Notes de mise à jour de VMware NSX for vSphere 6.3.7

VMware NSX for vSphere 6.3.7 | Publié le 15 novembre 2018 | Build 10667122

Consultez l'Historique de révision de ce document.

Contenu des notes de mise à jour

Les notes de mise à jour couvrent les sujets suivants :

Nouveautés de NSX 6.3.7

NSX for vSphere 6.3.7 résout un certain nombre de bogues clients. Pour plus d'informations, voir Problèmes résolus.

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

- NSX 6.3.6
- NSX 6.3.5
- NSX 6.3.4
- NSX 6.3.3
- NSX 6.3.2
- NSX 6.3.1
- NSX 6.3.0

Versions, configuration système et installation

Remarque :

- Le tableau ci-dessous répertorie les versions recommandées du logiciel VMware. Ces recommandations sont générales et ne doivent pas remplacer des recommandations spécifiques de l'environnement.
- Ces informations sont à jour à la date de publication de ce document.
- Pour voir les versions **minimales prises en charge** de NSX et d'autres produits VMware, consultez la matrice d'interopérabilité des produits VMware. VMware déclare des versions minimales prises en charge en fonction de tests internes.

- La version minimale prise en charge requise de l'interopérabilité vSphere for NSX passe de NSX 6.3.2 à NSX 6.3.3. Reportez-vous à la Matrice d'interopérabilité des produits VMware pour plus de détails.

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

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

Configuration système et installation

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

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

Fonctionnalités obsolètes et retirées

Avertissements sur la fin de vie et la fin du support

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

- **NSX for vSphere 6.1.x** est arrivé en fin de disponibilité et a atteint sa date de fin de support général le 15 janvier 2017. (Consultez également l'*article 2144769 de la base de connaissances de VMware*.)
- Le support général de **NSX for vSphere 6.2.x** prendra fin le 20 août 2018.
- **Suppression de NSX Data Security** : à partir de NSX 6.3.0, la fonctionnalité NSX Data Security est supprimée du produit.
- **NSX Activity Monitoring (SAM) abandonné** : À partir de NSX 6.3.0, Activity Monitoring n'est plus une fonctionnalité prise en charge de NSX. En remplacement, utilisez la Surveillance de point de terminaison. Pour plus d'informations, consultez Surveillance de point de terminaison dans le *Guide d'administration de NSX*.
- **Web Access Terminal supprimé** : Web Access Terminal (WAT) a été supprimé de NSX 6.3.0. vous ne pouvez pas configurer Web Access SSL VPN-Plus et activer l'accès URL public via NSX Edge. VMware recommande d'utiliser le client d'accès complet avec des déploiements VPN SSL pour une sécurité améliorée. Si vous utilisez la fonctionnalité WAT dans une version antérieure, vous devez la désactiver avant d'effectuer la mise à niveau vers la version 6.3.0.
- **IS-IS supprimé de NSX Edge** : à partir de NSX 6.3.0, vous ne pouvez pas configurer le protocole IS-IS à partir de l'onglet **Routage**.
- **Arrêt de la prise en charge des dispositifs vCNS Edge**. Vous devez effectuer une mise à niveau vers un dispositif NSX Edge avant de procéder à la mise à niveau vers NSX 6.3.x.

Changements généraux du comportement

Si vous disposez de plusieurs commutateurs vSphere Distributed Switch et que VXLAN est configuré sur l'un d'entre eux, vous devez connecter n'importe laquelle des interfaces de routeur logique distribué à des groupes de ports sur ce commutateur vSphere Distributed Switch. À partir de NSX 6.3.6, cette configuration s'applique dans l'interface utilisateur et l'API. Dans les versions antérieures, rien ne vous empêchait de créer une configuration non valide.

Suppressions d'API et modifications de comportement

Modifications de la gestion des erreurs d'API

NSX 6.3.5 présente les modifications suivantes liées à la gestion des erreurs :

- Si une demande API entraîne une exception de base de données sur NSX Manager, la réponse est *500 Erreur de serveur interne*. Dans les versions précédentes, NSX Manager répondait avec *200 OK*, même si la demande échouait.
- Si vous envoyez une demande API avec un corps vide lorsqu'un corps de demande est attendu, la réponse est *400 Demande incorrecte*. Dans les versions précédentes, NSX Manager répondait avec *500 Erreur de serveur interne*.
- Si vous spécifiez un groupe de sécurité incorrect dans cette API, GET /api/2.0/services/policy/securitygroup/{ID}/securitypolicies, la réponse est *404 Introuvable*. Dans les versions précédentes, NSX Manager répondait avec *200 OK.*

Modifications des valeurs par défaut des API de sauvegarde et de restauration

À partir de la version 6.3.3, les valeurs par défaut des deux paramètres de sauvegarde et de restauration ont été modifiées pour correspondre aux valeurs par défaut dans l'interface utilisateur. Précédemment, **passiveMode** et **useEPSV** étaient définis par défaut sur *false*. Ils sont désormais définis par défaut sur *true*. Ce problème concerne les API suivantes :

- PUT /api/1.0/appliance-management/backuprestore/backupsettings
- PUT /api/1.0/appliance-management/backuprestore/backupsettings/ftpsettings

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

- À partir de la version 6.3.0, cette demande est refusée si la section par défaut est spécifiée : `DELETE /api/4.0/firewall/globalroot-0/config/layer2sections|layer3sections/sectionId`
- Une nouvelle méthode est 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`** :

À partir de la version 6.3.0, le paramètre defaultOriginate est supprimé des méthodes suivantes pour des dispositifs NSX Edge de routeur logique (distribué) uniquement :

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

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

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

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

Suppressions de CLI et modifications de comportement

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

Notes relatives aux mises à niveau

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

Remarques générales sur la mise à niveau

- Pour mettre NSX à niveau, vous devez réaliser une mise à niveau complète de NSX, y compris la mise à niveau du cluster d'hôte (les VIB de l'hôte sont alors mis à niveau). Pour obtenir des instructions, consultez le *Guide de mise à niveau de NSX*, y compris la section Mettre à niveau des clusters d'hôte.

- **Configuration système requise** : pour plus d'informations sur la configuration système requise lors de l'installation et de la mise à niveau de NSX, consultez la section Configuration système requise pour NSX dans la documentation de NSX.

- **Chemin de mise à niveau à partir de NSX 6.x :** La matrice d'interopérabilité des produits VMware fournit des détails sur les chemins de mise à niveau à partir de VMware NSX.
- **La mise à niveau de cross-vCenter NSX** est abordée dans le Guide de mise à niveau de NSX.

- **Les rétrogradations ne sont pas prises en charge :**
  - Capturez toujours une sauvegarde de NSX Manager avant de procéder à une mise à niveau.
  - Lorsque NSX a été mis à niveau correctement, NSX ne peut pas être rétrogradé.

- **Pour vérifier** que la mise à niveau vers NSX 6.3.x est réussie, consultez l'article 2134525 de la base de connaissances.
- Il n'existe pas de support pour les mises à niveau depuis vCloud Networking and Security vers NSX 6.3.x. Vous devez d'abord effectuer une mise à niveau vers une version 6.2.x prise en charge.

- **Interopérabilité** : consultez la Matrice d'interopérabilité des produits VMware pour tous les produits VMware pertinents avant d'effectuer la mise à niveau.
  - **Mise à niveau vers vSphere 6.5a ou version ultérieure** : lors de la mise à niveau de vSphere 5.5 ou 6.0 vers vSphere 6.5a ou version ultérieure, vous devez d'abord effectuer la mise à niveau vers NSX 6.3.x. Consultez Mise à niveau de vSphere dans un environnement NSX dans le *Guide de mise à niveau de NSX*.
    Remarque : NSX 6.2.x n'est pas compatible avec vSphere 6.5.
  - **Mise à niveau vers NSX 6.3.3 ou version ultérieure :** la version minimale prise en charge de l'interopérabilité vSphere for NSX passe de NSX 6.3.2 à NSX 6.3.3. Reportez-vous à la Matrice d'interopérabilité des produits VMware pour plus de détails.

- **Compatibilité des services de partenaires** : si votre site utilise des services de partenaires VMware pour Guest Introspection ou Network Introspection, vous devez examiner le Guide de compatibilité VMware avant la mise à niveau, afin de vérifier que le service de votre fournisseur est compatible avec cette version de NSX.
- **Plug-in Networking and Security** : Après la mise à niveau de NSX Manager, vous devez vous déconnecter et vous reconnecter à vSphere Web Client. Si le plug-in NSX ne s'affiche pas correctement, videz le cache du navigateur et effacez l'historique. Si le plug-in Networking and

Security ne figure pas dans vSphere Web Client, réinitialisez le serveur vSphere Web Client, comme expliqué dans le *Guide de mise à niveau de NSX*.

- **Environnements sans état** : pour les mises à niveau de NSX dans un environnement d'hôtes sans état, les nouveaux VIB sont pré-ajoutés au profil d'image d'hôte lors du processus de mise à niveau de NSX. Par conséquent, le processus de mise à niveau de NSX sur des hôtes sans état s'effectue selon les étapes suivantes :
  Dans les versions antérieures à NSX 6.2.0, une seule URL de NSX Manager permettait de trouver les VIB pour une version spécifique de l'hôte ESX. (L'administrateur n'avait alors qu'à connaître une seule URL, quelle que soit la version de NSX.) Dans NSX 6.2.0 et versions ultérieures, les nouveaux VIB NSX sont disponibles sur plusieurs URL. Pour trouver les VIB adéquats, vous devez procéder comme suit :

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

Notes de mise à niveau pour les composants NSX

Mise à niveau de NSX Manager

- Important : Si vous mettez à niveau NSX 6.2.0, 6.2.1 ou 6.2.2 vers NSX 6.3.5 ou version ultérieure, vous devez appliquer une solution avant de démarrer la mise à niveau. Consultez l'article 000051624 de la base de connaissances de VMware pour obtenir plus de détails.

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

- Si vous souhaitez mettre à niveau NSX 6.3.3 vers NSX 6.3.4 ou version ultérieure, vous devez d'abord suivre les instructions de solution de l'*article 2151719 de la base de connaissances de VMware*.

- Lorsque vous mettez à niveau NSX Manager vers NSX 6.3.6 ou version ultérieure, une sauvegarde est automatiquement réalisée et enregistrée localement dans le cadre du processus de mise à niveau. Pour plus d'informations, consultez Mettre à niveau NSX Manager.

Mise à niveau du contrôleur

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

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

  Lorsque les contrôleurs sont supprimés, cela supprime également les règles d'anti-affinité de DRS associées. Vous devez créer des règles d'anti-affinité dans vCenter pour empêcher les nouvelles VM de contrôleur de résider sur le même hôte.

  Pour plus d'informations sur les mises à niveau du contrôleur, consultez Mettre à niveau le cluster NSX Controller.

Mise à niveau du cluster d'hôte

- Dans NSX 6.3.3, les noms des VIB NSX changent. Les VIB esx-vxlan et esx-vsip sont remplacés par esx-nsxv si vous avez installé NSX 6.3.3 ou version ultérieure.
- **Mise à niveau et désinstallation sans redémarrage sur les hôtes** : dans vSphere 6.0 et versions ultérieures, une fois que vous avez effectué la mise à niveau vers NSX 6.3.x, toutes les modifications suivantes apportées à des VIB NSX ne requièrent pas de redémarrage. Au lieu de cela, les hôtes doivent entrer en mode de maintenance pour terminer la modification de VIB.

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

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

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

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

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

Mise à niveau de NSX Edge

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

  - **Compacte, Grande, Super grande** : 1 disque de 584 Mo + 1 disque de 512 Mo
  - **Extra grande** : 1 disque de 584 Mo + 1 disque de 2 Go + 1 disque de 256 Mo
- Les **clusters d'hôtes doivent être préparés pour NSX avant la mise à niveau des dispositifs NSX Edge** : La communication au niveau du plan de gestion entre les dispositifs NSX Manager et Edge via le canal VIX n'est plus prise en charge à partir de la version 6.3.0. Seul le canal de bus de messages est pris en charge. Lorsque vous effectuez une mise à niveau à partir de NSX 6.2.x ou version antérieure vers NSX 6.3.0 ou version ultérieure, vous devez vérifier que les clusters d'hôtes où sont déployés les dispositifs NSX Edge sont préparés pour NSX, et que l'état de l'infrastructure de messagerie s'affiche en VERT. Si les clusters d'hôtes ne sont pas préparés pour NSX, la mise à niveau du dispositif NSX Edge échouera. Reportez-vous à Mise à niveau de NSX Edge dans le *Guide de mise à niveau de NSX* pour plus de détails.
- **Mise à niveau d'Edge Services Gateway (ESG)** :
  À partir de NSX 6.2.5, la réservation de ressources est réalisée au moment de la mise à niveau de NSX Edge. Lorsque vSphere HA est activé sur un cluster disposant de ressources insuffisantes,

l'opération de mise à niveau peut échouer en raison de contraintes vSphere HA non respectées. Pour éviter de tels échecs de mise à niveau, procédez comme suit avant de mettre une passerelle ESG à niveau :

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

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

1. Veillez toujours à ce que votre installation suive les meilleures pratiques établies pour vSphere HA. Consultez l'article 1002080 de la base de connaissances.
2. Utilisez l'API de configuration de réglage NSX : `PUT https://<NSXManager>/api/4.0/edgePublish/tuningConfiguration` en veillant à ce que les valeurs de `edgeVCpuReservationPercentage` et `edgeMemoryReservationPercentage` respectent les ressources disponibles pour le facteur de forme (voir les valeurs par défaut dans le tableau ci-dessus).

- **Désactiver l'option de démarrage de machine virtuelle de vSphere lorsque vSphere HA est activé et que des dispositifs Edge sont déployés.** Après avoir mis à niveau vos dispositifs NSX Edge de la version 6.2.4 ou antérieure vers la version 6.2.5 ou ultérieure, vous devez désactiver l'option de démarrage de machine virtuelle de vSphere pour chaque dispositif NSX Edge dans un cluster dans lequel vSphere HA est activé et des dispositifs Edge sont déployés. Pour cela, ouvrez vSphere Web Client, recherchez l'hôte ESXi sur lequel réside la machine virtuelle NSX Edge, cliquez sur Gérer > Paramètres et, sous Machines virtuelles, sélectionnez Démarrage/Arrêt de la VM, cliquez sur Modifier et vérifiez que la machine virtuelle est en mode Manuel (c'est-à-dire qu'elle n'est pas ajoutée à la liste Démarrage/Arrêt automatique).
- **Avant de procéder à la mise à niveau vers NSX 6.2.5 ou version ultérieure, vérifiez que toutes les listes de chiffrement d'équilibrage de charge sont séparées par un signe deux-points.** Si votre liste de chiffrement utilise un autre séparateur (par exemple, des virgules), effectuez un appel PUT à `https://nsxmgr_ip/api/4.0/edges/EdgeID/loadbalancer/config/applicationprofiles` et remplacez chaque liste *<ciphers>* dans *<clientSsl>* et *<serverSsl>* par une liste séparée par des deux-points. Par exemple, le segment pertinent du corps de demande peut ressembler à ce qui suit. Répétez cette procédure pour tous les profils d'application :

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

```
    <ciphers>AES128-SHA:AES256-SHA:ECDHE-ECDSA-AES256-SHA</ciphers>
    <serviceCertificate>certificate-4</serviceCertificate>
  </serverSsl>
  ...
</applicationProfile>
```

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

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

Mise à niveau de Guest Introspection

- Les VM Guest Introspection contiennent désormais des informations supplémentaires pour identifier l'hôte dans un fichier XML sur la machine. Lors de la connexion à la VM Guest Introspection, le fichier « /opt/vmware/etc/vami/ovfEnv.xml » doit inclure des informations sur l'identité de l'hôte.

Notes de mise à niveau pour FIPS

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

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

Conformité FIPS

- **NSS et OpenSwan** : le VPN IPsec NSX Edge utilise le module de chiffrement Mozilla NSS. En raison de problèmes de sécurité critiques, cette version de NSX utilise une version plus récente de NSS

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

Historique de révision du document

15 novembre 2018 : Première édition.
3 mars 2019 : Deuxième édition. Ajout du problème résolu 2249307.
13 mai 2019. Troisième édition. Mise à jour de la section Mise à niveau du cluster d'hôtes.

Problèmes résolus

Les problèmes résolus sont regroupés comme suit :

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

- **Problème résolu 2207483 : Latence élevée pour le trafic acheminé horizontal et vertical**
  TxWorld de VM générant le trafic acheminé prend 100 % de CPU, ce qui entraîne une latence élevée.

- **Problème résolu 2188666 : Impossible de se connecter à la passerelle avec un numéro de port à 5 chiffres à l'aide de la CLI de client Linux SSLVPN**
  Vous devez utiliser l'interface utilisateur graphique de client SSLVPN sous Linux pour vous connecter à la passerelle avec un numéro de port à 5 chiffres, car cela fonctionne avec l'interface utilisateur graphique, mais la CLI de Linux SSLVPN fonctionne avec des numéros de port contenant jusqu'à 4 chiffres.

- **Problème résolu 2185457 : Augmentation de la latence réseau des charges de travail pontées**
  Les charges de travail avec un trafic élevé (pps) sur des réseaux pontés peuvent entraîner une latence entre VLAN et VXLAN.

- **Problème résolu 2182874 : Impossible d'utiliser un ID VDR si des ID VDR se chevauchent sur les sites**
  La plage de segments d'un site doit être modifiée si plusieurs sites présentent un chevauchement de plages de segments lorsque vous tentez de mettre ce site dans multi-vc.

- **Problème résolu 2181650 : Acceptez GARP comme réponse valide lors de l'envoi d'une demande ARP d'actualisation de l'entrée ARP**
  Certains anciens périphériques envoient GARP comme réponse à une demande ARP.

- **Problème résolu 2181435 : Dans ESX 5.5, Hostd se bloque lors de l'interrogation des statistiques**
  Dans ESX 5.5, Hostd se bloque lors de l'interrogation des statistiques. Hostd doit être redémarré.

- **Problème résolu 2179054 : Empêchement du redémarrage du pilote IXGBE lors de l'installation**

et des mises à niveau de NSX
Il existe une panne réseau de 5 à 10 secondes des services sur l'hôte.

- Problème résolu 2178950 : Interruption du trafic sur plus de deux machines virtuelles de vCenter pour le même dispositif Edge lorsque la haute disponibilité (HA) est activée
  Une interruption du trafic est visible sur plus de deux machines virtuelles de vCenter pour le même dispositif Edge lorsque la haute disponibilité (HA) est activée. La restauration est effectuée par la modification des dispositifs ou un changement de position du dispositif entraîne le blocage des VM et par conséquent l'interruption du réseau.

- Problème résolu 2177514 : dans certains cas, le ping DaD est retransmis en retour, provoquant la détection d'adresses IP en double par le processus DaD
  L'événement système signale une fausse adresse IP en double détectée.

- Problème résolu 2176316 : Le nom du dispositif Edge n'est pas mis à jour dans la règle de pare-feu
  Lorsque le nom du dispositif Edge est modifié dans l'interface utilisateur Edge, l'interface utilisateur du pare-feu indique toujours l'ancien nom

- Problème résolu 2172005 : Le voisinage BGP bagotte lorsque la commande de CLI « show ip bgp » est émise
  Lorsque BGP apprend des itinéraires avec AS_PATH contenant plus de 126 caractères et que la commande « show ip bgp » est émise, la pile de routage redémarre. Évolution de l'itinéraire et panne possible du trafic jusqu'à ce que BGP converge de nouveau.

- Problème résolu 2171616 : Le processus client Windows SSL VPN se bloque lorsque le nom d'hôte ESG ne peut pas être résolu
  Lorsque le proxy HTTP est configuré et que le nom d'hôte ESG ne peut pas être résolu, le processus client se bloque.

- Problème résolu 2167176 : Saturation des dispositifs Edge de DLR avec partition tmpfs avec haute disponibilité activée
  Le répertoire /var/run (tmpfs) se remplit complètement lorsque la haute disponibilité a été activée. Lorsqu'il est plein, cela empêche le fonctionnement des configurations.

- Problème résolu 2164068 : Partition tmpfs Edge complète après un certain temps lorsque la haute disponibilité est activée
  La resynchronisation est utilisée pour synchroniser des fichiers entre les VM Edge d'une paire HA. En raison de la façon dont la resynchronisation a été compilée, chaque invocation périodique de resynchronisation générait un message d'erreur journal qui était enregistré dans un fichier journal sur la partition tmpfs. Après un certain temps, la partition devient complète, ce qui affecte sérieusement le fonctionnement normal du dispositif Edge.

- Problème résolu 2156094 : Impossible de se connecter à la passerelle avec un numéro de port à 5 chiffres à l'aide de la CLI de client Linux SSL VPN
  Vous devez utiliser l'interface utilisateur graphique de client SSL VPN sous Linux pour vous connecter à la passerelle avec un numéro de port à 5 chiffres, car cela fonctionne avec l'interface utilisateur graphique, mais la CLI de Linux SSL VPN fonctionne avec des numéros de port contenant jusqu'à 4 chiffres.

- Problème résolu 2152060 : Le moteur de service de surveillance (Nagios) sur Edge présente une fuite de mémoire
  L'équilibrage de charge n'est pas non plus fonctionnel lorsque sa configuration utilise le service de surveillance pour aucune mémoire.

- Problème résolu 2140512 : Après la mise à niveau vers la version 6.3.x ou ultérieure, les entrées manquantes de la zone de transport (vdnscope) dans la base de données MP entraînent des erreurs avec VXLAN et la mise en réseau logique
  Erreurs VXLAN et de réseau logique sur des clusters préparés pour NSX.

- Problème résolu 2134760 : L'installation du client Mac SSL VPN s'est terminée avec succès, mais impossible d'exécuter l'application
  Le client ne s'ouvre pas, même si l'installation est réussie.

- Problème résolu 2100704 : NSX Edge peut perdre les connexions VMCI à NSX Manager dans certains scénarios
  Les dispositifs Edge ne sont plus gérables, ce qui entraîne l'impossibilité de transférer des configurations aux dispositifs Edge.

- Problème résolu 2092516 : Plusieurs travailleurs de surveillance mettent à jour l'état de membre de pool en même temps
  L'équilibrage de charge ne fonctionne pas correctement, car du trafic met du temps à distribuer au serveur défectueux ou un serveur sain n'a jamais de trafic à gérer.

- Problème résolu 2078866 : Au redémarrage de l'hôte, nsxv-vib échoue dans refreshHostdNetstackCache()
  Les performances de débit Rx VXLAN peuvent être réduites.

- Problème résolu 2028337 : Les cinq processus consommant le plus de CPU ne s'affichent pas lorsque l'utilisation du CPU Edge est supérieure à 90 %
  Lorsque l'utilisation du CPU Edge est supérieure à 90 %, une notification est envoyée au gestionnaire affichant une liste des cinq processus consommant le plus de CPU, car le dispositif Edge a été démarré. Cette liste n'affiche probablement pas les cinq premiers utilisateurs de CPU à ce moment précis, ce qui complique le diagnostic des problèmes d'utilisation du CPU.

- Problème résolu 1983497 : Un écran violet s'affiche lorsqu'une modification du basculement de pont et une modification de la configuration de pont se produisent en même temps
  Lorsqu'une modification du basculement de pont et une modification de la configuration de pont se produisent en même temps, cela peut entraîner un blocage et un écran violet. Le risque de blocage est faible.

- Problème résolu 2181633 : La suppression ARP d'adresses IP de sous-interface de VM invitées échoue.
  La résolution ARP de ces interfaces est un peu plus longue que la normale (1 seconde) pour la première fois.

- Problème résolu 2170329 : La configuration DNS ne parvient pas à s'appliquer sur l'interface du client Windows SSLVPN
  La requête DNS échoue, ce qui affecte l'accès.

Problèmes résolus généraux

- Problème résolu 2183198 : L'interface utilisateur affiche une erreur lors de la récupération d'un port depuis un commutateur ToR qui ne dispose d'aucun port
  Si un commutateur physique sur une passerelle matérielle ne contient aucun port, l'interface utilisateur NSX génère une erreur lors de la tentative de récupération du port à partir du commutateur. L'erreur « Impossible d'extraire les informations de l'inventaire » s'affiche dans l'interface utilisateur lors de la tentative de récupération des informations sur le port.

- Problème résolu 2176000 : La différence de codage dans les messages envoyés par le plan de gestion et attendus par l'hôte a entraîné des noms de port de liaison montante non valides de DVS, ce qui entraîne l'échec de la résolution MAC
  DLR ne parvient pas à résoudre les adresses MAC des machines virtuelles sur les hôtes ESXi différents.

- Problème résolu 2170413 : API /api/3.0/ai/directorygroup ne fonctionne pas
  La valeur NullPointerException est générée à partir du serveur principal et l'API renvoie une erreur. Impossible d'automatiser le workflow.

- Problème résolu 2170395 : domain_object n'est pas synchronisé avec le tableau ai_group

Lorsque la page de Service Composer est chargée, la valeur SQLGrammarException est générée, car SQL contient une liste vide d'ID de groupe.

- **Problème résolu 2131680 : Les paquets de multidiffusion qui rencontrent une règle de pare-feu de rejet entraînent une journalisation excessive dans le journal vmkernel**
  Une journalisation excessive dans le journal vmkernel entraîne l'arrêt de la journalisation par l'hôte.

- **Problème résolu 2129177 : Si GI-SVM est supprimé ou retiré lors du processus de mise à niveau en mode de compatibilité descendante, le pare-feu d'identité via Guest Introspection (GI) ne fonctionnera pas, sauf si le cluster de GI est mis à niveau**
  Le pare-feu d'identité ne fonctionnera pas et aucun journal lié au pare-feu d'identité ne sera visible. La protection par pare-feu d'identité sera suspendue, sauf si le cluster est mis à niveau.

- **Problème résolu 2105632 : Les USVM tentent de synchroniser l'heure avec des serveurs NTP Google (externes).**
  Le service de synchronisation de l'heure a été modifié pour éviter ce comportement.

- **Problème résolu 2003396 : Les interfaces logiques DLR/itinéraires disparaissent après le redémarrage ou sur un nouvel hôte joint s'il existe un grand nombre d'itinéraires configurés**
  Les itinéraires ne sont pas visibles tels que configurés.

- **Problème 1960383 : Échec de la création du réseau en raison d'une expiration du délai lorsqu'un nombre élevé d'objets d'inventaire sont supprimés sur une courte période**
  Une expiration du délai de création du réseau se produit en raison d'un retard lors de la création de dvpg dans NSX.

- **Problème résolu 2058770 : un nombre excessif d'événements de connexion est généré sur vCenter, et une charge élevée se produit sur vCenter Server SSO**
  Un nombre excessif d'événements de connexion et une charge élevée se produisent sur vCenter Server SSO lorsque des utilisateurs de vCenter SSO effectuent de nombreuses requêtes d'API NSX durant un bref intervalle. Cela peut entraîner un comportement lent.

- **Problème résolu 2046427 : la modification de la stratégie d'association vmkNIC ou du groupe de ports LS DVS peut entraîner la panne de DP**
  Lors de la préparation de l'hôte (VXLAN), si l'utilisateur définit la stratégie d'association vmkNIC, la stratégie d'association de liaison montante sur DVS est définie en conséquence. Tout nouveau Les DVS PG du commutateur logique qui sont créés reçoivent également cette stratégie d'association.

- **Problème résolu 2178339 : rsyslog 8.15.0-7.ph1 a supprimé la ligne ExecReload dans le fichier de service systemd, ce qui entraîne la mauvaise journalisation de /var/log/syslog et /var/log/messages**
  Cela entraîne l'occupation à 100 % de l'espace disque par la partition /var/log donc les nouveaux journaux ne peuvent pas être écrits.

- **Problème résolu 2146879 : Dans une installation autonome, la synchronisation forcée ne synchronise pas ToR et les liaisons ToR**
  Dans une installation autonome, lorsque la liaison HW ou la configuration de nœud de transport HW n'est pas synchronisée entre le plan de gestion et le contrôleur, la synchronisation forcée ne peut pas synchroniser la configuration. Les configurations ToR ne peuvent pas être synchronisées avec le contrôleur si des liaisons ToR ne sont pas synchronisées.

- **Problème résolu 2146749 : L'hôte ESXi perd la configuration d'ID de paramètres régionaux après le redémarrage**
  L'hôte reçoit le mauvais ID de paramètres régionaux et les itinéraires correspondants sont vidés.

- **Problème résolu 2200396 : Les instances de VDR sont recréées sur l'hôte ESXi dans le site secondaire après le basculement**
  Interruption du trafic et panne réseau d'environ 40 secondes après le basculement.

- **Problème résolu 2100296 : Le plug-in NSX 6.3.5 Web Client n'affiche aucun NSX Manager après la désactivation de SSL/TLS 1.0 sur les instances de vCenter/PSC**
  À cause de la désactivation de SSL/TLS 1.0 sur les instances de vCenter, NSX interrompt la communication avec des instances de vCenter, NSX ou ESX. vCenter Application ne communiquera pas avec NSX Manager.

- **Problème résolu 2077492 : NSX Manager crée automatiquement un ID ipsecsite pour les sites ipsec déjà présents**
  - NSX Manager crée automatiquement un ID ipsecsite pour les sites ipsec déjà présents.
  - La mise à niveau de NSX for vSphere de la version 6.2.x à la version 6.3.5 ou 6.4.0a peut introduire des siteIds en double pour les sites Ipsec.
  - Lorsque des siteIds en double sont introduits, la configuration ipsec suivante échoue.
  - Une erreur semblable à celle-ci s'affiche : [13646] [Ipsec] ID de sites Ipsec en double ipsecsite-id trouvés.
- **Problème résolu 2177097 : Lorsque vous utilisez l'appel API /api/2.0/vdn/config/segments pour créer un pool avec 1 ID de segment, il échoue avec « L'ID de segment est en dehors de la plage, la plage valide est 5000-16777215 »**
  Lorsque vous utilisez l'API /api/2.0/vdn/config/segments, si vous fournissez la même valeur de début et de fin lors de la création d'un segment de valeur unique, il échoue avec une erreur.

- **Problème résolu 2172267 : La suppression de NSX Edge lors de l'absence de réponse de l'hôte entraîne des objets orphelins dans vCenter**
  L'instance Edge sur NSX Manager est supprimée, mais le dispositif Edge est toujours présent dans vCenter et sert de chemin de données jusqu'à ce que NSX Manager marque ce dispositif Edge comme orphelin et supprime le dispositif Edge du processus de nettoyage. Il n'existe aucun moyen de supprimer le dispositif Edge de NSX Manager.

- **Problème résolu 2097255 : Les interruptions SNMP ne sont pas envoyées lorsque FIPS est activé sur le dispositif NSX Manager**
  Aucune interruption SNMP n'est reçue.

Problèmes résolus de NSX Controller

- **Problème résolu 2181306 : Le contrôleur manque de mémoire et ne peut pas fournir le service normalement**
  Le contrôleur prend en charge une interface ssh pour l'interrogation de l'appartenance au cluster et l'état. Si un client y accède et ne ferme pas les sessions, le contrôleur maintient les sessions actives indéfiniment. Avec suffisamment de sessions ouvertes, le contrôleur manque de mémoire.

Problèmes résolus de NSX Manager

- **Problème résolu 2171653 : L'analyse de sécurité sur NSX Manager signale « En-tête de sécurité HTTP non détecté »**
  L'analyse de sécurité signale ce problème. Des attaques de détournement de clic peuvent se produire.

- **Problème résolu 2161066 : La connexion du compteur d'utilisation avec NSX Manager échoue ou erreur de caractères XML non valides lors du traitement d'une réponse de l'API**
  La connexion du compteur d'utilisation avec NSX Manager échoue avec une erreur.

- **Problème résolu 2145195 : Alerte de pulsation pour tous les USVM et utilisation du CPU élevée sur NSX Manager**
  NSX Manager signale que tous les USVM n'ont pas répondu à la pulsation. Son utilisation du CPU élevée est causée par une session postgres.

- **Problème résolu 2144825 : Partition racine du gestionnaire pleine en raison de nombreux fichiers nsx-tcserver-wrapper.log**
  L'interface utilisateur NSX n'est pas accessible et beaucoup d'autres services cessent de fonctionner en raison du manque d'espace.

- **Problème résolu 2141490 : désynchronisation entre la liaison ToR sur NSX Manager et le contrôleur**
  Impossible de modifier la liaison matérielle sur un commutateur logique ou de supprimer la configuration. L'interface utilisateur affiche l'erreur suivante : « Échec de l'opération sur le contrôleur. {0} »

- **Problème résolu 2066631 : Un message d'erreur contextuel s'affiche lors de la connexion avec un rôle d'utilisateur Administrateur de sécurité et de la sélection d'une machine virtuelle**
  Le message d'erreur « Il n'existe aucune autorité pour accéder à l'objet global et la fonction library.tagging. Confirmer l'autorité de la fonction et l'étendue d'accès de l'objet » s'affiche dans une fenêtre contextuelle.

- **Problème résolu 2189810 : Les VM invitées protégées par PAN abandonnent le trafic lorsqu'un appel d'API est effectué par une solution d'insertion de services tierce à NSX Manager pour récupérer tous les SecurityGroups/IPSets configurés dans le cadre de l'insertion de services**
  NSX Manager renvoie une configuration vide pour les IPSets ou les SecurityGroups contenant des IPSets. En conséquence, les IPSets ou les SecurityGroups contenant des IPSets sont signalés vides sur le gestionnaire tiers. Les VM invitées protégées par PAN ou d'autres périphériques de pare-feu tiers abandonnent le trafic, car aucune règle ne correspond à une règle de refus par défaut.
  L'exécution de l'appel d'API https://NSXMGR_IP/api/2.0/si/serviceprofile/serviceprofile-10/containerset ne renvoie aucune adresse IP pour les IPSets ou les SecurityGroups contenant des IPSets.

  Toutes les VM invitées protégées par PAN ou d'autres périphériques de pare-feu tiers abandonnent le trafic, car aucune règle ne correspond à une règle de refus par défaut.

- **Problème résolu 2178700 : NSX Manager ne parvient pas à synchroniser les informations de LIF VDR avec le contrôleur si l'une des LIF VDR consomme un câble virtuel supprimé**
  Les opérations de LIF VDR échouent et l'utilisateur ne peut donc pas modifier la configuration de LIF.

- **Problème résolu 2249307 : L'ID de paramètres régionaux sur l'hôte ESXi est réinitialisé sur la valeur par défaut lors de la reconnexion de l'hôte ESXi à NSX Manager**
  Itinéraires de DLR manquants. Le DLR ne route plus le trafic. L'hôte reçoit un ID de paramètres régionaux incorrect et les itinéraires de DLR prévus ne sont pas conservés.

Problèmes résolus de mise à niveau et d'installation

- **Problème résolu 2133143 : Entrées de cluster périmées dans la base de données NSX**
  Certaines entrées de cluster périmées sont présentes dans la base de données NSX après la mise à niveau de la version 6.2.2 à la version 6.2.9.

- **Problème résolu 2112773 : Échec de la mise à niveau du contrôleur**
  Un contrôleur a échoué lors de la mise à niveau de la version 6.2.4 à la version 6.3.6.

Problèmes résolus des services de sécurité

- **Problème résolu 2098645 : Exception de pointeur nulle lorsque le groupe de sécurité fait référence à un groupe AD supprimé**
  Si un groupe AD (ai_group) est supprimé et qu'un groupe de sécurité fait référence à un groupe AD supprimé, la traduction SG -> VM génère une exception de pointeur nulle. La page de Service Composer ne se charge pas correctement.

- **Problèmes corrigés 2032988, 2032990, 2032991 : Vulnérabilité causée par CVE-2017-5753, CVE-2017-5715 (Specter) et CVE-2017-5754 (Meltdown)**
  Problèmes de sécurité potentiels causés par les vulnérabilités CVE-2017-5753, CVE-2017-5715 (Specter) et CVE-2017-5754 (Meltdown).

Problèmes connus

Les problèmes connus sont classés comme suit.

- Problèmes connus de mise à niveau et d'installation
- Problèmes connus généraux

Problèmes connus de mise à niveau et d'installation

- **Problème 2001988 : Lors de la mise à niveau du cluster d'hôtes NSX, le statut de l'installation dans l'onglet Préparation de l'hôte alterne entre « Non prêt » et « Installation en cours » pour l'intégralité du cluster lorsque chaque hôte du cluster est mis à niveau**
  Lors de la mise à niveau de NSX, le fait de cliquer sur « Mise à niveau disponible » pour le cluster préparé pour NSX déclenche la mise à niveau de l'hôte. Pour les clusters configurés avec DRS FULL AUTOMATIC, le statut de l'installation alterne entre « Installation en cours » et « Non prêt », même si les hôtes sont mis à niveau en arrière-plan sans problème.

  Solution : il s'agit d'un problème d'interface utilisateur et peut être ignoré. Attendez la mise à niveau du cluster d'hôtes pour continuer.

Problèmes connus généraux

- **Problème 2158182 : Le fait que le service DHCP et HA avec une adresse IP de liaison partagent la même vNic entraîne l'abandon du paquet de renouvellement de DHCP**
  Si l'adresse HA est une adresse locale de liaison (169.x.x.x), la récupération d'urgence peut abandonner le paquet de monodiffusion de renouvellement de DHCP à cette adresse locale de liaison, ce qui risque d'entraîner l'échec du renouvellement du client DHCP.

  Solution : sélectionnez une vNic sans service DHCP comme interface HA ou utilisez une adresse IP routable comme adresse IP d'interface HA, par exemple, 192.168.x.x

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

  Solution :

  1. Connectez-vous au dispositif virtuel NSX Manager.
  2. Sous Gestion des dispositifs, cliquez sur Gérer les paramètres des dispositifs.
  3. Dans le panneau Paramètres, cliquez sur Réseau.
  4. Cliquez sur Modifier en regard de Serveurs DNS.
  5. Dans le champ Domaines de recherche, remplacez tous les espaces par des virgules.
  6. Cliquez sur OK pour enregistrer les modifications.
- **Problème 1849042/1849043 : Verrouillage du compte d'administrateur lorsqu'une période de validité du mot de passe est configurée sur le dispositif NSX Edge**
  Si une période de validité du mot de passe est configurée pour l'utilisateur administrateur sur le dispositif NSX Edge, lorsque le mot de passe expire, il sera demandé à l'utilisateur de modifier le mot de passe à chaque connexion au dispositif pendant 7 jours. La non-modification du mot de passe entraînera le verrouillage du compte. En outre, si le mot de passe est modifié au moment de la connexion à l'invite de l'interface de ligne de commande, le nouveau mot de passe peut ne pas être conforme à la stratégie de mot de passe fort appliquée par l'interface utilisateur et REST.

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

- **Problème 2204383 : Le client SSLVPN Linux ne parvient pas à vérifier le certificat de serveur**

pour les versions de Linux qui utilisent sql cert9.db
La validation du serveur échoue avec une erreur interne.

Solution : aucune.