Guide de mise à niveau de NSX

Mise à jour 10
Modifié le 29 mars 2018
VMware NSX Data Center for vSphere 6.3

vmware®

Vous trouverez la documentation technique la plus récente sur le site Web de VMware, à l'adresse :

https://docs.vmware.com/fr/

Les dernières mises à jour produit se trouvent également sur le site Web de VMware.

Si vous avez des commentaires à propos de cette documentation, envoyez-les à l'adresse suivante :

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware France SAS.
Tour Franklin
100-101 Terrasse Boieldieu
92042 Paris La Défense 8 Cedex
France
www.vmware.com/fr

Table des matières

Guide de mise à niveau de NSX 4
Lire les documents de support 4
Configuration système requise pour NSX 5
Ports et protocoles requis par NSX 7

1 Mise à niveau de NSX 11
Préparation de la mise à niveau de NSX 11
Mettre à niveau vers NSX 6.3.x 29
Mettre à niveau vers NSX 6.3.x avec cross-vCenter NSX 45

2 Mise à niveau de vSphere dans un environnement NSX 65
Effectuer une mise à niveau vers ESXi 6.0 dans un environnement NSX 66
Effectuer une mise à niveau vers ESXi 6.5 dans un environnement NSX 69
Redéployer Guest Introspection après une mise à niveau d'ESXi 73

Guide de mise à niveau de NSX

Le *Guide de mise à niveau de NSX*, explique comment mettre à niveau le système VMware NSX® for vSphere® à l'aide de l'interface utilisateur de NSX Manager et de vSphere Web Client. Il contient des instructions de mise à niveau pas à pas et des suggestions de meilleures pratiques.

Public visé

Ce guide est destiné à tous ceux qui veulent mettre à niveau ou utiliser NSX dans un environnement VMware vCenter. Les informations qu'il contient sont destinées aux administrateurs système expérimentés qui sont familiarisés avec la technologie des machines virtuelles et les opérations de centres de données virtuels. Ce guide suppose que vous connaissez VMware vSphere, notamment VMware ESXi vCenter Server et vSphere Web Client.

Glossaire VMware Technical Publications

VMware Technical Publications fournit un glossaire de termes pouvant ne pas vous être familiers. Pour consulter la définition des termes utilisés dans la documentation technique VMware, visitez le site Web http://www.vmware.com/support/pubs.

Lire les documents de support

Outre ce guide de mise à niveau, VMware publie divers autres documents qui peuvent s'avérer utiles pour la mise à niveau.

Notes de mise à jour

Avant de commencer la mise à niveau, consultez les notes de mise à jour. Les problèmes de mise à niveau connus et leurs solutions sont documentés dans les notes de mise à jour de NSX. En les lisant avant de procéder à la mise à niveau, vous pourrez économiser du temps et des efforts. Reportez-vous à la section https://docs.vmware.com/fr/VMware-NSX-for-vSphere/index.html.

Matrice d'interopérabilité des produits

Vérifiez l'interopérabilité avec les autres produits VMware, tels que vCenter. Consultez l'onglet **Interopérabilité (Interoperability)** de la matrice d'interopérabilité des produits VMware à l'adresse http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php#interop&93=.

Matrice des chemins de mise à niveau

Assurez-vous que le chemin de mise à niveau depuis votre version actuelle de NSX jusqu'à la version vers laquelle vous effectuez la mise à niveau est bien pris en charge. Consultez l'onglet **Chemin de mise à niveau (Upgrade Path)** de la matrice d'interopérabilité des produits VMware à l'adresse http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php#upgrade&solution=93.

Guide de compatibilité

Vérifiez la compatibilité des solutions de partenaires avec NSX dans le Guide de compatibilité de VMware, à l'adresse http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security.

Configuration système requise pour NSX

Avant d'installer ou de mettre à niveau NSX, étudiez la configuration et les ressources de votre réseau. Vous pouvez installer une instance de NSX Manager par vCenter Server, une instance de Guest introspection par hôte ESXi™ et plusieurs instances de NSX Edge par centre de données.

Matériel

Ce tableau répertorie la configuration matérielle requise pour les dispositifs NSX.

Tableau 1. Configuration matérielle requise pour les dispositifs

Dispositif	Mémoire	vCPU	Espace disque
NSX Manager	16 Go (24 Go pour les grands déploiements de NSX)	4 (8 pour les grands déploiements de NSX)	60 Go
NSX Controller	4 Go	4	28 Go
NSX Edge	■ Compacte : 512 Mo ■ Grande : 1 Go ■ Super grande : 2 Go ■ Extra grande : 8 Go	■ Compacte : 1 ■ Grande : 2 ■ Super grande : 4 ■ Extra grande : 6	■ 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
Guest Introspection	2 Go	2	5 Go (l'espace provisionné est de 6,26 Go)

En règle générale, augmentez les ressources de NSX Manager à 8 vCPU et 24 Go de RAM si votre environnement géré par NSX contient plus de 256 hyperviseurs ou plus de 2 000 machines virtuelles.

Pour obtenir des détails concernant des tailles spécifiques, prenez contact avec le support VMware.

Pour obtenir des informations sur l'augmentation de la mémoire et l'allocation de vCPU pour vos dispositifs virtuels, consultez Allouer les ressources en mémoire et Modifier le nombre de cœurs de CPU virtuelles dans *Administration d'une machine virtuelle vSphere*.

L'espace provisionné d'un dispositif Guest Introspection indique 6,26 Go pour Guest Introspection. Cela s'explique par le fait que vSphere ESX Agent Manager crée un snapshot de la VM de service pour créer des clones rapides, lorsque plusieurs hôtes d'un cluster partagent un stockage. Pour plus d'informations sur la désactivation de cette option via ESX Agent Manager, consultez la documentation de *ESX Agent Manager*.

Latence du réseau

Vous devez vous assurer que la latence du réseau entre les composants est égale ou inférieure à la latence maximale décrite.

Tableau 2. Latence maximale du réseau entre les composants

Composants	Latence maximale
NSX Manager et NSX Controller	150 ms RTT
NSX Manager et hôtes ESXi	150 ms RTT
NSX Manager et système vCenter Server	150 ms RTT
NSX Manager et NSX Manager dans un environnement cross-vCenter NSX	150 ms RTT

Logiciels

Pour obtenir les informations d'interopérabilité les plus récentes, consultez le tableau d'interopérabilité du produit à l'adresse http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

Pour connaître les versions recommandées de NSX, vCenter Server et ESXi, consultez les notes de mise à jour de la version de NSX vers laquelle vous mettez à niveau. Des notes de mise à jour sont disponibles sur le site de documentation de NSX for vSphere : https://docs.vmware.com/fr/VMware-NSX-for-vSphere/index.html.

Pour qu'une instance de NSX Manager participe à un déploiement cross-vCenter NSX, les conditions suivantes sont requises :

Composant	Version
NSX Manager	6.2 ou une version ultérieure
NSX Controller	6.2 ou une version ultérieure
vCenter Server	6.0 ou une version ultérieure
ESXi	■ ESXi 6.0 ou une version ultérieure ■ Clusters d'hôtes préparés avec des VIB NSX 6.2 ou version ultérieure

Pour gérer toutes les instances de NSX Manager sur un déploiement Cross-vCenter NSX depuis une seule instance de vSphere Web Client, vous devez connecter vos instances vCenter Server avec Enhanced Linked Mode. Consultez Utilisation de Enhanced Linked Mode dans *Gestion de vCenter Server et des hôtes* .

Pour vérifier la compatibilité des solutions de partenaires avec NSX, consultez le Guide de compatibilité de VMware pour Mise en réseau et sécurité à l'adresse http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security.

Accès client et utilisateur

Les éléments suivants sont requis pour gérer votre environnement NSX :

- Résolution de nom directe et inverse. Elle est nécessaire si vous avez ajouté des hôtes ESXi par nom à l'inventaire vSphere, sinon NSX Manager ne peut pas résoudre les adresses IP.
- Autorisations d'ajouter des machines virtuelles et de les mettre sous tension.
- Accès à la banque de données qui contient les fichiers de machine virtuelle et droits d'accès au compte pour copier les fichiers dans cette banque de données
- Les cookies doivent être activés dans votre navigateur Web pour accéder à l'interface utilisateur de NSX Manager.
- Le port 443 doit être ouvert entre NSX Manager et l'hôte ESXi, vCenter Server et les dispositifs NSX à déployer. Ce port est requis pour télécharger le fichier OVF sur l'hôte ESXi afin de le déployer.
- Un navigateur Web pris en charge pour la version de vSphere Web Client que vous utilisez. Consultez Utilisation de vSphere Web Client dans la documentation *Gestion de vCenter Server et des hôtes* pour obtenir des détails.

Ports et protocoles requis par NSX

Les ports suivants doivent être ouverts pour que NSX fonctionne correctement.

Note Si vous disposez d'un environnement cross-vCenter NSX et que vos systèmes vCenter Server sont en mode Enhanced Linked Mode, chaque dispositif NSX Manager doit disposer de la connectivité requise vers chaque système vCenter Server dans l'environnement pour gérer n'importe quel dispositif NSX Manager à partir de n'importe quel système vCenter Server.

Tableau 3. Ports et protocoles requis par NSX for vSphere

Source	Cible	Port	Protocole	Objectif	Données sensibles	TLS	Authentification
PC client	NSX Manager	443	TCP	Interface d'administration de NSX Manager	Non	Oui	Authentification PAM
PC client	NSX Manager	443	TCP	Accès au VIB de NSX Manager	Non	Non	Authentification PAM
Hôte ESXi	vCenter Server	443	TCP	Préparation d'hôtes ESXi	Non	Non	
vCenter Server	Hôte ESXi	443	TCP	Préparation d'hôtes ESXi	Non	Non	

Tableau 3. Ports et protocoles requis par NSX for vSphere (Suite)

Source	Cible	Port	Protocole	Objectif	Données sensibles	TLS	Authentification
Hôte ESXi	NSX Manager	5671	TCP	RabbitMQ	Non	Oui	Utilisateur/mot de passe de RabbitMQ
Hôte ESXi	NSX Controller	1234	TCP	Connexion de l'agent User World	Non	Oui	
NSX Controller	NSX Controller	2878, 2888, 3888	TCP	Cluster de contrôleurs - Synchronisation de l'état	Non	Oui	IPsec
NSX Controller	NSX Controller	7777	TCP	Port RPC inter-contrôleurs	Non	Oui	IPsec
NSX Controller	NSX Controller	30865	TCP	Cluster de contrôleurs - Synchronisation de l'état	Non	Oui	IPsec
NSX Manager	NSX Controller	443	TCP	Communication contrôleur-gestionnaire	Non	Oui	Utilisateur/Mot de passe
NSX Manager	vCenter Server	443	TCP	vSphere Web Access	Non	Oui	
NSX Manager	vCenter Server	902	TCP	vSphere Web Access	Non	Oui	
NSX Manager	Hôte ESXi	443	TCP	Connexion de gestion et de provisionnement	Non	Oui	
NSX Manager	Hôte ESXi	902	TCP	Connexion de gestion et de provisionnement	Non	Oui	
NSX Manager	Serveur DNS	53	TCP	Connexion au client DNS	Non	Non	
NSX Manager	Serveur DNS	53	UDP	Connexion au client DNS	Non	Non	
NSX Manager	Serveur Syslog	514	TCP	Connexion Syslog	Non	Non	
NSX Manager	Serveur Syslog	514	UDP	Connexion Syslog	Non	Non	
NSX Manager	Serveur de temps NTP	123	TCP	Connexion au client NTP	Non	Oui	
NSX Manager	Serveur de temps NTP	123	UDP	Connexion au client NTP	Non	Oui	
vCenter Server	NSX Manager	80	TCP	Préparation de l'hôte	Non	Oui	
Client REST	NSX Manager	443	TCP	API REST de NSX Manager	Non	Oui	Utilisateur/Mot de passe

Tableau 3. Ports et protocoles requis par NSX for vSphere (Suite)

Source	Cible	Port	Protocole	Objectif	Données sensibles	TLS	Authentification
VXLAN Tunnel End Point (VTEP)	VXLAN Tunnel End Point (VTEP)	8472 (valeur par défaut avant NSX 6.2.3) ou 4789 (par défaut dans les nouvelles installations de NSX 6.2.3 et versions ultérieures)	UDP	Encapsulation du réseau de transport entre VTEP	Non	Oui	
Hôte ESXi	Hôte ESXi	6999	UDP	ARP sur LIF VLAN	Non	Oui	
Hôte ESXi	NSX Manager	8301, 8302	UDP	Synchronisation DVS	Non	Oui	
NSX Manager	Hôte ESXi	8301, 8302	UDP	Synchronisation DVS	Non	Oui	
VM Guest Introspection	NSX Manager	5671	TCP	RabbitMQ	Non	Oui	Utilisateur/mot de passe de RabbitMQ
Instance principale de NSX Manager	Instance secondaire de NSX Manager	443	TCP	Service de synchronisation universelle de cross-vCenter NSX	Non	Oui	
Instance principale de NSX Manager	vCenter Server	443	TCP	vSphere API	Non	Oui	
Instance secondaire de NSX Manager	vCenter Server	443	TCP	vSphere API	Non	Oui	
Instance principale de NSX Manager	Cluster de contrôleur universel de NSX	443	TCP	API REST de NSX Controller	Non	Oui	Utilisateur/Mot de passe

Tableau 3. Ports et protocoles requis par NSX for vSphere (Suite)

Source	Cible	Port	Protocole	Objectif	Données sensibles	TLS	Authentification
Instance secondaire de NSX Manager	Cluster de contrôleur universel de NSX	443	TCP	API REST de NSX Controller	Non	Oui	Utilisateur/Mot de passe
Hôte ESXi	Cluster de contrôleur universel de NSX	1234	TCP	Protocole de plan de contrôle NSX	Non	Oui	
Hôte ESXi	Instance principale de NSX Manager	5671	TCP	RabbitMQ	Non	Oui	Utilisateur/mot de passe de RabbitMQ
Hôte ESXi	Instance secondaire de NSX Manager	5671	TCP	RabbitMQ	Non	Oui	Utilisateur/mot de passe de RabbitMQ

Mise à niveau de NSX

1

Ce chapitre contient les rubriques suivantes :

- Préparation de la mise à niveau de NSX
- Mettre à niveau vers NSX 6.3.x
- Mettre à niveau vers NSX 6.3.x avec cross-vCenter NSX

Préparation de la mise à niveau de NSX

Pour garantir le bon déroulement de la mise à niveau de NSX, consultez les notes de mise à jour afin de prendre connaissance des problèmes de mise à niveau, suivez la séquence de mise à niveau appropriée et assurez-vous que l'infrastructure est correctement préparée pour la mise à niveau.

Attention 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 Manager a été mis à niveau correctement, NSX ne peut pas être rétrogradé.

VMware vous recommande de réaliser la mise à niveau lors d'une période de maintenance décidée par votre entreprise.

Vous pouvez suivre les directives suivantes comme liste de contrôle préalable à la mise à niveau.

1. Vérifiez que vCenter répond à la configuration système requise de NSX. Reportez-vous à Configuration système requise pour NSX.
2. Si des services de partenaires Guest Introspection ou Network Extensibility sont déployés, vérifiez la compatibilité avant la mise à niveau :
   - Dans certains cas, NSX peut être mis à niveau sans incidence sur les solutions partenaires. Toutefois, si votre solution partenaire n'est pas compatible avec la version de NSX vers laquelle vous effectuez la mise à niveau, vous devez mettre à niveau la solution partenaire vers une version compatible avant de procéder à la mise à niveau de NSX.
   - Consultez le Guide de compatibilité de VMware pour Networking and Security. Reportez-vous à la section http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security.
   - Consultez la documentation des partenaires pour obtenir des détails sur la compatibilité et la mise à niveau.

3 Si Data Security est présent dans votre environnement, désinstallez-le avant d'effectuer la mise à niveau vers NSX. Data Security n'est pas pris en charge dans la version NSX 6.3.x. Reportez-vous à Désinstaller NSX Data Security.

4 Si une passerelle matérielle (VTEP matériel) est installée dans votre environnement, la mise à niveau vers NSX 6.3.0 et 6.3.1 est bloquée. Pour procéder à la mise à niveau, contactez le support VMware. Pour plus d'informations, reportez-vous à https://kb.vmware.com/kb/2148511. La mise à niveau vers NSX 6.3.2 est autorisée.

5 Si vous disposez d'un dispositif NSX 5.5 ou d'un dispositif NSX Edge d'une version antérieure, procédez à leur mise à niveau vers NSX 6.x avant d'effectuer leur mise à niveau vers NSX 6.3.x.

6 Si vous effectuez la mise à niveau vers NSX 6.3.3, le cluster NSX Controller doit contenir trois nœuds de contrôleur. S'il en contient moins de trois, vous devez ajouter des nœuds supplémentaires avant de commencer la mise à niveau. Consultez la section Déployer le cluster NSX Controller du *Guide d'installation de NSX* pour savoir comment ajouter des nœuds de contrôleur.

7 Déterminez les instances de NSX Manager à mettre à niveau dans la même fenêtre de maintenance.

   - Si vous disposez d'un environnement cross-vCenter NSX, vous devez mettre à niveau l'instance principale et toutes les instances secondaires de NSX Manager vers la même version NSX dans une fenêtre de maintenance unique.
   - Si plusieurs instances de NSX Manager sont connectées à des systèmes vCenter Server qui utilisent le même serveur SSO, toutes les combinaisons de version de NSX Manager ne sont pas prises en charge. Vous devez planifier la mise à niveau de vos instances de NSX Manager afin de disposer d'une configuration prise en charge à la fin de la fenêtre de maintenance.
     - Toutes les instances de NSX Manager utilisant la même version de NSX sont prises en charge.
     - Les instances de NSX Manager utilisant une version différente de NSX sont prises en charge si NSX 6.4.0 ou version ultérieure est installé sur au moins une instance de NSX Manager et si NSX 6.3.3 ou version ultérieure est installé sur toutes les autres instances de NSX Manager.

8 Vérifiez que vous disposez d'une sauvegarde actuelle des composants de NSX Manager, de vCenter et de NSX. Reportez-vous à la section Sauvegarde et restauration de NSX.

9 Créez un bundle de support technique.

10 Vérifiez que la résolution des noms de domaine directe et inverse fonctionne à l'aide de la commande nslookup.

11 Si VUM est utilisé dans l'environnement, vérifiez que l'indicateur bypassVumEnabled est réglé sur vrai dans vCenter. Ce paramètre configure EAM pour installer les VIB directement sur les hôtes ESXi même lorsque VUM est installé et/ou non disponible. Consultez http://kb.vmware.com/kb/2053782.

12 Téléchargez et organisez le bundle de mise à niveau, validez avec md5sum. Reportez-vous à la section Télécharger le bundle de mise à niveau de NSX et vérifier le total de contrôle MD5.

13 Il vous est recommandé de suspendre toutes les opérations dans l'environnement jusqu'à ce que toutes les sections de la mise à niveau soient terminées.

14 N'arrêtez ni ne supprimez les composants ou les dispositifs NSX avant d'y être invité.

Évaluer les besoins en termes de licence lors de la mise à niveau de NSX

NSX a introduit un nouveau modèle de licence en mai 2016.

Si vous disposez d'un contrat de support actif, lorsque vous effectuez la mise à niveau de NSX 6.2.2 ou version antérieure vers NSX 6.2.3 ou version ultérieure, votre licence existante est convertie en licence NSX Enterprise et vous serez autorisé à utiliser les mêmes fonctionnalités dans l'offre Enterprise.

Pour plus d'informations sur les éditions de licence NSX et les fonctionnalités associées, voir https://kb.vmware.com/kb/2145269.

Impacts opérationnels des mises à niveau de NSX

Le processus de mise à niveau de NSX peut prendre un certain temps. Il est important de comprendre l'état opérationnel des composants de NSX lors d'une mise à niveau, et notamment de pouvoir déterminer si seuls certains hôtes ont été mis à niveau ou si les dispositifs NSX Edge n'ont pas encore été mis à niveau.

VMware recommande d'effectuer en une seule fois la mise à niveau de tous les composants de NSX pour limiter le temps d'interruption et la confusion chez les utilisateurs de NSX qui ne peuvent pas accéder à certaines fonctions de gestion de NSX pendant la mise à niveau. Toutefois, si cela n'est pas possible sur votre site, les informations ci-dessous peuvent aider les utilisateurs de NSX à déterminer les fonctionnalités qui restent disponibles pendant la mise à niveau.

La mise à niveau d'un déploiement de NSX se déroule de la façon suivante :

NSX Manager —> NSX Controller Cluster —> Cluster d'hôtes NSX —> Routeurs logiques distribués —> Guest Introspection

ESG (Edge Services Gateways) peut être mis à niveau à tout moment après la mise à niveau de NSX Manager.

Important Avant de commencer la mise à niveau, lisez Préparation de la mise à niveau de NSX et les *Notes de mise à jour de NSX for vSphere* pour obtenir des informations détaillées sur les conditions préalables et sur les problèmes connus liés à la mise à niveau.

Mise à niveau de NSX Manager

Planification de la mise à niveau de NSX Manager :

- Dans un environnement cross-vCenter NSX, vous devez d'abord mettre à niveau l'instance principale de NSX Manager, puis les instances secondaires de NSX Manager.
- Dans un environnement cross-vCenter NSX, vous devez mettre à niveau toutes les instances de NSX Manager au cours de la même période de maintenance.

Impact lors de la mise à niveau de NSX Manager :

- La configuration de NSX Manager utilise vSphere Web Client et l'API est bloquée.
- La communication entre les machines virtuelles existantes reste opérationnelle.
- Le provisionnement de nouvelles machines virtuelles reste opérationnel dans vSphere, mais les nouvelles machines ne peuvent pas être connectées à NSX ni déconnectées des commutateurs logiques pendant la mise à niveau de NSX Manager.
- Pendant la mise à niveau de NSX Manager dans un environnement cross-vCenter NSX, n'apportez aucune modification aux objets universels tant que la mise à niveau de l'instance principale et de toutes les instances secondaires de NSX Manager n'est pas terminée. Cela inclut la création, la mise à jour ou la suppression d'objets universels, ainsi que des opérations impliquant des objets universels (par exemple, application d'une balise de sécurité universelle à une VM).

Après la mise à niveau de NSX Manager :

- La configuration de NSX peut être modifiée librement.
- À ce stade, si de nouveaux dispositifs NSX Controller doivent être déployés, ils le sont avec la version qui correspond au cluster NSX Controller existant jusqu'à la mise à niveau du cluster NSX Controller.
- La configuration existante de NSX peut être modifiée. De nouveaux commutateurs logiques, routeurs logiques et passerelles Edge Services Gateway peuvent être déployés.
- Pour le pare-feu distribué, si de nouvelles fonctionnalités sont introduites après la mise à niveau, vous ne pouvez pas les utiliser tant que tous les hôtes ne sont pas mis à niveau.
- Selon la version de NSX, une fois le dispositif NSX Manager mis à niveau, l'état d'intégrité du canal de communication peut s'afficher comme Inconnu pour le plan de contrôle. Vous devez effectuer une mise à niveau du contrôleur et de l'hôte pour que l'état s'affiche comme Actif.

Mise à niveau du cluster NSX Controller

Planification de la mise à niveau de NSX Controller :

- Vous pouvez mettre à niveau le cluster NSX Controller après celle de NSX Manager.
- Dans un environnement cross-vCenter NSX, vous devez mettre à niveau toutes les instances de NSX Manager avant de mettre à niveau le cluster NSX Controller.
- VMware recommande de mettre à niveau en une seule fois le cluster NSX Controller et NSX Manager.

Impact lors de la mise à niveau de NSX Controller :

- La création et la modification de réseaux logiques sont bloquées pendant la mise à niveau. N'apportez aucune modification à la configuration du réseau logique pendant la mise à niveau du cluster NSX Controller.
- Ne provisionnez pas de nouvelles machines virtuelles pendant ce processus. Par ailleurs, ne déplacez pas de machines virtuelles et n'autorisez pas DRS à en déplacer pendant la mise à niveau.

- En cas d'état de non-majorité temporaire pendant le processus, la mise en réseau des machines virtuelles existantes est préservée.
- N'autorisez pas le changement des itinéraires dynamiques pendant la mise à niveau.

Après la mise à niveau de NSX Controller :

- La configuration peut être modifiée.

Mise à niveau des hôtes NSX

Planification de la mise à niveau du cluster d'hôtes NSX :

- Vous pouvez mettre à niveau les clusters d'hôtes après la mise à niveau de NSX Manager et du cluster NSX Controller.
- Vous pouvez mettre à niveau vos clusters d'hôtes séparément de NSX Manager et du cluster NSX Controller.
- Vous n'avez pas besoin de mettre à niveau tous les clusters d'hôtes en une seule fois. Toutefois, si le pare-feu distribué est activé, il existe une limite sur la migration des machines virtuelles entre des clusters avec différentes versions NSX :
  - La migration de machines virtuelles à partir de clusters avec une version ultérieure de NSX vers des clusters avec une version antérieure de NSX peut entraîner une perte de connectivité réseau des machines virtuelles.
  - La migration de machines virtuelles à partir de clusters avec une version antérieure de NSX vers des clusters avec une version ultérieure de NSX est prise en charge.
- Les nouvelles fonctionnalités de la version NSX installées sur NSX Manager apparaissent dans vSphere Web Client et l'API, mais elles risquent de ne pas fonctionner tant que les VIB ne sont pas mis à niveau.
- Pour profiter de toutes les nouvelles fonctionnalités d'une version de NSX, mettez à niveau les clusters d'hôtes afin que les VIB hôtes correspondent à la version de NSX Manager.

Impact lors de la mise à niveau du cluster d'hôtes NSX :

- Les modifications de la configuration ne sont pas bloquées sur NSX Manager.
- La communication contrôleur-hôte bénéficie d'une compatibilité descendante, ce qui signifie que les contrôleurs mis à niveau peuvent communiquer avec les hôtes qui ne sont pas mis à niveau.
- La mise à niveau est effectuée cluster par cluster. Si DRS est activé sur le cluster, il gère l'ordre de mise à niveau des hôtes.
- Les hôtes en cours de mise à niveau doivent être placés en mode de maintenance, ce qui nécessite la mise hors tension des machines virtuelles ou leur évacuation vers d'autres hôtes. Cette opération peut être effectuée manuellement ou à l'aide de DRS.
- Les ajouts et modifications au niveau du réseau logique sont autorisés.
- Le provisionnement de nouvelles machines virtuelles reste opérationnel sur les hôtes qui ne sont pas en mode de maintenance.

Mise à niveau de NSX Edge

Planification de la mise à niveau de NSX Edge :

- Vous pouvez mettre à niveau les dispositifs NSX Edge séparément des autres composants NSX.
- Vous pouvez mettre à niveau les routeurs logiques après NSX Manager, le cluster NSX Controller et les clusters d'hôtes.
- Vous pouvez mettre à niveau un dispositif ESG même si la mise à niveau du cluster NSX Controller ou des clusters d'hôtes n'a pas encore été effectuée.
- Vous n'avez pas besoin de mettre à niveau tous les dispositifs NSX Edge en une seule fois.
- Si une mise à niveau est disponible pour NSX Edge mais que vous ne l'avez pas effectuée, tout changement de taille, des ressources ou de la banque de données, toute activation du débogage avancé et toute activation de HA sur le dispositif seront bloqués jusqu'à ce que NSX Edge soit mis à niveau.

Impact lors de la mise à niveau de NSX Edge :

- Les modifications de la configuration sont bloquées sur le périphérique NSX Edge en cours de mise à niveau. Les ajouts et modifications au niveau des commutateurs logiques sont autorisés. Le provisionnement de nouvelles machines virtuelles reste opérationnel.
- Le transfert de paquets est interrompu temporairement.
- Dans NSX Edge 6.0 et versions ultérieures, les contiguïtés OSPF sont retirées lors d'une mise à niveau si un redémarrage normal n'est pas activé.

Après la mise à niveau de NSX Edge :

- Les modifications de la configuration ne sont pas bloquées.

Mise à niveau de Guest Introspection

Planification de la mise à niveau de Guest Introspection :

- Vous pouvez mettre à niveau Guest Introspection après NSX Manager, le cluster NSX Controller et les clusters d'hôtes.
- Reportez-vous à la documentation du partenaire pour obtenir des informations sur la mise à niveau de la solution correspondante.

Impact lors de la mise à niveau de Guest Introspection :

- Les VM dans le cluster NSX ne sont plus protégées lorsqu'une modification est apportée aux VM, telle que des ajouts de VM, des migrations par vMotion ou des suppressions de VM.

Après la mise à niveau de Guest Introspection :

- Les VM sont protégées lors des ajouts de VM, des migrations par vMotion et des suppressions de VM.

Comprendre le mode FIPS et la mise à niveau de NSX

À partir de NSX 6.3.0, vous pouvez activer le mode FIPS, qui active les suites de chiffrement conformes aux FIPS.

Attention Lorsque vous effectuez la mise à niveau depuis une version de NSX antérieure à NSX 6.3.0 vers NSX 6.3.0 ou une 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.

Mise à niveau de NSX et statut FIPS

Tableau 1-1. Statut du mode FIPS des composants NSX après la mise à niveau vers NSX 6.3.x.

Composant NSX	Statut du mode FIPS
NSX Manager	Après la mise à niveau vers la version 6.3.x, le mode FIPS est disponible et activé sur les dispositifs NSX Manager. N'activez pas le mode FIPS avant la fin de la mise à niveau de tous les composants NSX, ni avant d'avoir activé FIPS sur tous les dispositifs NSX Edge.
Cluster NSX Controller	Après la mise à niveau vers la version 6.3.x, le cluster NSX Controller est compatible avec FIPS. Ce paramètre n'est pas configurable.
Cluster d'hôtes NSX	Après la mise à niveau vers la version 6.3.x, les clusters d'hôtes NSX sont compatibles avec FIPS. Ce paramètre n'est pas configurable.
NSX Edge	Après la mise à niveau vers la verison 6.3.x, le mode FIPS est disponible et activé sur les dispositifs NSX Edge. N'activez pas le mode FIPS avant la fin de la mise à niveau de l'ensemble des composants NSX.
VM du service Guest Introspection	Après la mise à niveau vers la version 6.3.x, la VM du service Guest Introspection est compatible avec FIPS. Ce paramètre n'est pas configurable.

Activer FIPS

Si vous effectuez une mise à niveau vers NSX 6.3.x et que vous souhaitez activer le mode FIPS, procédez comme suit :

1. Vérifiez que des solutions de partenaire sont certifiées pour le mode FIPS. Reportez-vous au Guide de compatibilité de VMware à l'adresse http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security. Pour plus d'informations, consultez la documentation des partenaires.
2. Mise à niveau de NSX Manager vers NSX 6.3.0 ou une version ultérieure.
3. Mise à niveau du cluster NSX Controller vers NSX 6.3.0 ou une version ultérieure.
4. Mise à niveau de tous les clusters d'hôtes qui utilisent des charges de travail NSX vers NSX 6.3.0 ou une version ultérieure.
5. Mise à niveau de tous les dispositifs NSX Edge vers NSX 6.3.0 ou une version ultérieure.
6. Si Guest Introspection est installé, mettez-le à niveau sur tous les clusters d'hôtes vers NSX 6.3.0 ou une version ultérieure.

7 Activez le mode FIPS sur les dispositifs NSX Edge. Consultez la rubrique Modifier le mode FIPS sur NSX Edge dans le *Guide d'administration de NSX*.

8 Activez le mode FIPS sur les dispositifs NSX Manager. Consultez la rubrique Modifier le mode FIPS et les paramètres TLS sur NSX Manager dans le *Guide d'administration de NSX*.

Vérifier l'état de marche de NSX

Il est important de tester l'état de marche de NSX avant de lancer la mise à niveau. Si vous ne le faites pas, vous ne pourrez pas déterminer si des problèmes détectés après la mise à niveau sont dus à la mise à niveau ou s'ils existaient auparavant.

Ne partez pas du principe que tout fonctionne avant de lancer la mise à niveau de l'infrastructure NSX. Vous devez d'abord vérifier que c'est bien le cas.

Procédure

1 Notez les versions actuelles de NSX Manager, vCenter Server, ESXi et NSX Edge.

2 Identifiez les ID et les mots de passe des utilisateurs administratifs.

3 Vérifiez que vous pouvez vous connecter aux composants suivants :

- vCenter Server
- Interface utilisateur Web de NSX Manager
- Dispositifs de passerelles Edge Services Gateway
- Dispositifs de routeurs logiques distribués
- Dispositifs NSX Controller

4 Vérifiez que les segments VXLAN sont fonctionnels.

Veillez à définir correctement la taille des paquets et à inclure le bit de non-fragmentation.

- Exécutez un ping entre deux machines virtuelles qui se trouvent sur le même commutateur logique, mais sur deux hôtes différents.
  - Depuis une machine virtuelle Windows : ping -l 1472 –f <dest VM>
  - Depuis une machine virtuelle Linux : ping -s 1472 –M do <dest VM>
- Exécutez un ping entre les interfaces VTEP de deux hôtes.
  - ping ++netstack=vxlan -d -s 1572 <dest VTEP IP>

  Note Pour obtenir l'adresse IP VTEP d'un hôte, recherchez l'adresse IP vmknicPG sur la page **Gérer > Mise en réseau > Commutateurs virtuels (Manage > Networking > Virtual Switches)** de l'hôte.

5 Lancez un ping depuis une machine virtuelle pour valider la connectivité verticale.

6 Inspectez visuellement l'environnement NSX pour vous assurer que tous les indicateurs d'état sont verts/normaux/déployés.
   - Vérifiez **Installation > Gestion (Installation > Management)**.
   - Vérifiez **Installation > Préparation de l'hôte (Installation > Host Preparation)**.
   - Vérifiez **Installation > Préparation du réseau logique > Transport VXLAN (Installation > Logical Network Preparation > VXLAN Transport)**.
   - Vérifiez **Commutateurs logiques (Logical Switches)**.
   - Vérifiez **Dispositifs NSX Edge (NSX Edges)**.
7 Notez les états BGP et OSPF sur les périphériques NSX Edge.
   - `show ip ospf neighbor`
   - `show ip bgp neighbor`
   - `show ip route`
8 Vérifiez que syslog est configuré.

   Reportez-vous à la rubrique Spécifier le serveur Syslog.
9 Si possible, créez des composants dans l'environnement avant la mise à niveau et vérifiez qu'ils fonctionnent.
   - Créez un commutateur logique.
   - Créez une passerelle Edge Services Gateway et un routeur logique distribué.
   - Connectez une machine virtuelle au nouveau commutateur logique et vérifiez qu'elle fonctionne.
10 Validez les connexions UWA de netcpad et vsfwd.
   - Sur un hôte ESXi, exécutez `esxcli network vswitch dvs vmware vxlan network list --vds-name=<VDS_name>` et vérifiez l'état de connexion du contrôleur.
   - Dans NSX Manager, exécutez la commande `show tech-support save session` et recherchez « 5671 » pour vous assurer que tous les hôtes sont connectés à NSX Manager.
11 (Facultatif) Si vous disposez d'un environnement de test, testez la mise à niveau et la fonctionnalité après la mise à niveau avant de mettre un environnement de production à niveau.

Désinstaller NSX Data Security

NSX Data Security a été déconseillé dans NSX 6.2.3 et a été supprimé dans NSX 6.3.0. Vous devez désinstaller NSX Data Security avant de passer à NSX 6.3.x.

Procédure

1 Dans l'onglet **Installation**, cliquez sur **Déploiements de services (Service Deployments)**.
2 Sélectionnez le service NSX Data Security, puis cliquez sur l'icône **Supprimer un déploiement de services (Delete Service Deployment)** ( ).

3 Dans la boîte de dialogue Confirmer la suppression, cliquez sur **Supprimer maintenant (Delete now)** ou sélectionnez la date et l'heure auxquelles la suppression doit prendre effet.

4 Cliquez sur **OK**.

Sauvegarde et restauration de NSX

Une sauvegarde appropriée de l'ensemble de vos composants NSX est indispensable pour pouvoir restaurer votre système en cas d'échec.

La sauvegarde NSX Manager contient toute la configuration de NSX, notamment les contrôleurs, les entités de commutation et de routage logiques, la sécurité, les règles de pare-feu et tout ce que vous configurez dans l'interface utilisateur ou l'API de NSX Manager. La base de données vCenter et les éléments liés, comme les commutateurs virtuels, doivent être sauvegardés séparément.

Nous vous recommandons d'effectuer au minimum des sauvegardes régulières de NSX Manager et vCenter. La planification et la fréquence de vos sauvegardes peuvent varier en fonction des besoins de votre entreprise et de vos procédures opérationnelles. Nous vous recommandons d'effectuer régulièrement des sauvegardes de NSX lors des périodes pendant lesquelles vous modifiez fréquemment votre configuration.

Vous pouvez effectuer des sauvegardes de NSX Manager à la demande ou sur une base horaire, quotidienne ou hebdomadaire.

Nous vous recommandons d'effectuer des sauvegardes dans les cas suivants :

- Avant une mise à niveau de NSX ou vCenter.
- Après une mise à niveau de NSX ou vCenter.
- Après le déploiement et la configuration initiale de composants NSX au jour 0, par exemple après la création d'instances de NSX Controller, de commutateurs logiques, de routeurs logiques, de passerelles Edge Services Gateway et de règles de sécurité et de pare-feu.
- Après des changements de topologie ou d'infrastructure.
- Après un changement majeur au jour 2.

Pour pouvoir restaurer l'intégralité du système à une date spécifiée, nous vous recommandons de synchroniser les sauvegardes des composants NSX (par exemple, NSX Manager) avec la sauvegarde planifiée d'autres composants d'interaction, tels que vCenter, les systèmes de gestion du Cloud, les outils opérationnels, etc.

Sauvegarder et restaurer NSX Manager

Vous pouvez configurer les sauvegardes et les restaurations de NSX Manager à partir de l'interface Web du dispositif virtuel de NSX Manager ou via l'API de NSX Manager. Vous pouvez planifier des sauvegardes sur une base horaire, quotidienne ou hebdomadaire.

Le fichier de sauvegarde est enregistré à un emplacement FTP ou SFTP distant auquel NSX Manager a accès. Les données de NSX Manager comprennent des configurations, des événements et des tables de journaux d'audit. Les tables de configuration sont incluses dans chaque sauvegarde.

Vous ne pouvez effectuer des restaurations que sur une version de NSX Manager identique à celle de la sauvegarde. Il est donc important de créer un fichier de sauvegarde avant et après une mise à niveau de NSX : une sauvegarde pour l'ancienne version et une autre pour la nouvelle version.

Sauvegarder les données de NSX Manager

Vous pouvez sauvegarder les données de NSX Manager en effectuant une sauvegarde à la demande ou planifiée.

Procédure

1. Connectez-vous au dispositif virtuel NSX Manager.
2. Sous Gestion des dispositifs, cliquez sur **Sauvegardes et restaurations (Backups & Restore)**.
3. Pour spécifier l'emplacement de sauvegarde, cliquez sur **Modifier (Change)** en regard de Paramètres de serveur FTP.
   a. Tapez l'adresse IP ou le nom d'hôte du système de sauvegarde.
   b. Dans le menu déroulant **Protocole de transfert (Transfer Protocol)**, sélectionnez **SFTP** ou **FTP**, selon ce que la destination prend en charge.
   c. Modifiez le port par défaut, si nécessaire.
   d. Tapez le nom d'utilisateur et le mot de passe requis pour se connecter au système de sauvegarde.
   e. Dans le champ **Répertoire de sauvegarde (Backup Directory)**, tapez le chemin absolu d'enregistrement des sauvegardes.

      Pour connaître le chemin absolu, connectez-vous au serveur FTP, accédez au répertoire que vous souhaitez utiliser, puis exécutez la commande de répertoire de travail actuel (`pwd`). Par exemple :

```
PS C:\Users\Administrator> ftp 192.168.110.60
Connected to 192.168.110.60.
220 server-nfs FTP server ready.
User (192.168.110.60:(none)): admin
331 Password required for admin.
Password:
230 User admin logged in.
ftp> ls
200 PORT command successful.
150 Opening BINARY mode data connection for 'file list'.
datastore-01
226 Transfer complete.
ftp: 22 bytes received in 0.00Seconds 22000.00Kbytes/sec.
ftp> cd datastore-01
250 CWD command successful.
ftp> pwd
257 "/datastore-01" is current directory.
```

f Tapez une chaîne de texte dans **Préfixe du nom de fichier (Filename Prefix)**.

Ce texte sera ajouté devant chaque nom de fichier de la sauvegarde pour faciliter la reconnaissance sur le système de sauvegarde. Si vous tapez par exemple **ppdb**, la sauvegarde résultante sera nommée *ppdbHH_MM_SS_DayDDMonYYYY*.

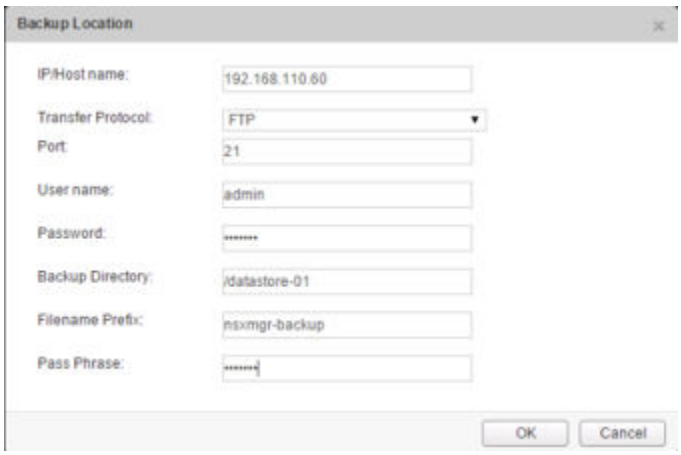
Note Le répertoire de sauvegarde doit contenir 100 fichiers au maximum. Si le nombre de fichiers dans le répertoire dépasse la limite, vous recevrez un message d'avertissement.

g Tapez la phrase secrète pour sécuriser la sauvegarde.

Cette phrase secrète est nécessaire pour restaurer la sauvegarde.

h Cliquez sur **OK**.

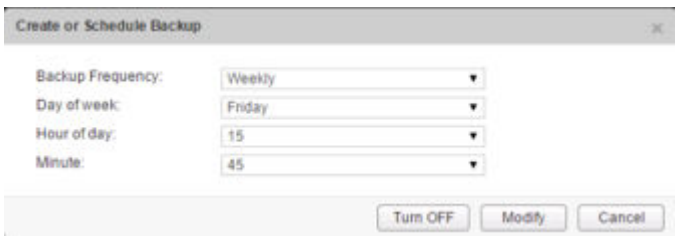
Par exemple :



4 Pour effectuer une sauvegarde à la demande, cliquez sur **Sauvegarde (Backup)**.

Un nouveau fichier est ajouté sous **Historique de sauvegarde (Backup History)**.

5 Pour planifier des sauvegardes, cliquez sur **Modifier (Change)** en regard de Planification.



a Dans le menu déroulant **Fréquence de sauvegarde (Backup Frequency)**, sélectionnez **Toutes les heures (Hourly)**, **Quotidien (Daily)** ou **Hebdomadaire (Weekly)**. Les menus déroulants Jour de semaine, Heure de la journée et Minute sont désactivés en fonction de la fréquence sélectionnée. Par exemple, si vous sélectionnez Quotidien, le menu déroulant Jour de semaine est désactivé, car ce champ ne s'applique pas à une fréquence quotidienne.

b Pour une sauvegarde hebdomadaire, sélectionnez le jour de la semaine où les données doivent être sauvegardées.

c Pour une sauvegarde hebdomadaire ou quotidienne, sélectionnez l'heure à laquelle la sauvegarde doit commencer.

d Sélectionnez la minute à laquelle commencer, puis cliquez sur **Planifier (Schedule)**.

6 Pour exclure de la sauvegarde les journaux et les données de flux, cliquez sur **Modifier (Change)** en regard de l'option Exclure.

a Sélectionnez les éléments à exclure de la sauvegarde.

b Cliquez sur **OK**.

7 Enregistrez l'adresse IP et le nom d'hôte de votre serveur FTP, vos informations d'identification, les détails du répertoire et votre phrase secrète. Ces informations sont nécessaires pour restaurer la sauvegarde.

Restaurer une sauvegarde de NSX Manager

La restauration de NSX Manager entraîne le chargement d'un fichier de sauvegarde sur un dispositif NSX Manager. Ce fichier de sauvegarde doit être enregistré à un emplacement FTP ou SFTP distant auquel NSX Manager a accès. Les données de NSX Manager comprennent des configurations, des événements et des tables de journaux d'audit.

Important Sauvegardez vos données en cours avant de restaurer un fichier de sauvegarde.

Conditions préalables

Avant de restaurer des données NSX Manager, nous vous recommandons de réinstaller le dispositif NSX Manager. La restauration sur un dispositif NSX Manager existant peut également fonctionner, mais elle n'est pas prise en charge. Il est considéré que le dispositif NSX Manager est défaillant et qu'un nouveau dispositif doit donc être déployé.

Il est recommandé de noter les paramètres actuels de l'ancien dispositif NSX Manager afin de les utiliser par la suite pour spécifier les informations sur l'adresse IP et sur l'emplacement de sauvegarde du nouveau dispositif NSX Manager déployé.

Procédure

1 Notez tous les paramètres du dispositif NSX Manager existant. Notez également les paramètres du serveur FTP.

2 Déployez un nouveau dispositif NSX Manager.

La version doit être identique à celle du dispositif NSX Manager sauvegardé.

3 Connectez-vous au nouveau dispositif NSX Manager.

4 Sous Gestion des dispositifs, cliquez sur **Sauvegardes et restaurations (Backups & Restore)**.

5 Dans les paramètres du serveur FTP, cliquez sur **Modifier (Change)** et ajoutez les paramètres du serveur FTP.

   Les champs **Adresse IP de l'hôte (Host IP Address)**, **Nom d'utilisateur (User Name)**, **Mot de passe (Password)**, **Répertoire de sauvegarde (Backup Directory)**, **Préfixe du nom de fichier (Filename Prefix)** et **Phrase secrète (Pass Phrase)** de l'écran Emplacement Sauvegarde doivent identifier l'emplacement de la sauvegarde à restaurer.

   La section **Historique de sauvegarde (Backup History)** affiche le dossier de sauvegarde.

   Note Si ce dernier n'apparaît pas dans la section **Historique de sauvegarde (Backup History)**, vérifiez les paramètres du serveur FTP. Vérifiez si vous pouvez vous connecter au serveur FTP et afficher le dossier de sauvegarde.

6 Dans la section **Historique de sauvegarde (Backup History)**, sélectionnez le dossier de sauvegarde nécessaire pour la restauration, puis cliquez sur **Restaurer (Restore)**.

   La restauration des données de NSX Manager commence.

La configuration de NSX est restaurée vers NSX Manager.

Attention Après la restauration d'une sauvegarde de NSX Manager, vous devrez peut-être prendre des mesures supplémentaires pour garantir le bon fonctionnement des dispositifs NSX Edge et des commutateurs logiques. Reportez-vous aux sections Restaurer des dispositifs NSX Edge et Résoudre les erreurs de désynchronisation sur des commutateurs logiques.

Restaurer des dispositifs NSX Edge

Lors d'une sauvegarde de données de NSX Manager, toutes les configurations de NSX Edge (routeurs logiques et passerelles Edge Services Gateway) sont sauvegardées.

Les sauvegardes individuelles de NSX Edge ne sont pas prises en charge.

Si vous disposez d'une configuration NSX Manager intacte, vous pouvez recréer une machine virtuelle de dispositif Edge ayant donné lieu à une erreur ou inaccessible en redéployant NSX Edge (cliquez sur **Redéployer le dispositif NSX Edge (Redeploy NSX Edge) ( )** dans vSphere Web Client). Reportez-vous à la section « Redéployer le dispositif NSX Edge » dans le *Guide d'administration de NSX*.

Attention Après la restauration d'une sauvegarde de NSX Manager, vous devrez peut-être prendre des mesures supplémentaires pour garantir le bon fonctionnement des dispositifs NSX Edge.

- Les dispositifs Edge créés après la dernière sauvegarde ne sont pas supprimés lors de la restauration. Vous devez supprimer la VM manuellement.
- Les dispositifs Edge supprimés après la dernière sauvegarde ne sont pas restaurés sauf s'ils sont redéployés.
- Si les emplacements configurés et actuels d'un dispositif NSX Edge enregistré dans la sauvegarde n'existent plus lorsque la sauvegarde est restaurée, les opérations telles que le redéploiement, la migration, l'activation ou la désactivation de HA, échouent. Vous devez modifier la configuration du dispositif et fournir des informations d'emplacement valides. Utilisez `PUT /api/4.0/edges/{edgeId}/appliances` pour modifier la configuration de l'emplacement du dispositif (*resourcePoolId*, *datastoreId*, *hostId* et *vmFolderId* si nécessaire). Reportez-vous à la section « Utilisation de la configuration du dispositif NSX Edge » dans le *Guide de NSX API*.

Si les modifications suivantes se sont produites depuis la dernière sauvegarde de NSX Manager, la configuration restaurée de NSX Manager et la configuration présente sur le dispositif NSX Edge seront différentes. Vous devez **Forcer la synchronisation (Force Sync)** du dispositif NSX Edge pour rétablir ces modifications sur le dispositif et garantir le bon fonctionnement du dispositif NSX Edge. Reportez-vous à la section « Forcer la synchronisation de NSX Edge avec NSX Manager » dans le *Guide d'administration de NSX*.

- Modifications effectuées via Pare-feu distribué pour preRules pour le pare-feu NSX Edge.
- Modifications dans l'appartenance des objets de regroupement.

Si les modifications suivantes se sont produites depuis la dernière sauvegarde de NSX Manager, la configuration restaurée de NSX Manager et la configuration présente sur le dispositif NSX Edge seront différentes. Vous devez **Redéployer (Redeploy)** le dispositif NSX Edge pour rétablir ces modifications sur le dispositif et garantir le bon fonctionnement du dispositif NSX Edge. Reportez-vous à la section « Redéployer le dispositif NSX Edge » dans le *Guide d'administration de NSX*.

- Modifications des paramètres du dispositif Edge :
  - HA a été activé ou désactivé
  - le dispositif est passé de l'état déployé à l'état non déployé
  - le dispositif est passé de l'état non déployé à l'état déployé
  - les paramètres de réservation de ressource ont été modifiés
- Modifications des paramètres de carte réseau virtuelle du dispositif Edge :
  - ajouter, supprimer ou déconnecter la carte réseau virtuelle
  - groupes de ports
  - ports de jonction
  - paramètres de clôture
  - stratégie de formation

Résoudre les erreurs de désynchronisation sur des commutateurs logiques

Si des commutateurs logiques ont été modifiés entre la sauvegarde de NSX Manager et la restauration de la sauvegarde, les commutateurs logiques peuvent signaler leur désynchronisation.

Procédure

1. Connectez-vous à vSphere Web Client.
2. Accédez à **Mise en réseau et sécurité (Networking & Security) > Commutateurs logiques (Logical Switches)**.
3. S'il est présent, cliquez sur le lien **Désynchronisé (Out of sync)** dans la colonne État pour afficher les détails de l'erreur.
4. Cliquez sur **Résoudre (Resolve)** pour recréer les groupes de ports de sauvegarde manquants pour le commutateur logique.

Sauvegarder des vSphere Distributed Switches

Vous pouvez exporter les configurations de groupes de ports distribués et de vSphere Distributed Switch dans un fichier.

Le fichier conserve les configurations de réseau valides, ce qui permet de distribuer ces configurations à d'autres déploiements.

Les paramètres de vSphere Distributed Switch et des groupes de ports sont inclus dans l'importation.

Il est recommandé d'exporter la configuration de vSphere Distributed Switch avant de préparer le cluster pour le protocole VXLAN. Pour en savoir plus, consultez le site http://kb.vmware.com/kb/2034602.

Sauvegarder vCenter

Afin de sécuriser votre déploiement NSX, il est important de sauvegarder votre base de données vCenter et de prendre des snapshots des machines virtuelles.

Reportez-vous à la documentation de vCenter correspondant à votre version pour obtenir des instructions et des conseils concernant les restaurations et les sauvegardes.

Pour en savoir plus sur les snapshots de machines virtuelles, consultez le site http://kb.vmware.com/kb/1015180.

Liens utiles pour vCenter 5.5 :

- http://kb.vmware.com/kb/2057353
- http://kb.vmware.com/kb/2034505
- http://www.vmware.com/files/pdf/techpaper/vmware-vcenter-server-availability-guide.pdf

Liens utiles pour vCenter 6.0 :

- https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.install.doc/GUID-539B47B4-114B-49BC-9736-F14058127ECA.html
- http://kb.vmware.com/kb/2110294

Gestion des sauvegardes de NSX Manager créées lors de la mise à niveau

Lorsque vous mettez à niveau NSX Manager vers NSX 6.3.6, une sauvegarde est réalisée et enregistrée localement dans le cadre du processus de mise à niveau. Vous devez contacter le support client de VMware pour restaurer cette sauvegarde. Cette sauvegarde automatique sert de recours en cas d'échec de la sauvegarde régulière.

Après la mise à niveau de NSX Manager, de nouvelles commandes sont disponibles en mode privilégié (**activer**) qui vous permettent de gérer les fichiers de sauvegarde. Vous pouvez utiliser ces commandes pour répertorier, copier ou supprimer les fichiers de sauvegarde.

Si vous ne les supprimez pas, les fichiers de sauvegarde restent jusqu'à la prochaine mise à niveau. Lorsque la mise à niveau suivante démarre, les fichiers de sauvegarde sont supprimés et une nouvelle sauvegarde est effectuée.

show backup

Répertoriez les fichiers de sauvegarde.

```
nsxmgr-01a.corp.local# show backup
total 3040
-rw-r--r-- 1 root root 3102752 Mar 23 01:12 backup_file
-rw-r--r-- 1 root root     230 Mar 23 01:12 backup_metadata
```

export backup

Copiez les fichiers de sauvegarde dans un autre emplacement.

```
nsxmgr-01a.corp.local# export backup scp root@backup-server:/backups
Exporting...
Password:
backup_file                                   100% 3030KB  19.8MB/s   00:00
backup_metadata                               100%  230    27.3KB/s   00:00
nsxmgr-01a.corp.local#
```

delete backup

Supprimez les fichiers de sauvegarde. Ne supprimez la sauvegarde que si vous êtes sûr que vous n'en avez plus besoin.

```
nsxmgr-01a.corp.local# delete backup
Do you want to delete the backup files (y|N)y
nsxmgr-01a.corp.local#
```

Télécharger le bundle de mise à niveau de NSX et vérifier le total de contrôle MD5

Le bundle de mise à niveau de NSX contient tous les fichiers nécessaires à la mise à niveau de l'infrastructure NSX. Avant la mise à niveau de NSX Manager, vous devez télécharger le bundle correspondant à la version souhaitée.

Conditions préalables

Un outil de calcul du total de contrôle MD5.

Procédure

1. Téléchargez le bundle de mise à niveau de NSX dans un emplacement accessible par NSX Manager. Le format du nom du fichier de bundle de mise à niveau est semblable à `VMware-NSX-Manager-upgrade-bundle-releaseNumber-NSXbuildNumber.tar.gz`.
2. Vérifiez que le nom de fichier de mise à niveau de NSX Manager se termine par tar.gz.

   Certains navigateurs peuvent modifier l'extension de fichier. Par exemple, si le fichier téléchargé porte le nom suivant :

   VMware-NSX-Manager-upgrade-bundle-6.x.x-xxxxx.gz

   Renommez-le comme suit :

   VMware-NSX-Manager-upgrade-bundle-6.x.x-xxxxx.tar.gz

   Si vous n'effectuez pas ce changement de nom, le message d'erreur suivant s'affiche après le téléchargement du bundle : « Nom de fichier de bundle de mise à niveau VMware-NSX-Manager-upgrade-bundle-6.x.x-xxxxx,gz non valide, les fichiers de mise à niveau doivent porter l'extension tar.gz ».
3. Utilisez un outil de calcul du total de contrôle MD5 pour comparer le total MD5 officiel du bundle indiqué sur le site Web de VMware au total MD5 calculé par l'outil.
   a. Dans l'outil, accédez au bundle de mise à niveau.
   b. Utilisez l'outil pour calculer le total de contrôle du bundle.
   c. Collez le total de contrôle indiqué sur le site Web de VMware.
   d. Comparez les deux totaux de contrôle dans l'outil.

   S'ils ne correspondent pas, téléchargez à nouveau le bundle de mise à niveau.

Mettre à niveau vers NSX 6.3.x

Pour passer à NSX 6.3.x, vous devez mettre à niveau les composants NSX dans l'ordre indiqué dans ce guide.

Les composants NSX doivent être mis à niveau dans l'ordre suivant :

1. Dispositif NSX Manager

2 Cluster NSX Controller

3 Clusters d'hôtes

4 NSX Edge (voir la remarque)

5 Guest Introspection

Note ESG (Edge Services Gateways) peut être mis à niveau à tout moment après la mise à niveau de NSX Manager. Toutefois, les routeurs logiques ne peuvent pas être mis à niveau tant que le cluster NSX Controller et les clusters d'hôtes n'ont pas été mis à niveau. Voir Impacts opérationnels des mises à niveau de NSX pour plus d'informations sur les dépendances de mise à niveau.

Le processus de mise à niveau est géré par NSX Manager. Si la mise à niveau d'un composant échoue ou est interrompue et si vous devez l'exécuter à nouveau ou la redémarrer, elle ne reprend pas depuis le début, mais à l'endroit où elle s'est arrêtée.

L'état de la mise à niveau est mis à jour pour chaque nœud et au niveau du cluster.

Mettre à niveau NSX Manager

La première étape du processus de mise à niveau de l'infrastructure NSX consiste à mettre à niveau le dispositif NSX Manager.

Lors de la mise à niveau, vous pouvez choisir de participer au Programme d'amélioration du produit (CEIP) pour NSX. Consultez le Programme d'amélioration du produit dans le *Guide d'administration de NSX* pour plus d'informations sur le programme, y compris comment participer ou quitter le programme.

Si vous procédez à la mise à niveau de NSX 6.3.0 ou version ultérieure, le téléchargement du bundle de mise à niveau et le démarrage de la mise à niveau peuvent se produire indépendamment. Pour démarrer une mise à niveau à partir d'un bundle de mise à niveau précédemment téléchargé, accédez à **Page d'accueil (Home) > Mise à niveau (Upgrade)** et cliquez sur **Commencer la mise à niveau (Begin Upgrade)**.

Lorsque vous mettez à niveau NSX Manager vers NSX 6.3.6, une sauvegarde est réalisée automatiquement et enregistrée localement dans le cadre du processus de mise à niveau. Reportez-vous à la section Gestion des sauvegardes de NSX Manager créées lors de la mise à niveau pour plus d'informations sur la gestion de ces fichiers de sauvegarde.

- Si la sauvegarde automatique réalisée pendant la mise à niveau échoue, la mise à niveau ne continue pas. Contactez le support client de VMware pour obtenir de l'aide.
- La sauvegarde automatique sert de recours en cas d'échec de votre sauvegarde régulière.
  - Effectuez toujours une sauvegarde régulière de NSX Manager avant toute mise à niveau. Pour plus d'informations, reportez-vous à Sauvegarder les données de NSX Manager. Vous pouvez restaurer cette sauvegarde sans l'aide du support client de VMware.
  - Si vous devez restaurer la sauvegarde automatique, vous devez contacter le support client de VMware.

Conditions préalables

- Validez l'utilisation du système de fichiers NSX Manager et exécutez un nettoyage si l'utilisation du système de fichiers est à 100 %.
  a Connectez-vous à NSX Manager et exécutez `show filesystems` pour afficher l'utilisation du système de fichiers.
  b Si l'utilisation est de 100 %, passez en mode privilégié (activer) et exécutez les commandes `purge log manager` et `purge log system`.
  c Redémarrez le dispositif NSX Manager pour que le nettoyage des journaux prenne effet.
- Vérifiez que la mémoire réservée du dispositif virtuel NSX Manager respecte la configuration système requise avant de procéder à la mise à niveau.

  Reportez-vous à la section Configuration système requise pour NSX.
- Si Data Security est présent dans votre environnement, désinstallez-le avant de mettre à niveau NSX Manager. Reportez-vous à la section Désinstaller NSX Data Security. Data Security a été supprimé de NSX 6.3.x.
- Sauvegardez votre configuration actuelle et téléchargez les journaux de support technique avant la mise à niveau. Reportez-vous à la section Sauvegarde et restauration de NSX.
- Téléchargez le bundle de mise à niveau et vérifiez le total de contrôle MD5. Reportez-vous à la section Télécharger le bundle de mise à niveau de NSX et vérifier le total de contrôle MD5.
- Assurez-vous de bien comprendre l'impact opérationnel de la mise à niveau de NSX Manager. Reportez-vous à la section Impacts opérationnels des mises à niveau de NSX.
- Vous devez mettre à niveau toutes les instances de NSX Manager dans un environnement cross-vCenter NSX dans la même fenêtre de maintenance.
- Déterminez les instances de NSX Manager à mettre à niveau dans la même fenêtre de maintenance.
  - Si vous disposez d'un environnement cross-vCenter NSX, vous devez mettre à niveau l'instance principale et toutes les instances secondaires de NSX Manager vers la même version NSX dans une fenêtre de maintenance unique.
  - Si plusieurs instances de NSX Manager sont connectées à des systèmes vCenter Server qui utilisent le même serveur SSO, toutes les combinaisons de version de NSX Manager ne sont pas prises en charge. Vous devez planifier la mise à niveau de vos instances de NSX Manager afin de disposer d'une configuration prise en charge à la fin de la fenêtre de maintenance.
    - Toutes les instances de NSX Manager utilisant la même version de NSX sont prises en charge.
    - Les instances de NSX Manager utilisant une version différente de NSX sont prises en charge si NSX 6.4.0 ou version ultérieure est installé sur au moins une instance de NSX Manager et si NSX 6.3.3 ou version ultérieure est installé sur toutes les autres instances de NSX Manager.

Procédure

1. Connectez-vous au dispositif virtuel NSX Manager.
2. Dans la page d'accueil, cliquez sur **Mettre à niveau (Upgrade)**.
3. Cliquez sur **Mettre à niveau (Upgrade)**, sur **Choisir un fichier (Choose File)** et accédez au fichier `VMware-NSX-Manager-upgrade-bundle-`*releaseNumber*`-`*NSXbuildNumber*`.tar.gz`. Cliquez sur **Continuer (Continue)** pour démarrer le téléchargement.

   Le statut de téléchargement s'affiche dans la fenêtre du navigateur.
4. Si vous voulez démarrer la mise à niveau plus tard, cliquez sur **Fermer (Close)** dans la boîte de dialogue Mettre à niveau.

   Lorsque vous êtes prêt à démarrer la mise à niveau, accédez à **Page d'accueil (Home) > Mise à niveau (Upgrade)** et cliquez sur **Commencer la mise à niveau (Begin Upgrade)**.
5. Dans la boîte de dialogue Mettre à niveau, sélectionnez si vous voulez activer SSH et si vous voulez participer au Programme d'amélioration du produit (CEIP) de VMware. Cliquez sur **Mettre à niveau (Upgrade)** pour démarrer la mise à niveau.

   L'état de la mise à niveau s'affiche dans la fenêtre du navigateur.

   Note La boîte de dialogue Mettre à niveau affiche un message indiquant que la sauvegarde automatique a été effectuée.

   Lorsque le processus de mise à niveau est terminé, la page de connexion à NSX Manager s'affiche.
6. Connectez-vous à nouveau au dispositif virtuel NSX Manager, puis dans la page d'accueil, cliquez sur **Mettre à niveau (Upgrade)**. Vérifiez que l'état de la mise à niveau est **Terminé (Complete)**, et que le numéro de build et de version en haut à droite correspond au bundle de mise à niveau que vous venez d'installer.

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 dans vSphere Web Client, videz le cache et l'historique de votre navigateur. Si cette étape n'est pas effectuée, vous pouvez voir un message d'erreur similaire à « Une erreur interne s'est produite - Erreur #1009 » lorsque vous modifiez la configuration de NSX dans vSphere Web Client.

Si l'onglet Networking and Security n'apparaît pas dans vSphere Web Client, réinitialisez le serveur vSphere Web Client :

- Dans vCenter 5.5, ouvrez https://<vcenter-ip>:5480 et redémarrez le serveur Web Client.

- Dans vCenter Server Appliance 6.0, connectez-vous au shell vCenter Server en tant qu'utilisateur racine et exécutez les commandes suivantes :

```
Command> shell.set --enabled True
Command> shell
localhost:~ # cd /bin
localhost:~ # service-control --stop vsphere-client
localhost:~ # service-control --start vsphere-client
```

- Dans vCenter Server 6.0 sous Windows, vous pouvez exécuter les commandes suivantes.

```
cd C:\Program Files\VMware\vCenter Server\bin
service-control --stop vspherewebclientsvc
service-control --start vspherewebclientsvc
```

Il est recommandé d'utiliser des clients Web différents pour gérer des instances de vCenter Server qui exécutent des versions différentes de NSX Manager, afin d'éviter les erreurs inattendues liées à l'exécution simultanée de plusieurs plug-ins NSX de version différente.

Après la mise à niveau de l'instance de NSX Manager, créez un fichier de sauvegarde de NSX Manager. Reportez-vous à la section Sauvegarde et restauration de NSX. La sauvegarde précédente de NSX Manager n'est valide que pour la version précédente.

Étape suivante

Mettez à niveau le cluster NSX Controller.

Mettre à niveau le cluster NSX Controller

Les contrôleurs de votre environnement sont mis à niveau au niveau du cluster. Si une mise à niveau est disponible pour un nœud de contrôleur, un lien correspondant s'affiche dans l'instance de NSX Manager.

Il est recommandé de procéder à la mise à niveau des contrôleurs lors d'une intervention de maintenance.

La mise à niveau de NSX Controller entraîne le téléchargement d'un fichier de mise à niveau sur chaque nœud de contrôleur. Les contrôleurs sont mis à niveau individuellement. Lors d'une mise à niveau, vous ne pouvez pas cliquer sur le lien **Mise à niveau disponible (Upgrade Available)** et les appels d'API pour la mise à niveau du cluster de contrôleurs sont bloqués tant que l'opération n'est pas terminée.

Si vous déployez de nouveaux contrôleurs avant la mise à niveau des contrôleurs existants, ils sont déployés sous l'ancienne version. Les nœuds de contrôleur doivent posséder la même version pour rejoindre un cluster.

Important Dans NSX 6.3.3, le système d'exploitation sous-jacent de NSX Controller est différent. 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 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.

Conditions préalables

- Vérifiez que l'état de tous les contrôleurs est normal. La mise à niveau est impossible dès lors qu'au moins un contrôleur est déconnecté. Pour reconnecter un contrôleur déconnecté, essayez de réinitialiser son dispositif virtuel. Dans la vue **Hôtes et clusters (Hosts and Clusters)**, cliquez avec le bouton droit sur le contrôleur et sélectionnez **Alimentation > Réinitialiser (Power > Reset)**.
- Un cluster NSX Controller valide contient trois nœuds de contrôleur. Connectez-vous à ces trois nœuds et exécutez la commande **show control-cluster status**.

```
controller-node# show control-cluster status

Type                Status                                          Since
--------------------------------------------------------------------------------
Join status:        Join complete                                   05/04 02:36:03
Majority status:    Connected to cluster majority                   05/19 23:57:23
Restart status:     This controller can be safely restarted         05/19 23:57:12
Cluster ID:         ff3ebaeb-de68-4455-a3ca-4824e31863a8
Node UUID:          ff3ebaeb-de68-4455-a3ca-4824e31863a8

Role                Configured status   Active status
--------------------------------------------------------------------------------
api_provider        enabled             activated
persistence_server  enabled             activated
switch_manager      enabled             activated
logical_manager     enabled             activated
directory_server    enabled             activated
```

  - Pour l'état de jointure, vérifiez que le nœud du contrôleur indique Jonction établie.
  - Pour l'état Majorité, vérifiez que le contrôleur est connecté à la majorité du cluster.
  - Pour l'ID de cluster, tous les nœuds de contrôleur d'un cluster doivent posséder un ID de cluster identique.
  - Pour l'état Configuré et l'état Actif, vérifiez que tous les rôles du contrôleur sont autorisés et activés.

- Assurez-vous de bien comprendre l'impact opérationnel de la mise à niveau de NSX Controller. Reportez-vous à la section Impacts opérationnels des mises à niveau de NSX.
- Si vous effectuez la mise à niveau vers NSX 6.3.3, le cluster NSX Controller doit contenir trois nœuds de contrôleur. S'il en contient moins de trois, vous devez ajouter des nœuds supplémentaires avant de commencer la mise à niveau. Consultez la section Déployer le cluster NSX Controller du *Guide d'installation de NSX* pour savoir comment ajouter des nœuds de contrôleur.

Procédure

- Accédez à **Accueil > Networking & Security > Installation (Home > Networking & Security > Installation)**, sélectionnez l'onglet **Gestion (Management)**, puis cliquez sur **Mise à niveau disponible (Upgrade Available)** dans la colonne **État du cluster de contrôleurs (Controller Cluster Status)**.

  Les contrôleurs de votre environnement sont mis à niveau et redémarrés individuellement. Une fois que vous avez lancé la mise à niveau, le système télécharge le fichier de mise à niveau, puis met à niveau, redémarre et met à jour l'état de mise à niveau de chaque contrôleur. Les champs suivants affichent l'état des contrôleurs :

  - La colonne **État du cluster de contrôleurs (Controller Cluster Status)** de la section NSX Manager indique l'état de mise à niveau du cluster. Au démarrage de la mise à niveau, l'état est **Téléchargement du fichier de mise à niveau (Downloading upgrade file)**. Une fois le fichier de mise à niveau téléchargé sur tous les contrôleurs du cluster, l'état passe à **En cours (In progress)**. Une fois que tous les contrôleurs du cluster ont été mis à niveau, l'état est **Complet (Complete)** et cette colonne ne s'affiche plus.
  - Dans la section Nœuds de NSX Controller, la colonne **État (Status)** affiche l'état de chaque contrôleur, qui est **Connecté (Connected)** ou **Normal** avant la mise à niveau, selon la version NSX d'origine. Lorsque les services de contrôleur sont arrêtés et que le contrôleur est redémarré, l'état passe à **Déconnecté (Disconnected)**. Une fois la mise à niveau de ce contrôleur terminée, l'état est **Connecté (Connected)**.
  - La colonne **État de la mise à niveau (Upgrade Status)** de la section des nœuds NSX Controller indique l'état de mise à niveau de chaque contrôleur. Elle indique tout d'abord **Téléchargement du fichier de mise à niveau (Downloading upgrade file)**, puis **Mise à niveau en cours (Upgrade in progress)** et enfin **Redémarrage (Rebooting)**. Une fois que le contrôleur a été mis à niveau, l'état **Mis à niveau (Upgraded)** s'affiche.

    Note Lorsque vous effectuez une mise à niveau à partir de NSX 6.3.2 ou version antérieure vers NSX 6.3.3 ou version ultérieure, l'état **Téléchargement du fichier de mise à niveau (Downloading upgrade file)** est remplacé par **En file d'attente pour la mise à niveau (Queued For Upgrade)**.

Lorsque la mise à niveau est terminée, la colonne **Version du logiciel (Software Version)** de la section des nœuds NSX Controller indique **6.3.***buildNumber* pour chaque contrôleur. Réexécutez la commande **show control-cluster status** pour vous assurer que les contrôleurs peuvent former une majorité. Si la majorité du cluster NSX Controller n'est pas rétablie, consultez les journaux des contrôleurs et de NSX Manager.

La durée moyenne de mise à niveau est de 6 à 8 minutes. Si la mise à niveau ne se termine pas avant le délai d'expiration (30 minutes), la colonne **État de la mise à niveau (Upgrade Status)** indique **Échec (Failed)**. Cliquez à nouveau sur **Mise à niveau disponible (Upgrade Available)** dans la section de NSX Manager pour reprendre la mise à niveau à l'endroit où elle s'est arrêtée.

Si des problèmes réseau ne permettent pas d'effectuer la mise à niveau en 30 minutes, vous devrez peut-être définir un délai plus long. Faites appel au support VMware pour diagnostiquer et résoudre les problèmes sous-jacents, et si nécessaire, prolonger le délai d'expiration de la mise à niveau.

Si la mise à niveau du contrôleur échoue, vérifiez la connectivité entre les contrôleurs et l'instance de NSX Manager.

Il peut arriver que la mise à niveau aboutisse pour le premier contrôleur et échoue pour le deuxième. Supposons que vous possédez un cluster contenant trois contrôleurs, que le premier est mis à niveau vers la nouvelle version et que le deuxième est en cours de mise à niveau. Si la mise à niveau de ce dernier échoue, il risque de rester déconnecté. Par ailleurs, le premier et le troisième contrôleur ne présentent plus la même version (l'un a été mis à niveau et l'autre non), ce qui ne leur permet pas de former une majorité. À ce stade, il est impossible de relancer la mise à niveau. Pour remédier au problème, créez un autre contrôleur. Le nouveau contrôleur présentera l'ancienne version, qui correspond à celle du troisième contrôleur, avec lequel il formera de ce fait une majorité. La mise à niveau peut alors être relancée. Voir Redéployer une instance de NSX Controller dans le *Guide de dépannage de NSX* pour des instructions sur la création d'un autre contrôleur.

Étape suivante

Mettez les clusters d'hôtes à niveau.

Mettre à niveau des clusters d'hôtes

Après la mise à niveau de NSX Manager et des instances de NSX Controller, vous pouvez mettre à jour les clusters appropriés de votre environnement.

La mise à niveau des clusters d'hôtes met à niveau les VIB de NSX.

Si vous effectuez une mise à niveau de NSX 6.2.x ou d'une version antérieure, ou de NSX 6.3.0 ou d'une version ultérieure avec ESXi 5.5, les hôtes doivent être redémarrés pour terminer la mise à niveau.

- Si DRS est activé sur le cluster, lorsque vous cliquez sur **Tout résoudre (Resolve all)**, DRS tente de redémarrer les hôtes d'une manière contrôlée permettant aux machines virtuelles de continuer de fonctionner. Les machines virtuelles sont déplacées vers d'autres hôtes du cluster et les hôtes passent en mode de maintenance et sont redémarrés.

- Si DRS n'est pas activé sur le cluster, vous devez mettre les machines virtuelles hors tension ou leur appliquer la fonction vMotion manuellement avant de commencer la mise à niveau. Lorsque vous cliquez sur **Tout résoudre (Resolve all)**, les hôtes passent en mode de maintenance et sont redémarrés.

Si vous effectuez une mise à niveau de NSX 6.3.0 ou version ultérieure avec ESXi 6.0 ou version ultérieure, les hôtes doivent passer en mode de maintenance pour terminer la mise à niveau. Un redémarrage n'est pas nécessaire.

- Si DRS est activé sur le cluster, lorsque vous cliquez sur **Tout résoudre (Resolve all)**, DRS tente de placer les hôtes en mode de maintenance d'une manière contrôlée permettant aux machines virtuelles de continuer de fonctionner. Les machines virtuelles sont déplacées vers d'autres hôtes du cluster et les hôtes passent en mode de maintenance.
- Si DRS n'est pas activé sur le cluster, vous devez mettre les machines virtuelles hors tension ou leur appliquer la fonction vMotion manuellement avant de commencer la mise à niveau. Vous devez mettre les hôtes en mode de maintenance manuellement pour terminer la mise à niveau.

Dans NSX 6.3.5 et versions ultérieures, vous pouvez afficher l'état d'EAM dans l'onglet **Préparation de l'hôte (Host Preparation)**.

Conditions préalables

- Mettez à niveau NSX Manager et le cluster NSX Controller.
- Déconnectez-vous de vSphere Web Client, puis reconnectez-vous après la mise à niveau de NSX Manager et avant la mise à niveau des clusters d'hôtes.
- Assurez-vous de bien comprendre l'impact opérationnel de la mise à niveau d'un cluster d'hôtes. Reportez-vous à la section Impacts opérationnels des mises à niveau de NSX.
- Assurez-vous que les noms de domaine complets de tous vos hôtes peuvent être résolus.
- Si DRS est désactivé, mettez les machines virtuelles hors tension ou déplacez-les manuellement (fonction vMotion) avant de lancer la mise à niveau.
- Si DRS est activé, les machines virtuelles en cours d'exécution sont automatiquement déplacées pendant la mise à niveau du cluster d'hôtes. Assurez-vous que DRS est compatible avec votre environnement avant de lancer la mise à niveau.
  - Vérifiez que DRS est activé sur les clusters d'hôtes.
  - Vérifiez que la fonction vMotion fonctionne correctement.
  - Vérifiez l'état de connexion des hôtes avec vCenter.
  - Vérifiez que chaque cluster d'hôtes comporte au moins trois hôtes ESXi. Lors de la mise à niveau de NSX, le risque de problèmes de contrôle d'admission DRS est plus élevé pour les clusters qui ne contiennent qu'un ou deux hôtes. Pour que la mise à niveau de NSX aboutisse, VMware recommande d'inclure au moins trois hôtes dans chaque cluster d'hôtes. Si un cluster contient moins de trois hôtes, il est recommandé de les évacuer manuellement.

- Dans un petit cluster contenant seulement deux ou trois hôtes, si vous avez créé des règles d'anti-affinité indiquant que certaines machines virtuelles doivent résider sur des hôtes distincts, ces règles peuvent empêcher DRS de déplacer les machines virtuelles pendant la mise à niveau. Ajoutez des hôtes au cluster ou désactivez les règles d'anti-affinité pendant la mise à niveau et réactivez-les une fois l'opération terminée. Pour désactiver une règle d'anti-affinité, accédez à **Hôtes et clusters (Hosts and Clusters) > *Cluster* > Gérer (Manage) > Paramètres (Settings) > Règles de VM/VM (VM/Host Rules)**. Modifiez la règle et désélectionnez **Activer une règle (Enable rule)**.

- Connectez-vous à l'un des hôtes du cluster et exécutez la commande `esxcli software vib list`.

  Les VIB présents dépendront des versions d'ESXi et de NSX. Ils peuvent donc changer dans le cadre de la mise à niveau. Notez la version actuelle des VIB installés :

Version d'ESXi	Version de NSX	VIB installés
5.5	6.1.x, 6.2.x ou 6.3.x	■ esx-vsip ■ esx-vxlan
6.0 ou une version ultérieure	6.3.2 ou une version antérieure	■ esx-vsip ■ esx-vxlan
6.0 ou une version ultérieure	6.3.3 ou une version ultérieure	■ esx-nsxv

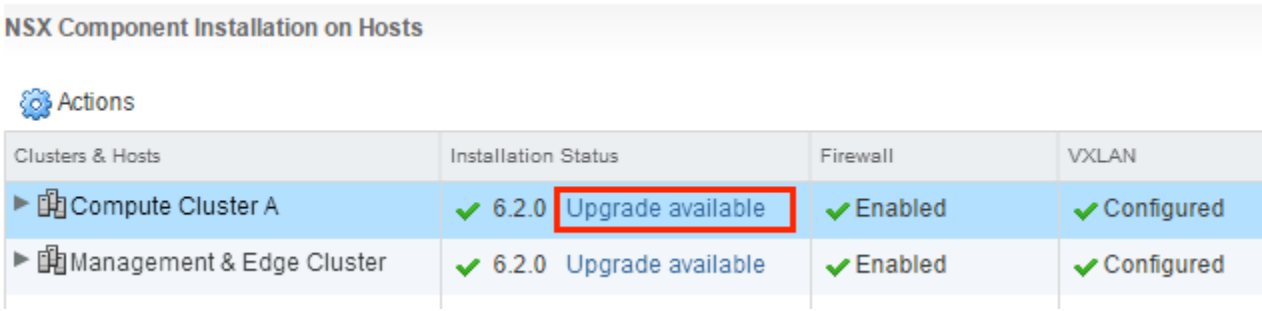
  Note Certaines versions de NSX contiennent des VIB supplémentaires qui seront supprimés pendant la mise à niveau.

  - Si vous procédez à une mise à niveau à partir d'une version de NSX antérieure à NSX 6.2, les hôtes préparés ont un VIB supplémentaire, esx-dvfilter-switch-security.
  - Si vous procédez à une mise à niveau à partir de NSX 6.2.x, version NSX 6.2.4 ou ultérieure, les hôtes préparés ont un VIB supplémentaire, esx-vdpi.

Procédure

1 Dans vSphere Web Client, accédez à **Accueil > Networking & Security > Installation (Home > Networking & Security > Installation)** et sélectionnez l'onglet **Préparation de l'hôte (Host Preparation)**.

2 Pour chaque cluster que vous souhaitez mettre à niveau, cliquez sur **Mise à niveau disponible (Upgrade available)**.



L'état d'installation affiche `Installation en cours`.

3 L'état d'installation du cluster indique `Non prêt`. Cliquez sur **Non prêt (Not Ready)** pour afficher plus d'informations. Cliquez sur **Tout résoudre (Resolve all)** pour tenter de terminer l'installation du module VIB.

Les hôtes sont mis en mode de maintenance et sont redémarrés si nécessaire, pour terminer la mise à niveau.

La colonne État de l'installation affiche `Installation en cours`. Une fois la mise à niveau terminée, la colonne État de l'installation affiche une coche verte et la version NSX mise à niveau.

4 Si l'action **Résoudre (Resolve)** échoue lorsque DRS est activé, les hôtes peuvent nécessiter une intervention manuelle pour passer en mode de maintenance (par exemple, en raison d'exigences de haute disponibilité ou de règles DRS), le processus de mise à niveau s'arrête et l'état d'installation du cluster affiche à nouveau `Non prêt`. Cliquez sur **Non prêt (Not Ready)** pour afficher plus d'informations. Vérifiez les hôtes affichés dans la vue **Hôtes et clusters (Hosts and Clusters)** et assurez-vous qu'ils sont allumés et connectés et qu'ils ne contiennent pas de machines virtuelles en cours d'exécution. Puis, essayez à nouveau d'exécuter l'action **Résoudre (Resolve)**.

La colonne État de l'installation affiche `Installation en cours`. Une fois la mise à niveau terminée, la colonne État de l'installation affiche une coche verte et la version NSX mise à niveau.

5 Si l'action **Résoudre (Resolve)** échoue lorsque DRS est désactivé et que vous effectuez une mise à niveau de NSX 6.3.0 ou version ultérieure avec ESXi 6.0 ou version ultérieure, vous devez mettre les hôtes en mode de maintenance manuellement pour terminer la mise à niveau.

a Placez les hôtes évacués en mode de maintenance.

b Accédez à **Networking & Security > Installation > Préparation de l'hôte (Host Preparation)**.

La mise à niveau démarre automatiquement lorsque les hôtes passent en mode de maintenance. La colonne État de l'installation affiche `Installation en cours`. Si vous ne voyez pas l'état `Installation en cours`, actualisez la page.

Une fois la mise à niveau terminée, la colonne État de l'installation affiche une coche verte et la version NSX mise à niveau.

c Retirez le mode de maintenance sur les hôtes.

Pour confirmer la mise à jour des hôtes, connectez-vous à l'un des hôtes du cluster et exécutez la commande `esxcli software vib list`. Vérifiez que les VIB appropriés ont été mis à jour vers la version attendue.

En cas d'échec de la mise à niveau des hôtes, effectuez les étapes de dépannage suivantes :

- Recherchez d'éventuelles alertes et erreurs dans ESX Agent Manager sur vCenter.
- Connectez-vous à l'hôte, consultez le fichier journal `/var/log/esxupdate.log` et recherchez les alertes et erreurs récentes.
- Vérifiez que DNS et NTP sont configurés sur l'hôte.

Reportez-vous à la section « Préparation de l'hôte » du *Guide de dépannage de NSX* pour voir d'autres étapes de dépannage.

Étape suivante

Mettre à niveau NSX Edge

Mettre à niveau NSX Edge

Pendant la mise à niveau, un nouveau dispositif virtuel Edge est déployé parallèlement au dispositif existant.

Lorsque le nouveau dispositif Edge est prêt, les cartes réseau virtuelles de l'ancien dispositif sont déconnectées et celles du nouveau dispositif sont connectées. Le nouveau dispositif Edge envoie ensuite des paquets ARP gratuits (GARP) pour mettre à jour le cache ARP des commutateurs connectés. Lorsque HA est déployé, le processus de mise à niveau est exécuté deux fois.

Ce processus peut affecter temporairement le transfert de paquets. Vous pouvez limiter les effets en configurant le dispositif Edge de sorte qu'il fonctionne en mode ECMP.

Les contiguïtés OSPF sont retirées lors de la mise à niveau si un redémarrage normal n'est pas activé.

Conditions préalables

- Vérifiez que NSX Manager a été mis à niveau.
- Vérifiez que le cluster et la préparation de l'hôte de NSX Controller ont été mis à niveau avant de mettre à niveau les routeurs logiques.
- Vérifiez qu'il existe un pool local d'ID de segments, même si vous ne prévoyez pas de créer des commutateurs logiques NSX.
- Vérifiez que les hôtes disposent de suffisamment de ressources pour déployer des dispositifs NSX Edge Services Gateway supplémentaires lors de la mise à niveau, en particulier si vous mettez à niveau plusieurs dispositifs NSX Edge en parallèle. Reportez-vous à la section Configuration système requise pour NSX pour voir les ressources requises pour chaque taille de NSX Edge.
    - Pour une instance unique de NSX Edge, deux dispositifs NSX Edge de la bonne taille ont l'état poweredOn lors de la mise à niveau.

    - Pour une instance de NSX Edge avec la haute disponibilité, les deux dispositifs de remplacement sont déployés avant le remplacement des anciens dispositifs. Cela signifie que quatre dispositifs NSX Edge de la bonne taille ont l'état poweredOn lors de la mise à niveau d'un dispositif NSX Edge donné. Une fois que l'instance de NSX Edge est mise à niveau, un dispositif HA peut devenir actif.

- Vérifiez que les clusters d'hôtes répertoriés dans l'emplacement configuré et l'emplacement en direct pour le dispositif NSX Edge sont préparés pour NSX et que l'état de leur infrastructure de messagerie est `GREEN`. Si l'emplacement configuré n'est pas disponible, par exemple, car le cluster a été supprimé depuis la création du dispositif NSX Edge, vérifiez uniquement l'emplacement en direct.
    - Obtenez l'identifiant de l'emplacement d'origine configuré (*configuredResourcePool* > *id*) et de l'emplacement en direct actuel (*resourcePoolId*) avec la demande d'API `GET https://NSX-Manager-IP-Address/api/4.0/edges/{edgeId}/appliances`.
    - Trouvez l'état de préparation de l'hôte et l'état de l'infrastructure de messagerie de ces clusters avec la demande d'API `GET https://NSX-Manager-IP-Address/api/2.0/nwfabric/status?resource={resourceId}`, où *resourceId* correspond à l'ID des emplacements configuré et en direct des dispositifs NSX Edge trouvés précédemment.
        - Recherchez l'état correspondant à l'identifiant *featureId* de `com.vmware.vshield.vsm.nwfabric.hostPrep` dans le texte de la réponse. L'état doit être `GREEN`.

          ```
          <nwFabricFeatureStatus>
            <featureId>com.vmware.vshield.vsm.nwfabric.hostPrep</featureId>
            <featureVersion>6.3.1.5124716</featureVersion>
            <updateAvailable>false</updateAvailable>
            <status>GREEN</status>
            <installed>true</installed>
            <enabled>true</enabled>
            <allowConfiguration>false</allowConfiguration>
          </nwFabricFeatureStatus>
          ```

        - Recherchez l'état correspondant à l'identifiant *featureId* de `com.vmware.vshield.vsm.messagingInfra` dans le texte de la réponse. L'état doit être `GREEN`.

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

- Comprenez l'impact opérationnel de la mise à niveau de NSX Edge. Reportez-vous à la section Impacts opérationnels des mises à niveau de NSX dans le *Guide de mise à niveau de NSX*.

- Si vous effectuez une mise à niveau à partir de NSX 6.0.x et que VPN L2 est activé sur un dispositif NSX Edge, vous devez supprimer la configuration de VPN L2 avant de procéder à la mise à niveau. Lorsque la mise à niveau est terminée, vous pouvez reconfigurer VPN L2. Consultez la section Présentation de VPN L2 dans le *Guide d'installation de NSX*.

Procédure

1. Dans vSphere Web Client, sélectionnez **Mise en réseau et sécurité (Networking & Security) > NSX Edge (NSX Edges)**.
2. Pour chaque instance de NSX Edge, sélectionnez **Mettre à niveau la version (Upgrade Version)** dans le menu **Actions (Actions) (⚙)**.

   Si la mise à niveau échoue en générant un message d'erreur indiquant que le déploiement du dispositif Edge a échoué, vérifiez que l'hôte sur lequel le dispositif NSX Edge est déployé est connecté et qu'il ne se trouve pas en mode de maintenance.

Après la mise à niveau du dispositif NSX Edge, le champ **État (Status)** affiche la valeur Déployé et la colonne **Version** indique la nouvelle version de NSX.

Si la mise à niveau d'un dispositif Edge échoue et si la version antérieure du dispositif n'est pas rétablie, cliquez sur l'icône **Redéployer le dispositif NSX Edge (Redeploy NSX Edge)** et tentez à nouveau d'effectuer la mise à niveau.

Étape suivante

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 le 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 ce faire, ouvrez vSphere Web Client et recherchez l'hôte ESXi où réside la machine virtuelle NSX Edge. Cliquez sur **Gérer (Manage) > Paramètres (Settings)** et sous Machines virtuelles, sélectionnez Démarrage/Arrêt de la VM, cliquez sur **Modifier (Edit)**, et assurez-vous que la machine virtuelle est en mode manuel (autrement dit, assurez-vous qu'elle ne figure pas dans la liste de démarrage/arrêt automatique).

Mettre à niveau Guest Introspection

Il est important de mettre à niveau Guest Introspection pour exécuter la même version que NSX Manager.

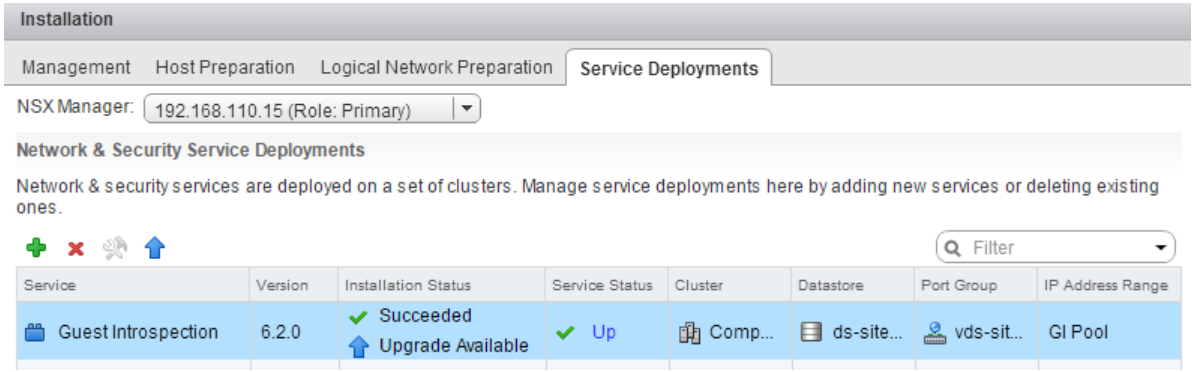
Note Les VM du service Guest Introspection peuvent être mises à niveau depuis vSphere Web Client. Vous n'avez pas besoin de supprimer la VM de service après la mise à niveau de NSX Manager pour la mettre à niveau. Si vous supprimez la VM de service, l'état de service indiquera `Échec`, car la VM agent est manquante. Cliquez sur **Résoudre (Resolve)** pour déployer une nouvelle VM de service, puis cliquez sur **Mise à niveau disponible (Upgrade Available)** pour déployer la dernière VM du service Guest Introspection.

Conditions préalables

Mettez à niveau NSX Manager, les contrôleurs, les clusters d'hôtes préparés et les dispositifs NSX Edge.

Procédure

1 Dans l'onglet **Installation**, cliquez sur **Déploiements de services (Service Deployments)**.

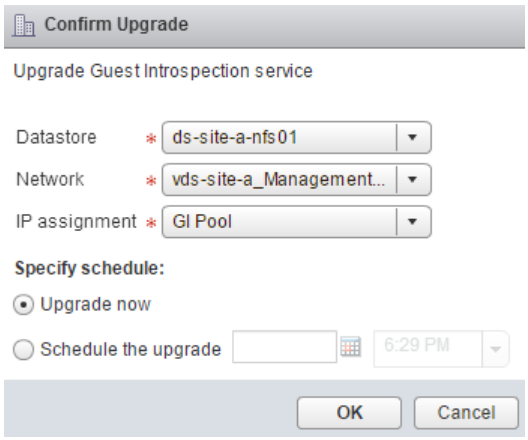


La colonne **Statut de l'installation (Installation Status)** indique **Mise à niveau disponible (Upgrade Available)**.

2 Sélectionnez le déploiement de Guest Introspection à mettre à niveau.

L'icône **Mettre à niveau (Upgrade)** (⬆) est activée dans la barre d'outils qui se trouve au-dessus du tableau des services.

3 Cliquez sur l'icône **Mettre à niveau (Upgrade)** (⬆) et suivez les invites de l'interface utilisateur.



Après la mise à niveau de Guest Introspection, l'état d'installation est `Réussi` et l'état de service est `Actif`. Les machines virtuelles du service Guest Introspection sont visibles dans l'inventaire de vCenter Server.

Une fois que Guest Introspection est mis à niveau pour un cluster particulier, vous pouvez mettre à niveau n'importe quelles solutions de partenaires. Si des solutions de partenaires sont activées, consultez la documentation de mise à niveau fournie par le partenaire. Même si la solution de partenaire n'est pas mise à niveau, la protection est maintenue.

NSX Services ne prenant pas en charge la mise à niveau directe

Certaines instances de NSX Services ne prennent pas en charge la mise à niveau directe. Dans ces cas, il vous faut désinstaller et réinstaller les services.

Dispositifs virtuels VMware Partner Security

Consultez la documentation du partenaire pour vérifier si le dispositif virtuel de sécurité partenaire peut être mis à niveau.

NSX SSL VPN

Depuis NSX 6.2, la passerelle VPN SSL n'accepte que le protocole TLS. Toutefois, après avoir effectué la mise à niveau vers NSX 6.2 ou version ultérieure, tout nouveau client que vous créez utilise automatiquement le protocole TLS lors de l'établissement de la connexion. En outre, à partir de NSX 6.2.3, TLS 1.0 n'est plus utilisé.

À cause du changement de protocole, lorsqu'un client NSX 6.0.x tente de se connecter à une passerelle NSX 6.2 ou version ultérieure, l'établissement de la connexion échoue à l'étape de l'établissement de liaison SSL.

Après une mise à niveau vers NSX 6.0.x, désinstallez vos anciens clients VPN SSL et installez la version NSX 6.3.x des clients VPN SSL. Voir « Installer le client SSL sur un site distant » dans le *Guide d'administration de NSX*.

VPN L2 NSX

La mise à niveau de NSX Edge n'est pas prise en charge si VPN L2 est installé sur un dispositif NSX Edge doté de NSX 6.0.x. La configuration de VPN L2 doit être supprimée du dispositif NSX Edge pour pouvoir effectuer une mise à niveau de ce dernier.

Liste de contrôle postérieure à la mise à niveau

Lorsque la mise à niveau est terminée, suivez ces étapes.

Procédure

1. Créez une sauvegarde actuelle de NSX Manager après la mise à niveau.
2. Vérifiez que les VIB ont été installés sur les hôtes.

   NSX installe ces VIB :

   ```
   esxcli software vib get --vibname esx-vxlan
   esxcli software vib get --vibname esx-vsip
   ```

Si Guest Introspection a été installé, vérifiez également que ce VIB est présent sur les hôtes :

```
esxcli software vib get --vibname epsec-mux
```

3 Resynchronisez le bus de messages d'hôte. VMware conseille à tous les clients de procéder à une resynchronisation après une mise à niveau.

Vous pouvez utiliser l'appel API suivant pour effectuer la resynchronisation sur chaque hôte.

```
URL : https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>
HTTP Method : POST

Headers:

Authorization : base64encoded value of username password
Accept : application/xml
Content-Type : application/xml
```

Mettre à niveau vers NSX 6.3.x avec cross-vCenter NSX

Pour passer à NSX 6.3.x dans un environnement cross-vCenter, vous devez mettre à niveau les composants NSX dans l'ordre indiqué dans ce guide.

Les composants NSX doivent être mis à niveau dans l'ordre suivant :

1 Dispositif NSX Manager principal

2 Tous les dispositifs NSX Manager secondaires

3 Cluster NSX Controller

4 Clusters d'hôtes

5 NSX Edge

6 Guest Introspection

Le processus de mise à niveau est géré par NSX Manager. Si la mise à niveau d'un composant échoue ou est interrompue et si vous devez l'exécuter à nouveau ou la redémarrer, elle ne reprend pas depuis le début, mais à l'endroit où elle s'est arrêtée.

L'état de la mise à niveau est mis à jour pour chaque nœud et au niveau du cluster.

Mettre à niveau le dispositif NSX Manager principal dans cross-vCenter NSX

La première étape du processus de mise à niveau de l'infrastructure NSX consiste à mettre à niveau le dispositif NSX Manager principal.

Attention L'exécution de dispositifs NSX Manager de différentes versions dans un environnement cross-vCenter NSX n'est pas prise en charge. Une fois que vous avez mis à niveau le dispositif NSX Manager principal, vous devez mettre à niveau les dispositifs NSX Manager secondaires.

Pendant la mise à niveau de NSX Manager dans un environnement cross-vCenter NSX, n'apportez aucune modification aux objets universels tant que la mise à niveau de l'instance principale et de toutes les instances secondaires de NSX Manager n'est pas terminée. Cela inclut la création, la mise à jour ou la suppression d'objets universels, ainsi que des opérations impliquant des objets universels (par exemple, application d'une balise de sécurité universelle à une VM).

Lors de la mise à niveau, vous pouvez choisir de participer au Programme d'amélioration du produit (CEIP) pour NSX. Consultez le Programme d'amélioration du produit dans le *Guide d'administration de NSX* pour plus d'informations sur le programme, y compris comment participer ou quitter le programme.

Si vous procédez à la mise à niveau de NSX 6.3.0 ou version ultérieure, le téléchargement du bundle de mise à niveau et le démarrage de la mise à niveau peuvent se produire indépendamment. Pour démarrer une mise à niveau à partir d'un bundle de mise à niveau précédemment téléchargé, accédez à **Page d'accueil (Home) > Mise à niveau (Upgrade)** et cliquez sur **Commencer la mise à niveau (Begin Upgrade)**.

Lorsque vous mettez à niveau NSX Manager vers NSX 6.3.6, une sauvegarde est réalisée automatiquement et enregistrée localement dans le cadre du processus de mise à niveau. Reportez-vous à la section Gestion des sauvegardes de NSX Manager créées lors de la mise à niveau pour plus d'informations sur la gestion de ces fichiers de sauvegarde.

- Si la sauvegarde automatique réalisée pendant la mise à niveau échoue, la mise à niveau ne continue pas. Contactez le support client de VMware pour obtenir de l'aide.
- La sauvegarde automatique sert de recours en cas d'échec de votre sauvegarde régulière.
  - Effectuez toujours une sauvegarde régulière de NSX Manager avant toute mise à niveau. Pour plus d'informations, reportez-vous à Sauvegarder les données de NSX Manager. Vous pouvez restaurer cette sauvegarde sans l'aide du support client de VMware.
  - Si vous devez restaurer la sauvegarde automatique, vous devez contacter le support client de VMware.

Conditions préalables

- Validez l'utilisation du système de fichiers NSX Manager et exécutez un nettoyage si l'utilisation du système de fichiers est à 100 %.
  a Connectez-vous à NSX Manager et exécutez `show filesystems` pour afficher l'utilisation du système de fichiers.

b Si l'utilisation est de 100 %, passez en mode privilégié (activer) et exécutez les commandes `purge log manager` et `purge log system`.

c Redémarrez le dispositif NSX Manager pour que le nettoyage des journaux prenne effet.

- Vérifiez que la mémoire réservée du dispositif virtuel NSX Manager respecte la configuration système requise avant de procéder à la mise à niveau.

  Reportez-vous à la section Configuration système requise pour NSX.

- Si Data Security est présent dans votre environnement, désinstallez-le avant de mettre à niveau NSX Manager. Reportez-vous à la section Désinstaller NSX Data Security. Data Security a été supprimé de NSX 6.3.x.
- Sauvegardez votre configuration actuelle et téléchargez les journaux de support technique avant la mise à niveau. Reportez-vous à la section Sauvegarde et restauration de NSX.
- Téléchargez le bundle de mise à niveau et vérifiez le total de contrôle MD5. Reportez-vous à la section Télécharger le bundle de mise à niveau de NSX et vérifier le total de contrôle MD5.
- Assurez-vous de bien comprendre l'impact opérationnel de la mise à niveau de NSX Manager. Reportez-vous à la section Impacts opérationnels des mises à niveau de NSX.
- Vous devez mettre à niveau toutes les instances de NSX Manager dans un environnement cross-vCenter NSX dans la même fenêtre de maintenance.
- Déterminez les instances de NSX Manager à mettre à niveau dans la même fenêtre de maintenance.
  - Si vous disposez d'un environnement cross-vCenter NSX, vous devez mettre à niveau l'instance principale et toutes les instances secondaires de NSX Manager vers la même version NSX dans une fenêtre de maintenance unique.
  - Si plusieurs instances de NSX Manager sont connectées à des systèmes vCenter Server qui utilisent le même serveur SSO, toutes les combinaisons de version de NSX Manager ne sont pas prises en charge. Vous devez planifier la mise à niveau de vos instances de NSX Manager afin de disposer d'une configuration prise en charge à la fin de la fenêtre de maintenance.
    - Toutes les instances de NSX Manager utilisant la même version de NSX sont prises en charge.
    - Les instances de NSX Manager utilisant une version différente de NSX sont prises en charge si NSX 6.4.0 ou version ultérieure est installé sur au moins une instance de NSX Manager et si NSX 6.3.3 ou version ultérieure est installé sur toutes les autres instances de NSX Manager.

Procédure

1 Connectez-vous au dispositif virtuel NSX Manager.

2 Dans la page d'accueil, cliquez sur **Mettre à niveau (Upgrade)**.

3 Cliquez sur **Mettre à niveau (Upgrade)**, sur **Choisir un fichier (Choose File)** et accédez au fichier `VMware-NSX-Manager-upgrade-bundle-`*`releaseNumber`*`-`*`NSXbuildNumber`*`.tar.gz`. Cliquez sur **Continuer (Continue)** pour démarrer le téléchargement.

   Le statut de téléchargement s'affiche dans la fenêtre du navigateur.

4 Si vous voulez démarrer la mise à niveau plus tard, cliquez sur **Fermer (Close)** dans la boîte de dialogue Mettre à niveau.

   Lorsque vous êtes prêt à démarrer la mise à niveau, accédez à **Page d'accueil (Home) > Mise à niveau (Upgrade)** et cliquez sur **Commencer la mise à niveau (Begin Upgrade)**.

5 Dans la boîte de dialogue Mettre à niveau, sélectionnez si vous voulez activer SSH et si vous voulez participer au Programme d'amélioration du produit (CEIP) de VMware. Cliquez sur **Mettre à niveau (Upgrade)** pour démarrer la mise à niveau.

   L'état de la mise à niveau s'affiche dans la fenêtre du navigateur.

   Note La boîte de dialogue Mettre à niveau affiche un message indiquant que la sauvegarde automatique a été effectuée.

   Lorsque le processus de mise à niveau est terminé, la page de connexion à NSX Manager s'affiche.

6 Connectez-vous à nouveau au dispositif virtuel NSX Manager, puis dans la page d'accueil, cliquez sur **Mettre à niveau (Upgrade)**. Vérifiez que l'état de la mise à niveau est **Terminé (Complete)**, et que le numéro de build et de version en haut à droite correspond au bundle de mise à niveau que vous venez d'installer.

Si vous êtes connecté à vSphere Web Client lors de la mise à niveau, vous verrez des avertissements indiquant un problème de synchronisation sur la page **Networking and Security > Installation > Gestion (Management)**. Cela s'explique, car vous disposez de dispositifs NSX Manager avec différentes versions de NSX. Vous devez mettre à niveau les dispositifs NSX Manager secondaires avant de passer à une autre partie de la mise à niveau.

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 dans vSphere Web Client, videz le cache et l'historique de votre navigateur. Si cette étape n'est pas effectuée, vous pouvez voir un message d'erreur similaire à « Une erreur interne s'est produite - Erreur #1009 » lorsque vous modifiez la configuration de NSX dans vSphere Web Client.

Si l'onglet Networking and Security n'apparaît pas dans vSphere Web Client, réinitialisez le serveur vSphere Web Client :

- Dans vCenter 5.5, ouvrez https://<vcenter-ip>:5480 et redémarrez le serveur Web Client.

- Dans vCenter Server Appliance 6.0, connectez-vous au shell vCenter Server en tant qu'utilisateur racine et exécutez les commandes suivantes :

```
Command> shell.set --enabled True
Command> shell
localhost:~ # cd /bin
localhost:~ # service-control --stop vsphere-client
localhost:~ # service-control --start vsphere-client
```

- Dans vCenter Server 6.0 sous Windows, vous pouvez exécuter les commandes suivantes.

```
cd C:\Program Files\VMware\vCenter Server\bin
service-control --stop vspherewebclientsvc
service-control --start vspherewebclientsvc
```

Il est recommandé d'utiliser des clients Web différents pour gérer des instances de vCenter Server qui exécutent des versions différentes de NSX Manager, afin d'éviter les erreurs inattendues liées à l'exécution simultanée de plusieurs plug-ins NSX de version différente.

Après la mise à niveau de l'instance de NSX Manager, créez un fichier de sauvegarde de NSX Manager. Reportez-vous à la section Sauvegarde et restauration de NSX. La sauvegarde précédente de NSX Manager n'est valide que pour la version précédente.

Étape suivante

Mettez à niveau tous les dispositifs NSX Manager secondaires.

Mettre à niveau tous les dispositifs NSX Manager secondaires dans cross-vCenter NSX

Vous devez mettre à niveau tous les dispositifs NSX Manager secondaires avant la mise à niveau des autres composants de NSX.

Exécutez les étapes suivantes pour mettre à niveau un dispositif NSX Manager secondaire. Répétez ces étapes pour tous les dispositifs NSX Manager secondaires dans l'environnement cross-vCenter NSX.

Pendant la mise à niveau de NSX Manager dans un environnement cross-vCenter NSX, n'apportez aucune modification aux objets universels tant que la mise à niveau de l'instance principale et de toutes les instances secondaires de NSX Manager n'est pas terminée. Cela inclut la création, la mise à jour ou la suppression d'objets universels, ainsi que des opérations impliquant des objets universels (par exemple, application d'une balise de sécurité universelle à une VM).

Lors de la mise à niveau, vous pouvez choisir de participer au Programme d'amélioration du produit (CEIP) pour NSX. Consultez le Programme d'amélioration du produit dans le *Guide d'administration de NSX* pour plus d'informations sur le programme, y compris comment participer ou quitter le programme.

Si vous procédez à la mise à niveau de NSX 6.3.0 ou version ultérieure, le téléchargement du bundle de mise à niveau et le démarrage de la mise à niveau peuvent se produire indépendamment. Pour démarrer une mise à niveau à partir d'un bundle de mise à niveau précédemment téléchargé, accédez à **Page d'accueil (Home) > Mise à niveau (Upgrade)** et cliquez sur **Commencer la mise à niveau (Begin Upgrade)**.

Lorsque vous mettez à niveau NSX Manager vers NSX 6.3.6, une sauvegarde est réalisée automatiquement et enregistrée localement dans le cadre du processus de mise à niveau. Reportez-vous à la section Gestion des sauvegardes de NSX Manager créées lors de la mise à niveau pour plus d'informations sur la gestion de ces fichiers de sauvegarde.

- Si la sauvegarde automatique réalisée pendant la mise à niveau échoue, la mise à niveau ne continue pas. Contactez le support client de VMware pour obtenir de l'aide.
- La sauvegarde automatique sert de recours en cas d'échec de votre sauvegarde régulière.
  - Effectuez toujours une sauvegarde régulière de NSX Manager avant toute mise à niveau. Pour plus d'informations, reportez-vous à Sauvegarder les données de NSX Manager. Vous pouvez restaurer cette sauvegarde sans l'aide du support client de VMware.
  - Si vous devez restaurer la sauvegarde automatique, vous devez contacter le support client de VMware.

Conditions préalables

- Vérifiez que l'instance principale de NSX Manager est mise à niveau.
- Validez l'utilisation du système de fichiers NSX Manager et exécutez un nettoyage si l'utilisation du système de fichiers est à 100 %.
  a Connectez-vous à NSX Manager et exécutez `show filesystems` pour afficher l'utilisation du système de fichiers.
  b Si l'utilisation est de 100 %, passez en mode privilégié (activer) et exécutez les commandes `purge log manager` et `purge log system`.
  c Redémarrez le dispositif NSX Manager pour que le nettoyage des journaux prenne effet.
- Vérifiez que la mémoire réservée du dispositif virtuel NSX Manager respecte la configuration système requise avant de procéder à la mise à niveau.

  Reportez-vous à la section Configuration système requise pour NSX.
- Si Data Security est présent dans votre environnement, désinstallez-le avant de mettre à niveau NSX Manager. Reportez-vous à la section Désinstaller NSX Data Security. Data Security a été supprimé de NSX 6.3.x.
- Sauvegardez votre configuration actuelle et téléchargez les journaux de support technique avant la mise à niveau. Reportez-vous à la section Sauvegarde et restauration de NSX.
- Téléchargez le bundle de mise à niveau et vérifiez le total de contrôle MD5. Reportez-vous à la section Télécharger le bundle de mise à niveau de NSX et vérifier le total de contrôle MD5.
- Assurez-vous de bien comprendre l'impact opérationnel de la mise à niveau de NSX Manager. Reportez-vous à la section Impacts opérationnels des mises à niveau de NSX.

- Vous devez mettre à niveau toutes les instances de NSX Manager dans un environnement cross-vCenter NSX dans la même fenêtre de maintenance.
- Déterminez les instances de NSX Manager à mettre à niveau dans la même fenêtre de maintenance.
  - Si vous disposez d'un environnement cross-vCenter NSX, vous devez mettre à niveau l'instance principale et toutes les instances secondaires de NSX Manager vers la même version NSX dans une fenêtre de maintenance unique.
  - Si plusieurs instances de NSX Manager sont connectées à des systèmes vCenter Server qui utilisent le même serveur SSO, toutes les combinaisons de version de NSX Manager ne sont pas prises en charge. Vous devez planifier la mise à niveau de vos instances de NSX Manager afin de disposer d'une configuration prise en charge à la fin de la fenêtre de maintenance.
    - Toutes les instances de NSX Manager utilisant la même version de NSX sont prises en charge.
    - Les instances de NSX Manager utilisant une version différente de NSX sont prises en charge si NSX 6.4.0 ou version ultérieure est installé sur au moins une instance de NSX Manager et si NSX 6.3.3 ou version ultérieure est installé sur toutes les autres instances de NSX Manager.

Procédure

1. Connectez-vous au dispositif virtuel NSX Manager.
2. Dans la page d'accueil, cliquez sur **Mettre à niveau (Upgrade)**.
3. Cliquez sur **Mettre à niveau (Upgrade)**, sur **Choisir un fichier (Choose File)** et accédez au fichier `VMware-NSX-Manager-upgrade-bundle-`*`releaseNumber`*`-`*`NSXbuildNumber`*`.tar.gz`. Cliquez sur **Continuer (Continue)** pour démarrer le téléchargement.

   Le statut de téléchargement s'affiche dans la fenêtre du navigateur.
4. Si vous voulez démarrer la mise à niveau plus tard, cliquez sur **Fermer (Close)** dans la boîte de dialogue Mettre à niveau.

   Lorsque vous êtes prêt à démarrer la mise à niveau, accédez à **Page d'accueil (Home) > Mise à niveau (Upgrade)** et cliquez sur **Commencer la mise à niveau (Begin Upgrade)**.
5. Dans la boîte de dialogue Mettre à niveau, sélectionnez si vous voulez activer SSH et si vous voulez participer au Programme d'amélioration du produit (CEIP) de VMware. Cliquez sur **Mettre à niveau (Upgrade)** pour démarrer la mise à niveau.

   L'état de la mise à niveau s'affiche dans la fenêtre du navigateur.

   Note La boîte de dialogue Mettre à niveau affiche un message indiquant que la sauvegarde automatique a été effectuée.

   Lorsque le processus de mise à niveau est terminé, la page de connexion à NSX Manager s'affiche.

6 Connectez-vous à nouveau au dispositif virtuel NSX Manager, puis dans la page d'accueil, cliquez sur **Mettre à niveau (Upgrade)**. Vérifiez que l'état de la mise à niveau est **Terminé (Complete)**, et que le numéro de build et de version en haut à droite correspond au bundle de mise à niveau que vous venez d'installer.

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 dans vSphere Web Client, videz le cache et l'historique de votre navigateur. Si cette étape n'est pas effectuée, vous pouvez voir un message d'erreur similaire à « Une erreur interne s'est produite - Erreur #1009 » lorsque vous modifiez la configuration de NSX dans vSphere Web Client.

Si l'onglet Networking and Security n'apparaît pas dans vSphere Web Client, réinitialisez le serveur vSphere Web Client :

- Dans vCenter 5.5, ouvrez https://<vcenter-ip>:5480 et redémarrez le serveur Web Client.
- Dans vCenter Server Appliance 6.0, connectez-vous au shell vCenter Server en tant qu'utilisateur racine et exécutez les commandes suivantes :

```
Command> shell.set --enabled True
Command> shell
localhost:~ # cd /bin
localhost:~ # service-control --stop vsphere-client
localhost:~ # service-control --start vsphere-client
```

- Dans vCenter Server 6.0 sous Windows, vous pouvez exécuter les commandes suivantes.

```
cd C:\Program Files\VMware\vCenter Server\bin
service-control --stop vspherewebclientsvc
service-control --start vspherewebclientsvc
```

Il est recommandé d'utiliser des clients Web différents pour gérer des instances de vCenter Server qui exécutent des versions différentes de NSX Manager, afin d'éviter les erreurs inattendues liées à l'exécution simultanée de plusieurs plug-ins NSX de version différente.

Après la mise à niveau de l'instance de NSX Manager, créez un fichier de sauvegarde de NSX Manager. Reportez-vous à la section Sauvegarde et restauration de NSX. La sauvegarde précédente de NSX Manager n'est valide que pour la version précédente.

Étape suivante

Mettre à niveau le cluster NSX Controller dans cross-vCenter NSX

Mettre à niveau le cluster NSX Controller dans cross-vCenter NSX

Les contrôleurs de votre environnement sont mis à niveau au niveau du cluster. Si une mise à niveau est disponible pour le cluster NSX Controller, un lien de mise à niveau s'affiche à côté de l'instance principale de NSX Manager dans le volet **Networking & Security > Installation > Gestion (Management)**.

Il est recommandé de procéder à la mise à niveau des contrôleurs lors d'une intervention de maintenance.

La mise à niveau de NSX Controller entraîne le téléchargement d'un fichier de mise à niveau sur chaque nœud de contrôleur. Les contrôleurs sont mis à niveau individuellement. Lors d'une mise à niveau, vous ne pouvez pas cliquer sur le lien **Mise à niveau disponible (Upgrade Available)** et les appels d'API pour la mise à niveau du cluster de contrôleurs sont bloqués tant que l'opération n'est pas terminée.

Si vous déployez de nouveaux contrôleurs avant la mise à niveau des contrôleurs existants, ils sont déployés sous l'ancienne version. Les nœuds de contrôleur doivent posséder la même version pour rejoindre un cluster.

Important Dans NSX 6.3.3, le système d'exploitation sous-jacent de NSX Controller est différent. 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 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.

Conditions préalables

- Vérifiez que l'état de tous les contrôleurs est normal. La mise à niveau est impossible dès lors qu'au moins un contrôleur est déconnecté. Pour reconnecter un contrôleur déconnecté, essayez de réinitialiser son dispositif virtuel. Dans la vue **Hôtes et clusters (Hosts and Clusters)**, cliquez avec le bouton droit sur le contrôleur et sélectionnez **Alimentation > Réinitialiser (Power > Reset)**.
- Un cluster NSX Controller valide contient trois nœuds de contrôleur. Connectez-vous à ces trois nœuds et exécutez la commande **show control-cluster status**.

```
controller-node# show control-cluster status

Type                Status                                          Since
--------------------------------------------------------------------------------
Join status:        Join complete                                   05/04 02:36:03
Majority status:    Connected to cluster majority                   05/19 23:57:23
Restart status:     This controller can be safely restarted         05/19 23:57:12
Cluster ID:         ff3ebaeb-de68-4455-a3ca-4824e31863a8
Node UUID:          ff3ebaeb-de68-4455-a3ca-4824e31863a8

Role                Configured status   Active status
--------------------------------------------------------------------------------
api_provider        enabled             activated
persistence_server  enabled             activated
switch_manager      enabled             activated
logical_manager     enabled             activated
directory_server    enabled             activated
```

  - Pour l'état de jointure, vérifiez que le nœud du contrôleur indique Jonction établie.

  - Pour l'état Majorité, vérifiez que le contrôleur est connecté à la majorité du cluster.
  - Pour l'ID de cluster, tous les nœuds de contrôleur d'un cluster doivent posséder un ID de cluster identique.
  - Pour l'état Configuré et l'état Actif, vérifiez que tous les rôles du contrôleur sont autorisés et activés.
- Assurez-vous de bien comprendre l'impact opérationnel de la mise à niveau de NSX Controller. Reportez-vous à la section Impacts opérationnels des mises à niveau de NSX.
- Si vous effectuez la mise à niveau vers NSX 6.3.3, le cluster NSX Controller doit contenir trois nœuds de contrôleur. S'il en contient moins de trois, vous devez ajouter des nœuds supplémentaires avant de commencer la mise à niveau. Consultez la section Déployer le cluster NSX Controller du *Guide d'installation de NSX* pour savoir comment ajouter des nœuds de contrôleur.

Procédure

- Accédez à **Accueil > Networking & Security > Installation (Home > Networking & Security > Installation)**, sélectionnez l'onglet **Gestion (Management)**, puis cliquez sur **Mise à niveau disponible (Upgrade Available)** dans la colonne **État du cluster de contrôleurs (Controller Cluster Status)**.

  Les contrôleurs de votre environnement sont mis à niveau et redémarrés individuellement. Une fois que vous avez lancé la mise à niveau, le système télécharge le fichier de mise à niveau, puis met à niveau, redémarre et met à jour l'état de mise à niveau de chaque contrôleur. Les champs suivants affichent l'état des contrôleurs :

  - La colonne **État du cluster de contrôleurs (Controller Cluster Status)** de la section NSX Manager indique l'état de mise à niveau du cluster. Au démarrage de la mise à niveau, l'état est **Téléchargement du fichier de mise à niveau (Downloading upgrade file)**. Une fois le fichier de mise à niveau téléchargé sur tous les contrôleurs du cluster, l'état passe à **En cours (In progress)**. Une fois que tous les contrôleurs du cluster ont été mis à niveau, l'état est **Complet (Complete)** et cette colonne ne s'affiche plus.
  - Dans la section Nœuds de NSX Controller, la colonne **État (Status)** affiche l'état de chaque contrôleur, qui est **Connecté (Connected)** ou **Normal** avant la mise à niveau, selon la version NSX d'origine. Lorsque les services de contrôleur sont arrêtés et que le contrôleur est redémarré, l'état passe à **Déconnecté (Disconnected)**. Une fois la mise à niveau de ce contrôleur terminée, l'état est **Connecté (Connected)**.

- La colonne **État de la mise à niveau (Upgrade Status)** de la section des nœuds NSX Controller indique l'état de mise à niveau de chaque contrôleur. Elle indique tout d'abord **Téléchargement du fichier de mise à niveau (Downloading upgrade file)**, puis **Mise à niveau en cours (Upgrade in progress)** et enfin **Redémarrage (Rebooting)**. Une fois que le contrôleur a été mis à niveau, l'état **Mis à niveau (Upgraded)** s'affiche.

  Note Lorsque vous effectuez une mise à niveau à partir de NSX 6.3.2 ou version antérieure vers NSX 6.3.3 ou version ultérieure, l'état **Téléchargement du fichier de mise à niveau (Downloading upgrade file)** est remplacé par **En file d'attente pour la mise à niveau (Queued For Upgrade)**.

Lorsque la mise à niveau est terminée, la colonne **Version du logiciel (Software Version)** de la section des nœuds NSX Controller indique **6.3.***buildNumber* pour chaque contrôleur. Réexécutez la commande **show control-cluster status** pour vous assurer que les contrôleurs peuvent former une majorité. Si la majorité du cluster NSX Controller n'est pas rétablie, consultez les journaux des contrôleurs et de NSX Manager.

Après la mise à niveau des contrôleurs, un ou plusieurs nœuds de contrôleur peuvent se voir attribuer un nouvel ID de contrôleur. Ce comportement est normal et dépend du moment auquel l'instance secondaire de NSX Manager interroge les nœuds.

La durée moyenne de mise à niveau est de 6 à 8 minutes. Si la mise à niveau ne se termine pas avant le délai d'expiration (30 minutes), la colonne **État de la mise à niveau (Upgrade Status)** indique **Échec (Failed)**. Cliquez à nouveau sur **Mise à niveau disponible (Upgrade Available)** dans la section de NSX Manager pour reprendre la mise à niveau à l'endroit où elle s'est arrêtée.

Si des problèmes réseau ne permettent pas d'effectuer la mise à niveau en 30 minutes, vous devrez peut-être définir un délai plus long. Faites appel au support VMware pour diagnostiquer et résoudre les problèmes sous-jacents, et si nécessaire, prolonger le délai d'expiration de la mise à niveau.

Si la mise à niveau du contrôleur échoue, vérifiez la connectivité entre les contrôleurs et l'instance de NSX Manager.

Il peut arriver que la mise à niveau aboutisse pour le premier contrôleur et échoue pour le deuxième. Supposons que vous possédez un cluster contenant trois contrôleurs, que le premier est mis à niveau vers la nouvelle version et que le deuxième est en cours de mise à niveau. Si la mise à niveau de ce dernier échoue, il risque de rester déconnecté. Par ailleurs, le premier et le troisième contrôleur ne présentent plus la même version (l'un a été mis à niveau et l'autre non), ce qui ne leur permet pas de former une majorité. À ce stade, il est impossible de relancer la mise à niveau. Pour remédier au problème, créez un autre contrôleur. Le nouveau contrôleur présentera l'ancienne version, qui correspond à celle du troisième contrôleur, avec lequel il formera de ce fait une majorité. La mise à niveau peut alors être relancée. Voir Redéployer une instance de NSX Controller dans le *Guide de dépannage de NSX* pour des instructions sur la création d'un autre contrôleur.

Étape suivante

Mettre à niveau des clusters d'hôtes dans cross-vCenter NSX.

Mettre à niveau des clusters d'hôtes dans cross-vCenter NSX

Après avoir mis à niveau tous les dispositifs NSX Manager et le cluster NSX Controller, vous devez mettre à jour tous les clusters d'hôtes dans l'environnement cross-vCenter NSX.

La mise à niveau des clusters d'hôtes met à niveau les VIB de NSX.

Si vous effectuez une mise à niveau de NSX 6.2.x ou d'une version antérieure, ou de NSX 6.3.0 ou d'une version ultérieure avec ESXi 5.5, les hôtes doivent être redémarrés pour terminer la mise à niveau.

- Si DRS est activé sur le cluster, lorsque vous cliquez sur **Tout résoudre (Resolve all)**, DRS tente de redémarrer les hôtes d'une manière contrôlée permettant aux machines virtuelles de continuer de fonctionner. Les machines virtuelles sont déplacées vers d'autres hôtes du cluster et les hôtes passent en mode de maintenance et sont redémarrés.
- Si DRS n'est pas activé sur le cluster, vous devez mettre les machines virtuelles hors tension ou leur appliquer la fonction vMotion manuellement avant de commencer la mise à niveau. Lorsque vous cliquez sur **Tout résoudre (Resolve all)**, les hôtes passent en mode de maintenance et sont redémarrés.

Si vous effectuez une mise à niveau de NSX 6.3.0 ou version ultérieure avec ESXi 6.0 ou version ultérieure, les hôtes doivent passer en mode de maintenance pour terminer la mise à niveau. Un redémarrage n'est pas nécessaire.

- Si DRS est activé sur le cluster, lorsque vous cliquez sur **Tout résoudre (Resolve all)**, DRS tente de placer les hôtes en mode de maintenance d'une manière contrôlée permettant aux machines virtuelles de continuer de fonctionner. Les machines virtuelles sont déplacées vers d'autres hôtes du cluster et les hôtes passent en mode de maintenance.
- Si DRS n'est pas activé sur le cluster, vous devez mettre les machines virtuelles hors tension ou leur appliquer la fonction vMotion manuellement avant de commencer la mise à niveau. Vous devez mettre les hôtes en mode de maintenance manuellement pour terminer la mise à niveau.

Dans NSX 6.3.5 et versions ultérieures, vous pouvez afficher l'état d'EAM dans l'onglet **Préparation de l'hôte (Host Preparation)**.

Conditions préalables

- Mettez à niveau NSX Manager et le cluster NSX Controller.
- Déconnectez-vous de vSphere Web Client, puis reconnectez-vous après la mise à niveau de NSX Manager et avant la mise à niveau des clusters d'hôtes.
- Assurez-vous de bien comprendre l'impact opérationnel de la mise à niveau d'un cluster d'hôtes. Reportez-vous à la section Impacts opérationnels des mises à niveau de NSX.
- Assurez-vous que les noms de domaine complets de tous vos hôtes peuvent être résolus.
- Si DRS est désactivé, mettez les machines virtuelles hors tension ou déplacez-les manuellement (fonction vMotion) avant de lancer la mise à niveau.

- Si DRS est activé, les machines virtuelles en cours d'exécution sont automatiquement déplacées pendant la mise à niveau du cluster d'hôtes. Assurez-vous que DRS est compatible avec votre environnement avant de lancer la mise à niveau.
  - Vérifiez que DRS est activé sur les clusters d'hôtes.
  - Vérifiez que la fonction vMotion fonctionne correctement.
  - Vérifiez l'état de connexion des hôtes avec vCenter.
  - Vérifiez que chaque cluster d'hôtes comporte au moins trois hôtes ESXi. Lors de la mise à niveau de NSX, le risque de problèmes de contrôle d'admission DRS est plus élevé pour les clusters qui ne contiennent qu'un ou deux hôtes. Pour que la mise à niveau de NSX aboutisse, VMware recommande d'inclure au moins trois hôtes dans chaque cluster d'hôtes. Si un cluster contient moins de trois hôtes, il est recommandé de les évacuer manuellement.
  - Dans un petit cluster contenant seulement deux ou trois hôtes, si vous avez créé des règles d'anti-affinité indiquant que certaines machines virtuelles doivent résider sur des hôtes distincts, ces règles peuvent empêcher DRS de déplacer les machines virtuelles pendant la mise à niveau. Ajoutez des hôtes au cluster ou désactivez les règles d'anti-affinité pendant la mise à niveau et réactivez-les une fois l'opération terminée. Pour désactiver une règle d'anti-affinité, accédez à **Hôtes et clusters (Hosts and Clusters) > *Cluster* > Gérer (Manage) > Paramètres (Settings) > Règles de VM/VM (VM/Host Rules)**. Modifiez la règle et désélectionnez **Activer une règle (Enable rule)**.
- Connectez-vous à l'un des hôtes du cluster et exécutez la commande `esxcli software vib list`.

  Les VIB présents dépendront des versions d'ESXi et de NSX. Ils peuvent donc changer dans le cadre de la mise à niveau. Notez la version actuelle des VIB installés :

Version d'ESXi	Version de NSX	VIB installés
5.5	6.1.x, 6.2.x ou 6.3.x	■ esx-vsip ■ esx-vxlan
6.0 ou une version ultérieure	6.3.2 ou une version antérieure	■ esx-vsip ■ esx-vxlan
6.0 ou une version ultérieure	6.3.3 ou une version ultérieure	■ esx-nsxv

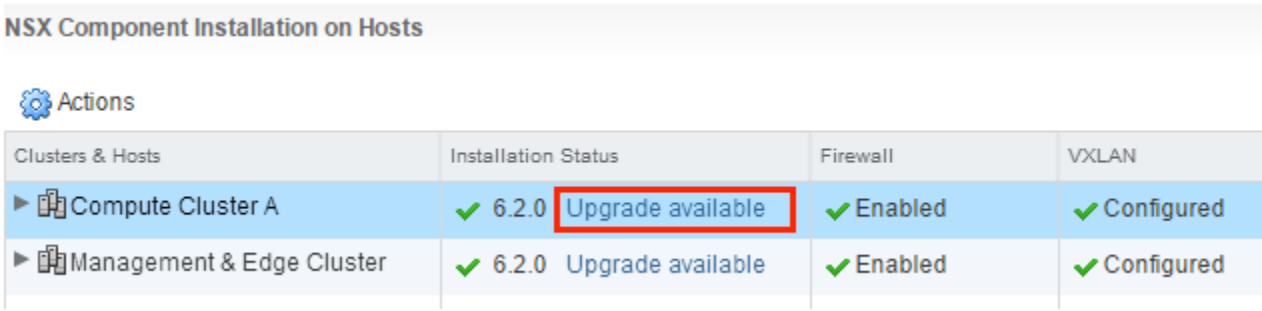
  Note Certaines versions de NSX contiennent des VIB supplémentaires qui seront supprimés pendant la mise à niveau.

  - Si vous procédez à une mise à niveau à partir d'une version de NSX antérieure à NSX 6.2, les hôtes préparés ont un VIB supplémentaire, esx-dvfilter-switch-security.
  - Si vous procédez à une mise à niveau à partir de NSX 6.2.x, version NSX 6.2.4 ou ultérieure, les hôtes préparés ont un VIB supplémentaire, esx-vdpi.

Procédure

1 Dans vSphere Web Client, accédez à **Accueil > Networking & Security > Installation (Home > Networking & Security > Installation)** et sélectionnez l'onglet **Préparation de l'hôte (Host Preparation)**.

2 Pour chaque cluster que vous souhaitez mettre à niveau, cliquez sur **Mise à niveau disponible (Upgrade available)**.



L'état d'installation affiche `Installation en cours`.

3 L'état d'installation du cluster indique `Non prêt`. Cliquez sur **Non prêt (Not Ready)** pour afficher plus d'informations. Cliquez sur **Tout résoudre (Resolve all)** pour tenter de terminer l'installation du module VIB.

Les hôtes sont mis en mode de maintenance et sont redémarrés si nécessaire, pour terminer la mise à niveau.

La colonne État de l'installation affiche `Installation en cours`. Une fois la mise à niveau terminée, la colonne État de l'installation affiche une coche verte et la version NSX mise à niveau.

4 Si l'action **Résoudre (Resolve)** échoue lorsque DRS est activé, les hôtes peuvent nécessiter une intervention manuelle pour passer en mode de maintenance (par exemple, en raison d'exigences de haute disponibilité ou de règles DRS), le processus de mise à niveau s'arrête et l'état d'installation du cluster affiche à nouveau `Non prêt`. Cliquez sur **Non prêt (Not Ready)** pour afficher plus d'informations. Vérifiez les hôtes affichés dans la vue **Hôtes et clusters (Hosts and Clusters)** et assurez-vous qu'ils sont allumés et connectés et qu'ils ne contiennent pas de machines virtuelles en cours d'exécution. Puis, essayez à nouveau d'exécuter l'action **Résoudre (Resolve)**.

La colonne État de l'installation affiche `Installation en cours`. Une fois la mise à niveau terminée, la colonne État de l'installation affiche une coche verte et la version NSX mise à niveau.

5 Si l'action **Résoudre (Resolve)** échoue lorsque DRS est désactivé et que vous effectuez une mise à niveau de NSX 6.3.0 ou version ultérieure avec ESXi 6.0 ou version ultérieure, vous devez mettre les hôtes en mode de maintenance manuellement pour terminer la mise à niveau.

   a Placez les hôtes évacués en mode de maintenance.

   b Accédez à **Networking & Security > Installation > Préparation de l'hôte (Host Preparation)**.

      La mise à niveau démarre automatiquement lorsque les hôtes passent en mode de maintenance. La colonne État de l'installation affiche `Installation en cours`. Si vous ne voyez pas l'état `Installation en cours`, actualisez la page.

      Une fois la mise à niveau terminée, la colonne État de l'installation affiche une coche verte et la version NSX mise à niveau.

   c Retirez le mode de maintenance sur les hôtes.

Pour confirmer la mise à jour des hôtes, connectez-vous à l'un des hôtes du cluster et exécutez la commande `esxcli software vib list`. Vérifiez que les VIB appropriés ont été mis à jour vers la version attendue.

En cas d'échec de la mise à niveau des hôtes, effectuez les étapes de dépannage suivantes :

- Recherchez d'éventuelles alertes et erreurs dans ESX Agent Manager sur vCenter.
- Connectez-vous à l'hôte, consultez le fichier journal `/var/log/esxupdate.log` et recherchez les alertes et erreurs récentes.
- Vérifiez que DNS et NTP sont configurés sur l'hôte.

Reportez-vous à la section « Préparation de l'hôte » du *Guide de dépannage de NSX* pour voir d'autres étapes de dépannage.

Étape suivante

Mettre à niveau NSX Edge dans cross-vCenter NSX

Mettre à niveau NSX Edge dans cross-vCenter NSX

Pendant la mise à niveau, un nouveau dispositif virtuel Edge est déployé parallèlement au dispositif existant.

Lorsque le nouveau dispositif Edge est prêt, les cartes réseau virtuelles de l'ancien dispositif sont déconnectées et celles du nouveau dispositif sont connectées. Le nouveau dispositif Edge envoie ensuite des paquets ARP gratuits (GARP) pour mettre à jour le cache ARP des commutateurs connectés. Lorsque HA est déployé, le processus de mise à niveau est exécuté deux fois.

Ce processus peut affecter temporairement le transfert de paquets. Vous pouvez limiter les effets en configurant le dispositif Edge de sorte qu'il fonctionne en mode ECMP.

Les contiguïtés OSPF sont retirées lors de la mise à niveau si un redémarrage normal n'est pas activé.

Mettez à niveau des dispositifs NSX Edge dans toutes les installations de NSX dans l'environnement cross-vCenter NSX.

Conditions préalables

- Vérifiez que NSX Manager a été mis à niveau.
- Vérifiez que le cluster et la préparation de l'hôte de NSX Controller ont été mis à niveau avant de mettre à niveau les routeurs logiques.
- Vérifiez qu'il existe un pool local d'ID de segments, même si vous ne prévoyez pas de créer des commutateurs logiques NSX.
- Vérifiez que les hôtes disposent de suffisamment de ressources pour déployer des dispositifs NSX Edge Services Gateway supplémentaires lors de la mise à niveau, en particulier si vous mettez à niveau plusieurs dispositifs NSX Edge en parallèle. Reportez-vous à la section Configuration système requise pour NSX pour voir les ressources requises pour chaque taille de NSX Edge.
  - Pour une instance unique de NSX Edge, deux dispositifs NSX Edge de la bonne taille ont l'état poweredOn lors de la mise à niveau.
  - Pour une instance de NSX Edge avec la haute disponibilité, les deux dispositifs de remplacement sont déployés avant le remplacement des anciens dispositifs. Cela signifie que quatre dispositifs NSX Edge de la bonne taille ont l'état poweredOn lors de la mise à niveau d'un dispositif NSX Edge donné. Une fois que l'instance de NSX Edge est mise à niveau, un dispositif HA peut devenir actif.
- Vérifiez que les clusters d'hôtes répertoriés dans l'emplacement configuré et l'emplacement en direct pour le dispositif NSX Edge sont préparés pour NSX et que l'état de leur infrastructure de messagerie est `GREEN`. Si l'emplacement configuré n'est pas disponible, par exemple, car le cluster a été supprimé depuis la création du dispositif NSX Edge, vérifiez uniquement l'emplacement en direct.
  - Obtenez l'identifiant de l'emplacement d'origine configuré (*configuredResourcePool* > *id*) et de l'emplacement en direct actuel (*resourcePoolId*) avec la demande d'API `GET https://NSX-Manager-IP-Address/api/4.0/edges/{edgeId}/appliances`.
  - Trouvez l'état de préparation de l'hôte et l'état de l'infrastructure de messagerie de ces clusters avec la demande d'API `GET https://NSX-Manager-IP-Address/api/2.0/nwfabric/status?resource={resourceId}`, où *resourceId* correspond à l'ID des emplacements configuré et en direct des dispositifs NSX Edge trouvés précédemment.
    - Recherchez l'état correspondant à l'identifiant *featureId* de `com.vmware.vshield.vsm.nwfabric.hostPrep` dans le texte de la réponse. L'état doit être `GREEN`.

```
<nwFabricFeatureStatus>
  <featureId>com.vmware.vshield.vsm.nwfabric.hostPrep</featureId>
  <featureVersion>6.3.1.5124716</featureVersion>
  <updateAvailable>false</updateAvailable>
  <status>GREEN</status>
  <installed>true</installed>
  <enabled>true</enabled>
  <allowConfiguration>false</allowConfiguration>
</nwFabricFeatureStatus>
```

- Recherchez l'état correspondant à l'identifiant *featureId* de `com.vmware.vshield.vsm.messagingInfra` dans le texte de la réponse. L'état doit être `GREEN`.

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

- Comprenez l'impact opérationnel de la mise à niveau de NSX Edge. Reportez-vous à la section Impacts opérationnels des mises à niveau de NSX dans le *Guide de mise à niveau de NSX*.
- Si vous effectuez une mise à niveau à partir de NSX 6.0.x et que VPN L2 est activé sur un dispositif NSX Edge, vous devez supprimer la configuration de VPN L2 avant de procéder à la mise à niveau. Lorsque la mise à niveau est terminée, vous pouvez reconfigurer VPN L2. Consultez la section Présentation de VPN L2 dans le *Guide d'installation de NSX*.

Procédure

1. Dans vSphere Web Client, sélectionnez **Mise en réseau et sécurité (Networking & Security) > NSX Edge (NSX Edges)**.
2. Pour chaque instance de NSX Edge, sélectionnez **Mettre à niveau la version (Upgrade Version)** dans le menu **Actions (Actions) (⚙)**.

   Si la mise à niveau échoue en générant un message d'erreur indiquant que le déploiement du dispositif Edge a échoué, vérifiez que l'hôte sur lequel le dispositif NSX Edge est déployé est connecté et qu'il ne se trouve pas en mode de maintenance.

Après la mise à niveau du dispositif NSX Edge, le champ **État (Status)** affiche la valeur Déployé et la colonne **Version** indique la nouvelle version de NSX.

Si la mise à niveau d'un dispositif Edge échoue et si la version antérieure du dispositif n'est pas rétablie, cliquez sur l'icône **Redéployer le dispositif NSX Edge (Redeploy NSX Edge)** et tentez à nouveau d'effectuer la mise à niveau.

Étape suivante

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 le 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 ce faire, ouvrez vSphere Web Client et recherchez l'hôte ESXi où réside la machine virtuelle NSX Edge. Cliquez sur **Gérer (Manage) > Paramètres (Settings)** et sous Machines virtuelles, sélectionnez Démarrage/Arrêt de la VM, cliquez sur **Modifier (Edit)**, et assurez-vous que la machine virtuelle est en mode manuel (autrement dit, assurez-vous qu'elle ne figure pas dans la liste de démarrage/arrêt automatique).

Mettre à niveau Guest Introspection dans cross-vCenter NSX

Mettre à niveau Guest Introspection dans cross-vCenter NSX

Il est important de mettre à niveau Guest Introspection pour exécuter la même version que NSX Manager.

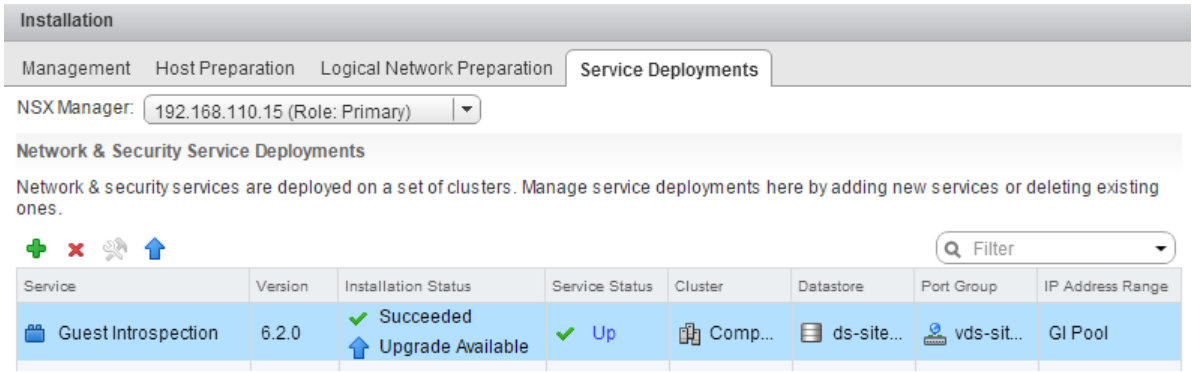
Note Les VM du service Guest Introspection peuvent être mises à niveau depuis vSphere Web Client. Vous n'avez pas besoin de supprimer la VM de service après la mise à niveau de NSX Manager pour la mettre à niveau. Si vous supprimez la VM de service, l'état de service indiquera Échec, car la VM agent est manquante. Cliquez sur **Résoudre (Resolve)** pour déployer une nouvelle VM de service, puis cliquez sur **Mise à niveau disponible (Upgrade Available)** pour déployer la dernière VM du service Guest Introspection.

Conditions préalables

Mettez à niveau NSX Manager, les contrôleurs, les clusters d'hôtes préparés et les dispositifs NSX Edge.

Procédure

1 Dans l'onglet **Installation**, cliquez sur **Déploiements de services (Service Deployments)**.

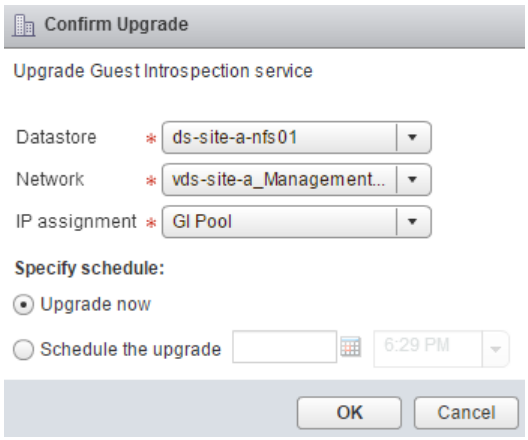


La colonne **Statut de l'installation (Installation Status)** indique **Mise à niveau disponible (Upgrade Available)**.

2 Sélectionnez le déploiement de Guest Introspection à mettre à niveau.

L'icône **Mettre à niveau (Upgrade)** ( ) est activée dans la barre d'outils qui se trouve au-dessus du tableau des services.

3 Cliquez sur l'icône **Mettre à niveau (Upgrade)** (⬆) et suivez les invites de l'interface utilisateur.



Après la mise à niveau de Guest Introspection, l'état d'installation est `Réussi` et l'état de service est `Actif`. Les machines virtuelles du service Guest Introspection sont visibles dans l'inventaire de vCenter Server.

Étape suivante

Une fois que Guest Introspection est mis à niveau pour un cluster particulier, vous pouvez mettre à niveau n'importe quelles solutions de partenaires. Si des solutions de partenaires sont activées, consultez la documentation de mise à niveau fournie par le partenaire. Même si la solution de partenaire n'est pas mise à niveau, la protection est maintenue.

NSX Services ne prenant pas en charge la mise à niveau directe

Certaines instances de NSX Services ne prennent pas en charge la mise à niveau directe. Dans ces cas, il vous faut désinstaller et réinstaller les services.

Dispositifs virtuels VMware Partner Security

Consultez la documentation du partenaire pour vérifier si le dispositif virtuel de sécurité partenaire peut être mis à niveau.

NSX SSL VPN

Depuis NSX 6.2, la passerelle VPN SSL n'accepte que le protocole TLS. Toutefois, après avoir effectué la mise à niveau vers NSX 6.2 ou version ultérieure, tout nouveau client que vous créez utilise automatiquement le protocole TLS lors de l'établissement de la connexion. En outre, à partir de NSX 6.2.3, TLS 1.0 n'est plus utilisé.

À cause du changement de protocole, lorsqu'un client NSX 6.0.x tente de se connecter à une passerelle NSX 6.2 ou version ultérieure, l'établissement de la connexion échoue à l'étape de l'établissement de liaison SSL.

Après une mise à niveau vers NSX 6.0.x, désinstallez vos anciens clients VPN SSL et installez la version NSX 6.3.x des clients VPN SSL. Voir « Installer le client SSL sur un site distant » dans le *Guide d'administration de NSX*.

VPN L2 NSX

La mise à niveau de NSX Edge n'est pas prise en charge si VPN L2 est installé sur un dispositif NSX Edge doté de NSX 6.0.x. La configuration de VPN L2 doit être supprimée du dispositif NSX Edge pour pouvoir effectuer une mise à niveau de ce dernier.

Liste de contrôle postérieure à la mise à niveau

Lorsque la mise à niveau est terminée, suivez ces étapes.

Procédure

1. Créez une sauvegarde actuelle de NSX Manager après la mise à niveau.
2. Vérifiez que les VIB ont été installés sur les hôtes.

   NSX installe ces VIB :

   ```
   esxcli software vib get --vibname esx-vxlan
   esxcli software vib get --vibname esx-vsip
   ```

   Si Guest Introspection a été installé, vérifiez également que ce VIB est présent sur les hôtes :

   ```
   esxcli software vib get --vibname epsec-mux
   ```

3. Resynchronisez le bus de messages d'hôte. VMware conseille à tous les clients de procéder à une resynchronisation après une mise à niveau.

   Vous pouvez utiliser l'appel API suivant pour effectuer la resynchronisation sur chaque hôte.

   ```
   URL : https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>
   HTTP Method : POST

   Headers:

   Authorization : base64encoded value of username password
   Accept : application/xml
   Content-Type : application/xml
   ```

Mise à niveau de vSphere dans un environnement NSX

2

Si vous devez mettre à niveau NSX et vSphere, VMware recommande de mettre à niveau NSX avant vSphere.

Dans le tableau d'interopérabilité de VMware, vérifiez quelles versions de vSphere et d'ESXi sont compatibles avec votre installation NSX. Reportez-vous à la section http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Pour obtenir des instructions détaillées sur la mise à niveau de vSphere, consultez la version appropriée de la documentation vSphere, comprenant le *Guide de mise à niveau vSphere* et le *guide Installation et administration de VMware vSphere Update Manager*.

Lorsque vous mettez à niveau ESXi sur un hôte, vous devez également installer les nouveaux modules VIB de NSX sur l'hôte pour assurer la compatibilité avec la nouvelle version ESXi. Les charges de travail NSX ne peuvent pas s'exécuter sur l'hôte mis à niveau tant que les modules VIB de NSX n'ont pas été mis à jour.

La procédure de mise à niveau d'ESXi lorsque NSX 6.3.x est installé peut varier selon la version d'ESXi depuis laquelle ou vers laquelle vous effectuez la mise à niveau.

Tableau 2-1. Procédure de mise à niveau d'ESXi lorsque NSX 6.3.x est installé

Type de mise à niveau de l'hôte	Exigences concernant l'utilisation du mode de maintenance	Exigences concernant le redémarrage de l'hôte
ESXi 5.5 vers ESXi 6.0. Reportez-vous à la section Effectuer une mise à niveau vers ESXi 6.0 dans un environnement NSX.	L'hôte doit rester en mode de maintenance jusqu'à la fin de la mise à niveau d'ESXi et des modules VIB NSX associés.	Le redémarrage est nécessaire durant la mise à niveau d'ESXi. Le redémarrage est nécessaire durant la mise à niveau des modules VIB NSX associés.
ESXi 5.5 vers ESXi 6.5. Reportez-vous à la section Effectuer une mise à niveau vers ESXi 6.5 dans un environnement NSX.	L'hôte peut quitter le mode de maintenance après la mise à niveau d'ESXi. La fonction vMotion des VM vers les commutateurs vSphere Distributed Switches préparés pour VXLAN est bloquée sur l'hôte mis à niveau tant que les modules VIB ultérieurs de NSX n'ont pas été mis à niveau.	Le redémarrage est nécessaire durant la mise à niveau d'ESXi. Le redémarrage est nécessaire durant la mise à niveau des modules VIB NSX associés.
ESXi 6.0 vers ESXi 6.5 Reportez-vous à la section Effectuer une mise à niveau vers ESXi 6.5 dans un environnement NSX.	L'hôte peut quitter le mode de maintenance après la mise à niveau d'ESXi. La fonction vMotion des VM vers les commutateurs vSphere Distributed Switches préparés pour VXLAN est bloquée sur l'hôte mis à niveau tant que les modules VIB ultérieurs de NSX n'ont pas été mis à niveau.	Le redémarrage est nécessaire durant la mise à niveau d'ESXi. Le redémarrage n'est pas nécessaire durant la mise à niveau des modules VIB NSX associés.

Ce chapitre contient les rubriques suivantes :

- Effectuer une mise à niveau vers ESXi 6.0 dans un environnement NSX
- Effectuer une mise à niveau vers ESXi 6.5 dans un environnement NSX
- Redéployer Guest Introspection après une mise à niveau d'ESXi

Effectuer une mise à niveau vers ESXi 6.0 dans un environnement NSX

Les VIB NSX dépendent de la version d'ESXi installée sur l'hôte. Si vous mettez à niveau ESXi, vous devez installer de nouveaux VIB NSX appropriés pour la nouvelle version d'ESXi.

Les VIB de NSX installés dépendent des versions d'ESXi et de NSX. Si NSX 6.3.3 ou version ultérieure est installé, et si vous effectuez la mise à niveau d'ESXi 5.5 vers la version 6.0, les VIB esx-vsip et esx-vxlan sont supprimés et remplacés par le VIB esx-nsxv.

Version d'ESXi	Version de NSX	VIB installés
5.5	N'importe quelle version 6.3.x	■ esx-vsip ■ esx-vxlan
6.0 ou une version ultérieure	6.3.2 ou une version antérieure	■ esx-vsip ■ esx-vxlan
6.0 ou une version ultérieure	6.3.3 ou une version ultérieure	■ esx-nsxv

Important Vous devez vous assurer que l'hôte reste en mode de maintenance pendant toute la procédure de mise à niveau pour éviter que DRS ou vMotion déplace les machines virtuelles sur l'hôte avant la fin de la procédure.

Conditions préalables

- Dans le tableau d'interopérabilité de VMware, vérifiez quelles versions de vSphere et d'ESXi sont compatibles avec votre installation NSX. Reportez-vous à la section http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
- Pour obtenir des instructions détaillées sur la mise à niveau de vSphere, consultez la version appropriée de la documentation vSphere, comprenant le *Guide de mise à niveau vSphere* et le *guide Installation et administration de VMware vSphere Update Manager*.
- Vérifiez que les systèmes Platform Services Controller et vCenter Server sont mis à niveau vers la nouvelle version de vSphere.
- Assurez-vous que les noms de domaine complets de tous vos hôtes peuvent être résolus.
- Si DRS est désactivé, mettez les machines virtuelles hors tension ou déplacez-les manuellement (fonction vMotion) avant de lancer la mise à niveau.
- Si DRS est activé, les machines virtuelles en cours d'exécution sont automatiquement déplacées pendant la mise à niveau du cluster d'hôtes. Assurez-vous que DRS est compatible avec votre environnement avant de lancer la mise à niveau.
  - Vérifiez que DRS est activé sur les clusters d'hôtes.
  - Vérifiez que la fonction vMotion fonctionne correctement.
  - Vérifiez l'état de connexion des hôtes avec vCenter.
  - Vérifiez que chaque cluster d'hôtes comporte au moins trois hôtes ESXi. Lors de la mise à niveau de NSX, le risque de problèmes de contrôle d'admission DRS est plus élevé pour les clusters qui ne contiennent qu'un ou deux hôtes. Pour que la mise à niveau de NSX aboutisse, VMware recommande d'inclure au moins trois hôtes dans chaque cluster d'hôtes. Si un cluster contient moins de trois hôtes, il est recommandé de les évacuer manuellement.
  - Dans un petit cluster contenant seulement deux ou trois hôtes, si vous avez créé des règles d'anti-affinité indiquant que certaines machines virtuelles doivent résider sur des hôtes distincts, ces règles peuvent empêcher DRS de déplacer les machines virtuelles pendant la mise à niveau. Ajoutez des hôtes au cluster ou désactivez les règles d'anti-affinité pendant la mise à niveau et

réactivez-les une fois l'opération terminée. Pour désactiver une règle d'anti-affinité, accédez à **Hôtes et clusters (Hosts and Clusters) > *Cluster* > Gérer (Manage) > Paramètres (Settings) > Règles de VM/VM (VM/Host Rules)**. Modifiez la règle et désélectionnez **Activer une règle (Enable rule)**.

Procédure

- Pour chaque hôte devant être mis à niveau, procédez comme suit.
  a. Placez l'hôte en mode de maintenance.

     Si DRS est activé sur le cluster, DRS tente de déplacer les VM sur d'autres hôtes. Si DRS échoue pour une raison quelconque, vous devrez peut-être déplacer les VM manuellement, puis placer l'hôte en mode de maintenance.

  b. Mettez à niveau ESXi sur l'hôte.

     Redémarrez l'hôte à la fin de la mise à niveau d'ESXi.

  c. Si l'hôte présente l'état `Non connecté` après le redémarrage, connectez-le. Cliquez avec le bouton droit sur l'hôte et sélectionnez **Connexion (Connection) > Connecter (Connect)**.

  d. Accédez à **Networking & Security > Installation > Préparation de l'hôte (Host Preparation)**.

  e. Sélectionnez l'hôte sur lequel vous avez mis à niveau ESXi. Le Statut de l'installation indique **Non prêt (Not Ready)**.

  f. Cliquez sur **Actions > Résoudre (Resolve)** pour effectuer la mise à jour des modules VIB de NSX.

     Les modules VIB de NSX sont installés sur l'hôte, qui redémarre.

  g. Une fois que l'hôte a redémarré, quittez le mode de maintenance.

Pour vérifier que les VIB sont à jour, allez sur la ligne de commande de l'hôte et exécutez la commande `esxcli software vib list`. La première partie de la version du VIB correspond à la version d'ESXi pour le VIB.

Par exemple, après la mise à niveau vers ESXi 6.0 avec NSX 6.3.2 ou version antérieure :

```
[root@host-1:~] esxcli software vib list
...
esx-vsip    6.0.0-0.0.XXXXXXX    VMware  VMwareCertified   2017-01-23
esx-vxlan   6.0.0-0.0.XXXXXXX    VMware  VMwareCertified   2017-01-23
...
```

Après la mise à niveau vers ESXi 6.0 avec NSX 6.3.3 ou version ultérieure :

```
[root@host-2:~] esxcli software vib list
...
esx-nsxv    6.0.0-0.0.XXXXXXX    VMware  VMwareCertified   2017-08-10
...
```

Effectuer une mise à niveau vers ESXi 6.5 dans un environnement NSX

Les VIB NSX dépendent de la version d'ESXi installée sur l'hôte. Si vous mettez à niveau ESXi, vous devez installer de nouveaux VIB NSX appropriés pour la nouvelle version d'ESXi.

Lorsque vous effectuez une mise à niveau vers ESXi 6.5 depuis NSX 6.3.x, la fonction vMotion des VM vers les commutateurs vSphere Distributed Switches préparés pour VXLAN sur l'hôte mis à niveau est bloquée tant que les nouveaux modules VIB de NSX n'ont pas été installés.

VMware recommande l'utilisation de vSphere Upgrade Manager pour mettre à niveau les hôtes vers ESXi 6.5 dans un environnement NSX 6.3.x.

Quelle que soit la méthode de mise à niveau d'ESXi, vous devez suivre ce workflow. Procédez comme suit, sur chaque hôte individuellement :

1 Mettez à niveau ESXi.

   À la fin de la mise à niveau d'ESXi, l'hôte sort du mode de maintenance, mais vous devez attendre la fin de l'étape suivante pour déplacer les VM connectées aux commutateurs logiques vers l'hôte.

2 Mettez à niveau les VIB NSX.

   Lorsque les VIB sont mis à niveau et que l'hôte est sorti du mode de maintenance, vous pouvez déplacer les VM connectées aux commutateurs logiques vers l'hôte.

Important Vous devez mettre les hôtes à niveau l'un après l'autre. Ne sélectionnez pas de cluster ni de centre de données pour effectuer une correction lorsque vous effectuez la mise à niveau vers ESXi.

Les VIB de NSX installés dépendent des versions d'ESXi et de NSX. Si NSX 6.3.3 ou version ultérieure est installé, et si vous effectuez la mise à niveau d'ESXi 5.5 vers la version 6.5, les VIB esx-vsip et esx-vxlan sont supprimés et remplacés par le VIB esx-nsxv.

Version d'ESXi	Version de NSX	VIB installés
5.5	N'importe quelle version 6.3.x	■ esx-vsip ■ esx-vxlan
6.0 ou une version ultérieure	6.3.2 ou une version antérieure	■ esx-vsip ■ esx-vxlan
6.0 ou une version ultérieure	6.3.3 ou une version ultérieure	■ esx-nsxv

Conditions préalables

- Vérifiez que NSX 6.3.x est installé.

- Dans le tableau d'interopérabilité de VMware, vérifiez quelles versions de vSphere et d'ESXi sont compatibles avec votre installation NSX. Reportez-vous à la section http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

  Important NSX 6.3.x n'est pas interopérable avec la version initiale d'ESXi 6.5. Vous devez procéder à la mise à niveau vers ESXi 6.5.0a ou une version ultérieure pour rendre cette version compatible avec NSX 6.3.0. Pour obtenir les informations d'interopérabilité les plus récentes, consultez le tableau d'interopérabilité.

- Pour obtenir des instructions détaillées sur la mise à niveau de vSphere, consultez la version appropriée de la documentation vSphere, comprenant le *Guide de mise à niveau vSphere* et le *guide Installation et administration de VMware vSphere Update Manager*.
- Vérifiez que les systèmes Platform Services Controller et vCenter Server sont mis à niveau vers la nouvelle version de vSphere.
- Vérifiez que vSphere Update Manager est installé et configuré.
- Assurez-vous que les noms de domaine complets de tous vos hôtes peuvent être résolus.
- Si DRS est désactivé, mettez les machines virtuelles hors tension ou déplacez-les manuellement (fonction vMotion) avant de lancer la mise à niveau.
- Si DRS est activé, les machines virtuelles en cours d'exécution sont automatiquement déplacées pendant la mise à niveau du cluster d'hôtes. Assurez-vous que DRS est compatible avec votre environnement avant de lancer la mise à niveau.
  - Vérifiez que DRS est activé sur les clusters d'hôtes.
  - Vérifiez que la fonction vMotion fonctionne correctement.
  - Vérifiez l'état de connexion des hôtes avec vCenter.
  - Vérifiez que chaque cluster d'hôtes comporte au moins trois hôtes ESXi. Lors de la mise à niveau de NSX, le risque de problèmes de contrôle d'admission DRS est plus élevé pour les clusters qui ne contiennent qu'un ou deux hôtes. Pour que la mise à niveau de NSX aboutisse, VMware recommande d'inclure au moins trois hôtes dans chaque cluster d'hôtes. Si un cluster contient moins de trois hôtes, il est recommandé de les évacuer manuellement.
  - Dans un petit cluster contenant seulement deux ou trois hôtes, si vous avez créé des règles d'anti-affinité indiquant que certaines machines virtuelles doivent résider sur des hôtes distincts, ces règles peuvent empêcher DRS de déplacer les machines virtuelles pendant la mise à niveau. Ajoutez des hôtes au cluster ou désactivez les règles d'anti-affinité pendant la mise à niveau et réactivez-les une fois l'opération terminée. Pour désactiver une règle d'anti-affinité, accédez à **Hôtes et clusters (Hosts and Clusters) > *Cluster* > Gérer (Manage) > Paramètres (Settings) > Règles de VM/VM (VM/Host Rules)**. Modifiez la règle et désélectionnez **Activer une règle (Enable rule)**.

Procédure

1 Dans vSphere Web Client, accédez à **Update Manager > *Objet Update Manager* (*Update Manager Object*) > Gérer (Manage)**.

2 Suivez les instructions *Importation d'images de mises à niveau d'hôte et création de lignes de base de mises à niveau d'hôtes* pour importer une image de mise à niveau d'hôte et créer une ligne de base de mise à niveau d'hôtes.

   a Cliquez sur l'onglet **Images ESXi (ESXi Images)**, puis sur **Importer l'image ESXi (Import ESXi Image)** et choisissez l'image à télécharger.

   b Cliquez sur l'onglet **Lignes de base d'hôte (Host Baselines)**, puis sur **Nouvelle ligne de base (New Baseline)**. Aidez-vous de l'Assistant Nouvelle ligne de base pour créer une ligne de base, et sélectionnez **Mise à niveau d'hôte (Host Upgrade)** comme type de ligne de base.

3 Mettez les hôtes à niveau l'un après l'autre. Répétez ces étapes pour chaque hôte.

   a Accédez à **Hôtes et clusters (Hosts and Clusters)** et sélectionnez l'hôte à mettre à niveau. Ne sélectionnez pas de cluster ni de centre de données.

   b Cliquez avec le bouton droit de la souris sur l'hôte et sélectionnez **Update Manager > Attacher une ligne de base... (Attach Baseline...)**. Aidez-vous de l'Assistant Attacher une ligne de base ou un groupe de lignes de base pour sélectionner une ligne de base. Pour obtenir des informations détaillées, consultez *Attachement de lignes de base et de groupes de lignes de base à des objets* dans la documentation vSphere.

   c Cliquez avec le bouton droit de la souris sur l'hôte et sélectionnez **Update Manager > Corriger... (Remediate...)**. Aidez-vous de l'Assistant Corriger pour sélectionner une ligne de base. Pour obtenir des informations détaillées, consultez *Correction des hôtes par rapport aux lignes de base de mise à niveau* dans la documentation vSphere.

   d Si l'hôte présente l'état `Non connecté` après le redémarrage, connectez-le. Cliquez avec le bouton droit sur l'hôte et sélectionnez **Connexion (Connection) > Connecter (Connect)**.

   e Pour vérifier que la mise à niveau est terminée, cliquez avec le bouton droit de la souris sur l'hôte et sélectionnez **Update Manager > Rechercher les mises à jour... (Scan for Updates...)**. Cochez la case **Mises à niveau (Upgrades)** pour rechercher la conformité de mise à niveau. Si l'État de conformité est Conforme, la mise à niveau est terminée.

      Pour obtenir des informations détaillées, consultez *Lancement manuel de l'analyse des hôtes ESXi* dans la documentation vSphere.

   f Accédez à **Networking & Security > Installation > Préparation de l'hôte (Host Preparation)**.

g Repérez l'hôte sur lequel vous avez mis à niveau ESXi. Le Statut de l'installation indique **Non prêt (Not Ready)**.

Cliquez sur **Non prêt (Not Ready)** pour afficher plus d'informations.

h Sélectionnez l'hôte et cliquez sur **Actions > Résoudre (Resolve)** pour déclencher l'installation des modules VIB de NSX.

Si vous effectuez une mise à niveau à partir d'ESXi 5.5 et que DRS est activé sur le cluster, DRS tente de redémarrer l'hôte d'une manière contrôlée permettant aux machines virtuelles de continuer à fonctionner. Si DRS échoue pour une raison quelconque, l'action **Résoudre (Resolve)** s'arrête. Dans ce cas, vous devrez éventuellement déplacer les machines virtuelles manuellement, puis tenter de nouveau l'action **Résoudre (Resolve)**, ou placer l'hôte en mode de maintenance et redémarrer manuellement.

Si vous effectuez une mise à niveau à partir d'ESXi 6.0 et que DRS est activé sur le cluster, DRS tente de mettre l'hôte en mode de maintenance d'une manière contrôlée permettant aux machines virtuelles de continuer à fonctionner. Si DRS échoue pour une raison quelconque, l'action **Résoudre (Resolve)** s'arrête. Dans ce cas, vous devrez éventuellement déplacer les machines virtuelles manuellement, puis tenter de nouveau l'action **Résoudre (Resolve)**, ou placer manuellement l'hôte en mode de maintenance.

Important Si vous effectuez une mise à niveau depuis ESXi 6.0, et que vous mettez manuellement un hôte en mode de maintenance pour installer les modules VIB de l'hôte, vous devez vérifier que l'installation des modules VIB de l'hôte est terminée avant de sortir l'hôte du mode de maintenance. L'**État de préparation de l'hôte (Host Preparation)** indique `Installation en cours`, même si l'installation est terminée.

1 Consultez le volet Tâches récentes de vSphere Web Client et vérifiez que toutes les tâches d'installation sont terminées.

2 Allez sur la ligne de commande de l'hôte et exécutez la commande `esxcli software vib list`. La première partie de la version du VIB correspond à la version d'ESXi pour le VIB.

Par exemple, après la mise à niveau vers ESXi 6.5 avec NSX 6.3.2 ou version antérieure :

```
[root@host-1:~] esxcli software vib list
...
esx-vsip    6.5.0-0.0.XXXXXXX    VMware  VMwareCertified   2017-01-23
esx-vxlan   6.5.0-0.0.XXXXXXX    VMware  VMwareCertified   2017-01-23
...
```

Après la mise à niveau vers ESXi 6.5 avec NSX 6.3.3 ou version ultérieure :

```
[root@host-2:~] esxcli software vib list
...
esx-nsxv    6.5.0-0.0.XXXXXXX    VMware  VMwareCertified   2017-08-10
...
```

Redéployer Guest Introspection après une mise à niveau d'ESXi

Si vous mettez à niveau ESXi sur un cluster où Guest Introspection est déployé, vous devez vérifier dans l'onglet Déploiements de services si Guest Introspection a besoin d'être redéployé.

Important Il est nécessaire de procéder à la mise à niveau d'ESXi et des modules VIB NSX associés avant de redéployer Guest Introspection.

Conditions préalables

- Effectuez la mise à niveau d'ESXi.
- Effectuez la mise à niveau des modules VIB de NSX (préparation de l'hôte) après la mise à niveau d'ESXi.

Procédure

1. Connectez-vous à vSphere Web Client.
2. Cliquez sur **Networking & Security**, puis sur **Installation**.
3. Cliquez sur l'onglet **Déploiements de services (Service Deployments)**.
4. Si la colonne État de l'installation indique `Réussi`, le redéploiement n'est pas nécessaire.
5. Si la colonne État de l'installation indique Non prêt, cliquez sur le lien **Non prêt (Not Ready)**. Cliquez sur **Tout résoudre (Resolve all)** pour redéployer Guest Introspection.