Notes de mise à jour de VMware NSX for vSphere 6.3.0

VMware NSX for vSphere 6.3.0 | Publié le 2 février 2017 | Build 5007049

Contenu des notes de mise à jour

Les notes de mise à jour couvrent les sujets suivants :

Nouveautés

Les nouvelles fonctionnalités de NSX 6.3.0 peuvent être divisées selon les catégories suivantes :

Plate-forme et fonctionnalités de conformité

- Côté plate-forme :
    - **Améliorations de DFW actif-veille dans cross-vCenter NSX** : NSX 6.3.0 présente les améliorations suivantes :
        - Plusieurs sections de DFW universel sont maintenant prises en charge. Les règles Universel et Local peuvent utiliser des groupes de sécurité dans les champs **Source**, **Destination** et **AppliedTo**.
        - Groupes de sécurité universels : l'appartenance au groupe de sécurité universel peut être définie de manière statique ou dynamique. L'appartenance statique est activée en ajoutant manuellement une balise de sécurité universelle à chaque VM. L'appartenance dynamique est activée en ajoutant des VM en tant que membres en fonction de critères dynamiques (nom de VM).

        - Balises de sécurité universelle : vous pouvez maintenant définir des balises de sécurité universelle sur l'instance principale de NSX Manager et les marquer pour synchronisation universelle avec des instances secondaires de NSX Manager. Les balises de sécurité universelle peuvent être attribuées à des VM de façon statique, en fonction d'une sélection d'ID unique, ou de façon dynamique, en réponse à des critères tels que des analyses d'antivirus ou de vulnérabilité.

        - Critères de sélection d'ID unique : dans les versions antérieures de NSX, les balises de sécurité sont locales pour une instance de NSX Manager, et elles sont mappées à des VM à l'aide de l'ID d'objet géré de la VM. Dans un environnement actif-veille, l'ID d'objet géré d'une VM donnée peut être différent dans les centres de données actifs et en veille. NSX 6.3.x vous permet de configurer des critères de sélection d'ID unique sur l'instance principale de NSX Manager à utiliser pour identifier des VM lors de l'association à des balises de sécurité universelle : UUID d'instance de VM, UUID BIOS de VM, nom de VM ou une combinaison de ces options. Consultez Sélection d'ID unique dans le *Guide d'administration de NSX* pour plus d'informations.

    - **Récupération automatique de l'agent du plan de contrôle (netcpa)** : un mécanisme de récupération automatique amélioré pour le processus netcpa assure la communication continue du chemin de données. De plus, le processus de surveillance netcpa automatique redémarre automatiquement en cas de problème et envoie des alertes via le serveur Syslog. Résumé des avantages :

        - surveillance du processus netcpa automatique
        - redémarrage automatique du processus en cas de problème, par exemple, si le système se bloque
        - génération automatique du fichier de base pour le débogage
        - alerte via Syslog pour l'événement de redémarrage automatique

    - **Compatibilité de vSphere 6.5** : NSX 6.3.0 introduit la prise en charge de vSphere 6.5a et versions ultérieures. NSX 6.3.0 conserve la compatibilité avec vSphere 5.5 et 6.0.

    - Version d'évaluation technique :**Mode CDO (Controller Disconnected Operation)** : le mode CDO (Controller Disconnected Operation) a été introduit en tant que fonctionnalité de la version d'évaluation technique. Ce mode garantit que la connectivité du plan de données n'est pas affectée lorsque les hôtes perdent la connectivité avec le contrôleur. Consultez la section Mode CDO (Controller Disconnected Operation) dans le *Guide d'administration de NSX.* Consultez également le problème 1803220.

- Fonctionnalité de conformité :

    - **FIPS** : NSX 6.3.0 dispose d'un mode FIPS qui utilise uniquement les suites de chiffrement compatibles avec la norme FIPS. NSX Manager et NSX Edge disposent d'un mode FIPS pouvant être activé via vSphere Web Client ou l'API REST NSX. Consultez Différence de fonctionnalité entre le mode FIPS et le mode non-FIPS dans le *Guide d'administration de NSX* pour voir une liste de fonctionnalités affectées par le mode FIPS.

      Remarque : les partenaires de développement de VMware sont en train de faire certifier de nouvelles solutions de partenaire compatibles avec FIPS pouvant être utilisées dans NSX. Les connexions sortantes de NSX 6.3.0 sont de type TLS 1.1 ou supérieur, et elles n'utilisent que des suites de chiffrement approuvées FIPS. Cela signifie que les dispositifs de partenaire qui reçoivent des rappels doivent configurer des écouteurs Web sécurisés sur des suites de chiffrement plus sécurisées. Voici des chiffrements en mode Par défaut et en mode FIPS :

- Chiffrements en mode Par défaut : (Mode FIPS désactivé)
  `[TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384, TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384, TLS_DHE_RSA_WITH_AES_256_CBC_SHA256, TLS_DHE_DSS_WITH_AES_256_CBC_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA, TLS_ECDH_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_DSS_WITH_AES_256_CBC_SHA, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256, TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256, TLS_DHE_RSA_WITH_AES_128_CBC_SHA256, TLS_DHE_DSS_WITH_AES_128_CBC_SHA256, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA, TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA, TLS_ECDH_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA, TLS_EMPTY_RENEGOTIATION_INFO_SCSV]`
- Chiffrements en mode FIPS : `[TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA]`

Les modes Par défaut et FIPS prennent en charge les protocoles TLS 1.1 et 1.2. Consultez le Guide de compatibilité de VMware pour vérifier si des solutions de partenaire sont certifiées pour le mode FIPS.

- **Critères communs** : pour la conformité des critères communs, NSX a été testé pour la conformité avec le niveau d'assurance EAL2+. L'exécution d'une installation NSX conforme aux critères communs requiert que vous configuriez NSX comme l'explique le document Configuration de NSX pour les critères communs. dans le cadre du *Guide d'administration de NSX*.

- **ICSA** : il s'agit d'une certification de normes reconnue dans l'industrie qui teste et certifie des produits tels que les antivirus, les pare-feu, VPN IPSec, la cryptographie, VPN SSL, IPS réseau, les logiciels anti-espion et les pare-feu pour PC. Distributed Firewall et Edge Firewall sont certifiés avec les critères ICSA Corporate Firewall.

- **Changement du format de journal de paquet DFW en raison d'une exigence de certification ICSA** : NSX 6.3.0 introduit un changement apporté aux journaux de paquet DFW. Dans les versions 6.3.0 et ultérieures, nous incluons le type et le code ICMP pour répondre aux exigences de certification ICSA.

  Voici à quoi ressemblait le journal avant la version 6.3.0, sans code ni type ICMP :

  ```
  2016-09-29T20:52:21.983Z 6673 INET6 match PASS domain-c27/1001 IN 96 ICMP
  ```

```
fe80:0:0:0:21d:b502:f984:c601->ff02:0:0:0:0:0:0:1
```

Dans les versions 6.3.0 et ultérieures, il ressemble à ce qui suit, avec le code et le type ICMP. Dans cet exemple, 8 est le code et 0 est le type :

```
2016-09-29T20:54:16.051Z 42991 INET match PASS domain-c27/1001 IN 84 ICMP 8
0 10.113.226.5->10.28.79.55
```

Améliorations des opérations

- **Dépannage du tableau de bord** : le tableau de bord de NSX est mis à jour dans NSX 6.3.0 pour inclure davantage de fonctionnalités, telles que l'état du déploiement du service, l'état de sauvegardes de NSX Manager et les notifications du dispositif Edge.
- **Balisage de sécurité** : cela permet d'attribuer et d'effacer plusieurs balises pour une VM donnée via des appels API.
- **Améliorations de Syslog** : une nouvelle mise à jour de Syslog est disponible spécifiquement pour l'équilibrage de charge.
- **Pack de contenu Log Insight** : il a été mis à jour pour que l'équilibrage de charge fournisse un tableau de bord centralisé, une surveillance de bout en bout et une meilleure planification des capacités à partir de l'interface utilisateur.
- **Contrôle d'accès basé sur les rôles** : cette fonctionnalité limite la gestion des utilisateurs aux seuls administrateurs d'entreprise. Par conséquent, l'administrateur NSX n'aura plus l'autorisation de créer des utilisateurs ou d'attribuer des rôles aux nouveaux utilisateurs. D'un point de vue sécurité, elle permet de créer une démarcation claire de ces deux rôles d'administration.
- **État Drainage pour les membres de pool de l'équilibrage de charge** : vous pouvez maintenant mettre un membre de pool en état *Drainage*, ce qui force le serveur à s'arrêter normalement pour des opérations de maintenance. Définir un membre de pool sur l'état de drainage supprime le serveur principal de l'équilibrage de charge, mais permet toujours au serveur d'accepter de nouvelles connexions persistantes.

Améliorations du service et du routage

- **Prise en charge d'ASN à 4 octets pour BGP** : la configuration de BGP avec la prise en charge d'ASN à 4 octets est rendue possible grâce à la compatibilité descendante pour les homologues BGP ASN 2 octets préexistants.
- **Amélioration de NAT pour la correspondance 5-tuple** : pour offrir une configuration et une flexibilité plus granulaires pour les règles NAT, une prise en charge de correspondance 5-tuple est disponible pour NSX 6.3.0 :
  - Les critères de correspondance sont basés sur cinq paramètres : protocole, adresse IP source, port source, adresse IP de destination et port de destination.
  - L'interface utilisateur a été modifiée pour vous permettre de spécifier plus facilement des configurations SNAT/DNAT. Lors de la modification de configurations DNAT/SNAT sur d'anciennes versions d'Edge, l'interface utilisateur affiche toujours l'ancien style de volets.
  - L'API REST NSX ajoute des champs pour les nouveaux paramètres :

```
<natRules>
  <natRule>
  {...}
<!-- new fields applicable for DNAT -->
    <dnatMatchSourceAddress>any</dnatMatchSourceAddress>
    <dnatMatchSourcePort>any</dnatMatchSourcePort>
  </natRule>
```

```
    <natRule>
    {...}
<!-- new fields applicable for SNAT -->
      <snatMatchDestinationAddress>any</snatMatchDestinationAddress>
      <snatMatchDestinationPort>any</snatMatchDestinationPort>
    </natRule>
</natRules>
```

- **Amélioration des performances du VPN de couche 2 :** les performances du VPN de couche 2 ont été améliorées. Cela permet à un dispositif Edge de prendre en charge un débit maximal de 1,5 Gb/s, ce qui est mieux que les 750 Mb/s précédents.
- **Amélioration de la configurabilité pour OSPF :** lors de la configuration d'OSPF sur Edge Services Gateway (ESG), NSSA peut traduire tous les LSA de type 7 en LSA de type 5.

Améliorations de la sécurité

Plusieurs améliorations ont été apportées à Distributed Firewall :

- **Temporisateurs DFW :** NSX 6.3.0 introduit des temporisateurs de session qui définissent la durée pendant laquelle une session est maintenue sur le pare-feu une fois qu'elle n'est plus active. Lorsque le délai d'expiration de la session pour le protocole expire, la session se ferme. Sur le pare-feu, vous pouvez définir des délais d'expiration pour les sessions TCP, UDP et ICMP et les appliquer à un ensemble de VM ou de vNIC défini par l'utilisateur. Consultez Temporisateurs de session dans le *Guide d'administration de NSX*.
- **Nouvelles fonctionnalités pour prendre en charge la micro-segmentation** : pour prendre en charge la micro-segmentation dans les outils de visibilité et de planification, deux nouvelles fonctionnalités ont été introduites :
    - Le Gestionnaire de règles d'application simplifie le processus de création des groupes de sécurité et de création d'une liste blanche des règles de pare-feu pour les applications existantes.
    - La Surveillance de point de terminaison permet à un propriétaire d'application de profiler son application et d'identifier les processus créant les connexions réseau.
- **Support Linux pour Guest Introspection** : NSX 6.3.0 active Guest Introspection pour les VM Linux. Sur les VM invitées Linux, la fonctionnalité NSX Guest Introspection exploite les capacités `fanotify` et `inotify` fournies par le noyau Linux. Consultez Installer Guest Introspection pour Linux dans le *Guide d'administration de NSX* pour plus d'informations. Consultez Versions pour voir une liste des versions Linux prises en charge par NSX.
- **État de publication de Service Composer** : l'état de publication de Service Composer est maintenant disponible pour vérifier si une stratégie est synchronisée. Cela offre une meilleure visibilité des traductions de stratégie de sécurité en règles DFW sur l'hôte.

CMP (Cloud Management Platform) et intégration des partenaires

- Une meilleure interopérabilité entre vCloud Director 8.20 et NSX 6.3.0 permet aux fournisseurs de services d'offrir des services de mise en réseau et de sécurité avancés à leurs locataires. vCloud Director 8.20 avec NSX 6.3.0 démontre des capacités NSX natives pour la prise en charge de plusieurs locataires et un libre-service de locataire.
- NSX 6.3.0 prend en charge le nouveau plug-in vRO version 1.1, qui prend en charge vRA et introduit la capacité de prendre en charge d'autres applications non-vRA.
- NSX NetX 6.3.0 présente des améliorations de l'échelle et des performances liées à l'insertion de services.

Installation et mise à niveau

- **Modules de noyau NSX maintenant indépendants de la version d'ESXi :** à partir de NSX 6.3.0, les modules de noyau NSX n'utilisent que le VMKAPI disponible publiquement de sorte que les interfaces sont garanties dans toutes les versions. Cette amélioration permet de réduire le risque d'échec des mises à niveau de l'hôte en raison de versions de module de noyau incorrectes. Dans les versions antérieures, chaque mise à niveau d'ESXi dans un environnement NSX nécessitait au moins deux redémarrages pour s'assurer que la fonctionnalité NSX était toujours opérationnelle (car il fallait transférer les nouveaux modules de noyau pour chaque nouvelle version d'ESXi).
- NSX 6.3.0 vérifie également la disponibilité de NSX avant de sortir un hôte du mode de maintenance. Cela garantit que DRS ne déplace que les charges de travail vers un hôte où NSX est prêt. Cela évite la perte de mise en réseau pour certaines VM de charge de travail.
- **Paramètres OVF maintenant séparés par des virgules :** les paramètres OVF suivants qui étaient séparés par des espaces sont maintenant séparés par des virgules :
    - Liste des serveurs DNS (vsm_dns1_0)
    - Liste de recherche de domaines (vsm_domain_0)
    - Liste des serveurs NTP (vsm_ntp_0)

Sauvegarde et restauration

À partir de NSX 6.3.0, les chiffrements suivants sont pris en charge pour la sauvegarde SFTP :

- **Chiffrement :** `aes128-cbc`, `aes128-ctr`, `aes192-cbc`, `aes192-ctr`, `aes256-cbc`, `aes256-ctr`
- **Authentification de messages (mac) :** `hmac-sha2-256`
- **Échanges de clés :** `diffie-hellman-group-exchange-sha256`

Remarque : `hmac-sha1` n'est pas pris en charge, seul `sha2-hmac-256` est pris en charge. Si vous utilisez SFTP pour la sauvegarde, choisissez `sha2-hmac-256` après une mise à niveau vers la version 6.3.0. Consultez l'*article 2149282 de la base de connaissances de VMware* pour plus d'informations.

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.

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.
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)
vRealize Orchestrator	Plug-in NSX-vRO version 1.1.0 ou ultérieure.

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** : la fin de disponibilité (EOA) et la fin du support général (EOGS) ont eu lieu pour NSX for vSphere 6.1.x le 15 janvier 2017. (Consultez également l'*article 2144769 de la base de connaissances de VMware*.)
- Nouveaux**Suppression de NSX Data Security** : à partir de NSX 6.3.0, la fonctionnalité NSX Data Security est supprimée du produit.
- Nouveaux**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*.
- Nouveaux**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.
- Nouveaux**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**.
- Nouveaux**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 configuration de pare-feu ou section par défaut :

- 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`

Notes relatives aux mises à niveau

- Notes de mise à niveau concernant NSX et vSphere
- Notes de mise à niveau concernant les composants NSX
- Notes de mise à niveau concernant FIPS

Remarque : Si vous utilisez SFTP pour les sauvegardes NSX, reportez-vous à la section Sauvegarde et restauration pour une liste des algorithmes de sécurité pris en charge à partir de la version 6.3.x.

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.

Notes de mise à niveau concernant NSX et vSphere

- 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.

  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
- **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 6.3.0. Vous devez d'abord effectuer une mise à niveau vers une version 6.2.x prise en charge.
- **Mise à niveau vers vSphere 6.5a** : lors de la mise à niveau de vSphere 5.5 ou 6.0 vers vSphere 6.5a, vous devez d'abord effectuer la mise à niveau vers NSX 6.3.0. 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.
- **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.

- Si une passerelle matérielle (VTEP matériel) est installée dans votre environnement, la mise à niveau vers NSX 6.3.0 est bloquée. Vous devez contacter le support VMware pour continuer la mise à niveau. Consultez l'*article 2148511 de la base de connaissances de VMware* pour plus d'informations.
- **Réinitialiser vSphere Web Client** : Après avoir mis à niveau NSX Manager, vous devez réinitialiser le serveur vSphere Web Client tel que cela est décrit dans la *documentation de mise à niveau de NSX*. Tant que cette opération n'a pas été réalisée, l'onglet **Mise en réseau et sécurité** peut ne pas apparaître dans vSphere Web Client. Vous pouvez également avoir besoin de vider le cache ou l'historique du navigateur.
- **Environnements sans état** : Les mises à niveau de NSX dans un environnement d'hôtes sans état utilisent de nouvelles URL de VIB : 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 :

  1. Téléchargez manuellement les derniers VIB NSX depuis NSX Manager à partir d'une URL fixe.
  2. Ajoutez les VIB au profil d'image d'hôte.

  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 :

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

Notes de mise à niveau concernant les composants NSX

- **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 :

  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-dessous).

     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

- 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.

  Suivez la procédure ci-après pour vérifier que l'état de l'infrastructure de messagerie des hôtes où NSX Edge sera déployé s'affiche en VERT :

  - Utilisez la méthode API `GET /api/2.0/nwfabric/status?resource={resourceId}`, où **resourceId** est l'ID d'objet géré vCenter d'un cluster ou d'un hôte (par ex. domaine-c33 ou hôte-21). Reportez-vous à la section « Recherche d'ID d'objets VCenter » du *Guide de NSX API* pour obtenir des instructions sur la recherche d'ID de ressource pour les clusters et les hôtes.
  - Recherchez l'état correspondant à l'identifiant **featureId** de `com.vmware.vshield.vsm.messagingInfra` dans le corps de la réponse :

    ```
    <nwFabricFeatureStatus>
        <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
        <updateAvailable>false</updateAvailable>
        <status>GREEN</status>
        <installed>true</installed>
        <enabled>true</enabled>
        <allowConfiguration>false</allowConfiguration>
    </nwFabricFeatureStatus>
    ```

- **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).

- **Disposition du disque du contrôleur** : les mises à niveau à partir des versions 6.2.2 et antérieures ne recevront pas la nouvelle disposition de disque introduite dans 6.2.3 qui fournit des partitions de disque séparées pour des données et des journaux afin d'améliorer la stabilité du contrôleur.

- **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"
            }
```

- **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.

Notes de mise à niveau concernant 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 6.3.0. 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.

Problèmes connus

Les problèmes connus sont regroupés de la manière suivante :

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

Problèmes connus généraux

NouveauxProblème 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 1558285 : La suppression du cluster avec Guest Introspection de vCenter entraîne une exception de pointeur nulle
Des services, tels que Guest Introspection, doivent être supprimés avant la suppression d'un cluster de vCenter.

Solution : supprimez EAM Agency pour le déploiement de service sans cluster associé.

Problème 1629030 : L'interface de ligne de commande centrale de capture de paquets (déboguer et afficher la capture de paquets) requiert vSphere 5.5U3 ou version ultérieure
Ces commandes ne sont pas prises en charge dans les versions antérieures à vSphere 5.5.

Solution : VMware conseille à tous les clients NSX d'exécuter vSphere 5.5U3 ou version ultérieure.

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.

Nouveaux**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.

Nouveaux**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>
```

NouveauxProblème 1808478 : le service vsfwd ne parvient pas à démarrer si la mémoire vmvisor ne peut pas être allouée après la mise à niveau de NSX 6.2.x vers NSX 6.3.0
Le service vsfwd ne parvient pas à démarrer si la mémoire vmvisor ne peut pas être allouée après la mise à niveau de NSX 6.2.x vers NSX 6.3.0. Consultez l'article 2148974 de la base de connaissances de VMware pour plus d'informations.

Solution : contactez le support client VMware.

NouveauxProblème 1818257 : Les informations de VTEP ne sont pas signalées aux contrôleurs lorsque LACP étendu est utilisé pour VXLAN après la mise à niveau de l'hôte de NSX 6.2.x vers NSX 6.3.0 avec ESXi 6.0
Lors de la mise à niveau de NSX 6.2.x vers NSX 6.3.0 avec ESXi 6.0, après la mise à niveau de l'hôte, les informations de VTEP ne sont pas signalées aux contrôleurs lorsque LACP étendu est utilisé. Consultez l'article 2149210 de la base de connaissances de VMware pour plus d'informations.

Solution : contactez le support client VMware.

NouveauxProblème 1791371 : Lors de la mise à niveau d'hôtes ESXi vers vSphere 6.5a, si des VIB Guest Introspection et des VIB VXLAN sont mis à niveau en parallèle, une alarme est déclenchée
Les VIB Guest Introspection et les VIB VXLAN sont différents pour vSphere 6.5a et, lorsque vous les mettez à niveau en parallèle, la mise à niveau des VIB VXLAN déclenche une alarme demandant un redémarrage de l'hôte.

Solution : installez d'abord les VIB VXLAN, puis les VIB Guest Introspection lorsque vous effectuez la mise à niveau vers vSphere 6.5a.

NouveauxProblème 1805983 : Lorsque vous effectuez la mise à niveau vers NSX 6.2.5, 6.2.6 ou 6.3.0, les serveurs virtuels ne fonctionnent pas s'ils ne contiennent pas un pool de serveurs.
Les serveurs virtuels sans pool de serveurs ne peuvent servir que pour la redirection HTTP/HTTPS. Aucune autre fonctionnalité n'est opérationnelle.

Solution : créez un pool factice sans aucun membre et attribuez-le au serveur virtuel.

NouveauxProblème 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.

NouveauxProblème 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.

NouveauxProblème 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&gt:/api/2.0/nwfabric/configure?action=synchronize

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

Nouveaux**Problème 1802688 : La mise à niveau de NSX 6.2.x vers NSX 6.3.0 ne reflète pas l'état mis à jour d'activation du DFW**

Après la mise à niveau de NSX de la version 6.2.x à la version 6.3.0 et des VIB de cluster à 6.3.0 bits, lorsque vous ajoutez un nouvel hôte au cluster mis à niveau, l'état du pare-feu de l'hôte et du cluster concernés indique toujours occupé et l'état n'est pas mis à jour, même si les nouveaux VIB ont été installés sur le nouvel hôte.

Solution : procédez comme suit :

1. Exécutez l'appel API Synchronisation du bus de messages pour l'hôte avec l'API `POST https://<NSX-IP>/api/2.0/nwfabric/configure?action=synchronize`. Cela passera l'état de pare-feu de cet hôte et de ce cluster sur « `Disabled` ».

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

2. Maintenant, activez le pare-feu pour ce cluster dans l'interface utilisateur sur la page Installation > Préparation de l'hôte. Cela devrait passer tous les hôtes du cluster en mode d'activation du DFW.

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 format, 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 1660355 : Les VM migrées de 6.1.5 vers 6.2.3 et versions ultérieures ne prendront pas en charge TFTP ALG
Même si l'hôte est activé, les VM migrées de 6.1.5 vers 6.2.3 et versions ultérieures ne prendront pas en charge TFTP ALG

Solution : ajoutez et supprimez la VM de la liste d'exclusion ou redémarrez la VM, pour qu'un nouveau filtre 6.2.3 (et versions ultérieures) prenant en charge TFTP ALG soit créé.

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 1332563 : 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 1473537 : 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 1266433 : 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 1474066 : L'appel de l'API NSX REST pour activer ou désactiver la détection d'adresses IP semble n'avoir aucun effet
Si la préparation du cluster de l'hôte n'est pas encore terminée, l'appel de l'API NSX REST pour activer ou désactiver la détection de l'adresse IP `(https://<nsxmgr-ip>/api/2.0/xvs/networks/universalwire-5/features)` n'a aucun effet.

Solution : avant d'effectuer cet appel de l'API, assurez-vous que la préparation du cluster de l'hôte est terminée.

Problème 1459032 : Erreur lors de la configuration de la passerelle VXLAN
Lors de la configuration de VXLAN à l'aide d'un pool d'adresses IP statiques (sous **Mise en réseau et sécurité** -> **Installation** -> **Préparation de l'hôte** -> **Configurer VXLAN**) et si la configuration ne parvient pas à définir une adresse IP de passerelle de pool d'adresses IP sur VTEP (du fait que la passerelle n'est pas correctement configurée ou n'est pas accessible), la configuration de VXLAN passe à l'état Erreur (ROUGE) pour le cluster hôte.

Le message d'erreur est `La passerelle VXLAN ne peut pas être définie sur l'hôte` et le statut d'erreur est `VXLAN_GATEWAY_SETUP_FAILURE`. Dans l'appel de l'API REST, `GET https://<nsxmgr-ip>/api/2.0/nwfabric/status?resource=<cluster-moid>`, le statut de VXLAN est le suivant :

```
<nwFabricFeatureStatus>
  <featureId>com.vmware.vshield.nsxmgr.vxlan</featureId>
  <featureVersion>5.5</featureVersion>
  <updateAvailable>false</updateAvailable>
  <status>RED</status>
  <message>VXLAN Gateway cannot be set on host</message>
  <installed>true</installed>
  <enabled>true</enabled>
  <errorStatus>VXLAN_GATEWAY_SETUP_FAILURE</errorStatus>
</nwFabricFeatureStatus>
```

Solution : il existe deux options permettant de corriger l'erreur.

- Option 1 : supprimez la configuration de VXLAN pour le cluster hôte, corrigez l'installation de la passerelle sous-jacente dans le pool d'adresses IP en vous assurant que la passerelle est correctement configurée et qu'elle est accessible, puis reconfigurez VXLAN pour le cluster hôte.
- Option 2 : suivez les étapes décrites ci-dessous.
    1. Corrigez l'installation de passerelle sous-jacente dans le pool d'adresses IP en vous assurant que la passerelle est correctement configurée et qu'elle est accessible.
    2. Mettez l'hôte (ou les hôtes) en mode de maintenance pour s'assurer que le trafic de VM est actif sur l'hôte.
    3. Supprimez les VTEP VXLAN de l'hôte.
    4. Faites sortir l'hôte du mode de maintenance. La sortie de l'hôte du mode de maintenance déclenche le processus de création du VTEP VXLAN sur NSX Manager. NSX Manager tentera de recréer les VTEP requis sur l'hôte.

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 1485862 : La désinstallation de NSX d'un cluster d'hôte génère parfois une condition d'erreur
Lors de l'utilisation de l'action Désinstaller dans l'onglet **Installation** : **Préparation de l'hôte**, une erreur peut se produire en affichant le message `eam.issue.OrphanedAgency` dans les journaux EAM des hôtes. Après avoir utilisé l'option Résoudre et après avoir redémarré les hôtes, l'état d'erreur continue même si les VIB NSX ont été désinstallés.

Solution : supprimez l'agence orpheline de vSphere ESX Agent Manager (**Administration**: **vCenter Server Extensions**: **vSphere ESX Agent Manager**).

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 : Suivez les étapes ci-dessous.

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

Nouveaux**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 UDLR a déjà été supprimée du système**
Lorsque le 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 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 le routeur logique distribué universel n'est pas connecté à ce nouveau commutateur logique universel.

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

Nouveaux**Problème 1770436 : Alertes générées même lorsque l'adresse IP n'est pas en double**
Il arrive que la commande `arping` signale que l'adresse IP de NSX Manager est dupliquée sur le réseau, même si ce n'est pas le cas. Cela génère un faux positif.

Solution : contactez le support client VMware.

NouveauxProblème 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.

NouveauxProblème 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.

NouveauxProblème 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 : procédez comme suit :

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.

NouveauxProblème 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 1787542 : Les exceptions dans les journaux des instances secondaires de NSX Manager après la restauration de base de données sur l'instance principale de NSX Manager
Après la restauration de la base de données sur l'instance principale, les sections DFW universel rétablies ne sont pas visibles sur les instances secondaires de NSX Manager.

Solution : aucune. Redémarrez l'instance secondaire de NSX Manager à récupérer.

NouveauxProblème 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 NSX Manager, lors de la sélection d'un ou de plusieurs 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 :

suivez les étapes décrites ci-dessous :

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 1534877 : 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 1537258 : 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 : tous les NSX Manager doivent être mis 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 1477041 : La page Résumé du dispositif virtuel NSX Manager n'affiche aucun nom DNS
Lorsque vous vous connectez au dispositif virtuel NSX Manager, la page Résumé contient un champ pour le nom DNS. Ce champ reste vide même si un nom DNS a été défini pour le dispositif NSX Manager.

Solution : vous pouvez afficher le nom d'hôte et les domaines de recherche de NSX Manager sur la page Gérer : Réseau.

Problème 1492880 : 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 1468613 : 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 : suivez les étapes décrites ci-dessous :

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 1489768 : Changement de comportement de l'appel de l'API NSX REST pour ajouter un espace de noms à un centre de données
Dans NSX 6.2, l'appel REST API `POST https://<nsxmgr-ip>/api/2.0/namespace/datacenter/` renvoie une URL avec un chemin absolu, par exemple `http://198.51.100.3/api/2.0/namespace/api/2.0/namespace/datacenter/datacenter-1628/2`. Dans les versions précédentes de NSX, cet appel de l'API renvoyait une URL avec un chemin d'accès relatif, par exemple : `/api/2.0/namespace/datacenter/datacenter-1628/2`.

Solution : aucune.

Problèmes connus de mise en réseau logique et de NSX Edge

Nouveaux**Problème 1825416 : Des vApp délimitées échouent dans vCloud Director 8.20 après la mise à niveau vers NSX for vSphere 6.3.x**
Après la mise à niveau vers NSX 6.3.x et des passerelles NSX Edge vers la version 6.3.x dans vCloud Director 8.20, les vApp délimitées échouent et les machines virtuelles dans un réseau délimité ne parviennent pas à communiquer avec leur passerelle. Consultez l'*article 2150010 de la base de connaissances de VMware* pour plus d'informations.

Solution : contactez le support client VMware.

NouveauxProblème 1781438 : Sur le dispositif 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.

NouveauxProblème 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.

NouveauxProblème 1791264 : Double-cliquer sur une zone de transport ne permet pas d'activer/désactiver le mode CDO.
Si vous essayez d'activer ou de désactiver le mode CDO à partir de la page de résumé à laquelle vous avez accédé en double-cliquant sur une zone de transport à partir de vSphere Web Client, rien ne se passe.

Solution : procédez comme suit :

1. Revenez à la page répertoriant les zones de transport : **Installation** > **Préparation du réseau logique** > **Zones de transport** et sélectionnez la zone de transport souhaitée.
2. Sélectionnez **Activer le mode CDO/Désactiver le mode CDO** dans le menu déroulant **Actions**.
3. L'action sélectionnée est appliquée.

NouveauxProblème 1773500 : Un itinéraire non valide (0.0.0.0/32) entraîne le blocage de NSX
Si vous transmettez l'itinéraire 0.0.0.0/32 sur le routeur logique distribué (DLR) NSX, celui-ci ne prend pas en charge cet itinéraire et le rejette. Toutefois, cela entraîne un incident (PSOD) lorsque la LIF associée est supprimée et rajoutée avec une adresse IP sur le même sous-réseau.

Solution : 0.0.0.0/32 n'est pas un itinéraire valide. Ne le configurez pas ou utilisez routemap pour le rejeter.

NouveauxProblème 1769941 : Table de pont L2VPN « contaminée » par le routeur logique distribué (DLR) PMAC en raison d'une réponse ARP en double
Le port de jonction vxlan du serveur L2VPN sur l'hôte n'abandonne pas la réponse ARP provenant de la machine virtuelle client dont l'adresse MAC de destination est pMAC. La table MAC du pont est ainsi contaminée, ce qui entraîne une perte de trafic.

Solution : Pour contourner ce problème, ajoutez un filtre de trafic au dvport de jonction VXLAN afin d'abandonner la réponse ARP destinée à pMAC.

Pour ajouter un qualificateur de trafic :

1. Accédez au dvport sur lequel le dispositif NSX Edge est connecté.
2. Accédez à Modifier les paramètres > Filtrage et balisage du trafic.
3. Ajoutez un qualificateur MAC avec une valeur de destination définie sur pMAC.

NouveauxProblème 1782321 : Certains dispositifs NSX Edge peuvent subir des scénarios split-brain, même si leur état Highavailability s'affiche correctement
En raison d'une condition de concurrence dans le mécanisme HA, certains dispositifs NSX Edge mis à niveau vers NSX 6.2.5 et versions ultérieures peuvent subir des scénarios split-brain même si leur « état Highavailability » s'affiche correctement. Cela peut également se produire après le redéploiement des dispositifs Edge.

Solution : Redémarrez le dispositif NSX Edge en veille.

NouveauxProblème 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.

NouveauxProblème 1771760 : Les paquets de réponse SNMP contenant le type d'OID Counter64 sont abandonnés par NSX Edge lorsque le mécanisme de traduction d'adresses (NAT) est activé.
La passerelle ALG SNMP de NSX Edge ne parvient pas à traiter les types Counter64 des paquets de réponse SNMP, et le paquet est abandonné. En conséquence, le client n'obtient pas de réponse à la demande.

Solution : Si vous rencontrez ce problème, contactez le support VMware.

NouveauxProblème 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.

NouveauxProblème 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.

NouveauxProblème 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

NouveauxProblème 1803220 : Perte de connectivité VXLAN à des hôtes activés pour CDO lorsque la connexion entre le contrôleur et l'hôte est coupée
La fonctionnalité CDO (Controller Disconnected Operation) garantit la connectivité VXLAN lorsque l'ensemble du cluster de contrôleur est inactif/inaccessible. Toutefois, dans les cas où le cluster de contrôleur est actif, mais qu'un hôte perd la connectivité avec lui, le trafic de plan de données destiné à cet hôte depuis d'autres hôtes connectés au contrôleur peut toujours être abandonné. Dans ce cas, l'hôte a été supprimé de la liste VTEP par VNI et les ARP envoyés par les hôtes distants sont abandonnés. Pour le trafic provenant de l'hôte qui a perdu la connectivité avec le contrôleur, la fonctionnalité CDO garantit qu'il pourra atteindre la bonne destination.

NouveauxProblème 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.

NouveauxProblème 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.

NouveauxProblème 1773127 : Lors de configurations avec un grand nombre d'hôtes et de commutateurs logiques, l'écran qui affiche les hôtes liés à un commutateur logique donné ne parvient pas à se charger correctement.
Lorsque vous sélectionnez Commutateur logique > Objets liés > Hôtes dans votre configuration avec un grande nombre d'hôtes, vSphere Web Client ne parvient pas à se charger après quelques minutes d'attente et l'erreur suivante s'affiche : `Le service de données a expiré, car une tâche principale a duré plus de 120 secondes.` Cela se produit, car le renvoi de l'appel API distant à NSX Manager a pris trop de temps.

Solution : il existe deux solutions à ce problème :

- Première option : vous pouvez éviter ce problème en augmentant le délai d'expiration de l'API comme décrit dans l'*article 2040626 de la base de connaissances de VMware*. Vous devrez peut-être redémarrer l'instance de vSphere Web Client après l'augmentation du délai d'expiration. L'augmentation du délai d'expiration ne va probablement engendrer aucune erreur, mais vous devrez attendre environ 2 à 4 minutes que la page se recharge.
- Seconde option : si vous ne voulez voir que les hôtes liés correctement, vous pouvez aller dans Accueil > Mise en réseau > Groupe de ports > Objets liés > Hôtes pour voir la liste d'hôtes associés au commutateur logique.

NouveauxProblème 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.

NouveauxProblème 1770114 : Le message d'erreur au niveau cluster ne s'efface pas après la préparation de l'hôte.
Lorsque vous attribuez un pool d'adresses IP à un cluster qui ne dispose pas de suffisamment d'adresses IP, puis que vous essayez d'ajouter un hôte à ce cluster, vous obtenez l'erreur « Adresses IP insuffisantes ». Une fois que vous avez modifié ce pool pour ajouter des adresses IP supplémentaires et que vous pouvez ajouter des hôtes à ce cluster, le message d'erreur reste au niveau cluster.

Solution : contactez le support client VMware.

Problème 1789088 : NSX Edge bloqué dans l'invite de ligne de commande `grub`
NSX Edge peut échouer à démarrer et peut être bloqué à l'invite de ligne de commande `grub`.

Solution :

- commencez par examiner :
  1. Vérifiez l'environnement existant avec la commande `set`.
  2. Utilisez les commandes `ls` et `cat` pour localiser et vider le fichier `/boot/grub/grub.cfg`.

     ```
     grub> ls /boot
     grub> ls /boot/grub
     grub> cat /boot/grub/grub.cfg
     ```

  3. Capturez les journaux d'hôte à cette heure-là (les plus proches du problème que possible). Certains journaux NFS peuvent indiquer un problème de stockage NFS.
- Ensuite, démarrez le dispositif NSX Edge manuellement. Essayez ce qui suit, dans cet ordre (essayez l'option suivante uniquement si la précédente ne démarre pas le dispositif Edge) :

1. Redémarrez la VM Edge en sélectionnant l'option Réinitialiser l'alimentation sur vSphere Web Client.

2. OU spécifiez de nouveau le fichier de configuration grub, ce qui devrait charger le menu qui démarre le dispositif Edge immédiatement.
   Appelez la commande suivante à l'invite grub :

   ```
   grub> configfile /boot/grub/grub.cfg
   ```

3. OU utilisez les commandes suivantes à l'invite `grub` :

   ```
   grub> insmod ext2
   grub> set root=(hd0,1)
   grub> linux /boot/vmlinuz loglevel=3 root=/dev/sda1
   grub> boot
   ```

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 1676085 : L'activation d'Edge HA échoue si la réservation des ressources échoue

À partir de NSX for vSphere 6.2.3, l'activation de la haute disponibilité sur un dispositif Edge existant échoue lorsque des ressources suffisantes ne peuvent pas être réservées pour le second dispositif de VM Edge. La configuration reviendra à la dernière configuration correcte connue. Dans les versions précédentes, si HA est activé après l'échec du déploiement d'Edge et de la réservation des ressources, la VM Edge est toujours créée.

Solution : ce changement de comportement est normal.

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 : utilisez l'API *https://NSX-Manager-IP-Address/api/4.0/edges/edgeId/status* avec *detailedStatus=true*.

Problème 1556924 : Perte de connectivité L3 avec l'erreur Possibilité de blocage de VXLAN

Lorsque des LIF du DLR sont configurées sur l'hôte, mais que la couche sous-jacente de VXLAN n'est pas complètement préparée, la connectivité via certaines des LIF du DLR peut être affectée. Certaines des VM appartenant au DLR ne sont pas accessibles. Il peut y avoir des journaux *« Échec de la création de l'état de jonction de VXLAN : possibilité de blocage »* dans le fichier */var/log/vmkernel.log*.

Solution : vous pouvez supprimer les LIF et les recréer. Une autre option consiste à redémarrer les hôtes ESX affectés.

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 1604514 : La modification/configuration d'une passerelle par défaut sur un DLR non géré échoue après un clic sur Publier

Lorsqu'une passerelle par défaut est ajoutée à un DLR non géré, la publication échoue avec l'erreur « La distance de routage n'est prise en charge que sur NSX Edge 6.2.0 et versions ultérieures avec des VM NSX Edge déployées ». Cela est dû au fait que la distance Admin par défaut est définie sur « 1 » sur l'interface utilisateur.

Solution : supprimez la distance Admin « 1 » définie par défaut.

Problème 1642087 : Après la modification du paramètre securelocaltrafficbyip dans l'extension VPN IPsec, le transfert vers les réseaux de destination échoue

Lorsque vous utilisez une passerelle NSX Edge Services Gateway, vous rencontrez le symptôme suivant :

- Après la modification du paramètre securelocaltrafficbyip sur 0 dans l'interface utilisateur de NSX (écran Modifier le VPN IPsec), le transfert vers un sous-réseau distant du tunnel VPN IPsec ne fonctionne plus
- Lorsque vous modifiez ce paramètre, vous ne voyez plus les informations correctes pour un sous-réseau distant dans la table de routage IP

Solution : désactivez et réactivez le service VPN IPSec. Ensuite, vérifiez que les informations de routage prévues sont affichées dans l'interface de ligne de commande et dans l'interface utilisateur.

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 1534603 : 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 1534799 : Convergence lente lorsque le routeur de frontière de zones OSPF avec l'adresse IP la plus élevée est mis hors tension
La convergence met beaucoup de temps lorsque le routeur de frontière de zones (ABR) OSPF basé sur NSX avec l'adresse IP la plus élevée est mis hors tension ou redémarré. Si un ABR qui ne dispose pas de l'adresse IP la plus élevée numériquement est mis hors tension ou redémarré, le trafic converge rapidement vers un autre chemin. Toutefois, si l'ABR avec l'adresse IP la plus élevée est mis hors tension ou redémarré, un délai de reconvergence de plusieurs minutes est affiché. Le processus OSPF peut être effacé manuellement pour réduire le délai de convergence.

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 1089745 : 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 1498965 : 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 1494025 : 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 1288487 : 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 conn
ected-->
</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

Nouveaux**Problème 1847753 : Les hôtes échouent avec un écran de diagnostic violet lors de la récupération de flux pour les protocoles avec ALG activé**
Après avoir effectué la mise à niveau de NSX for vSphere 6.2.4 vers la version 6.3.0 ou 6.3.1 avec Flow Monitoring activé dans l'environnement, l'hôte ESXi affiche un écran de diagnostic violet. Consultez l'*article 2149908 de la base de connaissances de VMware* pour plus d'informations et pour connaître la solution.

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

Nouveaux**Problème 1676043 : VM supprimée de la liste d'exclusion après deux ajouts simultanés**
Si deux utilisateurs ajoutent simultanément la même machine virtuelle à la liste d'exclusion, sans actualiser l'interface utilisateur, les machines virtuelles déjà ajoutées sont supprimées de la liste d'exclusion.

Solution : Actualisez l'interface utilisateur de vSphere Web Client avant d'ajouter la machine virtuelle à la liste d'exclusion.

Nouveaux**Problème 1770259 : Le champ `appliedTo` pour la règle DFW ne peut pas être modifié pour avoir plusieurs objets `appliedTo`**
Lorsque vous appliquez la règle DFW à un ensemble de vNIC ou de VM, ou à des clusters ou un centre de données, que vous la publiez, puis que vous voulez apporter des modifications en ajoutant des objets supplémentaires au champ `appliedTo`, les nouvelles modifications ne prennent pas effet même si la publication réussit.

Solution : aucune.

NouveauxProblème 1798779 : Après la mise à niveau de NSX 6.2.x vers NSX 6.3.0, la GUI de vSphere Web Client vous permet de façon erronée d'ajouter une balise de sécurité universelle
NSX 6.3.0 introduit les balises de sécurité universelle. Lorsque vous essayez d'ajouter une balise de sécurité universelle à un groupe de sécurité universelle créé sur 6.2.x avant la mise à niveau vers NSX 6.3.0, l'opération échoue avec l'erreur « Le membre demandé n'est pas un membre valide ». Cette erreur est correcte, car vous ne pouvez pas ajouter une balise de sécurité universelle à un groupe de sécurité universelle NSX 6.2.x. La GUI se trompe.

Solution : après la mise à niveau, créez un groupe de sécurité universelle NSX 6.3.0 et ajoutez les balises de sécurité universelle à ce groupe.

NouveauxProblème 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.

NouveauxProblème 1786780 : Le reclassement/déplacement de stratégies dans l'interface utilisateur de Service Composer dure longtemps avec une utilisation du CPU élevée
Le reclassement ou le déplacement de stratégies depuis l'interface utilisateur de Service Composer peut prendre un très long moment avec une utilisation du CPU élevée.

Solution : les étapes suivantes sont utiles :

- Lors de la création de la stratégie, essayez d'accorder la bonne priorité (poids) à la stratégie, de sorte qu'elle soit placée correctement à la première tentative et que vous n'ayez pas à reclasser les stratégies une nouvelle fois.
- Si vous devez déplacer une stratégie, modifiez la stratégie à déplacer et modifiez la priorité (poids) sur une valeur appropriée. Cela entraîne la modification rapide d'une seule stratégie.

NouveauxProblème 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 1462027 : Dans les déploiements de cross-vCenter NSX, plusieurs versions de configurations de pare-feu enregistrées ont été répliquées sur des instances secondaires de NSX Manager

La synchronisation universelle enregistre plusieurs copies de configurations universelles sur des NSX Manager secondaires. La liste des configurations enregistrées contient plusieurs ébauches créées par la synchronisation sur plusieurs dispositifs NSX Manager, avec le même nom et à la même heure, ou avec une différence de 1 seconde.

Solution : exécutez l'appel de l'API pour supprimer les ébauches dupliquées.

```
DELETE : https://<nsxmgr-ip>/api/4.0/firewall/config/drafts/
```

Recherchez les ébauches à supprimer en affichant toutes les ébauches :

```
GET: https://<nsxmgr-ip>/api/4.0/firewall/config/drafts
```

Dans l'exemple de sortie suivant, les ébauches 143 et 144 ont le même nom, elles ont été créées à la même heure et sont par conséquent dupliquées. De même, les ébauches 127 et 128 ont le même nom, elles sont décalées d'une seconde et sont également dupliquées.

```
<firewallDrafts>
    <firewallDraft id="144" name="AutoSaved_Wednesday, August 5, 2015 11:08:40 PM GMT
" timestamp="1438816120917">
        <description>Auto saved configuration</description>
        <preserve>false</preserve>
        <user>replicator-1fd96022-db14-434d-811d-31912b1cb907</user>
        <mode>autosaved</mode>
    </firewallDraft>
    <firewallDraft id="143" name="AutoSaved_Wednesday, August 5, 2015 11:08:40 PM GMT
" timestamp="1438816120713">
        <description>Auto saved configuration</description>
        <preserve>false</preserve>
        <user>replicator-1fd96022-db14-434d-811d-31912b1cb907</user>
        <mode>autosaved</mode>
    </firewallDraft>
   <firewallDraft id="128" name="AutoSaved_Wednesday, August 5, 2015 9:08:02 PM GMT"
timestamp="1438808882608">
        <description>Auto saved configuration</description>
        <preserve>false</preserve>
        <user>replicator-1fd96022-db14-434d-811d-31912b1cb907</user>
        <mode>autosaved</mode>
    </firewallDraft>
    <firewallDraft id="127" name="AutoSaved_Wednesday, August 5, 2015 9:08:01 PM GMT"
 timestamp="1438808881750">
        <description>Auto saved configuration</description>
        <preserve>false</preserve>
        <user>replicator-1fd96022-db14-434d-811d-31912b1cb907</user>
        <mode>autosaved</mode>
    </firewallDraft>
</firewallDrafts>
```

Problème 1449611 : Lorsqu'une stratégie de pare-feu de Service Composer n'est pas synchronisée en raison d'un groupe de sécurité supprimé, la stratégie de pare-feu ne peut pas être corrigée dans l'interface utilisateur

Solution : dans l'interface utilisateur, vous pouvez supprimer la stratégie de pare-feu non valide, puis l'ajouter de nouveau. Vous pouvez également, dans l'API, corriger la stratégie de pare-feu en supprimant le groupe de sécurité non valide. Vous pouvez ensuite synchroniser 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, modifiez les stratégies de pare-feu de façon qu'elles ne renvoient plus aux groupes de sécurité avant de supprimer les groupes de sécurité.

Problème 1557880 : Il peut manquer des règles de couche 2 (L2) si l'adresse MAC d'une machine virtuelle utilisée dans les règles est modifiée
Comme l'optimisation de règle L2 est activée par défaut, les règles L2 avec les champs source et de destination spécifiés (autres que « tous ») seront appliquées sur les vNIC (ou les filtres) uniquement si l'adresse MAC du vNIC correspond à la liste d'adresses MAC source ou de destination. Ces règles L2 ne seront pas appliquées sur les hôtes avec des machines virtuelles ne correspondant pas aux adresses MAC source ou de destination.

Solution : pour que les règles L2 soient appliquées sur tous les vNIC (ou les filtres), définissez l'un des champs source ou de destination sur « tous ».

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.

Problème 1626233 : lorsque la machine virtuelle de service (SVM) NetX abandonne des paquets, Traceflow ne génère pas d'observation perdue

La session Traceflow se ferme une fois le paquet envoyé à la SVM NetX. Lorsque la SVM NSX abandonne des paquets, Traceflow ne génère pas d'observation perdue.

Solution : Il n'existe pas de solution. Si le paquet Traceflow n'est pas réinjecté, on peut considérer que la SVM a abandonné le paquet.

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.

Problèmes connus de NSX Controller

Problème 1765354 : <deployType> est une propriété obligatoire mais elle n'est pas utilisée
<deployType> est une propriété obligatoire mais elle n'est pas utilisée et ne signifie rien.

Problème 1516207 : Des contrôleurs peuvent être isolés après la réactivation de la communication IPsec sur un cluster NSX Controller
Si un cluster de contrôleurs NSX est défini pour autoriser les communications contrôleur à contrôleur sécurisées (IPsec est désactivé), puis que la communication IPsec est réactivée ultérieurement, un ou plusieurs contrôleurs peuvent devenir isolés de la majorité des clusters à cause d'une clé prépartagée différente (« PSK »). Lorsque cela se produit, l'API NSX peut être incapable de modifier les paramètres IPsec des contrôleurs.

Solution :

suivez ces étapes pour résoudre ce problème :

1. Désactivez IPsec à l'aide de l'API NSX.

   ```
   PUT /2.0/vdn/controller/node

   <controllerNodeConfig>
     <ipSecEnabled>false</ipSecEnabled>
   </controllerNodeConfig>
   ```

2. Réactivez IPsec à l'aide de l'API NSX.

   ```
   PUT /2.0/vdn/controller/node

   <controllerNodeConfig>
     <ipSecEnabled>true</ipSecEnabled>
   </controllerNodeConfig>
   ```

Suivez ces meilleures pratiques pour éviter ce problème :

- Utilisez toujours l'API NSX pour désactiver IPsec. L'utilisation de l'interface de ligne de commande de NSX Controller pour désactiver IPsec n'est pas prise en charge.
- Vérifiez toujours que tous les contrôleurs sont actifs avant d'utiliser l'API pour modifier le paramètre IPsec.

Problème 1306408 : Les journaux de NSX Controller doivent être téléchargés dans l'ordre
Les journaux de NSX Controller ne peuvent pas être téléchargés simultanément. Même si vous téléchargez sur plusieurs contrôleurs, vous devez attendre que le téléchargement sur le contrôleur actuel soit terminé avant de pouvoir télécharger sur un autre contrôleur. Notez également que vous ne pouvez pas annuler un téléchargement ayant déjà commencé.

Solution : patientez jusqu'à la fin du téléchargement sur le contrôleur actuel avant de lancer le téléchargement d'un autre journal.

Problèmes résolus

NouveauxProblèmes résolus dans NSX 6.3.0

Les problèmes résolus dans NSX 6.3.0 sont groupés comme suit :

Problèmes généraux résolus dans NSX 6.3.0

Problème résolu 1497389 : Les utilisateurs disposant de privilèges d'administrateur NSX peuvent modifier leurs privilèges et accéder à des privilèges d'administrateur d'entreprise, qui est un rôle d'utilisateur plus élevé. À partir de NSX 6.3.0, les utilisateurs disposant de privilèges d'administrateur NSX ne peuvent pas gérer les utilisateurs, seuls les utilisateurs dotés de privilèges d'administrateur d'entreprise peuvent le faire. *Problème résolu dans la version 6.3.0.*

Problèmes résolus 1575342, 1719402 : Dans un environnement NSX for vSphere 6.x, lorsqu'une VM de service (SVM) est migrée (vMotion/SvMotion), le service peut être interrompu ou l'hôte ESXi peut se bloquer
À partir de la version 6.3.0, vous ne pouvez pas migrer une VM de service (SVM) avec vMotion/SvMotion. Les SVM doivent rester sur l'hôte sur lequel elles ont été déployées pour un fonctionnement correct. Auparavant, la migration vers un autre hôte était autorisée, mais pas prise en charge, et elle entraînait une interruption du service et des problèmes avec l'hôte.
Consultez l'*article 2141410 de la base de connaissances de VMware* pour plus d'informations. *Problème résolu dans la version 6.3.0.*

Problème résolu 1708769 : augmentation de la latence sur les SVM (Service VM) après un snapshot dans NSX
La création d'un snapshot d'une SVM (Service VM) peut entraîner une augmentation de la latence sur le réseau. Le snapshot est parfois appelé par les applications de sauvegarde qui s'exécutent dans l'environnement. *Problème résolu dans la version 6.3.0.*

Problème résolu 1760102 : Les machines virtuelles peuvent ne pas communiquer après que NSX Controller a été supprimé et redéployé pour récupérer après une panne de stockage
NSX Controller pour l'environnement vSphere 6.2.4/6.2.5 peut entrer en mode lecture seule en cas de panne de stockage, et si vous supprimez puis redéployez le contrôleur pour récupérer à partir de cet état, certaines machines virtuelles sont susceptibles de ne pas pouvoir communiquer. En principe, en cas de panne de stockage sur un contrôleur, le redémarrage du contrôleur devrait le sortir du mode lecture seule, mais actuellement cela ne se produit pas dans NSX. *Problème résolu dans la version 6.3.0.*

Problème résolu 1662842 : Guest Introspection : Connectivité perdue entre MUX et la USVM lors de la tentative de résolution de SID Windows ne pouvant pas être résolus
Le service Guest Introspection passe dans un état d'avertissement, et chaque Guest Introspection entre et sort de cet état. Tant que la VM Guest Introspection n'est pas reconnectée, les événements réseau ne seront pas remis à NSX Manager. Cela affectera la surveillance des activités et le pare-feu ID dans le cas où des événements de connexion sont détectés via le chemin Guest Introspection. *Problème résolu dans la version 6.3.0.*

Problème résolu 1752051 : L'état de service de Guest Introspection est signalé comme « Non prêt » lorsque la communication entre NSX Manager et la USVM expire

Un message d'erreur semblable à « PLAIN login refused: user 'usvm-admin-host-14' - invalid credentials » peut être signalé pour la SVM universelle de Guest Introspection lorsque le processus de changement de mot de passe attendu avec NSX Manager sur le bus de message interne (rabbit MQ) échoue. *Problème résolu dans la version 6.3.0.*

Problème résolu 1716328 : La suppression d'un hôte en mode maintenance peut entraîner l'échec ultérieur de la préparation du cluster.

Si un administrateur place un hôte ESXi activé par NSX en mode maintenance et le supprime d'un cluster préparé pour NSX, NSX ne supprime pas l'enregistrement de son numéro d'ID de l'hôte supprimé. Une fois l'installation basculée dans cette condition, si un autre hôte portant le même ID se trouve dans un autre cluster ou si cet hôte est ajouté à un autre cluster, le processus de préparation de ce dernier échoue. *Problème résolu dans la version 6.3.0.*

Problème résolu 1710624 : Le serveur de journaux des événements de Windows 2008 est ajouté avec « TYPE » défini sur « WIN2K3 » lorsque ServerType n'est pas spécifié dans le corps de la requête de l'API REST

Si vous créez une requête d'API pour le serveur EventLog, ce dernier est ajouté avec « TYPE » défini sur « WIN2K3 ». Si vous utilisez le serveur EventLog uniquement pour IDFW, il se peut qu'IDFW ne fonctionne pas correctement. *Problème résolu dans la version 6.3.0.*

Problèmes d'installation et de mise à niveau résolus dans NSX 6.3.0

Problème résolu 1463767 : Dans un déploiement cross-vCenter, une section de configuration de pare-feu universelle peut se trouver sous (subordonnée à) une section de configuration locale
Si vous passez une instance de NSX Manager à l'état autonome (transit), puis que vous la repassez à l'état secondaire, toute modification locale de configuration effectuée alors que cette instance se trouve temporairement à l'état autonome peut être indiquée au-dessus des sections de configuration universelles répliquées héritées de l'instance principale de NSX Manager. Cela génère la condition d'erreur suivante : `La section universelle doit être au-dessus de toutes les autres sections sur les instances secondaires de NSX Manager.`
Problème résolu dans la version 6.3.0.

Problème résolu 1402307 : si vCenter est redémarré lors du processus de mise à niveau de NSX for vSphere, le cluster affiche un statut incorrect
Lors de la préparation de l'hôte dans un environnement avec plusieurs clusters NSX préparés pendant une mise à niveau et si vCenter Server est redémarré suite à la préparation d'au moins un cluster, les autres clusters peuvent afficher le statut Non prêt plutôt que d'afficher un lien de mise à jour. Les hôtes dans vCenter peuvent également afficher Redémarrage requis.
Problème résolu dans la version 6.3.0.

Problème résolu 1495307 : Lors d'une mise à niveau, les règles de pare-feu L2 et L3 ne sont pas publiées vers les hôtes
Après avoir publié une modification de la configuration du pare-feu distribué, le statut reste `InProgress` de façon indéfinie dans l'interface utilisateur comme dans l'API. De plus, aucun journal des règles L2 ou L3 n'est écrit sur le fichier vsfwd.log. *Problème résolu dans la version 6.3.0.*

Problème résolu 1491820 : Le journal de NSX Manager collecte des messages `WARN messagingTaskExecutor-7` après la mise à niveau vers NSX 6.2
Après la mise à niveau de NSX 6.1.x vers NSX 6.2, le journal de NSX Manager est inondé de messages semblables aux suivants : `WARN messagingTaskExecutor-7 ControllerInfoHandler:48 - host is unknown: host-15 return empty list.` Ce problème n'a aucune répercussion opérationnelle.
Problème résolu dans la version 6.3.0.

Problèmes de NSX Manager résolus dans NSX 6.3.0

Problème résolu 1671067 : Le plug-in NSX n'apparaît pas dans vCenter Web Client lorsque le plug-in ESXTOP est également installé
Après le déploiement de NSX et l'enregistrement réussi avec vCenter, le plug-in NSX n'apparaît pas dans vCenter Web Client. Ce problème est causé par un conflit entre le plug-in NSX et le plug-in ESXTOP.
Problème résolu dans la version 6.3.0.

Problèmes de mise à niveau et de Services Edge résolus dans NSX 6.3.0

Problème résolu 1740231 : Impossible d'ajouter une adresse IP sur l'interface HA
À partir de la version 6.3.0, il est possible d'ajouter des adresses IP sur l'interface HA du routeur DLR. Cette fonctionnalité n'était pas disponible dans certaines versions plus anciennes de NSX, mais elle a été réintroduite pour assurer une compatibilité avec le comportement de l'API de l'interface de gestion HA du routeur DLR. *Problème résolu dans la version 6.3.0*

Problème résolu 1716333 : Le changement de taille d'une VM Edge ou d'un paramètre de placement pendant l'activation ou la désactivation d'Edge HA peut créer des VM Edge supplémentaires
Des opérations simultanées de modification de la taille d'une VM Edge ou d'un paramètre de placement (tel qu'une banque de données ou un pool de ressources) et l'activation ou la désactivation d'Edge HA peuvent endommager la base de données d'objet géré par NSX, ce qui rend des VM Edge inutilisables. De plus, dans un environnement avec cross-vCenter, les VM Edge abandonnées seront laissées sur le site secondaire. *Problème résolu dans la version 6.3.0.*

Problème résolu 1717369 : Lorsqu'elles sont configurées en mode HA, les VM Edge active et en attente peuvent être déployées sur le même hôte.
Ce problème est dû au fait que des règles d'anti-affinité n'ont pas été créées ni appliquées automatiquement sur les hôtes vSphere au cours des opérations de redéploiement et de mise à niveau. Ce problème ne se pose pas lorsque la HA est activée sur le dispositif Edge existant.

Problème résolu dans la version 6.3.0. Voici le comportement attendu :

- Lorsque vSphere HA est activé, des règles d'anti-affinité pour les VM Edge d'une paire HA sont créées au cours des opérations de redéploiement et de mise à niveau.
- Lorsque vSphere HA est désactivé, des règles d'anti-affinité pour les VM Edge d'une paire HA ne sont pas créées.

Problème résolu 1675659 : les itinéraires statiques flottants sont préférés aux itinéraires dynamiques OSPF
Un itinéraire statique flottant de sauvegarde est mal entré dans la table de routage d'un dispositif Edge lorsque la redistribution d'itinéraire est activée même si un itinéraire OSPF est disponible. *Problème résolu dans la version 6.3.0.*

Problème résolu 1733165 : IPsec peut entraîner la suppression des itinéraires dynamiques de la table de transfert NSX Edge
Si un sous-réseau accessible via un itinéraire dynamique est utilisé comme sous-réseau distant pour la configuration d'IPsec, NSX Edge supprime ce sous-réseau de la table de transfert et ne le réinstalle pas, même après que ce sous-réseau a été supprimé de la configuration IPsec. *Problème résolu dans la version 6.3.0.*

Problème résolu 1663902 : Renommer une VM NSX Edge interrompt le trafic circulant via le dispositif Edge
Renommer une VM NSX Edge interrompt le trafic circulant via le dispositif Edge. *Problème résolu dans la version 6.3.0.*

Problème résolu 1624663 : Cliquer sur « Configurer le débogage avancé » actualise l'interface utilisateur de vCenter et la modification n'est pas conservée
Cliquer sur l'ID Edge spécifique > Configuration > Action > Configurer le débogage avancé entraîne l'actualisation de l'interface utilisateur de vCenter et la modification n'est pas conservée. *Problème résolu dans la version 6.3.0.*

Problème résolu 1706429 : des problèmes de communication lors de l'activation de la haute disponibilité (HA) après le déploiement initial du routeur logique (distribué) peuvent entraîner l'activation des deux dispositifs de routeurs logiques.
Si vous déployez un routeur logique sans la haute disponibilité et que vous activez la haute disponibilité plus tard (en déployant un nouveau dispositif de routeur logique), ou si vous désactivez, puis réactivez, la haute disponibilité, il peut arriver qu'un des dispositifs de routeurs logiques perde une des routes connectées vers l'interface HA. Ceci entraîne l'activation des deux dispositifs. *Problème résolu dans la version 6.3.0.*

Problème résolu 1542416 : le chemin de données ne fonctionne pas pendant 5 minutes après le redéploiement Edge et le basculement HA avec sous-interfaces
L'opération de redéploiement ou de basculement HA connaît un arrêt de cinq minutes en cas d'utilisation de sous-interfaces. Ce problème ne se présente pas sur les interfaces. *Problème résolu dans la version 6.3.0.*

Problème résolu 1492547 : temps de convergence accru lorsque le routeur de frontière de zones OSPF basé sur NSX avec l'adresse IP la plus élevée est mis hors tension ou redémarré.
Si un routeur de frontière de zones NSSA qui ne dispose pas de l'adresse IP la plus élevée est mis hors tension ou redémarré, le trafic converge rapidement vers un autre chemin. Si un routeur de frontière de zones NSSA avec l'adresse IP la plus élevée est mis hors tension ou redémarré, un délai de reconvergence de plusieurs minutes est affiché. Le processus OSPF peut être effacé manuellement pour réduire le délai de convergence. *Problème résolu dans la version 6.3.0.*

Problème résolu 1510724 : les routes par défaut ne sont pas remplies sur les hôtes après la création d'un nouveau routeur logique distribué universel
Après avoir fait passer NSX Manager du mode autonome au mode principal afin de configurer Cross-vCenter dans NSX for vSphere 6.2.x, il est possible que vous rencontriez les problèmes suivants :

- Lorsque vous créez un nouveau routeur logique distribué universel, les routes par défaut ne sont pas remplies sur l'instance de l'hôte.
- Les routes sont remplies sur la VM de contrôle du routeur logique distribué universel, mais pas sur l'instance de l'hôte.
- La commande *show logical-router host host-ID dlr Edge-ID route* ne présente pas les itinéraires par défaut.

Problème résolu dans la version 6.3.0.

Problème résolu 1704540 : un grand nombre de mises à jour de la table d'apprentissage MAC avec un pont NSX L2 et LACP peut entraîner un problème de mémoire insuffisante
Lorsqu'un pont NSX L2 détecte une adresse MAC sur une autre liaison montante, il signale un changement dans la table d'apprentissage MAC aux contrôleurs via le processus netcpa. Les environnements réseau avec LACP enregistrent la même adresse MAC sur plusieurs interfaces, ce qui génère un grand nombre de mises à jour de la table et risque d'épuiser la mémoire nécessaire au processus netcpa. Consultez l'*article 2147181 de la base de connaissances de VMware*. *Problème résolu dans la version 6.3.0.*

Problème résolu 1716545 : le changement de taille du dispositif Edge n'affecte pas la quantité de CPU et de mémoire réservée en attente pour Edge
Seule la première VM Edge créée dans le cadre d'une paire HA se voit affecter les paramètres de réservation.

Problème résolu 1772004 : Le basculement Edge HA du nœud 0 vers le nœud 1 prend plus de temps que prévu
Le basculement du nœud 0 vers le nœud 1 prend plus de temps que prévu dans l'environnement configuré Edge HA alors que le basculement du trafic du nœud 1 vers le nœud 0 est normal. *Problème résolu dans la version 6.3.0.*

Problème résolu 1726379 : si une plage IP de multidiffusion dispose d'une valeur liée supérieure dépassant 99 dans les trois derniers octets, la configuration du groupe de ports de jonction VXLAN échoue.
Lors de la configuration de l'ID de segment, si vous créez une plage IP de multidiffusion avec une valeur liée supérieure dépassant 99 dans les trois derniers octets, par exemple 1.100.100.100, et un commutateur logique de multidiffusion ou hybride avec la même plage IP de multidiffusion, la configuration du groupe de ports de jonction VXLAN échouera. *Problème résolu dans la version 6.3.0.*

Problèmes de services de sécurité résolus dans NSX 6.3.0

Problème résolu 1767402 : Les règles DFW avec « Appliqué à » défini sur un « Groupe de sécurité » ne sont pas publiées sur des hôtes
Les règles DFW avec le champ « Appliqué à » défini sur un groupe de sécurité ne sont pas publiées sur des hôtes ESXi dans un nouveau cluster. *Problème résolu dans la version 6.3.0.*

Problème résolu 1743366 : Le contrôle de seuil NSX est désactivé par défaut pour éviter un blocage potentiel
Lorsque le module Pare-feu est exécuté, NSX désactive le contrôle de seuil pour la mémoire afin d'éviter un blocage potentiel. Lorsque l'hôte exécute ESX 6.5P01 ou ESX 6.0U3 ou version ultérieure, le contrôle de seuil de mémoire est automatiquement activé. *Problème résolu dans la version 6.3.0.*

Problème résolu 1491046 : L'adresse IP IPv4 n'est pas approuvée automatiquement
L'adresse IP IPv4 n'est pas approuvée automatiquement lorsque la stratégie SpoofGuard est définie sur Confiance à la première utilisation (TOFU) dans VMware NSX for vSphere 6.2.x. *Problème résolu dans la version 6.3.0.*

Problème résolu 1686036 : Les règles de pare-feu ne peuvent pas être ajoutées, modifiées ni supprimées en cas de suppression de la section par défaut.
Si la section Layer2 ou Layer3 par défaut est supprimée, la publication d'une règle de pare-feu peut échouer. *Problème résolu dans la version 6.3.0.*

Problème résolu 1717994 : La requête d'API de statut Distributed Firewall (DFW) signale par intermittence l'erreur de serveur interne 500.
Si cette requête est émise lors de l'ajout d'un nouvel hôte à un cluster préparé en conséquence, elle échoue avec l'erreur de serveur interne 500 pour les premières tentatives, puis renvoie la réponse correcte une fois que des VIB commencent à être installés sur l'hôte. *Problème résolu dans la version 6.3.0.*

Problème résolu 1717635 : L'opération de configuration du pare-feu échoue si l'environnement contient plusieurs clusters tandis que des modifications sont effectuées en parallèle
Dans un environnement contenant plusieurs clusters, si plusieurs utilisateurs modifient la configuration du pare-feu en continu dans un laps de temps réduit (par exemple, s'ils ajoutent/suppriment des sections ou des règles), certaines opérations échouent, et les utilisateurs obtiendront une réponse API semblable à celle-ci : `org.hibernate.exception.GenericJDBCException: Could not execute JDBC batch update; nested exception is javax.persistence.PersistenceException: org.hibernate.exception.GenericJDBCException: Could not execute JDBC batch update` *Problème résolu dans la version 6.3.0.*

Problème résolu 1707931 : l'ordre des règles de pare-feu distribué change lorsque des stratégies de service sont définies dans Service Composer et qu'une règle de pare-feu est modifiée ou publiée avec un filtre appliqué à l'interface du pare-feu
Toute réorganisation, suppression ou ajout de stratégies de service créées dans Service Composer après une ou plusieurs opérations de publication dans l'interface utilisateur Networking & Security > Pare-feu modifie l'ordre des règles de pare-feu, ce qui peut avoir des conséquences inattendues. *Problème résolu dans la version 6.3.0.*

Problème résolu 1682552 : Certains événements de seuil ne sont pas signalés pour la CPU, la mémoire et le CPS pour Distributed Firewall (DFW).
Même lorsque les seuils DFW de ces éléments sont définis pour être signalés, les événements de seuil ne sont pas consignés lorsque les seuils sont dépassés. *Problème résolu dans la version 6.3.0.*

Problème résolu 1620460 : NSX n'a pas pu empêcher les utilisateurs de créer des règles dans la section des règles de Service Composer
Dans le Client Web vSphere, l'interface Mise en réseau et sécurité : L'interface de pare-feu n'a pas pu empêcher les utilisateurs d'ajouter des règles dans la section des règles de Service Composer. Les utilisateurs doivent pouvoir ajouter des règles au-dessous/en dessus de la section Service Composer, mais pas à l'intérieur. *Problème résolu dans la version 6.3.0.*

Problème résolu 1445897 : La publication des règles de pare-feu distribué (DFW) échoue après la suppression de l'objet référencé dans VMware NSX for vSphere 6.1.x et 6.2.x *Problème résolu dans la version 6.2.3.*

Problème résolu 1704661/1739613 : les machines virtuelles perdent la connectivité réseau avec une erreur : "Failed to restore PF state: Limit exceeded"
les machines virtuelles perdent la connectivité réseau avec une erreur : "Failed to restore PF state: Limit exceeded." *Problème résolu dans la version 6.3.0.*

Problèmes d'interopérabilité de solution résolus dans NSX 6.3.0

Problème résolu 1527402 : La VM Windows avec le pilote NSX Network Introspection perd la connectivité TCP
Dans l'environnement VMware NSX for vSphere 6.x, une VM Windows avec le pilote NSX Network Introspection (vnetflt.sys) connecté à USVM (Guest Introspection SVM) perd la connectivité temporaire au réseau TCP. *Problème résolu dans la version 6.3.0.*

Problème résolu 1530360 : Après le basculement d'une VM NSX Manager, SRM (Site Recovery Manager) signale à tort une erreur de délai d'expiration
Lorsqu'une VM NSX Manager est basculée, SRM signale à tort une erreur de délai d'expiration en attente pour VMware Tools. Dans ce cas, VMware Tools est en fait actif et en cours d'exécution avant la fin du délai d'expiration de 300 secondes. *Problème résolu dans la version 6.3.0.*

Historique de révision du document

2 février 2017 : Première édition de NSX 6.3.0.
3 février 2017 : Deuxième édition de NSX 6.3.0. Ajout du problème connu 1799543
22 février 2017 : Troisième édition de NSX 6.3.0. Mise à jour des infos sur CDO
27 février 2017 : Quatrième édition de NSX 6.3.0. Ajout des problèmes connus 1808478 et 1818257
30 mars 2017 : Cinquième édition de NSX 6.3.0. Ajout des problèmes connus 1474650 et 1782321.
10 avril 2017 : Sixième édition de NSX 6.3.0. Ajout d'informations à la section Notes relatives aux mises à niveau.
3 mai 2017 : Septième édition de NSX 6.3.0. Ajout d'informations concernant le fait que les dispositifs vCNS Edge et VIX sont désormais déconseillés.
2 juin 2017 : Huitième édition de NSX 6.3.0. Ajout des problèmes connus 1860583, 1781438 et 1825416.
22 juin 2017 : Neuvième édition de NSX 6.3.0. Ajout du problème connu 1847753.
21 août 2017 : Dixième édition de NSX 6.3.0. Ajout du problème résolu 1463767 et suppression de quelques problèmes précédents.
2 octobre 2017 : Onzième édition de NSX 6.3.0. Mise à jour des versions recommandées minimales.