

# Notes de mise à jour de VMware NSX-T Data Center 2.3

VMware NSX-T Data Center 2.3 | 18 septembre 2018 | Build 10085361

Recherchez régulièrement les ajouts et mises à jour de ces notes.

## Contenu des notes de mise à jour

Les notes de mise à jour couvrent les sujets suivants :

- [Nouveautés](#)
- [Compatibilité et configuration système requise](#)
- [Changements généraux du comportement](#)
- [Informations sur la référence de l'API](#)
- [Problèmes résolus](#)
- [Problèmes connus](#)

## Nouveautés

NSX-T Data Center 2.3 est la version de mise à niveau incrémentielle qui améliore la nouvelle plate-forme à plusieurs hyperviseurs fournie pour le cloud et les conteneurs.

Les nouvelles fonctionnalités et améliorations de fonctionnalités suivantes sont disponibles dans NSX-T Data Center 2.3.

### Présentation de la prise en charge de NSX-T Data Center pour les hôtes bare-metal

La prise en charge bare-metal inclut les charges de travail basées sur Linux s'exécutant sur des serveurs bare-metal et des conteneurs s'exécutant sur des serveurs bare-metal sans hyperviseur. NSX-T Data Center utilise Open vSwitch pour permettre à n'importe quel hôte Linux d'agir comme nœud de transport NSX-T Data Center.

- **Prise en charge d'un serveur bare-metal** : inclut les charges de travail natives exécutant les systèmes d'exploitation RHEL 7.4, CentOS 7.4 et Ubuntu 16.0.4 pour permettre aux utilisateurs de mettre en réseau des charges de travail de calcul bare-metal sur des connexions de superposition VLAN et pour appliquer des stratégies de micro-segmentation (application de couche 4 avec état) pour les flux de communication virtuels-physiques et physiques-physiques.
- **Prise en charge des conteneurs Linux bare-metal** : exécute des conteneurs Docker à l'aide d'une plate-forme RedHat OpenShift Container sur des hôtes Linux bare-metal avec RHEL 7.4 ou RHEL 7.5.

### Améliorations de NSX Cloud

- **Prise en charge de déploiements AWS** : Prise en charge de NSX Cloud pour les charges de travail AWS.
- **Provisionnement automatique d'agents NSX Agent dans des VNET Azure**
- **Prise en charge de VPN entre site local et cloud public** : inclut des capacités VPN intégrées dans

la passerelle de cloud public NSX Cloud à l'aide d'API. Vous pouvez utiliser les fonctionnalités VPN pour créer des liens IPSEC entre les éléments suivants :

- VPC Amazon/VNet Azure de calcul gérés et machines virtuelles de service tiers dans des VPC Amazon/VNet Azure
- VPC Amazon/VNET Azure gérés et périphérique VPN sur site
- **Prise en charge élargie de système d'exploitation pour NSX Cloud Agent** : NSX Cloud prend en charge les systèmes d'exploitation RHEL 7.5 dans le cloud public.

## Prise en charge des services de sécurité

### Présentation de l'insertion de services à des niveaux de routage

- **Prise en charge de l'insertion de services sur des routeurs de niveau 0 et de niveau 1** : inclut la possibilité d'intégrer des solutions de sécurité tierces, de déployer une solution de sécurité tierce High Availability au niveau 0 ou au niveau 1 ou aux deux niveaux, et d'insérer la solution de sécurité tierce via une stratégie de redirection.  
Consultez le guide de compatibilité VMware – Réseau et sécurité pour connaître le dernier état de certification de solutions tierces sur NSX-T Data Center.

### Améliorations du pare-feu distribué

- **Prise en charge de sections multiples dans NSX Edge Firewall** : ajoute de multiples sections dans NSX Edge Firewall pour simplifier la gestion
- **Nombre de correspondances de règles de pare-feu et indice de popularité des règles** : surveillance de l'utilisation des règles et identification rapide des règles inutilisées pour nettoyage
- **Verrouillage de section de pare-feu** : permet à plusieurs administrateurs de sécurité de travailler simultanément sur le pare-feu
- **Regroupement d'objets** : prend en charge l'ajout d'un objet à un groupe s'il correspond aux cinq balises spécifiées, qui étaient précédemment au nombre de deux
- **Longueur de balise** : augmente la valeur de longueur de balise de 65 à 256 et l'étendue des balises de 20 à 128
- **Découverte d'applications** : découvre et classe par catégorie (ce qui permet également une catégorisation personnalisée par les utilisateurs) les applications installées à l'intérieur des machines virtuelles invitées. Les applications contiennent des informations détaillées sur les fichiers exécutables, le hachage, les informations d'éditeur et la date d'installation.

## Réseau et prise en charge des services NSX Edge

- **Prise en charge de la superposition pour le mode de chemin d'accès aux données amélioré dans N-VDS** : en liaison avec vSphere 6.7, le mode de chemin d'accès aux données amélioré dans N-VDS pour NSX-T Data Center 2.3 prend en charge les charges de travail de style NFV nécessitant un chemin d'accès aux données haute performance.
- **Prise en charge de NAT avec état et des services de pare-feu sur le port de service centralisé**
- **Prise en charge d'API pour effacer toutes les entrées DNS sur un redirecteur DNS** : offre la possibilité d'effacer toutes les entrées de cache DNS en un seul appel API sur un redirecteur DNS donné. Cette commande est utile lorsqu'un serveur DNS fournit des réponses erronées et pour éviter d'attendre le délai d'expiration de l'entrée DNS après la réparation du serveur DNS.
- **Améliorations de l'équilibreur de charge**
  - **Prise en charge d'une liste de chiffrements prédéfinis** : Profils SSL prédéfinis pour HTTPS VIP garantissant une sécurité ou des performances accrues.
  - **Améliorations de règle de l'équilibreur de charge** : nouvelles règles d'équilibreur de charge, *action de suppression d'en-tête*, *condition de correspondance SSL* et *attribution de variables sur condition de correspondance*.
  - **Prise en charge de l'équilibreur de charge sur un routeur de service autonome** : offre la possibilité de déployer un service d'équilibrage de charge sur un routeur de service ne disposant pas d'un port de routeur.

## Améliorations de l'Interface utilisateur

- **Nouvelle prise en charge linguistique** : interface utilisateur dorénavant disponible en anglais, allemand, français, japonais, chinois simplifié, coréen, chinois traditionnel et espagnol.
- **Navigation et page d'accueil améliorées** : la nouvelle page d'accueil met en évidence la recherche et présente un résumé synoptique du système.
- **Recherche améliorée** : la recherche inclut des suggestions de saisie semi-automatique, qui sont accessibles depuis la page d'accueil.
- **Visualisation de la topologie réseau** : NSX Policy Manager fournit la possibilité de surveiller les communications de groupe à groupe, de machine virtuelle à machine virtuelle et de processus à processus. Vous pouvez visualiser les relations entre objets réseau tels que commutateurs logiques, ports, routeurs et dispositifs NSX Edge.

## Prise en charge des opérations et du dépannage

- **Améliorations de l'installation et de la mise à niveau**
  - **NSX-T Data Center dans un environnement vSphere sans état** : active des options de déploiement supplémentaires en fournissant la prise en charge des hôtes ESXi sans état qui utilisent vSphere Auto Deploy et les profils d'hôte. La prise en charge de la fonctionnalité nécessite vSphere 6.7 U1 ou version ultérieure.
  - **Coexistence de la prise en charge des machines virtuelles NSX Edge et des nœuds bare-metal dans le même cluster de NSX Edge** : Les machines virtuelles de nœuds NSX Edge et les nœuds bare-metal peuvent désormais exister dans le même cluster NSX Edge afin de simplifier la mise à l'échelle des services hébergés sur le nœud NSX Edge, comme l'équilibreur de charge.
  - **Mise à niveau modulaire de NSX-T Data Center** : accepte la prise en charge de la mise à niveau modulaire dans le coordinateur de mise à niveau. Vous ne pouvez mettre à niveau que les composants NSX-T Data Center qui ont changé dans la nouvelle version. Cette fonctionnalité ajoutée réduit la surcharge opérationnelle de correction d'une version de NSX-T Data Center.
- **Surveillance et dépannage**
  - **ERSPAN pour KVM Hypervisor** : inclut la prise en charge de la mise en miroir de ports sur KVM – ERSPAN types II et III.
  - **Utilisation de Traceflow vers et depuis des liaisons montantes de routeur logique de niveau 0** : fournit la possibilité de générer un trafic Traceflow depuis les liaisons montantes de routeur logique de niveau 0 et de signaler la réception de paquets Traceflow sur des liaisons montantes de routeur logique de niveau 0 afin de simplifier les opérations de dépannage pour inclure les interfaces de niveau inférieur (données, fonctions) des nœuds NSX Edge dans les rapports Traceflow.
  - **Prise en charge de l'interface de ligne de commande pour arrêter les ports DPDK sur des nœuds Edge bare-metal** : donne la possibilité d'arrêter un port réclamé par DPDK sur le nœud NSX Edge bare-metal afin de simplifier l'isolation des ports lors des opérations d'installation et de dépannage.

## Prise en charge du plug-in OpenStack Neutron

Ces fonctionnalités sont prises en charge à partir de la version OpenStack Upstream Queens.

- **Possibilité pour le plug-in Neutron de provisionner un commutateur logique de superposition soutenu par un chemin d'accès aux données amélioré** : le plug-in NSX Neutron offre la possibilité d'utiliser le mode de chemin d'accès aux données amélioré pour la superposition, qui jusqu'ici était exclusivement VLAN. Avec cette prise en charge, vous pouvez tirer parti des performances du chemin d'accès aux données amélioré notamment en complément de l'environnement OpenStack pour les charges de travail liées à NFV.
- **Prise en charge de la co-existence de produits NSX avec OpenStack** : le plug-in NSX Neutron prend désormais en charge la gestion de NSX Data Center for vSphere et de NSX-T Data Center simultanément pour une implémentation d'OpenStack.
- **Possibilité de consommer VPN en tant que fonctionnalité de service dans OpenStack** : prise en charge d'OpenStack VPNaaS dans l'extension Neutron d'OpenStack qui introduit un ensemble de fonctionnalités VPN.

## Prise en charge de NSX Container Plug-in (NCP)

- **Processus Concourse pour installer NSX-T Data Center**
- **Annotation pour adresse IP SNAT d'équilibreur de charge** : Une adresse IP SNAT pour un équilibreur de charge est annotée dans un service Kubernetes de type LoadBalancer, `ncp/internal_ip_for_policy` : <Adresse IP SNAT>, et ajouté à l'état du service, `status.loadbalancer.ingress.ip`: [<Adresse IP SNAT>, <Adresse IP virtuelle>]. Cette adresse IP peut servir à créer une stratégie réseau qui autorise ce CIDR d'IP.
- **Amélioration de la stratégie réseau Kubernetes** : offre la possibilité de sélectionner des espaces à partir de différents espaces de noms avec des règles de stratégie réseau Kubernetes.
- **Amélioration de l'équilibreur de charge Kubernetes/annotation SNAT**
  - Si NCP ne parvient pas à configurer un équilibreur de charge pour un service, le service sera annoté avec `ncp/error.loadbalancer`.
  - Si NCP ne parvient pas à configurer une adresse IP SNAT pour un service, le service sera annoté avec `ncp/error.snat`.
- **Persistance de la session d'équilibreur de charge NSX-T Data Center pour routes Kubernetes Ingress et OpenShift**
- **Amélioration du script de nettoyage**

## Compatibilité et configuration système requise

Pour plus d'informations sur la compatibilité et la configuration système requise, consultez le [Guide d'installation de NSX-T Data Center](#).

**NSX-T Data Center dans un environnement vSphere sans état** : pour des hôtes ESXi sans état qui utilisent vSphere Auto Deploy et des profils d'hôte, vSphere 6.7 U1 ou version supérieure est requis.

Configuration requise de compatibilité NCP :

Produit	Version
Vignette NCP / NSX-T Data Center pour PAS	2.3.0
NSX-T Data Center	2.2, 2.3
Kubernetes	1.10, 1.11
OpenShift	3.9, 3.10
Système d'exploitation de machine virtuelle sur hôte Kubernetes	Ubuntu 16.04, RHEL 7.4, 7.5
Système d'exploitation de machine virtuelle sur hôte OpenShift	RHEL 7.4, RHEL 7.5
PAS (PCF)	OpsManager 2.1.x + PAS 2.1.x (sauf PAS 2.1.0) OpsManager 2.2.0 + PAS 2.2.0

## Changements généraux du comportement

Le mode HA par défaut des routeurs logiques de niveau 1 change de préemptif à non préemptif

Lors de la création d'un routeur logique de niveau 1, le mode HA par défaut était préemptif, ce qui entraînait un ralentissement du trafic lorsque le nœud NSX Edge préféré revenait en ligne. Avec le nouveau mode HA par défaut non préemptif, les routeurs logiques de niveau 1 récemment créés ne subissent pas ce ralentissement du trafic. Les routeurs logiques de niveau 1 existants ne sont pas touchés par cette modification.

Modification des communications entre le nœud de transport et NSX Controller

En raison de modifications apportées aux communications entre le nœud de transport et NSX Controller, vous devez désormais ouvrir le port TCP 1235 pour NSX-T 2.2 et versions ultérieures. Consultez le [Guide d'installation de NSX-T](#).

Lors de la mise à niveau de NSX-T 2.1 vers une version ultérieure, les deux ports TCP 1234 et 1235 doivent être ouverts. Une fois la mise à niveau terminée, le port TCP 1235 est en cours d'utilisation.

## Informations sur la référence de l'API

Reportez-vous à [Appels et propriétés d'API abandonnés de NSX-T Data Center et NSX Policy](#).

Les dernières informations de référence sur les API se trouvent dans [Informations sur le produit NSX-T Data Center](#).

## Problèmes résolus

Les problèmes résolus sont regroupés comme suit :

- [Problèmes généraux résolus](#)
- [Problèmes d'installation résolus](#)
- [Problèmes de NSX Manager résolus](#)
- [Problèmes de NSX Edge résolus](#)
- [Problèmes de mise en réseau logique résolus](#)
- [Problèmes des services de sécurité résolus](#)
- [Problèmes d'équilibreur de charge résolus](#)
- [Problèmes d'interopérabilité entre les solutions résolus](#)
- [Problèmes des opérations et des services de surveillance résolus](#)
- [Problèmes de mise à niveau résolus](#)
- [Problèmes de l'API résolus](#)
- [Problèmes de NSX Container Plug-in \(NCP\) résolus](#)

### Problèmes résolus généraux

- **Problème 1775315 : Une attaque CSRF se produit lorsque le client Postman est ouvert depuis le navigateur Web**  
Pour les appels d'API effectués avec Postman, CURL ou d'autres clients REST, vous devez fournir explicitement l'en-tête XSRF-TOKEN et sa valeur. Le premier appel d'API qui utilise une authN distante ou appelle /api/session/create(local authN) transporte le jeton XSRF dans l'objet réponse. Les appels d'API ultérieurs transportent la valeur du jeton dans l'en-tête XSRF-TOKEN dans le cadre de la demande.
- **Problème 1989412 : La suppression du domaine lorsque NSX Manager n'est pas accessible n'est pas prise en compte lorsque la connectivité est rétablie**  
Si un domaine est supprimé de la stratégie lorsque NSX Manager n'est pas accessible, le pare-feu et les règles correspondant au domaine supprimé existent toujours lorsque la connexion à NSX Manager est rétablie.
- **Problème 2018478 : Toute tentative de suppression d'un widget du tableau de bord entraîne un blocage avec une erreur de trace de pile**  
Les modifications de l'interface utilisateur du tableau de bord personnalisé, comme la suppression d'un widget à partir de widgets multiples, provoque un blocage de l'interface utilisateur avec une erreur de trace de pile.
- **Problème 1959647 : L'utilisation d'un nom d'alias de serveur de base de données pour créer un DSN peut entraîner l'échec de l'installation de vCenter Server**

Lorsque vous utilisez un nom d'alias de serveur de base de données pour créer un DSN, l'installation de vCenter Server avec une base de données Microsoft SQL externe échoue. L'erreur suivante s'affiche pendant l'installation d'Inventory Service : Une erreur s'est produite pendant le démarrage d'invsvc.

## Problèmes résolus d'installation

- **Problème 1739120** : après le redémarrage du plan de gestion ou du service Proton dans le plan de gestion, l'état de déploiement du nœud d'infrastructure devient blocage.  
Lorsque vous ajoutez un nouvel hôte pris en charge dans la page Infrastructure avec les informations d'identification de l'hôte, l'état passe à Installation en cours. Après le redémarrage du service de plan de gestion ou proton dans le plan de gestion, l'état du déploiement de l'hôte indique Installation en cours ou Désinstallation en cours indéfiniment.
- **Problème 1944669** : le déploiement de dispositifs NSX-T Data Center sur KVM nécessite la spécification de la taille de mémoire exacte  
Lors du déploiement de dispositifs NSX-TData sur ESX, vous pouvez effectuer des déploiements de petite, moyenne et grande tailles avec différentes configurations de RAM. Cependant, lors du déploiement de dispositifs NSX-TData sur KVM, l'allocation de RAM doit être explicitement configurée.
- **Problème 1944678** : le déploiement d'un dispositif NSX-T unifié exige un type de rôle valide  
Lorsque le dispositif NSX-T unifié est déployé dans KVM sans rôle spécifique ou avec un type de rôle non valide, il est déployé dans une configuration non prise en charge avec tous les rôles activés.
- **Problème 1958308** : La préparation de l'hôte ou la création du nœud de transport échoue lorsque l'hôte est en mode de verrouillage  
La préparation de l'hôte ou la création du nœud de transport échoue lorsque l'hôte est en mode de verrouillage. Le message d'erreur suivant s'affiche : `L'autorisation de réaliser cette opération a été refusée.`

## Problèmes résolus de NSX Manager

- **Problème 1954923** : une migration par vMotion de VM connectées à des commutateurs logiques échoue lors de la mise à niveau du plan de gestion  
Lorsque le plan de gestion est mis à niveau, si vous tentez d'effectuer une migration par vMotion d'une machine virtuelle connectée à un commutateur logique, la migration par vMotion échoue.
- **Problème 1954927** : après la restauration de NSX Manager, et si un nouvel hôte ESX non géré par VC est enregistré dans NSX Manager et que ses machines virtuelles sont connectées à des commutateurs logiques existants, l'adresse MAC de la machine virtuelle devient vide sur le MOB des hôtes ESX  
Après la restauration de NSX Manager, si un nouvel hôte ESX non géré par VC est enregistré dans NSX Manager et que ses machines virtuelles sont connectées à des commutateurs logiques existants, l'adresse MAC de la machine virtuelle devient vide sur le MOB des hôtes ESX
- **Problème 1978104** : Certaines pages de l'interface utilisateur de NSX Manager ne sont pas accessibles sur Internet Explorer 11  
Le tableau de bord, les workflows de démarrage et les pages d'équilibreur de charge dans l'interface utilisateur de NSX Manager ne sont pas accessibles lors de l'utilisation d'Internet Explorer sur une machine Windows.
- **Problème 1954986** : La clé de licence est indiquée dans les journaux lorsque la clé est supprimée de l'interface utilisateur

La clé de licence NSX est indiquée dans /var/log/syslog comme suit :

```
<182>1 2017-03-24T05:03:47.008Z bb-mgr-221 NSX - SYSTEM [nsx@6876 audit="true"
comp="nsx-manager" reqId="3d146f2b-fa34-460f-8ac3-56e3c7326015"
subcomp="manager"] UserName:'admin', ModuleName:'License',
Operation:'DeleteLicense, Operation status:'success', New value: ["
<license_key>"] <182>1 2017-03-24T05:03:47.009Z bb-mgr-221 NSX - - [nsx@6876
audit="true" comp="nsx-manager" subcomp="manager"] UserName:'admin',
ModuleName:'Batch', Operation:'RegisterBatchRequest, Operation status:'success',
New value: [{"atomic":false} {"request":
[{"method":"DELETE","uri":"/v1/licenses/<license_key>"}]}}
```

Si le dispositif est configuré pour envoyer des journaux à un collecteur de journaux externe, la valeur de clé est également visible à tout utilisateur autorisé sur le collecteur de journaux externe.

- **Problème 1956055 : L'utilisateur administrateur local ne peut pas accéder au bundle de support technique depuis l'interface utilisateur lorsque la banque de données du plan de gestion est inactive**  
L'utilisateur administrateur local ne peut pas accéder au bundle d'assistance technique depuis l'interface utilisateur lorsque la banque de données du plan de gestion est hors service
- **Problème 1957165 : le chargement de la dernière page d'un ensemble de résultats de recherche comptant plus de 10 040 enregistrements provoque une erreur**  
Dans un environnement important pouvant renvoyer 10 040 objets ou plus pour une requête de recherche, vous pouvez voir une erreur lors de la tentative de chargement des tout derniers enregistrements de l'ensemble de résultats.

#### Problèmes résolus de NSX Edge

- **Problème 1762064 : la configuration du profil IP-pool et de liaison montante de NSX Edge VTEP immédiatement après le redémarrage du dispositif NSX Edge entraîne le blocage de l'accès à la session VTEP BFD**  
Après le redémarrage de NSX Edge, le broker a besoin d'un peu de temps pour réinitialiser les connexions de NSX Edge.

#### Problèmes résolus de mise en réseau logique

- **Problème 1966641 : Si vous ajoutez un hôte et que vous le configurez comme un nœud de transport, l'état du nœud s'affiche comme Inactif s'il ne fait pas partie d'un commutateur logique**  
Après l'ajout et la configuration d'un nouvel hôte en tant que nœud de transport ou lors de la configuration d'un plan de mise à niveau vers NSX-T 2.1, l'état du nœud de transport s'affiche comme Inactif dans l'interface utilisateur s'il ne fait pas partie d'un commutateur logique.
- **Problème 2015445 : L'état du pare-feu sur le routeur de service actif peut ne pas être dupliqué sur le routeur de service récemment activé**  
Le routeur logique de locataires (TLR) peut présenter plusieurs basculements de NSX Edge1 vers NSX Edge2 et inversement. Les états de flux de pare-feu ou NAT sont synchronisés entre les routeurs de service TLR actifs et en veille. Lorsque le routeur TLR est configuré en mode de basculement non préemptif, la synchronisation a lieu avant le premier basculement, et non pas entre le premier basculement et le suivant. En conséquence, le trafic TCP peut expirer au deuxième basculement. Ce problème ne se produit pas lorsque le routeur TLR est configuré en mode préemptif.
- **Problème 2016629 : Échec de la session de mise en miroir RSPAN\_SRC après la migration**  
Lorsqu'une machine virtuelle connectée à un port attribué pour la session de mise en miroir RSPAN\_SRC est migrée vers un autre hyperviseur, et qu'aucun pNic requis n'est présent sur le réseau de l'hyperviseur de destination, la configuration de la session de mise en miroir RSPAN\_SRC sur le port échoue. Cet échec entraîne l'échec de connexion du port, mais le processus de migration de vMotion réussit.

- **Problème 1620144** : dans l'interface de ligne de commande NSX-T Data Center, `get logical-switches` répertorie les commutateurs logiques présentant l'état actif, même après la suppression du nœud de transport  
L'interface de ligne de commande peut tromper un utilisateur en indiquant qu'il existe un commutateur logique fonctionnel. Même lorsque des commutateurs logiques sont visibles, ils ne sont pas fonctionnels. Le commutateur opaque est désactivé lorsque le nœud de transport est supprimé, donc aucun trafic ne passe.
- **Problème 1590888** : Affichage nécessaire d'un avertissement indiquant que des ports logiques sélectionnés dans la section Ethernet s'appliquent uniquement dans le même réseau L2  
Pour le pare-feu distribué, dans la section Ethernet, lorsqu'un port logique ou une adresse MAC est entré dans la section source/destination, un avertissement indiquant que des adresses MAC ou des ports logiques doivent appartenir à des ports de VM dans le même réseau L2 (attachés au même commutateur logique) devrait s'afficher. Actuellement, aucun message d'avertissement n'apparaît.
- **Problème 1763576** : les hyperviseurs peuvent être supprimés en tant que nœuds de transport même lorsqu'ils disposent de machines virtuelles sur le réseau NSX-T Data Center  
NSX-T Data Center ne vous empêche pas de supprimer un nœud de transport même lorsqu'il existe sur le nœud des machines virtuelles faisant partie du réseau. Les machines virtuelles perdent la connectivité après la suppression du nœud de transport.
- **Problème 1780798** : Dans un environnement à grande échelle, certains hôtes peuvent entrer dans un état d'échec  
Dans un environnement à grande échelle avec 200 nœuds hôtes ou plus qui s'exécute depuis un certain temps, certains hôtes peuvent perdre la connectivité avec NSX Manager et le journal contient des messages d'erreur tels que :  

```
2016-12-09T00:57:58Z mpa: [nsx@6876 comp="nsx-esx" subcomp="mpa" level="WARN"]  
Unknown routing key: com.vmware.nsx.tz.*
```
- **Problème 1954997** : La suppression du nœud de transport échoue si des VM sur le nœud de transport sont connectées au commutateur logique au moment de la suppression
  1. Le nœud d'infrastructure et le nœud de transport sont créés.
  2. Attachez des VIF au commutateur logique.
  3. La suppression du nœud de transport sans supprimer les pièces jointes de VIF du commutateur logique échoue.
- **Problème 1958041** : Le trafic BUM peut ne pas fonctionner pour le flux de couche 3 sur des segments de couche 2 physiques lorsque l'hyperviseur ESX possède plusieurs liaisons montantes  
Si toutes les conditions suivantes sont remplies, il est possible que le trafic BUM de l'hyperviseur source sur le routeur logique n'atteigne pas l'hyperviseur de destination.
  - ESX possède plusieurs liaisons montantes
  - Les machines virtuelles source et de destination sont connectées via un routeur logique
  - Les hyperviseurs source et de destination se trouvent sur des segments physiques différents
  - Le réseau logique de destination utilise la réplication MTEP
 Cela se produit, car le module BFD peut ne pas avoir créé la session, ce qui signifie que la sélection MTEP pour le réseau logique de destination peut ne pas s'être produite.

## Problèmes résolus des services de sécurité

- **Problème 1520694** : Dans RHEL 7.1 noyau 3.10.0-229 et versions antérieures, l'ALG FTP ne parvient pas à ouvrir le port négocié sur le canal de données  
Pour une session FTP, où le client et le serveur résident dans des VM sur le même hyperviseur, la passerelle de niveau application (ALG) FTP n'ouvre pas le port négocié pour le canal de données. Ce problème est spécifique à Red Hat et est présent dans RHEL 7.1 noyau 3.10.0-229. Les noyaux RHEL ultérieurs ne sont pas affectés.
- **Problème 2008882** : Pour qu'Application Discovery fonctionne correctement, ne créez aucun



groupe de sécurité qui s'étend sur plusieurs hôtes

Si un seul groupe de sécurité possède des machines virtuelles qui s'étendent sur plusieurs hôtes, la session Application Discovery peut échouer.

### Problèmes résolus d'équilibreur de charge

- **Problème 1995228** : Les algorithmes round-robin et Least Connection pondérés peuvent ne pas distribuer le trafic de manière efficace après la modification et le rechargement d'une configuration  
Les serveurs perdent la connexion lorsqu'un algorithme round-robin ou Least Connection pondéré est modifié et rechargé. Après la perte de connectivité, les informations historiques de distribution du trafic ne sont pas conservées, ce qui entraîne une distribution incorrecte du trafic.
- **Problème 2018629** : La table de vérification de l'intégrité n'affiche pas le type de moniteur mis à jour pour le pool de groupes NS  
Lorsque vous créez des pools de groupes NS statiques et dynamiques avec des membres identiques et un type de moniteur, et que vous modifiez ce type de moniteur sur le pool dynamique, le contrôle de santé du pool dynamique n'apparaît pas dans la table de contrôle de santé.
- **Problème 2020372** : Le contrôle de santé passif ne tient pas compte des membres de pool inactifs une fois le nombre d'échecs maximal atteint  
Le contrôle de santé passif requiert un nombre d'échecs plus élevé que celui configuré afin de prendre en compte les membres de pool inactifs.

### Problèmes résolus d'interopérabilité entre les solutions

- **Problème : 2025624** : Blocage des tableaux de bord Splunk lors du chargement ou lorsque les graphiques des tableaux de bord sont vides  
Splunk extrait l'ancienne version de *nsx\_splunk\_app*, car le modèle HTML pointe incorrectement vers le chemin du script de requête antérieur. Par conséquent, les tableaux de bord exécutent d'anciennes requêtes qui contiennent des champs tels que *vmw\_nsxt\_comp*, *vmw\_nsxt\_subcomp* et *vmw\_nsxt\_errorcode*, dont les noms ont été modifiés dans la nouvelle version du script de requête. Les requêtes ne renvoient donc aucun résultat et les tableaux de bord sont vides.

### Problèmes résolus des opérations et des services de surveillance

- **Problème 1957092** : Échec de l'initialisation du cluster de NSX Controller, car une erreur se produit lors du chargement de l'image Docker  
La commande `initialize control-cluster` échoue avec le message d'erreur `Control cluster activation timed out. Please try again.` Les informations du journal suivantes sont également présentes dans le syslog :  

```
<30>1 2017-08-03T22:52:41.258925+00:00 localhost load-zookeeper-image 1183 - -  
grpc: the connection is unavailable.
```

### Problèmes résolus de mise à niveau

- **Problème 1847884** : n'apportez pas de modifications liées à NSX-T Data Center avant la fin du processus de mise à niveau du plan de gestion  
L'exécution des modifications comme la création, la mise à jour ou la suppression d'une zone de transport, d'un nœud de transport ou de commutateurs logiques pendant la mise à niveau du plan de gestion risque d'endommager le plan de gestion, ce qui peut provoquer des échecs de NSX Edge, de l'hôte ou de la connectivité au chemin d'accès aux données.
- **Problème 2005709** : La page du coordinateur de mise à niveau devient inaccessible lorsque vous utilisez le nom de domaine complet de NSX Manager

Lorsque vous utilisez le nom de domaine complet de NSX Manager pour ouvrir l'interface utilisateur de NSX Manager, un message d'erreur semblable au message suivant s'affiche dans la page du coordinateur de mise à niveau : Cette page est uniquement disponible sur NSX Manager lorsque le coordinateur de mise à niveau est en cours d'exécution. Pour activer le service, exécutez la commande « `set service install-upgrade enabled` » sur NSX Manager. Si le service d'installation et de mise à niveau est déjà activé, désactivez-le à l'aide de la commande « `clear service install-upgrade enabled` », puis réactivez-le.

- **Problème 2022609 : Les hôtes gérés sont traités comme des hôtes non gérés dans le coordinateur de mise à niveau**  
Si un environnement comporte plus de 128 hôtes gérés, pendant le processus de mise à niveau, les hôtes qui faisaient partie d'un cluster apparaissent dans le groupe ESXi non géré.
- **Problème 1944731 : Les baux DHCP peuvent avoir des enregistrements conflictuels si de nombreuses demandes sont effectuées par la première instance de NSX Edge mise à niveau lors de la mise à niveau de la deuxième instance de NSX Edge**  
Si de nombreuses demandes sont effectuées par une première instance de NSX Edge mise à niveau lors de la mise à niveau de la deuxième instance de NSX Edge, les baux DHCP peuvent avoir des enregistrements conflictuels.

### Problèmes résolus de l'API

- **Problème 1619450 : un test vertical est renvoyé par l'API de configuration de la fréquence d'interrogation `GET /api/v1/hpm/features`**  
`GET /api/v1/hpm/features` renvoie la liste de toutes les fonctionnalités pour lesquelles la fréquence d'interrogation peut être configurée. Cette API renvoie certaines fonctionnalités internes destinées uniquement aux tests. Le seul impact fonctionnel pour l'utilisateur est un bruit supplémentaire.
- **Problème 1781225 : l'API `GET https://<NSX-Manager>/api/v1/fabric/nodes/<node-id>/modules` ne fonctionne pas pour Ubuntu**  
L'API `GET https://<NSX-Manager>/api/v1/fabric/nodes/<node-id>/modules` fonctionne pour ESXi et RHEL, mais pas pour Ubuntu.
- **Problème 1954990 : Renvoi d'un état inexact de l'API de réalisation**  
Si vous utilisez une API de réalisation pour vérifier l'état de réalisation de toutes les API exécutées avant une barrière, l'état renvoyé par l'API de réalisation peut prêter à confusion par rapport à l'état réel. En raison de la complexité de l'exécution du DFW dans le plan de gestion, les API DFW peuvent glisser après la barrière qu'elles sont censées suivre, ce qui entraîne cette imprécision.

### Problèmes résolus de NSX Container Plug-in (NCP)

- **Problème 2167491 : NCP ne parvient pas à démarrer si l'équilibreur de charge NSX-T utilise le nombre maximal de serveurs virtuels**  
Dans ConfigMap pour NCP, vous pouvez définir la taille de l'équilibreur de charge NSX-T sur petit, moyen ou grand. Le nombre maximal de serveurs virtuels est 10 pour un petit équilibreur de charge, 100 pour un équilibreur de charge moyen et 1 000 pour un grand équilibreur de charge. Si l'équilibreur de charge a le nombre maximal de serveurs virtuels, NCP ne démarre pas. Pour voir si l'équilibreur de charge a le nombre maximal de serveurs virtuels, depuis l'interface utilisateur graphique de NSX-T Manager, recherchez l'équilibreur de charge (il a une balise portant le nom du cluster) et comptez le nombre de serveurs virtuels.
- **Problème 2160806 : la mise à jour de la spécification TLS d'une entrée active lorsque NCP n'est pas en cours d'exécution n'est pas prise en charge**

Si NCP a attribué une adresse IP externe à une ressource d'entrée et que vous mettez à jour la spécification TLS de l'entrée lorsque NCP n'est pas en cours d'exécution, par exemple, en supprimant ou en modifiant le nom secret du paramètre, NCP ne détecte pas les modifications. Lorsque NCP est exécuté à nouveau, le certificat correspondant à l'ancien secret existe toujours et n'est pas supprimé.

## Problèmes connus

Les problèmes connus sont classés comme suit.

- [Problèmes connus généraux](#)
- [Problèmes connus d'installation](#)
- [Problèmes connus de NSX Manager](#)
- [Problèmes connus de NSX Edge](#)
- [Problèmes connus de mise en réseau logique](#)
- [Problèmes connus des services de sécurité](#)
- [Problèmes connus de mise en réseau KVM](#)
- [Problèmes connus d'équilibreur de charge](#)
- [Problèmes connus d'interopérabilité entre les solutions](#)
- [Problèmes connus des opérations et des services de surveillance](#)
- [Problèmes connus de mise à niveau](#)
- [Problèmes connus de l'API](#)
- [Problèmes connus de NSX Policy Manager](#)
- [Problèmes connus de NSX Cloud](#)
- [Problèmes connus de NSX Container Plug-in \(NCP\)](#)
- [Errata et ajouts de la documentation](#)

### Problèmes connus généraux

- **Problème 1842511 : BFD à tronçons multiples non pris en charge pour les itinéraires statiques**  
Dans NSX-T 2.0, BFD (Bidirectional Forwarding Detection) peut être activé pour un voisin BGP à tronçons multiples (MH-BGP). La capacité à sauvegarder un itinéraire statique à tronçons multiples avec BFD n'est pas configurable dans NSX-T 2.0, BGP uniquement. Notez que si vous avez configuré un voisin BGP à tronçons multiples sauvegardé par BFD et que vous configurez un itinéraire statique à tronçons multiples correspondant à la même valeur nexthop que le voisin BGP, l'état de session de BFD a un impact sur la session BGP et sur l'itinéraire statique.

Solution : aucune.

- **Problème 1931707 : La fonctionnalité de nœud de transport automatique nécessite que tous les hôtes du cluster disposent de la même configuration de PNIC**  
Lorsque la fonctionnalité de nœud de transport automatique est activée pour un cluster, un modèle de nœud de transport est créé et doit être appliqué à tous les hôtes de ce cluster. Tous les PNIC du modèle doivent être disponibles sur tous les hôtes pour la configuration du nœud de transport, sinon la configuration du nœud de transport peut échouer sur les hôtes où les PNIC étaient manquants ou occupés.

Solution : si la configuration du nœud de transport a échoué, reconfigurez le nœud de transport individuel pour la correction.

- **Problème 1909703 : Un administrateur NSX est autorisé à créer des itinéraires statiques, des règles NAT et des ports dans un routeur créé par OpenStack directement à partir du serveur principal**

Dans le cadre de la fonctionnalité RBAC dans NSX-T 2.0, les ressources, telles que les commutateurs, les routeurs, les groupes de sécurité créés par le plug-in OpenStack, ne peuvent pas être supprimées ou modifiées directement par un administrateur NSX à partir de l'interface utilisateur/API NSX. Ces ressources ne peuvent être modifiées/supprimées que par les API envoyées via le plug-in OpenStack. Il existe une limite à cette fonctionnalité. Actuellement, la seule limite imposée à un administrateur NSX est qu'il ne peut pas supprimer/modifier les ressources créées par OpenStack. Par contre, il est autorisé à créer des ressources, telles que des itinéraires statiques, des règles NAT dans les ressources existantes créées par OpenStack.

Solution : aucune.

- **Problème 1957072 : Le profil de liaison montante pour le nœud de pont doit toujours utiliser LAG pour plusieurs liaisons montantes**  
Lorsque vous utilisez plusieurs liaisons montantes qui ne sont pas montées vers LAG, le trafic n'est pas à équilibreur de charge et peut ne pas fonctionner correctement.

Solution : utilisez LAG pour plusieurs liaisons montantes sur des nœuds de pont.

- **Problème 1970750 : Le profil N-VDS du nœud de transport à l'aide du protocole LACP à temporisateurs rapides ne s'applique pas aux hôtes vSphere ESXi**  
Lorsqu'un profil de liaison montante LACP à taux rapides est configuré et appliqué à un nœud de transport vSphere ESXi sur NSX Manager, NSX Manager indique que le profil est appliqué correctement, mais l'hôte vSphere ESXi utilise le temporisateur lent LACP par défaut.

Sur vSphere Hypervisor, vous ne pouvez pas voir l'effet de la valeur lacp-timeout (SLOW/FAST) lorsque le profil de commutateur distribué (VDS-N) géré par NSX LACP est utilisé sur le nœud de transport à partir de NSX Manager.

Solution : aucune.

- **Problème 1989407 : Les utilisateurs vIDM disposant du rôle d'administrateur d'entreprise ne peuvent pas remplacer la protection des objets**  
L'utilisateur vIDM disposant du rôle d'administrateur d'entreprise ne peut pas remplacer la protection des objets, ni créer ou supprimer des identités de principal.

Solution : connectez-vous avec les privilèges d'administration.

- **Problème 2030784 : impossible de se connecter à NSX Manager avec un nom d'utilisateur distant qui contient des caractères non-ASCII.**  
Vous ne pouvez pas vous connecter au dispositif NSX Manager comme utilisateur distant avec un nom d'utilisateur contenant des caractères non-ASCII.

Solution : le nom d'utilisateur distant doit contenir des caractères ASCII lors de la connexion au dispositif NSX Manager.

Les caractères non-ASCII peuvent être utilisés si le nom d'utilisateur distant est configuré avec des caractères non-ASCII dans le serveur Active Directory.

- **Problème 2111047 : Application Discovery n'est pas pris en charge sur les hôtes VMware vSphere 6.7 dans la version 2.2 de NSX-T**  
L'exécution d'Application Discovery sur un groupe de sécurité comportant des machines virtuelles en cours d'exécution sur un hôte vSphere 6.7 provoque l'échec de la session Application Discovery.

Solution : aucune

- **Problème 2157370 : lors de la configuration de L3 Switched Port Analyzer (SPAN) avec troncation, un commutateur physique abandonne des paquets mis en miroir**

Lors d'une configuration de L3 SPAN qui inclut GRE/ERSPAN avec troncation, les paquets mis en miroir tronqués sont abandonnés en raison de la stratégie du commutateur physique. Il est possible que le port reçoive des paquets dans lesquels le nombre d'octets de charge utile ne correspond pas au champ de longueur type.

Solution : supprimez la configuration de troncation L3 SPAN.

- **Problème 216992** : les paquets mis en miroir avec l'adresse MAC de destination 02:50:56:56:44:52 provenant d'autres hôtes sont abandonnés par la liaison montante vSphere ESXi.  
Lorsque l'hôte reçoit des paquets mis en miroir avec l'adresse MAC 02:50:56:56:44:52 en provenance d'autres hôtes, la liaison montante vSphere ESXi abandonne ces paquets mis en miroir.

Solution : aucune

- **Problème 2174583** : dans l'assistant Démarrage, le bouton Configurer les nœuds de transport ne fonctionne pas correctement dans le navigateur Microsoft Edge  
Dans l'assistant Démarrage, après que vous cliquez sur le bouton Configurer les nœuds de transport, le navigateur Web Microsoft Edge échoue avec une erreur JavaScript.

Solution : utilisez plutôt le navigateur Firefox ou Google Chrome.

## Problèmes connus d'installation

- **Problème 1617459** : La configuration d'hôte pour Ubuntu ne prend pas en charge l'approvisionnement de fichiers de configuration de l'interface  
Si l'interface PNIC ne se trouve pas dans le fichier /etc/network/interfaces, MTU n'est pas configuré correctement dans le fichier de configuration réseau. Pour cette raison, la configuration MTU sur le pont de transport est perdue après chaque redémarrage.

Solution : déplacez la configuration de l'interface PNIC vers /etc/network/interfaces

- **Problème 1906410** : La tentative de suppression de l'hôte depuis l'interface utilisateur sans suppression préalable du nœud de transport entraîne un état incohérent de l'hôte  
La tentative de suppression de l'hôte depuis l'interface utilisateur sans suppression préalable du nœud de transport entraîne un état incohérent de l'hôte Si vous tentez de supprimer le nœud de transport lorsque l'hôte est dans un état incohérent, l'interface utilisateur ne vous permet pas de supprimer cet hôte.

Solution :

1. avant de supprimer le nœud de transport, procédez à la mise hors tension de toutes les machines virtuelles locataires déployées sur ce nœud.
2. Supprimez la zone de transport du nœud de transport.
3. Supprimez le nœud de transport.
4. Si le nœud de transport est supprimé correctement, supprimez l'hôte respectif.

En cas d'échec de la suppression du nœud de transport, suivez les étapes indiquées dans l'article <https://kb.vmware.com/s/article/52068> de la base de connaissances.

- **Problème 1957059** : L'annulation de la préparation de l'hôte échoue si l'hôte avec des VIB existants est ajouté au cluster lors de la tentative d'annulation de la préparation  
Si les VIB ne sont pas complètement supprimés avant d'ajouter les hôtes au cluster, l'opération d'annulation de la préparation de l'hôte échoue.

Solution : vérifiez que les VIB sur les hôtes sont complètement supprimés et redémarrez l'hôte.

- **Problème 2106956** : la jointure de deux instances de NSX Controller du même cluster à deux instances de NSX Manager distinctes entraîne des problèmes de chemins de données non définis

la jointure de deux instances de NSX Controller du même cluster NSX Controller à deux instances de NSX Manager distinctes entraîne des problèmes de chemins de données non définis

Solution : utilisez la commande `detach` de l'interface de ligne de commande du NSX Manager pour supprimer l'instance de NSX Controller du cluster NSX Controller. Reconfigurez le cluster NSX Controller afin que toutes les instances de NSX Controller du cluster soient enregistrées dans la même instance de NSX Manager.

Reportez-vous à la section Installation et mise en cluster de NSX Controller du Guide d'installation de NSX-TDataCenter.

- **Problème 2106973** : après l'initialisation du cluster NSX Controller sur l'ensemble des instances de NSX Controller, chaque NSX Controller devient un cluster NSX Controller à un nœud, ce qui provoque des problèmes de connectivité à de chemins de données non définis

Évitez d'initialiser le cluster NSX Controller sur l'ensemble des instances de NSX Controller, car chaque NSX Controller devient alors un cluster NSX Controller à un nœud, ce qui provoque des problèmes de connectivité à de chemins de données non définis. Initialisez le cluster NSX Controller sur la première instance de NSX Controller uniquement et joignez ensuite les autres instances de NSX Controller au cluster en exécutant la commande d'interface de ligne de commande `join control-cluster` sur la première instance de NSX Controller.

Solution : Reconfigurez votre cluster NSX Controller, comme décrit dans la section Installation et mise en cluster de NSX Controller du Guide d'installation de NSX-TDataCenter.

- **Problème 2114756** : dans certains cas, les VIB ne sont pas supprimés lorsqu'un hôte est supprimé du cluster NSX-T Data Center préparé

Lorsqu'un hôte est supprimé du cluster NSX-TData Center préparé, certains VIB peuvent rester sur l'hôte.

Solution : désinstallez manuellement les VIB de l'hôte.

- **Problème 2059414** : l'installation du bundle RHEL LCP échoue en raison d'une ancienne version de python-gevent RPM

Si un hôte RHEL contient une version plus récente de python-gevent RPM, l'installation du bundle RHEL LCP échoue, car NSX-T Data Center RPM contient une ancienne version de python-gevent RPM.

Solution : installez manuellement le bundle LCP sur l'hôte RHEL si l'hôte contient la dernière version de python-gevent RPM.

Procédez comme suit :

1. Extrayez le bundle RHEL LCP.
  2. Accédez au dossier du bundle LCP.
  3. Supprimer libev, python-greenlet et les RPM python-gevent du dossier LCP.
  4. Installez les RPM restants. Consultez le Guide d'Installation de NSX-T Data Center.
- **Problème 2142755** : L'installation des modules de noyau OVS échoue en fonction du miroir sur lequel la version du noyau RHEL 7.4 est en cours d'exécution  
L'installation des modules de noyau OVS échoue sur un hôte RHEL 7.4 exécutant un noyau de version 17.1 mineure ou version ultérieure. L'échec d'installation provoque l'arrêt du fonctionnement des chemins d'accès aux données du noyau, ce qui entraîne l'indisponibilité de la console de gestion de dispositifs.

Solution : mettez à niveau la version du noyau RHEL 7.4. Avec des privilèges d'administration, exécutez le script `/usr/share/openvswitch/scripts/ovs-kmod-manage.sh` sur l'hôte et rechargez les modules de noyau OVS.

- **Problème 1950583** : La sauvegarde planifiée de NSX Manager peut échouer après une mise à niveau du système vers NSX-T 2.0.0

Certains environnements NSX-T peuvent échouer à exécuter une sauvegarde planifiée après la mise à niveau d'une version précédente de NSX-T vers la version 2.0.0. Ce problème est dû à un changement du format d'empreinte digitale SSH des versions précédentes.

Solution : reconfigurez la sauvegarde planifiée.

- **Problème 1576112** : Des hyperviseurs KVM requièrent une configuration manuelle de la passerelle s'ils résident dans des segments de couche 2 différents

Si vous configurez un pool IP sur NSX Manager et que vous utilisez ce pool IP pour créer des nœuds de transport, les cases d'Ubuntu KVM n'affichent aucun itinéraire pour la passerelle qui a été configurée dans la configuration du pool IP. Par conséquent, le trafic de superposition entre les VM qui résident sur des hyperviseurs se trouvant dans des segments L2 différents échoue, car l'infrastructure sous-jacente ne sait pas comment atteindre les nœuds d'infrastructure dans les segments distants.

Solution : ajoutez un itinéraire pour la passerelle pour qu'elle puisse acheminer le trafic vers d'autres hyperviseurs qui résident dans des segments différents. Si cette configuration n'est pas faite manuellement, le trafic de superposition échoue, car le nœud d'infrastructure ne sait pas comment atteindre les nœuds d'infrastructure distants.

- **Problème 1710152** : L'interface utilisateur graphique de NSX Manager ne fonctionne pas dans Internet Explorer 11 en mode de compatibilité

Solution : allez dans Outils > Paramètres d'affichage de compatibilité et vérifiez qu'Internet Explorer n'affiche pas l'interface utilisateur graphique de NSX Manager en mode de compatibilité.

- **Problème 2128476** : la mise à l'échelle d'un inventaire de plus de 500 hôtes, 1 000 machines virtuelles et 10 000 VIF peut nécessiter environ 30 minutes pour effectuer une synchronisation complète après le redémarrage matériel

Après le redémarrage de NSX Manager, chaque hôte est synchronisé avec NSX Manager afin que celui-ci reçoive les données les plus récentes sur l'hôte, notamment des informations concernant les machines virtuelles présentes sur l'hôte et les VIF présents sur les machines virtuelles. Pour la mise à l'échelle d'un inventaire comportant plus de 500 hôtes, 1 000 machines virtuelles et 10 000 VIF, la synchronisation complète requiert environ 30 minutes.

Solution : attendez que les informations les plus récentes s'affichent dans NSX Manager après un redémarrage matériel.

Utilisez l'API `api/v1/fabric/nodes/<nodeid>/status` pour vérifier la propriété `last_sync_time`, qui indique l'heure de la dernière synchronisation d'un nœud spécifique.

- **Problème 1928376** : État dégradé du nœud de membre du cluster de contrôleur après la restauration de NSX Manager

Le nœud de membre du cluster de contrôleur peut devenir instable et signaler un état dégradé si NSX Manager est restauré sur une image de sauvegarde qui a été prise avant que ce nœud de membre soit détaché du cluster.

Solution : si l'appartenance au cluster change, vérifiez qu'une nouvelle sauvegarde de NSX Manager est effectuée.

- **Problème 1956088** : la modification de la vue de l'interface utilisateur du pare-feu lorsque le filtrage est appliqué dans l'ensemble de règles de la vue peut être perdue avant l'enregistrement sur Manager si les filtres sont annulés.

La modification de la vue de l'interface utilisateur du pare-feu lorsque le filtrage est appliqué dans l'ensemble de règles de la vue peut être perdue avant l'enregistrement sur Manager si les filtres sont annulés.

Solution : aucune.

- **Problème 1928447** : Les hyperviseurs avec des adresses IP de point de terminaison de tunnel virtuel en double ne sont pas enregistrés dans le journal système du nœud de plan de gestion  
Les hyperviseurs avec des adresses IP de point de terminaison de tunnel virtuel en double ne sont pas enregistrés dans le journal système du nœud de plan de gestion. Vérifiez que des adresses IP uniques sont attribuées aux points de terminaison de tunnel virtuel d'hyperviseurs et aux interfaces de liaison montante des nœuds NSX Edge.

Solution : aucune.

- **Problème 2125725** : après la restauration de déploiements de topologie volumineux, les données de recherche ne sont plus synchronisées et plusieurs pages de NSX Manager cessent de répondre

Après la restauration de NSX Manager avec des déploiements de topologie volumineux, les données de recherche ne sont plus synchronisées et plusieurs pages de NSX Manager affichent le message d'erreur `Une erreur irrécupérable est survenue.`

Solution : procédez comme suit :

1. Connectez-vous à l'interface de ligne de commande de NSX Manager en tant qu'administrateur.
2. Redémarrez le service de recherche.  
`redémarrez le service de recherche`  
Attendez au moins 15 minutes que le service de recherche achève la correction des différences de données en arrière-plan.

- **Problème 2128361** : la commande d'interface de ligne de commande servant à définir le niveau de journalisation de NSX Manager en mode de débogage ne fonctionne pas correctement  
L'utilisation de la commande d'interface de ligne de commande `set service manager logging-level debug` pour définir le niveau de journalisation de NSX Manager en mode de débogage ne permet pas de collecter les informations du journal de débogage.

Solution : procédez comme suit :

1. Connectez-vous à l'interface de ligne de commande de NSX Manager en tant qu'administrateur.
2. Exécutez la commande `st e` pour basculer en tant qu'utilisateur racine.
3. Copiez les fichiers `log4j2.xml.default` et `log4j2.xml`.  
`cp /opt/vmware/proton-tomcat/conf/log4j2.xml.default /opt/vmware/proton-tomcat/conf/log4j2.xml`
4. Modifiez la propriété du fichier `log4j2.xml`.  
`chown uproton:uproton /opt/vmware/proton-tomcat/conf/log4j2.xml`

- **Problème 1964681** : l'onglet Hôtes dans l'interface utilisateur de Manager affiche l'état Suppression en cours pour un hôte du nœud de transport même après la suppression de l'hôte  
Sous Fabric > Nœuds > Nœuds de transport dans l'interface utilisateur de Manager, après la suppression d'un hôte du nœud de transport, l'onglet Hôtes affiche toujours l'état Suppression en cours pour l'hôte.

Solution : actualisez le navigateur.

- **Problème 2169998** : Avec le navigateur Chrome, l'effacement des données de navigation lorsque vous êtes connecté à NSX Manager provoque l'arrêt du fonctionnement de l'interface utilisateur de Manager

Après la connexion à NSX Manager à l'aide du navigateur Chrome, si vous accédez aux paramètres du navigateur et effacez toutes les données de navigation, y compris toutes les informations de base et avancées, le navigateur perdra sa connexion à NSX Manager.

Solution : n'effacez pas les données de navigation lorsque vous êtes connecté à NSX Manager.



- **Problème 1765087** : Les interfaces de noyau que NSX Edge crée pour transférer des paquets entre le chemin de données et le noyau Linux ne prennent en charge que le MTU avec une valeur maximale de 1 600  
Les interfaces de noyau entre le chemin de données et le noyau ne prennent pas en charge la trame Jumbo. Les paquets BGP dont la taille dépasse 1 600 sont tronqués et abandonnés par le démon BGP. Les paquets SPAN dont la taille dépasse 1 600 sont tronqués et l'utilitaire de capture de paquets affiche un avertissement. La charge utile n'est pas tronquée et reste valide.

Solution : aucune.

- **Problème 1738960** : Si un nœud NSX Edge de profil de serveur DHCP est remplacé par un nœud NSX Edge d'un autre cluster, les adresses IP données aux VM par le serveur DHCP changent

Ce problème est causé par un manque de coordination entre le nœud qui est remplacé et le nouveau nœud.

Solution : aucune.

- **Problème 1629542** : Définir un retard de transfert sur un nœud NSX Edge unique entraîne l'affichage d'un état de routage incorrect  
Lors de l'exécution d'un dispositif NSX Edge en tant que nœud NSX Edge unique (pas dans une paire HA), la configuration d'un retard de transfert peut entraîner l'affichage incorrect de l'état de routage. Lorsque le retard de transfert est configuré, l'état de routage indique INACTIF jusqu'à l'expiration du délai de transfert. Si la convergence de routeur est terminée, mais que le délai de transfert n'est pas encore expiré, le chemin de données nord-sud continue à circuler comme prévu, même si l'état de routage indiqué est INACTIF. Vous pouvez ignorer cet avertissement sans risque.
- **Problème 1601425** : Impossible de cloner la VM NSX Edge qui est déjà enregistrée avec le cluster NSX Manager  
Le clonage d'une VM NSX Edge, une fois qu'elle est enregistrée avec le cluster NSX Manager, n'est pas pris en charge. Au lieu de cela, une nouvelle image doit être déployée.

Solution : aucune.

- **Problème 1585575** : Impossible de modifier les détails du cluster NSX Edge sur un routeur de niveau 1 attaché à un routeur de niveau 0  
Si vous avez activé NAT sur un routeur logique de niveau 1, vous devez spécifier un nœud NSX Edge ou un cluster NSX Edge avant de connecter le routeur de niveau 1 à un routeur de niveau 0. NSX ne prend pas en charge la modification des détails du cluster NSX Edge sur un routeur de niveau 1 qui est déjà attaché à un routeur de niveau 0.

Solution : pour modifier les détails du cluster NSX Edge sur un routeur de niveau 1 déjà attaché à un routeur de niveau 0, déconnectez le routeur de niveau 1 du routeur de niveau 0, procédez aux modifications et reconnectez-le.

- **Problème 1955830** : La mise à niveau de NSX-T 1.1 vers NSX-T 2.0 échoue lorsque le nom du cluster NSX Edge contient des caractères hauts ou non-ASCII  
Lorsqu'un cluster NSX Edge est nommé avec des caractères hauts ou non-ASCII dans la configuration de NSX-T 1.1, la mise à niveau de NSX-T 1.1 vers NSX-T 2.0 échoue avec une erreur de boucle infinie.

Solution : renommez les clusters NSX Edge pour supprimer les caractères hauts ou non-ASCII sur l'instance de configuration de NSX-T 1.1 avant la mise à niveau.

- **Problème 2122332** : Dans certains cas, la connexion SSH à un dispositif Edge bare-metal ne fonctionne pas  
Parfois, la connexion SSH à un dispositif Edge bare-metal ne fonctionne pas.

Solution : ouvrez une invite de commandes et accédez au pilote iLO. Redémarrez le service Edge SSH.

- **Problème 2187888** : un dispositif NSX Edge automatiquement déployé à partir de l'interface utilisateur de NSX Manager reste indéfiniment dans l'état Enregistrement en attente  
Un dispositif NSX Edge déployé à partir de l'interface utilisateur de NSX Manager reste indéfiniment dans l'état Enregistrement en attente. Dans cet état, le dispositif NSX Edge devient non disponible pour toute autre configuration.

Solution : utilisez l'interface de ligne de commande pour enregistrer manuellement le dispositif NSX Edge dans NSX Manager.

#### Problèmes connus de mise en réseau logique

- **Problème 1769922** : Le plan de cluster de NSX Controller peut afficher l'adresse IP interne 172.17.0.1 sur vSphere Client plutôt que l'adresse IP réelle  
Sur vSphere Client, l'adresse IP de NSX Controller affichée est 172.17.0.1 plutôt que l'adresse IP réelle. Pour NSX Manager, l'adresse IP s'affiche correctement.

Solution : aucune requise. Le fonctionnement n'est pas affecté par ce problème esthétique.

- **Problème 1771626** : Le changement de l'adresse IP du nœud NSX Controller n'est pas pris en charge

Solution : redéployez le cluster NSX Controller.

- **Problème 1940046** : Lorsqu'un même itinéraire statique est ajouté et publié dans plusieurs routeurs logiques de niveau 1, le trafic horizontal échoue  
Si le même itinéraire statique est ajouté et publié dans plusieurs routeurs logiques de niveau 1, le trafic horizontal échoue

Solution : les itinéraires statiques doivent être publiés uniquement depuis le routeur logique de niveau 1 d'origine si le préfixe se trouve derrière un réseau connecté du routeur distribué de niveau 1.

- **Problème 1753468** : L'activation du protocole STP (Spanning Tree Protocol) sur un VLAN ponté entraîne l'affichage de l'état Inactif pour le cluster de pont  
Lorsque le protocole STP est activé sur des VLAN utilisés pour le pontage avec l'association LACP, le port-canal de commutateur physique est bloqué ce qui entraîne l'affichage de l'état Inactif pour le cluster de pont sur l'hôte ESX.

Solution : désactivez STP ou activez le filtre BPDU et la protection BPDU.

- **Problème 1753468** : Le routeur logique de niveau 0 n'agrège pas les itinéraires, mais les redistribue individuellement  
Le routeur logique de niveau 0 n'effectue pas l'agrégation d'itinéraires pour un préfixe qui ne couvre pas tous les sous-préfixes qui y sont connectés. Au lieu de cela, le routeur logique distribue les itinéraires séparément

Solution : aucune.

- **Problème 1536251 : La copie de VM entre un hôte ESX et un autre attaché au même commutateur logique n'est pas prise en charge**  
Le réseau de couche 2 échoue lorsqu'une VM est copiée entre un hôte ESX et que la même VM est enregistrée sur un autre hôte ESX.

Solution : utilisez le clonage de VM si l'hôte ESX fait partie de Virtual Center.

Si vous copiez une VM entre des hôtes ESX, l'ID externe doit être unique dans le fichier .vmx de la VM pour que le réseau de couche 2 fonctionne.

- **Problème 1747485 : La suppression d'une liaison montante de l'interface LAG rend tout le protocole BFD inactif et bloque les itinéraires BGP**  
Lorsqu'une interface est supprimée de l'interface LAG configurée, elle désactive tous les protocoles BFD et bloque les itinéraires BGP, ce qui affecte le flux de trafic.

Solution : aucune.

- **Problème 1741929 : Dans un environnement KVM, lorsque la mise en miroir de ports est configurée et que la troncation est activée, les paquets Jumbo de la source sont envoyés en fragments, mais sont réassemblés à la destination du miroir**

Solution : aucune solution nécessaire, car le réassemblage est effectué par le pilote vNIC de la VM de destination.

- **Problème 1619838 : Le changement d'une connexion de zone de transport d'un routeur logique sur un groupe différent de commutateurs logiques échoue avec une erreur de non-correspondance**  
Le routeur logique ne prend en charge qu'une seule zone de transport de superposition pour les ports de liaison descendante. Par conséquent, sans la suppression des ports de liaison descendante ou de liaison de routeur existants, vous ne pouvez pas changer une connexion de zone de transport sur un groupe différent de commutateurs logiques.

Solution : Procédez comme suit.

1. Supprimez tous les ports de liaison descendante ou de liaison de routeur existants.
2. Attendez quelques minutes que le système se mette à jour.
3. Réessayez de changer la connexion de zone de transport sur un groupe différent de commutateurs logiques.

- **Problème 1625360 : Après la création d'un commutateur logique, NSX Controller peut ne pas afficher les informations sur le commutateur logique qui vient d'être créé**

Solution : attendez 60 secondes après la création du commutateur logique pour vérifier les informations sur le commutateur logique sur NSX Controller.

- **Problème 1581649 : Après la création et la suppression du commutateur logique, la plage de pool VNI ne peut pas être réduite**  
La réduction de plage échoue, car des VNI ne sont pas publiés juste après la suppression d'un commutateur logique. Les VNI sont publiés après 6 heures. Cela empêche la réutilisation de VNI lorsqu'un autre commutateur logique est créé. Pour cette raison, vous ne pouvez pas réduire ou modifier des plages jusqu'à 6 heures après la suppression du commutateur logique.

Solution : pour modifier la plage depuis laquelle les VNI ont été alloués pour les commutateurs logiques, attendez 6 heures après la suppression des commutateurs logiques. Vous pouvez également utiliser d'autres plages du pool VNI ou réutilisez la même plage sans réduire ou supprimer la plage.

- **Problème 1516253** : les cartes réseau Intel 82599 disposent d'une limite matérielle sur QBRC (Queue Bytes Received Counter) ce qui entraîne un dépassement de capacité après que le nombre total d'octets reçus dépasse 0xFFFFFFFF

À cause de la limite matérielle, la sortie de l'interface de ligne de commande de `get dataplane physical-port stats` ne correspond pas au nombre réel en cas de dépassement de capacité.

Solution : exécutez l'interface de ligne de commande une fois pour que le compteur soit réinitialisé et exécuté de nouveau après un délai plus court.

- **Problème 2075246** : le déplacement d'un routeur logique de niveau 1 à partir d'un routeur logique de niveau 0 vers un autre n'est pas pris en charge.  
Le déplacement d'un routeur logique de niveau 1 à partir d'un routeur logique de niveau 0 vers un autre routeur logique provoque une perte de connexion de la route du port de liaison descendante pour le routeur logique de niveau 1.

Solution : procédez comme suit :

1. Détachez le routeur logique de niveau 1 du routeur logique de niveau 0.
2. Attendez environ 20 minutes que le routeur logique de niveau 1 se détache complètement du routeur logique de niveau 0.
3. Attachez le routeur logique de niveau 1 à un autre routeur logique de niveau 0.  
La connexion de la route du port de liaison descendante est restaurée.

- **Problème 2077145** : dans certains cas, la tentative de suppression forcée du nœud de transport peut créer des nœuds de transport orphelins

Les tentatives de suppression du nœud de transport à l'aide d'un appel d'API lorsque, par exemple, il existe une défaillance matérielle et les hôtes deviennent irrécupérables, modifient l'état du nœud de transport sur Orphelin.

Solution : supprimez le nœud d'infrastructure avec le nœud de transport orphelin.

- **Problème 2099530** : la modification de l'adresse IP VTEP du nœud de pont entraîne l'indisponibilité du trafic

Lorsque l'adresse IP VTEP du nœud de pont est modifiée, la table MAC du VLAN pour la superposition n'est pas mise à jour sur les hyperviseurs distants, ce qui entraîne une indisponibilité du trafic sur une période pouvant atteindre 10 minutes.

Solution : lancez les modifications du trafic depuis le VLAN de sorte que la table MAC de superposition soit mise à jour sur les hyperviseurs.

- **Problème 2106176** : l'installation automatique de NSX Controller se bloque à l'étape En attente d'enregistrement lors de l'installation

Lors de l'installation automatique de NSX Controller en utilisant l'API ou l'interface utilisateur de NSX Manager, l'état de l'une des instances de NSX Controller en cours d'exécution se bloque et indique l'état En attente d'enregistrement indéfiniment.

Solution : procédez comme suit :

1. Envoyez une demande d'API pour rechercher l'ID de machine virtuelle associé à l'instance de NSX Controller bloquée.

```
https://<nsx-mgr>/api/v1/cluster/nodes/deployments
```

2. Envoyez une demande d'API pour supprimer l'instance de NSX Controller bloquée.

```
https://<nsx-mgr>/api/v1/cluster/nodes/deployments/<Controller id>?action=delete
```

- **Problème 2112459** : le remplacement d'un nœud unique dans le cluster de pont entraîne une perte de trafic

Lorsque vous remplacez un nœud unique dans le cluster de pont, le trafic de pont est soumis à l'ancien nœud, ce qui entraîne des pertes de trafic jusqu'à ce que les entrées de transfert des hyperviseurs distants soient mises à jour ou deviennent obsolètes.

Solution : procédez comme suit :

1. Placez le nœud de remplacement dans le cluster de pont.
2. Autorisez l'utilisation de la haute disponibilité.
3. Supprimez l'ancien nœud.

- **Problème 216992 : l'utilisation du paramètre MTU personnalisé d'un port logique peut entraîner un rejet de paquets**

Lorsque vous utilisez un paramètre MTU personnalisé sur des ports logiques, comme des valeurs non conformes pour un port de liaison montante de routeur logique ou certains routeurs logiques de niveau 0 et 1, cela peut entraîner un rejet de paquets. Le paramètre MTU par défaut est 1500.

Solution : utilisez le paramètre MTU par défaut.

Dans le cas contraire, le MTU appliqué sur des ports logiques différents doit se conformer à la relation suivante :

1. Définissez le MTU de la liaison montante du routeur logique de niveau 0 sur 8900.
2. Définissez le MTU du VTEP de NSX Edge sur 9000.
3. Définissez le MTU de la machine virtuelle sur 8900.

Le routeur logique de niveau 0 et tous les routeurs logiques de niveau 1 connectés au routeur logique de niveau 0 doivent être colocalisés sur les mêmes nœuds NSX Edge.

- **Problème 2125514 : après un basculement de pont de couche 2, le commutateur logique de certaines machines virtuelles NSX Edge peut effectuer une réplication BUM de chaque paquet jusqu'à ce que l'adresse MAC soit réapprise**

Après un basculement de pont de couche 2, le commutateur logique de certaines machines virtuelles NSX Edge peut effectuer une réplication BUM de chaque paquet pendant presque 10 minutes jusqu'à ce que l'adresse MAC soit réapprise pour le point de terminaison. Le système récupère de lui-même après que les points de terminaison ont généré la prochaine ARP.

Solution : aucune

- **Problème 2113769 : le relais DHCP n'est pas pris en charge lors du pontage de couche 2 d'un VLAN NSX Edge**

Lors de la connexion d'un hôte VLAN au VNI du commutateur logique via un port de pontage de couche 2 sur NSX Edge, l'agent de relais DHCP sur le port de routeur logique ne peut pas fournir d'adresse IP à l'hôte VLAN.

Solution : procédez comme suit :

1. Configurez l'hôte VLAN manuellement.
2. Déplacez le port de pontage de couche 2 vers l'hôte ESXi.

- **Problème 2183549 : lorsque vous modifiez un port de service centralisé, il est impossible de voir un commutateur logique VLAN récemment créé**

Dans l'interface utilisateur de Manager, après la création d'un port de service centralisé et un nouveau commutateur logique VLAN, si vous modifiez le port du service centralisé, vous ne pouvez pas avoir le commutateur logique VLAN récemment créé.

Solution : utilisez l'API pour modifier le port.

- **Problème 2160634 : la modification de l'adresse IP sur une boucle peut modifier l'adresse IP de l'ID de routeur sur une liaison montante**

Si l'adresse IP sur le bouclage est modifiée, le dispositif NSX Edge sélectionne l'adresse IP sur la liaison montante en tant qu'ID de routeur. L'adresse IP de la liaison montante qui est attribuée comme ID de routeur ne peut pas être modifiée.

**\*Impact pour le client\*** : 1. L'effet secondaire attendu de l'ID de routeur est que toutes les sessions BGP s'arrêteront, puis redémarreront.  
2. L'impact réel est le changement d'ID de routeur, qui peut rendre le débogage de BGP plus difficile et peut créer une confusion.

**Solution** : Désactivez la configuration de BGP et modifiez l'adresse IP sur le bouclage.

- **Problème 2186040** : Si un nœud de transport ne fait pas partie des 250 premiers profils de liaison montante du système, la liste déroulante de liaison montante des cartes réseau physiques est désactivée dans l'interface utilisateur  
Si un nœud de transport ne fait pas partie des 250 premiers profils de liaison montante du système, la liste déroulante des liaisons montantes de la carte réseau physique est désactivée dans l'interface utilisateur. L'enregistrement de la suppression du nom de transport entraîne la suppression du nom de la liaison montante du nœud de transport.

**Solution** : Sélectionnez à nouveau le profil de la liaison montante et le nom de la liaison montante pour ce nœud de transport.

- **Problèmes 2106635** : Pendant la création de routes statiques, la modification de la distance d'administration des routes NULL entraîne dans l'interface utilisateur la disparition du paramètre NULL du prochain tronçon  
Pendant la création de routes statiques, lorsque vous définissez Tronçon suivant sur NULL et modifiez la distance d'administration des routes NULL, le paramètre NULL du tronçon suivant disparaît de l'interface utilisateur.

**Solution** : sélectionnez à nouveau le tronçon suivant.

#### Problèmes connus des services de sécurité

- **Problème 1680128** : La communication DHCP entre le client et le serveur n'est pas chiffrée

**Solution** : utilisez IPSEC pour sécuriser davantage la communication.

- **Problème 1711221** : Les données IPFIX sont envoyées sur le réseau en texte brut  
Par défaut, l'option pour collecter les flux IPFIX est désactivée.

**Solution** : aucune.

- **Problème 1726081** : Le trafic de tunnel Geneve (UDP) est refusé dans KVM

**Solution** : procédez comme suit :

Si KVM utilise firewalld, créez un trou dans le pare-feu avec la commande suivante :

```
# firewall-cmd --zone=public --permanent --add-port=6081/udp
```

Si KVM utilise IPtables directement, créez un trou avec la commande suivante :

```
# iptables -A INPUT -p udp --dport 6081 -j ACCEPT
```

Si KVM utilise UFW, créez un trou avec la commande suivante :

```
# ufw allow 6081/udp
```

- **Les paquets de résiliation et de renouvellement DHCP n'atteignent pas le serveur DHCP**  
lorsque le client se trouve sur un réseau différent et que le service de routage est fourni par une machine virtuelle invitée

NSX-T ne peut pas distinguer si une machine virtuelle agit comme un routeur, donc il est possible que les paquets DHCP de monodiffusion acheminés via une machine virtuelle de routeur soient abandonnés, car le champ CHADDR dans le paquet ne correspond pas à l'adresse MAC source. Le champ CHADDR contient l'adresse MAC de la machine virtuelle du client DHCP, tandis que l'adresse MAC source est celle de l'interface de routeur.

Solution : si une machine virtuelle se comporte comme un routeur, désactivez **Bloc de serveur DHCP** dans les profils de sécurité de commutateur appliqués à tous les VIF de la machine virtuelle de routeur.

- **Problème 2108290 : des serveurs bare-metal comme nœuds de transport ne peuvent pas mettre en œuvre les fonctionnalités de sécurité de NSX-T Data Center**  
Les serveurs bare-metal utilisés comme nouveau type de nœud de transport n'offrent pas le même niveau d'assurance de sécurité, tel que la micro-segmentation, que d'autres charges de travail d'hyperviseur. En effet, une frontière fiable n'est pas appliquée entre les charges de travail d'application et NSX Agent.

Solution : Pour des raisons de sécurité, n'attribuez pas aux machines virtuelles de locataires le privilège racine pour les serveurs bare-metal ou n'exécutez pas les applications en tant que racine. Si des machines virtuelles de locataire disposent d'un tel accès, un compte ou une application de locataire compromis peut effectuer une activité malveillante sur le serveur bare-metal et introduire des problèmes dans le réseau de NSX-T Data Center.

- **Problème 2162722 : L'indice de popularité n'est pas applicable aux règles DROP ou REJECT, et aux règles sans état**  
Lorsque le trafic rencontre une règle avec une action DROP/REJECT ou une règle sans état, le nombre de sessions pour la règle n'est pas incrémenté comme « session » et est uniquement applicable à une règle ALLOW avec état. L'indice de popularité utilise le nombre de sessions comme paramètre clé et il ne change pas pour de telles règles.

Solution : aucune

- **Problème 2170512 : la commande d'interface de ligne de commande permettant d'obtenir des règles de pare-feu échoue si une interface comporte plus de 1 000 règles**  
Si une interface comporte plus de 1 000 règles, la commande d'interface de ligne de commande `get firewall <VIF_ID> ruleset rules` renvoie une chaîne vide.

Solution : Il existe deux solutions :

- Exécutez plutôt la commande « `nsxcli -c get firewall <VIF_ID> ruleset rules | json` ».
- Exécutez la commande d'interface de ligne de commande suivante. Le nom d'un fichier contenant le résultat s'affiche.

```
ovs-appctl -t /var/run/vmware/nsx-agent/nsxa-ctl dfw/rules
```

## Problèmes connus de mise en réseau KVM

- **Problème 1775916 : L'API de programme de résolution POST /api/v1/error-resolver?action=resolve\_error ne résout pas les erreurs après l'échec de l'ajout d'un hôte RHEL KVM à l'infrastructure**

Lorsqu'un hôte RHEL KVM ne peut pas être ajouté à l'infrastructure et que l'interface utilisateur de NSX Manager indique que son état d'installation est échoué, l'API de programme de résolution POST /api/v1/error-resolver?action=resolve\_error est exécutée pour résoudre les erreurs. Toutefois, le nouvel ajout de l'hôte à l'infrastructure entraîne les messages d'erreur suivants : échec de l'installation du logiciel sur l'hôte. Action d'exécution du plug-in de déploiement non gérée. Échec de la commande d'installation.

**Solution : Procédez comme suit.**

1. **Supprimez manuellement les packages suivants.**

```
rpm -e glog-0.3.1-1nn5.x86_64
rpm -e json_spirit-v4.06-1.el6.x86_64
rpm -e kmod-openvswitch-2.6.0.4557686-1.el7.x86_64
rpm -e nicira-ovs-hypervisor-node-2.6.0.4557686-1.x86_64
rpm -e nsx-agent-1.1.0.0.0.4690847-1.el7.x86_64
rpm -e nsx-aggservice-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-cli-1.1.0.0.0.4690892-1.el6.x86_64
rpm -e nsx-da-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-host-1.1.0.0.0.4690932-1.x86_64 rpm -e nsx-
host_node_status_reporter-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-lldp-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-logical_exporter-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-mpa-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-netcpa-1.1.0.0.0.4690924-1.el7.x86_64 rpm -e nsx-sfhc-
1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-support-bundle-client-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-transport_node_status-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsxa-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e openvswitch-2.6.0.4557686-1.x86_64
rpm -e openvswitch-selinux-policy-2.6.0.4557686-1.noarch
rpm -e python-simplejson-3.3.3-1.el7.x86_64
```

En cas d'erreur lors de l'exécution de la commande rpm -e, incluez l'indicateur --noscripts dans la commande.

2. Exécutez l'API de programme de résolution POST /api/v1/error-resolver?action=resolve\_error.
3. Ajoutez de nouveau l'hôte KVM à l'infrastructure.

- **Problème 1602470 : L'association d'équilibreur de charge n'est pas prise en charge sur KVM**
- **Problème 1611154 : Des VM dans un nœud de transport KVM ne peuvent pas atteindre des VM situées dans un autre nœud de transport**

Lorsque plusieurs pools IP sont utilisés pour des VTEP appartenant à différents réseaux, la VM sur l'hôte KVM peut ne pas atteindre la VM déployée sur d'autres hôtes disposant d'adresses IP VTEP d'un pool IP différent.

**Solution :** ajoutez des itinéraires pour que le nœud de transport KVM puisse atteindre tous les réseaux utilisés pour VTEP sur d'autres nœuds de transport.

Par exemple, si vous disposez de deux réseaux 25.10.10.0/24 et 35.10.10.0/24 et que le VTEP local dispose de l'adresse IP 25.10.10.20 avec la passerelle 25.10.10.1, vous pouvez utiliser la commande suivante pour ajouter l'itinéraire pour un autre réseau :

```
ip route add dev nsx-vtep0.0 35.10.10.0/24 via 25.10.10.1
```



- **Problème 1654999 : Le suivi de connexion du trafic de sous-couche réduit la mémoire disponible**

Lors de l'établissement d'un grand nombre de connexions entre les machines virtuelles, vous pouvez rencontrer les symptômes suivants.

Dans le fichier `/var/log/syslog` ou `/var/log/messages`, les entrées sont semblables à ce qui suit :

```
Apr 26 11:45:44 prmh-nsx-perf-server149 kernel: [1625289.950872] net_ratelimit: 239 callbacks suppressed
```

```
Apr 26 11:45:44 prmh-nsx-perf-server149 kernel: [1625289.950875] nf_conntrack: table full, dropping packet
```

```
Apr 26 11:45:44 prmh-nsx-perf-server149 kernel: [1625289.958436] nf_conntrack: table full, dropping packet
```

Le problème semble se manifester lorsque des règles de pare-feu par défaut ont été configurées. Le problème ne se manifeste pas si des règles de pare-feu ne sont pas configurées (par exemple : des commutateurs logiques sont placés dans la liste d'exclusion de pare-feu).

Remarque : les extraits de journal précédents ne sont que des exemples. Les variables de date, d'heure et d'environnement peuvent varier selon votre environnement.

Solution : ajoutez une règle de pare-feu pour désactiver le suivi de connexion pour UDP sur le port 6081 sur des périphériques de sous-couche.

Voici un exemple de commande :

```
# iptables -A PREROUTING -t raw -p udp --dport 6081 -j CT --notrack
```

Elle doit être configurée pour s'exécuter lors du démarrage. Si un gestionnaire de pare-feu est également activé sur la plate-forme (Ubuntu : UFW ; RHEL : firewalld), la règle équivalente doit être configurée via le gestionnaire de pare-feu. Consultez l'[article 2145463 connexe de la base de connaissances](#).

- **Problème 2002353 : L'utilisation de Linux Network Manager pour gérer les liaisons montantes de l'hôte KVM n'est pas prise en charge**

NSX-TData gère toutes les cartes réseau sur les hôtes KVM qui sont utilisés pour N-VDS. Une erreur de configuration se produit lorsque le gestionnaire de réseau est également activé pour ces liaisons montantes.

Solution : pour les hôtes Ubuntu, excluez les cartes réseau à utiliser pour NSX-TData à partir du Gestionnaire de réseau.

Avant d'activer NSX-TData sur un hôte Red Hat, modifiez le script de configuration de la carte réseau dans `/etc/sysconfig/network-scripts` avec `NM_CONTROLLED="no"`. Si NSX-TData a déjà été activé pour l'hôte, effectuez la même modification du script et redémarrez la mise en réseau de l'hôte.

- **Problème 2186045 : Sur KVM, par défaut, logrotate s'exécute quotidiennement plutôt qu'à chaque minute**

Sur KVM, si la taille d'un fichier journal dépasse la limite de taille définie dans sa stratégie de rotation basée sur une taille d'une journée, elle ne sera pas recyclée avant la fin de ce jour, lors de l'exécution de logrotate. Par conséquent, les tailles de fichiers journaux peuvent être supérieures à la limite définie.

Solution : suivez les étapes décrites ci-dessous :

1. Créez un nouveau répertoire `/etc/cron.minutes`.
2. Créez le script `/etc/cron.minutes/logrotate` avec le contenu suivant :

```
#!/bin/sh
/usr/sbin/logrotate /etc/logrotate.conf
```

3. Modifiez l'autorisation de `/etc/cron.minutes/logrotate` :

```
chmod 755 /etc/cron.minutes/logrotate
```

4. Ajoutez `cron.minutes` comme entrée dans `/etc/crontab` :

```
echo "* * * * * root cd / && run-parts --report /etc/cron.minutes"
>>/etc/crontab
```

## Problèmes connus d'équilibreur de charge

- **Problème 2010428 : Limitations de la création et de l'application des règles d'équilibreur de charge**

Dans l'interface utilisateur, vous pouvez créer une règle d'équilibreur de charge uniquement à partir du serveur virtuel. Les règles d'équilibreur de charge créées à l'aide de l'API REST ne peuvent pas être connectées au serveur virtuel dans l'interface utilisateur.

Solution : si vous avez créé une règle d'équilibreur de charge à l'aide de l'API REST, attachez cette règle d'équilibreur de charge au serveur virtuel à l'aide de l'API REST. Les règles créées à l'aide de l'API REST s'affichent désormais dans le serveur virtuel à partir de l'interface utilisateur.

- **Problème 2016489 : LCP ne parvient pas à configurer le certificat par défaut lorsque l'indication du nom de serveur est sélectionnée**

L'ID de certificat par défaut devrait être défini en premier dans la liste de certificats lorsque plusieurs ID de certificat sont utilisés dans l'indication du nom de serveur (SNI), afin d'éviter que LCP n'ignore le certificat par défaut.

Solution : le certificat par défaut doit être défini en premier dans la liste de certificats SNI.

- **Problème 2115545 : lorsqu'un contrôle de santé de l'équilibreur de charge est activé, la connectivité directe des membres du pool de serveurs principal peut échouer**

Si un équilibreur de charge est attaché à un routeur logique, un client connecté à la liaison descendante du routeur logique ne peut pas accéder aux membres du pool en utilisant le même protocole que le contrôle de santé si les membres du pool sont accessibles à l'aide de la liaison montante du routeur logique.

Par exemple, si un équilibreur de charge est attaché au routeur logique LR1 et que le contrôle de santé ICMP est activé pour les membres du pool accessibles via une liaison montante LR1, un client situé sur la liaison descendante LR1 ne peut pas envoyer directement de ping à ces membres. Toutefois, ce client peut utiliser d'autres protocoles (tels que SSH ou HTTP) pour communiquer avec le serveur.

Solution : utilisez un différent type de contrôle de santé sur l'équilibreur de charge. Par exemple, pour pouvoir exécuter une commande ping sur le serveur principal, utilisez le contrôle de santé TCP ou UDP plutôt que le contrôle de santé ICMP.

- **Problème 2128560 : la configuration du routage automatique SNAT et du contrôle de santé de l'équilibreur de charge peut entraîner des contrôles de santé occasionnels ou des échecs de connexion**

La configuration du routage automatique SNAT et du contrôle de santé de l'équilibreur de charge avec TCP, HTTP, HTTPS ou UDP pour le même pool de serveurs peut entraîner des contrôles de santé occasionnels ou des échecs de connexion à ce pool de serveurs.

Solution : utilisez la liste d'adresses IP SNAT au lieu du routage automatique SNAT.

**Remarque :** les adresses IP SNAT spécifiées dans le mode de liste des adresses IP SNAT ne doivent pas inclure l'adresse IP de la liaison montante du routeur logique.

Par exemple, si un équilibreur de charge est attaché au routeur logique de niveau 1 LR1, la plage d'adresses IP SNAT spécifiée ne doit pas inclure l'adresse IP de la liaison montante de LR1.

## Problèmes connus d'interopérabilité entre les solutions

- **Problème 1588682** : Mettre les hôtes ESXi en mode verrouillage désactive l'utilisateur nsx-user  
Lorsqu'un hôte ESXi est mis en mode verrouillage, l'utilisateur vpxuser est le seul utilisateur à pouvoir s'authentifier avec l'hôte ou à exécuter des commandes. NSX-TData s'appuie sur un autre utilisateur, nsx-user, pour effectuer toutes les tâches associées à NSX-TData sur l'hôte.

Solution : n'utilisez pas le mode verrouillage. Consultez [Mode verrouillage](#) dans la documentation de vSphere.

## Problèmes connus des opérations et des services de surveillance

- **Problème 1749078** : Après la suppression d'une VM locataire sur un hôte ESXi et le nœud de transport hôte correspondant, la suppression de l'hôte ESXi échoue  
La suppression d'un nœud hôte implique la reconfiguration de divers objets et peut prendre plusieurs minutes.

Solution : attendez plusieurs minutes et réessayez l'opération de suppression. Répétez si nécessaire.

- **Problème 1761955** : Impossible de connecter la vNIC d'une machine virtuelle à un commutateur logique de NSX-T Data Center après l'enregistrement de la machine virtuelle  
Si un fichier VMX existant est utilisé pour enregistrer une VM sur un hôte ESXi, l'opération d'enregistrement ignore les erreurs spécifiques à vNIC suivantes :

- vNIC configurées avec une sauvegarde de réseau non valide.
- Échecs d'association de VIF pour des vNIC connectées à un commutateur logique NSX-T.

Solution : Procédez comme suit.

1. Créez un groupe de ports temporaire sur un vSwitch standard.
2. Attachez les vNIC avec l'état déconnecté au nouveau groupe de ports et marquez-les comme connectées.
3. Attachez les vNIC à un commutateur logique NSX-T Data Center valide.

- **Problème 1774858** : Très rarement, le cluster NSX Controller devient inactif après avoir été exécuté pendant plusieurs jours  
Lorsque le cluster NSX Controller devient inactif, tous les nœuds de transport et les nœuds NSX Edge perdent la connectivité aux instances de NSX Controller et il n'est pas possible de modifier la configuration. Toutefois, le trafic des données n'est pas affecté.

Solution : Procédez comme suit.

- Résolvez les problèmes de latence de disque, s'il en existe.
- Redémarrez le service cluster-mgmt sur tous les NSX Controller.

- **Problème 1576304** : Le nombre d'octets abandonnés n'est pas inclus dans le rapport Statut et statistiques du port  
Lorsque /api/v1/logical-ports/<port-id>/statistics ou NSX Manager est utilisé pour afficher le statut et les statistiques du port logique, la valeur du nombre de paquets abandonnés est de 0. Cette valeur n'est pas précise. Quel que soit le nombre de paquets abandonnés, le nombre affiché ici est toujours vide.

Solution : aucune.

- **Problème 1955822** : Le fichier csv de rapports sur l'utilisation de la licence doit également inclure les CPU, le droit de machine virtuelle et l'utilisation réelle  
Lors de la recherche dans un rapport sur l'utilisation des licences (via API/interface utilisateur), les données ne contiennent que l'utilisation actuelle.

Solution : recherchez les limites d'utilisation autorisées par la ou les licences actuelles via l'interface utilisateur ou REST API :

Méthode : GET; URI: /api/v1/licenses

- **Problème 2081979** : un hôte du nœud de transport ne peut pas se connecter à un contrôleur  
Le journal de proxy NSX affiche les informations suivantes. Un message « validation du certificat » est attendu mais n'est pas présent.

```
TCP connection started: 10.171.0.73:0::3a4de8a2-3bc1-41ea-a94d-c1427d8cd757:1234
Doing SSL handshake
TCP connection established: 10.171.0.73:0::3a4de8a2-3bc1-41ea-a94d-c1427d8cd757,
local addr: 10.171.0.59:36048, remote addr: 10.171.0.73
```

Solution : connectez-vous à un contrôleur en tant qu'administrateur et exécutez les commandes suivantes :

```
set debug
get mediator forcesync
```

## Problèmes connus de mise à niveau

- **Problème 1930705** : Échec de migration par vMotion de machines virtuelles connectées aux commutateurs logiques lors de la mise à niveau du plan de gestion  
Lors de la mise à niveau du plan de gestion, la tentative de migration par vMotion des machines virtuelles connectées à un commutateur logique échoue.

Solution : attendez la fin de la mise à niveau du plan de gestion et réessayez le processus de migration par vMotion.

- **Problème 2005423** : Les nœuds KVM mis à niveau depuis une version précédente de NSX-T ne sont pas modifiés automatiquement pour utiliser balance-tcp  
NSX-T ne modifie pas automatiquement le mode de liaison d'une liaison montante d'un hôte KVM mis à niveau depuis active-backup vers balance-tcp.

Solution : modifiez le nœud de transport, même s'il n'y a eu aucune modification de la configuration, afin de corriger le paramètre du mode.

- **Problème 2101728** : la mise à niveau de NSX Edge est parfois mise en pause après la mise à niveau réussie d'un groupe NSX Edge  
La mise à niveau du groupe NSX Edge a été réussie. Cependant, le processus est mis en pause lors de la seconde mise à niveau du groupe NSX Edge.

Solution : cliquez sur Continuer pour poursuivre la mise à niveau du groupe NSX Edge.

- **Problème 2106257** : le workflow d'acceptation de l'API CLUF est modifié pour la mise à niveau de NSX-T 2.1 vers NSX-T 2.2  
L'acceptation de l'API EULA doit être appelée après la mise à jour du coordinateur de mise à niveau et avant la mise à niveau des hôtes existants.

Solution : aucune

- **Problème 2108649** : la mise à niveau échoue si des fichiers ou des répertoires sont ouverts dans la partition sur laquelle s'exécute la mise à niveau  
Évitez de conserver des fichiers ou des répertoires ouverts dans la partition (par exemple, NSX Manager ou NSX Controller) qui vont être mis à niveau, car cela entraîne l'échec du processus de mise à niveau.

Solution : redémarrez le dispositif sur lequel la défaillance s'est produite et recommencez le processus de mise à niveau.

- **Problème 2116020** : après la mise à niveau de NSX-T 2.1 vers NSX-T 2.2, certains modules Ubuntu KVM obsolètes ne sont pas supprimés  
Après la mise à niveau de NSX-T 2.1 vers NSX-T 2.2, les modules Ubuntu KVM obsolètes suivants ne sont pas supprimés.

- nsx-host-node-status-reporter
- nsx-lldp
- nsx-logical-exporter
- nsx-netcpa
- nsx-support-bundle-client
- nsx-transport-node-status-reporter
- nsxa

Solution : Procédez comme suit.

1. Créez un fichier temporaire dans le répertoire /etc/vmware/nsxa/.

```
cd /etc/vmware/nsxa  
touch temp.txt
```

2. Répertoriez tous les fichiers et répertoires du module nsxa.

```
dpkg -L nsxa  
/etc/vmware/nsxa# ls
```

3. Supprimez les packages suivants.

- a) `dpkg --purge nsx-lldp`
- b) `dpkg --purge nsx-support-bundle-client`
- c) `dpkg --purge nsx-transport-node-status-reporter`
- d) `dpkg --purge nsx-logical-exporter`
- e) `dpkg --purge nsx-netcpa`
- f) `dpkg --purge nsxa`
- g) `dpkg --purge nsx-host-node-status-reporter`

4. Vérifiez que le répertoire suivant est disponible.

```
/etc/vmware/nsxa/
```

5. Supprimez le fichier temp.txt du répertoire /etc/vmware/nsxa/.

```
rm -f temp.txt
```

- **Problème 2164930** : la mise à niveau du plan de gestion se termine et affiche un état suspendu en présence d'un groupe d'unités de mise à niveau d'hôte vide  
L'état de mise à niveau du plan de gestion global s'affiche comme étant mis en pause et l'état de mise à niveau de l'hôte n'est pas marqué à 100 % lorsqu'un groupe d'unités de mise à niveau d'hôte vide est présent.

**\*Impact pour le client\*** : Si le client a des groupes d'hôtes vides pendant une mise à niveau, l'état de mise à niveau indique EN PAUSE à la fin de la mise à niveau MP.

Solution : supprimez le groupe d'unités de mise à niveau d'hôte vide avant de mettre à niveau le plan de gestion.

Si le plan de gestion est mis à niveau, supprimez le groupe d'unités de mise à niveau d'hôte vide et redémarrez `install-upgrade service` à l'aide de l'interface de ligne de commande.

- **Problème 2097094** : l'annulation dans le téléchargement de bundle de mise à niveau en cours de téléchargement n'est pas prise en charge  
Vous ne pouvez pas annuler l'opération de téléchargement lors du téléchargement du fichier.mub du bundle de mise à niveau.

Solution : attendez la fin du téléchargement du fichier .mub du bundle de mise à niveau.

- **Problème 2122242** : la mise à niveau d'un hôte Ubuntu KVM de NSX-T 2.1 vers NSX-T 2.2 ou vers NSX-T Data Center 2.3 ne supprime pas le module nsx-support-bundle-client

Lors de la mise à niveau d'un hôte Ubuntu KVM de NSX-T 2.1 vers une version plus récente (NSX-T 2.2 ou NSX-T Data 2.3), le module `nsx-support-bundle-client` est toujours installé, même s'il n'est plus utilisé. Les utilisateurs peuvent voir que le module est toujours installé en exécutant des commandes telles que `/usr/bin/dpkg -l`.

Solution : Connectez-vous en tant qu'utilisateur racine et exécutez la commande suivante pour supprimer manuellement le module :

```
# /usr/bin/dpkg --purge nsx-support-bundle-client
```

- **Problème 2186957 : un hôte ESXi ne sort pas du mode de maintenance après une mise à niveau**  
Un hôte ESXi ne sort pas du mode de maintenance après une mise à niveau si le cluster n'a qu'un seul hôte et si la précédente tentative de mise de l'hôte en mode de maintenance par le coordinateur de mise à niveau a échoué.

Solution : sortez manuellement l'hôte du mode de maintenance ou assurez-vous que l'hôte peut entrer en mode de maintenance (vous devez disposer d'au moins 2 hôtes par cluster).

- **Problème 2166207 : pendant la mise à niveau de NSX-T Data Center 2.2 vers NSX-T Data Center 2.3 avec 500 hyperviseurs, le processus global de mise à niveau peut rester indéfiniment dans l'état EN COURS**  
Pendant la mise à niveau de NSX-T Data Center 2.2 vers NSX-T Data Center 2.3 avec 500 hyperviseurs, le processus global de mise à niveau peut rester indéfiniment dans l'état EN COURS après que vous avez cliqué sur Pause, puis procédé à plusieurs actualisations du navigateur Web.

Solution : connectez-vous à l'interface de ligne de commande de NSX-T Data Center sur NSX Manager. Tapez la commande, `install-upgrade` pour redémarrer le service.

- **Problème 2113681 : si un hôte KVM devient inaccessible et échoue après la mise à niveau de NSX Edge, le coordinateur de mise à niveau tente de mettre à niveau l'hôte ayant échoué plutôt que de procéder à la mise à niveau des nœuds NSX Controller**  
Après la mise à niveau de l'hôte KVM et de NSX Edge, la désinstallation du nouveau RPM et l'installation d'un ancien RPM sur l'hôte, l'hôte devient indisponible dans le coordinateur de mise à niveau. Par conséquent, le coordinateur de mise à niveau tente de mettre à niveau l'hôte KVM au lieu de poursuivre la mise à niveau des nœuds de contrôleurs NSX.

Solution : actualisez l'interface utilisateur du coordinateur de mise à niveau, cliquez sur l'onglet Hôtes et tentez de mettre à niveau l'hôte KVM.

Vous pouvez également ignorer la mise à niveau de l'hôte KVM, ouvrir une invite de commandes et taper la commande, `curl -i -k -u admin -X POST https://<nsx-manager-ip-address>/api/v1/upgrade/plan?action=continue\&skip=true`

## Problèmes connus de l'API

- **Problème 1605461 : Les journaux de l'API NSX-T dans Syslog indiquent des appels API internes au système. NSX-T journalise dans Syslog les appels API effectués par l'utilisateur et par le système**  
La journalisation d'un événement d'appel API dans Syslog n'est pas la preuve qu'un utilisateur appelle directement l'API NSX-T. Vous pouvez voir des appels API de NSX Controller et de NSX Edge dans les journaux, même si ces dispositifs NSX-T ne disposent pas d'un service API exposé publiquement. Ces services API privés sont utilisés par d'autres services NSX-T, tels que l'interface de ligne de commande de NSX-T.

Solution : aucune.

- **Problème 1641035** : L'appel REST à `POST/hpm/features/<feature-stack-name? action=reset_collection_frequency>` ne restaure pas la fréquence de collecte pour les statistiques de remplacement  
Si vous tentez de réinitialiser la fréquence de collecte à sa valeur par défaut à l'aide de cet appel REST, cela ne fonctionne pas.  
Solution : utilisez `PUT /hpm/features/<feature-stack-name>` et définissez la fréquence de collecte sur la nouvelle valeur.
- **Problème 1648571** : Les requêtes sur demande d'état et de statistiques peuvent échouer par intermittence. Le code d'échec HTTP est incohérent  
Dans certaines situations, les requêtes sur demande échouent. Il arrive que ces requêtes échouent avec une erreur HTTP 500 au lieu d'une erreur HTTP 503, même si l'appel API réussit lors de la nouvelle tentative.  
Pour les API de statistiques, la condition de délai d'expiration peut entraîner de faux journaux d'erreur de routage de message. Ces journaux sont produits parce que la réponse est renvoyée après l'expiration du délai d'expiration.  
Par exemple, des erreurs comme les suivantes peuvent se produire :  
`java.lang.IllegalArgumentException: Unknown message handler for type com.vmware.nsx.management.aggr.messaging.AggService$OnDemandStatsResponseMsg.`  
Pour les API d'état, la condition de délai d'expiration, une réponse renvoyée après le délai d'expiration, peut entraîner la mise à jour prématurée du cache.

Solution : réessayez la requête API.

- **Problème 1963850** : L'API GET affiche des éléments triés en respectant la casse  
Lorsqu'une API GET renvoie des éléments qui sont triés par nom complet, le tri est sensible à la casse.  
Solution : aucune.
- **Problème 2070136** : Une API de pare-feu distribué qui traite une grande quantité de données échoue  
Une API de pare-feu distribué qui doit créer ou mettre à jour plus de 100 Mo de données échoue avec le code d'erreur 500 et un message indiquant qu'une transaction a échoué. L'API implique généralement une section comportant plus de 1 000 règles, chaque règle impliquant de nombreuses sources, destinations et objets cibles.  
Solution : créez ou mettez à jour les règles de façon incrémentielle.
- **Problème 1895497** : l'algorithme d'équilibreur de charge SRCDESTMACIPPORT dans l'API ne fonctionne pas  
L'appel d'une API pour créer un profil de liaison montante d'un nœud de transport avec LAG comportant l'adresse MAC, l'adresse IP et le port TCP/UDP source et de destination va échouer.  
Solution : aucune

## Problèmes connus de NSX Policy Manager

- **Problème 2057616** : lors de la mise à niveau de NSX Policy Manager depuis NSX-T 2.1 vers NSX-T 2.2, les NSServices et NSGroups non pris en charge ne sont pas transférés  
Les NSServices non pris en charge de type Ether et les NSGroups avec un ensemble d'adresses MAC et des critères d'appartenance à un port logique ne sont pas transférés lors de la mise à niveau de NSX Policy Manager depuis NSX-T 2.1 vers NSX-T 2.2.

Solution : Procédez comme suit.

1. Dans NSX-T 2.1, supprimez et modifiez les NSServices de type Ether utilisés dans toute entrée de communication.
2. Supprimez et modifiez les NSGroups avec un ensemble d'adresses MAC et des critères d'appartenance à un port logique utilisés dans toute entrée de communication.

3. Mettez à niveau NSX Manager depuis NSX-T 2.1 vers NSX-T 2.2.
  4. Mettez à niveau NSX Policy Manager en utilisant l'interface de ligne de commande.
- **Problème 2116117 : l'onglet topologie de NSX Policy Manager de l'interface utilisateur affiche le message Échec des connexions de données**  
L'onglet topologie de NSX Policy Manager de l'interface utilisateur affiche le message Échec des connexions de données, car les groupes du domaine de stratégie contiennent des machines virtuelles hébergées sur la version 6.7 d'ESXi, qui n'est pas prise en charge.

*Solution* : aucune

- **Problème 2126647 : les mises à jour simultanées du pare-feu distribué de NSX Policy Manager provoquent un remplacement**  
Lorsque deux utilisateurs modifient simultanément la section de pare-feu distribué de NSX Policy Manager, la modification du dernier utilisateur remplace les modifications effectuées précédemment par l'autre utilisateur.

*Solution* : rétablissez les modifications du pare-feu distribué effectuées par le premier utilisateur. Une fois les modifications enregistrées, le deuxième utilisateur peut effectuer des modifications.

## Problèmes connus de NSX Cloud

- **Problème 2112947 : lors de la mise à niveau des agents NSX Agent dans Cloud Service Manager (CSM), certaines instances peuvent afficher l'état Échec**  
Lors de la mise à niveau des agents NSX Agent dans CSM, certaines instances peuvent afficher l'état Échec car l'interface utilisateur ne répond pas.

*Solution* : actualisez l'interface utilisateur.

- **Problème 2111262 : lors du déploiement de la PCG, vous pouvez voir le message d'erreur : « Gateway deployment failed: [Errorcode: 60609] Async operation failed with provisioning state: Failed. » ou « Failed to create gateway virtual machine with name nsx-gw, Gateway deployment failed. »**  
Cette situation est rare et se produit en raison de l'infrastructure Microsoft Azure.

*Solution* : redéployez la passerelle de cloud public (PCG) en échec.

- **Problème 2110728 : si vous utilisez HA, mais avez installé NSX Agent sur des machines virtuelles en ne spécifiant que le nom DNS de la PCG à l'aide l'option --gateway, le basculement vers la PCG secondaire ne fonctionne pas.**  
Les machines virtuelles de charge de travail ne sont pas en mesure de se connecter à la PCG après basculement, et la PCG ne pourra donc pas appliquer ou détecter tout état logique sur la machine virtuelle.

*Solution* : N'utilisez jamais l'option `--gateway` lors de l'installation d'agents sur les machines virtuelles de charge de travail. Utilisez la valeur de l'écran de la passerelle du VPC ou VNet. Reportez-vous à **Installation de NSX Agent** dans le Guide d'administration de NSX-T Data Center pour plus de détails.

- **Problème 2071374 : des messages d'erreur anodins contenant « nscd » peuvent s'afficher lorsque vous installez NSX Agent sur certaines instances de machine virtuelle Linux**  
Description : sur les machines virtuelles sur lesquelles « nscd » est en cours d'exécution, vous verrez des messages d'erreur similaires à : « sent invalidate(passwd) request, exiting » lors de l'installation de NSX Agent. Cela se produit notamment sur les machines virtuelles exécutant Ubuntu 14.04 ou 16.04

*Solution* : les messages s'affichent en raison d'un bogue connu avec la distribution Linux. Ces messages sont inoffensifs et n'affectent pas l'installation de NSX Agent.

- **Problème 2010739 : les deux passerelles de cloud public (PCG) sont signalées comme étant en**



## veille

Si la PCG principale ne peut pas se connecter au contrôleur au cours de l'intégration de passerelle, les deux passerelles (primaire et secondaire) seront en mode veille jusqu'à ce que la connexion entre le contrôleur et la passerelle soit restaurée.

- **Problème 2121686** : CSM affiche l'exception « Le serveur n'a pas pu authentifier la demande. » Cette erreur s'affiche dans CSM et est due à une absence de synchronisation entre l'heure du dispositif CSM et celle du serveur de stockage Microsoft Azure ou NTP. Dans ce cas, Microsoft Azure renvoie l'exception « Le serveur n'a pas pu authentifier la demande. » qui est ambiguë, car la même erreur s'affiche dans CSM.

*Solution* : synchronisez l'heure du dispositif CSM avec celle du serveur de stockage NTP ou Microsoft Azure.

- **Problème 2092378** : le déploiement d'une PCG en mode HA affiche les deux PCG en mode veille et Cloud Sync indique que la PCG principale est active  
Après le déploiement d'une PCG en mode HA via CSM dans un réseau privé, l'état Veille/Veille ou Actif/Actif est affiché sur les PCG déployées pendant 1 heure au maximum. Pendant cet intervalle, l'utilisateur peut penser qu'un problème existe avec la PCG déployée et que l'état n'est pas suffisamment clair pour continuer.

*Solution* : Procédez comme suit :

1. Resynchronisez le compte à partir de l'interface utilisateur après le déploiement de la PCG via laquelle CSM peut extraire les données les plus récentes et les afficher.
  2. Si après la resynchronisation, CSM affiche toujours des PCG dans un état incorrect, vérifiez l'état de la connectivité des PCG dans NSX Manager.
  3. Si la connexion est ACTIVE et que les états sont toujours incorrects, poursuivez le débogage des PCG.
- **Problème 2119726** : lors du déploiement d'une PCG dans un réseau virtuel Microsoft Azure, les adresses IP publiquement précédemment associées aux machines virtuelles peuvent être signalées de manière incorrecte pour libre utilisation.  
Si les machines virtuelles auxquelles les adresses IP publiques ont été attribuées précédemment sont actuellement hors tension, ces adresses IP publiques ne leur sont plus associées. Cela est dû à la dissociation qu'effectue Microsoft Azure des adresses IP publiques associées aux machines virtuelles après une certaine période passée hors tension. Cette période n'est pas définie spécifiquement par Microsoft Azure.

*Solution* : ne mettez pas hors tension les PCG de votre réseau virtuel. Cela empêche la dissociation entre les adresses IP publiques et l'interface de liaison montante de la PCG principale. Si vous devez mettre hors tension les PCG, assurez-vous que les adresses PIP associées aux PCG ne sont pas réutilisées et que lorsque les PCG sont mises sous tension à nouveau, celles-ci disposent de la même adresse PIP.

- **Problème 2165915** : prise en charge de NSX Cloud pour Red Hat Enterprise Linux 7.4 avec `kmod.x86_64 0:20-15.el7_4.6`  
NSX Cloud ne prend pas en charge les instances de machines virtuelles qui exécutent Red Hat Enterprise Linux 7.4 avec `kmod-20-15.el7_4.6`. Cela est dû à un bogue signalé par Red Hat : [https://bugzilla.redhat.com/show\\_bug.cgi?id=1522994](https://bugzilla.redhat.com/show_bug.cgi?id=1522994).

*Solution* : effectuez la mise à jour vers la version `kmod` dans laquelle ce bogue est corrigé pour permettre l'installation de NSX Agent.

- **Problème 2102828** : dans les déploiements de Microsoft Azure, pendant et après la mise à niveau de NSX-T 2.2 vers NSX-T Data Center 2.3, la passerelle PCG (Public Cloud Gateway) peut sembler être non opérationnelle.

Dans les déploiements de Microsoft Azure où le système a été mis à niveau de NSX-T 2.2 vers NSX-T Data Center 2.3, dans de rares cas, la passerelle PCG (Public Cloud Gateway) risque de ne pas parvenir à obtenir des adresses IP sur ses interfaces. Cela peut se produire lors d'une mise à niveau à l'étape PCG où le processus de mise à niveau de la PCG semble se bloquer. Ce problème peut également prendre la forme d'une PCG non opérationnelle si l'administrateur redémarre le dispositif PCG à partir du portail Microsoft Azure. Ce problème ne s'applique pas aux nouveaux systèmes installant NSX-T Data Center 2.3 pour la première fois.

**Solution :** à partir du portail Microsoft Azure, redémarrez la PCG que vous mettez à niveau, puis dans Cloud Service Manager (CSM), vérifiez que l'état des PCG et des instances de machine virtuelle est valide.

- **Problème 2180531 : NSX Agent est pris en charge pour les instances de machine virtuelle Ubuntu 16.04 qui disposent du noyau 4.14 et inférieur**  
NSX Agent est pris en charge pour les instances de machine virtuelle Ubuntu 16.04 qui disposent du noyau 4.14 et inférieur. NSX Agent ne fonctionnera pas pour une instance de machine virtuelle Ubuntu 16.04 disposant du noyau 4.15 et versions ultérieures.

Il n'existe aucune solution pour ce problème

- **Problème 2170445 : après la mise à niveau de PCG depuis NSX-T Data Center 2.2 vers NSX-T Data Center 2.3, l'état HA PCG ne sera pas correctement défini pour les PCG de Microsoft Azure PCG**  
Après la mise à niveau de PCG Microsoft Azure de NSX-T 2.2 vers NSX-TData2.3, l'état HA des PCG ne devient pas Actif-En veille comme prévu. L'état HA PCG préféré indique SYNC et l'état HA PCG non préféré indique Actif. De ce fait, en cas d'un basculement HA après la mise à niveau, une seule PCG a un état valide.

**Solution :** Dans NSX-T 2.2, mettez à jour la MTU dans le profil de commutateur d'hôte de la liaison montante de la PCG à 1 500 avant de démarrer les mises à niveau vers NSX-TData2.3. Vous pouvez le faire à l'aide de l'interface utilisateur de NSX Manager ou des REST API de NSX Manager.

Via l'interface utilisateur, procédez comme suit :

1. Accédez à **Infrastructure > Profils**
2. Sélectionnez le profil portant le nom « PCG-Uplink-HostSwitch-Profile » et ayant la description « PublicCloudGateway Uplink HostSwitch Profile »
3. Cliquez sur **MODIFIER** et modifiez la valeur MTU à 1 500, puis cliquez sur **ENREGISTRER**
4. Démarrez la mise à niveau de NSX-T 2.2 vers NSX-TData2.3.

Via l'API REST, procédez comme suit :

1. Obtenez (GET) tous les profils de commutateur d'hôte à l'aide de :

```
curl -X GET \
  https://<NSX-Manager-URL>/api/v1/host-switch-profiles \
  -H 'authorization: Basic <AUTH ID>' \
  -H 'content-type: application/json'
```

2. Identifiez le profil de commutateur d'hôte portant le nom « PCG-Uplink-HostSwitch-Profile » et ayant la description « PublicCloudGateway Uplink HostSwitch Profile » et obtenez l'ID de ce profil :

```
curl -X PUT \
  https://<NSX-Manager-URL>/api/v1/host-switch-profiles/<host-switch-profile-id> \
```

```

-H 'authorization: Basic <AUTH ID>' \
-H 'content-type: application/json' \
-d '{
    "resource_type": "UplinkHostSwitchProfile",
    "description": "PublicCloudGateway Uplink HostSwitch Profile",
    "id": "<host-switch-profile-id>",
    "display_name": "PCG-Uplink-HostSwitch-Profile",
    "tags": [
        {
            "scope": "CrossCloud",
            "tag": "public-cloud-manager"
        },
        {
            "scope": "PcmId",
            "tag": "<Existing PCM ID>"
        },
        {
            "scope": "EntityType",
            "tag": "default"
        },
        {
            "scope": "CloudScope",
            "tag": "<Existing VPC/VNET name>"
        },
        {
            "scope": "CloudType",
            "tag": "<Existing cloud type>"
        },
        {
            "scope": "CloudVpcId",
            "tag": "<Existing Vpc/Vnet id>"
        }
    ],
    "transport_vlan": 0,
    "teaming": {
        "active_list": [
            {
                "uplink_type": "PNIC",
                "uplink_name": "uplink-1"
            }
        ],
        "policy": "FAILOVER_ORDER"
    },
    "overlay_encap": "GENEVE",
    "mtu": 1500,
    "_revision": 1
}'

```

- **Problème 2174725** : un VPC/VNet géré sur lequel des PCG sont déployées est affiché comme non géré dans CSM.

Un VPC AWS géré ou un VNet Microsoft Azure sur lequel des PCG sont déployées est affiché comme non géré dans CSM.

*Solution* : le redémarrage de CSM devrait résoudre le problème.

- **Problème 2162856** : des PCG Azure ont un état HA non valide (tous les deux actifs ou tous les

deux en veille)

Lorsque vous déployez une paire de PCG dans AWS, puis déployez une autre paire de PCG pour Azure, les PCG Azure auront un état HA non valide (tous les deux actifs ou tous les deux en veille).

Solution : mettez à jour la MTU dans le profil du commutateur d'hôte de liaison montante des PCM à 1 500 avant de démarrer la mise à niveau cloud vers NSX-T Data Center 2.3. Depuis l'interface utilisateur du gestionnaire, procédez comme suit :

- Accédez à Infrastructure > Profils.
  - Sélectionnez le profil portant le nom « PCG-Uplink-HostSwitch-Profile » et ayant la description « PublicCloudGateway Uplink HostSwitch Profile ».
  - Cliquez sur « MODIFIER », modifiez la valeur « MTU » à 1 500 et cliquez sur « ENREGISTRER ».
  - Démarrez le workflow de mise à niveau.
- **Problème 2102321 : certaines opérations de NSX Cloud peuvent être lentes sur Microsoft Azure pendant les périodes de trafic intense.**

NSX Cloud s'appuie sur l'API Microsoft Azure ARM pour certaines opérations telles que la gestion de machines virtuelles ou leur retrait à partir de la gestion NSX ; ou la prise de mesures de quarantaine sur une machine virtuelle. Pendant les périodes de pointe, Microsoft Azure peut atteindre les limites de l'API pour des abonnements donnés, auquel cas, il va démarrer la limitation des demandes d'API pour cet abonnement. Pendant ce temps, les opérations NSX mentionnées ci-dessus n'aboutissent pas dans les délais impartis. Ces opérations se termineront éventuellement lorsque Microsoft Azure arrête le ralentissement des demandes. Des journaux PCM sur la passerelle PCG comportent des journaux comme le journal suivant, indiquant qu'une limitation est actuellement en cours « *Azure Resource Manager read/write per hour limit reached. Will retry in: x seconds* »

**SOLUTION :** attendez que la limitation de Microsoft Azure s'arrête.

- **Problème 2189738 : Les machines virtuelles de charge de travail AWS ne peuvent pas être atteintes suite à la désactivation de la stratégie de quarantaine pour un VPC intégré, après que cette stratégie a été précédemment activée.**

Si une PCG est déployée alors que la stratégie de quarantaine est activée, et si vous désactivez le mode quarantaine plus tard, certaines machines virtuelles de charge de travail AWS gérées par NSX dans ce VPC ne parviennent pas à communiquer avec la PCG.

**Solution :** ajoutez les règles entrantes suivantes au groupe de sécurité NSX Cloud dans le VPC AWS : gw-mgmt-sg :

**Remarque :** supprimez ces règles lorsque vous réactivez la stratégie de quarantaine pour des raisons de sécurité.

TYPE	Protocole	Port	Source
CUSTOM-TCP	TCP	8080	VPC-CIDR
CUSTOM-TCP	TCP	5555	VPC-CIDR

- **Problème 2188950 : le message d'erreur suivant s'affiche : « VNet introuvable pour l'ID spécifié » lorsque vous utilisez l'API pour récupérer une liste de PCG.**  
Vous voyez cette erreur si un compte associé sur lequel des PCG sont déployées est supprimé de CSM.

**Solution :** ajoutez le compte Microsoft Azure dans CSM sur lequel les PCGs ont été déployées.

- **Problème 2191571 : Le déploiement de PCG ne démarre pas si la clé publique SSH pour le déploiement de PCG ne se termine pas par un ID d'e-mail.**  
La clé publique SSH doit se terminer par un ID d'e-mail, sinon le déploiement de PCG ne démarre pas et affiche une erreur.

**Solution :** vérifiez que la clé SSH se termine par un ID d'e-mail.

- **Problème 2092073** : sur des machines virtuelles de charge de travail Windows, des modèles IPFIX ne sont pas reçus correctement.

Sur des machines virtuelles de charge de travail Windows, les modèles IPFIX de commutateur logique et de pare-feu ne sont pas envoyés immédiatement lorsque le collecteur IPFIX est configuré dans le même sous-réseau que la machine virtuelle. Cela est dû au fait que Windows Socket attend une entrée ARP pour l'adresse IP du collecteur IPFIX avant d'envoyer le paquet UDP. Si une entrée ARP est manquante, il abandonne en silence tous les paquets UDP sauf le dernier. Par conséquent, sur le collecteur IPFIX, le paquet de données est reçu sans information de modèle.

*Solution* : utilisez l'une des méthodes suivantes :

- ajoutez une entrée ARP statique pour le collecteur IPFIX à l'aide de la commande :

```
netsh interface ipv4 add neighbors "<nom d'interface>" <adresse IP> <adresse physique du collecteur>
```

Par exemple :

```
netsh interface ipv4 add neighbors "Ethernet 3" 172.26.15.7 12-34-56-78-9a-bc
```

- Configurez le collecteur IPFIX sur un autre sous-réseau que celui des machines virtuelles de charge de travail.
- **Problème 2210490** : si vous ajoutez un profil de proxy dans CSM, le mot de passe sera visible par tous les utilisateurs de l'API CSM si un de ces rôles leur est attribué : Auditeur de service Cloud ou administrateur de service Cloud.

Si vous créez un profil de proxy dans CSM et fournissez un nom d'utilisateur et le mot de passe, même si vous ne pouvez pas afficher le mot de passe dans l'interface utilisateur de CSM, il sera visible en réponse à l'API suivante :

- /csm/proxy-server-profiles
- /csm/proxy-server-profiles/<profile-id>

- **Problème 2039804** : le déploiement de PCG échoue, mais l'instance de PCG n'est pas arrêtée dans AWS.

Si vous déployez PCG, mais que le déploiement échoue, vous verrez toujours la ou les instances de PCG dans votre VPC AWS et dans les entités logiques créées automatiquement dans NSX Manager.

*Solution* : supprimez les entités de NSX Manager créées automatiquement et arrêtez manuellement l'instance de PCG dans votre VPC AWS.

## Problèmes connus de NSX Container Plug-in (NCP)

- **Modification du plug-in CNI dans PAS 2.1.0**  
En raison de la modification du plug-in CNI dans PAS 2.1.0, aucune vignette NSX-T, quelle que soit la version, ne fonctionnera avec PAS 2.1.0. Ce problème est résolu dans PAS 2.1.1.
- **Problème 2118515** : Dans une configuration à grande échelle, la création de pare-feu par sur NSX-T est assez longue  
Dans une configuration à grande échelle (par exemple, 250 nœuds Kubernetes, 5 000 espaces, 2 500 stratégies réseau), NCP peut prendre quelques minutes pour créer les sections de pare-feu et les règles dans NSX-T.

*Solution* : aucune. Une fois les sections de pare-feu et les règles créées, les performances doivent revenir à la normale.

- **Problème 2125755** : un StatefulSet peut perdre la connectivité réseau lors de l'exécution des mises à jour de Canary et des mises à jour continues par phase  
Si un StatefulSet a été créé avant la mise à niveau de NCP vers la version actuelle, le StatefulSet peut perdre la connectivité réseau lors de l'exécution des mises à jour de Canary et des mises à jour continues par phase.

Solution : Créez le StatefulSet après la mise à niveau de NCP vers la version actuelle.

- **Problème 2131494 : NGINX Kubernetes Ingress fonctionne toujours après la redéfinition de la classe Ingress nginx sur nsx**  
Lorsque vous créez un objet NGINX Kubernetes Ingress, NGINX crée des règles de transfert du trafic. Si vous redéfinissez la classe Ingress sur une autre valeur, NGINX ne supprime pas les règles et continue à les appliquer, même si vous supprimez l'objet Kubernetes Ingress après la modification de la classe. Il s'agit d'une limitation de NGINX.

Solution : pour supprimer les règles créées par NGINX, supprimez l'objet Kubernetes Ingress lorsque la valeur de classe est nginx. Recréez ensuite l'objet Kubernetes Ingress.

- **Problème 2194845 : la fonctionnalité de l'API PAS Cloud Foundry V3 « plusieurs processus par application » n'est pas prise en charge**  
Lorsque vous utilisez l'API PAS Cloud Foundry V3 `v3-push` pour envoyer une application comportant plusieurs processus, NCP ne crée pas les ports de commutateur logique pour les processus, sauf celui par défaut. Ce problème existe dans NCP 2.3.0 et versions antérieures.

Solution : aucune

- **Problème 2193901 : l'utilisation de plusieurs PodSelectors ou de plusieurs NsSelectors pour une seule règle de stratégie réseau Kubernetes n'est pas prise en charge**  
L'application de plusieurs sélecteurs permet uniquement le trafic entrant depuis des espaces spécifiques.

Solution : utilisez plutôt matchLabels avec matchExpressions dans un seul PodSelector ou NsSelector.

- **Problème 2194646 : la mise à jour des stratégies réseau lorsque NCP est hors service n'est pas prise en charge**  
Si vous mettez à jour une stratégie réseau lorsque NCP est hors service, l'ensemble d'adresses IP de destination pour la stratégie réseau sera incorrect lorsque NCP est rétabli.

Solution : recréez la stratégie réseau lorsque NCP est en service.

- **Problème 2192489 : après la désactivation de « BOSH DNS server » dans PAS director config, le serveur DNS Bosh (169.254.0.2) figure toujours dans le fichier resolve.conf du conteneur.**  
Dans un environnement PAS exécutant PAS 2.2, après que vous désactivez « BOSH DNS server » dans PAS director config, le serveur DNS Bosh (169.254.0.2) figure toujours dans le fichier resolve.conf du conteneur. Dans ce cas, l'exécution d'une commande ping avec un nom de domaine complet est très longue. Ce problème n'existe pas avec PAS 2.1.

Solution : aucune. Il s'agit d'un problème PAS.

- **Problème 2194367 : la vignette NSX-T ne fonctionne pas avec les segments d'isolation PAS qui déploient leurs propre routeurs**  
La vignette NSX-T ne fonctionne pas avec des segments d'isolation PAS (Pivotal Application Service) qui déploient leurs propres routeurs GoRouters et routeurs TCP. En effet, NCP ne peut pas obtenir les adresses IP des machines virtuelles de routeur ni créer des règles de pare-feu NSX pour autoriser le trafic allant des routeurs aux conteneurs d'applications PAS.

Solution : aucune.

- **Problème 2199504 : le nom complet des ressources NSX-T créées par NCP est limité à 80 caractères**  
Quand NCP crée une ressource NSX-T pour une ressource dans l'environnement du conteneur, il génère le nom complet de la ressource NSX-T en combinant le nom du cluster, un espace de noms ou nom de projet, et le nom de la ressource dans l'environnement du conteneur. Si le nom complet contient plus de 80 caractères, il est tronqué à 80 caractères.

Solution : aucune

- **Problème 2199778 : avec NSX-T 2.2, Ingress, Service et Secrets portant des noms d'une longueur supérieure à 65 caractères ne sont pas pris en charge**  
Avec NSX-T 2.2, lorsque `use_native_loadbalancer` est défini sur `True`, les noms Ingresses, Secrets et Services référencés par Ingress et services de type LoadBalancer, doivent compter 65 caractères ou moins. Dans le cas contraire, Ingress ou Service ne fonctionne pas correctement.

Solution : lors de la configuration d'Ingress, Secret ou Service, spécifiez un nom comportant 65 caractères ou moins.

- **Problème 2065750 : l'installation du module NSX-T CNI échoue avec un conflit de fichier**  
Dans un environnement RHEL où kubernetes est installé, si vous installez le module NSX-T CNI à l'aide de `yum localinstall` ou `rpm -i`, vous obtenez une erreur indiquant un conflit avec un fichier du module kubernetes-cni.

Solution : installez le module NSX-T CNI avec la commande `rpm -i --replacefiles nsx-cni-2.3.0.xxxxxxxx-1.x86_64.rpm`.

- **Pour un service Kubernetes de type ClusterIP, l'affinité de session basée sur l'adresse IP du client n'est pas prise en charge**  
NCP ne prend pas en charge l'affinité de session basée sur l'adresse IP du client pour un service Kubernetes de type ClusterIP.

Solution : aucune

- **Pour un service Kubernetes de type ClusterIP, l'indicateur de mode épingle n'est pas pris en charge**  
NCP ne prend pas en charge l'indicateur de mode épingle pour un service Kubernetes de type ClusterIP.

Solution : aucune

## Errata et ajouts de la documentation

- **Problème 1372211 : Deux interfaces sur le même sous-réseau**  
Le trafic par tunnel peut fuir vers l'interface de gestion si le point de terminaison de tunnel se trouve sur le même sous-réseau que l'interface de gestion. Cela se produit car les paquets de tunnel peuvent traverser l'interface de gestion. Veillez à ce que les interfaces de gestion se trouvent sur un sous-réseau séparé des interfaces de point de terminaison de tunnel.