT:CLOSED 56 819 1 1
a5d914f7a5b8601e Active tcp 0800 IN 3072 0 0 100.64.80.1:Unknown(60120) -> 172.16.10.11:http(80) 320
TIMEWAIT:TIMEWAIT 373 5411 8 6
a5d914f7a5b8601f Active tcp 0800 OUT 3074 0 0 172.16.10.11:Unknown(46005) ->
172.16.20.11:Unknown(8443) 815 FINWAIT2:FINWAIT2 7418 1230 10 9
a5d914f7a5b86020 Active tcp 0800 IN 3072 0 0 100.64.80.1:Unknown(60126) -> 172.16.10.11:http(80) 229
EST:EST 173 5371 3 5
a5d914f7a5b86021 Active tcp 0800 OUT 3074 0 0 172.16.10.11:Unknown(46006) ->
172.16.20.11:Unknown(8443) 815 FINWAIT2:FINWAIT2 7418 1230 10 9

```

Détermination des règles de pare-feu qui s'appliquent à un hôte KVM

Pour résoudre les problèmes de pare-feu avec un hôte KVM, vous pouvez consulter les règles de pare-feu qui s'appliquent à l'hôte.

Pour obtenir la liste des commandes VIF soumises aux règles de pare-feu sur l'hôte KVM :

```
# ovs-appctl -t /var/run/openvswitch/nsxa-ctl dfw/vif
Vif ID      : da95fc1e-65fd-461f-814d-d92970029bf0
Port name   : db-01a-eth0
Port number : 2
```

Si vous n'obtenez rien, recherchez les problèmes de connectivité entre le nœud et les contrôleurs.

Pour obtenir la liste des règles appliquées à une commande VIF spécifique (dans cet exemple, da95fc1e-65fd-461f-814d-d92970029bf0 est l'ID de VIF) :

```
# ovs-appctl -t /var/run/vmware/nsx-agent/nsxa-ctl dfw/rules da95fc1e-65fd-461f-814d-d92970029bf0
Distributed firewall status: enabled

Vif ID      : da95fc1e-65fd-461f-814d-d92970029bf0
ruleset d035308b-cb0d-4e7e-aae5-a428b461db46 {
  rule 3072 inout protocol tcp from any to addrset 48822ec3-2670-497b-82f9-524618c16877 port 443
  accept with log;
  rule 3072 inout protocol tcp from any to addrset 48822ec3-2670-497b-82f9-524618c16877 port 80 accept
  with log;
  rule 3074 inout protocol tcp from addrset 48822ec3-2670-497b-82f9-524618c16877 to addrset 8b9e75e7-
  bc62-4d7f-9a58-a872f393448e port 8443 accept with log;
  rule 3074 inout protocol tcp from addrset 48822ec3-2670-497b-82f9-524618c16877 to addrset 8b9e75e7-
  bc62-4d7f-9a58-a872f393448e port 22 accept with log;
  rule 3075 inout protocol tcp from addrset 8b9e75e7-bc62-4d7f-9a58-a872f393448e to addrset
  b695c8df-9894-4068-a5e7-5504fe48d459 port 3306 accept with log;
}

ruleset 3027fed3-60b1-483e-aa17-c28719275704 {
  rule 3076 inout protocol tcp from 192.168.110.10 to addrset b695c8df-9894-4068-a5e7-5504fe48d459
  port 443 accept with log;
  rule 3076 inout protocol icmp type 8 code 0 from 192.168.110.10 to addrset b695c8df-9894-4068-
  a5e7-5504fe48d459 accept with log;
  rule 3076 inout protocol tcp from 192.168.110.10 to addrset b695c8df-9894-4068-a5e7-5504fe48d459
  port 22 accept with log;
  rule 3076 inout protocol tcp from 192.168.110.10 to addrset b695c8df-9894-4068-a5e7-5504fe48d459
  port 80 accept with log;
  rule 3076 inout protocol tcp from 192.168.110.10 to addrset 8b9e75e7-bc62-4d7f-9a58-a872f393448e
  port 443 accept with log;
  rule 3076 inout protocol icmp type 8 code 0 from 192.168.110.10 to addrset 8b9e75e7-bc62-4d7f-9a58-
  a872f393448e accept with log;
  rule 3076 inout protocol tcp from 192.168.110.10 to addrset 8b9e75e7-bc62-4d7f-9a58-a872f393448e
  port 22 accept with log;
  rule 3076 inout protocol tcp from 192.168.110.10 to addrset 8b9e75e7-bc62-4d7f-9a58-a872f393448e
  port 80 accept with log;
  rule 3076 inout protocol tcp from 192.168.110.10 to addrset 48822ec3-2670-497b-82f9-524618c16877
```

```

port 443 accept with log;
  rule 3076 inout protocol icmp type 8 code 0 from 192.168.110.10 to addrset
48822ec3-2670-497b-82f9-524618c16877 accept with log;
  rule 3076 inout protocol tcp from 192.168.110.10 to addrset 48822ec3-2670-497b-82f9-524618c16877
port 22 accept with log;
  rule 3076 inout protocol tcp from 192.168.110.10 to addrset 48822ec3-2670-497b-82f9-524618c16877
port 80 accept with log;
}

ruleset 5e9bdc3-adba-4f67-a680-5e6ed5b8f40a {
  rule 2 inout protocol any from any to any accept with log;
}

ruleset ddf93011-4078-4006-b8f8-73f979d7a717 {
  rule 1 inout ethertype any stateless from any to any accept;
}

```

Pour obtenir la liste des ensembles d'adresses utilisées dans une commande VIF spécifique :

```

# ovs-appctl -t /var/run/vmware/nsx-agent/nsxa-ctl dfw/addrsets da95fc1e-65fd-461f-814d-d92970029bf0
48822ec3-2670-497b-82f9-524618c16877 {
  mac 52:54:00:42:4d:38,
  ip 172.16.10.13,
}

8b9e75e7-bc62-4d7f-9a58-a872f393448e {
}

b695c8df-9894-4068-a5e7-5504fe48d459 {
  mac 52:54:00:64:0e:4f,
  ip 172.16.30.11,
}

```

Vérifiez les connexions via le module Linux Conntrack. Dans cet exemple, nous recherchons des flux entre deux adresses IP spécifiques.

```

# ovs-appctl -t ovs-l3d conntrack/show | grep 192.168.110.10 | grep 172.16.10.13
ACTIVE
icmp,orig=(src=192.168.110.10,dst=172.16.10.13,id=1,type=8,code=0),reply=(src=172.16.10.13,dst=192.168
.110.10,id=1,type=0,code=0),start=2018-03-26T04:43:28.325,id=3122159040,zone=23119,status=SEEN_REPLY|
CONFIRMED,timeout=29,mark=3076,labels=0x1f

```

Journaux de paquet de pare-feu

Si la journalisation est activée pour les règles de pare-feu, vous pouvez consulter les journaux de paquet de pare-feu pour résoudre les problèmes.

Le fichier journal est `/var/log/dfwpktlogs.log` pour les hôtes ESXi et KVM.

```

# tail -f /var/log/dfwpktlogs.log
2018-03-27T10:23:35.196Z INET TERM 3072 IN TCP FIN 100.64.80.1/60688->172.16.10.11/80 8/7 373/5451
2018-03-27T10:23:35.196Z INET TERM 3074 OUT TCP FIN 172.16.10.11/46108->172.16.20.11/8443 8/9
1178/7366

```

```

2018-03-27T10:23:35.196Z INET TERM 3072 IN TCP RST 100.64.80.1/60692->172.16.10.11/80 9/6 413/5411
2018-03-27T10:23:35.196Z INET TERM 3074 OUT TCP RST 172.16.10.11/46109->172.16.20.11/8443 9/7
1218/7262
2018-03-27T10:23:37.442Z 71d32787 INET match PASS 3074 IN 60 TCP 172.16.10.12/35770-
>172.16.20.11/8443 S
2018-03-27T10:23:38.492Z INET match PASS 2 OUT 1500 TCP 172.16.10.11/80->100.64.80.1/60660 A
2018-03-27T10:23:39.934Z INET match PASS 3072 IN 52 TCP 100.64.80.1/60720->172.16.10.11/80 S
2018-03-27T10:23:39.944Z INET match PASS 3074 OUT 60 TCP 172.16.10.11/46114->172.16.20.11/8443 S
2018-03-27T10:23:39.944Z 71d32787 INET match PASS 3074 IN 60 TCP 172.16.10.11/46114-
>172.16.20.11/8443 S
2018-03-27T10:23:42.449Z 71d32787 INET match PASS 3074 IN 60 TCP 172.16.10.12/35771-
>172.16.20.11/8443 S
2018-03-27T10:23:44.712Z INET TERM 3074 IN TCP RST 172.16.10.11/46109->172.16.20.11/8443 9/7 1218/7262
2018-03-27T10:23:44.712Z INET TERM 3074 IN TCP FIN 172.16.10.12/35766->172.16.20.11/8443 9/10
1233/7418
2018-03-27T10:23:44.712Z INET TERM 3074 IN TCP FIN 172.16.10.11/46110->172.16.20.11/8443 9/9 1230/7366
2018-03-27T10:23:44.712Z INET TERM 3074 IN TCP FIN 172.16.10.12/35767->172.16.20.11/8443 9/10
1233/7418
2018-03-27T10:23:44.939Z INET match PASS 3072 IN 52 TCP 100.64.80.1/60726->172.16.10.11/80 S
2018-03-27T10:23:44.957Z INET match PASS 3074 OUT 60 TCP 172.16.10.11/46115->172.16.20.11/8443 S
2018-03-27T10:23:44.957Z 71d32787 INET match PASS 3074 IN 60 TCP 172.16.10.11/46115-
>172.16.20.11/8443 S
2018-03-27T10:23:45.480Z INET TERM 2 OUT TCP TIMEOUT 172.16.10.11/80->100.64.80.1/60528 1/1 1500/56

```

Autres scénarios de dépannage

6

Cette section décrit le dépannage de plusieurs scénarios d'erreur.

Ce chapitre contient les rubriques suivantes :

- [Échec d'ajout ou de suppression d'un nœud de transport](#)
- [Un nœud de transport prend environ 5 minutes pour se connecter à un autre contrôleur](#)
- [Machine virtuelle NSX Manager dégradée](#)
- [Expiration de l'agent NSX lors de la communication avec NSX Manager](#)
- [Échec d'ajout d'un hôte ESXi](#)
- [État incorrect de NSX Controller](#)
- [Adresses IP de gestion de machines virtuelles KVM non accessibles lorsque IPFIX est activé](#)

Échec d'ajout ou de suppression d'un nœud de transport

Vous ne pouvez pas supprimer ou ajouter un nœud de transport.

Problème

L'erreur se produit dans le scénario suivant :

- 1 Un hôte ESXi est à la fois un nœud d'infrastructure et un nœud de transport.
- 2 L'hôte est supprimé en tant que nœud de transport. Cependant, la suppression du nœud de transport échoue. L'état du nœud de transport est Orphelin.
- 3 L'hôte est immédiatement supprimé en tant que nœud d'infrastructure.
- 4 L'hôte est ajouté à nouveau en tant que nœud d'infrastructure.
- 5 L'hôte est ajouté en tant qu'un nœud de transport avec une nouvelle zone de transport et un nouveau commutateur. Cette étape entraîne l'erreur Échec/Réussite partielle.

Cause

À l'étape 2, si vous attendez quelques minutes, la suppression du nœud de transport réussira, car NSX Manager réessayera la suppression. Si vous supprimez immédiatement le nœud d'infrastructure, NSX Manager ne peut pas effectuer de nouvelle tentative, car l'hôte est supprimé de NSX-T Data Center. Cela provoque un nettoyage incomplet de l'hôte, avec une configuration du commutateur encore présente, ce qui entraîne l'échec de l'étape 5.

Solution

- 1 Supprimez toutes les vmknics de vCenter Server présentes sur l'hôte qui sont connectés au commutateur NSX-T Data Center.
- 2 Récupérez le nom du commutateur à l'aide de la commande d'interface de ligne de commande `esxcfg-vswitch -l`. Par exemple :

```
esxcfg-vswitch -l
```

| Switch Name | Num Ports | Used Ports | Configured Ports | MTU | Uplinks |
|-------------|-----------|------------|------------------|------|---------|
| vSwitch0 | 1536 | 4 | 128 | 1500 | vmnic0 |

| PortGroup Name | VLAN ID | Used Ports | Uplinks |
|--------------------|---------|------------|---------|
| VM Network | 0 | 0 | vmnic0 |
| Management Network | 0 | 1 | vmnic0 |

| Switch Name | Num Ports | Used Ports | Uplinks |
|-------------|-----------|------------|---------|
| nsxvswitch | 1536 | 4 | |

- 3 Supprimez le nom du commutateur à l'aide de la commande d'interface de ligne de commande `esxcfg-vswitch -d <switch-name> --dvswitch`. Par exemple :

```
esxcfg-vswitch -d nsxvswitch --dvswitch
```

Un nœud de transport prend environ 5 minutes pour se connecter à un autre contrôleur

Lorsque le contrôleur connecté d'un nœud de transport ESXi tombe en panne, environ 5 minutes sont nécessaires au nœud de transport pour se connecter à un autre contrôleur.

Problème

Un nœud de transport ESXi est normalement connecté à un contrôleur spécifique dans un cluster de contrôleurs. Vous pouvez trouver le contrôleur connecté avec la commande d'interface de ligne de commande `get controllers`. Si le contrôleur connecté tombe en panne, environ 5 minutes sont nécessaires avant la connexion du nœud de transport à un autre contrôleur.

Cause

Le nœud de transport tente de se reconnecter au contrôleur en panne pendant un certain temps avant l'abandon et la connexion à un autre contrôleur. L'ensemble du processus dure environ 5 minutes. Il s'agit du comportement attendu.

Machine virtuelle NSX Manager dégradée

NSX Manager, déployé sur un hôte KVM, renvoie une erreur lors de l'exécution des commandes de l'interface de ligne de commande, telle que `get service` et `get interface`.

Problème

La commande d'interface de ligne de commande renvoie une erreur du service. Par exemple,

```
nsx-manager-1> get service
% An error occurred while processing the service command
```

D'autres commandes d'interface de ligne de commande peuvent aussi renvoyer une erreur. La commande `get support-bundle` indique que le répertoire `/tmp` est passé en lecture seule. Par exemple,

```
nsx-manager-1> get support-bundle file failed-to-get-service.tgz
% An error occurred while retrieving the support bundle: [Errno 30] Read-only file system: '/tmp/
tmpHzXF1u'
```

Le fichier journal `/var/log/messages-<timestamp>` contient un message tel que le suivant :

```
Nov 17 07:26:48 no kernel: NMI watchdog: BUG: soft lockup - CPU#5 stuck for 23s! [qemu-kvm:4386]
```

Cause

Un ou plusieurs systèmes de fichiers du dispositif NSX Manager sont endommagés. Certaines des causes possibles sont documentées dans <https://access.redhat.com/solutions/22621>.

Pour résoudre le problème, vous pouvez réparer les systèmes de fichiers endommagés ou effectuer une restauration à partir d'une sauvegarde.

Solution

- 1 Option 1 : Réparer les systèmes de fichiers endommagés. Les étapes suivantes sont spécifiques à NSX Manager en cours d'exécution sur un hôte KVM.

- a Exécutez la commande `virsh destroy` pour arrêter la machine virtuelle NSX Manager.
- b Exécutez la commande `virt-rescue` en mode écriture sur l'image `qcow2`. Par exemple,

```
virt-rescue --rw -a nsx-unified-appliance-2.0.0.0.6522097.phadniss-p0-DK-to-DGo-on-rhel-
prod_nsx_manager_1.qcow2
```

- c Dans l'invite de commande `virt-rescue`, exécutez la commande `e2fsck` pour corriger le système de fichiers `tmp`. Par exemple,

```
<rescue> e2fsck /dev/nsx/tmp
```


- d Si nécessaire, exécutez à nouveau la commande `e2fsck /dev/nsx/tmp` jusqu'à ce qu'il n'y ait plus d'erreurs.
 - e Redémarrez NSX Manager avec la commande `virsh start`.
- 2 Option 2 : Effectuer une restauration à partir d'une sauvegarde.
- Pour obtenir des instructions, consultez le *Guide d'administration de NSX-T*.

Expiration de l'agent NSX lors de la communication avec NSX Manager

Dans un environnement à grande échelle avec de nombreux nœuds de transport et machines virtuelles sur des hôtes ESXi, les agents NSX qui s'exécutent sur des hôtes ESXi peuvent expirer lors de la communication avec NSX Manager.

Problème

Certaines opérations échouent, comme lorsqu'une VNIC de machine virtuelle essaie de s'attacher à un commutateur logique. Le fichier `/var/run/log/nsx-opsagent.log` contient des messages tels que :

```
level="ERROR" errorCode="MPA41542" [MP_AddVnicAttachment] RPC call [0e316296-13-14] to NSX
management plane timeout
2017-05-15T05:32:13Z nsxa: [nsx@6876 comp="nsx-esx" subcomp="NSXA[VifHandlerThread:-2282640]"
tid="1000017079" level="ERROR" errorCode="MPA42003" [DoMpVifAttachRpc] MP_AddVnicAttachment()
failed: RPC call to NSX management plane timeout
```

Cause

Dans un environnement à grande échelle, certaines opérations peuvent être plus longues que d'habitude et finissent par échouer, car les valeurs de délai d'expiration par défaut sont dépassées.

Solution

1 Augmentez la valeur du délai d'expiration de l'agent NSX.

- a Sur l'hôte ESXi, arrêtez l'opsAgent NSX avec la commande suivante :

```
/etc/init.d/nsx-opsagent stop
```

- b Modifiez le fichier `/etc/vmware/nsx-opsagent/nsxa.json` et modifiez la valeur de `vifOperationTimeout` de 25 à 55, par exemple.

```
"mp" : {
  /* timeout for VIF operation */
  "vifOperationTimeout" : 25,
```

Note Cette valeur du délai d'expiration doit être inférieure à la valeur de délai d'expiration de `hostd` que vous avez défini à l'étape 2.

- c Démarrez l'opsAgent NSX avec la commande suivante :

```
/etc/init.d/nsx-opsagent start
```

2 Augmentez la valeur du délai d'expiration de `hostd`.

- a Sur l'hôte ESXi, arrêtez l'agent `hostd` avec la commande suivante :

```
/etc/init.d/hostd stop
```

- b Modifiez le fichier `/etc/vmware/hostd/config.xml`. Sous `<opaqueNetwork>`, supprimez le commentaire de l'entrée pour `<taskTimeout>` et modifiez la valeur de 30 à 60, par exemple.

```
<opaqueNetwork>
  <!-- maximum message size allowed in opaque network manager IPC, in bytes. -->
  <!-- <maxMsgSize> 65536 </maxMsgSize> -->
  <!-- maximum wait time for opaque network response -->
  <!-- <taskTimeout> 30 </taskTimeout> -->
```

- c Démarrez l'agent `hostd` avec la commande suivante :

```
/etc/init.d/hostd start
```

Échec d'ajout d'un hôte ESXi

Vous n'êtes pas en mesure d'ajouter un hôte ESXi à l'infrastructure NSX-T Data Center.

Problème

À partir de l'interface utilisateur graphique de NSX Manager, l'ajout d'un hôte ESXi échoue avec l'erreur « le chemin d'accès du fichier ... est réclamé par plusieurs VIB sans superposition ». Le fichier journal affiche des messages tels que le suivant :

```
Failed to install software on host. Failed to install software on host. 10.172.120.60 :
java.rmi.RemoteException: [DependencyError] File path of '/usr/lib/vmware/vmkmmod/nsx-vsip' is claimed
by multiple non-overlay VIBs
```

Cause

Certains VIB provenant d'une installation précédente sont toujours présents sur l'hôte, probablement car il n'ont pas été désinstallés proprement.

Solution

- 1 Dans le message d'erreur, récupérez les noms des VIB qui provoquent cet échec.
- 2 Utilisez des commandes ESXi pour désinstaller les VIB.

État incorrect de NSX Controller

Certains contrôleurs sont dans un état incorrect du rapport de cluster NSX Controller pour l'un des contrôleurs.

Problème

Lorsqu'un contrôleur est mis sous tension et hors tension un certain nombre de fois, les autres contrôleurs signalent qu'il est inactif alors qu'il est actif et en cours d'exécution.

Cause

Une erreur interne impliquant le module ZooKeeper se produit parfois lorsqu'un contrôleur est mis hors tension puis sous tension et entraîne un échec de la communication entre ce contrôleur et les autres contrôleurs du cluster.

Solution

- ◆ Supprimez le nœud de contrôleur qui est signalé comme inactif du cluster, supprimez la configuration de cluster du nœud et joignez de nouveau le nœud au cluster. Pour plus d'informations, reportez-vous à la section « Remplacer un membre du cluster NSX Controller » dans le *Guide d'Administration de NSX-T*.

Adresses IP de gestion de machines virtuelles KVM non accessibles lorsque IPFIX est activé

Lorsque IPFIX est activé sur plusieurs machines virtuelles d'un hôte KVM et que le taux d'échantillonnage est de 100 %, les adresses IP de gestion peuvent parfois être inaccessibles sur certaines machines virtuelles.

Problème

Lorsque vous activez IPFIX pour plusieurs machines virtuelles sur le même hôte et que vous définissez le taux d'échantillonnage à 100 %, il peut y avoir une grande quantité de trafic IPFIX. Cela peut impacter sur le trafic de gestion et rendre les adresses IP de gestion inaccessibles par intermittence, même si le trafic de production et le trafic de gestion passent par des OVS différents.

Cause

La charge de travail est trop importante pour l'hôte et les machines virtuelles.

Solution

- ◆ Réduisez la charge sur l'hôte en réduisant le nombre de machines virtuelles avec IPFIX activé ou en réduisant le taux d'échantillonnage.