



Notes de mise à jour de VMware NSX-T Data Center 2.5

VMware NSX-T Data Center 2.5 | 19 septembre 2019 | Build 14663974

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](#)
- [Obsolescences de l'API et changements de comportement](#)
- [Langues disponibles](#)
- [Ressources relatives aux interfaces de ligne de commande et aux API](#)
- [Historique de révision](#)
- [Problèmes résolus](#)
- [Problèmes connus](#)

Nouveautés

NSX-T Data Center 2.5 offre un grand nombre de nouvelles fonctionnalités destinées à la virtualisation de la mise en réseau et de la sécurité pour les clouds privés, publics et hybrides. Les nouveautés incluent des améliorations apportées à l'interface utilisateur de mise en réseau basée sur l'intention, le pare-feu sensible au contexte, les fonctionnalités Guest Introspection et Introspection réseau, la prise en charge d'IPv6, la gestion de clusters haute disponibilité, l'installation de NSX basée sur les profils pour les clusters de calcul et les améliorations apportées au coordinateur de migration pour la migration de NSX Data Center for vSphere vers NSX-T Data Center.

NSX Intelligence

NSX-T Data Center 2.5 inclut NSX Intelligence v1.0, un nouveau composant d'analyse NSX. NSX Intelligence inclut une interface utilisateur via un volet de gestion unique dans NSX Manager et propose les fonctionnalités suivantes :

- Informations de flux quasi en temps réel pour les charges de travail de votre environnement.
- NSX Intelligence corrèle les flux en direct ou historiques, les configurations d'utilisateur et l'inventaire des charges de travail.
- Possibilité d'afficher les dernières informations sur les flux, les configurations d'utilisateur et l'inventaire des charges de travail.
- Planification automatisée de la micro-segmentation en recommandant des règles de pare-feu, des groupes et des services.

Prise en charge de l'API de conteneur

La prise en charge d'une nouvelle API est disponible pour l'inventaire de conteneurs. Consultez la documentation de l'API.

Mise en réseau L2

- **Améliorations du pont Edge** : le pont Edge permet désormais d'associer le même segment à plusieurs profils de pont, permettant ainsi de relier plusieurs fois un segment aux VLAN de l'infrastructure physique. Cette nouvelle fonctionnalité remplace et annule le pont ESXi d'origine dans les versions précédentes de NSX-T Data Center. **Attention** : utilisez cette fonctionnalité à vos propres risques. Elle présente le risque de création d'une boucle de pontage en reliant deux fois le même segment au même domaine de couche 2 dans le réseau physique. Il n'existe aucun mécanisme d'atténuation de boucle.
- **Contrôle de santé du MTU/du VLAN** : d'un point de vue opérationnel, les problèmes de connectivité réseau causés par des erreurs de configuration sont souvent difficiles à identifier. Les scénarios courants incluent ceux dans lesquels les administrateurs de réseau virtuel utilisent NSX Manager alors que les administrateurs de réseau physique gèrent les commutateurs réseau physiques.
 - **Contrôle de santé du VLAN** : vérifie si les paramètres du N-VDS VLAN correspondent à la configuration du port de jonction sur les ports de commutateur physique adjacents.
 - **Contrôle de santé du MTU** : vérifie si la valeur MTU du port de commutateur d'accès physique basé sur chaque VLAN correspond à la valeur MTU N-VDS.
- **Balises d'invité inter-VLAN** : le N-VDS de chemin de données optimisé permet aux utilisateurs de mapper une balise VLAN d'invité à un segment. Cette fonction permet de surcharger la limite de 10 vNIC par VM et d'acheminer le trafic balisé du VLAN invité (mappé à différents segments) via l'infrastructure NSX.

Mise en réseau L3

- **Placement de niveau 1 dans le cluster Edge en fonction du domaine de pannes** : permet à NSX-T de placer automatiquement les passerelles de niveau 1 en fonction des domaines de pannes définis par l'utilisateur. Cela augmente la fiabilité des passerelles de niveau 1 dans les zones de disponibilité, les racks ou les hôtes, même en cas d'utilisation du placement automatique de la passerelle de niveau 1.
- **Partage de charges asymétriques après une panne de routeur dans la topologie ECMP** : sur la passerelle de niveau 0 active/active lorsqu'un routeur de service était défaillant, un autre routeur relayait le trafic du routeur défaillant, doublant ainsi le trafic passant par le routeur de service. Dans les 30 minutes suivant la défaillance d'un routeur, l'adresse IP du routeur défaillant est supprimée de la liste de tronçons suivants, ce qui évite le trafic supplémentaire vers un routeur spécifique.
- **Obtenir les itinéraires BGP publiés et reçus par homologue via l'API** : simplifie les opérations BGP en évitant l'utilisation de l'interface de ligne de commande pour vérifier les itinéraires reçus et envoyés aux homologues BGP.
- **Prise en charge étendue de la communauté BGP** : offre la possibilité d'utiliser des communautés conjointement avec un ASN à 4 octets, tel que défini dans RFC8092.
- **Option Mode d'assistance de redémarrage normal BGP par homologue** : offre l'option d'une passerelle de niveau 0 pour faciliter le maintien du routeur pour les routeurs physiques en direction du nord avec un plan de contrôle redondant sans compromettre la durée de basculement entre les routeurs de niveau 0.
- **API en vrac pour créer plusieurs règles NAT** : améliore l'API NAT existante pour regrouper la création d'un grand nombre de règles NAT en un seul appel d'API.

Plate-forme Edge

- **Prise en charge de Mellanox ConnectX-4 et de ConnectX-4 LX sur le nœud Edge Bare Metal** : les nœuds Bare Metal prennent désormais en charge les cartes réseau physiques Mellanox ConnectX-4 et Connect-4 LX dans 10/25/40/50/100 Gbits/s.
- **Gestion de PNIC Edge Bare Metal** : permet de sélectionner les cartes réseau physiques à utiliser comme cartes réseau de plan de données (chemin d'accès rapide). Cette option augmente

également le nombre de cartes réseau physiques prises en charge sur le nœud Edge Bare Metal de 8 à 16 PNIC.

Amélioration de la prise en charge d'IPv6

NSX-T 2.5 continue d'améliorer l'ensemble des fonctionnalités de routage/transfert IPv6. Cela comprend la prise en charge des éléments suivants :

- SLAAC IPv6 (configuration automatique d'adresse sans état), fournissant automatiquement des adresses IPv6 aux machines virtuelles.
- Annonce de routeur IPv6, la passerelle NSX-T fournit les paramètres IPv6 via l'annonce de routeur.
- IPv6 DAD, la passerelle NSX-T détecte l'allocation des adresses IPv6 en double.

Améliorations du pare-feu

Prise en charge de l'AppID de couche 7

NSX-T 2.5 ajoute des capacités de couche 7 supplémentaires pour le pare-feu distribué et de passerelle. Cela comprend la prise en charge des éléments suivants :

- Prise en charge de l'AppID de couche 7 pour le pare-feu distribué sur KVM.
- Prise en charge de l'AppID de couche 7 pour le pare-feu de passerelle.
- Configuration de plusieurs AppID de couche 7 dans une règle de pare-feu unique.

Améliorations du filtrage de nom de domaine complet/d'URL

NSX-T 2.5 présente des améliorations mineures de la prise en charge du filtrage de noms de domaines complets, notamment :

- Configuration des temporisateurs TTL pour les entrées DNS.
- Prise en charge des charges de travail exécutées sur l'hyperviseur KVM.

Les opérations de pare-feu ont été améliorées avec les fonctionnalités suivantes :

- **Fonctionnalité de configuration et de restauration de l'enregistrement automatique** : le système crée une copie de la configuration lors de sa publication. Cette configuration peut être redéployée pour revenir à un état existant.
- **Brouillons manuels** : les utilisateurs peuvent désormais enregistrer un brouillon de leurs règles avant de publier ces ensembles de règles pour application. Les utilisateurs peuvent organiser les règles dans les brouillons manuels. Le système vous permet d'autoriser plusieurs utilisateurs à travailler sur le même brouillon avec un mécanisme de verrouillage pour désactiver le remplacement des règles de différents utilisateurs.
- **Temporisateurs de session** : les utilisateurs peuvent configurer des temporisateurs de session pour les sessions TCP, UDP et ICMP.
- **Protection de propagation** : le pare-feu distribué et le pare-feu de passerelle peuvent comporter une protection SynFlood. Les utilisateurs peuvent fournir des seuils d'alerte, de journalisation et de rejet du trafic pour en faire des workflows personnalisés.
- **Le système génère automatiquement deux groupes** lorsque l'équilibreur de charge NSX est créé et que des serveurs virtuels sont déployés. Un groupe contient le pool de serveurs tandis que l'autre groupe contient l'adresse IP du serveur virtuel. Ces groupes peuvent être utilisés sur un pare-feu distribué ou un pare-feu de passerelle pour autoriser ou refuser le trafic par les administrateurs du pare-feu. Ces groupes suivent les modifications de configuration de l'équilibreur de charge NSX.
- **Le nombre d'adresses IP détecté par VM-vNIC a augmenté de 128 à 256 adresses IP.**

Pare-feu d'identité

- Avec NSX-T 2.5, nous prenons en charge les serveurs Active Directory déployés sur Windows 2016.
- Nous prenons en charge le pare-feu d'identité pour les charges de travail Windows Server sans activation des services Terminal Server. Cela permet aux clients de contrôler strictement le déplacement latéral des administrateurs d'un serveur vers un autre.

Insertion de services

- **Prise en charge de la copie de paquets** : outre la redirection du trafic via un service, NSX-T prend désormais en charge le cas d'utilisation de surveillance réseau, dans lequel une copie des paquets est transférée vers une machine virtuelle de service de partenaires (SVM), permettant ainsi l'inspection, la surveillance ou la collecte des statistiques lorsque le paquet d'origine ne passe pas par le service de surveillance réseau.
- **Déploiement automatique de SVM de partenaires basés sur l'hôte** : à partir de NSX-T 2.5, deux modes de déploiement de SVM de partenaires sont pris en charge : le déploiement en cluster dans lequel les machines virtuelles de service sont déployées sur un cluster vSphere (service) dédié et le déploiement basé sur l'hôte, où une machine virtuelle de service par service est déployée sur chaque hôte de calcul dans un cluster particulier. Dans ce mode, lorsqu'un nouvel hôte de calcul est ajouté à un cluster, les SVM appropriées sont automatiquement déployées.
- **Prise en charge des notifications pour l'insertion de services Nord-Sud** : NSX-T 2.4 a introduit la structure de notification pour l'insertion de services Est-Ouest, qui permet aux services de partenaires de recevoir automatiquement des notifications en cas de modifications pertinentes, telles que les mises à jour de groupe dynamiques. Avec NSX-T 2.5, cette infrastructure de notification a également été étendue à l'insertion de services N-S. Les partenaires peuvent tirer parti de ce mécanisme afin de permettre aux clients d'utiliser des groupes NSX dynamiques (c.-à-d. en fonction des balises, du système d'exploitation et du nom de la VM) dans la stratégie de partenaire.
- **Fonctionnalités supplémentaires de dépannage et de visualisation** : avec NSX-T 2.5, plusieurs améliorations de fonctionnement ont été apportées afin de permettre un meilleur dépannage des problèmes liés à l'insertion de services. Cela inclut la possibilité de vérifier l'état d'exécution d'une instance de service, la possibilité d'extraire les chemins de service disponibles via l'API et l'inclusion des journaux liés à l'insertion de services dans le bundle de support.

Protection de point de terminaison (Guest Introspection)

- **Prise en charge de Linux** : prise en charge des systèmes d'exploitation basés sur Linux avec protection de point de terminaison. Consultez le Guide d'administration de NSX-T des systèmes d'exploitation Linux pris en charge pour Guest Introspection.
- **Tableau de bord de protection de point de terminaison** : tableau de bord de protection de point de terminaison pour la visibilité et la surveillance de l'état de configuration des VM protégées et non protégées, problèmes liés à l'agent hôte et aux VM de service, et VM configurées avec le pilote d'introspection de fichiers installé dans le cadre de l'installation de VMware Tools.
- **Tableau de bord de surveillance** : permet de surveiller l'état du déploiement du service de partenaires sur les clusters du système.

Équilibrage de charge

- **API pour récupérer l'état sur la capacité Edge pour les équilibreurs de charge** : de nouveaux appels d'API ont été ajoutés afin de permettre à l'administrateur de surveiller la capacité du dispositif Edge en termes d'instances d'équilibrage de charge.
- **Sélection intelligente de l'adresse IP du contrôle de santé** : lorsque la liste d'adresses IP SNAT est configurée, la première adresse IP de la liste va être utilisée pour la surveillance de la santé à la place de l'adresse IP de liaison montante d'une passerelle de niveau 1. L'adresse IP peut être la même que l'adresse IP du serveur virtuel. Cette amélioration permet à l'équilibreur de charge d'utiliser une adresse IP unique pour la surveillance source-NAT et la surveillance de la santé.
- **Amélioration de la journalisation de l'équilibreur de charge** : grâce à cette amélioration, l'équilibreur de charge peut générer un message de journal enrichi par serveur virtuel pour la surveillance. Par exemple, le journal d'accès au serveur virtuel inclut non seulement l'adresse IP du client, mais également une adresse IP du membre du pool.
- **Amélioration persistante dans les règles d'équilibreur de charge** : une nouvelle action nommée « Persistance » est introduite dans les règles d'équilibreur de charge. L'action Persistance permet à l'équilibreur de charge d'assurer la persistance des applications en fonction d'un cookie défini par un membre du pool.

- **L'équilibreur de charge s'adapte** : une petite instance d'équilibreur de charge peut s'adapter à une VM Edge de petite taille. Une instance d'équilibreur de charge moyenne peut s'adapter à une VM Edge de taille moyenne. Auparavant, la VM Edge de petite taille ne prenait pas en charge les services d'équilibrage de charge, car la taille d'une VM Edge devait être supérieure à celle d'une instance d'équilibreur de charge.
- **Statistiques de VS/pool/membre** : toutes les statistiques liées à l'équilibreur de charge sont disponibles dans une interface simplifiée. Auparavant, les informations étaient uniquement disponibles dans l'interface avancée de mise en réseau et de sécurité.
- **Prise en charge d'ECC (Elliptical Curve Certificate) pour l'arrêt SSL** : des certificats EC peuvent être utilisés pour améliorer les performances de SSL.
- **Bouton FIPS** : il existe un paramètre global via l'API pour la conformité FIPS des équilibrages de charge. Par défaut, le paramètre est désactivé pour améliorer les performances.

VPN

- **Prise en charge du VPN IPsec sur la passerelle de niveau 1** : un VPN IPsec peut être déployé et arrêté sur une passerelle de niveau 1 pour améliorer l'isolation et l'évolutivité des locataires. Auparavant, ce dernier était pris en charge uniquement sur la passerelle de niveau 0.
- **Prise en charge du VLAN pour le VPN de couche 2 sur NSX géré par Edge** : grâce à cette amélioration, les segments basés sur VLAN peuvent être étendus. Auparavant, seuls les segments logiques étaient pris en charge pour l'extension de couche 2. Cela inclut la prise en charge de la jonction VLAN permettant l'extension de plusieurs VLAN sur une interface Edge et une session VPN de couche 2.
- **Verrouillage MSS TCP pour le VPN IPsec** : le verrouillage MSS TCP permet à l'administrateur d'appliquer la valeur MSS de toutes les connexions TCP afin d'éviter la fragmentation des paquets.
- **Prise en charge d'ECC (Elliptical Curve Certificate) pour le VPN IPsec** : le certificat EC est nécessaire pour activer diverses suites de conformité IPsec, telles que CNSA, UK Prime, etc.
- **Bouton simple pour la configuration de la suite de conformité** : CNSA, Suite-B-GCM, Suite-B-GMAC, Prime, Fondation et FIPS peuvent être configurés en un seul clic dans l'interface utilisateur ou un seul appel d'API.

Automatisation, OpenStack et autres CMP

- **Prise en charge étendue de la version d'OpenStack** : inclut désormais les versions Stein et Rocky.
- **Plug-in OpenStack Neutron prenant en charge l'API de stratégie** : en plus de l'API de gestion de prise en charge du plug-in existant, nous proposons désormais un plug-in OpenStack Neutron utilisant la nouvelle API de stratégie NSX-T. Ce plug-in prend en charge IPv6 pour la couche 2, L3, le pare-feu et SLAAC.
- **Optimisation du routeur OpenStack Neutron** : le plug-in optimise désormais le routeur OpenStack Neutron en gérant la création/suppression du routeur de service de façon dynamique. Cela permet à un client d'avoir uniquement un routeur distribué lorsqu'aucun service n'est configuré et un autre dès que les services sont ajoutés, tous gérés par le plug-in.
- **Plug-in OpenStack Neutron de pont de couche 2** : le pont de couche 2 configuré à partir d'OpenStack est désormais configuré sur le cluster Edge et non sur le cluster ESXi.
- **Prise en charge d'OpenStack Octavia** : en plus de LBaaSv2, le plug-in OpenStack Neutron prend en charge Octavia comme mode de prise en charge de l'équilibrage de charge. Pour plus d'informations, consultez les notes de mise à jour du plug-in VMware NSX-T Data Center 2.5 pour OpenStack Neutron.

NSX Cloud

- **Ajout d'un nouveau mode de fonctionnement** : NSX Cloud possède désormais deux modes de fonctionnement, ce qui fait officiellement de NSX Cloud la seule solution de cloud hybride sur le marché à prendre en charge les modes de fonctionnement avec agent et sans agent.
 - **Mode NSX appliqué (avec agent)** : fournit une structure de stratégie « cohérente » entre les sites locaux et tout cloud public. L'application de la stratégie NSX est effectuée avec des outils NSX qui sont installés dans chaque charge de travail. Cela fournit une granularité au niveau de

la VM et toutes les VM balisées seront gérées par NSX. Ce mode surmontera les différences/limitations des fournisseurs de cloud public individuels et fournira une structure de stratégie cohérente entre la charge de travail sur site et de cloud public.

- **Mode Cloud natif appliqué (sans agent)** : fournit une structure de stratégie « commune » entre les sites et n'importe quel cloud public. Ce mode ne nécessite pas l'installation de NSX Tools dans les charges de travail. Les stratégies de sécurité NSX sont converties en concepts de sécurité de fournisseurs de cloud natif. Par conséquent, toutes les limitations en matière d'échelle et de fonctionnalités du cloud public choisi sont applicables. La granularité du contrôle se situe au niveau du VPC/VPNET et chaque charge de travail à l'intérieur d'un VPC ou d'un réseau virtuel géré sera gérée par NSX, sauf si elle figure sur une liste blanche. Les deux modes garantiront l'appartenance au groupe dynamique et un ensemble complet d'abstractions pour les critères d'appartenance au groupe NSX.
- **Prise en charge de la visibilité et de la sécurité des services natifs de cloud public depuis NSX Cloud** : à partir de cette version, il sera possible de programmer les groupes de sécurité de services SaaS natifs dans Azure et AWS auxquels un point de terminaison VPC/VNET local et un groupe de sécurité sont associés. L'idée principale est de découvrir et de sécuriser les points de terminaison de service natifs de cloud avec des règles définies par l'utilisateur sur la stratégie NSX. Les services suivants seront pris en charge dans AWS (ELB, RDS et DynamoDB) et Azure (Azure Storage, Azure LB, Azure SQL Server et CosmosDB) dans cette version. Les futures versions de NSX-T incluront un support plus étendu qui s'appliquera à davantage de services.
- **Prise en charge de nouveaux systèmes d'exploitation** :
 - Prise en charge de Windows Server 2019
 - Windows 10 v1809
 - Prise en charge d'Ubuntu 18.04.
- **Amélioration de la stratégie de mise en quarantaine et mise en liste blanche de VM** : à partir de NSX 2.5, NSX Cloud permet aux utilisateurs de mettre en liste blanche des VM à partir de l'interface CSM. Une fois que les groupes de sécurité de ces VM ne sont pas gérés par NSX, les utilisateurs peuvent placer les machines virtuelles dans les groupes de sécurité de cloud souhaités.
- **Amélioration des rapports d'erreur sur l'interface CSM** : permet un dépannage plus rapide.

Opérations

- **Prise en charge de vSphere HA pour NSX Manager** : le cluster de gestion NSX peut désormais être protégé par vSphere HA. Cela permet de récupérer un nœud du cluster de gestion NSX en cas de défaillance de l'hôte en cours d'exécution. Cela permet également de récupérer l'intégralité du cluster de gestion NSX sur un site secondaire en cas de défaillance au niveau du site. Pour plus d'informations sur les scénarios pris en charge, consultez le Guide d'installation de NSX-T.
- **Améliorations du tableau de bord de capacité** : des mesures nouvelles et améliorées apportées au tableau de bord de capacité indiquent le nombre d'objets que le client a configurés par rapport au nombre maximal pris en charge dans le produit. Pour obtenir la liste complète des configurations maximales pour NSX-T Data Center, reportez-vous à l'outil Configurations maximales de VMware.
- **Prise en charge du mode de verrouillage vSphere** : activez des options de déploiement supplémentaires pour les clients en offrant la possibilité d'installer, de mettre à niveau et d'utiliser NSX-T dans un environnement en mode verrouillage vSphere.
- **Amélioration de la journalisation** : réduisez l'impact sur le service lors des opérations de dépannage en activant la modification dynamique des niveaux de journalisation via l'interface de ligne de commande NSX pour les agents d'espace utilisateur NSX.
- **Prise en charge de SNMPv3** : amélioration de la conformité de sécurité en ajoutant la prise en charge de la configuration de SNMPv3 pour le dispositif NSX Edge et Manager.
- **Nouvelle capacité Traceflow pour le dépannage des problèmes liés à la résolution d'adresses de VM** : renforcement de la prise en charge de l'injection de paquets ARP/NDP via Traceflow pour détecter des problèmes de connectivité lors de la résolution d'adresses pour une destination IP.
- **Modification de l'ordre de mise à niveau** : lors de la mise à niveau vers NSX-T 2.5, le nouvel ordre de mise à niveau est une mise à niveau du composant Edge avant la mise à niveau du composant hôte. Cette amélioration offre des avantages importants lors de la mise à niveau de l'infrastructure du cloud en permettant aux optimisations de réduire la fenêtre de maintenance globale.
- **Amélioration du pack de contenu Log Insight** : ajout de la prise en charge des alertes de

journalisation prédéfinies avec le nouveau pack de contenu NSX-T compatible avec NSX-T 2.5.

Sécurité de la plate-forme

- **FIPS** : les utilisateurs peuvent désormais générer des rapports de conformité FIPS, et notamment configurer et gérer leurs déploiements NSX en mode compatible FIPS. Les modules cryptographiques sont validés conformément aux normes FIPS, offrant ainsi une garantie de sécurité aux clients qui souhaitent garantir le respect des réglementations fédérales ou utiliser NSX d'une manière sécurisée et conforme aux normes FIPS prescrites. Avec quelques exceptions, tous les modules cryptographiques de NSX-T 2.5 sont certifiés FIPS. Pour consulter les certifications accordées pour les modules validés par FIPS, rendez-vous sur <https://www.vmware.com/security/certifications/fips.html>.
- **Améliorations de la gestion des mots de passe** : les utilisateurs peuvent désormais étendre la durée d'expiration des mots de passe (nombre de jours) depuis la dernière modification du mot de passe, même après la mise à niveau. Des avertissements d'expiration dans un délai de 30 jours et des notifications d'expiration du mot de passe s'affichent désormais dans l'interface, la CLI et les journaux système (syslogs).

Prise en charge de la conception de cluster unique

Prise en charge de conceptions de cluster uniques avec les machines virtuelles Edge + Management + Calcul entièrement réduites, gérées par un seul N-VDS, dans un cluster comportant au moins quatre hôtes. Les modèles de référence types pour VxRail et autres solutions d'hôte de fournisseur de cloud prescrivent les PNIC 4x10G avec deux commutateurs hôtes. Un commutateur est dédié à Edge + Management (VDS), tandis que l'autre est dédié aux machines virtuelles de calcul (N-VDS). Deux commutateurs hôtes séparent efficacement le trafic de gestion du trafic de calcul. Cependant, face à la tendance de l'économie de 10 et 25G, de nombreux clients de petits centres de données et de fournisseurs de cloud choisissent de définir un hôte à deux pNIC comme norme. Avec ce format, les petits centres de données et les clients de fournisseurs de cloud peuvent créer une solution NSX-T avec un seul N-VDS, optimisant ainsi tous les composants avec deux pNIC.

Migration de NSX Data Center for vSphere vers NSX-T Data Center

- **Améliorations du coordinateur de migration** : le coordinateur de migration introduit plusieurs améliorations de la convivialité pour l'optimisation du workflow du processus nécessaire à la migration de NSX Data Center for vSphere vers NSX-T Data Center, notamment des améliorations pour fournir à l'utilisateur des commentaires pendant la migration.

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](#).

Changements généraux du comportement

Modifications du port de communication du système NSX-T Data Center

À partir de NSX-T Data Center 2.5, le port TCP du canal de messagerie NSX de tous les nœuds transport et Edge vers les instances de NSX Manager a été remplacé par le port TCP 1234 à partir du port 5671. Avec cette modification, assurez-vous que tous les nœuds de transport NSX-T et Edge peuvent communiquer sur les ports TCP 1234 avec les instances de NSX Manager et sur le port TCP 1235 avec les instances de NSX Controller avant de procéder à la mise à niveau vers NSX-T Data Center 2.5. Assurez-vous également que le port 5671 reste ouvert pendant le processus de mise à niveau.

Mise en réseau L2

En raison des améliorations apportées aux ponts de couche 2, le pont ESXi est obsolète. NSX-T a été introduit initialement avec la capacité de dédier un hôte ESXi en tant que pont pour étendre un segment de superposition à un VLAN. Ce modèle est obsolète à partir de cette version, car le nouveau pont Edge le remplace en termes de fonctionnalités, ne nécessite pas d'hôte ESXi dédié et bénéficie du chemin de données optimisé du nœud Edge. Pour plus d'informations, reportez-vous à la section « Nouveautés ».

Obsolescences de l'API et changements de comportement

Les API de modèle de nœud de transport sont obsolètes dans cette version. Il est recommandé d'utiliser plutôt des API de profils de nœud de transport. Pour obtenir une liste des types et méthodes obsolètes, consultez le [Guide de l'API](#).

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**.

Langues disponibles

NSX-T Data Center a été localisé dans plusieurs langues : anglais, allemand, français, japonais, chinois simplifié, coréen, chinois traditionnel et espagnol. Étant donné que la localisation de NSX-T Data Center utilise les paramètres de langue du navigateur, assurez-vous que vos paramètres correspondent à la langue souhaitée.

Historique de révision du document

19 septembre 2019. Première édition.

23 septembre 2019. Ajout des problèmes connus 2424818 et 2419246. Ajout des problèmes résolus 2364756, 2406018 et 2383328.

24 septembre 2019. Mise à jour de la section Nouveautés.

3 octobre 2019. Ajout du problème résolu 2313673.

12 novembre 2019. Ajout des problèmes connus 2362688 et 2436302. Correction du problème 2282798 en le déplaçant vers Résolu.

17 décembre 2019. Ajout du problème connu 2444170.

14 janvier 2020. Ajout du problème résolu 2399994.

18 février 2020. Mise à jour du problème connu 2436302 avec lien vers l'article de la base de connaissances.

14 mai 2020. Ajout du problème connu 2467479.

25 septembre 2020. Ajout du problème connu 2586606.

15 mars 2021. Ajout du problème connu 2730634.

Problèmes résolus

- **Problème 2288774 résolu** : 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.

- **Problème 2334442 résolu** : 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.
- **Problème 2256709 résolu** : 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.
- **Problème 2261431 résolu** : 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.
- **Problème 2274988 résolu** : 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.
- **Problème 2277742 résolu** : l'appel de PUT `https://<nsx-manager>/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://<nsx-manager>/api/v1/configs/management` ne peut pas être appelé si un nom de domaine complet est configuré.
- **Problème 2279249 résolu** : 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.
- **Problème 2292116 résolu** : 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.
- **Problème 2268406 résolu** : 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.
- **Problème 2282798 résolu** : 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.
- **Problème 2383867 résolu** : la collecte de bundles de journaux échoue pour l'un des nœuds du plan de gestion.
Le processus de collecte de journaux subit une défaillance lors de la copie du bundle de support sur le serveur distant.

- **Problème 2332397 résolu :** 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`.
- **Problème 2410818 résolu :** après la mise à niveau vers la version 2.4.2, les serveurs virtuels créés dans NSX-T 2.3.x peuvent cesser de fonctionner après la création d'un nombre supplémentaire de serveurs virtuels.
Dans certains déploiements, les serveurs virtuels créés dans la version 2.3.x cessent de fonctionner après la mise à niveau vers la version 2.4.2 et la création d'un nombre supplémentaire de serveurs virtuels.
- **Problème 2310650 résolu :** 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. »
- **Problème 2314537 corrige :** 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 2316943 résolu :** charge de travail non protégée brièvement pendant son déplacement avec 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.
- **Problème 2318525 résolu :** les itinéraires IPv6 de tronçon suivant (comme l'adresse IP de l'homologue eBGP) sont modifiés 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.
- **Problème 2320147 résolu :** 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.
- **Problème 2320855 résolu :** 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.
- **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 2295819 résolu :** le pont L2 est bloqué à 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.

- **Problème 2243415 résolu : 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. »
- **Problème résolu 2364756 : échec de la réalisation du profil en raison d'une priorité en double.**
Lors de la configuration de l'échelle, lorsque l'utilisateur a associé vRNI au profil NSX IPFIX, celui-ci ne se réalise pas sur le plan de gestion et renvoie des erreurs de réalisation.
- **Problème 2392093 résolu : le trafic diminue en raison de la vérification RPF.**
La vérification RPF peut entraîner le rejet du trafic si ce dernier est épinglé par une liaison descendante TO et que des routeurs de niveau 0 et de niveau 1 se trouvent sur le même nœud Edge.
- **Problème 2307551 résolu : l'hôte NSX-T peut perdre la connectivité au réseau de gestion lors de la migration de tous les PNIC vers N-VDS.**
Le problème se produit lors de la nouvelle tentative de migration de l'hôte en supprimant tous les PNIC dans le N-VDS sur lequel vmk0 est configuré. La première migration d'hôte a migré tous les PNIC et vmk0 dans le N-VDS mais a échoué par la suite. Lorsque vous relancez la migration, tous les PNIC sont supprimés du N-VDS. Par conséquent, les utilisateurs ne peuvent pas accéder à l'hôte via le réseau ; toutes les machines virtuelles de l'hôte perdent également la connectivité réseau, rendant ainsi leurs services inaccessibles.
- **Problème résolu 2369792 : le processus CBM se bloque à plusieurs reprises en raison de l'augmentation de la mémoire du processus CBM.**
Les processus CSM et CBM sur le dispositif Cloud Service Manager échouent au compactage de la base de données. Par conséquent, l'augmentation de la mémoire du processus CBM entraîne un blocage répété du processus CBM.
- **Problème résolu 2361892 : le dispositif NSX Edge subit une fuite de mémoire, ce qui entraîne le blocage/redémarrage du processus.**
Pendant une période prolongée, le dispositif NSX Edge peut subir une fuite de mémoire en raison d'une recherche répétée de règles, provoquant ainsi le blocage/redémarrage du processus. Une fuite de mémoire a été détectée à chaque recherche de règles. Lorsque le cache de flux est effacé, l'interface VIF n'est pas supprimée, ce qui entraîne une accumulation dans la mémoire.
- **Problème résolu 2364529 : fuite de mémoire de l'équilibreur de charge après la reconfiguration.**
L'équilibreur de charge NSX peut perdre de la mémoire suite à des événements de configuration consécutifs/répétitifs, ce qui entraîne un vidage de mémoire du processus nginx.
- **Problème 2378876 résolu : le PSOD sur les hôtes ESXi présente des erreurs : « Usage error in dlmalloc » et « PF Exception 14 in world 3916803:VSIP PF Purg IP ».**
ESXi s'est bloqué (PSOD) après l'exécution du trafic pendant quelques jours. Aucun autre symptôme n'a été observé avant le blocage. Le problème a été identifié en dernier lieu dans le trafic ALG (FTP, Sunrpc, Oracle, Dcerpc, TFTP) où le compteur d'incrément non atomisée a entraîné des conditions de concurrence, ce qui endommage la structure de l'arborescence ALG.
- **Problème 2384922 résolu : BGPD utilise 100 % du CPU sur le nœud Edge.**
Le processus BGPD sur NSX-T Edge peut consommer 100 % de CPU lorsqu'il a plusieurs sessions ouvertes avec VTYSH.
- **Problème résolu 2386738 : règles NAT ignorées sur le trafic sur le port lié.**

Les services NAT ne sont pas activés sur le type de port de routeur lié qui connecte les routeurs logiques de niveau 0 et de niveau 1.

- **Problème résolu 2363618** : les utilisateurs de VMware Identity Manager ne parviennent pas à accéder aux pages de stratégie dans le tableau de bord NSX Manager.
Les utilisateurs disposant de rôles attribués à des autorisations de groupe dans VMware Identity Manager ne parviennent pas à accéder aux pages de stratégie dans le tableau de bord NSX Manager. Les autorisations de l'attribution de groupe sont ignorées.
- **Problème 2298274 résolu** : le groupe de stratégies peut être créé/mis à jour avec un nom de domaine non valide ou partiel via REST API.
L'interface permettait la création de groupes avec des expressions d'identité contenant un groupe Active Directory ou des membres de groupes individuels non valides pour un contenu valide unique. Cependant, chaque membre est valide uniquement s'il dispose exactement d'un groupe LDAP associé au nom de domaine. Par conséquent, ces groupes créés dans une version antérieure de NSX-T ne seront pas marqués dans le processus de mise à niveau, ce qui permet aux groupes non valides de subsister dans les versions suivantes. Problème résolu dans la version 2.5.
- **Problème 2317147 résolu** : les utilisateurs ne peuvent pas afficher les machines virtuelles effectives d'un groupe dont l'appartenance est basée sur des adresses IP ou MAC.
Si un utilisateur crée un groupe avec uniquement des adresses IP ou MAC dans le groupe, aucune VM n'est répertoriée lorsque l'appartenance effective de ce groupe est appelée à partir de l'API. Ce problème n'a aucune répercussion fonctionnelle. La stratégie crée correctement un NSGroup sur le plan de gestion, et la liste des adresses IP et MAC est directement envoyée au plan de contrôle central.
- **Problème 2327201 résolu** : les mises à jour des machines virtuelles sur les hyperviseurs KVM ne sont pas immédiatement synchronisées.
Les mises à jour de VM sur les hyperviseurs KVM peuvent prendre quelques heures pour se synchroniser sur NSX-T. Par conséquent, les nouvelles machines virtuelles créées sur des hyperviseurs KVM ne peuvent pas être ajoutées aux NSGroups. Aucune règle de pare-feu ne peut être appliquée sur ces machines virtuelles et la mise à niveau de l'hyperviseur KVM est impossible, car l'état d'alimentation de la VM n'est pas mis à jour.
- **Problème 2329443 résolu** : le cluster de contrôle n'est pas initialisé en raison d'un dépassement du délai d'expiration de forcesync.
Le cluster de contrôle n'est pas initialisé en raison d'un délai d'expiration de forcesync lorsque la plage IPV4 dans IPSET démarre à 0.0.0.0, par exemple 0.0.0.0-1.1.1.20. Cela est dû à un problème dans IPSetFullSyncMessageProvider qui est bloqué dans une boucle infinie. Étant donné que le plan de contrôle central n'est pas initialisé, les utilisateurs ne peuvent pas déployer de nouvelles charges de travail.
- **Problème 2337839 résolu** : les widgets de sauvegarde NSX-T affichent des noms de champs incorrects.
En particulier, les widgets de sauvegarde de NSX-T n'affichent pas le nombre correct d'erreurs de sauvegarde. Par conséquent, le client doit examiner l'onglet de sauvegarde de NSX Manager pour afficher le nombre exact d'erreurs de sauvegarde.
- **Problème 2341552 résolu** : le dispositif Edge ne parvient pas à démarrer si le système comprend un trop grand nombre de cartes réseau prises en charge.
Aucun service ni aucune connectivité au chemin d'accès aux données n'est visible, le service de chemin d'accès aux données est inactif et le nœud Edge est dans un état dégradé. Cela provoque une perte de connectivité partielle ou totale si le dispositif Edge est requis.
- **Problème 2390374 résolu** : NSX Manager devient très lent ou ne répond plus, et les journaux affichent de nombreuses exceptions corfu.
Il se peut également que NSX ne parvienne pas à démarrer. Les exceptions corfu indiquent que l'échelle des membres Active Directory est trop importante et au-delà des limites testées.

- **Problème 2371150 résolu** : impossible de configurer les règles de pare-feu de couche 7 sur les nœuds Edge Bare Metal.

Les règles de pare-feu de couche 7 sur les nœuds Edge Bare Metal ne sont pas prises en charge dans NSX-T 2.5. Une commande interne active cette prise en charge, mais n'est disponible que pour les validations de concept.

- **Problème 2361238 résolu** : le routeur de liaison descendante ne se couple pas au routeur de services.

Les règles NAT ne prennent pas effet sur le routeur de liaison descendante après la suppression d'un routeur de services couplé à un routeur de liaison descendante recréé.

- **Problème 2363248 résolu** : l'état de santé de l'instance de service sur l'interface semble être inactif, bien que l'appel d'API indique être connecté.

Ce rapport incohérent peut provoquer une fausse alarme.

Ce problème et cette solution sont décrits plus en détail dans l'[article 67165 de la base de connaissances : l'état de l'instance de service s'affiche comme étant « inactif » lorsqu'il n'y a aucune VM à protéger dans NSX-T](#).

- **Problème 2359936 résolu** : roulement fréquent de journaux cfgAgent sur l'hôte ESX.

L'actualisation fréquente du journal cfgAgent.log peut entraîner une perte d'informations utiles au débogage et au dépannage de l'hôte.

- **Problème 2332938 résolu** : lorsque le cache SYN est activé dans le profil de sécurité de la protection de saturation, la limite réelle de connexion semi-ouverte TCP peut être supérieure à celle configurée sur NSX Manager.

NSX-T calcule automatiquement une limite de connexion semi-ouverte TCP optimale, en fonction de la limite configurée. Cette limite calculée peut être supérieure à la limite configurée et repose sur la limite de formule $= (\text{PwrOf2} * \text{Profondeur})$, où PwrOf2 est une puissance de 2 non inférieure à 64 et Profondeur est un entier ≤ 32 .

- **Problème 2376336 résolu** : la famille d'adresses dans la redistribution des itinéraires n'est pas prise en charge par la stratégie et le dispositif Edge.

La famille d'adresses dans la redistribution ne fonctionne pas ou n'est pas utilisée dans l'application.

- **Problème 2412842 résolu** : limitez les journaux de mesures à 40 Mo sur ESX pour prendre en charge les hôtes avec RAMDisk.

Ce problème est résolu en détail dans l'[article 74574 de la base de connaissances](#).

- **Problème 2385070 résolu** : la détection d'adresses IP et DFW affichent des comportements opposés concernant le sous-réseau IPv6.

La détection d'adresses IP considère 2001::1/64 comme une adresse IP hôte, alors que DFW la considère comme un sous-réseau IPv6.

- **Problème 2394896 résolu** : l'hôte ne parvient pas à effectuer la mise à niveau de NSX-T Data Center 2.4.x vers 2.5.

L'hôte ne parvient pas à effectuer la mise à niveau de NSX-T Data Center 2.4.0, 2.4.1 et 2.4.2 vers 2.5. Ce problème peut être dû à un échec de déchargement du module KCP.

Ce problème est abordé plus en détail dans l'[article 74674 de la base de connaissances](#).

- **Problème résolu 2406018** : un événement/une alarme se déclenche si l'expiration du mot de passe est dans les 30 prochains jours.

Un événement/une alarme se déclenche pour l'expiration du mot de passe si celui-ci expire dans les 30 jours, même si l'expiration du mot de passe est désactivée.

- **Problème résolu 2383328** : demande de fonctionnalité pour fournir un utilitaire qui restitue les données de mesures dans un format lisible.

NSX-T Data Center collecte et enregistre les données de mesures dans un format binaire. Les utilisateurs ont demandé à pouvoir afficher ces données dans un format lisible. Ce problème fait suite à cette demande.

- **Problème résolu 2248345** : après l'installation du dispositif Edge NSX-T, la machine démarre avec un écran noir vide
Impossible d'installer le dispositif Edge NSX-T sur le serveur HPE ProLiant DL380 Gen9.
- **Problème résolu 2313673** : les utilisateurs ne peuvent pas connecter les liaisons montantes aux commutateurs/segments logiques NSX-T pour les nœuds de transport Edge basés sur une machine virtuelle.
Pour les nœuds de transport Edge basés sur une machine virtuelle, les utilisateurs ne peuvent pas connecter les liaisons montantes de ces nœuds aux commutateurs/segments logiques de NSX-T. Ils peuvent uniquement les connecter aux DVPG de l'instance de vCenter. Sur l'écran Configurer NSX pour les flux d'ajout/de modification d'un nœud de transport Edge basé sur une machine virtuelle, les utilisateurs sont invités à mapper les liaisons montantes uniquement aux DVPG de l'instance de vCenter. L'option permettant de mapper les liaisons montantes aux commutateurs/segments logiques NSX-T est manquante.
- **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 2399994 résolu** : routes redistribuées manquantes par intermittence.
Le trafic réseau peut être affecté, car l'itinéraire vers T1 n'est pas disponible pendant un certain temps.

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 de NSX Intelligence](#)
- [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 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.

- **Problème 2329273 :** aucune connectivité entre les VLAN reliés au même segment par le même nœud Edge.

Le pontage d'un segment à deux reprises sur le même nœud Edge n'est pas pris en charge.

Cependant, il est possible de relier deux VLAN au même segment sur deux nœuds Edge différents.

Solution : aucune

- **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 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 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 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://<nsx-manager>/api/v1/fabric/compute-collections/<CC Ext ID>/storage-resources?uniform_cluster_access=true&source=realtime`

où <nsx-manager> correspond à l'adresse IP de l'instance de NSX Manager dans laquelle l'API de déploiement de service a échoué, et CC Ext ID à l'identifiant dans NSX du cluster dans lequel le déploiement est tenté.

- **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 2370555 : l'utilisateur peut supprimer certains objets de l'interface avancée, mais les suppressions ne sont pas répercutées dans l'interface simplifiée.**
En particulier, les groupes ajoutés dans le cadre d'une liste d'exclusion de pare-feu distribué peuvent être supprimés dans les paramètres de la liste d'exclusion du pare-feu distribué de l'interface avancée. Cela provoque un comportement incohérent dans l'interface.

Solution : pour résoudre ce problème, procédez comme suit :

- Ajoutez un objet à une liste d'exclusion dans l'interface simplifiée.
- Vérifiez qu'il s'affiche dans la liste d'exclusion du pare-feu distribué dans l'interface avancée.
- Supprimez l'objet de la liste d'exclusion du pare-feu distribué dans l'interface avancée.
- Retournez à l'interface simplifiée et renvoyez un deuxième objet à la liste d'exclusion puis appliquez-le.
- Vérifiez que le nouvel objet apparaît dans l'interface avancée.

- **Problème 2377217** : après le redémarrage de l'hôte KVM, les flux de trafic entre les machines virtuelles peuvent ne pas fonctionner comme prévu.

Le redémarrage de l'hôte KVM peut entraîner des problèmes d'accessibilité entre les machines virtuelles.

Solution : après le redémarrage de l'hôte, redémarrez le service NSX-Agent à l'aide de la commande suivante :

```
# systemctl restart nsx-agent.service
```

- **Problème 2371251** : l'interface du tableau de bord clignote lors de la navigation vers la page Sauvegarde et restauration.

Ce problème n'a été observé que dans le navigateur Firefox et dans certains déploiements.

Solution : actualisez manuellement la page ou utilisez un autre navigateur pris en charge.

- **Problème 2408453** : VMware Tools 10.3.5 se bloque lorsque le pilote NSX Guest Introspection est installé.

VMware Tools 10.3.5 se bloque de façon irrégulière sur la VM Windows, notamment lorsque la session distante est déconnectée ou lorsque la VM invitée est en cours d'arrêt.

Solution : pour plus de détails, reportez-vous à l'[article 70543 de la base de connaissances](#).

- **Problème 2267964** : si vCenter est supprimé, l'utilisateur n'est pas averti de la perte des services s'exécutant sur vCenter.

Si un utilisateur supprime le gestionnaire d'ordinateur (vCenter) sur lequel des services comme Guest Introspection sont déployés, l'utilisateur n'est pas informé de la perte potentielle de ces services.

Solution : ce problème peut être évité si l'utilisateur suit la procédure correcte pour ajouter un nouveau vCenter en tant que gestionnaire d'ordinateur.

- **Problème 2444170** : Les commandes de l'interface CLI de NSX ne parviennent pas à désinstaller le chemin de données

La commande *del nsx* ne désinstalle pas la configuration de NSX-T et les modules de l'hôte. L'installation ou la mise à niveau de NSX-T échoue alors.

Solution : aucune.

- **Problème 2467479** : une fois le pare-feu défini sur Contournement pour une règle SNAT, il ne peut pas être bloqué après la modification de Contournement vers Aucun.

Une fois le pare-feu défini sur Contournement pour une règle SNAT, il ne peut pas être bloqué après la modification de Contournement vers Aucun.

Solution : supprimez puis recréez la règle SNAT.

- **Problème 2586606** : l'équilibreur de charge ne fonctionne pas lorsque la persistance IP source est configurée sur un grand nombre de serveurs virtuels.

Lorsque la persistance IP source est configurée sur un grand nombre de serveurs virtuels sur un équilibreur de charge, elle consomme beaucoup de mémoire et peut entraîner l'épuisement de la mémoire NSX Edge. Toutefois, le problème peut se produire à nouveau avec un plus grand nombre de serveurs virtuels.

Solution : désactivez la persistance de l'adresse IP source ou transférez les adresses IP virtuelles avec la persistance de l'adresse IP source à différents services d'équilibrage de charge.

- **Problème 2730634** : la page des composants de mise en réseau post-mise à niveau à échelle unique affiche une erreur « Index non synchronisé ».
La page des composants de mise en réseau post-mise à niveau à échelle unique affiche une erreur « Index non synchronisé ».

Solution : connectez-vous à NSX Manager avec les informations d'identification de l'admin et exécutez la commande « start search resync policy ». Le chargement des composants de mise en réseau prendra quelques minutes.

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 2378970** : paramètre Activer/Désactiver au niveau du cluster pour le pare-feu distribué affiché incorrectement comme étant désactivé.
Le paramètre Activer/Désactiver au niveau du cluster pour IDFW sur une interface utilisateur simplifiée peut s'afficher comme étant désactivé, même s'il est activé sur le plan de gestion. Après la mise à niveau de 2.4.x vers 2.5, cette inexactitude sera conservée jusqu'à ce qu'elle soit explicitement modifiée.

Solution : modifiez manuellement le paramètre Activer/Désactiver pour IDFW sur l'interface utilisateur simplifiée afin qu'il corresponde au même plan de gestion.

Problèmes connus de NSX Edge

- **Problème 2283559** : les API MP <https://<nsx-manager>/api/v1/routing-table> et <https://<nsx-manager>/api/v1/forwarding-table> renvoient une erreur si le dispositif Edge comprend plus de 65 000 itinéraires pour RIB et plus de 100 000 itinéraires 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.

- **Problème 2343954 :** l'interface de point de terminaison du pont de couche 2 Edge permet la configuration de plages de VLAN non prises en charge.

L'interface de configuration du point et du pont de couche 2 Edge vous permet de configurer la plage de VLAN et plusieurs plages de VLAN, même si elles ne sont pas prises en charge.

Solution : ne configurez pas ces plages de VLAN pour la configuration du pont et du point de couche 2 Edge.

Problèmes connus de mise en réseau logique

- **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.

- **Problème 2275412 :** la connexion de port ne fonctionne pas sur plusieurs zones de transport. La connexion de port ne peut être utilisée que sur une seule zone de transport.

Solution : aucune.

- **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 2304571 :** une erreur critique (PSOD) peut se produire lors de l'exécution du trafic L3 à l'aide de VDR.

L'entrée arp(ND) en attente n'est pas correctement protégée dans certains cas, ce qui peut entraîner une erreur critique (PSOD).

Solution : aucune.

- **Problème 2388158 :** l'utilisateur ne peut pas modifier les paramètres de sous-réseau de transit dans la configuration du routeur logique de niveau 0.

Après la création du routeur logique de niveau 0, la configuration du sous-réseau de transit ne peut pas être modifiée dans l'interface NSX Manager.

Solution : aucune. La meilleure option consiste à supprimer le routeur logique et à le recréer avec la configuration de sous-réseau de transit souhaitée.

Problèmes connus des services de sécurité

- **Problème 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.

Solution : aucune. Ce problème n'a aucune répercussion pour le client.

- **Problème 2395334** : paquets (Windows) abandonnés de manière incorrecte en raison de l'entrée contrtrack 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.

- **Problème 2366599** : règles relatives aux machines virtuelles avec des adresses IPv6 non appliquées.

Si une VM utilise une adresse IPv6, mais que l'écoute IPv6 n'est pas activée pour ce VIF via le profil de détection d'adresses IP, l'adresse IPv6 n'est pas renseignée dans la règle pour cette VM dans le chemin d'accès aux données. Par conséquent, cette règle n'est jamais appliquée.

Solution : vérifiez que l'option IPv6 dans le profil IPDiscovery est activée au niveau du VIF ou du commutateur logique lorsque des adresses IPv6 sont utilisées.

- **Problème 2296430** : l'API NSX-T Manager ne fournit pas de noms alternatifs de sujet lors de la génération de certificats.

L'API NSX-T Manager ne fournit pas de noms alternatifs de sujet pour émettre des certificats, en particulier lors de la génération de la CSR.

Solution : créez la CSR à l'aide d'un outil externe qui prend en charge les extensions. Une fois que le certificat signé est reçu de la part de l'autorité de certification, importez-le dans NSX-T Manager avec la clé de la CSR.

- **Problème 2379632** : plusieurs paquets sont journalisés lorsque vous atteignez la règle de couche 7 à l'étape classée.

Plusieurs paquets (2-3) sont journalisés (dfwpktlogs) lorsque vous atteignez la règle de couche 7 à l'étape classée.

Solution : aucune.

- **Problème 2368948** : règles de pare-feu distribué : l'état réalisé des sections individuelles peut ne pas être à jour.

L'actualisation de la vue de règle DFW ne met pas à jour l'état réalisé des sections individuelles dans cette vue. Par conséquent, les informations peuvent ne pas être à jour.

Solution : ce problème ne concerne que l'actualisation manuelle. L'interrogation de l'état réalisé est périodique et fournira des mises à jour précises. Les utilisateurs peuvent également actualiser des sections individuelles pour un état précis.

- **Problème 2380833** : la publication du brouillon de stratégie avec au moins 8 000 règles nécessite beaucoup de temps.

Un brouillon de stratégie contenant au moins 8 000 règles peut prendre beaucoup de temps à publier. Par exemple, un brouillon de stratégie contenant 8 000 règles peut prendre 25 minutes à publier.

Solution : aucune.

- **Problème 2424818** : les états de la couche 2 et du pare-feu distribué ne sont pas mis à jour sur l'interface de NSX Manager.

Les informations d'état produites par l'exportateur logique sur les machines virtuelles de charge de travail ne peuvent pas être transférées au plan de gestion. Par conséquent, les états affichés pour ces composants ne sont pas correctement mis à jour.

Solution : aucune. Vous pouvez accéder aux informations d'état correctes via la CLI sur les machines virtuelles correspondantes.

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 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 : 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.

- **Problème 2401715** : erreur lors de la mise à jour du gestionnaire de calcul indiquant que l'empreinte n'est pas valide, même si l'empreinte correcte est fournie.

Observé lorsqu'un vCenter v6.7U3 est ajouté en tant que gestionnaire de calcul dans NSX-T Manager. vSphere 6.7 prend en charge la modification du PNID où le nom de domaine complet ou l'adresse IP peuvent être modifiés. NSX-T 2.5 ne prend pas en charge cette fonctionnalité, d'où le problème d'empreinte.

Solution : supprimez le vCenter précédemment ajouté et ajoutez le VC avec un nom de domaine complet récemment modifié. L'ajout de l'enregistrement peut échouer, car l'extension précédente existe déjà sur vCenter. Corrigez les erreurs d'enregistrement afin qu'elles soient correctement enregistrées.

Problèmes connus de NSX Intelligence

- **Problème 2410806** : la publication de la recommandation générée échoue avec l'exception citant une limite totale de 500.

Si le nombre total de membres (adresses IP ou machines virtuelles) dans un groupe recommandé dépasse 500, la publication de la recommandation générée dans une configuration de stratégie échoue avec un message d'exception tel que « Le nombre total d'IPAdressExpressions, de MACAddressExpressions, de chemins d'accès dans un PathExpression et d'ID externes dans ExternalIDExpression ne doivent pas dépasser 500. »

Solution : s'il existe des scénarios dans lesquels 500 clients et plus se connectent à la VM d'application ou à l'équilibreur de charge, vous pouvez créer une règle pour micro-segmenter l'accès à l'équilibreur de charge de l'application, puis sélectionner les machines virtuelles d'application pour lancer la détection des recommandations. Dans l'alternative, vous pouvez sous-diviser le groupe de membres 500-plus en plusieurs groupes de plus petite taille.

- **Problème 2362865 : filtre par nom de règle non disponible pour la règle par défaut.**
Observé dans la page Planifier et dépanner > Détecter et effectuer une action et affecte uniquement les règles créées par la stratégie de connectivité. Ce problème est dû à l'absence d'une stratégie par défaut basée sur la stratégie de connectivité spécifiée. Une règle par défaut peut être créée sur le plan de gestion, mais sans aucune stratégie par défaut correspondante, l'utilisateur ne peut pas filtrer en fonction de cette règle par défaut. (Le filtre pour la visualisation des flux utilise le nom de la règle pour filtrer en fonction des flux qui atteignent cette règle.)

Solution : n'appliquez pas de filtre de nom de règle. À la place, vérifiez l'indicateur non protégé. Cette configuration inclut les flux qui atteignent la règle par défaut ainsi que toute règle pour laquelle la source « any » et la destination « any » sont spécifiées.

- **Problème 2368926 : la tâche de recommandations échoue si l'utilisateur redémarre le dispositif alors que la tâche est en cours.**
Si l'utilisateur redémarre le dispositif NSX Intelligence lorsqu'une tâche de recommandations est en cours, la tâche passe à l'état d'échec. Un utilisateur peut lancer une tâche de recommandation pour un ensemble de machines virtuelles contextuelles. Le redémarrage supprime le contexte et la tâche échoue en conséquence.

Solution : après le redémarrage, répétez la tâche de recommandations pour le même ensemble de machines virtuelles.

- **Problème 2385599 : groupes d'adresses IP statiques non prises en charge dans les recommandations de NSX-T Intelligence.**
Les machines virtuelles et les charges de travail qui ne sont pas reconnues dans l'inventaire NSX-T, si elles disposent d'adresses IP Intranet, peuvent toujours être soumises à recommandation en tant que groupe d'adresses IP statiques, y compris les règles de définition contenant ces groupes. Toutefois, NSX Intelligence ne prend pas en charge ces groupes et, par conséquent, la visualisation indique le trafic qui leur est envoyé, tel qu'il est envoyé à « inconnu » au lieu du groupe recommandé.

Solution : aucune. Toutefois, la recommandation fonctionne correctement. Il s'agit d'un problème d'affichage.

- **Problème 2374231 : pour les flux de protocole SCTP, GRE et ESP, le service est indiqué comme étant INCONNU et le port en tant que 0.**
NSX Intelligence ne prend pas en charge l'analyse du port source ou de destination pour les flux de protocole GRE, ESP et SCTP. NSX Intelligence permet une analyse d'en-tête complète pour les flux TCP et UDP, ainsi que des statistiques liées au flux. Pour les autres protocoles pris en charge (tels que GRE, ESP et SCTP), NSX Intelligence peut uniquement fournir des informations IP sans ports source ou de destination spécifiques au protocole. Pour ces protocoles, le port source ou de destination sera zéro.

Solution : aucune.

- **Problème 2374229 : le dispositif NSX Intelligence manque d'espace disque.**
Le dispositif NSX Intelligence dispose d'une période de rétention des données par défaut de 30 jours. Si la quantité de données de flux est supérieure à la quantité prévue dans un délai de 30 jours, le dispositif peut manquer d'espace disque prématurément et devenir partiellement ou totalement inopérant.

Solution : ce problème peut être évité ou atténué en surveillant l'utilisation du disque par le dispositif NSX Intelligence. Si l'utilisation du disque est effectuée à un taux élevé qui indique que l'espace peut être insuffisant, vous pouvez modifier la période de rétention des données afin qu'elle soit inférieure au nombre de jours.

1. Utilisez SSH dans le dispositif NSX Intelligence et accédez au fichier `/opt/vmware/pace/druid-config/druid_data_retention.properties`.
 2. Localisez et modifiez le paramètre `correlated_flow` à une valeur inférieure à 30 jours. Par exemple : `correlated_flow=P14D`
 3. Enregistrez le fichier et appliquez les modifications en exécutant la commande suivante :
`/opt/vmware/pace/druid-config/druid-config-data-retention.sh`
- REMARQUE : la suppression physique des données peut nécessiter jusqu'à deux heures.

- **Problème 2389691 : le travail de recommandation de publication échoue avec l'erreur « la taille de la charge utile de la demande dépasse la limite autorisée, un nombre maximal de 2 000 objets est autorisé par demande. »**

Si vous essayez de publier une seule tâche de recommandation contenant plus de 2 000 objets, elle échouera avec l'erreur « la taille de la charge utile de la demande dépasse la limite autorisée, un nombre maximal de 2 000 objets est autorisé par demande. »

Solution : réduisez le nombre d'objets à moins de 2 000 dans le travail de recommandation et retentez la publication.

- **Problème 2376389 : les machines virtuelles sont incorrectement marquées comme supprimées dans la vue « 24 dernières heures » lors de la configuration de l'échelle intermédiaire.**
Après la déconnexion ou la suppression d'un nœud de transport du gestionnaire de calcul, NSX Intelligence indique que les machines virtuelles précédentes ont été supprimées et que les nouvelles machines virtuelles les ont remplacées. Ce problème provient des mises à jour de l'inventaire de suivi NSX Intelligence dans la base de données NSX, et ce comportement reflète la manière dont l'inventaire gère la déconnexion du nœud de transport du gestionnaire de calcul. Cela n'affecte pas le nombre total de machines virtuelles actives dans NSX Intelligence, même si vous pouvez voir des machines virtuelles en double dans NSX Intelligence.

Solution : aucune action n'est requise. Les machines virtuelles en double sont finalement supprimées de l'interface en fonction de l'intervalle de temps sélectionné.

- **Problème 2393240 : les flux supplémentaires sont observés de la machine virtuelle à l'adresse IP.**

Le client voit des flux supplémentaires de la VM à l'adresse IP-xxxx. Cela est dû au fait que les données de configuration (les groupes, les machines virtuelles et les services) de NSX Policy Manager atteignent le dispositif NSX Intelligence après la création du flux. Par conséquent, le flux (précédemment) ne peut pas être mis en corrélation avec la configuration, car il n'existe pas du point de vue du flux. Le flux ne pouvant pas être généralement corrélé, il est défini par défaut sur IP-xxxx pour sa VM lors de la recherche de flux. Une fois la configuration synchronisée, le flux de VM réel s'affiche.

Solution : modifiez la fenêtre de délai pour exclure le flux que vous voulez voir.

- **Problème 2370660 : NSX Intelligence affiche des données incohérentes pour des machines virtuelles spécifiques.**
Ce problème est probablement dû au fait que ces machines virtuelles possèdent la même adresse IP dans le centre de données. Cette fonction n'est pas prise en charge par NSX Intelligence dans NSX-T 2.5.

Solution : aucune. Évitez d'attribuer la même adresse IP à deux machines virtuelles dans le centre de données.

- **Problème 2372657 : la corrélation de la relation VM-GROUPE et du flux GROUPE-GROUPE s'affiche temporairement de manière incorrecte.**

La corrélation de la relation VM-GROUPE et du flux GROUPE-GROUPE s'affiche temporairement incorrectement si le dispositif NSX Intelligence est déployé alors que des flux sont en cours dans le centre de données. En particulier, les éléments suivants peuvent s'afficher de manière incorrecte pendant cette période temporaire :

- Les machines virtuelles appartiennent de façon erronée à un groupe non classé.
- Les machines virtuelles appartiennent de façon erronée à un groupe inconnu.
- Les flux corrélés entre deux groupes peuvent s'afficher de manière incorrecte.

Ces erreurs seront automatiquement corrigées une fois que le dispositif NSX Intelligence aura été déployé plus longtemps que la période de visualisation sélectionnée par l'utilisateur.

Solution : aucune. Si l'utilisateur sort de la période de visualisation pendant laquelle le dispositif NSX Intelligence est déployé, le problème n'apparaît pas.

- **Problème 2366630 : la suppression de l'opération de nœud de transport peut échouer lorsque le dispositif NSX Intelligence est déployé.**

Si un nœud de transport est supprimé alors que le dispositif NSX Intelligence est déployé, la suppression peut échouer, car le nœud de transport est référencé par NSX-INTELLIGENCE-GROUP NSGroup. Pour supprimer un nœud de transport, l'option permettant de forcer la suppression est requise lorsque le dispositif NSX Intelligence est déployé.

Solution : utilisez l'option Forcer pour supprimer le nœud de transport.

- **Problème 2357296 : les flux peuvent ne pas être signalés à NSX Intelligence par certains hôtes ESX dans certaines conditions d'échelle et de contrainte.**

L'interface de NSX Intelligence peut ne pas afficher les flux de certaines machines virtuelles sur certains hôtes et ne peut pas fournir de recommandations concernant les règles de pare-feu pour ces machines virtuelles. Par conséquent, la sécurité du pare-feu peut être compromise sur certains hôtes. Ce problème est observé dans les déploiements avec des versions de vSphere inférieures à 6.7U2 et 6.5U3. Le problème est identifié comme une erreur de création et de suppression du filtre VM de l'hyperviseur ESX principal.

Solution : mettez à niveau l'hôte vers la version vSphere 6.7U2 et versions ultérieures ou vSphere 6.5U3 et versions ultérieures.

- **Problème 2393142 : la connexion à NSX Manager avec les informations d'identification de vIDM peut renvoyer une erreur d'utilisateur non autorisé 403.**

Ce problème concerne uniquement les utilisateurs se connectant en tant qu'utilisateurs vIDM, par opposition à un utilisateur local, sur NSX Manager. La connexion et l'intégration de vIDM ne sont pas prises en charge dans NSX-T 2.5 lors de l'interaction avec le dispositif NSX Intelligence.

Solution : connectez-vous en tant qu'utilisateur local en ajoutant l'adresse IP/le nom de domaine complet de NSX Manager avec la chaîne « login.jsp?local=true ».

- **Problème 2369802 : la sauvegarde du dispositif NSX Intelligence exclut la sauvegarde de la banque de données des événements.**

Cette fonctionnalité n'est pas prise en charge dans NSX 2.5.

Solution : aucune.

- **Problème 2346545 : dispositif NSX Intelligence : le remplacement du certificat concerne les rapports d'information sur les nouveaux flux.**

Si l'utilisateur remplace le certificat d'identité principal du dispositif NSX Intelligence par un certificat auto-signé, le traitement de nouveaux flux est affecté et le dispositif n'affiche pas les informations mises à jour à partir de ce moment.

Solution : aucune.

- **Problème 2407198 : les machines virtuelles s'affichent de manière incorrecte dans le groupe de VM non classées dans le dispositif de sécurité de NSX Intelligence.**

Lorsque les hôtes ESXi sont déconnectés de vCenter, les machines virtuelles de ces hôtes peuvent être affichées dans le groupe « VM non classées », même si elles appartiennent à d'autres groupes. Lorsque les hôtes ESXi se reconnectent avec vCenter, les machines virtuelles s'affichent dans leurs groupes appropriés.

Solution : reconnectez les hôtes à vCenter.

- **Problème 2410224** : après la fin de l'enregistrement du dispositif NSX Intelligence, l'actualisation de la vue peut renvoyer l'erreur 403 Interdit.
Après avoir terminé l'enregistrement du dispositif NSX Intelligence, si vous cliquez sur Actualiser pour afficher, le système peut renvoyer l'erreur 403 Interdit. Il s'agit d'une condition temporaire causée par le temps nécessaire au dispositif NSX Intelligence pour accéder à l'interface.

Solution : si cette erreur s'affiche, patientez quelques instants puis réessayez.

- **Problème 2410096** : après le redémarrage du dispositif NSX Intelligence, les flux collectés au cours des 10 dernières minutes avant le redémarrage peuvent ne pas s'afficher.
Causé par un problème d'indexation.

Solution : aucune.

- **Problème 2436302** : après le remplacement du certificat de cluster NSX-T Unified Appliance, il n'est pas possible d'accéder à NSX intelligence via l'API ou l'interface de Manager.
Dans l'interface de NSX-T Manager, accédez à l'onglet Planifier et dépanner, puis cliquez sur Découvrir et effectuer une action ou sur Recommandations. L'interface ne se chargera pas et renverra finalement une erreur semblable à : Échec du chargement de l'application demandée. Si le problème persiste, réessayez ou contactez le support.

Solution : pour obtenir plus d'informations et la solution, reportez-vous à l'[article 76223 de la base de connaissances](#).

Problèmes connus des opérations et des services de surveillance

- **Problème 2401164** : les sauvegardes sont incorrectement signalées comme réussies malgré l'erreur de serveur SFTP.
Si le mot de passe expire pour le serveur SFTP utilisé pour les sauvegardes, NSX-T signale l'erreur générique « erreur inconnue de l'opération de sauvegarde ».

Solution : vérifiez que les informations d'identification pour accéder au serveur SFTP sont à jour.

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 contrôle 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.

- **Problème 2348994** : échec intermittent lors de la mise à niveau des VIB NSX sur le nœud de transport ESXi 6.5 p03.

Observé dans certaines mises à niveau de 2.4.x vers 2.5. Lorsque les VIB NSX sur un nœud de transport ESXi 6.5 p03 sont mis à niveau, l'opération de mise à niveau échoue parfois avec l'erreur suivante : « Exception d'appel du SDK VI : Aucune donnée obtenue à partir du processus : LANG=en_US.UTF-8 ».

Solution : effectuez une mise à niveau vers ESXi 5 p04. Vous pouvez également mettre l'hôte en mode de maintenance et le redémarrer. Réessayez la mise à niveau et quittez le mode de maintenance.

- **Problème 2372653** : après la mise à niveau vers la version 2.5, l'utilisateur ne parvient pas à localiser les groupes basés sur le port logique et LogicalSwitch dans les versions antérieures de NSX-T.

Après la mise à niveau vers la version 2.5, les groupes basés sur le port logique et LogicalSwitch créés à partir de la stratégie dans les versions précédentes de NSX-T ne se trouvent pas dans l'interface du tableau de bord. Cependant, ils peuvent toujours être situés dans l'API. Cela est dû à une modification de nom causée par le processus de mise à niveau. Dans la version 2.5, les groupes basés sur LogicalPort et LogicalSwitch apparaissent sous forme de groupes basés sur Segment et SegmentPort.

Solution : utilisez l'API uniquement pour accéder à ces groupes de stratégies après la mise à niveau.

- **Problème 2408972** : pendant la mise à niveau, vSphere Update Manager ne parvient pas à corriger le dernier hôte.

Lors de la mise à niveau, la correction de vSphere Update Manager échoue pour le dernier hôte dont les charges de travail reposent sur un commutateur logique NSX-T.

Solution : migrez manuellement toutes les machines virtuelles de charge de travail reposant sur NSX-T vers un hôte déjà mis à niveau, puis relancez la mise à niveau de l'hôte défaillant.

- **Problème 2400379 : la page Profil de contexte affiche un message d'erreur d'APP_ID non pris en charge.**

La page Profil de contexte affiche le message d'erreur suivant : « Ce profil de contexte utilise un APP_ID-[<APP_ID>] non pris en charge. Ce profil de contexte utilise un APP_ID non pris en charge. Supprimez ce profil de contexte manuellement après vous être assuré qu'il n'est utilisé dans aucune règle. » Ce problème est dû à la présence de six APP_IDs obsolètes (AD_BKUP, SKIP, AD_NSP, SAP, SUNRPC, SVN) qui ne fonctionnent plus sur le chemin d'accès aux données.

Solution : après avoir vérifié qu'ils ne sont plus utilisés, supprimez manuellement les six profils de contexte APP_ID.

- **Problème 2419246 : échec de la mise à niveau d'Ubuntu KVM.**

La mise à niveau des nœuds Ubuntu KVM peut échouer en raison de la non-exécution du service nsx-vmtoolsd. Cependant, le service nsx-vmtoolsd dépend de l'agent nsx-agent, mais à ce stade de la mise à niveau, celui-ci n'est pas encore configuré. L'agent nsx-agent échoue, car le composant vm-command-relay n'est pas correctement démarré.

Solution : configurez l'agent nsx-agent incomplet. La commande suivante reconfigure tous les modules décompressés ou partiellement configurés :

```
dpkg --configure -a
```

Vous pouvez utiliser les commandes ci-dessous pour reconfigurer uniquement nsx-agent et nsx-vmtoolsd :

```
dpkg --configure nsx-agent
```

```
dpkg --configure nsx-vmtoolsd
```

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 2200856 : le redémarrage du service gestionnaire-service-cloud échoue.**

Le redémarrage du service gestionnaire-service-cloud peut échouer si l'utilisateur le teste sans attendre que le service API ne s'affiche pour la première fois.

Solution : patientez quelques minutes, puis réessayez.

- **Problème 2378752 : l'API permet la création de plusieurs cartes de liaison sous des segments ou des ports.**

Observé uniquement sur l'API. Lorsqu'un utilisateur crée plusieurs mappages de liaison sous un segment ou un port, aucune erreur n'est signalée. Ce problème se produit lorsque l'utilisateur tente de lier simultanément plusieurs profils sur un segment ou un port.

Solution : utilisez plutôt l'interface NSX Manager pour effectuer cette opération.

Problèmes connus de NSX Cloud

- **Problème 2275232 : DHCP ne fonctionne pas pour les machines virtuelles du cloud si la stratégie de connectivité 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.

- **Problème 2277814** : la VM est déplacée vers vm-overlay-sg en cas de saisie d'une valeur non valide pour la balise nsx.network.

La machine virtuelle marquée de la balise nsx.network est déplacée vers vm-overlay-sg.

Solution : supprimez la balise non valide.

- **Problème 2355113** : impossible d'installer NSX Tools sur les machines virtuelles de la charge de travail RedHat et CentOS avec l'option d'accélération de la mise en réseau activée dans Microsoft Azure.

Dans Microsoft Azure, lorsque l'accélération de mise en réseau est activée sur un système d'exploitation RedHat (7.4 ou version ultérieure) ou CentOS (7.4 ou version ultérieure) et si NSX Agent est installé, l'interface Ethernet n'obtient pas d'adresse IP.

Solution : après le démarrage d'une VM RedHat ou CentOS dans Microsoft Azure, installez le dernier pilote des Services d'intégration Linux, disponible à l'adresse <https://www.microsoft.com/en-us/download/details.aspx?id=55106> avant d'installer NSX Tools.

- **Problème 2391231** : la détection des modifications apportées aux machines virtuelles Azure peut être différée.

Par intermittence, les modifications apportées aux machines virtuelles Azure sur le cloud sont détectées avec un léger délai. Par conséquent, un retard correspondant peut affecter l'intégration des machines virtuelles et la création d'entités logiques pour les machines virtuelles dans NSX-T. Le retard maximal observé est de huit minutes environ.

Solution : aucune. Une fois le délai écoulé, le problème se résout de lui-même.

- **Problème 2424818** : les statistiques de L2 et DFW ne sont pas mises à jour sur l'interface utilisateur de NSX Manager.

Toutes les statistiques produites par l'exportateur logique sur les machines virtuelles de charge de travail ne sont pas transférées vers MP. Cela provoque un échec d'affichage des statistiques sur l'interface utilisateur de NSX Manager. Il n'y a aucune visibilité des statistiques de DFW à partir de l'interface utilisateur de NSX Manager. L'état opérationnel des ports de commutateur logique s'affiche comme étant INACTIF et leurs statistiques correspondantes ne fonctionneront pas. Cela s'applique uniquement aux machines virtuelles de cloud.

Solution : aucune. Les statistiques peuvent être consultées via l'interface de ligne de commande sur les machines virtuelles correspondantes.