Notes de mise à jour de VMware NSX-T Data Center 2.4

VMware NSX-T Data Center 2.4 | 28 février 2019 | Build 12456646

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

NSX-T Data Center 2.4 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. Une nouvelle interface utilisateur de mise en réseau basée sur l'intention, un pare-feu sensible au contexte, des fonctionnalités d'introspection réseau et d'introspection d'invités, le protocole IPv6, la gestion en cluster hautement disponible, l'installation NSX sur profil pour les clusters de calcul vSphere, le mode de mise à niveau et de maintenance sans redémarrage de la fonctionnalité de calcul de NSX for vSphere, le nouveau mode de mise à niveau sur place pour le calcul vSphere et le coordinateur de migration pour la migration de NSX Data Center for vSphere vers NSX-T Data Center font partie de ses points forts.

Les nouvelles fonctionnalités et améliorations de fonctionnalités suivantes sont disponibles dans NSX-T Data Center 2.4.

Cluster de gestion

NSX-T Data Center 2.4 prend désormais en charge la création d'un cluster de gestionnaires afin d'assurer la haute disponibilité de l'interface utilisateur et de l'API. Cette création de cluster prend en charge les deux équilibrages externes pour la redondance et la distribution de charge, ou une adresse IP virtuelle avec NSX pour la redondance. Par ailleurs, la fonction de plan de gestion et la fonction de plan de contrôle central ont été réduites dans ce nouveau cluster de gestion afin de diminuer le nombre de dispositifs virtuels que l'administration de NSX doit déployer et gérer. Le dispositif NSX Manager est disponible dans trois tailles différentes pour divers scénarios de déploiement. Un petit dispositif pour les déploiements de laboratoire ou de preuve de concept. Un dispositif moyen pour les déploiements sur 64 hôtes, et un grand dispositif pour les clients qui effectuent un déploiement dans un environnement de grande envergure. Pour plus d'informations sur les valeurs maximales de configuration de VMware, consultez la page relative à l'outil correspondant à l'adresse : https://configmax.vmware.com

Prise en charge de la conception de cluster unique

Les conceptions de cluster unique avec des VM Edge + de gestion + de calcul réduites toutes alimentées par un seul N-VDS sur un hôte physique unique sont prises en charge. Des conceptions de référence typiques pour les clients VCF SP prescrivent 4 pNIC 10G avec deux commutateurs d'hôte ; un pour les VM Edge+de gestion et un autre pour les VM de calcul. Cela permet d'isoler efficacement la communication entre la VM Edge et la VM de calcul afin que le trafic quitte l'hôte et y revienne. Toutefois, avec les prix actuels des cartes réseau 25G, les clients VCF SP ont tendance à utiliser 2 hôtes 25G et, grâce à cette conception, ils peuvent passer à un seul N-VDS alimentant un hôte avec 2 pNIC. Dans cette conception, la VM Edge et la VM de calcul appartenant au même sous-réseau peuvent communiquer sans trafic quittant les liaisons montantes de l'hôte et y revenant.

Stratégie et interface utilisateur

Automatisation et gestion NSX

- **Gestion des stratégies déclaratives** : simplifiez et automatisez les configurations de réseau et de sécurité grâce à des instructions de stratégie orientées résultats. Cette nouvelle API de stratégie déclarative réduit le nombre d'étapes de configuration en autorisant les utilisateurs à décrire les objectifs finaux souhaités, tout en laissant le système déterminer la meilleure façon d'y parvenir. Définissez une topologie réseau complète et déployez-la intégralement en une seule fois, de manière indépendante de l'ordre et normative.

Améliorations de l'Interface utilisateur

- **Navigation et disposition des pages optimisées** : disposition de la barre de navigation et des pages améliorée pour réduire le nombre de clics nécessaires à l'accès aux informations essentielles.
- **Internationalisation** : gestion améliorée des éléments spécifiques des paramètres régionaux, tels que le format de date/d'heure, le format des nombres et le fuseau horaire.

Remarque : la fonctionnalité de visualisation de la topologie réseau de NSX Policy Manager, introduite dans la version 2.3, est obsolète dans cette version.

Pare-feu

Le pare-feu distribué et les pare-feu de passerelle prennent en charge le filtrage du trafic IPv6 à partir de NSX-T Data Center 2.4. Par ailleurs, différentes fonctionnalités opérationnelles ont été ajoutées au produit, comme indiqué ci-dessous :

Bouton Publier/Restaurer

Un bouton Publier unique est disponible pour l'intégralité du tableau de pare-feu, qu'il s'agisse de pare-feu distribués ou de pare-feu de passerelle. Avant NSX-T Data Center 2.4, le bouton Publier fonctionnait pour chaque section individuellement. Cette nouvelle fonctionnalité est désormais disponible via l'API. En outre, vous avez la possibilité d'annuler vos modifications. Vous pouvez également verrouiller des sections lors de la mise à jour de modifications.

Statistiques de règle

Chaque règle comprend le nombre d'accès, le nombre de paquets, le nombre de sessions, le nombre d'octets et l'indice de popularité. Y figurent également les valeurs maximales observées par rapport au nombre d'accès actuel. Ces statistiques peuvent être réinitialisées par la simple activation d'un bouton.

Amélioration du regroupement

Des critères de regroupement supplémentaires dépendant du système d'exploitation pour les groupes de machines virtuelles et Active Directory sont disponibles.

Visibilité des règles par machine virtuelle

Pour accéder à la liste des règles de pare-feu d'une machine virtuelle particulière, observez le port du commutateur logique correspondant.

Découverte d'adresses IP pour les machines virtuelles

Le profil par défaut de la découverte d'adresses IP est mis à jour de manière à inclure la découverte d'adresses IP VMTools, outre les écoutes ARP et DHCP. La mise à niveau à partir de versions antérieures de clients existants requiert la mise à jour du profil de la découverte d'adresses IP pour activer la détection VMTools. Par ailleurs, la création d'un profil de découverte d'adresses IP global est prise en charge avec NSX-T 2.4. Les modifications suivantes ont également été apportées :

1. La découverte d'adresses IP IPv6 basée sur DHCPv6 et des mécanismes de découverte de voisin sont disponibles.
2. La découverte IPv6 est désactivée par défaut.
3. Les liaisons d'adresses IP détectées automatiquement peuvent être manuellement mises en liste verte ou ignorées.
4. Les adresses IPv4 de type lien local sont par défaut ignorées.

Pare-feu d'identité

NSX-T Data Center 2.4 introduit des règles basées sur l'identité (ID d'utilisateur) pour les pare-feu distribués. Les administrateurs de pare-feu peuvent désormais configurer des règles distribuées sur les machines virtuelles basées sur des groupes Active Directory. Cette fonctionnalité permet aux administrateurs de pare-feu de fournir des règles de pare-feu dépendant des utilisateurs connectés aux machines virtuelles. NSX détecte automatiquement les utilisateurs connectés/déconnectés et, en conséquence, des règles spécifiques sont activées pour les utilisateurs. Un pare-feu reposant sur l'identité peut détecter et appliquer des règles pour un seul utilisateur par machine virtuelle, voire suivre plusieurs utilisateurs avec des sessions particulières sur une même machine virtuelle. Les administrateurs de pare-feu créent des groupes NSX-T à l'aide de groupes Active Directory utilisés en guise de critère. Le gestionnaire NSX-T récupère automatiquement une liste de groupes Active Directory à partir des contrôleurs de domaine fournis. Les administrateurs de pare-feu peuvent contrôler l'accès est-ouest des utilisateurs, notamment dans les environnements de postes de travail virtuels ou les sessions de bureau à distance avec services de terminaux activés.

Signatures d'application L7 pour pare-feu distribué basé sur le contexte

NSX-T Data Center 2.4 offre la possibilité d'inclure des signatures d'application L7 dans les règles de pare-feu distribué. Les utilisateurs peuvent utiliser une combinaison de règles L3/L4 avec les signatures d'application L7 ou peuvent simplement créer des règles basées sur la signature d'application L7 uniquement. Nous prenons actuellement en charge les signatures d'application avec divers sous-attributs pour les communications serveur-serveur ou client-serveur uniquement. Dans NSX-T Data Center 2.4, cette fonctionnalité est disponible pour les nœuds de transport ESXi uniquement.

Mise en liste verte des noms de domaine complets/URL pour pare-feu distribué basé sur le contexte

NSX-T Data Center 2.4 introduit des règles basées sur la mise en liste verte des URL/noms de domaine complets dans un pare-feu distribué. NSX-T Data Center présente une autre innovation : l'utilisation de l'écoute sur un DNS distribué afin que chaque connexion opérée à partir de chacune des machines virtuelles puisse disposer de sa propre résolution d'URL/de nom de domaine complet. Les administrateurs de pare-feu peuvent utiliser des domaines d'URL prédéfinis et les appliquer aux règles d'un pare-feu distribué. Les applications hybrides ayant accès à des services SaaS ou basés sur le cloud peuvent entreprendre une microsegmentation en fonction des URL auxquelles elles accèdent. Les applications clientes ou les navigateurs ayant accès à des applications SaaS peuvent bénéficier d'un accès granulaire. Dans NSX-T Data Center 2.4, cette fonctionnalité est disponible pour les nœuds de transport ESXi uniquement.

Insertion de services

NSX-T Data Center 2.4 introduit un large éventail de fonctionnalités de sécurité natives, comme l'identité d'application de couche 7, la mise en liste verte des noms de domaine complets et le pare-feu d'identité, qui permettent une microsegmentation encore plus granulaire. Outre les contrôles de sécurité natifs fournis par les pare-feu de passerelle et distribués, la structure de l'insertion de services NSX permet l'insertion transparente de différents types de services de partenaires, comme des IDS/IPS, un NGFW et des solutions de surveillance réseau, dans le chemin d'accès aux données, et leur utilisation à partir de NSX, sans qu'il soit nécessaire de modifier la topologie.

Dans NSX-T Data Center 2.4, l'insertion de services prend désormais en charge le trafic est-ouest (c'est-à-dire le trafic entre les machines virtuelles dans le centre de données). Dans le centre de données, l'ensemble du trafic entre les machines virtuelles peut être redirigé vers une chaîne dynamique de services de partenaires.

Le plan de service est-ouest fournit son propre mécanisme de transfert qui permet la redirection du trafic, en fonction des stratégies, le long des chaînes de services. Le transfert le long du plan de service est entièrement automatisé par la plate-forme : les échecs sont détectés et les nouveaux flux ainsi que les flux existants sont redirigés si nécessaire, la mise en attente de flux est effectuée pour prendre en charge les services avec état et plusieurs stratégies de sélection de chemin d'accès sont disponibles pour optimiser le débit, la latence ou la densité.

Guest Introspection

NSX-T Data Center 2.4 introduit la plate-forme du service Guest Introspection pour les partenaires de VMware, afin de fournir les capacités de déchargement anti-programme malveillant et antivirus sans agent reposant sur des stratégies, nécessaires pour les charges de travail de machines virtuelles invitées Windows sur les hyperviseurs vSphere ESXi.

Dans NSX-T Data Center 2.4, la plate-forme de Guest Introspection fournit :

- Un déploiement et une gestion du cycle de vie simplifiés grâce à la consolidation du déploiement de Guest Introspection dans l'installation de préparation de l'hôte NSX Agent et à l'absence d'exigence de déploiement de la machine virtuelle du service universel Guest Introspection sur chaque hyperviseur ESXi.
- Des services cohérents reposant sur des stratégies, sur plusieurs systèmes vCenter.
- Des améliorations à l'échelle des partenaires de VMware via le dimensionnement d'une machine virtuelle de protection partenaire (c'est-à-dire, la définition de la dimension des dispositifs partenaires : petits, moyens ou grands).

Mise en réseau L2

Plusieurs N-VDS par hôte

En plus d'apporter la flexibilité nécessaire à l'organisation du trafic de la machine virtuelle, cette nouvelle fonctionnalité de prise en charge de plusieurs N-VDS par hôte facilite le respect de la réglementation PCI dans le cadre de laquelle un isolement strict est requis pour le trafic de la machine virtuelle.

Avec l'ajout de cette fonctionnalité, il est désormais possible de séparer les liaisons montantes ENS des liaisons montantes non ENS, une fonctionnalité utile car, ENS ne disposant actuellement pas de la parité des fonctionnalités avec N-VDS, les charges de travail ENS obtiennent un chemin d'accès rapide, mais ne sont pas performantes en termes de fonctionnalités.

Visualisation de N-VDS

Cette fonctionnalité permet de gérer le N-VDS comme un objet autonome avec la possibilité d'explorer au niveau du détail les hôtes connectés, etc. Lors de l'observation d'un hôte spécifique, il est possible de voir une grille d'interface utilisateur qui indique la manière dont il est connecté au N-VDS. Les interfaces logiques, comme les interfaces de noyau de machine virtuelle, sont également visibles dans le N-VDS. Il s'agit d'une amélioration considérable par rapport à la vue Hôte. La liste des interfaces (toutes les cartes réseau physiques, les interfaces de noyau de machine virtuelle et tous les ports OVS) est reflétée dans une seule vue.

Prise en charge LLDP des cartes réseau physiques

Cette fonctionnalité permet de combler les lacunes de la mise en œuvre LLDP pour NSX. Elle fournit une capacité de débogage pour la connectivité des commutateurs physiques. La possibilité d'identifier les ports physiques connectés aux interfaces d'un hôte est propice à la résolution aisée des problèmes de câblage. L'étendue de cette fonctionnalité s'applique à tous les hôtes physiques (ESXi, KVM, hôtes Linux bare metal et Edge bare metal) qui participent à un plan de données NSX.

Prise en charge d'un proxy ARP sur un nœud Edge

Lorsque des clients externes accèdent à des services tels que l'équilibreur de charge, IKE, etc. avec les mêmes adresses de sous-réseau, ils accèdent au routage des terminaux. Ils envoient des requêtes ARP pour ces adresses liées aux ports de bouclage. Toutefois, les ports de bouclage LR n'ont pas d'adresses MAC et ne répondent donc pas à ces requêtes ARP. Cela entraîne des problèmes d'accès.

La solution consiste actuellement à configurer un routage /32 dans ces clients, comme Adresse IP de bouclage/32 → Liaison montante/CSP, afin que le trafic puisse être transmis à des ports de liaison montante/CSP et qu'il puisse ensuite atteindre le port de bouclage approprié. Le proxy ARP est la solution idéale pour remédier à cet inconvénient.

Mise en réseau L3

Améliorations de la configuration MTU

NSX-T 2.4 offre deux nouveaux paramètres globaux de MTU :

- MTU de liaison montante physique globale, qui configure la valeur MTU pour toutes les instances de N-VDS dans le domaine NSX. Cela s'apparente à la taille maximale des trames GENEVE encapsulées ou MTU du TEP.
    - La valeur MTU du profil de liaison montante peut remplacer le paramètre de liaison montante physique globale sur un hôte spécifique.
- MTU d'interface logique globale, qui configure la valeur MTU pour toutes les interfaces de routeur logique.
    - La valeur MTU de liaison montante pour routeur logique et la valeur MTU de port CSP peuvent remplacer la valeur MTU d'interface logique globale sur un port spécifique, si nécessaire.

Grâce à cela, les communications de bout en bout pour la machine virtuelle configurée avec une valeur MTU supérieure à 1 500 octets sont possibles pour le trafic est-ouest et pour le trafic nord-sud.

Routage Inter SR

Les routeurs logiques de niveau 0 en mode actif/actif peuvent désormais établir automatiquement des appairages iBGP à maillage total sur tous les routeurs de service constituant un routeur logique de niveau 0 donné. Cela empêche les rejets de trafic en présence de routeurs de services configurés avec plusieurs liaisons montantes, parmi lesquels un seul est défaillant. Dans ce scénario d'échec, un routeur de services transfère désormais le trafic à un autre routeur de services si la destination n'est pas disponible sur ses liaisons montantes.

Améliorations du redirecteur DNS

- La fonction de redirecteur DNS peut désormais être activée ou désactivée sans perdre sa

configuration actuelle.
- La fonction de redirecteur DNS expose également des statistiques, événements et alarmes via l'API et l'interface utilisateur.

Prise en charge de SNAT d'une liaison montante à une autre

NSX-T 2.4 introduit la prise en charge de SNAT (traduction d'adresses source) pour le trafic entrant un routeur logique de niveau 0 via une liaison montante et quittant le même routeur logique via une autre liaison montante. Cette fonctionnalité est utile lorsque plusieurs routeurs logiques de niveau 0 sont reliés entre eux.

Prise en charge du proxy ARP sur le routeur logique de niveau 0

NSX-T 2.4 introduit la prise en charge du proxy ARP sur les liaisons montantes de routeur logique de niveau 0. Cela permet le déploiement de NSX-T dans des environnements où le routage ne peut pas être configuré sur les routeurs ascendants du routeur logique de niveau 0. Avec cette fonctionnalité, la NAT, l'équilibreur de charge ou n'importe quel service avec état peut être configuré avec une adresse IP appartenant au réseau de la liaison montante de niveau 0.

Améliorations du nœud Edge

- NSX-T 2.4 introduit l'option sur le nœud Edge bare metal pour prendre en charge la gestion sur les cartes réseau à accès rapide, et met ainsi un terme à l'utilisation d'une carte réseau de gestion dédiée.
- Le nœud Edge bare metal prend également en charge les cartes réseau Intel 25 Gbits/s XXV710.
- Le nœud Edge prend en charge plusieurs points de sortie du tunnel (Tunnel EndPoint, TEP) GENEVE. Grâce à cette particularité, les nœuds Edge ne sont pas obligés d'utiliser LAG pour la haute disponibilité du trafic de superposition.

Améliorations de BGP

- À partir de NSX-T 2.4, les routeurs logiques de niveau 0 prennent en charge l'appairage iBGP avec des routeurs physiques ascendants.
- NSX-T 2.4 introduit la possibilité d'activer ECMP entre des pairs eBGP dans différents ASN (commande « as-path multipath relax ») et également la prise en charge du routeur logique de niveau 0 pour autoriser son propre ASN dans AS-PATH (commande « allow-as in »).

IPv6

NSX-T 2.4 introduit le routage/transfert et la sécurité IPv6. Cela comprend la prise en charge des éléments suivants :

- Itinéraire statique IPv6
- Découverte de voisin IPv6
- Relais DHCPv6
- Pare-feu distribué (Distributed Firewall, DFW) IPv6
- Pare-feu Edge IPv6
- Plage d'adresses IPv6 pour MP-BGP et l'élément prefix-list/route-map associée
- Sécurité du commutateur IPv6
- Découverte d'adresses IPv6
- Outils dédiés aux opérations IPv6

Opérations

Améliorations de Traceflow

Traceflow ajoute la prise en charge d'un nombre encore supérieur de capacités de dépannage et de visualisation. Dans NSX-T 2.4, Traceflow fournit des observations aux services centralisés tels que l'équilibreur de charge, le pare-feu Edge, la NAT et le VPN sur route.

Améliorations de l'installation

- NSX permet des déploiements simplifiés grâce à une nouvelle procédure d'installation sur profil des composants NSX pour les clusters de calcul vSphere. Cette fonctionnalité permet d'accélérer les déploiements, favorise la cohérence de la configuration, évite le risque d'erreurs manuelles et offre un moyen de définir des paramètres une fois avant de les réutiliser plusieurs fois.
- Prise en charge d'une installation automatisée et de la mise en cluster des nœuds NSX Manager à partir de l'interface utilisateur.
- Prise en charge de plusieurs configurations de déploiement à des fins de création de plusieurs commutateurs N-VDS, et de migration de ports VMKernel et d'adaptateurs physiques à travers des profils.

Améliorations de la mise à niveau

- Améliorations apportées à des fins de mise à niveau entièrement orchestrée des hôtes ESXi, sans le coût inhérent au redémarrage de ces derniers, grâce à la mise à niveau de NSX en mode Maintenance par défaut.
- Introduction d'un nouveau mode de mise à niveau de NSX appelé « Mise à niveau sur place ». Cette fonctionnalité participe à la simplicité opérationnelle et permet des mises à niveau plus rapides. Lorsque vous utilisez ce mode, les composants de NSX sur les hôtes ESXi sont mis à niveau sans qu'il soit nécessaire de désactiver les charges de travail ou de les migrer vers un autre hyperviseur.
- Introduction d'une nouvelle infrastructure et application de tests prêts à l'emploi pour effectuer des vérifications préalables et ultérieures à la mise à niveau de NSX, afin de déceler des problèmes sous-jacents dormants avant la mise à niveau réelle ou immédiatement après cette dernière.

Sauvegarde de NSX lors de la détection de modifications

NSX améliore sa solution de récupération d'urgence en offrant la possibilité de détecter les modifications apportées à la configuration et de les sauvegarder de manière proactive dans un espace de stockage sécurisé. Cette fonctionnalité permet aux clients de bénéficier d'un meilleur SLA pour les sauvegardes de configuration, sans le coût inhérent à la sauvegarde de fichiers inutiles sur le serveur de stockage.

NFV

Le commutateur N-VDS prend désormais en charge les améliorations suivantes en mode EDP.

- Pare-feu distribué
- Découverte d'adresses IP
- SpoofGuard
- IPFIX
- IPv6
- Performances améliorées pour la machine virtuelle Edge, qui fournit désormais jusqu'à cinq fois plus de débit en mode EDP.
- Redondance du chemin d'accès pour les applications multirésidents. La possibilité d'épingler une machine virtuelle à une liaison montante spécifique permet aujourd'hui la construction d'un chemin redondant multirésidents sur NSX avec les VTEP.

Opérations - Sécurité AAA/RBAC et de la plate-forme

Opérations

- Améliorations de l'identité principale : Permet aux utilisateurs de l'identité principale d'enregistrer et d'installer des composants NSX. Ajout de la prise en charge de l'interface utilisateur pour la création d'utilisateurs de l'identité principale et l'attribution de rôles.

- **Améliorations de la stratégie de mot de passe** : Applique la longueur minimale de 12 caractères pour les mots de passe par défaut. Introduit la possibilité de définir des délais d'expiration de mot de passe et génère des alarmes lorsque le mot de passe est sur le point d'expirer. Par défaut, les mots de passe expirent après 90 jours. Consultez l'article 70691 de la base de connaissances pour obtenir des instructions sur la réinitialisation des mots de passe et sur la modification de l'expiration du mot de passe.

- **Gestion des certificats** : Permet de vérifier l'état de révocation du certificat.

VPN

NSX-T 2.4 a ajouté les capacités suivantes pour les services VPN :

- L'API et l'interface utilisateur dédiées aux stratégies sont disponibles pour les services VPN L3 et VPN L2.
- Les services VPN L3 prennent en charge l'authentification par certificat pour une meilleure gestion de la sécurité.
- Le mode Client VPN L2 est disponible pour la prise en charge de l'extension L2 d'un SDDC NSX-T à un autre.
- Les groupes DH 19, 20 et 21 sont disponibles pour répondre à des exigences élevées en matière de sécurité.

Équilibrage de charge

NSX-T 2.4 offre désormais les capacités suivantes pour les services d'équilibrage de charge :

- Une API et une nouvelle interface utilisateur dédiées aux stratégies sont disponibles. L'ancienne interface utilisateur dédiée à l'équilibreur de charge est toujours disponible sous l'onglet Mise en réseau et sécurité avancées.
- Les adresses IP virtuelles sur un SR autonome peuvent appartenir au même sous-réseau que celui sur lequel se trouve le port de service centralisé ou CSP. Avant cette version, si vous souhaitiez créer une adresse IP virtuelle sur le même sous-réseau que celui utilisé par le réseau CSP, l'adresse IP du CSP devait être utilisée pour l'adresse IP virtuelle. Sinon, vous deviez créer une adresse IP virtuelle sur un autre réseau.
- La DNAT et le pare-feu Edge sont pris en charge pour les flux de trafic d'équilibreur de charge sur la même passerelle de niveau 1. Avant cette version, les flux de trafic d'équilibreur de charge contournaient le pare-feu Edge.
- Les règles d'équilibreur de charge prennent en charge les en-têtes HTTP commençant par « _ ». Grâce à cette amélioration, l'équilibreur de charge NSX peut être déployé pour vIDM et AirWatch.
- Une adresse IP virtuelle peut être utilisée comme adresse IP source pour la SNAT de l'équilibreur de charge.
- La taille maximale de l'en-tête de réponse HTTP peut être configurée sur 64 Ko. La taille par défaut reste celle de la version précédente, soit 4 Ko.
- Une machine virtuelle Edge de grande dimension prend en charge une instance d'équilibreur de charge volumineuse. Avant cette version, la machine virtuelle Edge de grande dimension ne pouvait prendre en charge, au maximum, qu'une instance d'équilibreur de charge de taille moyenne.

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

NSX-T 2.4 est désormais équipé d'un coordinateur de migration qui peut être utilisé pour faciliter la migration de NSX Data Center for vSphere vers NSX-T Data Center. Cette fonctionnalité est conçue pour migrer les hôtes existants sans utiliser vMotion. Le coordinateur de migration prend en charge la migration de la mise en réseau de couche 2, de la mise en réseau de couche 3, du pare-feu, de l'équilibrage de charge et du VPN. Le *guide du coordinateur de migration NSX-T Data Center* fournit des détails concernant l'outil.

Aucune ressource de calcul supplémentaire n'est nécessaire au-delà du simple déploiement de gestionnaires NSX-T Manager et de nœuds Edge. Une fois la migration terminée, le client peut désinstaller NSX for vSphere, et les gestionnaires, contrôleurs et dispositifs Edge associés. Veuillez noter que cette migration affecte le trafic du plan de données et est conçue pour être exécutée dans une fenêtre de modification unique.

Automatisation, OpenStack et autres CMP

NSX-T 2.4 introduit les capacités suivantes pour la consommation OpenStack via son plug-in Neutron :

- Prise en charge de Rocky et de Queens
- Prise en charge de la mise en cluster du plan de gestion
  Le plug-in d'OpenStack Neutron exploite la possibilité de disposer d'un cluster de gestionnaires. Il peut utiliser les points de terminaison de l'API REST de trois gestionnaires sans adresse IP virtuelle externe, pour des performances accrues et une plus grande disponibilité.
- Prise en charge de Barbican
  Le plug-in d'OpenStack Neutron prend désormais en charge Barbican. Barbican est une API REST conçue pour le stockage sécurisé, le provisionnement et la gestion des secrets, comme les mots de passe, les clés de chiffrement et les certificats X.509. Elle permet de gérer le certificat prévu pour l'équilibreur de charge en tant que service à des fins d'arrêt du protocole HTTPS. Il s'agit d'une fonctionnalité actuellement prise en charge dans l'environnement VIO uniquement.

Le fournisseur Terraform pour NSX-T complète les capacités de NSX-T 2.4 (création de commutateurs logiques, routeurs, règles de pare-feu, etc.) avec les suivantes :

- Prise en charge d'un CRUD sur l'équilibreur de charge et la configuration de l'équilibreur de charge (moniteur, pool, etc.).
- Prise en charge d'un CRUD sur les serveurs DHCP
- Prise en charge d'un CRUD sur la fonction IPAM de NSX-T (bloc d'adresses IP, pool d'adresses IP)

NSX Cloud

NSX-T 2.4 pour NSX Cloud possède de nombreuses nouvelles fonctionnalités pour faciliter le déploiement/l'adoption d'un client, offrir davantage d'options quant à la manière dont un client peut procéder à l'insertion de services et à l'arrêt du VPN, gérer ses environnements VDI et ainsi gérer de réelles régions multiples, et entreprendre un déploiement multicloud hybride.
Voici quelques-unes des fonctionnalités clés de NSX Cloud avec NSX-T 2.4 :

- Passerelle partagée sur un réseau VPC/VNET de transit pour une intégration et une consolidation simplifiées et accélérées
- VPN pour le trafic acheminé par le réseau terrestre de retour vers un contrôleur de domaine sur site
- Insertion de services et intégration de partenaires nord-sud sélectives
- Microsegmentation sur Horizon Cloud pour Azure
- Stratégie basée sur l'intention pour les charges de travail hybrides

Architecture simplifiée d'un VPC/VNET de transit : À partir de la version 2.4, les clients peuvent installer une seule passerelle NSX Cloud sur un VPC/VNET de transit et gérer jusqu'à 10 VPC/VNET de calcul. Cela simplifie l'architecture de transit/de calcul hub-and-spoke et active le routage transitif entre les VPC de calcul, même lorsqu'ils n'ont pas de connexion d'homologue. À l'aide du tunneling de superposition NSX, le trafic entre les VPC peut désormais être envoyé dans un tunnel de superposition. Des stratégies de transfert peuvent être configurées au niveau de la VM pour indiquer si le trafic doit être encapsulé par Geneve et envoyé dans la superposition, ou s'il doit être envoyé dans le réseau de sous-couche du fournisseur de cloud public. Toutes ces fonctionnalités offrent plus de flexibilité quant à la manière dont les utilisateurs peuvent acheminer le trafic à l'intérieur et à l'extérieur de leur réseau de cloud public.

VPN pour le trafic acheminé par le réseau terrestre : NSX Cloud prend désormais en charge la multiplicité des tunnels VPN pour l'acheminement terrestre du trafic du cloud public au centre de données sur site. Les VPN partant du centre de données sur site peuvent désormais être directement interrompus au niveau de la passerelle NSX Cloud du cloud public. Les clients n'ont pas besoin de la VGW fournie par les fournisseurs du cloud public, ce qui réduit les coûts inhérents. Cette possibilité réduit également le temps système de gestion, la passerelle NSX Cloud propageant automatiquement les routes sur BGP. En termes de bande passante, NSX Cloud optimise également la capacité : Les flux de trafic inter-VPC peuvent être à 5 Gbits/s sur les réseaux VPC appariés contre seulement 1 Gbit/s sur la VGW.

Insertion de services et intégration de partenaires nord-sud sélectives : Les clients peuvent déployer le service de partenaires directement à partir du Marketplace du cloud public, dans l'architecture des services partagés/de transit. La passerelle NSX Cloud présente sur le réseau VPC/VNET de transit peut être programmée pour acheminer de manière sélective le trafic vers le dispositif de service de partenaires basé sur des stratégies NSX. Cette programmation peut représenter d'incroyables économies pour un client, car il n'est pas obligé de diriger l'ensemble du trafic via un dispositif de pare-feu L7 virtuel acquis pour le cloud public et facturé en fonction du trafic acheminé. Et si cela ne suffisait pas, l'insertion de services avec NSX Cloud ne nécessite aucun VPN pour les réseaux VPC/VNET de calcul. Davantage d'économies et moins d'opérations.

Microsegmentation sur Horizon Cloud pour Azure : NSX Cloud présente désormais une solution combinée avec Horizon Cloud pour Azure. Pour les clients qui choisissent un environnement de VDI Horizon déployé dans Azure, NSX Cloud fournit la microsegmentation nécessaire et sécurise l'environnement de VDI.

Stratégie basée sur l'intention pour les charges de travail hybrides : Cloud Service Manager (CSM) a été intégré à NSX Manager. Les clients peuvent désormais définir une stratégie unique basée sur l'intention à partir du gestionnaire de stratégies, sans se préoccuper de l'emplacement du déploiement des charges de travail ou de la destination de leur déplacement à venir. NSX Cloud applique cette stratégie de manière cohérente sur le contrôleur de domaine sur site, Azure et AWS.

Compatibilité et configuration système requise

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

Ressources relatives aux interfaces de ligne de commande et aux API

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

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

Historique de révision du document

28 février 2019. Première édition.
2 avril 2019. Deuxième édition. Ajout des problèmes connus : 2273651, 2279326, 2281095 et 2296888. Ajout du problème résolu : 2199785.
10 avril 2019. Troisième édition. Ajout des problèmes connus : 2203863, 2248186, 2252738, 2277543, 2276398, 2279326, 2281537, 2287124, 2290688, 2294178, 2295592, 2296430, 2297157, 2297918 et 2298499. Mise à jour de la section Nouveautés pour inclure Prise en charge de la conception de cluster unique.
20 juin 2019. Quatrième édition. Ajout du problème connu 2261818. Ajout du problème résolu 2182745.
23 août 2019. Cinquième édition. Ajout des problèmes connus 2362688, 2395334 et 2392093.

Problèmes résolus

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

- **Problème résolu 2279326 : Aucune erreur ne s'affiche lors de la création d'un collecteur IPFIX L2 avec plus de 4 combinaisons IP:PORT**
  Aucun message d'erreur ne s'affiche pour le nombre maximal de combinaisons IP:Port autorisées. Il n'y a aucun dommage, car l'interface utilisateur limite la création de balises si la limite maximale est dépassée.

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

- **Problème résolu 1909703 : Un administrateur NSX est autorisé à créer des itinéraires statiques, des règles nat et des ports dans un routeur créé par OpenStack directement à partir du serveur principal**
  Dans le cadre de la fonctionnalité RBAC dans NSX-T 2.0, les ressources, telles que les commutateurs, les routeurs, les groupes de sécurité créés par le plug-in OpenStack, ne peuvent pas être supprimées ou modifiées directement par un administrateur NSX à partir de l'interface utilisateur/API NSX. Ces ressources ne peuvent être modifiées/supprimées que par les API envoyées via le plug-in OpenStack. Il existe une limite à cette fonctionnalité. Actuellement, la seule limite imposée à un administrateur NSX est qu'il ne peut pas supprimer/modifier les ressources créées par OpenStack. Par contre, il est autorisé à créer des ressources, telles que des itinéraires statiques, des règles nat dans les ressources existantes créées par OpenStack.

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

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

- **Problème résolu 2111047 : Application Discovery n'est pas pris en charge sur les hôtes VMware**

vSphere 6.7 dans la version 2.2 de NSX-T
L'exécution d'Application Discovery sur un groupe de sécurité comportant des machines virtuelles en cours d'exécution sur un hôte vSphere 6.7 provoque l'échec de la session Application Discovery.

- Problème résolu 2157370 : lors de la configuration de L3 Switched Port Analyzer (SPAN) avec troncation, un commutateur physique spécifique abandonne des paquets mis en miroir
  Lors d'une configuration de L3 SPAN qui inclut GRE/ERSPAN avec troncation, les paquets mis en miroir tronqués sont abandonnés en raison de la stratégie du commutateur physique. Il est possible que le port reçoive des paquets dans lesquels le nombre d'octets de charge utile ne correspond pas au champ de longueur type.

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

- Problème résolu 2114756 : dans certains cas, les VIB ne sont pas supprimés lorsqu'un hôte est supprimé du cluster NSX-T préparé
  Lorsqu'un hôte est supprimé du cluster NSX-T préparé, certains VIB peuvent rester sur l'hôte.

- Problème résolu 2059414 : l'installation du bundle RHEL LCP échoue en raison d'une ancienne version de python-gevent RPM
  Si un hôte RHEL contient une version plus récente de python-gevent RPM, l'installation du bundle RHEL LCP échoue, car NSX-T Data Center RPM contient une ancienne version de python-gevent RPM.

- Problème résolu 2142755 : L'installation des modules de noyau OVS échoue en fonction du miroir sur lequel la version du noyau RHEL 7.4 est en cours d'exécution
  L'installation des modules de noyau OVS échoue sur un hôte RHEL 7.4 exécutant un noyau de version 17.1 mineure ou version ultérieure. L'échec d'installation provoque l'arrêt du fonctionnement des chemins d'accès aux données du noyau, ce qui entraîne l'indisponibilité de la console de gestion de dispositifs.

- Problème résolu 2125725 : après la restauration de déploiements de topologie volumineux, les données de recherche ne sont plus synchronisées et plusieurs pages de NSX Manager cessent de répondre
  Après la restauration de NSX Manager avec des déploiements de topologie volumineux, les données de recherche ne sont plus synchronisées et plusieurs pages de NSX Manager affichent le message d'erreur Une erreur irrécupérable est survenue.

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

- Problème résolu 2077145 : dans certains cas, la tentative de suppression forcée du nœud de transport peut créer des nœuds de transport orphelins
  Les tentatives de suppression du nœud de transport à l'aide d'un appel d'API lorsque, par exemple, il existe une défaillance matérielle et les hôtes deviennent irrécupérables, modifient l'état du nœud de transport sur Orphelin.

- Problème résolu 2099530 : la modification de l'adresse IP VTEP du nœud de pont entraîne l'indisponibilité du trafic
  Lorsque l'adresse IP VTEP du nœud de pont est modifiée, la table MAC du VLAN pour la superposition n'est pas mise à jour sur les hyperviseurs distants, ce qui entraîne une indisponibilité du trafic sur une période pouvant atteindre 10 minutes.

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

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

- **Problème résolu 2125514 : après un basculement de pont de couche 2, le commutateur logique de certaines machines virtuelles NSX Edge peut effectuer une réplication BUM de chaque paquet jusqu'à ce que l'adresse MAC soit réapprise**
  Après un basculement de pont de couche 2, le commutateur logique de certaines machines virtuelles NSX Edge peut effectuer une réplication BUM de chaque paquet pendant presque 10 minutes jusqu'à ce que l'adresse MAC soit réapprise pour le point de terminaison. Le système récupère de lui-même après que les points de terminaison ont généré la prochaine ARP.

- **Problème résolu 2183549 : lorsque vous modifiez un port de service centralisé, il est impossible de voir un commutateur logique VLAN récemment créé**
  Dans l'interface utilisateur de Manager, après la création d'un port de service centralisé et d'un commutateur logique VLAN, si vous modifiez le port du service centralisé, vous ne pouvez pas voir le commutateur logique VLAN créé.

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

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

- **Problème résolu 1928376 : État dégradé du nœud de membre du cluster de contrôleur après la restauration de NSX Manager**
  Le nœud de membre du cluster de contrôleur peut devenir instable et signaler un état dégradé si NSX Manager est restauré sur une image de sauvegarde qui a été prise avant que ce nœud de membre soit détaché du cluster.

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

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

- **Problème résolu 2160634 : la modification de l'adresse IP sur une boucle peut modifier l'adresse IP de l'ID de routeur sur une liaison montante**
  Si l'adresse IP sur le bouclage est modifiée, le dispositif NSX Edge sélectionne l'adresse IP sur la liaison montante en tant qu'ID de routeur. L'adresse IP de la liaison montante qui est attribuée comme ID de routeur ne peut pas être modifiée.

- **Problème résolu 2199785 : Noyau NGINX observé lors de l'ajout du moniteur d'intégrité (sans numéro de port) au pool dynamique (avec numéro de port)**

Lors de la configuration de l'équilibrage de charge avec un pool de serveurs ayant des membres dynamiques (avec numéro de port), puis tentant d'associer un moniteur de santé ne disposant pas d'un port de surveillance configuré, NGINX peut se bloquer.

- **Problème résolu 2182745 : Précédemment, le/ge dans les règles de redistribution n'étaient pas validés dans le gestionnaire et ne fonctionnaient pas correctement**
  Les règles de redistribution prennent en charge le/ge dans les listes de préfixes.

Problèmes connus

Les problèmes connus sont classés comme suit.

- Problèmes connus généraux
- Problèmes connus d'installation
- Problèmes connus de NSX Manager
- Problèmes connus de NSX Edge
- Problèmes connus de mise en réseau logique
- Problèmes connus des services de sécurité
- Problèmes connus de mise en réseau KVM
- Problèmes connus d'équilibreur de charge
- Problèmes connus d'interopérabilité entre les solutions
- Problèmes connus des opérations et des services de surveillance
- Problèmes connus de mise à niveau
- Problèmes connus de l'API
- Problèmes connus de NSX Policy Manager
- Problèmes connus de NSX Cloud

Problèmes connus généraux

- **Problème 2239365 : une erreur « Non autorisé » est signalée**
  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 2287482 : le tableau des liaisons détectées automatiquement peut inclure des liaisons qui n'ont pas encore été détectées**
  Dans le tableau des liaisons détectées automatiquement, les liaisons portant le libellé « En double » peuvent ne plus être découvertes.

  Solution : aucune.

- **Problème 2278142 : le profil global IPFIX d'un commutateur ne peut pas être modifié**
  Si des profils globaux sont disponibles dans le système, vous ne pouvez pas les modifier ou les supprimer via l'interface, car il n'existe aucun workflow pour ce type de profil.

  Solution : supprimez ce profil global en utilisant l'API.

- **Problème 2292222 : sur l'écran Résoudre l'erreur, l'utilisateur n'est pas informé de l'inexactitude de l'empreinte numérique**
  Si l'opération de préparation de l'hôte échoue, l'utilisateur peut résoudre le problème en cliquant sur Échec de l'installation de NSX, auquel cas il doit fournir le nom d'utilisateur, le mot de passe et l'empreinte numérique de l'hôte. Si l'utilisateur fournit une empreinte numérique incorrecte, le système n'en informe pas l'utilisateur et le problème reste non résolu.

Il n'existe aucun moyen de savoir que l'empreinte numérique était incorrecte. Consultez le journal dans lequel cette ThumbPrintValidationFailedException est consignée.

Solution : fournissez l'empreinte numérique correcte.

- **Problème 2252487 : l'état du nœud de transport n'est pas enregistré pour le nœud de transport BM Edge 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 2285117 : la mise à niveau du noyau sur les machines virtuelles gérées de NSX n'est pas prise en charge**
  Sur certaines images de Marketplace Linux Ubuntu, le noyau se met automatiquement à niveau lors du redémarrage de la machine virtuelle, et l'agent NSX ne fonctionne pas correctement. Bien que NSX Agent puisse paraître fonctionner, des stratégies de mise en réseau non réalisées affectent NSX Agent. L'agent tente encore et encore d'appliquer ces stratégies, sollicitant fortement le CPU.

  Solution : si une mise à niveau du noyau est requise, les en-têtes Linux appropriés pour ce noyau plus récent doivent d'abord être téléchargés et le module DKMS du chemin d'accès aux données Open vSwitch doit être recompilé.

- **Problème 2285544 : les hachages MD5 ne sont plus pris en charge lors de l'appel des API NSX exigeant la spécification d'une valeur ssh_fingerprint**
  NSX-T 2.4 ne prend plus en charge les algorithmes de chiffrement non FIPS, les hachages, etc., notamment l'appel des API NSX pour la sauvegarde/restauration, les magasins de fichiers et les bundles de support et la spécification d'un hachage MD5 pour la valeur ssh_fingerprint. En conséquence, les hachages MD5 ne sont plus pris en charge.

  Solution : indiquez un hachage différent calculé à l'aide d'un algorithme de hachage différent, par exemple, SHA256.

- **Problème 2256709 : une machine virtuelle Instant Clone ou une machine virtuelle restaurée à partir d'un snapshot perd brièvement la protection antivirus pendant son déplacement avec vMotion**
  Le snapshot d'une machine virtuelle est restaurée et migre la machine virtuelle vers un autre hôte. La console partenaire n'affiche pas la protection antivirus pour la machine virtuelle Instant Clone migrée. La protection antivirus est brièvement interrompue.

  Solution : aucune.

- **Problème 2261431 : une liste filtrée des banques de données est requise, selon les autres paramètres de déploiement**
  L'erreur correspondante est affichée sur l'interface utilisateur si l'option incorrecte a été sélectionnée. Le client peut supprimer ce déploiement et en créer un nouveau à des fins de récupération après erreur.

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

- **Problème 2266553 : dans le dispositif NSX, l'initialisation d'un service peut échouer lors de son premier démarrage**
  Le nœud déployé ne parvient pas à répondre aux demandes ou à former un cluster.

  Solution : essayez de redémarrer le service ayant échoué.

- **Problème 2267632 : perte de la configuration de la protection de l'IG**

La règle de protection des invités publiée sur l'interface utilisateur des stratégies indique une RÉUSSITE. Le changement de comportement correspondant n'est pas reflété sur la machine virtuelle invitée. Les journaux de l'agent d'opération indiquent en même temps un redémarrage. Perte de protection de la machine virtuelle invitée.

Solution : procédez manuellement à la relecture de la modification de la configuration.

- Problème 2269901 : l'interface vmk n'est pas incluse dans l'interface de ligne de commande dédiée à la capture de paquets
  Cette commande ne peut pas être émise.

  Solution : utilisez un réseau sans fil unifié pour la capture de paquets pour effectuer cette opération.

- Problème 2274988 : des chaînes de services ne prennent pas en charge les profils de service consécutifs provenant d'un même service
  Le trafic n'emprunte pas une chaîne de services et est interrompu dès lors que la chaîne comporte deux profils de service consécutifs appartenant à un même service.

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

- Problème 2275285 : un nœud formule une seconde demande pour rejoindre un même cluster avant l'aboutissement de la première demande et la stabilisation du cluster
  Le cluster peut ne pas fonctionner correctement, et les commandes de l'interface de ligne de commande « get cluster status » et « get cluster config » peuvent renvoyer une erreur.

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

- Problème 2275388 : les routes des interfaces de bouclage/connectées peuvent être redistribuées avant l'ajout de filtres destinés à refuser les routes
  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 2275985 : les cartes réseau virtuelles non connectées au commutateur logique sont répertoriées sous la forme d'options pour la sélection des membres directs du NSGroup
  Une carte réseau virtuelle qui n'est pas connectée à un commutateur logique est ajoutée en tant que membre direct du NSGroup. L'opération réussit mais les stratégies appliquées sur ce groupe n'entrent pas en vigueur sur la carte réseau virtuelle.

Solution : aucune.

Vérifiez si une carte réseau virtuelle est connectée à un commutateur logique avant de l'ajouter comme membre direct d'un NSGroup.

- **Problème 2277742 : l'appel de PUT https://<IP_MGR>/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 plutôt qu'un nom d'hôte seulement**
  PUT https://<IP_MGR>/api/v1/configs/management ne peut pas être appelée si un nom de domaine complet est configuré.

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

- **Problème 2279249 : la machine virtuelle Instant Clone perd brièvement la protection antivirus lors de son déplacement avec vMotion**
  La machine virtuelle Instant Clone a migré d'un hôte vers un autre. Immédiatement après la migration, le fichier eicar est oublié sur la machine virtuelle. Brève perte de la protection antivirus.

  Solution : aucune.

- **Problème 2290669 : le nombre de serveurs virtuels augmentant, le temps de configuration pour chacun d'eux augmente**
  Le nombre de serveurs virtuels augmentant, le temps de configuration pour chacun d'eux augmente en raison du grand nombre de validations nécessaires. Pour les 100 premiers serveurs virtuels, le temps de réponse moyen est environ d'1 seconde. Après 250 serveurs virtuels, le temps de réponse moyen passe de 5 à 10 secondes. Après 450 serveurs virtuels, le temps de réponse atteint 30 secondes environ.

  Solution : aucune. Vous pourrez configurer des serveurs virtuels sous la forme de plusieurs LbServices en fonction de la topologie. Si vous ne le faites pas, attendez-vous à un ralentissement des temps de réponse lors des configurations à grande échelle avec des serveurs virtuels.

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

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

- **Problème 2294821 : les informations concernant le dispositif NSX s'affichent dans le tableau de bord de surveillance des clusters avec l'erreur « échec de la suppression du nœud », sans aucune instruction pour gérer la situation**
  Ce problème est constaté lorsque l'utilisateur tente de supprimer le nœud autodéployé via l'interface et que la mise hors tension du nœud échoue. Si le cluster perd un nœud, vous devez manuellement ajouter un nouveau nœud et nettoyer les états de configuration à l'aide de la solution ci-dessous.

  Solution : une fois que la suppression du dispositif via l'API/interface utilisateur a échoué, supprimez ce dispositif manuellement à l'aide de l'API Forcer la suppression, comme suit :
  `POST api/v1/cluster/nodes/deployments/467a102d-472f-4f43-a93c-08b992b9f471?action=delete&force_delete=true`
  Détruisez ensuite la machine virtuelle dans vCenter.

- **Problème 2281095 : lorsque l'hôte sur lequel la SVM est déployée est ajouté à nouveau au même cluster, aucun rappel n'est déclenché dans EAM**

Toutes les VM invitées peuvent ne pas être protégées. L'interface utilisateur de NSX reste dans l'état En cours.

Solution : supprimez la SVM de l'hôte et ajoutez-la ensuite au cluster.

- 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 2261818 : Les routes apprises par le voisin eBGP sont annoncées 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.

Problèmes connus d'installation

- Problème 2238093 : le programme de résolution n'est pas pris en charge si les modules NSX sont supprimés de force
  Pour désinstaller NSX de l'hôte, les modules NSX sont supprimés de force. Cette opération peut les endommager. Le programme de résolution de l'installation des modules NSX peut ne pas fonctionner correctement, si, avant l'application du programme de résolution, les modules NSX sont supprimés de force. Emplacement du journal : `/var/log/proton/nsxapi.log`

  Solution : aucune.

  Ne supprimez pas les modules NSX de force. Désinstallez les composants NSX en exécutant les étapes standard décrites dans la documentation de NSX.

- Problème 2288872 : l'état d'installation indique « Nœud non prêt »
  Le nœud Edge n'est pas intégré. L'état de la configuration du nœud de transport est En attente et ne peut donc pas être ajouté à un cluster Edge. Emplacement du journal : `/var/log/proton/nsxapi.log`

  Solution : réessayez d'enregistrer le nœud Edge. Vous pouvez également mettre hors tension le nœud Edge. Au démarrage, il établira le canal MP-MPA.

- Problème 2252776 : l'application du profil du nœud de transport (TNP) sur l'un des hôtes membres du cluster échoue, même si l'erreur de validation qui s'est précédemment produite sur l'hôte est à présent résolue

Le TNP est appliqué sur le cluster. Toutefois, il ne peut pas être appliqué sur l'un des hôtes membres du cluster, l'une des validations n'ayant pas pu être transmise (par exemple, les machines virtuelles sont mises sous tension sur l'hôte). L'utilisateur résout le problème, mais la validation reste affichée sur l'interface utilisateur et le TNP n'est pas automatiquement appliqué sur cet hôte.

Solution : sortez l'hôte du cluster avant de l'y rajouter. Cette action déclenche l'activité prévoyant l'application du profil du nœud de transport sur l'hôte.

- **Problème 2284683 : impossible de supprimer le dispositif déployé automatiquement lorsqu'un gestionnaire de calcul enregistré est supprimé avant d'être rajouté**
  La suppression du dispositif a échoué. L'erreur « Échec de la mise hors tension » s'affiche et indique que le gestionnaire de calcul est introuvable.

  Solution : une fois que la suppression du dispositif via l'API/interface utilisateur a échoué, supprimez ce dispositif manuellement à l'aide de l'API Forcer la suppression, comme suit : POST api/v1/cluster/nodes/deployments/<id-nœud>?action=delete&force_delete=true. Détruisez la machine virtuelle du cluster virtuel.

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

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

- **Problème 2296888 : La configuration Nœud de transport (TN)/Profil du nœud de transport (TNP) ne peut pas avoir l'indicateur Migration uniquement PNIC défini sur true et les mappages VMK pour l'installation renseignés sur des commutateurs d'hôte**
  Lors d'une incompatibilité de configuration (indicateur Migration uniquement PNIC défini sur true et mappages VMK pour l'installation renseignés sur des commutateurs d'hôte) lors de CREATE, l'exception suivante s'affiche :

  VMK migration for host b17afc36-bbdc-491a-b944-21f73cf91585 failed with error [com.vmware.nsx.management.switching.common.exceptions.SwitchingException: TransportNode [TransportNode/b17afc36-bbdc-491a-b944-21f73cf91585] can not be updated or deleted while migrating ESX vmk interface null to [null].]. (Code d'erreur : 9418)

  Lors d'une incompatibilité de configuration pendant UPDATE, l'exception suivante s'affiche : Erreur générale (code d'erreur : 400)

  Une exception s'affiche lors de l'application de la configuration TN/TNP avec l'indicateur Migration uniquement PNIC défini sur true et un mappage de migration VMK.

  Solution : chaque configuration envoyée à l'hôte peut avoir l'indicateur Migration uniquement PNIC défini sur true ou les mappages VMK pour l'installation renseignés, mais pas les deux.

  1. Envoyez la configuration TN avec les commutateurs d'hôte qui nécessitent que la migration uniquement PNIC soit définie sur true.
  2. Mettez à jour la configuration TN en définissant tous les indicateurs Migration uniquement PNIC sur false et renseignez les mappages VMK pour l'installation comme vous le souhaitez. En d'autres termes, assurez-vous que la configuration envoyée à TN n'ait que l'indicateur Migration uniquement PNIC défini sur true ou les mappages VMK pour l'installation renseignés sur tous les commutateurs d'hôte. Deux appels de configuration distincts doivent être effectués pour toute configuration nécessitant les deux.
- **Problème 2273651 : après la suppression du nœud de transport, l'utilisateur ne parvient pas à utiliser SSH dans l'hôte.**

Observé dans les mises en œuvre de KVM. L'utilisateur supprime un nœud de transport et reçoit un message indiquant que la suppression a réussi. Toutefois, par la suite, l'utilisateur ne peut pas accéder au même hôte via SSH. Ce problème est probablement dû à la présence d'un commutateur virtuel ouvert (OVS) qui n'est pas géré par NSX-T et qui était probablement pré-installé dans le cadre du modèle KVM.

Solution : identifiez l'OVS problématique avant de supprimer le nœud de transport.

1. Exécutez `ovs-vsctl` afficher pour identifier l'OVS.
2. Migrez toutes les interfaces de VM de charge de travail depuis l'OVS vers le pont Linux.
3. Supprimez le nœud de transport comme suit :
   `DELETE api/v1/transport-nodes/<uuid>`

- **Problème 2281537 : après la migration, le nœud de transport ESXi avec plusieurs VTEP ne parvient pas à démarrer la session BFD.**
  Après la migration d'un nœud NSX-V vers NSX-T, le nœud de transport ESXi avec plusieurs VTEP ne parvient pas à démarrer la session BFD sur tous les VTEP vers les nœuds Edge.

  Solution : redémarrez le service netcpa.

Problèmes connus de NSX Manager

- **Problème 2285306 : l'état du déploiement des services Guest Introspection peut rester inconnu jusqu'à ce que la machine virtuelle de service soit mise sous tension**
  Dès lors qu'un déploiement de service a été créé et qu'il a été répertorié dans la grille de déploiement de service, l'état peut ne pas indiquer immédiatement « En cours » et rester inconnu jusqu'à l'actualisation de la grille.

  Solution : aucune. Actualisez la page après dix secondes. L'état doit se mettre à jour.

- **Problème 2292526 : message « Hôte inaccessible » indiqué lors de l'ajout d'un hôte**
  Lorsque vous ajoutez un hôte ESXi, le message « Hôte inaccessible » s'affiche, mais n'indique aucune raison. La cause probable est l'inexactitude des informations d'identification.

  Solution : passez en revue la configuration de l'hôte, saisissez à nouveau les informations d'identification et procédez une nouvelle fois à l'ajout de l'hôte.

- **Problème 2292701 : l'utilisateur ne parvient pas à mettre à jour le numéro de séquence dans une fiche de liaisons**
  L'utilisateur ne peut pas modifier la priorité ou l'ordre des profils appliqué à une entité en mettant à jour le numéro de séquence.

  Solution : supprimez la fiche de liaisons et recréez-la avec le nouveau numéro de séquence souhaité.

- **Problème 2294345 : l'exécution de la classification des découvertes d'applications sur un groupe de machines virtuelles à la fois hébergées par ESXi et KVM peut échouer**
  La fonctionnalité de découverte d'applications est uniquement prise en charge sur les hyperviseurs ESXi. Pour les groupes de machines virtuelles se trouvant sur des hôtes mixtes parmi lesquels figurent des hôtes non pris en charge, les résultats de la classification des découvertes d'applications ne sont pas garantis.

  Solution : aucune.

Problèmes connus de NSX Edge

- **Problème 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.

  Solution : utilisez une machine différente ou déployez le dispositif Edge NSX-T en tant que machine virtuelle sur un hyperviseur.

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

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

  - Ces API prennent en charge les options de filtrage basées sur les préfixes de réseau ou le type de route. Utilisez ces options pour télécharger les routes qui vous intéressent.
  - Prise en charge d'une interface de ligne de commande au cas où l'intégralité des tables RIB/FIB soit nécessaire et en l'absence de délai d'expiration.

Problèmes connus de mise en réseau logique

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

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

- **Problème 2264386 : la suppression du nœud de transport survient même si le nœud de transport fait partie du NSGroup**
  La suppression du nœud de transport est autorisée même si le nœud fait partie d'un NSGroup. La suppression doit être bloquée. Si vous rencontrez ce problème, vous devez recréer le NSGroup et rétablir les relations avec ses nœuds de transport.

  Solution : pour éviter ce problème, vérifiez manuellement si un nœud de transport est associé à un NSGroup. Dans l'interface Plan de gestion, accédez à **Mise en réseau avancée et sécurité** > **Inventaire** > **Groupes** ou à **Système** > **Nœuds** > **Nœuds de transport** > **Éléments associés** > **NSGroup**.

- **Problème 2292997 : la création de certaines interfaces de routeur logique pour une pile réseau Linux peut échouer**
  La création de certaines interfaces de routeur logique pour une pile réseau Linux peut échouer, ce qui renvoie l'erreur suivante : `errorCode="EDG0100002", Operation failed creating sub-interface: max sub-interface exceeded`. En conséquence, le trafic transmis par le routeur de service de niveau 0 (SR T0) peut être interrompu en raison de l'absence de routes.

  Solution : redémarrez le nœud Edge concerné.

- **Problème 228688 : le voisin BGP doit d'abord être supprimé lors de la suppression de la session de base de la route IPsec si BPG est configuré via l'interface de tunnel virtuelle (VTI)**
  Si BGP est configuré via la VTI et que vous supprimiez la session IPsec, l'état des deux SR est inactif, ce qui bloque le trafic. Afin de relancer le trafic, le voisin BGP configuré pour la VTI doit être supprimé. Dans ce scénario, seul le BGP configuré passe par la VTI.

  Solution : supprimez le voisin BGP avant de supprimer la session IPsec.

- **Problème 2288509 : la propriété MTU n'est pas prise en charge pour l'interface de service de niveau 0/niveau 1 (port de service central)**
  La propriété MTU n'est pas prise en charge pour l'interface de service de niveau 0/niveau 1 (port de service central).

Solution : configurez la propriété MTU à l'aide de l'API de plan de gestion, même si le port CSP est créé par le workflow de la stratégie.

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

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

- **Problème 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 2290083 : validation manquante lors de la création d'un segment basé un VLAN**
  Lorsque vous spécifiez une zone de transport VLAN avec une propriété d'ID de VLAN, le système ne parvient pas à valider et à identifier l'erreur. Par conséquent, l'intention échoue lors de la réalisation et déclenche une erreur.

  Solution : consultez les détails relatifs à l'erreur de réalisation pour obtenir des instructions permettant de corriger l'entrée.

- **Problème 2292096 : la commande de l'interface de ligne de commande « get service router config route-maps » renvoie un résultat vide**
  La commande de l'interface de ligne de commande « get service router config route-maps » renvoie un résultat vide, même lorsque des cartes de route sont configurées. Ce problème ne concerne que l'affichage.

  Solution : utilisez la commande de l'interface de ligne de commande `get service router config`, qui renvoie la configuration des cartes de route, sous la forme d'un sous-ensemble de l'intégralité du résultat.

- **Problème 2994002 : le niveau 1 ne figure pas dans la liste déroulante de la passerelle de niveau 0/1 à des fins de sélection lors de la création du redirecteur DNS**
  Lors d'un déploiement à grande échelle avec des milliers d'enregistrements, le niveau 1 n'est pas répertorié dans la liste déroulante de la passerelle de niveau 0/1 à des fins de sélection dans le cadre du workflow de création du redirecteur DNS. Par conséquent, vous devez utiliser l'API de configurer la création du redirecteur DNS.

  Solution : effectuez la configuration en utilisant l'API.

- **Problème 2298499 : le VPN échoue entre la passerelle de cloud public et l'hôte homologue si la passerelle n'est pas déployée avec une adresse IP publique.**
  Le tunnel VPN entre la passerelle de cloud public (PCG) et l'hôte homologue ne peut pas être établi si le PCG est déployé sans adresse IP publique sur la liaison montante. Cela est dû au fait que le PCG effectue par défaut SNAT sur le trafic VPN par défaut.

  Solution : lors du déploiement de la passerelle de cloud public, activez l'adresse IP publique pour l'interface de liaison montante.

- **Problème 2392093 : le trafic est abandonné en raison de la vérification RPF**
  La vérification RPF peut entraîner le rejet du trafic si ce dernier est épinglé par une liaison descendante T0 et que des routeurs de niveau 0 et de niveau 1 se trouvent sur le même nœud Edge.

  Solution : aucune.

Problèmes connus des services de sécurité

- **Problème 2288523 : le déchargement du pilote NSX Guest Introspection peut entraîner des problèmes de sécurité**
  IDFW s'appuie sur les informations relatives à l'identité de l'utilisateur, provenant du pilote NSX Guest Introspection. Le déchargement du pilote peut entraîner des problèmes de sécurité pour les utilisateurs connectés à partir du pilote Guest concerné. Ces problèmes présentent les symptômes suivants :
    - Non-application des règles de pare-feu pour les utilisateurs connectés à partir de certaines machines virtuelles invitées sur lesquelles le pilote Guest Introspection est déchargé.
    - Détails relatifs aux utilisateurs non connectés dans les composants IDFW pour les utilisateurs se connectant à partir de certaines machines virtuelles invitées sur lesquelles le pilote Guest Introspection est déchargé.
    - Les journaux du MUX n'indiquent aucune connexions à partir de ces machines virtuelles invitées, même si IDFW est activé sur l'hôte.
    - Les journaux du MUX n'indiquent aucun événement de réseau sur ces machines virtuelles invitées, même si IDFW est activé sur l'hôte.

  Par conséquent, le paramètre Refuser toutes les règles par défaut peut bloquer l'accès aux utilisateurs connectés à partir des machines virtuelles invitées sur lesquelles le pilote Guest Introspection est déchargé.

  Solution : aucune. L'administrateur informatique doit suivre les meilleures pratiques en matière de sécurité pour s'assurer qu'aucun utilisateur ne reçoit l'autorisation de décharger les pilotes Guest Introspection à l'intérieur des machines virtuelles invitées.

- **Problème 2288773 : l'ancienne API du protocole TLS est toujours disponible et provoque le remplacement des nouveaux paramètres**
  NSX-T dispose d'une nouvelle API pour la définition de versions et de suites de chiffrement pour le protocole TLS NSX, qui met à jour tous les nœuds d'un cluster NSX-T. Toutefois, l'ancienne API est toujours disponible. Elle peut être utilisée, mais les nouveaux paramètres sont remplacés par les paramètres globaux.

  Solution : utilisez la nouvelle API.

- **Problème 2291872 : le journal affiche un message d'avertissement lorsque le service TFTP est utilisé dans la règle de pare-feu**
  Le journal affiche un message d'avertissement non pertinent lorsque le service TFTP est utilisé dans la règle de pare-feu. Emplacement du journal sur le nœud ESXi : `/var/log/cfgAgent.log`.

  Solution : créez un service pour TFTP en tant que service L4PortSet et utilisez-le dans la règle de pare-feu.

- **Problème 2203863 : les règles de pare-feu d'identité ne sont pas prises en charge pour le trafic UDP et ICMP.**
  Les règles de pare-feu d'identité ne fonctionnent pas avec le test ping. La fonctionnalité actuelle est prise en charge uniquement pour le trafic TCP.

  Solution : utilisez TCP pour tester les règles de pare-feu d'identité. Ne définissez jamais ANY/UDP/ICMP dans la colonne Service lors de la configuration des règles de pare-feu d'identité

- **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 2252738 : pour les règles de nom de domaine complet, un paquet ne correspondant pas à la règle est autorisé à atteindre la destination.**

Lorsqu'une règle de nom de domaine complet spécifique est créée, le nom de domaine associé à une adresse IP est ajouté à la règle de correspondance de base de données de pare-feu et les paquets envoyés à ce nom de domaine sont autorisés à atteindre le serveur. Toutefois, si un utilisateur modifie le nom de domaine associé à cette adresse IP sur le serveur de nom de domaine, l'entrée de nom de domaine n'est pas mise à jour dans la base de données de pare-feu (sauf si d'autres règles de nom de domaine complet correspondant au nouveau nom de domaine existent). Par conséquent, les paquets sont envoyés au nouveau nom de domaine, même s'ils doivent être abandonnés par la règle de nom de domaine complet.

Solution : aucune.

- **Problème 2395334 : paquets (Windows) abandonnés de manière incorrecte en raison de l'entrée conntrack 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 2458384 : les pages d'interface de NSX-T Manager ne se chargent pas et indiquent l'erreur 403.**
  Observé dans les versions 2.4.0 et 2.4.1. Ce problème affecte les connexions administrateur et Identity Manager. Le nom de domaine complet de NSX-T Manager utilise le format *.SLD.TLD. Par exemple : *.co.uk, *.co.il, *.com.au etc.

  Solution : accédez à l'interface utilisateur de NSX-T Manager à l'aide du nom raccourci ou de l'IP au lieu du nom de domaine complet. Reportez-vous à https://kb.vmware.com/s/article/71217.

Problèmes connus de mise en réseau KVM

- **Problème 2292995 : l'état de réalisation est défini sur Erreur, même si toutes les règles configurées sont programmées en mode OVS**
  L'API donne une fausse impression négative, même lorsque les règles DFW sont programmées dans le plan de données.

  Solution : la mise à jour d'une règle DFW efface cette condition d'erreur. Par exemple, la simple activation de la journalisation de la règle contraint le module DFW KVM à effacer la condition d'erreur.

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 2297157 : les performances HTTPS d'équilibrage de charge sont affectées par le mode FIPS.**
  Les performances de l'équilibrage de charge peuvent être affectées de manière négative lorsque le mode FIPS par défaut est activé.

  Solution : pour obtenir une solution, consultez l'article 67400 de la base de connaissances NSX-T 2.4.0 Load Balance Service may observe low performance on HTTPs (Le service d'équilibreur de charge NSX-T 2.4.0 peut observer une faible performance sur HTTPs).

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

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

Problèmes connus des opérations et des services de surveillance

- **Problème 2275869 : le journal cfgAgent est actualisé dans un délai inférieur à 1 minute sur l'hôte ESXi si les balises des règles présentes sur l'hôte comportent plus de 31 caractères**
  L'actualisation fréquente du journal cfgAgent.log peut entraîner la perte d'informations utiles au débogage et au dépannage de l'hôte. Emplacement du journal sur l'hôte ESXi : `/var/log/cfgAgent.log`

  Solution : aucune.

- **Problème 2289984 : l'état de la connectivité du MUX apparaît CONNECTÉ même après l'arrêt du service nsx-context-mux sur l'hôte**
  Lorsque nsx-context-mux ou nsx-opsagent n'est pas exécuté sur l'hôte, le système (interface NSX ou API de l'instance de service) indique de manière erronée que la solution et l'état de l'agent de l'IG sont en cours d'exécution alors que l'horodatage reste inchangé. Par conséquent, les machines virtuelles invitées peuvent perdre la protection antivirus.

  Solution : essayez de démarrer manuellement le MUX et l'agent d'opération sur l'hôte s'ils ne sont pas déjà en cours d'exécution.

  1. Connectez-vous à l'hôte en tant qu'utilisateur racine et exécutez les commandes suivantes :
     ```
     /etc/init.d/nsx-opsagent start
     /etc/init.d/nsx-context-mux start
     ```
  2. Après le démarrage des agents, attendez quelques minutes et vérifiez que l'horodatage de l'état d'intégrité a été mis à jour sur l'interface utilisateur.

Problèmes connus de mise à niveau

- **Problème 2273737 : après la mise à niveau de NSX-T 2.3 vers NSX-T 2.4, les détails du serveur vIDM sont manquants**
  Si vous utilisez vIDM alors que le serveur vIDM est configuré uniquement sur le dispositif de stratégie NSX, le serveur vIDM est migré dans le cadre de la mise à niveau, mais il est absent du dispositif convergé.

  Solution : il existe deux options selon le moment auquel le client rencontre le problème :

  - Avant la mise à niveau de la version 2.3 vers la version 2.4 :
    Spécifiez les mêmes détails du serveur vIDM sur le dispositif NSX Policy et sur la machine virtuelle NSX Manager.
  - Après la mise à niveau de la version 2.3 vers la version 2.4 :
    Spécifiez les mêmes détails du serveur vIDM sur le dispositif convergé.

- **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 2279973 : si un groupe vide est créé et la mise à niveau se poursuit, après la mise à niveau du plan de gestion, ce groupe vide s'affiche comme n'ayant pas démarré**
  Cette situation survient si un groupe vide est créé et la mise à niveau se poursuit.

  Solution : ne créez pas de groupe vide.

  Effectuez l'une des étapes suivantes pour continuer :

  - Supprimez le groupe vide.
  - Cliquez sur le bouton Reprendre pour terminer la mise à niveau.
  - Réinitialisez le plan.
- **Problème 2282389 : le plan de mise à niveau UC n'est pas synchronisé avec l'appartenance au cluster virtuel si ESX est déplacé d'un cluster à un autre**
  Lorsqu'ESX est déplacé d'un cluster à un autre dans un cluster virtuel, la modification n'est pas reflétée dans le plan de mise à niveau UC. Cela peut entraîner l'activation du mode de maintenance pour plusieurs HÔTES en même temps si l'utilisateur a sélectionné « Mise à niveau parallèle » dans plusieurs groupes.

  Solution : sur la page Mise à niveau d'hôte, cliquez sur l'option « Réinitialiser » pour recréer le plan de mise à niveau UC afin qu'il soit synchronisé avec les clusters du cluster virtuel.

- **Problème 2288921 : l'état de mise à niveau est désynchronisé lors de l'ajout de nœuds Edge d'une version antérieure**
  L'état de mise à niveau est désynchronisé si l'utilisateur ajoute des nœuds Edge d'une version antérieure, suite à la mise à niveau d'Edge. La poursuite de l'appel de mise à niveau est de ce fait compromise.

  Solution : tout d'abord, évitez d'ajouter des nœuds Edge de version antérieure. Si vous rencontrez ce problème, redémarrez le service UC.

- **Problème 2291625 : l'état de mise à niveau de la PCG, RÉUSSITE, est redéfini sur NON_DÉMARRÉ après la synchronisation du plan de mise à niveau**
  Ce problème se produit uniquement si l'utilisateur met à niveau la PCG, puis tente par la suite de mettre à niveau plus d'agents/de PCG.
  Dans le workflow recommandé, après la mise à niveau de la PCG, il n'y a, dans le cloud, plus de composants à mettre à niveau via l'interface UC.

  Cela n'a aucune incidence sur les fonctionnalités. L'état de la mise à niveau de la PCG précédemment terminée avec succès indique « Aucun » dans l'interface utilisateur de la mise à niveau.

Solution : aucune. La fonctionnalité ne doit pas en être affectée.

- **Problème 2293227 : après la mise à niveau vers 2.4, les règles IDFW ne sont pas appliquées aux machines virtuelles exécutant VMTools 10.3.5**
  Après une mise à niveau de NSX-T en direct, les règles IDFW ne sont pas appliquées aux machines virtuelles exécutant VMTools 10.3.5, ce qui entraîne une perte possible de la protection antivirus de ces machines virtuelles.

  Solution : redémarrez les machines virtuelles concernées.

- **Problème 2295564 : la connectivité au contrôleur du nœud Edge peut devenir indisponible après la mise à niveau de la version 2.3 vers la version 2.4**
  Il s'agit d'un problème intermittent qui peut affecter certains types de trafic nord-sud.

  Solution : activez, puis désactivez le mode de maintenance sur le même nœud Edge.

- **Problème 2294178 : la mise à jour de VIB de l'hôte échoue lors de la mise à niveau de la version 2.3.1 vers la version 2.4.**
  Le processus de mise à niveau de la version 2.3.1 vers la version 2.4 peut échouer avec l'erreur Échec de l'installation du bundle hors ligne sur l'hôte. Plus spécifiquement, la mise à jour de VIB de l'hôte échoue en raison de l'échec du déchargement du module de sécurité du commutateur. Ce problème est connu pour se produire si la fonctionnalité de découverte d'adresses IP est activée dans le profil de commutation et lors de l'exécution d'une mise à niveau sur place de NSX-T 2.3.1 vers NSX-T 2.4 avec un hôte exécutant ESXi-6.7 EP06 (build 11675023).

  Solution : pour obtenir une solution, consultez l'article 67445 de la base de connaissances With IP Discovery enabled, host VIB update may fail when upgrading from NSX-T 2.3.1 to NSX-T 2.4 (Avec la découverte d'adresses IP activée, la mise à jour de VIB de l'hôte peut échouer lors de la mise à niveau de NSX-T 2.3.1 vers NSX-T 2.4).

- **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 2297918 : après la mise à niveau de la version 2.3.1 vers la version 2.4, il n'est pas possible de supprimer NSX du cluster.**
  Après la mise à niveau d'un cluster de la version 2.3.1 vers la version 2.4, NSX-T ne peut pas être supprimé et échoue avec le message suivant : « Impossible de supprimer NSX sur le cluster : un modèle de nœud de transport ou une collection de nœuds de transport connexe existe pour ce modèle d'infrastructure. Le modèle de nœud de transport ou la collection de nœuds de transport doit être supprimé avant d'effectuer une suppression/désactivation sur ce modèle d'infrastructure. »

Solution : détachez le profil de nœud de transport du cluster affecté, puis utilisez le workflow « Supprimer NSX ».

- **Problème 2286030 : la configuration du nœud de transport s'affiche comme en état d'échec lors de la mise à niveau de NSX-T 2.3.x et versions antérieures vers la version 2.4.x.**
  La configuration du nœud de transport passe à l'état d'échec lors de la mise à niveau de NSX-T 2.3.x et versions antérieures vers la version 2.4.x en raison d'une exception de pointeur Null. Lorsque vous avez un nœud de transport ESXi avec des adaptateurs vmkernel migrés vers un commutateur logique VLAN N-VDS, puis que vous effectuez une mise à niveau de NSX-T 2.3.x vers NSX-T 2.4.x, une condition de concurrence peut entraîner l'affichage de l'état de la configuration du nœud de transport ESXi comme ayant échoué. Toutefois, la connectivité du nœud de transport ESXi avec NSX Manager et les contrôleurs est intacte pendant la mise à niveau, même après l'échec du marquage du nœud pour l'état de configuration.

  Solution : mettez à jour ou renvoyez le nœud de transport pour réinitialiser l'état de configuration sur réussi.

  1. Dans NSX Manager, modifiez le nœud de transport ESXi qui s'affiche comme ayant échoué.
  2. Dans la fenêtre contextuelle de configuration du nœud de transport ESXi, cliquez sur **Enregistrer**.
     Cette action réinitialise l'état. Vous n'avez pas besoin de modifier la configuration.

Problèmes connus de l'API

Problèmes connus de NSX Policy Manager

- **Problème 2291267 : aucun numéro de séquence n'a été attribué à la section de la stratégie de passerelle par défaut créée par le PCM. Par conséquent, la stratégie la définit par défaut sur 0**
  Si un utilisateur crée des stratégies de passerelle sans options insert_top ni numéros de séquence, un conflit de stratégies survient. Emplacement du journal : `/var/log/policy/policy.log`

  Solution : évitez ce problème en créant toujours les stratégies avec les numéros de séquence appropriés ou à l'aide des paramètres d'URL `action=revise&operation=insert_top`.

- **Problème 2289278 : l'API dédiée aux stratégies génère une erreur, mais permet de configurer plusieurs serveurs virtuels avec le même pool et un profil de persistance différent**
  Le système ne prend pas en charge la configuration des types de persistance en conflit pour un même pool mais différents serveurs virtuels d'équilibreur de charge. Toutefois, la stratégie ne parvient pas à valider/rejeter correctement l'entrée en conflit et autorise la configuration. Par la suite, la stratégie déclenche une alarme avec message d'erreur.

  Solution : si vous rencontrez ce problème, vous pouvez le corriger en modifiant le paramètre de groupe sur le serveur virtuel d'équilibreur de charge.

- **Problème 2248186 : le routeur BGP installe des routes IPV6 depuis son voisin avec sa propre interface comme tronçon suivant.**
  Par conséquent, le transfert IPV6 de la route installée peut échouer et provoquer une boucle de transfert.

  Solution : pour éviter ce problème, configurez une carte de route pour filtrer les adresses connectées IPv6 en tant que tronçon suivant dans les mises à jour de BGP.

Problèmes connus de NSX Cloud

- **Problème 2287884 : certaines images du Marketplace CentOS ne sont pas prises en charge pour NSX Cloud**
  Seules les images du Marketplace CentOS dont les versions de distribution correspondent à la version mineure attendue pour leur noyau sont prises en charge pour NSX Cloud.
  Par exemple, les versions de distribution et la version correspondante de leur noyau sont supposées être les suivantes :

- RHEL 7.5 3.10.0-862
- RHEL 7.4 3.10.0-693
- RHEL 7.3 3.10.0-514

Solution : utilisez uniquement les distributions CentOS recommandées dans la documentation.

- **Problème 2275232 : DHCP ne fonctionne pas pour les machines virtuelles du cloud si la stratégie de connectivité du DFW, sur liste noire, est mise en liste verte**
  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 machine virtuelle 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 2280663 : le débarquement de plusieurs VPC en parallèle peut, dans de rares cas, entraîner des erreurs**
  Le débarquement de l'un des VPC de calcul échoue.

  Solution : nettoyez manuellement le VPC et les groupes correspondants présents sur la stratégie.

- **Problème résolu 2287124 : Après le déploiement de PCG sur un VNet Microsoft Azure, la vignette du VNet dans CSM signale par erreur un avertissement**
  Après le déploiement de PCG sur un VNet Microsoft Azure, dans CSM, le VNet signale un symbole d'avertissement (triangle jaune avec un point d'exclamation). Si vous passez le curseur sur l'icône d'avertissement, CSM signale que l'état de MP (plan de gestion) et de CCP (plan de contrôle) est Inconnu. Toutefois, il se peut qu'il n'y ait pas de problème de connectivité et que l'avertissement s'affiche par erreur.

- **Problème 2290688 : la mise à niveau de VM Windows 2016 dans AWS échoue.**
  La mise à niveau de plusieurs VM de charge de travail Windows échoue dans AWS. L'état de mise à niveau de VM s'affiche dans le portail AWS comme bloqué dans « Vérification 1/2 ». Une nouvelle tentative échoue également. Ce problème se produit uniquement dans les mises à niveau de même version de NSX-T.

  Solution : pour résoudre ce problème, effectuez les étapes suivantes :

  1. Assurez-vous que PCG est mis à niveau sur les hôtes affectés afin que la VM puisse télécharger les derniers composants de l'hôte.
  2. Redémarrez la VM pour obtenir un bon état.
  3. Exécutez manuellement uninstall cmd.
  4. Exécutez manuellement install cmd.