

Notes de mise à jour de VMware NSX-T Data Center 2.3.1 et NSX Container Plug-in 2.3.1

VMware NSX-T Data Center 2.3.1 | 20 décembre 2018

VMware NSX Container Plug-in 2.3.1 | 8 novembre 2018

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](#)
- [Conditions de compatibilité](#)
- [Problèmes résolus](#)
- [Problèmes connus](#)

Nouveautés

Nouveautés de NSX-T Data Center 2.3.1

NSX-T Data Center 2.3.1 est une version de maintenance qui résout un certain nombre de problèmes détectés dans les versions précédentes. Pour en savoir plus sur les nouvelles fonctionnalités de NSX-T Data Center 2.3 ainsi que sur les problèmes connus et résolus de NSX-T Data Center 2.3.1, consultez les [Notes de mise à jour de NSX-T Data Center 2.3](#).

Nouveautés de NSX Container Plug-in 2.3.1

NSX Container Plug-in (NCP) 2.3.1 est une version de maintenance qui résout un certain nombre de problèmes détectés dans les versions précédentes et offre la nouvelle fonctionnalité suivante :

- Mise à l'échelle automatique des équilibrages de charge NSX-T pour les services Kubernetes LoadBalancer. Si un service Kubernetes LoadBalancer nécessite des serveurs virtuels supplémentaires, un nouvel équilibreur de charge NSX-T sera créé si nécessaire.

Versions d'ESXi recommandées pour NSX-T Data Center 2.3.1

- ESXi 6.5 P03 Build 10884925
- ESXi 6.7 U1 Build 10302608

Conditions de compatibilité pour NCP 2.3.1

Produit	Version
Mosaïque NCP/NSX-T pour PAS	2.3.1
NSX-T	2.2, 2.3, 2.3.1
Kubernetes	1.11, 1.12
OpenShift	3.10, 3.11
Système d'exploitation de VM sur hôte Kubernetes	Ubuntu 16.04, RHEL 7.4, 7.5
Système d'exploitation de VM sur hôte OpenShift	RHEL 7.4, 7.5
PAS (PCF)	OpsManager 2.2.0 + PAS 2.2.0 OpsManager 2.3.x + PAS 2.3.x

Problèmes résolus

Les problèmes résolus sont regroupés comme suit :

- [Problèmes résolus dans NSX-T Data Center 2.3.1](#)
- [Problèmes résolus dans NCP 2.3.1](#)

Problèmes résolus dans NSX-T Data Center 2.3.1

- **Problème 2238957 : les ports hyperbus obsolètes ne sont pas nettoyés après le redémarrage d'un hôte ESXi**
Si vous redémarrez un hôte ESXi sans mettre hors tension les machines virtuelles de conteneur en cours d'exécution sur l'hôte, les ports hyperbus ne sont pas nettoyés comme prévu.
- **Problème 2226523 : la commande d'interface de ligne commande « get débogage bgp » ne fonctionne pas**
L'exécution de la commande de ligne de commande « get débogage bgp » ne génère aucune sortie.
- **Problème 2241365 : lors d'une mise à niveau de NSX-T Data Center 2.2 vers la version 2.3, les machines virtuelles protégées par pare-feu avec trafic ALG (passerelle de niveau application) perdent la connectivité réseau**
Lors d'une mise à niveau de NSX-T Data Center 2.2 vers la version 2.3, les machines virtuelles sont migrées à partir des hôtes exécutant NSX-T Data Center 2.2 vers les hôtes qui exécutent NSX-T Data Center 2.3. Les machines virtuelles protégées par pare-feu et sur lesquelles transite le trafic ALG perdent la connectivité réseau après la migration.
- **Problème 2241378 : des blocages et des pertes de trafic se produisent pour les tunnels VPN**
Les tunnels VPN qui disposent d'une règle d'abandon de pare-feu configurée et ont un trafic fragmenté sont confrontés à des blocages et des pertes de trafic.
- **Problème 2232034 : l'hôte ESXi s'arrête brutalement lors de la création d'un bundle de support si l'hôte dispose d'un pont DLR avec plus de 1 024 adresses MAC**
L'exécution de vm-support ou de la commande « net-bridge --mac-address-table \$bridgeName » entraîne un dépassement de la mémoire tampon s'il existe un grand nombre d'entrées de transfert de pont.
- **Problème 2216746 : la carte réseau d'une VM est déconnectée et celle-ci n'a aucune connectivité réseau lors d'une opération vMotion ou de la mise sous tension**
Si un grand nombre de machines virtuelles sont mises sous tension ou déplacées via vMotion simultanément, certaines cartes réseau des machines virtuelles peuvent se déconnecter et celles-ci n'ont aucune connectivité réseau.

- **Problème 2216747** : le déplacement vMotion d'une machine virtuelle entraîne la déconnexion de ses ports
Lorsque le stockage d'une machine virtuelle se trouve sur un système NFS et que celle-ci fait l'objet d'un déplacement vMotion, ce qui peut être déclenché par VMware HA, elle perd la connectivité réseau.
- **Problème 2229210** : des opérations répétées de création et de suppression de ports de commutateur logique entraînent une fuite de mémoire dans NSX Controller
Ce problème est dû à la non-suppression des objets de domaine SpoofGuard lorsque les ports de commutateur logique sont supprimés.
- **Problème 2220560** : un nombre excessif d'enregistrements dans les journaux d'événements dans metricRegistry peut entraîner une fuite de mémoire dans NSX Controller
Après le traitement d'un grand nombre de transactions par NSX Controller, le volume de journalisation peut entraîner une fuite de mémoire.
- **Problème 2221286** : les entrées ARP expirent peu après la perte de connexion de la machine virtuelle
Ce problème peut rendre les machines virtuelles inaccessibles pendant un certain temps.
- **Problème 2227882** : un VPN basé sur une stratégie tombe en panne avec l'erreur « Aucun SA IPsec actif. Suppression du SA IKE sans enfants »
Cette erreur entraîne une renégociation et des pertes de trafic.
- **Problèmes 2227885 et 2227879** : fuite de mémoire observée dans les VPN IPsec sur le nœud Edge avec certains modèles de trafic
Lorsque le trafic ESP encapsulé via UDP (paquets avec port de destination 4500) et avec l'adresse IP de destination détenue par le nœud Edge arrive pendant les fenêtres suivantes :
 - Les règles de redirection PBR (utilisées par HCX) sont programmées après la programmation FIB de l'adresse IP redirigée vers le port de bouclage
 - Adresse source manquante pour le tunnel VPN (par exemple, en cas d'événement iked misbehave ou coredumped)
- **Problème 2227890** : ID de VLAN non modifié après la modification des ID de tunnel dans la configuration du port logique
Lorsque vous effectuez un appel d'API pour modifier l'ID de tunnel d'un port logique, l'ID de VLAN n'est pas modifié.
- **Problème 2230277** : vidage des données d'exécution de ports pendant une opération vMotion
Avec ESXi 6.5, un problème se produisant lors d'une opération Storage vMotion entraîne le vidage des données d'exécution sur un port, avant que la structure vMotion puisse enregistrer les données.
- **Problème 2236206** : les nœuds de transport ESXi peuvent perdre l'accès réseau en raison d'une fuite de mémoire
Ce problème peut entraîner la perte de la connectivité réseau d'un nœud de transport ESXi dans un environnement PKS.

Problèmes résolus dans NCP 2.3.1

- **Problème 2216781** : la longueur maximale d'une valeur de balise est limitée à 65 caractères dans NCP 2.2.x et 256 caractères dans NCP 2.3.0
NCP 2.3.1 prend en charge les noms qui dépassent la limite de valeur de balise pour les ressources Kubernetes suivantes associées à l'équilibreur de charge :
 - Service LoadBalancer
 - Entrée
 - Secret spécifié dans une spécification d'entrée
 - Service spécifié dans une spécification d'entrée
- **Problème : 2217051** : l'adresse IP du serveur virtuel n'est pas mise à jour lorsque le service loadBalancerIP de LoadBalancer est modifié

Après la création d'un service LoadBalancer, si vous modifiez la valeur loadBalancerIP du service, la modification n'est pas reflétée dans l'adresse IP du serveur virtuel de l'équilibreur de charge NSX-T.

- **Problème 2216085 : après la suppression d'un espace de noms, les règles et les pools d'équilibreur de charge NSX-T ne sont pas supprimés**

Lorsque vous configurez les ressources d'entrée et l'équilibrage de charge NSX-T, des serveurs virtuels, des pools et des règles NSX-T sont créés. Si vous supprimez l'espace de noms dans lequel se trouvent les ressources d'entrée, certaines règles et pools ne sont pas supprimés de NSX-T.

Problèmes connus

Les problèmes connus sont classés comme suit.

- [Problèmes connus de NSX-T Data Center 2.3.1](#)
- [Problèmes connus de NCP 2.3.1](#)

Problèmes connus de NSX-T Data Center 2.3.1

- **Problème 2235834 : problème de trafic RDP et HTTPS avec cache de flux activé**
Lorsque le cache de flux est activé, des problèmes avec le trafic RDP et HTTPS peuvent se produire.

Solution : sur le nœud Edge, exécutez les commandes suivantes pour désactiver le cache de flux :

- set dataplane flow-cache disabled
- restart service dataplane
- **Problème 2227975 : perte de trafic TCP intermittente sur un nœud Edge**
Le trafic TCP transmis sur un nœud Edge est perdu par intermittence. Le trafic ICMP n'est pas affecté.

Solution : sur le nœud Edge, désactivez le cache de flux à l'aide des commandes suivantes :

- set dataplane flow-cache disabled
- restart service dataplane

Problèmes connus de NCP 2.3.1

- **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.

- **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

- **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 désactiviez « 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 prend actuellement pas en charge les segments d'isolation PAS qui déploient leurs propres 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`.

- **Problème 2224218 : après la suppression d'un service ou d'une application, la libération de l'adresse IP SNAT pour le pool IP dure 2 minutes**
Si vous supprimez un service ou une application et que vous le/la recréez en moins de 2 minutes, il/elle obtiendra une nouvelle IP SNAT du pool IP.

Solution : après la suppression d'un service ou d'une application, patientez 2 minutes avant de le/la recréer si vous souhaitez réutiliser la même adresse IP.

- **Problème 2218008 : la configuration de différents clusters Kubernetes afin d'utiliser le même bloc d'IP entraîne des problèmes de connectivité**
Si vous configurez différents clusters Kubernetes pour utiliser le même bloc d'IP, certains espaces ne seront pas en mesure de communiquer avec d'autres espaces ou des réseaux externes.

Solution : ne configurez pas différents clusters Kubernetes afin d'utiliser le même bloc d'IP.