Notes de mise à jour de VMware NSX for vSphere 6.3.4

VMware NSX for vSphere 6.3.4 | Publié le 12 octobre 2017 | Build 7087695

Consultez l'Historique de révision de ce document.

Contenu des notes de mise à jour

Les notes de mise à jour couvrent les sujets suivants :

Nouveautés de NSX 6.3.4

Informations importantes concernant NSX 6.3.4 : NSX for vSphere 6.3.4 a été reconditionné afin de résoudre les problèmes mentionnés dans les articles 2151719 et 000051144 de la base de connaissances de VMware. Le build 6845891 publié au départ est remplacé par le build 7087695. Consultez les articles de la base de connaissances pour plus de détails. Pour plus d'informations sur la mise à niveau, reportez-vous à la section Notes de mise à niveau.

NSX for vSphere 6.3.4 résout un certain nombre de bogues clients. Pour plus d'informations, voir Problèmes résolus.

Afficher les notes de mise à jour pour les versions précédentes :

- NSX 6.3.3
- NSX 6.3.2
- NSX 6.3.1
- NSX 6.3.0

Versions, configuration système et installation

Remarque :

- Le tableau ci-dessous répertorie les versions recommandées du logiciel VMware. Ces recommandations sont générales et ne doivent pas remplacer des recommandations spécifiques de l'environnement.
- Ces informations sont à jour à la date de publication de ce document.

- Pour voir les versions **minimales prises en charge** de NSX et d'autres produits VMware, consultez la matrice d'interopérabilité des produits VMware. VMware déclare des versions minimales prises en charge en fonction de tests internes.
    - La version minimale prise en charge requise de l'interopérabilité vSphere for NSX passe de NSX 6.3.2 à NSX 6.3.3. Reportez-vous à la Matrice d'interopérabilité des produits VMware pour plus de détails.

Produit ou composant	Version recommandée
NSX for vSphere	VMware recommande la dernière version de NSX 6.3 pour les nouveaux déploiements et la mise à niveau de 6.1.x. Lors de la mise à niveau de déploiements existants, consultez les notes de mise à jour de NSX ou contactez votre représentant du support technique VMware pour plus d'informations sur les problèmes spécifiques avant de planifier une mise à niveau.
vSphere	• vSphere 5.5U3 et versions ultérieures • vSphere 6.0U3 et versions ultérieures. vSphere 6.0U3 résout le problème des VTEP en double dans les hôtes ESXi après le redémarrage du serveur vCenter Server. Consultez l'*article 2144605 de la base de connaissances de VMware* pour plus d'informations. • vSphere 6.5U1 et versions ultérieures. vSphere 6.5U1 résout le problème d'échec d'EAM avec une erreur OutOfMemory. Consultez l'*article 2135378 de la base de connaissances de VMware* pour plus d'informations.
Guest Introspection pour Windows	Toutes les versions de VMware Tools sont prises en charge. Certaines fonctionnalités de Guest Introspection requièrent des versions VMware Tools plus récentes : • Utilisez VMware Tools 10.0.9 et 10.0.12 pour activer le composant Thin Agent Network Introspection facultatif fourni avec VMware Tools. • Effectuez la mise à niveau vers VMware Tools 10.0.8 et versions ultérieures pour résoudre la lenteur des VM après la mise à niveau de VMware Tools dans NSX/vCloud Networking and Security (consultez l'*article 2144236 de la base de connaissances de VMware)*. • Utilisez VMware Tools 10.1.0 et versions ultérieures pour la prise en charge de Windows 10. • Utilisez VMware Tools 10.1.10 et versions ultérieures pour la prise en charge de Windows Server 2016.

Guest Introspection pour Linux	Cette version de NSX prend en charge les versions suivantes de Linux : • RHEL 7 GA (64 bits) • SLES 12 GA (64 bits) • Ubuntu 14.04 LTS (64 bits)

Remarque : VMware ne prend actuellement pas en charge NSX for vSphere 6.3.x avec vRealize Networking Insight 3.2.

Configuration système et installation

Pour obtenir la liste complète des prérequis à l'installation de NSX, consultez la section Configuration système pour NSX dans le *Guide d'installation de NSX*.

Pour obtenir des instructions d'installation, consultez le *Guide d'installation de NSX* ou le *Guide d'installation de Cross-vCenter NSX*.

Fonctionnalités obsolètes et retirées

Avertissements sur la fin de vie et la fin du support

Pour plus d'informations sur NSX et d'autres produits VMware devant être mis à niveau rapidement, consultez la *Matrice du cycle de vie des produits VMware*.

- **NSX for vSphere 6.1.x** est arrivé en fin de disponibilité et a atteint sa date de fin de support général le 15 janvier 2017. (Consultez également l'*article 2144769 de la base de connaissances de VMware*.)
- **Suppression de NSX Data Security** : à partir de NSX 6.3.0, la fonctionnalité NSX Data Security est supprimée du produit.
- **NSX Activity Monitoring (SAM) abandonné** : À partir de NSX 6.3.0, Activity Monitoring n'est plus une fonctionnalité prise en charge de NSX. En remplacement, utilisez la Surveillance de point de terminaison. Pour plus d'informations, consultez Surveillance de point de terminaison dans le *Guide d'administration de NSX*.
- **Web Access Terminal supprimé** : Web Access Terminal (WAT) a été supprimé de NSX 6.3.0. vous ne pouvez pas configurer Web Access SSL VPN-Plus et activer l'accès URL public via NSX Edge. VMware recommande d'utiliser le client d'accès complet avec des déploiements VPN SSL pour une sécurité améliorée. Si vous utilisez la fonctionnalité WAT dans une version antérieure, vous devez la désactiver avant d'effectuer la mise à niveau vers la version 6.3.0.
- **IS-IS supprimé de NSX Edge** : à partir de NSX 6.3.0, vous ne pouvez pas configurer le protocole IS-IS à partir de l'onglet **Routage**.
- **Arrêt de la prise en charge des dispositifs vCNS Edge**. Vous devez effectuer une mise à niveau vers un dispositif NSX Edge avant de procéder à la mise à niveau vers NSX 6.3.x.

Suppressions d'API et modifications de comportement

Suppression de la section par défaut ou de configuration du pare-feu :

- La demande de suppression d'une section de pare-feu est maintenant refusée si la section par défaut est spécifiée : `DELETE /api/4.0/firewall/globalroot-0/config/layer2sections|layer3sections/sectionId`
- Nouvelle méthode introduite pour obtenir la configuration par défaut. Utilisez le résultat de cette méthode pour remplacer toute la configuration ou l'une des sections par défaut :

- Obtenez la configuration par défaut avec `GET /api/4.0/firewall/globalroot-0/defaultconfig`
- Mettez à jour toute la configuration avec `PUT /api/4.0/firewall/globalroot-0/config`
- Mettez à jour une section avec `PUT /4.0/firewall/globalroot-0/config/layer2sections|layer3sections/{sectionId}`

Paramètre `defaultOriginate` supprimé des méthodes suivantes pour des dispositifs NSX Edge de routeur logique (distribué) uniquement :

- `GET/PUT /api/4.0/edges/{edge-id}/routing/config/ospf`
- `GET/PUT /api/4.0/edges/{edge-id}/routing/config/bgp`
- `GET/PUT /api/4.0/edges/{edge-id}/routing/config`

La définition de `defaultOriginate` sur true sur un dispositif Edge de routeur logique (distribué) NSX 6.3.0 ou version ultérieure échoue.

Toutes les méthodes IS-IS ont été supprimées du routage NSX Edge.

- `GET/PUT/DELETE /4.0/edges/{edge-id}/routing/config/isis`
- `GET/PUT /4.0/edges/{edge-id}/routing/config`

Suppressions de CLI et modifications de comportement

N'utilisez pas les commandes non prises en charge sur les nœuds NSX Controller
Il existe des commandes non documentées pour configurer DNS et NTP sur les nœuds NSX Controller. Ces commandes ne sont pas prises en charge et ne doivent pas être utilisées sur les nœuds NSX Controller. Vous ne devez utiliser que les commandes qui sont documentées dans ce Guide de la CLI de NSX.

Notes relatives aux mises à niveau

Remarque : Pour obtenir la liste des problèmes connus affectant l'installation et les mises à niveau, consultez la section Problèmes connus de mise à niveau et d'installation.

Remarques générales sur la mise à niveau

- **Mise à niveau de NSX 6.3.4 build 6845891 vers NSX 6.3.4 build 7087695 :** cette mise à niveau nécessite uniquement une mise à niveau du cluster NSX Manager et NSX Controller. Il est inutile de mettre à niveau les hôtes, les dispositifs NSX Edge et Guest Introspection.
- **Mise à niveau complète de NSX :** Pour mettre NSX à niveau, vous devez réaliser une mise à niveau complète de NSX, y compris la mise à niveau du cluster d'hôte (les VIB de l'hôte sont alors mis à niveau). Pour obtenir des instructions, consultez le *Guide de mise à niveau de NSX*, y compris la section Mettre à niveau des clusters d'hôte.
- **Configuration système requise :** pour plus d'informations sur la configuration système requise lors de l'installation et de la mise à niveau de NSX, consultez la section Configuration système requise pour NSX dans la documentation de NSX.
- **Chemin de mise à niveau à partir de NSX 6.x :** La matrice d'interopérabilité des produits VMware fournit des détails sur les chemins de mise à niveau à partir de VMware NSX. La mise à niveau de cross-vCenter NSX est abordée dans le Guide de mise à niveau de NSX.

- **Les rétrogradations ne sont pas prises en charge :**
  - Capturez toujours une sauvegarde de NSX Manager avant de procéder à une mise à niveau.
  - Lorsque NSX a été mis à niveau correctement, NSX ne peut pas être rétrogradé.
- **Pour vérifier** que la mise à niveau vers NSX 6.3.x est réussie, consultez l'article 2134525 de la base de connaissances.
- Il n'existe pas de support pour les mises à niveau depuis vCloud Networking and Security vers NSX 6.3.x. Vous devez d'abord effectuer une mise à niveau vers une version 6.2.x prise en charge.
- **Interopérabilité** : consultez la Matrice d'interopérabilité des produits VMware pour tous les produits VMware pertinents avant d'effectuer la mise à niveau.
  - **Mise à niveau vers vSphere 6.5a ou version ultérieure** : lors de la mise à niveau de vSphere 5.5 ou 6.0 vers vSphere 6.5a ou version ultérieure, vous devez d'abord effectuer la mise à niveau vers NSX 6.3.x. Consultez Mise à niveau de vSphere dans un environnement NSX dans le *Guide de mise à niveau de NSX*.
    Remarque : NSX 6.2.x n'est pas compatible avec vSphere 6.5.
  - **Mise à niveau vers NSX 6.3.3 ou version ultérieure** : la version minimale prise en charge de l'interopérabilité vSphere for NSX passe de NSX 6.3.2 à NSX 6.3.3. Reportez-vous à la Matrice d'interopérabilité des produits VMware pour plus de détails.
- **Compatibilité des services de partenaires** : si votre site utilise des services de partenaires VMware pour Guest Introspection ou Network Introspection, vous devez examiner le Guide de compatibilité VMware avant la mise à niveau, afin de vérifier que le service de votre fournisseur est compatible avec cette version de NSX.
- **Plug-in Networking and Security** : Après la mise à niveau de NSX Manager, vous devez vous déconnecter et vous reconnecter à vSphere Web Client. Si le plug-in NSX ne s'affiche pas correctement, videz le cache du navigateur et effacez l'historique. Si le plug-in Networking and Security ne figure pas dans vSphere Web Client, réinitialisez le serveur vSphere Web Client, comme expliqué dans le *Guide de mise à niveau de NSX*.
- **Environnements sans état** : pour les mises à niveau de NSX dans un environnement d'hôtes sans état, les nouveaux VIB sont pré-ajoutés au profil d'image d'hôte lors du processus de mise à niveau de NSX. Par conséquent, le processus de mise à niveau de NSX sur des hôtes sans état s'effectue selon les étapes suivantes :
  Dans les versions antérieures à NSX 6.2.0, une seule URL de NSX Manager permettait de trouver les VIB pour une version spécifique de l'hôte ESX. (L'administrateur n'avait alors qu'à connaître une seule URL, quelle que soit la version de NSX.) Dans NSX 6.2.0 et versions ultérieures, les nouveaux VIB NSX sont disponibles sur plusieurs URL. Pour trouver les VIB adéquats, vous devez procéder comme suit :

  1. Recherchez la nouvelle URL du VIB sur `https://<NSXManager>/bin/vdn/nwfabric.properties`.
  2. Récupérez les VIB pour la version de l'hôte ESX requise à partir de l'URL correspondante.
  3. Ajoutez-les au profil d'image d'hôte.

Notes de mise à niveau pour les composants NSX

Mise à niveau de NSX Manager

- Si vous utilisez SFTP lors des sauvegardes NSX, choisissez `sha2-hmac-256` après la mise à niveau vers la version 6.3.x, car il n'y a aucune prise en charge pour `hmac-sha1`. Consultez l'*article 2149282 de la base de connaissances de VMware* pour obtenir la liste des algorithmes de sécurité pris en charge dans la version 6.3.x.
- Si vous souhaitez mettre à niveau NSX 6.3.3 vers NSX 6.3.4, vous devez d'abord suivre les instructions de solution de l'*article 2151719 de la base de connaissances de VMware*.

Mise à niveau du contrôleur

- Dans NSX 6.3.3, la taille de disque du dispositif NSX Controller passe de 20 Go à 28 Go.

- Le cluster NSX Controller doit contenir trois nœuds de contrôleur pour effectuer la mise à niveau vers NSX 6.3.3. S'il dispose de moins de trois contrôleurs, vous devez ajouter des contrôleurs avant de commencer la mise à niveau. Pour obtenir des instructions, reportez-vous à Déployer le cluster NSX Controller.
- Dans NSX 6.3.3, le système d'exploitation sous-jacent de NSX Controller change. Cela signifie que lorsque vous effectuez une mise à niveau de NSX 6.3.2 ou version antérieure vers NSX 6.3.3 ou version ultérieure, au lieu d'une mise à niveau logicielle sur place, les contrôleurs existants sont supprimés un à un et les nouveaux contrôleurs basés sur Photon OS sont déployés en utilisant les mêmes adresses IP. Voir Mettre à niveau le cluster NSX Controller.

Mise à niveau du cluster d'hôte

- Dans NSX 6.3.3, les noms des VIB NSX changent. Les VIB esx-vxlan et esx-vsip sont remplacés par esx-nsxv si vous avez installé NSX 6.3.3 ou version ultérieure.

- **Mise à niveau et désinstallation sans redémarrage sur les hôtes** : dans vSphere 6.0 et versions ultérieures, une fois que vous avez effectué la mise à niveau vers NSX 6.3.x, toutes les modifications suivantes apportées à des VIB NSX ne requièrent pas de redémarrage. Au lieu de cela, les hôtes doivent entrer en mode de maintenance pour terminer la modification de VIB.

  Un redémarrage des hôtes **n'est pas nécessaire** durant les tâches suivantes :

  - Les mises à niveau de NSX 6.3.0 vers NSX 6.3.x sur ESXi 6.0 ou une version ultérieure.
  - L'installation de VIB NSX 6.3.x qui est nécessaire après une mise à niveau d'ESXi 6.0 vers la version 6.5.0a ou une version ultérieure.
    Remarque : La mise à niveau d'ESXi nécessite toujours un redémarrage de l'hôte.

  - La désinstallation de VIB NSX 6.3.x sur ESXi 6.0 ou une version ultérieure.

  Un redémarrage des hôtes **est nécessaire** pendant les tâches suivantes :

  - Les mises à niveau de NSX 6.2.x ou version antérieure vers NSX 6.3.x (sur toutes les versions d'ESXi).
  - Les mises à niveau de NSX 6.3.0 vers NSX 6.3.x sur ESXi 5.5.
  - L'installation de VIB NSX 6.3.x qui est nécessaire après une mise à niveau d'ESXi 5.5 vers la version 6.0 ou une version ultérieure.
  - La désinstallation de VIB NSX 6.3.x sur ESXi 5.5.
- **L'hôte peut être bloqué dans l'état d'installation** : Lors de mises à niveau importantes de NSX, un hôte peut être bloqué dans l'état d'installation pendant un long moment. Cela se produit à cause de problèmes lors de la désinstallation d'anciens VIB NSX. Dans ce cas, le thread EAM associé à cet hôte sera signalé dans la liste de tâches de VI Client comme étant bloqué.
  Solution : procédez comme suit :

  - connectez-vous à vCenter à l'aide de VI Client.
  - Cliquez avec le bouton droit de la souris sur la tâche EAM bloquée et annulez-la.
  - Dans vSphere Web Client, effectuez une résolution sur le cluster. L'hôte bloqué peut maintenant indiquer qu'il a l'état InProgress.
  - Connectez-vous à l'hôte et effectuez un redémarrage pour forcer l'exécution de la mise à niveau sur cet hôte.

Mise à niveau de NSX Edge

- Dans NSX 6.3.0, les tailles de disque des dispositifs NSX Edge ont changé :

  - **Compacte, Grande, Super grande** : 1 disque de 584 Mo + 1 disque de 512 Mo

  - **Extra grande** : 1 disque de 584 Mo + 1 disque de 2 Go + 1 disque de 256 Mo

- **Les clusters d'hôtes doivent être préparés pour NSX avant la mise à niveau des dispositifs NSX Edge** : La communication au niveau du plan de gestion entre les dispositifs NSX Manager et Edge via le canal VIX n'est plus prise en charge à partir de la version 6.3.0. Seul le canal de bus de messages est pris en charge. Lorsque vous effectuez une mise à niveau à partir de NSX 6.2.x ou version antérieure vers NSX 6.3.0 ou version ultérieure, vous devez vérifier que les clusters d'hôtes où sont déployés les dispositifs NSX Edge sont préparés pour NSX, et que l'état de l'infrastructure de messagerie s'affiche en VERT. Si les clusters d'hôtes ne sont pas préparés pour NSX, la mise à niveau du dispositif NSX Edge échouera. Reportez-vous à Mise à niveau de NSX Edge dans le *Guide de mise à niveau de NSX* pour plus de détails.

- **Mise à niveau d'Edge Services Gateway (ESG) :**
  À partir de NSX 6.2.5, la réservation de ressources est réalisée au moment de la mise à niveau de NSX Edge. Lorsque vSphere HA est activé sur un cluster disposant de ressources insuffisantes, l'opération de mise à niveau peut échouer en raison de contraintes vSphere HA non respectées. Pour éviter de tels échecs de mise à niveau, procédez comme suit avant de mettre une passerelle ESG à niveau :

  Les réservations de ressources suivantes sont utilisées par NSX Manager si vous n'avez pas explicitement défini des valeurs lors de l'installation ou de la mise à niveau.

NSX Edge Facteur de forme	Réservation de CPU	Réservation de mémoire
COMPACTE	1 000 MHz	512 Mo
GRANDE	2 000 MHz	1 024 Mo
SUPER GRANDE	4 000 MHz	2 048 Mo
EXTRA GRANDE	6 000 MHz	8 192 Mo

  1. Veillez toujours à ce que votre installation suive les meilleures pratiques établies pour vSphere HA. Consultez l'article 1002080 de la base de connaissances.

  2. Utilisez l'API de configuration de réglage NSX :
     `PUT https://<NSXManager>/api/4.0/edgePublish/tuningConfiguration`
     en veillant à ce que les valeurs de `edgeVCpuReservationPercentage` et `edgeMemoryReservationPercentage` respectent les ressources disponibles pour le facteur de forme (voir les valeurs par défaut dans le tableau ci-dessus).

- **Désactiver l'option de démarrage de machine virtuelle de vSphere lorsque vSphere HA est activé et que des dispositifs Edge sont déployés.** Après avoir mis à niveau vos dispositifs NSX Edge de la version 6.2.4 ou antérieure vers la version 6.2.5 ou ultérieure, vous devez désactiver l'option de démarrage de machine virtuelle de vSphere pour chaque dispositif NSX Edge dans un cluster dans lequel vSphere HA est activé et des dispositifs Edge sont déployés. Pour cela, ouvrez vSphere Web Client, recherchez l'hôte ESXi sur lequel réside la machine virtuelle NSX Edge, cliquez sur Gérer > Paramètres et, sous Machines virtuelles, sélectionnez Démarrage/Arrêt de la VM, cliquez sur Modifier et vérifiez que la machine virtuelle est en mode Manuel (c'est-à-dire qu'elle n'est pas ajoutée à la liste Démarrage/Arrêt automatique).

- **Avant de procéder à la mise à niveau vers NSX 6.2.5 ou version ultérieure, vérifiez que toutes les listes de chiffrement d'équilibrage de charge sont séparées par un signe deux-points.** Si votre liste de chiffrement utilise un autre séparateur (par exemple, des virgules), effectuez un appel PUT à `https://nsxmgr_ip/api/4.0/edges/EdgeID/loadbalancer/config/applicationprofiles` et remplacez chaque liste *<ciphers>* dans *<clientSsl>* et *<serverSsl>* par une liste séparée par des deux-points. Par exemple, le segment pertinent du corps de demande peut ressembler à ce qui suit. Répétez cette procédure pour tous les profils d'application :

```
<applicationProfile>
  <name>https-profile</name>
  <insertXForwardedFor>false</insertXForwardedFor>
  <sslPassthrough>false</sslPassthrough>
  <template>HTTPS</template>
  <serverSslEnabled>true</serverSslEnabled>
  <clientSsl>
    <ciphers>AES128-SHA:AES256-SHA:ECDHE-ECDSA-AES256-SHA</ciphers>
    <clientAuth>ignore</clientAuth>
    <serviceCertificate>certificate-4</serviceCertificate>
  </clientSsl>
  <serverSsl>
    <ciphers>AES128-SHA:AES256-SHA:ECDHE-ECDSA-AES256-SHA</ciphers>
    <serviceCertificate>certificate-4</serviceCertificate>
  </serverSsl>
  ...
</applicationProfile>
```

- **Définir la version de chiffrement correcte pour les clients d'équilibrage de charge sur des versions de vROPs antérieures à la version 6.2.0** : les membres de pool vROPs sur des versions de vROPs antérieures à la version 6.2.0 utilisent TLS version 1.0 et, par conséquent, vous devez définir explicitement une valeur d'extension de moniteur en définissant `"ssl-version=10"` dans la configuration de l'équilibrage de charge NSX. Consultez Créer un contrôle de service dans le *Guide d'administration de NSX* pour plus d'informations.

```
{
                "expected" : null,
                "extension" : "ssl-version=10",
                "send" : null,
                "maxRetries" : 2,
            "name" : "sm_vrops",
            "url" : "/suite-api/api/deployment/node/status",
            "timeout" : 5,
            "type" : "https",
            "receive" : null,
            "interval" : 60,
            "method" : "GET"
        }
```

Notes de mise à niveau pour FIPS

Lorsque vous effectuez la mise à niveau depuis une version de NSX antérieure à NSX 6.3.0 vers NSX 6.3.0 ou version ultérieure, vous ne devez pas activer le mode FIPS avant la fin de la mise à niveau. L'activation du mode FIPS avant la fin de la mise à niveau interrompra la communication entre les composants mis à niveau et les composants non mis à niveau. Consultez Comprendre le mode FIPS et la mise à niveau de NSX dans le *Guide de mise à niveau de NSX* pour plus d'informations.

- Chiffrements pris en charge sous OS X Yosemite et OS X El Capitan : Si vous utilisez le client VPN SSL sous OS X 10.11 (El Capitan), vous pourrez vous connecter à l'aide des chiffrements `AES128-GCM-SHA256`, `ECDHE-RSA-AES128-GCM-SHA256`, `ECDHE-RSA-AES256-GCM-SHA38`, `AES256-SHA` et `AES128-SHA` et, si vous utilisez OS X 10.10 (Yosemite), vous pourrez vous connecter à l'aide des chiffrements `AES256-SHA` et `AES128-SHA` uniquement.
- N'activez pas FIPS avant la fin de la mise à niveau vers NSX 6.3.x. Consultez Comprendre le mode FIPS et la mise à niveau de NSX dans le *Guide de mise à niveau de NSX* pour plus d'informations.
- Avant d'activer FIPS, vérifiez que les solutions de partenaire sont certifiées pour le mode FIPS. Consultez le Guide de compatibilité VMware et la documentation de partenaire correspondante.

Conformité FIPS

- **NSS et OpenSwan** : le VPN IPsec NSX Edge utilise le module de chiffrement Mozilla NSS. En raison de problèmes de sécurité critiques, cette version de NSX utilise une version plus récente de NSS non validée pour FIPS 140-2. VMware confirme que le module fonctionne correctement, mais qu'il est n'est plus formellement validé.
- **NSS et la saisie de mots de passe** : le hachage de mot de passe NSX Edge utilise le module de chiffrement NSS Mozilla. En raison de problèmes de sécurité critiques, cette version de NSX utilise une version plus récente de NSS non validée pour FIPS 140-2. VMware confirme que le module fonctionne correctement, mais qu'il est n'est plus formellement validé.
- **Contrôleur et VPN de mise en cluster** : NSX Controller utilise le VPN IPsec pour connecter des clusters de contrôleur. Le VPN IPsec utilise le module de chiffrement du noyau VMware Linux (environnement Photon 1), qui est en cours de validation CMVP.

Historique de révision du document

12 octobre 2017 : Première édition.
27 octobre 2017 : Deuxième édition. Ajout du problème connu 1965859.
9 novembre 2017 : Troisième édition : Ajout d'informations sur le nouveau build pour 6.3.4. Ajout du problème résolu 1989763. Ajout des problèmes connus : 1783528, 1843197.
13 mai 2019 : quatrième édition. Mise à jour de la section Mise à niveau du cluster d'hôtes.

Problèmes résolus

Les problèmes résolus sont regroupés comme suit :

Problèmes de mise en réseau logique et de Services Edge résolus dans NSX 6.3.4

- **Problème résolu 1970527 : ARP ne parvient pas à résoudre pour des machines virtuelles lorsque le tableau ARP de routeur distribué logique dépasse la limite de 5K**
  Problème résolu dans la version 6.3.4.

- **Problème résolu 1961105 : La connexion du VTEP matériel échoue lors du redémarrage du contrôleur**
  Une exception BufferOverFlow est observée lorsque certaines configurations du VTEP matériel sont envoyées depuis NSX Manager à NSX Controller. Ce problème de dépassement empêche NSX Controller d'obtenir une configuration de passerelle matérielle complète. *Problème résolu dans la version 6.3.4.*

Problèmes de NSX Controller résolus dans NSX 6.3.4

- **Problème résolu 1955855 : L'API de contrôleur pouvait échouer en raison du nettoyage des fichiers de référence du serveur API**
  Après un nettoyage des fichiers requis, les workflows, comme Traceflow et CLI centrale, échoueront. Si des événements externes interrompent les connexions TCP persistantes entre NSX Manager et le contrôleur, NSX Manager ne pourra plus établir des connexions API aux contrôleurs et l'interface utilisateur affichera les contrôleurs comme étant déconnectés. Ce problème n'a aucune répercussion sur le chemin d'accès des données. *Problème résolu dans la version 6.3.4.*

- **Problème 1989763 : NSX Controller ne parvient pas à se déployer en raison de l'expiration des mots de passe sur le compte d'utilisateur**

Les comptes d'utilisateur sur NSX Controller disposent d'un délai d'expiration de 90 jours. Cela entraîne l'expiration immédiate des mots de passe des déploiements de NSX Controller si ces derniers ont lieu 90 jours après la création. Cela n'a aucune incidence sur le chemin de données.

Solution : consultez l'article 000051144 de la base de connaissances de VMware.
Problèmes résolus dans NSX 6.3.3 build 7087283 et NSX 6.3.4 build 7087695.

Problèmes connus

Les problèmes connus sont classés comme suit.

- Problèmes connus généraux
- Problèmes connus de mise à niveau et d'installation
- Problèmes connus de NSX Controller
- Problèmes connus liés à la mise en réseau logique et à NSX Edge
- Problèmes connus des services de sécurité
- Problèmes connus des services de surveillance
- Problèmes connus d'interopérabilité entre les solutions

Problèmes connus généraux

- **Problème 1874863 : Authentification impossible avec le mot de passe modifié après la désactivation/activation du service sslvpn avec le serveur d'authentification local**
  Lorsque le service VPN SSL est désactivé et réactivé, et lors de l'utilisation de l'authentification locale, les utilisateurs ne peuvent pas se connecter avec des mots de passe modifiés.

  Consultez l'*article 2151236 de la base de connaissances de VMware* pour plus d'informations.

- **Problème 1702339 : Les analyseurs de vulnérabilité peuvent signaler la vulnérabilité Quagga bgp_dump_routes CVE-2016-4049**
  Les analyseurs de vulnérabilité peuvent signaler la vulnérabilité Quagga bgp_dump_routes CVE-2016-4049 dans NSX for vSphere. NSX for vSphere utilise Quagga, mais la fonctionnalité BGP (y compris la vulnérabilité) n'est pas activée. Cette alerte de vulnérabilité peut être ignorée en toute sécurité.

  Solution : Comme le produit n'est pas vulnérable, aucune solution n'est nécessaire.

- **Problème 1740625, 1749975 : Problèmes d'interface utilisateur sous Mac OS dans Firefox et Safari**
  Si vous utilisez Firefox ou Safari sous Mac OS, le bouton de navigation vers l'arrière ne fonctionne pas dans NSX Edge sur la page Networking and Security dans vSphere 6.5 Web Client et, parfois, l'interface utilisateur se fige dans Firefox.

  Solution : utilisez Google Chrome sous Mac OS ou cliquez sur le bouton Accueil, puis continuez comme prévu.

- **Problème 1700980 : pour le correctif de sécurité CVE-2016-2775, une requête dont le nom est trop long peut provoquer une erreur de segmentation dans lwresd.**
  NSX 6.2.4 est installé avec BIND 9.10.4, mais n'utilise pas l'option lwres dans *named.conf*. Le produit n'est donc pas vulnérable.

  Solution : Comme le produit n'est pas vulnérable, aucune solution n'est nécessaire.

- **Problème 1568180 : Liste de fonctionnalités incorrecte pour NSX lors de l'utilisation de vCenter Server Appliance (vCSA) 5.5**
  Vous pouvez voir les fonctionnalités d'une licence dans vSphere Web Client en sélectionnant la licence et en cliquant sur **Actions > Afficher les fonctionnalités**. Si vous effectuez la mise à niveau vers NSX 6.2.3, votre licence est mise à niveau vers une licence Enterprise, qui active toutes les fonctionnalités. Toutefois, si NSX Manager est enregistré avec vCenter Server Appliance (vCSA) 5.5, le fait de sélectionner **Afficher les fonctionnalités** affichera la liste de fonctionnalités de la licence utilisée avant la mise à niveau, pas la nouvelle licence Enterprise.

  Solution : toutes les licences Enterprise disposent des mêmes fonctionnalités, même si elles ne sont pas affichées correctement dans vSphere Web Client. Pour plus d'informations, consultez la page de licence de NSX.

Problèmes connus de mise à niveau et d'installation

Avant d'effectuer la mise à niveau, lisez la section antérieure Notes relatives aux mises à niveau.

- **Problème 1932907 : Échec de la mise à niveau de la SVM de Guest Introspection**
  Lorsque vous tentez de mettre à niveau la SVM de Guest Introspection, l'état d'installation pour la SVM GI est « Échec ». Cette situation peut être applicable pour les SVM GI d'un ou plusieurs hôtes dans le cluster.

  Solution :
  1. Supprimez la SVM GI du VC.
  2. Dans le volet de déploiement du service SVM GI, cliquez sur **Résoudre**. Cette option va redéployer la SVM GI.

- **Problème 1848058 : La mise à niveau des VIB de l'hôte ESXi vers NSX 6.3.2 peut échouer**
  Dans certains cas, lors de la mise à niveau des VIB de l'hôte ESXi vers NSX 6.3.2, l'ancien répertoire de VIB est supprimé de NSX Manager, ce qui provoque l'échec de la mise à niveau. Cliquer sur le bouton Résoudre ne corrige pas le problème.

  Solution : pour résoudre ce problème, utilisez l'API de mise à niveau :

  ```
  PUT https://<nsx-mgr-ip>/api/2.0/nwfabric/configure

  <nwFabricFeatureConfig>
    <featureId>com.vmware.vshield.vsm.vxlan</featureId>
    <resourceConfig>
      <resourceId>domain-cXX</resourceId>
    </resourceConfig>
  </nwFabricFeatureConfig>
  ```

  où <nsx-mgr-ip> est l'adresse IP de votre instance de NSX Manager et `domain-cXX` est l'ID de domaine du cluster.
- **Problème 1747217 : La préparation d'hôtes ESXi provoque le mauvais fonctionnement de `muxconfig.xml.bad` et de Guest Introspection**
  Si le « chemin vmx » est manquant pour l'une des VM dans `muxconfig.xml`, lorsque MUX tente d'analyser le fichier de configuration et ne trouve pas la propriété « chemin xml », il renomme le fichier de configuration « muxconfig.xml.bad », envoie le message d'erreur « Erreur - configuration de l'analyse MUX » à l'USVM et ferme le canal de configuration.
  Solution : supprimez les VM orphelines dans l'inventaire vCenter.

- **Problème 1859572 : Lors de la désinstallation de VIB NSX version 6.3.x sur des hôtes ESXi gérés par vCenter 6.0.0, l'hôte reste en mode de maintenance**
  Si vous désinstallez des VIB NSX version 6.3.x sur un cluster, le workflow implique de mettre les hôtes en mode de maintenance, de désinstaller les VIB et de retirer les hôtes du mode de maintenance par le service EAM. Toutefois, si ces hôtes sont gérés par vCenter Server 6.0.0, cela bloque l'hôte en mode de maintenance après la désinstallation des VIB. Le service EAM responsable de la désinstallation des VIB met l'hôte en mode de maintenance, mais ne parvient pas

à l'en sortir.

Solution : sortez manuellement l'hôte du mode de maintenance. Ce problème ne se produit pas si l'hôte est géré par vCenter Server 6.5a et versions supérieures.

- **Problème 1435504 : La vérification de la santé HTTP/HTTPS apparaît inactive après la mise à niveau de la version 6.0.x ou 6.1.x vers la version 6.3.x avec la raison « Le code de retour 127 est hors limites - le plug-in est peut-être manquant »**
  Dans NSX 6.0.x et 6.1.x, les URL configurées sans guillemets ("") provoquaient l'échec de la vérification de la santé avec cette erreur : « Le code de retour 127 est hors limites - le plug-in est peut-être manquant ». La solution à ce problème consistait à ajouter les guillemets ("") à l'URL entrée (cela n'était pas requis pour les champs envoyer/recevoir/attendre). Toutefois, ce problème a été résolu dans la version 6.2.0. Par conséquent, si vous effectuez la mise à niveau à partir de la version 6.0.x ou 6.1.x vers la version 6.3.x, les guillemets supplémentaires entraînent l'affichage des membres du pool comme étant inactifs dans la vérification de la santé.

  Solution : supprimez les guillemets ("") dans le champ d'URL de toutes les configurations de vérification de la santé adéquates après la mise à niveau.

- **Problème 1734245 : Data Security entraîne l'échec des mises à niveau vers la version 6.3.0**
  Les mises à niveau vers la version 6.3.0 échouent si Data Security est configuré dans le cadre d'une stratégie de service. Veillez à supprimer Data Security des stratégies de service avant de procéder à la mise à niveau.
- **Problème 1801685 : Impossible d'afficher les filtres sur ESXi après une mise à niveau de la version 6.2.x vers la version 6.3.0 en raison d'un échec de connexion à l'hôte**
  Après une mise à niveau de NSX 6.2.x vers la version 6.3.0 et des modules VIB de cluster vers la version 6.3.0 bits, même si l'état de l'installation indique que cette dernière est terminée et que le pare-feu est activé, l'indicateur de « l'intégrité du canal de communication » signale une défaillance au niveau de la connectivité entre NSX Manager et l'agent de pare-feu et au niveau de la connectivité entre NSX Manager et l'agent ControlPlane. Cela entraîne des problèmes au niveau de la publication des règles de pare-feu et des stratégies de sécurité. En outre, la configuration du VXLan risque ne pas être envoyée vers les hôtes.

  Solution : Exécutez l'appel API Synchronisation du bus de messages pour le cluster avec l'API `POST https://<NSX-IP>/api/2.0/nwfabric/configure?action=synchronize`.
  Corps de l'API :

```
<nwFabricFeatureConfig>
 <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
 <resourceConfig>
   <resourceId>{Cluster-MOID}</resourceId>
 </resourceConfig>
</nwFabricFeatureConfig>
```

- **Problème 1797307 : NSX Edge peut être exécuté en mode Split-Brain après une mise à niveau ou un redéploiement**
  Sur le dispositif NSX Edge en veille, la commande d'interface de ligne de commande show service highavailability indique l'état de haute disponibilité « Veille » et l'état du moteur de configuration « Actif ».

  Solution : Redémarrez le dispositif NSX Edge en veille.

- **Problème 1789989 : Lors d'une mise à niveau du cluster d'hôte, une perte de paquet peut se produire dans le plan de données**
  Lors de la mise à niveau de VIB, le fichier de mot de passe de VSFWD (vShield Firewall Daemon) qui est conservé dans le VIB est supprimé. Par conséquent, VSFWD ne peut pas utiliser l'ancien mot de passe pour se connecter à NSX Manager et il doit attendre que le nouveau mot de passe soit mis à jour. Ce processus met un peu de temps à s'exécuter après le redémarrage de l'hôte. Toutefois, dans un cluster DRS entièrement automatisé, les VM sont déplacées immédiatement

lorsque l'hôte préparé est activé et, comme le processus VSFWD n'est pas prêt à ce stade, il existe un risque de perte de paquet dans le plan de données pendant un bref moment.

Solution : au lieu d'effectuer la restauration automatique dès que l'hôte se réactive, retardez la restauration automatique sur l'hôte de ces VM qui vient d'être préparé.

- **Problème 1797929 : Canal de bus de messages inactif après la mise à niveau du cluster d'hôte**
  Après la mise à niveau d'un cluster d'hôte, vCenter 6.0 (et versions antérieures) ne génère pas l'événement « reconnect » et, par conséquent, NSX Manager ne configure pas l'infrastructure de messagerie sur l'hôte. Ce problème a été résolu dans vCenter 6.5.

  Solution : resynchronisez l'infrastructure de messagerie comme suit :

```
POST https://<ip>:/api/2.0/nwfabric/configure?action=synchronize

<nwFabricFeatureConfig>
        <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
        <resourceConfig>
            <resourceId>host-15</resourceId>
        </resourceConfig>
    </nwFabricFeatureConfig>
```

- **Problème 1768144 : Les anciennes réservations de ressources de dispositif NSX Edge qui dépassent les nouvelles limites peuvent entraîner un échec lors de la mise à niveau ou du redéploiement**
  Dans NSX 6.2.4 et versions antérieures, vous pouviez spécifier une réserve de ressources arbitrairement importante pour un dispositif NSX Edge. NSX n'a pas imposé une valeur maximale. Après la mise à niveau de NSX Manager vers la version 6.2.5 ou ultérieure, si un dispositif Edge existant dispose de ressources réservées (en particulier, la mémoire) qui dépassent la nouvelle valeur maximale imposée pour le facteur de forme choisi, un échec est susceptible de survenir lors de la mise à niveau ou du redéploiement du dispositif Edge (déclenchant une mise à niveau). Par exemple, si l'utilisateur a spécifié une réservation de mémoire de 1 000 Mo sur un dispositif LARGE Edge antérieur à la version 6.2.5 et si, après la mise à niveau vers la version 6.2.5, il change la taille de dispositif en COMPACT, la réservation de la mémoire spécifiée dépassera la nouvelle valeur maximale (en l'occurrence 512 pour un dispositif COMPACT Edge) et l'opération échouera. Consultez Mise à niveau d'Edge Service Gateway (ESG) pour plus d'informations sur l'allocation de ressources recommandée à partir de NSX 6.2.5.
  Solution : Utilisez le dispositif API REST : `PUT https://<NSXManager>/api/4.0/edges/<edge-Id>/appliances/` afin de reconfigurer la réservation de mémoire pour qu'elle se situe dans la plage de valeurs spécifiées pour le facteur de forme, sans autre modification de dispositif. Vous pouvez modifier la taille du dispositif une fois cette opération terminée.

- **Problème 1600281 : L'état d'installation de la USVM indique Échec dans l'onglet Déploiements de service**
  Si la banque de données de sauvegarde de la SVM universelle Guest Introspection passe hors ligne ou devient inaccessible, il peut être nécessaire de redémarrer ou de redéployer la USVM à récupérer.

  Solution : redémarrez ou redéployez la USVM à récupérer.

- **Problème 1660373 : vCenter applique une licence NSX expirée**
  À partir de vSphere 5.5 update 3 ou de vSphere 6.0.x, vSphere Distributed Switch est inclus dans la licence NSX. Toutefois, vCenter n'autorise pas l'ajout d'hôtes ESX à vSphere Distributed Switch si la licence NSX est expirée.

  Solution : votre licence NSX doit être active pour pouvoir ajouter un hôte à vSphere Distributed Switch.

- **Problème 1569010/1645525 : Lors de la mise à niveau de 6.1.x vers NSX for vSphere 6.2.3 sur un système connecté à vCenter 5.5, le champ Produit dans la fenêtre « Attribuer une clé de licence » affiche la licence NSX comme valeur générique de « NSX for vSphere » et non une version plus spécifique telle que « NSX for vSphere - Enterprise ».**

  Solution : aucune.

- **Problème 1636916 : Dans un environnement vCloud Air, lorsque la version NSX Edge est mise à niveau de vCNS 5.5.x vers NSX 6.x, les règles de pare-feu Edge avec la valeur de protocole source « any » prennent la valeur « tcp:any, udp:any »**
  Par conséquent, le trafic ICMP est bloqué et des abandons de paquets peuvent avoir lieu.

  Solution : avant la mise à niveau de votre version de NSX Edge, créez des règles de pare-feu Edge plus spécifiques et remplacez « any » par des valeurs de port source spécifiques.

- **Problème 1474238 : Après la mise à niveau de vCenter, vCenter peut perdre la connectivité avec NSX**
  Si vous utilisez le service SSO intégré à vCenter, ce dernier risque de perdre la connexion avec NSX si vous procédez à une mise à niveau de la version 5.5 vers la version 6.0. Ce problème peut se produire si vCenter 5.5 a été enregistré auprès de NSX avec le nom d'utilisateur racine. Dans NSX 6.2, l'enregistrement de vCenter avec le nom racine est obsolète.
  Remarque : Si vous utilisez un service SSO externe, aucune modification n'est requise. Vous pouvez conserver le même nom d'utilisateur, par exemple, admin@monentreprise.mondomaine, sans perte de connectivité de vCenter.

  Solution : réenregistrez vCenter avec NSX en utilisant le nom d'utilisateur administrator@vsphere.local au lieu du nom d'utilisateur racine.

- **Problème 1375794 : Arrêtez le SE client pour les VM d'agents (SVA) avant la mise hors tension**
  Lorsqu'un hôte est placé en mode de maintenance, tous les dispositifs du service sont mis hors tension plutôt que d'être arrêtés normalement. Cela peut générer des erreurs sur les dispositifs tiers.

  Solution : aucune.

- **Problème 1112628 : Impossible de mettre sous tension le dispositif du service qui était déployé à l'aide de la vue Déploiements de services**
  Solution : avant de continuer, vérifiez ce qui suit :

  - Le déploiement de la machine virtuelle est terminé.
  - Aucune tâche telle que le clonage, la reconfiguration, etc., n'est en cours pour la machine virtuelle affichée dans le volet des tâches de vCenter.
  - Dans le volet des événements de vCenter de la machine virtuelle, les événements suivants s'affichent une fois le déploiement initié :

    ```
    La VM de l'agent <nom de vm> a été provisionnée.
    Marquez l'agent comme disponible pour continuer le workflow d'agent.
    ```

    Dans un tel cas, supprimez la machine virtuelle du service. Dans l'interface utilisateur du déploiement de services, le déploiement est affiché avec l'état Échec. En cliquant sur l'icône rouge, une alarme indiquant l'indisponibilité de la VM d'agent s'affiche pour l'hôte. Lorsque vous résolvez l'alarme, la machine virtuelle est redéployée et mise sous tension.

- **Si tous les clusters de votre environnement ne sont pas préparés, le message de mise à niveau pour Distributed Firewall ne s'affiche pas sur l'onglet Préparation de l'hôte de la page Installation.**
  Lorsque vous préparez des clusters pour la virtualisation réseau, le pare-feu distribué est activé sur ces clusters. Si les clusters de votre environnement ne sont pas tous préparés, le message de mise à niveau pour le pare-feu distribué ne s'affiche pas sur l'onglet Préparation de l'hôte.

  Solution : Utilisez l'appel REST suivant pour mettre à niveau le pare-feu distribué :
  `PUT https://<nsxmgr-ip>/api/4.0/firewall/globalroot-0/state`

- **Problème 1215460 : si un groupe de services est modifié à la suite de la mise à niveau pour ajouter ou supprimer des services, ces modifications ne sont pas reflétées dans le tableau du pare-feu.**
  Les groupes de services créés par les utilisateurs sont développés dans le tableau Edge Firewall lors de la mise à niveau, c'est-à-dire que la colonne Service du tableau du pare-feu affiche tous les services au sein du groupe de services. Si le groupe de services est modifié après la mise à niveau pour ajouter ou supprimer des services, ces modifications ne sont pas reflétées dans le tableau du pare-feu.

  Solution : créez un nouveau groupe de services avec un nom différent puis utilisez ce groupe de services dans la règle du pare-feu.

- **Problème 1413125 : Impossible de reconfigurer le serveur SSO après une mise à niveau**
  Lorsque le serveur SSO configuré sur NSX Manager est le serveur natif sur vCenter Server, vous ne pouvez pas reconfigurer les paramètres SSO sur NSX Manager après la mise à niveau de vCenter Server vers la version 6.0 et de NSX Manager vers la version 6.x.

  Solution : aucune.

- **Problème 1263858 : VPN SSL n'envoie pas de notification de mise à niveau au client distant**
  La passerelle VPN SSL n'envoie pas de notification de mise à niveau aux utilisateurs. L'administrateur doit informer manuellement les utilisateurs distants que la passerelle VPN SSL (serveur) est mise à jour et qu'ils doivent mettre à jour leurs clients.

  Solution : les utilisateurs doivent désinstaller l'ancienne version du client et installer la dernière version manuellement.

- **Problème 1462319 : Le VIB esx-dvfilter-switch-security n'est plus présent dans la sortie de la commande « esxcli software vib list | grep esx ».**
  Depuis NSX 6.2, les modules esx-dvfilter-switch-security sont inclus dans le VIB esx-vxlan. Les seuls VIB NSX installés pour la version 6.2 sont esx-vsip et esx-vxlan. Lors d'une mise à niveau de NSX vers la version 6.2, l'ancien VIB esx-dvfilter-switch-security est supprimé des hôtes ESXi.
  Depuis NSX 6.2.3, un troisième VIB, esx-vdpi, est fourni avec les VIB NSX esx-vsip et esx-vxlan. Lorsque l'installation est réussie, les trois VIB sont affichés.

  Solution : aucune.

- **Problème 1481083 : Après la mise à niveau, les routeurs logiques avec une association configurée peuvent échouer à transférer correctement des paquets**
  Lorsque les hôtes exécutent ESXi 5.5, l'association NSX 6.2 de basculement explicite ne prend pas en charge plusieurs liaisons montantes actives sur les routeurs logiques distribués.

  Solution : modifiez la stratégie d'association de basculement explicite de sorte qu'il n'y ait qu'une liaison montante active et que les autres liaisons montantes soient en mode veille.

- **Problème 1411275 : vSphere Web Client n'affiche pas l'onglet Networking and Security à la suite de la sauvegarde et de la restauration dans NSX for vSphere 6.2**
  Lorsque vous effectuez des opérations de sauvegarde et de restauration à la suite d'une mise à niveau vers NSX for vSphere 6.2, vSphere Web Client n'affiche pas l'onglet **Networking & Security**.

Solution : lorsqu'une sauvegarde de NSX Manager est restaurée, vous êtes déconnecté du gestionnaire de dispositif. Attendez quelques minutes avant de vous connecter à vSphere Web Client.

- **La machine virtuelle de service déployée à l'aide de l'onglet Déploiements de services dans la page Installation n'est pas mise sous tension**

  Solution :

  1. Supprimez manuellement la machine virtuelle de service du pool de ressources `Agents ESX` dans le cluster.
  2. Cliquez sur **Networking and Security**, puis cliquez sur **Installation**.
  3. Cliquez sur l'onglet **Déploiements de services**.
  4. Sélectionnez le service approprié, puis cliquez sur l'icône **Résoudre**.
     La machine virtuelle de service est redéployée.

- **Problème 1764460 : Une fois la préparation de l'hôte terminée, tous les membres du cluster affichent l'état « Prêt », mais le niveau de cluster affiche de façon erronée « Non valide »**
  Une fois que vous avez terminé la préparation de l'hôte, tous les membres du cluster affichent l'état « Prêt », mais le niveau de cluster affiche de façon erronée « Non valide ». Vous devez redémarrer l'hôte, même si ce dernier a déjà été redémarré, comme indiqué dans la raison affichée.

  Solution : Cliquez sur l'icône d'avertissement rouge et sélectionnez Résoudre.

Problèmes connus de NSX Manager

- **Problème 1892999 : Impossible de modifier les critères de sélection uniques, même lorsqu'aucune VM n'est attachée à la balise de sécurité universelle**
  Si une machine virtuelle attachée à une balise de sécurité universelle est supprimée, un objet interne représentant la VM reste encore attaché à la balise de sécurité universelle. Cela entraîne l'échec de la modification des critères de sélection universels avec une erreur indiquant que des balises de sécurité universelle sont encore attachées aux machines virtuelles.

  Solution : Supprimez toutes les balises de sécurité universelle, puis modifiez les critères de sélection universels.

- **Problème 1926309 : Le plug-in NSX Manager n'est pas en mesure de charger et indique « Exception d'authentification »**
  Il arrive que le plug-in NSX Manager ne parvienne pas à charger des pages et il finit par afficher une erreur de délai d'expiration.

  Solution : redémarrez le service de gestion de NSX ou redémarrez le dispositif NSX Manager.

- **Problème 1904842 : NSX Manager n'est pas enregistré avec vCenter ou Platform Services Controller**
  NSX Manager n'apparaît pas sur l'interface utilisateur et un appel REST à NSX Manager échoue.

  Solution : redémarrez le service de gestion de NSX ou redémarrez le dispositif NSX Manager.

- **Problème 1801325 : Événements système « Critique » et journalisation générés dans NSX Manager avec une utilisation élevée du CPU et/ou du disque**
  En cas d'une utilisation élevée de l'espace disque, d'une forte évolution des données de travail ou d'une taille élevée de la file d'attente des travaux sur NSX Manager, vous pouvez rencontrer un ou plusieurs des problèmes suivants :
  - Événements système « Critique » dans vSphere Web Client
  - Utilisation élevée du disque sur NSX Manager pour la partition `/common`
  - Utilisation élevée du CPU sur des périodes prolongées ou à des intervalles réguliers
  - Impact négatif sur les performances de NSX Manager

Solution : contactez le support client VMware. Consultez l'*article 2147907 de la base de connaissances de VMware* pour plus d'informations.

- **Problème 1781080 : La configuration de la recherche DNS échoue lorsque plusieurs domaines sont ajoutés, séparés par des virgules**
  Lorsque vous ajoutez plusieurs suffixes de recherche de domaine à NSX Manager, toutes les recherches DNS qui n'utilisent pas le nom complet échouent. Cela est dû à un problème de mise en forme interne de `/etc/resolv.conf`.

  Solution : utilisez un seul suffixe de recherche DNS.

- **Problème 1806368 : La réutilisation de contrôleurs d'une instance principale de NSX Manager ayant échoué précédemment qui redevient principale après un basculement provoque le non-transfert de la configuration du DLR à tous les hôtes**
  Dans une installation cross-vCenter NSX, lorsque l'instance principale de NSX Manager échoue, une instance secondaire de NSX Manager devient principale et un nouveau cluster de contrôleurs est déployé pour être utilisé avec l'instance secondaire de NSX Manager qui vient d'être promue (maintenant principale). Lorsque l'instance principale de NSX Manager est de nouveau active, l'instance secondaire de NSX Manager est rétrogradée et l'instance principale de NSX Manager est restaurée. Dans ce cas, si vous réutilisez des contrôleurs existants qui ont été déployés sur cette instance principale de NSX Manager avant le basculement, la configuration du DLR n'est pas transférée à tous les hôtes. Ce problème ne se pose pas si vous créez un cluster de contrôleurs à la place.

  Solution : déployez un nouveau cluster de contrôleur pour l'instance principale de NSX Manager restaurée.

- **Problème 1831131 : La connexion depuis NSX Manager vers SSO échoue lorsqu'elle est authentifiée avec l'utilisateur LocalOS**
  La connexion depuis NSX Manager vers SSO échoue lorsqu'elle est authentifiée avec l'utilisateur LocalOS avec l'erreur : « Impossible d'établir la communication avec NSX Manager. Contactez l'administrateur. »

  Solution : ajoutez le rôle d'administrateur d'entreprise pour `nsxmanager@localos` en plus de `nsxmanager@domain`.

- **Problème 1800820 : Échec de la mise à jour de l'interface du routeur logique universel distribué (UDLR) sur une instance secondaire de NSX Manager lorsque l'ancienne interface de l'UDLR a déjà été supprimée du système**
  Lorsque Universal Synchronization Service (réplicateur) cesse de fonctionner sur l'instance principale de NSX Manager, vous devez supprimer les interfaces du routeur logique universel distribué (UDLR) et du commutateur logique universel (ULS) sur l'instance principale de NSX Manager, créer de nouvelles interfaces, puis les répliquer sur une instance secondaire de NSX Manager. Dans ce cas, l'interface de l'UDLR n'est pas mise à jour sur l'instance secondaire de NSX Manager, car un nouvel ULS est créé sur celle-ci lors de la réplication, et l'UDLR n'est pas connecté à ce nouvel ULS.

  Solution : assurez-vous que le réplicateur est en cours d'exécution et supprimez l'interface de l'UDRL (LIF) sur l'instance principale de NSX Manager qui est dotée d'un ULS de secours nouvellement créé, et recréez l'interface de l'UDRL (LIF) avec le même ULS de secours.

- **Problème 1772911 : NSX Manager s'exécute très lentement avec la consommation de l'espace disque et les tailles de tableau des tâches et des travaux augmentent avec une utilisation du CPU de près de 100 %**
  Vous rencontrerez ce qui suit :
  - Le CPU de NSX Manager est à 100 % ou atteint régulièrement une consommation de 100 % et l'ajout de ressources supplémentaires au dispositif NSX Manager ne fait pas de différence.
  - L'exécution de la commande `show process monitor` dans l'interface de ligne de commande de NSX Manager affiche le processus Java qui consomme le plus de cycles de CPU.

- L'exécution de la commande `show filesystems` sur l'interface de ligne de commande de NSX Manager indique que le répertoire `/common` a un pourcentage d'utilisation très élevé, tel que > 90 %.
- Certaines modifications de la configuration expirent (prenant parfois plus de 50 minutes) et ne sont pas effectives.

Consultez l'*article 2147907 de la base de connaissances de VMware* pour plus d'informations.

Solution : contactez le support client VMware pour résoudre ce problème.

- **Problème 1785142 : Retard de l'affichage de « Problèmes de synchronisation » sur l'instance principale de NSX Manager lorsque la communication entre les instances principales et secondaires de NSX Manager est bloquée.**
  Lorsque la communication entre les instances principales et secondaires de NSX Manager est bloquée, vous ne voyez pas immédiatement « Problèmes de synchronisation » sur l'instance principale de NSX Manager.

  Solution : attendez environ 20 minutes que la communication soit rétablie.

- **Problème 1786066 : Dans une installation cross-vCenter de NSX, la déconnexion d'une instance secondaire de NSX Manager peut l'empêcher de se reconnecter comme instance secondaire**
  Dans une installation cross-vCenter de NSX, si vous déconnectez une instance secondaire de NSX Manager, vous pouvez être incapable de rajouter cette instance ultérieurement comme instance secondaire de NSX Manager. Les tentatives de reconnexion de l'instance de NSX Manager comme instance secondaire font apparaître l'état « Secondaire » pour l'instance de NSX Manager dans l'onglet Gestion de vSphere Web Client, mais la connexion à l'instance principale n'est pas établie.
  Solution :

  1. Déconnectez l'instance secondaire de NSX Manager de l'instance principale de NSX Manager.
  2. Ajoutez de nouveau l'instance secondaire de NSX Manager à l'instance principale de NSX Manager.

- **Problème 1713669 : NSX Manager échoue en raison d'un disque complet lorsque le tableau de base de données ai_useripmap devient trop volumineux**
  Ce problème entraîne la saturation du disque du dispositif NSX Manager et donc l'échec de NSX Manager. Le processus postgres ne peut pas être démarré après un redémarrage. La partition « /common » est complète. Cela se produit le plus souvent sur des sites qui placent une surcharge sur le serveur de journaux des événements (ELS) et sur des sites avec une grande quantité de trafic Guest Introspection (GI). Les sites qui utilisent Identity Firewall (IDFW) sont fréquemment affectés.
  Consultez l'*article 2148341 de la base de connaissances de VMware* pour plus d'informations.

  Solution : contactez le support client de VMware pour qu'il vous aide à résoudre ce problème.

- **Problème 1783528 : L'utilisation du CPU de NSX Manager connaît des pics tous les vendredis soir/samedis matin**
  NSX interroge LDAP pour une synchronisation complète tous les vendredis soir. Il n'existe aucune option pour configurer une unité d'organisation ou un conteneur Active Directory spécifique, par conséquent, NSX interroge tous les objets qui sont liés au domaine fourni.

  Solution : augmentez les CPU virtuels NSX Manager du nombre de 4 au nombre de 6.

- **Problème 1715354 : Retard de disponibilité de l'API REST**
  Il faut parfois du temps à l'API NSX Manager pour être active et en cours d'exécution après le redémarrage de NSX Manager lorsque le mode FIPS est enclenché. Il peut apparaître que l'API est suspendue, mais cela se produit car les contrôleurs ont besoin de temps pour rétablir la connexion avec NSX Manager. Vous êtes informé que vous devez attendre que le serveur NSX API soit actif et en cours d'exécution et que vous devez vérifier que tous les contrôleurs sont dans l'état connecté avant toute opération.

- **Problème 1441874 : la mise à niveau d'une instance de NSX Manager unique dans un environnement vCenter Linked Mode affiche un message d'erreur**
  Dans un environnement avec plusieurs serveurs VMware vCenter Server avec plusieurs instances de NSX Manager, lors de la sélection d'une ou de plusieurs instances de NSX Manager dans vSphere Web Client > Networking and Security > Installation > Préparation de l'hôte, vous voyez cette erreur :
  « Impossible d'établir la communication avec NSX Manager. Contactez l'administrateur. »
  Solution : consultez l'*article 2127061 de la base de connaissances de VMware* pour plus d'informations.

- **Problème 1696750 : l'affectation d'une adresse IPv6 à NSX Manager via l'API PUT nécessite un redémarrage**
  Pour pouvoir être activée, toute modification des paramètres réseau configurés pour NSX Manager via *https://{NSX Manager IP address}/api/1.0/appliance-management/system/network* nécessite un redémarrage. Jusqu'au redémarrage, les paramètres préexistants sont affichés.

  Solution : aucune.

- **Problème 1529178 : Le téléchargement d'un certificat de serveur qui n'inclut pas un nom commun renvoie le message « Erreur de serveur interne »**
  Si vous téléchargez un certificat de serveur sans nom commun, le message « Erreur de serveur interne » s'affiche.

  Solution : utilisez un certificat de serveur avec un nom SubAltName et un nom commun, ou au moins un nom commun.

- **Problème 1655388 : L'interface utilisateur de NSX Manager 6.2.3 s'affiche en langue anglaise au lieu de la langue locale lorsque le navigateur IE11/Edge est utilisé sur le système d'exploitation Windows 10 pour les langues JA, CN et DE**
  Lorsque vous lancez NSX Manager 6.2.3 avec le navigateur IE11/Edge sur le système d'exploitation Windows 10 pour les langues JA, CN et DE, la langue anglaise s'affiche.

  Solution :

  1. Lancez l'Éditeur du Registre Microsoft (regedit.exe) et accédez à **Ordinateur** > **HKEY_CURRENT_USER** > **SOFTWARE** > **Microsoft** > **Internet Explorer** > **International**.
  2. Modifiez la valeur du fichier *AcceptLanguage* sur la langue native. Par exemple, si vous voulez définir la langue sur **DE**, changez la valeur et faites apparaître **DE** en première position.
  3. Redémarrez le navigateur et reconnectez-vous à NSX Manager. La langue appropriée est affichée.

- **Problème 1435996 : Les fichiers journaux exportés au format CSV à partir de NSX Manager sont horodatés avec l'époque au lieu de la valeur datetime**
  Les fichiers journaux exportés au format CSV à partir de NSX Manager à l'aide de vSphere Web Client sont horodatés avec l'heure en millisecondes plutôt qu'avec l'heure appropriée correspondant au fuseau horaire.
  Solution : aucune.

- **Problème 1644297 : L'opération d'ajout/suppression pour une section du DFW sur l'instance principale de NSX crée deux configurations du DFW enregistrées sur l'instance secondaire de NSX**
  Dans une configuration cross-vCenter, lorsqu'une section de DFW universelle ou locale supplémentaire est ajoutée à l'instance principale de NSX Manager, deux configurations DFW sont enregistrées sur l'instance secondaire de NSX Manager. Bien qu'il n'affecte aucune fonctionnalité, ce problème entraînera l'atteinte plus rapide de la limite des configurations enregistrées, ce qui peut remplacer éventuellement des configurations critiques.
  Solution : aucune.

- **Problème 1477138 : NSX Management Service n'apparaît pas lorsque le nom d'hôte contient**

plus de 64 caractères
La création de certificat via la bibliothèque OpenSSL requiert un nom d'hôte contenant au maximum 64 caractères.

- Problème 1437664 : La liste de NSX Manager est lente à s'afficher dans Web Client
  Dans les environnements vSphere 6.0 avec plusieurs NSX Manager, vSphere Web Client peut prendre jusqu'à deux minutes pour afficher la liste de NSX Manager lorsque l'utilisateur connecté est validé avec un ensemble de groupes AD important. Une erreur de délai d'expiration du service de données peut apparaître lorsque vous essayez d'afficher la liste de NSX Manager. Il n'existe pas de solution. Vous devez attendre que la liste se charge/se reconnecte pour voir la liste de NSX Manager.
- Problème 1534606 : La page Préparation de l'hôte ne parvient pas à se charger
  Lors de l'exécution de vCenter en mode lié, chaque vCenter doit être connecté à une instance de NSX Manager sur la même version de NSX. Si les versions de NSX sont différentes, vSphere Web Client ne pourra communiquer qu'avec le NSX Manager exécutant la version la plus élevée de NSX. Une erreur semblable à « Impossible d'établir la communication avec NSX Manager. Contactez votre administrateur » s'affiche dans l'onglet Préparation de l'hôte.
  Solution : toutes les instances de NSX Manager doivent être mises à niveau vers la même version logicielle de NSX.

- Problème 1386874 : l'onglet Networking and Security non affiché dans vSphere Web Client
  À la suite de la mise à niveau de vSphere vers la version 6.0, il vous est impossible de voir l'onglet Networking and Security lors de votre connexion à vSphere Web Client en utilisant le nom d'utilisateur racine.
  Solution : connectez-vous en tant qu'administrateur@vsphere.local ou tout autre utilisateur vCenter existant sur vCenter Server avant la mise à niveau et dont le rôle était défini dans NSX Manager.

- Problème 1027066 : vMotion de NSX Manager peut afficher le message d'erreur « La carte Ethernet virtuelle Adaptateur réseau 1 n'est pas prise en charge »
  Vous pouvez ignorer cette erreur. La mise en réseau fonctionnera correctement après vMotion.
- Problème 1460766 : L'interface utilisateur de NSX Manager ne se déconnecte pas automatiquement après un changement de mot de passe via l'interface de ligne de commande de NSX
  Si vous êtes connecté à NSX Manager et si vous avez récemment changé votre mot de passe à l'aide de l'interface de ligne de commande, il est possible que vous restiez connecté à l'interface utilisateur de NSX Manager via votre ancien mot de passe. Généralement, le client NSX Manager devrait automatiquement vous déconnecter si la session expire suite à une inactivité.
  Solution : Déconnectez-vous de l'interface utilisateur de NSX Manager et reconnectez-vous avec votre nouveau mot de passe.

- Problème 1467382 : Impossible de modifier le nom d'hôte réseau
  Une fois que vous vous êtes connecté au dispositif virtuel NSX Manager et que vous avez accédé à la gestion des dispositifs, puis que vous avez cliqué sur Gérer les paramètres des dispositifs et sur Réseau sous Paramètres pour modifier le nom d'hôte réseau, une erreur de liste de noms de domaine non valide peut s'afficher. Cela se produit lorsque les noms de domaine spécifiés dans le champ Domaines de recherche sont séparés par un espace plutôt que par une virgule. NSX Manager n'accepte que des noms de domaine qui sont séparés par une virgule.

  Solution :

  1. Connectez-vous au dispositif virtuel NSX Manager.
  2. Sous **Gestion des dispositifs**, cliquez sur **Gérer les paramètres des dispositifs**.
  3. Dans le panneau Paramètres, cliquez sur **Réseau**.
  4. Cliquez sur **Modifier** en regard de Serveurs DNS.
  5. Dans le champ Domaines de recherche, remplacez tous les espaces par des virgules.

6. Cliquez sur OK pour enregistrer les modifications.

- **Problème 1436953 : Un faux événement système est généré même après avoir restauré avec succès NSX Manager à partir d'une sauvegarde.**
  Après avoir restauré avec succès NSX Manager à partir d'une sauvegarde, les événements système suivants peuvent se produire dans vSphere Web Client lorsque vous accédez à **Mise en réseau et sécurité** : **NSX Managers** : **Surveiller** : **Événements système**.
  - `Échec de restauration de NSX Manager à partir d'une sauvegarde (avec gravité=critique).`
  - `Restauration de NSX Manager réalisée avec succès (avec gravité=informatif).`

  Solution : si le message final d'un événement système affiche le statut de succès, vous pouvez ignorer les messages d'événement générés par le système.

- **Problème 1843197 : L'adaptateur réseau de NSX Manager affiche le message d'avertissement « Ce type d'adaptateur réseau n'est pas pris en charge par {0}Autre Linux (64 bits) »**
  Après l'installation et la configuration correctes de NSX Manager, accédez à vCenter > Modifier les paramètres de l'instance déployée de NSX Manager. Sous Adaptateur réseau, vous voyez le message d'avertissement « Ce type d'adaptateur réseau n'est pas pris en charge par {0}Autre Linux (64 bits) ».

Problèmes connus de NSX Controller

- **Problème 1856465 : Si un hôte ESXi est hors service sur l'un des sites dans un environnement Cross-vCenter NSX, le mode CDO n'est pas activé sur ce site**
  Si un hôte ESXi est hors service sur un site, l'activation ou la désactivation du mode CDO ne sera pas effectuée correctement sur ce site.
  Si l'hôte est hors service sur l'un des sites secondaires, le mode CDO sera fonctionnel sur le site principal. Cependant, le mode CDO ne fonctionnera pas sur le site secondaire. Cela peut entraîner un comportement incohérent.

  Solution : Ce problème affecte NSX 6.3.0 et les versions ultérieures.

  - Vérifiez que tous les hôtes ESXi sont actifs avant d'effectuer des opérations CDO.
  - Afin de rétablir l'état antérieur à un état incohérent, supprimez l'hôte de l'inventaire vCenter et ajoutez-le à nouveau.
- **Problème 1965859 : La mémoire de NSX Controller augmente avec une configuration du VTEP matériel à l'origine d'une utilisation élevée du CPU**
  Une augmentation de la mémoire du processus de contrôleur est observée à travers des configurations du VTEP matériel qui s'exécutent pendant quelques jours. L'augmentation de la mémoire entraîne une utilisation élevée du CPU qui dure un certain temps (minutes) pendant que le contrôleur récupère la mémoire. Pendant ce temps, le chemin de données est affecté.

  Solution : contactez le support client VMware.

Problèmes connus liés à la mise en réseau logique et à NSX Edge

- **Problème 1904612 : Le tunnel VPN de couche 2 indique « actif » sur le serveur L2VPN lorsque le client est hors tension**
  Si vous créez un VPN L2 entre deux dispositifs NSX Edge, puis mettez hors tension le client NSX Edge, le serveur NSX Edge continue à indiquer que le tunnel VPN est actif.

  Solution : aucune.

- **Problème 1242207 : La modification des ID de routeur pendant l'exécution n'est pas reflétée dans la topologie OSPF**
  Si vous essayez de modifier l'ID de routeur sans désactiver OSPF, de nouvelles annonces d'état des liens (LSA) externes ne sont pas générées de nouveau avec cet ID de routeur, ce qui entraîne la perte des itinéraires externes OSPF.

Désactivez OSPF, modifiez l'ID de routeur et activez OSPF à nouveau.

- **Problème 1894277 : Le PSK de configuration de site IPSec n'est pas conservé lorsque le sous-réseau local ou homologue est modifié**
  Comme le PSK masqué est enregistré dans la base de données, le tunnel entre les homologues ne s'active pas à cause de l'incompatibilité des mots de passe.

  Solution : reconfigurez la configuration IPSec avec un mot de passe valide.

- **Problème 1492497 : Impossible de filtrer le trafic DHCP NSX Edge**
  Vous ne pouvez pas appliquer de filtres de pare-feu au trafic DHCP sur un dispositif NSX Edge, car le serveur DHCP sur un dispositif NSX Edge utilise des sockets bruts qui ignorent la pile TCP/IP.

  Solution : aucune.

- **Problème 1781438 : Sur les dispositifs ESG ou DLR NSX Edge, le service de routage n'envoie pas de message d'erreur s'il reçoit l'attribut de chemin d'accès BGP MULTI_EXIT_DISC plusieurs fois.**
  Le routeur Edge ou un routeur logique distribué n'envoie pas de message d'erreur s'il reçoit l'attribut de chemin d'accès BGP MULTI_EXIT_DISC plusieurs fois. Conformément à RFC 4271 [Sec 5], le même attribut (attribut du même type) ne peut pas apparaître plusieurs fois dans le champ Attributs de chemin d'accès d'un message de mise à jour particulier.

  Solution : aucune.

- **Problème 1786515 : Un utilisateur disposant de privilèges « Administrateur de sécurité » ne peut pas modifier la configuration d'équilibrage de charge via l'interface utilisateur de vSphere Web Client.**
  Un utilisateur disposant de privilèges « Administrateur de sécurité » pour un dispositif NSX Edge spécifique n'est pas en mesure de modifier la configuration globale d'équilibrage de charge pour ce dispositif Edge, à l'aide de l'interface utilisateur de vSphere Web Client. Le message d'erreur suivant s'affiche : « L'utilisateur n'est pas autorisé à accéder à l'objet Global et à la fonctionnalité si.service. Vérifiez l'étendue d'accès aux objets et les fonctionnalités autorisées pour l'utilisateur. »

  Solution : aucune.

- **Problème 1849042/1849043 : Verrouillage du compte d'administrateur lorsqu'une période de validité du mot de passe est configurée sur le dispositif NSX Edge**
  Si une période de validité du mot de passe est configurée pour l'utilisateur administrateur sur le dispositif NSX Edge, lorsque le mot de passe expire, il sera demandé à l'utilisateur de modifier le mot de passe à chaque connexion au dispositif pendant 7 jours. La non-modification du mot de passe entraînera le verrouillage du compte. En outre, si le mot de passe est modifié au moment de la connexion à l'invite de l'interface de ligne de commande, le nouveau mot de passe peut ne pas être conforme à la stratégie de mot de passe fort appliquée par l'interface utilisateur et REST.

  Solution : pour éviter ce problème, utilisez toujours l'interface utilisateur ou l'API REST pour modifier le mot de passe administrateur avant l'expiration du mot de passe existant. Si le compte se verrouille, utilisez également l'interface utilisateur ou l'API REST pour configurer un nouveau mot de passe et le compte se déverrouille.

- **Problème 1711013 : Environ 15 minutes sont nécessaires pour synchroniser FIB avec un dispositif NSX Edge actif/en veille après le redémarrage d'une VM en veille.**
  Lorsqu'un dispositif NSX Edge en veille est mis hors tension, la session TCP n'est pas fermée entre le mode actif et le mode de veille. Le dispositif Edge actif détectera que la veille est inactive après l'échec KA (keepalive) (15 minutes). Au bout de 15 minutes, une nouvelle connexion de socket est établie avec le dispositif Edge en veille et FIB est synchronisé entre le dispositif Edge actif/en veille.

  Solution : aucune.

- **Problème 1733282 : NSX Edge ne prend plus en charge les itinéraires de périphérique statiques**

NSX Edge ne prend pas en charge la configuration d'itinéraires statiques avec l'adresse de tronçon suivant NULL.

Solution : aucune.

- **Problème 1860583 : Évitez d'utiliser des sysloggers distants comme nom de domaine complet si DNS n'est pas accessible.**
  Sur un dispositif NSX Edge, si les sysloggers distants sont configurés à l'aide du nom de domaine complet et que DNS n'est pas accessible, la fonctionnalité de routage peut être affectée. Le problème ne se produit pas systématiquement.

  Solution : il est recommandé d'utiliser des adresses IP au lieu du nom de domaine complet.

- **Problème 1850773 : Le NAT NSX Edge signale une configuration non valide lorsque plusieurs ports sont utilisés pour la configuration de l'équilibrage de charge**
  Ce problème se produit chaque fois que vous configurez un serveur virtuel d'équilibrage de charge avec plusieurs ports. Pour cette raison, le NAT devient ingérable pendant que cet état de configuration existe pour le dispositif NSX Edge affecté.

  Solution : Consultez l'*article 2149942 de la base de connaissances de VMware* pour plus d'informations et pour connaître la solution.

- **Problème 1764258 : Perte de trafic pendant une durée pouvant atteindre huit minutes après un basculement HA ou une synchronisation forcée configurée à l'aide d'une sous-interface sur un dispositif NSX Edge**
  Si un basculement HA se déclenche ou que vous démarrez une synchronisation forcée sur une sous-interface, le trafic n'aboutit pas pendant une durée pouvant atteindre huit minutes.

  Solution : N'utilisez pas de sous-interfaces pour la haute disponibilité.

- **Problème 1767135 : Erreurs lors de la tentative d'accès à des certificats et à des profils d'application sous l'équilibrage de charge**
  Les utilisateurs avec des privilèges d'administrateur de sécurité et de portée Edge ne peuvent pas accéder aux certificats et aux profils d'application sous l'équilibrage de charge. vSphere Web Client affiche des messages d'erreur.

  Solution : aucune.

- **Problème 1792548 : NSX Controller peut être bloqué au message : « En attente de jonction du cluster »**
  NSX Controller peut être bloqué au message : « En attente de jonction du cluster » (commande d'interface de ligne de commande :`show control-cluster status`). Cela se produit, car la même adresse IP a été configurée pour les interfaces `eth0` et `breth0` du contrôleur alors que ce dernier s'active. Vous pouvez vérifier cela en utilisant la commande d'interface de ligne de commande suivante sur le contrôleur : `show network interface`

  Solution : contactez le support client VMware.

- **Problème 1747978 : Les contiguïtés OSPF sont supprimées avec l'authentification MD5 après le basculement HA de NSX Edge**
  Dans un environnement NSX for vSphere 6.2.4 où NSX Edge est configuré pour HA avec le redémarrage normal OSPF configuré et où MD5 est utilisé pour l'authentification, OSPF ne parvient pas à démarrer normalement. Les formulaires de contiguïté uniquement après le temporisateur mort expirent sur les nœuds voisins OSPF.

  Solution : Aucune

- **Problème 1804116 : Le routeur logique passe à un état incorrect sur un hôte qui a perdu la communication avec l'instance de NSX Manager**
  Si un routeur logique est mis sous tension ou redéployé sur un hôte qui a perdu la communication avec l'instance de NSX Manager (à cause d'un échec de mise à niveau/installation de NSX VIB ou

d'un problème de communication de l'hôte), le routeur logique passe sur un état incorrect et l'opération continue de récupération automatique via la synchronisation forcée échoue.

Solution : une fois que le problème de communication entre l'hôte et NSX Manager est résolu, redémarrez le dispositif NSX Edge manuellement et attendez que toutes les interfaces s'activent. Cette solution n'est nécessaire que pour les routeurs logiques et pas pour NSX Edge Services Gateway (ESG), car le processus de récupération automatique via la synchronisation forcée redémarre NSX Edge.

- **Problème 1783065 : Impossible de configurer l'équilibrage de charge pour le port UDP avec TCP par adresse IPv4 et IPv6 en même temps**
  UDP ne prend en charge que ipv4-ipv4, ipv6-ipv6 (frontal-principal). Il existe un bogue dans NSX Manager qui provoque la lecture d'une adresse locale de lien IPv6 et son transfert en tant qu'adresse IP de l'objet de regroupement et qui vous empêche de sélectionner le protocole IP à utiliser dans la configuration d'équilibrage de charge.
  Voici un exemple de configuration d'équilibrage de charge faisant apparaître le problème :
  Dans la configuration d'équilibrage de charge, le pool « vCloud_Connector » est configuré avec un objet de regroupement (vm-2681) comme membre de pool et cet objet contient des adresses IPv4 et IPv6, qui ne peuvent pas être prises en charge par le moteur LB L4.

```
{
                "algorithm" : {
        ...
    },
                "members" : [
        {
             ...  ,
             ...
        }
                ],
                "applicationRules" : [],
                "name" : "vCloud_Connector",
                "transparent" : {
                   "enable" : false
                }
        }

  {
                "value" : [
                   "fe80::250:56ff:feb0:d6c9",
                   "10.204.252.220"
                ],
                "id" : "vm-2681"
             }
```

  Solution :

  - Option 1 : entrez l'adresse IP du membre de pool plutôt que des objets de regroupement dans le membre de pool.
  - Option 2 : n'utilisez pas IPv6 dans les VM.

- **Problème 1777792 : Le point de terminaison homologue défini sur ANY entraîne l'échec de la connexion IPSec**
  Lorsque la configuration IPSec de NSX Edge définit le point de terminaison homologue distant sur

« ANY », le dispositif Edge fonctionne comme un « serveur » IPSec et attend que les homologues distants lancent les connexions. Toutefois, lorsque l'initiateur envoie une demande d'authentification à l'aide de PSK+XAUTH, le dispositif Edge affiche ce message d'erreur : « `Message de mode principal initial reçu sur XXX.XXX.XX.XX:500, mais aucune connexion n'a été autorisée avec policy=PSK+XAUTH` » et IPsec ne peut pas être établi.

Solution : utilisez l'adresse IP ou le FQDN du point de terminaison homologue spécifique dans la configuration VPN d'IPSec au lieu de ANY.

- **Problème 1741158 : La création d'un nouveau dispositif NSX Edge non configuré et l'application de la configuration peuvent entraîner une activation prématurée du service Edge.**
  Si vous utilisez l'API NSX pour créer un nouveau dispositif NSX Edge non configuré, effectuez ensuite un appel API pour désactiver l'un des services Edge de ce dispositif Edge (par exemple, en définissant dhcp-enabled sur « false ») et terminez en appliquant les modifications de configuration au service Edge désactivé (ce service sera activé immédiatement).

  Solution : Après avoir apporté une modification de configuration à un service Edge que vous souhaitez conserver à l'état désactivé, lancez immédiatement un appel PUT pour définir l'indicateur activé sur « false » pour ce service.

- **Problème 1758500 : L'itinéraire statique avec plusieurs sauts suivants n'est pas installé dans les tables de routage et de transfert NSX Edge si au moins l'un des sauts suivants configurés correspond à l'adresse IP de la vNIC du dispositif Edge**
  Avec ECMP et plusieurs adresses de sauts suivants, NSX permet de configurer l'adresse IP de la vNIC du dispositif Edge en tant que saut suivant si au moins une des adresses IP du prochain saut est valide. Ceci est accepté sans aucune erreur ni avertissement, mais l'itinéraire pour le réseau est supprimé de la table de routage/transfert du dispositif Edge.

  Solution : Ne configurez pas l'adresse IP proprement dite de la vNIC du dispositif Edge en tant que saut suivant dans l'itinéraire statique lors de l'utilisation d'ECMP.

- **Problème 1716464 : l'équilibrage de charge NSX ne sera pas acheminé vers des VM récemment balisées avec une balise de sécurité.**
  Si on déploie deux VM avec une balise donnée, puis que l'on configure un équilibrage de charge pour l'acheminement vers cette balise, l'équilibrage de charge procédera à l'acheminement vers ces deux VM sans problème. En revanche, si on déploie ensuite une troisième VM avec cette balise, l'équilibrage de charge ne procède à l'acheminement que vers les deux premières VM.

  Solution : cliquez sur Enregistrer sur le pool d'équilibrage de charge. Cela analyse de nouveau les VM et démarre le routage vers les VM récemment balisées.

- **Problème 1753621 : lorsqu'un dispositif Edge avec un AS local privé envoie des itinéraires à des homologues EBGP, tous les chemins d'AS privé sont extraits des mises à jour de routage BGP envoyées.**
  Actuellement, NSX présente une limite qui l'empêche de partager le chemin d'AS complet avec des voisins eBGP lorsque le chemin d'AS contient uniquement des chemins d'AS privés. Alors que ce comportement est voulu dans la plupart des cas, il peut arriver que l'administrateur souhaite partager des chemins d'AS privés avec un voisin eBGP.

  Solution : aucune solution n'est disponible pour que le dispositif Edge annonce tous les chemins d'AS dans la mise à jour de BGP.

- **Problème 1461421 : la sortie de la commande « show ip bgp neighbor » pour NSX Edge conserve le nombre historique de connexions précédemment établies**
  La commande « show ip bgp neighbor » affiche le nombre de fois que la machine d'état BGP est passée à l'état Établi pour un homologue donné. La modification du mot de passe utilisé avec l'authentification MD5 entraîne la destruction et la recréation de la connexion homologue, ce qui en retour effacera les compteurs. Ce problème ne se produit pas avec un DLR Edge.

  Solution : pour effacer les compteurs, exécutez la commande « clear ip bgp neighbor ».

- **Problème 1656713 : Comme des stratégies de sécurité IPsec sont manquantes sur l'instance de NSX Edge après le basculement HA, le trafic ne peut pas circuler dans le tunnel**
  Le basculement **Veille>Actif** ne fonctionnera pas pour le trafic circulant sur les tunnels IPsec.

  Solution : désactivez/activez IPsec après la commutation NSX Edge.

- **Problème 1354824 : Lorsqu'une VM Edge est endommagée ou inaccessible à cause, par exemple, d'une coupure de courant, des événements système sont générés lorsque la vérification de l'intégrité par NSX Manager échoue**
  L'onglet des événements système signalera des événements « Inaccessibilité d'Edge ». La liste des dispositifs NSX Edge peut continuer à signaler l'état Déployé.

  Solution : pour obtenir des informations d'état détaillées sur un dispositif NSX Edge, utilisez l'API suivante :

  ```
  GET https://NSX-Manager-IP-Address/api/4.0/edges/edgeId/status?detailedStatus=true
  ```

- **Problème 1647657 : Lorsque des commandes sont affichées sur un hôte ESXi avec DLR (routeur logique distribué), 2 000 itinéraires s'affichent par instance de DLR au maximum**

  Lorsque des commandes sont affichées sur un hôte ESXi avec DLR activé, 2 000 itinéraires s'affichent par instance de DLR au maximum, même si plus d'itinéraires peuvent être en cours d'exécution. Ce problème est lié à l'affichage et le chemin de données fonctionnera comme prévu pour tous les itinéraires.

  Solution : aucune.

- **Problème 1634215 : La sortie des commandes CLI OSPF n'indique pas si le routage est désactivé**
  Lorsqu'OSPF est désactivé, la sortie des commandes CLI de routage n'affiche aucun message indiquant *« OSPF est désactivé »*. La sortie est vide.

  Solution : La commande *show ip ospf* affichera l'état correct.

- **Problème 1647739 : Redéployer une VM Edge après une opération vMotion entraînera le déplacement du dispositif Edge ou de la VM du DLR sur le cluster d'origine.**
  Solution : pour placer la VM Edge dans un pool de ressources ou un cluster différent, utilisez l'interface utilisateur de NSX Manager pour configurer l'emplacement souhaité.

- **Problème 1463856 : Lorsque NSX Edge Firewall est activé, les connexions TCP existantes sont bloquées**
  Les connexions TCP sont bloquées via le pare-feu d'état Edge, car l'établissement de liaison tridirectionnelle initial n'est pas visible.
  Solution : pour gérer ce type de flux existants, procédez comme suit. Utilisez l'API REST de NSX pour activer l'indicateur tcpPickOngoingConnections dans la configuration globale de pare-feu. Le pare-feu passe du mode strict au mode tolérant. Activez ensuite le pare-feu. Lorsque les connexions existantes sont choisies (cela peut prendre quelques minutes après l'activation du pare-feu), vous pouvez désactiver l'indicateur tcpPickOngoingConnections pour replacer le pare-feu en mode strict. (Ce paramètre est persistant.)

  ```
  PUT /api/4.0/edges/{edgeId}/firewall/config/global

  <globalConfig>
  <tcpPickOngoingConnections>true</tcpPickOngoingConnections>
  </globalConfig>
  ```

- **Problème 1374523 : Redémarrez ESXi ou exécutez *[services.sh restart]* après l'installation d'un VIB VXLAN pour rendre les commandes VXLAN disponibles à l'aide d'esxcli**

Après l'installation d'un VIB VXLAN, vous devez redémarrer ESXi ou exécuter la commande *[services.sh restart]* pour que les commandes VXLAN soient disponibles à l'aide d'esxcli.

Solution : utilisez localcli plutôt qu'esxcli.

- **Problème 1525003 : La restauration d'une sauvegarde NSX Manager avec une phrase secrète incorrecte échouera en mode silencieux, car des dossiers racine critiques ne sont pas accessibles**
  Solution : aucune.

- **Problème 1637639 : Lorsque le client PHAT SSL VPN de Windows 8 est utilisé, l'adresse IP virtuelle n'est pas attribuée à partir du pool d'adresses IP**
  Sous Windows 8, l'adresse IP virtuelle n'est pas attribuée comme prévu depuis le pool d'adresses IP lorsqu'une nouvelle adresse IP est attribuée par la passerelle Edge Services Gateway ou lorsque le pool d'adresses IP change pour utiliser une plage d'adresses IP différente.
  Solution : ce problème ne se produit que sous Windows 8. Utilisez un système d'exploitation Windows différent pour éviter ce problème.

- **Problème 1628220 : Les observations DFW ou NetX ne sont pas visibles du côté du récepteur**
  Traceflow peut ne pas afficher des observations DFW et NetX du côté du récepteur si le port de commutateur associé à la vNIC de destination a été modifié. Le problème ne sera pas résolu pour les versions vSphere 5.5. Pour vSphere 6.0 et versions ultérieures, ce problème n'existe pas.
  Solution : ne désactivez pas la vNIC. Redémarrez la VM.

- **Problème 1483426 : L'état de service IPsec et VPN L2 apparaît comme étant inactif même lorsque le service n'est pas activé**
  Dans l'onglet Paramètres de l'interface utilisateur, l'état de service L2 apparaît comme étant inactif alors que l'API indique qu'il est actif. Le service VPN L2 et IPsec apparaît toujours comme étant inactif dans l'onglet Paramètres tant que la page de l'interface utilisateur n'est pas actualisée.
  Solution : actualisez la page.

- **Problème 1446327 : Certaines applications TCP peuvent expirer lors de la connexion via NSX Edge**
  Le délai d'inactivité de connexion établie par TCP par défaut est de 3 600 secondes. NSX Edge supprime toutes les connexions inactives depuis plus longtemps que le délai d'inactivité et abandonne ces connexions.

  Solution :
  1. si l'application a un délai d'inactivité relativement long, activez les keepalives TCP sur les hôtes avec keep_alive_interval réglé sur moins de 3 600 secondes.
  2. Augmentez le délai d'inactivité TCP d'Edge sur plus de 2 heures à l'aide de l'API REST NSX suivant. Par exemple, pour augmenter le délai d'inactivité à 9 000 secondes. URL de NSX API :
     `/api/4.0/edges/{edgeId}/systemcontrol/config PUT Method <systemControl> <property>sysctl.net.netfilter.nf_conntrack_tcp_timeout_established=9000</property> </systemControl>`

- **Problème 1089238 : Impossible de configurer OSPF sur plusieurs liaisons montantes DLR Edge**
  Actuellement, il n'est pas possible de configurer OSPF sur plusieurs liaisons montantes DLR Edge. Cette limitation est due au partage d'une adresse de transfert unique par instance de DLR.
  Solution : il s'agit d'une limitation système actuelle et il n'existe pas de solution.

- **Problème 1499978 : Les messages de Syslog Edge n'atteignent pas le serveur Syslog distant**
  Tout de suite après le déploiement, le serveur Syslog Edge ne peut pas résoudre les noms d'hôte pour des serveurs Syslog distants configurés.
  Solution : configurez des serveurs syslog distants en utilisant leur adresse IP ou utilisez l'interface utilisateur pour forcer la synchronisation du dispositif Edge.

- **Problème 1489829 : Les paramètres de configuration du client DNS du routeur logique ne sont**

pas totalement appliqués après la mise à niveau de l'API Edge REST
Solution : lorsque vous utilisez l'API REST pour configurer le transitaire (résolveur) DNS, procédez comme suit :

1. Spécifiez les paramètres du serveur XML du client DNS pour qu'ils correspondent au paramètre du transitaire DNS.
2. Activez le transitaire DNS et assurez-vous que les paramètres du transitaire sont identiques aux paramètres du serveur du client DNS spécifiés dans la configuration XML.

- Problème 1243112 : Message de validation et d'erreur absents pour le prochain saut non valide sur l'itinéraire statique, ECMP activé
  Lorsque vous tentez d'ajouter un itinéraire statique avec ECMP activé, si la table de routage ne contient pas d'itinéraire par défaut et qu'il existe un prochain saut accessible sur la configuration de l'itinéraire statique, aucun message d'erreur ne s'affiche et l'itinéraire statique n'est pas installé.
  Solution : aucune.

- Problème 1281425 : si une machine virtuelle NSX Edge avec une sous-interface soutenue par un commutateur logique est supprimée via l'interface utilisateur vCenter Web Client, le chemin de données peut ne pas fonctionner pour une nouvelle machine virtuelle qui se connecte au même port
  Lorsque la machine virtuelle Edge est supprimée via l'interface utilisateur vCenter Web Client (plutôt qu'à partir de NSX Manager), la jonction VXLAN configurée sur dvPort sur le canal opaque n'est pas réinitialisée. Cela est dû au fait que la configuration de la jonction est gérée par NSX Manager.
  Solution : pour supprimer manuellement la configuration de la jonction VXLAN, procédez comme suit :

  1. Accédez à vCenter Managed Object Browser en tapant la commande suivante dans une fenêtre de navigateur :
     `https://<vc-ip>/mob?vmodl=1`
  2. Cliquez sur **Contenu**.
  3. Pour récupérer la valeur dvsUuid, procédez comme suit.
     a. Cliquez sur le lien rootFolder (par exemple, group-d1(Datacenters)).
     b. Cliquez sur le lien du nom du centre de données (par exemple, datacenter-1).
     c. Cliquez sur le lien networkFolder (par exemple, group-n6).
     d. Cliquez sur le lien du nom DVS (par exemple, dvs-1)
     e. Copiez la valeur d'uuid.
  4. Cliquez sur **DVSManager**, puis sur **updateOpaqueDataEx**.
  5. Dans *selectionSet*, ajoutez le code XML suivant.

     ```
     <selectionSet xsi:type="DVPortSelection">
       <dvsUuid>value</dvsUuid>
       <portKey>value</portKey> <!--port number of the DVPG where trunk vnic got
      connected-->
     </selectionSet>
     ```

  6. Dans *opaqueDataSpec*, ajoutez le code XML suivant

     ```
     <opaqueDataSpec>
       <operation>remove</operation>
       <opaqueData>
         <key>com.vmware.net.vxlan.trunkcfg</key>
         <opaqueData></opaqueData>
       </opaqueData>
     </opaqueDataSpec>
     ```

  7. Définissez **isRuntime** sur false.
  8. Cliquez sur **Appeler la méthode**.

9. Répétez les étapes 5 à 8 pour chaque port de jonction configuré sur la machine virtuelle Edge supprimée.

- **Problème 1637939 : Les certificats MD5 ne sont pas pris en charge lors du déploiement de passerelles matérielles**
  Lors du déploiement de commutateurs de passerelle matérielle sous forme de VTEP pour le pontage logique entre VLAN L2 et VXLAN, les commutateurs physiques prennent en charge au minimum des certificats SSL SHA1 pour la connexion OVSDB entre NSX Controller et le commutateur OVSDB.

  Solution : aucune.

- **Problème 1637943 : Aucune prise en charge des modes de réplication Hybride ou Multidiffusion pour les VNI avec une liaison de passerelle matérielle**
  Lorsqu'ils sont utilisés en tant que VTEP pour le pontage entre VXLAN L2 et VLAN, les commutateurs de passerelle matérielle ne prennent en charge que le mode de réplication Monodiffusion.

  Solution : utilisez uniquement le mode de réplication Monodiffusion.

Problèmes connus des services de sécurité

- **Problème 1918023 : L'USVM de Guest Introspection utilise 100 % de la mémoire**
  L'USVM de Guest Introspection utilise 100 % de la mémoire et peut entraîner la perte de connectivité des machines virtuelles invitées avec l'USVM de Guest Introspection.

  Solution : Consultez l'*article de la base de connaissances de VMware 2151235* pour plus d'informations et pour connaître les solutions.

- **Problème 1897878 : les tâches et événements ESXi affichent l'erreur « Communication avec le module ESX perdue »**
  Si le module Guest Introspection de l'hôte ESXi (EPSec Mux) perd la communication avec le module ESX, le message d'erreur « Communication avec le module ESX perdue » s'affiche sur les hôtes ESXi.

  Solution : Consultez l'*article de la base de connaissances de VMware 2151235* pour plus d'informations et pour connaître les solutions.

- **Problème 1944599 : Les adresses IP traduites ne sont pas ajoutées aux filtres vNIC ce qui entraîne l'abandon de trafic par le Pare-feu distribué**
  Lorsque de nouvelles machines virtuelles sont déployées, les filtres vNIC ne sont pas mis à jour avec le bon ensemble d'adresses IP, ce qui entraîne le blocage du trafic par le Pare-feu distribué.

  Solution :
  1. Forcez la synchronisation des règles de pare-feu distribué sur des clusters affectés avec les nouvelles machines virtuelles déployées. Reportez-vous à la section Forcer la synchronisation des règles de pare-feu.
  2. Cliquez sur Modifier dans le groupe de sécurité auquel il manque les adresses IP de VM et envoyez sans changement.

- **Problème 1854661 : Dans une installation cross-vCenter, les règles de pare-feu filtrées n'affichent pas la valeur d'index lorsque vous basculez entre des instances de NSX Manager**
  Lorsque vous appliquez un critère de filtre de règle à une instance de NSX Manager, puis que vous passez à une autre instance de NSX Manager, l'index de règle indique « 0 » pour toutes les règles filtrées au lieu d'afficher la position réelle de la règle.

  Solution : effacez le filtre pour afficher la position de la règle.

- **Problème 1846402 : Plusieurs adresses IP sur la même vNIC entraînent des retards de**

l'opération de publication du pare-feu
Le problème se produit lorsqu'une vNIC dispose de plusieurs adresses IP et que l'écoute ARP est activée. Chaque paquet de la vNIC peut provoquer un message d'ARP de l'hôte au gestionnaire avec l'adresse IP qui vient d'être découverte. Cela est dû au fait que l'hôte ne peut envoyer qu'une seule adresse IP écoutée par ARP au gestionnaire. Lorsque la vNIC bascule entre les adresses IP, l'hôte détecte l'adresse IP comme étant nouvelle et envoie le message écouté par ARP au gestionnaire. En général, cela entraîne de nombreux messages de conteneur sur NSX Manager, ce qui provoque des retards de la réalisation de la configuration du pare-feu sur l'hôte.

Solution : désactivez l'écoute ARP lorsque les vNIC disposent de plusieurs adresses IP. Utilisez plutôt l'écoute DHCP ou VMTools.

- Problème 1474650 : Pour les utilisateurs NetX, les hôtes ESXi 5.5.x et 6.x rencontrent un écran de diagnostic violet qui indique `ALERTE : NMI: 709: NMI IPI reçu`
  Lorsqu'un grand nombre de paquets est transmis ou reçu par une VM de service, DVFilter continue de monopoliser le CPU, ce qui entraîne des pertes de pulsation et un écran de diagnostic violet. Consultez l'*article 2149704 de la base de connaissances de VMware* pour plus d'informations.

  Solution : effectuez la mise à niveau de l'hôte ESXi vers n'importe laquelle des versions ESXi suivantes qui sont le minimum requis pour utiliser NetX :

  - 5.5 correctif 10
  - ESXi 6.0U3
  - ESXi 6.5
- Problème 1799543 : Après la mise à niveau de NSX 6.2.x vers NSX 6.3.0, vSphere Web Client s'affiche de façon erronée et vous permet de sélectionner des groupes de sécurité universelle NSX 6.2.x et des groupes de sécurité universelle non actif-veille lorsque vous créez le premier groupe de sécurité universelle actif-veille.
  Lorsque vous créez le tout premier groupe de sécurité universelle actif-veille, l'interface utilisateur de vSphere Web Client s'affiche et vous permet d'ajouter un groupe de sécurité universelle créé sur NSX 6.2.x. L'opération échoue avec l'erreur « Le membre demandé n'est pas un membre valide ».

  Solution : créez au moins un groupe de sécurité universelle actif-veille et, lors de la création du groupe de sécurité universelle actif-veille suivant, ce problème ne se produira pas.

- Problème 1787680 : La suppression de la section de pare-feu universel échoue lorsque NSX Manager est en mode Transit
  Lorsque vous essayez de supprimer une section de pare-feu universel de l'interface utilisateur de NSX Manager en mode Transit et de publier, la publication échoue et, par conséquent, vous ne pouvez pas définir NSX Manager en mode Autonome.

  Solution : utilisez l'API REST Supprimer une section pour supprimer la section de pare-feu universel.

- Problème 1741844 : L'utilisation de l'écoute ARP pour détecter l'adresse d'une vNIC avec plusieurs adresses IP entraîne une consommation de CPU de 100 %
  Ce problème se produit lorsque la vNIC d'une machine virtuelle est configurée avec plusieurs adresses IP et que l'écoute ARP est activée pour la détection d'adresses IP. Le module de découverte d'adresses IP continue d'envoyer sans arrêt des mises à jour vNIC-adresse IP au dispositif NSX Manager afin de modifier le mappage vNIC-adresse IP pour toutes les VM configurées avec plusieurs adresses IP.

  Solution : Il n'existe pas de solution. Actuellement, la fonctionnalité d'écoute ARP ne prend en charge qu'une seule adresse IP par vNIC. Pour plus d'informations, consultez la section Découverte d'adresses IP pour les machines virtuelles dans le *Guide d'administration de NSX*.

- Problème 1689159 : La fonctionnalité d'ajout de règle dans Flow Monitoring ne fonctionne pas correctement pour les flux ICMP.
  Lors de l'ajout d'une règle à partir de Flow Monitoring, le champ Services reste vide si vous ne le définissez pas explicitement sur ICMP. Par conséquent, vous pouvez finir par ajouter une règle avec le type de service « ANY ».

Solution : mettez à jour le champ Services pour refléter le trafic ICMP.

- **Problème 1632235 : Lors de l'installation de Guest Introspection, la liste déroulante du réseau n'affiche que « Spécifié sur l'hôte »**
  Lors de l'installation de Guest Introspection avec la licence antivirus uniquement de NSX et la licence Essential ou Standard de vSphere, la liste déroulante du réseau n'affiche que la liste existante de groupes de ports DV. Cette licence ne prend pas en charge la création de DVS.
  Solution : avant d'installer Guest Introspection sur un hôte vSphere avec l'une de ces licences, spécifiez d'abord le réseau dans la fenêtre « Paramètres de la VM agent ».

- **Problème 1652155 : La création ou la migration de règles de pare-feu utilisant des API REST peut échouer sous certaines conditions et signaler l'erreur HTTP 404**
  L'ajout ou la migration de règles de pare-feu utilisant des API REST n'est pas pris(e) en charge sous ces conditions :

  - Création de règles de pare-feu sous forme d'une opération en bloc quand autosavedraft=true est défini.
  - Ajout simultané de règles de pare-feu dans des sections.

  Solution : définissez le paramètre autoSaveDraft sur false dans l'appel API lors de la création ou de la migration de règles de pare-feu en bloc.

- **Problème 1509687 : L'URL peut contenir au maximum 16 000 caractères lors de l'attribution d'une seule balise de sécurité à plusieurs VM en même temps dans un appel API**
  Une seule balise de sécurité ne peut pas être attribuée à un grand nombre de VM en même temps avec une seule API si l'URL contient plus de 16 000 caractères.
  Solution : pour optimiser les performances, balisez jusqu'à 500 VM dans un seul appel.

- **Problème 1662020 : L'opération de publication peut échouer avec le message d'erreur « La dernière publication a échoué sur l'hôte *numéro de l'hôte* » sur l'interface utilisateur de DFW dans les sections Général et Services de sécurité partenaires**
  Après la modification d'une règle, l'interface utilisateur affiche « La dernière publication a échoué sur l'hôte *numéro de l'hôte* ». Les hôtes répertoriés sur l'interface utilisateur ne disposent peut-être pas de la version correcte des règles de pare-feu, ce qui entraîne un manque de sécurité et/ou une interruption du réseau.

  En général, le problème a lieu dans les scénarios suivants :

  - Après la mise à niveau d'une version antérieure de NSXv vers la dernière version.
  - Sortie d'un hôte du cluster et retour dedans.
  - Déplacement d'un hôte d'un cluster à un autre.

  Solution : pour récupérer, vous devez forcer la synchronisation des clusters affectés (pare-feu uniquement).

- **Problème 1481522 : La migration des ébauches de règle de pare-feu entre 6.1.x et 6.2.3 n'est pas prise en charge, car les ébauches ne sont pas compatibles entre les versions**

  Solution : aucune.

- **Problème 1628679 : Avec le pare-feu basé sur l'identité, la VM d'utilisateurs supprimés fait toujours partie du groupe de sécurité**

  Lorsqu'un utilisateur est supprimé d'un groupe sur le serveur AD, la VM sur laquelle l'utilisateur est connecté fait toujours partie du groupe de sécurité. Cela conserve les stratégies de pare-feu de la vNIC de VM sur l'hyperviseur, ce qui octroie à l'utilisateur un accès complet aux services.

  Solution : aucune. Ce comportement est normalement prévu.

- **Problème 1496273 : L'interface utilisateur permet de créer des règles entrantes/sortantes de pare-feu NSX qui ne peuvent pas s'appliquer aux dispositifs Edge**

Le client Web autorise de manière incorrecte la création d'une règle de pare-feu NSX appliquée à un ou plusieurs dispositifs NSX Edge lorsque la règle permet d'acheminer le trafic dans le sens entrant ou sortant et lorsque PacketType est IPV4 ou IPV6. L'interface utilisateur ne devrait pas autoriser la création de ce type de règles, du fait que NSX ne peut pas les appliquer aux dispositifs NSX Edge.
Solution : aucune.

- **Problème 1557924 : Le commutateur logique universel est autorisé à être consommé dans le champ appliedTo d'une règle DFW locale**
  Lorsqu'un commutateur logique universel est utilisé comme membre d'un groupe de sécurité, la règle DFW peut utiliser ce groupe de sécurité dans le champ AppliedTo. Cela applique indirectement la règle sur le commutateur logique universel, ce qui ne devrait pas être autorisé car cela peut entraîner le comportement inconnu de ces règles.

  Solution : aucune.

- **Problème 1559971 : Liste d'exclusion de pare-feu cross-vCenter NSX non publiée si le pare-feu est désactivé sur un cluster**
  Dans cross-vCenter NSX, la liste d'exclusion de pare-feu n'est publiée sur aucun cluster lorsque le pare-feu est désactivé sur l'un des clusters.
  Solution : forcez la synchronisation des dispositifs NSX Edge affectés.

- **Problème 1407920 : La republication de la règle de pare-feu échoue après l'utilisation de l'API DELETE**
  Si vous supprimez la totalité de la configuration du pare-feu par la méthode de l'API DELETE, et que vous essayez ensuite de republier toutes les règles d'un projet de règles de pare-feu enregistré, la publication des règles échouera.
- **Problème 1494718 : De nouvelles règles de pare-feu universelles ne peuvent pas être créées et des règles universelles existantes ne peuvent pas être modifiées à partir de l'interface utilisateur de la surveillance de flux**
  Solution : les règles universelles ne peuvent pas être ajoutées ni modifiées à partir de l'interface utilisateur Flow Monitoring. EditRule sera automatiquement désactivé.

- **Problème 1442379 : Configuration du pare-feu de Service Composer non synchronisée**
  Dans NSX service composer, si une stratégie de pare-feu n'est pas valide (par exemple, si vous avez supprimé un groupe de sécurité utilisé par une stratégie de pare-feu), la suppression ou la modification d'une autre stratégie de pare-feu désynchronise Service Composer et le message d'erreur suivant s'affiche : `Firewall configuration is not in sync` (La configuration du pare-feu n'est pas synchronisée).
  Solution : supprimez les stratégies de pare-feu non valides, puis synchronisez la configuration du pare-feu. Sélectionnez **Service Composer** : **Stratégies de sécurité**, puis pour chaque stratégie de sécurité ayant des stratégies de pare-feu associées, cliquez sur **Actions** et sélectionnez **Synchroniser la configuration du pare-feu**. Pour éviter ce problème, corrigez ou supprimez toujours les configurations de pare-feu non valides avant d'appliquer d'autres modifications à la configuration du pare-feu.

- **Problème 1066277 : Le nom d'une stratégie de sécurité ne peut pas excéder 229 caractères**
  Le champ du nom d'une stratégie de sécurité dans l'onglet Stratégie de sécurité de Service Composer peut accepter jusqu'à 229 caractères. Cela est dû au fait que les noms des stratégies sont préparés en interne avec un préfixe.
  Solution : aucune.

- **Problème 1443344 : Certaines versions de la série VM de réseaux tiers ne fonctionnent pas avec les paramètres par défaut de NSX Manager**
  Certains composants de NSX 6.1.4 ou versions ultérieures désactivent par défaut le protocole SSLv3. Avant de procéder à la mise à niveau, vérifiez que toutes les solutions tierces intégrées à votre déploiement de NSX ne reposent *pas* sur la transmission SSLv3. Ainsi, certaines versions de la solution de la série VM de Palo Alto Networks requièrent la prise en charge de SSLv3. Vérifiez auprès de vos fournisseurs leurs exigences en matière de version.

- **Problème 1660718 : L'état de stratégie de Service Composer indique « En cours » sur l'interface utilisateur et « En attente » dans la sortie d'API**

  Solution : aucune.

- **Problème 1620491 : L'état de synchronisation de niveau de stratégie dans Service Composer n'indique pas l'état de publication des règles dans une stratégie**

  Lorsqu'une stratégie est créée ou modifiée, Service Composer affiche un état de réussite qui indique uniquement l'état de persistance. Il n'indique pas si les règles ont été publiées correctement sur l'hôte.
  Solution : utilisez l'interface utilisateur du pare-feu pour voir l'état de publication.

- **Problème 1317814 : Service Composer n'est pas synchronisé lorsque des modifications de la stratégie sont effectuées alors qu'une instance de Service Manager est en panne**
  Lorsqu'une stratégie est modifiée alors que l'une des instances de Service Manager est en panne, les modifications échoueront et Service Composer sera désynchronisé.
  Solution : vérifiez que Service Manager réponde, puis publiez une synchronisation forcée à partir de Service Composer.

- **Problème 1070905 : impossible de supprimer et de rajouter un hôte à un cluster protégé par Guest Introspection et par des solutions de sécurité tierces**
  Si vous supprimez un hôte d'un cluster protégé par Guest Introspection et par des solutions de sécurité tierces en le déconnectant, puis en le supprimant de vCenter Server, vous pouvez rencontrer des problèmes si vous essayez de rajouter le même hôte au même cluster.
  Solution : Pour supprimer un hôte d'un cluster protégé, placez tout d'abord l'hôte en mode de maintenance. Placez ensuite l'hôte dans un cluster non protégé ou en dehors de l'ensemble des clusters, puis déconnectez-le et supprimez-le.

- **Problème 1648578 : NSX force l'ajout de cluster/réseau/stockage lors de la création d'une instance de service basé sur l'hôte NetX**
  Lorsque vous créez une instance de service à partir de vSphere Web Client pour des services basés sur l'hôte NetX tels que Pare-feu, ID et Adresses IP, vous êtes obligé d'ajouter cluster/réseau/stockage même si ces éléments ne sont pas obligatoires.

  Solution : lors de la création d'une instance de service, vous pouvez ajouter des informations pour cluster/réseau/stockage afin de remplir les champs. Cela permet de créer l'instance de service et vous pourrez continuer comme prévu.

- **Problème 1772504 : Service Composer ne prend pas en charge les groupes de sécurité avec un ensemble MAC**
  Service Composer autorise l'utilisation de groupes de sécurité dans des configurations de stratégie. S'il existe un groupe de sécurité contenant un ensemble MAC, Service Composer accepte ce groupe de sécurité sans problème, mais ne parvient pas à appliquer des règles pour cet ensemble MAC spécifique. Cela s'explique par le fait que Service Composer fonctionne sur une couche 3 et qu'il ne prend pas en charge les constructions de couche 2. Notez que si un groupe de sécurité dispose d'un ensemble d'IP et d'un ensemble MAC, l'ensemble d'IP sera toujours effectif, mais l'ensemble MAC sera ignoré. Il n'y a aucun risque à faire référence à un groupe de sécurité contenant un ensemble MAC ; l'utilisateur doit savoir que l'ensemble MAC sera ignoré.

  Solution : si l'intention de l'utilisateur est de créer des règles de pare-feu utilisant un ensemble MAC, il doit utiliser une configuration DFW couche 2/Ethernet au lieu de Service Composer.

- **Problème 1718726 : impossible d'effectuer une synchronisation forcée de Service Composer après la suppression manuelle de la section Stratégie de Service Composer avec DFW REST API**
  Dans un environnement cross-vCenter NSX, un utilisateur qui tente d'effectuer une synchronisation forcée de la configuration de NSX Service Composer échouera s'il a précédemment supprimé la seule section Stratégie existante (gérée par Service Composer) via un appel REST API.

Solution : ne supprimez pas la section Stratégie gérée par Service Composer via un appel REST API. (Notez que l'interface utilisateur empêche déjà la suppression de cette section.)

Problèmes connus des services de surveillance

- **Problème 1466790 : Impossible de choisir les VM sur le réseau ponté à l'aide de l'outil NSX Traceflow**
  Vous ne pouvez pas sélectionner de VM qui ne sont pas associées à un commutateur logique à l'aide de l'outil NSX Traceflow. Autrement dit, les VM d'un réseau ponté L2 ne peuvent pas être choisies par nom de VM comme adresse source ou adresse de destination pour l'inspection Traceflow.

  Solution : pour les VM associées à des réseaux pontés L2, utilisez l'adresse IP ou l'adresse MAC de l'interface que vous souhaitez spécifier comme destination d'inspection Traceflow. Vous ne pouvez pas choisir des VM associées à des réseaux pontés L2 comme source. Pour plus d'informations, consultez l'article 2129191 de la base de connaissances.

Problèmes connus d'interopérabilité entre les solutions

- **Problème 1568861 : Le déploiement de NSX Edge échoue lors du déploiement d'un dispositif Edge depuis une cellule vCloud Director qui ne possède pas l'écouteur vCenter**

  Le déploiement de NSX Edge échoue lors du déploiement d'un dispositif Edge depuis une cellule vCloud Director qui ne possède pas l'écouteur vCenter. De plus, les actions de NSX Edge, notamment un redéploiement, échouent à partir de vCloud Director.

  Solution : déployez un dispositif NSX Edge depuis la cellule vCloud Director qui possède l'écouteur vCenter.