

Notes de mise à jour de VMware NSX-T Data Center 2.4.3

VMware NSX-T Data Center 2.4.3 | 7 novembre 2019 | Build 15008150

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 :

- [Compatibilité et configuration système requise](#)
- [Ressources relatives aux interfaces de ligne de commande et aux API](#)
- [Historique de révision](#)
- [Problèmes résolus](#)
- [Problèmes connus](#)

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](#).

Ressources relatives aux interfaces de ligne de commande et aux API

Pour utiliser les API ou les interfaces de ligne de commande de NSX-T Data Center pour l'automatisation, consultez code.vmware.com.

La documentation de l'API est disponible dans l'onglet Référence de l'API. La documentation de l'interface de ligne de commande est disponible dans l'onglet Documentation.

Historique de révision du document

7 novembre 2019. Première édition.

Problèmes résolus

- **Problème résolu 2294410** : certains ID d'application sont détectés par le pare-feu L7. Les ID d'application L7 suivants sont détectés en fonction du port, et non de l'application : SAP, SUNRPC et SVN. Les ID d'application L7 suivants ne sont pas pris en charge : AD_BKUP, SKIP et AD_NSP.
- **Problème 2295470 résolu** : les filtres de pare-feu ne sont pas présents après la migration vers NSX-T depuis NSX for vSphere.

Si des services sont utilisés dans de nombreuses règles de pare-feu, des mises à jour fréquentes sur les services peuvent être causées lors du processus de migration. Par conséquent, les filtres de pare-feu ne sont pas installés sur l'hôte ESXi. Cela peut provoquer une interruption du trafic.

- **Problème 2314537 corrigé : l'état de la connexion est inactif après la mise à jour du certificat et de l'empreinte numérique de vCenter.**
Aucune nouvelle mise à jour de vCenter n'est synchronisée avec NSX et toutes les requêtes à la demande pour extraire des données de vCenter échoueront. Les utilisateurs ne peuvent pas déployer de nouvelles VM Edge/Service. Les utilisateurs ne peuvent pas préparer de nouveaux clusters ou hôtes ajoutés dans le vCenter. Emplacements du journal : /var/log/cm-inventory/cm-inventory.log et /var/log/proton/nsxapi.log sur le nœud NSX Manager.
- **Problème 2331683 résolu : le formulaire add-load-balancer dans l'interface utilisateur avancée n'affiche pas la capacité mise à jour de la version 2.4.**
Lorsque le formulaire add-load-balancer est ouvert, la capacité form-factor-capacity indiquée sur l'interface utilisateur avancée n'est pas mise à jour en fonction de la version 2.4. La capacité indiquée provient de la version précédente.
- **Problème résolu 2424081 : routes redistribuées manquantes par intermittence.**
Le trafic réseau peut être affecté, car l'itinéraire vers T1 n'est pas disponible pendant un certain temps.
- **Problème résolu 2424293 : après la migration de la machine virtuelle vers un nouvel hôte, la VIF connectée à un autre port logique, les règles de pare-feu distribué ne parviennent pas à être appliquées.**
L'adresse IP de la VM n'a pas été réalisée, car l'interface utilisateur indique qu'elle est dupliquée sur l'adresse IP sur un port supprimé.
- **Problème résolu 2424372 : vIDM ne parvient pas à fournir un jeton d'accès à NSX-T en raison d'une demande incorrecte effectuée par le proxy inverse NSX-T à vIDM.**
Condition de concurrence dans le proxy inverse selon laquelle la logique de lecture a été lue avant la fin de l'écriture du fichier sur le disque par le scripteur (NAPI).
- **Problème résolu 2424386 : les routes statiques configurées sur le routeur T0 ne parviennent pas à s'installer correctement.**
Le VRF pour le routeur T0 n'affiche pas les routes statiques configurées. Aucune nouvelle configuration n'est réalisée.
- **Problème résolu 2424402 : la mise à niveau de l'hôte NSX-T peut échouer en raison d'un espace insuffisant dans /tmp.**
Échec de la mise à niveau de l'hôte, car /tmp ne dispose pas d'un espace suffisant.
- **Problème résolu 2424852 : les hôtes utilisant un certificat signé par une autorité de certification peuvent échouer lors de la mise à niveau avec l'erreur « Erreur inattendue lors de la mise à niveau de l'unité : empreinte numérique de l'hôte non valide ».**
Échec de la mise à niveau de l'hôte.
- **Problème résolu 2424855 : l'opération de sauvegarde NSX peut échouer ou peut mettre un certain temps à se terminer.**
La sauvegarde du cluster peut prendre plus de 30 minutes, puis échouer.
- **Problème résolu 2327494 : la mise à niveau de l'hôte NSX-T peut échouer si SNMP est activé sur l'hôte ESXi.**
La mise à niveau de NSX-T échoue si SNMP est activé sur ESX.
- **Problème résolu 2416081 : ajoutez de la capacité pour augmenter le nombre de serveurs virtuels (de 10 à 20) dans un équilibreur de charge NSX-T de petit format.**
Certains serveurs virtuels ne fonctionnent pas pour un équilibreur de charge de petite taille.
- **Problème résolu 2426255 : ajouter une capacité de redémarrage pour les services JVM sur le**

nœud NSX-T Manager.

Système inutilisable pour une configuration ou une opération de réseau NSX associée significative si un composant de service critique est affecté.

- **Problème résolu 2432859** : les événements FIREWALL-PKTLOG à partir de machines virtuelles de cloud ne sont pas transférés par la passerelle de cloud public via syslog.
Les journaux de pare-feu des machines virtuelles de cloud exécutant le mode NSX appliqué ne sont pas transférés via syslog depuis la passerelle de cloud public (PCG). L'interface de ligne de commande sur PCG pour transférer les journaux des machines virtuelles ne fonctionne pas.
- **Problème résolu 2424394** : les paquets DHCP relayés par la récupération d'urgence NSX-T ne peuvent pas atteindre plus de 10 tronçons.
Lorsque le serveur DHCP fait plus de 10 tronçons, les paquets DHCP relayés ne peuvent pas atteindre le serveur.
- **Problème résolu 2441080** : NAT peut ne pas être exécuté lorsque le cache de flux est activé.
Pour un flux de trafic donné en cours de NAT sur le dispositif Edge, certains paquets du flux peuvent ne pas être traduits comme prévu. Les systèmes finaux accessibles via NAT peuvent devenir inaccessibles.
- **Problème résolu 2444968** : les sauvegardes automatiques ne sont pas générées.
Les sauvegardes ne sont pas générées même si l'indicateur de sauvegardes automatiques est activé.
- **Problème résolu 2448712** : la mise à niveau de l'hôte NSX-T échoue en raison d'un espace insuffisant dans la partition bootbank.
La mise à niveau échoue s'il n'y a pas suffisamment d'espace dans la partition bootbank d'un hôte ESXi.
- **Problème résolu 2424838** : des règles non valides sont appliquées au trafic lorsqu'une liaison descendante T0 est associée à un service T1 SR.
Le trafic commuté 2 T1 était soumis au service sur le T0, lorsqu'un T1 disposait d'un SR.
- **Problème résolu 2422004** : la liste de préfixes IP générée par le système n'est pas migrée correctement lors de la mise à niveau de NSX-T 2.3 vers 2.4.
La liste de préfixes IP générée par le système n'affiche aucun préfixe pour certains ports de liaison descendante. L'adresse IP de liaison descendante de niveau 0 ne permet pas de publier correctement le trafic.
- **Problème résolu 2415066** : la mise à niveau de l'hôte NSX-T depuis les versions antérieures de NSX-T 2.4.3 vers NSX-T 2.5.0 échouera.
Les journaux vmkernel indiquent que le module nsxt-kcp effectue un téléchargement, mais il ne peut pas terminer le processus.
- **Problème résolu 2434224** : le dispositif Edge 2.4.0 NSX-T peut subir un impact sur le chemin de données en raison d'une erreur de segmentation causée par l'épuisement du masque du cache de flux.
Le dispositif Edge actif sera basculé vers le dispositif Edge en veille.
- **Problème résolu 2387301** : l'état LACP resterait inactif sur les commutateurs physiques lorsqu'il est intégré à l'hôte préparé NSX-T configuré pour LACP.
Perte de connectivité entre les machines virtuelles et les connexions de service (routeurs de service, etc.).
- **Problème résolu 2448254** : perte de connectivité réseau intermittente sur les machines virtuelles dans les environnements à locataires multiples avec des sous-réseaux IP se chevauchant.
Perte de connectivité réseau.
- **Problème résolu** : 2425861 - NSX-T /api/v1/edge-clusters/<id>/state API renvoie l'état de

réalisation « in_sync », qui n'est pas documenté comme étant un état attendu.

L'état et les mesures d'état du cluster Edge ne sont pas collectés en tant que mesures en ligne.

- **Problème résolu 2438550** : corriger l'alerte positive fausse « CorfuDB est déconnecté, définissez l'état du cluster hors service ».
Exceptions détectées dans le journal, mais elles ne sont pas irrécupérables.

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 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 Cloud](#)

Problèmes connus généraux

- **Problème 2389109** : BGP/le routage ne fonctionne pas sur TO-SR si le nom d'hôte Edge commence par un nombre.
BGP/Routing ne fonctionne pas sur TO-SR si le nom d'hôte Edge commence par un nombre et que la configuration n'est pas envoyée vers la pile de routage. Cette limitation est connue.

Solution : utilisez l'interface de ligne de commande pour modifier le nom d'hôte afin qu'un nombre ne soit plus le premier chiffre dans le nom d'hôte. Activez et désactivez le mode de maintenance sur le nœud Edge pour appliquer la modification.

- **Problème 2239365** : une erreur « non autorisée » est générée.
Cette erreur peut se produire lorsque l'utilisateur tente d'ouvrir plusieurs sessions d'authentification sur le même type de navigateur. En conséquence, la connexion échoue, l'erreur ci-dessus s'affiche et l'authentification est impossible. Emplacement du journal : `/var/log/proxy/reverse-proxy.log` `/var/log/syslog`

Solution : fermez l'ensemble des fenêtres/onglets d'authentification ouverts et retentez l'authentification.

- **Problème 2252487** : l'état du nœud de transport n'est pas enregistré pour le nœud de transport Edge BM lorsque plusieurs nœuds de transport sont ajoutés en parallèle.
L'état du nœud de transport ne s'affiche pas correctement dans l'interface utilisateur du plan de gestion.

Solution :

1. redémarrez le proton, l'état de tous les nœuds de transport peut être mis à jour correctement.
 2. Vous pouvez également utiliser l'API `https://<nsx-manager>/api/v1/transport-nodes/<id-nœud>/status?source=realtime` pour interroger l'état des nœuds de transport.
- **Problème 2256709** : une machine virtuelle Instant Clone ou une machine virtuelle restaurée à partir d'un snapshot perd brièvement la protection antivirus pendant son déplacement avec vMotion.

Le snapshot d'une machine virtuelle est restaurée et migre la machine virtuelle vers un autre hôte. La console partenaire n'affiche pas la protection antivirus pour la machine virtuelle Instant Clone migrée. La protection antivirus est brièvement interrompue.

Solution : aucune.

- **Problème 2261431 : une liste filtrée des banques de données est requise, selon les autres paramètres de déploiement.**

L'erreur correspondante est affichée sur l'interface utilisateur si l'option incorrecte a été sélectionnée. Le client peut supprimer ce déploiement et en créer un nouveau à des fins de récupération après erreur.

Solution : sélectionnez la banque de données partagée si vous créez un déploiement en cluster.

- **Problème 2274988 : des chaînes de services ne prennent pas en charge les profils de service consécutifs provenant d'un même service.**

Le trafic n'emprunte pas une chaîne de services et est interrompu dès lors que la chaîne comporte deux profils de service consécutifs appartenant à un même service.

Solution : ajoutez un profil de service à partir d'un autre service pour vous assurer que deux profils de service consécutifs n'appartiennent pas à un même service. Vous pouvez également définir un troisième profil de service qui effectuera les mêmes opérations que celles des deux profils d'origine concaténés, puis utiliser ce profil troisième seul dans la chaîne de services.

- **Problème 2275285 : un nœud formule une seconde demande pour rejoindre un même cluster avant l'aboutissement de la première demande et la stabilisation du cluster.**

Le cluster peut ne pas fonctionner correctement, et les commandes de l'interface de ligne de commande « get cluster status » et « get cluster config » peuvent renvoyer une erreur.

Solution : n'émettez pas de nouvelle commande de jonction dans un délai de 10 minutes suivant la première demande de jonction, en vue de rejoindre un même cluster.

- **Problème 2275388 : les itinéraires des interfaces de bouclage/connectés peuvent être redistribués avant l'ajout de filtres destinés à refuser les itinéraires.**

Des mises à jour inutiles des routes peuvent entraîner le détournement du trafic de quelques secondes à quelques minutes.

Solution : aucune.

- **Problème 2275708 : impossible d'importer un certificat avec sa clé privée lorsque celle-ci comporte une phrase secrète.**

Le message renvoyé est le suivant : « Données PEM reçues non valides pour le certificat. (Code d'erreur : 2002) ». Impossible d'importer un nouveau certificat avec une clé privée.

Solution :

1. Créez un certificat avec une clé privée. N'entrez pas une nouvelle phrase secrète lorsque vous y êtes invité. Appuyez plutôt sur Entrée.
2. Sélectionnez « Importer un certificat », puis sélectionnez le fichier de certificat et le fichier de clé privé.

Vérifiez l'opération en ouvrant le fichier de clé. Si une phrase secrète a été entrée lors de la génération de la clé, la deuxième ligne du fichier indique quelque chose comme « Proc-Type: 4,ENCRYPTED ».

Cette ligne est manquante si le fichier de clé a été généré sans phrase secrète.

- **Problème 2277742 : l'appel de PUT https://<MGR_IP>/api/v1/configs/management avec un corps de demande définissant publish_fqdns sur true peut échouer si le dispositif NSX-T Manager est configuré avec un nom de domaine complet et non un simple nom d'hôte.**

PUT https://<IP_MGR>/api/v1/configs/management ne peut pas être appelée si un nom de domaine complet est configuré.

Solution : déployez NSX Manager à l'aide d'un nom d'hôte au lieu d'un nom de domaine complet.

- **Problème 2279249** : la VM Instant Clone perd brièvement la protection AV pendant son déplacement avec vMotion.

La machine virtuelle Instant Clone a migré d'un hôte vers un autre. Immédiatement après la migration, le fichier eicar est oublié sur la machine virtuelle. Brève perte de la protection antivirus.

Solution : aucune.

- **Problème 2292116** : le profil IPFIX L2 appliqué avec un groupe d'adresses IP basé sur le CIDR ne s'affiche pas sur l'interface utilisateur lorsque le groupe est créé via la page IPFIX L2. Si vous essayez de créer un groupe d'adresses IP à partir de la boîte de dialogue Appliqué à et si vous saisissez une adresse IP ou un CIDR incorrect dans la boîte de dialogue Définir les membres, ces derniers ne sont pas répertoriés dans Groupes. Vous devez modifier à nouveau ce groupe pour entrer des adresses IP valides.

Solution : accédez à la page répertoriant les groupes et ajoutez des adresses IP dans le groupe concerné. Ce groupe peut ensuite commencer à compléter la boîte de dialogue Appliqué à.

- **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 2268406** : la boîte de dialogue Ancrage de balise n'affiche pas toutes les balises lorsque le nombre maximal de balises est ajouté.

La boîte de dialogue Ancrage de balise n'affiche pas toutes les balises lorsque le nombre maximal de balises est ajouté, et il n'est pas possible de la redimensionner ou de la faire défiler. Toutefois, l'utilisateur peut toujours afficher toutes les balises sur la page Résumé. Aucune donnée n'est perdue.

Solution : affichez plutôt les balises dans la page Résumé.

- **Problème 2310650** : l'interface affiche le message d'erreur « La demande a expiré ». Plusieurs pages sur l'interface affichent le message suivant : « La demande a expiré. Cela peut se produire lorsque le système subit une charge ou s'il manque de ressources. »

Solution : à l'aide de SSH, connectez-vous à la VM NSX Manager et exécutez la commande d'interface de ligne de commande `start search resync manager`.

- **Problème 2320529** : l'erreur « Le stockage n'est pas accessible pour le déploiement du service » s'est produite après l'ajout de VM tierces pour les banques de données récemment ajoutées.

L'erreur « Le stockage n'est pas accessible pour le déploiement du service » s'est produite après l'ajout de VM tierces pour les banques de données récemment ajoutées, même si le stockage est accessible depuis tous les hôtes du cluster. Cet état d'erreur dure 30 minutes au maximum.

Solution : réessayez au bout de 30 minutes. Vous pouvez également effectuer l'appel d'API suivant pour mettre à jour l'entrée de cache de la banque de données :

`https://{{NsxMgrIP}}/api/v1/fabric/compute-collections/<CC Ext ID>/storage-resources?uniform_cluster_access=true&source=realtime`

où NsxMgrIP est l'adresse IP de l'instance de NSX Manager dans laquelle l'API de déploiement de service a échoué, et CC Ext ID est l'identifiant dans NSX du cluster dans lequel le déploiement est tenté.

- **Problème 2320855** : la nouvelle balise de sécurité de VM n'est pas créée si l'utilisateur ne clique pas sur le bouton Ajouter/vérifier.

Problème d'interface. Si un utilisateur ajoute une nouvelle balise de sécurité à un objet de stratégie ou à un inventaire et clique sur Enregistrer sans d'abord cliquer sur le bouton Ajouter/vérifier en regard du champ de paire balise-étendue, la nouvelle paire de balises n'est pas créée.

Solution : veillez à cliquer sur le bouton Ajouter/vérifier avant de cliquer sur Enregistrer.

- **Problème 2328126** : problème de bare metal : L'interface de liaison du système d'exploitation Linux utilisée dans le profil de liaison montante NSX renvoie une erreur.

Lorsque vous créez une interface de liaison dans le système d'exploitation Linux, puis que vous utilisez cette interface dans le profil de liaison montante NSX, le message d'erreur suivant s'affiche : « La création du nœud de transport peut échouer. » Ce problème se produit, car VMware ne prend pas en charge la liaison du système d'exploitation Linux. Toutefois, VMware prend en charge la liaison Open vSwitch (OVS) pour les nœuds de transport de serveur bare metal.

Solution : si vous rencontrez ce problème, reportez-vous à l'article 67835 de la base de connaissances [Bare Metal Server supports OVS bonding for Transport Node configuration in NSX-T \(Le serveur bare metal prend en charge la liaison OVS pour la configuration du nœud de transport dans NSX-T\)](#).

- **Problème 2334442** : l'utilisateur n'est pas autorisé à modifier ni à supprimer des objets créés après le changement de nom de l'utilisateur admin.

L'utilisateur n'a pas l'autorisation de modifier ou de supprimer des objets créés après le changement de nom de l'utilisateur admin. Impossible de renommer des utilisateurs admin/auditeur.

Solution : redémarrez la stratégie après le changement de nom en émettant la commande « service nsx-policy-manager restart »

- **Problème 2261818** : les itinéraires appris par le voisin eBGP sont annoncés en retour au même voisin.

L'activation des journaux de débogage BGP indique les paquets reçus en retour et les paquets abandonnés avec un message d'erreur. Le processus BGP consommera des ressources de CPU supplémentaires lors de la suppression des messages de mise à jour envoyés aux homologues. S'il existe un grand nombre de routes et d'homologues, cela peut affecter la convergence de route.

Solution : aucune.

- **Problème 2390624** : la règle d'anti-affinité empêche la machine virtuelle de service de vMotion lorsque l'hôte est en mode de maintenance.

Si une machine virtuelle de service est déployée dans un cluster avec exactement deux hôtes, la paire HA avec la règle d'anti-affinité empêchera les machines virtuelles de se déplacer vers l'autre hôte pendant les tâches en mode de maintenance. Cela peut empêcher l'hôte d'entrer automatiquement en mode de maintenance.

Solution : mettez la machine virtuelle de service hors tension sur l'hôte avant le démarrage de la tâche en mode de maintenance sur vCenter.

Problèmes connus d'installation

- **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.

Problèmes connus de NSX Manager

- **Problème 2282798** : l'enregistrement de l'hôte peut échouer lorsqu'un trop grand nombre de demandes/hôtes essaient de s'enregistrer simultanément avec NSX Manager. Ce problème entraîne le passage de l'état du nœud d'infrastructure sur ÉCHEC. L'appel d'API de l'état du nœud d'infrastructure indique « Le client n'a pas encore répondu aux signaux de pulsation ». Le fichier `/etc/vmware/nsx-mpa/mpaconfig.json` sur l'hôte est également vide.

Solution : utilisez la procédure suivante pour résoudre ce problème.

1. Utilisez l'option Programme de résolution.
2. Supprimez le nœud d'infrastructure de NSX.
3. Rajoutez de nouveau le nœud d'infrastructure manuellement via la commande d'interface de ligne de commande « `join management-plane` ».

Problèmes connus de NSX Edge

- **Problème 2283559** : les API `MP /routing-table` et `/forwarding-table` renvoient une erreur si le dispositif Edge comporte plus de 65 000 routes pour RIB et plus de 100 000 pour FIB. Si le dispositif Edge comporte plus de 65 000 routes pour RIB et plus de 100 000 pour FIB, la demande de l'interface multiprotocole au dispositif Edge prend plus de 10 secondes et expire. Il s'agit d'une API en lecture seule qui a un impact uniquement s'il est nécessaire de télécharger les 65 000 routes minimum pour RIB et les 100 000 routes minimum pour FIB à l'aide de l'API/interface utilisateur.

Solution : il existe deux options pour extraire les tables RIB/FIB.

- Ces API prennent en charge les options de filtrage basées sur les préfixes de réseau ou le type de route. Utilisez ces options pour télécharger les routes qui vous intéressent.
- Prise en charge d'une interface de ligne de commande au cas où l'intégralité des tables RIB/FIB soit nécessaire et en l'absence de délai d'expiration.
- **Problème 2204932** : la configuration de l'homologation BGP peut retarder la récupération du basculement HA. Lorsque l'homologation BGP dynamique est configurée sur les routeurs qui s'associent aux dispositifs Edge T0 et qu'un événement de basculement se produit sur les dispositifs Edge (mode actif-en veille), le voisin BGP peut prendre jusqu'à 120 secondes.

Solution : configurez des homologues BGP spécifiques pour éviter le retard.

- **Problème 2285650** : les tables de route BGP sont remplies avec des routes indésirables. Lorsque l'option `allowas-in` est activée dans le cadre de la configuration de BGP, les routes annoncées par les nœuds Edge sont reçues et installées dans la table de route BGP. Cela entraîne un excès de consommation de mémoire et de traitement du calcul de routage. Si une préférence locale supérieure est configurée pour les routes excédentaires, cette boucle de transfert peut entraîner le remplissage de la table de route sur certains routeurs avec des routes redondantes.

Par exemple, la route X est issue du routeur D, qui est annoncé aux routeurs A et B. Le routeur C, sur lequel `allowas-in` est activé, est associé à B, il apprend donc la route X et l'installe dans sa table de route. Par conséquent, il existe maintenant deux chemins pour que l'itinéraire X soit annoncé au routeur C, ce qui entraîne le problème.

Solution : vous pouvez empêcher les boucles de transfert en configurant le routeur problématique (ou son homologue) pour qu'il bloque les routes qui lui sont annoncées.

Problèmes connus de mise en réseau logique

- **Problème 2243415 :** le client ne parvient pas à déployer le service EPP en utilisant le commutateur logique (comme un réseau de gestion).
Dans l'écran de déploiement d'EPP, l'utilisateur ne peut pas voir un commutateur logique dans la commande de sélection du réseau. Si l'API est utilisée directement avec le commutateur logique indiqué comme réseau de gestion, l'utilisateur voit le message d'erreur suivant : « Le réseau spécifié n'est pas accessible pour le déploiement du service. »

Solution : effectuez le déploiement en utilisant un autre type de commutateur, comme un commutateur local ou distribué.

- **Problème 2288774 :** le port de segment génère une erreur de réalisation en raison du dépassement du nombre maximal de balises (erreur), soit 30.
La saisie de l'utilisateur tente, à tort, d'appliquer plus de 30 balises. Cependant, le workflow de la stratégie ne valide/rejette pas correctement la saisie de l'utilisateur et autorise la configuration. La stratégie affiche ensuite une alarme avec le message d'erreur approprié, indiquant que l'utilisateur ne doit pas utiliser plus de 30 balises. À ce stade, l'utilisateur peut corriger ce problème.

Solution : corrigez la configuration après l'affichage du message d'erreur.

- **Problème 2320147 :** VTEP manquant sur l'hôte affecté.
Si un LogSwitchStateMsg est supprimé et ajouté dans la même transaction et que cette opération est traitée par le plan de contrôle central avant que le plan de gestion n'ait envoyé le commutateur logique, l'état du commutateur logique ne sera pas mis à jour. Par conséquent, le trafic ne peut pas circuler vers ou depuis le VTEP manquant.

Solution : si vous rencontrez ce problème, redémarrez le plan de contrôle central.

- **Problème 2327904 :** après l'utilisation de l'interface de liaison Linux pré-crée en tant que liaison montante, le trafic est instable ou échoue.
NSX-T ne prend pas en charge les interfaces de liaison Linux pré-crées comme liaison montante.

Solution : pour la liaison montante, utilisez la configuration d'une liaison native OVS à partir du profil de liaison montante.

- **Problème 2295819 :** le pont L2 est bloqué dans l'état « Arrêté », même si la VM Edge et PNIC sont actifs.
Le pont L2 peut être bloqué dans l'état « Arrêté », même si la VM Edge et le PNIC qui soutient le port de pont L2 sont actifs. Cela est dû au fait que le LCP Edge ne parvient pas à mettre à jour l'état de PNIC dans son cache local, ce qui suppose que le PNIC est inactif.

***Impact pour le client* :**

Interruption du trafic pour les VM accessibles par le port I2bridge Edge

Solution : redémarrez l'agent de contrôle local sur la VM Edge concernée.

- **Problème 2389993 :** la carte de route a été supprimée après la modification de la règle de redistribution à l'aide de la page de stratégie ou de l'API.
Une carte de route ajoutée à une règle de redistribution à partir de l'interface du plan de gestion ou de l'API peut être supprimée si la même règle de redistribution est ensuite modifiée via l'interface de la page de stratégie ou l'API. Cela est dû au fait que l'interface de page de stratégie ou l'API ne prend pas en charge l'ajout de mappages de route. Cela peut entraîner l'annonce de préfixes indésirables à l'homologue BGP.

Solution : vous pouvez restaurer la carte de route en renvoyant l'interface du plan de gestion ou l'API pour l'ajouter à nouveau à la même règle. Si vous souhaitez inclure une carte de route dans une règle de redistribution, il est recommandé de toujours utiliser l'interface du plan de gestion ou l'API pour la créer et la modifier.

Problèmes connus des services de sécurité

- **Problème 2395334** : paquets (Windows) abandonnés de manière incorrecte en raison de l'entrée *contrack* de règle de pare-feu sans état.

Les règles de pare-feu sans état ne sont pas correctement prises en charge sur les machines virtuelles Windows.

Solution : ajoutez plutôt une règle de pare-feu avec état.

Problèmes connus d'équilibreur de charge

- **Problème 2290899** : le VPN IPsec ne fonctionne pas ; la réalisation du plan de contrôle pour IPsec échoue.

Le VPN IPsec (ou L2VPN) ne parvient pas à fonctionner si plus de 62 serveurs d'équilibreur de charge sont activés sur le même nœud Edge que le service IPsec de niveau 0.

Solution : abaissez le nombre de serveurs d'équilibreur de charge en dessous de 62.

- **Problème 2318525** : les routes IPv6 de tronçon suivant (comme l'adresse IP de l'homologue eBGP) sont modifiées par leurs propres adresses IP.

Dans le cas de sessions IP4 eBGP, des routes IPv4 annoncées qui ont leur homologue eBGP comme tronçon suivant, le tronçon suivant de la route n'est pas modifié du côté de l'expéditeur par sa propre adresse IP. Cela fonctionne pour IPv4 mais, pour les sessions IPv6, le tronçon suivant de la route est modifié du côté de l'expéditeur par sa propre adresse IP. Ce comportement peut entraîner des boucles de route.

Solution : aucune.

- **Problème 2362688** : si certains membres du pool sont INACTIFS dans un service d'équilibreur de charge, l'interface utilisateur affiche l'état consolidé comme étant ACTIF.

Lorsqu'un membre du pool est inactif, il n'existe aucune indication sur l'interface utilisateur de la stratégie dans laquelle l'état du pool est vert et Actif.

Solution : Solution : aucune.

Problèmes connus d'interopérabilité entre les solutions

- **Problème 2289150** : les appels PCM au démarrage d'AWS échouent.

Si vous redéfinissez le rôle de la PCG *ancien-rôle-pcg* d'un compte AWS du CSM sur *nouveau-rôle-pcg*, le CSM met à jour le rôle de l'instance de la PCG sur AWS vers *nouveau-rôle-pcg*. Toutefois, le PCM ne sait pas que le rôle de la PCG a été mis à jour et, par conséquent, il continue d'utiliser les anciens clients AWS qu'il avait créés à l'aide du rôle *ancien-rôle-pcg*. Cela entraîne l'échec de l'analyse de l'inventaire cloud AWS PCM et des autres appels cloud AWS.

Solution : si vous rencontrez ce problème, ne modifiez/supprimez pas l'ancien rôle de la PCG immédiatement après la définition du nouveau rôle. Attendez au moins 6,5 heures. Le redémarrage de la PCG réinitialise tous les clients AWS avec les informations d'identification du nouveau rôle.

Problèmes connus des opérations et des services de surveillance

- **Problème 2316943** : charge de travail non protégée brièvement pendant vMotion.

VMware Tools prend quelques secondes pour signaler le nom d'ordinateur correct pour la VM après vMotion. Par conséquent, les VM ajoutées à NSGroups à l'aide du nom d'ordinateur ne sont pas protégées pendant quelques secondes après vMotion.

Solution : pour les groupes à utiliser dans les règles DFW, utilisez des critères basés sur le nom de VM plutôt que des critères basés sur le nom d'ordinateur.

Problèmes connus de mise à niveau

- **Problème 2288549** : RepoSync échoue avec un échec du total de contrôle sur le fichier de manifeste.

Observé dans les déploiements récemment mis à niveau vers 2.4. Lorsqu'une configuration mise à niveau est sauvegardée et restaurée sur un nouveau gestionnaire déployé, le total de contrôle du manifeste du référentiel présent dans la base de données et le total de contrôle du fichier de manifeste réel ne correspondent pas. Cela entraîne le marquage de RepoSync comme ayant échoué après la restauration d'une sauvegarde.

Solution : pour remédier à cet échec, effectuez les étapes suivantes :

1. Exécutez la commande de l'interface de ligne de commande `get service install-upgrade`.
Notez l'adresse IP indiquée par « Activé sur » dans les résultats.
2. Connectez-vous à l'adresse IP de NSX Manager indiqué dans l'élément renvoyé « Activé sur » de la commande ci-dessus.
3. Accédez à **Système > Présentation** et recherchez le nœud ayant la même adresse IP que l'élément renvoyé « Activé sur ».
4. Cliquez sur **Résoudre** sur ce nœud.
5. Une fois l'opération de résolution ci-dessus réussie, cliquez sur **Résoudre** sur tous les nœuds se trouvant dans la même interface.

Les trois nœuds indiquent à présent l'état RepoSync Terminé.

- **Problème 2277543** : la mise à jour de VIB de l'hôte échoue lors de la mise à niveau sur place avec l'erreur « Échec de l'installation du bundle hors ligne sur l'hôte ».

Cette erreur peut se produire lorsque Storage vMotion a été exécuté sur l'hôte avant d'effectuer une mise à niveau sur place de NSX-T 2.3.x vers 2.4 et des hôtes exécutant ESXi-6.5 P03 (build 10884925). Le module de sécurité du commutateur de 2.3.x n'est pas supprimé si Storage vMotion a été exécuté juste avant la mise à niveau de l'hôte. Storage vMotion déclenche une fuite de mémoire provoquant l'échec du déchargement du module de sécurité du commutateur.

Solution : consultez l'article 67444 de la base de connaissances [Host VIB update may fail when upgrading from NSX-T 2.3.x to NSX-T 2.4.0 if VMs are storage vMotioned before host upgrade](#) (La mise à jour de VIB de l'hôte peut échouer lors de la mise à niveau de NSX-T 2.3.x vers NSX-T 2.4.0 si des VM sont migrées par Storage vMotion avant la mise à niveau de l'hôte).

- **Problème 2276398** : lorsqu'une VM de service de partenaires AV est mise à niveau à l'aide de NSX, il peut y avoir jusqu'à 20 minutes de perte de protection.

Lorsqu'une SVM de partenaire est mise à niveau, la nouvelle SVM est déployée et l'ancienne SVM est supprimée. Des erreurs de connexion SolutionHandler peuvent s'afficher sur l'hôte Syslog.

Solution : supprimez l'entrée de cache ARP sur l'hôte après la mise à niveau, puis exécutez une commande ping sur l'adresse IP du contrôleur de partenaire sur l'hôte pour résoudre ce problème.

- **Problème 2330417** : impossible de procéder à la mise à niveau pour les nœuds de transport non mis à niveau.

Lors de la mise à niveau, la mise à niveau est marquée comme réussie, même si certains nœuds de transport ne sont pas mis à niveau. Emplacement du journal : `/var/log/upgrade-coordinator/upgrade-coordinator.log`.

Solution : redémarrez le service `upgrade-coordinator`.

Problèmes connus de l'API

- **Problème 2260435** : des stratégies/règles de redirection sans état sont créées par défaut par l'API, ce qui n'est pas pris en charge pour les connexions horizontales.

Des stratégies/règles de redirection sans état sont créées par défaut par l'API, ce qui n'est pas pris en charge pour les connexions horizontales. Par conséquent, le trafic n'est pas redirigé vers les partenaires.

Solution : lors de la création de stratégies de redirection à l'aide de l'API de stratégie, créez une section avec état.

- **Problème 2332397 : l'API permet de créer des stratégies DFW dans un domaine inexistant.**
Après la création d'une telle stratégie sur un domaine qui n'existe pas, l'interface cesse de répondre lorsque l'utilisateur ouvre un onglet de sécurité DFW. Le journal approprié est `/var/log/policy/policy.log`.

Solution : créez le domaine avec le même ID que celui sur lequel la stratégie a été créée. Cela permet de réussir la validation.

Problèmes connus de NSX Cloud

- **Problème 2275232 : DHCP ne fonctionne pas pour les machines virtuelles du cloud si Connectivity_statregy du DFW passe de LISTE NOIRE à LISTE BLANCHE.**
Toutes les machines virtuelles demandant de nouveaux baux DHCP perdent alors des adresses IP. Vous devez explicitement autoriser DHCP dans le DFW pour les machines virtuelles du cloud.

Solution : autorisez explicitement DHCP dans le DFW pour les machines virtuelles du cloud.